IBM Spectrum Protect
8.1.12

Plattenspeicherlösung für einen einzelnen Standort

Anmerkung:

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen” auf Seite 129 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 Plattenspeicherdatenschutz-lösung für einen einzelnen Standort

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

Implementierungsoptionen

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

Server unter Verwendung des Operations Center und von Verwaltungsbefehlen konfigurieren

In dieser Dokumentation werden Schritte zum Konfigurieren einer Reihe von Speichersystemen und der Server-Software für Ihre Lösung bereitgestellt. Konfigurationstasks werden mithilfe von Assistenten und Optionen im Operations Center und mithilfe von IBM Spectrum Protect-Befehlen ausgeführt. Informationen zu ersten Schritten finden Sie in „Planungsroadmap" auf Seite 1.

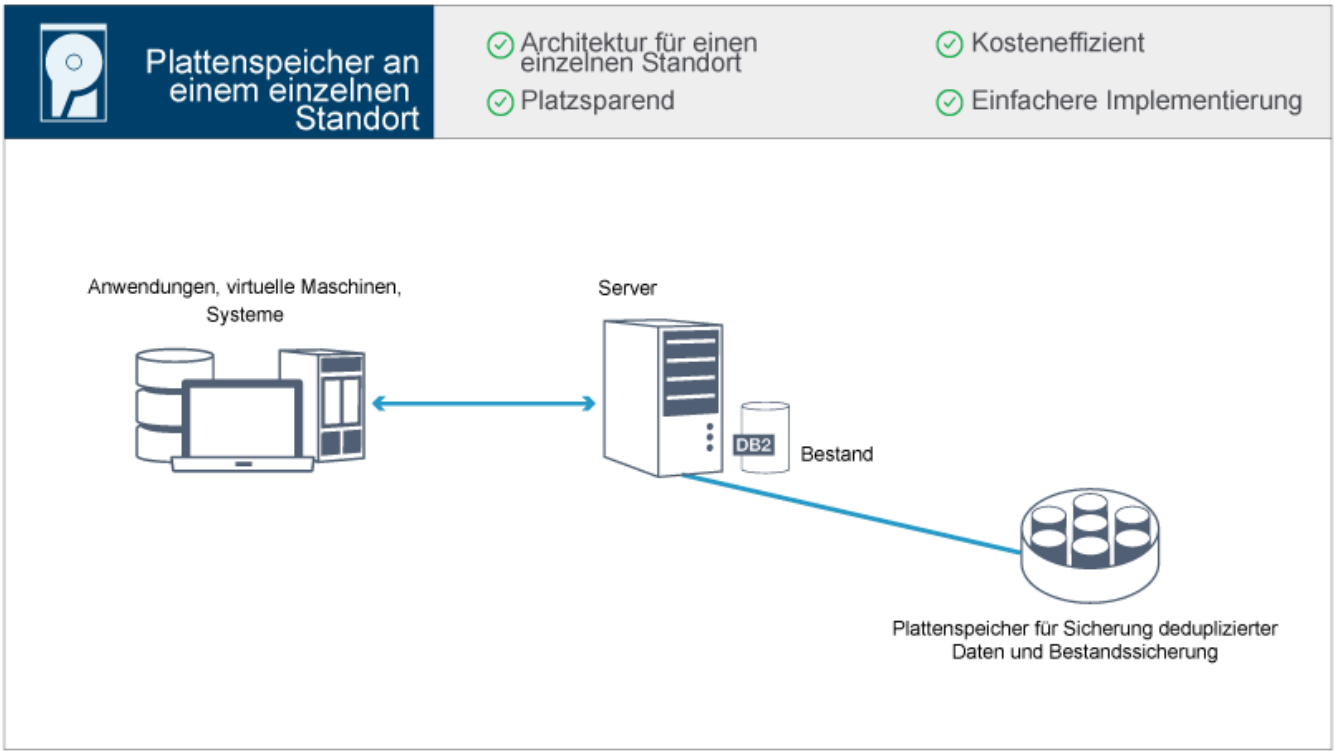
Server mithilfe automatisierter Scripts konfigurieren

Eine ausführliche Anleitung zur Implementierung einer Plattenspeicherlösung für einen einzelnen Standort mit bestimmten IBM StorwizeSpeichersystemen sowie zur Verwendung automatisierter Scripts zur Konfiguration des Servers finden Sie in den IBM Spectrum Protect Blueprints.

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

Planungsroadmap

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



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

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

Systemgröße auswählen

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

Informationen zu diesem Vorgang

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

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

Tabelle 1. Größe des Servers bestimmen

Gesamtvolumen der verwalteten Daten	**Volumen an täglich zu sichernden neuen Daten**	**Erforderliche Servergröße**
60 TB bis 240 TB	Bis zu 10 TB pro Tag	Klein
360 TB bis 1440 TB	10 bis 30 TB pro Tag	Mittelgroß
1000 TB bis 4000 TB	30 bis 100 TB pro Tag	Groß

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

Systemvoraussetzungen für eine Plattenspeicherlösung für einen einzelnen Standort

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

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

Zugehörige Informationen

IBM Spectrum Protect Supported Operating Systems

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.

Eine Definition der Systemgrößen finden Sie in „Systemgröße auswählen” auf Seite 2.

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

Verwenden Sie die Informationen in der folgenden Tabelle als Ausgangspunkt. Die neuesten Informationen zu Hardwarevoraussetzungen und Spezifikationen für den Server und Speicher finden Sie in den IBM Spectrum Protect Blueprints.

Hardwarekomponente	Kleines System	Mittelgroßes System	Großes System
Serverprozessor	AIX 6 Prozessorkerne, 3,42 GHz oder schneller Linux Windows 16 Prozessorkerne, 1,7 GHz oder schneller	AIX 10 Prozessorkerne, 3,42 GHz oder schneller Linux Windows 20 Prozessorkerne, 2,2 GHz oder schneller	AIX 20 Prozessorkerne, 3,42 GHz Linux Windows 44 Prozessorkerne, 2,2 GHz oder schneller
Serverspeicher	64 GB RAM	128 GB RAM	256 GB RAM
Netz	• 10 GB Ethernet (1 Port) • 8 GB Fibre Channel-Adapter (2 Ports)	• 10 GB Ethernet (2 Ports) • 8 GB Fibre Channel-Adapter (2 Ports)	• 10 GB Ethernet (4 Ports) • 8 GB Fibre Channel-Adapter (4 Ports)
Speicher	• 1,45 TB SSD-Platten für die Datenbank plus Speicherbereich für Operations Center-Datensätze • 67 TB deduplizierter Verzeichniscontainerspeicherpool	• 2,53 TB SSD-Platten für die Datenbank plus Speicherbereich für Operations Center-Datensätze • 207.9 TB deduplizierter Verzeichniscontainerspeicherpool	• 6,54 TB SSD-Platten für die Datenbank plus Speicherbereich für Operations Center-Datensätze • 1049,67 TB deduplizierter Verzeichniscontainerspeicherpool

Speicherbedarf für die Datenbank 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 Aufnehmen von Datensätzen für verwaltete Clients verwendet, in die vorherige Tabelle eingeschlossen.

Wenn Sie nicht planen, das Operations Center auf demselben System wie den 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 Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen erfordert. Wie viel Speicherbereich erforderlich ist, ist von der Anzahl

Clients abhängig, die auf einem Server überwacht werden. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr Server erfordert.

Speicherbereich in der Datenbank

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

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

Speicherbereich für das Archivprotokoll

Das Operations Center verwendet alle 24 Stunden ungefähr 8 GB Speicherbereich für das Archivprotokoll pro 1000 Clients. In dem Beispiel mit den 6500 Clients auf dem Hub-Server und den Peripherieservern werden in einem Zeitraum von 24 Stunden für den Hub-Server 56 GB Speicherbereich für das Archivprotokoll verwendet.

Für jeden Peripherieserver in dem Beispiel werden im Verlauf von 24 Stunden etwa 16 GB Speicherbereich für das Archivprotokoll verwendet. 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. Das folgende Beispiel zeigt die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten:

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

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

Softwarevoraussetzungen

Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für einen einzelnen Standort umfasst Installations- und Konfigurationstasks für die folgenden 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

Zugehörige Informationen
AIX-Netzoptionen definieren

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.

AIX

Tabelle 2. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
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	`/home/tsminst1/tsminst1`		50 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den Db2-Instanzeigner in Tabelle 3 auf Seite 9.
Verzeichnis für Serverinstallation	/		5 GB	
Verzeichnis für Serverinstallation	`/usr`		5 GB	

Tabelle 2. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems (Forts.)				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Anmerkungen**
Verzeichnis für Serverinstallation	`/var`		5 GB	
Verzeichnis für Serverinstallation	`/tmp`		5 GB	
Verzeichnis für Serverinstallation	`/opt`		10 GB	
Verzeichnis für die aktive Protokolldatei	`/tsminst1/TSMalog`		• Windows Besonders klein: 30 GB • Klein und mittel: 140 GB • Groß: 300 GB	Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB.
Verzeichnis für das Archivprotokoll	`/tsminst1/TSMarchlog`		• Windows Besonders klein: 250 GB • Klein: 1 TB • Mittel: 2 TB • Groß: 4 TB	

Verzeichnisse für die Datenbank	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 200 GB
			• Klein: Mindestens 1 TB
			• Mittel: Mindestens 2 TB
			• Groß: Mindestens 4 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:
				• Windows Besonders klein: Mindestens 1 Dateisystem
				• Klein: Mindestens 4 Dateisysteme
				• Mittel: Mindestens 4 Dateisysteme
				• Groß: Mindestens 8 Dateisysteme

Tabelle 2. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems (Forts.)

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen

Verzeichnisse für Speicher	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 10 TB
			• Klein: Mindestens 38 TB
			• Mittel: Mindestens 180 TB
			• Groß: Mindestens 500 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:
				• Windows Besonders klein: Mindestens 2 Dateisysteme
				• Klein: Mindestens 2 Dateisysteme
				• Mittel: Mindestens 10 Dateisysteme
				• Groß: Mindestens 30 Dateisysteme

Tabelle 2. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems (Forts.)				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Anmerkungen**

Verzeichnisse für Datenbanksicherung	`/tsminst1/TSMbkup00`
	`/tsminst1/TSMbkup01`
	`/tsminst1/TSMbkup02`
	`/tsminst1/TSMbkup03`
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 1 TB
			• Klein: Mindestens 3 TB
			• Mittel: Mindestens 10 TB
			• Groß: Mindestens 16 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank:
				• Windows Besonders klein: Mindestens 1 Dateisystem
				• Klein: Mindestens 2 Dateisysteme
				• Mittel: Mindestens 3 Dateisysteme
				• Groß: Mindestens 3 Dateisysteme
				Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 3. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect			
Element	**Standardwert**	**Eigener Wert**	**Anmerkungen**
Db2-Instanzeigner	`tsminst1`		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 2 auf Seite 6 in einen anderen Wert geändert hatten, ändern Sie auch den Wert für den Db2-Instanzeigner.

Tabelle 3. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect (Forts.)			
Element	**Standardwert**	**Eigener Wert**	**Anmerkungen**
Kennwort des Db2-Instanzeigners	`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	`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`		
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.

Tabelle 3. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect (Forts.)			
Element	**Standardwert**	**Eigener Wert**	**Anmerkungen**
Startzeit des Zeitplans	`22:00`		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.

Linux

Tabelle 4. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Anmerkungen**
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	`/home/tsminst1/tsminst1`		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 5 auf Seite 14.

Tabelle 4. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems (Forts.)				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Anmerkungen**
Verzeichnis für die aktive Protokolldatei	`/tsminst1/TSMalog`		• Windows Besonders klein: 30 GB • Klein und mittel: 140 GB • Groß: 300 GB	
Verzeichnis für das Archivprotokoll	`/tsminst1/TSMarchlog`		• Windows Besonders klein: 250 GB • Klein: 1 TB • Mittel: 2 TB • Groß: 4 TB	

Verzeichnisse für die Datenbank	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 200 GB
			• Klein: Mindestens 1 TB
			• Mittel: Mindestens 2 TB
			• Groß: Mindestens 4 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:
				• Windows Besonders klein: Mindestens 1 Dateisystem
				• Klein: Mindestens 4 Dateisysteme
				• Mittel: Mindestens 4 Dateisysteme
				• Groß: Mindestens 8 Dateisysteme

Tabelle 4. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems (Forts.)				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Anmerkungen**

Verzeichnisse für Speicher	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 10 TB
			• Klein: Mindestens 38 TB
			• Mittel: Mindestens 180 TB
			• Groß: Mindestens 500 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:
				• Windows Besonders klein: Mindestens 2 Dateisysteme
				• Klein: Mindestens 2 Dateisysteme
				• Mittel: Mindestens 10 Dateisysteme
				• Groß: Mindestens 30 Dateisysteme

Tabelle 4. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems (Forts.)				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Anmerkungen**

Verzeichnisse für Datenbanksicherung	`/tsminst1/TSMbkup00`
	`/tsminst1/TSMbkup01`
	`/tsminst1/TSMbkup02`
	`/tsminst1/TSMbkup03`
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 1 TB
			• Klein: Mindestens 3 TB
			• Mittel: Mindestens 10 TB
			• Groß: Mindestens 16 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank:
				• Windows Besonders klein: Mindestens 1 Dateisystem
				• Klein: Mindestens 2 Dateisysteme
				• Mittel: Mindestens 3 Dateisysteme
				• Groß: Mindestens 3 Dateisysteme
				Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 5. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect			
Element	**Standardwert**	**Eigener Wert**	**Anmerkungen**
Db2-Instanzeigner	`tsminst1`		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 4 auf Seite 11 in einen anderen Wert geändert hatten, ändern Sie auch den Wert für den Db2-Instanzeigner.

Tabelle 5. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect (Forts.)

Element	Standardwert	Eigener Wert	Anmerkungen
Kennwort des Db2-Instanzeigners	`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	`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`		
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.

Tabelle 5. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect (Forts.)			
Element	**Standardwert**	**Eigener Wert**	**Anmerkungen**
Startzeit des Zeitplans	`22:00`		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.

Windows

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

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

Tabelle 6. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems				
Element	**Standardwert**	**Eigener Wert**	**Minimale Verzeichnisgröße**	**Anmerkungen**
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.

Tabelle 6. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems (Forts.)

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
Verzeichnis für die Serverinstanz	`C:\tsminst1`		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 7 auf Seite 19.
Verzeichnis für die aktive Protokolldatei	`C:\tsminst1\TSMalog`		• Windows Besonders klein: 30 GB • Klein und mittel: 140 GB • Groß: 300 GB	
Verzeichnis für das Archivprotokoll	`C:\tsminst1\TSMarchlog`		• Windows Besonders klein: 250 GB • Klein: 1 TB • Mittel: 2 TB • Groß: 4 TB	

Verzeichnisse für die Datenbank	`C:\tsminst1\TSMdbspace00`
	`C:\tsminst1\TSMdbspace01`
	`C:\tsminst1\TSMdbspace02`
	`C:\tsminst1\TSMdbspace03`
	...
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 200 GB
			• Klein: Mindestens 1 TB
			• Mittel: Mindestens 2 TB
			• Groß: Mindestens 4 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:
				• Windows Besonders klein: Mindestens 1 Dateisystem
				• Klein: Mindestens 4 Dateisysteme
				• Mittel: Mindestens 4 Dateisysteme
				• Groß: Mindestens 8 Dateisysteme

Tabelle 6. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems (Forts.)

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen

Verzeichnisse für Speicher	`C:\tsminst1\TSMfile00`
	`C:\tsminst1\TSMfile01`
	`C:\tsminst1\TSMfile02`
	`C:\tsminst1\TSMfile03`
	...
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 10 TB
			• Klein: Mindestens 38 TB
			• Mittel: Mindestens 180 TB
			• Groß: Mindestens 500 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:
				• Windows Besonders klein: Mindestens 2 Dateisysteme
				• Klein: Mindestens 2 Dateisysteme
				• Mittel: Mindestens 10 Dateisysteme
				• Groß: Mindestens 30 Dateisysteme

Tabelle 6. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems (Forts.)

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen

Verzeichnisse für Datenbanksicherung	`C:\tsminst1\TSMbkup00`
	`C:\tsminst1\TSMbkup01`
	`C:\tsminst1\TSMbkup02`
	`C:\tsminst1\TSMbkup03`
			Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:
			• Windows Besonders klein: Mindestens 1 TB
			• Klein: Mindestens 3 TB
			• Mittel: Mindestens 10 TB
			• Groß: Mindestens 16 TB
				Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank:
				• Windows Besonders klein: Mindestens 1 Dateisystem
				• Klein: Mindestens 2 Dateisysteme
				• Mittel: Mindestens 3 Dateisysteme
				• Groß: Mindestens 3 Dateisysteme
				Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 7. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Anmerkungen
Db2-Instanzeigner	`tsminst1`		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 6 auf Seite 16 in einen anderen Wert geändert hatten, ändern Sie auch den Wert für den Db2-Instanzeigner.

Tabelle 7. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect (Forts.)			
Element	**Standardwert**	**Eigener Wert**	**Anmerkungen**
Kennwort des Db2-Instanzeigners	`pAssW0rd`		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
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`		
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	`22:00`		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.

Planung für Speicher

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 und aktive Protokolldatei

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

Speicherpool

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

Zugehörige Informationen

Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten

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 8 auf Seite 22 und Tabelle 9 auf Seite 22 sind die Layoutanforderungen für die Speichergruppen- und Datenträgerkonfiguration beschrieben.

Tabelle 8. 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.
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 9. 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 zwi-

schen Platten und Speichergruppen. Sie können die Beispiele herunterladen und die Arbeitsblätter editieren, um die Speicherkonfiguration für Ihren Server zu planen.

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.

Richtlinien zum Schutz Ihrer Speicherumgebung vor Ransomware-Attacken und zur Wiederherstellung Ihrer Speicherumgebung nach einer Attacke finden Sie in Speicherumgebung vor Ransomware-Attacken schützen.

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 10 auf Seite 23 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 10. 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

Tabelle 10. Szenarios für Administratorrollen (Forts.)	
Szenario	**Typ der zu konfigurierenden Administrator-ID**
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.

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 Informationen

Kommunikation schützen

Planung für die Speicherung verschlüsselter Daten

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

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

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

Zugehörige Informationen

Data encryption considerations for cloud-container storage pools in IBM Spectrum Protect

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 11 auf Seite 25 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 11. 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, anstatt den Standardwert zu verwenden. Der mit der Option **TCPPORT** angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Für den Datenverkehr des Verwaltungsclients können Sie zum Festlegen von Portwerten die Optionen **TCPADMINPORT** und **ADMINONCLIENTPORT** verwenden.
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. Um sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation zu unterstützen, verwenden Sie die Option **TCPPORT** oder **TCPADMINPORT**.
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.

Tabelle 11. Vom Server, Client und Operations Center verwendete Ports (Forts.)

Element	Standardwert	Richtung	Beschreibung
NDMP	Kein Standardwert	Eingehend/ Abgehend	Der Server muss eine abgehende NDMP-Steuerportverbindung zu der NAS-Einheit öffnen können. Der abgehende Steuerport ist die Adresse der unteren Ebene in der Definition der Einheit zum Versetzen von Daten für die NAS-Einheit. Während einer NDMP-Zurückschreibung vom Dateiserver auf den Server muss der Server eine abgehende NDMP-Datenverbindung zu der NAS-Einheit öffnen können. Der Datenverbindungsport, der während einer Zurückschreibung verwendet wird, kann auf der NAS-Einheit konfiguriert werden. Während NDMP-Sicherungen vom Dateiserver auf den Server muss die NAS-Einheit abgehende Datenverbindungen zum Server öffnen können und der Server muss eingehende NDMP-Datenverbindungen akzeptieren können. Mithilfe der Serveroption **NDMPPORTRANGE** können Sie die für die Verwendung als NDMP-Datenverbindungen verfügbare Gruppe von Ports einschränken. Sie können eine Firewall für Verbindungen zu diesen Ports konfigurieren.
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.
Port für den Clientverwaltungsservice	Client-Port: 9028	Eingehend	Der Zugriff auf den Port für den Clientverwaltungsservice muss 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.

Teil 2. Implementierung einer Plattenspeicherdaten-schutzlösung für einen einzelnen Standort

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

Implementierungsroadmap

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

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

Speicherhardware konfigurieren

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

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 Speicher” auf Seite 21.
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.

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 12 auf Seite 30 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 12. 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 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 13 auf Seite 33, 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 13. 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.

Tabelle 13. Optimale Einstellungen für Linux-Kernelparameter (Forts.)	
Parameter	**Beschreibung**
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 14 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 14. 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`

Tabelle 14. Benutzergrenzwerte (ulimit-Werte) (Forts.)			
Typ des Benutzergrenzwerts	**Einstellung**	**Wert**	**Befehl zum Abfragen des Werts**
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

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
    3321360050763008101057800000000000003004214503IBMfcp
   ```

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

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

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 39 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/36005076300810105780000000000003 134G  188M 132G  1%   /tsminst1/
   TSMalog
   ```

6. Überprüfen Sie, ob die in „Benutzer-ID für den Server erstellen” auf Seite 39 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 44.
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 6), 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 für kleine Systeme	Wert für mittelgroße Systeme	Wert für große Systeme
ACTIVELOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Yes	No	No
ARCHLOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	`devconf.dat`	`devconf.dat`	`devconf.dat`
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	`volhist.dat`	`volhist.dat`	`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. Wenn einer der Serveroptionswerte 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.

Zugehörige Informationen

Referenz für Serveroptionen

SETOPT (Serveroption für dynamische Aktualisierung definieren)

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 49 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 81 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.

Zugehörige Tasks

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

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.

Zugehörige Informationen
REGISTER LICENSE (Neue Lizenz registrieren)

Datendeduplizierung konfigurieren

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

Vorbereitende Schritte

Verwenden Sie für diese Task die aufgezeichneten Informationen zu Speicherpoolverzeichnissen (siehe „Arbeitsblätter zur Planung” auf Seite 6).

Vorgehensweise

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

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.

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

Operation	Zeitplan
Clientsicherung	Startet um 22:00 Uhr.
Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall	• Die Datenbanksicherungsoperation startet um 11:00 Uhr bzw. 13 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt. • Die Sicherungsoperationen für Einheitenkonfigurationsinformationen und das Datenträgerprotokoll starten um 17:00 Uhr bzw. 6 Stunden nach dem Start der Datenbanksicherungsoperation. • Das Löschen des Datenträgerprotokolls startet um 20:00 Uhr bzw. 9 Stunden nach dem Start der Datenbanksicherungsoperation.
Bestandsverfall	Startet um 12:00 Uhr bzw. 14 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.

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 Sicherungsoperationen.

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

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

   Dabei ist *Datenbanksicherungsverzeichnisse* eine Liste der für die Datenbanksicherung erstellten Verzeichnisse.

   Linux AIX Wenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit `/tsminst1/TSMbkup00` als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

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

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

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

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

   ```
   set dbrecovery dbback_filedev
   ```

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

Operation	**Beispielbefehl**
Sichern der Datenbank	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **BACKUP DB**. Wenn Sie ein kleines System konfigurieren, setzen Sie den Parameter **COMPRESS** auf YES. Geben Sie beispielsweise auf einem kleinen System den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet: `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Datenbank sichern." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
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`
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 starttime=20:00:00 duration=45 durunits=minutes`

Operation	Beispielbefehl
Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde	Erstellen Sie einen Zeitplan für die Ausführung des Befehls **EXPIRE INVENTORY**. Definieren Sie den Parameter **RESOURCE** auf der Basis der Systemgröße, die Sie konfigurieren: • Kleine Systeme: 10 • Mittelgroße Systeme: 30 • Große Systeme: 40 Geben Sie beispielsweise auf einem mittelgroßen System den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

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

DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

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 53 geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

Clients für Sichern/Archivieren installieren und konfigurieren

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

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

Nächste Schritte

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

Clients registrieren und Zeitplänen zuordnen

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

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**.

Clientverwaltungsservice installieren

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

Vorbereitende Schritte

- Lesen Sie Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices.
- Stellen Sie vor der Installation des Clientverwaltungsservice sicher, dass eine erfolgreiche Verbindung zwischen dem Client für Sichern/Archivieren und dem Server hergestellt wurde. Die Server-Truststore-Datei, die der Client verwendet, verfügt erst über das Secure Sockets Layer-(SSL-)Zertifikat des Servers, nachdem das Clientsystem die Verbindung zum Server hergestellt hat.

Vorgehensweise

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

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM Download-Site, wie beispielsweise IBM Passport Advantage® oder IBM Fix Central, herunter. Suchen Sie nach einem ähnlichen Dateinamen wie `<Version>-IBM_Spectrum_Protect-CMS-Betriebssystem.bin`.
2. Erstellen Sie auf dem Clientsystem, das verwaltet werden soll, ein Verzeichnis und kopieren Sie das Installationspaket in dieses Verzeichnis.
3. Extrahieren Sie den Inhalt der Installationspaketdatei.
4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in das die Installationsdateien und die zugehörigen Dateien extrahiert wurden. Dabei handelt es sich um das in Schritt 2 erstellte Verzeichnis.
5. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen im Assistenten von IBM Installation Manager aus.

   Wenn IBM Installation Manager noch nicht auf dem Clientsystem installiert ist, müssen Sie sowohl IBM Installation Manager als auch die IBM Spectrum Protect-Clientverwaltungsservices auswählen.

Zugehörige Informationen

Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen

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

Vorgehensweise

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

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

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

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

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

  Die Ausgabe sieht ähnlich wie die folgende aus:

```
Listing CMS configuration

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

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

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

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

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

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

Die Ausgabe sieht ähnlich wie die folgende aus:

```
Listing CMS configuration

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

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

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, wird in der Ausgabe die Position der Fehlerprotokolldatei angezeigt.

Der Ausgabetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

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

- Auf Windows-Clientsystemen:

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

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

Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

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

Vorbereitende Schritte

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

- Der Clientverwaltungsservice verwendet nicht die Standardportnummer 9028.
- Der Zugriff auf den Client für Sichern/Archivieren erfolgt nicht über dieselbe IP-Adresse wie für das Clientsystem, auf dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse kann beispielsweise in den folgenden Situationen verwendet werden:

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

Vorgehensweise

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

1. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus.
2. Klicken Sie auf **Details** > **Merkmale**.
3. Geben Sie im Feld 'URL für Ferndiagnose' im Abschnitt 'Allgemein' die URL für den Clientverwaltungsservice auf dem Clientsystem an.

   Die Adresse muss mit `https` beginnen. In der folgenden Tabelle sind Beispiele für die URL für Ferndiagnose aufgeführt.

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

4. Klicken Sie auf **Sichern**.

Nächste Schritte

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

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, „Plattenspeicherlösung für einen einzelnen Standort überwachen", auf Seite 61 ausführen.

Teil 3. Plattenspeicherlösung für einen einzelnen Standort überwachen

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

Informationen zu diesem Vorgang

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 eines täglichen E-Mail-Berichts mit einer Zusammenfassung des Systemstatus konfigurieren.

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

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

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. Um zu überprüfen, ob Ihre IBM Spectrum Protect-Lösung die die Lizenzierungsanforderungen erfüllt, führen Sie die Anweisungen in Überprüfen der Lizenzeinhaltung aus.
4. Informationen zur Konfiguration des Operations Center zum Erstellen von E-Mail-Statusberichten finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.

Nächste Schritte

Beheben Sie alle erkannten Probleme. Wenn ein Problem durch Ändern der Konfiguration Ihrer Lösung behoben werden soll, führen Sie die Anweisungen in Teil 4, „Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten", auf Seite 83 aus. Die folgenden Ressourcen sind ebenfalls verfügbar:

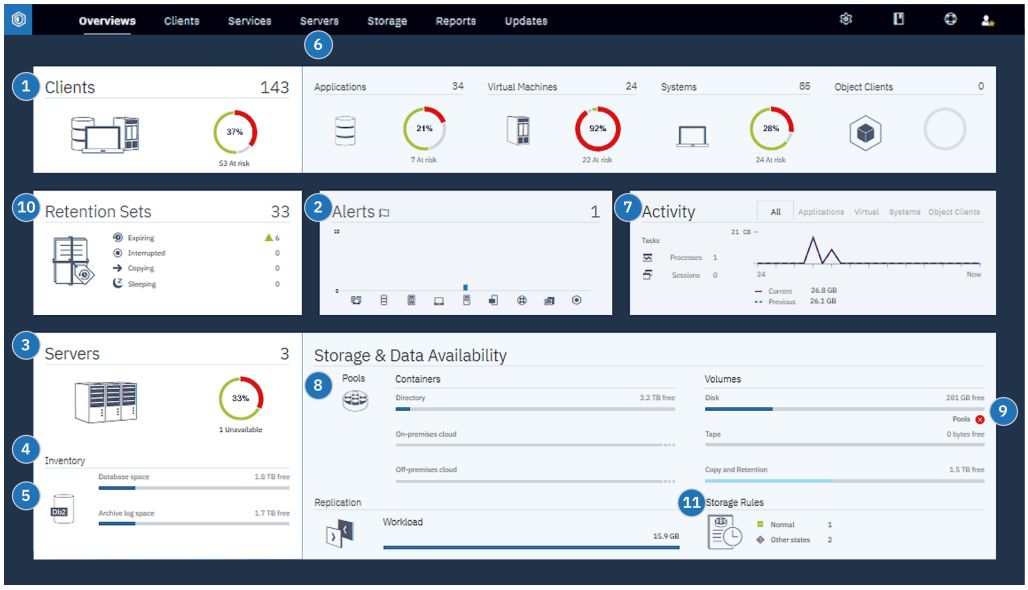
- Informationen zur Behebung von Leistungsproblemen finden Sie in Leistung.
- Informationen zur Behebung anderer Typen von Problemen finden Sie in Fehlerbehebung.

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 15. 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 15. 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 15. 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 15. 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 15. 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 15. 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 15. 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**.	Platteneinheiten können aus den folgenden Gründen den Status 'Kritisch' oder 'Warnung' haben: • Für Einheitenklassen DISK können Datenträger offline sein oder den Zugriffsstatus READONLY (Lesezugriff) haben. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Datenträger angezeigt. • Für nicht gemeinsam genutzte Einheitenklassen FILE können Verzeichnisse offline sein. Außerdem ist unter Umständen nicht genügend freier Speicherbereich für die Zuordnung von Arbeitsdatenträgern verfügbar. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Verzeichnisse angezeigt. • Für gemeinsam genutzte Einheitenklassen FILE sind Laufwerke unter Umständen nicht verfügbar. Ein Laufwerk ist inaktiviert, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. In anderen Spalten der Tabelle 'Platteneinheiten' wird der Status der Laufwerke und Pfade angezeigt.

Tabelle 15. 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 15. 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 Ihre IBM Spectrum Protect-Lösung ordnungsgemäß funktioniert, 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 16. 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**. Führen Sie die Anweisungen in QUERY ACTLOG (Aktivitätenprotokoll abfragen) aus. 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**.	Informationen zur Verkürzung 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 16. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Bestimmen Sie die Platteneinsparungen, die durch die Datendeduplizierung bereitgestellt werden.	1. Klicken Sie auf der Seite **Übersicht** im Operations Center auf **Pools**. 2. Wählen Sie einen Pool aus und klicken Sie auf **Kurzübersicht**. 3. Zeigen Sie im Bereich 'Datendeduplizierung' die Zeile 'Eingesparter Speicherbereich' an.	Um für die erweiterte Überwachung detaillierte Statistikdaten zu dem Datendeduplizierungsprozess für einen bestimmten Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abzurufen, 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. Fordern Sie einen Statistikbericht an, indem Sie den Befehl **GENERATE DEDUPSTATS** ausgeben. Führen Sie die Anweisungen in GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool generieren) aus. 3. Zeigen Sie den Statistikbericht an, indem Sie den Befehl **QUERY DEDUPSTATS** ausgeben. Führen Sie die Anweisungen in QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen) aus.

Tabelle 16. 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 16. Regelmäßige Überwachungstasks (Forts.)

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Bestimmen Sie, ob für das Instanzverzeichnisdateisystem genügend Speicherbereich verfügbar ist.	Stellen Sie sicher, dass im Instanzverzeichnisdateisystem mindestens 20 % 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:
	• AIX Linux `/home/tsminst1/tsminst1`
	• Windows `C:\tsminst1`
	Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.	

Tabelle 16. 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 16. 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 in dem Containerspeicherpool.

Tabelle 16. 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.
Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass die Start- und Endzeiten von Clientzeitplänen Ihre Geschäftsanforderungen erfüllen.	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**.
Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass die Start- und Endzeiten von Verwaltungstasks Ihre Geschäftsanforderungen erfüllen.	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.	**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. Anweisungen finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Informationen

QUERY ACTLOG (Aktivitätenprotokoll abfragen)
UPDATE STGPOOL (Speicherpool aktualisieren)
QUERY EXTENTUPDATES (Aktualisierte Datenbereiche 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.

Option	Bezeichnung
	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 sendet, 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.

Zugehörige Informationen

UPDATE ADMIN (Administrator aktualisieren)

Teil 4. Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten

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

Operations Center verwalten

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. 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.

Peripherieserver hinzufügen und entfernen

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

Informationen zu diesem Vorgang

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

Peripherieserver hinzufügen

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

Vorbereitende Schritte

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

Vorgehensweise

1. Klicken Sie in der Menüleiste des Operations Center auf **Server**.

   Die Seite **Server** wird geöffnet.

   In der Tabelle auf der Seite **Server** könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl **DEFINE SERVER** für den Hub-Server definiert hat - der Server noch nicht als Peripherieserver konfiguriert ist.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf **Peripherieserver überwachen**.
   - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf **+Peripherieserver**.
3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.

Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

Peripherieserver entfernen

Sie können einen Peripherieserver aus dem Operations Center entfernen.

Informationen zu diesem Vorgang

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

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

Vorgehensweise

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

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

   ```
   QUERY MONITORSETTINGS
   ```

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

   ```
   DELETE GRPMEMBER Gruppenname Mitgliedsname
   ```

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

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

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

   ```
   DELETE SERVER Name_des_Peripherieservers
   ```

   Tipp: Wenn eine Serverdefinition sofort nach dem Entfernen des Servers aus der überwachten Gruppe gelöscht wird, können Statusinformationen für den Server ohne zeitliche Begrenzung im Operations Center verbleiben.

   Um dieses Problem zu verhindern, warten Sie, bis das Intervall für die Erfassung von Statusdaten überschritten wurde, bevor Sie die Serverdefinition löschen. Das Intervall für die Erfassung von Statusdaten wird auf der Seite 'Einstellungen' des Operations Center angezeigt.

Web-Server starten und stoppen

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

Vorgehensweise

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

     ```
     ./stopserver.sh
     ```

   - Linux Geben Sie den folgenden Befehl aus:

     ```
     service opscenter.rc stop
     ```

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

     ```
     ./startserver.sh
     ```

   - Linux Geben Sie die folgenden Befehle aus:

     Starten Sie den Server:

     ```
     service opscenter.rc start
     ```

     Starten Sie den Server erneut:

     ```
     service opscenter.rc restart
     ```

     Bestimmen Sie, ob der Server aktiv ist:

     ```
     service opscenter.rc status
     ```

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

Assistenten für die Erstkonfiguration erneut starten

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

Vorbereitende Schritte

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

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

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

Informationen zu diesem Vorgang

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

Vorgehensweise

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

   Beispiel:
   - AIX Linux /opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Windows c:\Programme\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Löschen Sie im Verzeichnis guiServer die Datei serverConnection.properties.
4. Starten Sie den Web-Server des Operations Center.
5. Öffnen Sie das Operations Center.
6. Rekonfigurieren Sie mithilfe des Konfigurationsassistenten das Operations Center.

   Geben Sie ein neues Kennwort für die Überwachungsadministrator-ID an.
7. Aktualisieren auf jedem Peripherieserver, der bereits zuvor mit dem Hub-Server verbunden war, das Kennwort für die Überwachungsadministrator-ID, indem Sie den folgenden Befehl in der IBM Spectrum Protect-Befehlszeilenschnittstelle ausgeben:

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

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

Hub-Server ändern

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

Vorgehensweise

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

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

Zugehörige Tasks

Assistenten für die Erstkonfiguration erneut starten

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

Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben

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

Vorgehensweise

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

1. Stoppen Sie den Web-Server des Operations Center.

2. Dekonfigurieren Sie den Hub-Server, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie auf dem Hub-Server die folgenden Befehle aus:

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

   Tipp: IBM-OC-*Name_des_Hub-Servers* ist die Überwachungsadministrator-ID, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

   b) Setzen Sie das Kennwort für den Hub-Server zurück, indem Sie den folgenden Befehl auf dem Hub-Server ausgeben:

```
SET SERVERPASSWORD ""
```

   Achtung: Führen Sie diesen Schritt nicht aus, wenn der Hub-Server für andere Server für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation konfiguriert ist.

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

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

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

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

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

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

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

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

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

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

```
DELETE SERVER Name_des_Hub-Servers
```

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

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

```
DELETE SERVER Name_des_Peripherieservers
```

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

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

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

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

Zugehörige Tasks

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

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

Anwendungen, virtuelle Maschinen und Systeme schützen

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

Clients hinzufügen

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

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 89 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 91 aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in „Sicherungs- und Archivierungsoperationen planen" auf Seite 94 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 95 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 96 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 96 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 94 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 92 ausführen.
2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in „Maßnahmen editieren" auf Seite 93 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**.

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 95 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 ge-

stellt 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 97.

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

Software	Link zu Anweisungen
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
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 95).
   - 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. 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” auf Seite 57 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 98 aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in „Client/Server-Kommunikation durch eine Firewall konfigurieren” auf Seite 100 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 104 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.

Clientoperationen verwalten

Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

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.

Detaillierte Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in Clientprobleme lösen.

Fehler in Clientfehlerprotokollen auswerten

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

Vorbereitende Schritte

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” auf Seite 57. Anweisungen zur Überprüfung der Installation finden Sie in „Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen” auf Seite 57.

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 ge-

sperrt. 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.

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.

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

Speicherpoolcontainer prüfen

Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

Informationen zu diesem Vorgang

Sie prüfen einen Speicherpoolcontainer in den folgenden Situationen:

- Sie geben den Befehl **QUERY DAMAGED** aus und es wird ein Problem erkannt.

- Der Server zeigt Nachrichten zu beschädigten Datenbereichen an.
- Ihre Hardware meldet ein Problem und es werden Fehlernachrichten angezeigt, die sich auf den Speicherpoolcontainer beziehen.

Vorgehensweise

1. Um einen Speicherpoolcontainer zu prüfen, geben Sie den Befehl **AUDIT CONTAINER** aus. Geben Sie beispielsweise den folgenden Befehl aus, um den Container `000000000000076c.dcf` zu prüfen:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Überprüfen Sie die Ausgabe der Nachricht ANR4891I auf Informationen zu allen beschädigten Datenbereichen.

Nächste Schritte

Wenn Sie Probleme mit dem Speicherpoolcontainer erkennen, können Sie Daten auf der Basis Ihrer Konfiguration zurückschreiben. Geben Sie den Befehl **AUDIT CONTAINER** aus und geben Sie den Containernamen an.

Zugehörige Informationen

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)

QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)

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.
- 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 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 Verzeich-

nisse 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.

- Um die Größe der Datenbank für Server der Version 7.1 und höher zu verringern, geben Sie im Serverinstanzverzeichnis die folgenden IBM Db2-Befehle aus:

  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.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- 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. Wenn ein Protokollspiegel vorhanden ist, muss auch die Position für den Spiegel über genügend Speicherbereich für die erhöhte Protokollgröße verfügen.
  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 17. 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)

Speichernutzung und Prozessorauslastung verwalten

Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datendeduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.

Vorbereitende Schritte

- Stellen Sie sicher, dass Ihre Konfiguration die erforderliche Hardware und Software verwendet. Weitere Informationen finden Sie in Supported Operating Systems.
- Weitere Informationen zur Verwaltung von Ressourcen, wie beispielsweise Datenbank und Wiederherstellungsprotokoll, finden Sie in Planung der Speicherarrays.

- Fügen Sie zusätzlichen Systemspeicher hinzu, um festzustellen, ob sich die Leistung verbessert. Überwachen Sie die Speichernutzung regelmäßig, um zu bestimmen, ob weiterer Speicher erforderlich ist.

Vorgehensweise

1. Geben Sie, falls möglich, Speicherbereich aus dem Dateisystemcache frei.
2. Verwenden Sie zur Verwaltung des Systemspeichers, den jeder Server auf einem System verwendet, die Serveroption DBMEMPERCENT. Begrenzen Sie den Prozentsatz des Systemspeichers, der vom Datenbankmanager jedes Servers verwendet werden kann. Wenn alle Server gleich wichtig sind, verwenden Sie denselben Wert für jeden Server. Wenn ein Server der Produktionsserver ist und die anderen Server Testserver sind, definieren Sie für den Produktionsserver einen höheren Wert als für die Testserver.
3. Definieren Sie den Benutzerdatengrenzwert und den privaten Speicher für die Datenbank, um sicherzustellen, dass immer genügend privater Speicher verfügbar ist. Wenn der private Speicher knapp wird, kann dies Fehler, eine nicht optimale Leistung und Instabilität zur Folge haben.

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, „Plattenspeicherlösung für einen einzelnen Standort überwachen", auf Seite 61.
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

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.

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 18. 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 erforder-

lich, 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 19. 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

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`

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.

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 20. 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`

Zugehörige Informationen

IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren

Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1)

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 115.
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
   ```

Zugriff über Porteinschränkungen einschränken

Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

Informationen zu diesem Vorgang

Gegebenenfalls müssen Sie abhängig von Ihren Sicherheitsanforderungen den Zugriff auf bestimmte Server einschränken. Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass er an vier TCP/IP-Ports empfangsbereit ist: zwei Ports, die für reguläre TCP/IP-Protokolle oder SSL-/TLS-Protokolle verwendet werden können, und zwei Ports, die nur für das SSL-/TLS-Protokoll verwendet werden können.

Vorgehensweise

Sie können die Serveroptionen wie in Tabelle 21 auf Seite 118 aufgeführt zur Angabe des erforderlichen Ports festlegen.

Tabelle 21. Serveroptionen und Portzugriff

Serveroption	Portzugriff
TCPPORT	Gibt die Nummer des Ports an, dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist 1500.

Tabelle 21. Serveroptionen und Portzugriff (Forts.)	
Serveroption	**Portzugriff**
TCPADMINPORT	Gibt die Nummer des Ports an, an dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von anderen Sitzungen als Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist der Wert für **TCPPORT**. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen **TCPPORT** und **SSLTCPPORT** verwendet, zu trennen.
SSLTCPPORT	Gibt die SSL-TCP/-IP-Portadresse für einen Server an. Dieser Port ist nur für SSL-fähige Sitzungen empfangsbereit. Ein Standardwert für den Port ist nicht verfügbar.
SSLTCPADMINPORT	Gibt die Portadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen von SSL-fähigen Sitzungen wartet. Ein Standardwert für den Port ist nicht verfügbar. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen **TCPPORT** und **SSLTCPPORT** verwendet, zu trennen.

Einschränkungen:

Wenn Sie die Server-Ports, die nur für SSL gelten, (**SSLTCPPORT** und **SSLTCPADMINPORT**) angeben, gelten die folgenden Einschränkungen:

- Wenn Sie den Server-Port, der nur für SSL gilt, für den Parameter **LLADDRESS** im Befehl **DEFINE SERVER** oder im Befehl **UPDATE SERVER** angeben, müssen Sie auch den Parameter **SSL=YES** angeben.
- Wenn Sie den Server-Port, der nur für SSL gilt, für die Clientoption **TCPPORT** angeben, müssen Sie auch **YES** für die SSL-Clientoption angeben.

Zugehörige Verweise

Planung des Firewallzugriffs

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

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.

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**.

Plan zur Wiederherstellung nach einem Katastrophenfall implementieren

Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.

Informationen zu diesem Vorgang

Bestimmen Sie Ihre Anforderungen für die Wiederherstellung nach einem Katastrophenfall, indem Sie die Geschäftsprioritäten für die Clientknotenwiederherstellung und die Systeme, die zum Wiederherstellen von Daten verwendet werden, angeben und prüfen, ob Clientknoten über eine Verbindung zu einem Wiederherstellungsserver verfügen. Verwenden Sie zum Schützen von Daten Replikation und Speicherpoolschutz. Außerdem müssen Sie bestimmen, wie oft Verzeichniscontainerspeicherpools geschützt werden.

Wiederherstellungsdrilloperationen 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.

Informationen zu diesem Vorgang

Einschränkungen: Für Plattenspeicherlösungen für einen einzelnen Standort gelten die folgenden Einschränkungen:

- Sie können nur die Datenbank zurückschreiben.
- Die Replikation kann nicht verwendet werden, da am Wiederherstellungsstandort kein Zielserver vorhanden ist.
- Bei beschädigten Speicherpools ist keine Wiederherstellung möglich.

Vorgehensweise

Stellen Sie sicher, dass die Datenbank gesichert wird, indem Sie die folgenden Schritte ausführen:

a. Wählen Sie auf der Seite **TSM-Server** im Operations Center den Server aus, dessen Datenbank gesichert werden soll.
b. Klicken Sie auf **Sichern** und führen Sie die Anweisungen im Fenster **Serverdatenbank sichern** aus.

Wiederherstellung nach einem Systemausfall

Bei IBM Spectrum Protect-Plattenspeicherlösungen für einen einzelnen Standort können Sie den Bestand nur lokal wiederherstellen und die Datenbank zum Schutz Ihrer Daten zurückschreiben.

Vorgehensweise

Verwenden Sie abhängig vom Typ der gesicherten Informationen eine der folgenden Methoden, um den Bestand an einem lokalen Standort wiederherzustellen.

Einschränkung: Da bei Plattenspeicherlösungen für einen einzelnen Standort keine zweite Kopie des Speicherpools vorhanden ist, können Speicherpools nicht zurückgeschrieben werden. Informationen zur Architektur von Plattenspeicherlösungen finden Sie in -Lösung für Ihre Umgebung auswählen.

Tabelle 22. Szenarios für die Wiederherstellung nach einem Katastrophenfall

Szenario	Prozedur
Der Zugriff auf Ihr System ist nicht möglich und das System soll mithilfe von Systemtools lokal mit dem Stand einer früheren Version zurückgeschrieben werden.	• Verwenden Sie IBM Spectrum Protect, um den Server auf einem anderen Server zu sichern. • Verwenden Sie Betriebssystemtools, um Ihr System zu sichern und mit dem Stand einer früheren Version zurückzuschreiben.
Bei einem Ausfall oder einer Katastrophe sollen Ihre Daten aus gesicherten Versionen der Daten zurückgeschrieben werden.	• Um einen Client zu sichern, wählen Sie auf der Seite **TSM-Clients** im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf **Sichern**. • Wählen Sie auf der Seite **TSM-Server** im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf **Sichern** und führen Sie die Anweisungen im Fenster **Serverdatenbank sichern** aus. Um einen Speicherpool aus einer gesicherten Version des Speicherpools zurückzuschreiben, müssen Sie die Datenbank zurückschreiben. Geben Sie den Befehl **DSMSERV RESTORE DB** aus, um die Datenbank und zugehörige Speicherpools mit dem Stand einer gesicherten Version zurückzuschreiben.

Zugehörige Informationen

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
DSMSERV RESTORE DB (Datenbank zurückschreiben)

Datenbank zurückschreiben

Unter Umständen müssen Sie die IBM Spectrum Protect-Datenbank nach einem Katastrophenfall zurückschreiben. Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Zum Zurückschreiben der Datenbank benötigen Sie Datenträger mit einer Datenbankgesamt-, -teil- oder -momentaufnahmesicherung.

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** verwenden. Verwenden Sie beispielsweise die folgenden Befehle:

Linux AIX

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

Windows

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

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 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.

Informationen zu diesem Vorgang

Operationen für die Zurückschreibung nach Zeitpunkt werden normalerweise bei der Wiederherstellung nach einem Katastrophenfall oder zum Entfernen der Auswirkungen von Fehlern verwendet, die Inkonsistenzen in der Datenbank zur Folge haben können. 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.

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 2015 erstellt wurde, verwenden Sie den folgenden Befehl:

```
dsmserv restore db todate=04/19/2015
```

Nächste Schritte

Wenn Sie die Datenbank zurückgeschrieben haben und Verzeichniscontainerspeicherpools auf dem Server vorhanden sind, müssen Sie Inkonsistenzen zwischen der Datenbank und dem Dateisystem ermitteln.

1. Wenn Sie die Datenbank mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben haben und die Wiederverwendung des Verzeichniscontainerspeicherpools nicht verzögert wurde, müssen Sie alle Container prüfen. Um alle Container zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool
   ```

2. Wenn der Server keine Container auf dem System identifizieren kann, führen Sie die folgenden Schritte aus, um eine Liste der Container anzuzeigen:

   a. Geben Sie über einen Verwaltungsclient den folgenden Befehl aus:

      ```
      select container_name from containers
      ```

   b. Geben Sie für das Dateisystem den folgenden Befehl für das Speicherpoolverzeichnis auf dem Quellenserver aus:

      Tipp: Das Speicherpoolverzeichnis wird in der Befehlsausgabe angezeigt:

      Linux AIX
      ```
      [Root@Quelle]$ ls -lR
      ```

      Windows
      ```
      c:\Quellenspeicherpoolverz>Verz /s
      ```

   c. Vergleichen Sie die für das Dateisystem und den Server aufgelisteten Container.

   d. Geben Sie den Befehl **AUDIT CONTAINER** unter Angabe des Containers aus, der in der Serverausgabe fehlt. Geben Sie den Parameter **ACTION=REMOVEDAMAGED** an, um den Container zu löschen.

   e. Um sicherzustellen, dass die Container im Dateisystem gelöscht wurden, überprüfen Sie die angezeigten Nachrichten.

      Tipp: Wenn nach einer Datenbankzurückschreibungsoperation Container in dem Dateisystem vorhanden sind, die nicht in der Serverdatenbank referenziert werden, wird mit dem Befehl **QUERY STGPOOL** die Speicherpoolverwendung nicht korrekt angezeigt. Wenn Sie eine Datenbank mit dem Stand eines bestimmten Zeitpunkts zurückschreiben, verbleiben Container möglicherweise im Dateisystem, werden aber in der Serverdatenbank nicht referenziert. Um sicherzustellen, dass die Statistikdaten zur Speicherpoolverwendung korrekt sind, müssen Sie alle Container, die im Dateisystem verfügbar sind, aber in der Serverdatenbank nicht referenziert werden, manuell löschen.

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

G

H

I

K

L

M

O

P

R

S

T

U

V

W

Z

Programmnummer: 5725-W98
5725-W99
5725-X15