IBM Spectrum Protect
8.1.12

Bandspeicherlösung

Anmerkung:

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen” auf Seite 239 gelesen werden.

Impressum

Diese Ausgabe bezieht sich auf Version 8, Release 1, Modifikation 12 von IBM Spectrum Protect (Produktnummern 5725-W98, 5725-W99, 5725-X15) und auf alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Inhaltsverzeichnis

Zu dieser Veröffentlichung

In dieser Veröffentlichung werden Informationen zur Planung, Implementierung, Überwachung und Ausführung einer Datenschutzlösung, die Best Practices von IBM Spectrum Protect verwendet, bereitgestellt.

Zielgruppe

Dieses Handbuch richtet sich an alle Personen, die als Administrator für IBM Spectrum Protect registriert sind. Ein einzelner Administrator kann IBM Spectrum Protect verwalten oder die Zuständigkeit für Verwaltungsaufgaben kann auf mehrere Personen übertragen werden.

Sie sollten mit dem Betriebssystem, unter dem der Server ausgeführt wird, und den Kommunikationsprotokollen vertraut sein, die für die Client- oder Serverumgebung erforderlich sind. Außerdem müssen Sie über Kenntnisse in den Speicherverwaltungspraktiken Ihres Unternehmens verfügen. Sie müssen beispielsweise wissen, wie gegenwärtig Workstationdateien gesichert und Speichereinheiten verwendet werden.

Veröffentlichungen

Die IBM Spectrum Protect-Produktfamilie umfasst IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases und verschiedene andere Speicherverwaltungsprodukte von IBM®.

Die IBM Produktdokumentation finden Sie unter IBM Knowledge Center.

Neuerungen in diesem Release

In diesem Release von IBM Spectrum Protect werden neue Funktionen und Aktualisierungen eingeführt.

Eine Liste der neuen Funktionen und Aktualisierungen in diesem Release finden Sie in den folgenden Abschnitten:

- Neuerungen für Serverkomponenten
- Neuerungen für Clientkomponenten

Änderungen, die in der Dokumentation vorgenommen wurden, sind durch einen vertikalen Strich (|) am Rand gekennzeichnet.

Teil 1. Planung für eine bandbasierte Datenschutzlösung

Führen Sie die Planung für eine Datenschutzlösung durch, die Platte-Platte-Band-Sicherungsoperationen und Sicherungsoperationen von Platte auf Band zur Optimierung des Speichers umfasst.

Planungsroadmap

Führen Sie die Planung für die Bandspeicherlösung durch, indem Sie das Architekturlayout in Abbildung 1 auf Seite 1 überprüfen und dann die Roadmap-Tasks ausführen, die auf die Abbildung folgen.

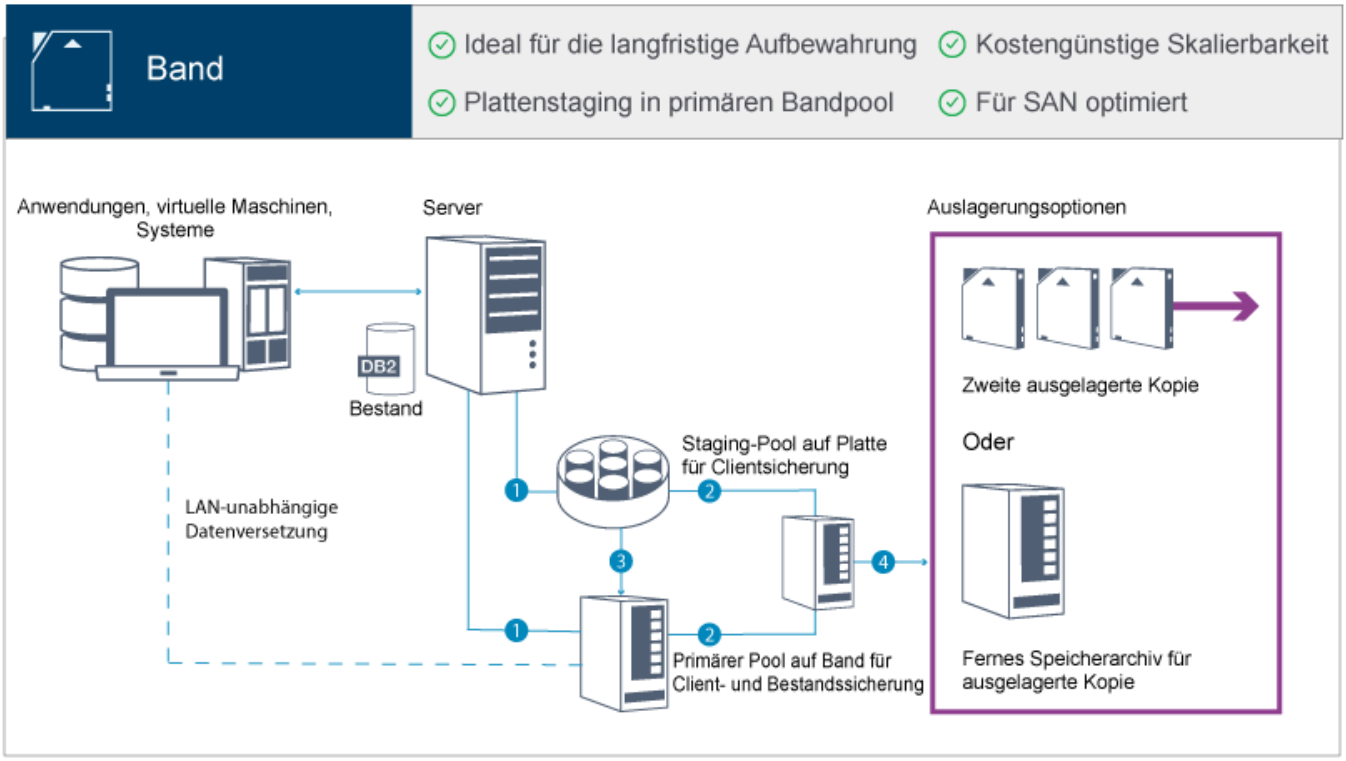


Abbildung 1. Bandspeicherlösung

Bei dieser Datenschutzkonfiguration verwendet der Server sowohl Platten- als auch Bandspeicherhardware. Es wird Speicherpoolstaging verwendet, bei dem Clientdaten anfänglich in Plattenspeicherpools gespeichert und dann später in Bandspeicherpools umgelagert werden. Für die Wiederherstellung nach einem Katastrophenfall können Banddatenträger an einem anderen Standort gespeichert werden. Auslagerungsoptionen umfassen den physischen Transport einer zweiten Kopie an einen anderen Standort durch einen Kurier oder das Schützen von Kopien an einem anderen Standort durch elektronisches Vaulting in einem fernen Speicherarchiv.

Tipps:

- In der beschriebenen Lösung werden Daten aus Plattenspeicherpools in Bandspeicherpools *umgelagert*. Anstatt die Daten umzulagern, können Sie jedoch die Band-Tiering-Funktion verwenden, die in IBM Spectrum Protect Version 8.1.8 eingeführt wurde. Mit dieser Funktion können Sie Daten automatisch mit Tiering aus Verzeichniscontainerspeicherpools auf Platte in Bandspeicher versetzen. Sie können angeben, dass alle Daten auf der Basis eines angegebenen Altersschwellenwerts mit Tiering versetzt werden oder dass nur inaktive Daten auf der Basis eines Altersschwellenwerts mit Tiering versetzt werden. Weitere Informationen zum Versetzen von Daten mit Tiering in Bandspeicher finden Sie in Daten mit Tiering in Cloud- oder Bandspeicher versetzen.

- Die beschriebene Lösung umfasst keine Knotenreplikation. Wenn die Knotenreplikation zum Sichern eines Speicherpools von Platte auf Platte verwendet werden soll, müssen Sie sicherstellen, dass die Replikationsoperation abgeschlossen ist, bevor Daten von Platte auf Band umgelagert werden. Sie können die Knotenreplikation auch verwenden, um einen Speicherpool auf einer lokalen Bandeinheit in einem Kopienspeicherpool auf einer lokalen Bandeinheit zu sichern.

Um die Planung für eine bandbasierte Lösung durchzuführen, führen Sie die folgenden Tasks aus:

1. Erfüllen Sie die Systemvoraussetzungen für Hardware und Software.
2. Notieren Sie die Werte für Ihre Systemkonfiguration in den Arbeitsblättern zur Planung.
3. Führen Sie die Planung für den Plattenspeicher durch.
4. Führen Sie die Planung für den Bandspeicher durch.
5. Führen Sie die Planung für die Sicherheit durch.

Planungsvoraussetzungen für Bänder

Bevor Sie eine Bandspeicherlösung implementieren, lesen Sie die allgemeinen Richtlinien zu Systemvoraussetzungen. Legen Sie fest, ob Daten auf Platte und/oder Band gesichert werden sollen.

Netzbandbreite
Das Netz muss über genügend Bandbreite für die erwarteten Datenübertragungen zwischen dem Client und dem Server sowie für die standortübergreifenden Zurückschreibungsoperationen verfügen, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind. Verwenden Sie ein Speicherbereichsnetz (SAN) für Datenübertragungen zwischen dem Server, Platteneinheiten und Bandeinheiten. Weitere Informationen finden Sie in „Hardwarevoraussetzungen” auf Seite 3.

Datenumlagerung
Lagern Sie täglich alle Daten von Platte auf Band um. Geben Sie die Einheitenklasse FILE für plattenbasierte Speicherpools an. Planen Sie die Umlagerung, um zu steuern, wann die Verarbeitung erfolgt. Um die automatische Umlagerung auf der Basis des Umlagerungsschwellenwerts zu verhindern, geben Sie den Wert 100 für den Parameter **HIGHMIG** und den Wert 0 für den Parameter **LOWMIG** an, wenn Sie den Befehl **DEFINE STGPOOL** ausgeben. Es müssen immer mindestens 20 % der Bandlaufwerke für Zurückschreibungsoperationen verfügbar bleiben. Um bis zu 80 % der verfügbaren Bandlaufwerke zu verwenden und den Durchsatz zu verbessern, geben Sie den Parameter **MIGPROCESS** an.

Berücksichtigen Sie, abhängig vom Typ der Daten, die umgelagert werden, die folgenden Informationen:

- Verwenden Sie Bänder, um Daten von Clients zu sichern, die über große Objekte, wie beispielsweise Datenbanken, verfügen.

  Tipp: Der Hersteller Ihres Bandlaufwerks kann Ihnen Auskunft über die Größe der Datenbank geben, die für das Schreiben auf Band geeignet ist.
- Verwenden Sie Platten, um Daten von Clients zu sichern, die über kleinere Objekte verfügen.
- Um Daten direkt auf Band zu sichern, verwenden Sie die LAN-unabhängige Datenversetzung. Weitere Informationen finden Sie in „LAN-unabhängige Datenversetzung konfigurieren” auf Seite 128.
- Sichern Sie keine virtuellen Maschinen auf Band. Verwenden Sie einen separaten plattenbasierten Speicherpool, der nicht in einen bandbasierten Speicherpool umgelagert wird. Weitere Informationen zur Unterstützung virtueller Maschinen finden Sie in and IBM Tivoli Storage Manager (TSM) guest support for Virtual Machines and Virtualization.

Speicherpoolkapazität
Stellen Sie sicher, dass immer genügend Speicherpoolkapazität für 2 Tage mit Clientsicherungen und ein Puffer von 20 % verfügbar ist. Möglicherweise müssen Sie Gesamtsicherungen für einige Tage planen, um sicherzustellen, dass genügend Speicherbereich im Speicherpool vorhanden ist.

Bandlaufwerke

Lesen Sie die Herstellerspezifikationen und schätzen Sie die Kapazität eines Bandlaufwerks. Bestimmen Sie die Größe des Speicherbereichs, der für Sicherungs- und Umlagerungsoperationen erforderlich ist. Reservieren Sie 20 % der Bandlaufwerke für Zurückschreibungsoperationen.

Zugehörige Informationen

MIGRATE STGPOOL (Speicherpool in den nächsten Speicherpool umlagern)

Systemvoraussetzungen für eine bandbasierte Lösung

Hardware- und Softwarevoraussetzungen werden für eine bandbasierte Speicherlösung mit einer Datenaufnahmerate von 14 TB pro Stunde bereitgestellt.

Lesen Sie die Informationen, um die Hardware- und Softwarevoraussetzungen für Ihre Speicherumgebung zu bestimmen. Unter Umständen müssen Sie auf der Basis Ihrer Systemgröße Anpassungen vornehmen.

Hardwarevoraussetzungen

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

Weitere Informationen zur Planung für Platteneinheiten finden Sie in Planung für Plattenspeicher.

Weitere Informationen zur Planung für Bandeinheiten finden Sie in Planung für Bandspeicher.

Die folgende Tabelle enthält Hardwaremindestvoraussetzungen für den Server und Speicher. Wenn Sie logische Partitionen (LPARs) oder Arbeitspartitionen (WPARs) verwenden, passen Sie die Netzvoraussetzungen an, um den Partitionsgrößen Rechnung zu tragen. Die Zahlen in der Tabelle basieren auf einer Datenaufnahmerate von 14 TB pro Stunde.

Hardwarekomponente	**Systemvoraussetzungen**
Serverprozessor	AIX 8 Prozessorkerne, 3,42 GHz oder schneller Verwenden Sie beispielsweise einen POWER8-prozessorbasierten Server. Linux Windows 16 Prozessorkerne, 2,0 GHz oder schneller Verwenden Sie beispielsweise einen Intel Xeon-Prozessor.
Serverspeicher	64 GB Arbeitsspeicher.
Netz	Gemäß der folgenden Größe werden etwa 14 TB Daten pro Stunde verwaltet: • 10 Gb Ethernet (mindestens vier Ports) • 8 Gb Fibre Channel-Adapter (mindestens vier Ports) Die Anzahl Ports ist vom Prozentsatz der täglichen Datenaufnahme in Plattenspeicherpools gegenüber Bandspeicher abhängig. Verwenden Sie separate Fibre Channel-Adapter für Band- und Plattendaten.

Hardwarekomponente	Systemvoraussetzungen

Speicher	**Platte**
	Geben Sie auf der Basis des Datenvolumens, das auf Platte geschrieben wird, die Anzahl Platten an, die erforderlich sind.
	Stellen Sie sicher, dass der Durchsatz der sequenziellen Ein-/Ausgabe des Speicherbereichsnetzes (SAN) mit dem Durchsatz der Ein-/Ausgabe für das Netz (siehe oben) übereinstimmt.
	Wenn Sie beispielsweise 10 TB Daten in einem 4-Stunden-Fenster sichern müssen, beträgt der Durchsatz ungefähr 700 MB pro Sekunde. In diesem Fall erfordert der Server ein Front-End-Netz (Pfad vom Client zum Server), das einen Mindestdurchsatz von 700 MB pro Sekunde unterstützt. Das Back-End-SAN (Pfad vom Server zur Speichereinheit) muss ebenfalls einen Mindestdurchsatz von 700 MB pro Sekunde unterstützen.
	Verwenden Sie zur Berechnung der erforderlichen Plattengeschwindigkeit die folgenden Formeln:
	`(Gesamtvolumen der täglichen Datenaufnahme - Volumen der täglichen Datenaufnahme direkt auf Band) ÷ (Anzahl Stunden für tägliche Clientsicherungsoperationen) = Megabyte der Datenaufnahme auf Platte pro Stunde`
	`(Megabyte der Datenaufnahme auf Platte pro Stunde) ÷ (3600 Sekunden pro Stunde) = Megabyte der Datenaufnahme pro Sekunde, die von der Plattentechnologie unterstützt werden müssen`
	Band
	Wählen Sie die Bandtechnologie aus, die für Ihre Geschäftsanforderungen am besten geeignet ist. Verwenden Sie beispielsweise IBM Linear Tape-Open-Bandlaufwerke (LTO-Bandlaufwerke) oder IBM TS1150-Bandlaufwerke. Stellen Sie sicher, dass genügend Mountpunkte für Clientsicherungsoperationen und für die Umlagerung vorhanden sind. Weitere Informationen zur Planung für Bandspeicher finden Sie in Planung für Bandspeicher. Eine Liste der unterstützten Bandeinheiten finden Sie im IBM Support Portal for IBM Spectrum Protect.
	Tipp: Um die Datenversetzung zu optimieren, verwenden Sie die LAN-unabhängige Datenversetzung.

SAN-E/A-Adapter	Trennen Sie die Platten- und Bandein-/ausgabe voneinander. Weitere Informationen zum Auswählen eines Adapters finden Sie in der Dokumentation für Brocade-Hardwareprodukte und für IBM Storwize-Speicherlösungen. **Platte** Verwenden Sie mindestens zwei Adapter. **Band** Verwenden Sie mindestens zwei Adapter.

Speicherbedarf für das Operations Center schätzen

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

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

Die Verwaltung des Operations Center auf dem IBM Spectrum Protect-Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen auf dem Hub-Server und allen Peripherieservern erfordert. Der Speicherbedarf auf dem Hub-Server für das Archivprotokoll ist höher, wenn der Hub-Server einen oder mehrere Peripherieserver überwacht. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr IBM Spectrum Protect-Server erfordert.

Speicherbereich in der Datenbank für das Operations Center

Das Operations Center benötigt ungefähr 4,4 GB Speicherbereich in der Datenbank pro 1000 Clients, die auf diesem Server überwacht werden. Diese Berechnung gilt sowohl für Hub-Server als auch für Peripherieserver in einer Konfiguration.

Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1000 Clients. Bei dieser Konfiguration sind insgesamt 5000 Clients auf den vier Servern vorhanden. Jeder der Peripherieserver erfordert 4,4 GB Speicherbereich in der Datenbank. Bei Peripherieservern der IBM Spectrum Protect Version 8.1.2 oder höher erfordert der Hub-Server 8,8 GB Speicherbereich in der Datenbank allein für die Überwachung seiner 2000 Clients:

```
(4,4 GB x 2) = 8,8 GB
```

Speicherbereich in der Datenbank für verwaltete Daten

Verwaltete Daten ist das Datenvolumen, das geschützt wird, einschließlich des Datenvolumens aller aufbewahrten Versionen.

- Bei Clienttypen, die immer inkrementelle Sicherungen ausführen, kann die folgende Formel zum Schätzen des Gesamtvolumens der verwalteten Daten verwendet werden:

  ```
  Front-End-Daten + (Front-End-Daten * Änderungsrate * (Aufbewahrungszeitraum - 1))
  ```

  Wenn Sie beispielsweise 100 TB Front-End-Daten sichern, einen Aufbewahrungszeitraum von 30 Tagen verwenden und eine Änderungsrate von 5 % haben, berechnen Sie das Gesamtvolumen der verwalteten Daten wie folgt:

  ```
  100 TB + (100 TB × 0,05 × (30-1)) = 245 TB Gesamtvolumen der verwalteten Daten
  ```

- Bei Clienttypen, die täglich Gesamtsicherungen ausführen, kann die folgende Formel zum Schätzen des Gesamtvolumens der verwalteten Daten verwendet werden:

  ```
  Front-End-Daten × Aufbewahrungszeitraum × (1 + Änderungsrate)
  ```

  Wenn Sie beispielsweise 10 TB Front-End-Daten sichern, einen Aufbewahrungszeitraum von 30 Tagen verwenden und eine Änderungsrate von 3 % haben, berechnen Sie das Gesamtvolumen der verwalteten Daten wie folgt:

  ```
  10 TB × 30 × (1 + 0,03) = 309 TB Gesamtvolumen der verwalteten Daten
  ```

  Unstrukturierte Daten; durchschnittliche Objektgröße: 4 MB

  Strukturierte Daten; durchschnittliche Objektgröße: 128 MB

  Unstrukturierte Daten; Anzahl Objekte =

  ```
  (245 TB × 1024 × 1024) / 4 MB = 64225280
  ```

  Strukturierte Daten; Anzahl Objekte =

  ```
  (309 TB × 1024 × 1024) / 128 MB = 2531328
  ```

  Gesamtzahl Objekte: 66756608

  Kosten der verwalteten Daten (1 KB pro Objekt) =

  ```
  (66756608 KB) / (1024 × 1024) = 63,66 GB
  ```

Planen Sie 20 % zusätzlichen Speicherbereich ein, damit Datenbanksysteme nicht 100 % ihrer Kapazität nutzen:

```
Gesamtbedarf des physischen Speicherbereichs in der Datenbank =
(Speicherbereich für verwaltete Daten + Speicherbereich für das Operations Center) ×
(1,20)
```

In diesem Beispiel würden Sie den Speicherbereich unter Verwendung der folgenden Zahlen berechnen:

```
(66,33 GB + 8,4 GB) × 1,20 = 76,41 GB
```

Speicherbereich für das Archivprotokoll

Das Operations Center verwendet alle 24 Stunden ungefähr 18 GB Speicherbereich für das Archivprotokoll pro Server für jeweils 1000 Clients, die auf diesem Server überwacht werden. Darüber hinaus wird für jeweils 1000 Clients, die auf Peripherieservern überwacht werden, zusätzlicher Speicherbereich für das Archivprotokoll auf dem Hub-Server benötigt. Für Peripherieserver der Version 8.1.2 oder höher beträgt dieses zusätzliche Volumen 1,2 GB Speicherbereich für das Archivprotokoll auf dem Hub-Server pro 100 Clients, die alle 24 Stunden überwacht werden.

Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1000 Clients. Bei dieser Konfiguration sind insgesamt 5000 Clients auf den vier Servern vorhanden. Sie können den Speicherbereich für das Archivprotokoll für den Hub-Server mithilfe der folgenden Formel berechnen:

```
((18 GB x 2) + (1,2 GB x 3)) = 39,6 GB Speicherbereich für das Archivprotokoll
```

Diese Schätzungen basieren auf dem Standardintervall von 5 Minuten zur Erfassung von Statusdaten. Wenn Sie das Erfassungsintervall von einmal alle 5 Minuten auf einmal alle 3 Minuten reduzieren, erhöht sich der Speicherbedarf. Die folgenden Beispiele zeigen die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten für eine Konfiguration, in der Peripherieserver der Version 8.1.2 oder höher überwacht werden:

- Hub-Server: im Bereich von 39,6 GB bis 66 GB
- Jeder Peripherieserver: im Bereich von 18 GB bis 30 GB

Ordnen Sie Speicherbereich für das Archivprotokoll zu, damit das Operations Center ohne Auswirkungen auf Serveroperationen unterstützt werden kann.

Softwarevoraussetzungen

Die Dokumentation für die bandbasierte IBM Spectrum Protect-Lösung umfasst Installations- und Konfigurationstasks für IBM AIX-, Linux®- und Microsoft Windows-Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

AIX-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	IBM AIX 7.1 Weitere Informationen zu Betriebssystemvoraussetzungen finden Sie in den IBM Spectrum Protect-Installationsinformationen.
Dienstprogramm gunzip	Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie die Installation oder das Upgrade für den IBM Spectrum Protect-Server ausführen. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und der Pfad zu diesem Dienstprogramm in der Umgebungsvariablen PATH definiert ist.

Softwaretyp	Softwaremindestvoraussetzungen
Dateisystemtyp	JFS2-Dateisysteme AIX-Systeme können ein großes Volumen an Dateisystemdaten zwischenspeichern, wodurch der Speicherplatz, der für Server- und IBM Db2-Prozesse erforderlich ist, reduziert werden kann. Um beim AIX-Server eine Auslagerung zu verhindern, verwenden Sie die Mountoption `rbrw` für das JFS2-Dateisystem. Für den Dateisystemcache wird weniger Speicher verwendet und für IBM Spectrum Protect ist mehr Speicher verfügbar. Verwenden Sie nicht die Mountoptionen für Dateisysteme, gleichzeitige E/A (CIO = Concurrent I/O) und direkte E/A (DIO = Direct I/O) für Dateisysteme, die die IBM Spectrum Protect-Datenbank, Protokolle oder Speicherpooldatenträger enthalten. Diese Optionen können eine Leistungsverschlechterung vieler Serveroperationen zur Folge haben. IBM Spectrum Protect und Db2 können, wenn dies von Vorteil ist, weiterhin DIO verwenden, IBM Spectrum Protect erfordert die Mountoptionen jedoch nicht, um die Vorteile dieser Verfahren selektiv nutzen zu können.
Andere Software	Korn-Shell (ksh)

Linux-Systeme

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

Windows-Systeme

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

Arbeitsblätter zur Planung

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

Jedes Arbeitsblatt unterstützt Sie bei den Vorbereitungen für unterschiedliche Teile der Systemkonfiguration mithilfe der Standardwerte:

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

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

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Weitere Informationen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	Linux AIX `/home/tsminst1/tsminst1` Windows `C:\tsminst1`		AIX 50 GB Linux Windows 25 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den Db2-Instanzeigner in Tabelle 2 auf Seite 10.
Verzeichnis für Serverinstallation	• Linux AIX `/` • Windows `C:`		AIX Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB Linux Windows Mindestspeicherbereich, der für das Verzeichnis erforderlich ist: 30 GB	

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines Serversystems (Forts.)				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Weitere Informationen**
Verzeichnis für Serverinstallation	`/usr`		AIX Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	AIX `/var`		AIX Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	AIX `/tmp`		AIX Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	AIX `/opt`		AIX Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 10 GB	
Verzeichnis für die aktive Protokolldatei	Linux AIX `/tsminst1/TSMalog` Windows `C:\tsminst1\TSMalog`		128 GB	Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB.
Verzeichnis für das Archivprotokoll	Linux AIX `/tsminst1/TSMarchlog` Windows `C:\tsminst1\TSMarchlog`		3 TB	

Verzeichnisse für die Datenbank	Linux AIX
	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	Windows
	`C:\tsminst1\TSMdbspace00`
	`C:\tsminst1\TSMdbspace01`
	`C:\tsminst1\TSMdbspace02`
	`C:\tsminst1\TSMdbspace03`
			Anweisungen zum Berechnen des Speicherbedarfs finden Sie in „Hardwarevoraussetzungen” auf Seite 3.	Erstellen Sie vier Dateisysteme für die Datenbank.

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines Serversystems (Forts.)

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Weitere Informationen

Verzeichnisse für Speicher	Linux AIX
	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
	Windows
	`C:\tsminst1\TSMfile00`
	`C:\tsminst1\TSMfile01`
	`C:\tsminst1\TSMfile02`
	`C:\tsminst1\TSMfile03`
	...
			Ermitteln Sie die minimale Gesamtkapazität für alle Verzeichnisse mithilfe der folgenden Berechnung:
			`Prozentsatz der täglich aufgenommenen Daten, die auf Platte geschrieben werden, + 20% = Minimale Gesamtkapazität`
				Die bevorzugte Methode ist die Definition mindestens eines Verzeichnisses für jede Bandeinheit.

Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Weitere Informationen
Db2-Instanzeigner	`tsminst1`		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 1 auf Seite 8 in einen anderen Wert geändert hatten, ändern Sie auch den Wert für den Db2-Instanzeigner.
Kennwort des Db2-Instanzeigners	Linux AIX `passw0rd` Windows `pAssW0rd`		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Primärgruppe für den Db2-Instanzeigner	Linux AIX `tsmsrvrs`		
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		
Serverkennwort	`passw0rd`		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	`admin`		

Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect (Forts.)

Element	Standardwert	Eigener Wert	Weitere Informationen
Kennwort für die Administrator-ID	`passw0rd`		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Startzeit des Zeitplans	`23:00`		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. In diesem Handbuch wird 23:00 Uhr als Startzeit für Clientsicherungsoperationen vorgeschlagen.

Tabelle 3. Arbeitsblatt für die Bandkonfiguration			
Element	**Standardwert**	**Eigener Wert**	**Weitere Informationen**
Dateien für automatische Einheiten	IBM Einheiten mit einem IBM Bandeinheitentreiber: • AIX `/dev/smcX` • Linux `/dev/IBMchangerX` • Windows `ChangerX` Einheiten eines anderen Herstellers als IBM mit einem IBM Spectrum Protect-Einheitentreiber: • AIX `/dev/lbX` • Linux `/dev/tsmscsi/lbX` • Windows `lbA.B.C.D`		Um die Dateien für Speicherarchiveinheiten manuell zu definieren, verwenden Sie die folgenden Befehle: • **DEFINE LIBRARY** • **DEFINE DRIVE** • **DEFINE PATH** Für SCSI-Einheiten können Sie den Befehl **PERFORM LIBACTION** verwenden, um alle Laufwerke und zugehörigen Pfade für ein einzelnes Speicherarchiv in einem einzigen Schritt zu definieren. Um diesen Befehl zum Definieren aller Laufwerke und Pfade verwenden zu können, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein.
Bandlaufwerke	IBM Einheiten mit einem IBM Bandeinheitentreiber: • AIX `/dev/rmtX` • Linux `/dev/IBMtapeX` • Windows `TapeX` Einheiten eines anderen Herstellers als IBM mit einem IBM Spectrum Protect-Einheitentreiber: • AIX `/dev/mtX` • Linux `/dev/tsmscsi/mtX` • Windows `mtA.B.C.D`		

Planung für Plattenspeicher

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

Speicherhardwareeinheiten haben unterschiedliche Kapazitäts- und Leistungsmerkmale, die festlegen, wie die Einheiten effizient mit IBM Spectrum Protect verwendet werden können. Die folgenden Richtlinien

stellen eine allgemeine Anleitung zur Auswahl der für Ihre Lösung geeigneten Speicherhardware und Konfiguration dar.

Datenbank, aktive Protokolldatei und Archivprotokoll

- Verwenden Sie eine Solid-State-Platte (SSD) oder eine schnelle Platte mit 15.000 Umdrehungen pro Minute für die IBM Spectrum Protect-Datenbank und die aktive Protokolldatei.
- Verwenden Sie beim Erstellen von Arrays für die Datenbank RAID-Stufe 5.
- Verwenden Sie separate Platten für den Speicher für das Archivprotokoll und die Datenbanksicherung.

Speicherpool

Verwenden Sie RAID-Stufe 6 für Speicherpoolarrays, um bei Verwendung von Typen großer Platten Schutz vor dem Ausfall von zwei Laufwerken hinzuzufügen.

Planung der Speicherarrays

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

Sie entwerfen Speicherarrays mit einer Größe und mit Leistungsmerkmalen, die für eine der IBM Spectrum Protect-Serverspeicherkomponenten, wie beispielsweise die Serverdatenbank oder einen Speicherpool, geeignet sind. Bei der Speicherplanungsaktivität müssen Laufwerktyp, RAID-Stufe, Anzahl Laufwerke und Anzahl Ersatzlaufwerke usw. berücksichtigt werden. In den Lösungskonfigurationen enthalten Speichergruppen RAID-Arrays im internen Speicher und bestehen aus mehreren physischen Platten, die im System als logische Datenträger dargestellt werden. Wenn Sie das Plattenspeichersystem konfigurieren, erstellen Sie zunächst Speichergruppen oder Datenspeicherpools und dann Speicherarrays in den Gruppen.

Aus den Speichergruppen erstellen Sie Datenträger oder LUNs. Die Speichergruppe definiert, welche Platten den Speicher bereitstellen, der den Datenträger bildet. Wenn Sie Datenträger erstellen, ordnen Sie diese vollständig zu. Typen schnellerer Platten werden zum Aufnehmen der Datenbankdatenträger und der Datenträger für die aktive Protokolldatei verwendet. Typen langsamerer Platten können für die Speicherpool-, die Archivprotokoll- und Datenbanksicherungsdatenträger verwendet werden. Wenn Sie einen kleineren Plattenspeicherpool verwenden, um Daten zwischenzuspeichern, müssen Sie möglicherweise schnellere Platten verwenden, um die tägliche Auslastungsleistung in Bezug auf Datenaufnahme und Datenumlagerung handhaben zu können.

In Tabelle 4 auf Seite 13 und Tabelle 5 auf Seite 14 sind die Layoutanforderungen für die Speichergruppen- und Datenträgerkonfiguration beschrieben.

Tabelle 4. Komponenten der Speichergruppenkonfiguration

Komponente	**Details**
Serverspeicheranforderung	Angabe, wie der Speicher vom Server verwendet wird.
Plattentyp	Größe und Geschwindigkeit für den Plattentyp der für die Speicheranforderung verwendet wird.
Anzahl Platten	Anzahl jedes Plattentyps, der für die Speicheranforderung benötigt wird.
Hot-Spare-Kapazität	Anzahl Platten, die als Ersatzspeicher (Spare) für die Übernahme bei Plattenfehlern reserviert sind.
RAID-Stufe	Stufe des RAID-Arrays, das für logischen Speicher verwendet wird. Die RAID-Stufe definiert den Redundanztyp, der von dem Array bereitgestellt wird, beispielsweise 5 oder 6.
Anzahl RAID-Arrays	Anzahl RAID-Arrays, die erstellt werden sollen.
DDMs pro RAID-Array	Anzahl Plattenlaufwerkmodule (DDMs = Disk Drive Modules), die in jedem der RAID-Arrays verwendet werden sollen.

Tabelle 4. Komponenten der Speichergruppenkonfiguration (Forts.)	
Komponente	**Details**
Verwendbare Größe pro RAID-Array	Größe, die für die Datenspeicherung in jedem RAID-Array verfügbar ist, abzüglich des Speicherbereichs, der aufgrund von Redundanz verloren geht.
Insgesamt verwendbare Größe	Gesamtgröße, die in den RAID-Arrays für die Datenspeicherung verfügbar ist: `Anzahl x Verwendbare Größe`
Vorgeschlagene Namen für Speichergruppen und -arrays	Bevorzugter Name für MDisks und MDisk-Gruppen.
Verwendung	Serverkomponente, die einen Teil der physischen Platte verwendet.

Tabelle 5. Komponenten der Datenträgerkonfiguration	
Komponente	**Details**
Serverspeicheranforderung	Anforderung, für die die physische Platte verwendet wird.
Datenträgername	Eindeutiger Name, der einem bestimmten Datenträger zugeordnet wird.
Speichergruppe	Name der Speichergruppe, aus der der Speicherbereich zum Erstellen des Datenträgers angefordert wird.
Größe	Größe jedes Datenträgers.
Geplanter Server-Mountpunkt	Verzeichnis auf dem Serversystem, in dem der Datenträger bereitgestellt wird.
Anzahl	Anzahl Datenträger, die für eine bestimmte Anforderung erstellt werden sollen. Verwenden Sie für jeden Datenträger, der für dieselbe Anforderung erstellt wird, denselben Benennungsstandard.
Verwendung	Serverkomponente, die einen Teil der physischen Platte verwendet.

Beispiele

Konfigurationsbeispiele für Speichergruppen und Datenträger sind über den folgenden Link verfügbar: Beispielarbeitsblätter für die Planung von Speicherarrays. Die Beispiele zeigen die Planung des Speichers für verschiedene Servergrößen. In den Beispielkonfigurationen besteht eine Eins-zu-eins-Zuordnung zwischen Platten und Speichergruppen. Sie können die Beispiele herunterladen und die Arbeitsblätter editieren, um die Speicherkonfiguration für Ihren Server zu planen.

Planung für Bandspeicher

Bestimmen Sie, welche Bandeinheiten verwendet werden sollen und wie diese zu konfigurieren sind. Um die Systemleistung zu optimieren, planen Sie die Verwendung schneller Bandeinheiten mit hoher Speicherkapazität. Stellen Sie genügend Bandlaufwerke bereit, um Ihre Geschäftsanforderungen erfüllen zu können.

Unterstützte Bandeinheiten und Speicherarchive

Der Server kann eine Vielzahl von Bandeinheiten und Speicherarchiven verwenden. Wählen Sie für Ihre Geschäftsanforderungen geeignete Bandeinheiten und Speicherarchive aus.

Eine Liste der unterstützten Einheiten und gültigen Einheitenklassenformate finden Sie auf der Website für Ihr Betriebssystem:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Weitere Informationen zu Speichereinheiten und Speicherobjekten finden Sie in Typen von Speichereinheiten.

Jede Einheit, die für IBM Spectrum Protect definiert ist, ist einer einzigen *Einheitenklasse* zugeordnet. Die Einheitenklasse gibt den Einheitentyp und die Datenträgerverwaltungsinformationen, wie beispielsweise Aufzeichnungsformat, geschätzte Kapazität und Kennzeichnungspräfixe, an.

Ein *Einheitentyp* kennzeichnet eine Einheit als Mitglied einer Gruppe von Einheiten mit gemeinsamen Datenträgermerkmalen. Beispielsweise gilt der Einheitentyp LTO für alle Generationen von LTO-Bandlaufwerken.

Eine Einheitenklasse für ein Bandlaufwerk muss auch ein Speicherarchiv angeben. Ein *physisches Speicherarchiv* besteht aus einem oder mehreren Laufwerken, die ähnliche Anforderungen in Bezug auf die Bereitstellung von Datenträgern haben. Das heißt, das Laufwerk kann von einem Bediener oder durch einen automatisierten Bereitstellungsmechanismus bereitgestellt werden.

Eine *Speicherarchivobjektdefinition* gibt den Speicherarchivtyp und andere Merkmale an, die diesem Speicherarchivtyp zugeordnet sind.

In der folgenden Tabelle sind die bevorzugten Speicherarchivtypen für eine Bandspeicherlösung in IBM Spectrum Protect Version 8.1.6 aufgelistet.

Tabelle 6. Speicherarchivtypen für eine Bandspeicherlösung in IBM Spectrum Protect 8.1.6

Speicherarchivtyp	**Beschreibung**	**Weitere Informationen**
SCSI	Ein SCSI-Speicherarchiv wird über eine SCSI-Schnittstelle gesteuert, die entweder direkt über SCSI-Verkabelung oder über ein Speicherbereichsnetz an den Host des Servers angeschlossen ist. Ein Robotermechanismus oder ein anderer Mechanismus handhabt automatisch das Bereitstellen von Banddatenträgern und das Aufheben der Bereitstellung von Banddatenträgern. Wenn Sie unterschiedliche Laufwerktypen für ein SCSI-Speicherarchiv erstellen, erstellen Sie mehrere logische Speicherarchive, die nicht auf verschiedene Typen von Laufwerken aufgeteilt werden können. Ein SCSI-Speicherarchiv kann Laufwerke mit gemischten Technologien enthalten, einschließlich LTO Ultrium- und DLT-Laufwerke. Beispiel: • Oracle StorageTek L700-Speicherarchiv • Bandeinheit IBM 3592	„Speicherarchive für die Verwendung durch einen Server konfigurieren” auf Seite 96 Es gelten Einschränkungen, wenn Sie verschiedene Generationen von Datenträgern und Laufwerken kombiniert verwenden. Weitere Informationen finden Sie in: • „Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen” auf Seite 105 • „LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen” auf Seite 102

Tabelle 6. Speicherarchivtypen für eine Bandspeicherlösung in IBM Spectrum Protect 8.1.6 (Forts.)		
Speicherarchiv-typ	**Beschreibung**	**Weitere Informationen**
SHARED	Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die durch SCSI-Speicherarchive dargestellt werden. Das Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist. IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den Speicherarchivmanager-Server. Gemeinsam genutzte Speicherarchive referenzieren einen Speicherarchivmanager.	

Unterstützte Bandeinheitenkonfigurationen

Lesen Sie die Informationen zu lokalen Netzen (LAN) und Speicherbereichsnetzen (SAN). Um die Datenversetzung zu optimieren, planen Sie die Konfiguration der LAN-unabhängigen Datenversetzung. Überlegen Sie außerdem, ob die gemeinsame Speicherarchivnutzung verwendet werden soll.

Wählen Sie die Einheitenkonfiguration aus, die für Ihre Geschäftsanforderungen am besten geeignet ist.

LAN-gestützte und LAN-unabhängige Datenversetzung

Sie können Daten zwischen Clients und Speichereinheiten, die an ein lokales Netz (LAN) angeschlossen sind, oder Speichereinheiten, die an ein Speicherbereichsnetz (SAN) angeschlossen sind, versetzen; dies wird als LAN-unabhängige Datenversetzung bezeichnet.

In einer konventionellen LAN-Konfiguration sind einem einzelnen IBM Spectrum Protect-Server ein oder mehrere Bandarchive zugeordnet. Durch die LAN-unabhängige Datenversetzung wird LAN-Bandbreite für andere Verwendungszwecke verfügbar gemacht und die IBM Spectrum Protect-Serverauslastung verringert.

In einer LAN-Konfiguration müssen Clientdaten, E-Mails, Terminalverbindung, Anwendungsprogramm und Einheitensteuerinformationen von demselben Netz gehandhabt werden. Einheitensteuerinformationen und Clientsicherungs- und -zurückschreibungsdaten fließen über das LAN.

Ein Speicherbereichsnetz (SAN) ist ein dediziertes Speichernetz, das die Systemleistung verbessern kann.

Durch die Verwendung von IBM Spectrum Protect in einem SAN profitieren Sie von den folgenden Funktionen:

- Gemeinsame Nutzung von Speichereinheiten durch mehrere IBM Spectrum Protect-Server.

  Einschränkung: Eine Speichereinheit mit dem Einheitentyp GENERICTAPE kann nicht von mehreren Servern gemeinsam genutzt werden.
- Versetzen von IBM Spectrum Protect-Clientdaten direkt auf Speichereinheiten (LAN-unabhängige Datenversetzung) durch die Konfiguration eines Speicheragenten auf dem Clientsystem.

In einem SAN können Sie Bandlaufwerke und Speicherarchive, die vom IBM Spectrum Protect-Server unterstützt werden, einschließlich der meisten SCSI-Bandeinheiten, gemeinsam nutzen.

Wenn IBM Spectrum Protect-Server ein SCSI-Bandarchiv gemeinsam nutzen, ist der *Speicherarchivmanager* der Eigner der Einheit und steuert die Einheit. Die Speicheragenten und andere IBM Spectrum Protect-Server, die die dieses Speicherarchiv gemeinsam nutzen, sind *Speicherarchivclients*. Ein Speicherarchivclient fordert gemeinsam genutzte Speicherarchivressourcen, wie beispielsweise Laufwerke oder Datenträger, vom Speicherarchivmanager an, verwendet die Ressourcen jedoch unabhängig. Der Speicherarchivmanager koordiniert den Zugriff auf diese Ressourcen. IBM Spectrum Protect-Server, die als Speicherarchivclients definiert sind, kontaktieren den Speicherarchivmanager mithilfe der Kommunikation zwischen

Servern und fordern Einheitenservice an. Daten werden über das SAN zwischen den einzelnen Servern und der Speichereinheit versetzt.

Voraussetzung: Wenn Sie einen Speicherarchivmanager-Server definieren, der mit dem IBM Spectrum Protect-Server gemeinsam genutzt wird, muss die Option **SANDISCOVERY** auf ON gesetzt werden. Standardmäßig ist diese Option auf OFF gesetzt.

IBM Spectrum Protect-Server verwenden die folgenden Funktionen für die gemeinsame Nutzung eines automatisierten Speicherarchivs:

Partitionierung des Datenträgerbestands
Der Bestand der Datenträger im gemeinsam genutzten Speicherarchiv wird unter den Servern aufgeteilt. Entweder ist ein einzelner Server Eigner eines bestimmten Datenträgers oder der Datenträger befindet sich im globalen Arbeitsdatenträgerpool. Keiner der Server ist Eigner des Arbeitsdatenträgerpools.

Serialisierter Laufwerkzugriff
Es greift jeweils nur ein einziger Server auf das jeweilige Bandlaufwerk zu. Der Laufwerkzugriff erfolgt serialisiert. IBM Spectrum Protect steuert den Laufwerkzugriff, damit Server nicht die Bereitstellung von Datenträgern anderer Server aufheben oder nicht auf Laufwerke schreiben, in denen andere Server ihre Datenträger bereitstellen.

Serialisierter Mountzugriff
Der Datenträgerwechsler des Speicherarchivs führt jeweils nur eine einzige Operation zum Bereitstellen (Mountoperation) oder Aufheben der Bereitstellung aus. Der Speicherarchivmanager führt alle Mountoperationen aus, um diese Serialisierung bereitzustellen.

Gemeinsame Speicherarchivnutzung

Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie die gemeinsame Speicherarchivnutzung konfigurieren. Bei der gemeinsamen Speicherarchivnutzung können mehrere IBM Spectrum Protect-Server dasselbe Bandarchiv und dieselben Laufwerke in einem Speicherbereichsnetz (SAN) nutzen und die Sicherungs- und Wiederherstellungsleistung sowie die Nutzung der Bandhardware verbessern.

Wenn IBM Spectrum Protect-Server ein Speicherarchiv gemeinsam nutzen, wird ein Server als Speicherarchivmanager konfiguriert, der Speicherarchivoperationen wie Bereitstellung und Aufhebung der Bereitstellung steuert. Der Speicherarchivmanager steuert auch das Eigentumsrecht für Datenträger und den Speicherarchivbestand. Weitere Server werden als Speicherarchivclients konfiguriert und kontaktieren den Speicherarchivmanager mithilfe der Kommunikation zwischen Servern und fordern Ressourcen an.

Speicherarchivclients müssen dieselbe Version oder eine frühere Version wie der Speicherarchivmanager-Server haben. Ein Speicherarchivmanager kann keine Speicherarchivclients unterstützen, die eine höhere Version haben. Weitere Informationen finden Sie in Storage-agent and library-client compatibility with an IBM Spectrum Protect server (Kompatibilität des Speicheragenten und des Speicherarchivclients mit einem IBM Spectrum Protect-Server).

LAN-unabhängige Datenversetzung

Mit IBM Spectrum Protect wird einem Client über einen Speicheragenten die Funktionalität bereitgestellt, um Daten direkt in einem Bandarchiv in einem Speicherbereichsnetz (SAN) zu sichern und aus ihm zurückzuschreiben. Dieser Typ von Datenversetzung ist auch als LAN-unabhängige Datenversetzung bekannt.

Einschränkung: Centera-Speichereinheiten können keine Ziele für LAN-unabhängige Operationen sein.

Abbildung 2 auf Seite 18 zeigt eine SAN-Konfiguration, bei der ein Client direkt auf ein Bandarchiv zugreift, um Daten zu lesen oder zu schreiben.

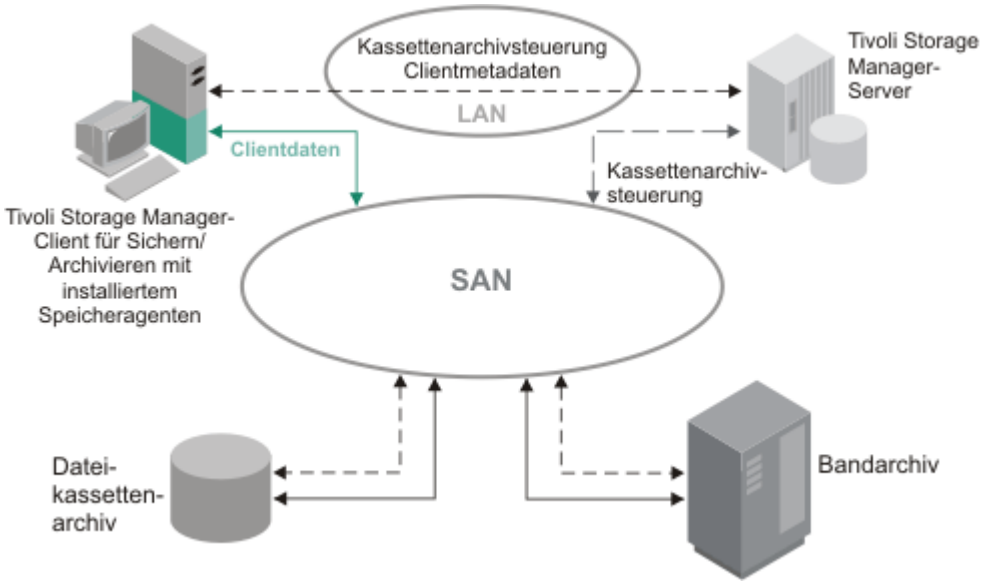


Abbildung 2. LAN-unabhängige Datenversetzung

Die LAN-unabhängige Datenversetzung erfordert die Installation eines Speicheragenten auf dem Clientsystem. Der Server verwaltet die Datenbank und das Wiederherstellungsprotokoll und fungiert als Speicherarchivmanager, um Operationen der Einheiten zu steuern. Der Speicheragent auf dem Client handhabt die Datenübertragung zu der Einheit im SAN. Diese Implementierung gibt Bandbreite im LAN frei, die andernfalls für das Versetzen von Clientdaten verwendet würde.

Gemischte Einheitentypen in Speicherarchiven

IBM Spectrum Protect unterstützt das Mischen unterschiedlicher Einheitentypen in einem einzelnen automatisierten Speicherarchiv, sofern das Speicherarchiv die verschiedenen Datenträger für die unterschiedlichen Einheitentypen unterscheiden kann. Um den Konfigurationsprozess zu vereinfachen, sollten Sie keine unterschiedlichen Einheitentypen in einem Speicherarchiv mischen. Wenn das Mischen von Einheitentypen erforderlich ist, berücksichtigen Sie die Einschränkungen.

Bei Speicherarchiven mit dieser Funktionalität handelt es sich um Modelle, die über integrierte gemischte Laufwerke verfügen oder die das Hinzufügen gemischter Laufwerke unterstützen. Weitere Informationen finden Sie in der Dokumentation des Herstellers. Informationen zu Speicherarchiven, die für IBM Spectrum Protect mit gemischten Einheitentypen getestet wurden, finden Sie in den Informationen für Ihr Betriebssystem:

- IBM Spectrum Protect Supported Devices for AIX, HP-UX, Solaris, and Windows
- IBM Spectrum Protect Supported Devices for Linux

Beispielsweise können LTO Ultrium-Laufwerke und IBM TS1100-Laufwerke in einem einzelnen Speicherarchiv vorhanden sein, das für den IBM Spectrum Protect-Server definiert ist.

Verschiedene Datenträgergenerationen in einem Speicherarchiv

Der IBM Spectrum Protect-Server erlaubt zwar unterschiedliche Einheitentypen in einem automatisierten Speicherarchiv, das Mischen verschiedener Generationen desselben Laufwerktyps wird jedoch im Allgemeinen nicht unterstützt. Neue Laufwerke können keine Daten mit den älteren Datenträgerformaten schreiben und alte Laufwerke können neue Formate nicht lesen. LTO Ultrium-Laufwerke sind eine Ausnahme von dieser Regel.

Wenn mit der neuen Laufwerktechnologie keine Daten auf Datenträger geschrieben werden können, die von Laufwerken einer älteren Generation formatiert wurden, müssen die älteren Datenträger als schreibgeschützt markiert werden, um Probleme bei Serveroperationen zu verhindern. Außerdem müssen die älteren Laufwerke aus dem Speicherarchiv entfernt werden oder die Definitionen der älteren Laufwerke müssen vom Server entfernt werden. Beispielsweise unterstützt der IBM Spectrum Protect-Server nicht

die Verwendung von Oracle StorageTek 9940A-Laufwerken mit 9940B-Laufwerken in Kombination mit anderen Einheitentypen in einem einzelnen Speicherarchiv.

Im Allgemeinen unterstützt IBM Spectrum Protect nicht das Mischen unterschiedlicher Generationen von LTO Ultrium-Laufwerken und -Datenträgern. Die folgenden Kombinationen werden jedoch unterstützt:

- LTO Ultrium Generation 3 (LTO-3) mit LTO Ultrium Generation 4 (LTO-4)
- LTO Ultrium Generation 4 (LTO-4) mit LTO Ultrium Generation 5 (LTO-5)
- LTO Ultrium Generation 5 (LTO-5) mit LTO Ultrium Generation 6 (LTO-6)
- LTO Ultrium Generation 6 (LTO-6) mit LTO Ultrium Generation 7 (LTO-7)
- LTO Ultrium-Datenträger der Generation 7 (LTO-7) mit LTO Ultrium-Datenträgern der Generation 8 (LTO-8 und LTO-M8) in einem Speicherarchiv mit LTO-8-Bandlaufwerken oder einem Speicherarchiv mit einer Kombination aus LTO-8-Bandlaufwerken und LTO-7-Bandlaufwerken

Der Server unterstützt diese Kombinationen, da die verschiedenen Laufwerke Daten von den unterschiedlichen Datenträgern lesen und auf diese schreiben können. Wenn Sie planen, für alle Laufwerke ein Upgrade auf Generation 4 (oder Generation 5, 6, 7 oder 8) durchzuführen, müssen Sie alle vorhandenen LTO Ultrium-Laufwerkdefinitionen und die Pfade, die ihnen zugeordnet sind, löschen. Anschließend können Sie die neuen Laufwerke und Pfade der Generation 4 (oder Generation 5, 6, 7 oder 8) definieren.

Einschränkungen, die für das Mischen von LTO Ultrium-Bandlaufwerken und -Datenträgern gelten

- LTO-5-Laufwerke können nur LTO-3-Datenträger lesen. Wenn Sie LTO-3- und LTO-5-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-3-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-3-Arbeitsdatenträger entnehmen.
- LTO-6-Laufwerke können nur LTO-4-Datenträger lesen. Wenn Sie LTO-4- und LTO-6-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-4-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-4-Arbeitsdatenträger entnehmen.
- LTO-7-Laufwerke können nur LTO-5-Datenträger lesen. Wenn Sie LTO-5- und LTO-7-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-5-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-5-Arbeitsdatenträger entnehmen.
- LTO-8-Laufwerke können keine LTO-6-Datenträger lesen. Wenn Sie LTO-6-Laufwerke und -Datenträger mit LTO-8-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen, müssen Sie das Speicherarchiv in zwei Speicherarchive partitionieren. Ein Speicherarchiv verfügt nur über LTO-8-Laufwerke und -Datenträger und das andere Speicherarchiv nur über LTO-6-Laufwerke und -Datenträger.

Einschränkungen, die für gemischte Generationen von LTO Ultrium-Bandlaufwerken in einem Speicherarchiv gelten

Sie müssen Bandkassetten einer früheren Generation als das Bandlaufwerk verwenden. Ein Bandlaufwerk einer späteren Generation kann Daten von einer Bandkassette einer früheren Generation lesen und auf diese schreiben. Wenn beispielsweise ein Speicherarchiv über LTO-7- und LTO-6-Bandlaufwerke verfügt, müssen Sie LTO-6-Bandkassetten verwenden. Sowohl die LTO-7- als auch die LTO-6-Bandlaufwerke können Daten von LTO-6-Bandkassetten lesen und auf Bandkassetten dieser Generation schreiben.

Einschränkungen, die für gemischte Generationen von LTO Ultrium-Bandkassetten in einem Speicherarchiv gelten

Sie müssen eine Bandkassette verwenden, die dieselbe Generation wie das Bandlaufwerk hat, oder exakt eine Generation früher. Wenn beispielsweise ein Speicherarchiv über LTO-7-Bandlaufwerke verfügt, können Sie LTO-7-Bandkassetten oder eine Kombination aus LTO-7- und LTO-6-Bandkassetten verwenden. Wenn dieses Speicherarchiv über LTO-7-, LTO-6- und LTO-5-Bandkassetten verfügt, müssen Sie den Zugriffsmodus für die LTO-5-Bandkassetten in READONLY (Lesezugriff) ändern.

Weitere Informationen zum Mischen von LTO Ultrium-Generationen finden Sie in „Einheitenklassen LTO definieren” auf Seite 101.

Wenn Sie IBM Spectrum Protect verwenden, können Sie keine Laufwerke der Laufwerkgenerationen 3592, TS1130, TS1140, TS1150 oder späterer Laufwerkgenerationen mischen. Verwenden Sie eine von

drei speziellen Konfigurationen. Ausführliche Informationen finden Sie in „Einheitenklassen 3592 definieren” auf Seite 104.

Wenn Sie planen, Datenträger in einem Speicherarchiv zu verschlüsseln, mischen Sie keine Datenträgergenerationen in dem Speicherarchiv.

Gemischte Datenträger und Speicherpools

Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie Datenträgerformate in einem Speicherpool nicht mischen. Anstatt Formate zu mischen, ordnen Sie jedes eindeutige Datenträgerformat über seine eigene Einheitenklasse einem separaten Speicherpool zu. Diese Einschränkung gilt auch für LTO-Formate.

Mehrere Speicherpools und ihre Einheitenklassen verschiedenen Typs können auf dasselbe Speicherarchiv verweisen, das diese wie in „Verschiedene Datenträgergenerationen in einem Speicherarchiv” auf Seite 18 beschrieben unterstützen kann.

Sie können eine Migration auf eine neue Generation eines Datenträgertyps innerhalb desselben Speicherpools durchführen, indem Sie die folgenden Schritte ausführen:

1. Ersetzen Sie in dem Speicherarchiv alle älteren Laufwerke durch die Laufwerke der neueren Generation. Die Laufwerke dürfen nicht gemischt werden.
2. Markieren Sie die vorhandenen Datenträger mit den älteren Formaten als schreibgeschützt, wenn das neue Laufwerk diese Bänder im alten Format nicht hinzufügen kann. Wenn das neue Laufwerk auf die vorhandenen Datenträger mit ihrem alten Format schreiben kann, ist dies nicht notwendig; Schritt 1 ist jedoch dennoch erforderlich. Wenn verschiedene Laufwerkgenerationen, die lese- aber nicht schreibkompatibel sind, in demselben Speicherarchiv erforderlich sind, verwenden Sie für jede Laufwerkgeneration einen separaten Speicherpool.

Definitionen für Bandspeichereinheiten

Bevor der IBM Spectrum Protect-Server eine Bandeinheit verwenden kann, muss die Einheit für das Betriebssystem und den Server konfiguriert werden. Bestimmen Sie im Rahmen des Planungsprozesses die Definitionen für Ihre Bandspeichereinheiten.

Tipp: Mithilfe des Befehls **PERFORM LIBACTION** können Sie den Prozess zum Hinzufügen von Einheiten zu SCSI- und VTL-Speicherarchiven vereinfachen.

In Tabelle 7 auf Seite 20 sind die Definitionen für unterschiedliche Einheitentypen zusammengefasst.

Tabelle 7. Definitionen für Speichereinheiten

Einheit	Einheitentypen	Definitionen			
		Speicherarchiv	**Laufwerk**	**Pfad**	**Einheitenklasse**
Magnetplatte	DISK	—	—	—	Ja [1]
	FILE [2]	—	—	—	Yes
	AIX Windows CENTERA Linux CENTERA [3]	—	—	—	Yes

Tabelle 7. Definitionen für Speichereinheiten (Forts.)					
		Definitionen			
Einheit	**Einheitentypen**	**Speicher-archiv**	**Laufwerk**	**Pfad**	**Einheiten-klasse**
Band	3590 3592 DLT LTO NAS VOLSAFE AIX Windows GENERIC-TAPE ECARTRIDGE [4]	Yes	Ja	Ja	Yes
Austauschbare Datenträger (Dateisystem)	REMOVABLEFILE	Yes	Yes	Ja	Yes

1. Die Einheitenklasse DISK ist bei der Installation vorhanden und kann nicht geändert werden.
2. FILE-Speicherarchive, -Laufwerke und -Pfade sind für die gemeinsame Nutzung mit Speicheragenten erforderlich.
3. Linux Der Einheitentyp CENTERA ist nur für Linux x86_64-Systeme verfügbar.
4. Der Einheitentyp ECARTRIDGE gilt für Oracle StorageTek-Kassettenbandlaufwerke wie beispielsweise 9840- und T10000-Laufwerke.

Planung der Speicherpoolhierarchie

Planen Sie die Speicherpoolhierarchie, um sicherzustellen, dass Daten täglich von Platte auf Band umgelagert werden. Bei der Umlagerung wird Speicherbereich auf der Platteneinheit freigegeben und die Daten werden für die langfristige Aufbewahrung auf Band versetzt. Auf diese Weise können Sie die Vorteile der Skalierbarkeit, Kosteneffizienz und Sicherheitsfunktionen von Bandspeicher nutzen.

Vorbereitende Schritte

Die Speicherpoolhierarchie unterstützt Sie bei der Verwaltung des Datenflusses. Schauen Sie sich zum besseren Verständnis des Datenflusses Abbildung 3 auf Seite 22 an.

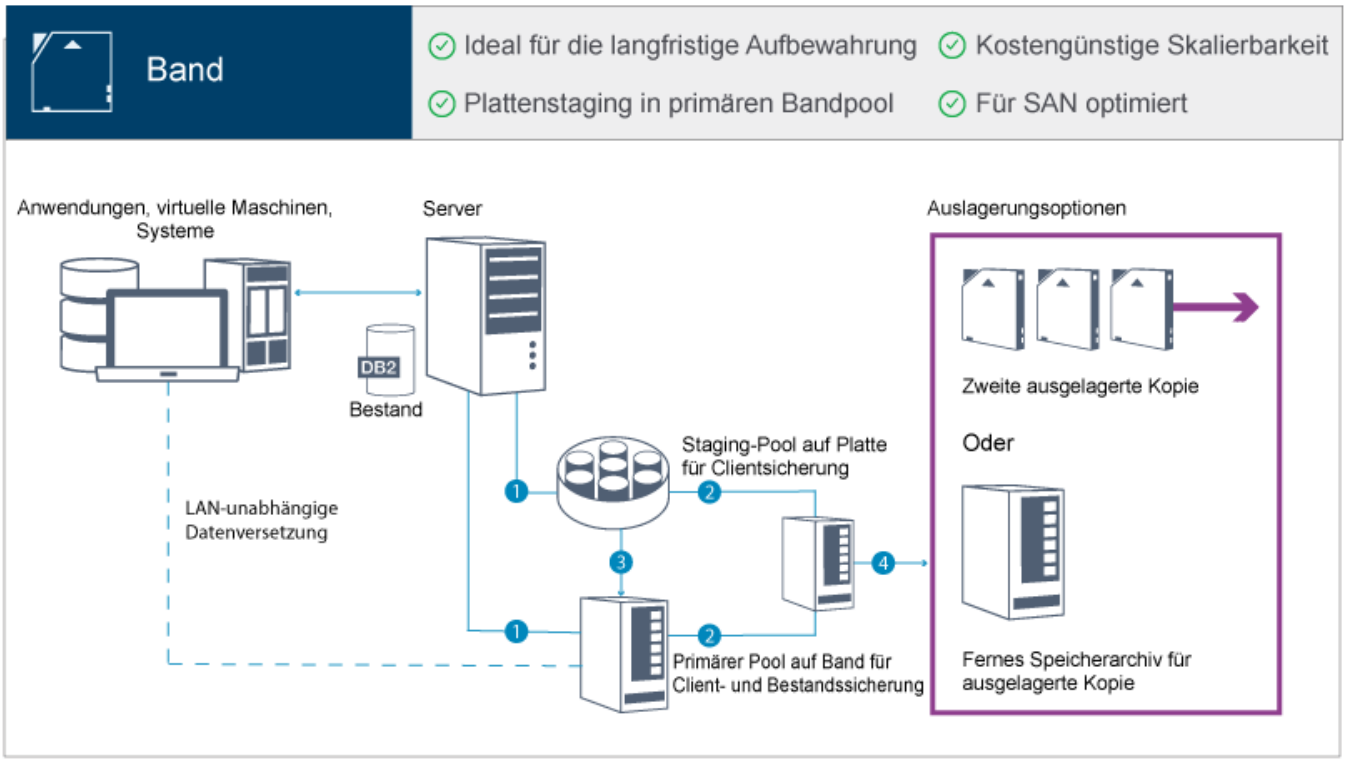


Abbildung 3. Bandspeicherlösung

Die folgenden Schritte entsprechen den Zahlen in der Abbildung:

1. Der Server empfängt Daten von Clients (Anwendungen, virtuelle Maschinen oder Systeme) und speichert die Daten in primären Speicherpools. Abhängig vom Clienttyp werden die Daten in einem primären Speicherpool auf Platte oder Band gespeichert.
2. Die Daten auf Platte und Band werden in einem Kopienspeicherpool auf Band gesichert.
3. Daten in dem primären Speicherpool auf Platte werden täglich in den primären Speicherpool auf Band umgelagert.
4. Daten aus dem Kopienspeicherpool auf Band werden an einen anderen Standort versetzt werden, um die langfristige Aufbewahrung und die Wiederherstellung nach einem Katastrophenfall zu unterstützen.

Vorgehensweise

Um die Speicherpoolhierarchie zu planen, beantworten Sie die folgenden Fragen:

a. Welche Clients sollten Daten auf Platte sichern und welche Clients sollten Daten auf Band sichern?

- Die bevorzugte Methode ist das Sichern von Clients, die große Objekte wie beispielsweise Datenbanken enthalten, auf Band.
- Die bevorzugte Methode ist das Sichern aller anderen Clients auf Platte.
- Clients virtueller Maschinen (VMs) können auf Platte oder Band gesichert werden. Die bevorzugte Methode ist das Sichern eines VM-Clients in einem separaten Plattenspeicherpool, der nicht auf Band umgelagert wird. Wenn ein VM-Client auf Band umgelagert werden muss, erstellen Sie einen kleineren Plattenspeicherpool zum Speichern der VMware-Steuerdateien. Dieser kleinere Plattenspeicherpool darf nicht auf Band umgelagert werden. Weitere Informationen zum Sichern eines VM-Clients auf Band finden Sie in Richtlinien für Banddatenträger und and IBM Tivoli Storage Manager (TSM) guest support for Virtual Machines and Virtualization.

Tipp: Wenn viele Clients Daten in einem einzigen Speicherpool sichern müssen, ziehen Sie die Verwendung eines Speicherpools auf Platte in Erwägung, da Sie viele Mountpunkte angeben können. Sie können einen Maximalwert von 999 für den Parameter **MAXNUMMP** im Befehl **REGISTER NODE** angeben.

b. Was ist bei der Angabe der Kapazität plattenbasierter Speicherpools zu beachten?

   Planen Sie zumindest genügend Kapazität zum Speichern der Daten von Sicherungsoperationen eines einzelnen Tages ein. Die bevorzugte Methode ist das Planen von genügend Kapazität, um Daten von Sicherungsoperationen zweier Tage zu speichern, zuzüglich eines Puffers von 20 %.

c. Was ist bei der Angabe der Einheitenklasse für den plattenbasierten Speicherpool zu beachten?

   Die bevorzugte Methode ist die Angabe der Einheitenklasse FILE. Setzen Sie den Parameter **MOUNTLIMIT** auf 4000. Stellen Sie außerdem sicher, dass der Knoten über eine ausreichend große Anzahl Mountpunkte verfügt; diesen Wert können Sie über den Parameter **MAXNUMMP** im Befehl **REGISTER NODE** angeben.

d. Sollte Datendeduplizierung für den Plattenspeicherpool angegeben werden?

   Nein, da die Daten nur für einen einzigen Tag auf Platte gespeichert werden, bevor die Daten auf Band umgelagert werden.

e. Sollte die automatische Umlagerung von Daten auf der Basis eines Umlagerungsschwellenwerts angegeben werden?

   Nein. Planen Sie stattdessen die tägliche Umlagerung mithilfe des Befehls **MIGRATE STGPOOL**. (Um die automatische Umlagerung auf der Basis des Umlagerungsschwellenwerts zu verhindern, geben Sie den Wert 100 für den Parameter **HIGHMIG** und den Wert 0 für den Parameter **LOWMIG** an, wenn Sie den Befehl **DEFINE STGPOOL** ausgeben.)

f. Sollte eine Umlagerungsverzögerung angegeben werden?

   Die bevorzugte Methode ist die Angabe der täglichen Umlagerung von Platte auf Band und nicht die Angabe einer Umlagerungsverzögerung, die weitere Planung erfordert. Weitere Informationen zur Umlagerungsverzögerung finden Sie in. Dateien in einer Speicherpoolhierarchie umlagern.

g. Wie kann die Anzahl Bandlaufwerke berechnet werden?

   i) Bestimmen Sie die native Datenübertragungsrate des Laufwerks anhand der Dokumentation des Herstellers. Um eine Schätzung der kontinuierlichen Datenübertragungsrate in Ihrer Speicherumgebung zu ermitteln, subtrahieren Sie 30 % von der nativen Datenübertragungsrate.

   ii) Berechnen Sie die erforderlich Datenaufnahmerate des Servers. Dividieren Sie dann diese Zahl durch die kontinuierliche Datenübertragungsrate einer einzelnen Bandeinheit. Das Ergebnis gibt die minimale Anzahl Laufwerke zur Unterstützung der Datenaufnahme an.

   iii) Berechnen Sie die Anzahl Mountpunkte, die für Clients erforderlich sind, die Daten auf Band sichern, einschließlich der Clients, die mehrere Sitzungen verwenden. Sie können die Mountpunkte über das Fenster zum Durchführen von Sicherungen verteilen; dabei müssen Sie beachten, dass Clients wahrscheinlich große Objekte sichern, die unter Umständen den größten Teil des Fensters in Anspruch nehmen.

   iv) Berechnen Sie die Leistungsanforderungen *und* Mountpunkte, die für Verwaltungstasks, wie beispielsweise Umlagerung von Platte auf Band und Kopieroperationen von Band auf Band, erforderlich sind. Durch die Sicherung von Daten auf Band, können Sie die Umlagerungsverarbeitung vermeiden, durch die Ausführung von Kopieroperationen von Band auf Band verdoppeln sich jedoch die Anforderungen für Bandlaufwerke.

   v) Berechnen Sie die Anzahl zusätzlicher Laufwerke, die gegebenenfalls erforderlich sind:

   - Wenn ein Bandlaufwerk nicht korrekt funktioniert, hat das Problem Auswirkungen auf die Anzahl verfügbarer Mountpunkte und die Aufnahmerate. Ziehen Sie die Bereitstellung von Ersatzlaufwerken in Erwägung. Wenn beispielsweise fünf Bandlaufwerke für normale Operationen erforderlich sind, sollten Sie die Bereitstellung von zwei Ersatzlaufwerken in Erwägung ziehen.
   - Für Zurückschreibungs- und Abrufoperationen sind unter Umständen zusätzliche Bandlaufwerke erforderlich, wenn Sie planen, die Operationen gleichzeitig mit Datenaufnahme- und Verwaltungsoperationen auszuführen. Stellen Sie, falls erforderlich, zusätzliche Bandlaufwerke bereit und stellen Sie sicher, dass diese noch nicht verwendet wurden, wenn Sie die Zurückschreibungs- oder Abrufoperationen starten.

h. Welche Alternativen sind für die Optimierung von Zurückschreibungsoperationen verfügbar?

Sie können die Kollokation verwenden, um die Systemleistung zu verbessern und Organisation von Daten zu optimieren. Mithilfe der Kollokation kann die Anzahl Datenträger reduziert werden, auf die zugegriffen werden muss, wenn ein großes Datenvolumen zurückgeschrieben werden muss:

- Für plattenbasierte Speicherpools ist die bevorzugte Methode die Verwendung der Kollokation nach Knoten. Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.
- Für bandbasierte Speicherpools ist die bevorzugte Methode die Verwendung der Kollokation nach Gruppe. Die Kollokation nach Gruppe hat eine Verringerung der nicht genutzten Bandkapazität zur Folge, wodurch mehr kollokierte Daten auf einzelnen Bändern gespeichert werden können.

Weitere Informationen zur Kollokation finden Sie in „Operationen durch Aktivierung der Kollokation von Clientdateien optimieren” auf Seite 181.

Wenn Sie ein erfahrener Systemadministrator sind, können Sie weitere Aktionen zur Optimierung von Zurückschreibungsoperationen planen. Siehe Zurückschreibungsoperationen für Clients optimieren, Dateisicherungsmethoden und MOVE NODEDATA (Daten nach Knoten in einen Speicherpool mit sequenziellem Zugriff versetzen).

Auslagerung von Daten

Um die Datenwiederherstellung zu erleichtern und in Ihre Strategie zur Wiederherstellung nach einem Katastrophenfall zu integrieren, speichern Sie Bandkopien an einen anderen Standort.

Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um einen Plan zur Wiederherstellung nach einem Katastrophenfall zu konfigurieren und automatisch zu generieren, der die Informationen, Scripts und Prozeduren enthält, die erforderlich sind, um den Server nach einem Katastrophenfall automatisch zurückzuschreiben und Clientdaten wiederherzustellen. Wählen Sie eine der folgenden Optionen für die Auslagerung von Daten als Strategie zur Wiederherstellung nach einem Katastrophenfall aus, um Bandkopien zu schützen:

Vaulting an einem anderen Standort für einen einzelnen Produktionsstandort
Speicherdatenträger, wie beispielsweise Bandkassetten und Datenträger werden an einem anderen Standort durch Vaulting geschützt. Ein Kurier transportiert die Daten von der Speichereinrichtung an dem anderen Standort zum Wiederherstellungsstandort. Wenn ein Katastrophenfall eintritt, werden die Datenträger wieder an den Produktionsstandort gesendet, nachdem die Hardware und der IBM Spectrum Protect-Server wiederhergestellt wurden.

Vaulting an einem anderen Standort mit einem Wiederherstellungsstandort
Ein Kurier transportiert Speicherdatenträger vom Produktionsstandort an eine Speichereinrichtung an einem anderen Standort. Da ein zugeordneter Wiederherstellungsstandort vorhanden ist, können Sie die Wiederherstellungszeit im Vergleich zur Wiederherstellungszeit bei einem einzelnen Produktionsstandort verringern. Diese Option erhöht jedoch die Kosten für die Wiederherstellung nach einem Katastrophenfall, da weitere Hardware und Software verwaltet werden muss. Beispielsweise muss der Wiederherstellungsstandort über kompatible Bandeinheiten und IBM Spectrum Protect-Server-Software verfügen. Bevor der Produktionsstandort wiederhergestellt werden kann, müssen die Hardware und Software am Wiederherstellungsstandort konfiguriert und aktiv sein.

Elektronisches Vaulting
Um elektronisches Vaulting als Strategie zur Wiederherstellung nach einem Katastrophenfall verwenden zu können, muss am Wiederherstellungsstandort ein aktiver IBM Spectrum Protect-Server vorhanden sein. Kritische Daten des Produktionsstandorts werden durch elektronisches Vaulting am Wiederherstellungsstandort geschützt. DRM wird auch für das Vaulting nicht kritischer Daten an einem anderen Standort verwendet. Beim elektronischen Vaulting werden kritische Daten schneller und häufiger als bei traditionellen Methoden mittels Kurier ausgelagert. Die Wiederherstellungszeit verkürzt sich, da kritische Daten bereits am Wiederherstellungsstandort gespeichert sind. Da der Wiederherstellungsstandort ständig aktiv ist, sind die Kosten der Strategie zur Wiederherstellung nach einem Katastrophenfall jedoch höher als beim Vaulting an einem anderen Standort.

Zugehörige Konzepte

Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM

IBM Spectrum Protect stellt die Funktion Disaster Recovery Manager (DRM) für die Wiederherstellung Ihrer Server- und Clientdaten bei einem Katastrophenfall zur Verfügung.

Planung für Sicherheit

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

Planung für Administratorrollen

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

Sie können Administratoren eine der folgenden Berechtigungsstufen zuordnen:

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

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

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

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

Die Szenarios in Tabelle 8 auf Seite 25 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 8. Szenarios für Administratorrollen

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

Zugehörige Tasks

Administratoren verwalten
Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

Planung für sichere Kommunikation

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

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

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

TLS und SSL stellen sichere Kommunikation zwischen dem Server und dem Client bereit, können sich jedoch auf die Systemleistung auswirken. Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung, ohne Objektdaten zu verschlüsseln. Informationen zur Angabe, ob der Server TLS für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und der Beschreibung des Parameters **UPDATE SERVER=SSL** für die Kommunikation zwischen Servern.

Ab Version 8.1.2 wird TLS standardmäßig für die Authentifizierung verwendet. Wenn Sie sich für die Verwendung von TLS entscheiden, um vollständige Sitzungen zu verschlüsseln, verwenden Sie das Protokoll nur für Sitzungen, für die es erforderlich ist; fügen Sie außerdem auf dem Server Prozessorressourcen hinzu, um den wachsenden Datenaustausch im Netz handhaben zu können. Sie können auch versuchsweise andere Optionen verwenden. Beispielsweise stellen einige Netzeinheiten wie Router und Switches die TLS- oder SSL-Funktion bereit.

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

- Operations Center: vom Browser zum Hub-Server; vom Hub-Server zum Peripherieserver
- Vom Client zum Server
- Vom Server zum Server: Knotenreplikation

Zugehörige Tasks

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

Planung für die Speicherung verschlüsselter Daten

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

Tabelle 9. Datenverschlüsselungsverfahren auswählen

Geschäftsanforderung	**Verschlüsselungsverfahren**	**Weitere Informationen**
Daten auf Clientebene schützen	IBM Spectrum Protect-Clientverschlüsselung	Sie können Daten auf Dateiebene unter Verwendung einer Einschluss-/Ausschlussliste verschlüsseln. Auf diese Weise haben Sie ein hohes Maß an Kontrolle darüber, welche Daten verschlüsselt werden. Auf dem Client sind sind zusätzliche IT-Ressourcen erforderlich, die sich auf die Leistung von Sicherungs- und Zurückschreibungsprozessen auswirken können. Weitere Informationen zu diesem Verfahren finden Sie in IBM Spectrum Protect-Clientverschlüsselung.
Daten in Speicherpooldatenträgern auf einem Bandlaufwerk schützen	Anwendungsverfahren	Wenn Sie das Anwendungsverfahren verwenden, verwaltet IBM Spectrum Protect die Verschlüsselungsschlüssel, um Daten in Speicherpooldatenträgern zu schützen. Sie müssen Sie besonders vorsichtig vorgehen, um Datenbanksicherungen zu schützen, da die Verschlüsselungsschlüssel in der Serverdatenbank gespeichert sind. Ohne Zugriff auf Datenbanksicherungen und zugehörige Verschlüsselungsschlüssel können Sie Ihre Daten nicht zurückschreiben. Sie können dieses Verfahren nicht verwenden, um Datenbanksicherungen, exportierte Daten oder Sicherungsgruppen zu verschlüsseln. Weitere Informationen zum Anwendungsverfahren finden Sie in „Verschlüsselungsverfahren für Bänder” auf Seite 130.
Daten auf einem Bandlaufwerk schützen	Speicherarchivverfahren	Wenn Sie das Speicherarchivverfahren verwenden, werden die Verschlüsselungsschlüssel vom Speicherarchiv verwaltet. Sie können sowohl Daten in Speicherpools als auch andere Daten auf einem Bandlaufwerk verschlüsseln. Sie können steuern, welche Datenträger unter Verwendung ihrer Barcodeseriennummern verschlüsselt werden. Weitere Informationen zum Speicherarchivverfahren finden Sie in „Verschlüsselungsverfahren für Bänder” auf Seite 130.
Daten auf einem Bandlaufwerk schützen	Systemverfahren	Wenn Sie das Systemverfahren verwenden, wird die Verschlüsselung von einem Einheitentreiber oder dem AIX-Betriebssystem verwaltet. Dieses Verschlüsselungsverfahren ist nur unter dem Betriebssystem AIX verfügbar. Sie können sowohl Daten in Speicherpools als auch andere Daten auf einem Bandlaufwerk verschlüsseln. Weitere Informationen zum Systemverfahren finden Sie in „Verschlüsselungsverfahren für Bänder” auf Seite 130.

Planung des Firewallzugriffs

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

In Tabelle 10 auf Seite 28 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 10. Vom Server, Client und Operations Center verwendete Ports

Element	Standardwert	Richtung	Beschreibung
Basisport (**TCPPORT**)	1500	Abgehend/ Eingehend	Jede Serverinstanz erfordert einen eindeutigen Port. Sie können eine alternative Portnummer angeben. Der mit der Option **TCPPORT** angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Mithilfe der Option **TCPADMINPORT** und der Option **ADMINONCLIENTPORT** können Sie Portwerte für den Datenverkehr des Verwaltungsclients festlegen.
Port ausschließlich für SSL (**SSLTCPPORT**)	Kein Standardwert	Abgehend/ Eingehend	Dieser Port wird verwendet, wenn die Kommunikation am Port auf ausschließlich SSL-fähige Sitzungen beschränkt werden soll. Ein Server kann sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation unterstützen, indem die Option **TCPPORT** oder die Option **TCPADMINPORT** verwendet wird.
SMB	45	Eingehend/ Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SSH	22	Eingehend/ Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SMTP	25	Abgehend	Dieser Port wird zum Senden von E-Mail-Alerts vom Server verwendet.
Replikation	Kein Standardwert	Abgehend/ Eingehend	Der Port und das Protokoll für den Port für abgehende Daten für die Replikation werden mit dem Befehl **DEFINE SERVER** festgelegt, der zum Konfigurieren der Replikation verwendet wird. Bei den Ports für eingehende Daten für die Replikation handelt es sich um die TCP-Ports und SSL-Ports, die für den Quellenserver im Befehl **DEFINE SERVER** angegeben werden.
Port für Clientzeitplan	Client-Port: 1501	Abgehend	Der Client ist an dem angegebenen Port empfangsbereit und teilt die Portnummer dem Server mit. Der Server kontaktiert den Client, wenn die servergesteuerte Zeitplanung verwendet wird. Sie können eine alternative Portnummer in der Clientoptionsdatei angeben.
Lange laufende Sitzungen	Einstellung für **KEEPALIVE**: YES	Abgehend	Wenn die Option **KEEPALIVE** aktiviert ist, werden während Client/Server-Sitzungen Keepalive-Pakete gesendet, um zu verhindern, dass die Firewall-Software lange laufende inaktive Verbindungen schließt.
Operations Center	HTTPS: 11090	Eingehend	Diese Ports werden für den Web-Browser des Operations Center verwendet. Sie können eine alternative Portnummer angeben.

Tabelle 10. Vom Server, Client und Operations Center verwendete Ports (Forts.)			
Element	**Standardwert**	**Richtung**	**Beschreibung**
Port für den Clientverwaltungsservice	Client-Port: 9028	Eingehend	Wenn Sie planen, IBM Spectrum Protect-Clientverwaltungsservices zu verwenden, muss der Zugriff auf den Port für den Clientverwaltungsservice über das Operations Center möglich sein. Stellen Sie sicher, dass Verbindungen nicht durch Firewalls verhindert werden können. Der Clientverwaltungsservice verwendet den TCP-Port des Servers für den Clientknoten für die Authentifizierung unter Verwendung einer Verwaltungssitzung.

Zugehörige Informationen

Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen

Serveroption ADMINONCLIENTPORT

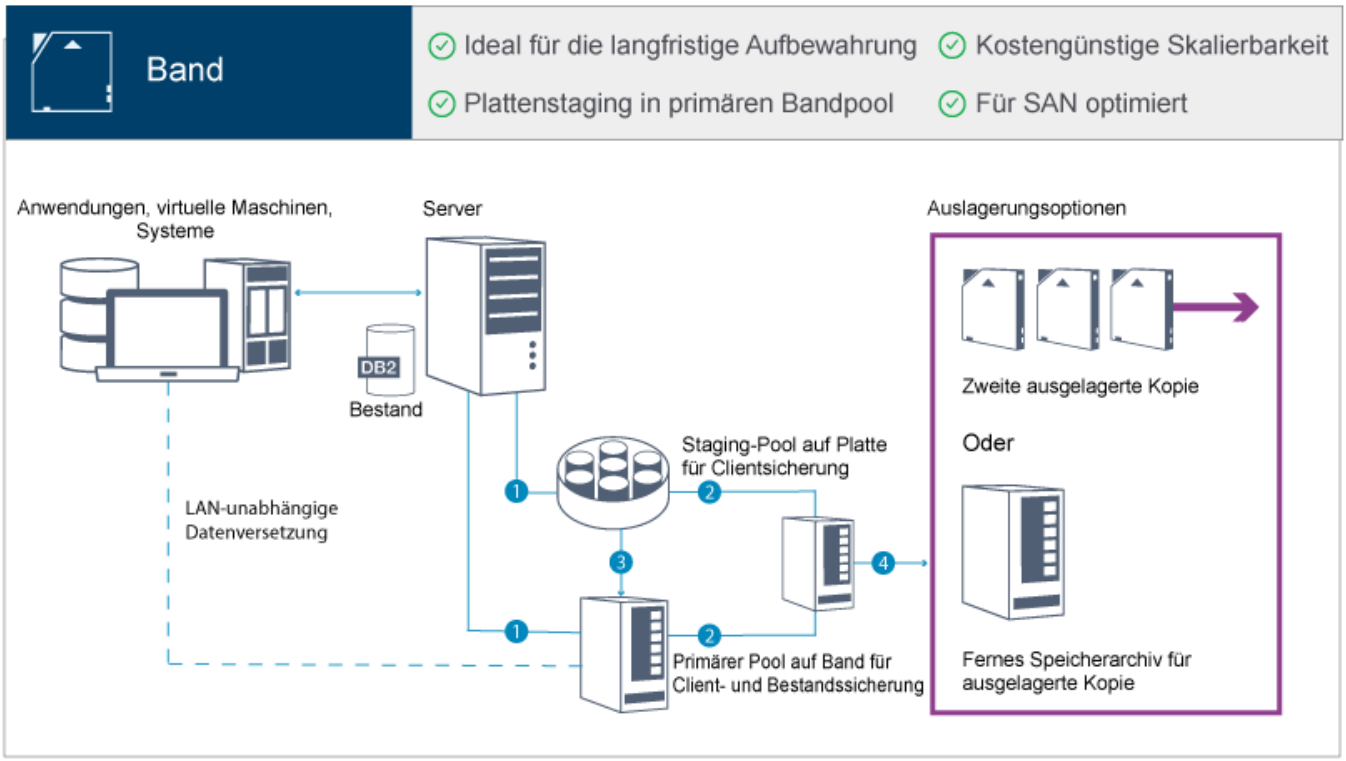
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

Serveroption TCPADMINPORT

Serveroption TCPPORT

Teil 2. Implementierung einer bandbasierten Datenschutzlösung

Implementieren Sie die bandbasierte Lösung, die die Platte-Platte-Band-Sicherung und Plattenstaging zur Optimierung des Speichers verwendet. Durch die Implementierung der Bandspeicherlösung können Sie die langfristige Aufbewahrung von Daten ermöglichen und kostengünstige Skalierbarkeit erzielen.



Tipps:

- In der beschriebenen Lösung werden Daten aus Plattenspeicherpools in Bandspeicherpools *umgelagert*. Anstatt die Daten umzulagern, können Sie jedoch die Band-Tiering-Funktion verwenden, die in IBM Spectrum Protect Version 8.1.8 eingeführt wurde. Mit dieser Funktion können Sie Daten automatisch mit Tiering aus Verzeichniscontainerspeicherpools auf Platte in Bandspeicher versetzen. Sie können angeben, dass alle Daten auf der Basis eines angegebenen Altersschwellenwerts mit Tiering versetzt werden oder dass nur inaktive Daten auf der Basis eines Altersschwellenwerts mit Tiering versetzt werden. Weitere Informationen zum Versetzen von Daten mit Tiering in Bandspeicher finden Sie in Daten mit Tiering in Cloud- oder Bandspeicher versetzen.
- Die beschriebene Lösung umfasst keine Knotenreplikation. Wenn die Knotenreplikation zum Sichern eines Speicherpools von Platte auf Platte verwendet werden soll, müssen Sie sicherstellen, dass die Replikationsoperation abgeschlossen ist, bevor Daten von Platte auf Band umgelagert werden. Sie können die Knotenreplikation auch verwenden, um einen Speicherpool auf einer lokalen Bandeinheit in einem Kopienspeicherpool auf einer lokalen Bandeinheit zu sichern.

Implementierungsroadmap

Die folgenden Schritte sind zum Konfigurieren einer bandbasierten Lösung erforderlich.

1. Konfigurieren Sie das System.
2. Installieren Sie den Server und das Operations Center.
3. Konfigurieren Sie den Server und das Operations Center.

4. Schließen Sie Bandeinheiten für den Server an.
5. Konfigurieren Sie Bandarchive für die Verwendung durch den Server.
6. Konfigurieren Sie eine Speicherpoolhierarchie.
7. Installieren und konfigurieren Sie Clients.
8. Konfigurieren Sie die LAN-unabhängige Datenversetzung.
9. Wählen Sie ein Verschlüsselungsverfahren aus und konfigurieren Sie die Verschlüsselung.
10. Konfigurieren Sie Bandspeicheroperationen.
11. Schließen Sie die Implementierung ab.

System konfigurieren

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

Informationen zu diesem Vorgang

Tipp: Es werden Prozeduren zum Konfigurieren des Servers und des Plattenspeichersystems beschrieben. Erste Schritte zum Konfigurieren von Bandeinheiten finden Sie in „Bandeinheiten für den Server anschließen” auf Seite 81.

Speicherhardware konfigurieren

Um Plattenspeicher zu optimieren, prüfen Sie die Richtlinien zum Konfigurieren von Plattenspeicher mithilfe von IBM Spectrum Protect. Stellen Sie dann eine Verbindung zwischen dem Server und den Plattenspeichereinheiten her und führen Sie weitere Konfigurationstasks aus.

Vorbereitende Schritte

Richtlinien zum Konfigurieren von Plattenspeicher finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.

Vorgehensweise

1. Stellen Sie unter Berücksichtigung der folgenden Richtlinien eine Verbindung zwischen dem Server und den Speichereinheiten her:
   - Verwenden Sie einen Switch oder eine Direktverbindung für Fibre Channel-Verbindungen.
   - Berücksichtigen Sie die Anzahl Ports, die verbunden sind, und die erforderliche Bandbreite.
   - Berücksichtigen Sie die Anzahl Ports auf dem Server und die Anzahl Host-Ports auf dem Plattensystem, die verbunden sind.
2. Stellen Sie sicher, dass die Einheitentreiber und die Firmware für das Serversystem, die Adapter und das Betriebssystem aktuell sind und die empfohlenen Versionen haben.
3. Konfigurieren Sie Speicherarrays. Stellen Sie sicher, dass Sie entsprechend geplant haben, um die optimale Leistung zu gewährleisten.

   Weitere Informationen finden Sie in „Planung für Plattenspeicher” auf Seite 12.
4. Stellen Sie sicher, dass das Serversystem Zugriff auf Plattendatenträger hat, die erstellt werden. Führen Sie die folgenden Schritte aus:
   a) Wenn das System mit einem Fibre Channel-Switch verbunden ist, verzonen Sie den Server, um die Platten anzuzeigen.
   b) Ordnen Sie alle Datenträger zu, um dem Plattensystem mitzuteilen, dass diesem spezifischen Server die Anzeige jeder Platte ermöglicht werden soll.

5. Stellen Sie sicher, dass Band- und Platteneinheiten unterschiedliche HBA-Ports verwenden. Steuern Sie die Band- und Platten-E/A mithilfe des Speicherbereichsnetzes (SAN). Verwenden Sie separate Fibre Channel-Ports für Band- und Platten-E/A.

Zugehörige Tasks

Multipath I/O konfigurieren

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

Serverbetriebssystem installieren

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

Installation auf AIX-Systemen

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

Vorgehensweise

1. Installieren Sie AIX Version 7.1, TL4, SP6 oder höher gemäß den Anweisungen des Herstellers.
2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
3. Öffnen Sie die Datei `/etc/hosts` und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

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

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

     ```
     127.0.0.1  localhost
     ```

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

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

   Die Olson-Zeitzonendefinition kann sich auf die Serverleistung auswirken.
5. Um die Leistung zu optimieren, ändern Sie Ihr Systemzeitzonenformat von Olson in POSIX. Verwenden Sie das folgende Befehlsformat zum Aktualisieren der Zeitzoneneinstellung:

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

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

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

6. Stellen Sie sicher, dass in der Datei `.profile` des Instanzbenutzers die folgende Umgebungsvariable festgelegt ist:

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

   In höheren Versionen des IBM Spectrum Protect-Servers wird dieser Wert automatisch beim Start des Servers festgelegt. Wenn der Instanzbenutzer nicht verfügbar ist, führen Sie diesen Schritt zu einem späteren Zeitpunkt aus, wenn der Instanzbenutzer wieder verfügbar ist.
7. Legen Sie fest, dass das System vollständige Anwendungskerndateien erstellen soll. Geben Sie den folgenden Befehl aus:

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

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

   Wenn Sie nicht die Standardwerte für Ports verwenden, stellen Sie sicher, dass die verwendeten Ports offen sind.
9. Aktivieren Sie TCP-Hochleistungsverbesserungen. Geben Sie den folgenden Befehl aus:

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

10. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, kombinieren Sie für ein mittelgroßes System zwei 10-Gb-Ethernet-Ports durch Bonding miteinander und für ein großes System vier 10-Gb-Ethernet-Ports. Verwenden Sie das System Management Interface Tool (SMIT), um die Ports durch Bonding unter Verwendung von Etherchannel zu kombinieren.

    Beim Testen wurden die folgenden Einstellungen verwendet:

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

11. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 11 auf Seite 34 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 11. Benutzergrenzwerte (ulimit-Werte)

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

Tabelle 11. Benutzergrenzwerte (ulimit-Werte) (Forts.)			
Typ des Benutzergrenzwerts	**Einstellung**	**Wert**	**Befehl zum Abfragen des Werts**
Maximale Anzahl Benutzerprozesse	`nproc`	16384	`ulimit -Hu`

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

Installation auf Linux-Systemen

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

Vorbereitende Schritte

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

Vorgehensweise

1. Installieren Sie Red Hat Enterprise Linux Version 7.8 oder höher bzw. Version 8.2 oder höher gemäß den Anweisungen des Herstellers.

   Fordern Sie eine bootfähige DVD an, die Red Hat Enterprise Linux mit einer unterstützten Version enthält, und starten Sie Ihr System von dieser DVD. Für Installationsoptionen siehe die folgende Anleitung. Wenn ein Element in der folgenden Liste nicht aufgeführt ist, übernehmen Sie die Standardauswahl unverändert.

   a) Wählen Sie nach dem Starten der DVD im Menü **Install or upgrade an existing system** (Installation oder Aktualisierung eines bestehenden Systems) aus.

   b) Wählen Sie in der Eingangsanzeige **Test this media & install Red Hat Enterprise Linux 7.8** (Diese Medien überprüfen & Red Hat Enterprise Linux 7.8 installieren) aus.

   c) Wählen Sie Ihre Sprache und Tastaturbelegung aus.

   d) Wählen Sie Ihren Standort aus, um die korrekte Zeitzone festzulegen.

   e) Wählen Sie **Software Selection** (Softwareauswahl) und in der nächsten Anzeige **Server with GUI** (Server mit GUI) aus.

   f) Klicken Sie auf der Installationszusammenfassungsseite auf **Installation Destination** (Installationsziel) und überprüfen Sie die folgenden Einträge:

   - Die lokale 300-GB-Platte ist als Installationsziel ausgewählt.
   - Unter 'Other Storage Options' (Weitere Speicheroptionen) ist `Automatically configure partitioning` (Partitionierung automatisch konfigurieren) ausgewählt.

   Klicken Sie auf **Done** (Fertig).

   g) Klicken Sie auf **Begin Installation** (Installation starten).

   Legen Sie nach dem Start der Installation das Rootkennwort für Ihr Rootbenutzerkonto fest.

   Führen Sie nach dem Abschluss der Installation einen Neustart für das System durch und melden Sie sich als Rootbenutzer an. Geben Sie den Befehl **df** aus, um die Basispartitionierung zu überprüfen.

   Auf einem Testsystem hatte die Erstpartitionierung beispielsweise das folgende Ergebnis zur Folge:

```
[root@tvapp02]# df –h
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root    50G  3.0G   48G   6% /
devtmpfs                 32G     0   32G   0% /dev
tmpfs                    32G   92K   32G   1% /dev/shm
```

```
tmpfs                    32G  8.8M   32G   1% /run
tmpfs                    32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home   220G   37M  220G   1% /home
/dev/sda1               497M  124M  373M  25% /boot
```

2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.

   Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, sollten Sie das Bonding mehrerer Netzports in Erwägung ziehen. Kombinieren Sie für ein mittelgroßes System zwei Ports durch Bonding und für ein großes System vier Ports. Erstellen Sie dazu eine LACP-Netzverbindung (LACP = Link Aggregation Control Protocol), bei der mehrere untergeordnete Ports in einer einzigen logischen Verbindung aggregiert werden. Die bevorzugte Methode ist die Verwendung des Bondmodus 802.3ad, des Werts 100 für die Einstellung **miimon** und der Angabe 'layer3+4' für die Einstellung **xmit_hash_policy**.

   Einschränkung: Um eine LACP-Netzverbindung verwenden zu können, muss ein Netzswitch vorhanden sein, der LACP unterstützt.

   Weitere Anweisungen zur Konfiguration von Bonding-Netzverbindungen mit Red Hat Enterprise Linux Version 7 finden Sie unter Create a Channel Bonding Interface.
3. Öffnen Sie die Datei `/etc/hosts` und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```
   - Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

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

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```
   b) Überprüfen Sie, ob die DVD bereitgestellt wurde, indem Sie den Befehl **mount** ausgeben.
      Es sollte eine ähnliche Ausgabe wie in dem folgenden Beispiel angezeigt werden:

      ```
      /dev/sr0 on /mnt type iso9660
      ```
   c) Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

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

      Für RHEL 8:

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

      Wenn das Verzeichnis `repos.d` nicht vorhanden ist, erstellen Sie es.
   d) Listen Sie den Verzeichnisinhalt auf:

      ```
      ls rhel-source.repo
      ```
   e) Benennen Sie die ursprüngliche repo-Datei um, indem Sie den Befehl **mv** ausgeben.
      Beispiel:

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

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

```
vi rhel78_dvd.repo
```

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

```
[rhel78_dvd]
name=DVD Redhat Enterprise Linux 7.8
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

Für RHEL 8:

```
[InstallMedia-BaseOS]
name=Red Hat Enterprise Linux 8.2.0
mediaid=None
metadata_expire=-1
gpgcheck=0
cost=500
enabled=1
baseurl=file:///mnt/BaseOS/

[InstallMedia-AppStream]
name=Red Hat Enterprise Linux 8.2.0
mediaid=None
metadata_expire=-1
gpgcheck=0
cost=500
enabled=1
baseurl=file:///mnt/AppStream/
```

h) Installieren Sie zusätzliche vorausgesetzte Softwarepakete, indem Sie den Befehl **yum** ausgeben. Beispiel:

```
yum install ksh.x86_64
yum install sysstat
Für RHEL 8:
yum install libnsl
```

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

```
unmount /mnt
```

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

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

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

```
mv rhel78_dvd.repo rhel78_dvd.repo.orig
```

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

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

6. Bestimmen Sie, ob Änderungen an Kernelparametern erforderlich sind. Führen Sie die folgenden Schritte aus:
   a) Listen Sie mithilfe des Befehls **sysctl -a** die Parameterwerte auf.
   b) Analysieren Sie die Ergebnisse anhand der Richtlinien in Tabelle 12 auf Seite 38, um zu bestimmen, ob Änderungen erforderlich sind.

c) Wenn Änderungen erforderlich sind, definieren Sie die Parameter in der Datei `/etc/sysctl.conf`.

Die Dateiänderungen werden angewendet, wenn das System gestartet wird.

Tipp: Passen Sie Kernelparametereinstellungen automatisch an und eliminieren Sie die Notwendigkeit manueller Aktualisierungen dieser Einstellungen. Unter Linux passt die Db2-Datenbanksoftware automatisch die Werte der Kernelparameter für die Interprozesskommunikation (IPC) an und setzt sie auf die bevorzugten Einstellungen. Weitere Informationen zu Kernelparametereinstellungen finden Sie bei Verwendung des Suchbegriffs Linux-Kernelparameter im Produktdokumentation zu Version 11.5.

Tabelle 12. Optimale Einstellungen für Linux-Kernelparameter

Parameter	Beschreibung
kernel.shmmni	Die maximale Anzahl Segmente.
kernel.shmmax	Die maximale Größe eines gemeinsam genutzten Speichersegments (Byte). Dieser Parameter muss definiert werden, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird.
kernel.shmall	Die maximale Zuordnung von Seiten im gemeinsam genutzten Speicher (Seiten).
kernel.sem Für den Parameter **kernel.sem** gibt es vier Werte.	(SEMMSL) Die maximale Anzahl Semaphore pro Array.
	(SEMMNS) Die maximale Anzahl Semaphore pro System.
	(SEMOPM) Die maximale Anzahl Operationen pro Semaphoraufruf.
	(SEMMNI) Die maximale Anzahl Arrays.
kernel.msgmni	Die maximale Anzahl systemweiter Nachrichtenwarteschlangen.
kernel.msgmax	Die maximale Größe von Nachrichten (Byte).
kernel.msgmnb	Die standardmäßige maximale Größe der Warteschlange (Byte).
kernel.randomize_va_space	Mit dem Parameter **kernel.randomize_va_space** wird die Verwendung von Speicher-ASLR für den Kernel konfiguriert. Aktivieren Sie ASLR für Server der Version 7.1 und höher. Weitere ausführliche Informationen zu Linux-ASLR und Db2 finden Sie in der Technote 1365583.
vm.swappiness	Der Parameter **vm.swappiness** definiert, ob der Kernel Anwendungsspeicher aus physischem Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern enthält die Db2-Produktinformation.
vm.overcommit_memory	Der Parameter **vm.overcommit_memory** hat Auswirkungen darauf, wie viel virtueller Speicher gemäß dem Kernel zugeordnet werden kann. Weitere Informationen zu Kernelparametern enthält die Db2-Produktinformation.

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

      Geben Sie den folgenden Befehl aus:

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

   b) Um die Standardportadresse für die Kommunikation mit dem Server zu verwenden, öffnen Sie TCP/IP-Port 1500 in der Linux-Firewall.

      Geben Sie den folgenden Befehl aus:

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

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

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

      Geben Sie den folgenden Befehl aus:

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

   d) Laden Sie die Firewalldefinitionen erneut, damit die Änderungen wirksam werden.

      Geben Sie den folgenden Befehl aus:

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

8. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 13 auf Seite 39 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 13. Benutzergrenzwerte (ulimit-Werte)

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

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

Installation auf Windows-Systemen

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

Vorgehensweise

1. Installieren Sie Windows Server 2016 oder 2019 Standard Edition gemäß den Anweisungen des Herstellers.
2. Ändern Sie die Windows-Kontensteuerungsrichtlinien, indem Sie die folgenden Schritte ausführen.
   a) Öffnen Sie den Editor für lokale Sicherheitsrichtlinien, indem Sie `secpol.msc` ausführen.
   b) Klicken Sie auf **Lokale Richtlinien** > **Sicherheitsoptionen** und stellen Sie sicher, dass die folgenden Benutzerkontensteuerungsrichtlinien inaktiviert sind:
      - Administratorbestätigungsmodus für das integrierte Administratorkonto
      - Alle Administratoren im Administratorbestätigungsmodus ausführen
3. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Installationsanweisungen für das Betriebssystem.
4. Wenden Sie Windows-Updates an und aktivieren Sie Zusatzfunktionen (optionale Features), indem Sie die folgenden Schritte ausführen:
   a) Wenden Sie die neuesten Windows Server-Updates an.
   b) Aktualisieren Sie, falls erforderlich, die FC- und Ethernet-HBA-Einheitentreiber mit neueren Versionen.
5. Öffnen Sie den TCP/IP-Standardport (1500) für die Kommunikation mit dem IBM Spectrum Protect-Server.
   Geben Sie beispielsweise den folgenden Befehl aus:

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

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

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

Multipath I/O konfigurieren

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

AIX-Systeme

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

Vorgehensweise

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

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

- Geben Sie auf großen Systemen die folgenden Befehle aus:

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

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

```
cfgmgr
```

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

```
lsdev -Ccdisk
```

   Die Ausgabe sieht ähnlich wie die in dem folgenden Beispiel aus:

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

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

   Beispielsweise könnte eine Einheiten-ID `hdisk4` lauten. Sichern Sie die Liste der Einheiten-IDs für die Verwendung bei der Erstellung von Dateisystemen für den IBM Spectrum Protect-Server.
6. Korrelieren Sie die SCSI-Einheiten-IDs zu bestimmten Platten-LUNs aus dem Plattensystem, indem Sie detaillierte Informationen zu allen physischen Datenträgern im System auflisten. Geben Sie den folgenden Befehl aus:

```
lspv -u
```

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

```
hdisk4  00f8cf083fd97327  None  active
 3321360050763008101057800000000000030042145O3IBMfcp
```

   In dem Beispiel ist *600507630081010578000000000000030* die UID für den Datenträger, die von der Storwize-Managementschnittstelle zurückgemeldet wurde.

   Um die Plattengröße in Megabyte zu überprüfen und den Wert mit dem für das System aufgelisteten Wert zu vergleichen, geben Sie den folgenden Befehl aus:

```
bootinfo -s hdisk4
```

Linux-Systeme

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

Vorgehensweise

1. Editieren Sie die Datei `/etc/multipath.conf`, um Multipathing für Linux-Hosts zu aktivieren.

Wenn die Datei `multipath.conf` nicht vorhanden ist, können Sie die Datei erstellen, indem Sie den folgenden Befehl ausgeben:

```
mpathconf --enable
```

Die folgenden Parameter wurden in `multipath.conf` zu Testzwecken auf einem IBM FlashSystem-Speichersystem festgelegt:

```
defaults {
         user_friendly_names no
}

devices {
         device {
                  vendor "IBM "
                  product "2145"
                  path_grouping_policy group_by_prio
                  user_friendly_names no
                  path_selector "round-robin 0"
                  prio "alua"
                  path_checker "tur"
                  failback "immediate"
                  no_path_retry 5
                  rr_weight uniform
                  rr_min_io_rq "1"
                  dev_loss_tmo 120
        }
}
```

2. Definieren Sie die Multipath-Option so, dass Multipath zusammen mit dem System gestartet wird.

   Geben Sie die folgenden Befehle aus:

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

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

   ```
   multipath -l
   ```

4. Stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.

   Beispielsweise zeigt die folgende Ausgabe, dass einer 2-TB-Platte zwei Pfadgruppen und vier aktive Pfade zugeordnet sind. Die Größe von 2 TB bestätigt, dass die Platte einem Pooldateisystem entspricht. Suchen Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 12) in der Managementschnittstelle des Plattensystems nach dem Datenträger.

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

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

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

   Sie können für eine erneute Überprüfung der Platten-LUN/Host-Zuordnungen auch das System erneut starten.

   b) Stellen Sie sicher, dass Platten jetzt für Multipath I/O verfügbar sind, indem Sie den Befehl **multipath -l** erneut ausgeben.

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

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

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

Windows-Systeme

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

Vorgehensweise

1. Stellen Sie sicher, dass Multipath I/O installiert ist. Installieren Sie, falls erforderlich, weitere anbieterspezifische Multipath-Treiber. Verwenden Sie für IBM FlashSystem-Einheiten das Microsoft-DSM (Microsoft Device Specific Module = Gerätespezifisches Modul von Microsoft). Installationsanweisungen enthält die Dokumentation zu IBM FlashSystem (https://www.ibm.com/support/knowledgecenter/STHGUJ_8.3.1/com.ibm.storwize.v5000.831.doc/svc_w2kmpio_21oxvp.html).
2. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath I/O verwaltet werden, öffnen Sie eine Microsoft Windows PowerShell-Eingabeaufforderung und geben Sie den folgenden Befehl aus:

   ```
   mpclaim -e
   ```

3. Überprüfen Sie die Ausgabe des Befehls mpclaim und stellen Sie sicher, dass sich der IBM Speicher unter MPIO-Steuerung befindet.

   ```
   "Ziel-Hardware-ID        "   Bustyp       Mit MPIO     ALUA-Unterstützung
   -------------------------------------------------------------------------------
   "IBM     2145            "   SAS          Ja           Nur implizit
   ```

4. Weitere Details zu zugeordneten Platteneinheiten können mithilfe des Windows-Befehl wmic abgerufen werden.

   ```
   wmic diskdrive get
   ```

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

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

Benutzer-ID für den Server erstellen

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

Informationen zu diesem Vorgang

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

- Die Länge darf 8 Zeichen nicht überschreiten.

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

Vorgehensweise

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

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

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

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

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

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

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

     ```
     net localgroup Administratoren tsminst1 /add
     net localgroup DB2ADMNS tsminst1 /add
     ```
2. Melden Sie die neue Benutzer-ID ab.

Dateisysteme für den Server vorbereiten

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

AIX-Systeme

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

Vorgehensweise

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

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

Sie dürfen diese Befehle nicht für interne Betriebssystemplatten, beispielsweise *hdisk0*, ausführen.

2. Erstellen Sie Datenträgergruppen für die IBM Spectrum Protect-Datenbank, die aktive Protokolldatei, das Archivprotokoll, die Datenbanksicherung und den Speicherpool. Geben Sie den Befehl **mkvg** unter Angabe der Einheiten-IDs für die entsprechenden zuvor ermittelten Platten aus.

   Wenn beispielsweise die Einheitennamen *hdisk4, hdisk5* und *hdisk6* Datenbankplatten entsprechen, schließen Sie diese in die Datenbankdatenträgergruppe ein.

   Systemgröße: Die folgenden Befehle basieren auf einer Konfiguration für ein mittelgroßes System. Für kleine und große Systeme müssen Sie die Syntax wie erforderlich anpassen.

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

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

   Beispiel:

   ```
   lsvg -p tsmdb
   ```

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

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

4. Erstellen Sie mit dem Befehl **mklv** logische Datenträger in jeder Datenträgergruppe. Die Datenträgergröße, die Datenträgergruppe und die Einheitennamen sind, abhängig von der Größe Ihres Systems und Variationen in Ihrer Plattenkonfiguration, unterschiedlich.

   Um beispielsweise die Datenträger für die IBM Spectrum Protect-Datenbank auf einem mittelgroßen System zu erstellen, geben Sie die folgenden Befehle aus:

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

5. Formatieren Sie Dateisysteme auf jedem logischen Datenträger mit dem Befehl **crfs**.

   Um beispielsweise die Dateisysteme für die Datenbank auf einem mittelgroßen System zu formatieren, geben Sie die folgenden Befehle aus:

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

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

   ```
   mount -a
   ```

7. Listen Sie alle Dateisysteme auf, indem Sie den Befehl **df** ausgeben.

   Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.

   Das folgende Beispiel der Befehlsausgabe zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

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

8. Überprüfen Sie, ob die in „Benutzer-ID für den Server erstellen” auf Seite 43 erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den Server hat.

Linux-Systeme

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

Vorgehensweise

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

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

   Formatieren Sie für Speicherpool-LUNs `xfs`-Dateisysteme:

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

   Abhängig davon, wie viele verschiedene Einheiten vorhanden sind, können Sie den Befehl **mkfs** bis zu 50 Mal ausgeben.
2. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

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

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

   ```
   mkdir /tsminst1
   ```

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

   Beispiel:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 de
   faults 0 0
   ```
4. Führen Sie für die Dateisysteme, die der Datei `/etc/fstab` hinzugefügt wurden, einen Mount durch, indem Sie den Befehl **mount -a** ausgeben.
5. Listen Sie alle Dateisysteme auf, indem Sie den Befehl **df** ausgeben.

   Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.

   Das folgende Beispiel für ein IBM Storwize-System zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Filesystem                                      Size  Used Avail Use% Mounted on
   /dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%   /tsminst1/
   TSMalog
   ```
6. Überprüfen Sie, ob die in „Benutzer-ID für den Server erstellen” auf Seite 43 erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den IBM Spectrum Protect-Server hat.

Windows-Systeme

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

Vorgehensweise

1. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

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

   ```
   md c:\tsminst1
   ```

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

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

   a) Schalten Sie die Platte online.

   b) Initialisieren Sie die Platte mit dem GPT-Basistyp, dem Standardwert.

   c) Erstellen Sie einen einfachen Datenträger, der den gesamten Speicherbereich auf der Platte belegt. Formatieren Sie das Dateisystem mit NTFS und ordnen Sie einen Kennsatz zu, der den Zweck des Datenträgers angibt, wie beispielsweise `TSMfile00`. Ordnen Sie den neuen Datenträger keinem Laufwerkbuchstaben zu. Ordnen Sie den Datenträger stattdessen einem Verzeichnis unter dem Instanzverzeichnis zu, wie beispielsweise `C:\tsminst1\TSMfile00`.

      Tipp: Legen Sie den Datenträgerkennsatz und die Bezeichnungen für Verzeichniszuordnungen auf der Basis der Größe der aufgelisteten Platte fest.
3. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Listen Sie alle Dateisysteme auf, indem Sie den Befehl **mountvol** ausgeben; überprüfen Sie dann die Ausgabe.
   Beispiel:

   ```
   \\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
     C:\tsminst1\TSMdbspace00\
   ```
4. Starten Sie nach dem Abschluss der Plattenkonfiguration das System erneut.

Nächste Schritte

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

Server und das Operations Center installieren

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

Installation auf AIX- und Linux-Systemen

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

Vorbereitende Schritte

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

Vorgehensweise

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

   Ausführliche Informationen finden Sie in „Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren” auf Seite 49.
2. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden.

   Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 588093.
3. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
4. Stellen Sie sicher, dass für das Paket die Berechtigung zur Ausführung festgelegt ist. Ändern Sie, falls erforderlich, die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

   ```
   chmod a+x Paketname.bin
   ```
5. Extrahieren Sie das Paket, indem Sie den folgenden Befehl ausgeben:

   ```
   ./Paketname.bin
   ```

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

   ```
   lsuser
   ```

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

   ```
   ./install.sh
   ```

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

Nächste Schritte

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

  Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf **Datei** > **Protokoll anzeigen**. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf **Hilfe** > **Daten zur Fehleranalyse exportieren**.
- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die -Unterstützungssite auf. Klicken Sie auf **Support und Downloads** und wenden Sie alle zutreffenden Fixes an.

AIX Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren

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

Vorgehensweise

1. Überprüfen Sie, ob die folgenden Dateien auf Ihrem System installiert sind. Wenn die Dateien nicht installiert sind, fahren Sie mit Schritt 2 fort.

```
atk-1.12.3-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
pango-1.14.5-4.aix5.2.ppc.rpm
pixman-0.12.0-3.aix5.2.ppc.rpm
xcursor-1.1.7-3.aix5.2.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
xrender-0.9.1-3.aix5.2.ppc.rpm
zlib-1.2.3-3.aix5.1.ppc.rpm
```

2. Stellen Sie sicher, dass mindestens 150 MB freier Speicherbereich im Dateisystem `/opt` vorhanden sind.
3. Wechseln Sie von dem Verzeichnis, in das die Installationspaketdatei extrahiert wird, in das Verzeichnis `gtk`.
4. Laden Sie die RPM-Dateien von der Website für IBM AIX Toolbox for Linux Applications in das aktuelle Arbeitsverzeichnis herunter, indem Sie den folgenden Befehl ausgeben:

```
download-prerequisites.sh
```

5. Geben Sie in dem Verzeichnis, das die heruntergeladenen RPM-Dateien enthält, den folgenden Befehl aus, um die Dateien zu installieren:

```
rpm -Uvh *.rpm
```

Installation auf Windows-Systemen

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

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

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

Vorgehensweise

1. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden.

   Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 588095.
2. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
3. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
4. Doppelklicken Sie auf die ausführbare Datei, um die Datei in das aktuelle Verzeichnis zu extrahieren.
5. Starten Sie in dem Verzeichnis, in das die Installationsdateien extrahiert wurden, den Installationsassistenten, indem Sie auf die Datei `install.bat` doppelklicken.

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

Nächste Schritte

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

  Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf **Datei** > **Protokoll anzeigen**. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf **Hilfe** > **Daten zur Fehleranalyse exportieren**.
- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die -Unterstützungssite auf. Klicken Sie auf **Support und Downloads** und wenden Sie alle zutreffenden Fixes an.

Server und das Operations Center konfigurieren

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

Serverinstanz konfigurieren

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

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

Linux AIX

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

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

1. Klicken Sie auf **Start** > **Verwaltung** > **Dienste**. Wählen Sie im Fenster **Dienste Remoteregistrierung** aus. Wurde der Dienst nicht gestartet, klicken Sie auf **Starten**.
2. Stellen Sie sicher, dass die Ports 137, 139 und 445 nicht durch eine Firewall blockiert sind:
   a. Klicken Sie auf **Start** > **Systemsteuerung** > **Windows-Firewall**.
   b. Wählen Sie **Erweiterte Einstellungen** aus.
   c. Wählen Sie **Eingehende Regeln** aus.
   d. Wählen Sie **Neue Regel** aus.

e. Erstellen Sie eine Portregel für die TCP-Ports 137, 139 und 445, um Verbindungen für Domänennetze und private Netze zu ermöglichen.

3. Konfigurieren Sie die Benutzerkontensteuerung, indem Sie auf die Optionen für die lokale Sicherheitsrichtlinie zugreifen und die folgenden Schritte ausführen.

   a. Klicken Sie auf **Start** > **Verwaltung** > **Lokale Sicherheitsrichtlinie**. Erweitern Sie **Lokale Richtlinien** > **Sicherheitsoptionen**.

   b. Falls noch nicht bereits aktiviert, aktivieren Sie das integrierte Administratorkonto, indem Sie **Konten: Administratorkontostatus** > **Aktivieren** > **OK** auswählen.

   c. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren, indem Sie **Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen** > **Inaktivieren** > **OK** auswählen.

   d. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto, indem Sie **Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto** > **Inaktivieren** > **OK** auswählen.

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

Informationen zu diesem Vorgang

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

Vorgehensweise

1. Starten Sie die lokale Version des Assistenten.

   - Linux AIX Öffnen Sie das Programm `dsmicfgx` im Verzeichnis `/opt/tivoli/tsm/server/bin`. Dieser Assistent kann nur als Rootbenutzer ausgeführt werden.
   - Windows Klicken Sie auf **Start** > **Alle Programme** > **IBM Spectrum Protect** > **Konfigurationsassistent**.

2. Führen Sie die Anweisungen aus, um die Konfiguration auszuführen.

   Verwenden Sie die während der IBM Spectrum Protect-Systemkonfiguration aufgezeichneten Informationen (siehe „Arbeitsblätter zur Planung" auf Seite 8), um Verzeichnisse und Optionen im Assistenten anzugeben.

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

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

Client für Sichern/Archivieren installieren

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

Prozedur

- Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.
  - UNIX- und Linux-Clients für Sichern/Archivieren installieren
  - Erstinstallation des Windows-Clients

Optionen für den Server festlegen

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

Vorgehensweise

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

Serveroption	Wert
ACTIVELOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad
ACTIVELOGSIZE	131072
ARCHLOGCOMPRESS	No
ARCHLOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad
COMMMETHOD	TCPIP
COMMTIMEOUT	3600
DEVCONFIG	`devconf.dat`
EXPINTERVAL	0
IDLETIMEOUT	60
MAXSESSIONS	500
NUMOPENVOLSALLOWED	20
TCPADMINPORT	1500
TCPPORT	1500
VOLUMEHISTORY	`volhist.dat`

Aktualisieren Sie, falls erforderlich, Serveroptionseinstellungen in Übereinstimmung mit den Werten in der Tabelle. Um Aktualisierungen durchzuführen, schließen Sie die Datei `dsmserv.opt` und definieren Sie die Optionen mit dem Befehl **SETOPT** in der Verwaltungsbefehlszeilenschnittstelle.

Um beispielsweise die Option `IDLETIMEOUT` mit 60 zu aktualisieren, geben Sie den folgenden Befehl aus:

```
setopt idletimeout 60
```

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

Serveroption	Alle Systemgrößen
SSLDISABLELEGACYTLS	YES
SSLFIPSMODE	NO
SSLTCPPORT	Geben Sie die SSL-Portnummer an. Der TCP/IP-DFV-Treiber des Servers wartet an diesem Port auf Anforderungen für SSL-fähige Sitzungen vom Client.

Serveroption	Alle Systemgrößen
SSLTCPADMINPORT	Geben Sie die Adresse des Ports an, an dem der Server auf Anforderungen von SSL-fähigen Sitzungen des Verwaltungsbefehlszeilenclients wartet.
TLS12	YES

Wenn einer der Optionswerte aktualisiert werden muss, editieren Sie die Datei `dsmserv.opt` unter Verwendung der folgenden Anleitungen:

- Entfernen Sie den Stern am Anfang einer Zeile, um eine Option zu aktivieren.
- Geben Sie in jeder Zeile nur eine einzige Option und den für die Option angegebenen Wert ein.
- Wenn eine Option in mehreren Einträgen in der Datei vorkommt, verwendet der Server den letzten Eintrag.

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

Sicherheitskonzepte

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

Tipp: In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

Einschränkung: Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer IBM Db2-Datenbankinstanz verwenden, die von einem IBM Spectrum Protect-Server verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdiges selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

Berechtigungsstufen

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl **GRANT AUTHORITY** Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl **UPDATE NODE** die Knoteneinstellungen, um Sicherungen zu ermöglichen.

Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Tabelle 14. Merkmale der Kennwortauthentifizierung

Merkmale	**Weitere Informationen**
Abhängigkeit von der Groß-/Kleinschreibung	Nicht von der Groß-/Kleinschreibung abhängig.
Standardwert für Kennwortablauf	90 Tage. Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden.
Ungültige Kennworteingabeversuche	Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.
Standardlänge des Kennworts	8 Zeichen. Der Administrator kann eine Mindestlänge angeben. Ab Version 8.1.4 hat sich die Standardmindestlänge für Serverkennwörter von 0 in 8 Zeichen geändert.

Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter **SESSIONSECURITY** festgelegt wird.

Der Parameter **SESSIONSECURITY** kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn **SESSIONSECURITY=TRANSITIONAL** angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Anmerkung: Es ist nicht erforderlich, für Clients für Sichern/Archivieren eine Aktualisierung auf Version 8.1.2 oder höher durchzuführen, bevor ein Upgrade für Server erfolgt. Nachdem für einen Server ein Upgrade auf Version 8.1.2 oder höher durchgeführt wurde, kommunizieren Knoten und Administratoren, die frühere Versionen der Software verwenden, weiterhin mit dem Server unter Verwendung des Werts TRANSITIONAL, bis die Entität die Voraussetzungen für den Wert STRICT erfüllt. Dementsprechend können Sie für Clients für Sichern/Archivieren ein Upgrade auf Version 8.1.2 oder höher durchführen, bevor Sie ein Upgrade für Ihre IBM Spectrum Protect-Server durchführen; es ist jedoch nicht erforderlich, zuerst ein Upgrade für Server durchzuführen. Die Kommunikation zwischen Servern und Clients wird nicht unterbrochen.

Weitere Informationen zu den Werten für den Parameter **SESSIONSECURITY** enthalten die Beschreibungen der folgenden Befehle.

Tabelle 15. Befehle zum Festlegen des Parameters SESSIONSECURITY

Entität	**Befehl**
Clientknoten	• REGISTER NODE • UPDATE NODE
Administratoren	• REGISTER ADMIN • UPDATE ADMIN
Server	• DEFINE SERVER • UPDATE SERVER

Administratoren, die sich unter Verwendung des Befehls **DSMADMC**, des Befehls **DSMC** oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:

Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator unter Verwendung von Software der Version 8.1.2 oder höher oder Software der Version 7.1.8 oder höher erfolgreich beim Server authentifiziert hat, kann sich der Administrator nicht mehr mit Client- oder Serverversionen vor Version 8.1.2 oder Version 7.1.8 bei diesem Server authentifizieren. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls **SELECT** können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

Zugehörige Informationen

Kommunikation schützen

Sichere Kommunikation mit Transport Layer Security konfigurieren

Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem

Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.

Informationen zu diesem Vorgang

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

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

Operations Center konfigurieren

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

Vorbereitende Schritte

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

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

Vorgehensweise

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

   Führen Sie die Anweisungen in „Kommunikation zwischen dem Operations Center und dem Hub-Server schützen” auf Seite 57 aus.
2. Legen Sie den Hub-Server fest.

   Geben Sie in einem Web-Browser die folgende Adresse ein:

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

   Erläuterungen:

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

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

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

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

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

   Führen Sie die Anweisungen in „Systemstatus mithilfe von E-Mail-Berichten verfolgen” auf Seite 168 aus.

Kommunikation zwischen dem Operations Center und dem Hub-Server schützen

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

Vorbereitende Schritte

Die Truststore-Datei des Operations Center ist ein Container für Zertifikate, auf die vom Operations Center zugegriffen werden kann. Während der Installation des Operations Center müssen Sie ein Kennwort für die Truststore-Datei erstellen. Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen. Wenn Sie dieses Kennwort vergessen haben, müssen Sie es jetzt erneut erstellen und die Truststore-Datei konfigurieren. Anweisungen finden Sie in Kennwort für die Truststore-Datei des Operations Center löschen und erneut zuordnen.

Die folgende Abbildung zeigt die Komponenten für die Konfiguration einer Secure Sockets Layer-(SSL-)Verbindung zwischen dem Hub-Server und dem Operations Center.

Informationen zu diesem Vorgang

Diese Prozedur stellt Schritte zur Implementierung der sicheren Kommunikation mithilfe selbst signierter Zertifikate bereit.

Wenn Sie Zertifikate verwenden, die von einer Zertifizierungsstelle (CA) signiert wurden, führen Sie die Anweisungen in Kommunikation zwischen dem Operations Center und dem Hub-Server mithilfe CA-signierter Zertifikate schützen aus.

Vorgehensweise

Um die SSL-Kommunikation mithilfe selbst signierter Zertifikate zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den Web-Server des Operations Center.
2. Öffnen Sie auf dem System, auf dem das Operations Center installiert ist, die Betriebssystem-Befehlszeile und wechseln Sie in das folgende Verzeichnis:

- Linux AIX *Installationsverzeichnis*/ui/jre/bin
- Windows *Installationsverzeichnis*\ui\jre\bin

Dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist.

3. Öffnen Sie das Fenster 'IBM Key Management', indem Sie den folgenden Befehl ausgeben:

```
ikeyman
```

4. Klicken Sie auf **Key Database File** > **Open** (Schlüsseldatenbankdatei > Öffnen).
5. Klicken Sie auf **Browse** (Durchsuchen) und wechseln Sie in das folgende Verzeichnis; dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist:
   - Linux AIX *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer
6. Wählen Sie im Verzeichnis `guiServer` die Datei `gui-truststore.jks` aus.
7. Klicken Sie auf **Open** (Öffnen) und klicken Sie auf **OK**.
8. Geben Sie das Kennwort für die Truststore-Datei ein und klicken Sie auf **OK**.
9. Klicken Sie im Bereich **Key database content** (Inhalt der Schlüsseldatenbank) des Fensters 'IBM Key Management' auf den Pfeil und wählen Sie **Signer Certificates** (Unterzeichnerzertifikate) aus der Liste aus. Klicken Sie auf **Add** (Hinzufügen).
10. Klicken Sie im Fenster 'Open' (Öffnen) auf **Browse** (Durchsuchen) und wechseln Sie in das Verzeichnis der Hub-Server-Instanz, das von dem Administrator angegeben wurde, von dem die Instanz erstellt wurde. Beispiel:
    - Linux AIX `home/tsminst1`
    - Windows `c:\Programme\Tivoli\TSM\server1`

    Das Verzeichnis enthält das Zertifikat `cert256.arm`.

    Wenn der Zugriff auf das Verzeichnis der Hub-Server-Instanz über das Fenster 'Open' (Öffnen) nicht möglich ist, führen Sie die folgenden Schritte aus:

    a) Kopieren Sie mithilfe von FTP oder einer anderen Dateiübertragungsmethode die `cert256.arm`-Dateien aus dem Instanzverzeichnis des Hub-Servers in das folgende Verzeichnis auf dem Computer, auf dem das Operations Center installiert ist:
       - Linux AIX *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
       - Windows *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

    b) Wechseln Sie im Fenster 'Open' (Öffnen) in das Verzeichnis `guiServer`.
11. Wählen Sie das Zertifikat `cert256.arm` als SSL-Zertifikat aus.
12. Klicken Sie auf **Open** (Öffnen) und klicken Sie auf **OK**.
13. Geben Sie eine Zertifikatsbezeichnung ein. Geben Sie beispielsweise den Namen des Hub-Servers ein.
14. Klicken Sie auf **OK**. Das SSL-Zertifikat des Hub-Servers wird der Truststore-Datei hinzugefügt; die Bezeichnung wird im Bereich **Key database content** (Inhalt der Schlüsseldatenbank) des Fensters 'IBM Key Management' angezeigt.
15. Schließen Sie das Fenster 'IBM Key Management'.
16. Starten Sie den Web-Server des Operations Center.

    Wenn Sie zum ersten Mal die Verbindung zum Operations Center herstellen, werden Sie zur Angabe der IP-Adresse oder des Netznamens des Hub-Servers sowie zur Angabe der Portnummer für die Kommunikation mit dem Hub-Server aufgefordert. Wenn die Serveroption ADMINONCLIENTPORT für den IBM Spectrum Protect-Server aktiviert ist, geben Sie die durch die Serveroption TCPADMINPORT angegebene Portnummer an. Wenn die Serveroption ADMINONCLIENTPORT nicht aktiviert ist, geben Sie die durch die Serveroption TCPPORT angegebene Portnummer an.

Produktlizenz registrieren

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

Informationen zu diesem Vorgang

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

Vorgehensweise

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

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

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

Nächste Schritte

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

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

Datenaufbewahrungsregeln für Ihr Unternehmen definieren

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

Vorgehensweise

1. Wählen Sie auf der Seite **Services** im Operations Center die Domäne STANDARD aus und klicken Sie auf **Details**.
2. Klicken Sie auf der Seite **Zusammenfassung** für die Maßnahmendomäne auf die Registerkarte **Maßnahmengruppen**.
   Die Seite **Maßnahmengruppen** gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche **Konfigurieren** und führen Sie die folgenden Änderungen durch:
   - Ändern Sie das Sicherungsziel für die Verwaltungsklasse STANDARD in den Verzeichniscontainerspeicherpool.

- Ändern Sie den Wert für die Spalte 'Sicherungen' in **Keine Begrenzung**.
- Ändern Sie den Aufbewahrungszeitraum. Setzen Sie den Wert für die Spalte 'Zusätzliche Sicherungen aufbewahren' abhängig von Ihren Geschäftsanforderungen auf 30 Tage oder mehr.

4. Sichern Sie Ihre Änderungen und klicken Sie erneut auf die Umschaltfläche **Konfigurieren**, damit die Maßnahmengruppe nicht mehr editierbar ist.
5. Aktivieren Sie die Maßnahmengruppe, indem Sie auf **Aktivieren** klicken.

Zeitpläne für Serververwaltungsaktivitäten definieren

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

Informationen zu diesem Vorgang

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

Die folgende Abbildung zeigt ein Beispiel für die Planung von Verwaltungsoperationen.

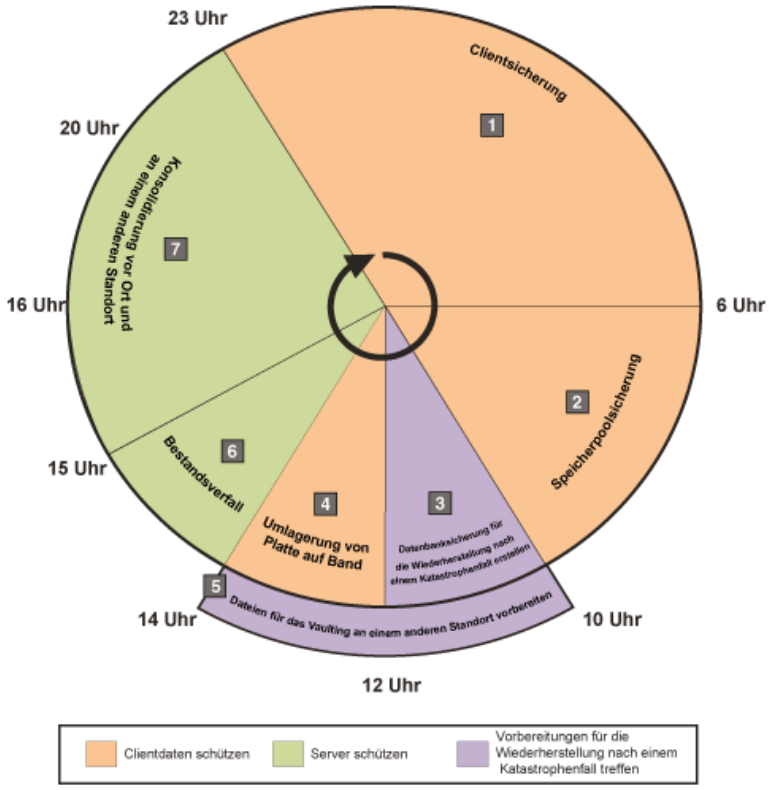


Abbildung 4. Tagesplan der Serveroperationen für eine Bandspeicherlösung

Die folgende Tabelle zeigt die Planung von Serververwaltungsprozessen in Kombination mit dem Clientsicherungszeitplan für eine Bandspeicherlösung.

Operation	Zeitplan
Clientsicherung	Startet um 23 Uhr.

Operation	Zeitplan
Speicherpoolsicherung	Startet um 6 Uhr.
Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall	• Die Datenbanksicherungsoperation startet um 10 Uhr bzw. 11 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt. • Die Sicherungsoperationen für Einheitenkonfigurationsinformationen und das Datenträgerprotokoll starten um 17 Uhr bzw. 7 Stunden nach dem Start der Datenbanksicherungsoperation. • Das Löschen des Datenträgerprotokolls startet um 20 Uhr bzw. 10 Stunden nach dem Start der Datenbanksicherungsoperation.
Vorbereitung der Dateien für das Vaulting an einem anderen Standort	Startet um 10 Uhr zu demselben Zeitpunkt wie die Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall.
Umlagerung von Platte auf Band	Startet um 12 Uhr bzw. 2 Stunden nach dem Start der Datenbanksicherungsoperation.
Bestandsverfall	Startet um 14 Uhr bzw. 15 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.
Speicherbereichskonsolidierung	Startet um 15 Uhr bzw. 16 Stunden nach dem Start der Clientsicherungsoperation.

Vorgehensweise

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

1. Definieren Sie eine Einheitenklasse für die Sicherungsoperation, bevor Sie den Zeitplan für Datenbanksicherungen erstellen.

   Erstellen Sie mit dem Befehl **DEFINE DEVCLASS** eine Einheitenklasse mit dem Namen LTOTAPE:

   ```
   define devclass ltotape devtype=lto library=ltolib
   ```

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

   ```
   set dbrecovery ltotape
   ```

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

Operation	Beispielbefehle und weitere Informationen
Sichern von Speicherpools	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **BACKUP STGPOOL**. Geben Sie beispielsweise den folgenden Befehl aus, um einen Sicherungszeitplan für einen primären Speicherpool mit dem Namen PRIMARY_POOL zu erstellen. Der Pool wird in einem Kopienspeicherpool mit dem Namen COPYSTG gesichert: `define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1`
Sichern der Datenbank	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **BACKUP DB**. Geben Sie beispielsweise den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet: `define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Datenbank sichern." startdate=today starttime=10:00:00 duration=45 durunits=minutes`
Replizieren von Knoten	Verwenden Sie wahlweise die Knotenreplikation, um Clientdaten zu schützen, indem Sie die Daten auf einem sekundären Server sichern. Anweisungen finden Sie in Clientdaten auf einen anderen Server replizieren. Stellen Sie sicher, dass die Knotenreplikation abgeschlossen ist, bevor Umlagerungsoperationen beginnen.

Operation	Beispielbefehle und weitere Informationen
Tägliches Umlagern von Daten von Platte auf Band	Erstellen Sie einen Zeitplan für die Speicherpoolumlagerung. Wenn beispielsweise ein Plattenspeicherpool mit dem Namen DISKPOOL vorhanden ist und der nächste Speicherpool der Speicherpool mit dem Namen TAPEPOOL ist, können Sie die Speicherpoolumlagerung planen, indem Sie den folgenden Befehl ausgeben: `define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="Plattenspeicherpool in Bandpool umlagern" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days` Um den Durchsatz zu maximieren, können Sie die Anzahl paralleler Prozesse angeben, die für die Umlagerung von Dateien verwendet werden soll, indem Sie die folgenden Schritte ausführen: a. Stellen Sie für den Bandspeicherpool sicher, dass die Kollokation aktiviert ist. Um zu überprüfen, ob die Kollokation aktiviert ist, führen Sie den Befehl **QUERY STGPOOL** aus. Stellen Sie sicher, dass der Wert GROUP, NODE oder FILESPACE im Feld COLLOCATE angegeben ist. Wenn der Wert GROUP, NODE oder FILESPACE nicht angegeben ist, verwenden Sie den Befehl **UPDATE STGPOOL**, um abhängig von Ihrer Systemkonfiguration COLLOCATE=GROUP, COLLOCATE=NODE oder COLLOCATE=FILESPACE anzugeben. b. Geben Sie für den Plattenspeicherpool mithilfe des Befehls **DEFINE STGPOOL** oder **UPDATE STGPOOL** einen Wert für den Parameter **MIGPROCESS** an. Wenn beispielsweise 12 Bandlaufwerke vorhanden sind, geben Sie MIGPROCESS=10 an. Auf diese Weise werden maximal 10 Bandlaufwerke für Umlagerungsprozesse verwendet. Zwei Laufwerke sind für andere Tasks, wie beispielsweise Zurückschreibungs-, Datenbanksicherungs- und Clientsicherungsoperationen, reserviert.
Vorbereiten von Dateien für das Vaulting an einem anderen Standort	a. Versetzen Sie Banddatenträger an einen anderen Standort, indem Sie die Anweisungen in „Sicherungsdatenträger versetzen” auf Seite 65 ausführen. b. Erstellen Sie die Plandatei zur Wiederherstellung nach einem Katastrophenfall, indem Sie den Befehl **PREPARE** auf dem Quellenserver ausgeben: `prepare` c. Stellen Sie sicher, dass alle Datenträger, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind, in die Wiederherstellungsplandatei eingeschlossen sind. Weitere Informationen finden Sie in „Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM” auf Seite 230.
Sichern der Einheitenkonfigurationsinformationen	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **BACKUP DEVCONFIG**: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Einheitenkonfigurationsdatei sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`

Operation	Beispielbefehle und weitere Informationen
Sichern des Datenträgerprotokolls	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **BACKUP VOLHISTORY**: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Datenträgerprotokoll sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Entfernen älterer Versionen von Datenbanksicherungen, die nicht mehr erforderlich sind	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **DELETE VOLHISTORY**: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Alte Datenbanksicherungen entfernen." startdate=today start time=20:00:00 duration=45 durunits=minutes`
Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **EXPIRE INVENTORY**. Legen Sie für den Parameter **RESOURCE** auf der Basis der Systemgröße, die Sie konfigurieren, einen Wert fest, der mit der Anzahl Prozessorkerne, die für Ihr System angegeben wurden, übereinstimmt. Geben Sie beispielsweise den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=8 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=14:00:00 duration=1 durunits=hours`
Konsolidieren von Speicherbereich	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **RECLAIM STGPOOL**. Geben Sie beispielsweise den folgenden Befehl aus, um einen Zeitplan mit dem Namen RECLAIM zu erstellen: `define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours` **Tipp:** Um den Durchsatz zu maximieren, können Sie die Anzahl paralleler Prozesse angeben, die für die Konsolidierung von Speicherbereich verwendet werden soll. Aktualisieren Sie den Bandspeicherpool mithilfe des Befehls **UPDATE STGPOOL** und geben Sie einen Wert für den Parameter **RECLAIMPROCESS** an. Wenn beispielsweise 12 Bandlaufwerke vorhanden sind, geben Sie RECLAIMPROCESS=5 an. Da für jeden Konsolidierungsprozess zwei Laufwerke verwendet werden, beträgt die Gesamtzahl Laufwerke, die für die Konsolidierung verwendet werden kann, 10. Zwei Laufwerke sind für Sicherungsoperationen reserviert.

Nächste Schritte

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

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

Zugehörige Informationen

UPDATE STGPOOL (Speicherpool aktualisieren)
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Sicherungsdatenträger versetzen

Für die Wiederherstellung nach einem Katastrophenfall benötigen Sie Datenbanksicherungsdatenträger, Kopienspeicherpooldatenträger und weitere Dateien. Um auf einen Katastrophenfall vorbereitet zu sein, müssen Sie tägliche Tasks ausführen.

Vorbereitende Schritte

Um alle virtuellen Kopienspeicherpooldatenträger und Datenbanksicherungsdatenträger anzuzeigen, deren Sicherungsobjekte auf dem fernen Zielserver gespeichert sind, geben Sie den Befehl **QUERY DRMEDIA** aus:

```
query drmedia * wherestate=remote
```

Informationen zu diesem Vorgang

Die Funktion 'Disaster Recovery Manager' (DRM) ermöglicht es Ihnen, das Versetzen von Datenträgern an einem anderen Standort zu verfolgen. Die folgende Abbildung zeigt den Lebenszyklus einer typischen Operation, mit der Sicherungsdatenträger im Rahmen von Wiederherstellungsoperationen nach einem Katastrophenfall an einen anderen Standort und wieder vor Ort versetzt werden.

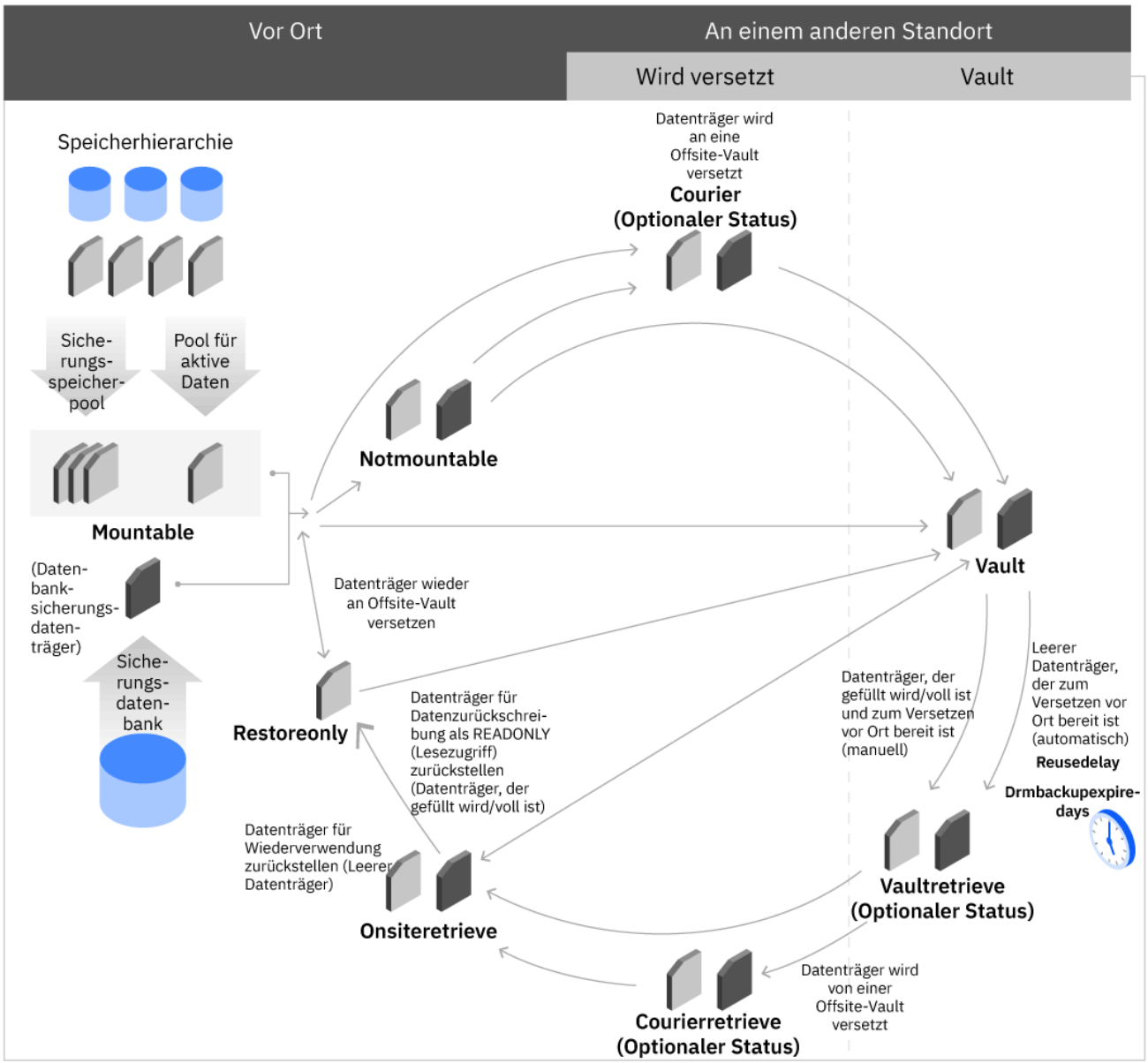


Abbildung 5. Versetzung von Sicherungsdatenträgern an einen anderen Standort und vor Ort

Datenträgern werden von DRM die folgenden Datenträgerstatus zugeordnet. Mithilfe der Datenträgerstatus kann ein Datenträger verfolgt werden, während er von einem Standort an einen anderen versetzt wird. Einige Datenträgerstatus sind optional. Abhängig davon, wie detailliert Ihr Unternehmen das Versetzen eines Datenträgers verfolgen möchte, kann Ihr Unternehmen diese optionalen Datenträgerstatus überspringen. Die folgenden Datenträgerstatus werden angezeigt:

MOUNTABLE
Der Datenträger enthält gültige Daten, befindet sich vor Ort und der Zugriff auf den Datenträger durch den IBM Spectrum Protect-Server ist möglich.

NOTMOUNTABLE
Der Datenträger enthält gültige Daten und befindet sich vor Ort, der Zugriff auf den Datenträger durch den IBM Spectrum Protect-Server ist jedoch nicht möglich.

COURIER
Der Datenträger enthält gültige Daten und wird gerade an die Vault versetzt.

VAULT
Der Datenträger enthält gültige Daten und befindet sich an der Vault.

VAULTRETRIEVE
Der Datenträger, der sich an der Offsite-Vault befindet, enthält keine gültigen Daten mehr und ist bereit, wieder vor Ort versetzt zu werden.

COURIERRETRIEVE
Der Datenträger enthält keine gültigen Daten mehr und wird vom Kurier wieder vor Ort versetzt.

ONSITERETRIEVE
Der Datenträger enthält keine gültigen Daten mehr und wird zurück vor Ort versetzt. Die Datenträgersätze für Datenbanksicherungsdatenträger, Arbeitsdatenträger in Kopienspeicherpools und Arbeitsdatenträger in Pools für aktive Daten werden aus der Datenbank gelöscht. Für private Datenträger in Kopienspeicherpools und Datenträger in Pools für aktive Daten wird der Zugriffsmodus in READWRITE (Lesen/Schreiben) geändert.

RESTOREONLY
Der Datenträger wird in das Speicherarchiv zurückgestellt, um die Zurückschreibung von Daten zu ermöglichen. Der Datenträger wird nur für die Zurückschreibung von Daten verwendet.

Kopienspeicherpooldatenträger an einen anderen Standort versetzen

Sie können Ihre Sicherungsdatenträger an einen anderen Standort senden, nachdem Sie die Sicherungskopien Ihrer primären Speicherpools und Ihrer Datenbank erstellt haben. Um Datenträger an einen anderen Standort zu senden, markieren Sie die Datenträger für IBM Spectrum Protect als nicht verfügbar und übergeben Sie die Datenträger dem Kurier.

Vorbereitende Schritte

Stellen Sie sicher, dass die Speicherpoolsicherungsprozesse abgeschlossen sind. Auf diese Weise können Sie Probleme verhindern, die auftreten könnten, wenn die Befehle **MOVE DRMEDIA** und **BACKUP STGPOOL** gleichzeitig ausgeführt werden.

Einschränkung: Verwenden Sie diese Prozedur nicht, um Aufbewahrungsdatenträger, das heißt Banddatenträger, die Aufbewahrungsgruppendaten enthalten, an einen anderen Standort zu versetzen. Sie müssen den Befehl **MOVE RETMEDIA** oder Operationen zum Versetzen von Datenträgern im Operations Center verwenden. Anweisungen finden Sie in „Aufbewahrungsgruppendaten in und aus Bandspeicher versetzen” auf Seite 72.

Vorgehensweise

1. Um die Kopienspeicherpooldatenträger und Datenbanksicherungsdatenträger zu identifizieren, die an einen anderen Standort versetzt werden sollen, geben Sie den Befehl **QUERY DRMEDIA** unter Angabe des Parameters **WHERESTATE** aus.

   ```
   query drmedia * wherestate=mountable
   ```

2. Geben Sie die Versetzung von Datenträgern an, deren aktueller Status MOUNTABLE lautet, indem Sie den Befehl **MOVE DRMEDIA** unter Angabe des Parameters **WHERESTATE** ausgeben:

   ```
   move drmedia * wherestate=mountable
   ```

   a) Bei SCSI-Speicherarchiven wird während der Entnahmeverarbeitung ein Bedienereingriff angefordert. Übergehen Sie diese Anforderungen und geben Sie die Kassetten aus dem Speicherarchiv aus, indem Sie den folgenden Befehl ausgeben:

   ```
   move drmedia * wherestate=mountable remove=no
   ```

   b) Greifen Sie auf eine Liste der Datenträger zu, um die Kassetten zu identifizieren und aus dem Speicherarchiv zu entfernen, indem Sie den folgenden Befehl ausgeben:

   ```
   query drmedia wherestate=notmountable
   ```

Für alle Datenträger im Status MOUNTABLE werden von DRM die folgenden Tasks ausgeführt:

- Der Datenträgerstatus wird in NOTMOUNTABLE geändert; wenn der Befehl **SET DRMNOTMOUNTABLENAME** ausgegeben wurde, wird der Datenträgerstandort aktualisiert. Wenn Sie den Befehl **SET DRMNOTMOUNTABLENAME** nicht ausgeben, ist der Standardstandort NOTMOUNTABLE.
- Der Zugriffsmodus wird für einen Kopienspeicherpooldatenträger in UNAVAILABLE geändert.
- Datenträger werden aus automatisierten Speicherarchiven entnommen.

3. Senden Sie die Datenträger zum Versetzen an den anderen Standort an den Kurier und geben Sie den folgenden Befehl aus:

```
move drmedia * wherestate=notmountable
```

Für alle Datenträger im Status NOTMOUNTABLE ändert DRM den Datenträgerstatus in COURIER und aktualisiert den Datenträgerstandort gemäß dem Befehl **SET DRMCOURIERNAME**. Wenn der Befehl **SET** nicht ausgegeben wurde, ist der Standardstandort COURIER.

Tipp: Sie können das Durchlaufen aller Datenträgerstatus verhindern, indem Sie den Befehl **MOVE DRMEDIA** mit der Parametereinstellung **TOSTATE** zur Angabe des Zielstatus ausgeben. Um beispielsweise den Status von Datenträgern von NOTMOUNTABLE in VAULT zu ändern, geben Sie den folgenden Befehl aus:

```
move drmedia * wherestate=notmountable tostate=vault
```

Für alle Datenträger im Status NOTMOUNTABLE ändert DRM den Datenträgerstatus in VAULT und aktualisiert den Datenträgerstandort gemäß dem Befehl **SET DRMVAULTNAME**. Wenn der Befehl **SET** noch nicht ausgegeben wurde, ist der Standardstandort VAULT.

4. Wenn der Erhalt der Datenträger am Vaultstandort bestätigt wird, geben Sie den Befehl **MOVE DRMEDIA** aus, um den Status COURIER anzugeben:

```
move drmedia * wherestate=courier
```

Für alle Datenträger im Status COURIER ändert DRM den Datenträgerstatus in VAULT und aktualisiert den Datenträgerstandort gemäß dem Befehl **SET DRMVAULTNAME**. Wenn der Befehl **SET** nicht ausgegeben wurde, ist der Standardstandort VAULT.

5. Zeigen Sie eine Liste der Datenträger am Aufbewahrungsort, die gültige Daten enthalten, an, indem Sie den folgenden Befehl ausgeben:

```
query drmedia wherestate=vault
```

Kopienspeicherpooldatenträger vor Ort versetzen

Sie können Sicherungsdatenträger im Rahmen von im Rahmen von Operationen zur Wiederherstellung nach einem Katastrophenfall vor Ort versetzen. Sie können die Datenträger wieder vor Ort versetzen, um Daten zurückzuschreiben. Es ist auch möglich, nicht virtuelle Datenbanksicherungsdatenträger als verfallen zu definieren und die Datenträger für die Wiederverwendung oder das Entfernen wieder vor Ort zu versetzen.

Vorbereitende Schritte

Einschränkung: Verwenden Sie diese Prozedur nicht, um Datenträger, die Aufbewahrungsgruppendaten enthalten, wieder vor Ort zu versetzen. Sie müssen den Befehl **MOVE RETMEDIA** oder Operationen zum Versetzen von Datenträgern im Operations Center verwenden. Anweisungen finden Sie in „Aufbewahrungsgruppendaten in und aus Bandspeicher versetzen” auf Seite 72.

Wenn Datenträger für die Wiederverwendung wieder vor Ort versetzt werden, bestätigen Sie, dass die Verfallsdaten für diese Datenträger erreicht sind. Sie können einen Datenbanksicherungsdatenträger als verfallen definieren, wenn alle der folgenden Bedingungen erfüllt sind:

- Das Alter des letzten Datenträgers der Serien überschreitet den Verfallswert. Der Verfallswert ist die Anzahl Tage seit der letzten Sicherung in der Serie. Bei der Installation beträgt der Verfallswert 60 Tage. Um diesen Wert zu überschreiben, können Sie den Befehl **SET DRMDBBACKUPEXPIREDAYS** ausgeben.
- Alle Datenträger in der Serie haben den Status VAULT.
- Der Datenträger ist nicht Bestandteil der neuesten Datenbanksicherungsserie.

Starten Sie die Verfallsverarbeitung entweder manuell, indem Sie den Befehl **EXPIRE INVENTORY** ausgeben, oder automatisch unter Verwendung der Optionseinstellung EXPINTERVAL, die in der Serveroptionsdatei angegeben ist.

Vorgehensweise

Um Speicherpooldatenträger vor Ort zu versetzen, führen Sie eine der folgenden Aktionen aus:

Task	Prozedur

Leeren Datenträger für die Wiederverwendung oder das Entfernen vor Ort versetzen	Um leere Speicherpooldatenträger vor Ort zu versetzen, führen Sie die folgenden Schritte aus:
	
	a. Geben Sie die Anzahl Tage an, bevor eine Datenbanksicherungsserie verfällt, indem Sie den Befehl **SET DRMDBBACKUPEXPIREDAYS** ausgeben. Um beispielsweise die Anzahl Tage auf 30 zu setzen, geben Sie den folgenden Befehl aus:
	`set drmdbbackupexpiredays 30`
	Tipp: Geben Sie den Befehl **DEFINE STGPOOL** aus und geben Sie denselben Wert für den Parameter **REUSEDELAY** in Ihrer Kopienspeicherpooldefinition an, um Folgendes sicherzustellen:
	• Die Datenbank kann mit einem früheren Stand zurückgeschrieben werden.
	• Die Datenbankverweise auf Dateien im Kopienspeicherpool sind noch gültig.
	Wenn Kopienspeicherpools, die von DRM verwaltet werden, unterschiedliche Werte für **REUSEDELAY** haben, geben Sie den Befehl **SET DRMDBBACKUPEXPIREDAYS** aus und setzen Sie den Parameter **REUSEDELAY** auf den höchsten Wert.
	b. Identifizieren Sie alle Datenträger an der Offsite-Vault, die keine gültigen Daten mehr enthalten und wieder vor Ort versetzt werden können. Bei leeren Datenträgern versetzt der Server den Datenträger automatisch in den Datenträgerstatus VAULTRETRIEVE. Geben Sie den folgenden Befehl aus:
	`query drmedia * wherestate=vaultretrieve`

Task	Prozedur

	c. Um den Prozess zum Versetzen eines Kopienspeicherpools zu starten, geben Sie den folgenden Befehl aus:
	`move drmedia * wherestate=vaultretrieve`
	Einschränkung: Ein Kopienspeicherpooldatenträger kann vor Ort versetzt werden, wenn er mindestens so lange leer war (Status EMPTY) wie durch den Parameter **REUSEDELAY** im Befehl **DEFINE STGPOOL** angegeben.
	Für alle Datenträger im Status **VAULTRETRIEVE** werden vom Server die folgenden Aktionen ausgeführt:
	• Der Datenträgerstatus wird in **COURIERRETRIEVE** geändert.
	• Der Standort des Datenträgers wird gemäß dem Wert im Befehl **SET DRMCOURIERNAME** aktualisiert.
	Tipp:
	Sie können auch das Ziel für die Datenträger angeben, indem Sie den Befehl **MOVE DRMEDIA** unter Angabe der Parametereinstellung **TOSTATE** ausgeben. Um beispielsweise Datenträger aus dem Status **VAULTRETRIEVE** in den Status **ONSITERETRIEVE** zu versetzen, geben Sie den folgenden Befehl aus:
	`move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve`
	Für alle Datenträger im Status **VAULTRETRIEVE** werden vom Server die folgenden Aktionen ausgeführt:
	• Die Datenträger werden vor Ort versetzt, wo sie wiederverwendet oder entfernt werden können.
	• Die Datenbanksicherungsdatenträger werden aus der Datenträgerprotokolltabelle gelöscht.
	• Der Satz für Arbeitsdatenträger in Kopienspeicherpools wird aus der Datenbank gelöscht; für private Datenträger in Kopienspeicherpools wird der Zugriffsmodus in READWRITE (Lesen/Schreiben) geändert.
	d. Wenn der Kurier den Datenträger wieder vor Ort bringt, geben Sie den folgenden Befehl aus:
	`move drmedia * wherestate=courierretrieve`
	Für alle Datenträger im Status **COURIERRETRIEVE** werden vom Server die folgenden Aktionen ausgeführt:
	• Die Datenträger werden vor Ort versetzt, wo sie wiederverwendet oder ausgesondert werden können.
	• Die Datenbanksicherungsdatenträger werden aus der Datenträgerprotokolltabelle gelöscht.
	• Der Satz für Arbeitsdatenträger in Kopienspeicherpools wird aus der Datenbank gelöscht. Für private Datenträger in Kopienspeicherpools wird der Zugriffsmodus in READWRITE (Lesen/Schreiben) geändert.

Nicht leeren Datenträger für die Zurückschreibung von Daten vor Ort versetzen	Um Speicherpooldatenträger zum Zurückschreiben von Daten vor Ort zu versetzen, führen Sie die folgenden Schritte aus:

Task	Prozedur

	a. Identifizieren Sie die Datenträger, die wieder vor Ort versetzt werden sollen. Um einen erforderlichen Datenträger zu lokalisieren, geben Sie den Befehl **QUERY DRMEDIA** unter Angabe des Parameters **WHERESTATE** aus. Um beispielsweise alle Datenträger anzuzeigen, die sich an der Offsite-Vault befinden, geben Sie den folgenden Befehl aus:
	`query drmedia * wherestate=vault`
	b. Versetzen Sie den Datenträger vor Ort. Geben Sie das Ziel des Datenträgers an, indem Sie den Befehl **MOVE DRMEDIA** unter Angabe der Parametereinstellung **TOSTATE** ausgeben. Um beispielsweise den Datenträger VOL001 vor Ort zu versetzen, geben Sie den folgenden Befehl aus:
	`move drmedia vol001 wherestate=vault tostate=onsiteretrieve`
	Der Server führt die folgenden Aktionen für alle angegebenen Datenträger im Status VAULT aus:
	• Die Datenträger werden vor Ort versetzt, wo sie zum Zurückschreiben von Daten verwendet werden können.
	• Der Datenträgerstatus wird in ONSITERETRIEVE geändert.
	c. Stellen Sie den Datenträger in das Bandarchiv zurück und machen Sie den Datenträger für Zurückschreibungsoperationen verfügbar. Um den Datenträger aus dem Status ONSITERETRIEVE in den Status RESTOREONLY zu versetzen, geben Sie den Befehl **CHECKIN LIBVOL** aus. Wenn beispielsweise der Name des Speicherarchivs LIBNAME ist, können Sie den folgenden Befehl ausgeben:
	`checkin libvol libname search=bulk waittime=0 checklabel=barcode status=pri vate`
	Tipp: Für Banddatenträger in SCSI-Speicherarchiven können Sie die Rückstellzeit reduzieren, indem Sie festlegen, dass der Server das Barcodeetikett lesen soll.
	Der Datenträger wird einem automatisierten Speicherarchiv hinzugefügt und der Datenträgerstatus des Datenträgers wird in RESTOREONLY geändert.
	d. Die Daten werden von dem Banddatenträger zurückgeschrieben. Nachdem die Zurückschreibung von Daten abgeschlossen ist, können Sie die Banddatenträger wieder zurück an die Offsite-Vault senden. Sie können den Banddatenträger zusammen mit anderen Banddatenträgern verarbeiten, die an einen anderen Standort versetzt werden. Der Datenträgerstatus des Datenträgers ändert sich standardmäßig in MOUNTABLE. Geben Sie den folgenden Befehl aus:
	`move drmedia * wherestate=restoreonly`
	Sie können auch stattdessen das Ziel des Datenträgers angeben, indem Sie den Befehl **MOVE DRMEDIA** unter Angabe der Parametereinstellung **TOSTATE** ausgeben. Um beispielsweise den Status von Datenträgern von RESTOREONLY in VAULT zu ändern, geben Sie den folgenden Befehl aus:
	`move drmedia * wherestate=restoreonly tostate=vault`

Ergebnisse

Die ausgewählten Speicherpooldatenträger werden wieder vor Ort versetzt und in das Bandarchiv zurückgestellt. Leere Banddatenträger werden in den Status SCRATCH zurückversetzt und sind für die Wiederverwendung verfügbar. Nicht leere Datenträger haben den Status RESTOREONLY und können zum Zurückschreiben der Daten verwendet werden.

Aufbewahrungsgruppendaten in und aus Bandspeicher versetzen

Sie können Aufbewahrungsgruppendaten auf Banddatenträger kopieren, die Sie von einem Speicherarchiv vor Ort an eine Bandspeichervault an einem anderen Standort versetzen können. Vaults dienen der Bereitstellung von sicherem Langzeitspeicher. Nachdem die Aufbewahrungsgruppe auf Band kopiert wurde und der Banddatenträger aus dem Bandarchiv entfernt wurde, können Sie die Versetzung des Datenträgers an einen anderen Standort und vor Ort verfolgen.

Ein Banddatenträger, der Daten für eine oder mehrere Aufbewahrungsgruppen enthält, wird als *Aufbewahrungsdatenträger* bezeichnet. Wenn der Banddatenträger von einem Standort an einen anderen versetzt wird, ändert sich der Datenträgerstatus, um den neuen Standort widerzuspiegeln; mithilfe dieser Informationen können Sie den physischen Standort des Datenträgers verfolgen.

Der Lebenszyklus eines Aufbewahrungsdatenträgers umfasst die folgenden Hauptphasen:

1. Wenn der Prozess zum Schreiben einer Aufbewahrungsgruppe auf einen Banddatenträger beginnt, wird entweder ein Arbeitsdatenträger aus dem Arbeitsdatenträgerpool des Bandarchivs angefordert oder ein vorhandener Arbeitsdatenträger aus dem Aufbewahrungspool ausgewählt. Daten einer oder mehrerer Aufbewahrungsgruppen werden auf den Datenträger geschrieben. Wenn der Datenträger voll ist, wird er vom Kurier an eine Offsite-Vault versetzt.
2. Wenn der Datenträger Daten enthält, die zurückgeschrieben werden müssen, wird der Datenträger von der Vault abgerufen und vom Kurier wieder vor Ort gebracht. Nachdem die Daten in der Aufbewahrungsgruppe zurückgeschrieben wurden, wird der Datenträger wieder zurück an die Offsite-Vault versetzt.
3. Im Laufe der Zeit können Daten in Aufbewahrungsgruppen abhängig von Verfallsmaßnahmen verfallen. Wenn die Verfallsdaten für alle Aufbewahrungsgruppen, für die Daten auf dem Datenträger vorhanden sind, erreicht sind, kann der Datenträger für die Wiederverwendung wieder vor Ort versetzt werden.

Die folgende Abbildung zeigt den Lebenszyklus einer typischen Operation, mit der Aufbewahrungsdatenträger an einen anderen Standort und wieder vor Ort versetzt werden.

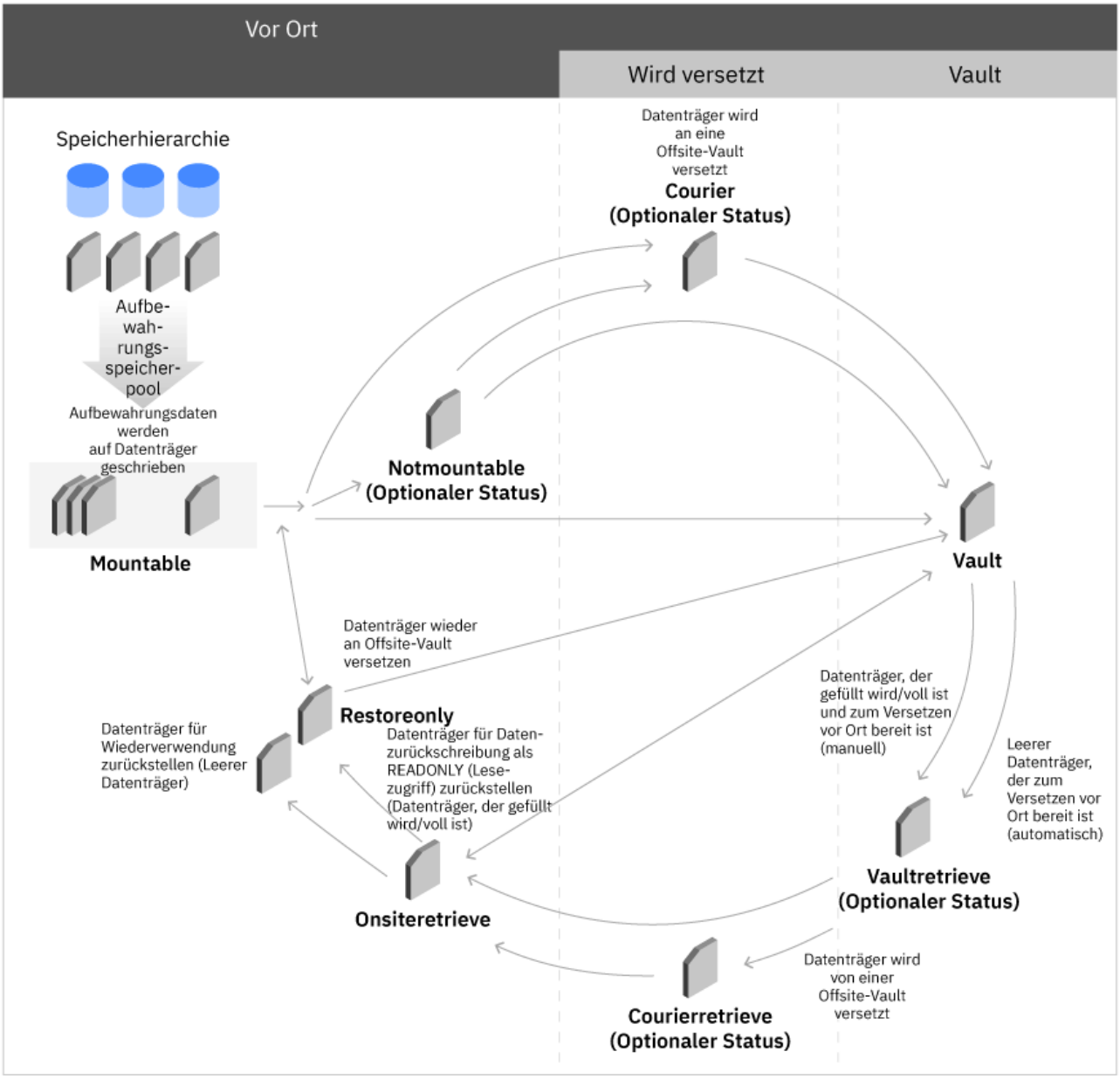


Abbildung 6. Versetzung von Aufbewahrungsdatenträgern an einen anderen Standort und vor Ort

Der Datenträgerstatus des Datenträgers ermöglicht es Ihnen, den aktuellen Standort des Datenträgers zu identifizieren, während der Datenträger von Ihrem Speicherarchiv vor Ort an eine Offsite-Vault versetzt wird und dann zur Zurückschreibung von Daten oder zur Wiederverwendung von Bändern wieder vor Ort versetzt wird. Der Datenträgerstatus des Datenträgers ist eine logische Bezeichnung, die sich auf den physischen Standort des Datenträgers bezieht. Einige Datenträgerstatus sind optional. Abhängig davon, wie detailliert Ihr Unternehmen das Versetzen eines Datenträgers verfolgen möchte, kann Ihr Unternehmen diese optionalen Datenträgerstatus überspringen. Die folgenden Datenträgerstatus werden angezeigt:

MOUNTABLE
Der Datenträger befindet sich vor Ort und wird in das Speicherarchiv zurückgestellt. Daten einer oder mehrerer Aufbewahrungsgruppen werden auf den Datenträger geschrieben.

NOTMOUNTABLE
Der Datenträger befindet sich vor Ort, wurde aber aus dem Speicherarchiv entnommen und ist bereit, an einen anderen Standort gesendet zu werden.

COURIER
Der Datenträger wird gerade an eine Offsite-Vault versetzt.

VAULT
Der Datenträger befindet sich für die langfristige Speicherung an einer Offsite-Vault.

VAULTRETRIEVE
Der Datenträger ist bereit, um von einer Offsite-Vault zurück vor Ort versetzt zu werden. Leere Datenträger können wieder vor Ort gebracht und wiederverwendet werden. Der Server erkennt, dass der Datenträger nur verfallene Daten enthält, und versetzt den Datenträger automatisch in den Datenträgerstatus VAULTRETRIEVE. Auch Datenträger, die gefüllt werden, oder volle Datenträger können für die Zurückschreibung von Daten wieder vor Ort gebracht werden; Sie müssen diese Aktion jedoch mithilfe der Parametereinstellung **TOSTATE** im Befehl **MOVE RETMEDIA** angeben.

COURIERRETRIEVE
Der Datenträger wird von einer Offsite-Vault zurück vor Ort versetzt.

ONSITERETRIEVE
Der Datenträger wurde von der Offsite-Vault abgerufen und befindet sich wieder vor Ort. Nicht leere Datenträger können für die Zurückschreibung von Aufbewahrungsgruppendaten von dem Datenträger in das Speicherarchiv zurückgestellt werden. Leere Datenträger können zurückgestellt und wiederverwendet werden.

RESTOREONLY
Der Datenträger wird in das Speicherarchiv zurückgestellt, um die Zurückschreibung von Aufbewahrungsgruppendaten zu ermöglichen.

Aufbewahrungsdatenträger an einen anderen Standort versetzen

Sie können Aufbewahrungsdatenträger, die Daten einer oder mehrerer Aufbewahrungsgruppen enthalten, an einen anderen Standort senden. Offsite-Vaults dienen zur Bereitstellung sicheren Speichers für Banddatenträger und stellen sicher, dass die Daten im Bedarfsfall zurückgeschrieben werden können.

Vorbereitende Schritte

Tipp: Wenn nicht der Befehl **MOVE DRMEDIA** verwendet werden soll, um Datenbanksicherungsdatenträger an einen anderen Standort und wieder vor Ort zu versetzen, kann dies auch mithilfe des Befehls **MOVE RETMEDIA** erfolgen. Weitere Informationen finden Sie in „Kopienspeicherpooldatenträger an einen anderen Standort versetzen” auf Seite 67.

- Sichern Sie nach der Erstellung der Aufbewahrungsgruppe, die an einen anderen Standort gesendet werden soll, die Serverdatenbank, indem Sie den Befehl **BACKUP DB** ausgeben. Wenn sichergestellt werden soll, dass der Datenbanksicherungsdatenträger zusammen mit dem Aufbewahrungsdatenträger an einen anderen Standort gesendet wird, müssen Sie den Parameter **SOURCE** im Befehl **MOVE RETMEDIA** angeben.

  Einschränkung: Im Operations Center können Sie keine Operationen zum Versetzen von Datenträgern verwenden, um einen Datenbanksicherungsdatenträger an einen anderen Standort zu senden. Datenbanksicherungsdatenträger werden mithilfe des Befehls **MOVE RETMEDIA** versetzt.

  Informationen zur Verwendung des Operations Center zum Versetzen von Aufbewahrungsdatenträgern finden Sie in der Onlinehilfe des Operations Center.

- Stellen Sie sicher, dass die Aufbewahrungsgruppen, die kopiert werden sollen, den Status 'Abgeschlossen' haben. Dieser Status gibt an, dass die Aufbewahrungsgruppen vollständig auf Band kopiert wurden und die Banddatenträger an eine Offsite-Vault versetzt werden können. Auf diese Weise können Sie Probleme verhindern, die auftreten könnten, wenn Operationen zum Versetzen von Datenträgern und zum Kopieren von Aufbewahrungsgruppen gleichzeitig ausgeführt werden.

Vorgehensweise

1. Identifizieren Sie die Aufbewahrungsspeicherpooldatenträger und Datenbanksicherungsdatenträger, die an einen anderen Standort versetzt werden sollen, indem Sie den Befehl **QUERY RETMEDIA** ausführen:

   ```
   query retmedia * wherestate=mountable
   ```

2. Starten Sie die Versetzung von Datenträgern, deren aktueller Status MOUNTABLE lautet. Standardmäßig werden alle nicht leeren Datenträger eingeschlossen, unabhängig davon, ob sie zu Aufbewahrungsgruppen gehören, die gerade kopiert werden, oder zu Aufbewahrungsgruppen, die bereits vollständig kopiert wurden. Geben Sie den folgenden Befehl aus:

   ```
   move retmedia * wherestate=mountable
   ```

   a) Wenn Sie ein SCSI-Speicherarchiv verwenden, wird von SCSI-Speicherarchiven während der Entnahmeverarbeitung ein Bedienereingriff angefordert. Übergehen Sie diese Anforderungen und geben Sie die Kassetten aus dem Speicherarchiv aus, indem Sie den folgenden Befehl ausgeben:

   ```
   move retmedia * wherestate=mountable remove=no
   ```

   b) Rufen Sie eine Liste der Datenträger ab, um die Datenträger zu identifizieren und aus dem Speicherarchiv zu entfernen, indem Sie den folgenden Befehl ausgeben:

   ```
   query retmedia wherestate=notmountable
   ```

   Für alle Datenträger im Status MOUNTABLE werden mit dem Befehl **MOVE RETMEDIA** die folgenden Tasks ausgeführt:

   - Der Datenträgerstatus wird in NOTMOUNTABLE geändert; wenn der Befehl **SET DRMNOTMOUNTABLENAME** ausgegeben wurde, wird der Datenträgerstandort aktualisiert. Wenn der Befehl **SET DRMNOTMOUNTABLENAME** nicht ausgegeben wurde, ist der Standardstandort NOTMOUNTABLE.
   - Der Zugriffsmodus für Datenträger wird in UNAVAILABLE (Nicht verfügbar) geändert.
   - Datenträger werden aus automatisierten Speicherarchiven entnommen.

   Tipp: Abhängig davon, wie detailliert Ihr Unternehmen das Versetzen eines Datenträgers verfolgen möchte, kann Ihr Unternehmen einige Datenträgerstatus überspringen. Sie können das Durchlaufen der einzelnen unterschiedlichen Datenträgerstatus verhindern, indem Sie im Befehl **MOVE RETMEDIA** mit dem Parameter **TOSTATE** den Zielstatus angeben. Um beispielsweise den Status der Datenträger direkt von NOTMOUNTABLE in VAULT zu ändern, geben Sie den folgenden Befehl aus:

   ```
   move retmedia * wherestate=notmountable tostate=vault
   ```

3. Senden Sie die Datenträger zum Versetzen an den Auslagerungsstandort an den Kurier und geben Sie den folgenden Befehl aus:

   ```
   move retmedia * wherestate=notmountable
   ```

   Für alle Datenträger im Status NOTMOUNTABLE wird der Datenträgerstatus in den Status COURIER geändert und der Datenträgerstandort gemäß dem Befehl **SET DRMCOURIERNAME** aktualisiert. Wenn der Befehl **SET DRMCOURIERNAME** nicht ausgegeben wurde, ist der Standardstandort COURIER.

4. Verfolgen Sie das Versetzen des Banddatenträgers, während er an eine Offsite-Vault versetzt wird. Geben Sie den folgenden Befehl aus:

   ```
   query retmedia * wherestate=courier
   ```

5. Wenn der Vaultstandort den Erhalt der Datenträger bestätigt, geben Sie den Befehl **MOVE RETMEDIA** aus, um den Status COURIER anzugeben:

   ```
   move retmedia * wherestate=courier
   ```

Für alle Datenträger im Status COURIER wird der Datenträgerstatus in VAULT geändert und der Datenträgerstandort gemäß dem Befehl **SET DRMVAULTNAME** aktualisiert. Wenn der Befehl **SET DRMVAULTNAME** nicht ausgegeben wurde, ist der Standardstandort VAULT.

Für alle Datenträger im Status NOTMOUNTABLE ändert der Befehl **MOVE RETMEDIA** den Datenträgerstatus in VAULT und der Datenträgerstandort wird gemäß dem Befehl **SET DRMVAULTNAME** aktualisiert. Wenn der Befehl **SET DRMVAULTNAME** noch nicht ausgegeben wurde, ist der Standardstandort VAULT.

Ergebnisse

Die Aufbewahrungsdatenträger und alle angegebenen Datenbanksicherungsdatenträger werden an die Offsite-Bandvault versetzt. Wenn die Aufbewahrungsgruppendaten zurückgeschrieben werden müssen, können die Datenträger von der Vault abgerufen werden.

Aufbewahrungsdatenträger vor Ort versetzen

Wenn eine Aufbewahrungsgruppe zurückgeschrieben werden muss, können Sie die Banddatenträger, die Aufbewahrungsgruppendaten enthalten, für Zurückschreibungsoperationen vor Ort bringen. Wenn die Verfallsdaten für alle Aufbewahrungsgruppen, für die Daten auf dem Aufbewahrungsdatenträger vorhanden sind, erreicht sind, können Sie den leeren Datenträger für die Wiederverwendung wieder vor Ort bringen.

Vorbereitende Schritte

Wenn leere Datenträger für die Wiederverwendung wieder vor Ort versetzt werden, bestätigen Sie, dass die Verfallsdaten für alle Aufbewahrungsgruppen, für die Daten auf dem Datenträger vorhanden sind, erreicht sind und die Aufbewahrungsgruppe verfallen ist. Sie können die Verfallsverarbeitung manuell starten, indem Sie den Befehl **EXPIRE INVENTORY** ausgeben, oder Sie können den Befehl **DELETE RETSET** verwenden, um die Aufbewahrungsgruppe zum Löschen zu markieren.

Tipp: Wenn nicht der Befehl **MOVE DRMEDIA** verwendet werden soll, um Datenbanksicherungsdatenträger an einen anderen Standort und wieder vor Ort zu versetzen, kann dies auch mithilfe des Befehls **MOVE RETMEDIA** erfolgen. Weitere Informationen finden Sie in „Kopienspeicherpooldatenträger an einen anderen Standort versetzen” auf Seite 67.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Aufbewahrungsdatenträger vor Ort zu versetzen.

Task	Prozedur

Leeren Datenträger für die Wiederverwendung vor Ort versetze	Um leere Aufbewahrungsdatenträger vor Ort zu versetzen, führen Sie die folgenden Schritte aus:
	a. Identifizieren Sie die Aufbewahrungsdatenträger an der Offsite-Vault, die wieder vor Ort versetzt werden sollen. Bei leeren Datenträgern erkennt der Server, dass der Datenträger nur verfallene Daten enthält, und versetzt den Datenträger automatisch in den Datenträgerstatus VAULTRETRIEVE. Geben Sie den folgenden Befehl aus:
	`query retmedia * wherestate=vaultretrieve volstatus=empty`
	b. Versetzen Sie die Banddatenträger vor Ort. Geben Sie das Ziel für die Datenträger an, indem Sie den Befehl **MOVE RETMEDIA** unter Angabe des Parameters **TOSTATE** ausgeben. Geben Sie den folgenden Befehl aus:
	`move retmedia * wherestate=vaultretrieve volstatus=empty tostate=onsiteretrieve`
	Einschränkung: Ein Aufbewahrungsspeicherpooldatenträger kann vor Ort gebracht werden, wenn er mindestens so lange leer war (Status EMPTY) wie durch den Parameter **REUSEDELAY** im Befehl **DEFINE STGPOOL** angegeben.
	Der Server führt die folgenden Aktionen aus:
	• Der Datenträgerstatus wird in **ONSITERETRIEVE** geändert.
	• Die Datenbanksicherungsdatenträger werden aus der Datenträgerprotokolltabelle gelöscht.
	• Der Satz für Aufbewahrungsarbeitsdatenträger wird aus der Datenbank gelöscht.
	c. Stellen Sie den leeren Datenträger in das Bandarchiv zurück und machen Sie ihn für die Wiederverwendung verfügbar, indem Sie den Befehl **CHECKIN LIBVOL** ausgeben und den Datenträger als Arbeitsdatenträger angeben.
	Tipp: Für Banddatenträger in SCSI-Speicherarchiven können Sie die Rückstellzeit reduzieren, indem Sie festlegen, dass der Server das Barcodeetikett lesen soll.
	Geben Sie den folgenden Befehl aus:
	`checkin libvol libname search=bulk waittime=0 checklabel=barcode status=scratch`

Task	Prozedur

Nicht leeren Datenträger für die Zurückschreibung von Daten vor Ort versetzen	Um Aufbewahrungsdatenträger für die Datenzurückschreibung vor Ort zu versetzen, führen Sie die folgenden Schritte aus:
	a. Identifizieren Sie die Datenträger, die Aufbewahrungsgruppendaten enthalten, die zurückgeschrieben werden sollen.
	• Um die Datenträger zu identifizieren, die von den einzelnen Aufbewahrungsgruppen verwendet werden, geben Sie den folgenden Befehl aus:
	`query retset listvolumes=yes`
	• Um die Aufbewahrungsgruppen zu identifizieren, für die Daten auf einem Aufbewahrungsdatenträger vorhanden sind, geben Sie den folgenden Befehl aus:
	`query volume listretsets=yes`
	b. Lokalisieren Sie den erforderlichen Datenträger an seinem Auslagerungsstandort, indem Sie den Befehl **QUERY RETMEDIA** unter Angabe des Parameters **WHERESTATE** ausgeben. Um beispielsweise alle Datenträger anzuzeigen, die sich an der Offsite-Vault befinden, geben Sie den folgenden Befehl aus:
	`query retmedia * wherestate=vault`
	c. Versetzen Sie den erforderlichen Datenträger vor Ort. Geben Sie das Ziel für die Datenträger an, indem Sie den Befehl **MOVE RETMEDIA** unter Angabe des Parameters **TOSTATE** ausgeben. Um beispielsweise den Datenträger VOL001 vor Ort zu versetzen, geben Sie den folgenden Befehl aus:
	`move retmedia VOL001 wherestate=vault tostate=onsiteretrieve`
	Wichtig: Damit Aufbewahrungsspeicherpooldatenträger für die Konsolidierung auswählbar sind, müssen sie den Status MOUNTABLE haben. Bei der Konsolidierungsverarbeitung werden keine Datenträger konsolidiert, die den Status ONSITERETRIEVE oder RESTOREONLY haben. Wenn Sie Aufbewahrungsspeicherpooldatenträger wieder vor Ort versetzen, indem Sie den Befehl **MOVE RETMEDIA** unter Angabe des Parameterwerts **TOSTATE=ONSITERETRIEVE** oder **TOSTATE=RESTOREONLY** ausgeben, werden diese Datenträger bei der Speicherkonsolidierungsverarbeitung übersprungen.
	d. Stellen Sie den Datenträger in das Bandarchiv zurück und machen Sie den Datenträger für Zurückschreibungsoperationen verfügbar. Um sicherzustellen, dass der Datenträger nur für die Zurückschreibung von Daten verwendet werden kann, hat er den Zugriffsmodus READONLY (Lesezugriff). Um den Datenträger aus dem Status ONSITERETRIEVE in den Status RESTOREONLY zu versetzen, geben Sie den Befehl **CHECKIN LIBVOL** aus. Geben Sie den folgenden Befehl aus:
	`checkin libvol libname search=bulk waittime=0 checklabel=barcode status=pri vate`
	Tipp: Für Banddatenträger in SCSI-Speicherarchiven können Sie die Rückstellzeit reduzieren, indem Sie festlegen, dass der Server das Barcodeetikett lesen soll.
	Der Datenträger wird einem automatisierten Speicherarchiv hinzugefügt und der Datenträgerstatus des Datenträgers wird in RESTOREONLY geändert.

Ergebnisse

Die ausgewählten Aufbewahrungsdatenträger werden wieder vor Ort versetzt und in das Bandarchiv zurückgestellt. Leere Banddatenträger werden in den Status SCRATCH zurückversetzt und sind für die Wiederverwendung verfügbar. Nicht leere Datenträger haben den Status RESTOREONLY und können zum Zurückschreiben der Daten verwendet werden.

Nächste Schritte

Nachdem die Zurückschreibung von Daten abgeschlossen ist, können Sie die Banddatenträger wieder zurück an die Offsite-Vault senden. Geben Sie den folgenden Befehl aus:

```
move retmedia * wherestate=restoreonly tostate=vault
```

Alertnachrichten zum Überwachen der Versetzung von Aufbewahrungsdatenträgern

Wenn Sie Aufbewahrungsdatenträger an einen anderen Standort senden oder wieder vor Ort bringen, generiert der IBM Spectrum Protect-Server Alerts in Form von ANR-Nachrichten, um Probleme zurückzumelden und Sie bei der Überwachung des Status zu unterstützen.

Um alle Nachrichten anzuzeigen, rufen Sie das IBM Spectrum Protect-Fehlerprotokoll auf. Eine detaillierte Dokumentation der Nachrichten liefern die ANR-Nachrichten. Häufig ausgegebene Nachrichten sind in der folgenden Tabelle beschrieben:

Tabelle 16. Aufbewahrungsbanddatenträger an eine Offsite-Vault senden

Aktion	ANR-Nachricht	Beschreibung
Die Aufbewahrungsgruppe wird auf den Banddatenträger kopiert.	ANR3852I	Diese Informationsnachricht gibt an, dass die Aufbewahrungsgruppe erfolgreich auf den Banddatenträger kopiert wurde. Es werden Details zu der Kopieroperation bereitgestellt. Der Status der Aufbewahrungsgruppe lautet COMPLETED.
Banddatenträger werden aus einem Bandarchiv entnommen.	ANR6697I	Diese Informationsnachricht gibt an, dass Banddatenträger im Status MOUNTABLE erfolgreich aus einem Bandarchiv entnommen wurden.
Der Banddatenträger wird aus dem Speicherarchiv entnommen und vom Status MOUNTABLE in den Status VAULT versetzt.	ANR6683I	Diese Informationsnachricht gibt an, dass Aufbewahrungsdaten erfolgreich versetzt wurden und der Status geändert wurde.

Tabelle 17. Banddatenträger für die Verwendung bei Zurückschreibungsoperationen in das Bandarchiv zurückstellen

Aktion	ANR-Nachricht	Beschreibung
Ein Aufbewahrungsdatenträger, der Daten enthält, wurde erfolgreich in das Bandarchiv vor Ort zurückgestellt.	ANR8532I	Diese Informationsnachricht gibt an, dass ein Datenträger mit Daten erfolgreich in das Bandarchiv vor Ort zurückgestellt wurde. Für Aufbewahrungsdatenträger ändert sich der Datenträgerstatus von ONSITERETRIEVE in RESTOREONLY; der Zugriffsmodus lautet READONLY (Lesezugriff). Die Aufbewahrungsgruppendaten auf dem Datenträger können jetzt zurückgeschrieben werden. **Tipp:** Diese Nachricht wird nicht angezeigt, wenn der Banddatenträger, der zurückgestellt wird, leer ist.
Es wird versucht, einen nicht leeren Aufbewahrungsdatenträger als Arbeitsdatenträger in das Bandarchiv zurückzustellen.	ANR8443E	Diese Fehlernachricht wird ausgelöst, da ein Aufbewahrungsdatenträger, der Daten enthält, nicht in ein Bandarchiv zurückgestellt werden kann, wenn ihm der Status SCRATCH zugeordnet wird. Der Datenträger wird nicht zurückgestellt und die Daten auf dem Band werden nicht überschrieben.

Tabelle 18. Verfallene Aufbewahrungsdatenträger in ein Bandarchiv zurückstellen

Aktion	ANR-Nachricht	Beschreibung
Ein leerer Aufbewahrungsdatenträger wird in ein Bandarchiv vor Ort zurückgestellt.	ANR8430I	Diese Informationsnachricht gibt an, dass ein leerer Datenträger erfolgreich in ein Bandarchiv vor Ort zurückgestellt wurde. Der Datenträger wird in den Status SCRATCH zurückversetzt.
Ein Versuch, einen leeren Aufbewahrungsdatenträger in ein Bandarchiv vor Ort zurückzustellen, ist fehlgeschlagen.	ANR8832E	Diese Fehlernachricht gibt an, dass eine Operation zum Zurückstellen eines leeren Aufbewahrungsdatenträgers in ein Bandarchiv vor Ort fehlgeschlagen ist.

Clientzeitpläne definieren

Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über **Clients**.
2. Klicken Sie auf **Zeitpläne**.
3. Klicken Sie auf **+Zeitplan**.
4. Führen Sie die Schritte im Assistenten **Zeitplan erstellen** aus.

   Definieren Sie auf der Basis der in „Zeitpläne für Serververwaltungsaktivitäten definieren” auf Seite 60 geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

Bandeinheiten für den Server anschließen

Bevor der Server eine Bandeinheit verwenden kann, müssen Sie die Einheit an Ihr Serversystem anschließen und den entsprechenden Bandeinheitentreiber installieren.

Informationen zu diesem Vorgang

Um die Systemleistung zu optimieren, verwenden Sie schnelle Bandeinheiten mit hoher Speicherkapazität. Stellen Sie genügend Bandlaufwerke bereit, um Ihre Geschäftsanforderungen erfüllen zu können.

Schließen Sie Bandeinheiten an ihren eigenen Hostbusadapter (HBA) an, der nicht mit anderen Einheitentypen, wie beispielsweise Platte, gemeinsam genutzt wird. IBM Bandlaufwerke haben einige spezielle Anforderungen in Bezug auf HBAs und zugehörige Treiber.

Automatisierte Speicherarchiveinheit an das System anschließen

Sie können eine automatisierte Speicherarchiveinheit an Ihr System anschließen, um Ihre Daten auf Bändern zu speichern.

Informationen zu diesem Vorgang

Berücksichtigen Sie die folgenden Einschränkungen, bevor Sie eine automatisierte Speicherarchiveinheit anschließen:

- Angeschlossene Einheiten müssen sich an ihrem eigenen Hostbusadapter (HBA) befinden.
- Ein HBA darf nicht mit anderen Einheitentypen, wie beispielsweise einer Platte, gemeinsam genutzt werden. .
- Bei Fibre Channel-HBAs mit mehreren Ports müssen Einheiten an ihren eigenen Ports angeschlossen sein. Diese Ports dürfen nicht mit anderen Einheitentypen gemeinsam genutzt werden.
- IBM Bandlaufwerke haben einige spezielle Anforderungen in Bezug auf HBA und zugehörige Treiber. Weitere Informationen zu Einheiten finden Sie auf der Website für Ihr Betriebssystem:
  - IBM Spectrum Protect Supported Devices for AIX
  - IBM Spectrum Protect Supported Devices for Linux and Windows

Vorgehensweise

Um den Fibre Channel-Adapter (FC-Adapter) verwenden zu können, führen Sie die folgenden Schritte aus:

1. Installieren Sie den FC-Adapter und die zugehörigen Treiber.
2. Installieren Sie die geeigneten Einheitentreiber für die angeschlossenen Datenträgerwechsler.

Zugehörige Konzepte

Bandeinheitentreiber auswählen

Um Bandeinheiten mit IBM Spectrum Protect verwenden zu können, müssen Sie den entsprechenden Bandeinheitentreiber installieren.

Speicherarchivmodus festlegen

Damit der IBM Spectrum Protect-Server auf ein SCSI-Speicherarchiv zugreifen kann, muss die Bandeinheit für den entsprechenden Modus definiert werden.

Informationen zu diesem Vorgang

Einige Speicherarchive verfügen über Bedienfeldmenüs und -anzeigen, die für explizite Bedieneranforderungen verwendet werden können. Wenn die Einheit für die Beantwortung derartiger Anforderungen definiert ist, antwortet sie normalerweise jedoch nicht auf IBM Spectrum Protect-Anforderungen.

Einige Speicherarchive können in den sequenziellen Modus versetzt werden, in dem Datenträger automatisch sequenziell in Laufwerke geladen werden. Dieser Modus steht im Konflikt mit der Art und Weise, auf die IBM Spectrum Protect auf die Bandeinheit zugreift. Ein Speicherarchiv, das im sequenziellen Modus konfiguriert ist, wird vom Systemeinheitentreiber nicht als Speicherarchivwechsler, IBM Bandeinheitentreiber oder IBM Spectrum Protect-Bandeinheitentreiber erkannt.

Vorgehensweise

1. Ziehen Sie die Dokumentation zu Ihrer Bandeinheit zu Rate, um zu bestimmen, wie der Speicherarchivmodus festgelegt werden kann.
2. Legen Sie für Ihre Bandeinheit den entsprechenden Modus fest. Bei den meisten Bandeinheiten wird der entsprechende Modus als wahlfreier Modus bezeichnet. Wenn Ihre Bandeinheit nicht über einen wahlfreien Modus verfügt, ziehen Sie die Dokumentation zu Ihrer Einheit zu Rate, um den entsprechenden Modus zu ermitteln.

Bandeinheitentreiber auswählen

Um Bandeinheiten mit IBM Spectrum Protect verwenden zu können, müssen Sie den entsprechenden Bandeinheitentreiber installieren.

Zugehörige Verweise

Bandeinheitentreiber installieren und konfigurieren

Sie können Bandeinheiten erst mit IBM Spectrum Protect verwenden, nachdem der korrekte Bandeinheitentreiber installiert wurde.

IBM Bandeinheitentreiber

IBM Einheitentreiber sind für die meisten IBM Bandeinheiten mit Kennsätzen verfügbar.

Sie können IBM Bandeinheitentreiber von der Website für Fix Central herunterladen:

1. Rufen Sie die Website für Fix Central unter Website für Fix Central auf.
2. Klicken Sie auf **Produkt auswählen**.
3. Wählen Sie **System Storage** im Menü für die **Produktgruppe** aus.
4. Wählen Sie **Tape systems** im Menü für **System Storage** aus.
5. Wählen Sie **Tape drivers and software** im Menü für **Tape systems** aus.
6. Wählen Sie **Tape device drivers** im Menü für **Tape drivers and software** aus. Zusätzlich zu Bandtreibern erhalten Sie auch Zugriff auf Tools wie das IBM Tape Diagnostic Tool (ITDT).
7. Wählen Sie Ihr Betriebssystem im Menü **Plattform** aus.

AIX Windows

Die aktuelle Liste der Einheiten und Betriebssystemversionen, die von IBM Bandeinheitentreibern unterstützt werden, finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten unter Supported devices for AIX and Windows.

Linux

Die aktuelle Liste der Bandeinheiten und Betriebssystemversionen, die von IBM Bandeinheitentreibern unterstützt werden, finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten unter Supported devices for Linux.

IBM Bandeinheitentreiber unterstützen nur einige Linux-Kernel-Level. Weitere Informationen zu unterstützten Kernel-Leveln finden Sie in Website für Fix Central.

IBM Spectrum Protect-Bandeinheitentreiber

Bandeinheitentreiber werden vom IBM Spectrum Protect-Server bereitgestellt.

Ein IBM Spectrum Protect-Bandeinheitentreiber wird mit dem Server installiert.

AIX

Sie können den generischen SCSI-Bandeinheitentreiber, der vom IBM AIX-Betriebssystem bereitgestellt wird, verwenden, um mit Bandeinheiten zu arbeiten, die nicht vom IBM Spectrum Protect-Einheitentreiber unterstützt werden. Wenn der generische SCSI-Bandeinheitentreiber unter AIX verwendet wird, muss die Einheitenklasse GENERICTAPE auf den Einheitentyp gesetzt werden, der im Befehl **DEFINE DEVCLASS** angegeben ist.

Bei den folgenden Bandeinheiten können Sie auswählen, ob der IBM Spectrum Protect-Bandeinheitentreiber oder der native Einheitentreiber für Ihr Betriebssystem installiert werden soll:

ECART
LTO (nicht von IBM)

Alle über SCSI angeschlossenen Speicherarchive, die Bandlaufwerke aus der Liste enthalten, müssen den IBM Spectrum Protect-Wechslertreiber verwenden.

Bandeinheitentreiber anderer Hardwareanbieter können verwendet werden, wenn sie der Einheitenklasse GENERICTAPE zugeordnet sind. Generische Einheitentreiber werden in Einheitenklassen WORM (Write Once Read Many) nicht unterstützt.

Linux

Sie können den IBM Spectrum Protect-Durchgriffseinheitentreiber verwenden. IBM Spectrum Protect-Durchgriffseinheitentreiber erfordern den generischen Linux-SCSI-Einheitentreiber (sg) zusammen mit dem Linux-Betriebssystem für die Installation der Kernel.

Sie können beispielsweise den IBM Spectrum Protect-Durchgriffseinheitentreiber für die folgenden Bandeinheiten installieren:

ECART
LTO (nicht von IBM)

Alle über SCSI angeschlossenen Speicherarchive, die Bandlaufwerke enthalten, die in der Liste nicht mit IBM gekennzeichnet sind, müssen ebenfalls den IBM Spectrum Protect-Durchgriffseinheitentreiber verwenden.

Sie können den generischen SCSI-Bandeinheitentreiber (st), der vom Linux-Betriebssystem bereitgestellt wird, nicht verwenden. Demzufolge wird der Einheitentyp GENERICTAPE für den Befehl **DEFINE DEVCLASS** nicht unterstützt.

Windows Sie können einen durch Windows Hardware Quality Labs (WHQL) zertifizierten Treiber anstelle des IBM Spectrum Protect-Einheitentreibers auswählen. Der durch die Windows Hardware Qualification Labs (WHQL) zertifizierte Einheitentreiber kann nur für Einheiten verwendet werden, die keinen IBM Kennsatz haben, sowie für Bandlaufwerke eines anderen Herstellers als IBM. Für den durch die Windows Hardware Qualification Labs zertifizierten Einheitentreiber können Sie entweder den IBM Spectrum Protect-SCSI-Durchgriffseinheitentreiber oder den Windows-Bandeinheitentreiber auswählen. Wenn der SCSI-Durchgriffseinheitentreiber verwendet wird, darf die Einheitenklasse im Befehl **DEFINE DEVCLASS** nicht GENERICTAPE lauten. Wenn der Windows-Bandeinheitentreiber verwendet wird, muss die Einheitenklasse GENERICTAPE lauten.

Gerätedateinamen für Bandeinheiten

Eine Bandeinheit muss einen Gerätedateinamen haben, damit der Server mit Bandeinheiten, Datenträgerwechslern oder Einheiten für austauschbare Datenträger arbeiten kann.

AIX

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 19 auf Seite 84 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. Sie können den Betriebssystembefehl **SMIT** verwenden, um den Gerätedateinamen für die Einheit abzurufen. In den Beispielen gibt *x* eine ganze Zahl größer-gleich 0 an.

Tabelle 19. Beispiele für Einheiten

Einheit	Beispiel für Einheit	Name der logischen Datei
Bandlaufwerke, die vom IBM Spectrum Protect-Einheitentreiber verwendet werden können	/dev/mt*x*	mt*x*
Bandlaufwerke, die vom IBM Bandeinheitentreiber verwendet werden können	/dev/rmt*x*	rmt*x*
Bandlaufwerke, die vom generischen IBM AIX-Bandeinheitentreiber verwendet werden können	/dev/rmt*x*	rmt*x*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Einheitentreiber verwendet werden können	/dev/lb*x*	lb*x*
Speicherarchiveinheiten, die vom IBM Bandeinheitentreiber verwendet werden können	/dev/smc*x*	smc*x*

Linux

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 20 auf Seite 84 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. In den Beispielen gibt *x* eine ganze Zahl größer-gleich 0 an.

Tabelle 20. Beispiele für Einheiten

Einheit	Beispiel für Einheit	Name der logischen Datei
Bandlaufwerke, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet werden können	/dev/tsmscsi/mt*x*	mt*x*
Bandlaufwerke, die vom IBM lin_tape-Einheitentreiber verwendet werden können	/dev/IBMtape*x*	IBMtape*x*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet werden können	/dev/tsmscsi/lb*x*	lb*x*
Speicherarchiveinheiten, die vom IBM lin_tape-Einheitentreiber verwendet werden können	/dev/IBMchanger*x*	IBMchanger*x*

Windows

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 21 auf Seite 85 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. In den Beispielen geben *a*, *b*, *c*, *d* und *x* jeweils eine ganze Zahl größer-gleich 0 an; dabei gilt Folgendes:

- *a* gibt die Ziel-ID an.
- *b* gibt die Nummer der logischen Einheit (LUN) an.
- *c* gibt die SCSI-Bus-ID an.
- *d* gibt die Port-ID an.

Tabelle 21. Beispiele für Einheiten

Einheit	Beispiel für Einheit	Konvertierter Einheitenname
Bandlaufwerke, die vom IBM Spectrum Protect-Einheitentreiber unterstützt werden	mt*a.b.c.d*	mt*a.b.c.d*
Bandlaufwerke, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber unterstützt werden	mt*a.b.c.d*	mt*a.b.c.d*
Bandlaufwerke, die vom IBM Einheitentreiber unterstützt werden	Tape*x*	mt*a.b.c.d*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Einheitentreiber unterstützt werden	lb.*a.b.c.d*	lb*a.b.c.d*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber unterstützt werden	lb*a.b.c.d*	lb*a.b.c.d*
Speicherarchiveinheiten, die vom IBM Einheitentreiber unterstützt werden	Changer*x*	lb*a.b.c.d*

Bandeinheitentreiber installieren und konfigurieren

Sie können Bandeinheiten erst mit IBM Spectrum Protect verwenden, nachdem der korrekte Bandeinheitentreiber installiert wurde.

IBM Spectrum Protect unterstützt alle Einheiten, die von IBM Bandeinheitentreibern unterstützt werden. IBM Spectrum Protect unterstützt jedoch nicht alle Betriebssystemversionen, die von IBM Bandeinheitentreiber unterstützt werden.

IBM Einheitentreiber für IBM Bandeinheiten installieren und konfigurieren

Installieren und Konfigurieren Sie einen IBM Bandeinheitentreiber, um eine IBM Bandeinheit verwenden zu können.

Informationen zu diesem Vorgang

Anweisungen zum Installieren und Konfigurieren von IBM Bandeinheitentreibern finden Sie in der Veröffentlichung IBM Tape Device Drivers Installation and User's Guide.

AIX Nachdem Sie die Installationsprozedur wie im Handbuch *IBM Tape Device Drivers Installation and User's Guide* beschrieben ausgeführt haben, werden, abhängig von dem Einheitentreiber, der installiert wird, unterschiedliche Nachrichten ausgegeben. Wenn Sie den Einheitentreiber für ein IBM Bandlaufwerk oder Speicherarchiv installieren, werden die folgenden Nachrichten zurückgegeben:

```
rmtx Verfügbar
```

oder

```
smcx Verfügbar
```

Notieren Sie den Wert von *x*, der vom IBM Bandeinheitentreiber zugeordnet wird. Um den Gerätedateinamen Ihrer Einheit zu bestimmen, geben Sie einen der folgenden Befehle aus:

- Für Bandlaufwerke: `ls -l /dev/rmt*`
- Für Bandarchive: `ls -l /dev/smc*`

Der Dateiname kann weitere Zeichen am Ende haben, um verschiedene Betriebsmerkmale anzugeben, die aber von IBM Spectrum Protect nicht benötigt werden. Verwenden Sie für IBM Einheitentreiber den Basisdateinamen im Parameter **DEVICE** des Befehls **DEFINE PATH**, um eine Einheit einem Laufwerk (`/dev/rmtx`) oder einem Speicherarchiv (`/dev/smcx`) zuzuordnen.

Nachdem Sie den Einheitentreiber installiert haben, können Sie mithilfe von SMIT (System Management Interface Tool) Bandlaufwerke und Bandarchive anderer Hersteller als IBM konfigurieren. Führen Sie die folgenden Schritte aus:

1. Führen Sie das Programm SMIT aus.
2. Klicken Sie auf **Devices**.
3. Klicken Sie auf **IBM Spectrum Protect Devices**.
4. Klicken Sie auf **Fibre Channel SAN Attached devices**.
5. Klicken Sie auf **Discover Devices Supported by IBM Spectrum Protect**. Warten Sie, bis der Erkennungsprozess abgeschlossen ist.
6. Kehren Sie zum Menü **Fibre Channel SAN Attached devices** zurück und klicken Sie auf **List Attributes of a Discovered Device**.

Linux Nachdem Sie die Installationsprozedur wie im Handbuch *IBM Tape Device Drivers Installation and User's Guide* beschrieben ausgeführt haben, werden, abhängig von dem Einheitentreiber, der installiert wird, unterschiedliche Nachrichten ausgegeben. Wenn Sie den Einheitentreiber für eine IBM LTO- oder 3592-Einheit installieren, werden die folgenden Nachrichten zurückgegeben:

```
IBMtapex Verfügbar
```

oder

```
IBMChangerx Verfügbar
```

Notieren Sie den Wert von *x*, der vom IBM Bandeinheitentreiber zugeordnet wird. Um den Gerätedateinamen Ihrer Einheit zu bestimmen, geben Sie einen der folgenden Befehle aus:

- Für Bandlaufwerke: `ls -l /dev/IBMtape*`
- Für Bandarchive: `ls -l /dev/IBMChange*`

Der Dateiname kann weitere Zeichen am Ende haben, um verschiedene Betriebsmerkmale anzugeben, die aber von IBM Spectrum Protect nicht benötigt werden. Verwenden Sie für IBM Einheitentreiber den Basisdateinamen im Parameter **DEVICE** des Befehls **DEFINE PATH**, um eine Einheit einem Laufwerk (`/dev/IBMtapex`) oder einem Speicherarchiv (`/dev/IBMChangerx`) zuzuordnen.

Einschränkung: Der Einheitentyp dieser Klasse darf nicht **GENERICTAPE** lauten.

Windows Für Windows-Betriebssysteme stellt IBM Spectrum Protect zwei Einheitentreiber zur Verfügung:

Durchgriffseinheitentreiber
Wenn der Hersteller der Bandeinheit einen SCSI-Einheitentreiber bereitstellt, installieren Sie den IBM Spectrum Protect-Durchgriffseinheitentreiber.

SCSI-Einheitentreiber für Bandeinheiten
Wenn der Hersteller der Bandeinheit keinen SCSI-Einheitentreiber bereitstellt, installieren Sie den IBM Spectrum Protect-SCSI-Einheitentreiber für Bandeinheiten. Der Name der Treiberdatei ist `tsmscsi64.sys`.

Anweisungen zum Installieren und Konfigurieren von IBM Bandeinheitentreibern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*. Nach der Installation des IBM Bandeinheitentreibers gibt der Server einen Gerätedateinamen `Tape`*X* für IBM Bandlaufwerke und `Changer`*Y* für IBM Datenträgerwechsler an. Für einen IBM Spectrum Protect-SCSI-Einheitentreiber oder einen IBM Spectrum Protect-Durchgriffseinheitentreiber können Sie den Windows-Betriebssystembefehl **regedit** ausgeben, um den Namen der Gerätedatei für die Einheit zu überprüfen. Der IBM Spectrum Protect-Server stellt auch ein Dienstprogramm zur Überprüfung der Einheit für das Windows-Betriebssystem zur Verfügung. Das Dienstprogramm **tsmdlst** ist im Serverpaket enthalten. Um das Dienstprogramm zu verwenden, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Anwendungsprogrammierschnittstelle (API) des Hostbusadapters installiert ist.

2. Um Einheitendaten aus dem Hostsystem abzurufen, geben Sie Folgendes ein:

```
tsmdlst
```

Zugehörige Konzepte

Multipath I/O-Zugriff mit IBM Bandeinheiten

Multipath I/O ist ein Verfahren, das unterschiedliche Pfade für den Zugriff auf dieselbe physische Einheit verwendet, beispielsweise über mehrere Hostbusadapter (HBA) oder Switches. Mithilfe des Multipathverfahrens kann sichergestellt werden, dass kein Single Point of Failure auftritt.

Multipath I/O-Zugriff mit IBM Bandeinheiten

Multipath I/O ist ein Verfahren, das unterschiedliche Pfade für den Zugriff auf dieselbe physische Einheit verwendet, beispielsweise über mehrere Hostbusadapter (HBA) oder Switches. Mithilfe des Multipathverfahrens kann sichergestellt werden, dass kein Single Point of Failure auftritt.

Der IBM Bandeinheitentreiber stellt Multipathing-Unterstützung bereit, sodass der Server beim Fehlschlagen eines Pfads einen anderen Pfad für den Zugriff auf die Daten auf einer Speichereinheit verwenden kann. Das Fehlschlagen und der Übergang zu einem anderen Pfad werden vom aktiven Server oder einem Speicheragenten nicht erkannt. Der IBM Bandeinheitentreiber verwendet Multipath I/O auch, um eine dynamische Lastverteilung für eine verbesserte Ein-/Ausgabeleistung zur Verfügung zu stellen.

Um redundante Pfade für IBM Bandeinheiten bereitzustellen, verbinden Sie jede Einheit in einer der folgenden Konfigurationen:

- Stellen Sie die Verbindung zu zwei oder mehr Ports in einem Fibre Channel-HBA mit mehreren Ports her.
- Stellen Sie die Verbindung zu einem SAS-Hostbusadapter her, sofern auf Ihrem Betriebssystem verfügbar.
- Stellen Sie die Verbindung zu einzelnen unterschiedlichen Fibre Channel-Hostbusadaptern her.

Wenn Multipath I/O aktiviert ist und ein permanenter Fehler in einem Pfad auftritt (wie beispielsweise ein defekter HBA oder ein defektes Kabel), stellen Einheitentreiber eine automatische Pfadübernahme durch einen Alternativpfad zur Verfügung.

Nach der Aktivierung von Multipath I/O erkennt der IBM Bandeinheitentreiber alle Pfade für eine Einheit auf dem Hostsystem. Ein Pfad ist als der primäre Pfad festgelegt. Die übrigen Pfade sind Alternativpfade. Die maximale Anzahl Alternativpfade für eine Einheit beträgt 16. Für jeden Pfad erstellt der IBM Bandeinheitentreiber eine Gerätedatei mit einem eindeutigen Namen. Bevor der Treiber eine Gerätedatei für den Pfad erstellen kann, muss ein Pfad auf dem System vorhanden sein. Wenn kein Pfad vorhanden ist, erstellt der Treiber keine Gerätedatei. Wenn Sie den Pfad zu einem Ziel mithilfe des Befehls **DEFINE PATH** angeben, geben Sie die Datei, die dem primären Pfad zugeordnet ist, als Wert des Parameters **DEVICE** an.

AIX

Bei AIX wird Multipath I/O nicht automatisch aktiviert, wenn der IBM Bandeinheitentreiber installiert wird. Sie müssen Multipath I/O nach der Installation für jede logische Einheit konfigurieren. Multipath I/O bleibt so lange aktiviert, bis die Einheit gelöscht wird oder die Unterstützung dekonfiguriert wird. Konfigurationsanweisungen finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*.

Um die Namen von Gerätedateien abzurufen, verwenden Sie den Befehl **ls -l**, beispielsweise **ls -l /dev/rmt***. Primäre Pfade und Alternativpfade sind, wie in dem folgenden Beispiel gezeigt, durch **PRI** bzw. **ALT** gekennzeichnet:

```
rmt0 Available 20-60-01-PRI IBM 3590 Tape Drive and Medium Changer (FCP)
rmt1 Available 30-68-01-ALT IBM 3590 Tape Drive and Medium Changer (FCP)
```

In diesem Beispiel sind dem Bandlaufwerk IBM 3590 die folgenden Pfade zugeordnet:

- 20-60-01-PRI
- 30-68-01-ALT

Der Name der Gerätedatei, die dem primären Pfad zugeordnet ist, lautet `/dev/rmt0`. Geben Sie `/dev/rmt0` als Wert des Parameters **DEVICE** im Befehl **DEFINE PATH** an.

Um pfadbezogene Details zu einem bestimmten Bandlaufwerk anzuzeigen, können Sie auch den Befehl **itdt -f /dev/rmtx path** verwenden; dabei ist *x* die Nummer des konfigurierten Bandlaufwerks. Um pfadbezogene Details zu einem bestimmten Datenträgerwechsler anzuzeigen, verwenden Sie den Befehl **itdt -f /dev/smcy path**; dabei ist *y* die Nummer des konfigurierten Datenträgerwechslers.

Linux

Bei Linux wird Multipath I/O für Datenträgerwechsler und Bandlaufwerke nicht automatisch aktiviert, wenn der Einheitentreiber installiert wird. Anweisungen zur Konfiguration von Multipath I/O finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*.

Wenn Multipath I/O für eine logische Einheit aktiviert ist, bleibt Multipath I/O so lange aktiviert, bis die Einheit gelöscht oder die Unterstützung dekonfiguriert wird.

Um die Namen von Gerätedateien für IBM Bandlaufwerke und Datenträgerwechsler anzuzeigen, verwenden Sie den Befehl **ls -l /dev/IBMx**; dabei ist *x* die Indexnummer der Einheit. Sie können auch den Befehl **cat /proc/scsi/IBMtape** für Bandlaufwerke eingeben. Wie in der Datei `IBMtape` gezeigt, sind primäre Pfade und Alternativpfade mit `Primary` bzw. `Alternate` gekennzeichnet:

```
Number     Model       SN              HBA             FO Path
 0         03592       IBM1234567      qla2xxx         Primary
 1         03592       IBM1234567      qla2xxx         Alternate
```

Der Name der Gerätedatei, die dem primären Pfad für dieses Bandlaufwerk zugeordnet ist, lautet `/dev/IBMtape0`. Geben Sie `/dev/IBMTape0` als Wert des Parameters **DEVICE** im Befehl **DEFINE PATH** für diese Einheit an.

Um die Namen der Gerätedateien abzurufen, die den primären Pfaden für alle auf dem System konfigurierten Datenträgerwechsler zugeordnet sind, führen Sie den Befehl **cat /proc/scsi/IBMchanger** aus. Das folgende Beispiel stammt aus der Datei `IBMchanger`:

```
Number     Model          SN              HBA             FO Path
 3         03584L22       IBM1002345      qla2xxx         Primary
 4         03584L22       IBM1002345      qla2xxx         Alternate
```

Der Name der Gerätedatei, die dem primären Pfad für diesen Datenträgerwechsler zugeordnet ist, lautet `/dev/IBMchanger3`. Geben Sie `/dev/IBMchanger3` als Wert des Parameters **DEVICE** im Befehl **DEFINE PATH** für diese Einheit an.

Um pfadbezogene Details zu einem bestimmten Bandlaufwerk auf dem System anzuzeigen, verwenden Sie den Befehl **itdt -f /dev/IBMtapex path**; dabei ist *x* die Nummer einer konfigurierten Bandeinheit. Um pfadbezogene Details zu einem bestimmten Datenträgerwechsler auf dem System anzuzeigen, verwenden Sie den Befehl **itdt -f /dev/IBMchangerx path**; dabei ist *x* die Nummer eines konfigurierten Datenträgerwechslers.

Windows Bei Windows wird Multipath I/O für Datenträgerwechsler und Bandlaufwerke nicht automatisch aktiviert, wenn der Einheitentreiber installiert wird. Anweisungen zur Konfiguration von Multipath I/O finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*. Wenn Multipath I/O konfiguriert ist, hat eine Einheit zwei übereinstimmende Einheitennamen mit unterschiedlichen Positionen. Um ausführliche Informationen zum primären Pfad und zum Alternativpfad abzurufen, führen Sie das IBM Tape Diagnostic Tool mit der Funktion **qrypath** aus. Die Ausgabe sieht ähnlich wie die in dem folgenden Beispiel aus:

```
C:\Users\Administrator\Downloads\ITDT> .\itdt.exe qrypath -f \\.\Tape0
Querying SCSI paths...
Total paths configured.......... 2
Alternate Path
Logical Device................. Tape0
Serial Number.................. 0000078F7612
SCSI Host ID................... 8
SCSI Channel................... 0
Target ID...................... 3
```

```
Logical Unit..................... 0
Path Enabled.................. Yes

Primary Path
Logical Device................. Tape0
Serial Number................. 0000078F7612
SCSI Host ID.................. 8
SCSI Channel.................. 0
Target ID..................... 1
Logical Unit..................... 0
Path Enabled.................. Yes


Exit with code: 0
```

AIX Bandeinheitentreiber auf AIX-Systemen konfigurieren

Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Bandeinheitentreibern anderer Hersteller als IBM auf AIX-Systemen.

Informationen zu diesem Vorgang

Anweisungen zum Installieren und Konfigurieren von IBM Bandeinheitentreibern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*.

AIX SCSI- und Fibre Channel-Einheiten

Die Menüs und Eingabeaufforderungen zur Definition von IBM Spectrum Protect-Einheiten in SMIT ermöglichen die Verwaltung von Einheiten, die über SCSI und Fibre Channel (FC) angeschlossen sind.

Das Hauptmenü von IBM Spectrum Protect verfügt über zwei Optionen:

Über SCSI angeschlossene Einheiten
Verwenden Sie diese Option, um SCSI-Einheiten zu konfigurieren, die mit einem SCSI-Adapter im Host verbunden sind.

Über Fibre Channel-SAN-angeschlossene Einheiten
Verwenden Sie diese Option, um Einheiten zu konfigurieren, die mit einem Fibre Channel-Adapter (FC-Adapter) im Host verbunden sind. Wählen Sie eines der folgenden Attribute aus:

Attribute einer erkannten Einheit auflisten
Listet Attribute einer Einheit auf, die der aktuellen ODM-Datenbank bekannt ist.

- FC Port ID:

  24-Bit FC Port ID(N(L)_Port oder F(L)_Port). Dies ist die Adress-ID, die innerhalb der zugeordneten Topologie, in der die Einheit verbunden ist, eindeutig ist. In den Switch- oder Fabric-Umgebungen kann sie durch den Switch anhand der oberen 2 Byte, die nicht null sind, bestimmt werden. In einer Private Arbitrated Loop ist dies die Arbitrated Loop Physical Address (AL_PA), wobei die oberen 2 Byte null sind. Wenden Sie sich an Ihren Fibre Channel-Hersteller, um zu bestimmen, wie wie eine AL_PA oder eine Port-ID zugeordnet wird.

- Mapped LUN ID:

  Ein FC-zu-SCSI-Brückenmodul (auch als Umsetzer, Router oder Gateway bezeichnet). Informationen zur Zuordnung von LUNs erhalten Sie von Ihrem Brückenhersteller. Zugeordnete LUN-IDs sollten nicht geändert werden.

- WW Name:

  Der weltweite Name (WWN) des Ports, an den die Einheit angeschlossen ist. Dies ist die eindeutige 64-Bit-Kennung, die von Herstellern von Fibre Channel-Komponenten wie Brücken oder nativen Fibre Channel-Einheiten zugeordnet wird. Wenden Sie sich an Ihren Fibre Channel-Hersteller, um den WWN eines Ports zu bestimmen.

- Product ID:

Die Produkt-ID einer Einheit. Wenden Sie sich an Ihren Einheitenhersteller, um die Produkt-ID zu bestimmen.

Von IBM Spectrum Protect unterstützte Einheiten erkennen
Mit dieser Option werden Einheiten in einem Fibre Channel-SAN, die von IBM Spectrum Protect unterstützt werden, erkannt und verfügbar gemacht. Wenn eine Einheit einer vorhandenen SAN-Umgebung hinzugefügt oder aus einer vorhandenen SAN-Umgebung entfernt wird, müssen Sie mithilfe dieser Option eine erneute Erkennung für die Einheiten ausführen. Einheiten müssen zunächst erkannt werden, damit aktuelle Werte der Einheitenattribute mit der Option `Attribute einer erkannten Einheit auflisten` angezeigt werden. Unterstützte Einheiten in einem Fibre Channel-SAN sind Bandlaufwerke und Datenträgerwechsler. Der IBM Spectrum Protect-Einheitentreiber ignoriert alle anderen Einheitentypen, wie beispielsweise Platte.

Alle definierten Einheiten entfernen
Mit dieser Option werden alle an ein Fibre Channel-SAN angeschlossenen IBM Spectrum Protect-Einheiten mit dem Status `DEFINED` in der ODM-Datenbank entfernt. Falls erforderlich, müssen Sie für Einheiten eine erneute Erkennung ausführen, indem Sie die Option `Von IBM Spectrum Protect unterstützte Einheiten erkennen` auswählen, nachdem alle definierten Einheiten entfernt wurden.

Einheit entfernen
Mit dieser Option wird eine einzelne an ein Fibre Channel-SAN angeschlossene IBM Spectrum Protect-Einheit mit dem Status `DEFINED` in der ODM-Datenbank entfernt. Falls erforderlich, müssen Sie für die Einheit eine erneute Erkennung ausführen, indem Sie die Option `Von IBM Spectrum Protect unterstützte Einheiten erkennen` auswählen, nachdem eine definierte Einheit entfernt wurde.

AIX IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler konfigurieren

Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler für Speicherarchive anderer Hersteller zu konfigurieren.

Vorgehensweise

Führen Sie das Programm SMIT aus, um den Einheitentreiber für jeden Datenträgerwechsler oder Robotermechanismus zu konfigurieren:

1. Wählen Sie **Devices** aus.
2. Wählen Sie **IBM Spectrum Protect Devices** aus.
3. Wählen Sie **Library/MediumChanger** aus.
4. Wählen Sie **Add a Library/MediumChanger** aus.
5. Wählen Sie den IBM Spectrum Protect-SCSI-LB für jedes von IBM Spectrum Protect unterstützte Speicherarchiv aus.
6. Wählen Sie den übergeordneten Adapter aus, mit dem die Einheit verbunden wird. Diese Nummer wird im Format 00-0X aufgelistet; dabei gibt X die Steckplatznummer der SCSI-Adapterkarte an.
7. Geben Sie, wenn Sie dazu aufgefordert werden, die Verbindungsadresse der Einheit ein, die Sie installieren. Die Verbindungsadresse ist eine zweistellige Zahl. Die erste Ziffer ist die SCSI-ID (der Wert, der auf dem Arbeitsblatt notiert wurde). Die zweite Ziffer ist die Nummer der logischen SCSI-Einheit (LUN), die - sofern nicht anders angegeben - normalerweise null ist. Die SCSI-ID und die LUN müssen durch ein Komma (,) voneinander getrennt werden.
   Beispielsweise hat die Verbindungsadresse `4,0` eine SCSI-ID=4 und eine LUN=0.
8. Klicken Sie auf **DO**.

   Sie erhalten eine Nachricht (Name einer logischen Datei) in der Form `lbX Verfügbar`. Notieren Sie den Wert von X; dabei handelt es sich um eine Zahl, die automatisch vom System zugeordnet wird. Verwenden Sie diese Informationen, um das Feld **Einheitenname** auf Ihrem Arbeitsblatt auszufüllen.

Wenn die Nachricht beispielsweise `lb0 Verfügbar` lautet, enthält das Feld **Einheitenname** auf dem Arbeitsblatt den Wert `/dev/lb0`. Verwenden Sie immer das Präfix `/dev/` mit dem von SMIT zur Verfügung gestellten Namen.

AIX IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke konfigurieren

Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke für Speicherarchive anderer Hersteller zu konfigurieren.

Vorgehensweise

Wichtig: IBM Spectrum Protect kann *tar*- oder *dd*-Bänder nicht überschreiben, *tar* oder *dd* kann jedoch IBM Spectrum Protect-Bänder überschreiben.

Einschränkung: Bandlaufwerke können nur gemeinsam genutzt werden, wenn das Laufwerk nicht definiert oder der Server nicht gestartet ist. Der Befehl **MKSYSB** funktioniert nicht, wenn sowohl IBM Spectrum Protect als auch AIX dasselbe Laufwerk oder dieselben Laufwerke gemeinsam nutzen. Um den nativen Bandeinheitentreiber des Betriebssystems mit einem SCSI-Laufwerk verwenden zu können, muss die Einheit zuerst für AIX und dann für IBM Spectrum Protect konfiguriert werden. Ihre AIX-Dokumentation enthält Informationen zu diesen nativen Einheitentreibern.

Führen Sie das Programm SMIT aus, um den Einheitentreiber für jedes Laufwerk (einschließlich Laufwerke in Speicherarchiven) wie folgt zu konfigurieren:

1. Wählen Sie **Devices** aus.
2. Wählen Sie **IBM Spectrum Protect Devices** aus.
3. Wählen Sie **Tape Drive** aus.
4. Wählen Sie **Add a Tape Drive** aus.
5. Wählen Sie den IBM Spectrum Protect-SCSI-MT für jedes unterstützte Bandlaufwerk aus.
6. Wählen Sie den Adapter aus, mit dem die Einheit verbunden wird. Diese Nummer wird im Format 00-0X aufgelistet; dabei gibt X die Steckplatznummer der SCSI-Adapterkarte an.
7. Geben Sie, wenn Sie dazu aufgefordert werden, die Verbindungsadresse der Einheit ein, die Sie installieren. Die Verbindungsadresse ist eine zweistellige Zahl. Die erste Ziffer ist die SCSI-ID (der Wert, der auf dem Arbeitsblatt notiert wurde). Die zweite Ziffer ist die Nummer der logischen SCSI-Einheit (LUN), die - sofern nicht anders angegeben - normalerweise null ist. Die SCSI-ID und die LUN müssen durch ein Komma (,) voneinander getrennt werden.
   Beispielsweise hat die Verbindungsadresse `4,0` eine SCSI-ID=4 und eine LUN=0.
8. Klicken Sie auf **DO**. Sie erhalten eine Nachricht:

   Wenn Sie den Einheitentreiber für eine Bandeinheit (kein IBM Bandlaufwerk) konfigurieren, erhalten Sie eine Nachricht (Name einer logischen Datei) in der Form `mtX Verfügbar`. Notieren Sie den Wert von X; dabei handelt es sich um eine Zahl, die automatisch vom System zugeordnet wird. Verwenden Sie diese Informationen, um das Feld **Einheitenname** auf dem Arbeitsblatt auszufüllen.

   Wenn die Nachricht beispielsweise `mt0 Verfügbar` lautet, enthält das Feld **Einheitenname** auf dem Arbeitsblatt den Wert `/dev/mt0`. Verwenden Sie immer das Präfix `/dev/` mit dem von SMIT zur Verfügung gestellten Namen.

AIX An ein Fibre Channel-SAN angeschlossene Einheiten konfigurieren

Um eine an ein Fibre Channel-SAN angeschlossene Einheit zu konfigurieren, führen Sie die Prozedur aus.

Vorgehensweise

1. Führen Sie das Programm SMIT aus.
2. Wählen Sie **Devices** aus.
3. Wählen Sie **IBM Spectrum Protect Devices** aus.

4. Wählen Sie **Fibre Channel SAN Attached devices** aus.
5. Wählen Sie **Discover Devices Supported by IBM Spectrum Protect** aus. Der Erkennungsprozess kann einige Zeit dauern.
6. Kehren Sie zum Menü **Fibre Channel** zurück und wählen Sie **List Attributes of a Discovered Device** aus.
7. Beachten Sie die aus drei Zeichen bestehende Einheiten-ID, die verwendet wird, wenn ein Pfad zu der Einheit für IBM Spectrum Protect definiert wird.
   Wenn ein Bandlaufwerk beispielsweise die ID `mt2` hat, geben Sie `/dev/mt2` als den Einheitennamen an.

Linux Bandeinheitentreiber auf Linux-Systemen konfigurieren

Lesen Sie die folgenden Abschnitte, wenn Sie Bandeinheitentreiber auf Linux-Systemen installieren und konfigurieren.

Linux IBM Spectrum Protect-Durchgriffstreiber für Bandeinheiten und Speicherarchive konfigurieren

Um den IBM Spectrum Protect-Durchgriffstreiber unter Linux verwenden zu können, müssen Sie die folgenden Schritte ausführen.

Vorgehensweise

1. Stellen Sie sicher, dass die Einheit mit Ihrem System verbunden ist, eingeschaltet und aktiv ist.
2. Stellen Sie sicher, dass die Einheit von Ihrem System korrekt erkannt wird, indem Sie den folgenden Befehl ausgeben:

   ```
   cat /proc/scsi/scsi
   ```

3. Stellen Sie sicher, dass sowohl das IBM Spectrum Protect-Einheitentreiberpaket (`tsmscsi`) als auch das Speicherserverpaket installiert ist.
4. Im IBM Spectrum Protect-Einheitentreiberpaket stehen zwei Treiberkonfigurationsmethoden zur Verfügung: `autoconf` und `tsmscsi`. Mit beiden Methoden werden die folgenden Tasks ausgeführt:
   - Laden des generischen Linux-SCSI-Treibers (sg) in den Kernel
   - Erstellen der erforderlichen Gerätedateien für den Durchgriffstreiber
   - Erstellen der Einheitendatendateien für Bandeinheiten (`/dev/tsmscsi/mtinfo`) und Speicherarchive (`/dev/tsmscsi/lbinfo`)
5. Führen Sie die bevorzugte Konfigurationsmethode (`autoconf` oder `tsmscsi`) für den IBM Spectrum Protect-Durchgriffstreiber aus.
   - Um die Konfigurationsmethode `autoconf` auszuführen, geben Sie den folgenden Befehl aus:

     ```
     autoconf
     ```

   - Um die Konfigurationsmethode `tsmscsi` auszuführen, führen Sie die folgenden Schritte aus:
     a. Kopieren Sie die beiden Beispielkonfigurationsdateien, die sich im Installationsverzeichnis befinden, von *mt.conf.smp* und *lb.conf.smp* in *mt.conf* bzw. *lb.conf*.
     b. Editieren Sie die Dateien `mt.conf` und `lb.conf`. Fügen Sie (wie in dem Beispiel gezeigt am Anfang der Datei) eine Zeilengruppe für jede Kombination aus SCSI-Ziel, ID und LUN hinzu. Jede Kombination aus Einträgen für SCSI-Ziel, ID und LUN entspricht einem Bandlaufwerk oder einem Speicherarchiv, das konfiguriert werden soll. Stellen Sie sicher, dass die Dateien diese Voraussetzungen erfüllen:
        – Entfernen Sie das Beispiel, das sich am Anfang der Dateien befindet.
        – Zwischen jeder Zeilengruppe muss sich eine neue Zeile befinden.
        – Hinter der letzten Zeilengruppe muss sich eine neue Zeile befinden.

– Stellen Sie sicher, dass keine der Dateien ein Nummernzeichen (#) enthält.

c. Führen Sie im Installationsverzeichnis des Einheitentreibers das Script `tsmscsi` aus.

6. Prüfen Sie, ob die Einheit korrekt konfiguriert ist, indem Sie die Textdateien für Bandeinheiten (`/dev/tsmscsi/mtinfo`) und Speicherarchive (`/dev/tsmscsi/lbinfo`) anzeigen.
7. Bestimmen Sie die Gerätedateinamen für die Bandlaufwerke und Speicherarchive:
   - Um die Namen für Bandeinheiten zu bestimmen, geben Sie den folgenden Befehl aus:

     ```
     > ls  /dev/tsmscsi/mt*
     ```

   - Um die Namen für Speicherarchive zu bestimmen, geben Sie den folgenden Befehl aus:

     ```
     > ls  /dev/tsmscsi/lb*
     ```

   Mithilfe dieser Informationen können Sie ermitteln, welche der Gerätedateinamen `/dev/tsmscsi/mtx` und `/dev/tsmscsi/lbx` dem Server zur Verfügung gestellt werden müssen, wenn Sie einen Befehl **`DEFINE PATH`** ausgeben.

Nächste Schritte

Wenn Sie das Hostsystem erneut starten, müssen Sie das Script `autoconf` oder `tsmscsi` erneut ausführen, um IBM Spectrum Protect-Einheiten zu rekonfigurieren. Wenn Sie die IBM Spectrum Protect-Serverinstanz erneut starten, müssen Sie Einheiten nicht rekonfigurieren. Im Allgemeinen ist der generische Linux-SCSI-Treiber im Kernel vorinstalliert. Um zu prüfen, ob sich der Treiber im Kernel befindet, geben Sie den folgenden Befehl aus:

```
> lsmod | grep sg
```

Wenn sich der Treiber nicht im Kernel befindet, geben Sie den Befehl **`modprobe sg`** aus, um den sg-Treiber in den Kernel zu laden.

Linux zSeries LinuxFibre Channel-Adapter-Einheitentreiber (zfcp) installieren

Der zSeries Linux Fibre Channel-Adapter-Einheitentreiber (zfcp) ist ein spezieller Adaptertreiber auf dem IBM zSeries-System.

Informationen zu diesem Vorgang

IBM Spectrum Protect und IBM Bandeinheitentreiber können auf zSeries-Plattformen mit Linux-Betriebssystemen in 64-Bit-Umgebungen ausgeführt werden. Sie unterstützen die meisten OEM-Bandeinheiten (OEM = Original-Equipment-Manufacturer) und IBM Bandeinheiten mit Fibre Channel-Schnittstellen.

Weitere Informationen zum Treiber zfcp finden Sie im IBM Redpaper, *Getting Started with zSeries Fibre Channel Protocol*, das unter IBM Redbooks verfügbar ist.

Vorgehensweise

1. Laden Sie das Modul qdio.
2. Installieren Sie den Treiber zfcp.
3. Ordnen Sie das Fibre Channel Protocol (FCP) zu und konfigurieren Sie den Treiber zfcp.
4. Installieren und konfigurieren Sie den IBM Bandeinheitentreiber.

Linux Informationen zu SCSI-Einheiten Ihres Systems

Informationen zu den Einheiten, die von Ihrem System erkannt werden, befinden sich in der Datei */proc/scsi/scsi*. Diese Datei enthält eine Liste aller erkannten SCSI-Einheiten.

Die folgenden Einheitendaten sind verfügbar: Hostnummer, Kanalnummer, SCSI-ID, Nummer der logischen Einheit, Anbieter, Firmwareversion, Einheitentyp und SCSI-Modus. Wenn ein System beispielsweise einige StorageTek- und IBM Speicherarchive, ein SAN-Gateway und einige Quantum DLT-Laufwerke enthält, sieht die Datei */proc/scsi/scsi* ähnlich nachfolgend gezeigt aus:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor:  STK    Model: 9738     Rev: 2003
  Type:  Medium Changer        ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  PATHLIGHT Model: SAN Gateway     Rev: 32aC
  Type: Unknown         ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  QUANTUM  Model: DLT7000     Rev: 2560
  Type:  Sequential-Access         ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM     Model: 7337     Rev: 1.63
  Type:  Medium Changer         ANSI SCSI revision: 02
```

Linux Überschreiben von Bandkennsätzen verhindern

Der IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet den generischen Linux-SCSI-Einheitentreiber (sg), um Bandeinheiten, die an das System angeschlossen sind, zu steuern und zu betreiben. Wenn der generische Linux-SCSI-Bandeinheitentreiber (st) in den Kernel geladen wird und angeschlossene Bandeinheiten konfiguriert, können in Bezug auf die Art und Weise, wie eine Einheit verwaltet wird, Konflikte auftreten, da der generische sg-Treiber und der st-Treiber beide dieselbe Einheit steuern können.

Informationen zu diesem Vorgang

Wenn der st-Treiber Einheiten steuert, die von IBM Spectrum Protect verwendet werden, können interne IBM Spectrum Protect-Bandkennsätze überschrieben werden und Daten verloren gehen. Wenn eine Anwendung den st-Treiber zum Steuern von Einheiten verwendet und die Option, die angibt, dass Bänder nicht zurückgespult werden sollen, nicht definiert ist, werden Bänder automatisch nach Beendigung einer Operation zurückgespult. Mit der Operation zum automatischen Zurückspulen wird der Bandkennsatz wieder auf den Bandanfang positioniert. Wenn das Band im Laufwerk geladen bleibt, wird der IBM Spectrum Protect-Bandkennsatz bei der nächsten Schreiboperation, die keine IBM Spectrum Protect-Schreiboperation ist, überschrieben, da sich der Kennsatz am Anfang des Bands befindet.

Um zu verhindern, dass IBM Spectrum Protect-Kennsätze überschrieben werden, was zu einem Datenverlust führen kann, müssen Sie sicherstellen, dass nur der IBM Spectrum Protect-Durchgriffstreiber Einheiten steuert, die von IBM Spectrum Protect verwendet werden. Entfernen Sie den st-Treiber aus dem Kernel oder löschen Sie, wenn der Treiber von einigen Anwendungen auf dem System verwendet wird, die Gerätedateien, die den IBM Spectrum Protect-Einheiten entsprechen, sodass der st-Treiber diese nicht mehr steuern kann.

Wenn Sie den IBM Bandeinheitentreiber zum Steuern von Einheiten auf Ihrem System verwenden, können dieselben Probleme in Bezug auf Konflikte bei der Steuerung durch den Einheitentreiber auftreten. Bestimmen Sie anhand der Dokumentation zum IBM Bandeinheitentreiber, wie dieses Problem behoben und ein Datenverlust verhindert werden kann.

Entfernen Sie den st-Treiber.

Wenn keine anderen Anwendungen auf dem System st-Einheiten verwenden, entfernen Sie den st-Treiber aus dem Kernel. Geben Sie den folgenden Befehl aus, um den st-Treiber zu entladen:

```
rmmod st
```

Löschen Sie Gerätedateien für Einheiten, die IBM Spectrum Protect-Einheiten entsprechen.

Wenn Anwendungen vorhanden sind, die die Verwendung des st-Treibers erfordern, löschen Sie die Gerätedateien, die IBM Spectrum Protect-Einheiten entsprechen. Diese Gerätedateien werden vom st-Treiber generiert. Wenn diese Dateien gelöscht werden, kann der st-Treiber die entsprechenden IBM Spectrum Protect-Einheiten nicht mehr steuern. Gerätedateinamen für Bandlaufwerke werden im Verzeichnis `/dev/` angezeigt. Ihre Namen haben das Format `/dev/[n]st[0-1024][l][m][a]`.

Listen Sie die Gerätedateinamen für st-Laufwerke und die Gerätedateinamen für IBM Spectrum Protect-Einheiten mit dem Befehl ls auf. Abhängig von der Ausgabe der Einheitenfolgen können Sie Einheiten in der Liste der st-Einheiten finden, die mit Einheiten in der Liste der IBM Spectrum Protect-Einheiten übereinstimmen. Mithilfe des Befehls rm können Sie dann die st-Einheiten löschen.

Geben Sie die folgenden Befehle aus, um die st-Einheiten und die IBM Spectrum Protect-Einheiten aufzulisten:

```
ls -l /dev/*st*
ls -l /dev/tsmscsi/mt*
```

Löschen Sie die st-Einheiten mit dem Befehl `rm`:

```
rm /dev/*st*
```

Windows Bandeinheitentreiber auf Windows-Systemen konfigurieren

Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Treibern für Bandeinheiten und Speicherarchive auf Windows-Systemen.

Windows Verwendung des IBM Spectrum Protect-Durchgriffstreibers für Bandeinheiten und Speicherarchive vorbereiten

Um den IBM Spectrum Protect-Durchgriffseinheitentreiber unter Windows für Bandeinheiten und Speicherarchive verwenden zu können, müssen Sie die Treiber installieren und die Einheitennamen für den zu verwendenden Server abrufen.

Vorbereitende Schritte

1. Stellen Sie fest, ob der Hersteller der Bandeinheit oder des Bandarchivs einen Einheitentreiber zur Verfügung stellt.
2. Wenn der Hersteller ein Einheitentreiberpaket bereitstellt, laden Sie das Paket herunter und installieren Sie es.
3. Konfigurieren Sie die SCSI-Einheitentreiber, indem Sie die Anweisungen des Herstellers ausführen.

Vorgehensweise

1. Installieren Sie den IBM Spectrum Protect-Durchgriffseinheitentreiber.
2. Rufen Sie die Einheitennamen ab, die der Server verwenden muss, indem Sie eine der folgenden Aktionen ausführen:
   - Führen Sie auf dem Server den Befehl **QUERY SAN** aus. In der Ausgabe werden alle Einheitennamen und ihre zugehörigen Einheitenseriennummern angezeigt.
   - Führen Sie im Serververzeichnis das Dienstprogramm **tsmdlst.exe** aus. In der Ausgabe werden alle Einheitennamen, ihre zugehörigen Einheitenseriennummern und die zugehörigen Einheitenpositionen angezeigt.
   - Führen Sie in der Windows-Eingabeaufforderung den Befehl **regedit** aus. Rufen Sie in der Ausgabe die Einheitendateinamen auf der Basis der Einheitenpositionen ab. Die Position besteht aus der Port-ID, der SCSI-Bus-ID, der LUN-ID und der SCSI-Ziel-ID. Der IBM Spectrum Protect-Einheitendateiname hat das Format mt*A*.*B*.*C*.*D* für Bandlaufwerke und lb*A*.*B*.*C*.*D* für Bandarchive; dabei gilt Folgendes:
     - *A* ist die SCSI-Ziel-ID.
     - *B* ist die LUN-ID.
     - *C* ist die SCSI-Bus-ID.
     - *D* ist die Port-ID.

Windows IBM Spectrum Protect-SCSI-Treiber für Bandeinheiten und Speicherarchive konfigurieren

Wenn der Hersteller eines Bandlaufwerks oder Bandarchivs keinen SCSI-Einheitentreiber bereitstellt, müssen Sie den IBM Spectrum Protect-SCSI-Einheitentreiber installieren.

Informationen zu diesem Vorgang

Der Name der Datei für den IBM Spectrum Protect-SCSI-Einheitentreiber ist `tsmscsi64.sys`.

Vorgehensweise

1. Lokalisieren Sie die Einheit in der Konsole des Geräte-Managers (`devmgmt.msc`) und wählen Sie sie aus. Bandlaufwerke sind unter **Bandlaufwerke**, Datenträgerwechsler unter **Datenträgerwechsler** aufgelistet.
2. Konfigurieren Sie die Einheit für die Verwendung durch den Einheitentreiber `tsmscsi64.sys`:
   a. Klicken Sie mit der rechten Maustaste auf die Einheit und klicken Sie auf **Treibersoftware aktualisieren**.
   b. Klicken Sie auf **Auf dem Computer nach Treibersoftware suchen**.
3. Klicken Sie auf **Aus einer Liste von Gerätetreibern auf dem Computer auswählen**.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie die entsprechende Option aus:
   a. Wählen Sie für ein Bandlaufwerk **IBM Spectrum Protect für Bandlaufwerke** aus.
   b. Wählen Sie für einen Datenträgerwechsler **IBM Spectrum Protect für Datenträgerwechsler** aus.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Schließen**.
8. Prüfen Sie, ob die Einheit korrekt für den Einheitentreiber `tsmscsi64` konfiguriert wurde:
   a. Klicken Sie mit der rechten Maustaste auf die Einheit und klicken Sie auf **Eigenschaften**.
   b. Klicken Sie auf die Registerkarte **Treiber** und dann auf **Treiberdetails**. Im Fenster **Treiberdetails** wird der Einheitentreiber angezeigt, der die Einheit steuert.

Speicherarchive für die Verwendung durch einen Server konfigurieren

Um ein Speicherarchiv oder Speicherarchive für Speicher eines IBM Spectrum Protect-Servers verwenden zu können, müssen Sie zunächst die Einheiten auf dem Serversystem konfigurieren.

Vorbereitende Schritte

1. Schließen Sie Einheiten an die Server-Hardware an. Führen Sie die Anweisungen in „Automatisierte Speicherarchiveinheit an das System anschließen" auf Seite 81 aus.
2. Wählen Sie die Bandeinheitentreiber aus. Führen Sie die Anweisungen in „Bandeinheitentreiber auswählen" auf Seite 82 aus.
3. Installieren und konfigurieren Sie die Bandeinheitentreiber. Führen Sie die Anweisungen in „Bandeinheitentreiber installieren und konfigurieren" auf Seite 85 aus.
4. Bestimmen Sie die Einheitennamen, die zum Definieren des Speicherarchivs für den Server benötigt werden. Führen Sie die Anweisungen in „Gerätedateinamen für Bandeinheiten" auf Seite 83 aus.

Vorgehensweise

1. Definieren Sie das Speicherarchiv und den Pfad vom Server zum Speicherarchiv. Führen Sie die Anweisungen in „Speicherarchive definieren” auf Seite 98 aus.
2. Definieren Sie die Laufwerke im Speicherarchiv. Führen Sie die Anweisungen in „Laufwerke definieren” auf Seite 99 aus.

   Bei SCSI-Speicherarchiven und können Sie mithilfe des Befehls **PERFORM LIBACTION** Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren, anstatt die beiden Schritte „2” auf Seite 97 und „3” auf Seite 97 auszuführen. Um den Befehl **PERFORM LIBACTION** zum Definieren von Laufwerken und Pfaden für ein Speicherarchiv verwenden zu können, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein.
3. Definieren Sie mithilfe des Befehls **DEFINE PATH** einen Pfad vom Server zu jedem Laufwerk.
4. Definieren Sie eine Einheitenklasse. Führen Sie die Anweisungen in „Bandeinheitenklassen definieren” auf Seite 101 aus.

   Einheitenklassen geben die Aufzeichnungsformate für Laufwerke an und klassifizieren diese gemäß dem Typ. Verwenden Sie den Standardwert **FORMAT=DRIVE** nur dann als Aufzeichnungsformat, wenn alle Laufwerke, die der Einheitenklasse zugeordnet sind, Daten von allen Datenträgern lesen bzw. auf alle Datenträger schreiben können.

   Angenommen, es ist eine Kombination aus Ultrium-Laufwerken der Generation 3 und Ultrium-Laufwerken der Generation 4 vorhanden, es sind aber nur Ultrium-Datenträger der Generation 3 vorhanden. Sie können **FORMAT=DRIVE** angeben, da sowohl die Laufwerke der Generation 4 als auch die Laufwerke der Generation 3 Daten von Datenträgern der Generation 3 lesen bzw. auf Datenträger der Generation 3 schreiben können.
5. Definieren Sie einen Speicherpool mithilfe des Befehls **DEFINE STGPOOL**.

   Beachten Sie beim Definieren von Speicherpools die folgenden wichtigsten Auswahlmöglichkeiten:

   - Arbeitsdatenträger sind leere Datenträger, die für die Verwendung verfügbar sind. Wenn Sie für die maximale Anzahl Arbeitsdatenträger in dem Speicherpool einen Wert angeben, kann der Server aus den in dem Speicherarchiv verfügbaren Arbeitsdatenträgern eine Auswahl treffen.

     Wenn keine Arbeitsdatenträger zulässig sind, müssen Sie einen zusätzlichen Schritt ausführen, in dem Sie jeden im Speicherpool zu verwendenden Datenträger explizit definieren. Geben Sie außerdem den Parameter **MAXSCRATCH=0** an, wenn Sie den Speicherpool definieren, damit keine Arbeitsdatenträger verwendet werden.
   - Die Standardeinstellung für primäre Speicherpools ist die Kollokation nach Gruppe. Für Kopienspeicherpools und Pools für aktive Daten ist die Kollokation standardmäßig inaktiviert. Mithilfe der *Kollokation* speichert der Server alle Dateien, die zu einer Gruppe von Clientknoten, einem einzelnen Clientknoten, einem Clientdateibereich oder einer Gruppe von Clientdateibereichen gehören, auf möglichst wenigen Datenträgern. Wenn die Kollokation für einen Speicherpool inaktiviert ist und Clients mit dem Speichern von Daten beginnen, können Sie die Daten in dem Pool nicht einfach so ändern, dass sie kollokiert werden.
6. Stellen Sie Datenträger in das Speicherarchiv zurück und ordnen Sie ihnen Kennsätze zu. Führen Sie die Anweisungen in „Datenträger in ein automatisiertes Speicherarchiv zurückstellen” auf Seite 194 und „Banddatenträgern Kennsätze zuordnen” auf Seite 192 aus.

   Stellen Sie sicher, dass genügend Datenträger in dem Speicherarchiv für den Server verfügbar sind. Halten Sie genügend Datenträger mit Kennsätzen bereit, damit während einer Operation, wie beispielsweise einer Clientsicherung, keine Datenträger fehlen. Ordnen Sie zusätzlichen Arbeitsdatenträgern Kennsätze zu, damit später für mögliche Wiederherstellungsoperationen Arbeitsdatenträger verfügbar sind.

   Die Prozeduren für das Zurückstellen von Datenträgern und das Zuordnen von Kennsätzen sind, unabhängig davon, ob das Speicherarchiv Laufwerke mit einem einzigen Einheitentyp oder Laufwerke mit mehreren Einheitentypen enthält, identisch. Mit dem Befehl **CHECKIN LIBVOLUME** können Sie Datenträger, denen bereits ein Kennsatz zugeordnet wurde, zurückstellen. Wenn Datenträger gleichzeitig mit

dem Zuordnen eines Kennsatzes zurückgestellt werden sollen, geben Sie den Befehl **LABEL LIBVOLUME** aus.

Speicherarchive mit mehreren Einheitentypen: Wenn Ihr Speicherarchiv Laufwerke mit mehreren Einheitentypen enthält und Sie zwei Speicherarchive für den IBM Spectrum Protect-Server definiert hatten, stellen die beiden definierten Speicherarchive ein einziges physisches Speicherarchiv dar. Sie müssen Banddatenträger separat in jedes definierte Speicherarchiv zurückstellen. Stellen Sie sicher, dass die Datenträger in das korrekte IBM Spectrum Protect-Speicherarchiv zurückgestellt werden.

Nächste Schritte

Überprüfen Sie Ihre Einheitendefinitionen, um sicherzustellen, dass die gesamte Konfiguration korrekt ist. Mit dem Befehl **QUERY** können Sie Informationen zu jedem Speicherobjekt überprüfen.

Stellen Sie bei der Überprüfung der Ergebnisse des Befehls **QUERY DRIVE** sicher, dass der Einheitentyp für das Laufwerk wie erwartet lautet. Wenn ein Pfad nicht definiert ist, wird der Laufwerkeinheitentyp als UNKNOWN aufgelistet; wenn der falsche Pfad verwendet wird, wird GENERIC_TAPE oder ein anderer Einheitentyp angezeigt. Dieser Schritt ist insbesondere dann wichtig, wenn gemischte Datenträger verwendet werden.

Konfigurieren Sie wahlweise die gemeinsame Speicherarchivnutzung. Führen Sie die Anweisungen in „Gemeinsame Speicherarchivnutzung konfigurieren” auf Seite 108 aus.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Speicherarchiv definieren oder löschen)

Bandeinheiten definieren

Bevor Sie Daten sichern oder auf Band umlagern können, müssen Sie eine Bandeinheit für den Server definieren.

Speicherarchive und Laufwerke definieren

Ein Bandarchiv kann ein oder mehrere Bandlaufwerke enthalten. Nachfolgend ist beschrieben, wie Speicherarchive, Laufwerke und Pfade für den IBM Spectrum Protect-Server definiert werden.

Speicherarchive definieren

Bevor ein Laufwerk verwendet werden kann, muss das Speicherarchiv, zu dem das Laufwerk gehört, definiert werden.

Vorgehensweise

1. Definieren Sie das Speicherarchiv mit dem Befehl **DEFINE LIBRARY**.

   Beispielsweise können Sie bei einem Bandarchiv IBM TS3500 mithilfe des folgenden Befehls ein Speicherarchiv mit dem Namen ROBOTMOUNT definieren:

   ```
   define library robotmount libtype=scsi
   ```

   Wenn die gemeinsame Speicherarchivnutzung oder die LAN-unabhängige Datenversetzung erforderlich ist, lesen Sie die folgenden Informationen:

   - „Gemeinsame Speicherarchivnutzung konfigurieren” auf Seite 108
   - „LAN-unabhängige Datenversetzung konfigurieren” auf Seite 128
2. Definieren Sie mithilfe des Befehls **DEFINE PATH** einen Pfad vom Server zum Speicherarchiv. Wenn Sie den Parameter **DEVICE** angeben, geben Sie den Gerätedateinamen für die Einheit ein. Dieser Name wird vom Server für die Kommunikation mit Bandlaufwerken, Datenträgerwechslern, und Ein-

heiten für austauschbare Datenträger benötigt. Weitere Informationen zu Gerätedateinamen für Einheiten finden Sie in „Gerätedateinamen für Bandeinheiten” auf Seite 83.

AIX
```
define path server1 robotmount srctype=server desttype=library
device=/dev/lb0
```

Linux
```
define path server1 robotmount srctype=server desttype=library
device=/dev/tsmscsi/lb0
```

Windows
```
define path server1 robotmount srctype=server desttype=library
device=lb0.0.1.0
```

Zugehörige Informationen

DEFINE LIBRARY (Speicherarchiv definieren)

DEFINE PATH (Pfad definieren)

SCSI-Speicherarchive in einem SAN definieren

Beim Speicherarchivtyp SCSI in einem SAN kann der Server die Seriennummer des Speicherarchivs verfolgen. Mit der Seriennummer kann der Server die Identität der Einheit bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

Informationen zu diesem Vorgang

Falls gewünscht, können Sie die Seriennummer angeben, wenn Sie das Speicherarchiv für den Server definieren. Aus Gründen der Benutzerfreundlichkeit wird es dem Server standardmäßig ermöglicht, die Seriennummer vom Speicherarchiv abzurufen, wenn Sie den Pfad definieren.

Wenn Sie die Seriennummer angeben, bestätigt der Server, dass die Seriennummer korrekt ist, wenn Sie den Pfad zu dem Speicherarchiv definieren. Wenn Sie den Pfad definieren, können Sie den Parameter **AUTODETECT=YES** angeben, um dem Server die Korrektur der Seriennummer zu ermöglichen, wenn die von ihm erkannte Nummer nicht mit Ihrer Eingabe bei der Definition des Speicherarchivs übereinstimmt. Ein bewährtes Verfahren ist die Angabe des Parameters **AUTODETECT=YES**, damit die Seriennummer für das Laufwerk automatisch in der Datenbank aktualisiert wird, wenn der Pfad definiert wird.

Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. Nicht alle Einheiten können eine Seriennummer zurückgeben, wenn sie durch eine Anwendung wie den Server dazu aufgefordert werden. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet. Weitere Informationen finden Sie in „Auswirkungen von Einheitenänderungen im SAN” auf Seite 140.

Laufwerke definieren

Um den Server über ein Laufwerk zu informieren, das für den Zugriff auf Speicherdatenträger verwendet werden kann, geben Sie den Befehl **DEFINE DRIVE** gefolgt vom Befehl **DEFINE PATH** aus.

Vorbereitende Schritte

Ein *Laufwerkobjekt* stellt einen Laufwerkmechanismus in einem Speicherarchiv dar, das austauschbare Datenträger verwendet. Bei Einheiten mit mehreren Laufwerken, einschließlich automatisierter Speicherarchive, müssen Sie jedes Laufwerk separat definieren und einem Speicherarchiv zuordnen. Laufwerkdefinitionen können Informationen wie die Elementadresse für Laufwerke in SCSI-Speicherarchiven, die Anzahl Reinigungsvorgänge für ein Bandlaufwerk und die Angabe enthalten, ob das Laufwerk online ist.

IBM Spectrum Protect unterstützt Bandlaufwerke, bei denen es sich um Standalone-Bandlaufwerke handeln kann oder die Teil eines automatisierten Speicherarchivs sein können. Die bevorzugte Methode ist die Konfiguration der Bandspeicherlösung durch die Verwendung automatisierter Speicherarchive.

Informationen zu diesem Vorgang

Wenn Sie den Befehl **DEFINE DRIVE** ausgeben, müssen Sie einen Teil oder alle der folgenden Informationen zur Verfügung stellen:

Speicherarchivname
Der Name des Speicherarchivs, in dem sich das Laufwerk befindet.

Laufwerkname
Der Name, der dem Laufwerk zugeordnet ist.

Seriennummer
Die Seriennummer des Laufwerks. Der Parameter für die Seriennummer gilt nur für Laufwerke in SCSI-Speicherarchiven. Mit der Seriennummer kann der Server die Identität der Einheit bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

Falls gewünscht, können Sie die Seriennummer angeben. Standardmäßig kann der Server die Seriennummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird. Wenn Sie die Seriennummer angeben, bestätigt der Server, dass die Seriennummer korrekt ist, wenn Sie den Pfad zu dem Laufwerk definieren. Wenn Sie den Pfad definieren, können Sie den Parameter **AUTODETECT=YES** angeben, um dem Server die Korrektur der Seriennummer zu ermöglichen, wenn die von ihm erkannte Nummer nicht mit Ihrer Eingabe bei der Definition des Laufwerks übereinstimmt. Ein bewährtes Verfahren ist die Angabe des Parameters **AUTODETECT=YES**, damit die Seriennummer für das Laufwerk automatisch in der Datenbank aktualisiert wird, wenn der Pfad definiert wird.

Abhängig vom Leistungsspektrum des Laufwerks kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet. Siehe „Auswirkungen von Einheitenänderungen im SAN" auf Seite 140.

Elementadresse
Die Elementadresse des Laufwerks. Der Parameter **ELEMENT** gilt nur für Laufwerke in SCSI-Speicherarchiven. Die Elementadresse ist eine Zahl, die die physische Position eines Laufwerks in einem automatisierten Speicherarchiv angibt. Der Server benötigt die Elementadresse, um die physische Position des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Der Server kann die Elementadresse vom Laufwerk abrufen, wenn Sie den Pfad definieren, oder Sie können die Elementadresse angeben, wenn Sie das Laufwerk definieren. Ein bewährtes Verfahren ist die Angabe des Parameters **ELEMENT=AUTODETECT**, damit der Server die Elementnummer automatisch erkennt, wenn der Pfad zu dem Laufwerk definiert wird.

Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Elementadresse möglicherweise nicht automatisch erkennen. In diesem Fall müssen Sie die Elementadresse angeben, wenn Sie das Laufwerk definieren, falls das Speicherarchiv über mehrere Laufwerke verfügt. Um die Elementadresse abzurufen, rufen Sie das IBM Support Portal for IBM Spectrum Protect auf.

Tipp: IBM Bandeinheitentreiber und Bandeinheitentreiber anderer Hersteller als IBM generieren unterschiedliche Einheitendateien und Formate:

- Bei IBM Bandeinheitentreibern beginnen Einheitennamen mit `rmt`, gefolgt von einer ganzen Zahl, beispielsweise `/dev/rmt0`.
- Bei IBM Spectrum Protect-Bandeinheitentreibern beginnen Bandeinheitennamen mit `mt`, gefolgt von einer ganzen Zahl, beispielsweise `/dev/mt0`.

Sie müssen die korrekte Einheitendatei verwenden, wenn Sie einen Pfad definieren.

Vorgehensweise

1. Ordnen Sie einem Speicherarchiv ein Laufwerk zu, indem Sie den Befehl **DEFINE DRIVE** ausgeben.
2. Damit der Server das Laufwerk verwenden kann, geben Sie den Befehl **DEFINE PATH** aus.

   Beispiele für die Konfiguration von Speicherarchiven, Pfaden und Laufwerken finden Sie in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurie-

ren und Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren.

Bandeinheitenklassen definieren

Eine Einheitenklasse definiert eine Reihe von Merkmalen, die von einer Gruppe von Datenträgern verwendet wird, die in einem Speicherpool erstellt werden kann. Sie müssen eine Einheitenklasse für eine Bandeinheit definieren, um sicherzustellen, dass der Server die Einheit verwenden kann.

Vorbereitende Schritte

Sie müssen Speicherarchive und Laufwerke für den Server definieren, bevor Sie Einheitenklassen definieren.

Informationen zu diesem Vorgang

Eine Liste der unterstützten Einheiten und gültigen Einheitenklassenformate finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten für Ihr Betriebssystem:

- AIX | Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Sie können mehrere Einheitenklassen für jeden Einheitentyp definieren. Beispielsweise möchten Sie möglicherweise unterschiedliche Attribute für unterschiedliche Speicherpools angeben, die denselben Typ von Bandlaufwerk verwenden. Unter Umständen sind Variationen erforderlich, die nicht einheitenspezifisch sind, sondern davon abhängig sind, wie die Einheit verwendet werden soll (zum Beispiel Mount-Aufbewahrungszeitraum oder Mountlimit).

Richtlinien:

- Eine einzelne Einheitenklasse kann mehreren Speicherpools zugeordnet werden, jeder Speicherpool ist jedoch nur einer einzigen Einheitenklasse zugeordnet.
- SCSI-Speicherarchive können Bandlaufwerke mehrerer Einheitentypen umfassen. Wenn Sie die Einheitenklasse in dieser Umgebung definieren, müssen Sie einen Wert für den Parameter **FORMAT** deklarieren.

  Weitere Informationen finden Sie in „Gemischte Einheitentypen in Speicherarchiven” auf Seite 18.

Vorgehensweise

Um eine Einheitenklasse zu definieren, verwenden Sie den Befehl **DEFINE DEVCLASS** mit dem Parameter **DEVTYPE**, mit dem der Einheitenklasse ein Einheitentyp zugeordnet wird.

Ergebnisse

Wenn Sie die Option DEVCONFIG in die Datei `dsmserv.opt` einschließen, werden die über diese Option angegebenen Dateien automatisch mit den Ergebnissen der Befehle **DEFINE DEVCLASS**, **UPDATE DEVCLASS** und **DELETE DEVCLASS** aktualisiert.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

QUERY DEVCLASS (Informationen zu einer oder mehreren Einheitenklassen anzeigen)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Einheitenklassen LTO definieren

Um Probleme beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv zu vermeiden, beachten Sie die Einschränkungen. Beachten Sie außerdem die Einschränkungen für die LTO-Laufwerkverschlüsselung.

LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen

Beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern müssen Sie die Schreib-/Lesefunktionalität jeder Generation berücksichtigen. Die bevorzugte Methode ist die Konfiguration einer anderen Einheitenklasse für jede Generation von Datenträgern.

Informationen zu diesem Vorgang

Wenn Sie das Mischen verschiedener Generationen von LTO-Datenträgern und -Laufwerken in Betracht ziehen, beachten Sie die folgenden Einschränkungen:

Tabelle 22. Schreib-/Lesefunktionalität für verschiedene Generationen von LTO-Laufwerken

Laufwerke	Datenträger der Generation 1	Datenträger der Generation 2	Datenträger der Generation 3	Datenträger der Generation 4	Datenträger der Generation 5	Datenträger der Generation 6	Datenträger der Generation 7	Datenträger der Generation M8	Datenträger der Generation 8
Generation 1	Schreib-/ Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 2	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 3	Lesezugriff	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 4	nicht zutreffend	Lesezugriff	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 5	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 6	nicht zutreffend	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 7	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff	nicht zutreffend	nicht zutreffend
Generation 8	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff	Schreib-/ Lesezugriff

Beispiel

Wenn Sie verschiedene Typen von Laufwerken und Datenträgern mischen, konfigurieren Sie unterschiedliche Einheitenklassen: eine Einheitenklasse für jeden Datenträgertyp. Um den Datenträgertyp anzugeben, verwenden Sie den Parameter **FORMAT** in jeder der Einheitenklassendefinitionen. (Geben Sie nicht `FORMAT=DRIVE` an.) Wenn Sie beispielsweise Ultrium-Laufwerke der Generation 5 und Ultrium-Laufwerke der Generation 6 mischen, geben Sie `FORMAT=ULTRIUM5C` (oder `ULTRIUM5`) für die Ultrium-Einheitenklasse der Generation 5 und `FORMAT=ULTRIUM6C` (oder `ULTRIUM6`) für die Ultrium-Einheitenklasse der Generation 6 an.

In diesem Beispiel können beide Einheitenklassen auf dasselbe Speicherarchiv mit Ultrium-Laufwerken der Generation 5 und Ultrium-Laufwerken der Generation 6 verweisen. Die Laufwerke werden von den beiden Speicherpools gemeinsam genutzt. Ein Speicherpool verwendet ausschließlich die erste Einheitenklasse und Ultrium-Datenträger der Generation 5. Der andere Speicherpool verwendet ausschließlich die zweite Einheitenklasse und Ultrium-Datenträger der Generation 6. Da die beiden Speicherpools ein einzelnes Speicherarchiv gemeinsam nutzen, können Ultrium-Datenträger der Generation 5 in Ultrium-Laufwerken der Generation 6 bereitgestellt werden, sobald sie während der Mountpunktverarbeitung verfügbar werden.

Wenn Sie ältere Generationen von Datenträgern mit Lesezugriff mit neueren Generationen von Datenträgern mit Schreib-/Lesezugriff in einem einzelnen Speicherarchiv mischen, müssen Sie die Datenträger mit Lesezugriff als schreibgeschützt markieren und alle Arbeitsdatenträger mit Lesezugriff entnehmen. Wenn Sie beispielsweise Ultrium-Laufwerke und -Datenträger der Generation 4 und Ultrium-Laufwerke und -Datenträger der Generation 6 in einem einzelnen Speicherarchiv mischen, müssen Sie die Datenträger der Generation 4 als schreibgeschützt markieren. Außerdem müssen alle Arbeitsdatenträger der Generation 4 entnommen werden.

Mountlimits in LTO-Umgebungen mit gemischten Datenträgern

In einem Speicherarchiv mit gemischten Datenträgern, in dem mehrere Einheitenklassen auf dasselbe Speicherarchiv verweisen, werden kompatible Laufwerke von Speicherpools gemeinsam genutzt. Stellen Sie sicher, dass Sie für den Parameter **MOUNTLIMIT** in jeder der Einheitenklassen einen geeigneten Wert festlegen.

Beispielsweise können in einem Speicherarchiv mit gemischten Datenträgern, das Ultrium-Laufwerke und -Datenträger der Generation 1 und Ultrium-Laufwerke und -Datenträger der Generation 2 enthält, Ultrium-Datenträger der Generation 1 in Ultrium-Laufwerken der Generation 2 bereitgestellt werden.

Betrachten Sie das Beispiel für ein Speicherarchiv mit gemischten Datenträgern, das die folgenden Laufwerke und Datenträger enthält:

- Vier LTO Ultrium-Laufwerke der Generation 1 und LTO Ultrium-Datenträger der Generation 1
- Vier LTO Ultrium-Laufwerke der Generation 2 und LTO Ultrium-Datenträger der Generation 2

Sie haben die folgenden Einheitenklassen erstellt:

- Einheitenklasse LTO1CLASS für LTO Ultrium Generation 1 mit der Angabe FORMAT=ULTRIUM1C
- Einheitenklasse LTO2CLASS für LTO Ultrium Generation 2 mit der Angabe FORMAT=ULTRIUM2C

Außerdem haben Sie die folgenden Speicherpools erstellt:

- LTO Ultrium-Speicherpool LTO1POOL der Generation 1, der auf Einheitenklasse LTO1CLASS basiert
- LTO Ultrium-Speicherpool LTO2POOL der Generation 2, der auf Einheitenklasse LTO2CLASS basiert

Die Anzahl Mountpunkte, die von jedem Speicherpool verwendet werden können, wird mit dem Parameter **MOUNTLIMIT** in der Einheitenklasse angegeben. Der Parameter **MOUNTLIMIT** in der Einheitenklasse LTO2CLASS muss auf 4 gesetzt werden, damit er mit der Anzahl verfügbarer Laufwerke übereinstimmt, die nur LTO7-Datenträger bereitstellen können. Der Parameter **MOUNTLIMIT** in der Einheitenklasse LTO1CLASS muss auf einen Wert gesetzt werden, der größer als die Anzahl verfügbarer Laufwerke (5 oder möglicherweise 6) ist, um der Tatsache Rechnung zu tragen, dass Ultrium-Datenträger der Generation 1 in Ultrium-Laufwerken der Generation 7 bereitgestellt werden können. Der optimale Wert für **MOUNTLIMIT** ist von der Workload und Speicherpoolzugriffsmustern abhängig.

Überwachen Sie die Einstellung für **MOUNTLIMIT** und passen Sie sie gemäß sich ändernden Workloads an. Wenn der Wert für **MOUNTLIMIT** für LTO1POOL zu hoch definiert wird, können Mountanforderungen für LTO2POOL verzögert werden oder fehlschlagen, da die Ultrium-Laufwerke der Generation 2 zur Ausführung von Mountanforderungen für Ultrium Generation 1 verwendet werden. Im Worst-Case-Szenario kann ein zu starkes Konkurrieren um Ultrium-Laufwerke der Generation 2 dazu führen, dass Mounts für Datenträger der Generation 2 mit der folgenden Nachricht fehlschlagen:

```
ANR8447E Gegenwärtig sind keine Laufwerke im Kassettenarchiv verfügbar.
```

Wenn der Wert für **MOUNTLIMIT** für LTO1POOL nicht hoch genug definiert wird, werden Mountanforderungen, die von LTO Ultrium-Laufwerken der Generation 2 ausgeführt werden könnten, verzögert.

Einschränkung: Aufgrund der Art und Weise, auf die Mountpunkte zugeordnet werden, gelten beim Kombinieren von Ultrium-Laufwerken der Generation 1 mit Ultrium-Laufwerken der Generation 2 oder der Generation 3 Einschränkungen. Prozesse, die mehrere Mountpunkte erfordern, die sowohl Ultrium-Datenträger der Generation 1 als auch Ultrium-Datenträger der Generation 2 einschließen, versuchen beispielsweise unter Umständen, nur Ultrium-Laufwerke der Generation 2 zu reservieren, selbst wenn ein einzelner Mount von einem verfügbaren Ultrium-Laufwerk der Generation 6 ausgeführt werden kann. Zu den Prozessen, die dieses Verhalten zeigen, gehören die Befehle **MOVE DATA** und **BACKUP STGPOOL**. Diese Prozesse warten, bis die erforderliche Anzahl Mountpunkte mit Ultrium-Laufwerken der Generation 2 erreicht werden kann.

Zugehörige Informationen

BACKUP STGPOOL (Daten in primären Speicherpools in einem Kopienspeicherpool sichern)

DEFINE DEVCLASS (Einheitenklasse definieren)

MOVE DATA (Dateien auf einen Speicherpooldatenträger versetzen)

Laufwerkverschlüsselung für LTO-Bandlaufwerke der Generation 4 oder späterer Generationen aktivieren und inaktivieren

IBM Spectrum Protect unterstützt die drei Typen von Laufwerkverschlüsselung, die für LTO-Laufwerke der Generation 4 oder späterer Generationen verfügbar sind: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

Informationen zu diesem Vorgang

Der Parameter **DRIVEENCRYPTION** im Befehl **DEFINE DEVCLASS** gibt an, ob die Laufwerkverschlüsselung für IBM und HP LTO-Formate der Generation 4 oder späterer Generationen sowie für Ultrium 4- und Ultrium 4C-Formate zulässig ist. Mit diesem Parameter wird IBM Spectrum Protect-Kompatibilität mit Hardwareverschlüsselungseinstellungen für leere Datenträger sichergestellt. Sie können diesen Parameter nicht für Speicherpooldatenträger verwenden, die voll sind oder gefüllt werden.

IBM Spectrum Protect unterstützt das Anwendungsverschlüsselungsverfahren mit IBM und HP LTO-4-Laufwerken oder Laufwerken späterer Generationen. Die System- und Speicherarchivverfahren werden nur von IBM LTO-4 oder späteren Generationen unterstützt. Das Speicherarchivverschlüsselungsverfahren kann nur verwendet werden, wenn es von Ihrer Systemhardware (beispielsweise IBM TS3500) unterstützt wird.

Einschränkung: Sie können keine Laufwerkverschlüsselung für WORM-Datenträger (WORM = Write Once Read Many) verwenden.

Das Anwendungsverfahren wird über die Hardware definiert. Um das Anwendungsverfahren zu verwenden, bei dem IBM Spectrum Protect Verschlüsselungsschlüssel generiert und verwaltet, setzen Sie den Parameter **DRIVEENCRYPTION** auf ON. Mit dieser Aktion wird die Datenverschlüsselung für leere Datenträger aktiviert. Wenn der Parameter auf ON gesetzt wird und die Hardware für ein anderes Verschlüsselungsverfahren konfiguriert ist, schlagen Sicherungsoperationen fehl.

Vorgehensweise

Das folgende vereinfachte Beispiel zeigt die Schritte für die Aktivierung und die Inaktivierung der Datenverschlüsselung für leere Datenträger in einem Speicherpool:

1. Definieren Sie ein Speicherarchiv, indem Sie den Befehl **DEFINE LIBRARY** ausgeben:

   ```
   define library 3584 libtype=SCSI
   ```

2. Definieren Sie eine Einheitenklasse mit dem Namen LTO_ENCRYPT, indem Sie den Befehl **DEFINE DEVCLASS** unter Angabe von IBM Spectrum Protect als Schlüsselmanager ausgeben:

   ```
   define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
   ```

3. Definieren Sie einen Speicherpool, indem Sie den Befehl **DEFINE STGPOOL** ausgeben:

   ```
   define stgpool lto_encrypt_pool lto_encrypt
   ```

4. Um die Verschlüsselung für neue Datenträger zu inaktivieren, setzen Sie den Parameter **DRIVEENCRYPTION** auf OFF. Der Standardwert ist ALLOW. Die Laufwerkverschlüsselung für leere Datenträger ist zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

Zugehörige Konzepte

Verschlüsselungsverfahren für Bänder
Die Entscheidung über das zu verwendende Verschlüsselungsverfahren ist davon abhängig, wie Ihre Daten verwaltet werden sollen.

Einheitenklassen 3592 definieren

Einheitenklassendefinitionen für 3592-, TS1130-, TS1140-, TS1150-Einheiten und Einheiten späterer Generationen umfassen Parameter für höhere Datenträgerzugriffsgeschwindigkeiten und Laufwerkverschlüsselung. Um Probleme beim Mischen verschiedener Generationen von 3592- und TS1130-Laufwer-

ken und Laufwerken späterer Generationen in einem Speicherarchiv zu verhindern, lesen Sie die Richtlinien.

Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen

Um eine optimale Leistung zu erzielen, dürfen Sie keine Generationen von 3592-Datenträgern in einem einzelnen Speicherarchiv mischen. Es können Datenträgerprobleme auftreten, wenn verschiedene Laufwerkgenerationen gemischt werden. Beispielsweise kann IBM Spectrum Protect möglicherweise den Kennsatz eines Datenträgers nicht lesen.

Informationen zu diesem Vorgang

Die folgende Tabelle zeigt Schreib-/Leseinteroperabilität für Laufwerkgenerationen.

Laufwerke	Format der Generation 1	Format der Generation 2	Format der Generation 3	Format der Generation 4	Format der Generation 5
Generation 1	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 2	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 3	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend
Generation 4	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend
Generation 5	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff

Wenn Generationen von Laufwerken in einem Speicherarchiv gemischt werden müssen, schauen Sie sich das Beispiel und die Einschränkungen an, um Probleme zu vermeiden.

Tabelle 23. Generationen von Laufwerken mischen

Speicherarchivtyp	Beispiel und Einschränkungen
SCSI	Definieren Sie einen neuen Speicherpool und eine neue Einheitenklasse für die neueste Laufwerkgeneration. Angenommen, Sie verfügen über einen Speicherpool und eine Einheitenklasse für 3592-2. Der Speicherpool enthält alle Datenträger, die im Format der Generation 2 geschrieben wurden. Angenommen, der Wert des Parameters **FORMAT** in der Einheitenklassendefinition ist auf 3952-2 (nicht **DRIVE**) gesetzt. Sie fügen dem Speicherarchiv Laufwerke der Generation 3 hinzu. Führen Sie die folgenden Schritte aus: 1. Setzen Sie in der neuen Einheitenklassendefinition für die Laufwerke der Generation 3 den Wert für den Parameter **FORMAT** auf 3592-3 oder 3592-3C. Geben Sie nicht **DRIVE** an. 2. Aktualisieren Sie in der Definition des Speicherpools, der Laufwerken der Generation 2 zugeordnet ist, den Parameter **MAXSCRATCH** mit 0, beispielsweise: `update stgpool genpool2 maxscratch=0` Diese Methode ermöglicht beiden Generationen die Verwendung ihres optimalen Formats und minimiert mögliche Datenträgerprobleme, die aus dem Mischen von Generationen resultieren können. Es werden jedoch nicht alle Datenträgerprobleme behoben. Beispielsweise könnten Konkurrenzsituationen bei Mountpunkten und Mountfehler die Folge sein. (Weitere Informationen zu Konkurrenzsituationen bei Mountpunkten im Kontext von 3592-Laufwerken und -Datenträgern finden Sie in „Einheitenklassen 3592 definieren” auf Seite 104.) **Einschränkung:** In der folgenden Liste sind Einschränkungen beschrieben, die für Datenträger gelten: • **CHECKIN LIBVOL**: Das Problem liegt in der Verwendung der Option CHECKLABEL=YES. Wenn der Kennsatz in einem Format der Generation 3 oder einem späteren Format geschrieben ist und Sie die Option CHECKLABEL=YES angeben, schlägt die Verwendung dieses Befehls für Laufwerke früherer Generationen fehl. Um dieses Problem zu verhindern, geben Sie CHECKLABEL=BARCODE an. • **LABEL LIBVOL**: Wenn der Server versucht, Laufwerke einer früheren Generation zum Lesen des Kennsatzes zu verwenden, der in einem Format der Generation 3 oder einem späteren Format geschrieben ist, schlägt der Befehl **LABEL LIBVOL** fehl, es sei denn, OVERWRITE=YES wird angegeben. Stellen Sie sicher, dass Datenträger, denen unter Angabe von OVERWRITE=YES ein Kennsatz zugeordnet wird, keine aktiven Daten enthalten. • **CHECKOUT LIBVOL**: Wenn IBM Spectrum Protect feststellt, dass der Kennsatz (CHECKLABEL=YES) in einem Format der Generation 3 oder einem Format einer späteren Generation geschrieben ist, und Leseoperationen durch Laufwerke früherer Generationen erfolgen, schlägt der Befehl fehl. Um dieses Problem zu verhindern, geben Sie CHECKLABEL=NO an.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
UPDATE STGPOOL (Speicherpool aktualisieren)

Datenzugriffsgeschwindigkeiten für 3592-Datenträger steuern

Sie können die Speicherkapazität optimieren und Datenzugriffsgeschwindigkeiten verbessern, wenn Sie Datenträger erstellen. Indem Daten in Speicherpools mit Datenträgern partitioniert werden, können Sie die Skalierungskapazität in Prozent angeben, um maximale Speicherkapazität oder schnellen Zugriff auf den Datenträger bereitstellen zu können.

Informationen zu diesem Vorgang

Um die Datenträgerkapazität zu reduzieren, geben Sie den Parameter **SCALECAPACITY** an, wenn Sie die Einheitenklasse mit dem Befehl **DEFINE DEVCLASS** definieren oder wenn Sie die Einheitenklasse mit dem Befehl **UPDATE DEVCLASS** aktualisieren.

Geben Sie einen Prozentwert von 20, 90 oder 100 an. Mit einem Wert von 20 Prozent wird die schnellste Zugriffszeit und mit einem Wert von 100 Prozent die größte Speicherkapazität zur Verfügung gestellt. Wird beispielsweise eine Skalierungskapazität von 20 für eine Einheitenklasse 3592 ohne Komprimierung angegeben, würde ein 3592-Datenträger in dieser Einheitenklasse 20 Prozent seiner vollen Kapazität von 300 GB, d. h. ungefähr 60 GB, speichern.

Die Skalierungskapazität hat nur Auswirkungen, wenn Daten zum ersten Mal auf einen Datenträger geschrieben werden. Aktualisierungen an der Einheitenklasse für die Skalierungskapazität haben erst Auswirkungen auf einen Datenträger, auf den bereits Daten geschrieben wurden, wenn der Datenträger in den Arbeitsstatus zurückversetzt wird.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen aktivieren und inaktivieren

Bei IBM Spectrum Protect können Sie die folgenden Typen von Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen verwenden: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

Informationen zu diesem Vorgang

Der Parameter **DRIVEENCRYPTION** im Befehl **DEFINE DEVCLASS** gibt an, ob die Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen zulässig ist. Verwenden Sie diesen Parameter, um IBM Spectrum Protect-Kompatibilität mit Hardwareverschlüsselungseinstellungen für leere Datenträger sicherzustellen. Sie können diesen Parameter nicht für Speicherpooldatenträger verwenden, die voll sind oder gefüllt werden.

- Um das Anwendungsverfahren zu verwenden, bei dem IBM Spectrum Protect Verschlüsselungsschlüssel generiert und verwaltet, setzen Sie den Parameter **DRIVEENCRYPTION** auf ON. Damit wird die Verschlüsselung von Daten für leere Datenträger aktiviert. Wenn der Parameter auf ON gesetzt wird und die Hardware für ein anderes Verschlüsselungsverfahren konfiguriert ist, schlagen Sicherungsoperationen fehl.
- Um das Speicherarchiv- oder Systemverschlüsselungsverfahren zu verwenden, setzen Sie den Parameter auf **ALLOW**. Damit wird angegeben, dass IBM Spectrum Protect nicht der Schlüsselmanager für die Laufwerkverschlüsselung ist, der Hardware wird jedoch die Verschlüsselung der Daten des Datenträgers über eines der anderen Verfahren ermöglicht. Bei Angabe dieses Parameters werden Datenträger nicht automatisch verschlüsselt. Daten können nur verschlüsselt werden, wenn der Parameter **ALLOW** angegeben wird und die Hardware für die Verwendung eines dieser Verfahren konfiguriert wird.

Der Parameter **DRIVEENCRYPTION** ist optional. Gemäß dem Standardwert ist das Speicherarchiv- oder Systemverschlüsselungsverfahren zulässig.

Vorgehensweise

Das folgende vereinfachte Beispiel zeigt, wie Daten für leere Datenträger in einem Speicherpool unter Verwendung von IBM Spectrum Protect als Schlüsselmanager verschlüsselt werden können:

1. Definieren Sie ein Speicherarchiv, indem Sie den Befehl **DEFINE LIBRARY** ausgeben.
   Geben Sie beispielsweise den folgenden Befehl aus:

```
define library 3584 libtype=SCSI
```

2. Definieren Sie eine Einheitenklasse mit dem Namen 3592_ENCRYPT, indem Sie den Befehl **DEFINE DEVCLASS** unter Angabe des Werts ON für den **DRIVEENCRYPTION** Parameter ausgeben.
   Geben Sie beispielsweise den folgenden Befehl aus:

```
define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
```

3. Definieren Sie einen Speicherpool.
   Geben Sie beispielsweise den folgenden Befehl aus:

```
define stgpool 3592_encrypt_pool 3592_encrypt
```

Nächste Schritte

Um eines des Verschlüsselungsverfahren für neue Datenträger zu inaktivieren, setzen Sie den Parameter **DRIVEENCRYPTION** auf OFF. Wenn die Hardware für die Verschlüsselung von Daten durch das Speicherarchiv- oder Systemverfahren konfiguriert ist und **DRIVEENCRYPTION** auf OFF gesetzt ist, schlagen Sicherungsoperationen fehl.

Gemeinsame Speicherarchivnutzung konfigurieren

Mehrere IBM Spectrum Protect-Server können Speichereinheiten unter Verwendung eines Speicherbereichsnetzes (SAN) gemeinsam nutzen. Ein Server wird als Speicherarchivmanager konfiguriert, die anderen Server werden als Speicherarchivclients konfiguriert.

Vorbereitende Schritte

Stellen Sie sicher, das Ihre Systeme die Lizenzierungsanforderungen für die gemeinsame Speicherarchivnutzung erfüllen. Ein Nutzungsrecht für IBM Spectrum Protect for SAN ist für jeden IBM Spectrum Protect-Server erforderlich, der als Speicherarchivclient oder Speicherarchivmanager in einer SAN-Umgebung konfiguriert wird.

Informationen zu diesem Vorgang

Bei der LAN-unabhängigen Datenversetzung können IBM Spectrum Protect-Clientsysteme direkt auf Speichereinheiten zugreifen, die für einen IBM Spectrum Protect-Server definiert sind. Speicheragenten werden auf den Clientsystemen zur Ausführung der Datenversetzung installiert und konfiguriert.

Um die gemeinsame Speicherarchivnutzung zu konfigurieren, müssen Sie einen einzelnen IBM Spectrum Protect-Server als den Speicherarchivmanager für die Konfiguration der gemeinsamen Speicherarchivnutzung definieren. Anschließend definieren Sie weitere IBM Spectrum Protect-Server als Speicherarchivclients, die mit dem Speicherarchivmanager kommunizieren und Speicherressourcen vom Speicherarchivmanager anfordern. Der Speicherarchivmanager-Server muss dieselbe Version oder eine höhere Version wie der Server oder die Server haben, die als Speicherarchivclients definiert sind.

Vorgehensweise

Um Speicherarchivressourcen in einem SAN zwischen mehreren IBM Spectrum Protect-Servern gemeinsam nutzen zu können, führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie die Kommunikation zwischen Servern.

   Um eine Speichereinheit in einem SAN gemeinsam nutzen zu können, definieren Sie Server mithilfe der Überkreuzdefinitionsfunktion füreinander. Jeder Server muss einen eindeutigen Namen haben.
2. Definieren Sie ein gemeinsam genutztes Speicherarchiv und konfigurieren Sie Bandeinheiten auf den Serversystemen.

Verwenden Sie die in „Speicherarchive für die Verwendung durch einen Server konfigurieren” auf Seite 96 beschriebene Prozedur zum Definieren eines Speicherarchivs für die Verwendung in einer Umgebung mit gemeinsamer Nutzung. Ändern Sie die Prozedur, um das Speicherarchiv als gemeinsam genutzt zu definieren, indem Sie den Parameter **SHARED=YES** für den Befehl **DEFINE LIBRARY** angeben.

3. Definieren Sie den Speicherarchivmanager-Server.
4. Definieren Sie das gemeinsam genutzte Speicherarchiv auf dem Server, der der Speicherarchivclient ist.
5. Definieren Sie auf dem Speicherarchivmanager-Server Pfade vom Speicherarchivclient zu jedem Laufwerk, auf das der Speicherarchivclient zugreifen kann.

   Der Einheitenname muss die Art und Weise widerspiegeln, auf die das Speicherarchivclientsystem die Bandeinheit erkennt. Vom Speicherarchivmanager muss ein Pfad zu jedem Laufwerk definiert werden, damit der Speicherarchivclient das Laufwerk verwenden kann.

   Um Probleme zu verhindern, stellen Sie sicher, dass alle Laufwerkpfaddefinitionen, die für den Speicherarchivmanager definiert werden, auch für jeden Speicherarchivclient definiert werden.

   Wenn beispielsweise der Speicherarchivmanager drei Bandlaufwerke definiert, muss auch der Speicherarchivclient drei Bandlaufwerke definieren. Um die Anzahl Bandlaufwerke, die ein Speicherarchivclient gleichzeitig nutzen kann, zu begrenzen, verwenden Sie den Parameter **MOUNTLIMIT** der Einheitenklasse auf dem Speicherarchivclient.
6. Definieren Sie Einheitenklassen für das gemeinsam genutzte Speicherarchiv.

   Die bevorzugte Methode ist, auf beiden Servern identische Einheitenklassennamen zu verwenden, um Unklarheiten zu vermeiden, wenn mehrere Einheitenklassen mit demselben Einheitentyp und denselben Speicherarchivparametern definiert werden. Bei einigen Operationen, wie beispielsweise der Datenbanksicherung, wird der Einheitenklassenname zur Identifikation der Daten für die Sicherung verwendet.

   Die Einheitenklassenparameter, die auf dem Speicherarchivmanager angegeben sind, überschreiben die für den Speicherarchivclient angegebenen Parameter. Wenn die Einheitenklassennamen unterschiedlich sind, verwendet der Speicherarchivmanager die Parameter, die in einer Einheitenklasse angegeben sind, die mit dem für den Speicherarchivclient angegebenen Einheitentyp übereinstimmt.
7. Definieren Sie einen Speicherpool für das gemeinsam genutzte Speicherarchiv.
8. Wiederholen Sie die Schritte, um einen anderen Server als Speicherarchivclient zu konfigurieren.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

DEFINE LIBRARY (Speicherarchiv definieren)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Linux AIX Beispiel: Gemeinsame Speicherarchivnutzung für AIX- und Linux-Server

Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für SCSI-Speicherarchive für Server, die auf AIX- oder Linux-Systemen ausgeführt werden, konfiguriert werden kann.

Informationen zu diesem Vorgang

In diesem Beispiel werden ein Speicherarchivmanager-Server mit dem Namen ASTRO und ein Speicherarchivclient mit dem Namen JUDY konfiguriert. Um zu verdeutlichen, auf welchem Server der Schritt jeweils ausgeführt wird, steht vor dem jeweiligen Befehl der Name des Servers, auf dem der Befehl ausgegeben wird. Der größte Teil der Befehle wird auf dem Speicherarchivclient ausgegeben.

Definieren Sie für SCSI-Speicherarchive das Speicherarchiv unter Angabe des Parameters **libtype=scsi**.

Vorgehensweise

1. Um ASTRO als den Speicherarchivmanager-Server zu konfigurieren, definieren Sie ein gemeinsam genutztes SCSI-Speicherarchiv mit dem Namen SANGROUP.

   Beispiel:

   ```
   astro> define library sangroup libtype=scsi shared=yes
   ```

   Führen Sie dann die übrigen Schritte zum Konfigurieren des Speicherarchivs wie in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren beschrieben aus.

   Tipp: Mithilfe des Befehls **PERFORM LIBACTION** können Sie Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren.
2. Definieren Sie ASTRO als den Speicherarchivmanager-Server, indem Sie den Befehl **DEFINE SERVER** ausgeben.

   ```
   judy> define server astro serverpassword=secret hladdress=192.0.2.24
    lladdress=1777 crossdefine=yes
   ```
3. Definieren Sie das gemeinsam genutzte Speicherarchiv SANGROUP, indem Sie den Befehl **DEFINE LIBRARY** ausgeben. Sie müssen den im Parameter **PRIMARYLIBMANAGER** angegebenen Namen des Speicherarchivmanager-Servers und LIBTYPE=SHARED verwenden.

   ```
   judy> define library sangroup libtype=shared primarylibmanager=astro
   ```

   Stellen Sie sicher, dass der Speicherarchivname mit dem Speicherarchivnamen auf dem Speicherarchivmanager übereinstimmt.
4. Definieren Sie Pfade vom Speicherarchivmanager ASTRO zu zwei Laufwerken in dem gemeinsam genutzten Speicherarchiv, indem Sie den Befehl **DEFINE PATH** ausgeben.

   AIX
   ```
   astro> define path judy drivea srctype=server desttype=drive
    library=sangroup device=/dev/rmt6
   astro> define path judy driveb srctype=server desttype=drive
    library=sangroup device=/dev/rmt7
   ```

   Linux
   ```
   astro> define path judy drivea srctype=server desttype=drive
    library=sangroup device=/dev/IBMtape6
   astro> define path judy driveb srctype=server desttype=drive
    library=sangroup device=/dev/IBMtape7
   ```
5. Definieren Sie alle Einheitenklassen, die dem gemeinsam genutzten Speicherarchiv zugeordnet sind.

   AIX
   ```
   judy> define devclass tape library=sangroup devtype=lto
   ```

   Linux
   ```
   judy> define devclass tape library=sangroup devtype=lto
   ```

   Die folgenden Parameter für die Einheitenklassendefinition müssen auf dem Speicherarchivclient und dem Speicherarchivmanager übereinstimmen:

   - **LIBRARY**
   - **DRIVEENCRYPTION**
   - **WORM**
   - **FORMAT**
6. Definieren Sie einen Speicherpool mit dem Namen BACKTAPE für die Verwendung durch das gemeinsam genutzte Speicherarchiv. Geben Sie den Befehl **DEFINE STGPOOL** aus.

   ```
   judy> define stgpool backtape tape maxscratch=50
   ```

Nächste Schritte

Wiederholen Sie die Prozedur, um weitere Speicherarchivclients für Ihren Speicherarchivmanager zu definieren.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

DEFINE DRIVE (Laufwerk für ein Speicherarchiv definieren)

DEFINE LIBRARY (Speicherarchiv definieren)

DEFINE PATH (Pfad definieren)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Windows Beispiel: Gemeinsame Speicherarchivnutzung für Windows-Server

Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für Server, die auf Windows-Systemen ausgeführt werden, konfiguriert werden kann.

Informationen zu diesem Vorgang

In diesem Beispiel werden ein Speicherarchivmanager-Server mit dem Namen ASTRO und ein Speicherarchivclient mit dem Namen JUDY konfiguriert.

Definieren Sie für SCSI-Speicherarchive das Speicherarchiv unter Angabe des Parameters **`libtype=scsi`**.

Windows Speicherarchivmanager-Server konfigurieren

Sie müssen den Speicherarchivmanager-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

Vorgehensweise

Die folgende Beispielprozedur zeigt, wie ein IBM Spectrum Protect-Server mit dem Namen ASTRO als Speicherarchivmanager konfiguriert wird:

1. Stellen Sie sicher, dass der Speicherarchivmanager-Server aktiv ist:
   a) Starten Sie die Windows-Diensteverwaltungskonsole (services.msc).
   b) Wählen Sie den Dienst aus, beispielsweise `TSM Server1`.
   c) Wenn der Dienst nicht aktiv ist, klicken Sie mit der rechten Maustaste auf den Namen des Dienstes und wählen Sie **Starten** aus.
2. Rufen Sie die Speicherarchiv- und Laufwerkdaten für die gemeinsam genutzte Speicherarchiveinheit ab:
   a) Führen Sie das Dienstprogramm `tsmdlst.exe` aus. Das Dienstprogramm befindet sich im Verzeichnis `\Programme\Tivoli\TSM\server`.
3. Definieren Sie ein Speicherarchiv mit dem Speicherarchivtyp SCSI.
   Beispiel:

   ```
   define library sangroup libtype=scsi shared=yes
   ```

   In diesem Beispiel wird die Standardeinstellung für die Seriennummer des Speicherarchivs verwendet, gemäß der der Server die Seriennummer vom Speicherarchiv selbst abruft, wenn der Pfad definiert wird. Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.
4. Definieren Sie den Pfad vom Server zum Speicherarchiv.

   ```
   define path astro sangroup srctype=server desttype=library
    device=lb0.0.0.2
   ```

Wenn die Seriennummer beim Definieren des Speicherarchivs nicht eingeschlossen wurde, fragt der Server das Speicherarchiv jetzt ab, um diese Informationen abzurufen. Wenn die Seriennummer beim Definieren des Speicherarchivs eingeschlossen wurde, überprüft der Server die Definition und gibt eine Nachricht aus, wenn eine Übereinstimmung vorliegt.

5. Definieren Sie die Laufwerke im Speicherarchiv.

```
define drive sangroup drivea
define drive sangroup driveb
```

In diesem Beispiel wird die Standardeinstellung für die Seriennummer des Laufwerks verwendet, gemäß der der Server die Seriennummer vom Laufwerk selbst abruft, wenn der Pfad definiert wird. Abhängig vom Leistungsspektrum des Laufwerks kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

In diesem Beispiel wird auch die Standardeinstellung für die Elementadresse des Laufwerks verwendet, gemäß der der Server die Elementnummer vom Laufwerk selbst abruft, wenn der Pfad definiert wird.

Die Elementadresse ist eine Zahl, die die physische Position eines Laufwerks in einem automatisierten Speicherarchiv angibt. Der Server benötigt die Elementadresse, um die physische Position des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Der Server kann die Elementnummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird, oder Sie können die Elementnummer angeben, wenn Sie das Laufwerk definieren.

Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Elementadresse möglicherweise nicht automatisch erkennen. In diesem Fall müssen Sie die Elementadresse angeben, wenn Sie das Laufwerk definieren. Elementnummern für viele Speicherarchive sind unter IBM Support Portal for IBM Spectrum Protect verfügbar.

6. Definieren Sie den Pfad vom Server zu jedem der Laufwerke.

```
define path astro drivea srctype=server desttype=drive library=sangroup
 device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
 device=mt0.2.0.2
```

Wenn die Seriennummer oder Elementadresse beim Definieren des Laufwerks nicht eingeschlossen wurde, fragt der Server das Laufwerk oder Speicherarchiv jetzt ab, um diese Informationen abzurufen.

7. Definieren Sie mindestens eine Einheitenklasse.

```
define devclass tape devtype=dlt library=sangroup
```

8. Stellen Sie den Speicherarchivbestand zurück. Bei dem folgenden Beispiel werden alle Datenträger als Arbeitsdatenträger in den Speicherarchivbestand zurückgestellt. Der Server verwendet den Namen auf dem Barcodeetikett als den Datenträgernamen.

```
checkin libvolume sangroup search=yes status=scratch
 checklabel=barcode
```

9. Konfigurieren Sie einen Speicherpool mit maximal 50 Arbeitsdatenträgern für das gemeinsam genutzte Speicherarchiv.

```
define stgpool backtape tape
 description='Speicherpool für gemeinsam genutztes Speicherarchiv sangroup' maxscratch=50
```

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE DRIVE (Laufwerk für ein Speicherarchiv definieren)
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE PATH (Pfad definieren)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Windows Speicherarchivclient-Server konfigurieren

Sie müssen einen oder mehrere Speicherarchivclient-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

Vorbereitende Schritte

Stellen Sie sicher, dass ein Speicherarchivmanager-Server definiert ist.

Informationen zu diesem Vorgang

Sie müssen den Speicherarchivmanager-Server definieren. Die folgende Beispielprozedur zeigt, wie ein IBM Spectrum Protect-Server mit dem Namen JUDY als Speicherarchivclient konfiguriert wird.

Vorgehensweise

1. Stellen Sie sicher, dass der Speicherarchivmanager-Server aktiv ist:
   a) Starten Sie die Windows-Diensteverwaltungskonsole (services.msc).
   b) Wählen Sie den Dienst aus, beispielsweise TSM `Server1`.
   c) Wenn der Dienst nicht aktiv ist, klicken Sie mit der rechten Maustaste und wählen Sie **Starten** aus.
2. Rufen Sie die Speicherarchiv- und Laufwerkdaten für die gemeinsam genutzte Speicherarchiveinheit ab:
   a) Führen Sie das Dienstprogramm `tsmdlst.exe` aus. Das Dienstprogramm befindet sich im Verzeichnis `\Programme\Tivoli\TSM\server`.
3. Definieren Sie das gemeinsam genutzte Speicherarchiv SANGROUP und geben Sie den Speicherarchivmanager an. Stellen Sie sicher, dass der Speicherarchivname mit dem Speicherarchivnamen auf dem Speicherarchivmanager übereinstimmt.

   ```
   define library sangroup libtype=shared primarylibmanager=astro
   ```

4. Definieren Sie die Pfade vom Speicherarchivclient-Server zu jedem der Laufwerke, indem Sie Befehle auf dem Verwaltungsclient ausgeben:

   ```
   define path judy drivea srctype=server desttype=drive library=sangroup
    device=mt0.1.0.3
    define path judy driveb srctype=server desttype=drive library=sangroup
    device=mt0.2.0.3
   ```

5. Definieren Sie mindestens eine Einheitenklasse, indem Sie Befehle auf dem Speicherarchivclient ausgeben:

   ```
   define devclass tape devtype=dlt mountretention=1 mountwait=10
   library=sangroup
   ```

   Definieren Sie die Parameter für die Einheitenklasse auf dem Speicherarchivclient mit denselben Werten wie auf dem Speicherarchivmanager. Es ist zwar sinnvoll, auf beiden Servern identische Einheitenklassennamen zu verwenden, dies ist jedoch nicht erforderlich.

   Die Einheitenklassenparameter, die auf dem Speicherarchivmanager-Server angegeben sind, überschreiben die für den Speicherarchivclient angegebenen Parameter. Dies gilt unabhängig davon, ob die Einheitenklassennamen auf beiden Servern identisch sind. Wenn die Einheitenklassennamen unterschiedlich sind, verwendet der Speicherarchivmanager die Parameter, die in einer Einheitenklasse angegeben sind, die mit dem für den Speicherarchivclient angegebenen Einheitentyp übereinstimmt.

   Wenn ein Speicherarchivclient eine andere Einstellung als die in der Einheitenklasse des Speicherarchivmanagers angegebene Einstellung (beispielsweise ein anderes Mountlimit) erfordert, führen Sie die folgenden Schritte aus:

a. Erstellen Sie auf dem Speicherarchivmanager-Server eine zusätzliche Einheitenklasse. Geben Sie die Parametereinstellungen an, die der Speicherarchivclient verwenden soll.

b. Erstellen Sie auf dem Speicherarchivclient eine Einheitenklasse mit demselben Namen und Einheitentyp wie die neue Einheitenklasse, die Sie auf dem Speicherarchivserver erstellt haben.

6. Definieren Sie den Speicherpool BACKTAPE, der das gemeinsam genutzte Speicherarchiv verwenden wird:

```
define stgpool backtape tape
description='Speicherpool für gemeinsam genutztes Speicherarchiv sangroup' maxscratch=50
```

7. Wiederholen Sie diese Prozedur, um weitere Server als Speicherarchivclients zu definieren.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

DEFINE LIBRARY (Speicherarchiv definieren)

DEFINE PATH (Pfad definieren)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Speicherpoolhierarchie konfigurieren

Im Rahmen des Implementierungsprozesses müssen Sie eine Speicherpoolhierarchie konfigurieren. Konfigurieren Sie mindestens einen primären Speicherpool auf Platte und einen primären Speicherpool auf Band. Stellen Sie sicher, dass Daten täglich von Platte auf Band umgelagert werden.

Vorbereitende Schritte

1. Stellen Sie sicher, dass Sie die Informationen in „Planung der Speicherpoolhierarchie” auf Seite 21 gelesen haben.
2. Stellen Sie sicher, dass die entsprechenden Regeln, die auch als *Maßnahmen* bezeichnet werden, zum Sichern von Clientdaten angegeben sind. Führen Sie die Anweisungen in „Regeln zum Sichern und Archivieren von Clientdaten angeben” auf Seite 118 aus.
3. Stellen Sie sicher, dass jedem Knoten eine Maßnahme zugeordnet ist. Anweisungen zum Zuordnen einer Maßnahme beim Registrieren eines Knotens finden Sie in „Clients registrieren” auf Seite 123.

Vorgehensweise

Um eine Speicherpoolhierarchie zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Definieren Sie einen primären Speicherpool für die Bandeinheit, indem Sie den Befehl **DEFINE STGPOOL** ausgeben.

   Definieren Sie beispielsweise einen primären Speicherpool mit dem Namen TAPE1 mit der Einheitenklasse LTO und aktivieren Sie die Grupppenkollokation. Legen Sie die maximale Anzahl Arbeitsdatenträger, die der Server für diesen Speicherpool anfordern kann, mit 999 fest. Geben Sie den folgenden Befehl aus:

```
define stgpool tape1 lto pooltype=primary collocate=group
maxscratch=999
```

2. Definieren Sie die Laufwerke, Pfade, und Speicherarchive für den primären Speicherpool auf Band. Führen Sie die Anweisungen in „Bandeinheiten definieren” auf Seite 98 aus.
3. Definieren Sie einen primären Speicherpool für die Platteneinheit, indem Sie den Befehl **DEFINE STGPOOL** ausgeben.

   Definieren Sie beispielsweise einen Speicherpool mit dem Namen DISK1 mit der Einheitenklasse FILE. Stellen Sie sicher, dass Daten in den Bandspeicherpool TAPE1 umgelagert werden können, verhindern

Sie jedoch die automatische Umlagerung, indem Sie 100 für den Parameter **HIGHMIG** und 0 für den Parameter **LOWMIG** angeben. Verhindern Sie die Konsolidierung, indem Sie 100 für den Parameter **RECLAIM** angeben. Aktivieren Sie die Knotenkollokation. Legen Sie die maximale Anzahl Arbeitsdatenträger, die der Server für diesen Speicherpool anfordern kann, mit 9999 fest. Geben Sie mithilfe des Parameters **MIGPROCESS** die Anzahl Umlagerungsprozesse an. Der Wert des Parameters **MIGPROCESS** sollte der Anzahl Laufwerke in dem Speicherarchiv minus der Anzahl Laufwerke, die für Zurückschreibungsoperationen reserviert sind, entsprechen. Geben Sie den folgenden Befehl aus:

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

Weitere Informationen zum Konfigurieren der Umlagerung von Platte auf Band finden Sie in Plattenspeicherpools umlagern.

Nächste Schritte

Eine Speicherpoolhierarchie umfasst nur primäre Speicherpools. Nachdem Sie die Speicherpoolhierarchie konfiguriert haben, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Kopienspeicherpool auf einer Bandeinheit. Anweisungen finden Sie in DEFINE STGPOOL (Kopienspeicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet ist).
2. Sichern Sie den bandbasierten primären Speicherpool im Kopienspeicherpool mithilfe des Befehls **BACKUP STGPOOL**. Anweisungen finden Sie in BACKUP STGPOOL (Daten in primären Speicherpools in einem Kopienspeicherpool sichern).
3. Um sicherzustellen, dass Daten in einem Katastrophenfall wiederhergestellt werden können, definieren Sie eine Prozedur zum Versetzen von Banddatenträgern aus dem Kopienspeicherpool an einen anderen Standort. Anweisungen finden Sie in „Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM” auf Seite 230.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Anwendungen und Systeme schützen

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können.

Clients hinzufügen

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

Informationen zu diesem Vorgang

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

Anwendungsclientknoten

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

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

- IBM Spectrum Protect for Virtual Environments

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

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

Vorgehensweise

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

1. Wählen Sie die Software aus, die auf dem Clientknoten installiert werden soll, und planen Sie die Installation. Führen Sie die Anweisungen in „Client-Software auswählen und Installation planen" auf Seite 116 aus.
2. Geben Sie an, wie Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in „Regeln zum Sichern und Archivieren von Clientdaten angeben" auf Seite 118 aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in „Sicherungs- und Archivierungsoperationen planen" auf Seite 122 aus.
4. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, registrieren Sie den Client. Führen Sie die Anweisungen in „Clients registrieren" auf Seite 123 aus.
5. Um einen Clientknoten zu schützen, installieren und konfigurieren Sie die ausgewählte Software auf dem Clientknoten. Führen Sie die Anweisungen in „Clients installieren und konfigurieren" auf Seite 124 aus.

Client-Software auswählen und Installation planen

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

Informationen zu diesem Vorgang

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

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

Vorgehensweise

Wählen Sie abhängig von Ihrer Zielsetzung die zu installierenden Produkte aus und lesen Sie die Installationsanweisungen.

Tipp: Wenn Sie die Client-Software jetzt installieren, müssen Sie auch die in „Clients installieren und konfigurieren" auf Seite 124 beschriebenen Clientkonfigurationstasks ausführen, bevor Sie den Client verwenden können.

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz eines Dateiservers oder einer Workstation	Der Client für Sichern/Archivieren sichert und archiviert Dateien und Verzeichnisse von Dateiservern und Workstations in Speicher. Es ist auch möglich, Sicherungsversionen und archivierte Kopien von Dateien zurückzuschreiben und abzurufen.	• Clientumgebungsvoraussetzungen • UNIX- und Linux-Clients für Sichern/Archivieren installieren • Erstinstallation des Windows-Clients

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz von Anwendungen mit Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität	IBM Spectrum Protect Snapshot schützt Daten mit integrierter anwendungsgesteuerter Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität. Sie können Daten schützen, die von IBM Db2-Datenbanksoftware sowie SAP-, Oracle-, Microsoft Exchange Server- und Microsoft SQL Server-Anwendungen gespeichert werden.	• Installation und Upgrade für for UNIX and Linux durchführen • Installation und Upgrade für for VMware durchführen • Installation und Upgrade für for Windows durchführen
Schutz einer E-Mail-Anwendung auf einem IBM Domino-Server	IBM Spectrum Protect for Mail: Data Protection for IBM Domino automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass IBM Domino-Server heruntergefahren werden.	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)
Schutz einer E-Mail-Anwendung auf einem Server mit Microsoft Exchange Server	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Server mit Microsoft Exchange Server heruntergefahren werden.	Installation, Upgrade und Migration für durchführen
Schutz einer Db2-Datenbank	Mithilfe der Anwendungsprogrammierschnittstelle (API) des Clients für Sichern/Archivieren können Db2-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer IBM Informix-Datenbank	Mithilfe der API des Clients für Sichern/Archivieren können Informix-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer Microsoft SQL-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server schützt Microsoft SQL-Daten.	Data Protection for SQL Server unter Windows Server Core installieren
Schutz einer Oracle-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Oracle schützt Oracle-Daten.	Installation von Data Protection for Oracle
Schutz einer SAP-Umgebung	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP stellt Schutz bereit, der für SAP-Umgebungen angepasst ist. Das Produkt dient der Verbesserung der Verfügbarkeit von SAP-Datenbankservern und der Verringerung des Verwaltungsaufwands.	• Data Protection for SAP für Db2 installieren • Data Protection for SAP für Oracle installieren

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

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

Regeln zum Sichern und Archivieren von Clientdaten angeben

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

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Maßnahmen, die für Ihre Lösung konfiguriert sind, vertraut sind und wissen, dass für die Maßnahmen keine Änderungen erforderlich sind, fahren Sie mit „Sicherungs- und Archivierungsoperationen planen” auf Seite 122 fort.
- Wenn Sie mit den Maßnahmen nicht vertraut sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

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

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

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

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client

verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme weiter an. Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen definiert werden und ihre Verwendung über Clientoptionen zugeordnet wird.

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

Vorgehensweise

1. Überprüfen Sie die Maßnahmen, die für Ihre Lösung konfiguriert sind, indem Sie die Anweisungen in „Maßnahmen anzeigen" auf Seite 119 ausführen.
2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in „Maßnahmen editieren" auf Seite 120 aus.
3. Optional: Wenn Maßnahmendomänen erstellt oder umfangreiche Änderungen an Maßnahmen durchgeführt werden müssen, um Datenaufbewahrungsanforderungen zu erfüllen, lesen Sie die Informationen in Maßnahmen anpassen.

Maßnahmen anzeigen

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

Vorgehensweise

1. Um die aktive Maßnahmengruppe für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a) Wählen Sie auf der Seite **Services** im Operations Center eine Maßnahmendomäne aus und klicken Sie auf **Details**.
   b) Klicken Sie auf der Seite **Zusammenfassung** für die Maßnahmendomäne auf die Registerkarte **Maßnahmengruppen**.

      Tipp: Um sicherzustellen, dass Sie Daten nach einer Ransomware-Attacke wiederherstellen können, beachten Sie die folgenden Richtlinien:

      - Stellen Sie sicher, das der Wert in der Spalte 'Sicherungen' mindestens 2 beträgt. Der bevorzugte Wert ist 3, 4 oder höher.
      - Stellen Sie sicher, dass der Wert in der Spalte 'Zusätzliche Sicherungen aufbewahren' mindestens 14 Tage beträgt. Der bevorzugte Wert ist 30 Tage oder mehr.
      - Stellen Sie sicher, dass der Wert in der Spalte 'Archivierungen aufbewahren' mindestens 30 Tage beträgt.

      Wenn IBM Spectrum Protect for Space Management-Software auf dem Client installiert ist, stellen Sie sicher, dass diese Daten vor ihrer Umlagerung gesichert werden. Geben Sie im Befehl **DEFINE MGMTCLASS** oder **UPDATE MGMTCLASS MIGREQUIRESBKUP=YES** an. Befolgen Sie dann die Richtlinien im Tipp.
2. Um inaktive Maßnahmengruppen für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a) Klicken Sie auf der Seite **Maßnahmengruppen** auf die Umschaltfläche **Konfigurieren**. Jetzt können Sie die inaktiven Maßnahmengruppen anzeigen und editieren.
   b) Blättern Sie mithilfe der vorwärts und rückwärts gerichteten Pfeile durch die inaktiven Maßnahmengruppen. Wenn Sie eine inaktive Maßnahmengruppe anzeigen, sind die unterschiedlichen Einstellungen für die inaktive und aktive Maßnahmengruppe hervorgehoben.
   c) Klicken Sie auf die Umschaltfläche **Konfigurieren**. Die Maßnahmengruppen sind nicht mehr editierbar.

Maßnahmen editieren

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

Vorbereitende Schritte

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

Informationen zu diesem Vorgang

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

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

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

Vorgehensweise

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

   Die Seite **Maßnahmengruppen** gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche **Konfigurieren**. Die Maßnahmengruppe ist editierbar.
4. Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
5. Editieren Sie die Maßnahmengruppe, indem Sie eine der folgenden Aktionen ausführen:

Option	Bezeichnung
Verwaltungsklasse hinzufügen	a. Klicken Sie in der Tabelle 'Maßnahmengruppen' auf **+ Verwaltungsklasse**. b. Um die Regeln zum Sichern und Archivieren von Daten anzugeben, füllen Sie die Felder im Fenster **Verwaltungsklasse hinzufügen** aus. c. Um die Verwaltungsklasse als Standardverwaltungsklasse festzulegen, wählen Sie das Kontrollkästchen **Als Standardwert definieren** aus. d. Klicken Sie auf **Hinzufügen**.
Verwaltungsklasse löschen	Klicken Sie in der Spalte 'Verwaltungsklasse' auf **-**. **Tipp:** Um die Standardverwaltungsklasse zu löschen, müssen Sie zunächst eine andere Verwaltungsklasse als Standardverwaltungsklasse zuordnen.
Legen Sie eine Verwaltungsklasse als Stan-	Klicken Sie in der Spalte 'Standard' für die Verwaltungsklasse auf das Optionsfeld.

Option	Bezeichnung
dardverwaltungsklasse fest.	**Tipp:** Die Standardverwaltungsklasse verwaltet Clientdateien, wenn einer Datei keine andere Verwaltungsklasse zugeordnet ist oder keine andere Verwaltungsklasse zur Verwaltung geeignet ist. Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl Regeln für das Sichern als auch für das Archivieren von Dateien enthält.
Verwaltungsklasse ändern	Um die Merkmale einer Verwaltungsklasse zu ändern, aktualisieren Sie die Felder in der Tabelle.

6. Klicken Sie auf **Sichern**.

   Achtung: Wenn Sie eine neue Maßnahmengruppe aktivieren, können Daten verloren gehen. Daten, die unter einer Maßnahmengruppe geschützt werden, werden möglicherweise unter einer anderen Maßnahmengruppe nicht geschützt. Daher müssen Sie vor dem Aktivieren einer Maßnahmengruppe sicherstellen, dass die Unterschiede zwischen der vorherigen Maßnahmengruppe und der neuen Maßnahmengruppe keinen Datenverlust zur Folge haben.
7. Klicken Sie auf **Aktivieren**. Es wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt. Stellen Sie sicher, dass die Änderungen in der neuen Maßnahmengruppe mit Ihren Datenaufbewahrungsanforderungen konsistent sind, indem Sie die folgenden Schritte ausführen:
   a) Überprüfen Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der aktiven Maßnahmengruppe gebunden sind, werden in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
   b) Ermitteln Sie Verwaltungsklassen in der aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
   c) Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden sollen, akzeptabel sind, wählen Sie das Kontrollkästchen **Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können** aus und klicken Sie auf **Aktivieren**.

Bereich einer Clientsicherung ändern

Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

Informationen zu diesem Vorgang

Indem Sie nicht benötigte Objekte von Sicherungsoperationen ausschließen, können Sie die Größe des Speicherbereichs, der für Sicherungsoperationen erforderlich ist, und die Speicherkosten besser steuern. Abhängig von Ihrem Lizenzpaket ist es unter Umständen auch möglich, die Lizenzierungskosten zu begrenzen.

Prozedur

Die Vorgehensweise beim Ändern des Bereichs von Sicherungsoperationen ist von dem Produkt abhängig, das auf dem Clientknoten installiert ist:

- Bei einem Client für Sichern/Archivieren können Sie eine Einschluss-/Ausschlussliste erstellen, um eine Datei, Dateigruppen oder Verzeichnisse in Sicherungsoperationen einzuschließen oder von Sicherungsoperationen auszuschließen. Um eine Einschluss-/Ausschlussliste zu erstellen, führen Sie die Anweisungen in Einschluss-/Ausschlussliste erstellen aus.

Um die konsistente Verwendung einer Einschluss-/Ausschlussliste für alle Clients eines bestimmten Typs zu gewährleisten, können Sie auf dem Server eine Clientoptionsgruppe erstellen, die die erforderlichen Optionen enthält. Anschließend ordnen Sie die Clientoptionsgruppe jedem Client desselben Typs zu. Ausführliche Informationen finden Sie in Clientoperationen über Clientoptionsgruppen steuern.

- Für einen Client für Sichern/Archivieren können Sie die Objekte, die in eine Teilsicherungsoperation eingeschlossen werden sollen, mithilfe der Option **domain** angeben. Führen Sie die Anweisungen in Option 'domain' aus.
- Führen Sie für andere Produkte die Anweisungen in der Produktdokumentation aus, um zu definieren, welche Objekte in Sicherungsoperationen eingeschlossen und von Sicherungsoperationen ausgeschlossen werden sollen.

Sicherungs- und Archivierungsoperationen planen

Bevor Sie einen neuen Client beim Server registrieren, müssen Sie sicherstellen, dass ein Zeitplan verfügbar ist, um anzugeben, wann Sicherungs- und Archivierungsoperationen ausgeführt werden. Während des Registrierungsprozesses können Sie dem Client einen Zeitplan zuordnen.

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Zeitplänen, die für die Lösung konfiguriert sind, vertraut sind und für die Zeitpläne keine Änderungen erforderlich sind, fahren Sie mit „Clients registrieren” auf Seite 123 fort.
- Wenn Sie mit den Zeitplänen nicht vertraut sind oder für die Zeitpläne Änderungen erforderlich sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

Normalerweise müssen Sicherungsoperationen für alle Clients täglich ausgeführt werden. Planen Sie Client- und Server-Workloads, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Um die Überschneidung von Client- und Serveroperationen zu verhindern, planen Sie die Ausführung von Clientsicherungs- und -archivierungsoperationen gegebenenfalls für die Nacht. Wenn sich Client- und Serveroperationen überschneiden oder ihnen nicht genügend Zeit und Ressourcen zur Verarbeitung zur Verfügung gestellt werden, können eine Verschlechterung der Systemleistung, fehlgeschlagene Operationen und andere Probleme die Folge sein.

Vorgehensweise

1. Überprüfen Sie die verfügbaren Zeitpläne, indem Sie den Mauszeiger in der Menüleiste des Operations Center über **Clients** bewegen. Klicken Sie auf **Zeitpläne**.
2. Optional: Ändern oder Erstellen Sie einen Zeitplan, indem Sie die folgenden Schritte ausführen:

Option	Bezeichnung
Zeitplan ändern	a. Wählen Sie in der Sicht **Zeitpläne** den Zeitplan aus und klicken Sie auf **Details**. b. Zeigen Sie auf der Seite **Zeitplandetails** Details an, indem Sie auf die blauen Pfeile am Anfang der Zeilen klicken. c. Ändern Sie die Einstellungen im Zeitplan und klicken Sie auf **Sichern**.
Zeitplan erstellen	Klicken Sie in der Sicht **Zeitpläne** auf **+Zeitplan** und führen Sie die Schritte zum Erstellen eines Zeitplans aus.

3. Optional: Verwenden Sie zum Konfigurieren von Zeitplaneinstellungen, die im Operations Center nicht sichtbar sind, einen Serverbefehl. Angenommen, Sie möchten eine Clientoperation planen, mit der ein bestimmtes Verzeichnis gesichert und einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zugeordnet wird.

a) Bewegen Sie auf der Seite **Übersicht** im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf **Command Builder**.

b) Geben Sie zum Erstellen eines Zeitplans den Befehl **DEFINE SCHEDULE** und zum Ändern eines Zeitplans den Befehl **UPDATE SCHEDULE** aus. Weitere Informationen zu den Befehlen finden Sie in DEFINE SCHEDULE (Clientzeitplan definieren) bzw. UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Informationen

Zeitplan für tägliche Operationen optimieren

Clients registrieren

Registrieren Sie einen Client, um sicherzustellen, dass der Client die Verbindung zum Server herstellen und der Server Clientdaten schützen kann.

Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963.

Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

Vorgehensweise

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

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

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

  Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.
- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:

  a. Klicken Sie in der Menüleiste des Operations Center auf **Clients**.

  b. Klicken Sie in der Tabelle 'Clients' auf **+Client**.

  c. Führen Sie die Schritte im Assistenten **Client hinzufügen** aus:

  i) Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen **Aktivieren** aus.

  ii) Kopieren Sie im Fenster **Konfiguration** die Werte für die Optionen **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** und **DEDUPLICATION**.

  Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.

  iii) Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.

  iv) Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.

  v) Klicken Sie auf **Client hinzufügen**.

Zugehörige Informationen
Option 'tcpserveraddress'
Option 'tcpport'
Option 'nodename'
Option 'deduplication'

Clients installieren und konfigurieren

Bevor Sie einen Clientknoten schützen können, müssen Sie die ausgewählte Software installieren und konfigurieren.

Vorgehensweise

Wenn Sie die Software bereits installiert haben, starten Sie mit Schritt „2" auf Seite 125.

1. Führen Sie eine der folgenden Aktionen aus:
   - Um Software auf einem Anwendungs- oder Clientknoten zu installieren, führen Sie die Anweisungen aus.

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	– UNIX- und Linux-Clients für Sichern/Archivieren installieren – Erstinstallation des Windows-Clients **Tipp:** Vorhandene Clients können auch mithilfe des Operations Center aktualisiert werden. Anweisungen finden Sie in Clientaktualisierungen planen.
IBM Spectrum Protect for Databases	– Installation von Data Protection for Oracle – Data Protection for SQL Server unter Windows Server Core installieren
IBM Spectrum Protect for Mail	– Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) – Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) – Installation, Upgrade und Migration für durchführen
IBM Spectrum Protect Snapshot	– Installation und Upgrade für for UNIX and Linux durchführen – Installation und Upgrade für for VMware durchführen – Installation und Upgrade für for Windows durchführen
IBM Spectrum Protect for Enterprise Resource Planning	– Data Protection for SAP für Db2 installieren – Data Protection for SAP für Oracle installieren

   - Um Software auf einem VM-Clientknoten zu installieren, führen Sie die Anweisungen für den ausgewählten Sicherungstyp aus.

Sicherungstyp	Link zu Anweisungen
Wenn Sie planen, VMware-Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie den IBM Spectrum Protect-Client für Sichern/Archivieren.	– UNIX- und Linux-Clients für Sichern/Archivieren installieren – Erstinstallation des Windows-Clients

Sicherungstyp	Link zu Anweisungen
Wenn Sie planen, immer inkrementelle Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren auf demselben Clientknoten oder auf unterschiedlichen Clientknoten.	– Data Protection for VMware **Tipp:** Die Software für IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren sind im IBM Spectrum Protect for Virtual Environments-Installationspaket enthalten.

2. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, fügen Sie die Werte für die Optionen **TCPSERVERADDRESS**, **TCPPORT** und **NODENAME** in der Clientoptionsdatei hinzu oder aktualisieren Sie diese. Verwenden Sie die Werte, die Sie beim Registrieren des Clients notiert haben („Clients registrieren” auf Seite 123).
   - Fügen Sie für Clients, die unter einem AIX-, Linux- oder Mac OS X-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei `dsm.sys` hinzu.
   - Fügen Sie für Clients, die unter einem Windows-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei `dsm.opt` hinzu.

   Standardmäßig befinden sich die Optionsdateien im Installationsverzeichnis.
3. Optional: Wenn ein Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem installiert wurde, installieren Sie den Clientverwaltungsservice auf dem Client. Führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.
4. Konfigurieren Sie den Client für die Ausführung geplanter Operationen. Führen Sie die Anweisungen in „Client für die Ausführung geplanter Operationen konfigurieren” auf Seite 125 aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in „Client/Server-Kommunikation durch eine Firewall konfigurieren” auf Seite 127 aus.
6. Führen Sie eine Testsicherung aus, um sicherzustellen, dass Daten wie geplant geschützt werden.

   Führen Sie beispielsweise für einen Client für Sichern/Archivieren die folgenden Schritte aus:

   a) Wählen Sie auf der Seite **Clients** im Operations Center den Client aus, der gesichert werden soll, und klicken Sie auf **Sichern**.

   b) Überprüfen Sie, ob die Sicherung erfolgreich ausgeführt wird und keine Warnungen oder Fehlernachrichten vorhanden sind.
7. Überwachen Sie die Ergebnisse der geplanten Operationen für den Client im Operations Center.

Nächste Schritte

Wenn geändert werden muss, welche Daten vom Client gesichert werden, führen Sie die Anweisungen in „Bereich einer Clientsicherung ändern” auf Seite 121 aus.

Client für die Ausführung geplanter Operationen konfigurieren

Sie müssen einen Client-Scheduler auf dem Clientknoten konfigurieren und starten. Der Client-Scheduler ermöglicht die Kommunikation zwischen dem Client und dem Server, sodass geplante Operationen erfolgen können. Beispielsweise umfassen geplante Operationen normalerweise das Sichern von Dateien von einem Client.

Informationen zu diesem Vorgang

Die bevorzugte Methode ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert. Der Clientakzeptor verwaltet den Client-Scheduler derart, dass der Scheduler nur in erforderlichen Fällen ausgeführt wird:

- Wenn der Zeitpunkt erreicht ist, an dem der Server nach der nächsten geplanten Operation abgefragt werden soll
- Wenn der Zeitpunkt erreicht ist, an dem die nächste geplante Operation gestartet werden soll

Durch die Verwendung des Clientakzeptors ist es möglich, die Anzahl Hintergrundprozesse auf dem Client zu reduzieren und Probleme in Bezug auf die Speicheraufbewahrungsdauer zu vermeiden.

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

Wenn Ihr Unternehmen standardmäßig ein Zeitplanungstool eines anderen Anbieters verwendet, können Sie statt des Clientakzeptors dieses Zeitplanungstool verwenden. Normalerweise starten Zeitplanungstools anderer Anbieter Clientprogramme direkt mithilfe von Betriebssystembefehlen. Informationen zum Konfigurieren eines Zeitplanungstools eines anderen Anbieters enthält die Produktdokumentation.

Vorgehensweise

Um den Client-Scheduler mithilfe des Clientakzeptors zu konfigurieren und zu starten, führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf **Editieren** > **Clientvorgaben**.
b. Klicken Sie auf die Registerkarte **Web-Client**.
c. Klicken Sie im Feld **Optionen für verwaltete Services** auf **Zeitplan**. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option **Beides**.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option **passwordaccess** auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

```
dsmc query sess
```

f. Starten Sie den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
/usr/bin/dsmcad
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie der Systemstartdatei (normalerweise `/etc/inittab`) den folgenden Eintrag hinzu:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Clientakzeptordämon
```

Linux

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf **Editieren** > **Clientvorgaben**.
b. Klicken Sie auf die Registerkarte **Web-Client**.
c. Klicken Sie im Feld **Optionen für verwaltete Services** auf **Zeitplan**. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option **Beides**.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option **passwordaccess** auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

```
dsmc query sess
```

f. Starten Sie den Clientakzeptor, indem Sie sich mit der Rootbenutzer-ID anmelden und den folgenden Befehl ausgeben:

```
service dsmcad start
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service hinzu, indem Sie in einer Shelleingabeaufforderung den folgenden Befehl ausgeben:

```
# chkconfig --add dsmcad
```

MAC OS X

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf **Editieren** > **Clientvorgaben**.

b. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, klicken Sie auf **Berechtigung**, wählen Sie **Kennwort generieren** aus und klicken Sie auf **Anwenden**.

c. Um anzugeben, wie Services verwaltet werden, klicken Sie auf **Web-Client**, wählen Sie **Zeitplan** aus, klicken Sie auf **Anwenden** und dann auf **OK**.

d. Um sicherzustellen, dass das generierte Kennwort gespeichert wird, starten Sie den Client für Sichern/Archivieren erneut.

e. Starten Sie den Clientakzeptor mithilfe der Anwendung 'IBM Spectrum Protect Tools for Administrators'.

Windows

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf **Dienstprogramme** > **Setup-Assistent** > **Hilfe zum Konfigurieren des Client-Schedulers**. Klicken Sie auf **Weiter**.

b. Lesen Sie die Informationen auf der Seite **Schedulerassistent** und klicken Sie auf **Weiter**.

c. Wählen Sie auf der Seite **Scheduler-Task** die Option **Neuen oder zusätzlichen Scheduler installieren** aus und klicken Sie auf **Weiter**.

d. Geben Sie auf der Seite **Schedulername und -position** einen Namen für den Client-Scheduler an, der hinzugefügt wird. Wählen Sie dann **Scheduler mit Clientakzeptordämon (CAD) verwalten** aus, um den Scheduler zu verwalten, und klicken Sie auf **Weiter**.

e. Geben Sie den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist 'Clientakzeptor'. Klicken Sie auf **Weiter**.

f. Schließen Sie die Konfiguration ab, indem Sie den Assistenten durchlaufen.

g. Aktualisieren Sie die Clientoptionsdatei, `dsm.opt`, und setzen Sie die Option **`passwordaccess`** auf `generate`.

h. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl in der Eingabeaufforderung aus:

```
dsmc query sess
```

Geben Sie auf Anforderung das Clientknotenkennwort ein.

i. Starten Sie den Clientakzeptorservice über die Seite **Systemsteuerung**. Wenn Sie beispielsweise den Standardnamen verwendet haben, starten Sie den Service 'Clientakzeptor'. Starten Sie nicht den Scheduler-Service, den Sie auf der Seite **Schedulername und -position** angegeben haben. Der Scheduler-Service wird wie erforderlich automatisch vom Clientakzeptorservice gestartet und gestoppt.

Client/Server-Kommunikation durch eine Firewall konfigurieren

Wenn ein Client durch eine Firewall mit einem Server kommunizieren muss, müssen Sie die Client/Server-Kommunikation durch die Firewall ermöglichen.

Vorbereitende Schritte

Wenn Sie den Assistenten 'Client hinzufügen' zum Registrieren eines Clients verwendet hatten, bestimmen Sie die Optionswerte in der Clientoptionsdatei, die während dieses Prozesses abgerufen wurden. Sie können die Werte zur Angabe von Ports verwenden.

Informationen zu diesem Vorgang

Achtung: Konfigurieren Sie eine Firewall nicht derart, dass dies eine Beendigung der Sitzungen zur Folge hätte, die von einem Server oder Speicheragenten verwendet werden. Die Beendigung einer gültigen Sitzung kann zu unvorhersehbaren Ergebnissen führen. Prozesse und Sitzungen scheinen unter Umständen aufgrund von Ein-/Ausgabefehlern gestoppt zu werden. Um das Ausschließen von Sitzungen von Zeitlimitbeschränkungen zu erleichtern, konfigurieren Sie bekannte Ports für IBM Spectrum Protect-Komponenten. Stellen Sie sicher, dass die Serveroption **KEEPALIVE** auf den Standardwert YES gesetzt bleibt. Auf diese Art und Weise kann sichergestellt werden, dass die Client/Server-Kommunikation unterbrechungsfrei erfolgt. Anweisungen zum Definieren der Serveroption **KEEPALIVE** finden Sie in KEEPALIVE.

Vorgehensweise

Öffnen Sie die folgenden Ports, um Zugriff durch die Firewall zu ermöglichen:

TCP/IP-Port für den Client für Sichern/Archivieren, den Verwaltungsbefehlszeilenclient und den Client-Scheduler

Geben Sie den Port über die Option **tcpport** in der Clientoptionsdatei an. Die Option **tcpport** in der Clientoptionsdatei muss mit der Option **TCPPORT** in der Serveroptionsdatei übereinstimmen. Der Standardwert ist 1500. Wenn ein anderer Wert als der Standardwert verwendet werden soll, geben Sie eine Zahl zwischen 1024 und 32767 an.

HTTP-Port, um die Kommunikation zwischen dem Web-Client und fernen Workstations zu ermöglichen

Geben Sie den Port für die ferne Workstation an, indem Sie die Option **httpport** in der Clientoptionsdatei der fernen Workstation festlegen. Der Standardwert ist 1581.

TCP/IP-Ports für die ferne Workstation

Der Standardwert von 0 (null) hat zur Folge, dass zwei freie Portnummern der fernen Workstation nach dem Zufallsprinzip zugeordnet werden. Wenn die Portnummern nicht nach dem Zufallsprinzip zugeordnet werden sollen, geben Sie über die Option **webports** in der Clientoptionsdatei der fernen Workstation Werte an.

TCP/IP-Port für Verwaltungssitzungen

Geben Sie den Port an, an dem der Server auf Anforderungen von Verwaltungsclientsitzungen wartet. Der Wert der Clientoption **tcpadminport** muss mit dem Wert der Serveroption **TCPADMINPORT** übereinstimmen. Auf diese Art und Weise können Sie sichere Verwaltungssitzungen in einem privaten Netz gewährleisten.

LAN-unabhängige Datenversetzung konfigurieren

Sie können den Client und Server so konfigurieren, dass der Client seine Daten über einen Speicheragenten direkt in Speicher in einem SAN versetzen kann.

Informationen zu diesem Vorgang

Die LAN-unabhängige Datenversetzung wird vom Produkt IBM Spectrum Protect for SAN bereitgestellt. Weitere Informationen finden Sie in der Dokumentation für IBM Spectrum Protect for SAN.

Vorgehensweise

Um die LAN-unabhängige Datenversetzung zu konfigurieren, führen Sie die folgenden Schritte aus.

1. Überprüfen Sie die Netzverbindung.
2. Richten Sie die Kommunikation zwischen dem Client, dem Speicheragenten und dem Server ein.
3. Installieren und konfigurieren Sie die Software auf Clientsystemen.
4. Konfigurieren Sie Einheiten auf dem Server für den Zugriff durch den Speicheragenten.
5. Konfigurieren Sie IBM Spectrum Protect-Maßnahmen für die LAN-unabhängige Datenversetzung für den Client.
6. Wenn Sie gemeinsam genutzten Speicher des Typs FILE verwenden, installieren und konfigurieren Sie IBM Spectrum Scale.

   Einschränkung: Windows Wenn ein IBM Spectrum Scale-Datenträger von einem AIX-Server formatiert wird, verwendet das Windows-System TCP/IP und nicht das Speicherbereichsnetz für die Übertragung von Daten.
7. Definieren Sie Pfade vom Speicheragenten zu Laufwerken.
8. Starten Sie den Speicheragenten und überprüfen Sie die LAN-unabhängige Konfiguration.

Nächste Schritte

Zur Optimierung Ihrer LAN- und SAN-Ressourcennutzung können Sie den Pfad steuern, über den Datenübertragungen für Clients mit der Fähigkeit zur LAN-unabhängigen Datenversetzung erfolgen. Um den Pfad zu steuern, führen Sie den folgenden Befehl aus aus: **UPDATE NODE**

Für jeden Client können Sie für Lese- und Schreiboperationen für Daten eine der folgenden Einstellungen auswählen. Geben Sie Operationen zum Lesen von Daten mit dem Parameter **DATAREADPATH** und Operationen zum Schreiben von Daten mit dem Parameter **DATAWRITEPATH** an. Der Parameter ist optional. Der Standardwert ist ANY.

LAN (nur LAN-Pfad)
Wenn eine der folgenden Bedingungen erfüllt ist, geben Sie den Wert LAN an:

- Es soll ein kleines Datenvolumen gesichert oder zurückgeschrieben werden.
- Der Client verfügt nicht über SAN-Konnektivität.

LANFREE (nur LAN-unabhängiger Pfad)
Wenn sich der Client und der Server in demselben SAN befinden und eine der folgenden Bedingungen erfüllt ist, geben Sie den Wert LANFREE an:

- Es soll ein großes Datenvolumen gesichert oder zurückgeschrieben werden.
- Die Serververarbeitungslast soll auf den Client verlagert werden.
- Das LAN soll entlastet werden.

ANY (jeder beliebige verfügbare Pfad)
Wenn ein LAN-unabhängiger Pfad verfügbar, wird dieser Pfad verwendet. Wenn kein LAN-unabhängiger Pfad verfügbar ist, werden die Daten über das LAN übertragen.

LAN-unabhängige Konfiguration prüfen

Nach der Konfiguration eines IBM Spectrum Protect-Clients für die LAN-unabhängige Datenversetzung können Sie die Konfiguration und die Serverdefinitionen mithilfe des Befehls **VALIDATE LANFREE** prüfen.

Informationen zu diesem Vorgang

Mit dem Befehl **VALIDATE LANFREE** können Sie bestimmen, welche Ziele für einen Knoten, der einen bestimmten Speicheragenten verwendet, für die LAN-unabhängige Datenversetzung verwendet werden können. Anhand der Befehlsausgabe können Sie außerdem feststellen, ob bei einer vorhandenen LAN-unabhängigen Konfiguration ein Problem vorliegt. Sie können die Maßnahmen-, Speicherpool- und Pfaddefinitionen für einen Knoten und den von diesem Knoten verwendeten Speicheragenten auswerten, um sicherzustellen, dass eine Operation ordnungsgemäß ausgeführt wird.

Prozedur

- Stellen Sie fest, ob ein Clientknoten ein Problem mit der LAN-unabhängigen Konfiguration hat, indem Sie den Befehl **VALIDATE LANFREE** ausgeben. Wenn beispielsweise der Clientknoten mit dem Namen FRED den Speicheragenten FRED_STA verwendet, geben Sie den folgenden Befehl aus:

  ```
  validate lanfree fred fred_sta
  ```

  Mithilfe der Ergebnisse können Sie Anpassungen ermitteln, die unter Umständen in der Speicherkonfiguration oder den Maßnahmen erforderlich sind. In der Ausgabe wird angezeigt, welche Verwaltungsklassenziele für einen bestimmten Operationstyp nicht für LAN-unabhängige Datenübertragungen verwendet werden können. Außerdem wird die Gesamtzahl LAN-unabhängiger Ziele zurückgemeldet.

Zugehörige Informationen

VALIDATE LANFREE (LAN-unabhängige Pfade validieren)

Verschlüsselungsverfahren für Bänder

Die Entscheidung über das zu verwendende Verschlüsselungsverfahren ist davon abhängig, wie Ihre Daten verwaltet werden sollen.

Es ist wichtig, Clientdaten zu schützen, insbesondere dann, wenn diese Daten sensibel sind. Mithilfe von IBM Bandverschlüsselungstechnologie kann sichergestellt werden, dass Daten auf Datenträgern vor Ort und an einem anderen Standort geschützt sind.

Diese Technologie verwendet eine stärkere Verschlüsselungsstufe, indem sie 256-Bit-AES-Verschlüsselungsschlüssel erfordert. Schlüssel werden von einem Schlüsselmanager zum Verschlüsseln und Entschlüsseln von Daten an das Laufwerk übergeben.

IBM Bandtechnologie unterstützt verschiedene Verfahren der Laufwerkverschlüsselung für die folgenden Einheiten:

- IBM 3592 Generation 2 und Generation 3
- IBM Linear Tape-Open Generation 4 und Generation 5

Die Verfahren der Laufwerkverschlüsselung, die Sie mit IBM Spectrum Protect verwenden können, werden auf der Hardwareebene konfiguriert. IBM Spectrum Protect kann nicht steuern oder ändern, welches Verschlüsselungsverfahren in der Hardwarekonfiguration verwendet wird. Wenn die Hardware für das Anwendungsverfahren konfiguriert ist, kann IBM Spectrum Protect die Verschlüsselung abhängig vom Wert für **DRIVEENCRYPTION** für die Einheitenklasse aktivieren oder inaktivieren.

Um alle Daten in einem bestimmten logischen Speicherarchiv zu verschlüsseln oder Daten auf mehr als nur Speicherpooldatenträgern zu verschlüsseln, verwenden Sie die das Speicherarchiv- oder Systemverfahren. Wenn der Verschlüsselungsschlüsselmanager für die gemeinsame Nutzung von Schlüsseln konfiguriert ist, können die Speicherarchiv- und Systemverfahren den Verschlüsselungsschlüssel gemeinsam nutzen, was den gegenseitigen Austausch der beiden Verfahren ermöglicht. IBM Spectrum Protect kann Verschlüsselungsschlüssel zwischen dem Anwendungsverfahren und dem Speicherarchiv- oder dem Systemverschlüsselungsverfahren nicht gemeinsam nutzen oder verwenden.

Tabelle 24. Verschlüsselungsverfahren

Verschlüsselungsverfahren	**Beschreibung**
Anwendungsverschlüsselung	Bei der anwendungsverwalteten Verschlüsselung, können Sie dedizierte Speicherpools erstellen, die nur verschlüsselte Datenträger enthalten. Auf diese Weise können Sie Speicherpoolhierarchien und Maßnahmen verwenden, um zu steuern, wie die Daten verschlüsselt werden. Verschlüsselungsschlüssel werden von der Anwendung verwaltet, in diesem Fall von IBM Spectrum Protect. IBM Spectrum Protect generiert und speichert die Schlüssel in der Serverdatenbank. Daten werden während der Ausführung von Schreiboperationen verschlüsselt, wenn der Verschlüsselungsschlüssel vom Server an das Laufwerk übergeben wird. Daten werden für Leseoperation entschlüsselt. Um Speicherpooldatenträger zu verschlüsseln und einen Teil der Verschlüsselungsverarbeitung auf Ihrem System zu eliminieren, aktivieren Sie das Anwendungsverfahren. Verwenden Sie die anwendungsverwaltete Verschlüsselung nur für Speicherpooldatenträger. Andere Datenträger, wie beispielsweise Bänder mit Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger, werden nicht mithilfe des Anwendungsverfahrens verschlüsselt. **Voraussetzung:** Wenn die Anwendungsverschlüsselung aktiviert ist, müssen Sie beim Schützen von Datenbanksicherungen besonders vorsichtig vorgehen, da die Verschlüsselungsschlüssel zum Verschlüsseln und Entschlüsseln von Daten in der Serverdatenbank gespeichert sind. Um Ihre Daten zurückschreiben zu können, müssen Sie über die korrekte Datenbanksicherung und die zugehörigen Verschlüsselungsschlüssel verfügen, um auf Ihre Informationen zugreifen zu können. Stellen Sie sicher, dass die Datenbank häufig gesichert wird, und schützen Sie die Sicherungen, um Datenverlust oder Diebstahl zu verhindern. Jeder, der sowohl Zugriff auf die Datenbanksicherung als auch auf die Verschlüsselungsschlüssel hat, hat Zugriff auf Ihre Daten.

Tabelle 24. Verschlüsselungsverfahren (Forts.)	
Verschlüsselungsverfahren	**Beschreibung**
Speicherarchivverschlüsselung	Bei der speicherarchivverwalteten Verschlüsselung können Sie steuern, welche Datenträger unter Verwendung ihrer Seriennummern verschlüsselt werden. Sie können einen Bereich oder eine Gruppe von Datenträgern angeben, die verschlüsselt werden sollen. Verschlüsselungsschlüssel werden vom Speicherarchiv verwaltet. Schlüssel sind in einem Verschlüsselungsschlüsselmanager gespeichert und werden dem Laufwerk zur Verfügung gestellt. Wenn Sie die Hardware für die Verwendung der speicherarchivverwalteten Verschlüsselung konfigurieren, können Sie dieses Verfahren verwenden, indem Sie den Befehl **DEFINE DEVCLASS** unter Angabe des Parameters **DRIVEENCRYPTION=ALLOW** ausführen. **Einschränkung:** Die Verschlüsselung mit IBM LTO-4 und späteren Generationen wird nur von bestimmten IBM Speicherarchiven unterstützt. Weitere Informationen finden Sie in „Bandlaufwerkverschlüsselung konfigurieren” auf Seite 132.
Systemverschlüsselung	Die systemverwaltete Verschlüsselung ist nur unter dem Betriebssystem AIX® verfügbar. Verschlüsselungsschlüssel, die dem Laufwerk zur Verfügung gestellt werden, werden vom Einheitentreiber oder Betriebssystem verwaltet und in einem Verschlüsselungsschlüsselmanager gespeichert. Wenn die Hardware für die Verwendung der Systemverschlüsselung konfiguriert ist, können Sie dieses Verfahren verwenden, indem Sie den Befehl **DEFINE DEVCLASS** unter Angabe des Parameters **DRIVEENCRYPTION=ALLOW** ausführen.

Um festzustellen, ob ein Datenträger verschlüsselt ist und welches Verfahren verwendet wurde, führen Sie den Befehl **QUERY VOLUME** unter Angabe des Parameters **FORMAT=DETAILED** aus.

Bandlaufwerkverschlüsselung konfigurieren

Mithilfe der Laufwerkverschlüsselung können Sie Bänder schützen, die kritische oder sensible Daten enthalten, wie beispielsweise Bänder mit vertraulichen Finanzdaten. Die Laufwerkverschlüsselung kann hilfreich sein, wenn Sie Bänder aus der IBM Spectrum Protect-Serverumgebung an einen Standort vor Ort oder an einen anderen Standort versetzen.

Informationen zu diesem Vorgang

Mithilfe der folgenden Tabelle können Sie bestimmen, welche Verschlüsselungsverfahren mit den verschiedenen Laufwerktypen verwendet werden können.

Tabelle 25. Verfügbare Verschlüsselungsverfahren			
	Anwendungsverfahren	**Speicherarchivverfahren**	**Systemverfahren**
3592 Generation 2 und später	Ja	Ja	Ja
HP LTO-4 und später	Ja	Nein	Nein
IBM LTO-4 und später	Ja	Ja, aber nur, wenn Ihre Systemhardware (beispielsweise ein TS3500-Bandarchiv) das Verfahren unterstützt.	Yes
Oracle StorageTek T10000B	Ja	Nein	Nein
Oracle StorageTek T10000C	Ja	Nein	Nein
Oracle StorageTek T10000D	Ja	Nein	Nein

Ein Speicherarchiv kann eine Kombination aus Laufwerken enthalten, von denen einige die Verschlüsselung unterstützen und andere nicht. Beispielsweise könnte ein Speicherarchiv zwei LTO-2-Laufwerke, zwei LTO-3-Laufwerke und zwei LTO-4-Laufwerke enthalten. Sie können Datenträger in einem Speicherarchiv auch mischen, indem Sie beispielsweise verschlüsselte und nicht verschlüsselte Einheitenklassen verwenden, die verschiedene Band- und Laufwerktechnologien haben.

Einschränkungen:

- Um die Verschlüsselung auf LTO-4-Laufwerke oder Laufwerke späterer Generationen anzuwenden, müssen alle Laufwerke die Verschlüsselung unterstützen.
- Um die Verschlüsselung auf ein logisches Speicherarchiv anwenden zu können, müssen Sie für alle Laufwerke in dem Speicherarchiv dasselbe Verschlüsselungsverfahren verwenden. Erstellen Sie keine Umgebung, in der einige Laufwerke das Anwendungsverfahren und einige Laufwerke das Speicherarchiv- oder Systemverfahren als Verschlüsselungsverfahren verwenden.

Weitere Informationen zum Einrichten Ihrer Hardwareumgebung für die Verwendung der Laufwerkverschlüsselung finden Sie in Ihrer Hardwaredokumentation.

Vorgehensweise

1. Installieren Sie einen Einheitentreiber, der die Laufwerkverschlüsselung unterstützt:
   - Um die Verschlüsselung für ein IBM LTO-4-Laufwerk oder ein Laufwerk späterer Generationen zu aktivieren, müssen Sie den IBM RMSS Ultrium-Einheitentreiber installieren. SCSI-Laufwerke unterstützen nicht die Verschlüsselung mit IBM LTO-4 oder später.
   - Um die Verschlüsselung für ein HP LTO-4-Laufwerk oder ein Laufwerk späterer Generationen zu aktivieren, müssen Sie den IBM Spectrum Protect-Einheitentreiber installieren.
2. Aktivieren Sie die Laufwerkverschlüsselung, indem Sie den Parameter **DRIVEENCRYPTION** im Befehl **DEFINE DEVCLASS** oder im Befehl **UPDATE DEVCLASS** für den Einheitentyp 3592, LTO oder ECARTRIDGE angeben.

Nächste Schritte

Bei Verwendung von verschlüsselungsfähigen Laufwerken mit einem unterstützten Verschlüsselungsverfahren wird ein anderes Format verwendet, um verschlüsselte Daten auf Bänder zu schreiben. Wenn Daten auf Datenträger geschrieben werden, die das andere Format verwenden, und die Datenträger dann wieder als Arbeitsdatenträger verwendet werden, enthalten sie Kennsätze, die nur von Laufwerken mit

aktivierter Verschlüsselung gelesen werden können. Um diese Arbeitsdatenträger in einem Laufwerk verwenden zu können, das nicht für die Verschlüsselung aktiviert ist, da die Hardware nicht verschlüsselungsfähig ist oder das Verschlüsselungsverfahren auf NONE gesetzt ist, müssen Sie den Datenträgern neue Kennsätze zuordnen.

Zugehörige Tasks

Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen aktivieren und inaktivieren

Bei IBM Spectrum Protect können Sie die folgenden Typen von Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen verwenden: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

Laufwerkverschlüsselung für LTO-Bandlaufwerke der Generation 4 oder späterer Generationen aktivieren und inaktivieren

IBM Spectrum Protect unterstützt die drei Typen von Laufwerkverschlüsselung, die für LTO-Laufwerke der Generation 4 oder späterer Generationen verfügbar sind: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Bandspeicheroperationen steuern

Einheitenklassendefinitionen für Bänder umfassen Parameter, die Ihnen die Steuerung von Speicheroperationen ermöglichen.

Wie Datenträger von IBM Spectrum Protect gefüllt werden

Der Befehl **DEFINE DEVCLASS** hat einen optionalen Parameter **ESTCAPACITY**, der die geschätzte Kapazität sequenzieller Datenträger angibt, die der Einheitenklasse zugeordnet sind. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent.

Wenn der Parameter **ESTCAPACITY** nicht angegeben wird, verwendet IBM Spectrum Protect einen Standardwert, der auf dem Aufzeichnungsformat basiert, das für die Einheitenklasse unter Verwendung des Parameters **FORMAT** angegeben wird.

Wenn Sie eine geschätzte Kapazität angeben, die die tatsächliche Kapazität des Datenträgers in der Einheitenklasse überschreitet, aktualisiert IBM Spectrum Protect die geschätzte Kapazität des Datenträgers, wenn der Datenträger voll wird. Wenn IBM Spectrum Protect das Ende des Datenträgers erreicht, wird die Kapazität in Übereinstimmung mit dem Datenvolumen, das auf den Datenträger geschrieben wurde, aktualisiert.

Sie können den Standardwert für die geschätzte Kapazität für die Einheitenklasse akzeptieren oder explizit eine geschätzte Kapazität angeben. Ein genauer Wert für die geschätzte Kapazität ist nicht erforderlich, aber nützlich. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent. Unter Umständen möchten Sie die geschätzte Kapazität ändern, wenn eine oder beide der folgenden Bedingungen erfüllt sind:

- Der Standardwert für die geschätzte Kapazität ist aufgrund der Datenkomprimierung ungenau.
- Es sind Datenträger vorhanden, deren Größe vom Standard abweicht.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Geschätzte Kapazität von Banddatenträgern angeben

IBM Spectrum Protect bestimmt anhand der geschätzten Kapazität außerdem, wann die Konsolidierung von Speicherpooldatenträgern beginnen soll.

Informationen zu diesem Vorgang

Bei Bandeinheitenklassen sind die vom Server ausgewählten Standardwerte von dem Aufzeichnungsformat abhängig, mit dem Daten auf den Datenträger geschrieben werden. Sie können entweder den Standardwert für einen Einheitentyp akzeptieren oder einen Wert angeben.

Um die geschätzte Kapazität für Banddatenträger anzugeben, verwenden Sie den Parameter **ESTCAPACITY**, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Aufzeichnungsformate für Banddatenträger angeben

Sie können das Aufzeichnungsformat angeben, das von IBM Spectrum Protect zum Schreiben von Daten auf Banddatenträger verwendet wird. Wenn Sie planen, Generationen von Laufwerken oder unterschiedliche Laufwerktypen in einem Speicherarchiv zu mischen, müssen Sie für jede Laufwerkgeneration und jeden Laufwerktyp ein Aufzeichnungsformat angeben. Auf diese Weise kann der Server zwischen den einzelnen Laufwerkgenerationen und Laufwerktypen unterscheiden.

Informationen zu diesem Vorgang

Um ein Aufzeichnungsformat anzugeben, verwenden Sie den Parameter **FORMAT**, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

Wenn alle Laufwerke, die dieser Einheitenklasse zugeordnet sind, identisch sind, geben Sie **FORMAT=DRIVE** an. Der Server wählt das höchste Format aus, das von dem Laufwerk unterstützt wird, in dem ein Datenträger bereitgestellt wird.

Wenn einige der Laufwerke, die der Einheitenklasse zugeordnet sind, ein Format mit höherer Speicherdichte als andere unterstützen, geben Sie ein Format an, das mit allen Laufwerken kompatibel ist.

Wenn Laufwerke in einem einzelnen SCSI-Speicherarchiv verschiedene Bandtechnologien (beispielsweise DLT und LTO Ultrium) verwenden, geben Sie einen eindeutigen Wert für den Parameter **FORMAT** in jeder Einheitenklassendefinition an.

Ein Konfigurationsbeispiel befindet sich in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren.

Das Aufzeichnungsformat, das der Server für einen Datenträger verwendet, wird ausgewählt, wenn zum ersten Mal Daten auf den Datenträger geschrieben werden. Eine Aktualisierung des Parameters **FORMAT** wirkt sich auf Datenträger, die bereits Daten enthalten, erst dann aus, wenn diese Datenträger ab dem Anfang neu beschrieben werden. Dies kann nach dem Konsolidieren oder Löschen eines Datenträgers oder nach dem Verfall aller Daten auf dem Datenträger der Fall sein.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Speicherarchivobjekte Einheitenklassen zuordnen

Ein Speicherarchiv enthält die Laufwerke, die zum Bereitstellen des Datenträgers verwendet werden können. Einer Einheitenklasse kann nur ein einziges Speicherarchiv zugeordnet werden. Mehrere Einheitenklassen können jedoch dasselbe Speicherarchiv referenzieren.

Informationen zu diesem Vorgang

Um eine Einheitenklasse einem Speicherarchiv zuzuordnen, verwenden Sie den Parameter **LIBRARY** wenn Sie eine Einheitenklasse definieren oder ihre Definition aktualisieren.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Datenträgermountoperationen für Bandeinheiten steuern

Mithilfe von Einheitenklassendefinitionen können Sie die Anzahl bereitgestellter Datenträger, die Zeit, die ein Datenträger bereitgestellt bleibt, und die Zeit, die der IBM Spectrum Protect-Server auf ein verfügbares Laufwerk wartet, steuern.

Anzahl gleichzeitig bereitgestellter Datenträger steuern

Wenn Sie ein Mountlimit für eine Einheitenklasse festlegen, müssen Sie die Anzahl Speichereinheiten berücksichtigen, die mit Ihrem System verbunden sind. Außerdem müssen Sie berücksichtigen, ob die Funktion für gleichzeitiges Schreiben verwendet wird und ob mehrere Einheitenklassen einem einzelnen Speicherarchiv zugeordnet werden; darüber hinaus müssen Sie die Anzahl Prozesse berücksichtigen, die gleichzeitig ausgeführt werden.

Informationen zu diesem Vorgang

Wenn Sie ein Mountlimit für eine Einheitenklasse auswählen, müssen Sie Folgendes berücksichtigen:

- Wie viele Speichereinheiten sind an Ihr System angeschlossen?

  Geben Sie keinen Wert für das Mountlimit an, der größer als die Anzahl zugeordneter, verfügbarer Laufwerke in Ihrer Installation ist. Wenn der Server versucht, die durch das Mountlimit angegebene Anzahl Datenträger bereitzustellen und keine Laufwerke für den erforderlichen Datenträger verfügbar sind, tritt ein Fehler auf und Clientsitzungen werden möglicherweise beendet. (Diese Einschränkung gilt nicht, wenn der Parameter **DRIVES** angegeben wird.)

  Wenn Speicherarchivressourcen in einem SAN von IBM Spectrum Protect-Servern gemeinsam genutzt werden, müssen Sie die Anzahl Bandlaufwerke, die ein Speicherarchivclient gleichzeitig nutzen kann, begrenzen. Um mehreren Speicherarchivclient-Servern die gleichzeitige Verwendung eines Speicherarchivs zu ermöglichen, geben Sie den Parameter **MOUNTLIMIT** an, wenn Sie die Einheitenklasse auf dem Speicherarchivclient definieren oder aktualisieren. Weitere Informationen zum Konfigurieren der gemeinsamen Speicherarchivnutzung finden Sie in „Gemeinsame Speicherarchivnutzung konfigurieren” auf Seite 108.
- Verwenden Sie die Funktion für gleichzeitiges Schreiben für primäre Speicherpools, Kopienspeicherpools und Pools für aktive Daten?

  Geben Sie einen Wert für das Mountlimit an, mit dem genügend Mountpunkte bereitstellt werden, um das gleichzeitige Schreiben von Daten in den primären Speicherpool und in alle zugehörigen Kopienspeicherpools und Pools für aktive Daten zu unterstützen.
- Ordnen Sie mehrere Einheitenklassen einem einzigen Speicherarchiv zu?

  Eine Einheitenklasse, die einem Speicherarchiv zugeordnet ist, kann jedes Laufwerk in dem Speicherarchiv verwenden, das mit dem Einheitentyp der Einheitenklasse kompatibel ist. Da Sie einem Speicherarchiv mehrere Einheitenklassen zuordnen können, kann ein einzelnes Laufwerk im Speicherarchiv von mehreren Einheitenklassen verwendet werden. IBM Spectrum Protect stellt sicher, dass zwei Operationen nicht gleichzeitig dasselbe Laufwerk mit zwei unterschiedliche Einheitenklassen verwenden können.
- Wie viele IBM Spectrum Protect-Prozesse sollen unter Verwendung der Einheiten in dieser Einheitenklasse gleichzeitig ausgeführt werden?

IBM Spectrum Protect bricht einige Prozesse automatisch ab, um andere Prozesse mit höherer Priorität auszuführen. Wenn der Server alle verfügbaren Laufwerke in einer Einheitenklasse zur Ausführung von Prozessen mit höherer Priorität verwendet, müssen Prozesse mit niedriger Priorität warten, bis ein Laufwerk verfügbar wird. IBM Spectrum Protect bricht beispielsweise den Prozess für einen Client ab, der Daten direkt auf Band sichert, wenn das Laufwerk für einen Servermigrations- oder Bandkonsolidierungsprozess benötigt wird. IBM Spectrum Protect bricht einen Bandkonsolidierungsprozess ab, wenn das Laufwerk für eine Clientzurückschreibungsoperation benötigt wird. Weitere Informationen finden Sie in „Operationen zurückstellen” auf Seite 138.

Wenn Prozesse häufig durch andere Prozesse abgebrochen werden, überlegen Sie, ob IBM Spectrum Protect mehr Laufwerke zur Verfügung gestellt werden können. Überprüfen Sie andernfalls die Planung von Operationen, um Laufwerkkonflikte zu reduzieren.

Diese Überlegungen gelten auch für die Funktion für gleichzeitiges Schreiben. Es müssen genügend Laufwerke verfügbar sein, um eine Operation für gleichzeitiges Schreiben erfolgreich ausführen zu können.

Um die maximale Anzahl Datenträger anzugeben, die gleichzeitig bereitgestellt werden können, verwenden Sie den Parameter **MOUNTLIMIT** wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Steuern, wie lange ein Datenträger bereitgestellt bleibt

Sie können steuern, wie lange ein bereitgestellter Datenträger nach seiner letzten E/A-Aktivität bereitgestellt bleiben soll. Wenn ein Datenträger häufig verwendet wird, können Sie die Leistung verbessern, indem Sie einen längeren Mount-Aufbewahrungszeitraum definieren, um unnötige Operationen zum Bereitstellen und Aufheben der Bereitstellung zu vermeiden.

Informationen zu diesem Vorgang

Wenn Mountoperationen durch manuelle Bedieneraktivitäten ausgeführt werden, möchten Sie möglicherweise einen langen Mount-Aufbewahrungszeitraum angeben. Wenn beispielsweise der gesamte Betrieb an einem Wochenende durch nur einen einzigen Bediener unterstützt wird, definieren Sie einen langen Mount-Aufbewahrungszeitraum, damit der Bediener nicht ständig zur Bereitstellung von Datenträgern aufgefordert wird.

Um zu steuern, wie lange ein bereitgestellter Datenträger bereitgestellt bleiben soll, verwenden Sie den Parameter **MOUNTRETENTION**, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren. Wenn der Wert für den Mount-Aufbewahrungszeitraum beispielsweise 60 ist und ein bereitgestellter Datenträger 60 Minuten lang inaktiv ist, wird seine Bereitstellung vom Server aufgehoben.

Solange ein Datenträger für IBM Spectrum Protect bereitgestellt ist, ist das Laufwerk IBM Spectrum Protect zugeordnet und kann nicht anderweitig verwendet werden. Wenn das Laufwerk für andere Verwendungszwecke freigegeben werden muss, können Sie IBM Spectrum Protect-Operationen, die das Laufwerk verwenden, abbrechen und dann die Bereitstellung des Datenträgers aufheben. Sie können beispielsweise Servermigrations- oder -sicherungsoperationen abbrechen. Informationen zum Abbrechen von Prozessen und zum Aufheben der Bereitstellung von Datenträgern finden Sie in „Serveranforderungen für Datenträger verwalten” auf Seite 209.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Zeit steuern, die der Server auf ein Laufwerk wartet

Sie können die Höchstdauer in Minuten angeben, die der IBM Spectrum Protect-Server für die aktuelle Mountanforderung auf ein verfügbares Laufwerk wartet.

Informationen zu diesem Vorgang

Um zu steuern, wie lange gewartet werden soll, bis ein Laufwerk für eine Mountanforderung verfügbar wird, verwenden Sie den Parameter **MOUNTWAIT**, wenn Sie eine Einheitenklasse definieren oder aktualisieren.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Operationen zurückstellen

Der Server kann Server- oder Clientoperationen für eine Operation mit höherer Priorität zurückstellen, wenn ein Mountpunkt im Gebrauch ist und keine anderen Mountpunkte verfügbar sind oder der Zugriff auf einen bestimmten Datenträger erforderlich ist. Wenn eine Operation zurückgestellt wird, wird sie abgebrochen.

Mit dem Befehl **QUERY MOUNT** können Sie den Status des Datenträgers für den Mountpunkt anzeigen.

Standardmäßig ist die Zurückstellung auf dem Server aktiviert. Um die Zurückstellung zu inaktivieren, geben Sie **NOPREEMPT** in der Serveroptionsdatei an. Wenn Sie diese Option angeben, sind der Befehl **BACKUP DB** und die Export- und Importbefehle die einzigen Operationen, durch die andere Operationen zurückgestellt werden können.

Zugehörige Informationen

BACKUP DB (Datenbank sichern)

QUERY MOUNT (Informationen zu bereitgestellten Datenträgern mit sequenziellem Zugriff anzeigen)

Zurückstellung von Operationen für einen Mountpunkt

Wenn eine Operation mit hoher Priorität einen Mountpunkt in einer bestimmten Einheitenklasse erfordert und alle Mountpunkte in der Einheitenklasse im Gebrauch sind, kann ein Mountpunkt einer Operation mit niedrigerer Priorität durch die Operation mit hoher Priorität zurückgestellt werden.

Mountpunkte können nur zurückgestellt werden, wenn die Einheitenklasse der Operation, die die Zurückstellung ausführt, mit der Einheitenklasse der Operation, die zurückgestellt wird, übereinstimmt.

Die folgenden Operationen mit hoher Priorität können eine Zurückstellung anderer Operationen für einen Mountpunkt bewirken.

- Datenbanksicherungsoperationen
- Abruf-, Zurückschreibungs- oder HSM-Rückrufoperationen, die von Clients eingeleitet werden
- Zurückschreibungsoperationen mithilfe einer fernen Einheit zum Versetzen von Daten
- Exportoperationen
- Importoperationen
- Operationen zum Generieren von Sicherungsgruppen

Die folgenden Serveroperationen können keine Zurückstellung anderer Operationen bewirken bzw. nicht durch andere Operationen zurückgestellt werden:

- Prüfen eines Datenträgers
- Zurückschreiben von Daten aus einem Kopienspeicherpool oder einem Pool für aktive Daten
- Vorbereiten einer Wiederherstellungsplandatei
- Speichern von Daten mithilfe einer fernen Einheit zum Versetzen von Daten

Die folgenden Operationen können zurückgestellt werden und sind in der Reihenfolge von der höchsten zur niedrigsten Priorität aufgelistet. Der Server wählt die Operation mit der niedrigsten Priorität, beispielsweise die Identifikation doppelter Daten, für die Zurückstellung aus.

- Replizieren von Knoten

- Sichern von Daten in einem Kopienspeicherpool
- Kopieren aktiver Daten in einen Pool für aktive Daten
- Versetzen von Daten auf einen Speicherpooldatenträger
- Umlagern von Daten von Platte auf sequenzielle Datenträger
- Umlagern von Daten von sequenziellen Datenträgern auf sequenzielle Datenträger
- Sicherungs-, Archivierungs- oder HSM-Umlagerungsoperationen, die von Clients eingeleitet werden
- Konsolidieren von Datenträgern in einem Speicherpool mit sequenziellem Zugriff
- Identifizieren doppelter Daten

Zurückstellung des Datenträgerzugriffs

Wenn eine Operation mit hoher Priorität Zugriff auf einen bestimmten Datenträger erfordert und dieser Datenträger im Gebrauch ist, kann die Operation mit niedrigerer Priorität für diesen Datenträger durch die Operation mit hoher Priorität zurückgestellt werden.

Wenn beispielsweise eine Zurückschreibungsanforderung Zugriff auf einen Datenträger erfordert, der von einer Konsolidierungsoperation verwendet wird, und ein Laufwerk verfügbar ist, wird die Konsolidierungsoperation abgebrochen.

Die folgenden Operationen mit hoher Priorität können eine Zurückstellung von Operationen für den Zugriff auf einen bestimmten Datenträger bewirken:

- Datenbanksicherungsoperationen
- Abruf-, Zurückschreibungs- oder HSM-Rückrufoperationen, die von Clients eingeleitet werden
- Zurückschreibungsoperationen mithilfe einer fernen Einheit zum Versetzen von Daten
- Exportoperationen
- Importoperationen
- Operationen zum Generieren von Sicherungsgruppen

Die folgenden Operationen können keine Zurückstellung anderer Operationen bewirken bzw. nicht durch andere Operationen zurückgestellt werden:

- Prüfen eines Datenträgers
- Zurückschreiben von Daten aus einem Kopienspeicherpool oder einem Pool für aktive Daten
- Vorbereiten eines Wiederherstellungsplans
- Speichern von Daten mithilfe einer fernen Einheit zum Versetzen von Daten

Die folgenden Operationen können zurückgestellt werden und sind in der Reihenfolge von der höchsten zur niedrigsten Priorität aufgelistet. Der Server wählt die Operation mit der niedrigsten Priorität, beispielsweise die Identifikation doppelter Daten, für die Zurückstellung aus.

- Replizieren von Knoten
- Sichern von Daten in einem Kopienspeicherpool
- Kopieren aktiver Daten in einen Pool für aktive Daten
- Versetzen von Daten auf einen Speicherpooldatenträger
- Umlagern von Daten von Platte auf sequenzielle Datenträger
- Umlagern von Daten von sequenziellen Datenträgern auf sequenzielle Datenträger
- Sicherungs-, Archivierungs- oder HSM-Umlagerungsoperationen, die vom Client eingeleitet werden
- Konsolidieren von Datenträgern in einem Speicherpool mit sequenziellem Zugriff
- Identifizieren doppelter Daten

Auswirkungen von Einheitenänderungen im SAN

Die SAN-Umgebung kann sich aufgrund von Änderungen an den Einheiten oder an der Verkabelung dramatisch ändern. Aufgrund der dynamischen Natur des SAN können statische Definitionen fehlschlagen oder unvorhersehbar werden.

Einheiten-IDs, die vom SAN zugeordnet werden und dem Server oder Speicheragenten bekannt sind, können sich aufgrund von Buszurücksetzungen oder aufgrund anderer Umgebungsänderungen ändern. Beispielsweise kann dem Server eine Einheit X auf der Basis der ursprünglichen Pfadspezifikation für den Server und der ursprünglichen Konfiguration des LAN als *rmt0* (unter AIX) bekannt sein. Ein Ereignis im SAN, beispielsweise das Hinzufügen der neuen Einheit Y, führt jedoch dazu, dass der Einheit X die ID *rmt1* zugeordnet wird. Wenn der Server versucht, auf Einheit X unter Verwendung von *rmt0* zuzugreifen, schlägt der Zugriff fehl oder der Zugriff erfolgt auf die falsche Zieleinheit. Der Server versucht, die Wiederherstellung nach Änderungen an Einheiten im SAN durch Verwendung von Seriennummern auszuführen, um die Identität der Einheiten, auf die er zugreift, zu bestätigen.

Wenn Sie ein Laufwerk oder Speicherarchiv definieren, können Sie wahlweise die Seriennummer für diese Einheit angeben. Wenn Sie die Seriennummer bei der Definition der Einheiten nicht angeben, ruft der Server die Seriennummer ab, wenn Sie den Pfad für die Einheit definieren. In beiden Fällen wird die Einheitenseriennummer in der Datenbank des Servers gespeichert und kann zum Bestätigen der Identität einer Einheit für Operationen verwendet werden.

Wenn der Server Laufwerke und Speicherarchive in einem SAN verwendet, versucht der Server zu überprüfen, ob die korrekte Einheit verwendet wird. Der Server kontaktiert die Einheit unter Verwendung des Einheitennamens in dem von Ihnen für die Einheit definierten Pfad. Anschließend fordert der Server die Seriennummer von der Einheit an und vergleicht diese Seriennummer mit der Seriennummer, die für diese Einheit in der Serverdatenbank gespeichert ist.

Wenn die Seriennummern nicht übereinstimmen, startet der Server den Erkennungsprozess im SAN und versucht, die Einheit mit der übereinstimmenden Seriennummer zu finden. Wenn der Server die Einheit mit der übereinstimmenden Seriennummer findet, korrigiert er die Definition des Pfads in der Serverdatenbank, indem er den Einheitennamen in diesem Pfad aktualisiert. Der Server gibt eine Nachricht mit Informationen zu der an der Einheit durchgeführten Änderung aus. Anschließend wird die Einheit vom Server verwendet.

Um festzustellen, wann sich Einheitenänderungen im SAN auf den IBM Spectrum Protect-Server auswirken, können Sie das Aktivitätenprotokoll auf Nachrichten überwachen. Die folgenden Nachrichten betreffen Seriennummern:

- ANR8952 bis ANR8958
- ANR8961 bis ANR8968
- ANR8974 bis ANR8975

Einschränkung: Einige Einheiten können ihre Seriennummern nicht an Anwendungen wie den IBM Spectrum Protect-Server melden. Wenn der Server die Seriennummer einer Einheit nicht abrufen kann, kann der Server das System nicht bei der Wiederherstellung nach der Änderung einer Einheitenposition im SAN unterstützen.

Windows Einheitendaten anzeigen

Mithilfe des Dienstprogramms für Einheitendaten (tsmdlst) können Sie Informationen zu Einheiten anzeigen, die mit dem Server verbunden sind.

Vorbereitende Schritte

- Stellen Sie sicher, dass die HBA-API installiert ist. Die HBA-API ist erforderlich, um das Dienstprogramm für Einheitendaten auszuführen.
- Stellen Sie sicher, dass der Bandeinheitentreiber installiert und konfiguriert ist.

Vorgehensweise

1. Wechseln Sie über eine Eingabeaufforderung in das Unterverzeichnis `server` im Serverinstallationsverzeichnis, beispielsweise `C:\Programme\Tivoli\TSM\server`.
2. Führen Sie die ausführbare Datei `tsmdlst.exe` aus.

Zugehörige Informationen

QUERY SAN (Einheiten im SAN abfragen)

tsmdlst (Informationen zu Einheiten anzeigen)

WORM-Banddatenträger

WORM-Datenträger können als Schutz vor dem versehentlichen oder absichtlichen Löschen kritischer Daten verwendet werden. In IBM Spectrum Protect gibt es jedoch bestimmte Einschränkungen und Richtlinien, die bei der Verwendung von WORM-Datenträgern zu beachten sind.

Die folgenden Typen von WORM-Datenträgern können mit IBM Spectrum Protect verwendet werden:

- IBM 3592, alle unterstützten Generationen
- IBM LTO-3 und alle unterstützten Generationen
- HP LTO-3 und alle unterstützten Generationen
- Quantum LTO-3 und alle unterstützten Generationen
- Quantum SDLT 600, Quantum DLT V4 und Quantum DLT S4
- StorageTek VolSafe
- Sony AIT50 und AIT100

Tipps:

- Ein Speicherpool kann entweder aus WORM-Datenträgern oder aus RW-Datenträgern bestehen, aber nicht aus Datenträgern beider Typen.
- Um die Verschwendung von Bändern nach einer Zurückschreibungs- oder Importoperation zu verhindern, verwenden Sie keine WORM-Bänder für Datenbanksicherungs- oder Exportoperationen.

WORM-fähige Laufwerke

Um WORM-Datenträger in einem Speicherarchiv verwenden zu können, müssen alle Laufwerke in dem Speicherarchiv WORM-fähig sein. Ein Mount schlägt fehl, wenn eine WORM-Kassette in einem Laufwerk mit Schreib-/Lesezugriff (RW-Laufwerk) bereitgestellt wird.

Ein WORM-fähiges Laufwerk kann jedoch als RW-Laufwerk verwendet werden, wenn der Parameter WORM in der Einheitenklasse auf NO gesetzt wird. Jeder Typ von Speicherarchiv kann sowohl über WORM- als auch über RW-Datenträger verfügen, wenn *alle* Laufwerke für WORM aktiviert sind. Die einzige Ausnahme von dieser Regel sind NAS-Speicherarchive, in denen WORM-Banddatenträger nicht verwendet werden können.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

WORM-Datenträger zurückstellen

Der Typ des WORM-Datenträgers legt fest, ob der Datenträgerkennsatz beim Zurückstellen gelesen werden muss.

Speicherarchivwechsler können nicht zwischen standardmäßigen Banddatenträgern mit Schreib-/Lesezugriff (RW-Banddatenträgern) und den folgenden Typen von WORM-Banddatenträgern unterscheiden:

- VolSafe
- Sony AIT

- LTO
- SDLT
- DLT

Um den Typ des WORM-Datenträgers zu bestimmen, der verwendet wird, muss ein Datenträger in ein Laufwerk geladen werden. Daher müssen Sie beim Zurückstellen einer dieser Typen von WORM-Datenträgern die Option CHECKLABEL=YES im Befehl **CHECKIN LIBVOLUME** verwenden.

Wenn Speicherarchivwechsler IBM 3592 Unterstützung für WORM-Datenträger zur Verfügung stellen, können diese Speicherarchivwechsler feststellen, ob ein Datenträger ein WORM-Datenträger ist, ohne den Datenträger in ein Laufwerk laden zu müssen. Die Angabe von CHECKLABEL=YES ist nicht erforderlich. Prüfen Sie mit Ihren Hardwareanbietern, ob Ihre 3592-Laufwerke und -Speicherarchive die erforderliche Unterstützung zur Verfügung stellen.

Zugehörige Informationen
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Einschränkungen für WORM-Datenträger

Sie können keine WORM-Datenträger, denen vorab Kennsätze zugeordnet wurden, mit der Einheitenklasse LTO oder ECARTRIDGE verwenden.

Wenn IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung angegeben ist, können Sie für die folgenden Laufwerke keine WORM-Datenträger verwenden:

- IBM LTO-5, LTO-6 und später
- HP LTO-5, LTO-6 und später
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

Mountfehler bei WORM-Datenträgern

Wenn WORM-Banddatenträger für einen Mount mit einer Einheitenklasse mit Schreib-/Lesezugriff (RW) in ein Laufwerk geladen werden, hat dies einen Mountfehler zur Folge. Dementsprechend hat, wenn RW-Banddatenträger für einen Mount mit einer Einheitenklasse WORM in ein Laufwerk geladen werden, dies ebenfalls das Fehlschlagen des Mounts zur Folge.

WORM-Datenträgern neue Kennsätze zuordnen

Einer WORM-Kassette kann kein neuer Kennsatz zugeordnet werden, wenn sie Daten enthält. Dies gilt für Sony AIT WORM-, LTO WORM-, SDLT WORM-, DLT WORM- und IBM 3592-Kassetten. Der Kennsatz auf einem VolSafe-Datenträger sollte nur einmal überschrieben werden und sollte nur überschrieben werden, wenn der Datenträger keine verwendbaren, gelöschten oder verfallenen Daten enthält.

Geben Sie den Befehl **LABEL LIBVOLUME** nur einmal für VolSafe-Datenträger aus. Um zu verhindern, dass der Kennsatz überschrieben wird, können Sie die Option OVERWRITE=NO im Befehl **LABEL LIBVOLUME** verwenden.

Zugehörige Informationen
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Private WORM-Datenträger aus einem Speicherarchiv entfernen

Wenn Sie eine Aktion für einen WORM-Datenträger ausführen (wenn Sie beispielsweise Dateibereiche löschen) und der Server den Datenträger nicht als voll markiert, wird der Datenträger in den Arbeitsstatus zurückversetzt. Wenn ein WORM-Datenträger nicht als voll markiert wird und aus einem Speicherpool gelöscht wird, bleibt der Datenträger ein privater Datenträger. Um einen privaten WORM-Datenträger aus einem Speicherarchiv zu entfernen, müssen Sie den Befehl **CHECKOUT LIBVOLUME** ausgeben.

Zugehörige Informationen

CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)

Erstellung von DLT WORM-Datenträgern

DLT WORM-Datenträger können aus Datenträgern mit Schreib-/Lesezugriff (RW-Datenträgern) erstellt werden, indem sie konvertiert werden.

Wenn SDLT-600-, DLT-V4- oder DLT-S4-Laufwerke vorhanden sind und diese für WORM-Datenträger aktiviert werden sollen, führen Sie für die Laufwerke unter Verwendung von V30 oder einer späteren Firmware, die von Quantum verfügbar ist, ein Upgrade durch. Sie können auch DLTIce-Software verwenden, um unformatierte RW-Datenträger oder leere Datenträger in WORM-Datenträger zu konvertieren.

In SCSI-Speicherarchiven erstellt der IBM Spectrum Protect-Server automatisch DLT WORM-Arbeitsdatenträger, wenn der Server keine WORM-Arbeitsdatenträger im Bestand eines Speicherarchivs finden kann. Der Server konvertiert verfügbare unformatierte oder leere RW-Arbeitsdatenträger oder leere private RW-Datenträger in WORM-Arbeitsdatenträger. Der Server schreibt auch die Kennsätze auf neu erstellten WORM-Datenträgern neu, indem die Kennsatzinformationen auf den vorhandenen RW-Datenträgern verwendet werden.

Unterstützung für kurze und normale 3592 WORM-Bänder

IBM Spectrum Protect unterstützt sowohl kurze als auch normale 3592 WORM-Bänder. Die besten Ergebnisse werden erzielt, wenn Sie die Bänder in separaten Speicherpools definieren.

Einheitenklasse nach der Einstellung des Parameters WORM abfragen

Sie können die Einstellung des Parameters WORM für eine Einheitenklasse mithilfe des Befehls **QUERY DEVCLASS** bestimmen. Die Ausgabe enthält ein Feld mit der Bezeichnung WORM und einen Wert (YES oder NO).

Zugehörige Informationen

QUERY DEVCLASS (Informationen zu einer oder mehreren Einheitenklassen anzeigen)

Einheitenfehler beheben

Sie können Fehler beheben, die bei der Konfiguration oder Verwendung von Einheiten mit IBM Spectrum Protect auftreten.

Informationen zu diesem Vorgang

Verwenden Sie Tabelle 26 auf Seite 143, um eine Lösung für den einheitenbezogenen Fehler zu finden.

Tabelle 26. Behebung von Einheitenfehlern

Symptom	Problem	Lösung
Konflikte mit anderen Anwendungen	IBM Spectrum Protect erfordert für die gemeinsame Nutzung von Einheiten ein Speicherbereichsnetz.	Konfigurieren Sie ein Speicherbereichsnetz. **Achtung:** Wenn mehrere IBM Spectrum Protect-Server dieselbe Einheit verwenden, kann dies zu einem Datenverlust führen. Definieren oder verwenden Sie eine Einheit nur für einen einzigen IBM Spectrum Protect-Server. Linux AIX Andere Anwendungen können auf IBM Spectrum Protect-Einheiten unter Verwendung eines SCSI-Bandtreibers zugreifen.
Fehlschlagen der Zuordnung von Kennsätzen	Eine Einheit kann nicht zum Zuordnen von Kennsätzen zu Datenträgern verwendet werden, wenn der Server die Einheit gleichzeitig für andere Prozesse verwendet.	Sie können vorhandene Datenträger in einem Speicherpool nicht überschreiben. Sie müssen alle Hardwareprobleme lösen, bevor Sie einem Datenträger einen Kennsatz zuordnen können.

Tabelle 26. Behebung von Einheitenfehlern (Forts.)

Symptom	Problem	Lösung
	Falsche oder unvollständige Lizenzregistrierung	Registrieren Sie die Lizenz für die gekaufte Einheitenunterstützung.
Konflikte zwischen Einheitentreibern	IBM Spectrum Protect gibt Nachrichten zu E/A-Fehlern aus, wenn Sie eine Einheit mit sequenziellem Zugriff definieren oder verwenden.	Windows Bei Windows-Einheitentreibern und von anderen Anwendungen bereitgestellten Treibern können Konflikte mit dem IBM Spectrum Protect-Einheitentreiber auftreten, wenn der IBM Spectrum Protect-Treiber nicht zuerst gestartet wird. Um die Reihenfolge zu überprüfen, in der die Einheitentreiber vom System gestartet werden, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf **Systemsteuerung**. 2. Klicken Sie auf **Geräte**. Einheitentreiber und ihre Starttypen werden aufgelistet.
E/A-Fehler	Wenn Sie versuchen, eine Bandeinheit zu definieren oder zu verwenden, können Konflikte mit Einheitentreibern auftreten. Bei Windows-Einheitentreibern und von anderen Anwendungen bereitgestellten Treibern können Konflikte mit dem IBM Spectrum Protect-Einheitentreiber auftreten, wenn dieser nicht zuerst gestartet wird.	

Linux Präemptive Verarbeitung eines Bandlaufwerkreservierungskonflikts mit persistenter Reserve auf Linux-Plattform nicht möglich	Linux Auf einer Linux-Plattform erfordert der IBM Spectrum Protect-Server oder -Speicheragent die Konfiguration des IBM Einheitentreibers lin_tape für die persistente Reserve und die Erstellung einer IBM Pseudoeinheitendatei `/dev/TSMtape`.	Linux Wenn die Datenpfadübernahme im IBM Treiber lin_tape aktiviert ist, wird die Datei `/dev/TSMtape` automatisch erstellt und die persistente Reserve kann verwendet werden. Es ist auch möglich, die persistente Reserve für die Bandlaufwerkreservierung auf einer Linux-Plattform gemäß der folgenden Prozedur zu konfigurieren:
		Tipp: Standardmäßig verwendet der IBM Einheitentreiber lin_tape die SCSI-2-Reserve für die Reservierung von Bandlaufwerken.
		Linux
		1. Entladen Sie den IBM Einheitentreiber lin_tape.
		2. Fügen Sie in der lin_tape-Konfigurationsdatei `/etc/modprobe.conf` oder `/etc/modprobe.conf.local` (oder `/etc/modprobe.d/lin_tape.conf`, wenn RHEL 6 oder höher ausgeführt wird) die folgende Zeile hinzu:
		`options lin_tape tape_reserve_type=persistent`
		3. Fügen Sie in der Regeldatei `/etc/udev/rules.d/98-lin_tape.rules` die folgende Zeile hinzu:
		`KERNEL=="TSMtape", MODE="0666"`
		4. Laden Sie den IBM Einheitentreiber lin_tape erneut.
		Linux Die IBM Pseudodatei `/dev/TSMtape` wird erstellt und der IBM Spectrum Protect-Server kann die persistente Reserve für die präemptive Verarbeitung der Bandlaufwerkreservierung auf Linux-Plattformen verwenden.

Implementierung abschließen

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

Vorgehensweise

1. Testen Sie Sicherungsoperationen, um sicherzustellen, dass Ihre Daten wie erwartet geschützt werden.
   a) Wählen Sie auf der Seite **Clients** im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf **Sichern**.
   b) Wählen Sie auf der Seite **Server** im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf **Sichern** und führen Sie die Anweisungen im Fenster **Datenbank sichern** aus.
   c) Überprüfen Sie, ob die Sicherungsoperationen erfolgreich ohne Warnungen oder Fehlernachrichten ausgeführt wurden.

      Tipp: Sie können auch stattdessen die GUI des Clients für Sichern/Archivieren zum Sichern von Clientdaten verwenden und die Serverdatenbank sichern, indem Sie den Befehl **BACKUP DB** in einer Verwaltungsbefehlszeile ausgeben.
2. Konfigurieren Sie die Überwachung für Ihre Lösung, indem Sie die Anweisungen in Teil 3, „Bandspeicherlösung überwachen”, auf Seite 147 ausführen.

Teil 3. Bandspeicherlösung überwachen

Überwachen Sie Ihre bandbasierte Lösung, um die korrekte Funktionsweise sicherzustellen.

Informationen zu diesem Vorgang

Überwachen Sie nach der Implementierung Ihrer Bandspeicherlösung mit IBM Spectrum Protect die Lösung täglich und in regelmäßigen Abständen, um vorhandene und potenzielle Probleme zu erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden. Die Überwachung einer Lösung erfolgt bevorzugt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren von E-Mail-Berichten zur Zusammenfassung des Systemstatus konfigurieren.

Vorgehensweise

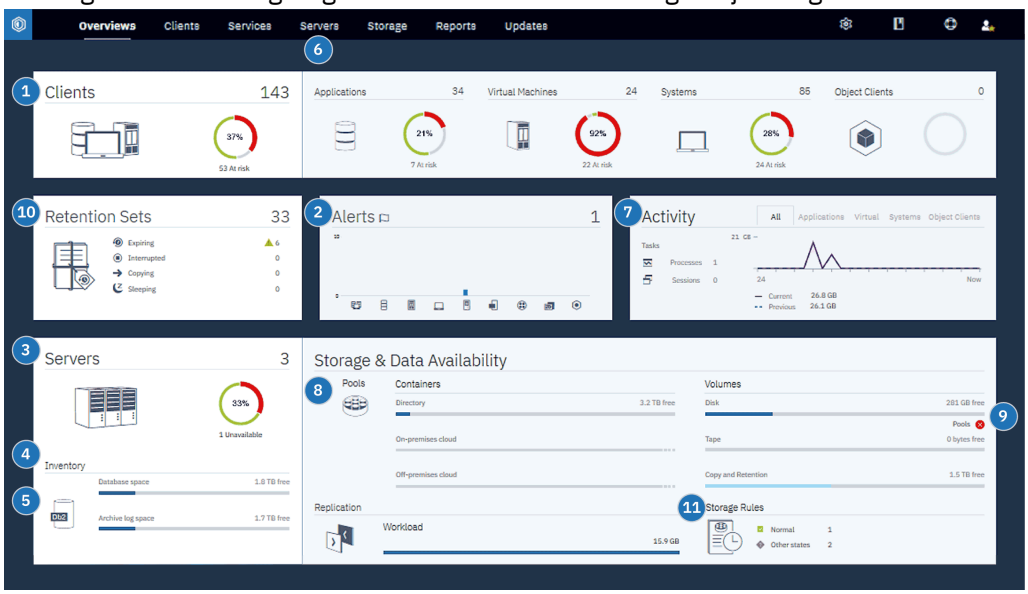
1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Überprüfen Sie, ob Ihr System die Lizenzierungsanforderungen erfüllt. Anweisungen finden Sie in Lizenzeinhaltung überprüfen.
4. Optional: Konfigurieren Sie E-Mail-Berichte des Systemstatus. Anweisungen finden Sie in „Systemstatus mithilfe von E-Mail-Berichten verfolgen” auf Seite 168.

Prüfliste für tägliche Überwachungstasks

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

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

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



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

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

Tabelle 27. Tägliche Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
Achten Sie auf Sicherheitsbenachrichtigungen, die eine Ransomware-Attacke anzeigen können.	Wenn eine potenzielle Ransomware-Attacke in der IBM Spectrum Protect-Umgebung erkannt wird, wird eine Sicherheitsbenachrichtigung im Vordergrund des Operations Center angezeigt. Um weitere Informationen zu erhalten, klicken Sie auf die Benachrichtigung, um die Seite **Sicherheitsbenachrichtigungen** zu öffnen.	Auf der Seite **Sicherheitsbenachrichtigungen** können Sie die folgenden Aktionen ausführen: • Benachrichtigungsdetails nach Client anzeigen. **Einschränkung:** Benachrichtigungen sind nur für Clients für Sichern/Archivieren und IBM Spectrum Protect for Virtual Environments-Clients verfügbar. • Bestätigen Sie eine Sicherheitsbenachrichtigung, indem Sie die Benachrichtigung auswählen und auf **Bestätigen** klicken. Wenn Sie eine Sicherheitsbenachrichtigung bestätigen, wird in der Spalte 'Bestätigt' auf der Seite **Sicherheitsbenachrichtigungen** für den ausgewählten Client ein Häkchen hinzugefügt. Wie eine Benachrichtigung standardmäßig bestätigt wird, wird von Ihrem Unternehmen festgelegt. Ein Häkchen kann bedeuten, dass das Problem untersucht wurde und festgestellt wurde, dass es falsch-positiv ist. Es kann auch bedeuten, dass ein Problem vorhanden ist und behoben wird. • Ordnen Sie eine Sicherheitsbenachrichtigung einem Administrator zu, indem Sie die Sicherheitsbenachrichtigung auswählen und auf **Zuordnen** klicken. Um die Zuordnung anzuzeigen, muss sich der Administrator beim Operations Center anmelden und auf **Übersichten** > **Sicherheit** klicken. Wenn Sie nicht sicher sind, ob der Administrator die Seite **Sicherheitsbenachrichtigungen** regelmäßig überwacht, benachrichtigen Sie den Administrator über die Zuordnung. • Wenn die Benachrichtigung eine 'falsch-positiv'-Benachrichtigung ist, können Sie die Sicherheitsbenachrichtigung auswählen und auf **Zurücksetzen** klicken. Die Sicherheitsbenachrichtigung wird gelöscht. Protokolldaten, die für Baselinevergleiche mit der neuesten Sicherungsoperation verwendet werden, werden gelöscht. Im weiteren Verlauf werden neue Vergleichsdaten berechnet. • Wahlweise können Sie die Sicherheitsbenachrichtigungen mithilfe des Befehls **SET SECURITYNOTIF** inaktivieren.

Tabelle 27. Tägliche Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
1 Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.	Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis **Gefährdet**. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'. **Achtung:** Wenn der Prozentsatz für **Gefährdet** sehr viel höher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Eine Ransomware-Attacke kann das Fehlschlagen von Sicherungsoperationen zur Folge haben und somit Clients in den Status 'Gefährdet' versetzen. Wenn beispielsweise der Prozentsatz gefährdeter Clients normalerweise zwischen 5 % und 10 % liegt, sich aber auf 40 % oder 50 % erhöht, ermitteln Sie die Ursache. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen: 1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf **Details**. 2. Um ein Problem zu diagnostizieren, klicken Sie auf **Diagnose**.	Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.
2 Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedienereingriff erfordern.	Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.	Um weitere Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Alerts'. 2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus. 3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. Im Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.
3 Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.	1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis **Nicht verfügbar**. 2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'. 3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf **Details**.	**Tipp:** Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale: 1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf **Details**. 2. Um die Servermerkmale zu aktualisieren, klicken Sie auf **Merkmale**.

Tabelle 27. Tägliche Überwachungstasks (Forts.)

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

Tabelle 27. Tägliche Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
5 Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.	Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Server'. 2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.	Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus: 1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf **Details**. 2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen. Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten: 1. Klicken Sie auf der Seite **Übersicht** im Operations Center auf den Bereich 'Server'. 2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf **Sichern**. Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus: 1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf **Command Builder**. 2. Geben Sie den Befehl **QUERY DB** aus: `query db f=d` 3. Überprüfen Sie in der Ausgabe das Feld `Einheitenklassenname für Gesamtsicherungen`. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.

Tabelle 27. Tägliche Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
6 Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.	Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf **Server** > **Verwaltung**. 2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an. 3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.	Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.
7 Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.	• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an. • Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.	• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datendeduplizierung nicht ordnungsgemäß. **Achtung:** Wenn das Volumen gesicherter Daten deutlich umfangreicher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Wenn Daten durch Ransomware verschlüsselt werden, werden die Daten vom System als geändert wahrgenommen und die geänderten Daten werden gesichert. Demzufolge wird das Volumen gesicherter Daten umfangreicher. Um die betroffenen Clients zu bestimmen, klicken Sie auf die Registerkarte **Anwendungen**, **Virtuelle Maschinen** oder **Systeme**. • Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.

Tabelle 27. Tägliche Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
8 Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.	1. Wenn im Bereich 'Speicher & Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf **Pools**, um die Details anzuzeigen: • Wenn der Status **Kritisch** angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar). **Achtung:** Wenn der Status kritisch ist, ermitteln Sie die Ursache: – Wenn die Datendeduplizierungsrate für einen Speicherpool deutlich fällt, kann dies eine Ransomware-Attacke anzeigen. Während einer Ransomware-Attacke werden Daten verschlüsselt und können nicht dedupliziert werden. Um die Datendeduplizierungsrate zu verifizieren, überprüfen Sie in der Tabelle 'Speicherpools' den Wert in der Spalte 'Einsparungen in %'. – Wenn ein Speicherpool wider Erwarten zu 100 % ausgelastet ist, kann dies eine Ransomware-Attacke anzeigen. Um die Auslastung zu verifizieren, überprüfen Sie den Wert in der Spalte 'Verwendete Kapazität'. Bewegen Sie den Mauszeiger über die Werte, um den Prozentsatz für den verwendeten Speicherbereich und den Prozentsatz für den freien Speicherbereich anzuzeigen. • Wenn der Status **Warnung** angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff). 2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.	Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf **Details**.

Tabelle 27. Tägliche Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.	Überprüfen Sie im Bereich 'Speicher & Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben **Einheiten** angegeben ist. Wenn der Status **Kritisch** ⊗ oder **Warnung** ⚠ für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf **Einheiten**.	Bandeinheiten können den Status 'Warnung' oder 'Kritisch' haben, wenn Laufwerke nicht verfügbar sind. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. Eine Bandeinheit kann auch den Status 'Kritisch' haben, wenn das Speicherarchiv offline ist. In anderen Spalten der Tabelle 'Bandeinheiten' wird der Status der automatischen Einheiten im Speicherarchivs, der Laufwerke und der Pfade angezeigt. Um Probleme mit Bandlaufwerken zu beheben, die einen kritischen Status haben, können Sie das Laufwerk offline schalten, wenn es für eine andere Aktivität, wie beispielsweise Wartung, verwendet werden muss. Um ein Laufwerk offline zu schalten, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite **Speicher** im Operations Center Bandeinheiten aus. 2. Um weitere Informationen zu einem Bandarchiv anzuzeigen, wählen Sie eine Zeile aus und klicken Sie auf **Details**. 3. Um ein Laufwerk offline zu schalten, wählen Sie das Bandlaufwerk aus und klicken Sie auf **Offline**. Stellen Sie bei Bandsicherungsoperationen sicher, dass genügend Arbeitsbänder verfügbar sind. Wenn Sie sich nicht sicher sind, ob die Anzahl verfügbarer Arbeitsbänder ausreichend ist, öffnen Sie das Notizbuch 'Details', um die Bandnutzung sowie eine Schätzung der Verfügbarkeit von Arbeitsbändern anzuzeigen. Um das Notizbuch 'Details' zu öffnen, wählen Sie in der Tabelle ein Speicherarchiv aus und klicken Sie auf 'Details'.

Tabelle 27. Tägliche Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
10 Überwachen Sie Aufbewahrungsgruppen.	Um den Gesamtstatus der Aufbewahrungsgruppen abzurufen, zeigen Sie den Bereich **Aufbewahrungsgruppen** auf der Seite **Übersicht** im Operations Center an: • Das Feld **Abgeschlossen** gibt die Anzahl Aufbewahrungsgruppen an, die in der Serverdatenbank erstellt wurden und im Serverbestand verfolgt werden. • Das Feld **Verfallen** gibt die Anzahl Aufbewahrungsgruppen an, deren Daten verfallen sind. • Das Feld **Gelöscht** gibt die Anzahl Aufbewahrungsgruppen an, die gelöscht wurden. Um Aufbewahrungsregeln anzuzeigen oder zu ändern, klicken Sie auf **Services** > **Aufbewahrungsregeln**.	Um weitere Informationen zu Aufbewahrungsgruppen zu erhalten, klicken Sie auf den Bereich **Aufbewahrungsgruppen**, um die Seite **Aufbewahrungsgruppen** zu öffnen. Um Merkmale von Aufbewahrungsgruppen anzuzeigen oder zu ändern, doppelklicken Sie auf eine Aufbewahrungsgruppe. Um weitere detaillierte Informationen zu erhalten, können Sie zugehörige Befehle ausführen: 1. Bewegen Sie auf der Seite **Übersicht** im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf **Command Builder**. 2. Um zu bestimmen, welche Jobs zur Erstellung von Aufbewahrungsgruppen aktiv, unterbrochen oder abgeschlossen sind, führen Sie den Befehl **QUERY JOB** aus. Anweisungen finden Sie in QUERY JOB (Job abfragen). 3. Um Aufbewahrungsregeln abzufragen, führen Sie den Befehl **QUERY RETRULE** aus. Anweisungen finden Sie in QUERY RETRULE (Aufbewahrungsregel abfragen). 4. Um Aufbewahrungsgruppen abzufragen, führen Sie den Befehl **QUERY RETSET** aus. Anweisungen finden Sie in QUERY RETSET (Aufbewahrungsgruppe abfragen). 5. Um den Inhalt einer Aufbewahrungsgruppe abzufragen, führen Sie den Befehl **QUERY RETSETCONTENTS** aus. Anweisungen finden Sie in QUERY RETSETCONTENTS (Inhalt einer Aufbewahrungsgruppe abfragen).

Tabelle 27. Tägliche Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
11 Überwachen Sie Speicherregeln.	Um den Gesamtstatus der Speicherregeloperationen abzurufen, zeigen Sie den Bereich **Speicherregeln** auf der Seite **Übersicht** im Operations Center an.	In der Statuszusammenfassung werden die neuesten Verarbeitungsergebnisse für Speicherregeln angezeigt. Die Anzahl Speicherregeln in jedem der folgenden Status wird angezeigt: **Normal** Die Anzahl Speicherregeln, die ohne Fehler ausgeführt wurden. **Warnung** Die Anzahl Speicherregeln, deren Verarbeitung abgeschlossen wurde, mit denen aber nicht alle auswählbaren Daten versetzt oder kopiert wurden. Entweder wurden einige Dateien übersprungen, das Zeitlimit der Regel wurde erreicht oder der Prozess wurde abgebrochen. **Fehlgeschlagen** Die Anzahl Speicherregeln, deren Verarbeitung nicht abgeschlossen wurde. Beispielsweise kann die Verarbeitung von Daten durch den Server fehlgeschlagen, da im Zielspeicherpool nicht genügend Speicherbereich verfügbar ist oder der Server nicht auf den Speicherpool zugreifen kann. **Andere Status** Die Anzahl Speicherregeln in anderen Status. Möglicherweise kann der Server, auf dem die Speicherregel definiert ist, die Daten nicht bereitstellen oder auf dem Server wird eine frühere Version von IBM Spectrum Protect ausgeführt, die den Status nicht unterstützt. Der Status ist möglicherweise nicht gültig, da die Speicherregel nicht aktiviert oder nicht ausgeführt wurde. **Tipps:** • Ein Symbol wird nur angezeigt, wenn eine oder mehrere Speicherregeln im entsprechenden Status vorhanden sind. Um detaillierte Informationen zu der jeweiligen Speicherregel anzuzeigen, klicken Sie auf **Speicherregeln**, um die Seite **Speicherregeln** zu öffnen. • Um zu bestimmen, welche Speicherregeljobs aktiv oder abgeschlossen sind, führen Sie den Befehl **QUERY JOB** aus. Anweisungen finden Sie in QUERY JOB (Job abfragen).

Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Operationen korrekt ausgeführt werden, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.

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

Tabelle 28. Regelmäßige Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie die Systemleistung.	Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum: 1. Klicken Sie auf der Seite **Übersicht** im Operations Center auf **Clients**. Suchen Sie den Server, der dem Client zugeordnet ist. 2. Klicken Sie auf **Server**. Wählen Sie den Server aus und klicken Sie auf **Details**. 3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossenen wurden, klicken Sie auf **Abgeschlossene Tasks**. 4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl **QUERY ACTLOG**. Informationen zu diesem Befehl finden Sie in QUERY ACTLOG (Aktivitätenprotokoll abfragen). 5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen: 1. Klicken Sie auf der Seite **Übersicht** im Operations Center auf **Clients**. 2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf **Details**. 3. Um Clientprotokolle abzurufen, klicken Sie auf **Diagnose**.	Begrenzen Sie die Zeit für Clientsicherungsoperationen auf 8 bis 12 Stunden. Stellen Sie sicher, dass sich Clientzeitpläne nicht mit Serververwaltungstasks überschneiden. Anweisungen zur Reduzierung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen. Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren. Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.

Tabelle 28. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

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

Tabelle 28. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Bestimmen Sie, ob im Verzeichnis für die Serverinstanz genügend Speicherbereich verfügbar ist.	Stellen Sie sicher, dass im Verzeichnis für die Serverinstanz mindestens 50 GB freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:
	• AIX Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -g Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Linux Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -h Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Windows Klicken Sie in Windows Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf **Eigenschaften**. Zeigen Sie die Kapazitätsdaten an.
	Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:
	• Linux AIX `/home/tsminst1/tsminst1`
	• Windows `C:\tsminst1`
	Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.	

Tabelle 28. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Ermitteln Sie nicht erwartete Clientaktivität.	Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf der Seite **Übersicht** im Operations Center auf den Bereich 'Clients'. 2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client. 3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte **Merkmale**. 4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.	Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich **Aktivität im Lauf von 2 Wochen** das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde. Überprüfen Sie in regelmäßigen Abständen die SQL-Aktivitätsübersichtstabelle, die statistische Daten zu Clientsitzungen enthält. Um die aktuelle Aktivität mit der vorherigen Aktivität zu vergleichen, verwenden Sie eine Anweisung SQL SELECT. Wenn der Grad an Aktivität sich deutlich von dem für die vorherige Aktivität unterscheidet, kann dies eine Ransomware-Attacke anzeigen. Überprüfen Sie das Aktivitätenprotokoll in regelmäßigen Abständen. Suchen Sie nach ANE-Nachrichten, die angeben, wie viele Dateien gesichert und überprüft wurden. Vergleichen Sie die aktuellen Datendeduplizierungsraten mit den vorherigen Raten. Wenn eine ungewöhnlich hohe Anzahl Dateien gesichert wurde oder die Datendeduplizierungsrate wider Erwarten auf 0 fällt, kann dies eine Ransomware-Attacke anzeigen.

Tabelle 28. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.	1. Klicken Sie auf der Seite **Übersicht** im Operations Center auf den Bereich 'Pools'. 2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf **Details**.	**Tipps:** • Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite **Speicherpools** im Operations Center den Speicherpool aus. 2. Klicken Sie auf **Details** > **Merkmale**. 3. Geben Sie im Feld `Verzögerungszeitraum für Containerwiederverwendung` den Zeitraum an. • Bestimmen Sie die Datendeduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls **GENERATE DEDUPSTATS**. • Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite **Speicherpools** im Operations Center den Speicherpool aus. 2. Klicken Sie auf **Details** > **Merkmale**. Verwenden Sie dementsprechend den Befehl **QUERY EXTENTUPDATES**, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs, der im Containerspeicherpool verfügbar ist.

Tabelle 28. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
		• Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Datendeduplizierungseinsparungen belegt wird, verwenden Sie den Befehl **`select * from occupancy`**. Die Befehlsausgabe umfasst den Wert für LOGICAL_MB. LOGICAL_MB gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.
Überwachen und verwalten Sie Bandeinheiten.	Überwachen Sie Ihre Umgebung auf Hardwarefehler auf Bandlaufwerken und in Bandarchiven. Anweisungen finden Sie in „Bandalertnachrichten auf Hardwarefehler überwachen" auf Seite 165. Überwachen Sie die Datenträgerkompatibilität, um Fehler auf Bandlaufwerken zu verhindern. Anweisungen finden Sie in „Durch Datenträgerinkompatibilität verursachte Fehler verhindern" auf Seite 166. Überwachen Sie Reinigungsnachrichten für Bandlaufwerke. Anweisungen finden Sie in „Operationen mit Reinigungskassetten" auf Seite 166.	
Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass sich die Start- und Endzeiten von Clientzeitplänen nicht mit denen von Serververwaltungstasks überschneiden. Begrenzen Sie die Zeit für Clientsicherungsoperationen auf 8 bis 12 Stunden.	Klicken Sie auf der Seite **Übersicht** im Operations Center auf **Clients** > **Zeitpläne**. In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	**Tipp:** Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über **Clients** und klicken Sie auf **Zeitpläne**. 2. Wählen Sie einen Zeitplan aus und klicken Sie auf **Details**. 3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken. 4. Geben Sie im Feld **Ausführungszeitalert** die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird. 5. Klicken Sie auf **Sichern**.

Tabelle 28. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass sich die Start- und Endzeiten von Verwaltungstasks nicht mit denen von Clientzeitplänen überschneiden.	Klicken Sie auf der Seite **Übersicht** im Operations Center auf **Server** > **Verwaltung**. Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Bei der bevorzugten Methode wird sichergestellt, dass jede Verwaltungstask bis zum Abschluss ausgeführt wird, bevor die nächste Verwaltungstask gestartet wird. Beispiele für Verwaltungstasks umfassen Bestandsverfall, Kopieren von Speicherpools, Speicherbereichskonsolidierung und Datenbanksicherung. **Tipp:** Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite **Übersicht** im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf **Command Builder**. 2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl **UPDATE SCHEDULE** aus. Informationen zu diesem Befehl finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Informationen

QUERY ACTLOG (Aktivitätenprotokoll abfragen)

Bandalertnachrichten auf Hardwarefehler überwachen

Bandalertnachrichten werden von Band- und Speicherarchiveinheiten generiert, um Hardwarefehler zurückzumelden. Diese Nachrichten unterstützen Sie bei der Bestimmung von Fehlern, die sich nicht auf den Server beziehen.

Informationen zu diesem Vorgang

Es wird eine Protokollseite erstellt, die jederzeit oder zu einem bestimmten Zeitpunkt, beispielsweise wenn ein Laufwerk abgehängt wird, abgerufen werden kann.

Eine Bandalertnachricht kann eine der folgenden Bewertungsstufen haben:

- Information (beispielsweise wird versucht, einen nicht unterstützten Kassettentyp einzulegen)
- Warnung (beispielsweise wird ein Hardwarefehler vorhergesagt)
- Kritisch (beispielsweise liegt ein Bandfehler vor und Ihre Daten sind gefährdet)

Bandalertnachrichten sind standardmäßig inaktiviert.

Prozedur

- Um Bandalertnachrichten zu aktivieren, geben Sie den Befehl **SET TAPEALERTMSG** unter Angabe des Werts **ON** aus: `set tapealertmsg on`
- Um zu überprüfen, ob Bandalertnachrichten aktiviert sind, geben Sie den Befehl **QUERY TAPEALERTMSG** aus: `query tapealertmsg`

Durch Datenträgerinkompatibilität verursachte Fehler verhindern

Indem Datenträgerkompatibilitätsprobleme überwacht und behoben werden, können Sie Fehler in einer bandbasierten Lösung verhindern. Ein neues Laufwerk hat möglicherweise nur eingeschränkt die Fähigkeit zur Verwendung der von einer vorherigen Version des Laufwerks unterstützten Datenträgerformate. Häufig kann ein neues Laufwerk Daten mit dem vorherigen Datenträgerformat lesen, aber nicht schreiben.

Informationen zu diesem Vorgang

Standardmäßig verbleiben vorhandene Datenträger mit dem Status `FILLING` nach einem Laufwerkupgrade in diesem Status. In einigen Fällen möchten Sie vielleicht ein älteres Laufwerk weiterhin nutzen, um diese Datenträger mit Daten zu füllen. Dadurch bleibt die Schreib-/Lesefunktionalität für die vorhandenen Datenträger erhalten, bis sie konsolidiert werden. Wenn für alle Laufwerke in einem Speicherarchiv ein Upgrade durchgeführt werden soll, stellen Sie sicher, dass die Datenträgerformate von der neuen Hardware unterstützt werden. Wenn nicht ausschließlich die neuesten Datenträger mit dem neuen Laufwerk verwendet werden sollen, müssen Sie sich aller Kompatibilitätsprobleme bewusst sein. Anweisungen zum Umlagern von Daten finden Sie in „Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde" auf Seite 222.

Um ein neues Laufwerk mit Datenträgern zu verwenden, von denen Daten gelesen, auf die aber keine Daten geschrieben werden können, geben Sie den Befehl **UPDATE VOLUME** aus, um Lesezugriff für diese Datenträger festzulegen. Damit wird verhindert, dass durch Schreib-/Leseinkompatibilität Fehler auftreten. Beispielsweise kann ein neues Laufwerk unter Umständen Datenträger, auf die Daten in einem von dem Laufwerk nicht unterstützten Format geschrieben wurden, ausgeben, sobald die Datenträger in das Laufwerk geladen werden. Es kann auch vorkommen, dass ein neues Laufwerk den ersten Schreibbefehl nicht für einen Datenträger ausführt, der teilweise in einem Format beschrieben ist, das von dem Laufwerk nicht unterstützt wird.

Wenn Daten auf dem Datenträger mit Lesezugriff verfallen und der Datenträger konsolidiert wird, ersetzen Sie ihn durch einen Datenträger, der mit dem neuen Laufwerk vollständig kompatibel ist. Fehler können generiert werden, wenn ein neues Laufwerk einen in einem älteren Format beschriebenen Datenträger nicht korrekt kalibrieren kann. Um dieses Problem zu verhindern, stellen Sie sicher, dass das ursprüngliche Laufwerk voll funktionsfähig ist und über aktuelle Mikrocodeversionen verfügt.

Operationen mit Reinigungskassetten

Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

Reinigungsprozess überwachen

Wenn eine Reinigungskassette in ein Speicherarchiv zurückgestellt wird und ein Laufwerk gereinigt werden muss, hebt der Server die Bereitstellung des Datenträgers auf und führt die Reinigungsoperation aus. Wenn die Reinigungsoperation fehlschlägt oder wenn sie abgebrochen wird oder wenn keine Reinigungskassette verfügbar ist, sind Sie sich der Tatsache, dass das Laufwerk gereinigt werden muss, möglicherweise nicht bewusst. Überwachen Sie Reinigungsnachrichten auf diese Probleme, um sicherzustellen, dass Laufwerke wie erforderlich gereinigt werden. Geben Sie, falls erforderlich, den Befehl **CLEAN DRIVE** aus, damit der Server den Reinigungsversuch wiederholt, oder laden Sie manuell eine Reinigungskassette in das Laufwerk.

Mehrere Reinigungskassetten verwenden

Der Server verwendet eine Reinigungskassette für die Anzahl Reinigungen, die Sie beim Zurückstellen der Reinigungskassette angeben. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen, verwendet der Server nur eine der Kassetten, bis die angegebene Anzahl Reinigungen für diese Kassette erreicht ist. Dann verwendet der Server die nächste Reinigungskassette. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen und zwei oder mehr Befehle **CLEAN DRIVE** gleichzeitig ausgegeben, verwendet der Server mehrere Kassetten gleichzeitig und verringert die verbleibenden Reinigungen auf jeder Kassette.

Zugehörige Informationen

AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
CLEAN DRIVE (Laufwerk reinigen)
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
QUERY LIBVOLUME (Datenträger im Speicherarchiv abfragen)

Lizenzeinhaltung überprüfen

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

Informationen zu diesem Vorgang

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

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

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

Tipps:

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

PVU-Lizenzierung
Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.

Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM License Metric Tool angesehen. Gemäß Entwurf spiegelt das IBM License Metric Tool die tatsächliche Verwendung wider. Beispielsweise zählt das Tool nachdem der IBM Spectrum Protect-Client für Sichern/Archivieren installiert wurde, den Client nur nach der ersten Verwendung. Weitere Informationen zum IBM License Metric Tool finden Sie in IBM License Metric Tool.

Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

Vorgehensweise

Führen Sie zur Überwachung der Lizenzeinhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen.

Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf **Berichte**.

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

Systemstatus mithilfe von E-Mail-Berichten verfolgen

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

Vorbereitende Schritte

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

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sen-

det, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.

- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.
- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters **EMAILADDRESS** im Befehl **UPDATE ADMIN** angeben.

Informationen zu diesem Vorgang

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzeinhaltungsberichts und eines oder mehrerer angepasster Berichte konfigurieren. Angepasste Berichte werden erstellt, indem Sie eine Schablone aus einer Gruppe gängiger Berichtsschablonen auswählen oder indem Sie Anweisungen SQL SELECT eingeben, um verwaltete Server abzufragen.

Vorgehensweise

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

1. Klicken Sie in der Menüleiste des Operations Center auf **Berichte**.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf **Mail-Server konfigurieren** und füllen Sie die Felder aus.

   Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzeinhaltungsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf **Details** und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten Bericht hinzuzufügen, klicken Sie auf **+ Bericht** und füllen Sie die Felder aus.

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

Ergebnisse

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.

Nächste Schritte

Der Bericht über allgemeine Operationen umfasst eine Anlage. Um detaillierte Informationen anzuzeigen, erweitern Sie die Abschnitte in der Anlage.

Wenn Sie das Image in einem Bericht nicht anzeigen können, verwenden Sie möglicherweise einen E-Mail-Client, der HTML in ein anderes Format konvertiert. Informationen zu Einschränkungen finden Sie in der Onlinehilfe des Operations Center.

Teil 4. Operationen für eine Bandspeicherlösung verwalten

Verwenden Sie diese Informationen, um Operationen für eine Bandspeicherimplementierung für einen IBM Spectrum Protect-Server zu verwalten.

Operations Center verwalten

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit.

Informationen zu diesem Vorgang

Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt. Weitere Informationen zur Verwaltung des Operations Center finden Sie in Operations Center verwalten.

Clientoperationen verwalten

Sie können Clientfehler beheben, Client-Upgrades verwalten und Clientknoten, die nicht mehr erforderlich sind, stilllegen. Um Speicherbereich auf dem Server freizugeben, können Sie veraltete Daten, die von Anwendungsclients gespeichert werden, inaktivieren.

Informationen zu diesem Vorgang

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Ausführliche Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in Clientprobleme lösen.

Anweisungen zum Hinzufügen von Clients finden Sie in „Anwendungen und Systeme schützen” auf Seite 115.

Fehler in Clientfehlerprotokollen auswerten

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

Vorbereitende Schritte

(Optional) Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in Clientverwaltungsservice installieren.

Prozedur

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:

a) Klicken Sie auf der Seite 'Übersicht' im Operations Center auf **Clients** und wählen Sie den Client aus.

b) Klicken Sie auf **Details**.

c) Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte **Diagnose**.

d) Überprüfen Sie die abgerufenen Protokollnachrichten.

Tipps:

– Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.

– Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.

e) Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.

Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.

- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

Clientakzeptor stoppen und erneut starten

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

Informationen zu diesem Vorgang

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client erfolgen können. Wenn Sie beispielsweise die IP-Adresse oder den Domänennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

Vorgehensweise

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:

  a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

  ```
  ps -ef | grep dsmcad
  ```

  Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

  ```
  root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
  ```

  b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

  ```
  kill -9 PID
  ```

  Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.

- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

```
/usr/bin/dsmcad
```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad stop
```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad restart
```

MAC OS X

Klicken Sie auf **Applications** > **Utilities** > **Terminal**.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf **Start** > **Verwaltung** > **Dienste**.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf **Beenden** und **OK**.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf **Start** > **Verwaltung** > **Dienste**.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf **Starten** und **OK**.

Zugehörige Informationen
Fehler für Clientzeitplanung beheben

Kennwörter zurücksetzen

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

Prozedur

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:
  1. Generieren Sie ein neues Kennwort, indem Sie den Befehl **UPDATE NODE** ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Clientknoten und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.

Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option **passwordaccess** in der Clientoptionsdatei auf `generate` gesetzt haben.

- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:

  1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl **UNLOCK ADMIN** aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
  2. Legen Sie mit dem Befehl **UPDATE ADMIN** ein neues Kennwort fest:

     ```
     update admin Administratorname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Administratorname* den Namen des Administrators und *neues_Kennwort* das Kennwort an, das Sie zuordnen.

- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:

  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl **UNLOCK NODE**. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl **UPDATE NODE** ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Namen des Knotens und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.

     Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option **passwordaccess** in der Clientoptionsdatei auf `generate` gesetzt haben.

Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in IBM Spectrum Protect Server-Client Compatibility and Upgrade Considerations . Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Storage-agent and library-client compatibility with an IBM Spectrum Protect server.

   Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	• Clientaktualisierungen planen
IBM Spectrum Protect Snapshot	• Installation und Upgrade für for UNIX and Linux durchführen • Installation und Upgrade für for VMware durchführen • Installation und Upgrade für for Windows durchführen
IBM Spectrum Protect for Databases	• Upgrade für Data Protection for SQL Server durchführen • Installation von Data Protection for Oracle • Installation, Upgrade und Migration für durchführen
IBM Spectrum Protect for Enterprise Resource Planning	• Upgrade für durchführen • Upgrade für durchführen
IBM Spectrum Protect for Mail	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) • Installation, Upgrade und Migration für durchführen
IBM Spectrum Protect for Virtual Environments	• Installation und Upgrade für durchführen • Installation und Upgrade für Data Protection for Microsoft Hyper-V durchführen

Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

Informationen zu diesem Vorgang

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

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

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

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

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

Einschränkung: Sie können einen Objektclientknoten nicht stilllegen.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.

Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl **DECOMMISSION NODE** oder **DECOMMISSION VM** ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

Prozedur

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  a) Klicken Sie auf der Seite **Übersicht** im Operations Center auf **Clients** und wählen Sie den Client aus.
  b) Klicken Sie auf **Weitere** > **Stilllegen**.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie eine der folgenden Aktionen aus:
  - Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl **DECOMMISSION NODE** aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

    ```
    decommission node austin
    ```

  - Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl **DECOMMISSION NODE** unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

    ```
    decommission node austin wait=yes
    ```

  - Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl **DECOMMISSION VM** aus. Wenn beispielsweise der Datencenterknoten den Namen AUSTIN hat und die Dateibereichs-ID 7 lautet, geben Sie den folgenden Befehl aus:

    ```
    decommission vm austin 7 nametype=fsid
    ```

    Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Wenn beispielsweise der Name der virtuellen Maschine CODY 2 und der Dateibereichsname `\VMFULL-CODY 2` lautet, geben Sie den folgenden Befehl aus:

    ```
    decommission vm austin "\vmfull-cody 2"
    ```

– Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl **DECOMMISSION VM** unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Wenn beispielsweise der Name der virtuellen Maschine CODY 2 und der Dateibereichsname `\VMFULL-CODY 2` lautet, geben Sie den folgenden Befehl aus:

```
decommission vm austin "\vmfull-cody 2" wait=yes
```

Nächste Schritte

Achten Sie auf Fehlernachrichten, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite **Übersicht** im Operations Center auf **Clients**.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
   - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
   - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
   - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

   Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

   ```
   query process
   ```

3. Überprüfen Sie die Befehlsausgabe:
   - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

   ```
   query process
    Prozess-    Prozessbeschreibung           Prozessstatus
    nummer
   --------     --------------------     -------------------------------------------
          3          DECOMMISSION NODE        Anzahl der für Knoten NODE1 inaktivierten
                                               Sicherungsobjekte: 8 Objekte inaktiviert.
   ```

   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlernachricht empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlernachricht empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

Zugehörige Informationen

DECOMMISSION NODE (Clientknoten stilllegen)
DECOMMISSION VM (Virtuelle Maschine stilllegen)

Daten zum Freigeben von Speicherbereich inaktivieren

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

Informationen zu diesem Vorgang

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegeben Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

Vorgehensweise

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf **Clients**.
2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf **Weitere** > **Bereinigen**.

   Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl **DEACTIVATE DATA**.

Zugehörige Informationen

DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

Datenspeicher verwalten

Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.

Zugehörige Informationen

Speicherpooltypen

Bestandskapazität verwalten

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

Vorbereitende Schritte

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in „Planung der Speicherarrays” auf Seite 13.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

Prozedur

- Um den Plattenspeicherplatz für die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:

- Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
- Geben Sie den Befehl **EXTEND DBSPACE** aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.

  Tipps:

  - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
  - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.
- Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
- Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Resolving and preventing issues related to database growth and degraded performance in Tivoli Storage Manager V7.1.1.200 and later servers.

- Informationen zur Verringerung der Größe der Datenbank für Server der Version 7.1 und höher finden Sie in Resolving and preventing issues related to database growth and degraded performance in Tivoli Storage Manager V7.1.1.200 and later servers.

  Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die Db2-Befehle können ausgegeben werden, wenn der Server aktiv ist.
- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  a) Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt.
  b) Stoppen Sie den Server.
  c) Aktualisieren Sie in der Datei `dsmserv.opt` die Option **ACTIVELOGSIZE** mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).

  Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option `ACTIVELOGSIZE`. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

Tabelle 29. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

Wert für die Option ACTIVELOGSize	**Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSize**
16 GB bis 128 GB	5120 MB
129 GB bis 256 GB	10240 MB
257 GB bis 512 GB	20480 MB

Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

```
activelogsize 524288
```

d) Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption **ACTIVELOGDIRECTORY** angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.

e) Starten Sie den Server erneut.

- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren.
  Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

  ```
  setopt archlogcompress yes
  ```

  Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption **ARCHLOGCOMPRESS** auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption **ARCHLOGCOMPRESS** inaktiviert werden. Mit dem Befehl **SETOPT** können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

Zugehörige Informationen

Serveroption ACTIVELOGSIZE
EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
SETOPT (Serveroption für dynamische Aktualisierung definieren)

Geplante Aktivitäten optimieren

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Vorgehensweise

1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Sicherungs- und Verwaltungstasks erfolgreich ausgeführt werden. Weitere Informationen zur Überwachung finden Sie in Teil 3, „Bandspeicherlösung überwachen”, auf Seite 147.
2. Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, müssen Sie die Planungsinformationen gegebenenfalls überprüfen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
   - Erhöhung der Anzahl Clients
   - Zunahme des Datenvolumens, das gesichert wird
   - Änderung des Zeitraums, der für Sicherungen verfügbar ist
3. Bestimmen Sie, ob für Ihre Lösung Leistungsprobleme vorliegen.
   Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
   a. Wählen Sie auf der Seite **Clients** im Operations Center den Client aus.
   b. Klicken Sie auf **Details**.

c. Überprüfen Sie auf der Seite **Zusammenfassung** des Clients die für **Gesichert** und **Repliziert** angegebene Aktivität, um alle Risiken zu ermitteln.

Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.

4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
   a. Sichern der Datenbank
   b. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

Zugehörige Informationen

Daten deduplizieren (Version 7.1.1)

Leistung

Operationen durch Aktivierung der Kollokation von Clientdateien optimieren

Die Kollokation von Clientdateien reduziert die Anzahl Datenträgermounts, die erforderlich sind, wenn Benutzer viele Dateien aus einem Speicherpool zurückschreiben, abrufen oder zurückrufen. Die Kollokation reduziert somit die Zeit, die für diese Operationen erforderlich ist.

Informationen zu diesem Vorgang

Bei aktivierter Kollokation versucht der Server, Dateien auf möglichst wenigen Speicherdatenträgern mit sequenziellem Zugriff zu speichern. Die Dateien können zu einem einzelnen Clientknoten, einer Gruppe von Clientknoten, einem Clientdateibereich oder einer Gruppe von Dateibereichen gehören. Sie können die Kollokation für jeden Speicherpool mit sequenziellem Zugriff festlegen, wenn Sie den Pool definieren oder aktualisieren.

Abbildung 7 auf Seite 181 zeigt ein Beispiel für die Kollokation nach Clientknoten mit drei Clients, von denen jeder über einen separaten Datenträger verfügt, der Daten dieses Clients enthält.

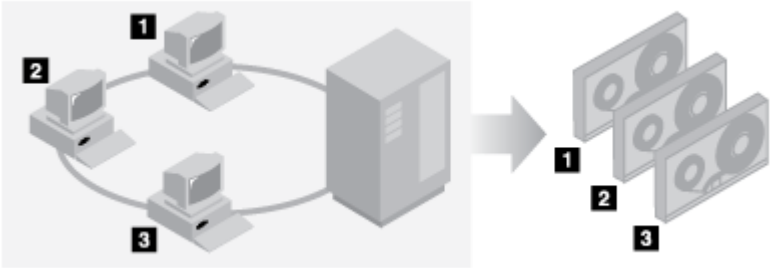


Abbildung 7. Beispiel für die aktivierte Kollokation nach Knoten

Abbildung 8 auf Seite 182 zeigt ein Beispiel für die Kollokation nach Clientknotengruppe. Es sind drei Gruppen definiert und die Daten jeder Gruppe werden auf separaten Datenträgern gespeichert.

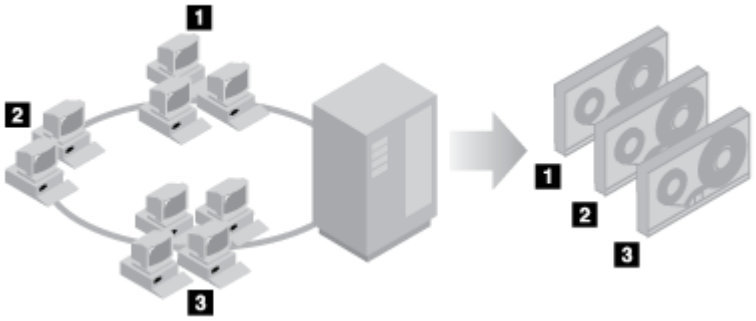


Abbildung 8. Beispiel für die aktivierte Kollokation nach Knotenkollokationsgruppe

Abbildung 9 auf Seite 182 zeigt ein Beispiel für die Kollokation nach Dateibereichsgruppe. Es sind sechs Gruppen definiert. Jede Gruppe enthält Daten aus Dateibereichen, die zu einem einzelnen Knoten gehören. Die Daten jeder Gruppe werden auf einem separaten Datenträger gespeichert.

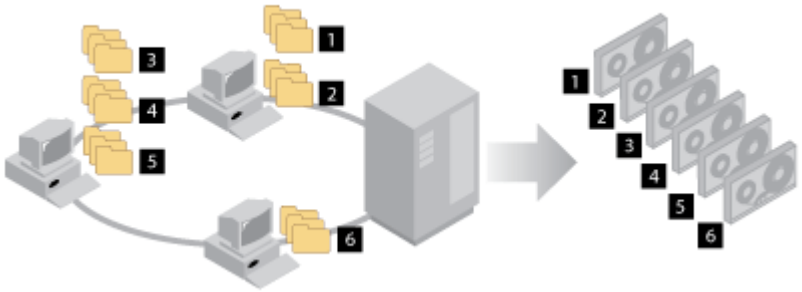


Abbildung 9. Beispiel für die aktivierte Kollokation nach Dateibereichskollokationsgruppe

Bei inaktivierter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich auf jedem Datenträger zu nutzen, bevor er einen neuen Datenträger auswählt. Dieser Prozess ermöglicht zwar eine bessere Nutzung einzelner Datenträger, Benutzerdateien können jedoch über viele Datenträger verstreut werden. Abbildung 10 auf Seite 182 zeigt ein Beispiel für die inaktivierte Kollokation mit drei Clients, die Speicherbereich auf einem einzelnen Datenträger gemeinsam nutzen.

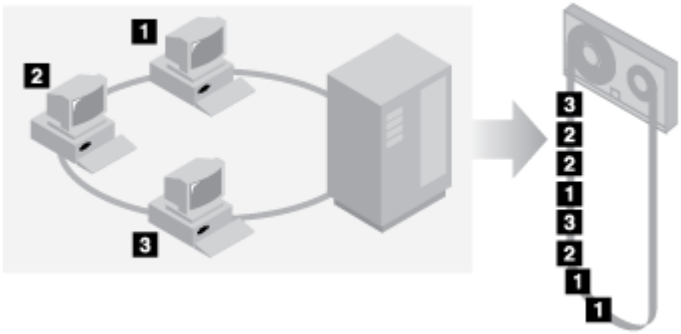


Abbildung 10. Beispiel für die inaktivierte Kollokation

Bei inaktivierter Kollokation sind unter Umständen mehr Datenträgermountoperationen zum Bereitstellen von Datenträgern erforderlich, wenn Benutzer viele Dateien zurückschreiben, abrufen oder zurückrufen.

Die Kollokation nach Gruppe ist der IBM Spectrum Protect-Systemstandardwert für primäre Speicherpools mit sequenziellem Zugriff. Für Kopienspeicherpools und Aufbewahrungsspeicherpools erfolgt standardmäßig keine Kollokation.

Auswirkungen der Kollokation auf Operationen

Die Auswirkungen der Kollokation auf Ressourcen und die Systemleistung sind vom Typ der Operation abhängig, die ausgeführt wird.

In Tabelle 30 auf Seite 183 sind die Auswirkungen der Kollokation auf Operationen zusammengefasst.

Tabelle 30. Auswirkungen der Kollokation auf Operationen

Operation	Kollokation aktiviert	Kollokation inaktiviert
Sichern, Archivieren oder Umlagern von Clientdateien	Mehr Datenträgermounts zum Kollokieren von Dateien.	Es sind weniger Datenträgermounts erforderlich.
Zurückschreiben, Abrufen oder Rückrufen von Clientdateien	Eine große Anzahl Dateien kann schneller zurückgeschrieben, abgerufen oder zurückgerufen werden, da sich die Dateien auf weniger Datenträgern befinden.	Möglicherweise sind mehrere Datenträgermounts für einen einzelnen Benutzer erforderlich, da Dateien auf mehrere Datenträger verteilt sein können. Die Dateien mehrerer Benutzer können auf demselben Speicherdatenträger mit sequenziellem Zugriff gespeichert sein. Wenn beispielsweise zwei Benutzer versuchen, eine Datei wiederherzustellen, die sich auf demselben Datenträger befindet, muss ein Benutzer warten, bis der andere Benutzer seine Dateien wiederhergestellt hat.
Speichern von Daten auf Band	Der Server versucht, alle verfügbaren Banddatenträger zum Trennen von Benutzerdateien zu verwenden, bevor der gesamte verfügbare Speicherbereich auf jedem Banddatenträger genutzt wird.	Der Server versucht, den gesamten verfügbaren Speicherbereich auf jedem einzelnen Banddatenträger zu nutzen, bevor ein anderer Banddatenträger verwendet wird.
Datenträgermountoperationen	Es sind mehr Mountoperationen erforderlich, wenn Benutzerdateien von Clientknoten direkt auf Datenträger mit sequenziellem Zugriff gesichert, archiviert oder umgelagert werden. Während der Konsolidierung und Speicherpoolumlagerung sind mehr Mountoperationen erforderlich. Es werden mehr Datenträger verwaltet werden, da Datenträger nicht vollständig genutzt werden.	Während der Zurückschreibung, des Abrufs und des Rückrufs von Clientdateien sind mehr Mountoperationen erforderlich.
Generieren von Sicherungsgruppen	Es wird weniger Zeit für die Suche nach Datenbankeinträgen benötigt und es sind weniger Mountoperationen erforderlich.	Es wird mehr Zeit für die Suche nach Datenbankeinträgen benötigt und es sind weniger Mountoperationen erforderlich.

Tabelle 30. Auswirkungen der Kollokation auf Operationen (Forts.)

Operation	Kollokation aktiviert	Kollokation inaktiviert
Kopieren von Aufbewahrungsgruppen auf Band **Wichtig:** Aufgrund Ihrer Kollokationseinstellung kann sich die Anzahl Banddatenträger, die für die Aufbewahrungsgruppe erforderlich sind, deutlich erhöhen.	Der Server versucht, Dateien derselben kollokierten Entität auf möglichst wenigen Banddatenträgern zu speichern. Die Verarbeitungszeit zum Schreiben einer Aufbewahrungsgruppe auf Band kann sich gegebenenfalls verlängern.	Der Server versucht, den gesamten verfügbaren Speicherbereich auf jedem einzelnen Banddatenträger zu nutzen, bevor ein anderer Banddatenträger verwendet wird. Wenn Daten aus einer Aufbewahrungsgruppe zurückgeschrieben werden müssen, sind möglicherweise mehr Bandmounts für einen einzelnen Aufbewahrungsgruppenbenutzer erforderlich, da Dateien auf mehrere Datenträger verteilt sein können.

Wenn die Kollokation für eine Gruppe, einen einzelnen Clientknoten oder einen einzelnen Dateibereich aktiviert ist, werden alle Daten, die zu der Gruppe, dem Knoten oder dem Dateibereich gehören, durch einen einzigen Serverprozess versetzt oder kopiert. Wenn beispielsweise Daten nach Gruppe kollokiert werden, werden alle Daten für alle Knoten, die zu derselben Kollokationsgruppe gehören, durch denselben Prozess umgelagert.

Bei der Kollokation von Daten versucht der IBM Spectrum Protect-Server, Dateien auf möglichst wenigen Speicherdatenträgern mit sequenziellem Zugriff zu speichern. Wenn der Server Daten auf Datenträgern in einem Speicherpool mit sequenziellem Zugriff sichert, hat der Sicherungsprozess jedoch Priorität vor den Kollokationseinstellungen. Demzufolge führt der Server die Sicherungsoperation aus, kann aber die Daten möglicherweise nicht kollokieren.

Angenommen, die Kollokation erfolgt nach Knoten und Sie geben an, dass ein Knoten zwei Mountpunkte auf dem Server verwenden kann. Weiterhin sei angenommen, dass die Daten, die von dem Knoten gesichert werden, problemlos auf einen einzigen Banddatenträger passen. Während der Sicherung stellt der Server möglicherweise zwei Banddatenträger bereit und die Daten des Knotens werden möglicherweise auf zwei Bänder verteilt und nicht auf einem einzigen Band gespeichert. Wenn Sie die Kollokation aktivieren, verwenden die folgenden Serveroperationen einen einzigen Serverprozess:

- Versetzen von Daten von Datenträgern mit wahlfreiem Zugriff und sequenziellem Zugriff
- Versetzen von Knotendaten von Datenträgern mit sequenziellem Zugriff
- Sichern eines Speicherpools mit wahlfreiem Zugriff oder sequenziellem Zugriff
- Zurückschreiben eines Speicherpools mit sequenziellem Zugriff
- Konsolidierung von Speicherbereich in einem Speicherpool mit sequenziellem Zugriff oder auf ausgelagerten Datenträgern
- Umlagerung von Daten aus einem Speicherpool mit wahlfreiem Zugriff

Wenn die Umlagerung von Daten aus einem Plattenspeicherpool mit wahlfreiem Zugriff in einen Speicherpool mit sequenziellem Zugriff erfolgt und die Kollokation nach Knoten oder Dateibereich erfolgt, werden Knoten oder Dateibereiche automatisch für die Umlagerung auf der Basis des umzulagernden Datenvolumens ausgewählt. Der Knoten oder Dateibereich mit den meisten Daten wird zuerst umgelagert. Wenn die Kollokation nach Gruppe erfolgt, werden alle Knoten in dem Speicherpool ausgewertet, um den Knoten mit den meisten Daten zu bestimmen. Der Knoten mit den meisten Daten wird zusammen mit allen Daten für alle Knoten, die zu dieser Kollokationsgruppe gehören, zuerst umgelagert. Dieser Prozess erfolgt unabhängig von dem Datenvolumen, das in den Dateibereichen der Knoten gespeichert ist, und unabhängig davon, ob der untere Umlagerungsschwellenwert erreicht wurde.

Wenn jedoch kollokierte Daten aus einem Speicherpool mit sequenziellem Zugriff in einen anderen Speicherpool mit sequenziellem Zugriff umgelagert werden, ordnet der Server die Datenträger gemäß dem Datum, an dem zuletzt auf den Datenträger zugegriffen wurde. Der Datenträger mit dem frühesten Zu-

griffsdatum wird zuerst umgelagert und der Datenträger mit dem neuesten Zugriffsdatum wird zuletzt umgelagert.

Ein Grund für die Kollokation nach Gruppe besteht darin, dass einzelne Clientknoten oft nicht über ausreichend Daten verfügen, um Banddatenträger mit hoher Speicherkapazität zu füllen. Durch die Kollokation von Daten nach Gruppen von Knoten kann die nicht verwendete Bandkapazität reduziert werden, indem mehr kollokierte Daten auf einzelnen Bändern gespeichert werden. Durch die Kollokation von Daten nach Gruppen von Dateibereichen wird die nicht verwendete Bandkapazität noch stärker reduziert.

Die Daten, die zu allen Knoten in derselben Kollokationsgruppe gehören, werden durch denselben Prozess umgelagert. Demzufolge kann durch die Kollokation nach Gruppe die Häufigkeit der erforderlichen Mounts für einen Datenträger, der umgelagert werden soll, reduziert werden. Die Kollokation nach Gruppe kann auch das Durchsuchen der Datenbank minimieren und Bandübergaben während der Übertragung von Daten von einem Speicherpool mit sequenziellem Zugriff in einen anderen reduzieren.

Datenträger bei aktivierter Kollokation auswählen

Die Auswahl der Datenträger ist davon abhängig, ob die Kollokation nach Gruppe, nach Knoten oder nach Dateibereich erfolgt.

Tabelle 31 auf Seite 185 zeigt, wie der IBM Spectrum Protect-Server den ersten Datenträger auswählt, wenn die Kollokation für einen Speicherpool auf Clientknoten-, Kollokationsgruppen- und Dateibereichsebene aktiviert ist.

Tabelle 31. Wie der Server Datenträger bei aktivierter Kollokation auswählt

Reihenfolge bei der Auswahl der Datenträger	Bei Kollokation nach Gruppe	Bei Kollokation nach Knoten	Bei Kollokation nach Dateibereich
1	Ein Datenträger, der bereits Dateien aus der Kollokationsgruppe enthält, zu der der Client gehört	Ein Datenträger, der bereits Dateien desselben Clientknotens enthält	Ein Datenträger, der bereits Dateien aus demselben Dateibereich dieses Clientknotens enthält
2	Ein leerer vordefinierter Datenträger	Ein leerer vordefinierter Datenträger	Ein leerer vordefinierter Datenträger
3	Ein leerer Arbeitsdatenträger	Ein leerer Arbeitsdatenträger	Ein leerer Arbeitsdatenträger
4	Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich	Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich	Ein Datenträger, der Daten desselben Clientknotens enthält
5	Nicht zutreffend	Nicht zutreffend	Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich

Wenn der Server das Speichern der Daten auf einem zweiten Datenträger fortsetzen muss, fordert er weiteren Speicherbereich in der folgenden Auswahlreihenfolge an:

1. Ein leerer vordefinierter Datenträger
2. Ein leerer Arbeitsdatenträger
3. Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich
4. Ein beliebiger verfügbarer Datenträger im Speicherpool

Wenn die Kollokation nach Clientknoten oder Dateibereich erfolgt, versucht der Server, die beste Nutzung einzelner Datenträger zu ermöglichen, und minimiert das Mischen von Dateien von unterschiedlichen Clients oder aus unterschiedlichen Dateibereichen auf Datenträgern. Diese Konfiguration ist in Abbildung 11 auf Seite 186 dargestellt. Die Abbildung zeigt, dass die Datenträgerauswahl *horizontal* erfolgt, wobei alle verfügbaren Datenträger verwendet werden, bevor der gesamte verfügbare Speicherbereich auf jedem einzelnen Datenträger genutzt wird. A, B, C und D stellen Dateien aus vier verschiedenen Clientknoten dar.

Tipps:

1. Wenn die Kollokation nach Knoten erfolgt und der Knoten mehrere Dateibereiche hat, versucht der Server nicht, diese Dateibereiche zu kollokieren.
2. Wenn die Kollokation nach Dateibereich erfolgt und ein Knoten mehrere Dateibereiche hat, versucht der Server, Daten für verschiedene Dateibereiche auf unterschiedlichen Datenträgern zu speichern.

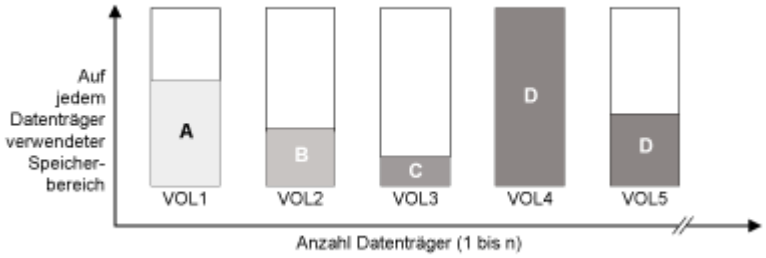


Abbildung 11. Verwendung aller verfügbaren Speicherdatenträger mit sequenziellem Zugriff bei aktivierter Kollokation auf Knoten- oder Dateibereichsebene

Die Kollokation kann nach Dateibereichsgruppe oder Knotengruppe erfolgen. Wenn die Kollokation nach Knotengruppe (Knotenkollokationsgruppe) erfolgt, versucht der Server, Daten von Knoten, die zu derselben Kollokationsgruppe gehören, zu kollokieren. Eine Dateibereichskollokationsgruppe verwendet dieselben Methoden wie eine Knotenkollokationsgruppe, kann jedoch aufgrund der Granularität der Dateibereichsgrößen mehr Speicherbereich verwenden. Wie in Abbildung 12 auf Seite 186 gezeigt wurden Daten für die folgenden Gruppen von Knoten kollokiert:

- Gruppe 1 besteht aus Knoten A, B und C.
- Gruppe 2 besteht aus Knoten D und E.
- Gruppe 3 besteht aus Knoten F, G, H und I.

Wenn möglich, kollokiert der IBM Spectrum Protect-Server Daten, die zu einer Gruppe von Knoten gehören, auf einem einzigen Band. Dies ist in der Abbildung durch Gruppe 2 dargestellt. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind (Gruppe 1 und 2). Wenn die Knoten in der Kollokationsgruppe mehrere Dateibereiche haben, versucht der Server nicht, diese Dateibereiche zu kollokieren.

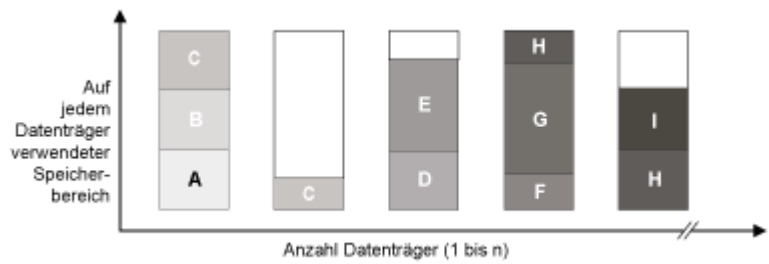


Abbildung 12. Verwendung aller verfügbaren Speicherdatenträger mit sequenziellem Zugriff bei aktivierter Kollokation auf Gruppenebene

Normalerweise schreibt der IBM Spectrum Protect-Server Daten für die aktive Operation immer auf den Datenträger, der gerade gefüllt wird. Gelegentlich kann es jedoch vorkommen, dass sich mehr als ein Datenträger, der mit Daten gefüllt wird, in einem kollokierten Speicherpool befindet. Es kann vorkommen, dass sich mehrere Datenträger, die mit Daten gefüllt werden, in einem kollokierten Speicherpool befinden, wenn verschiedene Serverprozesse oder Clientsitzungen versuchen, Daten gleichzeitig in dem kollokierten Pool zu speichern. In dieser Situation ordnet IBM Spectrum Protect einen Datenträger für jeden Prozess oder jede Sitzung zu, der bzw. die einen Datenträger benötigt, sodass beide Operationen so schnell wie möglich ausgeführt werden.

Datenträger bei inaktivierter Kollokation auswählen

Bei inaktivierter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich in einem Speicherdatenträger zu nutzen, bevor er auf einen neuen Datenträger zugreift.

Wenn Sie Clientdateien in einem Speicherpool mit sequenziellem Zugriff speichern, für den die Kollokation inaktiviert ist, erfolgt die Auswahl eines Datenträgers durch den Server in der folgenden Reihenfolge:

1. Ein zuvor verwendeter sequenzieller Datenträger mit verfügbarem Speicherbereich (ein Datenträger mit dem größten Datenvolumen wird zuerst ausgewählt)
2. Ein leerer Datenträger

Wenn der Server das Speichern der Daten auf einem zweiten Datenträger fortsetzen muss, versucht er, einen leeren Datenträger auszuwählen. Wenn kein leerer Datenträger vorhanden ist, versucht der Server, einen der übrigen verfügbaren Datenträger im Speicherpool auszuwählen.

Abbildung 13 auf Seite 187 zeigt dass die Datenträgerverwendung vertikal erfolgt, wenn die Kollokation inaktiviert ist. In diesem Beispiel werden weniger Datenträger verwendet, da der Server versucht, den gesamten verfügbaren Speicherbereich durch Mischen von Clientdateien auf einzelnen Datenträgern zu nutzen. A, B, C und D stellen Dateien aus vier verschiedenen Clientknoten dar.

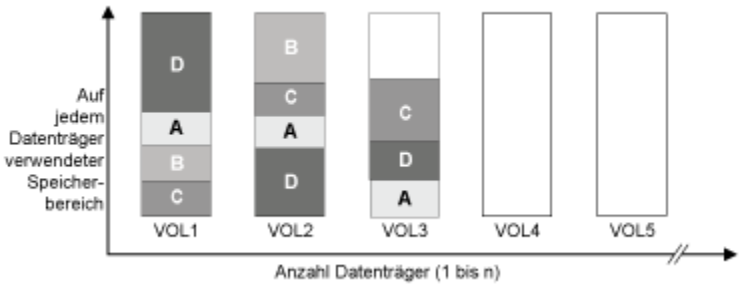


Abbildung 13. Verwendung des gesamten verfügbaren Speicherbereichs auf Datenträgern mit sequenziellem Zugriff bei inaktivierter Kollokation

Kollokationseinstellungen

Nach der Definition eines Speicherpools können Sie die Kollokationseinstellung durch Aktualisieren des Speicherpools ändern. Die Änderung der Kollokation für den Pool hat keine Auswirkungen auf Dateien, die bereits in dem Pool gespeichert sind.

Wenn beispielsweise die Kollokation für einen Speicherpool inaktiviert ist und jetzt aktiviert wird, werden ab diesem Zeitpunkt Clientdateien, die in dem Pool gespeichert werden, kollokiert. Dateien, die zuvor in dem Speicherpool gespeichert wurden, werden nicht versetzt, um kollokiert zu werden. Wenn Datenträger konsolidiert oder zurückgeschrieben werden, werden die Daten in dem Pool im Laufe der Zeit immer stärker kollokiert. Sie können auch den Befehl **MOVE DATA** oder **MOVE NODEDATA** verwenden, um Daten auf neue Datenträger zu versetzen, um die Kollokation zu erhöhen. Das Versetzen von Daten auf neue Datenträger führt jedoch zu einer Verlängerung der Verarbeitungszeit und zu einer Erhöhung der Datenträgermountaktivität.

Tipp: Wenn die Kollokation nach Dateibereich aktiviert ist und ein Knoten über einen Datenträger mit mehreren Dateibereichen verfügt, kann eine Mountwartezeit auftreten oder der Mount länger als üblich

dauern. Wenn ein Datenträger für den Datenempfang auswählbar ist, wartet IBM Spectrum Protect auf diesen Datenträger.

Kollokation von Kopienspeicherpools

Bei der Verwendung der Kollokation für Kopienspeicherpools müssen bestimmte Hinweise beachtet werden. Die Kollokation von Kopienspeicherpools, insbesondere die Kollokation nach Knoten oder Dateibereich, hat mehr teilweise gefüllte Datenträger und möglicherweise unnötige Konsolidierungsaktivität für ausgelagerte Datenträger zur Folge.

Primäre Speicherpools spielen bei der Wiederherstellung eine andere Rolle als Kopienspeicherpools. Normalerweise werden primäre Speicherpools verwendet, um Daten direkt auf Clients wiederherzustellen. Wenn in einem Katastrophenfall sowohl Clients als auch der Server verloren gehen, können Sie ausgelagerte Kopienspeicherpooldatenträger verwenden, um die primären Speicherpools wiederherzustellen. Mithilfe der Typen von Wiederherstellungsszenarios können Sie bestimmen, ob die Kollokation für Ihre Kopienspeicherpools verwendet werden sollte.

Die Kollokation hat in der Regel teilweise gefüllte Datenträger zur Folge, wenn die Kollokation nach Knoten oder Dateibereich erfolgt. Teilweise gefüllte Datenträger sind jedoch seltener vorhanden, wenn die Kollokation nach Gruppe erfolgt. Teilweise gefüllte Datenträger können für primäre Speicherpools akzeptabel sein, da die Datenträger verfügbar bleiben und während des nächsten Umlagerungsprozesses gefüllt werden können. Teilweise gefüllte Datenträger können jedoch für Kopienspeicherpools, deren Speicherpooldatenträger sofort ausgelagert werden, inakzeptabel sein. Wenn Sie die Kollokation für Kopienspeicherpools verwenden, müssen Sie die folgenden Entscheidungen treffen:

- Auslagerung einer größeren Anzahl teilweise gefüllter Datenträger, wodurch sich die Konsolidierungsaktivität erhöht, wenn der Konsolidierungsschwellenwert verringert oder erreicht wird.
- Verbleib dieser teilweise gefüllten Datenträger vor Ort, bis sie voll sind, wobei das Risiko besteht, dass keine ausgelagerte Kopie der Daten auf diesen Datenträgern vorhanden ist.
- Angabe, ob die Kollokation nach Gruppe erfolgen soll, um möglichst viel Bandkapazität zu nutzen.

Wenn die Kollokation für einen Kopienspeicherpool inaktiviert ist, sind nach dem Sichern von Daten im Kopienspeicherpool normalerweise nur einige wenige teilweise gefüllte Datenträger vorhanden.

Überprüfen Sie Ihre Optionen sorgfältig, bevor Sie die Kollokation für Kopienspeicherpools verwenden, und wägen Sie ab, ob gleichzeitiges Schreiben verwendet werden soll. Wenn bei Verwendung der Kollokation für Ihre primären Speicherpools kein gleichzeitiges Schreiben verwendet wird, können Sie die Kollokation für Kopienspeicherpools gegebenenfalls inaktivieren. Die Kollokation für Kopienspeicherpools kann sinnvoll sein, wenn nur wenige Clients vorhanden sind und für jeden dieser Clients täglich sehr viele Teilsicherungsdaten anfallen. Wenn die Kollokation zusammen mit gleichzeitigem Schreiben verwendet wird, müssen Sie sicherstellen, dass die Kollokationseinstellungen für die primären Speicherpools und die Kopienspeicherpools identisch sind.

Kollokation von Aufbewahrungsspeicherpools

Der Wert, den Sie für das Kollokationsmerkmal auswählen, hat Auswirkungen darauf, wie die Daten einer Aufbewahrungsgruppe auf Banddatenträger verteilt werden. Im Allgemeinen sollte die Kollokation inaktiviert werden, um die Anzahl verwendeter Banddatenträger möglichst gering zu halten. Standardmäßig ist die Kollokationseinstellung für Aufbewahrungsspeicherpools inaktiviert.

Bei inaktivierter Kollokationseinstellung versucht der Server während der Datenträgerauswahl für die Prozesse zum Kopieren von Aufbewahrungsgruppen, den gesamten verfügbaren Speicherbereich auf jedem Banddatenträger zu nutzen, bevor er einen neuen Datenträger auswählt. Bei diesem Prozess werden die einzelnen Banddatenträger zwar effizienter genutzt, die Daten für jede Aufbewahrungsgruppe werden jedoch nicht zusammen kollokiert und können unter Umständen auf viele Banddatenträger verteilt werden.

Ihre Kollokationseinstellungen können erhebliche Auswirkungen auf die Systemleistung haben, wenn die Aufbewahrungsgruppendaten auf Band geschrieben werden, sowie auf die Systemleistung während Operationen zum Zurückschreiben der Aufbewahrungsgruppendaten. Prüfen Sie, bevor Sie die Aktivierung von Kollokationseinstellungen für Aufbewahrungsspeicherpools in Erwägung ziehen, Ihre Anforderungen und die Auswirkungen auf die Leistung.

- Wenn die Kollokation aktiviert ist, versucht der Server, Dateien für jede Entität auf möglichst wenigen Banddatenträgern zu speichern. Diese Option erfordert jedoch mehr Serververarbeitungszeit, um Dateien zum Speichern zu kollokieren, sowie eine größere Anzahl Datenträger. Auch die Einstellung des Parameters **STACK**, die für die Aufbewahrungsgruppe definiert ist, von Bedeutung.

  Tipp: Wenn Datenträger-Stacking für die Aufbewahrungsgruppe aktiviert ist, können die Aufbewahrungsgruppendaten Banddatenträger mit kopierten Daten anderer Aufbewahrungsgruppen gemeinsam nutzen. Bei der Datenträgerauswahl wird zuerst nach Datenträgern gesucht, die gefüllt werden (Status FILLING) und bereits Daten enthalten; dies ist jedoch nur der Fall, wenn diese Datenträger nicht bereits von Aufbewahrungsgruppen verwendet werden, die einen separaten Datenträger erfordern. Wenn Datenträger-Stacking für die Aufbewahrungsgruppe nicht aktiviert ist, wird die Aufbewahrungsgruppe auf einem oder mehreren Banddatenträgern kollokiert und es werden keine Daten anderer Aufbewahrungsgruppen auf diese Datenträger gestellt. Bei der Datenträgerauswahl wird nach leeren Datenträgern gesucht; Daten können jedoch nur dann auch auf Datenträger kopiert werden, die mit Daten gefüllt werden (Status FILLING), wenn die Datenträger bereits Daten für die Aufbewahrungsgruppe enthalten, die gerade kopiert wird.
- Bei inaktivierter Kollokation sind, da die Daten für einzelne Aufbewahrungsgruppen möglicherweise auf viele Datenträger verteilt sind, unter Umständen mehr Bandmounts erforderlich, wenn die Daten aus der Aufbewahrungsgruppe zurückgeschrieben werden müssen. Wenn mehr Bandmounts erforderlich sind, kann sich die für Zurückschreibungsoperationen erforderliche Verarbeitungszeit verlängern.

Tipp: Sie können die Kollokation aktivieren oder Kollokationseinstellungen ändern, indem Sie den Parameter **COLLOCATE** im Befehl **DEFINE STGPOOL** oder **UPDATE STGPOOL** angeben.

Von einer Änderung der Kollokationseinstellung sind nur die Daten betroffen, die nachfolgend in den Aufbewahrungsspeicherpool geschrieben werden. Dateien, die bereits in dem Pool gespeichert sind, sind nicht betroffen.

Zugehörige Konzepte

„Datenträger bei inaktivierter Kollokation auswählen” auf Seite 187
Bei inaktivierter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich in einem Speicherdatenträger zu nutzen, bevor er auf einen neuen Datenträger zugreift.

„Auswirkungen der Kollokation auf Operationen” auf Seite 183
Die Auswirkungen der Kollokation auf Ressourcen und die Systemleistung sind vom Typ der Operation abhängig, die ausgeführt wird.

Kollokation planen und aktivieren

Zu wissen, welche Auswirkungen die Kollokation hat, kann hilfreich sein, um die Anzahl der Datenträgermounts zu reduzieren, den Speicherbereich auf sequenziellen Datenträgern besser zu nutzen und die Effizienz von Serveroperationen zu verbessern.

Informationen zu diesem Vorgang

In Tabelle 32 auf Seite 189 sind die vier Kollokationsoptionen aufgeführt, die Sie in den Befehlen **DEFINE STGPOOL** und **UPDATE STGPOOL** angeben können. Die Tabelle zeigt auch die Auswirkungen der Kollokation auf Daten, die zu Knoten gehören, die Mitglieder einer Kollokationsgruppe sind, bzw. die zu Knoten gehören, die keine Mitglieder einer Kollokationsgruppe sind.

Tabelle 32. Kollokationsoptionen und Auswirkungen auf Knotendaten

Kollokationsoption	Wenn ein Knoten nicht als Mitglied einer Kollokationsgruppe definiert ist	Wenn ein Knoten als Mitglied einer Kollokationsgruppe definiert ist
Keine	Die Daten für den Knoten werden nicht kollokiert.	Die Daten für den Knoten werden nicht kollokiert.

Tabelle 32. Kollokationsoptionen und Auswirkungen auf Knotendaten (Forts.)

Kollokationsoption	Wenn ein Knoten nicht als Mitglied einer Kollokationsgruppe definiert ist	Wenn ein Knoten als Mitglied einer Kollokationsgruppe definiert ist
Gruppe	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern im Speicherpool.	Der Server speichert die Daten für den Knoten und für andere Knoten, die zu derselben Kollokationsgruppe gehören, auf möglichst wenigen Datenträgern.
Knoten	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.
Dateibereich	Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.	Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.

Tabelle 33. Kollokationsgruppenoptionen und Auswirkungen auf Dateibereichsdaten

Kollokationsoption	Wenn ein Dateibereich nicht als Mitglied einer Kollokationsgruppe definiert ist	Wenn ein Dateibereich als Mitglied einer Kollokationsgruppe definiert ist
Keine	Die Daten für den Dateibereich werden nicht kollokiert.	Die Daten für den Dateibereich werden nicht kollokiert.
Gruppe	Der Server speichert die Daten für den Dateibereich auf möglichst wenigen Datenträgern im Speicherpool.	Der Server speichert die Daten für den Dateibereich und für andere Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf möglichst wenigen Datenträgern.
Knoten	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.
Dateibereich	Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.	Der Server speichert die Daten für die Dateibereiche auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.

Vorgehensweise

Um festzulegen, ob und wie Daten kollokiert werden, führen Sie die folgenden Schritte aus:

1. Legen Sie fest, wie Daten zusammengefasst werden sollen, ob nach Clientknoten, nach Clientknotengruppe oder nach Dateibereich. Bei der Kollokation nach Gruppe müssen Sie entscheiden, wie Knoten in Gruppen zusammengefasst werden sollen:
   - Wenn das Einsparen von Speicherbereich das Ziel ist, möchten Sie möglicherweise kleine Knoten in einer Gruppe zusammenfassen, um Bänder besser zu nutzen.
   - Wenn schnellere Clientzurückschreibungen das Ziel sind, gruppieren Sie Knoten so, dass sie möglichst viele Bänder füllen. Indem Knoten in Gruppen zusammengefasst werden, werden die Daten der einzelnen Knoten auf zwei oder mehr Bänder verteilt und es können mehr Bänder während einer Mehrfachsitzung für eine Zurückschreibungsoperation ohne Abfrage gleichzeitig bereitgestellt werden.

- Wenn die Aufteilung der Daten nach Abteilung das Ziel ist, können Sie Knoten nach Abteilung gruppieren.

2. Um Gruppen zu kollokieren, führen Sie die folgenden Schritte aus:
   a) Definieren Sie Kollokationsgruppen mit dem Befehl **DEFINE COLLOCGROUP**.
   b) Fügen Sie den Kollokationsgruppen mit dem Befehl **DEFINE COLLOCMEMBER** Clientknoten hinzu.

   Die folgenden Abfragebefehle sind zum Kollokieren von Gruppen verfügbar:

   QUERY COLLOCGROUP
   Zeigt die Kollokationsgruppen an, die auf dem Server definiert sind.

   QUERY NODE
   Zeigt die Kollokationsgruppe an (falls vorhanden), zu der ein Knoten gehört.

   QUERY NODEDATA
   Zeigt Informationen zu den Daten für einen oder mehrere Knoten in einem Speicherpool mit sequenziellem Zugriff an.

   QUERY STGPOOL
   Zeigt Informationen zur Position von Clientdaten in einem Speicherpool mit sequenziellem Zugriff und zum Umfang des Speicherbereichs an, den ein Knoten auf einem Datenträger belegt.

   Sie können auch IBM Spectrum Protect-Server-Scripts oder PERL-Scripts verwenden, um Informationen anzuzeigen, die beim Definieren von Kollokationsgruppen hilfreich sein können.
3. Geben Sie an, wie Daten in einem Speicherpool kollokiert werden müssen, indem Sie den Befehl **DEFINE STGPOOL** oder **UPDATE STGPOOL** unter Angabe des Parameters **COLLOCATE** ausgeben.

Nächste Schritte

Tipp: Um die Anzahl Datenträgermounts zu reduzieren, Speicherbereich auf sequenziellen Datenträgern effizienter zu verwenden und die Kollokation zu aktivieren, führen Sie die folgenden Schritte aus:

- Definieren Sie eine Speicherpoolhierarchie und eine Maßnahme, die erfordert, dass gesicherte, archivierte oder speicherverwaltete Dateien anfänglich in Plattenspeicherpools gespeichert werden.

  Wenn Dateien aus einem Plattenspeicherpool umgelagert werden, versucht der Server, alle Dateien umzulagern, die zu dem Clientknoten oder zu der Kollokationsgruppe gehören, der bzw. die den meisten Plattenspeicherplatz in dem Speicherpool belegt. Dieser Prozess funktioniert gut mit der Kollokationsoption, da der Server versucht, alle Dateien eines bestimmten Clients auf demselben Speicherdatenträger mit sequenziellem Zugriff zu speichern.
- Verwenden Sie Arbeitsdatenträger für Speicherpools mit sequenziellem Zugriff, damit der Server neue Datenträger für die Kollokation auswählen kann.
- Geben Sie die Clientoption COLLOCATEBYFILESPEC an, um die Anzahl Bänder zu begrenzen, auf die Objekte, die einer einzelnen Dateispezifikation zugeordnet sind, geschrieben werden. Diese Kollokationsoption hat eine effizientere Kollokation durch den Server zur Folge; diese Kollokationsoption überschreibt nicht die Kollokation nach Dateibereich oder die Kollokation nach Knoten.

Bandeinheiten verwalten

Routinemäßige Bandoperationen umfassen die Vorbereitung von Banddatenträgern für die Verwendung, die Steuerung, wie und wann Datenträger wiederverwendet werden, und die Sicherstellung, dass genügend Datenträger verfügbar sind. Außerdem müssen Sie auf Bedieneranforderungen antworten und Speicherarchive, Laufwerke, Pfade und Einheiten zum Versetzen von Daten verwalten.

Austauschbare Datenträger vorbereiten

Sie müssen austauschbare Datenträger vorbereiten, bevor sie zum Speichern von Daten verwendet werden können. Typische Vorbereitungstasks umfassen das Zuordnen von Kennsätzen und das Zurückstellen von Datenträgern.

Informationen zu diesem Vorgang

Wenn IBM Spectrum Protect auf einen austauschbaren Datenträger zugreift, wird der Datenträgername im Kennsatzheader geprüft, um sicherzustellen, dass auf den korrekten Datenträger zugegriffen wird.

Banddatenträgern müssen Kennsätze zugeordnet werden, bevor sie vom Server verwendet werden können.

Vorgehensweise

Um einen Datenträger für die Verwendung vorzubereiten, führen Sie die folgenden Schritte aus:

1. Ordnen Sie dem Datenträger einen Kennsatz zu, indem Sie den Befehl **LABEL LIBVOLUME** ausgeben.
2. Stellen Sie bei automatisierten Speicherarchiven den Datenträger in das Speicherarchiv zurück. Anweisungen finden Sie in „Datenträger in ein automatisiertes Speicherarchiv zurückstellen” auf Seite 194.

   Tipp: Wenn Sie den Befehl **LABEL LIBVOLUME** für Laufwerke in einem automatisierten Speicherarchiv verwenden, ist es mit einem einzigen Befehl möglich, den Datenträgern Kennsätze zuzuordnen und die Datenträger zurückzustellen.
3. Wenn der Speicherpool keine Arbeitsdatenträger enthalten kann (MAXSCRATCH=0), identifizieren Sie den Datenträger in IBM Spectrum Protect anhand des Namens, damit später auf den Datenträger zugegriffen werden kann.

   Wenn der Speicherpool Arbeitsdatenträger enthalten kann (**MAXSCRATCH** ist auf einen Wert ungleich null gesetzt), überspringen Sie diesen Schritt.

Banddatenträgern Kennsätze zuordnen

Sie müssen Banddatenträgern Kennsätze zuordnen, bevor diese vom Server verwendet werden können.

Informationen zu diesem Vorgang

Bei automatisierten Speicherarchiven werden Sie zum Einlegen des Datenträgers in den Eingangs-/Ausgangsschacht des Speicherarchivs aufgefordert. Wenn keine Serviceein-/-ausgabestation verfügbar ist, legen Sie den Datenträger in einen leeren Schacht ein. Sie können den Datenträgern Kennsätze zuordnen, wenn Sie die Datenträger zurückstellen oder bevor Sie die Datenträger zurückstellen.

Vorgehensweise

Um Banddatenträgern Kennsätze zuzuordnen, bevor sie zurückgestellt werden, führen Sie die folgenden Schritte aus:

1. Ordnen Sie Banddatenträgern Kennsätze zu, indem Sie den Befehl **LABEL LIBVOLUME** ausgeben. Um beispielsweise einem Datenträger in einem Speicherarchiv mit dem Namen LIBRARY1 den Namen VOLUME1 zuzuordnen, geben Sie den folgenden Befehl aus:

   ```
   label libvolume library1 volume1
   ```

   Voraussetzung: Es muss mindestens ein Laufwerk verfügbar sein. Das Laufwerk darf nicht von einem anderen IBM Spectrum Protect-Prozess verwendet werden. Wenn ein Laufwerk inaktiv ist, wird das Laufwerk als nicht verfügbar betrachtet.
2. Um einen vorhandenen Kennsatz zu überschreiben, geben Sie den Parameter OVERWRITE=YES an. Standardmäßig wird ein vorhandener Kennsatz mit dem Befehl **LABEL LIBVOLUME** nicht überschrieben.

Zugehörige Tasks

Neuen Datenträgern mit AUTOLABEL Kennsätze zuordnen
Die Verwendung des Parameters **AUTOLABEL** im Befehl **DEFINE LIBRARY** oder **UPDATE LIBRARY** ist effizienter als die Verwendung des Befehls **LABEL LIBVOLUME**, der das separate Bereitstellen von Datenträgern erfordert.

Zugehörige Informationen

LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Datenträgern in einem SCSI-Speicherarchiv Kennsätze zuordnenSpeicherarchiv

Sie können Datenträgern einzeln einen Kennsatz zuordnen oder das Speicherarchiv mithilfe von IBM Spectrum Protect durchsuchen und den gefundenen Datenträgern Kennsätze zuordnen.

Datenträgern einzeln Kennsätze zuordnen

Wenn Sie Datenträgern einzeln mithilfe des Befehls **LABEL LIBVOLUME** einen Kennsatz zuordnen, müssen Sie einen Datenträgernamen angeben.

Vorgehensweise

1. Legen Sie Datenträger in den Eingangs-/Ausgangsschacht des Speicherarchivs ein, wenn Sie vom Server dazu aufgefordert werden. Das Speicherarchiv lädt jeden eingelegten Datenträger in ein Laufwerk.
2. Geben Sie bei einem SCSI-Speicherarchiv einen Datenträgernamen ein, wenn Sie dazu aufgefordert werden. Ein Kennsatz mit dem angegebenen Namen wird auf den Datenträger geschrieben.

   Tipp: Damit bei einem SCSI-Speicherarchiv für den Datenträgername eine Eingabeaufforderung angezeigt wird, geben Sie den Befehl **LABEL LIBVOLUME** unter Angabe des Parameters **LABELSOURCE=PROMPT** aus.
3. Wenn das Speicherarchiv über keinen Eingangs-/Ausgangsport verfügt, werden Sie dazu aufgefordert, das Band aus dem Schacht mit der angegebenen Nummer zu entfernen. Entfernen Sie das Band aus dem angegebenen Schacht.

   Wenn das Speicherarchiv über einen Eingangs-/Ausgangsport verfügt, wird mit dem Befehl standardmäßig jeder Datenträger mit Kennsatz in den Eingangs-/Ausgangsport des Speicherarchivs zurückgestellt.

Datenträgerkennsätze in einem SCSI-Speicherarchiv überschreiben

Mithilfe des Befehls **LABEL LIBVOLUME** können Sie vorhandene Datenträgerkennsätze überschreiben, wenn auf den Speicherdatenträgern keine gültigen Daten vorhanden sind.

Informationen zu diesem Vorgang

Sie können Datenträgern in einem SCSI-Speicherarchiv selbst dann Kennsätze zuordnen, wenn kein Eingangs-/Ausgangsport vorhanden ist. Sie müssen jeden neuen Datenträger manuell in das Speicherarchiv einlegen und die Datenträger in Speicherschächte in dem Speicherarchiv stellen, nachdem die Kennsätze der Datenträger geschrieben wurden.

Vorgehensweise

Überschreiben Sie die vorhandenen Datenträgerkennsätze, indem Sie den Befehl **LABEL LIBVOLUME** ausgeben. Wenn beispielsweise der Name des Speicherarchivs LIB1 und der Datenträgername VOLNAME lautet, geben Sie den folgenden Befehl aus:

```
label libvolume lib1 volname overwrite=yes
```

Neuen Datenträgern mit AUTOLABEL Kennsätze zuordnen

Die Verwendung des Parameters **AUTOLABEL** im Befehl **DEFINE LIBRARY** oder **UPDATE LIBRARY** ist effizienter als die Verwendung des Befehls **LABEL LIBVOLUME**, der das separate Bereitstellen von Datenträgern erfordert.

Vorgehensweise

Geben Sie den Befehl **DEFINE LIBRARY** oder **UPDATE LIBRARY** unter Angabe des Parameters **AUTOLABEL** aus.

Tipp: Wenn Sie den Parameter **AUTOLABEL** für ein SCSI-Speicherarchiv verwenden, müssen Sie Bänder unter Angabe des Parameters **CHECKLABEL=BARCODE** im Befehl **CHECKIN LIBVOLUME** zurückstellen. Für den Parameter **AUTOLABEL** wird standardmäßig NO für SCSI-Speicherarchive und YES für alle anderen Speicherarchivtypen angenommen. Der Parameter **CHECKLABEL=BARCODE** wird nur berücksichtigt, wenn das Speicherarchiv über einen Barcodeleser verfügt.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

DEFINE LIBRARY (Speicherarchiv definieren)

LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Speicherarchiv durchsuchen und Datenträgern Kennsätze zuordnen

IBM Spectrum Protect kann alle Speicherschächte in einem Speicherarchiv nach Datenträgern durchsuchen und versuchen, jedem gefundenen Datenträger einen Kennsatz zuzuordnen.

Vorgehensweise

Um ein Speicherarchiv zu durchsuchen und Datenträgern Kennsätze zuzuordnen, geben Sie den Befehl **LABEL LIBVOLUME** unter Angabe des Parameters **SEARCH=YES** aus.

Tipp: Wenn Sie ein SCSI-Speicherarchiv verwenden und das Speicherarchiv über einen Barcodeleser verfügt, können über den Befehl **LABEL LIBVOLUME** mithilfe des Barcodelesers Datenträgernamen abgerufen werden; Sie werden dann nicht zur Angabe der Datenträgernamen aufgefordert. Der Parameter **LABELSOURCE=BARCODE** ist nur für SCSI-Speicherarchive gültig.

Um beispielsweise allen Datenträgern in einem SCSI-Speicherarchiv Kennsätze zuzuordnen, geben Sie den folgenden Befehl aus:

```
label libvolume Speicherarchivname search=yes labelsource=barcode
```

IBM Spectrum Protect wählt das nächste verfügbare Laufwerk aus, sodass Sie Ihre Suche fortsetzen können.

Ergebnisse

Nachdem einem Datenträger ein Kennsatz zugeordnet wurde, wird der Datenträger wieder an seine ursprüngliche Position im Speicherarchiv gestellt.

Zugehörige Informationen

LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Datenträger in ein automatisiertes Speicherarchiv zurückstellen

Sie können einen Datenträger mithilfe des Befehls **CHECKIN LIBVOLUME** in ein automatisiertes Speicherarchiv zurückstellen.

Vorbereitende Schritte

Um Bändern automatisch Kennsätze zuzuordnen, bevor sie zurückgestellt werden, geben Sie den Befehl **DEFINE LIBRARY** unter Angabe des Parameters **AUTOLABEL=YES** aus. Wenn der Parameter **AUTOLABEL**

verwendet wird, entfällt die Notwendigkeit, einer Gruppe von Bändern vorab Kennsätze zuordnen zu müssen.

Informationen zu diesem Vorgang

Jeder Datenträger, der von einem Server für einen beliebigen Zweck verwendet wird, muss einen eindeutigen Namen haben. Diese Voraussetzung gilt für alle Datenträger, unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen wie beispielsweise Datenbanksicherung oder Export verwendet werden. Die Voraussetzung gilt auch für Datenträger, die sich in unterschiedlichen Speicherarchiven befinden, aber von demselben Server verwendet werden.

Tipps:

- Verwenden Sie nicht ein einzelnes Speicherarchiv für Datenträger mit Barcodeetiketten und Datenträger ohne Barcodeetiketten. Das Scannen von Barcodes kann bei Datenträgern ohne Kennsatz lange dauern.
- Der Server akzeptiert nur Bänder, denen IBM Standardkennsätze zugeordnet wurden.
- Jeder Datenträger mit einem Barcode, der mit CLN beginnt, wird als Reinigungsband betrachtet.
- Wenn für einen Datenträger ein Eintrag im Datenträgerprotokoll vorhanden ist, kann der Datenträger nicht als Arbeitsdatenträger zurückgestellt werden.

Vorgehensweise

1. Um einen Speicherdatenträger in ein Speicherarchiv zurückzustellen, geben Sie den Befehl **CHECKIN LIBVOLUME** aus.

   Tipp: Der Befehl wird immer als Hintergrundprozess ausgeführt. Warten Sie, bis die Verarbeitung des Prozesses **CHECKIN LIBVOLUME** abgeschlossen ist, bevor Sie Datenträger definieren; andernfalls schlägt der Definitionsprozess fehl. Sie können Zeit sparen, indem Sie Datenträger im Rahmen der Operation zum Zuordnen von Kennsätzen zurückstellen.
2. Geben Sie den Namen des Speicherarchivs an und geben Sie an, ob es sich bei dem Datenträger um einen privaten Datenträger oder einen Arbeitsdatenträger handelt. Führen Sie abhängig davon, ob Sie Arbeitsdatenträger oder private Datenträger verwenden, einen der folgenden Schritte aus:
   - Wenn Sie nur Arbeitsdatenträger verwenden, stellen Sie sicher, dass genügend Arbeitsdatenträger verfügbar sind. Beispielsweise müssen Sie gegebenenfalls weiteren Datenträgern Kennsätze zuordnen. In dem Maße, wie Datenträger verwendet werden, müssen Sie unter Umständen auch die Anzahl zulässiger Arbeitsdatenträger in dem Speicherpool erhöhen, der für dieses Speicherarchiv definiert wurde.
   - Wenn private Datenträger zusätzlich zu oder anstelle von Arbeitsdatenträgern in dem Speicherarchiv verwendet werden sollen, definieren Sie Datenträger für den Speicherpool mithilfe des Befehls **DEFINE VOLUME**. Sie müssen den Datenträgern, die Sie definieren, Kennsätze zuordnen und die Datenträger zurückstellen.

Zugehörige Tasks

Banddatenträgern Kennsätze zuordnen
Sie müssen Banddatenträgern Kennsätze zuordnen, bevor diese vom Server verwendet werden können.

Einzelnen Datenträger in ein SCSI-Speicherarchiv zurückstellen

Sie können einen einzelnen Datenträger zurückstellen, indem Sie den Befehl **CHECKIN LIBVOLUME** unter Angabe des Parameters **SEARCH=NO** ausgeben. IBM Spectrum Protect fordert den Bediener, der den Mount durchführt, dazu auf, den Datenträger in den Eingangs-/Ausgangsport des Speicherarchivs zu laden.

Vorgehensweise

1. Geben Sie den Befehl **CHECKIN LIBVOLUME** aus.

Um beispielsweise den Datenträger VOL001 zurückzustellen, geben Sie den folgenden Befehl ein:

```
checkin libvolume tapelib vol001 search=no status=scratch
```

2. Antworten Sie auf die Eingabeaufforderung des Servers.
   - Wenn das Speicherarchiv über einen Eingangs-/Ausgangsport verfügt, werden Sie zum Einlegen eines Bands in den Eingangs-/Ausgangsport aufgefordert.
   - Wenn das Speicherarchiv über keinen Eingangs-/Ausgangsport verfügt, werden Sie zum Einlegen eines Bands in einen der Schächte im Speicherarchiv aufgefordert. Diese Schächte werden durch Elementadressen angegeben. Wenn der Server beispielsweise erkennt, dass der erste leere Schacht die Elementadresse 5 hat, wird die folgende Nachricht zurückgegeben:

     ```
     ANR8306I 001: 8MM-Datenträger VOL001 R/W innerhalb von 60 Minuten
     in Schacht mit Elementnummer 5 in Kassettenarchiv TAPELIB einlegen;
     wenn bereit, 'REPLY' zusammen mit der Anforderungs-ID ausgeben.
     ```

     Wenn Sie die Position von Elementadresse 5 in dem Speicherarchiv nicht kennen, überprüfen Sie das Arbeitsblatt auf die Einheit. Angaben zur Lokalisation des Arbeitsblattes enthält die Dokumentation zu Ihrem Speicherarchiv. Nachdem Sie den Datenträger wie angefordert eingelegt haben, antworten Sie auf die Nachricht von einem IBM Spectrum Protect-Verwaltungsclient. Geben Sie den Befehl **REPLY** gefolgt von der Anforderungsnummer (die Nummer am Anfang der Mountanforderung) aus, beispielsweise:

     ```
     reply 1
     ```

     Tipp: Elementadressen beginnen nicht notwendigerweise mit der Zahl 1. Überprüfen Sie das Arbeitsblatt dahingehend. Wenn für Ihre Einheit im IBM Support Portal for IBM Spectrum Protect kein Arbeitsblatt aufgelistet ist, ziehen Sie die Dokumentation zu Ihrem Speicherarchiv zu Rate.

   Wenn Sie über den optionalen Parameter **WAITTIME** im Befehl **CHECKIN LIBVOLUME** eine Wartezeit von 0 angeben, ist kein Befehl **REPLY** erforderlich. Die Standardwartezeit beträgt 60 Minuten.

Datenträger aus Speicherarchivspeicherschächten zurückstellen

Wenn viele Datenträger zurückgestellt werden müssen und verhindert werden soll, dass für jeden Datenträger ein Befehl **CHECKIN LIBVOLUME** ausgegeben werden muss, können Sie Speicherschächte nach neuen Datenträgern durchsuchen. Der Server findet Datenträger, die dem Datenträgerbestand noch nicht hinzugefügt wurden.

Vorgehensweise

1. Öffnen Sie das Speicherarchiv und legen Sie die neuen Datenträger in freie Schächte ein.
   Öffnen Sie beispielsweise bei einer SCSI-Einheit die Zugangstür des Speicherarchivs, legen Sie alle neuen Datenträger in freie Schächte ein und schließen Sie die Zugangstür.
2. Wenn den Datenträgern kein Kennsatz zugeordnet ist, ordnen Sie dem Datenträger mit dem Befehl **LABEL LIBVOLUME** einen Kennsatz zu.
3. Geben Sie den Befehl **CHECKIN LIBVOLUME** unter Angabe des Parameters **SEARCH=YES** aus.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Datenträger aus Eingangs-/Ausgangsports eines Speicherarchivs zurückstellen

Sie können alle Schächte von Masseneingangs-/-ausgangsports nach Datenträgern mit Kennsätzen durchsuchen und der Server kann diese automatisch zurückstellen.

Vorbereitende Schritte

Geben Sie den Befehl **LABEL LIBVOLUME** aus, um allen Datenträgern ohne Kennsatz einen Kennsatz zuzuordnen.

Informationen zu diesem Vorgang

Bei SCSI-Speicherarchiven durchsucht der Server alle Eingangs-/Ausgangsports in dem Speicherarchiv nach Datenträgern. Wenn ein Datenträger gefunden wird, der einen gültigen Datenträgerkennsatz enthält, wird der Datenträger automatisch zurückgestellt.

Vorgehensweise

Geben Sie den Befehl **CHECKIN LIBVOLUME** unter Angabe des Parameters **SEARCH=BULK** aus.

- Um ein Band in ein Laufwerk zu laden und den Kennsatz zu lesen, geben Sie den Parameter **CHECKLABEL=YES** an. Nachdem der Kennsatz vom Server gelesen wurde, versetzt der Server das Band aus dem Laufwerk in einen Speicherschacht.
- Damit der Server den Barcodeleser zur Überprüfung externer Kennsätze auf Bändern verwendet, geben Sie den Parameter **CHECKLABEL=BARCODE** an. Wenn das Lesen von Barcodes aktiviert ist, liest der Server den Kennsatz und versetzt das Band aus dem Eingangs-/Ausgangsport in einen Speicherschacht.

Datenträger mithilfe von Barcodelesern in Speicherarchiven zurückstellen

Sie können Zeit sparen, wenn Sie Datenträger in Speicherarchive mit Barcodelesern zurückstellen, indem Sie die Zeichen auf den Barcodeetiketten als Namen für die Datenträger verwenden.

Informationen zu diesem Vorgang

Der Server liest die Barcodeetiketten und verwendet die Informationen zum Schreiben der internen Datenträgerkennsätze. Bei Datenträgern ohne Barcodeetiketten stellt der Server die Datenträger in einem Laufwerk bereit und versucht, den internen aufgezeichneten Kennsatz zu lesen.

Vorgehensweise

Geben Sie den Befehl **CHECKIN LIBVOLUME** unter Angabe des Parameters **CHECKLABEL=BARCODE** aus. Um beispielsweise mithilfe eines Barcodelesers ein Speicherarchiv mit dem Namen TAPELIB zu durchsuchen und ein Arbeitsband zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Datenträger mithilfe eines Barcodelesers zurückstellen

Sie können Zeit sparen, wenn Sie Datenträger mithilfe eines Barcodelesers zurückstellen, vorausgesetzt, Ihr Speicherarchiv verfügt über einen Barcodeleser.

Informationen zu diesem Vorgang

Wenn Sie einen Datenträger zurückstellen, können Sie angeben, ob die Datenträgerkennsätze während der Zurückstellungsverarbeitung gelesen werden sollen. Wenn die Kennsatzprüfung aktiviert ist, stellt IBM Spectrum Protect jeden Datenträger bereit, um den internen Kennsatz zu lesen, und stellt einen Datenträger nur dann zurück, wenn der Kennsatz korrekt ist. Mithilfe der Kennsatzprüfung können zukünftige Fehler verhindert werden, wenn Datenträger in Speicherpools verwendet werden; dadurch verlängert sich jedoch die Verarbeitungszeit beim Zurückstellen.

Wenn ein Datenträger kein Barcodeetikett hat, stellt IBM Spectrum Protect die Datenträger in einem Laufwerk bereit und versucht, den aufgezeichneten Kennsatz zu lesen.

Vorgehensweise

Um Datenträger mithilfe eines Barcodelesers zurückzustellen, geben Sie den Befehl **CHECKIN LIBVOLUME** unter Angabe von **CHECKLABEL=BARCODE** aus. Um beispielsweise mithilfe des Barcodelesers alle Datenträger als Arbeitsdatenträger in ein Speicherarchiv mit dem Namen TAPELIB zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Zugehörige Tasks

Austauschbare Datenträger vorbereiten
Sie müssen austauschbare Datenträger vorbereiten, bevor sie zum Speichern von Daten verwendet werden können. Typische Vorbereitungstasks umfassen das Zuordnen von Kennsätzen und das Zurückstellen von Datenträgern.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Datenträger mit der Auslagerungsfunktion in ein volles Speicherarchiv zurückstellen

Wenn beim Zurückstellen von Datenträgern keine leeren Schächte in dem Speicherarchiv verfügbar sind, schlägt die Zurückstelloperation fehl, es sei denn, Sie aktivieren die *Auslagerungsfunktion*. Wenn Sie die Auslagerungsfunktion aktivieren und das Speicherarchiv voll ist, wählt der Server einen Datenträger zum Ausgeben aus und stellt dann den angeforderten Datenträger zurück.

Informationen zu diesem Vorgang

Bei der Auswahl des auszugebenden Datenträgers prüft der Server zunächst, ob ein verfügbarer Arbeitsdatenträger vorhanden ist und sucht dann nach dem Datenträger mit der geringsten Anzahl Mounts. Der Server gibt den für die Auslagerungsoperation ausgewählten Datenträger aus dem Speicherarchiv aus und ersetzt ihn durch den Datenträger, der zurückgestellt wird.

Prozedur

- Um Datenträger auszulagern, wenn kein leerer Speicherarchivschacht zum Zurückstellen eines Datenträgers verfügbar ist, geben Sie den Befehl **CHECKIN LIBVOLUME** unter Angabe des Parameters **SWAP=YES** aus.
  Um beispielsweise einen Datenträger mit dem Namen VOL1 in ein Speicherarchiv mit dem Namen AUTO zurückzustellen und die Auslagerungsfunktion zu aktivieren, geben Sie den folgenden Befehl aus:

  ```
  checkin libvolume auto vol1 swap=yes
  ```

Zugehörige Tasks

Volles Speicherarchiv mit einer Überlaufposition verwalten
Mit zunehmendem Speicherbedarf überschreitet die Anzahl Datenträger, die für einen Speicherpool erforderlich sind, unter Umständen die physische Kapazität eines automatisierten Speicherarchivs. Um Speicherbereich für neue Datenträger verfügbar zu machen und vorhandene Datenträger zu überwachen, können Sie eine Überlaufposition für einen Speicherpool definieren.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Private Datenträger und Arbeitsdatenträger

Lesen Sie zur Optimierung von Bandspeicher die Informationen zu privaten Datenträgern und Arbeitsdatenträgern. Verwenden Sie private Datenträger und Arbeitsdatenträger dementsprechend.

Private Datenträger können nicht überschrieben werden, wenn die Bereitstellung eines Arbeitsdatenträgers angefordert wird. Sie können einen Datenträger im Arbeitsstatus nicht zurückstellen, wenn dieser

Datenträger von einem Speicherpool verwendet wird, um Daten zu exportieren, eine Datenbank zu sichern oder einen Sicherungsgruppendatenträger zu sichern.

Teilweise beschriebene Datenträger sind immer private Datenträger. Datenträger haben entweder den Status SCRATCH (Arbeitsdatenträger) oder PRIVATE (privater Datenträger); wenn IBM Spectrum Protect jedoch Daten auf ihnen speichert, wird ihnen der Status PRIVATE zugeordnet.

Tabelle 34. Verwendung privater Datenträger und Arbeitsdatenträger

Datenträgertyp	**Verwendung**
Private Datenträger	Verwenden Sie private Datenträger, um die von einzelnen Speicherpools verwendeten Datenträger festzulegen und die Datenträger manuell zu steuern. Geben Sie zum Definieren privater Datenträger den Befehl **DEFINE VOLUME** aus. Bei Zurückschreibungen, Hauptspeicherauszügen oder Ladevorgängen für Datenbanken oder bei Serverimportoperationen müssen Sie private Datenträger angeben.
Arbeitsdatenträger	In einigen Fällen können Sie die Datenträgerverwaltung durch Verwendung von Arbeitsdatenträgern vereinfachen. Arbeitsdatenträger können unter den folgenden Bedingungen verwendet werden: • Es ist nicht erforderlich, jeden einzelnen Speicherpooldatenträger zu definieren. • Die Vorteile der Automatisierung automatischer Einheiten sollen genutzt werden. • Verschiedene Speicherpools nutzen ein automatisiertes Speicherarchiv gemeinsam und die Speicherpools können Datenträger dynamisch von den Arbeitsdatenträgern in dem Speicherarchiv anfordern. Die Datenträger müssen den Speicherpools nicht vorab zugeordnet werden.

Zugehörige Tasks

Status eines Datenträgers in einem automatisierten Speicherarchiv ändern
Sie können den Status eines Datenträgers von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) oder umgekehrt ändern.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
DELETE VOLUME (Speicherpooldatenträger löschen)

Elementadressen für Speicherarchivspeicherschächte

Eine Elementadresse ist eine Zahl, die die physische Position eines Speicherschachts oder Laufwerks in einem automatisierten Speicherarchiv angibt.

Wenn ein Speicherarchiv über Eingangs-/Ausgangsports verfügt, können Sie Datenträger unter Verwendung der Ports hinzufügen und entfernen. Wenn keine Eingangs-/Ausgangsports vorhanden sind, müssen Sie Bänder in Speicherschächte laden.

Wenn Sie Bänder in Speicherschächte laden, müssen Sie auf Mountanforderungen antworten, die Speicherschächte mit Elementadressen angeben. Wenn Sie im Befehl **CHECKIN LIBVOLUME** oder im Befehl **LABEL LIBVOLUME** eine Wartezeit von 0 angeben, müssen Sie nicht auf eine Mountanforderung antworten.

Informationen zu Elementadressen finden Sie in der Dokumentation des Einheitenherstellers oder bei der Suche nach Elementadressen im IBM Support Portal for IBM Spectrum Protect.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Datenträgerbestand verwalten

Sie können den Datenträgerbestand verwalten, indem Sie den Zugriff des Servers auf Datenträger steuern, Bänder wiederverwenden und Datenträger wiederverwenden, die für Datenbanksicherungs- und Exportoperationen verwendet werden. Sie können den Bestand auch verwalten, indem Sie einen Vorrat an Arbeitsdatenträgern bereithalten.

Informationen zu diesem Vorgang

Jeder Datenträger, der von einem Server verwendet wird, muss - unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen wie beispielsweise Datenbanksicherung oder Export verwendet werden - einen eindeutigen Namen haben. Auch Datenträger, die sich in unterschiedlichen Speicherarchiven befinden, aber von demselben Server verwendet werden, müssen einen eindeutigen Namen haben.

Zugriff auf Datenträger steuern

Sie können verschiedene Methoden verwenden, um den Zugriff auf Datenträger zu steuern.

Prozedur

Um den Zugriff auf Datenträger zu steuern, führen Sie eine der folgenden Aktionen aus:

- Um zu verhindern, dass der Server einen Datenträger bereitstellt, geben Sie den Befehl **UPDATE VOLUME** unter Angabe des Parameters **ACCESS=UNAVAILABLE** aus.
- Um Datenträger nicht verfügbar zu machen und zum Schutz an einen anderen Standort zu senden, verwenden Sie einen Kopienspeicherpool oder einen Speicherpool für aktive Daten.
- Sie können primäre Speicherpools in einem Kopienspeicherpool sichern und dann die Kopienspeicherpooldatenträger auslagern.
- Sie können aktive Versionen von Clientsicherungsdaten in Speicherpools für aktive Daten kopieren und dann die Datenträger auslagern.
- Sie können Kopienspeicherpooldatenträger und Datenträger in Pools für aktive Daten verfolgen, indem Sie ihren Zugriffsmodus in OFFSITE ändern und das Datenträgerprotokoll aktualisieren, um ihren Standort zu identifizieren.

Zugehörige Informationen

UPDATE VOLUME (Speicherpooldatenträger aktualisieren)

Bänder wiederverwenden

Um sicherzustellen, dass immer ein ausreichender Vorrat an Bändern verfügbar ist, können Sie alte Dateien verfallen lassen, Datenträger konsolidieren und Datenträger, die das Ende des Lebenszyklus erreicht haben, löschen. Sie können auch einen Vorrat an Arbeitsdatenträgern bereithalten.

Informationen zu diesem Vorgang

Im Laufe der Zeit altern Datenträger und ein Teil der auf den Datenträgern gespeicherten Sicherungsdaten wird unter Umständen nicht mehr benötigt. Sie können Servermaßnahmen definieren, um festzulegen, wie viele Sicherungsversionen und wie lange Sicherungsversionen aufbewahrt werden sollen. Mithilfe der Verfallsverarbeitung können Dateien, die nicht mehr erforderlich sind, gelöscht werden. Sie können die erforderlichen Daten auf den Datenträgern beibehalten. Wenn die Daten nicht mehr benötigt werden, können Sie die Datenträger konsolidieren und wiederverwenden.

Vorgehensweise

1. Löschen Sie nicht benötigte Clientdaten durch regelmäßige Ausführung der Verfallsverarbeitung. Bei der Verfallsverarbeitung werden Daten gelöscht, die nicht mehr gültig sind, da sie den in der Maßnahme angegebenen Aufbewahrungszeitraum überschreiten oder da Benutzer oder Administratoren die aktiven Versionen der Daten gelöscht haben.
2. Verwenden Sie Datenträger in Speicherpools wieder, indem Sie die Konsolidierungsverarbeitung ausführen.

   Bei der Konsolidierungsverarbeitung werden alle nicht verfallenen Daten konsolidiert, indem sie von mehreren Datenträgern auf eine geringere Anzahl Datenträger versetzt werden. Die Datenträger können dann wieder in den Speicherpool gestellt und wiederverwendet werden.
3. Verwenden Sie Datenträger wieder, die veraltete Datenbanksicherungen oder exportierte Daten enthalten, die nicht mehr erforderlich sind, indem Sie das Datenträgerprotokoll löschen.

   Bevor der Server Datenträger wiederverwenden kann, die im Datenträgerprotokoll protokolliert sind, müssen Sie die Datenträgerinformationen durch Ausgabe des Befehls **DELETE VOLHISTORY** aus der Protokolldatei für Datenträger löschen.

   Tipp: Wenn Ihr Server die Funktion Disaster Recovery Manager (DRM) verwendet, werden die Datenträgerinformationen automatisch während der Verarbeitung des Befehls **MOVE DRMEDIA** gelöscht.
4. Legen Sie fest, wann Banddatenträger das Ende des Lebenszyklus erreichen. Mithilfe des Servers können Sie Statistikdaten zu Datenträgern anzeigen, die die Anzahl Schreiboperationen für die Datenträger und die Anzahl Schreibfehler umfassen. Für private Datenträger und Arbeitsdatenträger werden die folgenden statistischen Daten angezeigt:

   Private Datenträger
   Bei Datenträgern, die anfänglich als private Datenträger definiert wurden, werden diese statistischen Daten vom Server selbst dann beibehalten, wenn der Datenträger konsolidiert wird. Sie können die Informationen mit der vom Hersteller empfohlenen Anzahl Schreiboperationen und Schreibfehler vergleichen.

   Arbeitsdatenträger
   Bei Datenträgern, die anfänglich als Arbeitsdatenträger definiert wurden, überschreibt der Server diese statistischen Daten bei jeder Konsolidierung der Datenträger.
5. Konsolidieren Sie alle gültigen Daten von Datenträgern, die das Ende des Lebenszyklus erreicht haben. Wenn sich die Datenträger in automatisierten Speicherarchiven befinden, entnehmen Sie diese aus dem Datenträgerbestand. Löschen Sie private Datenträger mit dem Befehl **DELETE VOLUME** aus der Datenbank.
6. Stellen Sie sicher, dass Datenträger für die Bandrotation verfügbar sind, damit der Speicherbereich im Speicherpool nicht knapp wird. Mithilfe des Operations Center können Sie die Verfügbarkeit von Arbeitsdatenträgern überwachen. Stellen Sie sicher, dass die Anzahl Arbeitsdatenträger hoch genug ist, um den Bedarf zu decken. Weitere Informationen finden Sie in „Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten" auf Seite 203.

   WORM-Datenträger: WORM-Laufwerke (WORM = Write Once Read Many) können zur Datenträgerverschwendung führen, wenn der Server Transaktionen abbricht, da keine Datenträger zur Ausführung der Sicherungsoperation zur Verfügung stehen. Nachdem Daten vom Server auf WORM-Datenträger geschrieben wurden, kann der Speicherbereich auf den Datenträgern selbst dann nicht wiederverwendet werden, wenn die Transaktionen abgebrochen werden (beispielsweise wenn eine Sicherung wegen Datenträgerknappheit in der Einheit abgebrochen wird). Um die Verschwendung von WORM-Datenträgern zu minimieren, führen Sie die folgenden Aktionen aus:

   a. Stellen Sie sicher, dass die maximale Anzahl Arbeitsdatenträger für den Speicherpool der Einheit mindestens der Anzahl Speicherschächte in dem Speicherarchiv entspricht.
   b. Stellen Sie genügend Datenträger in den Datenträgerbestand der Einheit zurück, um dem erwarteten Bedarf gerecht zu werden.

   Wenn die meisten Sicherungsoperationen kleine Dateien betreffen, kann sich die Steuerung der Transaktionsgröße auf die Verwendung von WORM-Platten auswirken. Kleinere Transaktionen bedeuten,

dass weniger Speicherbereich verschwendet wird, wenn eine Transaktion, wie beispielsweise eine Sicherungsoperation, abgebrochen werden muss. Die Transaktionsgröße wird durch die Serveroption TXNGROUPMAX und die Clientoption TXNBYTELIMIT gesteuert.

Zugehörige Tasks

Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde
Wenn Sie ein Upgrade für alle Bandlaufwerke in einem Speicherarchiv durchführen, können Sie Ihre vorhandenen Maßnahmendefinitionen für die Umlagerung und den Verfall bestehender Daten beibehalten, während Sie die neuen Laufwerke zum Speichern neuer Daten verwenden können.

Serveranforderungen für Datenträger verwalten
IBM Spectrum Protect zeigt allen Verwaltungsbefehlszeilenclients, die im Konsolenmodus gestartet werden, Anforderungen und Statusnachrichten an. Für diese Anforderungsnachrichten ist häufig ein Zeitlimit festgelegt. Erfolgreiche Serveroperationen müssen innerhalb des angegebenen Zeitlimits abgeschlossen werden; andernfalls tritt für die Operation eine Zeitlimitüberschreitung auf.

Zugehörige Informationen

DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)
DELETE VOLUME (Speicherpooldatenträger löschen)
EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)
RECLAIM STGPOOL (Datenträger in einem Speicherpool mit sequenziellem Zugriff konsolidieren)
Option 'txnbytelimit'
Serveroption TXNGROUPMAX

Vorrat an Arbeitsdatenträgern bereithalten

Sie müssen die die maximale Anzahl Arbeitsdatenträger für einen Speicherpool auf einen entsprechend hohen Wert setzen, um dem erwarteten Bedarf gerecht zu werden.

Informationen zu diesem Vorgang

Wenn Sie einen Speicherpool definieren, müssen Sie die maximale Anzahl Arbeitsdatenträger angeben, die der Speicherpool verwenden kann. Der Server fordert bei Bedarf automatisch einen Arbeitsdatenträger an. Wenn die Anzahl Arbeitsdatenträger, die der Server für den Speicherpool verwendet, den angegebenen maximalen Wert überschreitet, kann der Speicherbereich im Speicherpool knapp werden.

Vorgehensweise

Wenn für einen Speicherpool mehr als die maximale Anzahl Arbeitsdatenträger erforderlich ist, können Sie eine oder beide der folgenden Aktionen ausführen:

1. Erhöhen Sie die maximale Anzahl Arbeitsdatenträger, indem Sie den Befehl **UPDATE STGPOOL** unter Angabe des Parameters **MAXSCRATCH** ausgeben.
2. Machen Sie Datenträger für die Wiederverwendung verfügbar, indem Sie die Verfallsverarbeitung und die Konsolidierung ausführen, um Daten auf weniger Datenträgern zu konsolidieren.
   a) Geben Sie den Befehl **EXPIRE INVENTORY** aus, um die Verfallsverarbeitung auszuführen.

      Tipp: Standardmäßig wird dieser Prozess täglich ausgeführt. Sie können auch die Serveroption **EXPINTERVAL** in der Serveroptionsdatei `dsmserv.opt` angeben, um die Verfallsverarbeitung automatisch auszuführen. Der Wert 0 gibt an, dass der Befehl **EXPIRE INVENTORY** zur Ausführung der Verfallsverarbeitung verwendet werden muss.

   b) Geben Sie den Befehl **RECLAIM STGPOOL** aus, um die Konsolidierungsverarbeitung auszuführen.

      Tipp: Sie können auch Konsolidierungsschwellenwerte angeben, wenn Sie den Speicherpool definieren, indem Sie den Befehl **DEFINE STGPOOL** verwenden und den Parameter **RECLAIMPROCESS** angeben.

Nächste Schritte

Wenn weitere Datenträger für zukünftige Sicherungsoperationen benötigt werden, ordnen Sie weiteren Arbeitsdatenträgern mit dem Befehl **LABEL LIBVOLUME** Kennsätze zu.

Zugehörige Tasks

Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten

Wenn Sie einen Speicherpool definieren, der einem automatisierten Speicherarchiv zugeordnet ist, können Sie eine maximale Anzahl Arbeitsdatenträger angeben, die der physischen Kapazität des Speicherarchivs entspricht. Wenn der Server eine größere Anzahl Arbeitsdatenträger für den Speicherpool verwendet, müssen Sie sicherstellen, dass genügend Datenträger verfügbar sind.

Zugehörige Informationen

EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)

LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

RECLAIM STGPOOL (Datenträger in einem Speicherpool mit sequenziellem Zugriff konsolidieren)

UPDATE STGPOOL (Speicherpool aktualisieren)

Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten

Bei Speicherarchiven, die WORM-Datenträger (WORM = Write Once Read Many) enthalten, können Sie den Abbruch von Datenspeicherungstransaktionen verhindern, indem Sie einen Vorrat an Arbeitsdatenträgern oder neuen privaten Datenträgern in dem Speicherarchiv bereithalten. Abgebrochene Transaktionen können zur Folge haben, dass WORM-Datenträger verschwendet werden.

Informationen zu diesem Vorgang

IBM Spectrum Protect bricht eine Transaktion ab, wenn keine Datenträger (private Datenträger oder Arbeitsdatenträger) verfügbar sind, um die Datenspeicherungsoperation auszuführen. Nachdem IBM Spectrum Protect eine Transaktion startet, indem Daten auf einen WORM-Datenträger geschrieben werden, kann der beschriebene Bereich auf dem Datenträger selbst dann nicht wiederverwendet werden, wenn die Transaktion abgebrochen wird.

Angenommen, es sind WORM-Datenträger mit einer Speicherkapazität von jeweils 2,6 GB vorhanden und ein Client beginnt mit der Sicherung einer 12-GB-Datei. Wenn IBM Spectrum Protect keinen fünften Arbeitsdatenträger anfordern kann, nachdem vier Datenträger gefüllt wurden, bricht IBM Spectrum Protect die Sicherungsoperation ab. Die vier Datenträger, die IBM Spectrum Protect bereits mit Daten gefüllt hat, können nicht wiederverwendet werden.

Um das Abbrechen von Transaktionen auf ein Mindestmaß zu reduzieren, müssen genügend Datenträger in dem Speicherarchiv verfügbar sein, um die erwarteten Clientoperationen, wie beispielsweise Sicherungen, ausführen zu können.

Vorgehensweise

1. Stellen Sie sicher, dass der Speicherpool, der dem Speicherarchiv zugeordnet ist, über genügend Arbeitsdatenträger verfügt. Geben Sie den Befehl **UPDATE STGPOOL** unter Angabe des Parameters **MAXSCRATCH** aus.
2. Um dem erwarteten Bedarf gerecht zu werden, stellen Sie eine ausreichende Anzahl Arbeitsdatenträger oder private Datenträger in das Speicherarchiv zurück, indem Sie den Befehl **CHECKIN LIBVOLUME** ausgeben.
3. Um die Transaktionsgröße zu steuern, geben Sie die Serveroption TXNGROUPMAX und die Clientoption TXNBYTELIMIT an. Wenn Ihre Clients hauptsächlich kleine Dateien speichern, kann eine Steuerung der Transaktionsgröße die Verwendung von WORM-Datenträgern beeinflussen. Bei kleineren Transaktionen wird weniger Speicherbereich verschwendet, wenn eine Transaktion, wie beispielsweise eine Sicherung, abgebrochen werden muss.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

UPDATE STGPOOL (Speicherpool aktualisieren)
Option 'txnbytelimit'
Serveroption TXNGROUPMAX

Datenträgerbestand in automatisierten Speicherarchiven verwalten

Der IBM Spectrum Protect-Server verwendet den Datenträgerbestand eines Speicherarchivs, um Arbeitsdatenträger und private Datenträger, die in einem automatisierten Speicherarchiv verfügbar sind, zu verfolgen. Sie müssen sicherstellen, dass der Bestand mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind.

Der Datenträgerbestand des Speicherarchivs entspricht nicht dem Datenträgerbestand jedes Speicherpools. Um dem Datenträgerbestand des Speicherarchivs einen Datenträger hinzuzufügen, stellen Sie einen Datenträger in dieses IBM Spectrum Protect-Speicherarchiv zurück.

Eine Liste der Datenträger im Datenträgerbestand des Speicherarchivs ist möglicherweise nicht mit einer Liste der Datenträger im Datenträgerbestand des Speicherpools für die Einheit identisch. Sie können beispielsweise Arbeitsdatenträger in das Speicherarchiv zurückstellen, diese aber nicht für einen Speicherpool definieren. Wenn Arbeitsdatenträger nicht für Sicherungsoperationen ausgewählt werden, können Sie private Datenträger für einen Speicherpool definieren, diese aber nicht in den Datenträgerbestand für die Einheit zurückstellen.

Um sicherzustellen, dass der Datenträgerbestand für das Serverspeicherarchiv immer korrekt ist, entnehmen Sie Datenträger, um die Datenträger physisch aus einem SCSI--Speicherarchiv zu entfernen. Wenn Sie einen Datenträger entnehmen, der von einem Speicherpool verwendet wird, verbleibt der Datenträger in dem Speicherpool. Wenn Sie den Datenträger bereitstellen müssen, während dieser entnommen ist, wird an der Konsole des Bedieners, der den Mount durchführt, eine Nachricht mit der Aufforderung, den Datenträger zurückzustellen, angezeigt. Wenn die Zurückstelloperation nicht erfolgreich ist, markiert der Server den Datenträger als nicht verfügbar.

Wenn sich ein Datenträger im Datenträgerbestand des Speicherarchivs befindet, können Sie den Status des Datenträgers von SCRATCH (Arbeitsdatenträger) in PRIVATE (privater Datenträger) ändern.

Um zu überprüfen, ob der Datenträgerbestand für das Serverspeicherarchiv mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind, können Sie das Speicherarchiv prüfen. Der Bestand kann inkonsistent werden, wenn Datenträger in das Speicherarchiv gestellt bzw. aus dem Speicherarchiv entfernt werden, ohne dass der Server über Entnahme- oder Zurückstelloperationen für Datenträger informiert wird.

Zugehörige Tasks

Datenträger in ein automatisiertes Speicherarchiv zurückstellen
Sie können einen Datenträger mithilfe des Befehls **CHECKIN LIBVOLUME** in ein automatisiertes Speicherarchiv zurückstellen.

Zugehörige Informationen

AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)

Status eines Datenträgers in einem automatisierten Speicherarchiv ändern

Sie können den Status eines Datenträgers von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) oder umgekehrt ändern.

Vorgehensweise

Um den Status eines Datenträgers zu ändern, geben Sie den Befehl **UPDATE LIBVOLUME** aus.
Um beispielsweise den Status eines Datenträgers mit dem Namen VOL1 in PRIVATE (privater Datenträger) zu ändern, geben Sie den folgenden Befehl aus:

```
update libvolume lib1 vol1 status=private
```

Einschränkungen:

- Sie können den Status eines Datenträgers nicht von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) ändern, wenn der Datenträger zu einem Speicherpool gehört oder in der Protokolldatei für Datenträger definiert ist.
- Private Datenträger müssen vom Administrator definierte Datenträger ohne Daten oder mit ungültigen Daten sein. Sie dürfen keine teilweise beschriebenen Datenträger sein, die aktive Daten enthalten. Die Datenträgerstatistik geht verloren, wenn der Datenträgerstatus geändert wird.

Datenträger aus einem automatisierten Speicherarchiv entfernen

Datenträger können aus einem automatisierten Speicherarchiv entfernt werden, wenn Daten auf einen Datenträger exportiert wurden und die Daten in ein anderes System importiert werden sollen. Möglicherweise sollen auch Datenträger entfernt werden, um Speicherbereich für neue Datenträger zu erstellen.

Informationen zu diesem Vorgang

Standardmäßig wird der Datenträger, der entnommen werden soll, vom Server bereitgestellt und der interne Kennsatz überprüft. Nach der Überprüfung des Kennsatzes entfernt der Server den Datenträger aus dem Datenträgerbestand des Speicherarchivs und versetzt ihn dann in den Eingangs-/Ausgangsport oder die Serviceein-/-ausgabestation des Speicherarchivs. Wenn das Speicherarchiv über keinen Eingangs-/Ausgangsport verfügt, fordert der Server den Bediener, der den Mount durchführt, dazu auf, den Datenträger aus einem Schacht oder einer Einheit in dem Speicherarchiv zu entfernen.

Prozedur

- Um einen Datenträger aus einem automatisierten Speicherarchiv zu entfernen, geben Sie den Befehl **CHECKOUT LIBVOLUME** aus.
- Geben Sie bei automatisierten Speicherarchiven mit mehreren Eingangs-/Ausgangsports den Befehl **CHECKOUT LIBVOLUME** unter Angabe des Parameters **REMOVE=BULK** aus. Der Server gibt den Datenträger am nächsten verfügbaren Eingangs-/Ausgangsport aus.

Nächste Schritte

Wenn Sie einen Datenträger entnehmen, der in einem Speicherpool definiert ist, und der Server später auf den Datenträger zugreifen muss, fordert der Server das Zurückstellen des Datenträgers an. Um Datenträger in ein Speicherarchiv zurückzustellen, geben Sie den Befehl **CHECKIN LIBVOLUME** aus.

Zugehörige Informationen

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)

Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten

Wenn Sie einen Speicherpool definieren, der einem automatisierten Speicherarchiv zugeordnet ist, können Sie eine maximale Anzahl Arbeitsdatenträger angeben, die der physischen Kapazität des Speicherarchivs entspricht. Wenn der Server eine größere Anzahl Arbeitsdatenträger für den Speicherpool verwendet, müssen Sie sicherstellen, dass genügend Datenträger verfügbar sind.

Vorgehensweise

Wenn die Anzahl Arbeitsdatenträger, die der Server für den Speicherpool verwendet, die in der Speicherpooldefinition angegebene Anzahl überschreitet, führen Sie die folgenden Schritte aus:

1. Fügen Sie dem Speicherarchiv Arbeitsdatenträger hinzu, indem Sie den Befehl **CHECKIN LIBVOLUME** ausgeben.

   Tipp: Möglicherweise müssen Sie eine Überlaufposition verwenden, um Datenträger aus dem Speicherarchiv zu entfernen, um Platz für diese Arbeitsdatenträger zu schaffen. Weitere Informationen finden Sie in „Volles Speicherarchiv mit einer Überlaufposition verwalten” auf Seite 206.

2. Erhöhen Sie die maximale Anzahl Arbeitsdatenträger, die einem Speicherpool hinzugefügt werden können, indem Sie den Befehl **UPDATE STGPOOL** unter Angabe des Parameters **MAXSCRATCH** ausgeben.

Nächste Schritte

Da unter Umständen weitere Datenträger für zukünftige Wiederherstellungsoperationen erforderlich sind, ordnen Sie gegebenenfalls zusätzlichen Arbeitsdatenträgern Kennsätze zu und halten Sie diese Datenträger als Vorrat bereit.

Zugehörige Tasks

Vorrat an Arbeitsdatenträgern bereithalten
Sie müssen die die maximale Anzahl Arbeitsdatenträger für einen Speicherpool auf einen entsprechend hohen Wert setzen, um dem erwarteten Bedarf gerecht zu werden.

Volles Speicherarchiv mit einer Überlaufposition verwalten

Mit zunehmendem Speicherbedarf überschreitet die Anzahl Datenträger, die für einen Speicherpool erforderlich sind, unter Umständen die physische Kapazität eines automatisierten Speicherarchivs. Um Speicherbereich für neue Datenträger verfügbar zu machen und vorhandene Datenträger zu überwachen, können Sie eine Überlaufposition für einen Speicherpool definieren.

Informationen zu diesem Vorgang

Der Server überwacht die Datenträger, die in den Überlaufbereich versetzt werden, und macht Speicherschächte für neue Datenträger verfügbar.

Vorgehensweise

1. Erstellen Sie eine Überlaufposition für Datenträger. Definieren oder aktualisieren Sie den Speicherpool, der dem automatisierten Speicherarchiv zugeordnet ist, indem Sie den Befehl **DEFINE STGPOOL** bzw. **UPDATE STGPOOL** unter Angabe des Parameters **OVFLOCATION** ausgeben.
   Um beispielsweise eine Überlaufposition mit dem Namen R00M2948 für einen Speicherpool mit dem Namen ARCHIVEPOOL zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   update stgpool archivepool ovflocation=Room2948
   ```

2. Wenn in dem Speicherarchiv Speicherbereich für Arbeitsdatenträger erstellt werden muss, versetzen Sie volle Datenträger an die Überlaufposition, indem Sie den Befehl **MOVE MEDIA** ausgeben.
   Um beispielsweise alle vollen Datenträger in dem angegebenen Speicherpool aus dem Speicherarchiv zu versetzen, geben Sie den folgenden Befehl aus:

   ```
   move media * stgpool=archivepool
   ```

3. Stellen Sie Arbeitsdatenträger nach Bedarf zurück.

   Einschränkung: Wenn für einen Datenträger ein Eintrag in der Protokolldatei für Datenträger vorhanden ist, kann der Datenträger nicht als Arbeitsdatenträger zurückgestellt werden. Weitere Informationen finden Sie in „Datenträger in ein automatisiertes Speicherarchiv zurückstellen” auf Seite 194.

4. Identifizieren Sie die leeren Arbeitsbänder an der Überlaufposition, indem Sie den Befehl **QUERY MEDIA** ausgeben.
   Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   query media * stg=* whereovflocation=Room2948 wherestatus=empty
   ```

5. Wenn der Server weitere Datenträger anfordert, lokalisieren Sie Datenträger und stellen Sie diese von der Überlaufposition zurück.

   Um Datenträger an einer Überlaufposition zu finden, geben Sie den Befehl **QUERY MEDIA** aus. Sie können den Befehl **QUERY MEDIA** auch verwenden, um Befehle zum Zurückstellen von Datenträgern zu generieren.

Um beispielsweise die Datenträger an der Überlaufposition aufzulisten und gleichzeitig die Befehle zum Zurückstellen dieser Datenträger in das Speicherarchiv zu generieren, geben Sie einen ähnlichen Befehl wie in dem folgenden Beispiel aus:

```
query media format=cmd stgpool=archivepool whereovflocation=Room2948
cmd="checkin libvol autolib &vol status=private"
cmdfilename="\storage\move\media\checkin.vols"
```

Tipps:

- Mountanforderungen vom Server umfassen den Standort der Datenträger.
- Um die Anzahl Tage anzugeben, die verstreichen müssen, bevor die Datenträger für die Verarbeitung auswählbar sind, geben Sie den Befehl **UPDATE STGPOOL** unter Angabe des Parameters **REUSEDELAY** aus.
- Die Datei, die die generierten Befehle enthält, kann mit dem IBM Spectrum Protect-Befehl **MACRO** ausgeführt werden.

Zugehörige Informationen

MOVE MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff versetzen)
QUERY MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff abfragen)
UPDATE STGPOOL (Speicherpool aktualisieren)

Datenträgerbestand in einem Speicherarchiv prüfen

Sie können ein automatisiertes Speicherarchiv prüfen, um sicherzustellen, dass der Datenträgerbestand des Speicherarchivs mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind. Die Prüfung eines Speicherarchivs bietet sich an, wenn der Datenträgerbestand des Speicherarchivs aufgrund manueller Versetzungen der Datenträger in dem Speicherarchiv oder aufgrund von Datenbankproblemen nicht mehr korrekt ist.

Vorgehensweise

1. Stellen Sie sicher, dass keine Datenträger in den Speicherarchivlaufwerken bereitgestellt sind. Wenn Datenträger im Status IDLE (Inaktiv) bereitgestellt sind, geben Sie den Befehl **DISMOUNT VOLUME** aus, um die Bereitstellung dieser Datenträger aufzuheben.
2. Prüfen Sie den Datenträgerbestand, indem Sie den Befehl **AUDIT LIBRARY** ausgeben. Führen Sie eine der folgenden Aktionen aus:
   - Wenn das Speicherarchiv über einen Barcodeleser verfügt, können Sie Zeit sparen, indem Sie Datenträger mithilfe des Barcodelesers identifizieren. Um beispielsweise das Speicherarchiv TAPELIB mithilfe seines Barcodelesers zu prüfen, geben Sie den folgenden Befehl aus:

     ```
     audit library tapelib checklabel=barcode
     ```

   - Wenn das Speicherarchiv über keinen Barcodeleser verfügt, geben Sie den Befehl **AUDIT LIBRARY** ohne Angabe von **CHECKLABEL=BARCODE** aus. Jeder Datenträger wird vom Server zur Überprüfung seines Kennsatzes bereitgestellt. Nachdem der Kennsatz überprüft wurde, führt der Server die Überprüfung für alle verbleibenden Datenträger aus.

Ergebnisse

Der Server löscht fehlende Datenträger aus dem Bestand und aktualisiert die Positionen von Datenträgern, die seit der letzten Prüfung versetzt wurden.

Einschränkung: Während einer Prüfoperation kann der Server dem Bestand keine neuen Datenträger hinzufügen.

Zugehörige Tasks

Banddatenträgern Kennsätze zuordnen
Sie müssen Banddatenträgern Kennsätze zuordnen, bevor diese vom Server verwendet werden können.

Zugehörige Informationen

AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
DISMOUNT VOLUME (Datenträger nach Datenträgername abhängen)

Teilweise beschriebene Datenträger

Teilweise beschriebene Datenträger sind immer private Datenträger; dies ist auch dann der Fall, wenn ihr Status vor dem Bereitstellen durch den Server PRIVATE lautete. Der Server protokolliert den ursprünglichen Status von Arbeitsdatenträgern und versetzt diese wieder in den Arbeitsstatus, wenn sie leer sind.

Mit Ausnahme von Datenträgern in automatisierten Speicherarchiven erkennt der Server einen Arbeitsdatenträger erst nach dessen Bereitstellung. Der Datenträgerstatus ändert sich dann in PRIVATE und der Datenträger wird automatisch als Teil des Speicherpools definiert, für den die Mountanforderung erfolgte.

Zugehörige Tasks

Status eines Datenträgers in einem automatisierten Speicherarchiv ändern
Sie können den Status eines Datenträgers von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) oder umgekehrt ändern.

Operationen für gemeinsam genutzte Speicherarchive

Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die physisch durch SCSI-Speicherarchive dargestellt werden. Das physische Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist. IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den IBM Spectrum Protect-Speicherarchivmanager-Server.

Der Speicherarchivclient kontaktiert den Speicherarchivmanager, wenn der Speicherarchivmanager startet und die Speichereinheit initialisiert wird oder nachdem ein Speicherarchivmanager für einen Speicherarchivclient definiert wurde. Der Speicherarchivclient bestätigt, dass der kontaktierte Server der Speicherarchivmanager für die angegebene Speicherarchiveinheit ist. Der Speicherarchivclient vergleicht außerdem die Laufwerkdefinitionen mit dem Speicherarchivmanager auf Konsistenz. Der Speicherarchivclient kontaktiert den Speicherarchivmanager für jede der folgenden Operationen:

Datenträgermount
Ein Speicherarchivclient sendet eine Zugriffsanforderung für einen bestimmten Datenträger in der gemeinsam genutzten Speicherarchiveinheit an den Speicherarchivmanager. Bei einem Arbeitsdatenträger gibt der Speicherarchivclient keinen Datenträgernamen an. Wenn der Speicherarchivmanager nicht auf den angeforderten Datenträger zugreifen kann oder wenn keine Arbeitsdatenträger verfügbar sind, weist der Speicherarchivmanager die Mountanforderung zurück. Wenn der Mount erfolgreich ist, gibt der Speicherarchivmanager den Namen des Laufwerks zurück, in dem der Datenträger bereitgestellt ist.

Datenträgerfreigabe
Wenn ein Speicherarchivclient nicht mehr auf einen Datenträger zugreifen muss, teilt er dem Speicherarchivmanager mit, dass der Datenträger wieder als Arbeitsdatenträger verwendet werden kann. Die Datenbank des Speicherarchivmanagers wird mit der neuen Position des Datenträgers, der sich jetzt im Bestand des Speicherarchivservers befindet, aktualisiert. Der Datenträger wird aus dem Datenträgerbestand des Speicherarchivclients gelöscht.

Tabelle 35 auf Seite 209 zeigt die Interaktion zwischen Speicherarchivclients und dem Speicherarchivmanager bei der Verarbeitung von IBM Spectrum Protect-Operationen.

Tabelle 35. Wie SAN-fähige Server IBM Spectrum Protect-Operationen verarbeiten		
Operation **(Befehl)**	**Speicherarchivmanager**	**Speicherarchivclient**
Datenträger im Speicherarchiv abfragen (**QUERY LIBVOLUME**)	Zeigt die in das Speicherarchiv zurückgestellten Datenträger an. Bei privaten Datenträgern wird außerdem der Eignerserver angezeigt.	Nicht zutreffend
Speicherarchivdatenträger zurückstellen und entnehmen (**CHECKIN LIBVOLUME**, **CHECKOUT LIBVOLUME**)	Sendet die Befehle an die Speicherarchiveinheit.	Nicht zutreffend Wenn eine Zurückstelloperation aufgrund einer Clientzurückschreibungsoperation erforderlich ist, wird eine Anforderung an den Speicherarchivmanager-Server gesendet.
Datenträger und DRM-Datenträger versetzen (**MOVE MEDIA**, **MOVE DRMEDIA**)	Nur gültig für Datenträger, die vom Speicherarchivmanager-Server verwendet werden.	Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an. Generiert einen Entnahmeprozess auf dem Speicherarchivmanager-Server.
Speicherarchivbestand prüfen (**AUDIT LIBRARY**)	Synchronisiert den Bestand mit der Speicherarchiveinheit.	Synchronisiert den Bestand mit dem Speicherarchivmanager-Server.
Datenträger im Speicherarchiv einen Kennsatz zuordnen (**LABEL LIBVOLUME**)	Ordnet Datenträgern Kennsätze zu und stellt Datenträger zurück.	Nicht zutreffend
Bereitstellung eines Datenträgers aufheben (**DISMOUNT VOLUME**)	Sendet die Anforderung an die Speicherarchiveinheit.	Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an.
Datenträger abfragen (**QUERY VOLUME**)	Prüft, ob der anfordernde Speicherarchivclient Eigner des Datenträgers ist und ob sich der Datenträger in der Speicherarchiveinheit befindet.	Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an.

Serveranforderungen für Datenträger verwalten

IBM Spectrum Protect zeigt allen Verwaltungsbefehlszeilenclients, die im Konsolenmodus gestartet werden, Anforderungen und Statusnachrichten an. Für diese Anforderungsnachrichten ist häufig ein Zeitlimit festgelegt. Erfolgreiche Serveroperationen müssen innerhalb des angegebenen Zeitlimits abgeschlossen werden; andernfalls tritt für die Operation eine Zeitlimitüberschreitung auf.

Informationen zu diesem Vorgang

Verwenden Sie bei automatisierten Speicherarchiven die Befehle **CHECKIN LIBVOLUME** und **LABEL LIBVOLUME**, um Kassetten in Schächte einzulegen. Wenn Sie einen Wert für den Parameter **WAITTIME** angeben, wird eine Antwortnachricht angezeigt. Wenn der Wert des Parameters 0 ist, ist keine Antwort

erforderlich. Wenn Sie den Befehl **CHECKOUT LIBVOLUME** ausgeben, müssen Sie Kassetten in Schächte einlegen und es wird in jedem Fall eine Antwortnachricht angezeigt.

Prozedur

- Die folgende Tabelle enthält Informationen zur Handhabung verschiedener Serverdatenträgertasks.

Task	Details
Verwaltungsclient für Mountnachrichten verwenden	Der Server sendet Statusnachrichten für Mountanforderungen an die Serverkonsole und an alle Verwaltungsbefehlszeilenclients im Mountmodus oder Konsolenmodus. Um einen Verwaltungsbefehlszeilenclient im Mountmodus zu starten, geben Sie im Verwaltungsbefehlszeilenclient den Befehl **dsmadmc -mountmode** aus.
Nachrichten zu automatisierten Speicherarchiven empfangen	Sie können Mountnachrichten und Fehlernachrichten zu automatisierten Speicherarchiven auf Verwaltungsbefehlszeilenclients im Mountmodus oder Konsolenmodus anzeigen. Mountnachrichten werden an das Speicherarchiv und nicht an einen Bediener gesendet. Nachrichten zu Problemen mit dem Speicherarchiv werden an die Mountnachrichtenwarteschlange gesendet.
Informationen zu anstehenden Bedieneranforderungen abrufen	Um Informationen zu anstehenden Bedieneranforderungen abzurufen, geben Sie den Befehl **QUERY REQUEST** aus oder zeigen Sie die Mountnachrichtenwarteschlange auf einem Verwaltungsbefehlszeilenclient an, der im Mountmodus gestartet wurde. Wenn Sie den Befehl **QUERY REQUEST** ausgeben, zeigt der Server angeforderte Aktionen und die verbleibende Zeit, bevor das Zeitlimit für die Anforderungen überschritten wird.
Bedieneranforderungen beantworten	Wenn der Server eine explizite Antwort auf eine abgeschlossene Mountanforderung erfordert, verwenden Sie den Befehl **REPLY**. Der Parameter *Anforderungsnummer* gibt die Anforderungsidentifikationsnummer an, die dem Server anzeigt, welche anstehende Bedieneranforderung abgeschlossen ist. Diese dreistellige Zahl wird immer in der Anforderungsnachricht angezeigt.
Bedieneranforderung abbrechen	Um eine Mountanforderung für ein Speicherarchiv abzubrechen, geben Sie den Befehl **CANCEL REQUEST** aus. Bei den meisten Anforderungen, die automatisierten SCSI-Speicherarchiven zugeordnet sind, muss ein Bediener eine Hardware- oder Systemaktion ausführen, um den angeforderten Mount abzubrechen. Bei derartigen Anforderungen wird der Befehl **CANCEL REQUEST** nicht vom Server akzeptiert. Der Befehl **CANCEL REQUEST** muss die Anforderungsidentifikationsnummer enthalten. Diese Nummer ist in die Anforderungsnachricht eingeschlossen. Wenn der angeforderte Datenträger als **UNAVAILABLE** markiert werden soll, geben Sie den Befehl **CANCEL REQUEST** unter Angabe des Parameters **PERMANENT** aus. Wenn Sie den Parameter **PERMANENT** angeben, versucht der Server nicht, den angeforderten Datenträger erneut bereitzustellen. Dies ist beispielsweise hilfreich, wenn sich der Datenträger an einem fernen Standort befindet oder aus einem anderen Grund nicht verfügbar ist.

Task	Details
Anforderung zum Zurückstellen eines Datenträgers beantworten	Wenn der Server einen bestimmten Datenträger, der in einem automatisierten Speicherarchiv bereitgestellt werden soll, nicht finden kann, fordert der Server den Bediener zum Zurückstellen des Datenträgers auf. Wenn der angeforderte Datenträger verfügbar ist, legen Sie den Datenträger in das Speicherarchiv ein und stellen Sie ihn zurück. Weitere Informationen finden Sie in „Datenträger in ein automatisiertes Speicherarchiv zurückstellen" auf Seite 194. Wenn der angeforderte Datenträger nicht verfügbar ist, aktualisieren Sie den Zugriffsmodus des Datenträgers, indem Sie den Befehl **UPDATE VOLUME** unter Angabe des Parameters **ACCESS=UNAVAILABLE** ausgeben. Brechen Sie dann die Zurückstellanforderung mit dem Befehl **CANCEL REQUEST** ab. Brechen Sie nicht den Clientprozess ab, der die Anforderung zur Folge hatte! Rufen Sie mithilfe des Befehls **QUERY REQUEST** die ID der Anforderung ab, die abgebrochen werden soll. Wenn Sie nicht innerhalb der für die Einheitenklasse des Speicherpools angegebene Mountwartezeit auf die Zurückstellanforderung des Servers antworten, markiert der Server den Datenträger als nicht verfügbar.
Bereitgestellte Datenträger bestimmen	Um einen Bericht zu allen Datenträgern anzufordern, die momentan für die Verwendung durch den Server bereitgestellt sind, geben Sie den Befehl **QUERY MOUNT** aus. Der Bericht zeigt, welche Datenträger bereitgestellt sind, welche Laufwerke auf die Datenträger zugegriffen haben und ob die Datenträger im Gebrauch sind.
Bereitstellung inaktiver Datenträger aufheben	Wenn ein Datenträger inaktiv ist, hebt der Server die Bereitstellung des Datenträgers nicht sofort auf; der Datenträger bleibt vielmehr so lange bereitgestellt, wie im Parameter für den Mount-Aufbewahrungszeitraum für die Einheitenklasse angegeben ist. Durch die Verwendung eines Mount-Aufbewahrungszeitraums kann die Zugriffszeit reduziert werden, wenn Datenträger wiederholt verwendet werden. Um die Bereitstellung eines inaktiven Datenträgers für das Laufwerk aufzuheben, in dem er bereitgestellt ist, geben Sie den Befehl **DISMOUNT VOLUME** aus. Informationen zum Festlegen des Mount-Aufbewahrungszeitraums finden Sie in „Steuern, wie lange ein Datenträger bereitgestellt bleibt" auf Seite 137.

Zugehörige Informationen

QUERY REQUEST (Eine oder mehrere anstehende Mountanforderungen abfragen)

Bandlaufwerke verwalten

Sie können Bandlaufwerke abfragen, aktualisieren und löschen. Außerdem können Sie Bandlaufwerke reinigen und Bandlaufwerkverschlüsselung und Datenprüfung konfigurieren.

Laufwerke aktualisieren

Sie können die Attribute einer Laufwerkdefinition ändern, um ein Laufwerk offline zu schalten oder ein Laufwerk zu rekonfigurieren.

Informationen zu diesem Vorgang

Sie können die folgenden Attribute eines Laufwerks ändern:

- Die Elementadresse, wenn sich das Laufwerk in einem SCSI-Speicherarchiv befindet
- Die Reinigungshäufigkeit
- Den Laufwerkstatus: ONLINE oder OFFLINE

Einschränkung: Wenn ein Laufwerk im Gebrauch ist, können Sie die Elementnummer oder den Einheitennamen nicht ändern. Anweisungen zum Offlineschalten von Laufwerken finden Sie in „Bandlaufwerke offline schalten" auf Seite 212.

Wenn ein Datenträger im Laufwerk bereitgestellt, aber inaktiv ist, kann seine Bereitstellung explizit aufgehoben werden. Anweisungen zum Aufheben der Bereitstellung inaktiver Datenträger finden Sie in „Serveranforderungen für Datenträger verwalten" auf Seite 209.

Prozedur

- Ändern Sie die Elementadresse eines Laufwerks, indem Sie den Befehl **UPDATE DRIVE** ausgeben. Ändern Sie beispielsweise in einem Speicherarchiv mit dem Namen AUTO die Elementadresse von DRIVE3 in 119, indem Sie den folgenden Befehl ausgeben:

```
update drive auto drive3 element=119
```

- Ändern Sie den Einheitennamen eines Laufwerks, indem Sie den Befehl **UPDATE PATH** ausgeben. Um beispielsweise den Einheitennamen eines Laufwerks mit dem Namen DRIVE3 zu ändern, geben Sie den folgenden Befehl aus:

```
AIX update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/rmt0
```

```
Linux update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/IBMtape0
```

```
Windows update path server1 drive3 srctype=server desttype=drive library=scsilib
  device=mt3.0.0.0
```

Zugehörige Informationen

UPDATE DRIVE (Laufwerk aktualisieren)

UPDATE PATH (Pfad ändern)

Bandlaufwerke offline schalten

Sie können ein Bandlaufwerk offline schalten, während es im Gebrauch ist. Sie können ein Laufwerk beispielsweise zur Ausführung der Wartung offline schalten.

Informationen zu diesem Vorgang

Wenn Sie den Status eines Laufwerks in OFFLINE ändern, während es im Gebrauch ist, schließt der Server die Verarbeitung des Bands im Laufwerk ab und stoppt dann die Verwendung des Laufwerks. Wenn das Band, das im Gebrauch war, jedoch Teil einer Serie von Bändern für eine einzelne Transaktion war, ist das Laufwerk nicht mehr verfügbar, um die Verarbeitung der Serie abzuschließen. Wenn keine anderen Laufwerke verfügbar sind, schlägt die Transaktion unter Umständen fehl.

Prozedur

- Um den Status eines Laufwerks zu ändern, geben Sie den Befehl **UPDATE DRIVE** unter Angabe des Parameters **ONLINE** aus. Um beispielsweise das Laufwerk DRIVE3 im Speicherarchiv MANLIB zu aktualisieren und das Laufwerk offline zu schalten, geben Sie den folgenden Befehl aus:

```
update drive manlib drive3 online=no
```

Einschränkung: Geben Sie keine weiteren optionalen Parameter an, wenn Sie den Parameter **ONLINE** angeben. Andernfalls wird das Laufwerk nicht aktualisiert und der Befehl schlägt fehl, wenn das Laufwerk im Gebrauch ist.

Ergebnisse

Wenn Sie alle Laufwerke in einem Speicherarchiv mit dem Status OFFLINE aktualisieren, schlagen Prozesse, die einen Speicherarchivmountpunkt erfordern, fehl.

Der aktualisierte Status des Laufwerks wird selbst dann beibehalten, wenn der Server angehalten und erneut gestartet wird. Ist ein Laufwerk als offline markiert, wenn der Server erneut gestartet wird, wird eine Warnung ausgegeben, die angibt, dass das Laufwerk manuell online geschaltet werden muss.

Zugehörige Informationen

UPDATE DRIVE (Laufwerk aktualisieren)

Datenprüfung während Schreib-/Leseoperationen auf Band

Um Daten zu prüfen und beschädigte Daten zu identifizieren, können Sie eine Funktion verwenden, die als 'Schutz logischer Blöcke' bezeichnet wird. Wenn Sie den Schutz logischer Blöcke verwenden, fügt IBM Spectrum Protect einen Wert für zyklische Blockprüfung (CRC = Cyclic Redundancy Check) am Ende jedes logischen Blocks mit Daten ein, während die Daten auf Band geschrieben werden.

Der Schutz logischer Blöcke ermöglicht es Ihnen, Fehler zu identifizieren, die auftreten, während Daten auf Band geschrieben werden und während Daten über das Speicherbereichsnetz vom Bandlaufwerk an IBM Spectrum Protect übertragen werden. Laufwerke, die den Schutz logischer Blöcke unterstützen, prüfen Daten während Lese- und Schreiboperationen. Der IBM Spectrum Protect-Server prüft Daten während Leseoperationen.

Wenn die Prüfung durch das Laufwerk während Schreiboperationen fehlschlägt, kann dies darauf hinweisen, dass Daten während der Übertragung auf Band beschädigt wurden. In diesem Fall schlägt die Schreiboperation für den IBM Spectrum Protect-Server fehl. Sie müssen die Operation erneut starten, um fortfahren zu können. Wenn die Prüfung durch das Laufwerk während Leseoperationen fehlschlägt, kann dies darauf hinweisen, dass die Banddatenträger beschädigt sind. Wenn die Prüfung durch den IBM Spectrum Protect-Server während Leseoperationen fehlschlägt, kann dies darauf hinweisen, dass die Daten während der Übertragung vom Bandlaufwerk beschädigt wurden; der Server versucht, die Operation erneut auszuführen. Wenn die Prüfung durchgängig fehlschlägt, gibt der IBM Spectrum Protect-Server eine Fehlernachricht aus, die auf Hardwarefehler oder Verbindungsprobleme hinweist.

Wenn der Schutz logischer Blöcke auf einem Bandlaufwerk inaktiviert ist oder das Laufwerk den Schutz logischer Blöcke nicht unterstützt, kann der IBM Spectrum Protect-Server geschützte Daten nur lesen. Die Daten werden jedoch nicht geprüft.

Der Schutz logischer Blöcke hat eine höhere Priorität als die zyklische Blockprüfung, die Sie beim Definieren oder Aktualisieren einer Speicherpooldefinition angeben können. Wenn Sie die zyklische Blockprüfung für einen Speicherpool angeben, werden Daten nur während Datenträgerprüfoperationen geprüft. Fehler werden identifiziert, nachdem die Daten auf Band geschrieben wurden.

Einschränkungen:

- Sie können den Schutz logischer Blöcke nicht für sequenzielle Daten wie Sicherungsgruppen und Datenbanksicherungen verwenden.
- Die CRC-Prüfung hat Auswirkungen auf die Leistung, da mehr Prozessorauslastung auf dem Client und dem Server erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen.
- Ändern Sie bei einem Arbeitsdatenträger, wenn Sie den Schutz logischer Blöcke für Schreib-/Leseoperationen (**LBPROTECT=READWRITE**) angeben, den Parameterwert nicht, nachdem Daten auf den Datenträger geschrieben wurden. Das Ändern des Parameterwerts während des Lebenszyklus des Datenträgers auf dem IBM Spectrum Protect-Server wird nicht unterstützt.

Laufwerke, die den Schutz logischer Blöcke unterstützen

Der Schutz logischer Blöcke ist nur für die Einheitentypen 3592, LTO und ECARTRIDGE verfügbar. 3592-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM TS1130, TS1140 und spätere Generationen. LTO-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM LTO-5-Laufwerke und unterstützte LTO-6-Laufwerke. Oracle StorageTek-Laufwerke, die diese Art von Schutz bereitstellen, umfassen Laufwerke mit dem T10000C-Format und dem T10000D-Format.

In der folgenden Tabelle sind die Datenträger und Formate aufgeführt, die Sie zusammen mit Laufwerken verwenden können, die den Schutz logischer Blöcke unterstützen.

Laufwerk	Banddatenträger	Laufwerkformate
IBM TS1130	3592 Generation 2	3592-3 und 3592-3C
IBM TS1140	3592 Generation 2 3592 Generation 3	Generation 2: 3592-3 und 3592-3C Generation 3: 3592-4 und 3592-4C
IBM TS1150	3592 Generation 3 3592 Generation 4	Generation 4: 3592-5 und 3592-5C
IBM LTO-5	LTO-5	Ultrium 5 und Ultrium 5C
IBM LTO-6	LTO-6 LTO-5	Ultrium 6 und Ultrium 6C Ultrium 5 und Ultrium 5C
IBM LTO-7	LTO-7 LTO-6	Ultrium 7 und Ultrium 7C Ultrium 6 und Ultrium 6C
Oracle T10000C	Oracle StorageTek T10000 T2	T10000C und T10000C-C
Oracle T10000D	Oracle StorageTek T10000 T2	T10000D und T10000D-C

Tipps:

- Um den Schutz logischer Blöcke für einen Banddatenträger zu aktivieren und den Datenträger dann zum Sichern von Daten wiederzuverwenden, müssen Sie den Schutz logischer Blöcke für die Einheitenklasse und das Laufwerk aktivieren.
- Bei einem 3592-, LTO- oder Oracle StorageTek-Laufwerk, das keinen Schutz logischer Blöcke bereitstellen kann, können Sie für das Laufwerk ein Upgrade mit Firmware durchführen, die Schutz logischer Blöcke bereitstellt.

Der Schutz logischer Blöcke ist für Laufwerke in Speicherarchiven des Typs SCSI verfügbar. Aktuelle Informationen zur Unterstützung für den Schutz logischer Blöcke finden Sie in Technote 1568108.

Um den Schutz logischer Blöcke für Schreiboperationen verwenden zu können, müssen alle Laufwerke in einem Speicherarchiv den Schutz logischer Blöcke unterstützen. Wenn ein Laufwerk keinen Schutz logischer Blöcke bereitstellen kann, werden Datenträger mit Schreib-/Lesezugriff nicht bereitgestellt. Der Server kann jedoch mithilfe des Laufwerks Datenträger mit Lesezugriff bereitstellen. Die geschützten Daten werden vom IBM Spectrum Protect-Server gelesen und geprüft, wenn der Schutz logischer Blöcke für Schreib-/Leseoperationen aktiviert ist.

Schutz logischer Blöcke aktivieren und inaktivieren

Sie können den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben. Es ist auch möglich, den Schutz logischer Blöcke zu inaktivieren. Standardmäßig ist der Schutz logischer Blöcke wegen der Auswirkungen, die die zyklische Blockprüfung auf dem Server und dem Bandlaufwerk auf die Leistung hat, inaktiviert.

Informationen zu diesem Vorgang

Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden. Wenn Sie die Einstellung für den Schutz logischer Blöcke ändern, gilt die Änderung nur für leere Datenträger. Datenträger, die mit Daten gefüllt werden, und volle Datenträger behalten ihren Status für den Schutz logischer Blöcke bei, bis sie leer und zum erneuten Füllen bereit sind. Wenn Sie beispielsweise den Schutz logischer Blöcke inaktivieren und der Server einen Datenträger auswählt, der einer Einheitenklasse zugeordnet ist, für die der Schutz logischer Blöcke definiert ist, schreibt der Server weiterhin geschützte Daten auf den Datenträger.

Einschränkung: Der Schutz logischer Blöcke ist nur für bestimmte Einheitentypen verfügbar. Weitere Informationen finden Sie in „Laufwerke, die den Schutz logischer Blöcke unterstützen" auf Seite 214.

Vorgehensweise

1. Um den Schutz logischer Blöcke für die Einheitentypen 3592, LTO und ECARTRIDGE zu aktivieren, geben Sie den Befehl **DEFINE DEVCLASS** oder den Befehl **UPDATE DEVCLASS** unter Angabe des Parameters **LBPROTECT** aus.
   Um beispielsweise den Schutz logischer Blöcke während Lese- und Schreiboperationen für eine Einheitenklasse 3592 mit dem Namen 3592_lbprotect anzugeben, geben Sie den folgenden Befehl aus:

   ```
   define devclass 3592_lbprotect library=3594 lbprotect=readwrite
   ```

   Tipps:

   - Wenn Sie den Wert des Parameters **LBPROTECT** von NO in READWRITE oder WRITEONLY ändern und der Server einen Datenträger auswählt, der mit Daten gefüllt wird und für den kein Schutz logischer Blöcke für Schreiboperationen definiert ist, gibt der Server jedes Mal eine Nachricht aus, wenn der Datenträger bereitgestellt wird. Die Nachricht gibt an, dass Daten auf den Datenträger ohne Schutz logischer Blöcke geschrieben werden. Soll die Anzeige dieser Nachricht verhindert werden oder soll IBM Spectrum Protect nur Daten mit Schutz logischer Blöcke auf den Datenträger schreiben, ändern Sie den Zugriff für Datenträger ohne Schutz logischer Blöcke, die mit Daten gefüllt werden, in Lesezugriff.
   - Um die Leistung zu verbessern, geben Sie den Parameter **CRCDATA** nicht im Befehl **DEFINE STGPOOL** oder **UPDATE STGPOOL** an.
   - Wenn Daten während Leseoperationen sowohl vom Laufwerk als auch vom IBM Spectrum Protect-Server geprüft werden, kann dies die Serverleistung während Zurückschreibungs- und Abrufoperationen verschlechtern. Um die für Zurückschreibungs- und Abrufoperationen erforderliche Zeit zu verringern, ändern Sie die Einstellung des Parameters **LBPROTECT** von READWRITE in WRITEONLY. Nachdem die Daten zurückgeschrieben oder abgerufen wurden, können Sie den Parameter **LBPROTECT** auf READWRITE zurücksetzen.
2. Um den Schutz logischer Blöcke zu inaktivieren, geben Sie den Befehl **DEFINE DEVCLASS** oder den Befehl **UPDATE DEVCLASS** unter Angabe des Parameters **LBPROTECT=NO** aus.

   Einschränkung: Wenn der Schutz logischer Blöcke inaktiviert ist, schreibt der Server keine Daten auf ein leeres Band, für das der Schutz logischer Blöcke definiert ist. Wenn jedoch ein Datenträger, der mit Daten gefüllt wird und für den der Schutz logischer Blöcke definiert ist, ausgewählt wird, schreibt der Server weiterhin Daten auf den Datenträger, für den der Schutz logischer Blöcke definiert ist. Um zu verhindern, dass der Server Daten auf Bänder mit Schutz logischer Blöcke schreibt, ändern Sie den Zugriff für Datenträger, die mit Daten gefüllt werden und für die der Schutz logischer Blöcke definiert ist, in Lesezugriff. Wenn Daten gelesen werden, werden die Ergebnisse der zyklischen Blockprüfung nicht vom Laufwerk oder Server geprüft.

   Wenn in einem Katastrophenfall der Standort zur Wiederherstellung über keine Laufwerke verfügt, die den Schutz logischer Blöcke unterstützen, müssen Sie den Parameter **LBPROTECT=NO** angeben. Wenn die Bandlaufwerke für Schreiboperationen verwendet werden, müssen Sie den Datenträgerzugriff für Datenträger mit geschützten Daten in Lesezugriff ändern, um eine Verwendung der Datenträger durch den Server zu verhindern.

Wenn der Server den Schutz logischer Blöcke aktivieren muss, gibt der Server eine Fehlernachricht aus, die angibt, dass das Laufwerk den Schutz logischer Blöcke nicht unterstützt.

Nächste Schritte

Um festzustellen, ob für einen Datenträger der Schutz logischer Blöcke definiert ist, geben Sie den Befehl **QUERY VOLUME** aus und prüfen Sie den Wert im Feld `Schutz logischer Blöcke`.

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

QUERY VOLUME (Speicherpooldatenträger abfragen)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

UPDATE STGPOOL (Speicherpool aktualisieren)

Schreib-/Leseoperationen für Datenträger mit Schutz logischer Blöcke

Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden.

Wenn Sie mit dem Befehl **UPDATE DEVCLASS** die Einstellung für den Schutz logischer Blöcke ändern, gilt die Änderung nur für leere Datenträger. Datenträger, die mit Daten gefüllt werden, und volle Datenträger behalten ihren Status für den Schutz logischer Blöcke bei, bis sie leer und zum erneuten Füllen bereit sind.

Angenommen, Sie ändern den Wert des Parameters **LBPROTECT** von `READWRITE` in `NO`. Wenn der Server einen Datenträger auswählt, der der Einheitenklasse zugeordnet ist und über Schutz logischer Blöcke verfügt, schreibt der Server weiterhin geschützte Daten auf den Datenträger.

Tipps:

- Wenn ein Laufwerk den Schutz logischer Blöcke nicht unterstützt, können Datenträger mit Schutz logischer Blöcke für Schreiboperationen nicht bereitgestellt werden. Um zu verhindern, dass der Server den geschützten Datenträger für Schreiboperationen bereitstellt, ändern Sie den Datenträgerzugriff in Lesezugriff. Inaktivieren Sie außerdem den Schutz logischer Blöcke, um zu verhindern, dass der Server die Funktion auf dem Bandlaufwerk aktiviert.
- Wenn ein Laufwerk den Schutz logischer Blöcke nicht unterstützt und der Schutz logischer Blöcke inaktiviert ist, liest der Server Daten von geschützten Datenträgern. Die Daten werden jedoch nicht vom Server und dem Bandlaufwerk geprüft.

Zugehörige Informationen

QUERY VOLUME (Speicherpooldatenträger abfragen)

UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Speicherpoolverwaltung in einem Bandarchiv

Um geschützte und ungeschützte Daten in einem Speicherarchiv zu mischen, müssen Sie unterschiedliche Einheitenklassen und unterschiedliche Speicherpools erstellen, um die Daten voneinander zu trennen. Wenn eine Einheitenklasse geschützten Daten zugeordnet ist, können Sie den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben.

Um Einheitenklassen und Speicherpools für ein TS3500-Speicherarchiv mit LTO-5-Laufwerken für geschützte und ungeschützte Daten zu definieren, können Sie eine Folge von Befehlen ausgeben wie in dem folgenden Beispiel gezeigt:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

Zugehörige Informationen

DEFINE DEVCLASS (Einheitenklasse definieren)

DEFINE LIBRARY (Speicherarchiv definieren)

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Bandlaufwerke reinigen

Die Steuerung der Bandlaufwerkreinigung kann durch den Server erfolgen. Der Server kann steuern, wie Bandlaufwerke in SCSI-Speicherarchiven gereinigt werden.

Informationen zu diesem Vorgang

Um Bandlaufwerke reinigen zu können, müssen Sie über Systemberechtigung oder uneingeschränkte Speicherberechtigung verfügen. Bei automatisierten Speicherarchiven können Sie die Reinigung automatisieren, indem Sie die Häufigkeit der Reinigungsoperationen angeben und eine Reinigungskassette in den Datenträgerbestand des Speicherarchivs zurückstellen. IBM Spectrum Protect stellt die Reinigungskassette wie angegeben bereit. Wenn Sie planen, bei einem SCSI-Speicherarchiv, das in seiner Einheitenhardware die Unterstützung für die automatische Laufwerkreinigung bereitstellt, die servergesteuerte Laufwerkreinigung zu verwenden, sind spezielle Hinweise zu berücksichtigen.

Tipp: Wenn ein automatisiertes Bandarchiv die Speicherarchivlaufwerkreinigung unterstützt, stellen Sie sicher, dass die Funktion aktiviert ist.

Sie können die vorzeitige Abnutzung der Schreib-/Leseköpfe von Laufwerken verhindern, indem Sie die Speicherarchivreinigungsfunktionen Ihres Einheitenherstellers verwenden.

Bei Laufwerken und Speicherarchiven unterschiedlicher Hersteller bestehen Unterschiede in der Handhabung von Reinigungskassetten und in der Art und Weise, wie das Vorhandensein einer Reinigungskassette in einem Laufwerk zurückgemeldet wird. Möglicherweise kann ein Laufwerk, das eine Reinigungskassette enthält, vom Einheitentreiber nicht geöffnet werden. Die von Einheiten ausgegebenen Prüfcodes und Fehlercodes für die Laufwerkreinigung sind unterschiedlich. Die Speicherarchivlaufwerkreinigung ist normalerweise Anwendungen nicht bekannt. Daher kann IBM Spectrum Protect möglicherweise die Reinigungskassetten in Laufwerken nicht immer erkennen und unter Umständen nicht bestimmen, wann die Reinigung beginnt.

Einige Einheiten erfordern eine kurze Leerlaufzeit zwischen Mountanforderungen, um die Laufwerkreinigung starten zu können. IBM Spectrum Protect versucht jedoch, die Leerlaufzeit für ein Laufwerk zu minimieren. Dies kann dazu führen, dass die Speicherarchivlaufwerkreinigung nicht effektiv funktioniert. Verwenden Sie in diesem Fall IBM Spectrum Protect zur Steuerung der Laufwerkreinigung. Sie können die Häufigkeit so festlegen, dass sie mit den Reinigungsempfehlungen des Herstellers übereinstimmt.

Methoden zum Reinigen von Bandlaufwerken

Im Laufe der Zeit können die Leseköpfe für Bänder verschmutzen, was zum Fehlschlagen von Lese- und Schreiboperationen führen kann. Aktivieren Sie die Bandreinigung, um diese Probleme zu verhindern. Sie können die Bandreinigung über das Laufwerk oder IBM Spectrum Protect aktivieren.

Sie können entweder die Speicherarchivlaufwerkreinigungsmethode oder die IBM Spectrum Protect-Laufwerkreinigungsmethode verwenden, aber nicht beide Methoden gleichzeitig. Einige SCSI-Speicherarchive stellen eine automatische Laufwerkreinigung zur Verfügung. Wählen Sie die Speicherarchivlaufwerkreinigungsmethode aus, sofern diese verfügbar ist. Ist sie nicht verfügbar oder hat sie Probleme zur Folge, verwenden Sie IBM Spectrum Protect zur Steuerung der Speicherarchivlaufwerkreinigung.

Speicherarchivlaufwerkreinigungsmethode

Die Speicherarchivlaufwerkreinigungsmethode bietet für automatisierte Bandarchive, die diese Funktion verwenden, eine Reihe von Vorteilen:

- Sie verringert den Aufwand, den der IBM Spectrum Protect-Administrator hat, um die Reinigung mithilfe von Kassetten physisch zu handhaben.

- Sie verbessert die Verwendungsraten von Reinigungskassetten. Bei den meisten Bandarchiven wird die Häufigkeit, mit der Laufwerke gereinigt werden können, auf der Basis von Hardwareanzeigern verfolgt. IBM Spectrum Protect verwendet eine Rohzählung.
- Sie reduziert die Häufigkeit unnötiger Reinigungen. Moderne Bandlaufwerke müssen nicht in festen Intervallen gereinigt werden; sie können erkennen, wann eine Reinigung erforderlich ist, und diese dann anfordern.

Hersteller, die eine Speicherarchivlaufwerkreinigungsmethode zur Verfügung stellen, empfehlen die Verwendung dieser Funktion, um eine vorzeitige Abnutzung der Schreib-/Leseköpfe der Laufwerke zu verhindern. Bei Laufwerken und Speicherarchiven unterschiedlicher Hersteller bestehen Unterschiede in der Handhabung von Reinigungskassetten und in der Art und Weise, wie das Vorhandensein einer Reinigungskassette in einem Laufwerk zurückgemeldet wird. Möglicherweise kann ein Laufwerk, das eine Reinigungskassette enthält, vom Einheitentreiber nicht geöffnet werden. Die von Einheiten ausgegebenen Prüfcodes und Fehlercodes für die Laufwerkreinigung sind unterschiedlich. Die Speicherarchivlaufwerkreinigung ist normalerweise für alle Anwendungen transparent. IBM Spectrum Protect kann jedoch möglicherweise Reinigungskassetten in Laufwerken nicht immer erkennen und unter Umständen nicht bestimmen, wann die Reinigung beginnt.

IBM Spectrum Protect-Laufwerkreinigungsmethode

Einige Einheiten erfordern eine kurze Leerlaufzeit zwischen Mountanforderungen, um die Laufwerkreinigung starten zu können. IBM Spectrum Protect versucht jedoch, die Leerlaufzeit für ein Laufwerk zu minimieren. Dies kann dazu führen, dass die Speicherarchivlaufwerkreinigung nicht effektiv funktioniert. Versuchen Sie in diesem Fall, IBM Spectrum Protect zur Steuerung der Laufwerkreinigung zu verwenden. Legen Sie die Häufigkeit so fest, dass sie mit den Reinigungsempfehlungen des Herstellers übereinstimmt.

Wenn der Laufwerkreinigungsprozess durch IBM Spectrum Protect gesteuert wird, inaktivieren Sie die Speicherarchivlaufwerkreinigungsfunktion, um Probleme zu verhindern. Wenn die Speicherarchivlaufwerkreinigungsfunktion aktiviert ist, versetzen einige Einheiten automatisch alle Reinigungskassetten, die im Speicherarchiv gefunden werden, in die Schächte des Speicherarchivs, die für Reinigungskassetten vorgesehen sind. Sie können eine Reinigungskassette erst nach der Inaktivierung der Speicherarchivlaufwerkreinigungsfunktion in den IBM Spectrum Protect-Speicherarchivbestand zurückstellen.

Um die Reinigung über das Laufwerk zu aktivieren, führen Sie die Anweisungen des Laufwerkherstellers aus. Informationen zum Aktivieren der Bereinigung mithilfe von IBM Spectrum Protect finden Sie in „Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren” auf Seite 218.

Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren

Wenn Sie die servergesteuerte Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren, können Sie angeben, wie oft die Laufwerke gereinigt werden sollen.

Vorbereitende Schritte

Bestimmen Sie, wie oft das Laufwerk gereinigt werden muss. Dieser Schritt ist erforderlich, damit Sie einen geeigneten Wert für den Parameter **CLEANFREQUENCY** im Befehl **DEFINE DRIVE** oder **UPDATE DRIVE** angeben können. Um beispielsweise ein Laufwerk zu reinigen, nachdem 100 GB Daten in dem Laufwerk verarbeitet wurden, würden Sie **CLEANFREQUENCY=100** angeben.

Richtlinien zur Reinigungshäufigkeit enthält die Dokumentation des Laufwerkherstellers. Wenn die Dokumentation Richtlinien zur Reinigungshäufigkeit in Nutzungsstunden angibt, rechnen Sie den Wert in einen Gigabytewert um, indem Sie die folgenden Schritte ausführen:

1. Verwenden Sie den Wert für Byte pro Sekunde des Laufwerks, um einen Wert für Gigabyte pro Stunde zu ermitteln.
2. Multiplizieren Sie den Wert für Gigabyte pro Stunde mit der empfohlenen Anzahl Nutzungsstunden zwischen Reinigungen.

3. Verwenden Sie das Ergebnis als Wert für die Reinigungshäufigkeit.

Sie können entweder einen Wert für den Parameter **CLEANFREQUENCY** angeben oder **ASNEEDED** angeben, um das Laufwerk nach Bedarf zu reinigen.

Einschränkungen:

1. Bei Laufwerken IBM 3592 müssen Sie einen numerischen Wert für den Parameter **CLEANFREQUENCY** angeben. Bei Einhaltung der in der Produktinformation aufgelisteten Reinigungshäufigkeit werden die Laufwerke nicht übermäßig gereinigt.
2. Der Parameterwert **CLEANFREQUENCY=ASNEEDED** funktioniert nicht für alle Bandlaufwerke. Die Informationen für Ihr Betriebssystem geben Auskunft darüber, ob ein Laufwerk diese Funktion unterstützt:

   AIX Windows Supported devices for AIX and Windows

   Linux Supported devices for Linux

   Klicken Sie in der Technote auf den Laufwerknamen, um detaillierte Informationen anzuzeigen. Wenn der Wert ASNEEDED nicht unterstützt wird, geben Sie die Anzahl Gigabyte an.

Vorgehensweise

Definieren oder aktualisieren Sie die Laufwerke in dem Speicherarchiv unter Angabe des Parameters **CLEANFREQUENCY** im Befehl **DEFINE DRIVE** oder **UPDATE DRIVE**.
Um beispielsweise ein Laufwerk mit dem Namen DRIVE1 nach der Verarbeitung von 100 GB Daten zu reinigen, geben Sie den folgenden Befehl aus:

```
update drive autolib1 drive1 cleanfrequency=100
```

Ergebnisse

Nachdem die Reinigungskassette zurückgestellt wurde, wird sie vom Server in ein Laufwerk geladen, wenn dieses gereinigt werden muss. Der Server verwendet diese Reinigungskassette gemäß den Angaben für die Reinigungsanzahl. Weitere Informationen finden Sie in „Operationen mit Reinigungskassetten” auf Seite 166.

Nächste Schritte

Stellen Sie die Reinigungskassette in den Datenträgerbestand im Speicherarchiv zurück, indem Sie die Anweisungen in „Reinigungskassette in ein Speicherarchiv zurückstellen” auf Seite 219 ausführen.

Zugehörige Informationen

DEFINE DRIVE (Laufwerk für ein Speicherarchiv definieren)

UPDATE DRIVE (Laufwerk aktualisieren)

Reinigungskassette in ein Speicherarchiv zurückstellen

Um die automatische Bandlaufwerkreinigung zu ermöglichen, müssen Sie eine Reinigungskassette in den Datenträgerbestand des automatisierten Speicherarchivs zurückstellen.

Informationen zu diesem Vorgang

Wenn Sie eine Reinigungskassette in ein Speicherarchiv zurückstellen, stellen Sie sicher, dass sie vom Server korrekt als Reinigungskassette erkannt wird. Stellen Sie sicher, dass sich keine Reinigungskassette in einem Schacht befindet, der beim Suchvorgang erkannt wird. Fehler und Verzögerungen von mindestens 15 Minuten können anzeigen, dass eine Reinigungskassette falsch platziert wurde.

Bei der bevorzugten Methode werden Reinigungskassetten einzeln zurückgestellt. Wenn Sie sowohl Datenkassetten als auch Reinigungskassetten zurückstellen müssen, stellen Sie zuerst die Datenkassetten in das Speicherarchiv zurück. Stellen Sie anschließend die Reinigungskassetten in das Speicherarchiv zurück.

Vorgehensweise

Um eine Reinigungskassette in ein Speicherarchiv zurückzustellen, geben Sie den Befehl **CHECKIN LIBVOLUME** aus.
Um beispielsweise eine Reinigungskassette mit dem Namen AUTOLIB1 zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10
 checklabel=no
```

Der Server gibt die Anforderung aus, die Kassette in den Eingangs-/Ausgangsport oder in einen bestimmten Schacht einzulegen.

Zugehörige Informationen
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Operationen mit Reinigungskassetten

Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

Reinigungsprozess überwachen
Wenn eine Reinigungskassette in ein Speicherarchiv zurückgestellt wird und ein Laufwerk gereinigt werden muss, hebt der Server die Bereitstellung des Datenträgers auf und führt die Reinigungsoperation aus. Wenn die Reinigungsoperation fehlschlägt oder wenn sie abgebrochen wird oder wenn keine Reinigungskassette verfügbar ist, sind Sie sich der Tatsache, dass das Laufwerk gereinigt werden muss, möglicherweise nicht bewusst. Überwachen Sie Reinigungsnachrichten auf diese Probleme, um sicherzustellen, dass Laufwerke wie erforderlich gereinigt werden. Geben Sie, falls erforderlich, den Befehl **CLEAN DRIVE** aus, damit der Server den Reinigungsversuch wiederholt, oder laden Sie manuell eine Reinigungskassette in das Laufwerk.

Mehrere Reinigungskassetten verwenden
Der Server verwendet eine Reinigungskassette für die Anzahl Reinigungen, die Sie beim Zurückstellen der Reinigungskassette angeben. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen, verwendet der Server nur eine der Kassetten, bis die angegebene Anzahl Reinigungen für diese Kassette erreicht ist. Dann verwendet der Server die nächste Reinigungskassette. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen und zwei oder mehr Befehle **CLEAN DRIVE** gleichzeitig ausgegeben, verwendet der Server mehrere Kassetten gleichzeitig und verringert die verbleibenden Reinigungen auf jeder Kassette.

Zugehörige Informationen
AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
CLEAN DRIVE (Laufwerk reinigen)
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
QUERY LIBVOLUME (Datenträger im Speicherarchiv abfragen)

Fehler bei der Laufwerkreinigung beheben

Während Kassetten in einem Speicherarchiv versetzt werden, wird eine Datenkassette möglicherweise an eine Stelle versetzt, an der sich eine Reinigungskassette befinden sollte. Überprüfen Sie den Prozess, den der Server ausführt, und die Nachrichten, die ausgegeben werden, sodass Sie das Problem beheben können.

Wenn ein Laufwerk gereinigt werden muss, lädt der Server das, was laut Datenbank eine Reinigungskassette sein müsste, in das Laufwerk. Das Laufwerk wird dann in den Bereitstatus (READY) versetzt und IBM Spectrum Protect erkennt, dass es sich bei der Kassette um eine Datenkassette handelt. Der Server führt die folgenden Schritte aus:

1. Der Server versucht, den internen Bandkennsatz der Datenkassette zu lesen.

2. Der Server gibt die Kassette aus dem Laufwerk aus und stellt sie innerhalb des Speicherarchivs in den Ausgangsspeicherschacht der Reinigungskassette zurück. Wenn die Ausgabeoperation fehlschlägt, markiert der Server das Laufwerk als offline und gibt eine Nachricht aus, die besagt, dass sich die Kassette noch im Laufwerk befindet.
3. Der Server entnimmt die Reinigungskassette, um zu verhindern, dass sie für eine weitere Laufwerkreinigungsanforderung ausgewählt wird. Die Reinigungskassette verbleibt im Speicherarchiv, erscheint jedoch nicht mehr im IBM Spectrum Protect-Speicherarchivbestand.
4. Unter Verwendung des internen Bandkennsatzes gleicht der Server den Datenträgernamen mit dem aktuellen Speicherarchivbestand, mit den Speicherpooldatenträgern und mit der Protokolldatei für Datenträger ab.
   - Wenn der Datenträgername im Speicherarchivbestand nicht gefunden wird, wird unter Umständen fälschlicherweise eine Datenkassette als Reinigungskassette zurückgestellt. Wenn der Datenträger entnommen wird, müssen Sie keine weitere Aktion ausführen.
   - Wenn der Datenträgername im Speicherarchivbestand gefunden wird, gibt der Server Nachrichten aus, dass ein manueller Eingriff und eine Speicherarchivprüfung erforderlich sind. Um das Problem zu beheben, führen Sie die Anweisungen in „Datenträgerbestand in einem Speicherarchiv prüfen" auf Seite 207 aus.

Bandlaufwerke ersetzen

Wenn Sie ein Laufwerk in einem Bandarchiv ersetzen, das für IBM Spectrum Protect definiert ist, müssen Sie die Laufwerk- und Pfaddefinitionen für das alte Laufwerk löschen und das neue Laufwerk samt Pfad definieren.

Das Ersetzen von Laufwerk- und Pfaddefinitionen ist selbst dann erforderlich, wenn Sie ein Laufwerk durch ein anderes Laufwerk desselben Typs mit derselben logischen Adresse, derselben physischen Adresse, derselben SCSI-ID und derselben Portnummer austauschen. Die Aliasnamen der Einheiten können sich ändern, wenn Sie Ihre Laufwerkverbindungen ändern.

Wenn es sich bei dem neuen Laufwerk um ein Upgrade handelt, das ein neues Datenträgerformat unterstützt, müssen Sie unter Umständen auch ein neues logisches Speicherarchiv, eine neue Einheitenklasse und einen neuen Speicherpool definieren. Die Prozeduren für das Konfigurieren einer Maßnahme für ein neues Laufwerk in einem Speicherarchiv mit mehreren Laufwerken sind je nach Laufwerktyp und Datenträgertyp in dem Speicherarchiv unterschiedlich.

Bandlaufwerke löschen

Sie können Bandlaufwerke aus einem Speicherarchiv löschen. Beispielsweise können Sie ein Laufwerk, das nicht mehr verwendet wird oder das ersetzt werden soll, löschen.

Vorgehensweise

1. Stoppen Sie den IBM Spectrum Protect-Server und fahren Sie das Betriebssystem herunter.
2. Entfernen Sie das alte Laufwerk und befolgen Sie zum Installieren des neuen Laufwerks die Anweisungen des Herstellers.
3. Starten Sie das Betriebssystem und den IBM Spectrum Protect-Server erneut.
4. Löschen Sie den Pfad vom Server zum Laufwerk.
   Um beispielsweise einen Pfad von SERVER1 zu LIB1 zu löschen, geben Sie den folgenden Befehl aus:

   ```
   delete path server1 lib1 srctype=server desttype=drive
   ```

5. Löschen Sie die Laufwerkdefinition.
   Geben Sie beispielsweise den folgenden Befehl aus, um ein Laufwerk mit dem Namen DLT1 aus einem Speicherarchiv mit dem Namen LIB1 zu löschen:

   ```
   delete drive lib1 dlt1
   ```

Zugehörige Informationen

DELETE DRIVE (Laufwerk aus einem Speicherarchiv löschen)

DELETE PATH (Pfad löschen)

Laufwerke durch andere Laufwerke desselben Typs ersetzen

Um ein Laufwerk hinzuzufügen, das dieselben Datenträgerformate wie das zu ersetzende Laufwerk unterstützt, müssen Sie ein neues Laufwerk und einen neuen Pfad definieren.

Informationen zu diesem Vorgang

Wenn ein Speicherarchiv nur ein einziges Laufwerkmodell enthält und ein Laufwerk ersetzt werden soll, müssen Sie das Laufwerk durch ein Laufwerk desselben Modells ersetzen. Wenn ein Speicherarchiv unterschiedliche Laufwerkmodelle enthält und ein Laufwerk ersetzt werden soll, können Sie das Laufwerk durch ein Laufwerk eines beliebigen Modells, das im Speicherarchiv vorhanden ist, ersetzen.

Vorgehensweise

1. Löschen Sie die Pfad- und Laufwerkdefinitionen für das alte Laufwerk. Um beispielsweise ein Laufwerk mit dem Namen DRIVE1 aus einem Speicherarchiv mit dem Namen LIB1 zu löschen, geben Sie den folgenden Befehl ein:

   ```
   delete path server2 drive1 srctype=server desttype=drive library=lib1
   delete drive lib1 drive1
   ```

2. Schalten Sie das Speicherarchiv aus, entfernen Sie das ursprüngliche Laufwerk, ersetzen Sie es durch das neue Laufwerk und schalten Sie das Speicherarchiv ein.
3. Aktualisieren Sie das Hostsystem, um sicherzustellen, dass das System das neue Laufwerk erkennt.
4. Definieren Sie das neue Laufwerk und den neuen Pfad. Um beispielsweise ein neues Laufwerk mit dem Namen DRIVE2 und einen Pfad von SERVER2 zu diesem Laufwerk zu definieren, wenn der IBM Spectrum Protect-Einheitentreiber verwendet wird, geben Sie die folgenden Befehle ein:

   AIX
   ```
   define drive lib1 drive2
   define path server2 drive2 srctype=server desttype=drive library=lib1
      device=/dev/mt0
   ```

   Linux
   ```
   define drive lib1 drive2
   define path server2 drive2 srctype=server desttype=drive library=lib1
      device=/dev/tsmscsi/mt0
   ```

   Windows
   ```
   define drive lib1 drive2
   define path server2 drive2 srctype=server desttype=drive library=lib1
      device=mt3.0.0.1
   ```

   Tipp: Sie können Ihre vorhandenen Speicherarchiv-, Einheitenklassen- und Speicherpooldefinitionen verwenden.

Zugehörige Informationen

DELETE DRIVE (Laufwerk aus einem Speicherarchiv löschen)

DELETE PATH (Pfad löschen)

Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde

Wenn Sie ein Upgrade für alle Bandlaufwerke in einem Speicherarchiv durchführen, können Sie Ihre vorhandenen Maßnahmendefinitionen für die Umlagerung und den Verfall bestehender Daten beibehalten, während Sie die neuen Laufwerke zum Speichern neuer Daten verwenden können.

Vorbereitende Schritte

Bei dem folgenden Szenario wird vorausgesetzt, dass bereits ein primärer Speicherpool mit dem Namen POOL1 für eine Einheitenklasse DISK vorhanden ist.

Vorgehensweise

1. Um Daten in einen Speicherpool umzulagern, der für die neuen Laufwerke erstellt wird, geben Sie den Parameter **NEXTSTGPOOL** an. Um beispielsweise Daten aus einem vorhandenen Speicherpool mit dem Namen POOL1 in den neuen Speicherpool mit dem Namen POOL2 umzulagern, geben Sie den folgenden Befehl aus:

   ```
   update stgpool pool1 nextstgpool=pool2
   ```

2. Aktualisieren Sie die Verwaltungsklassendefinitionen, um Daten mithilfe des Befehls **UPDATE MGMTCLASS** in dem neuen DISK-Speicherpool zu speichern.

Zugehörige Informationen

DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)
UPDATE STGPOOL (Speicherpool aktualisieren)

IBM Spectrum Protect-Server schützen

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

Task	Prozedur

Administrator hinzufügen	Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:
	a. Registrieren Sie den Administrator und geben Sie **Pa$#$twO** als Kennwort an, indem Sie den folgenden Befehl ausgeben:
	`register admin admin1 Pa$#$twO`
	b. Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`

Task	Prozedur

Administratorberechtigung ändern	Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.
	• Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`
	• Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`revoke authority admin1 classes=system`

Administratoren entfernen	Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zuzugreifen kann, indem Sie den folgenden Befehl ausgeben: `remove admin admin1`
Zugriff auf den Server vorübergehend verhindern	Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl **LOCK ADMIN** bzw. **UNLOCK ADMIN** verwenden.

Zugehörige Konzepte

Planung für Administratorrollen

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

Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 36. Authentifizierungstasks für IBM Spectrum Protect-Server

Task	Prozedur
Grenzwert für ungültige Kennworteingabeversuche festlegen	a. Wählen Sie auf der Seite **Server** im Operations Center den Server aus. b. Klicken Sie auf **Details** und klicken Sie dann auf die Registerkarte **Merkmale**. c. Geben Sie die Anzahl ungültiger Versuche im Feld **Grenzwert für ungültige Anmeldeversuche** an. Der Standardwert bei der Installation ist 0.
Mindestlänge für Kennwörter festlegen	a. Wählen Sie auf der Seite **Server** im Operations Center den Server aus. b. Klicken Sie auf **Details** und klicken Sie dann auf die Registerkarte **Merkmale**. c. Geben Sie die Anzahl Zeichen im Feld **Mindestlänge für Kennwort** an.
Ablaufzeitraum für Kennwörter festlegen	a. Wählen Sie auf der Seite **Server** im Operations Center den Server aus. b. Klicken Sie auf **Details** und klicken Sie dann auf die Registerkarte **Merkmale**. c. Geben Sie die Anzahl Tage im Feld **Allgemeine Kennwortablaufdauer** an.

Standardauthentifizierungsmethode festlegen	Geben Sie den Befehl **SET DEFAULTAUTHENTICATION** aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:
	`set defaultauthentication local`
	Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie AUTHENTICATION=LOCAL in den Befehl **UPDATE NODE** ein:
	`update node authentication=local`

Server auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

Benutzerzugriff auf den Server einschränken

Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Vorgehensweise

1. Nachdem Sie einen Administrator mit dem Befehl **REGISTER ADMIN** registriert haben, legen Sie die Berechtigungsstufe des Administrators mithilfe des Befehls **GRANT AUTHORITY** fest.

   Ausführliche Informationen zum Festlegen und Ändern der Berechtigung finden Sie in „Administratoren verwalten" auf Seite 223.
2. Um die Berechtigung eines Administrators zur Ausführung bestimmter Tasks zu steuern, verwenden Sie die beiden folgenden Serveroptionen:
   a) Über die Serveroption **QUERYAUTH** können Sie die Berechtigungsstufe auswählen, die ein Administrator haben muss, um Befehle **QUERY** und **SELECT** ausgeben zu können. Standardmäßig ist keine Berechtigungsstufe erforderlich. Sie können die Anforderung in eine der Berechtigungsstufen, einschließlich Systemberechtigung, ändern.
   b) Über die Serveroption **REQSYSAUTHOUTFILE** können Sie angeben, dass Systemberechtigung für Befehle erforderlich ist, die zur Folge haben, dass der Server Daten in eine externe Datei schreibt. Standardmäßig ist für diese Befehle Systemberechtigung erforderlich.
3. Sie können die Datensicherung auf einem Clientknoten ausschließlich auf Rootbenutzer-IDs oder berechtigte Benutzer beschränken.
   Um beispielsweise Sicherungen auf die Rootbenutzer-ID zu beschränken, geben Sie den Befehl **REGISTER NODE** oder **UPDATE NODE** unter Angabe des Parameters **BACKUPINITIATION=root** aus:

   ```
   update node backupinitiation=root
   ```

Server stoppen und starten

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

Vorbereitende Schritte

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

Server stoppen

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

Informationen zu diesem Vorgang

Wenn Sie den Befehl **HALT** zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

Vorgehensweise

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl **DISABLE SESSIONS** ausgeben:

   ```
   disable sessions all
   ```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:

   a. Rufen Sie die Seite **Übersicht** im Operations Center auf, auf der im Bereich **Aktivität** die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.

   b. Zeigen Sie das Diagramm im Bereich **Aktivität** an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:

      - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
      - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden Periode

      Wenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.

   c. Wählen Sie auf der Seite **Server** einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf **Details**. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl **QUERY PROCESS** aus, um Prozesse abzufragen; geben Sie den Befehl **QUERY SESSION** aus, um Informationen zu Sitzungen abzurufen.

3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:

   - Wählen Sie auf der Seite **Server** einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf **Details**.
   - Klicken Sie auf die Registerkarte **Aktive Tasks** und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   - Klicken Sie auf **Abbrechen**.
   - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl **CANCEL SESSION** aus, um eine Sitzung abzubrechen; geben Sie den Befehl **CANCEL PROCESS** aus, um Prozesse abzubrechen.

     Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountanforderung abgebrochen. Wenn Sie beispielsweise einen Befehl **EXPORT**, **IMPORT** oder **MOVE DATA** ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.

4. Stoppen Sie den Server, indem Sie den Befehl **HALT** ausgeben:

   ```
   halt
   ```

Server für Verwaltungs- oder Rekonfigurationstasks starten

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Informationen zu diesem Vorgang

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm **DSMSERV** mit dem Parameter **MAINTENANCE** ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.

Tipps:

- Sie müssen die Serveroptionsdatei, `dsmserv.opt`, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung (-wiederherstellung), den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

Prozedur

- Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

  ```
  dsmserv maintenance
  ```

  Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl **HALT** ausgeben:

   ```
   halt
   ```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
   - AIX
   - Linux
   - Windows

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

Durchführung eines Upgrades für den Server planen

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für

Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

Informationen zu diesem Vorgang

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster **IBM Installation Manager** auf das Symbol zum **Aktualisieren**; klicken Sie nicht auf das Symbol zum **Installieren** oder **Ändern**!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

Vorgehensweise

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe IBM Spectrum Protect Downloads - Latest Fix Packs and Interim Fixes.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.

   Tipp: Wenn Sie die Installationspaketdatei von der -Unterstützungssite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Storage-agent and library-client compatibility with an IBM Spectrum Protect server.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe IBM Spectrum Protect Server-Client Compatibility and Upgrade Considerations .
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

Nächste Schritte

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

- AIX -Server-Fixpack installieren
- Linux -Server-Fixpack installieren
- Windows

Vorbereitungen für einen Ausfall oder eine Systemaktualisierung

Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass Sie die regelmäßige Ausführung von Aktivitäten planen, um den Server zu verwalten und zu schützen. Informationen zum Planen von Aktivitäten wie beispielsweise Sichern der Datenbank, Sichern der Einheitenkonfigurationsdatei und Sichern des Datenträgerprotokolls finden Sie in „Zeitpläne für Serververwaltungsaktivitäten definieren” auf Seite 60.

Vorgehensweise

1. Brechen Sie Prozesse und Sitzungen, die aktiv sind, ab, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie im Operations Center auf der Seite **Server** einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf **Details**.
   b. Klicken Sie auf die Registerkarte **Aktive Tasks** und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   c. Klicken Sie auf **Abbrechen**.
2. Stoppen Sie den Server, indem Sie den Befehl **HALT** ausgeben:

   ```
   halt
   ```

   Tipp: Sie können den Befehl HALT im Operations Center ausgeben, indem Sie den Mauszeiger über das Symbol für **Einstellungen** bewegen und auf **Command Builder** klicken. Wählen Sie dann den Server aus, geben Sie `halt` ein und drücken Sie die **Eingabetaste**.

Zugehörige Informationen
HALT (Server herunterfahren)

Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM

IBM Spectrum Protect stellt die Funktion Disaster Recovery Manager (DRM) für die Wiederherstellung Ihrer Server- und Clientdaten bei einem Katastrophenfall zur Verfügung.

DRM verfolgt die Versetzung ausgelagerter Datenträger und registriert diese Informationen in der IBM Spectrum Protect-Datenbank. DRM konsolidiert Pläne, Scripts und andere Informationen in einer Plandatei, die im Katastrophenfall oder bei einer ungeplanten Betriebsunterbrechung zum Wiederherstellen des IBM Spectrum Protect-Servers erforderlich ist. Wenn mögliche Malware-Attacken, einschließlich Ransomware-Attacken, ein Thema für Sie sind, ziehen Sie die Verwendung von DRM in Betracht, das Sie bei der Wiederherstellung Ihrer Server nach einer Attacke unterstützen kann.

Einschränkung: DRM ist nur im Produkt IBM Spectrum Protect Extended Edition verfügbar.

Plandatei zur Wiederherstellung nach einem Katastrophenfall

Die Plandatei zur Wiederherstellung nach einem Katastrophenfall, die auch als Wiederherstellungsplandatei bezeichnet wird, enthält die Informationen, die zum Wiederherstellen eines IBM Spectrum Protect-Servers mit dem Stand des Zeitpunkts der letzten Datenbanksicherungsoperation, die vor der Erstellung des Plans abgeschlossen wurde, erforderlich sind.

Der Plan besteht aus Zeilengruppen, die Sie in mehrere Dateien aufteilen können. Jede Zeilengruppe verfügt über eine Anfangsanweisung (begin) und eine Endanweisung (end).

Tabelle 37. Zeilengruppen in der Wiederherstellungsplandatei

Zeilengruppe	Informationen in der Zeilengruppe
SERVER.REQUIREMENTS	Gibt den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll für den Server an.
RECOVERY.INSTRUCTIONS.GENERAL	Gibt standortspezifische Anweisungen an, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.GENERAL angegebene Datei eingibt. Die Anweisungen umfassen die Wiederherstellungsstrategie, die Namen der wichtigsten Ansprechpartner, eine Übersicht über die wichtigsten Anwendungen, die von diesem Server gesichert werden, und andere relevante Wiederherstellungsanweisungen.

Tabelle 37. Zeilengruppen in der Wiederherstellungsplandatei (Forts.)

Zeilengruppe	Informationen in der Zeilengruppe
RECOVERY.INSTRUCTIONS.OFFSITE	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.OFFSITE angegebene Datei eingibt. Die Anweisungen umfassen den Namen und den Standort der Vault an einem anderen Standort sowie Informationen dazu, wie Kontakt zum Vaultadministrator aufgenommen werden kann (beispielsweise ein Name und eine Telefonnummer).
RECOVERY.INSTRUCTIONS.INSTALL	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.INSTALL angegebene Datei eingibt. Die Anweisungen umfassen Informationen, die angeben, wie der Basisserver wiederhergestellt wird, und den Aufbewahrungsort der Sicherungskopien des Systemimage.
RECOVERY.INSTRUCTIONS.DATABASE	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.DATABASE angegebene Datei eingibt. Die Anweisungen umfassen Informationen, die angeben, wie die Datenbankwiederherstellung vorbereitet wird. Sie können beispielsweise Anweisungen eingeben, die angeben, wie die Sicherungsdatenträger für ein automatisiertes Speicherarchiv initialisiert oder geladen werden sollen. Für diese Zeilengruppe wird kein Beispiel bereitgestellt.
RECOVERY.INSTRUCTIONS.STGPOOL	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.STGPOOL angegebene Datei eingibt. Die Anweisungen umfassen die Namen Ihrer Softwareanwendungen und der Kopienspeicherpools, die die Sicherung dieser Anwendungen enthalten. Für diese Zeilengruppe wird kein Beispiel bereitgestellt.
RECOVERY.VOLUMES.REQUIRED	Stellt eine Liste der Datenbanksicherungs- und Kopienspeicherpooldatenträger bereit, die zum Wiederherstellen des Servers erforderlich sind. Ein Datenbanksicherungsdatenträger wird eingeschlossen, wenn er Bestandteil der neuesten Datenbanksicherungsserie ist. Ein Kopienspeicherpooldatenträger wird eingeschlossen, wenn er nicht leer und nicht als dauerhaft beschädigt markiert ist.
RECOVERY.DEVICES.REQUIRED	Stellt Details zu den Einheiten bereit, die zum Lesen der Sicherungsdatenträger erforderlich sind.
RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE	Enthält ein Script mit den Befehlen, die zum Wiederherstellen des Servers erforderlich sind.
RECOVERY.SCRIPT.NORMAL.MODE	Enthält ein Script mit den Befehlen, die zum Zurückschreiben der primären Speicherpools des Servers erforderlich sind.
DB.STORAGEPATHS	Gibt die Verzeichnisse für die IBM Spectrum Protect-Datenbank an.
LICENSE.REGISTRATION	Enthält ein Makro zum Registrieren Ihrer Serverlizenzen.
COPYSTGPOOL.VOLUMES.AVAILABLE	Enthält ein Makro zum Markieren von Kopienspeicherpooldatenträgern, die an einen anderen Standort versetzt wurden und anschließend wieder vor Ort versetzt wurden. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle ausgeben. Es ist auch möglich, das Makro in eine Datei zu kopieren, zu ändern und auszuführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.
COPYSTGPOOL.VOLUMES.DESTROYED	Enthält ein Makro, mit dem Kopienspeicherpooldatenträger als nicht verfügbar markiert werden können, wenn sich die Datenträger zum Zeitpunkt der Katastrophe vor Ort befanden. Diese Datenträger werden als ausgelagert betrachtet und wurden bei einem Katastrophenfall nicht dauerhaft beschädigt. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausgeben oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.

Tabelle 37. Zeilengruppen in der Wiederherstellungsplandatei (Forts.)

Zeilengruppe	Informationen in der Zeilengruppe
PRIMARY.VOLUMES.DESTROYED	Enthält ein Makro, mit dem Datenträger für primäre Speicherpools als dauerhaft beschädigt markiert werden können, wenn sich die Datenträger zum Zeitpunkt der Katastrophe vor Ort befanden. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.
PRIMARY.VOLUMES.REPLACEMENT	Enthält ein Makro zum Ermitteln der Ersatzdatenträger für primäre Speicherpools. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.
STGPOOLS.RESTORE	Enthält ein Makro zum Zurückschreiben der primären Speicherpools. Sie können die Zeilengruppe als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen. Es ist auch möglich, das Makro in eine Datei zu kopieren, zu ändern und auszuführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.NORMAL.MODE gestartet.
VOLUME.HISTORY.FILE	Enthält eine Kopie der Datenträgerprotokolldaten zum Erstellungszeitpunkt des Wiederherstellungsplans. Das Dienstprogramm **DSMSERV RESTORE DB** bestimmt mithilfe der Protokolldatei für Datenträger, welche Datenträger zum Zurückschreiben der Datenbank erforderlich sind. Die Protokolldatei für Datenträger wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.
DEVICE.CONFIGURATION.FILE	Enthält eine Kopie der Servereinheitenkonfigurationsdaten zum Erstellungszeitpunkt des Wiederherstellungsplans. Das Dienstprogramm **DSMSERV RESTORE DB** liest mithilfe der Einheitenkonfigurationsdatei die Datenbanksicherungsdatenträger. Die Einheitenkonfigurationsdatei wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.
DSMSERV.OPT.FILE	Enthält eine Kopie der Serveroptionsdatei. Diese Zeilengruppe wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.
LICENSE.INFORMATION	Enthält eine Kopie der neuesten Ergebnisse der Lizenzprüfung und der Serverlizenzbedingungen.
MACHINE.GENERAL.INFORMATION	Stellt Informationen für die Servermaschine bereit, wie beispielsweise ihr Standort, die zum Wiederherstellen der Servermaschine erforderlich sind. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Maschineninformationen mithilfe des Befehls **DEFINE MACHINE** unter Angabe von **ADSMSERVER=YES** in der Datenbank gespeichert werden.
MACHINE.RECOVERY.INSTRUCTIONS	Stellt die Wiederherstellungsanweisungen für die Servermaschine bereit. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Wiederherstellungsanweisungen für die Maschine in der Datenbank gespeichert werden.
MACHINE.RECOVERY.CHARACTERISTICS	Stellt die Hardware- und Softwarekenndaten für die Servermaschine bereit. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Maschinenkenndaten in der Datenbank gespeichert werden.
MACHINE.RECOVERY.MEDIA	Stellt Informationen zu den Datenträgern bereit, die für die Wiederherstellung der Maschine, die den Server enthält, erforderlich sind. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn Informationen zu Wiederherstellungsdatenträgern in der Datenbank gespeichert werden und der Maschine zugeordnet sind, die den Server enthält.

Server und Clientdaten mithilfe von DRM wiederherstellen

Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um den IBM Spectrum Protect-Server und Clientdaten im Katastrophenfall wiederherzustellen.

Vorbereitende Schritte

IBM Spectrum Protect ist für die Verwendung des Protokolls Secure Sockets Layer (SSL) für die Client/Server-Authentifizierung konfiguriert. Wenn Sie den Server starten, wird im Rahmen des Prozesses eine Datei mit einem digitalen Zertifikat (`cert.kdb`) erstellt. Diese Datei enthält den öffentlichen Schlüssel des Servers, der dem Client das Verschlüsseln von Daten ermöglicht. Die Datei mit dem digitalen Zertifikat kann nicht in der Serverdatenbank gespeichert werden, da Global Security Kit (GSKit) eine separate Datei in einem bestimmten Format erfordert.

1. Bewahren Sie Sicherungskopien der Dateien `cert.kdb`, `cert.sth` und `cert256.arm` auf.
2. Wenn sowohl die ursprünglichen Zertifikatsdateien als auch alle Kopien verloren gehen oder beschädigt werden, generieren Sie neue Zertifikatsdateien.

Der Masterverschlüsselungsschlüssel ist in einer neuen, von GSKit verwalteten Schlüsseldatenbank, `dsmkeydb.kdb`, gespeichert. Wenn der Server über einen vorhandenen Masterverschlüsselungsschlüssel verfügt, wird der Masterverschlüsselungsschlüssel aus der Datei `dsmserv.pwd` in die Schlüsseldatenbank `dsmkeydb.kdb` umgelagert. Bewahren Sie Sicherungskopien der Dateien `dsmkeydb.kdb` und `dsmkeydb.sth` auf. Sie können den Befehl **BACKUP DB** zum Sichern des Masterverschlüsselungsschlüssels konfigurieren oder die Dateien `dsmkeydb.kdb` und `dsmkeydb.sth` selbst manuell sichern. Ohne den Masterverschlüsselungsschlüssel ist keine Wiederherstellung nach einem Katastrophenfall möglich.

1. Bewahren Sie Sicherungskopien der Dateien `dsmkeydb.kdb` und `dsmkeydb.sth` auf.

Vorgehensweise

1. Rufen Sie den neuesten Wiederherstellungsplan ab.
2. Überprüfen Sie die Wiederherstellungsschritte, die in der Zeilengruppe RECOVERY.INSTRUCTIONS.GENERAL des Plans beschrieben sind.
3. Unterteilen Sie die Zeilengruppen der Plandatei nach allgemeinen Vorabanweisungen, Scripts zur Wiederherstellung des IBM Spectrum Protect-Servers und Anweisungen zur Clientwiederherstellung in einzelne Dateien.
4. Rufen Sie alle erforderlichen Wiederherstellungsdatenträger (wie in dem Plan aufgelistet) vom Aufbewahrungsort ab.
5. Überprüfen Sie die Einheitenkonfigurationsdatei, um sicherzustellen, dass die Hardwarekonfiguration am Wiederherstellungsstandort mit der am ursprünglichen Standort identisch ist. Alle Unterschiede müssen in der Einheitenkonfigurationsdatei aktualisiert werden. Für die folgenden Beispielkonfigurationsänderungen sind Aktualisierungen der Konfigurationsinformationen erforderlich:
   - Unterschiedliche Einheitennamen
   - Anforderung bei automatisierten Speicherarchiven, die Datenbanksicherungsdatenträger manuell in das automatisierte Speicherarchiv einlegen und die Konfigurationsinformationen aktualisieren zu müssen, um das Element in dem Speicherarchiv zu identifizieren. Dies ermöglicht es dem Server, die erforderlichen Datenbanksicherungsdatenträger zu lokalisieren.
6. Konfigurieren Sie Ersatzhardware für den IBM Spectrum Protect-Server, einschließlich der Installation des Betriebssystems und des IBM Spectrum Protect-Basisrelease.
7. Führen Sie die Scripts zur Wiederherstellung des IBM Spectrum Protect-Servers im Wiederherstellungsplan aus. Die Zeilengruppen RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE und RECOVERY.SCRIPT.NORMAL.MODE enthalten ausführbare Befehlsdateien, mit denen die Wiederherstellung des IBM Spectrum Protect-Servers gesteuert werden kann, indem andere im Plan generierte Befehlsdateien aufgerufen werden. Mit dem Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE wird der Server bis zu dem Punkt wiederhergestellt, an dem Clients Zurückschreibungen direkt von den Kopienspeicherpooldatenträgern starten können.

8. Schreiben Sie die primären Speicherpools mithilfe des Scripts RECOVERY.SCRIPT.NORMAL.MODE zurück.
9. Starten Sie Clientzurückschreibungsoperationen beginnend mit der höchsten Priorität gemäß der allgemeinen Planung.

Nächste Schritte

Der IBM Spectrum Protect-Server kann jetzt für normale Serveroperationen verwendet werden. Stellen Sie sicher, dass alle erforderlichen Operationen geplant sind. Anweisungen finden Sie in „Zeitpläne für Serververwaltungsaktivitäten definieren" auf Seite 60 und Sicherungs- und Archivierungsoperationen planen.

Zugehörige Informationen

PREPARE (Wiederherstellungsplandatei erstellen)

Daten in Verzeichniscontainerspeicherpools reparieren und wiederherstellen

Drilloperation für die Wiederherstellung nach einem Katastrophenfall ausführen

Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.

Vorbereitende Schritte

Führen Sie die folgenden Tasks aus:

- Planen Sie die regelmäßige Ausführung von Aktivitäten, um den Server zu verwalten und zu schützen. Weitere Informationen zur Planung von Aktivitäten finden Sie in „Zeitpläne für Serververwaltungsaktivitäten definieren" auf Seite 60. Stellen Sie sicher, dass Sie die folgenden Tasks planen:
  - Sichern der Datenbank.
  - Versetzen von Datenträgern an einen anderen Standort.
  - Sichern der Einheitenkonfigurationsdatei, der Protokolldatei für Datenträger und der Serveroptionsdatei `dsmserv.opt`.
  - **Optional:** Ausgabe des Befehls **PREPARE** zum Erstellen der Plandatei zur Wiederherstellung nach einem Katastrophenfall.

  Tipp:

  Wenn Sie den Befehl **PREPARE** ausgeben, wird von der IBM Spectrum Protect-Funktion 'Disaster Recovery Manager' (DRM) exakt eine Kopie der Plandatei zur Wiederherstellung nach einem Katastrophenfall erstellt.

  Sie können die Wiederherstellung nach einem Katastrophenfall mithilfe eines anderen Standorts ohne die Verwendung von DRM ausführen, DRM ist jedoch hilfreich, um Pläne, Scripts und andere Informationen, die während der Wiederherstellung nach einem Katastrophenfall erforderlich sind, zu konsolidieren.

  Erstellen Sie zur Sicherheit mehrere Kopien des Plans. Bewahren Sie Kopien beispielsweise in gedruckter Form, auf einem USB-Flashlaufwerk, in Plattenspeicher an einem anderen Standort oder auf einem fernen Server auf. Die Wiederherstellungsplandatei wird täglich zusammen mit den Bändern ausgelagert. Weitere Informationen zu DRM finden Sie in „Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM" auf Seite 230.
- Konfigurieren Sie die folgenden Ressourcen am Standort zur Wiederherstellung nach einem Katastrophenfall:

1. Einen IBM Spectrum Protect-Wiederherstellungsserver. Der Server am Standort zur Wiederherstellung nach einem Katastrophenfall muss dieselbe Version wie der Server am Produktionsstandort haben.
2. Ein Bandarchiv zum Speichern der Datenträger, die vom Produktionsstandort geliefert werden. Weitere Informationen zu Auslagerungsstandorten für die Wiederherstellung finden Sie in „Auslagerung von Daten" auf Seite 24.
3. Plattenspeicherplatz für die Datenbank, das Archivprotokoll, aktive Protokolldateien und Speicherpools.
4. Clients zum Testen von Zurückschreibungsoperationen.

Informationen zu diesem Vorgang

Testen Sie den Plan zur Wiederherstellung nach einem Katastrophenfall und die Wiederherstellbarkeit des IBM Spectrum Protect-Servers häufig und in einer ähnlichen Umgebung wie der Produktionsumgebung.

Vorgehensweise

1. Stellen Sie sicher, dass Bänder vor Ort verfügbar sind. Geben Sie den Befehl **QUERY LIBVOLUME** aus, um Datenträger, die in ein automatisiertes Speicherarchiv zurückgestellt wurden, zu ermitteln.
2. Sichern Sie die Datenbank auf den Bändern vor Ort, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie auf der Seite **Server** im Operations Center den Server aus, dessen Datenbank gesichert werden soll.
   b. Klicken Sie auf **Sichern** und führen Sie die Anweisungen im Fenster **Datenbank sichern** aus.
3. Kopieren Sie die folgenden Dateien in das Ausgangsverzeichnis des Servers am Wiederherstellungsstandort:
   - Wiederherstellungsplandatei
   - Protokolldatei für Datenträger
   - Einheitenkonfigurationsdatei
   - Optional: Serveroptionsdatei `dsmserv.opt`
4. Senden Sie das Band an den Auslagerungsstandort für die Wiederherstellung.
5. Schreiben Sie die Serverdatenbank zurück, indem Sie auf dem Wiederherstellungsserver den Befehl **DSMSERV RESTORE DB** verwenden.
6. Geben Sie den Befehl **UPDATE VOLUME** unter Angabe des Parameters **ACCESS=DESTROYED** aus, um anzugeben, dass ein Datenträger vollständig zurückgeschrieben werden muss.
7. Schreiben Sie auf dem Wiederherstellungsserver die Speicherpooldatenträger mithilfe des Befehls **RESTORE STGPOOL** zurück.

Nächste Schritte

Stellen Sie sicher, dass Sie auf die Daten in dem Speicherarchiv zugreifen können, indem Sie einen Banddatenträger in dem zurückgeschriebenen Speicherpool prüfen, um zu verifizieren, dass die Daten konsistent sind. Geben Sie den Befehl **AUDIT VOLUME** aus, um einen Banddatenträger zu prüfen. Prüfen Sie für eine schnellere Verarbeitung nur zurückgeschriebene Daten.

Zugehörige Tasks

Datenträgerbestand in einem Speicherarchiv prüfen

Sie können ein automatisiertes Speicherarchiv prüfen, um sicherzustellen, dass der Datenträgerbestand des Speicherarchivs mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind. Die Prüfung eines Speicherarchivs bietet sich an, wenn der Datenträgerbestand des Speicherarchivs aufgrund manueller Versetzungen der Datenträger in dem Speicherarchiv oder aufgrund von Datenbankproblemen nicht mehr korrekt ist.

Zugehörige Informationen

AUDIT VOLUME (Datenbankinformationen für einen Speicherpooldatenträger prüfen)

DSMSERV RESTORE DB (Datenbank zurückschreiben)
RESTORE STGPOOL (Speicherpooldaten zurückschreiben)

Datenbank zurückschreiben

Wenn die Funktion 'Disaster Recovery Manager' (DRM) aktiviert ist und Sie die Prozedur zur Vorbereitung auf einen Katastrophenfall ausgeführt haben, können Sie die Datenbank nach einem Katastrophenfall zurückschreiben. Wenn DRM nicht konfiguriert ist, können Sie die Datenbank dennoch zurückschreiben, vorausgesetzt, Sie verfügen über die erforderlichen Sicherungsdateien.

Vorbereitende Schritte

Wenn die Verzeichnisse für die Datenbank und das Wiederherstellungsprotokoll nicht mehr vorhanden sind, erstellen Sie diese erneut, bevor Sie das Serverdienstprogramm **DSMSERV RESTORE DB** ausführen.

Informationen zu diesem Vorgang

Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Um die Datenbank mit dem Stand wiederherzustellen, den sie zu dem Zeitpunkt hatte, zu dem sie verloren ging, stellen Sie die Datenbank mit der neuesten Version wieder her.

Einschränkungen:

- Um die Datenbank mit der neuesten Version zurückzuschreiben, müssen Sie das Archivprotokollverzeichnis lokalisieren. Wenn Sie das Verzeichnis nicht lokalisieren können, kann die Datenbank nur mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben werden.
- Sie können das Protokoll Secure Sockets Layer (SSL) nicht für Datenbankzurückschreibungsoperationen verwenden.
- Wenn der Release-Level der Datenbanksicherung und der Release-Level des Servers, für den die Zurückschreibung erfolgt, unterschiedlich sind, können Sie die Serverdatenbank nicht zurückschreiben. Wenn Sie beispielsweise einen Server der Version 8.1 verwenden und versuchen, eine Datenbank der Version 7.1 zurückzuschreiben, tritt ein Fehler auf.

Vorgehensweise

Verwenden Sie das Serverdienstprogramm **DSMSERV RESTORE DB**, um die Datenbank zurückzuschreiben. Wählen Sie abhängig von der Version der Datenbank, die zurückgeschrieben werden soll, eine der folgenden Methoden aus:

- Zurückschreiben einer Datenbank mit der neuesten Version. Verwenden Sie beispielsweise den folgenden Befehl:

  ```
  dsmserv restore db
  ```

- Zurückschreiben einer Datenbank mit dem Stand eines bestimmten Zeitpunkts. Um beispielsweise die Datenbank mit einer Sicherungsserie zurückzuschreiben, die am 19. April 2017 erstellt wurde, verwenden Sie den folgenden Befehl:

  ```
  dsmserv restore db todate=04/19/2017
  ```

Zugehörige Informationen

DSMSERV RESTORE DB (Datenbank zurückschreiben)

Anhang A. Funktionen zur behindertengerechten Bedienung für die IBM Spectrum Protect-Produktfamilie

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

Übersicht

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

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

Die IBM Spectrum Protect-Produktfamilie verwendet den neuesten W3C-Standard WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), um die Einhaltung von US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) und der Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) sicherzustellen. Um die Funktionen zur behindertengerechten Bedienung zu nutzen, verwenden Sie das neueste Release Ihres Sprachausgabeprogramms in Verbindung mit dem neuesten Web-Browser, der von diesem Produkt unterstützt wird.

Die Produktdokumentation im IBM Knowledge Center ist für die behindertengerechte Bedienung aktiviert. Eine Beschreibung der Funktionen zur behindertengerechten Bedienung im IBM Knowledge Center finden Sie im Abschnitt 'Accessibility' der IBM Knowledge Center-Hilfe (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navigation mithilfe der Tastatur

Dieses Produkt verwendet Standardnavigationstasten.

Schnittstelleninformationen

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

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

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

Software anderer Anbieter

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

Zugehörige Informationen zur behindertengerechten Bedienung

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

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

Weitere Informationen zum Engagement von IBM im Bereich der behindertengerechten Bedienung finden Sie in IBM Accessibility (www.ibm.com/able).

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. IBM stellt dieses Material möglicherweise auch in anderen Sprachen zur Verfügung. Für den Zugriff auf das Material in einer anderen Sprache kann eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich sein.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die in diesem Dokument enthaltenen Leistungsdaten wurden von bestimmten Betriebsbedingungen abgeleitet. Die tatsächlichen Ergebnisse können davon abweichen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten: © (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Adobe ist eine eingetragene Marke der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Linear Tape-Open, LTO und Ultrium sind Marken von HP, der IBM Corporation und von Quantum in den USA und/oder anderen Ländern.

Intel und Itanium sind Marken oder eingetragene Marken der Intel Corporation oder der zugehörigen Tochtergesellschaften in den USA und/oder anderen Ländern.

Die eingetragene Marke Linux wird gemäß einer Unterlizenz der Linux Foundation verwendet, dem exklusiven Lizenznehmer von Linus Torvalds, dem Eigentümer der Marke auf einer weltweiten Basis.

Microsoft, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java™ und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Red Hat, OpenShift®, Ansible® und Ceph® sind Marken oder eingetragene Marken der Red Hat, Inc. oder der zugehörigen Tochtergesellschaften in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

VMware, VMware vCenter Server und VMware vSphere sind eingetragene Marken oder Marken der VMware, Inc. oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

Bedingungen für die Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit
Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung
Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung
Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Berechtigungen
Abgesehen von den hier gewährten Berechtigungen werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Dieses Softwareangebot verwendet keine Cookies oder andere Technologien zur Erfassung personenbezogener Daten.

Wenn die für dieses Softwareangebot bereitgestellten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen,

müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung rechtlich beraten lassen, insbesondere Meldepflichten sowie die Einforderung von Einwilligungen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und auf der Seite "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Glossar

Für die IBM Spectrum Protect-Produktfamilie steht ein Glossar mit Begriffen und Definitionen zur Verfügung.

Siehe das Glossar für IBM Spectrum Protect.

Index

Numerische Stichwörter

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Programmnummer: 5725-W98
5725-W99
5725-X15