IBM Spectrum Protect for Virtual Environments
Version 8.1.6

Data Protection for VMware Installationshandbuch

IBM Spectrum Protect for Virtual Environments
Version 8.1.6

Data Protection for VMware Installationshandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 135 gelesen werden.

Diese Ausgabe bezieht sich auf Version 8, Release 1, Modifikation 6 von IBM Spectrum Protect for Virtual Environments (Produktnummer 5725-X00) und auf alle nachfolgenden Releases und Modifikationen, sofern in neuen Ausgaben nicht anders angegeben.

Inhaltsverzeichnis

Informationen zu dieser Veröffentlichung

IBM Spectrum Protect for Virtual Environments stellt inkrementelle Off-Host-Sicherungen auf Blockebene sowie eine Dateiwiederherstellung und einen Instant Restore aus einer vollständigen VM-Sicherung für Windows- und Linux-Gastmaschinen bereit. Inkrementelle Sicherungen auf Blockebene sind verfügbar, wenn Sie IBM Spectrum Protect for Virtual Environments zusammen mit der IBM Spectrum Protect-Einheit zum Versetzen von Daten verwenden.

Zielgruppe

Diese Veröffentlichung richtet sich an Benutzer und Administratoren, die IBM Spectrum Protect for Virtual Environments installieren und konfigurieren möchten.

Übersichtsinformationen, Benutzertasks, Szenarios für Sicherung und Zurückschreibung, eine Befehlsreferenz und Fehlernachrichten sind im *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware Benutzerhandbuch* dokumentiert.

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 Version 8.1.6

IBM Spectrum Protect for Virtual Environments Version 8.1.6 enthält neue Funktionen und Aktualisierungen.

Eine Liste der neuen Funktionen und Aktualisierungen in diesem Release und in vorherigen Releases von Version 8 finden Sie in Aktualisierungen für Data Protection for VMware.

Neue und geänderte Informationen in dieser Produktdokumentation sind durch einen vertikalen Balken (|) am linken Rand gekennzeichnet.

Kapitel 1. Data Protection for VMware installieren und aktualisieren

Die Installation von IBM Spectrum Protect for Virtual Environments umfasst die Planung, die Installation und die Erstkonfiguration.

Installierbare Komponenten

Data Protection for VMware umfasst verschiedene Komponenten, die Sie installieren können, um Ihre virtuelle Umgebung zu schützen.

Je nach der Betriebssystemumgebung sind die folgenden Data Protection for VMware-Features für die Installation verfügbar:

Einschränkung: Jedes Installationspaket umfasst eine Benutzerlizenzdatei (EULA). Wenn Sie die Bedingungen in der Datei nicht akzeptieren, wird der Installationsprozess gestoppt.

Tabelle 1. Verfügbare Data Protection for VMware-Features nach Betriebssystem

Komponente	Linux	Windows
IBM Spectrum Protect Recovery Agent Diese Komponente stellt Funktionalität für virtuelle Bereitstellung und Instant Restore zur Verfügung.		√
Recovery Agent-Befehlszeilenschnittstelle Die Befehlszeilenschnittstelle, die für Mountoperationen verwendet wird.		√
Dokumente Die Dokumente umfassen die Readme-Datei und die Datei mit den Bemerkungen.	√	√
Data Protection for VMware-Aktivierungsdatei Diese Komponente versetzt IBM Spectrum Protect in die Lage, die folgenden Sicherungstypen auszuführen: • Sicherung des Typs 'Immer inkrementell - Inkrementell' • Sicherung des Typs 'Immer inkrementell - Vollständig' Diese Komponente ist für den Anwendungsschutz erforderlich. Wenn Sie Sicherungsarbeitslast auslagern, muss diese Datei auf dem vStorage-Sicherungsserver installiert sein.	√	√

Tabelle 1. Verfügbare Data Protection for VMware-Features nach Betriebssystem (Forts.)

Komponente	Linux	Windows
Data Protection for VMware vSphere-GUI Diese Komponente ist eine grafische Benutzerschnittstelle (Graphical User Interface - GUI), die auf VM-Daten auf dem VMware vCenter-Server zugreift. Der Inhalt der GUI ist in diesen Sichten verfügbar: • Web-Browser-Sicht. Der Zugriff auf diese Sicht erfolgt in einem unterstützten Web-Browser unter Verwendung der URL für den Web-Server-Host der GUI. Beispiel: `https://guihost.mycompany.com:9081/TsmVMwareUI/` • Sicht des IBM Spectrum Protect vSphere-Client-Plug-ins im VMware vSphere-Web-Client. Die Anzeigen in dieser Sicht wurden speziell für die Integration in den Web-Client entwickelt; die Daten und Befehle für diese Sicht werden jedoch von demselben GUI-Web-Server abgerufen wie bei den anderen Sichten. Das IBM Spectrum Protect vSphere-Client-Plug-in stellt eine Untergruppe der Funktionen, die in der Web-Browser-Sicht verfügbar sind, sowie einige zusätzliche Funktionen bereit. Funktionen für die Konfiguration und erweiterte Berichte sind in dieser Sicht nicht verfügbar. Sie können während der Installation eine oder mehrere Sichten angeben.	√	√
GUI für Dateizurückschreibung Diese Komponente ist eine webbasierte GUI, mit der Sie ohne Administratorunterstützung Dateien aus der Sicherung einer virtuellen VMware-Maschine zurückzuschreiben können. Die GUI wird automatisch mit der Data Protection for VMware-GUI installiert. Sie wird über den Konfigurationsassistenten aktiviert.	[1]	√
Einheit zum Versetzen von Daten Die IBM Spectrum Protect-Einheit zum Versetzen von Daten versetzt Daten für Data Protection for VMware. Diese Funktionalität wird als 'Einheit zum Versetzen von Daten' bezeichnet. Die Einheit zum Versetzen von Daten versetzt Daten aus der virtuellen Umgebung auf den IBM Spectrum Protect-Server. Wenn Sie die Einheit zum Versetzen von Daten auf einem Server installieren, kann der Server als vStorage-Sicherungsserver verwendet werden. Sie können die Einheit zum Versetzen von Daten auf demselben System wie Data Protection for VMware oder auf einem anderen Server installieren.	√	√

1. Die Komponente der Schnittstelle für Dateizurückschreibung muss zwar auf einem Windows-System installiert und aktiviert sein, aber mithilfe dieser Schnittstelle können Sie Dateien sowohl auf virtuellen Windows- als auch auf virtuellen Linux-Gastmaschinen zurückschreiben.

2. Der Client für Sichern/Archivieren und die Data Protection for VMware-Einheit zum Versetzen von Daten dürfen nicht auf demselben Windows- oder Linux-System installiert sein.

Data Protection for VMware lagert die Sicherungsarbeitslast von virtuellen Maschinen auf einen vStorage-Sicherungsserver aus. Damit diese Task ausgeführt werden kann, muss die Einheit zum Versetzen von Daten V8.1.4 auf dem vStorage-Sicherungsserver installiert sein.

Data Protection for VMware vSphere-GUI

Die Komponente Data Protection for VMware vSphere-GUI (vSphere-GUI) ist eine grafische Benutzerschnittstelle, die auf VM-Daten auf dem VMware vCenter-Server zugreift.

Übersicht

Die Data Protection for VMware vSphere-GUI ist die wichtigste Schnittstelle für die Ausführung der folgenden Tasks:

- Sicherungen Ihrer VMs einleiten oder planen, die auf einem IBM Spectrum Protect-Server gespeichert werden.
- Vollständige Wiederherstellung Ihrer VMs aus einem IBM Spectrum Protect-Server einleiten.
- Berichte zum Fortschritt Ihrer Tasks, zu den kürzlich abgeschlossenen Ereignissen, zum Sicherungsstatus und zur Speicherbereichsbelegung ausgeben. Diese Informationen sind bei der Behebung von Fehlern hilfreich, die bei der Sicherungsverarbeitung aufgetreten sind.

Tipp: Informationen zur Vorgehensweise bei der Ausführung von Tasks mit der vSphere-GUI werden in der Onlinehilfe bereitgestellt, die mit der GUI installiert wird. Klicken Sie in einem beliebigen GUI-Fenster auf **Weitere Informationen**, um die Onlinehilfe mit Informationen zur Ausführung von Tasks zu öffnen.

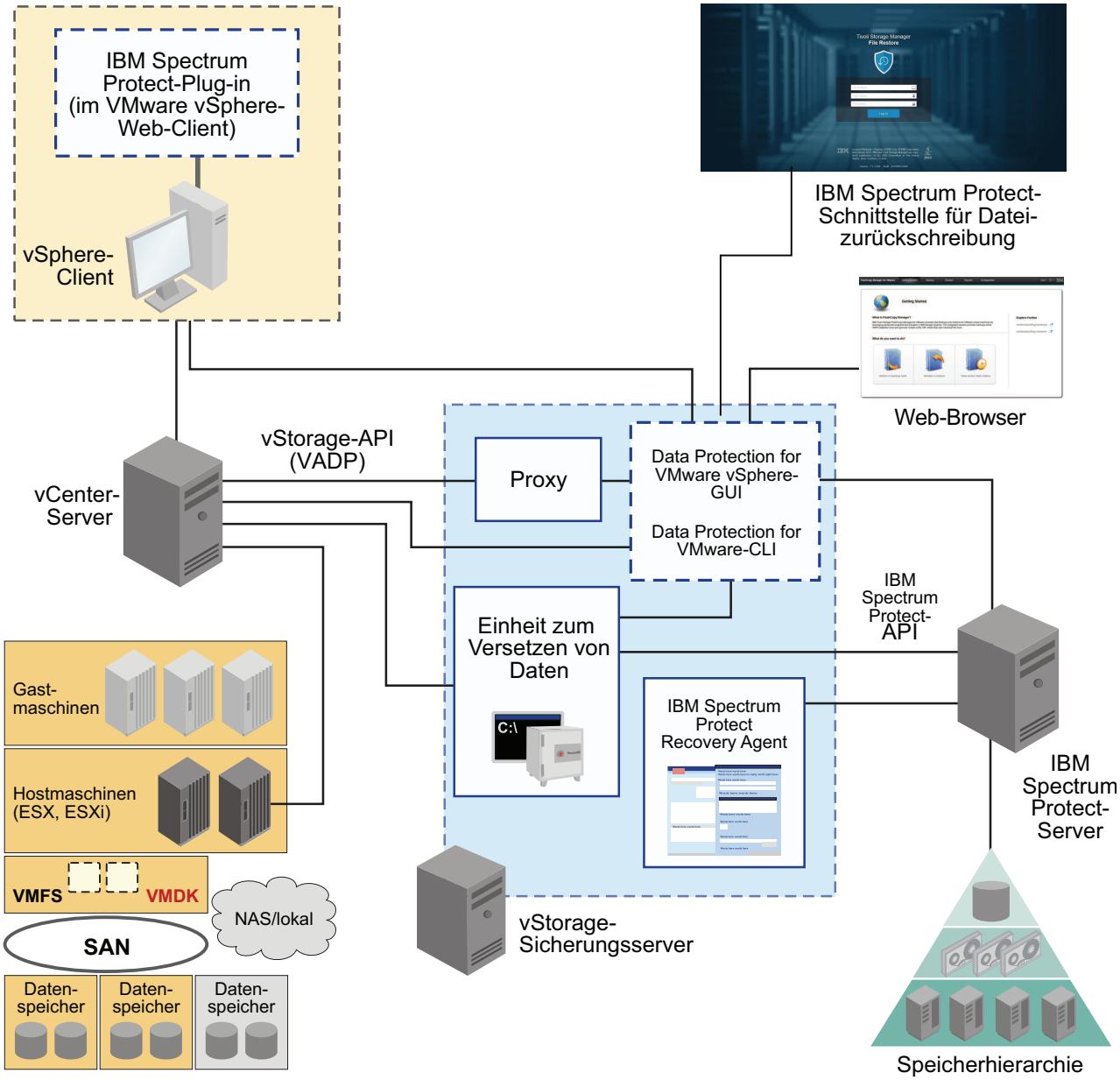

Abbildung 1. Systemkomponenten von Data Protection for VMware in einer VMware vSphere-Benutzerumgebung

Voraussetzungen

Die Data Protection for VMware vSphere-GUI kann auf jedem System installiert werden, das die Betriebssystemvoraussetzungen erfüllt. Der Ressourcenbedarf der vSphere-GUI ist minimal, da sie keine E/A-Datenübertragungen verarbeitet.

Tipp: Die Installation der vSphere-GUI auf dem vStorage-Sicherungsserver ist die häufigste Konfiguration.

Die vSphere-GUI benötigt Netzkonnektivität zu den folgenden Systemen:

- vStorage-Sicherungsserver
- IBM Spectrum Protect-Server
- vCenter-Server

Darüber hinaus müssen Ports für die Derby-Datenbank (Standardwert: 1527) und den GUI-Web-Server (Standardwert: 9081) verfügbar sein.

Konfiguration

Sie können mehrere vSphere-GUIs bei einem einzigen vCenter-Server registrieren. Durch dieses Szenario reduziert sich die Anzahl der Datencenter (und ihrer Sicherungen für VM-Gastmaschinen), die von einer einzelnen VMware vSphere-GUI verwaltet werden. Ein vCenter-Server kann anschließend eine Untergruppe aller Datencenter verwalten, die auf dem vCenter-Server definiert sind.

Zum Aktualisieren der verwalteten Datencenter rufen Sie **Konfiguration** > **Konfiguration editieren** auf.

Wenn Sie mehrere vSphere-GUIs bei einem einzigen vCenter-Server registrieren, gelten die folgenden Richtlinien:

- Jedes Datencenter kann nur von einer einzigen installierten vSphere-GUI verwaltet werden.
- Ein eindeutiger VMCLI-Knotenname ist für jede installierte vSphere-GUI erforderlich.
- Die Verwendung eindeutiger Knotennamen der Einheit zum Versetzen von Daten für jede installierte vSphere-GUI vereinfacht die Verwaltung der Knoten.

Auf die vSphere-GUI zugreifen

Für die vSphere-GUI werden die folgenden Zugriffsmethoden bereitgestellt:

- Eine eigenständige Web-Browser-GUI. Auf diese GUI greifen Sie über ein URL-Lesezeichen für den GUI-Web-Server zu, z. B.:

  `https://`*`Hostname`*`:`*`Port`*`/TsmVMwareUI/`

  Dabei gilt Folgendes:
  - *Hostname* ist der Name des Systems, auf dem die Data Protection for VMware vSphere-GUI installiert ist.
  - *Port* ist die Portnummer, über die auf die vSphere-GUI zugegriffen wird. Die Standardportnummer ist 9081.
- Eine vSphere-Web-Client-Erweiterung, die eine Verbindung zu einem GUI-Web-Server herstellt, um auf virtuelle Maschinen im IBM Speicher zuzugreifen (wird als Data Protection-Erweiterung bezeichnet). Der Inhalt ist eine Untergruppe des Inhalts, der in der Web-Browser-GUI zur Verfügung gestellt wird.

Sie können während der Installation eine oder mehrere Zugriffsmethoden angeben.

Windows Das Standardinstallationsverzeichnis ist `C:\IBM\SpectrumProtect\webserver`.

Linux Das Standardinstallationsverzeichnis ist `/opt/tivoli/tsm/tdpvmware/common/webserver`.

IBM Spectrum Protect Recovery Agent

Verwenden Sie den Recovery Agent-Service, um einen beliebigen Momentaufnahmedatenträger vom IBM Spectrum Protect-Server bereitzustellen.

Übersicht

Sie können das iSCSI-Protokoll verwenden, um von einem fernen System aus auf eine Momentaufnahme zuzugreifen.

Wenn Sie Momentaufnahmen lokal mit Lesezugriff auf dem Clientsystem anzeigen müssen, verwenden Sie Data Protection for VMware Version 8.1.4 oder frühere Versionen.

Darüber hinaus stellt der Recovery Agent sowohl die Funktion Instant Restore als auch Schutz für In-Guest-Anwendungen bereit. Mit Instant Restore bleibt der verwendete Datenträger verfügbar, während die Zurückschreibungsoperation im Hintergrund fortgesetzt wird. Mit Anwendungsschutz sind Anwendungen wie Microsoft Exchange Server und Microsoft SQL Server, die auf einer virtuellen Gastmaschine installiert sind, für den Schutz durch Sicherung und Zurückschreibung verfügbar.

Der Recovery Agent kann die folgenden Tasks von einem fernen System aus ausführen:

- Informationen zu den Daten zusammenstellen, die zurückgeschrieben werden können, z. B.:
  - Gesicherte VMs
  - Verfügbare Momentaufnahmen für eine gesicherte virtuelle Maschine
  - Verfügbare Partitionen in einer bestimmten Momentaufnahme

Ausführliche Informationen zu Befehlen, Parametern und Rückkehrcodes enthält der Befehlsreferenzabschnitt im *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware Benutzerhandbuch*.

Voraussetzungen

Windows Auf Windows-Systemen werden die Recovery Agent-GUI und die Befehlszeilenschnittstelle im Rahmen einer vollständigen Installation von Data Protection for VMware oder einer erweiterten Installation der Einheit zum Versetzen von Daten installiert.

Auf den Recovery Agent zugreifen

Windows Sie können über das **Start**-Menü auf den Recovery Agent zugreifen: **Start** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**

IBM Spectrum Protect vSphere-Client-Plug-in

Das IBM Spectrum Protect vSphere-Client-Plug-in ist eine Erweiterung des VMware vSphere-Web-Clients, die eine Sicht der Data Protection for VMware vSphere-GUI bereitstellt.

Übersicht

Das IBM Spectrum Protect vSphere-Client-Plug-in stellt eine Untergruppe der Funktionen, die in der Browsersicht für die Data Protection for VMware vSphere-GUI verfügbar sind, sowie einige zusätzliche Funktionen bereit.

Voraussetzung

Zum Installieren des IBM Spectrum Protect vSphere-Client-Plug-ins müssen Sie die folgenden Optionen auswählen, wenn Sie den Konfigurationsassistenten von IBM Spectrum Protect for Virtual Environments ausführen:

- Auf der Seite **vCenter-Einstellungen** des Konfigurationsassistenten wählen Sie **Registrierung aktualisieren** aus, um das Plug-in bei dem zugehörigen vCenter zu registrieren.
- Geben Sie die Adresse des GUI-Hosts, den vCenter-Benutzer und das Kennwort ein.

Nach Beendigung des Assistenten ist das Plug-in beim vCenter registriert.

Auf die Data Protection-Erweiterung zugreifen

Sie können über den vSphere-Web-Client auf die Erweiterung zugreifen.

Data Protection for VMware-Befehlszeilenschnittstelle

Die Data Protection for VMware-Befehlszeilenschnittstelle ist eine Befehlszeilenschnittstelle mit vollem Funktionsumfang, die mit der Data Protection for VMware vSphere-GUI installiert wird.

Übersicht

Mit der Data Protection for VMware-Befehlszeilenschnittstelle können Sie die folgenden Tasks ausführen:

- Sicherungen Ihrer VMs einleiten oder planen, die auf einem IBM Spectrum Protect-Server gespeichert werden.
- Vollständige Wiederherstellung Ihrer VMs, VM-Dateien oder VM-Platten (VMDKs) aus einem IBM Spectrum Protect-Server einleiten.
- Konfigurationsinformationen zur Sicherungsdatenbank und -umgebung anzeigen.

Die Data Protection for VMware vSphere-GUI ist zwar die primäre Taskschnittstelle, aber die Data Protection for VMware-Befehlszeilenschnittstelle stellt eine hilfreiche sekundäre Schnittstelle dar.

Beispielsweise kann die Data Protection for VMware-Befehlszeilenschnittstelle verwendet werden, um einen Zeitplanungsmechanismus zu implementieren, der sich von dem Mechanismus unterscheidet, der von der Data Protection for VMware vSphere-GUI implementiert wird. Die Data Protection for VMware-Befehlszeilenschnittstelle ist außerdem hilfreich, wenn Sie Automatisierungsergebnisse mit Scripts auswerten.

Auf die Data Protection for VMware-Befehlszeilenschnittstelle zugreifen

Sie können über eine Befehlszeile auf die Data Protection for VMware-Befehlszeilenschnittstelle zugreifen.

Ausführliche Informationen zu den verfügbaren Befehlen enthält der Befehlsreferenzabschnitt im *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware Benutzerhandbuch*.

IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung

Sie können einzelne Dateien aus einer Sicherung der virtuellen VMware-Maschine zurückschreiben.

Übersicht

Die Schnittstelle für Dateizurückschreibung ist eine webbasierte Schnittstelle, mit der Sie einzelne Dateien aus einer VM-Sicherung zurückschreiben können. Der Vorteil dieser Schnittstelle ist, dass Datei-, Software- und Plattformeigner ihre eigenen Dateien ohne Vorkenntnisse zu IBM Spectrum Protect-Sicherungs- und -Zurückschreibungsoperationen zurückschreiben können.

Das Feature der Schnittstelle für Dateizurückschreibung wird installiert, wenn Sie die Option zum Schützen von Daten in einer vSphere-Umgebung auswählen. Im Data Protection for VMware-Konfigurationsassistenten müssen Sie das Feature für Dateizurückschreibung aktivieren, damit die Schnittstelle verfügbar ist.

Auf die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zugreifen

Für den Zugriff auf die Schnittstelle für Dateizurückschreibung öffnen Sie einen Web-Browser und geben Sie die URL ein, die Ihr Administrator zur Verfügung gestellt hat. Beispiel:

```
https://Hostname:9081/FileRestoreUI
```

Dabei ist *Hostname* der Hostname des Systems, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

Feature der Einheit zum Versetzen von Daten

Eine Einheit zum Versetzen von Daten ist eine Softwarekomponente von Data Protection for VMware, die Daten auf den IBM Spectrum Protect-Server und von diesem Server versetzt.

Übersicht

In einer typischen VMware-Umgebung wird die Einheit zum Versetzen von Daten verwendet, um Sicherungen virtueller Maschinen auf einem Datencenterknoten zu speichern.

Wenn Sie Data Protection for VMware installieren, ist die Einheit zum Versetzen von Daten in der Installation enthalten. Die Einheit zum Versetzen von Daten wird auf demselben System wie die Data Protection for VMware vSphere-GUI und weitere Data Protection for VMware-Komponenten installiert.

Sie können Einheiten zum Versetzen von Daten auch unabhängig von den anderen Data Protection for VMware-Komponenten auf fernen Systemen installieren, um die Sicherungsarbeitslast auf mehrere Systeme zu verteilen.

Momentaufnahmedifferenzsicherungsoperationen werden in der VMware-Umgebung nicht unterstützt. Sie können keine Momentaufnahmedifferenzsicherungsoperationen für ein Dateisystem ausführen, das sich auf einem NetApp-Dateiserver auf einem Host befindet, auf dem auch die Data Protection for VMware-Einheit zum Versetzen von Daten installiert ist.

Einheiten zum Versetzen von Daten einrichten

Die folgende Liste enthält Informationen zur Planung, Installation und Konfiguration von Einheiten zum Versetzen von Daten:

Aktion	Beschreibung
Anzahl der Einheiten zum Versetzen von Daten bestimmen, die für den Schutz Ihrer vSphere-Umgebung erforderlich sind	Möglicherweise sind mehrere Knoten der Einheit zum Versetzen von Daten erforderlich, um Ihre vSphere-Umgebung zu schützen. Informationen zum Bestimmen der erforderlichen Anzahl der Knoten der Einheit zum Versetzen von Daten enthält Technote 2007197. Diese Technote beinhaltet außerdem Hinweise zur Verwendung virtueller oder physischer Maschinen für Knoten der Einheit zum Versetzen von Daten und zum Standort von Einheiten zum Versetzen von Daten.
Data Protection for VMware installieren	Zum Installieren von Data Protection for VMware führen Sie das Data Protection for VMware-Installationsprogramm aus. Wählen Sie für Windows-Betriebssysteme **Standardinstallation** oder für Linux-Betriebssysteme **Vollständig** aus. Mit dieser Installationsoption werden alle Data Protection for VMware-Komponenten einschließlich der Einheit zum Versetzen von Daten installiert. Informationen zum Ausführen des Data Protection for VMware-Installationsprogramms finden Sie in „Data Protection for VMware-Komponenten installieren” auf Seite 23.

Aktion	Beschreibung
Einheiten zum Versetzen von Daten für Ihre Umgebung definieren	Wenn der Data Protection for VMware-Installationsassistent beendet ist, wird der Konfigurationsassistent für die Data Protection for VMware vSphere-GUI geöffnet, damit Sie die Kommunikation mit dem IBM Spectrum Protect-Server einrichten können. Auf der Seite **Knoten der Einheit zum Versetzen von Daten** des Konfigurationsassistenten definieren Sie die Informationen für die lokale Einheit zum Versetzen von Daten und für eventuelle ferne Einheiten zum Versetzen von Daten, die Sie auf separaten Systemen installieren werden. Wenn Sie die Installation unter einem Windows-Betriebssystem ausführen und bei der Definition der Einheit zum Versetzen von Daten **Services erstellen** auswählen, werden die Konfigurationsinformationen für die Einheit zum Versetzen von Daten in einer Optionsdatei an der folgenden Position gespeichert: `C:\Programme\Tivoli\TSM\baclient\` Darüber hinaus werden die Services konfiguriert, die für die Einheit zum Versetzen von Daten erforderlich sind. Wenn Sie die Einheit zum Versetzen von Daten unter einem Linux-Betriebssystem installieren oder wenn Sie die Installation unter einem Windows-Betriebssystem ausführen und bei der Konfiguration nicht **Services erstellen** auswählen, müssen Sie die Schritte in „Knoten der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI definieren" auf Seite 97 ausführen, um die Optionsdatei zu erstellen und die erforderlichen Services zu konfigurieren.
Bei Bedarf zusätzliche Einheiten zum Versetzen von Daten auf fernen Systemen installieren und konfigurieren	Zum Installieren einer Einheit zum Versetzen von Daten auf einem fernen System führen Sie das Data Protection for VMware-Installationsprogramm aus und führen Sie eine der folgenden Aktionen durch: Unter Windows-Betriebssystemen wählen Sie **Erweiterte Installation** > **Nur das Feature der Einheit zum Versetzen von Daten installieren** im Konfigurationsassistenten aus. Unter Linux-Betriebssystemen wählen Sie in der Liste der Installationsgruppen im Konfigurationsassistenten **Angepasst** aus. Stellen Sie sicher, dass **Data Protection for VMware-Einheit zum Versetzen von Daten** ausgewählt ist. Diese Option ist standardmäßig ausgewählt. Wenn die Installation beendet ist, führen Sie die Anweisungen in „Knoten der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI definieren" auf Seite 97 aus, um Einheiten zum Versetzen von Daten auf fernen Systemen einzurichten.

Installation von Data Protection for VMware planen

Data Protection for VMware eliminiert die Auswirkungen, die die Ausführung von Sicherungen auf eine virtuelle Maschine hat, indem die Arbeitslast für die Sicherungen von einem ESX- oder ESXi-basierten VMware-Host auf einen vStorage-Sicherungsserver ausgelagert wird.

Data Protection for VMware verwendet die integrierte Einheit zum Versetzen von Daten, um Sicherungen des Typs 'Immer inkrementell - Vollständig' und 'Immer inkrementell - Inkrementell' von VMs auszuführen. Der Knoten der Einheit zum Versetzen von Daten 'versetzt' die Daten auf den IBM Spectrum Protect-Server, damit sie dort gespeichert und zu einem späteren Zeitpunkt für eine VM-Zurückschreibung auf Imageebene verwendet werden können. Instant Restore ist auf der Plattendatenträgerebene und der Ebene der vollständigen VM verfügbar.

Tipp: Die Einheit zum Versetzen von Daten ist eine Komponente mit separater Lizenz, die eigene Benutzerschnittstellen und eine eigene Dokumentation umfasst. Mit diesem Produkt und der zugehörigen Dokumentation müssen Sie hinreichend vertraut sein, damit Sie einen umfassenden Plan für den Schutz Ihrer virtuellen Maschinen mit Data Protection for VMware adäquat integrieren können. Data Protection for VMware für Windows 64 Bit umfasst das Feature der Einheit zum Versetzen von Daten.

Installationsroadmap

In der folgenden Tabelle sind die Schritte zur Ausführung eines erfolgreichen Installationsprozesses beschrieben.

Tabelle 2. Installationstasks für Data Protection for VMware-Neukunden oder -Bestandskunden

Schritt	Task	Einstiegspunkt
1	Systemvoraussetzungen überprüfen.	Stellen Sie sicher, dass das System, auf dem Data Protection for VMware installiert werden soll, die Systemvoraussetzungen erfüllt.
2	Voraussetzungen in Bezug auf Benutzerberechtigungen überprüfen.	Vermeiden Sie potenzielle Fehler oder Verzögerungen bei der Installation, indem Sie die erforderlichen Benutzerberechtigungsstufen verwenden.
3	Verfügbarkeit der erforderlichen Kommunikationsports überprüfen.	Vermeiden Sie Fehler oder Verzögerungen bei der Installation, indem Sie die nötigen Kommunikationsports öffnen, bevor Sie Data Protection for VMware installieren.

Tabelle 2. Installationstasks für Data Protection for VMware-Neukunden oder -Bestandskunden (Forts.)

Schritt	Task	Einstiegspunkt
4	Data Protection for VMware installieren: • Data Protection for VMware mit dem Installationsassistenten installieren • „Data Protection for VMware-Komponenten im unbeaufsichtigten Modus installieren" auf Seite 28 Upgrade für Data Protection for VMware durchführen: Upgrade für Data Protection for VMware durchführen	Jedes Installationspaket umfasst eine Benutzerlizenzdatei (EULA). Wenn Sie die Bedingungen in der Datei nicht akzeptieren, wird die Installation beendet.
5	„Neuinstallation mit dem Assistenten konfigurieren" auf Seite 43 Wenn Sie ein Upgrade für Data Protection for VMware durchführen möchten, können je nach den installierten Komponenten weitere Konfigurationstasks erforderlich sein.Die Konfigurationsthemen im *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware Benutzerhandbuch* enthalten weitere Informationen.	Verwenden Sie den Konfigurationsassistenten für eine Erstkonfiguration. Je nach den installierten Features sind möglicherweise mehr Konfigurationstasks als in diesem Abschnitt beschrieben erforderlich.

Tipp: Als Unterstützung für die Planung der Anzahl der Proxy-Hosts, die für Ihre spezielle Data Protection for VMware-Sicherungsumgebung erforderlich sind, steht die folgende Veröffentlichung im IBM Spectrum Protect-Wiki zur Verfügung:
Step by Step Guide To vStorage Backup Server (Proxy) Sizing
Diese Veröffentlichung finden Sie im Abschnitt zu dem Produkt IBM Spectrum Protect for Virtual Environments.

Installationsszenarios

Wählen Sie vor der Installation von Data Protection for VMware das Szenario aus, das die Anforderungen Ihres Unternehmens am besten erfüllt.

Sie können Data Protection for VMware und die Einheit zum Versetzen von Daten mithilfe der GUI oder im unbeaufsichtigten Modus installieren:

- „Data Protection for VMware-Komponenten mit dem Installationsassistenten installieren" auf Seite 25
- „Data Protection for VMware-Komponenten im unbeaufsichtigten Modus installieren" auf Seite 28

Eine Liste der Features und Komponenten, die je nach Plattform verfügbar sind, finden Sie in „Installierbare Komponenten" auf Seite 1.

Tabelle 3. Installationsszenarios

Szenarionummer	Beschreibung	Auszuführende Tasks
1	Verwenden Sie dieses Szenario für eine Neuinstallation, wenn Sie Data Protection for VMware und die Einheit zum Versetzen von Daten auf demselben System installieren möchten.	Windows Sie können das Installationsprogramm der Suite im GUI-Modus oder im unbeaufsichtigten Modus verwenden. Linux Sie können InstallAnywhere im GUI-Modus oder im unbeaufsichtigten Modus verwenden.
2	Verwenden Sie dieses Szenario, wenn Sie eine Einheit zum Versetzen von Daten (einen Mount-Proxy), Recovery Agent und die erforderlichen Unterstützungspakete auf diesem System installieren möchten.	Windows Sie können eine erweiterte Installation mithilfe des Installationsprogramms der Suite ausführen. Linux Das Feature der Einheit zum Versetzen von Daten ist jetzt mit Data Protection for VMware installiert.

Systemvoraussetzungen

Damit Sie Data Protection for VMware-Komponenten implementieren können, muss Ihr System die entsprechenden Systemvoraussetzungen erfüllen.

Softwarevoraussetzungen

Die Details der Software- und Betriebssystemvoraussetzungen können sich im Lauf der Zeit ändern. Informationen zu den aktuellen Softwarevoraussetzungen finden Sie in der Technote 1505139.

Hardwarevoraussetzungen

Hardwarevoraussetzungen können variieren und sind von Folgendem abhängig:

- Anzahl geschützter Server
- Anzahl geschützter Datenträger
- Datenmenge
- LAN- und SAN-Konnektivität

Anmerkung: Die Komponente Recovery Agent unterstützt keine Operationen in einer LAN-unabhängigen Umgebung.

In der folgenden Tabelle sind die Hardwarevoraussetzungen beschrieben, die für die Installation von Data Protection for VMware benötigt werden.

Tabelle 4. Hardwarevoraussetzungen für Data Protection for VMware

Komponente	Mindestanforderung	Bevorzugt
System	IntelPentium D 3 GHz Dual Core-Prozessor oder kompatibler Prozessor	Nicht zutreffend
Arbeitsspeicher	2 GB Arbeitsspeicher, 2 GB virtueller Adressraum	Nicht zutreffend

Tabelle 4. Hardwarevoraussetzungen für Data Protection for VMware (Forts.)

Komponente	Mindestanforderung	Bevorzugt
Verfügbarer Festplattenspeicherplatz	200 MB für den Ordner 'Dokumente und Einstellungen'	2 GB
NIC-Karte	1 NIC - 100 Mb/s	1 NIC - 1 Gb/s

Anmerkung: Je nach der Anzahl der parallelen Prozesse können Sicherungen virtueller Maschinen viel Speicherkapazität beanspruchen.

Der Speicherbedarf für den Befehl **dsmc backup vm** kann erheblich sein und lässt sich anhand der folgenden Formel berechnen:

Erforderlicher Speicher = (Plattengröße/MBLK-Größe) * Lesepuffergröße * VMMAXPARALLEL

Dabei gilt Folgendes:

- **Plattengröße** ist die Größe der Platte der Gastmaschine, die zurzeit verarbeitet wird.
- **MBLK-Größe** ist die Größe eines Megablocks. Sie ist 128 MB für Platten, die kleiner als 2 TB sind, und 1 GB für Platten, die größer als 2 TB sind.
- **Lesepuffergröße** ist die Größe des internen IBM Spectrum Protect-Puffers, der für die MBLK-Informationen verwendet wird. Die Puffergröße ist 256 KB.
- **VMMAXPARALLEL** ist die maximale Anzahl der virtuellen Maschinen, die durch einen einzigen Sicherungsprozess gleichzeitig gesichert werden können.

Beispiel: Es sollen 10 Gastmaschinen gesichert werden, die jeweils eine 40-GB-Platte enthalten. Für die Ausführung der Sicherung mit 'VMMAXPARALLEL 2' durch einen einzigen Sicherungsprozess ist die folgende Speicherkapazität erforderlich:

- **Plattengröße** = 40 GB = 41943040 KB;
- **MBLK-Größe** = 128 MB = 131072 KB;
- **Lesepuffergröße** = 256 KB;
- **VMMAXPARALLEL** = 2.

Erforderliche Speicherkapazität = (41943040/131072) * 256 KB * 2 = 163840 KB = 160 MB.

Anmerkung: Für die Sicherung derselben Anzahl Gastmaschinen mit 'VMMAXPARALLEL 2' in fünf parallelen Sicherungsprozessen wird (maximal) 5-mal so viel Speicher wie im vorherigen Beispiel, d. h. 800 MB benötigt.

Ein Windows-Proxy-Host ist für Recovery Agent unter Linux erforderlich. Auf diesem Windows-Proxy-Host muss Recovery Agent installiert sein.

Einschränkung: Die folgenden Einschränkungen gelten für VMware-VMDKs, die in eine Sicherungsoperation einbezogen sind:

- Für den Sicherungsmodus 'Immer inkrementell - Inkrementell' darf jede einzelne VMDK, die an einer Sicherungsoperation teilnimmt, die Größe von 8 TB nicht überschreiten. Überschreitet eine VMDK 8 TB, schlägt die Sicherungsoperation fehl. Soll die VMDK vergrößert werden, sodass sie die Standardgröße von 2 TB überschreitet, geben Sie die maximale Größe mit der Option `vmmaxvirtualdisks` an. Weitere Informationen finden Sie, wenn Sie im IBM Knowledge Center nach `vmmaxvirtualdisks` suchen.

- Für den Sicherungsmodus 'Immer inkrementell - Vollständig' darf jede einzelne VMDK, die an einer Sicherungsoperation teilnimmt, die Größe von 2 TB nicht überschreiten. Überschreitet eine VMDK 2 TB, schlägt die Sicherungsoperation fehl.

Zur Verhinderung von Fehlern in beiden Sicherungsmodi können Sie die Verarbeitung der VMDK durch Angabe von `vmskipmaxvirtualdisks yes` in der Optionsdatei der Einheit zum Versetzen von Daten überspringen. Weitere Informationen finden Sie in Vmskipmaxvirtualdisks.

Voraussetzungen für die Dateizurückschreibung

Stellen Sie sicher, dass Ihre Umgebung die Mindestvoraussetzungen erfüllt, bevor Sie Dateien mit der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zurückschreiben.

Zur Aktivierung des Features für Dateizurückschreibung muss Data Protection for VMware auf einem Windows-System installiert sein.

Voraussetzungen für virtuelle VMware-Maschinen

Die folgenden Voraussetzungen gelten für die virtuelle VMware-Maschine, die die zurückzuschreibenden Dateien enthält:

- Linux Windows Auf der virtuellen Maschine muss VMware Tools installiert sein.
- Linux Windows Die virtuelle Maschine muss während der Dateizurückschreibungsoperation aktiv sein.
- Windows Die virtuelle Maschine muss derselben Windows-Domäne wie das System der Einheit zum Versetzen von Daten angehören.
- Windows Wenn eine virtuelle Maschine aus einer Windows-Domäne gelöscht und zu einem späteren Zeitpunkt zurückgeschrieben wird, muss die virtuelle Maschine wieder in die Domäne eingebunden werden, damit die Domänenvertrauensbeziehung sichergestellt ist. Versuchen Sie nicht, eine Datei der virtuellen Maschine zurückzuschreiben, bis die Domänenvertrauensbeziehung wiederhergestellt ist.
- Windows Ist der Benutzer nicht der Eigner der zurückzuschreibenden Datei, muss dem Benutzer für diese virtuelle Maschine die Microsoft Windows-Berechtigung `Wiederherstellen von Dateien und Verzeichnissen` zugeordnet werden.
- Linux Für die virtuelle Maschine ist lokale Benutzerauthentifizierung erforderlich. Authentifizierung ist nicht über die Windows-Domäne, Lightweight Directory Access Protocol (LDAP), Kerberos oder andere Netzauthentifizierungsmethoden verfügbar.
- Linux Unter einem Red Hat Enterprise Linux 6-Betriebssystem muss für die Option `ChallengeResponseAuthentication` in der Konfigurationsdatei des Dämons sshd (`/etc/ssh/sshd_config`) YES angegeben sein oder diese Option muss auf Kommentar gesetzt sein. Beispielsweise sind beide der folgenden Anweisungen gültig:

  ```
  ChallengeResponseAuthentication yes
  #ChallengeResponseAuthentication no
  ```

  Starten Sie den sshd-Dämon erneut, nachdem Sie diese Option geändert haben.

Voraussetzungen für die Einheit zum Versetzen von Daten

Das System der Einheit zum Versetzen von Daten stellt eine bestimmte Einheit zum Versetzen von Daten dar, die Daten von einem System auf ein anderes 'versetzt'.

Windows Das System der Einheit zum Versetzen von Daten muss derselben Windows-Domäne wie die virtuelle Maschine angehören, die die zurückzuschreibenden Dateien enthält.

Voraussetzungen für den Mount-Proxy

Das Mount-Proxy-System ist das Linux- oder Windows-Proxy-System, das über eine iSCSI-Verbindung auf die bereitgestellten Platten der virtuellen Maschine zugreift. Dieses System ermöglicht es, dass die Dateisysteme auf den bereitgestellten Platten der virtuellen Maschine als Zurückschreibungspunkte für die Schnittstelle für Dateizurückschreibung zugänglich sind.

Linux Linux-Betriebssysteme stellen einen Dämon zur Verfügung, der LVM-Datenträgergruppen (LVM - Logical Volume Manager) aktiviert, wenn diese Gruppen für das System verfügbar werden. Definieren Sie diesen Dämon auf dem Linux-Mount-Proxy-System so, dass LVM-Datenträgergruppen nicht aktiviert werden, wenn sie für das System verfügbar werden. Ausführliche Informationen zur Vorgehensweise für die Definition dieses Dämons finden Sie in der entsprechenden Linux-Dokumentation.

Linux Windows Das Windows-Mount-Proxy-System und das Linux-Mount-Proxy-System müssen sich in demselben Teilnetz befinden.

Voraussetzungen für Microsoft Windows-Domänenkonten

Die folgenden Voraussetzungen gelten für Windows-Domänenkonten:

- Windows Berechtigungsnachweise eines Windows-Domänenadministrators sind erforderlich, um auf die Netzfreigabe zuzugreifen. Ein Administrator gibt diese Berechtigungsnachweise im Konfigurationsassistenten oder Notizbuch der Data Protection for VMware vSphere-GUI ein, um die Umgebung für Dateizurückschreibungsoperationen zu aktivieren.
- Windows Ein Dateieigner greift mit den Berechtigungsnachweisen eines Windows-Domänenbenutzers auf die ferne virtuelle Maschine (die die zurückzuschreibenden Dateien enthält) zu. Diese Berechtigungsnachweise werden bei der Anmeldung in der Schnittstelle für Dateizurückschreibung eingegeben. Die Berechtigungsnachweise des Domänenbenutzers bestätigen, dass der Dateieigner berechtigt ist, sich bei der fernen virtuellen Maschine anzumelden und Dateien in die ferne virtuelle Maschine zurückzuschreiben. Für diese Berechtigungsnachweise sind keine besonderen Berechtigungen erforderlich.
- Windows Verwendet ein Dateieigner ein Benutzerkonto der Windows-Domäne, bei dem der Zugriff auf bestimmte Computer beschränkt ist (sodass nicht auf alle Computer in der Domäne Zugriff besteht), stellen Sie sicher, dass das Mount-Proxy-System sich in der Liste der Computer befindet, auf die dieses Domänenbenutzerkonto zugreifen kann. Andernfalls kann der Dateieigner sich nicht bei der Schnittstelle für Dateizurückschreibung anmelden.

Voraussetzungen für Banddatenträger

Die Dateizurückschreibung von Banddatenträgern wird nicht unterstützt. Die Dateizurückschreibung von Plattenspeicher ist die bevorzugte Methode.

Für die Installation erforderliche Berechtigungen

Stellen Sie vor dem Beginn der Installation sicher, dass Ihre Benutzer-ID über die erforderliche Berechtigungsstufe verfügt.

Informationen zu diesem Vorgang

Tabelle 5. Für die Installation und Konfiguration von Data Protection for VMware erforderliche Benutzerberechtigungen

System	Erforderliche Berechtigung
Windows	Administrator
Linux	Root
vCenter-Server	Administratorberechtigungen Für die vCenter-Serverrolle sind die folgenden Berechtigungen erforderlich: **Erweiterung** > **Erweiterung registrieren, Registrierung der Erweiterung aufheben, Erweiterung aktualisieren**. Diese neue Rolle muss auf das vCenter-Objekt in der VMware vCenter-Serverhierarchie für die Benutzer-ID angewendet werden, die während der Installation angegeben wird.
IBM Spectrum Protect-Server **Einschränkung:** Der Server muss gestartet sein.	Verwaltungszugriff (Berechtigung **System** oder **Uneingeschränkte Maßnahmendomäne**)

Erforderliche Kommunikationsports

Zeigen Sie eine Liste der Kommunikationsports an, die in der Firewall offen sein müssen, wenn Sie Data Protection for VMware installieren.

Die Ports, die in der Tabelle angegeben sind, spiegeln eine Standardinstallation wider. Eine Standardinstallation besteht aus den folgenden Komponenten auf demselben Windows-System:

- Server der Data Protection for VMware-GUI
- vStorage-Sicherungsserver (Einheit zum Versetzen von Daten)
- Windows-Mount-Proxy
- IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung

Bei einer anderen Installation als der Standardinstallation sind möglicherweise weitere Ports erforderlich.

Einschränkung: Der Windows-Mount-Proxy und der Linux-Mount-Proxy müssen sich in demselben Teilnetz befinden.

Tabelle 6. Erforderliche Kommunikationsports. In dieser Tabelle sind die Ports aufgeführt, auf die Data Protection for VMware zugreift.

TCP-Port	Initiator: Abgehend (vom Host)	Ziel: Eingehend (zum Host)
443	vStorage-Sicherungsserver	vCenter-Server (sicheres HTTP)

Tabelle 6. Erforderliche Kommunikationsports (Forts.). In dieser Tabelle sind die Ports aufgeführt, auf die Data Protection for VMware zugreift.

TCP-Port	Initiator: Abgehend (vom Host)	Ziel: Eingehend (zum Host)
443	Data Protection for VMware vSphere-GUI-Server	vCenter-Server
443 Diese Einstellung ist nur erforderlich, wenn die Einheit zum Versetzen von Daten ein Linux-System ist.	Windows-Mount-Proxy	vCenter-Server
443	vStorage-Sicherungsserver	Platform Services Controller
443	Data Protection for VMware vSphere-GUI-Server	Platform Services Controller
443	Windows-Mount-Proxy	Platform Services Controller
902 443	vCenter-Server	ESXi-Hosts
902 443	vStorage-Sicherungsserver (Proxy)	ESXi-Hosts (alle geschützten Hosts)
1500 (**tcpport**)	vStorage-Sicherungsserver (Proxy)	IBM Spectrum Protect-Server
1500 (**tcpadminport**)	Data Protection for VMware vSphere-GUI-Server • 1500 (**tcpadminport**) für die Nicht-SSL-Kommunikation • Für die SSL-Kommunikation ist **tcpadminport** der einzige Port, der die SSL-Kommunikation mit dem IBM Spectrum Protect-Server unterstützt. Die korrekte Portnummer für das SSL-Protokoll ist normalerweise der Wert, der durch die Option **ssltcpadminport** in der Datei dsmserv.opt des IBM Spectrum Protect-Servers angegeben ist. Ist jedoch **adminonclient no** in der Datei dsmserv.opt angegeben, ist die korrekte Portnummer für das SSL-Protokoll der Wert, der durch die Option **ssltcpadminport** angegeben wird. Die Option **ssltcpadminport** hat keinen Standardwert. Daher muss der Wert vom Benutzer angegeben werden.	IBM Spectrum Protect-Server
1527 Interne Derby-Datenbank		

Tabelle 6. Erforderliche Kommunikationsports (Forts.). In dieser Tabelle sind die Ports aufgeführt, auf die Data Protection for VMware zugreift.

TCP-Port	Initiator: Abgehend (vom Host)	Ziel: Eingehend (zum Host)
1501 1581 (**httpport**)	IBM Spectrum Protect-Server	vStorage-Sicherungsserver • Scheduler der Einheit zum Versetzen von Daten • Web-Client • Clientakzeptordämon
1581 (**httpport**) 1582, 1583 (**webports**)	Data Protection for VMware vSphere-GUI-Server	vStorage-Sicherungsserver
9081 GUI-Web-Server (HTTPS-Protokoll)	vSphere-Client	Data Protection for VMware vSphere-GUI-Server (sicherer HTTPS-Port für den Zugriff auf das vCenter über einen Web-Browser)
22 SSH-Standardport für Recovery Agent	Recovery Agent	Windows-"Mount"-Host für Data Protection for VMware • SSH für Linux Recovery Agent
3260	Data Protection for VMware-Dateizurückschreibung für Linux	Windows-"Mount"-Host für Data Protection for VMware • iSCSI
3260 iSCSI-Standardport für Recovery Agent	Windows-Ziel bei dynamischer Platte für Dateizurückschreibung	Windows-"Mount"-Host für Data Protection for VMware • iSCSI
5985	Operationen der GUI für Dateizurückschreibung	Windows Remote Management
135	Windows-Mount-Proxy	Virtuelle VMware-Maschine, die die Dateien enthält, die mit der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zurückgeschrieben werden sollen

Anforderungen hinsichtlich der Benutzerberechtigungen für den VMware vCenter-Server

Für die Ausführung von Data Protection for VMware-Operationen sind bestimmte Berechtigungen für den VMware vCenter-Server erforderlich.

Erforderliche vCenter-Serverberechtigungen für den Schutz von VMware-Datencentern mit der Web-Browser-Sicht für die Data Protection for VMware vSphere-GUI

Die Benutzer-ID des vCenter-Servers, die sich bei der Browser-Sicht für die Data Protection for VMware vSphere-GUI anmeldet,

muss über ausreichende VMware-Berechtigungen zum Anzeigen des Inhalts eines Datencenters verfügen, das von der GUI verwaltet wird.

Beispiel: Eine VMware vSphere-Umgebung enthält fünf Datencenter. Der Benutzer „jenn" verfügt nur für zwei dieser Datencenter über ausreichende Berechtigungen. Daher sind nur die beiden Datencenter, für die ausreichende Berechtigungen vorhanden sind, für „jenn" in den Sichten sichtbar. Die übrigen drei Datencenter (für die „jenn" keine Berechtigungen hat) sind für den Benutzer „jenn" nicht sichtbar.

Auf dem VMware vCenter-Server wird eine Gruppe von Berechtigungen gemeinsam als Rolle definiert. Eine Rolle wird für einen bestimmten Benutzer oder eine bestimmte Gruppe auf ein Objekt angewendet, um eine Berechtigung zu erstellen. Vom VMware vSphere-Web-Client aus müssen Sie eine Rolle mit einer Gruppe von Berechtigungen erstellen. Verwenden Sie die Funktion **Add a Role** des VMware vSphere-Clients, um eine vCenter-Serverrolle für Sicherungs- und Zurückschreibungsoperationen zu erstellen.

Wenn die Berechtigungen an alle Datencenter innerhalb des vCenters weitergegeben werden sollen, geben Sie den vCenter-Server an und wählen Sie das Kontrollkästchen `Propagate to children` aus. Andernfalls können Sie die Berechtigungen begrenzen, wenn Sie die Rolle nur den erforderlichen Datencentern zuordnen und das Kontrollkästchen `Propagate to children` auswählen. Bei der Browser-GUI werden Berechtigungen auf der Ebene des Datencenters erzwungen.

Das folgende Beispiel zeigt die Zugriffssteuerung zu Datencentern für zwei VMware-Benutzergruppen. Erstellen Sie zuerst eine Rolle, die alle in der Technote 7047438 definierten Berechtigungen enthält. Die Gruppe von Berechtigungen in diesem Beispiel werden durch die Rolle „TDPVMwareManage" identifiziert. Gruppe 1 benötigt Zugriff zum Verwalten virtueller Maschinen für die Datencenter `Primary1_DC` und `Primary2_DC`. Gruppe 2 benötigt Zugriff zum Verwalten virtueller Maschinen für die Datencenter `Secondary1_DC` und `Secondary2_DC`.

Für Gruppe 1 ordnen Sie die Rolle „TDPVMwareManage" den Datencentern `Primary1_DC` und `Primary2_DC` zu. Für Gruppe 2 ordnen Sie die Rolle „TDPVMwareManage" den Datencentern `Secondary1_DC` und `Secondary2_DC` zu.

Die Benutzer in jeder VMware-Benutzergruppe können mithilfe der Data Protection for VMware-GUI nur virtuelle Maschinen in ihren jeweiligen Datencentern verwalten.

Tipp: Wenn Sie eine Rolle erstellen, empfiehlt es sich möglicherweise, der Rolle zusätzliche Berechtigungen hinzuzufügen, die Sie später für weitere Tasks mit Objekten benötigen.

Erforderliche vCenter-Serverberechtigungen für die Verwendung der Einheit zum Versetzen von Daten

Auf der IBM Spectrum Protect-Einheit zum Versetzen von Daten, die auf dem vStorage-Sicherungsserver installiert ist, (dem Knoten der Einheit zum Versetzen von Daten) müssen die Optionen `VMCUser` und `VMCPw` definiert sein. Die Option `VMCUser` gibt die Benutzer-ID des vCenter- oder ESX-Servers an, der gesichert, zurückgeschrieben oder abgefragt werden soll. Die erforderlichen Berechtigungen, die dieser Benutzer-ID (`VMCUser`) zugeordnet sind, stellen sicher, dass der Client Operationen mit der virtuellen Maschine und in der VMware-Umgebung ausführen kann. Diese Benutzer-ID muss über die VMware-Berechtigungen verfügen, die in der oben genannten Technote beschrieben sind.

Verwenden Sie die Funktion **Add a Role** des VMware vSphere-Clients, um eine vCenter-Serverrolle für Sicherungs- und Zurückschreibungsoperationen zu erstellen. Sie müssen die Option `Propagate to children` auswählen, wenn Sie Berechtigungen für diese Benutzer-ID (`VMCUser`) hinzufügen. Zudem ist es möglicherweise sinnvoll, dieser Rolle zusätzliche Berechtigungen für weitere Tasks neben der Sicherung und Zurückschreibung hinzuzufügen. Für die Option `VMCUser` werden Berechtigungen beim Objekt der höchsten Ebene erzwungen.

Erforderliche vCenter-Serverberechtigungen für den Schutz von VMware-Datencentern mit der Sicht des IBM Spectrum Protect vSphere-Client-Plug-ins für die Data Protection for VMware vSphere-GUI

Für das IBM Spectrum Protect vSphere-Client-Plug-in werden separate Berechtigungen benötigt, die sich von den Berechtigungen für die Anmeldung bei der GUI unterscheiden.

Während der Installation werden die folgenden angepassten Berechtigungen für das IBM Spectrum Protect vSphere-Client-Plug-in erstellt:

- **Datencenter** > **IBM Data Protection**
- **Global** > **IBM Data Protection konfigurieren**

Angepasste Berechtigungen, die für das IBM Spectrum Protect vSphere-Client-Plug-in erforderlich sind, werden als separate Erweiterung registriert. Der Schlüssel für die Berechtigungserweiterung lautet `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Mit diesen Berechtigungen kann der VMware-Administrator den Zugriff auf den Inhalt des IBM Spectrum Protect vSphere-Client-Plug-ins aktivieren und inaktivieren. Nur Benutzer, die über diese angepassten Berechtigungen für das erforderliche VMware-Objekt verfügen, können auf den Inhalt des IBM Spectrum Protect vSphere-Client-Plug-ins zugreifen. Ein einziges IBM Spectrum Protect vSphere-Client-Plug-in wird für jeden vCenter-Server registriert und von allen GUI-Hosts gemeinsam genutzt, die für die Unterstützung des vCenter-Servers konfiguriert sind.

Vom VMware vSphere-Web-Client aus müssen Sie eine Rolle für Benutzer erstellen, die Datenschutzfunktionen für virtuelle Maschinen mithilfe des IBM Spectrum Protect vSphere-Client-Plug-ins ausführen können. Für diese Rolle müssen Sie neben den Standardberechtigungen der Administratorrolle für virtuelle Maschinen, die der Web-Client erfordert, die Berechtigung **Datencenter** > **IBM Data Protection** angeben. Für jedes Datencenter ordnen Sie diese Rolle jedem Benutzer oder jeder Benutzergruppe zu, dem bzw. der Sie die Berechtigung zum Verwalten virtueller Maschinen erteilen möchten.

Die Berechtigung **Global** > **IBM Data Protection** ist auf der vCenter-Ebene für den Benutzer notwendig. Mit dieser Berechtigung kann der Benutzer die Verbindung zwischen dem vCenter-Server und dem Web-Server für die Data Protection for VMware vSphere-GUI verwalten, editieren oder löschen. Ordnen Sie diese Berechtigung Administratoren zu, die mit der Data Protection for VMware vSphere-GUI für den Schutz ihres jeweiligen vCenter-Servers vertraut sind. Verwalten Sie die Verbindungen des IBM Spectrum Protect vSphere-Client-Plug-ins auf der Seite **Verbindungen** der Erweiterung.

Das folgende Beispiel zeigt die Zugriffssteuerung zu Datencentern für zwei Benutzergruppen. Gruppe 1 benötigt Zugriff zum Verwalten virtueller Maschinen für die

Datencenter NewYork_DC und Boston_DC. Gruppe 2 benötigt Zugriff zum Verwalten virtueller Maschinen für die Datencenter LosAngeles_DC und SanFrancisco_DC.

Erstellen Sie vom VMware vSphere-Client aus beispielsweise die Rolle „IBMDataProtectManage" und ordnen Sie dieser die Standardberechtigungen der Administratorrolle für virtuelle Maschinen sowie die Berechtigung **Datencenter** > **IBM Data Protection** zu.

Für Gruppe 1 ordnen Sie die Rolle „IBMDataProtectManage" den Datencentern NewYork_DC und Boston_DC zu. Für Gruppe 2 ordnen Sie die Rolle „IBMDataProtectManage" den Datencentern LosAngeles_DC und SanFrancisco_DC zu.

Die Benutzer in jeder Gruppe können mithilfe des IBM Spectrum Protect vSphere-Client-Plug-ins im vSphere-Web-Client nur virtuelle Maschinen in ihren jeweiligen Datencentern verwalten.

Probleme im Zusammenhang mit unzureichenden Berechtigungen

Wenn der Web-Browser-Benutzer für kein Datencenter über ausreichende Berechtigungen verfügt, ist der Zugriff auf die Sicht blockiert. Stattdessen wird die Fehlernachricht GVM2013E ausgegeben, um den Benutzer darüber zu informieren, dass aufgrund unzureichender Berechtigungen der Zugriff auf verwaltete Datencenter nicht möglich ist. Außerdem sind weitere neue Nachrichten verfügbar, die Benutzer über Probleme aufgrund unzureichender Berechtigungen informieren. Stellen Sie zum Beheben von Problemen mit Berechtigungen sicher, dass die Benutzerrolle wie in den obigen Abschnitten beschrieben eingerichtet ist. Die Benutzerrolle muss alle Berechtigungen haben, die in der Tabelle 'Erforderliche Berechtigungen für die Benutzer-ID des vCenter-Servers und die Einheit zum Versetzen von Daten' angegeben sind, und diese Berechtigungen müssen mit dem Kontrollkästchen Propagate to children auf der Ebene des Datencenters angewendet werden.

Wenn der Benutzer des IBM Spectrum Protect vSphere-Client-Plug-ins nicht über ausreichende Berechtigungen für ein Datencenter verfügt, sind die Datenschutzfunktionen für dieses Datencenter und seinen Inhalt in der Erweiterung nicht verfügbar.

Wenn die Berechtigungen der IBM Spectrum Protect-Benutzer-ID (die durch die Option VMCUser angegeben ist) für eine Sicherungs- oder Zurückschreibungsoperation nicht ausreichen, wird die folgende Nachricht angezeigt:

```
ANS9365E VMware vStorage-API-Fehler.
"Die Berechtigung zum Ausführen dieser Operation wurde verweigert."
```

Wenn die Berechtigungen der IBM Spectrum Protect-Benutzer-ID zum Anzeigen einer Maschine nicht ausreichen, werden die folgenden Nachrichten angezeigt:

```
Befehl 'Backup VM' gestartet. Gesamtzahl zu verarbeitender VMs: 1
ANS4155E Virtuelle Maschine 'tango' konnte auf dem VMware-Server nicht gefunden werden.
ANS4148E Vollständige VM-Sicherung der virtuellen Maschine 'foxtrot' ist mit Rückkehrcode 4390 fehlg
```

Weitere Informationen zur Verwendung von Berechtigungen enthält der Hinweis in **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

Führen Sie die folgenden Schritte aus, um bei Berechtigungsproblemen Protokollinformationen über den VMware Virtual Center-Server abzurufen:

1. Im Fenster mit den **vCenter-Servereinstellungen** wählen Sie **Protokollierungsoptionen** aus und setzen Sie **vCenter-Protokollierung** auf **Trivia (Trivia)**.

2. Reproduzieren Sie den Berechtigungsfehler.
3. Setzen Sie **vCenter-Protokollierung** auf den vorherigen Wert zurück, um zu verhindern, dass sehr viele Protokollinformationen aufgezeichnet werden.
4. Suchen Sie im Fenster mit den **Systemprotokollen** das neueste vCenter-Serverprotokoll (`vpxd-wxyz.log`) und suchen Sie nach der Zeichenfolge `NoPermission`. Beispiel:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Diese Protokollnachricht gibt an, dass die Benutzer-ID nicht über ausreichende Berechtigungen zum Erstellen einer Momentaufnahme (`createSnapshot`) verfügte.

Data Protection for VMware-Komponenten installieren

Sie können alle oder einige der Komponenten installieren, die im Data Protection for VMware-Paket für Ihr Betriebssystem verfügbar sind.

Informationen zu diesem Vorgang

Mithilfe des Data Protection for VMware-Installationsprogramms können Sie die folgenden Komponenten installieren:

- IBM Spectrum Protect Recovery Agent
- Windows Recovery Agent-Befehlszeilenschnittstelle
- Windows Dokumentation (Readme-Datei und Datei mit den Bemerkungen)
- Data Protection for VMware-Aktivierungsdatei
- Data Protection for VMware vSphere-GUI
- Feature der Einheit zum Versetzen von Daten, das die folgenden Elemente umfasst:
  - GUI der Einheit zum Versetzen von Daten
  - Web-Client der Einheit zum Versetzen von Daten
  - Laufzeitdateien der Client-API (64 Bit)
  - Befehlszeile des Verwaltungsclients
  - Laufzeitdateien der VMware vStorage-API

Sie können eine vollständige Installation auswählen oder die Option für erweiterte Installation verwenden, wenn Sie eine Einheit zum Versetzen von Daten (einen Mount-Proxy), Recovery Agent und die erforderlichen Unterstützungspakete installieren möchten.

Tipp: Sie können mehrere Einheiten zum Versetzen von Daten auf dem System erstellen, das auch die Data Protection for VMware-Software enthält, oder Sie können Einheiten zum Versetzen von Daten auf fernen Systemen erstellen. Bei der letzteren Konfiguration sind mehr Ressourcen für die Verwendung durch Data Protection for VMware verfügbar. Die Systeme, auf denen die Einheit zum Versetzen von Daten installiert ist, werden als vStorage-Sicherungsserver bezeichnet.

Data Protection for VMware-Installationspaket abrufen

Sie können das Data Protection for VMware-Installationspaket von einer IBM Download-Site wie IBM Passport Advantage abrufen.

Linux

Vorbereitende Schritte

Wenn Sie die Dateien herunterladen möchten, setzen Sie den Systembenutzergrenzwert für die maximale Dateigröße auf unbegrenzt, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können:

1. Geben Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

   ```
   ulimit -Hf
   ```

2. Ist der Systembenutzergrenzwert für die maximale Dateigröße nicht auf unbegrenzt gesetzt, ändern Sie ihn entsprechend, indem Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem befolgen.

Vorgehensweise

1. Laden Sie die korrekte Paketdatei von einer der folgenden Websites herunter:
   - Bei einer erstmaligen Installation oder einem neuen Release rufen Sie Passport Advantage unter der folgenden Adresse auf: http://www.ibm.com/software/lotus/passportadvantage/. Passport Advantage ist die einzige Site, von der Sie eine lizenzierte Paketdatei herunterladen können.
   - Neueste Informationen, Updates und Wartungsfixes finden Sie auf der Unterstützungssite für IBM Spectrum Protect: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.
2. Wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben, führen Sie die folgenden Schritte aus:
   a. Laden Sie die Paketdatei in ein Verzeichnis Ihrer Wahl herunter. Der Pfad darf nicht mehr als 40 Zeichen enthalten. Stellen Sie sicher, dass Sie die Installationsdateien in ein leeres Verzeichnis extrahieren. Extrahieren Sie die Dateien nicht in ein Verzeichnis, in das bereits Dateien extrahiert wurden oder das sonstige Dateien enthält.

   b. Linux Stellen Sie sicher, dass die Ausführungsberechtigung für das Paket definiert ist. Ändern Sie gegebenenfalls die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

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

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

      ```
      ./Paketname.bin
      ```

      Dabei ist *Paketname* der Name der heruntergeladenen Datei.

   d. Windows Extrahieren Sie das Paket, indem Sie doppelt auf *Paketname* klicken. Dabei ist *Paketname* der Name der heruntergeladenen Datei.

Data Protection for VMware-Komponenten mit dem Installationsassistenten installieren

Sie können die Data Protection for VMware-Komponenten mit dem Installationsassistenten installieren.

Informationen zu diesem Vorgang

Windows Sie können das Installationsprogramm der Suite verwenden, um sowohl Data Protection for VMware als auch die Einheit zum Versetzen von Daten zu installieren.

Linux Sie können das eigenständige Installationsprogramm verwenden, um sowohl Data Protection for VMware als auch die Einheit zum Versetzen von Daten zu installieren.

Data Protection for VMware-Komponenten auf Windows-Systemen installieren

Installieren Sie Data Protection for VMware-Komponenten und -Features mit dem Installationsassistenten.

Vorbereitende Schritte

Stellen Sie vor der Installation der Data Protection for VMware-Komponenten sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Benutzer-ID mit Administratorzugriffsberechtigung.
- Netzkonnektivität zu einem VMware vCenter Server der Version 6.x (oder höher) mit Administratorzugriffsberechtigung.
- Netzkonnektivität zu einem IBM Spectrum Protect-Server mit Administratorzugriff (Berechtigung **System** oder **Uneingeschränkte Maßnahmendomäne**). Dieser Server muss verfügbar und aktiv sein.
- Stellen Sie sicher, dass Sie die folgenden Voraussetzungen überprüft haben:
  - „Systemvoraussetzungen” auf Seite 13
  - „Für die Installation erforderliche Berechtigungen” auf Seite 17
  - „Erforderliche Kommunikationsports” auf Seite 17

Informieren Sie sich vor der Installation von Data Protection for VMware über die folgenden Optionen:

Installationstyp

Standardinstallation
Bei der Standardinstallation werden alle Data Protection for VMware-Komponenten und -Features installiert.

Erweiterte Installation
Die Anzeige 'Erweiterte Installation' bietet die Option zum Installieren einer einzelnen Einheit zum Versetzen von Daten. Bei diesem Prozess werden eine Einheit zum Versetzen von Daten, (ein Mount-Proxy), Recovery Agent und die erforderlichen Unterstützungspakete auf dem System installiert. Verwenden Sie diese Installationsoption, um einzelne Einheiten zum Versetzen von Daten hinzuzufügen. Mit dieser Option werden außerdem Agenten für Anwendungsschutz installiert, um die Wiederherstellung einzelner Datenbanken zu aktivieren. Nach der Installation können Sie mit-

hilfe der IBM Spectrum Protect-GUI die Einheit zum Versetzen von Daten und die Services über ein VMware vSphere-Plug-in konfigurieren.

Informationen zu diesem Vorgang

Sie können das Installationsprogramm der Suite verwenden, um Data Protection for VMware zu installieren. Die Datei `spinstall.exe` für das Installationsprogramm der Suite befindet sich im Stammverzeichnis des Installationspakets.

Eine Liste der Komponenten und Features, die Sie installieren können, finden Sie in „Installierbare Komponenten" auf Seite 1.

Vorgehensweise

Zum Installieren von Data Protection for VMware führen Sie die folgenden Schritte in dem Verzeichnis aus, das die Datei `spinstall.exe` für die zu installierende Komponente enthält:

1. Klicken Sie doppelt auf die Datei `spinstall.exe`.
2. Befolgen Sie die Anweisungen des Assistenten, um die ausgewählten Komponenten zu installieren.

Nächste Schritte

Informationen zum Zugriff auf die Data Protection for VMware vSphere-GUI finden Sie in:

- „Auf die Data Protection for VMware vSphere-GUI zugreifen" auf Seite 32

Wenn Sie die GUI zum ersten Mal starten, wird automatisch der Konfigurationsassistent angezeigt.

Data Protection for VMware auf Linux-Systemen installieren

Installieren Sie Data Protection for VMware auf Linux-Systemen im InstallAnywhere-Modus.

Vorbereitende Schritte

Stellen Sie vor der Installation von Data Protection for VMware sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Stellen Sie sicher, dass die Benutzer-ID über die notwendige Berechtigungsstufe verfügt und die erforderlichen Kommunikationsports offen sind, bevor Sie fortfahren.
- Der Installationsprozess erstellt den Benutzer `tdpvmware`. Sie müssen alle **`vmcli`**-Befehle als Benutzer `tdpvmware` und mit der Rootbenutzer-ID ausgeben.
- X Window Server ist erforderlich, wenn Sie im Konsolenmodus installieren.
- Stellen Sie sicher, dass Sie die folgenden Voraussetzungen überprüft haben:
  - „Systemvoraussetzungen" auf Seite 13
  - „Für die Installation erforderliche Berechtigungen" auf Seite 17
  - „Erforderliche Kommunikationsports" auf Seite 17

Vorgehensweise

Führen Sie zur Installation von Data Protection for VMware die folgenden Schritte aus:

1. Wechseln Sie vom Stammverzeichnis des Installationsordners in das Verzeichnis `CD/Linux/DataProtectionForVMware`.
2. Geben Sie den folgenden Befehl in eine Befehlszeile ein:
   `./install-Linux.bin`

Ergebnisse

Falls Sie Warnungen oder Fehler empfangen, überprüfen Sie die Protokolldateien auf weitere Informationen. Siehe „Protokolldateiaktivität" auf Seite 90.

Wenn Sie Data Protection for VMware aufgrund eines Fehlers nicht installieren können, finden Sie weitere Informationen in der Prozedur "Data Protection for VMware manuell entfernen" in „Data Protection for VMware auf einem Linux-System deinstallieren" auf Seite 38.

Neuinstallation von Data Protection for VMware unter Linux ausführen

Falls eine Installation unter Linux unterbrochen wird, können Sie die Installation normalerweise erneut starten. Schlägt jedoch der Neustart der Installation fehl, ist eine Neuinstallation erforderlich.

Informationen zu diesem Vorgang

Stellen Sie vor einer Neuinstallation sicher, dass das Produkt entfernt wurde. Führen Sie die folgenden Schritte aus, um für eine bereinigte Umgebung zu sorgen:

Vorgehensweise

1. Falls die Data Protection for VMware vSphere-GUI installiert ist, führen Sie die folgenden Tasks aus:
   a. Stoppen Sie die Data Protection for VMware-Befehlszeilenschnittstelle, indem Sie den folgenden Befehl ausgeben:
      `/etc/init.d/vmcli stop`
   b. Stoppen Sie den Web-Server der Data Protection for VMware-GUI, indem Sie den folgenden Befehl ausgeben:
      `/etc/init.d/webserver stop`
   c. Entfernen Sie das Paket `.rpm`, indem Sie den folgenden Befehl ausgeben:
      `rpm -e TIVsm-TDPVMwarePlugin`
2. Entfernen Sie die Produkteinträge aus der Implementierungsengine (Deployment Engine):
   a. Geben Sie den folgenden Befehl aus, um alle Einträge in der Implementierungsengine (Deployment Engine) aufzulisten:
      `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b. Geben Sie den folgenden Befehl aus, um alle Einträge aus der Implementierungsengine (Deployment Engine) zu entfernen:
      `/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <Diskriminante>`
   c. Entfernen Sie das Verzeichnis `/var/ibm/common`.
   d. Entfernen Sie das Verzeichnis `/usr/ibm/common`.
   e. Bereinigen Sie das Verzeichnis `/tmp`, indem Sie die Datei `acu_de.log` entfernen, falls sie vorhanden ist.
   f. Entfernen Sie das Verzeichnis `/tmp`, das die ID des Benutzers enthält, der die Implementierungsengine (Deployment Engine) installiert hat
   g. Entfernen Sie alle Einträge der Implementierungsengine (Deployment Engine) aus der Systemdatei `/etc/inittab`. Die Einträge sind durch die Angaben

`#Begin AC Solution Install block` und `#End AC Solution Install block` begrenzt. Entfernen Sie den gesamten Text zwischen diesen Begrenzern und entfernen Sie auch den Begrenzungstext.

h. Entfernen Sie alle Verweise auf die Implementierungsengine (Deployment Engine) aus der Systemdatei `/etc/services`.

3. Entfernen Sie alle Data Protection for VMware-Dateien aus der fehlgeschlagenen Installation:
   a. Entfernen Sie Dateien im *<BENUTZERINSTALLATIONSVERZEICHNIS>*, also unter dem Pfad, unter dem Sie die fehlgeschlagene Installation versucht haben. Beispiel: `/opt/tivoli/tsm/TDPVMware/`
   b. Entfernen Sie alle Desktopverknüpfungen.
4. Sichern Sie die globale Registry-Datei (`/var/.com.zerog.registry.xml`). Entfernen Sie nach der Sicherung dieser Datei alle Tags, die auf Data Protection for VMware verweisen.
5. Entfernen Sie Protokolldateien unter dem Stammverzeichnis, die die Zeichenfolge `TDPVMware` enthalten. Beispiel:
   `IA-TDPVMware-00.log` oder `IA-TDPVMware_Uninstall-00.log`.
6. Entfernen Sie den Benutzer, der die Data Protection for VMware-Befehlszeilenschnittstelle ausgeführt hat.
   a. Geben Sie den folgenden Befehl aus:
      ```
      userdel -r tdpvmware
      ```
   b. Geben Sie den folgenden Befehl aus:
      ```
      groupdel tdpvmware
      ```

      Tipp: In einigen Linux-Versionen entfernt der Befehl **`userdel`** auch die Gruppe, wenn kein weiterer zugehöriger Benutzer vorhanden ist. Daher können Sie Nachrichten in Bezug auf einen Fehlschlag zu diesem Befehl ignorieren.

Ergebnisse

Starten Sie nach Abschluss dieser Schritte die Neuinstallation.

Data Protection for VMware-Komponenten im unbeaufsichtigten Modus installieren

Sie können Data Protection for VMware im Hintergrund installieren. Während dieser unbeaufsichtigten Installation werden keine Nachrichten angezeigt.

Informationen zu diesem Vorgang

Windows Sie können das Installationsprogramm der Suite verwenden, um sowohl Data Protection for VMware als auch die Einheit zum Versetzen von Daten zu installieren.

Linux Sie können das eigenständige Installationsprogramm verwenden, um sowohl Data Protection for VMware als auch die Einheit zum Versetzen von Daten zu installieren.

Data Protection for VMware auf Windows-Systemen im unbeaufsichtigten Modus installieren

Installieren Sie alle Data Protection for VMware-Komponenten und das Feature der Einheit zum Versetzen von Daten mit dem Installationsprogramm der Suite im unbeaufsichtigten Modus.

Vorbereitende Schritte

Stellen Sie vor der Installation von Data Protection for VMware und des Features der Einheit zum Versetzen von Daten anhand der folgenden Abschnitte sicher, dass Ihr System die Voraussetzungen erfüllt:

- „Systemvoraussetzungen" auf Seite 13
- „Für die Installation erforderliche Berechtigungen" auf Seite 17
- „Erforderliche Kommunikationsports" auf Seite 17

Informationen zu diesem Vorgang

Einschränkung: Alle Features werden an ihrer Standardposition installiert. Informationen zur Lokalisierung der Standardinstallationsverzeichnisse für die Komponenten enthalten die Unterthemen in „Installierbare Komponenten" auf Seite 1.

Vorgehensweise

Führen Sie zur Installation von Data Protection for VMware die folgenden Schritte aus:

1. Geben Sie bei einer Eingabeaufforderung den folgenden Befehl aus:

   ```
   cd Extraktionsordner\TSMVMWARE_WIN
   ```

2. Geben Sie den folgenden Befehl ein:

   ```
   spinstall.exe /silent
   ```

   Bei der erstmaligen Bereitstellung eines Datenträgers wird die folgende Nachricht angezeigt:

   ```
   Der Treiber für virtuelle Datenträger ist noch nicht registriert. Recovery Agent kann den Treiber
   jetzt registrieren. Während der Registrierung wird möglicherweise eine Microsoft Windows-Logowarnung ange
   damit die Registrierung ausgeführt werden kann.
   Möchten Sie den Treiber für virtuelle Datenträger jetzt registrieren?
   ```

   Geben Sie zum Fortsetzen des Vorgangs **Ja** ein, um den Treiber für virtuelle Datenträger zu registrieren.

Zugehörige Tasks:

„Data Protection for VMware für Windows im unbeaufsichtigten Modus deinstallieren" auf Seite 37

Data Protection for VMware auf Linux-Systemen im unbeaufsichtigten Modus installieren

Sie können anpassen, welche Data Protection for VMware-Features unter einem Linux-Betriebssystem im unbeaufsichtigten Modus installiert werden sollen.

Vorbereitende Schritte

Stellen Sie vor der Installation von Data Protection for VMware sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Stellen Sie sicher, dass die Benutzer-ID über die notwendige Berechtigungsstufe verfügt und die erforderlichen Kommunikationsports offen sind, bevor Sie fortfahren.
- Der Installationsprozess erstellt den Benutzer `tdpvmware`. Sie müssen alle **`vmcli`**-Befehle als Benutzer `tdpvmware` und mit der Rootbenutzer-ID ausgeben.
- X Window Server ist erforderlich, wenn Sie im Konsolenmodus installieren.
- Stellen Sie sicher, dass Sie die folgenden Voraussetzungen überprüft haben:
  - „Systemvoraussetzungen" auf Seite 13
  - „Für die Installation erforderliche Berechtigungen" auf Seite 17
  - „Erforderliche Kommunikationsports" auf Seite 17

Informationen zu diesem Vorgang

Data Protection for VMware stellt die folgenden Features für unbeaufsichtigte Installation für Linux-Betriebssysteme zur Verfügung:

Tabelle 7. Data Protection for VMware-Features für unbeaufsichtigte Installation

Feature	Beschreibung	Standardmäßig installiert?
Docs	Readme-Datei	Ja
TDPVMwareDM	Die Installation dieses Features umfasst die Aktivierungsdatei. Ermöglicht IBM Spectrum Protect die Ausführung der folgenden Sicherungstypen: • VM-Sicherung des Typs 'Periodisch inkrementell' • Vollständige VM-Sicherung des Typs 'Immer inkrementell' • VM-Sicherung des Typs 'Immer inkrementell - Inkrementell' Wenn Sie Sicherungsarbeitslast auslagern, muss diese Datei auf dem vStorage-Sicherungsserver installiert sein.	Ja
TDPVMwareGUI	Data Protection for VMware vSphere-GUI. **Anmerkung:** Umfasst auch die Installation der Aktivierungsdatei.	Nein

Vorgehensweise

Zum Installieren von Data Protection for VMware führen Sie die folgenden Schritte in dem Verzeichnis aus, in das Sie das Installationspaket extrahiert haben:

1. Öffnen Sie die Datei *Pfad*`../Linux/DataProtectionForVMware/installer.properties` und entfernen Sie die Kommentarzeichen des folgenden Eintrags, um die Lizenzvereinbarung zu akzeptieren (dabei ist *Pfad* der Installationsordner):

   ```
   LICENSE_ACCEPTED=TRUE
   ```

2. Wählen Sie eine der folgenden Methoden aus, um die Data Protection for VMware-Komponenten zu installieren:
   - Für eine Standardinstallation öffnen Sie den Ordner `CD/Linux/DataProtectionForVMware` und geben Sie den folgenden Befehl ein:

     ```
     ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
     ```

   - Für eine angepasste Installation führen Sie die folgenden Schritte aus:
     a. Editieren Sie die Datei `installer.properties` mit den entsprechenden Werten:
        1) Geben Sie **`INSTALL_MODE=Custom`** an. Stellen Sie sicher, dass das Nummernzeichen (#) aus dieser Anweisung entfernt wird.
        2) Geben Sie die zu installierenden Features mit der Option **`CHOSEN_INSTALL_FEATURE_LIST`** an. Mit dem folgenden Wert werden beispielsweise alle Features installiert:

           ```
           CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
           ```

     b. Im Ordner `CD/Linux/DataProtectionForVMware` geben Sie den folgenden Befehl aus:

        ```
        ./install-Linux.bin -i silent -f installer.properties
        ```

Erste Schritte nach der Installation von Data Protection for VMware

Nach der Installation von Data Protection for VMware führen Sie die Konfiguration durch. Die Verwendung des Konfigurationsassistenten ist die bevorzugte Methode für die Konfiguration von Data Protection for VMware.

Arbeitsblatt zur Konfiguration

Verwenden Sie dieses Arbeitsblatt, um Informationen aufzuzeichnen, die Sie bei der Konfiguration und Verwaltung von Data Protection for VMware benötigen. Das Arbeitsblatt soll als Merkhilfe für die Werte dienen, die Sie nach der Konfiguration angegeben haben.

Tabelle 8. Data Protection for VMware-Arbeitsblatt zur Konfiguration

Eintrag	Ihr Wert	Notizen
Informationen zum IBM Spectrum Protect-Server		
Adresse des IBM Spectrum Protect-Servers		
Port des IBM Spectrum Protect-Servers		
ID/Kennwort des IBM Spectrum Protect-Serveradministrators		
Administratorport des IBM Spectrum Protect-Servers		
Knotendefinitionsoptionen		
Präfix, das den Knoten hinzugefügt werden soll		
Maßnahmendomäne, die beim Registrieren neuer Knoten verwendet werden soll		
Name/Kennwort des vCenter-Knotens		
Name/Kennwort des VMCLI-Knotens		

Tabelle 8. Data Protection for VMware-Arbeitsblatt zur Konfiguration (Forts.)

Eintrag	Ihr Wert	Notizen
Namen/Kennwörter der Datencenterknoten **Hinweis:** Sie können mehrere Datencenterknoten erstellen.		Der Name des Datencenterknotens besteht aus dem angegebenen Präfix, auf das ein Unterstreichungszeichen gefolgt vom Datencenternamen folgt. Beispiel: *Knotenpräfix_Datencentername*
Namen/Kennwörter der Knoten der Einheit zum Versetzen von Daten auf dem vStorage-Sicherungsserver **Hinweis:** Sie können mehrere Knoten der Einheit zum Versetzen von Daten erstellen.		Der Name des Knotens der Einheit zum Versetzen von Daten besteht aus dem Datencenterknotennamen, auf den ein Unterstreichungszeichen gefolgt von den Buchstaben `DM` folgt. Beispiel: *Datencenterknotenname*_DM
Namen/Kennwörter der Knoten der Einheit zum Versetzen von Daten auf fernen Servern **Hinweis:** Sie können mehrere Knoten der Einheit zum Versetzen von Daten erstellen, die sich nicht auf dem vStorage-Sicherungsserver befinden.		
Mount-Proxy-Knoten Der Mount-Proxy-Knoten wird beim Zurückschreiben von Daten verwendet.	Windows: Linux:	

Auf die Data Protection for VMware vSphere-GUI zugreifen

Verwenden Sie die Data Protection for VMware vSphere-GUI, um virtuelle Maschinen in einer VMware vCenter-Umgebung zu sichern, zurückzuschreiben und zu verwalten.

Vorbereitende Schritte

Damit Sie auf die Data Protection for VMware vSphere-GUI zugreifen können, müssen Sie bei der Installation die Option zum Schützen Ihrer Daten in einer vSphere-Umgebung ausgewählt haben.

Vorgehensweise

- Wenn Sie bei der Installation die Option **Zugriff auf die GUI über einen Web-Browser aktivieren** ausgewählt haben, können Sie über den Browser auf die Data Protection for VMware vSphere-GUI zugreifen:
  1. Öffnen Sie einen Web-Browser und geben Sie die folgende URL ein:
     `https://`*`Hostname`*`:`*`Port`*`/TsmVMwareUI`

     Dabei gilt Folgendes:
     - *Hostname* ist der Name des Systems, auf dem die Data Protection for VMware vSphere-GUI installiert ist.
     - *Port* ist die Portnummer, über die auf die vSphere-GUI zugegriffen wird. Die Standardportnummer ist 9081.
  2. Melden Sie sich mit Ihrer vCenter-Benutzer-ID und dem zugehörigen Kennwort an.

- Wenn Sie bei der Installation nicht die Option **Zugriff auf die GUI über einen Web-Browser aktivieren** ausgewählt haben, können Sie die Data Protection for VMware vSphere-GUI starten, indem Sie die folgenden Schritte ausführen:
  1. Öffnen Sie den VMware vSphere-Client und melden Sie sich mit der vCenter-Benutzer-ID und dem zugehörigen Kennwort an.
  2. In der Anzeige für Lösungen und Anwendungen (**Solutions and Applications**) des vSphere-Clients klicken Sie auf das Symbol für die Data Protection for VMware vSphere-GUI.

Upgrade für Data Protection for VMware durchführen

Sie können für Data Protection for VMware ausgehend von einer Vorgängerversion der Software ein Upgrade durchführen.

Informationen zur Kompatibilität mit früheren Versionen finden Sie in Technote 1993819.

Upgrade von Version 7.1.8 durchführen: Wird während des Upgradeprozesses eine Nachricht mit der Frage angezeigt, ob die vorhandene `jextract`-Datei überschrieben werden soll, wählen Sie die Option um Überschreiben aller Dateien aus.

Upgrade für Data Protection for VMware durchführen

In dieser Prozedur ist dokumentiert, wie Sie ein Upgrade auf Data Protection for VMware V8.1.4 durchführen.

Vorbereitende Schritte

Wichtig: Diese Upgradeprozedur wird bei einem System angewendet, auf dem IBM Spectrum Protect Snapshot for VMware nicht installiert ist.

Für das Upgrade von Data Protection for VMware benötigen Sie Administratorberechtigungen.

Aktualisierungen für die vorhandene Data Protection for VMware vSphere-GUI werden wie folgt verarbeitet:

- Parameterdateien werden gesichert, bevor der Upgradeprozess für die Data Protection for VMware vSphere-GUI beginnt.
- Es werden dieselben Portnummern für die Derby-Datenbank und für den Standardbasisport von WebSphere Application Server verwendet.
- Linux Die Werte im Profil (`vmcliprofile`) werden für die Data Protection for VMware-Befehlszeilenschnittstelle verwendet.

Einschränkung:

- Windows Wenn IBM Spectrum Protect for Virtual Environments an einer anderen Position als der Standardposition installiert war, werden die Features von IBM Spectrum Protect for Virtual Environments V8.1.4 durch den Upgradeprozess im Standardinstallationsverzeichnis installiert. Es ist nicht möglich, ein Upgrade an eine andere Position als die Standardposition auszuführen. Informationen zu den Standardinstallationsverzeichnissen für jedes Feature finden Sie in den Unterthemen unter „Installierbare Komponenten” auf Seite 1.
- Linux Windows Beim Upgradeprozess werden keine neuen Komponenten installiert.

Falls in Ihrer Vorgängerversion beispielsweise nur die Recovery Agent-GUI installiert war, wird die Recovery Agent-Befehlszeilenschnittstelle mit der Upgradeprozedur nicht installiert. In einem solchen Szenario müssen Sie das Installationsprogramm erneut ausführen und die Installation der fehlenden Komponente auswählen.

- Linux Die Version von Recovery Agent unter Linux muss mit der Version von Recovery Agent auf dem Windows-Proxy identisch sein. Bei einem Upgrade von Recovery Agent unter Linux müssen Sie daher auch für die Version von Recovery Agent auf dem Windows-Proxy ein Upgrade durchführen.

Vorgehensweise

Führen Sie zum Upgrade von Data Protection for VMware die folgenden Schritte aus:

1. Stoppen Sie alle aktiven Data Protection for VMware-Komponenten und -Services.
2. Heben Sie die Bereitstellung aller bereitgestellten virtuellen Datenträger auf. Sie können die Recovery Agent-GUI oder -Befehlszeilenschnittstelle (Befehl **mount del**) verwenden, um die Bereitstellung von Datenträgern aufzuheben.
3. Befolgen Sie die Anweisungen in „Data Protection for VMware-Komponenten auf Windows-Systemen installieren” auf Seite 25.

   Anmerkung: Linux Ist die Einheit zum Versetzen von Daten Version 6.x installiert, müssen Sie diese deinstallieren, bevor Sie V8.1.4 installieren. Befolgen Sie die Anweisungen im Thema "IBM Spectrum Protect Linux x86_64-Client deinstallieren".
4. Laden Sie das Codepaket herunter.
5. Starten Sie von dem Ordner, in dem das Codepaket gespeichert wurde, den Upgradeprozess:
   a. Windows Führen Sie die Datei `spinstall.exe` aus.
   b. Linux Führen Sie die Datei `install-Linux.bin` aus.

   Sie können nur eine einzige Data Protection for VMware vSphere-GUI auf einer Maschine installieren. Daher sind mehrere Data Protection for VMware vSphere-GUIs auf derselben Maschine nicht zulässig.

Upgrade für Data Protection for VMware auf einem 64-Bit-Windows-System im unbeaufsichtigten Modus durchführen

Sie können ein Upgrade für Data Protection for VMware auf einem unterstützten 64-Bit-Betriebssystem im unbeaufsichtigten Modus durchführen.

Vorbereitende Schritte

Wenn Data Protection for VMware Version 6.x an einer anderen Position als der Standardposition installiert wurde, werden die Features von Data Protection for VMware V8.1.4 durch den unbeaufsichtigten Upgradeprozess im Standardinstallationsverzeichnis installiert. Es ist nicht möglich, ein Upgrade im unbeaufsichtigten Modus an eine andere Position als die Standardposition auszuführen. Informationen zu den Standardinstallationsverzeichnissen für jedes Feature finden Sie in den Unterthemen des Abschnitts „Installierbare Komponenten” auf Seite 1.

Vorgehensweise

Führen Sie zum Upgrade von Data Protection for VMware die folgenden Schritte aus:

1. Stoppen Sie alle aktiven Data Protection for VMware-Komponenten.
2. Heben Sie die Bereitstellung aller bereitgestellten virtuellen Datenträger auf. Sie können die Recovery Agent-GUI oder -Befehlszeilenschnittstelle (Befehl **mount del**) verwenden, um die Bereitstellung von Datenträgern aufzuheben.
3. Heben Sie die Bereitstellung aller bereitgestellten virtuellen Datenträger auf. Sie können die Recovery Agent-GUI oder -Befehlszeilenschnittstelle (Befehl **mount del**) verwenden, um die Bereitstellung von Datenträgern aufzuheben.
4. Laden Sie das Codepaket herunter.
5. Wechseln Sie in dem Ordner für Data Protection for VMware zu dem Ordner `X64`.
6. Geben Sie in dem Fenster mit Eingabeaufforderung den folgenden Befehl ein:
   ```
   spinstall.exe /s /v"/qn REBOOT=ReallySuppress"
   ```

Upgrade für Data Protection for VMware auf einem Linux-System im unbeaufsichtigten Modus durchführen

Sie können ein Upgrade für Data Protection for VMware auf einem unterstützten Linux-Betriebssystem im unbeaufsichtigten Modus durchführen.

Informationen zu diesem Vorgang

Verwenden Sie die folgenden Data Protection for VMware-Parameter mit dem Feature für unbeaufsichtigte Installation:

Tabelle 9. Data Protection for VMware-Parameter für das unbeaufsichtigte Upgrade

Parameter	Beschreibung	Standardwert
VCENTER_HOSTNAME	Der vollständig qualifizierte Domänenname oder die IP-Adresse des vCenter-Servers.	Keiner
VCENTER_USERNAME	Die vCenter-Benutzer-ID. Diese Benutzer-ID muss ein VMware-Administrator sein, der über die Berechtigung zum Registrieren und Aufheben der Registrierung für Erweiterungen verfügt.	Keiner
VCENTER_PASSWORD	Das vCenter-Kennwort.	Keiner
DIRECT_START	Für den Zugriff auf die Data Protection for VMware vSphere-GUI in einem Web-Browser geben Sie **DIRECT_START=YES** an. Sie greifen über ein URL-Lesezeichen für den GUI-Web-Server auf die Data Protection for VMware vSphere-GUI zu. Wenn Sie nicht in einem Web-Browser auf die Data Protection for VMware vSphere-GUI zugreifen möchten, geben Sie **DIRECT_START=NO** an.	`YES` **Wichtig:** Nach dem Abschluss des Upgrades kann der Wert für **DIRECT_START** nur durch eine Neuinstallation des Produkts geändert werden.

Vorgehensweise

Führen Sie zum Upgrade von Data Protection for VMware die folgenden Schritte aus:

1. Stellen Sie sicher, dass keine Sicherungs-, Zurückschreibungs- oder Bereitstellungssitzungen aktiv sind.
2. Stellen Sie sicher, dass alle vorhandenen Instanzen der Data Protection for VMware vSphere-GUI oder Recovery Agent-GUI geschlossen sind.
3. Laden Sie das Codepaket herunter.
4. Wechseln Sie vom Data Protection for VMware-Ordner in den Linux-Ordner.
5. Geben Sie in einem Fenster mit Eingabeaufforderung den Befehl `././install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` mit den bevorzugten Parametern ein.
   Beispiel:

```
././install-Linux.bin -i silent -LICENSE_ACCEPTED=true
-VCENTER_HOSTNAME=Hostname -VCENTER_USERNAME=Benutzername
-VCENTER_PASSWORD=Kennwort
-DIRECT_START=yes -REGISTER_PLUGIN=yes
```

Data Protection for VMware deinstallieren

Der Prozess zum Deinstallieren von Data Protection for VMware ist für eine Neuinstallation und für eine Version, für die ein Upgrade durchgeführt wurde, identisch.

Data Protection for VMware unter Windows deinstallieren

Deinstallieren Sie Data Protection for VMware-Komponenten und entfernen Sie Dateien und Verzeichnisse aus einem Windows-System.

Vorbereitende Schritte

Verwenden Sie die folgenden Anleitungen, damit eine erfolgreiche Deinstallation sichergestellt ist:

- Wenn andere Web-GUI-Hosts für Data Protection for VMware das IBM Spectrum Protect vSphere-Client-Plug-in verwenden, dürfen Sie die Registrierung der Web-Client-Erweiterung nicht aufheben.

Informationen zu diesem Vorgang

Nach der Beendigung der Deinstallation befinden sich die Konfigurations- und Eigenschaftendateien in `C:\Programme\IBM\SpectrumProtect\Framework\VEGUI\config`.

Vorgehensweise

1. Stoppen Sie alle aktiven Data Protection for VMware-Komponenten.
2. Heben Sie die Bereitstellung aller bereitgestellten virtuellen Datenträger auf.
3. Löschen Sie vorhandene Sicherungen virtueller Maschinen mit dem Befehl `delete backup` der Einheit zum Versetzen von Daten.
4. Entfernen Sie die installierten Services der Einheit zum Versetzen von Daten mit dem Befehl `dsmcutil remove`.

   Zum Aufrufen einer Liste der Services wechseln Sie in `C:\Programme\Tivoli\TSM\baclient\` und führen Sie den Befehl `dsmcutil list` aus.

   Entfernen Sie die Services mit einem ähnlichen Befehl wie dem folgenden, wobei Sie den Namen in Anführungszeichen durch den aufgelisteten Service ersetzen:

```
 dsmcutil remove /name:"Ferner TSM-Clientagent"
dsmcutil remove /name:"TSM-Clientakzeptor"
```

5. Klicken Sie auf **Start** > **Systemsteuerung** > **Programme und Funktionen** > **Programm deinstallieren**. Deinstallieren Sie die folgenden Programme:
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware Suite
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware-Lizenz
   - IBM Spectrum Protect JVM
6. Entfernen Sie die folgenden Data Protection for VMware-Dateien und -Verzeichnisse aus dem Dateisystem, falls sie vorhanden sind. Für IBM Spectrum Protect for Virtual Environments Version 8.1.6 und höher löschen Sie Folgendes:

   ```
   C:\IBM\SpectrumProtect
   C:\Programme\IBM\SpectrumProtect
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   C:\IBM\SpectrumProtect
   C:\Programme\IBM\SpectrumProtect
   ```

   Sie können außerdem Folgendes entfernen:

   ```
   C:\Programme\Tivoli\TSM
   ```

   falls die verbleibenden Protokoll- und Konfigurationsdateien nicht mehr benötigt werden. Falls Sie diese Dateien behalten möchten: Sie befinden sich in `C:\Programme\Tivoli\TSM\baclient`. Für IBM Spectrum Protect for Virtual Environments Version 8.1.4 und ältere Versionen löschen Sie Folgendes:

   ```
   C:\IBM\tivoli
   C:\Programme (x86)\Common Files\Tivoli\TDPVMware
   C:\Programme\Common Files\Tivoli
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   ```

   Sie können außerdem Folgendes entfernen:

   ```
   C:\Programme\Tivoli\TSM
   ```

   falls die verbleibenden Protokoll- und Konfigurationsdateien nicht mehr benötigt werden. Falls Sie diese Dateien behalten möchten: Sie befinden sich in `C:\Programme\Tivoli\TSM\baclient`.

Nächste Schritte

Überprüfen Sie, ob alle Komponenten von dem System entfernt wurden.

Data Protection for VMware für Windows im unbeaufsichtigten Modus deinstallieren

Sie können Data Protection for VMware unter einem Windows-Betriebssystem im unbeaufsichtigten Modus deinstallieren.

Informationen zu diesem Vorgang

Nach der Beendigung der Deinstallation befinden sich die Konfigurations- und Eigenschaftendateien in `C:\Programme\IBM\SpectrumProtect\Framework\VEGUI\config`.

Vorgehensweise

Führen Sie zur Deinstallation von Data Protection for VMware die folgenden Schritte aus:

1. Stoppen Sie alle aktiven Data Protection for VMware-Komponenten.
2. Heben Sie die Bereitstellung aller bereitgestellten virtuellen Datenträger auf. Sie können die Recovery Agent-GUI oder -Befehlszeilenschnittstelle (Befehl **mount del**) verwenden, um die Bereitstellung von Datenträgern aufzuheben.
3. Verwenden Sie in einem Fenster mit Eingabeaufforderung den Befehl **cd**, um in einen der folgenden Ordner zu wechseln:
   - Zum Anpassen der Deinstallationsoperation wechseln Sie in den Ordner `X64`.
   - Zum Deinstallieren von Data Protection for VMware mit dem Installationsprogramm der Suite wechseln Sie in `<Extraktionsordner>TSM4VE_WIN`.
4. Führen Sie im Fenster mit Eingabeaufforderung den folgenden Befehl aus:
   - Für eine angepasste Deinstallationsoperation wählen Sie aus den folgenden Befehlen aus:
     - Geben Sie den folgenden Befehl ein, um Data Protection for VMware zu deinstallieren und die Registrierung der Data Protection for VMware vSphere-GUI aufzuheben:

       ```
       spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
       VCENTER_HOSTNAME=<Hostname oder IP-Adresse für vCenter>
       VCENTER_USERNAME=<vCenter-Benutzername>
       VCENTER_PASSWORD=<vCenter-Kennwort>"
       ```
   - Geben Sie den folgenden Befehl ein, um alle Features mit dem Installationsprogramm der Suite zu deinstallieren:

     ```
     spinstall.exe /silent /remove
     ```
5. Starten Sie das System erneut, wenn die Deinstallation abgeschlossen ist.

Data Protection for VMware auf einem Linux-System deinstallieren

Deinstallieren Sie Data Protection for VMware und entfernen Sie Dateien und Verzeichnisse unter einem unterstützten Linux-Betriebssystem.

Vorbereitende Schritte

Verwenden Sie die folgenden Anleitungen, damit eine erfolgreiche Deinstallation sichergestellt ist:

- Entfernen Sie die Knoten vom IBM Spectrum Protect-Server. Diese Task müssen Sie vor der Deinstallation des Produkts Data Protection for VMware ausführen:
  1. Führen Sie den Befehl `dsmadmc` im Verzeichnis `/opt/tivoli/tsm/client/ba/bin/dsmadmc` aus.
  2. Möglicherweise müssen Sie den Befehl `del` verwenden, um die Dateibereiche für die Knoten zu löschen: `del file` *`Knotenname`* `*`
  3. Verwenden Sie den Befehl `q`, um die Knoten abzufragen: `q filespace` *`Knotenname`* `*`
  4. Verwenden Sie den Befehl `rem`, um die Knoten zu entfernen: `rem node` *`Knotenname`*
- Stoppen Sie die `dsmcad`-Services, die für Einheiten zum Versetzen von Daten erstellt wurden. Befolgen Sie die Anweisungen in dem technischen Hinweis http://www-01.ibm.com/support/docview.wss?uid=swg21358414.

1. Verwenden Sie den Befehl `ps`, um zu prüfen, ob der `dsmcad`-Service aktiv ist: `ps -ef|grep dsmcad`
2. Verwenden Sie den Befehl `kill`, um den `dsmcad`-Service zu stoppen: `kill -9` *`dsmcad-Prozess-ID`*

- Sie müssen die Dateien bereinigen, die zu der Erstellung von Services für eine Einheit zum Versetzen von Daten gehören. Wechseln Sie in das Installationsverzeichnis und geben Sie den folgenden Befehl aus:

  ```
  /opt/tivoli/tsm/client/ba/bin/dsmutillnx cleanupDmFiles 1
  ```

  Drücken Sie die Eingabetaste, um den Knotennamen auszuwählen, und drücken Sie erneut die Eingabetaste, um die Löschung auszuführen.

  Sie finden die Knotennamen in der Datei `dsm.sys`.
- Wenn Sie das IBM Spectrum Protect vSphere-Client-Plug-in in einer Umgebung mit VMware vSphere 5.5 deinstallieren, werden nur die zugehörigen Bezeichnungen und Beschreibungen der Berechtigungen entfernt. Die tatsächlichen Berechtigungen bleiben installiert. Dieses Problem ist eine bekannte VMware-Einschränkung. Weitere Informationen dazu enthält der folgende Artikel in der VMware-Knowledge Base: http://kb.vmware.com/kb/2004601.
- Die Data Protection for VMware-Aktivierungsdatei wird nach der Deinstallation des Produkts nicht entfernt.

Informationen zu diesem Vorgang

Wenn Sie Data Protection for VMware auf einem Linux-System deinstallieren, ist der Typ der Deinstallation standardmäßig derselbe Prozess wie der Typ der ursprünglichen Installation. Um einen anderen Deinstallationsprozess zu verwenden, müssen Sie den korrekten Parameter angeben. Falls Sie beispielsweise einen Prozess für die unbeaufsichtigte Installation verwendet haben, können Sie den Installationsassistenten zur Deinstallation verwenden, indem Sie den Parameter `–i swing` angeben. Führen Sie den Deinstallationsprozess als Root aus. Das Rootbenutzerprofil muss als Quelle verwendet werden. Wenn Sie den Befehl `su` verwenden, um zum Root zu wechseln, verwenden Sie den Befehl `su -`, um das Rootprofil als Quelle zu benutzen.

Sobald der Deinstallationsprozess mit dem Entfernen von Programmdateien begonnen hat, kann das System bei einem Abbruch nicht in einen bereinigten Zustand zurückgesetzt werden. Diese Situation kann dazu führen, dass der Versuch einer Neuinstallation fehlschlägt. Bereinigen Sie daher das System, indem Sie die Tasks ausführen, die in „Data Protection for VMware manuell aus einem Linux-System entfernen” auf Seite 40 beschrieben sind.

Führen Sie zur Deinstallation von Data Protection for VMware die folgenden Schritte aus:

Vorgehensweise

1. Wechseln Sie in das Verzeichnis für das Deinstallationsprogramm. Der folgende Pfad ist die Standardposition für das Deinstallationsprogramm: `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`
2. Verwenden Sie abhängig vom Typ der Installation eine der folgenden Methoden, um Data Protection for VMware zu deinstallieren:

   Anmerkung: Die Befehle in dieser Prozedur müssen in einer einzigen Zeile eingegeben werden. Zur besseren Seitenformatierung sind diese Beispiele in zwei Zeilen dargestellt.

- Soll der Installationsassistent verwendet werden, um Data Protection for VMware zu deinstallieren, geben Sie den folgenden Befehl ein:

  ```
  ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
  ```

- Soll die Konsole verwendet werden, um Data Protection for VMware zu deinstallieren, geben Sie den folgenden Befehl ein:

  ```
  ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
  ```

- Soll Data Protection for VMware im unbeaufsichtigten Modus deinstalliert werden, geben Sie den folgenden Befehl ein:

  ```
  ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
  -f uninstall.properties
  ```

  Die Datei `uninstall.properties` enthält die vCenter-Verbindungsinformationen. Diese Informationen sind erforderlich, um die Data Protection for VMware vSphere-GUI zu deinstallieren.

Data Protection for VMware manuell aus einem Linux-System entfernen

Informationen zu diesem Vorgang

Wenn Data Protection for VMware nicht mit dem Standarddeinstallationsverfahren deinstalliert werden kann, müssen Sie Data Protection for VMware wie nachfolgend beschrieben manuell aus dem System entfernen. Führen Sie diesen Prozess als Root aus.

Vorgehensweise

1. Wenn Sie die Data Protection for VMware vSphere-GUI installieren haben, entfernen Sie das entsprechende Paket mit dem folgenden Befehl aus der Paketmanagerdatenbank:

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. Entfernen Sie die IBM Spectrum Protect-API mit dem folgenden Befehl:

   ```
   rpm -e TIVsm-API64
   gskssl64.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. Entfernen Sie die Produkteinträge aus der Implementierungsengine (Deployment Engine):

   a. Geben Sie den folgenden Befehl aus, um eine Liste aller Einträge anzuzeigen:

      ```
      /usr/ibm/common/acsi/bin/de_lsrootiu.sh
      ```

   b. Geben Sie den folgenden Befehl aus, um die Einträge der installierten Einheiten zu entfernen, die mit Data Protection for VMware in Verbindung stehen:

      ```
      /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <Diskriminante>
      ```

      Stellen Sie sicher, dass die folgenden Einheiteneinträge entfernt werden:

      ```
      FBJRE
      TDPVMwareGUI
      JavaHelp
      TDPVMwareDM
      ```

      Entfernen Sie nach der Beendigung des Deinstallationsprogramms die folgenden Verzeichnisse, falls sie vorhanden sind:

      - `/opt/tivoli/tsm/client`
      - `/opt/tivoli/tsm/tdpvmware`

Entfernen Sie den Benutzer `tdpvmware` und die zugehörigen Verzeichnisse:

- `userdel tdpvmware`
- `/home/tdpvmware`
- `/etc/adsm`

4. Sichern Sie die globale Registry-Datei (`/var/.com.zerog.registry.xml`). Entfernen Sie nach dem Sichern der Datei alle Tags, die sich auf Data Protection for VMware beziehen.
5. Entfernen Sie alle Dateien im Installationsverzeichnis (`/opt/tivoli/tsm/tdpvmware`). Entfernen Sie außerdem alle Verknüpfungen, die sich auf dem Desktop befinden.
6. Sichern Sie die Protokolldateien im Verzeichnis `/root`, deren Dateiname die Zeichenfolge `TDPVMware` enthält. Beispiel: `IA-TDPVMware-00.log` oder `IA-TDPVMware_Uninstall-00.log`. Entfernen Sie diese Protokolldateien, nachdem Sie sie gesichert haben. Durch das Entfernen der Dateien können Sie alle Fehler anzeigen, die ausgegeben werden, falls der Installationsprozess erneut fehlschlägt.
7. Sie können das Produkt jetzt gemäß der Beschreibung in „Data Protection for VMware auf Linux-Systemen installieren" auf Seite 26 erneut installieren.

Vorhandene Installation von Data Protection for VMware ändern

Dieser Abschnitt enthält Anweisungen zum Ändern der Pakete und Features in einer vorhandenen Data Protection for VMware-Installation.

Mit dem Installationsprogramm der Suite können Sie die zugrunde liegenden Pakete ändern, die auf dem System installiert sind. Zum Ändern der einzelnen Paketfeatures können Sie **Programme und Funktionen** in der Windows-Systemsteuerung verwenden.

Pakete in einer vorhandenen Installation von Data Protection for VMware ändern

Sie können das Installationsprogramm der Suite verwenden, um in einer vorhandenen Installation von Data Protection for VMware Änderungen an den Paketen vorzunehmen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Quellendatenträger vorliegen, bevor Sie das Installationsprogramm der Suite verwenden. Die ausführbare Datei `spinstall.exe` für das Installationsprogramm der Suite befindet sich im Stammverzeichnis des Installationspakets.

Informationen zu diesem Vorgang

Verwenden Sie das Installationsprogramm der Suite, um die installierten Pakete in einer vorhandenen Installation von Data Protection for VMware zu ändern. Sie können Folgendes hinzufügen oder entfernen:

- Einheit zum Versetzen von Daten
- Data Protection for VMware

Führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Klicken Sie doppelt auf die Datei `spinstall.exe`, um das Paket für das Installationsprogramm der Suite auszuführen.
2. Verwenden Sie die Kontrollkästchen für Pakete in der Anzeige **Angepasste Installation**, um die Pakete anzugeben, die installiert werden sollen.
3. Wählen Sie die Pakete aus, die für diese Installation erforderlich sind.

Features in einer vorhandenen Installation von Data Protection for VMware ändern

Sie können 'Programme und Funktionen' in der Windows-Systemsteuerung verwenden, um in einer vorhandenen Installation von Data Protection for VMware Änderungen an den Features vorzunehmen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Quellendatenträger vorliegen, bevor Sie das Installationspaket ändern.

Informationen zu diesem Vorgang

Verwenden Sie Windows, um die verfügbaren Paketfeatures in einer vorhandenen Installation von Data Protection for VMware zu ändern. Sie können die Features von Folgendem ändern:

- Einheit zum Versetzen von Daten
- Data Protection for VMware

Führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Im Abschnitt **Programme und Funktionen** der Windows-**Systemsteuerung** klicken Sie mit der rechten Maustaste auf die Anwendung IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
2. Klicken Sie auf **Ändern**, um die zurzeit installierten Features des Pakets zu aktualisieren.
3. Wählen Sie die Features aus, die für diese Installation erforderlich sind.

Kapitel 2. Data Protection for VMware konfigurieren

Dieser Abschnitt enthält Anweisungen zum Konfigurieren von Data Protection for VMware und zum Starten der zugehörigen Services.

Neuinstallation mit dem Assistenten konfigurieren

Verwenden Sie den Konfigurationsassistenten für die Erstkonfiguration oder für die Ausführung kleiner Änderungen.

Vorbereitende Schritte

Das System, auf dem Data Protection for VMware installiert ist, muss über Netzkonnektivität zu den folgenden Servern verfügen:

- vStorage-Sicherungsserver
- IBM Spectrum Protect-Server
- vCenter-Server

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Data Protection for VMware-Umgebung zu konfigurieren:

Vorgehensweise

1. Öffnen Sie einen Web-Browser und geben Sie die Adresse des GUI-Web-Servers ein. Beispiel:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   - In einer vSphere-Umgebung melden Sie sich mit dem vCenter-Benutzernamen und -Kennwort an.
2. Wechseln Sie im Fenster **Einführung** in das Fenster **Konfiguration** und klicken Sie auf **Konfigurationsassistenten ausführen**.
3. Befolgen Sie auf jeder Assistentenseite die Anweisungen, bis das Fenster **Zusammenfassung** angezeigt wird. Prüfen Sie die Einstellungen und klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen und den Assistenten zu beenden.

   Tipp: Informationen zu jeder Konfigurationsseite enthält die Onlinehilfe, die mit der GUI installiert wird. Klicken Sie in einem beliebigen GUI-Fenster auf **Weitere Informationen**, um die Onlinehilfe mit Informationen zur Ausführung von Tasks zu öffnen. Siehe Thema *Konfigurationsassistenten ausführen*.
4. Stellen Sie sicher, dass die Knoten der Einheit zum Versetzen von Daten korrekt konfiguriert sind:
   a. Klicken Sie auf die Registerkarte **Konfiguration**, um die Seite **Konfigurationsstatus** anzuzeigen.
   b. Wählen Sie auf der Seite **Konfigurationsstatus** einen Knoten der Einheit zum Versetzen von Daten aus, damit seine Statusinformationen im Teilfenster **Statusdetails** angezeigt werden. Wenn für einen Knoten eine Warnung oder ein Fehler angezeigt wird, klicken Sie auf diesen Knoten und beheben Sie das Problem unter Zuhilfenahme der Informationen im Teilfenster **Statusdetails**. Wählen Sie anschließend den Knoten aus und klicken Sie auf

Ausgewählten Knoten prüfen, um festzustellen, ob das Problem gelöst wurde. Klicken Sie auf **Aktualisieren**, um alle Knoten erneut zu testen.

Ergebnisse

Direktaufruf: Nachdem Sie diese Assistententask erfolgreich abgeschlossen haben, sind zum Sichern Ihrer VM-Daten keine weiteren Konfigurationstasks erforderlich.

Notizbuch zum Editieren einer vorhandenen Installation verwenden

Verwenden Sie das Notizbuch 'Konfiguration editieren', um Einstellungen für eine vorhandene Konfiguration zu editieren.

Vorbereitende Schritte

Das Notizbuch 'Konfiguration editieren' bietet die folgenden Tasks für eine vorhandene Konfiguration:

- IBM Spectrum Protect-Administrator-ID festlegen oder ändern.
- Kennwort zurücksetzen und VMCLI-Knoten entsperren.
- (vSphere-Umgebung) VMware-Datencenter in Ihrer Data Protection for VMware vSphere-GUI-Domäne hinzufügen oder entfernen.
- Mount-Proxy-Knoten hinzufügen oder entfernen. Kennwort für einen vorhandenen Mount-Proxy-Knoten ändern.
- Knoten der Einheit zum Versetzen von Daten hinzufügen oder entfernen. Kennwort für einen vorhandenen Knoten der Einheit zum Versetzen von Daten ändern.
- Dateizurückschreibung aktivieren.
- Tagging-Unterstützung für einen Knoten der Einheit zum Versetzen von Daten aktivieren.

Informationen zu diesem Vorgang

Zum Editieren einer vorhandenen Konfiguration führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Öffnen Sie einen Web-Browser und geben Sie die Adresse des GUI-Web-Servers ein. Beispiel:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   Melden Sie sich mit dem vCenter-Benutzernamen und -Kennwort an.
2. Wechseln Sie im Fenster **Einführung** in das Fenster **Konfiguration** und klicken Sie auf **Konfiguration editieren**.
3. Rufen Sie die für Ihre Editiertask relevante Seite auf und befolgen Sie die Anweisungen. Sie müssen zum Speichern Ihrer Änderungen auf **OK** klicken, bevor Sie zu einer anderen Seite unter **Konfigurationseinstellungen** wechseln. Andernfalls werden Ihre Änderungen nicht wirksam.

   Wichtig: Informationen zu jeder Konfigurationsseite enthält die Onlinehilfe, die mit der GUI installiert wird. Klicken Sie in einem beliebigen GUI-Fenster auf **Weitere Informationen**, um die Onlinehilfe mit Informationen zur Ausführung von Tasks zu öffnen. Siehe Thema *Vorhandene Konfiguration editieren*.

Ergebnisse

Die aktualisierten Einstellungen werden im Fenster **Konfiguration** angezeigt.

Umgebung für Dateizurückschreibungsoperationen aktivieren

Windows

Wenn das Feature für Dateizurückschreibung vom Administrator aktiviert wurde, können Dateieigner Dateien ohne Unterstützung zurückschreiben.

Vorbereitende Schritte

Wenn Sie noch nicht überprüft haben, ob alle Voraussetzungen erfüllt sind, lesen Sie das Thema zu Voraussetzungen für die Dateizurückschreibung im *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware Benutzerhandbuch*.

Informationen zu diesem Vorgang

Führen Sie diese Schritte auf dem System aus, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

Vorgehensweise

1. Starten Sie die Data Protection for VMware vSphere-GUI, indem Sie einen Web-Browser öffnen und die Adresse des GUI-Web-Servers eingeben. Beispiel:

   `https://<Adresse des GUI-Web-Servers>:9081/TsmVMwareUI/`

   Melden Sie sich mit der vCenter-Benutzer-ID und dem zugehörigen Kennwort an.
2. Im Fenster **Einführung** klicken Sie auf **Konfiguration** und wählen Sie eine der folgenden Tasks in der Liste **Tasks** aus:
   - Wenn Sie eine neue Umgebung konfigurieren, führen Sie die folgenden Schritte aus:
     a. Wählen Sie **Clientkonfigurationsassistenten ausführen** aus.
     b. Befolgen Sie die Anweisungen auf jeder Seite des Assistenten. Verwenden Sie die folgenden Anleitungen beim Ausfüllen der Seite **Dateizurückschreibung**:
        1) Wählen Sie die Option **Dateizurückschreibung aktivieren** aus.
        2) Geben Sie die Kontaktinformationen für den Administrator ein, die in der Schnittstelle für Dateizurückschreibung angezeigt werden. Wenn Sie keine Kontaktinformationen zur Verfügung stellen möchten, inaktivieren Sie das Kontrollkästchen.
        3) Wenn die Umgebung Sicherungen virtueller Windows-Maschinen enthält, geben Sie die Berechtigungsnachweise des Windows-Domänenadministrators ein. Andernfalls wählen Sie das Kontrollkästchen ab und geben keine Berechtigungsnachweise ein.

           Tipp: Bei einer Dateizurückschreibungsoperation werden die Berechtigungsnachweise des Domänenadministrators verwendet, um auf Netzfreigaben auf der fernen virtuellen Maschine zuzugreifen. Eine Operation schlägt fehl, wenn die Umgebung Sicherungen virtueller Windows-Maschinen enthält und keine oder die falschen Berechti-

gungsnachweise eingegeben werden. Wählen Sie dieses Kontrollkästchen daher nur ab, wenn keine Sicherungen virtueller Windows-Maschinen vorhanden sind.

4) Klicken Sie auf die URL der Schnittstelle für Dateizurückschreibung, um zu überprüfen, ob die Schnittstelle zugänglich ist.

   Hinweis: Notieren Sie sich die URL der Schnittstelle für Dateizurückschreibung. Der Eigner der virtuellen Gastmaschine greift über diese URL auf die Schnittstelle für Dateizurückschreibung zu.

5) Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

- Wenn Sie eine vorhandene Umgebung aktualisieren, führen Sie die folgenden Schritte aus:
  a. Wählen Sie **TSM-Konfiguration editieren** aus.
  b. Verwenden Sie die folgenden Anleitungen für die Seite **Dateizurückschreibung**:
     1) Wählen Sie die Option **Dateizurückschreibung aktivieren** aus.
     2) Geben Sie die Kontaktinformationen für den Administrator ein, die in der Schnittstelle für Dateizurückschreibung angezeigt werden. Wenn Sie keine Kontaktinformationen zur Verfügung stellen möchten, inaktivieren Sie das Kontrollkästchen.
     3) Wenn die Umgebung Sicherungen virtueller Windows-Maschinen enthält, geben Sie die Berechtigungsnachweise des Windows-Domänenadministrators ein. Andernfalls wählen Sie das Kontrollkästchen ab und geben keine Berechtigungsnachweise ein.

        Tipp: Bei einer Dateizurückschreibungsoperation werden die Berechtigungsnachweise des Domänenadministrators verwendet, um auf Netzfreigaben auf der fernen virtuellen Maschine zuzugreifen. Eine Operation schlägt fehl, wenn die Umgebung Sicherungen virtueller Windows-Maschinen enthält und keine oder die falschen Berechtigungsnachweise eingegeben werden. Wählen Sie dieses Kontrollkästchen daher nur ab, wenn keine Sicherungen virtueller Windows-Maschinen vorhanden sind.

     4) Klicken Sie auf die URL der Schnittstelle für Dateizurückschreibung, um zu überprüfen, ob die Schnittstelle zugänglich ist.

        Hinweis: Notieren Sie sich die URL der Schnittstelle für Dateizurückschreibung. Der Eigner der virtuellen Gastmaschine greift über diese URL auf die Schnittstelle für Dateizurückschreibung zu.

     5) Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ergebnisse

Die Umgebung ist für Dateizurückschreibungsoperationen aktiviert. Dateieigner können ihre Dateien zurückschreiben, indem Sie mit der URL auf die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zugreifen.

Dateizurückschreibungsoperationen unter Linux einrichten

Linux

Soll das Feature für Dateizurückschreibung aktiviert werden, wenn Data Protection for VMware auf einem Linux-System installiert ist, muss eine zusätzliche Data Protection for VMware-Umgebung auf einem Windows-System eingerichtet werden.

Informationen zu diesem Vorgang

Wenn Sie Data Protection for VMware in einer Linux-Umgebung ausführen, muss das Feature für Dateizurückschreibung auf einem Windows-System installiert werden, um das Feature für Dateizurückschreibung zu aktivieren.

Vorgehensweise

1. Richten Sie einen separaten Windows-Server ein, der für das Feature für Dateizurückschreibung verwendet wird.
2. Installieren Sie Data Protection for VMware auf dem Windows-System. Akzeptieren Sie während der Installation die Standardwerte.
3. Verwenden Sie die folgenden Knotennamen, wenn Sie Data Protection for VMware auf dem Windows-System konfigurieren:
   a. Erstellen Sie einen vCenter-Knoten mit dem Namen `VCENTER_FR`.
   b. Erstellen Sie einen VMCLI-Knoten mit dem Namen `VMCLI_FR`.
   c. Verwenden Sie den Namen des Datencenterknotens aus der Linux-Umgebung wieder.
      Beispiel: `DATACENTER`.
   d. Erstellen Sie keinen Knoten der Einheit zum Versetzen von Daten. Ein Knoten der Einheit zum Versetzen von Daten ist für das Feature für Dateizurückschreibung in diesem Szenario nicht erforderlich.
   e. Erstellen Sie das folgende neue Paar von Mount-Proxy-Knoten mit den Namen `REMOTE_FR_MP_WIN` und `REMOTE_FR_MP_LNX`.
4. Auf der Seite **Dateizurückschreibung** im Konfigurationsassistenten wählen Sie die Option `Dateizurückschreibung aktivieren` aus.
5. Für den Zugriff auf die Schnittstelle für Dateizurückschreibung öffnen Sie einen Web-Browser und geben Sie die URL ein, die Ihr Administrator zur Verfügung gestellt hat. Beispiel:

   ```
   https:\\Hostname:9081\FileRestoreUI
   ```

   Dabei ist `Hostname` der Hostname des Windows-Systems, auf dem Data Protection for VMware installiert ist.

Ergebnisse

Das folgende Beispiel zeigt die Proxy-Knotenbeziehungen auf dem IBM Spectrum Protect-Server:

```
tsm: SERVER>q proxy

Zielknoten          Agentenknoten
---------------     --------------------------------------------
VCENTER             VMCLI DATACENTER
VCENTER_FR          VMCLI_FR DATACENTER
DATACENTER          VMCLI VMCLI_FR
                     DATAMOVER1
                     REMOTE_MP_WIN REMOTE_MP_LNX
                     REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

Die zusätzlichen Knoten, die zur Aktivierung des Features für Dateizurückschreibung erstellt werden, haben das Suffix _FR.

Optionen für Dateizurückschreibungsoperationen ändern

Windows

Wenn Sie es Administratoren ermöglichen möchten, die Zurückschreibungsverarbeitung für Dateizurückschreibungsoperationen zu konfigurieren und zu steuern, ändern Sie die Optionen in der Datei frConfig.props.

Informationen zu diesem Vorgang

Führen Sie diese Schritte auf dem System aus, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis, in dem die Datei frConfig.props sich befindet. Öffnen Sie beispielsweise eine Eingabeaufforderung und geben Sie den folgenden Befehl aus:

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
   ```

2. Öffnen Sie die Datei frConfig.props mit einem Texteditor im Administratormodus und ändern Sie die Optionen nach Bedarf. Anhand der Informationen in „Optionen für die Dateizurückschreibung" können Sie feststellen, welche Optionen geändert werden müssen.
3. Speichern Sie Ihre Änderungen und schließen Sie die Datei frConfig.props.

Ergebnisse

Die geänderten Optionen werden auf die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung angewendet.

Optionen für die Dateizurückschreibung

Die frConfig.props-Optionen steuern die Konfiguration, Unterstützung und Zurückschreibungsverarbeitung für Dateizurückschreibungsoperationen.

enable_contact_info=false | true
Geben Sie an, ob Kontaktinformationen für den Administrator zur Verfügung gestellt werden, mit deren Hilfe die Dateieigner Unterstützung anfordern können.

false
Die Dateieigner erhalten keine Kontaktinformationen für den Administrator. Dieser Wert ist der Standardwert.

true
Die Dateieigner erhalten Kontaktinformationen für den Administrator.

Wenn Sie **enable_contact_info=true** angeben, müssen Sie Informationen für die Option **contact_info** angeben.

enable_filerestore=false | true
Geben Sie an, ob die Dateieigner ihre Dateien aus einer virtuellen Maschine mit der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zurückschreiben können.

false
Die Dateieigner können ihre Dateien nicht mit der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zurückschreiben. Dieser Wert ist der Standardwert.

true
Die Dateieigner können ihre Dateien mit der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zurückschreiben.

maximum_mount_points=*Anzahl_Mountpunkte*
Geben Sie die maximale Anzahl der simultanen Wiederherstellungspunkte an, die für das Benutzerkonto verfügbar sind. Der Mindestwert ist 1 Wiederherstellungspunkt. Der Maximalwert ist 256 Mountpunkte. Der Standardwert ist 2 Mountpunkte.

Tipp: Wenn Sie verhindern möchten, dass eine virtuelle Maschine für simultane Zurückschreibungsoperationen mehrfach bereitgestellt wird, setzen Sie diese Option auf einen niedrigen Wert.

mount_session_timeout_minutes=*Anz_Min*
Geben Sie die Zeit in Minuten an, während der eine Zurückschreibung und der bereitgestellte Wiederherstellungspunkt inaktiv sein können, bevor die Sitzung abgebrochen wird. Bei einem Abbruch wird die Bereitstellung des Wiederherstellungspunkts aufgehoben. Der Maximalwert ist 8 Stunden (480 Minuten). Der Standardwert ist 30 Minuten.

Tipp: Wenn Sie verhindern möchten, dass die Sitzung unerwartet abgebrochen wird, erhöhen Sie die Anzahl der Minuten.

restore_info_duration_hours=*Anz_Std*
Geben Sie die Zeit in Stunden an, während der Informationen zu kürzlich ausgeführten Zurückschreibungsaktivitäten in der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung aufbewahrt wird. Verwenden Sie das Fenster für Zurückschreibungsaktivitäten, um Informationen zu Fehlern und vor Kurzem abgeschlossenen Tasks anzuzeigen. Diese Informationen helfen Ihnen bei der Lokalisierung von Dateien, die vor Kurzem zurückgeschrieben wurden. Der Maximalwert ist 14 Tage (336 Stunden). Der Standardwert ist eine Woche (168 Stunden).

contact_info=*Administratorinformationen*
Stellen Sie Kontaktinformationen für den Administrator zur Verfügung, mit deren Hilfe die Dateieigner Unterstützung anfordern können. Die Kontaktinformationen werden in der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung an den folgenden Positionen angezeigt:

- Anmeldefenster
- Teilfenster **Produktinformation** im Hilfemenü
- Link zu Unterstützungsinformationen in den Schnittstellennachrichten

Sie können die folgenden Optionen mit dem Konfigurationsassistenten oder Notizbuch der Data Protection for VMware vSphere-GUI überschreiben:

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

Protokollaktivität für Dateizurückschreibungsoperationen konfigurieren

Wenn Sie es Administratoren ermöglichen möchten, die Formatierung und Protokollierung des Inhalts für Dateizurückschreibungsoperationen zu konfigurieren und zu steuern, ändern Sie die Optionen in der Datei `FRLog.config`.

Vorbereitende Schritte

Die Datei `FRLog.config` wird beim ersten Zugriff auf die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung generiert.

Informationen zu diesem Vorgang

Führen Sie diese Schritte auf dem System aus, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis, in dem die Datei `FRLog.config` sich befindet. Öffnen Sie eine Eingabeaufforderung und geben Sie den folgenden Befehl aus:
   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
   ```
2. Öffnen Sie die Datei `FRLog.config` mit einem Texteditor im Administratormodus und ändern Sie die Optionen nach Bedarf. Anhand der Informationen in „Optionen für die Protokollaktivität bei der Dateizurückschreibung" können Sie feststellen, welche Optionen geändert werden müssen.
3. Speichern Sie Ihre Änderungen und schließen Sie die Datei `FRLog.config`.
4. Starten Sie den GUI-Web-Server erneut:
   a. Klicken Sie auf **Start** > **Systemsteuerung** > **Verwaltung** > **Dienste**.
   b. Klicken Sie mit der rechten Maustaste auf **Data Protection for VMware-Web-Server-Service** und klicken Sie auf **Neu starten**.

Ergebnisse

Die Einstellungen werden auf den Inhalt und die Formatierung der Protokollierungsinformationen für Dateizurückschreibungsoperationen angewendet.

Optionen für die Protokollaktivität bei der Dateizurückschreibung

Die `FRLog.config`-Optionen steuern den Inhalt und das Format der Protokollierungsinformationen bei Dateizurückschreibungsoperationen.

Mit den folgenden Optionen werden Informationen zu Dateizurückschreibungstasks in der Datei `fr_gui.log` protokolliert:

MAX_LOG_FILES=*Anzahl*
Geben Sie die maximale Anzahl der `fr_gui.log`-Dateien an, die aufbewahrt werden sollen. Der Standardwert ist 8.

MAX_LOG_FILE_SIZE=*Anzahl*
Geben Sie die maximale Größe der Datei `fr_gui.log` in KB an. Der Standardwert ist 8192 KB.

Mit den folgenden Optionen werden Informationen zu Dateizurückschreibungsservices in der Datei `fr_api.log` protokolliert. Diese Services sind interne API-Services, die zur Dateizurückschreibungsaktivität gehören:

API_MAX_LOG_FILES=*Anzahl*
Geben Sie die maximale Anzahl der `fr_api.log`-Dateien an, die aufbewahrt werden sollen. Der Standardwert ist 8.

API_MAX_LOG_FILE_SIZE=*Anzahl*
Geben Sie die maximale Größe der Datei `fr_api.log` in KB an. Der Standardwert ist 8192 KB.

API_LOG_FILE_NAME=*Name_der_API-Protokolldatei*
Geben Sie den Namen der API-Protokolldatei an. Der Standardwert ist `fr_api.log`.

API_LOG_FILE_LOCATION=*Position_der_API-Protokolldatei*
Geben Sie die Position der API-Protokolldatei an. Die Position muss mit einem Schrägstrich (/) angegeben werden. Die Standardposition ist `C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs`.

FR.API.LOG=ON | OFF
Geben Sie an, ob die Protokollierung für Dateizurückschreibungsservices aktiviert werden soll.

- Um die Protokollierung für Dateizurückschreibungsservices zu aktivieren, geben Sie ON an. Der Standardwert ist ON.
- Um die Protokollierung für Dateizurückschreibungsservices zu inaktivieren, geben Sie OFF an.

Informationen zur Behebung von Fehlern, die möglicherweise bei Dateizurückschreibungsoperationen auftreten, finden Sie in Traceoptionen für die Dateizurückschreibung. Traceoptionen sind auch in der Datei `FRLog.config` angegeben.

Knoten der Einheit zum Versetzen von Daten für Tagging-Unterstützung konfigurieren

Wenn Tagging-Unterstützung auf einem Knoten der Einheit zum Versetzen von Daten aktiviert ist, können Administratoren Datenschutztags auf Bestandsobjekte im VMware vCenter anwenden.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der VMware vCenter-Server muss Version 6.0 Update 1 oder höher aufweisen.
- Damit die Data Protection for VMware vSphere-GUI mit der Tagging-Unterstützung korrekt funktioniert, müssen Sie sicherstellen, dass die folgenden Voraussetzungen während der Installation der GUI erfüllt sind:
  - Mindestens eine Einheit zum Versetzen von Daten und die Data Protection for VMware vSphere-GUI müssen auf demselben Server installiert sein. Dieser Knoten der Einheit zum Versetzen von Daten muss so konfiguriert sein, dass die Berechtigungsnachweise des vCenter-Servers gespeichert werden. Sie können die Berechtigungsnachweise speichern, indem der Konfigurationsassistent zum Speichern des Kennworts für den Knoten der Einheit zum Versetzen von Daten ausgeführt wird oder indem der Befehl **dsmc set password** in der Befehlszeile der Einheit zum Versetzen von Daten verwendet wird.

    Wenn Sie andere Einheiten zum Versetzen von Daten verwenden, die auf virtuellen Maschinen oder physischen Maschinen als zusätzliche Einheiten zum Versetzen von Daten ausgeführt werden, können Sie diese auf anderen Servern installieren. Für die Tagging-Unterstützung müssen alle diese Einheiten zum Versetzen von Daten ebenfalls mit der Option `VMTAGDATAMOVER YES` konfi-

guriert sein. Für diese zusätzlichen Einheiten zum Versetzen von Daten ist es nicht erforderlich, dass die Data Protection for VMware vSphere-GUI auf demselben Server installiert ist, damit sie als tagbasierte Einheiten zum Versetzen von Daten ordnungsgemäß funktionieren.

– Linux Stellen Sie für Linux-Einheiten zum Versetzen von Daten sicher, dass Sie das Installationsverzeichnis der Einheit zum Versetzen von Daten und die gemeinsam genutzte Java™-Bibliothek `libjvm.so` in der Umgebungsvariablen `LD_LIBRARY_PATH` angeben. Der Pfad zu `libjvm.so` wird für die Tagging-Unterstützung verwendet, wenn Sie die Option `vmtagdatamover` auf der Einheit zum Versetzen von Daten aktivieren. Anweisungen dazu finden Sie in Knoten der Einheit zum Versetzen von Daten in einer vSphere-Umgebung definieren.

– Linux Unter Linux-Betriebssystemen muss die Data Protection for VMware vSphere-GUI unter Verwendung des Standardbenutzernamens (`tdpvmware`) installiert werden.

– Auf UNIX- und Linux-Clients werden die vorhandenen Kennwörter in den Dateien `TSM.PWD` in den neuen Kennwortspeicher an derselben Position migriert. Für Rootbenutzer ist `/etc/adsm` die Standardposition für den Kennwortspeicher. Für Benutzer ohne Rootberechtigung wird die Position des Kennwortspeichers durch die Option `passworddir` angegeben.

  Die Datei `TSM.PWD` wird nach der Migration gelöscht.

Anmerkung: Weitere Informationen zur Verwendung der Berechtigungen, die zum Arbeiten mit Tagging erforderlich sind, finden Sie in Data Protection for VMware-Komponenten installieren.

Informationen zu diesem Vorgang

Sie können Datenschutztags verwenden, um die Sicherungsmaßnahme für virtuelle Maschinen in VMware-Bestandsobjekten zu konfigurieren. Diese Datenschutztags werden als Einstellungen dargestellt, die im IBM Spectrum Protect vSphere-Client-Plug-in geändert werden können.

Vorgehensweise

Verwenden Sie eine der folgenden Methoden:

Option	Bezeichnung
Gehen Sie zum Konfigurieren eines Knotens der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI wie folgt vor:	1. Im vSphere-Plug-in wählen Sie IBM Spectrum Protect aus. 2. Auf der Registerkarte **Konfigurieren** wählen Sie **Einheiten zum Versetzen von Daten** aus. 3. In der Anzeige **Einheit zum Versetzen von Daten hinzufügen** wählen Sie im Dropdown-Menü ein Datencenter aus. 4. Akzeptieren Sie die Standardwerte oder editieren Sie die Einstellungen für **Name der Einheit zum Versetzen von Daten**, **Hostname der Einheit zum Versetzen von Daten**, **vCenter-Benutzer** und **vCenter-Kennwort**. 5. Klicken Sie auf **Hinzufügen**, wenn die Einstellungen fertig sind. Weitere Informationen finden Sie im Thema "Knoten der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI definieren" im Installationshandbuch für die Data Protection for VMware vSphere-GUI.

Option	Bezeichnung
Eine *neue* Einheit zum Versetzen von Daten unter Windows oder Linux mit der Data Protection for VMware vSphere-GUI für Tagging-Unterstützung konfigurieren	1. Auf dem System, auf dem die Data Protection for VMware vSphere-GUI installiert ist, starten Sie die GUI, indem Sie einen Web-Browser öffnen und die Adresse des GUI-Web-Servers eingeben. Beispiel: `https://<Adresse des GUI-Web-Servers>:9081/TsmVMwareUI/` 2. Melden Sie sich mit der vCenter-Benutzer-ID und dem zugehörigen Kennwort an. 3. Rufen Sie die Registerkarte **Konfiguration** auf und wählen Sie die Aktion **IBM Spectrum Protect-Konfiguration editieren** aus. 4. Rufen Sie die Seite **Knoten der Einheit zum Versetzen von Daten** des Konfigurationsnotizbuchs auf. 5. Führen Sie die folgenden Schritte aus, um einen Knoten der Einheit zum Versetzen von Daten hinzuzufügen: a. Für den Knoten der Einheit zum Versetzen von Daten, für den Sie Tagging-Unterstützung einrichten möchten, wählen Sie **Services erstellen** aus. Standardmäßig ist **Tagbasierter Knoten** ausgewählt, um den Knoten der Einheit zum Versetzen von Daten für Tagging-Unterstützung zu aktivieren. b. Zum Festlegen des tagbasierten Knotens als standardmäßigen Knoten der Einheit zum Versetzen von Daten wählen Sie **Standardmäßige Einheit zum Versetzen von Daten** aus. Ein standardmäßiger Knoten der Einheit zum Versetzen von Daten sichert alle neuen VMs, die einem Container im Datencenter hinzugefügt werden, wenn der Container sich bereits in einer Schutzgruppe befindet. Die standardmäßige Einheit zum Versetzen von Daten sichert außerdem alle VMs in der Schutzgruppe, denen der Tag `Data Mover` nicht zugeordnet wurde. **Tipp:** Für Linux-Systeme: Wenn Sie einen neuen Knoten der Einheit zum Versetzen von Daten als standardmäßigen Tagging-Knoten auswählen, entfernen Sie die Zeile `vmtagdefaultdatamover` aus den Optionsdateien aller anderen Einheiten zum Versetzen von Daten, die diesem Datencenter zugeordnet sind. c. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern. Die Optionen `vmtagdatamover` und `vmtagdefaultdatamover` (falls definiert) werden der Optionsdatei der Einheit zum Versetzen von Daten (`dsm.opt`) hinzugefügt.

Option	Bezeichnung
Einen *vorhandenen* Windows-Knoten der Einheit zum Versetzen von Daten für Tagging-Unterstützung konfigurieren, wenn der Knoten sich auf demselben Server wie die Data Protection for VMware vSphere-GUI befindet	1. Führen Sie die Schritte 1-3 in den vorhergehenden Anweisungen aus, um einen neuen Knoten der Einheit zum Versetzen von Daten für Tagging-Unterstützung zu konfigurieren. 2. Wählen Sie auf der Seite **Knoten der Einheit zum Versetzen von Daten** das Feld **Tagbasierter Knoten** für den Knoten aus, für den Sie Tagging-Unterstützung aktivieren möchten. 3. **Optional:** Zum Festlegen des tagbasierten Knotens als standardmäßigen Knoten der Einheit zum Versetzen von Daten wählen Sie **Standardmäßige Einheit zum Versetzen von Daten** aus.
Einen *vorhandenen* Linux-Knoten der Einheit zum Versetzen von Daten oder einen vorhandenen Windows-Knoten der Einheit zum Versetzen von Daten, der sich auf einem anderen Server als die Data Protection for VMware vSphere-GUI befindet, für Tagging-Unterstützung konfigurieren	1. Fügen Sie die Option `vmtagdatamover yes` in der Optionsdatei der Einheit zum Versetzen von Daten (`dsm.sys` für Linux und `dsm.opt` für Windows) hinzu. 2. **Optional:** Zum Festlegen des tagbasierten Knotens als standardmäßigen Knoten der Einheit zum Versetzen von Daten fügen Sie die Option `vmtagdefaultdatamover yes` oder `vmtagdefaultdatamover` *Name_der_Einheit_zum_Versetzen_von_Daten* der Optionsdatei der Einheit zum Versetzen von Daten hinzu. **Tipp:** Für Linux-Systeme: Wenn Sie einen neuen Knoten der Einheit zum Versetzen von Daten als standardmäßigen Tagging-Knoten auswählen, entfernen Sie die Zeile `vmtagdefaultdatamover` aus den Optionsdateien aller anderen Einheiten zum Versetzen von Daten, die diesem Datencenter zugeordnet sind.

Ergebnisse

Nachdem der Knoten der Einheit zum Versetzen von Daten für Tagging-Unterstützung aktiviert wurde, fragt die Einheit zum Versetzen von Daten den VMware-Bestand nach Tagging-Informationen ab, wenn sie eine Sicherung ausführt. Anschließend sichert die Einheit zum Versetzen von Daten die virtuellen Maschinen entsprechend den definierten Datenschutztags. Ist der Knoten der Einheit zum Versetzen von Daten nicht für Tagging-Unterstützung konfiguriert, werden alle Datenschutztags während einer Sicherungsoperation ignoriert.

Zugehörige Informationen:

- `Vmtagdatamover`
- `Vmtagdefaultdatamover`
- Sicherungsmaßnahmen konfigurieren

Umgebung für Instant Restore-Operationen vollständiger virtueller Maschinen konfigurieren

Richten Sie ein dediziertes iSCSI-Netz für Instant Restore- und Instant Access-Operationen vollständiger virtueller Maschinen ein.

Vorbereitende Schritte

Der entsprechenden VMware-Dokumentation (ESXi oder vSphere) können Sie die genauen Schritte entnehmen, die bei der iSCSI-Konfiguration des virtuellen Switch und des VM-Netzes auszuführen sind. Zwar werden allgemeine Richtlinien zur Verfügung gestellt; eine genaue Dokumentation und Erläuterungen zum Hinzufügen von virtuellen Netzen und virtuellen Switches gehen jedoch über den Rahmen der Produktdokumentation hinaus. Zum Zeitpunkt der Veröffentlichung dieses Textes war die Dokumentation zu VMware vSphere ESXi und vCenter 5.5 unter Dokumentation zu VMware vSphere ESXi und vCenter Server 5 verfügbar. Die Themen zum Netzbetrieb enthalten Informationen zum Hinzufügen und Konfigurieren von virtuellen Switches und virtuellen Netzen.

Wichtig: Diese Konfigurationseinstellungen werden bereitgestellt, um Ihnen bei der Einrichtung der VMware-Umgebung für effiziente Instant Restore- und Instant Access-Operationen vollständiger virtueller Maschinen zu helfen. Da diese Einstellungen sich jedoch auf VMware-Konfigurationstasks und VMware-Benutzerschnittstellen beziehen, müssen Sie ausführliche schrittweise Anleitungen der entsprechenden VMware-Dokumentation entnehmen.

Informationen zu diesem Vorgang

Für diese Prozedur ist ein iSCSI-Adapter auf jedem ESXi-Host erforderlich, der für Instant Restore-Operationen verwendet wird. Verwenden Sie die entsprechende VMware-Dokumentation, um den Adapter einzurichten. Zum Zeitpunkt der Veröffentlichung dieses Textes waren die folgenden Prozeduren unter dieser VMware vSphere-Ressource verfügbar.

- Zum Einrichten eines Software-iSCSI-Adapters befolgen Sie die Anweisungen in der VMware-Prozedur zum Konfigurieren von Software-iSCSI-Adaptern.
- Zum Einrichten eines Hardware-iSCSI-Adapters befolgen Sie die Anweisungen in der VMware-Prozedur zum Einrichten unabhängiger Hardware-iSCSI-Adapter.

1. iSCSI-Software auf dem ESXi-Host konfigurieren

Vorgehensweise

Mit dieser Task wird die iSCSI-Software für eine Basiskonfiguration eingerichtet.

1. Melden Sie sich bei dem ESXi-Host an, der für Instant Restore-Operationen verwendet werden soll.
2. Befolgen Sie die Anweisungen in dem folgenden Artikel in der VMware-Knowledge Base, bis der iSCSI-Adapter aktiviert ist: http://kb.vmware.com/kb/1008083
   IBM Spectrum Protect erkennt den iSCSI-Zielserver automatisch.
3. Prüfen Sie, ob die IP-Adresse des iSCSI-Adapters (auf dem ESXi-Host) dieselbe Teilnetzadresse aufweist wie die Einheit zum Versetzen von Daten.
4. Prüfen Sie, ob die Storage vMotion-Lizenz auf dem ESXi-Host aktiviert ist.

Nächste Schritte

Nachdem die iSCSI-Software auf dem ESXi-Host eingerichtet ist, installieren und konfigurieren Sie Anwendungen auf dem System der Einheit zum Versetzen von Daten.

2. Anwendungen auf der Einheit zum Versetzen von Daten installieren und konfigurieren

Vorbereitende Schritte

Sind Recovery Agent und die IBM Spectrum Protect-Einheit zum Versetzen von Daten auf dem System der Einheit zum Versetzen von Daten bereits installiert und konfiguriert, beginnen Sie mit Schritt 3.

Vorgehensweise

Mit dieser Task werden die Anwendungen und Einstellungen für Instant Restore-Operationen auf dem System der Einheit zum Versetzen von Daten eingerichtet.

1. Installieren Sie Recovery Agent und die IBM Spectrum Protect-Einheit zum Versetzen von Daten auf dem System der Einheit zum Versetzen von Daten.
   In Schritt 4 der Prozedur Data Protection for VMware installieren wählen Sie den Installationstyp **Vollständige Einheit zum Versetzen von Daten für den In-Guest-Anwendungsschutz installieren** aus.
2. Konfigurieren Sie die Einheit zum Versetzen von Daten.
   Befolgen Sie die Anweisungen im Thema zum Konfigurieren der Einheit zum Versetzen von Daten in der Client-Dokumentation.
3. Definieren Sie die IP-Adresse des iSCSI-Servers:
   a. Rufen Sie die Datei `C:\Programme\Tivoli\TSM\baclient\dsm.opt` auf und geben Sie den folgenden Parameter an:

      ```
      VMISCSIServeraddress=<IP-Adresse der Netzkarte auf dem System der Einheit zum
      Versetzen von Daten, das die iSCSI-Ziele verfügbar macht>
      ```

      Wenn Ihr System der Einheit zum Versetzen von Daten über mehrere Netzkarten verfügt, müssen Sie sicherzustellen, dass Sie die korrekte Netzkarte für das iSCSI-Netz angeben.

Nächste Schritte

Nachdem das System der Einheit zum Versetzen von Daten eingerichtet ist, stellen Sie eine Verbindung zwischen der Recovery Agent-CLI und der Recovery Agent-GUI her.

3. Recovery Agent-Verbindung definieren

Vorbereitende Schritte

Die Befehlszeilenschnittstelle (CLI) von Recovery Agent Version 7.1.x kann als Befehlszeilen-API für die grafische Benutzerschnittstelle (GUI) von Recovery Agent angesehen werden. Sie können die Recovery Agent-CLI für die Kommunikation mit der Recovery Agent-GUI verwenden.

Vorgehensweise

Mit dieser Task wird eine Verbindung zwischen der Recovery Agent-CLI und der Recovery Agent-GUI hergestellt.

1. Starten Sie die Recovery Agent-CLI auf dem System der Einheit zum Versetzen von Daten.
   Klicken Sie im Windows-Menü **Start** auf **Programme** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**.
2. In dem Fenster mit Eingabeaufforderung geben Sie den folgenden Befehl ein:

   ```
   RecoveryAgentShell.exe -c set_connection mount_computer <IP-Adresse
   der Netzkarte auf dem System der Einheit zum Versetzen von Daten, das die iSCSI-Ziele verfügbar m
   ```

   Mit diesem Befehl wird eine Verbindung zwischen der Recovery Agent-CLI und der Recovery Agent-GUI hergestellt.

Nächste Schritte

Nachdem Sie eine Verbindung hergestellt haben, konfigurieren Sie ein dediziertes iSCSI-Netz.

4. Dediziertes iSCSI-Netz für den ESXi-Host und die Einheit zum Versetzen von Daten konfigurieren

Vorbereitende Schritte

Lesen Sie die folgenden Richtlinien, bevor Sie diese Task fortsetzen:

- Verwenden Sie ein dediziertes iSCSI-Netz für Instant Restore-Operationen.
- Für jeden ESXi-Host, der für Instant Restore-Operationen verwendet wird, muss eine zweite physische Netzkarte verfügbar sein. Diese zweite Netzkarte wird an den Software-iSCSI-Adapter des jeweiligen ESXi-Hosts gebunden.
- Für das System der Einheit zum Versetzen von Daten, das in einer virtuellen Maschine ausgeführt wird, muss eine zweite Netzkarte verfügbar sein. Diese zweite Netzkarte wird an den Software-iSCSI-Adapter des ESXi-Hosts gebunden.
- Für jeden ESXi-Host, der für Instant Restore-Operationen verwendet wird, muss ein sekundärer VMware-Datenspeicher verfügbar sein. Dieser temporäre Datenspeicher enthält die Konfigurationsinformationen und die Daten der virtuellen Maschine, die während der Operation erstellt wird.

Vorgehensweise

Mit dieser Task wird ein dediziertes iSCSI-Netz für den ESXi-Host und für die Einheit zum Versetzen von Daten eingerichtet, die in einer virtuellen Maschine ausgeführt wird.

1. Melden Sie sich bei dem ESXi-Host an, der für Instant Restore-Operationen verwendet werden soll.
2. Richten Sie den virtuellen Switch für das iSCSI-Netz ein.
   Bei diesen Schritten wird *vSwitch1* als virtueller Switch verwendet.
   a. Wählen Sie **VMkernel Network Adapter** (VMkernel-Netzadapter) als **Connection Type** (Verbindungstyp) aus.
      Für das iSCSI-Netz ist dieser Verbindungstyp erforderlich.
   b. Wählen Sie **Create a vSphere standard switch** (vSphere-Standardswitch erstellen) bei **VMkernel Network Access** (VMkernel-Netzzugriff) aus.
   c. Wählen Sie **Network Label** (Netzbezeichnung) bei **VMkernel Connection Settings** (VMkernel-Verbindungseinstellungen) aus.
      Geben Sie eine Bezeichnung an, aus der hervorgeht, dass *vSwitch1* und dieses Netz für den iSCSI-Datenverkehr vorgesehen sind.
      Beispiel: *VMkernel iSCSI*.

d. Geben Sie eine IP-Adresse und eine Teilnetzmaske für *vSwitch1* bei **VMkernel IP Connection Settings** (Einstellungen für VMkernel-IP-Verbindung) an. Ändern Sie nicht die Werte für **Subnet Mask (Teilnetzmaske)** oder **VMkernel Default Gateway (VMkernel-Standardgateway)**.

e. Geben Sie den Kernel-Port für den Betrieb des iSCSI-Netzes an.

3. Richten Sie den virtuellen Switch für das VM-Netz ein.
   Bei diesen Schritten wird *vSwitch0* als virtueller Switch verwendet.
   a. Wählen Sie **Virtual Machine** (Virtuelle Maschine) als **Connection Type** (Verbindungstyp) aus.
   b. Wählen Sie **Create a vSphere standard switch** (vSphere-Standardswitch erstellen) bei **VMkernel Network Access** (VMkernel-Netzzugriff) aus.
   c. Rufen Sie die Registerkarte **Port Group Properties** (Portgruppeneigenschaften) auf und wählen Sie **Network Label** (Netzbezeichnung) aus.
      Geben Sie die Bezeichnung an, die Sie auch für das VM-Netz *vSwitch1* angegeben haben.
      Beispiel: *VMkernel iSCSI*.
4. Binden Sie den neu erstellten iSCSI-Adapter an den **VMkernel Network Adapter** (VMkernel-Netzadapter).
   Befolgen Sie die Anweisungen in der VMware-Prozedur zum Binden von iSCSI-Adaptern an VMkernel-Adapter. Zum Zeitpunkt der Veröffentlichung dieses Textes war diese Prozedur unter Dokumentation zu VMware vSphere ESXi und vCenter Server 5 verfügbar.

   Tipp: Wenn beim Scannen der iSCSI-Einheiten eine Zeitlimitüberschreitung auftritt, reduzieren Sie die Anzahl der iSCSI-Einheiten, die mit dem ESXi-Host verbunden sind. Scannen Sie die iSCSI-Einheiten anschließend erneut.
5. Überprüfen Sie, ob die Bindungseigenschaften für den iSCSI-Adapter korrekt sind.
   a. Rufen Sie im VMware vSphere-Client **Hardware** > **Storage Adapters (Speicheradapter)** auf.
   b. Klicken Sie mit der rechten Maustaste auf den iSCSI-Adapter und wählen Sie **iSCSI Initiator Properties** (iSCSI-Initiatoreigenschaften) aus. Stellen Sie sicher, dass die folgenden Bindungseigenschaften vorhanden sind:

Tabelle 10. iSCSI-Netzeinstellungen

VM-Netz	iSCSI-Netz
Standard Switch (Standardswitch): *vSwitch0*	**Standard Switch** (Standardswitch): *vSwitch1*
Virtual Machine Port Group (VM-Portgruppe): *VM-Netz*	**VMkernel Port** (VMkernel-Port): *VMkernel iSCSI* **Tipp:** *VMkernel iSCSI* ist an den **VMkernel Adapter** (VMkernel-Adapter) *vmk1* gebunden, der sich auf **Physical Network Adapter** (Physischer Netzadapter) *vmnic1* befindet.
Physical Adapter (Physischer Adapter): *vmnic0*	**VMkernel Network Adapter** (VMkernel-Netzadapter): *vmk1*
	Physical Network Adapter (Physischer Netzadapter): *vmnic1*
	IP address (IP-Adresse) des virtuellen Netzadapters: 192.168.42.x (Teilnetz für das iSCSI-Netz)

Ergebnisse

Ein dediziertes iSCSI-Netz steht für Instant Restore- und Instant Access-Operationen vollständiger VMs bereit.

Sicherheitseinstellungen für Data Protection for VMware konfigurieren

Die Data Protection for VMware-Einheiten zum Versetzen von Daten sowie die Komponenten vmcli-Befehlszeilenschnittstelle und Data Protection for VMware vSphere-GUI müssen für die sichere Verbindung zum IBM Spectrum Protect-Server konfiguriert werden.

Sicherheitseinstellungen für die Verbindung von Knoten der Einheit zum Versetzen von Daten und VMCLI-Knoten mit dem IBM Spectrum Protect-Server konfigurieren

Es stehen mehrere Konfigurationsoptionen zur Verfügung, die die Data Protection for VMware-Sicherheitseinstellungen für Knoten der Einheit zum Versetzen von Daten und VMCLI-Knoten betreffen, wenn diese Knoten eine Verbindung zu einem IBM Spectrum Protect-Server mit Version 7.1.8 oder 8.1.2 oder höher herstellen. Wenn Sie die Standardwerte für diese Optionen akzeptieren, werden diese Komponenten auf transparente Weise für eine erweiterte Sicherheit konfiguriert. Dies wird für die meisten Anwendungsfälle empfohlen.

Mit den Standardsicherheitseinstellungen konfigurieren (Schnellverfahren)

Das Schnellverfahren umfasst die Konfigurationsoptionen, die sich auf die Sicherheit der Verbindung des Knotens der Einheit zum Versetzen von Daten und des VMCLI-Knotens zum Server sowie auf das Verhalten für verschiedene Anwendungsfälle auswirken, wenn die Standardwerte akzeptiert werden. Das Szenario für das Schnellverfahren minimiert die Schritte im Konfigurationsprozess an den Endpunkten.

In diesem Szenario werden Zertifikate automatisch vom Server abgerufen, wenn der Knoten zum ersten Mal eine Verbindung herstellt. Dabei wird angenommen, dass der Parameter **SESSIONSECURITY** des IBM Spectrum Protect-Servers auf **TRANSITIONAL** gesetzt ist. Dies ist der Standardwert für die erste Verbindung. Sie können dieses Szenario befolgen, wenn Sie zuerst den IBM Spectrum Protect-Server auf Version 7.1.8 und höhere Stufen von Version 7 oder auf Version 8.1.2 und höhere Stufen von Version 8 und anschließend Data Protection for VMware auf diese Stufen aktualisieren oder umgekehrt.

Achtung: Dieses Szenario kann nicht verwendet werden, wenn der IBM Spectrum Protect-Server für LDAP-Authentifizierung konfiguriert ist. Wenn LDAP verwendet wird, können Sie die notwendigen Zertifikate mit dem Dienstprogramm 'dsmcert' manuell importieren. Weitere Informationen finden Sie in „Ohne automatische Zertifikatsverteilung konfigurieren” auf Seite 63.

Optionen für den Knoten der Einheit zum Versetzen von Daten mit Auswirkungen auf die Sitzungssicherheit

Mit den folgenden dsmc-Optionen werden die Sicherheitseinstellungen für den Knoten der Einheit zum Versetzen von Daten angegeben. Weitere Informationen zu diesen Optionen finden Sie in Clientoptionsreferenz.

- SSLREQUIRED. Der Standardwert Default ermöglicht vorhandene Verbindungen mit Sitzungssicherheit zu Servern mit früheren Versionen als 7.1.8 oder 8.1.2. Zu-

dem wird die Data Protection for VMware-Einheit zum Versetzen von Daten automatisch für die Herstellung sicherer Verbindungen zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher konfiguriert, indem TLS für die Authentifizierung verwendet wird.

- SSLACCEPTCERTFROMSERV. Mit dem Standardwert Yes akzeptiert die Einheit zum Versetzen von Daten automatisch ein selbst signiertes öffentliches Zertifikat vom Server. Zudem wird die Einheit zum Versetzen von Daten automatisch so konfiguriert, dass dieses Zertifikat verwendet wird, wenn die Einheit zum Versetzen von Daten eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellt.
- SSL. Der Standardwert No gibt an, dass keine Verschlüsselung verwendet wird, wenn Daten zwischen der Einheit zum Versetzen von Daten und einem Server mit einer früheren Version als 7.1.8 oder 8.1.2 übertragen werden. Wenn die Einheit zum Versetzen von Daten eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellt, gibt der Standardwert No an, dass Objektdaten nicht verschlüsselt werden. Alle anderen Informationen werden verschlüsselt, wenn die Einheit zum Versetzen von Daten mit dem Server kommuniziert. Der Wert Yes gibt an, dass alle Informationen einschließlich der Objektdaten mit TLS verschlüsselt werden, wenn die Einheit zum Versetzen von Daten mit dem Server kommuniziert.
- SSLFIPSMODE. Der Standardwert No gibt an, dass keine FIPS-zertifizierte TLS-Bibliothek erforderlich ist (FIPS - Federal Information Processing Standard).

Darüber hinaus finden die folgenden Optionen nur dann Anwendung, wenn die Einheit zum Versetzen von Daten eine TLS-Verbindung zu einem Server mit einer früheren Version als 7.1.8 oder 8.1.2 verwendet. Sie werden ignoriert, wenn die Einheit zum Versetzen von Daten eine Verbindung zu einem Server mit einer höheren Version herstellt.

- SSLDISABLELEGACYTLS. Der Wert No gibt an, dass die Einheit zum Versetzen von Daten für SSL-Sitzungen nicht TLS 1.2 erzwingt. Sie lässt Verbindungen mit TLS 1.1 und niedrigeren SSL-Protokollen zu. Wenn die Einheit zum Versetzen von Daten mit einem IBM Spectrum Protect-Server mit Version 7.1.7 oder 8.1.1 oder früher kommuniziert, ist No der Standardwert.
- LANFREESSL. Der Standardwert No gibt an, dass die Einheit zum Versetzen von Daten bei der Kommunikation mit dem Speicheragenten nicht TLS verwendet, wenn LAN-unabhängige Datenübertragung konfiguriert ist.
- REPLSSLPORT. Gibt die TCP/IP-Portadresse an, die für TLS aktiviert ist, wenn die Einheit zum Versetzen von Daten mit dem Zielreplikationsserver kommuniziert.

Optionen für den VMCLI-Knoten mit Auswirkungen auf die Sitzungssicherheit

Die folgenden Parameter geben die Sicherheitseinstellungen für den VMCLI-Knoten an. Weitere Informationen zu diesen Optionen finden Sie in Profilparameter.

- VE_TSM_SSL. Der Standardwert NO gibt an, dass keine Verschlüsselung verwendet wird, wenn Daten zwischen der Einheit zum Versetzen von Daten und einem Server mit einer früheren Version als 7.1.8 oder 8.1.2 übertragen werden. Setzen Sie diesen Wert auf YES, wenn bei der Herstellung einer Verbindung zu einem Server mit einer früheren Version als 7.1.8 alle Informationen mit TLS verschlüsselt werden sollen.
- VE_TSM_SSLACCEPTCERTFROMSERV. Mit dem Standardwert YES akzeptiert die Schnittstelle automatisch ein selbst signiertes öffentliches Zertifikat vom Server. Zudem wird die Schnittstelle automatisch so konfiguriert, dass dieses Zertifikat

verwendet wird, wenn die Einheit zum Versetzen von Daten eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellt.

- `VE_TSM_SSLREQUIRED`. Der Standardwert `DEFAULT` ermöglicht vorhandene Verbindungen mit Sitzungssicherheit zu Servern mit früheren Versionen als 7.1.8 oder 8.1.2. Zudem wird die Schnittstelle automatisch für die Herstellung sicherer Verbindungen zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher konfiguriert, indem TLS für die Authentifizierung verwendet wird.

Anwendungsfälle für die Standardsicherheitseinstellungen

- Zuerst wird der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert. Anschließend wird Data Protection for VMware aktualisiert. Der vorhandene Knoten der Einheit zum Versetzen von Daten und VMCLI-Knoten *verwenden keine* SSL-Kommunikation:
  - An den Sicherheitsoptionen für den Knoten der Einheit zum Versetzen von Daten und den VMCLI-Knoten sind keine Änderungen erforderlich.
  - Die Konfiguration wird automatisch so aktualisiert, dass TLS verwendet wird, wenn die Knoten sich beim Server authentifizieren.
- Zuerst wird der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert. Anschließend wird Data Protection for VMware aktualisiert. Der vorhandene Knoten der Einheit zum Versetzen von Daten und VMCLI-Knoten *verwenden* SSL-Kommunikation:
  - An den Sicherheitsoptionen für den Knoten der Einheit zum Versetzen von Daten und den VMCLI-Knoten sind keine Änderungen erforderlich.
  - Es wird weiterhin SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
  - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Stufe erweitert, die für den Server erforderlich ist.
- Zuerst wird Data Protection for VMware auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert. Der Server wird zu einem späteren Zeitpunkt aktualisiert. Der vorhandene Knoten der Einheit zum Versetzen von Daten und VMCLI-Knoten *verwenden keine* SSL-Kommunikation:
  - An den Sicherheitsoptionen für den Knoten der Einheit zum Versetzen von Daten und den VMCLI-Knoten sind keine Änderungen erforderlich.
  - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server mit früheren Versionen als 7.1.8 oder 8.1.2 verwendet.
  - Nachdem der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert wurde, wird die Konfiguration automatisch so aktualisiert, dass TLS verwendet wird, wenn die Knoten sich beim Server authentifizieren.
- Zuerst wird Data Protection for VMware auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert. Der Server wird zu einem späteren Zeitpunkt aktualisiert. Der vorhandene Knoten der Einheit zum Versetzen von Daten und VMCLI-Knoten *verwenden* SSL-Kommunikation:
  - An den Sicherheitsoptionen für den Knoten der Einheit zum Versetzen von Daten und den VMCLI-Knoten sind keine Änderungen erforderlich.
  - Für Server mit früheren Versionen als 7.1.8 oder 8.1.2 wird weiterhin SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
  - Nachdem der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert wurde, wird die SSL-Kommunikation automatisch für die Verwendung der TLS-Stufe erweitert, die für den Server erforderlich ist.
- Zuerst wird Data Protection for VMware auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert. Anschließend stellen der Knoten der Einheit zum Versetzen von Da-

ten und der VMCLI-Knoten Verbindungen zu mehreren Servern her. Die Server werden zu unterschiedlichen Zeitpunkten aktualisiert:
  - An den Sicherheitsoptionen für den Knoten der Einheit zum Versetzen von Daten und den VMCLI-Knoten sind keine Änderungen erforderlich.
  - Der Knoten der Einheit zum Versetzen von Daten und der VMCLI-Knoten verwenden das vorhandene Protokoll für Authentifizierung und Sitzungssicherheit für Server mit früheren Versionen als 7.1.8 oder 8.1.2. Wenn die Knoten zum ersten Mal eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellen, werden sie automatisch für die Verwendung der TLS-Authentifizierung aktualisiert. Die Sitzungssicherheit wird pro Server verwaltet.
- Neue Clientinstallation; Server hat Version 7.1.8 oder 8.1.2 oder höher:
  - Konfigurieren Sie Data Protection for VMware wie für eine Neuinstallation.
  - Mit den Standardwerten für die Sicherheitsoptionen werden der Knoten der Einheit zum Versetzen von Daten und der VMCLI-Knoten automatisch für die mit TLS verschlüsselte Sitzungsauthentifizierung konfiguriert.
  - Setzen Sie den SSL-Parameter auf den Wert `Yes`, wenn die Verschlüsselung aller Datenübertragungen zwischen Client und Server erforderlich ist.
- Neue Clientinstallation; Server hat eine frühere Version als 7.1.8 oder 8.1.2:
  - Konfigurieren Sie den Client wie für eine neue Clientinstallation.
  - Akzeptieren Sie die Standardwerte für die Sicherheitsparameter der Clientsitzung, wenn die SSL-Verschlüsselung aller Datenübertragungen nicht erforderlich ist.
    - Ein Nicht-SSL-Authentifizierungsprotokoll wird verwendet, bis der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert wird.
  - Setzen Sie den SSL-Parameter auf den Wert `Yes`, wenn die Verschlüsselung aller Datenübertragungen zwischen der Einheit zum Versetzen von Daten und dem Server erforderlich ist, und fahren Sie mit der manuellen Konfiguration für SSL fort.
    - Konfigurationsanweisungen finden Sie in Tivoli Storage Manager-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
    - Nachdem der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert wurde, wird die SSL-Kommunikation automatisch für die Verwendung der TLS-Stufe erweitert, die für den Server erforderlich ist.

Ohne automatische Zertifikatsverteilung konfigurieren

In diesem Szenario sind die Konfigurationsoptionen beschrieben, die sich auf die Sicherheit der Knoten der Einheit zum Versetzen von Daten und der VMCLI-Knoten auswirken, wenn die automatische Verteilung der Zertifikate vom Server nicht zulässig ist. Beispielsweise ist die automatische Verteilung der Zertifikate vom Server nicht zulässig, wenn der Server für die Verwendung der LDAP-Authentifizierung konfiguriert ist oder wenn die Zertifikate von einer Zertifizierungsstelle (Certificate Authority - CA) signiert sein müssen.

Optionen mit Auswirkungen auf die Sitzungssicherheit

Die Optionen für Sicherheitseinstellungen entsprechen den in „Mit den Standardsicherheitseinstellungen konfigurieren (Schnellverfahren)" auf Seite 60 beschriebenen Optionen, mit der Ausnahme, dass Sie die Option `SSLACCEPTCERTFROMSERV` auf `No` setzen müssen, um sicherzustellen, dass der Knoten der Einheit zum Versetzen von Daten nicht automatisch ein selbst signiertes öffentliches Zertifikat vom Server akzeptiert, wenn der Knoten zum ersten Mal eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellt.

Anwendungsfälle für die Konfiguration der Knoten der Einheit zum Versetzen von Daten ohne automatische Zertifikatsverteilung

Wenn die automatische Zertifikatsverteilung nicht möglich oder erwünscht ist, verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Server oder von einer CA an. Die CA kann ein Unternehmen wie VeriSign oder Thawte oder eine interne CA innerhalb Ihrer Firma sein.

Wenn der Knoten der Einheit zum Versetzen von Daten und der VMCLI-Knoten sich auf derselben Maschine befinden, ist nur ein Zertifikat erforderlich. Befinden die Knoten sich auf separaten Maschinen, ist ein Zertifikat auf jeder Maschine erforderlich.

- Zuerst wird der Server auf Version 7.1.8 oder 8.1.2 aktualisiert. Anschließend wird Data Protection for VMware aktualisiert. Die vorhandenen Knoten der Einheit zum Versetzen von Daten *verwenden keine* SSL-Kommunikation:
  - Setzen Sie die Option `SSLACCEPTCERTFROMSERV` auf den Wert `No`.
  - Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Server oder von einer CA an und importieren Sie das Zertifikat mit dem Dienstprogramm 'dsmcert'. Konfigurationsanweisungen finden Sie in Tivoli Storage Manager-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
- Zuerst wird der Server auf Version 7.1.8 oder 8.1.2 aktualisiert. Anschließend wird Data Protection for VMware aktualisiert. Die vorhandenen Knoten der Einheit zum Versetzen von Daten *verwenden* SSL-Kommunikation:
  - An den Sicherheitsoptionen für die Knoten der Einheit zum Versetzen von Daten sind keine Änderungen erforderlich. Wenn die Knoten bereits über ein Serverzertifikat für die SSL-Kommunikation verfügen, findet die Option `SSLACCEPTCERTFROMSERV` keine Anwendung.
  - Es wird weiterhin SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
  - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Stufe erweitert, die für den Server erforderlich ist.
- Zuerst wird Data Protection for VMware auf Version 7.1.8 oder 8.1.2 aktualisiert. Der Server wird zu einem späteren Zeitpunkt aktualisiert. Die vorhandenen Knoten der Einheit zum Versetzen von Daten *verwenden keine* SSL-Kommunikation:
  - Setzen Sie die Option `SSLACCEPTCERTFROMSERV` auf den Wert `No`.
  - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server mit früheren Versionen als 7.1.8 oder 8.1.2 verwendet.
  - Bevor die Knoten der Einheit zum Versetzen von Daten eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellen:
    - Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Server oder von einer CA an und importieren Sie das Zertifikat mit dem Dienstprogramm 'dsmcert'. Konfigurationsanweisungen finden Sie in Tivoli Storage Manager-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
- Zuerst wird Data Protection for VMware auf Version 7.1.8 oder 8.1.2 aktualisiert. Der Server wird zu einem späteren Zeitpunkt aktualisiert. Die vorhandenen Knoten der Einheit zum Versetzen von Daten *verwenden* SSL-Kommunikation:
  - An den Sicherheitsoptionen für die Knoten der Einheit zum Versetzen von Daten sind keine Änderungen erforderlich. Wenn die Knoten bereits über ein

Serverzertifikat für die SSL-Kommunikation verfügen, findet die Option SSLACCEPTCERTFROMSERV keine Anwendung.

  - Für Server mit früheren Versionen als 7.1.8 oder 8.1.2 wird weiterhin SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
  - Nachdem der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert wurde, wird die SSL-Kommunikation automatisch für die Verwendung der TLS-Stufe erweitert, die für den Server erforderlich ist.

- Zuerst wird Data Protection for VMware auf Version 7.1.8 oder 8.1.2 aktualisiert. Anschließend stellen die Knoten der Einheit zum Versetzen von Daten Verbindungen zu mehreren Servern her. Die Server werden zu unterschiedlichen Zeitpunkten aktualisiert:
  - Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
  - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server mit früheren Versionen als 7.1.8 oder 8.1.2 verwendet.
  - Bevor die Knoten der Einheit zum Versetzen von Daten eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellen oder wenn auf einem Server mit beliebiger Version SSL-Kommunikation erforderlich ist:
    - Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Server oder von einer CA an und importieren Sie das Zertifikat mit dem Dienstprogramm 'dsmcert'. Konfigurationsanweisungen finden Sie in Tivoli Storage Manager-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
  - Die Knoten der Einheit zum Versetzen von Daten verwenden das vorhandene Protokoll für Authentifizierung und Sitzungssicherheit für Server mit früheren Versionen als 7.1.8 oder 8.1.2. Wenn die Knoten zum ersten Mal eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellen, werden sie automatisch für die Verwendung der TLS-Authentifizierung aktualisiert. Die Sitzungssicherheit wird pro Server verwaltet.
- Neue Data Protection for VMware-Installation; Server hat Version 7.1.8 oder 8.1.2 oder höher:
  - Konfigurieren Sie Data Protection for VMware wie für eine Neuinstallation.
  - Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
  - Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Server oder von einer CA an und importieren Sie das Zertifikat mit dem Dienstprogramm 'dsmcert'. Konfigurationsanweisungen finden Sie in Tivoli Storage Manager-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
  - Setzen Sie den SSL-Parameter auf den Wert Yes, wenn die Verschlüsselung aller Datenübertragungen zwischen der Einheit zum Versetzen von Daten und dem Server erforderlich ist.
- Neue Data Protection for VMware-Installation; Server hat eine frühere Version als 7.1.8 oder 8.1.2; mit SSL verschlüsselte Sitzungen *sind* erforderlich:
  - Konfigurieren Sie Data Protection for VMware wie für eine Neuinstallation.
  - Setzen Sie den SSL-Parameter auf den Wert Yes.
  - Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Server oder von einer CA an und importieren Sie das Zertifikat mit dem Dienstprogramm 'dsmcert'. Konfigurationsanweisungen finden Sie in Tivoli Storage Manager-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
- Neue Data Protection for VMware-Installation; Server hat eine frühere Version als 7.1.8 oder 8.1.2; mit SSL verschlüsselte Sitzungen *sind nicht* erforderlich:
  - Konfigurieren Sie Data Protection for VMware wie für eine Neuinstallation.

– Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
  - Ein Nicht-SSL-Authentifizierungsprotokoll wird verwendet, bis der Server auf Version 7.1.8 oder 8.1.2 oder höher aktualisiert wird.
– Bevor die Knoten der Einheit zum Versetzen von Daten eine Verbindung zu einem Server mit Version 7.1.8 oder 8.1.2 oder höher herstellen:
  - Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Server oder von einer CA an und importieren Sie das Zertifikat mit dem Dienstprogramm 'dsmcert'. Konfigurationsanweisungen finden Sie in Tivoli Storage Manager-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.

Kommunikation der Data Protection for VMware vSphere-GUI über Transport Layer Security konfigurieren

Die Data Protection for VMware vSphere-GUI verwendet das Protokoll Transport Layer Security (TLS), um sichere Kommunikation mit Web-Browsern, dem VMware vCenter-Server und optional dem IBM Spectrum Protect-Server bereitzustellen.

Informationen zu diesem Vorgang

Für die Kommunikation mit Web-Browsern und dem VMware vCenter-Server ist das TLS-Protokoll immer aktiviert. Bei der Installation von Data Protection for VMware wird ein selbst signiertes digitales TLS-Zertifikat generiert und anschließend für die Herstellung der Verbindung verwendet.

Sie können auch ein Zertifikat verwenden, das von einer Zertifizierungsstelle (Certificate Authority - CA) signiert wurde, um mit Web-Browsern zu kommunizieren. Data Protection for VMware Informationen zur Verwendung eines Zertifikats von einer CA finden Sie in Zertifikat eines Drittanbieters für Web-Browser-Sitzungen verwenden.

Für die Kommunikation mit dem IBM Spectrum Protect-Server ist die Verwendung des TLS-Protokolls von der Version des Servers abhängig.

Wenn Sie einen IBM Spectrum Protect-Server mit Version 7.1.7 oder 8.1.1 oder früher verwenden

Die Verwendung des TLS-Protokolls für die Kommunikation mit dem Server ist optional. Sie können die Data Protection for VMware vSphere-GUI manuell für die Kommunikation mit dem Server über das TLS-Protokoll aktivieren, indem Sie den Truststore erstellen oder aktualisieren und ein Zertifikat importieren, wie in „Sichere Kommunikation mit dem IBM Spectrum Protect-Server aktivieren" auf Seite 67 beschrieben.

Wenn Sie einen IBM Spectrum Protect-Server mit Version 7.1.8 oder 8.1.2 oder höher verwenden

Das TLS-Protokoll ist erforderlich. In den meisten Fällen wird der Truststore bei der ersten Verwendung automatisch erstellt. Dabei werden die Standardsicherheitseinstellungen verwendet, die in „Mit den Standardsicherheitseinstellungen konfigurieren (Schnellverfahren)" auf Seite 60 beschrieben sind. In einigen Szenarios müssen Sie den Truststore jedoch möglicherweise manuell erstellen.

Wichtig: Im Szenario für das Schnellverfahren werden Zertifikate automatisch abgerufen, wenn die Data Protection for VMware vSphere-GUI zum ersten Mal mit dem Server kommuniziert. Dabei wird angenommen, dass der Parameter **SESSIONSECURITY** des IBM Spectrum Protect-Servers auf

TRANSITIONAL gesetzt ist. Dies ist der Standardwert für die erste Verbindung. Nachdem die GUI eine Verbindung zum Server hergestellt hat, wird der Parameter **SESSIONSECURITY** auf **STRICT** gesetzt. Da die GUI für die Herstellung der Verbindung zum Server die Serveradministrator-ID verwendet, wird beim Versuch, eine Verbindung zum Server herzustellen, eine Fehlernachricht in der GUI angezeigt, wenn eine andere Entität diese ID bereits verwendet hat, um eine Verbindung herzustellen. Setzen Sie den Parameter **SESSIONSECURITY** wieder auf **TRANSITIONAL**, um dieses Problem zu beheben.

Sichere Kommunikation mit dem IBM Spectrum Protect-Server aktivieren

Wenn Sie einen IBM Spectrum Protect-Server mit Version 7.1.7 oder früher bzw. Version 8.1.2 oder früher verwenden, ist die Herstellung der Verbindung zum Server über das TLS-Protokoll optional. Wenn Sie die Data Protection for VMware vSphere-GUI für die Kommunikation mit dem Server über das TLS-Protokoll aktivieren möchten, müssen Sie die Kommunikation manuell aktivieren.

Vorbereitende Schritte

Fordern Sie eine Kopie des Zertifikats vom Serveradministrator an.

Informationen zu diesem Vorgang

Wenn Sie einen Server mit Version 7.1.8 oder 8.1.2 oder höher verwenden, ist das TLS-Protokoll erforderlich. Bei der ersten Herstellung einer Verbindung wird automatisch ein Truststore mit einem Zertifikat erstellt. Dabei werden die Standardsicherheitseinstellungen verwendet, die in „Mit den Standardsicherheitseinstellungen konfigurieren (Schnellverfahren)" auf Seite 60 beschrieben sind. In einigen Szenarios müssen Sie jedoch möglicherweise gemäß der Beschreibung in diesem Thema manuell den Truststore erstellen und die Data Protection for VMware vSphere-GUI konfigurieren.

Bei der folgenden Prozedur wird das Java™-Tool **keytool** für das Schlüssel- und Zertifikatsmanagement verwendet.

Unter Linux-Betriebssystemen befindet das Tool sich im Verzeichnis `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Unter Microsoft Windows-Betriebssystemen befindet das Tool sich im Verzeichnis `C:\Programme\Common Files\Tivoli\TSM\jvm80516\jre\bin`.

Sie müssen möglicherweise den vollständigen Pfad angeben, wenn Sie den Befehl **keytool** ausführen.

Vorgehensweise

1. In der Befehlszeile wechseln Sie in das Verzeichnis, das die Truststores enthält:
   - Unter Linux: `/opt/tivoli/tsm/tdpvmware/common/scripts/`
   - Unter Windows: `C:\Programme\IBM\SpectrumProtect\Framework\VEGUI\scripts\`
2. Erstellen Sie den Truststore und importieren Sie das Zertifikat mit dem folgenden Befehl:

   ```
   keytool -importcert -alias mein-Zertifikat -file cert.pem -keystore
   tsm-ve-truststore.jks -storepass Kennwort
   ```

Dabei gilt:

-alias *mein-Zertifikat*
Der eindeutige Aliasname, der das Zertifikat im Truststore identifiziert.

-file *cert.pem*
Die Datei, die das selbst signierte Serverzertifikat oder das CA-Stammzertifikat enthält.

-storepass *Kennwort*
Das Schlüsselspeicherkennwort. Merken Sie sich dieses Kennwort für die künftige Verwendung.

3. Starten Sie die Data Protection for VMware vSphere-GUI und rufen Sie das Fenster **Konfiguration** auf.
   - Wenn Sie eine Erstkonfiguration erstellen, klicken Sie auf **Tasks** > **IBM Spectrum Protect-Konfigurationsassistenten ausführen** und rufen Sie die Seite **Serverberechtigungsnachweise** auf.
   - Wenn Sie eine vorhandene Konfiguration ändern, klicken Sie auf **Tasks** > **IBM Spectrum Protect-Konfiguration editieren** und rufen Sie die Seite **Serverberechtigungsnachweise** auf.
4. Geben Sie die Portnummer in das Feld **IBM Spectrum Protect-Administratorport** ein. Dies ist der Server-Port, der Verwaltungsverbindungen über SSL oder TLS ermöglicht.
5. Wählen Sie **Verschlüsselte Kommunikation am Administratorport verwenden** aus.
6. Wenn Sie diese Einstellung in künftigen GUI-Sitzungen verwenden möchten, wählen Sie **Die Administrator-ID, das Kennwort und die Porteinstellungen speichern** aus.
7. Klicken Sie auf **OK**, um die Änderungen anzuwenden.

Zertifikat von einer Zertifizierungsstelle verwenden

Zur Verwendung eines Zertifikats, das von einer Zertifizierungsstelle (Certificate Authority - CA) signiert wurde, müssen Sie mehrere Schritte durchführen.

Informationen zu diesem Vorgang

In den folgenden Prozeduren wird das Standardtool für Schlüssel- und Zertifikatsmanagement, **keytool**, verwendet.

Unter Linux-Betriebssystemen befindet es sich im Verzeichnis `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Unter Microsoft Windows-Betriebssystemen befindet es sich im Verzeichnis `C:\Programme\Common Files\Tivoli\TSM\jvm80516\jre`.

Sie müssen möglicherweise den vollständigen Pfad angeben, wenn Sie **keytool** über die Befehlszeile ausführen.

Vorgehensweise

1. Fordern Sie Zugriff auf den Schlüsselspeicher an.
2. Erstellen Sie eine Zertifikatssignieranforderung (Certificate Signing Request - CSR).
3. Senden Sie die Zertifikatssignieranforderung zum Signieren an die Zertifizierungsstelle.

4. Laden Sie das signierte Zertifikat in die Data Protection for VMware vSphere-GUI herunter.

Zugriff auf den Schlüsselspeicher anfordern:

Zertifikate sind in einem Java-Schlüsselspeicher gespeichert. Der Inhalt des Schlüsselspeichers ist durch ein Kennwort geschützt. Zum Bearbeiten der Zertifikate in dem Schlüsselspeicher müssen Sie Zugriff auf den Schlüsselspeicher anfordern.

Informationen zu diesem Vorgang

Das standardmäßige selbst signierte Zertifikat und Schlüsselspeicherkennwort werden während der Installation automatisch generiert. Daher ist es unwahrscheinlich, dass Ihnen das Anfangskennwort bekannt ist.

Führen Sie die folgende Prozedur aus, um den ursprünglichen Schlüsselspeicher durch einen neuen Schlüsselspeicher mit einem neuen selbst signierten Zertifikat zu ersetzen. Der neue Schlüsselspeicher ist durch ein Kennwort Ihrer Wahl geschützt.

Wenn Ihnen das Schlüsselspeicherkennwort bereits bekannt ist, überspringen Sie diese Prozedur.

Vorgehensweise

1. Stoppen Sie den Service der Data Protection for VMware vSphere-GUI.
2. In der Befehlszeile wechseln Sie in das Verzeichnis, das die Schlüsselspeicher enthält.
   - Unter Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Unter Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
3. Erstellen Sie eine Sicherungskopie der Schlüsselspeicherdatei (`key.jks`), indem Sie sie umbenennen oder an eine andere Position verschieben.
4. Erstellen Sie einen neuen Schlüsselspeicher mit einem neuen selbst signierten Zertifikat, indem Sie den folgenden Befehl ausgeben:

   ```
   keytool -genkeypair -alias vekey -dname
   CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
   -sigalg SHA256withRSA -keysize 2048 -validity Tage -keystore
   key.jks -storepass Kennwort -keypass Kennwort
   ```

   Dabei gilt:

   -dname CN=*fqdn*,OU=Tivoli_Storage_Manager_for_VMware,O=IBM
   : *fqdn* ist der DNS-Name oder vollständig qualifizierte Domänenname des Computers, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

   -validity *Tage*
   : Der Zertifikatsgültigkeitszeitraum.

   -storepass *Kennwort*
   : Das Schlüsselspeicherkennwort. Merken Sie sich dieses Kennwort für die künftige Verwendung.

   -keypass *Kennwort*
   : Das Kennwort für privaten Schlüssel für das Zertifikat. Dieses Kennwort muss mit dem Schlüsselspeicherkennwort übereinstimmen.

5. Codieren Sie das Schlüsselspeicherkennwort mit dem Tool **securityUtility**. Geben Sie den folgenden Befehl aus.
   - Unter Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
   - Unter Windows: `C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode`

   Geben Sie bei der entsprechenden Aufforderung Ihr Schlüsselspeicherkennwort ein und speichern Sie die Ausgabe (kopieren Sie sie beispielsweise in die Zwischenablage).
6. Öffnen Sie die Datei `bootstrap.properties` in einem Editor und setzen Sie die Eigenschaft `veProfile.keystore.pswd` auf den codierten Wert aus dem vorherigen Schritt. Die Datei `bootstrap.properties` befindet sich an der folgenden Position:
   - Unter Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`
   - Unter Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\`
7. Starten Sie den Service der Data Protection for VMware vSphere-GUI.

Zugehörige Verweise:

„Services für Data Protection for VMware starten und ausführen" auf Seite 93

Zertifikatssignieranforderung erstellen:

Wenn Sie Zugriff auf den Schlüsselspeicher erhalten haben, müssen Sie eine Zertifikatssignieranforderung (Certificate Signing Request - CSR) erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine CSR zu erstellen:

1. In der Befehlszeile wechseln Sie in das Verzeichnis, das die Schlüsselspeicher enthält.
   - Unter Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Unter Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Erstellen Sie ein neues Zertifikat, indem Sie den folgenden Befehl ausgeben:

   ```
   keytool -genkeypair -alias mein-Schlüssel -dname
   CN=fqdn,OU=Bereich,O=Organisation -keyalg RSA -sigalg SHA256withRSA
   -keysize 2048 -validity Tage -keystore key.jks -storepass
   Kennwort -keypass Kennwort
   ```

   Dabei gilt:

   -alias *mein-Schlüssel*
   : *mein-Schlüssel* ist der eindeutige Aliasname, der das Zertifikat im Schlüsselspeicher identifiziert. Er wird umbenannt, wenn das signierte Zertifikat empfangen wird.

   -dname CN=*fqdn***,OU=***Bereich***,O=***Organisation*
   : *fqdn* ist der DNS-Name oder vollständig qualifizierte Domänenname des Computers, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

Bereich und *Organisation* sind die Informationen zur Organisation, die für Ihre Maßnahmen oder für die Zertifizierungsstelle erforderlich sind.

-validity *Tage*
Der Zertifikatsgültigkeitszeitraum.

-storepass *Kennwort*
Das Schlüsselspeicherkennwort. Wenn Sie das Schlüsselspeicherkennwort nicht kennen oder vergessen haben, finden Sie weitere Informationen in „Zugriff auf den Schlüsselspeicher anfordern" auf Seite 69.

-keypass *Kennwort*
Das Kennwort für privaten Schlüssel für das Zertifikat. Dieses Kennwort muss mit dem Schlüsselspeicherkennwort übereinstimmen.

3. Erstellen Sie eine CSR, indem Sie den folgenden Befehl ausgeben:

   ```
   keytool -certreq -alias mein-Schlüssel -file certreq.pem -keystore key.jks
   ```

   Dabei gilt:

   -alias *mein-Schlüssel*
   Der Zertifikatsaliasname aus dem vorherigen Schritt.

   -file *certreq.pem*
   Die Datei, in der die Zertifikatssignieranforderung gespeichert werden soll.

Zertifikatssignieranforderung an die Zertifizierungsstelle senden:

Nachdem Sie die Zertifikatsanforderung (`certreq.pem`) erstellt haben, müssen Sie sie zum Signieren an die Zertifizierungsstelle senden. Befolgen Sie die speziellen Anweisungen von der Zertifizierungsstelle.

Signiertes Zertifikat empfangen:

Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle (Certificate Authority - CA) erhalten haben, müssen Sie das Zertifikat in den Schlüsselspeicher herunterladen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das signierte Zertifikat zu empfangen:

1. In der Befehlszeile wechseln Sie in das Verzeichnis, das die Schlüsselspeicher enthält.
   - Unter Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Unter Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Kopieren Sie die Dateien, die Sie von der CA empfangen haben, an diese Position. Diese Dateien umfassen das CA-Stammzertifikat, ggf. CA-Zwischenzertifikate und das signierte Zertifikat für die Data Protection for VMware vSphere-GUI.
3. Stoppen Sie den Service der Data Protection for VMware vSphere-GUI.
4. Erstellen Sie eine Sicherungskopie der Schlüsselspeicherdatei (`key.jks`), indem Sie sie unter einem anderen Namen oder an eine andere Position kopieren.

5. Importieren Sie ggf. die CA-Zwischenzertifikate mit dem folgenden Befehl. Auf die Anfrage, ob den Zertifikaten vertraut werden soll, antworten Sie mit *ja*. Wiederholen Sie diesen Schritt für mehrere CA-Zwischenzertifikate nach Bedarf.

   ```
   keytool -importcert -alias CA-Zwischenzertifikat -file intermediate.pem
   -keystore key.jks -storepass Kennwort
   ```

   Dabei gilt:

   -alias *CA-Zwischenzertifikat*
   Der eindeutige Aliasname, der das Zertifikat im Schlüsselspeicher identifiziert. Jedes Zwischenzertifikat muss über einen eindeutigen Aliasnamen verfügen.

   -file *intermediate.pem*
   Die Zwischenzertifikatsdatei, die von der CA erhalten wurde.

   -storepass *Kennwort*
   Das Schlüsselspeicherkennwort.

6. Importieren Sie das CA-Stammzertifikat, indem Sie den folgenden Befehl ausgeben. Auf die Anfrage, ob diesem Zertifikat vertraut werden soll, antworten Sie mit *ja*.

   ```
   keytool -importcert -alias CA-Stammzertifikat -file root.pem -keystore
   key.jks -storepass Kennwort
   ```

   Dabei gilt:

   -alias *CA-Stammzertifikat*
   Der eindeutige Aliasname, der das Zertifikat im Schlüsselspeicher identifiziert.

   -file *root.pem*
   Die Stammzertifikatsdatei, die von der CA erhalten wurde.

   -storepass *Kennwort*
   Das Schlüsselspeicherkennwort.

7. Importieren Sie das signierte Zertifikat, indem Sie den folgenden Befehl ausgeben:

   ```
   keytool -importcert -alias mein-Schlüssel -file signedcert.pem -keystore
   key.jks -storepass Kennwort
   ```

   Dabei gilt:

   -alias *mein-Schlüssel*
   Der Aliasname für das signierte Zertifikat. Der Aliasname muss der Name sein, der auch bei der Generierung der Zertifikatssignieranforderung (Certificate Signing Request - CSR) verwendet wurde.

   -file *signedcert.pem*
   Die Datei für das signierte Zertifikat, die von der CA empfangen wurde.

   -storepass *Kennwort*
   Das Schlüsselspeicherkennwort.

8. Löschen Sie das vorhandene Zertifikat, das den Aliasnamen `vekey` enthält:

   ```
   keytool -delete -alias vekey -keystore key.jks -storepass Kennwort
   ```

   Dabei ist `-storepass` *Kennwort* das Kennwort für den Schlüsselspeicher.

9. Benennen Sie das signierte Zertifikat in `vekey` um:

```
keytool -changealias -alias mein-Schlüssel -destalias vekey -keystore
key.jks -storepass Kennwort
```

Dabei gilt:

-alias *mein-Schlüssel*
Der Aliasname des signierten Zertifikats.

-storepass *Kennwort*
Das Schlüsselspeicherkennwort.

10. Starten Sie den Service der Data Protection for VMware vSphere-GUI.

Zugehörige Verweise:

„Services für Data Protection for VMware starten und ausführen" auf Seite 93

Anforderungen hinsichtlich der Benutzerberechtigungen für den VMware vCenter-Server

Für die Ausführung von Data Protection for VMware-Operationen sind bestimmte Berechtigungen für den VMware vCenter-Server erforderlich.

Erforderliche vCenter-Serverberechtigungen für den Schutz von VMware-Datencentern mit der Web-Browser-Sicht für die Data Protection for VMware vSphere-GUI

Die Benutzer-ID des vCenter-Servers, die sich bei der Browser-Sicht für die Data Protection for VMware vSphere-GUI anmeldet,

muss über ausreichende VMware-Berechtigungen zum Anzeigen des Inhalts eines Datencenters verfügen, das von der GUI verwaltet wird.

Beispiel: Eine VMware vSphere-Umgebung enthält fünf Datencenter. Der Benutzer „jenn" verfügt nur für zwei dieser Datencenter über ausreichende Berechtigungen. Daher sind nur die beiden Datencenter, für die ausreichende Berechtigungen vorhanden sind, für „jenn" in den Sichten sichtbar. Die übrigen drei Datencenter (für die „jenn" keine Berechtigungen hat) sind für den Benutzer „jenn" nicht sichtbar.

Auf dem VMware vCenter-Server wird eine Gruppe von Berechtigungen gemeinsam als Rolle definiert. Eine Rolle wird für einen bestimmten Benutzer oder eine bestimmte Gruppe auf ein Objekt angewendet, um eine Berechtigung zu erstellen. Vom VMware vSphere-Web-Client aus müssen Sie eine Rolle mit einer Gruppe von Berechtigungen erstellen. Verwenden Sie die Funktion **Add a Role** des VMware vSphere-Clients, um eine vCenter-Serverrolle für Sicherungs- und Zurückschreibungsoperationen zu erstellen.

Wenn die Berechtigungen an alle Datencenter innerhalb des vCenters weitergegeben werden sollen, geben Sie den vCenter-Server an und wählen Sie das Kontrollkästchen `Propagate to children` aus. Andernfalls können Sie die Berechtigungen begrenzen, wenn Sie die Rolle nur den erforderlichen Datencentern zuordnen und das Kontrollkästchen `Propagate to children` auswählen. Bei der Browser-GUI werden Berechtigungen auf der Ebene des Datencenters erzwungen.

Das folgende Beispiel zeigt die Zugriffssteuerung zu Datencentern für zwei VMware-Benutzergruppen. Erstellen Sie zuerst eine Rolle, die alle in der Technote 7047438 definierten Berechtigungen enthält. Die Gruppe von Berechtigungen in diesem Beispiel werden durch die Rolle „TDPVMwareManage" identifiziert. Gruppe 1 benötigt Zugriff zum Verwalten virtueller Maschinen für die Datencenter

Primary1_DC und Primary2_DC. Gruppe 2 benötigt Zugriff zum Verwalten virtueller Maschinen für die Datencenter Secondary1_DC und Secondary2_DC.

Für Gruppe 1 ordnen Sie die Rolle „TDPVMwareManage" den Datencentern Primary1_DC und Primary2_DC zu. Für Gruppe 2 ordnen Sie die Rolle „TDPVMwareManage" den Datencentern Secondary1_DC und Secondary2_DC zu.

Die Benutzer in jeder VMware-Benutzergruppe können mithilfe der Data Protection for VMware-GUI nur virtuelle Maschinen in ihren jeweiligen Datencentern verwalten.

Tipp: Wenn Sie eine Rolle erstellen, empfiehlt es sich möglicherweise, der Rolle zusätzliche Berechtigungen hinzuzufügen, die Sie später für weitere Tasks mit Objekten benötigen.

Erforderliche vCenter-Serverberechtigungen für die Verwendung der Einheit zum Versetzen von Daten

Auf der IBM Spectrum Protect-Einheit zum Versetzen von Daten, die auf dem vStorage-Sicherungsserver installiert ist, (dem Knoten der Einheit zum Versetzen von Daten) müssen die Optionen VMCUser und VMCPw definiert sein. Die Option VMCUser gibt die Benutzer-ID des vCenter- oder ESX-Servers an, der gesichert, zurückgeschrieben oder abgefragt werden soll. Die erforderlichen Berechtigungen, die dieser Benutzer-ID (VMCUser) zugeordnet sind, stellen sicher, dass der Client Operationen mit der virtuellen Maschine und in der VMware-Umgebung ausführen kann. Diese Benutzer-ID muss über die VMware-Berechtigungen verfügen, die in der oben genannten Technote beschrieben sind.

Verwenden Sie die Funktion **Add a Role** des VMware vSphere-Clients, um eine vCenter-Serverrolle für Sicherungs- und Zurückschreibungsoperationen zu erstellen. Sie müssen die Option Propagate to children auswählen, wenn Sie Berechtigungen für diese Benutzer-ID (VMCUser) hinzufügen. Zudem ist es möglicherweise sinnvoll, dieser Rolle zusätzliche Berechtigungen für weitere Tasks neben der Sicherung und Zurückschreibung hinzuzufügen. Für die Option VMCUser werden Berechtigungen beim Objekt der höchsten Ebene erzwungen.

Erforderliche vCenter-Serverberechtigungen für den Schutz von VMware-Datencentern mit der Sicht des IBM Spectrum Protect vSphere-Client-Plug-ins für die Data Protection for VMware vSphere-GUI

Für das IBM Spectrum Protect vSphere-Client-Plug-in werden separate Berechtigungen benötigt, die sich von den Berechtigungen für die Anmeldung bei der GUI unterscheiden.

Während der Installation werden die folgenden angepassten Berechtigungen für das IBM Spectrum Protect vSphere-Client-Plug-in erstellt:

- **Datencenter** > **IBM Data Protection**
- **Global** > **IBM Data Protection konfigurieren**

Angepasste Berechtigungen, die für das IBM Spectrum Protect vSphere-Client-Plug-in erforderlich sind, werden als separate Erweiterung registriert. Der Schlüssel für die Berechtigungserweiterung lautet com.ibm.tsm.tdpvmware.IBMDataProtection.privileges.

Mit diesen Berechtigungen kann der VMware-Administrator den Zugriff auf den Inhalt des IBM Spectrum Protect vSphere-Client-Plug-ins aktivieren und inaktivieren. Nur Benutzer, die über diese angepassten Berechtigungen für das erforderliche VMware-Objekt verfügen, können auf den Inhalt des IBM Spectrum Protect vSphere-Client-Plug-ins zugreifen. Ein einziges IBM Spectrum Protect vSphere-Client-Plug-in wird für jeden vCenter-Server registriert und von allen GUI-Hosts gemeinsam genutzt, die für die Unterstützung des vCenter-Servers konfiguriert sind.

Vom VMware vSphere-Web-Client aus müssen Sie eine Rolle für Benutzer erstellen, die Datenschutzfunktionen für virtuelle Maschinen mithilfe des IBM Spectrum Protect vSphere-Client-Plug-ins ausführen können. Für diese Rolle müssen Sie neben den Standardberechtigungen der Administratorrolle für virtuelle Maschinen, die der Web-Client erfordert, die Berechtigung **Datencenter** > **IBM Data Protection** angeben. Für jedes Datencenter ordnen Sie diese Rolle jedem Benutzer oder jeder Benutzergruppe zu, dem bzw. der Sie die Berechtigung zum Verwalten virtueller Maschinen erteilen möchten.

Die Berechtigung **Global** > **IBM Data Protection** ist auf der vCenter-Ebene für den Benutzer notwendig. Mit dieser Berechtigung kann der Benutzer die Verbindung zwischen dem vCenter-Server und dem Web-Server für die Data Protection for VMware vSphere-GUI verwalten, editieren oder löschen. Ordnen Sie diese Berechtigung Administratoren zu, die mit der Data Protection for VMware vSphere-GUI für den Schutz ihres jeweiligen vCenter-Servers vertraut sind. Verwalten Sie die Verbindungen des IBM Spectrum Protect vSphere-Client-Plug-ins auf der Seite **Verbindungen** der Erweiterung.

Das folgende Beispiel zeigt die Zugriffssteuerung zu Datencentern für zwei Benutzergruppen. Gruppe 1 benötigt Zugriff zum Verwalten virtueller Maschinen für die Datencenter `NewYork_DC` und `Boston_DC`. Gruppe 2 benötigt Zugriff zum Verwalten virtueller Maschinen für die Datencenter `LosAngeles_DC` und `SanFrancisco_DC`.

Erstellen Sie vom VMware vSphere-Client aus beispielsweise die Rolle „IBMDataProtectManage" und ordnen Sie dieser die Standardberechtigungen der Administratorrolle für virtuelle Maschinen sowie die Berechtigung **Datencenter** > **IBM Data Protection** zu.

Für Gruppe 1 ordnen Sie die Rolle „IBMDataProtectManage" den Datencentern `NewYork_DC` und `Boston_DC` zu. Für Gruppe 2 ordnen Sie die Rolle „IBMDataProtectManage" den Datencentern `LosAngeles_DC` und `SanFrancisco_DC` zu.

Die Benutzer in jeder Gruppe können mithilfe des IBM Spectrum Protect vSphere-Client-Plug-ins im vSphere-Web-Client nur virtuelle Maschinen in ihren jeweiligen Datencentern verwalten.

Probleme im Zusammenhang mit unzureichenden Berechtigungen

Wenn der Web-Browser-Benutzer für kein Datencenter über ausreichende Berechtigungen verfügt, ist der Zugriff auf die Sicht blockiert. Stattdessen wird die Fehlernachricht GVM2013E ausgegeben, um den Benutzer darüber zu informieren, dass aufgrund unzureichender Berechtigungen der Zugriff auf verwaltete Datencenter nicht möglich ist. Außerdem sind weitere neue Nachrichten verfügbar, die Benutzer über Probleme aufgrund unzureichender Berechtigungen informieren. Stellen Sie zum Beheben von Problemen mit Berechtigungen sicher, dass die Benutzerrolle wie in den obigen Abschnitten beschrieben eingerichtet ist. Die Benutzerrolle muss alle Berechtigungen haben, die in der Tabelle 'Erforderliche Berechtigungen für die

Benutzer-ID des vCenter-Servers und die Einheit zum Versetzen von Daten' angegeben sind, und diese Berechtigungen müssen mit dem Kontrollkästchen `Propagate to children` auf der Ebene des Datencenters angewendet werden.

Wenn der Benutzer des IBM Spectrum Protect vSphere-Client-Plug-ins nicht über ausreichende Berechtigungen für ein Datencenter verfügt, sind die Datenschutzfunktionen für dieses Datencenter und seinen Inhalt in der Erweiterung nicht verfügbar.

Wenn die Berechtigungen der IBM Spectrum Protect-Benutzer-ID (die durch die Option `VMCUser` angegeben ist) für eine Sicherungs- oder Zurückschreibungsoperation nicht ausreichen, wird die folgende Nachricht angezeigt:

```
ANS9365E VMware vStorage-API-Fehler.
"Die Berechtigung zum Ausführen dieser Operation wurde verweigert."
```

Wenn die Berechtigungen der IBM Spectrum Protect-Benutzer-ID zum Anzeigen einer Maschine nicht ausreichen, werden die folgenden Nachrichten angezeigt:

```
Befehl 'Backup VM' gestartet. Gesamtzahl zu verarbeitender VMs: 1
ANS4155E Virtuelle Maschine 'tango' konnte auf dem VMware-Server nicht gefunden werden.
ANS4148E Vollständige VM-Sicherung der virtuellen Maschine 'foxtrot' ist mit Rückkehrcode 4390 fehlg
```

Weitere Informationen zur Verwendung von Berechtigungen enthält der Hinweis in **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

Führen Sie die folgenden Schritte aus, um bei Berechtigungsproblemen Protokollinformationen über den VMware Virtual Center-Server abzurufen:

1. Im Fenster mit den **vCenter-Servereinstellungen** wählen Sie **Protokollierungsoptionen** aus und setzen Sie **vCenter-Protokollierung** auf **Trivia (Trivia)**.
2. Reproduzieren Sie den Berechtigungsfehler.
3. Setzen Sie **vCenter-Protokollierung** auf den vorherigen Wert zurück, um zu verhindern, dass sehr viele Protokollinformationen aufgezeichnet werden.
4. Suchen Sie im Fenster mit den **Systemprotokollen** das neueste vCenter-Serverprotokoll (`vpxd-`*`wxyz`*`.log`) und suchen Sie nach der Zeichenfolge `NoPermission`. Beispiel:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Diese Protokollnachricht gibt an, dass die Benutzer-ID nicht über ausreichende Berechtigungen zum Erstellen einer Momentaufnahme (`createSnapshot`) verfügte.

Benutzerrollen der Data Protection for VMware vSphere-GUI

Die Verfügbarkeit von Funktionen der Data Protection for VMware vSphere-GUI basiert auf der Berechtigungsstufe, die Ihrer IBM Spectrum Protect-Administrator-ID zugeordnet ist.

Die Administrator-ID muss mit dem Knotennamen übereinstimmen. In früheren Produktreleases wurde mit dem Befehl **REGISTER NODE** automatisch eine Benutzer-ID mit Administratorberechtigung erstellt, deren Name mit dem Knotennamen übereinstimmte. Ab IBM Spectrum Protect V8.1 wird mit dem Befehl **REGISTER NODE** nicht automatisch eine Benutzer-ID mit Administratorberechtigung erstellt, die mit dem Knotennamen übereinstimmt.

Bei der Registrierung eines neuen Knotens muss der IBM Spectrum Protect-Serveradministrator den Parameter `userid` mit dem Serverbefehl **REGISTER NODE** angeben:

```
REGISTER NODE Knotenname Kennwort userid=Benutzer-ID
```

Dabei müssen der Knotenname und die Benutzer-ID mit Administratorberechtigung identisch sein. Beispiel:

```
REGISTER NODE Knoten_a meinkennwort userid=Knoten_a
```

Standardmäßig verfügt der Knoten über die Clienteignerberechtigung.

Die Tasks, die Sie mit der Data Protection for VMware vSphere-GUI ausführen können, basieren auf der Berechtigungsklasse, die der Administrator-ID zugeordnet ist.

Wenn die Administrator-ID nicht über die Berechtigung für uneingeschränkte Maßnahmendomäne verfügt, können Sie keine neuen Knoten registrieren oder ihre Proxy-Beziehung auf dem IBM Spectrum Protect-Server definieren. Wenn Sie keine Administrator-ID eingeben, wird ein Makroscript erstellt, das auf dem IBM Spectrum Protect-Server ausgeführt werden kann.

Eine IBM Spectrum Protect-Administrator-ID wird bei der Konfiguration der Data Protection for VMware vSphere-GUI angefordert. In dieser Tabelle sind die Funktionen aufgelistet, die je nach der dieser ID zugeordneten Berechtigungsklasse verfügbar sind:

- Der Wert "Ja" gibt an, dass diese Funktion für die Benutzerrolle verfügbar ist.
- Der Wert "Nein" gibt an, dass diese Funktion nicht für die Benutzerrolle verfügbar ist.

Sie können Ihre aktuelle Data Protection for VMware vSphere-GUI-Rolle anzeigen, indem Sie den Cursor über Ihre Benutzer-ID in der Navigationsleiste bewegen.

Tabelle 11. Verfügbare Funktionen auf der Basis von Berechtigungsanforderungen für die IBM Spectrum Protect-Administrator-ID

	Bediener	**Bediener mit Berichterstellung**	**Eingeschränkter Administrator**	**Administrator**
Zusammenfassung	Sicherung jetzt ausführen und Zurückschreibung	Bediener plus Berichterstellung	Bediener plus Berichterstellung und Planungsoperationen für aufgelistete Maßnahmendomänen	Alle Rollen einschließlich Erstkonfiguration
IBM Spectrum Protect-Administrator-ID Berechtigungsklasse	Keine	Eine der folgenden Berechtigungsklassen: • Speicher • Bediener • Analytiker	Maßnahme (Eingeschränkt) oder eine der folgenden Berechtigungsklassen: • Speicher • Bediener • Analytiker	Maßnahme (Uneingeschränkt) oder System

Tabelle 11. Verfügbare Funktionen auf der Basis von Berechtigungsanforderungen für die IBM Spectrum Protect-Administrator-ID (Forts.)

	Bediener	Bediener mit Berichterstellung	Eingeschränkter Administrator	Administrator
Registerkarte 'Sichern'				
Sicherungstasks des Typs **Jetzt ausführen** steuern	Ja	Ja	Ja	Ja
Sicherungstasks des Typs **Geplant** steuern	Nein[1]	Nein[1]	Ja, innerhalb von Maßnahmendomänen	Ja
Sicherungstasks des Typs **Jetzt ausführen** anzeigen	Ja	Ja	Ja	Ja
Sicherungstasks des Typs **Geplant** anzeigen	Nein	Ja	Ja	Ja
Sicherungstask des Typs **Geplant** löschen	Nein	Nein	Ja, innerhalb von Maßnahmendomänen	Ja
Registerkarte 'Zurückschreiben'				
Task **Zurückschreiben** ausführen	Ja	Ja	Ja	Ja
Registerkarte 'Berichte'				
Ereignisse	Nein	Ja	Ja	Ja
Letzte Tasks	Ja	Ja	Ja	Ja
Sicherungsstatus	Nein	Ja	Ja	Ja
Anwendungsschutz	Nein	Ja	Ja	Ja
Datencenterbelegung	Nein	Ja	Ja	Ja
Registerkarte 'Konfiguration'				
Knotenregistrierung (**Konfigurationsstatus** -> **Konfigurationsassistenten ausführen**)	Nein	Nein	Nein[2]	Ja

Tabelle 11. Verfügbare Funktionen auf der Basis von Berechtigungsanforderungen für die IBM Spectrum Protect-Administrator-ID (Forts.)

	Bediener	Bediener mit Berichterstellung	Eingeschränkter Administrator	Administrator
IBM Spectrum Protect-Administrator-ID-Berechtigungsnachweise ändern (**Konfigurationsstatus -> Konfiguration editieren**)	Ja	Ja	Ja	Ja
Kennwort für VMCLI-Knoten ändern (**Konfigurationsstatus -> Konfiguration editieren**)	Nein	Nein	Ja	Ja
GUI-Domänen ändern (**Konfigurationsstatus -> Konfiguration editieren**)	Ja[3]	Ja[3]	Ja[3]	Ja
Knoten der Einheit zum Versetzen von Daten ändern (**Konfigurationsstatus -> Konfiguration editieren**)	Nein	Nein	Nein[2]	Ja
Mount-Proxy-Knoten ändern (**Konfigurationsstatus -> Konfiguration editieren**)	Nein	Nein	Nein[2]	Ja

1. Sie können den Knoten nicht registrieren, weil eine uneingeschränkte Maßnahmenberechtigung für die Domäne erforderlich ist.
2. Sie können VMware-Datencenter hinzufügen oder entfernen und Datencenterknoten registrieren.

Gehen Sie wie folgt vor, um die Berechtigungsstufe der IBM Spectrum Protect-Administrator-ID und die entsprechende Data Protection for VMware vSphere-GUI-Rolle anzuzeigen:

1. Rufen Sie das Fenster **Konfiguration** auf.
2. Klicken Sie auf **Konfiguration editieren**.
3. Die relevanten Informationen werden auf der Seite **Spectrum Protect-Serverberechtigungsnachweise** angezeigt.

Wichtig:

- Wenn die Berechtigungsstufe der IBM Spectrum Protect-Administrator-ID auf dem IBM Spectrum Protect-Server sich ändert, muss die Data Protection for VMware vSphere-GUI erneut gestartet werden, damit diese Änderung sich widerspiegelt.

- Wenn Sie die **Benutzerrolle** ändern, müssen Sie auf **OK** klicken, um Ihre Änderungen zu speichern, bevor Sie zu einer anderen Seite **Konfigurationseinstellungen** wechseln oder versuchen, eine weitere Konfigurationsänderung auszuführen. Andernfalls werden Ihre Änderungen an der **Benutzerrolle** nicht wirksam.

Registrierungsschlüssel für die Data Protection for VMware-GUI

Je nach den Optionen, die Sie während der Installation auswählen, können Sie mit verschiedenen Methoden auf die Data Protection for VMware-GUI zugreifen. Für die Data Protection for VMware-GUIs werden Registrierungsschlüssel erstellt.

Die Bezeichnung „Data Protection for VMware-GUI" bezieht sich auf die folgenden GUIs:

- Data Protection for VMware vSphere-GUI, auf die Sie in einem Web-Browser zugreifen
- IBM Spectrum Protect vSphere-Client-Plug-in in der vSphere-Web-Client-GUI

Der Registrierungsschlüssel für das IBM Spectrum Protect vSphere-Client-Plug-in lautet `com.ibm.tsm.tdpvmware.IBMDataProtection`. Dieser Schlüssel wird registriert, wenn Sie während der Installation das Kontrollkästchen **vSphere-Web-Client-Erweiterung registrieren** auswählen. Pro vCenter-Server wird eine einzige Instanz des IBM Spectrum Protect vSphere-Client-Plug-ins registriert.

Für die Data Protection for VMware vSphere-GUI mit Zugriff in einem Web-Browser wird kein Registrierungsschlüssel erstellt.

Zum Anzeigen der Registrierungsschlüssel melden Sie sich beim VMware Managed Object Browser (MOB) an. Nachdem Sie sich beim MOB angemeldet haben, rufen Sie **Content→Extension Manager** auf, um die Registrierungsschlüssel anzuzeigen.

Recovery Agent-GUI konfigurieren

Es werden Anweisungen zum Konfigurieren der Recovery Agent-GUI für Mount-, Dateizurückschreibungs- und Instant Restore-Operationen bereitgestellt.

Vorbereitende Schritte

Diese Konfigurationstasks müssen abgeschlossen sein, bevor in der Recovery Agent-GUI Operationen ausgeführt werden können.

Wichtig: Informationen zur Vorgehensweise bei der Ausführung von Tasks mit der Recovery Agent-GUI werden in der Onlinehilfe bereitgestellt, die mit der GUI installiert wird. Klicken Sie in einem beliebigen GUI-Fenster auf **Hilfe**, um die Onlinehilfe mit Informationen zur Ausführung von Tasks zu öffnen.

Vorgehensweise

1. Melden Sie sich bei dem System an, auf das Dateien zurückgeschrieben werden sollen. Recovery Agent muss auf dem System installiert sein.
2. Klicken Sie auf **TSM-Server auswählen** in der Recovery Agent-GUI, um eine Verbindung zu einem IBM Spectrum Protect-Server herzustellen. Wenn Recovery Agent auf demselben System wie die Data Protection for VMware vSphere-GUI installiert ist und die Anwendungen erfolgreich mit dem Konfigurationsassistenten der Data Protection for VMware vSphere-GUI konfiguriert wurden, herrschen die folgenden Bedingungen:

- Der Knoten der Einheit zum Versetzen von Daten und der IBM Spectrum Protect-Server sind im Recovery Agent-Feld **TSM-Server** ausgefüllt.
- Die folgenden Felder sind in der Anzeige **Tivoli Storage Manager-Serverinformationen** ausgefüllt:
  - **Authentifizierungsknoten** enthält eine Liste der verfügbaren Knoten der Einheit zum Versetzen von Daten.
  - **Zielknoten** enthält eine Liste der Datencenterknoten, die für den ausgewählten Knoten der Einheit zum Versetzen von Daten verfügbar sind.

Wenn nur ein einziger Knoten der Einheit zum Versetzen von Daten lokal mit dem Konfigurationsassistenten definiert wurde, verwendet Recovery Agent beim Starten diesen Knoten für die Authentifizierung.Recovery Agent speichert den letzten Knotennamen, der mit dem IBM Spectrum Protect-Server verbunden wurde. Wenn für diesen Knoten (den letzten verbundenen Knotennamen) **Kennwortzugriff 'generate' verwenden** ausgewählt wird, verwendet Recovery Agent beim Starten diese Berechtigungsnachweise zum Verbinden mit dem IBM Spectrum Protect-Server. Wenn es keine vorherige Verbindung zum IBM Spectrum Protect-Server gibt und mit dem Assistenten nur ein Knoten zum Versetzen von Daten und ein Datencenterknoten konfiguriert wurden, verwendet Recovery Agent beim Starten diese Berechtigungsnachweise zum Verbinden mit dem IBM Spectrum Protect-Server.

Geben Sie die folgenden Optionen an:

Serveradresse
Geben Sie die IP-Adresse oder den Hostnamen des IBM Spectrum Protect-Servers ein.

Server-Port
Geben Sie die Portnummer ein, die für die TCP/IP-Kommunikation mit dem Server verwendet wird. Die Standardportnummer ist 1500.

Knotenzugriffsmethode:

Als Knotenname
Wählen Sie diese Option aus, um einen Proxy-Knoten für den Zugriff auf die VM-Sicherungen zu verwenden, die sich auf dem Zielknoten befinden. Der Proxy-Knoten ist ein Knoten, dem "Proxy"-Berechtigung für die Ausführung von Operationen für den Zielknoten erteilt wird.

Normalerweise verwendet der IBM Spectrum Protect-Administrator den Befehl `grant proxynode`, um die Proxy-Beziehung zwischen zwei vorhandenen Knoten zu erstellen.

Wenn Sie diese Option auswählen, führen Sie die folgenden Schritte aus:

a. Geben Sie den Namen des Zielknotens (der Knoten, auf dem sich die VM-Sicherungen befinden) in das Feld **Zielknoten** ein.
b. Geben Sie den Namen des Proxy-Knotens in das Feld **Authentifizierungsknoten** ein.
c. Geben Sie das Kennwort für den Proxy-Knoten in das Feld **Kennwort** ein.
d. Klicken Sie auf **OK**, um diese Einstellungen zu speichern und den IBM Spectrum Protect-Informationsdialog zu verlassen.

Bei Verwendung dieser Methode kennt der Benutzer von Recovery Agent nur das Kennwort des Proxy-Knotens; das Kennwort des Zielknotens ist geschützt.

Von Knoten

Wählen Sie diese Option aus, um einen Knoten zu verwenden, dessen Zugriff auf die Momentaufnahmedaten von bestimmten virtuellen Maschinen auf dem Zielknoten begrenzt ist.

Normalerweise wird diesem Knoten mit dem Befehl `set access` von dem Zielknoten Zugriff erteilt, der Eigner der VM-Sicherungen ist:

```
set access backup -TYPE=VM VM-Anzeigenname Mountknotenname
```

Der folgende Befehl erteilt zum Beispiel dem Knoten mit dem Namen `MeinMountknoten` die Berechtigung zum Zurückschreiben von Dateien von der virtuellen Maschine mit dem Namen `MeineTestVM`:

```
set access backup -TYPE=VM MeineTestVM MeinMountknoten
```

Wenn Sie diese Option auswählen, führen Sie die folgenden Schritte aus:

a. Geben Sie den Namen des Zielknotens (der Knoten, auf dem sich die VM-Sicherungen befinden) in das Feld **Zielknoten** ein.
b. Geben Sie den Namen des Knotens, dem begrenzter Zugriff erteilt wird, in das Feld **Authentifizierungsknoten** ein.
c. Geben Sie das Kennwort für den Knoten, dem begrenzter Zugriff erteilt wird, in das Feld **Kennwort** ein.
d. Klicken Sie auf **OK**, um diese Einstellungen zu speichern und den IBM Spectrum Protect-Informationsdialog zu verlassen.

Mit dieser Methode können Sie eine vollständige Liste der gesicherten virtuellen Maschinen anzeigen. Sie können jedoch nur die VM-Sicherungen zurückschreiben, für die dem Knoten der Zugriff erteilt wurde. Außerdem sind die Momentaufnahmedaten nicht vor dem Verfall auf dem Server geschützt. Instant Restore wird bei dieser Methode daher nicht unterstützt.

Direkt Wählen Sie diese Option aus, um sich direkt mit dem Zielknoten zu authentifizieren (der Knoten, auf dem sich die VM-Sicherungen befinden).

Wenn Sie diese Option auswählen, führen Sie die folgenden Schritte aus:

a. Geben Sie den Namen des Zielknotens (der Knoten, auf dem sich die VM-Sicherungen befinden) in das Feld **Authentifizierungsknoten** ein.
b. Geben Sie das Kennwort für den Zielknoten in das Feld **Kennwort** ein.
c. Klicken Sie auf **OK**, um diese Einstellungen zu speichern und den IBM Spectrum Protect-Informationsdialog zu verlassen.

Kennwortzugriff 'generate' verwenden

Wenn diese Option ausgewählt und das Kennwortfeld leer ist, authentifiziert sich Recovery Agent mit einem bestehenden Kennwort, das in der Registry gespeichert ist. Wenn sie nicht ausgewählt ist, müssen Sie das Kennwort manuell eingeben.

Damit Sie diese Option verwenden können, müssen Sie zunächst manuell ein Anfangskennwort für den Knoten festlegen, auf den die Option angewendet werden soll. Sie müssen das Anfangskennwort angeben, wenn Sie erstmals eine Verbindung zum IBM Spectrum Protect-Knoten

herstellen, indem Sie das Kennwort in das Feld **Kennwort** eingeben und das Kontrollkästchen **Kennwortzugriff 'generate' verwenden** auswählen.

Wenn Sie jedoch den lokalen Knoten der Einheit zum Versetzen von Daten als **Authentifizierungsknoten** verwenden, ist das Kennwort möglicherweise bereits in der Registry gespeichert. Wählen Sie deshalb das Kontrollkästchen **Kennwortzugriff 'generate' verwenden** aus und geben Sie kein Kennwort ein.

Recovery Agent fragt den angegebenen Server nach einer Liste der geschützten virtuellen Maschinen ab und zeigt die Liste an.

3. Definieren Sie die folgenden Mount-, Sicherungs- und Zurückschreibungsoptionen durch Klicken auf **Einstellungen**:

Schreibcache des virtuellen Datenträgers
Der Recovery Agent, der auf dem Windows-Sicherungsproxy-Host ausgeführt wird, speichert Datenänderungen, die während eines Instant Restore und Mounts erstellt werden. Diese Änderungen werden auf einem virtuellen Datenträger im Schreibcache gespeichert. Standardmäßig ist der Schreibcache aktiviert und gibt den Pfad `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\` an. Die maximale Cachegröße beträgt 90 % des verfügbaren Speicherplatzes für den ausgewählten Ordner. Um zu verhindern, dass der Systemdatenträger voll wird, ändern Sie den Schreibcache in einen Pfad, der sich auf einem anderen Datenträger als dem Systemdatenträger befindet.

Ordner für temporäre Dateien
Geben Sie den Pfad an, in dem Datenänderungen gespeichert werden. Der Schreibcache muss sich auf einem lokalen Laufwerk befinden und darf keinen Pfad zu einem gemeinsam genutzten Ordner haben. Wenn der Schreibcache inaktiviert oder voll ist, schlägt der Versuch fehl, eine Instant Restore- oder Mountsitzung zu starten.

Cachegröße
Geben Sie die Größe des Schreibcache an. Die maximal zulässige Cachegröße beträgt 90 % des verfügbaren Speicherplatzes für den ausgewählten Ordner.

Einschränkung: Schließen Sie den Pfad des Schreibcache bei allen Zugriffsschutzeinstellungen von Antivirensoftwareprogrammen aus, um jegliche Unterbrechungen während der Zurückschreibungsverarbeitung zu verhindern.

Datenzugriff
Geben Sie den Typ der Daten an, auf die zugegriffen werden soll. Wenn Sie eine Offlineeinheit verwenden (z. B. ein Band oder ein virtuelles Bandarchiv), müssen Sie den entsprechenden Datentyp angeben.

Speichertyp
Geben Sie eine der folgenden Speichereinheiten an, von der die Momentaufnahme bereitgestellt werden soll:

Platte/Datei
Die Momentaufnahme wird von einer Platte oder einer Datei bereitgestellt. Diese Einheit ist der Standardwert.

Band Die Momentaufnahme wird von einem Bandspeicherpool bereitgestellt. Wenn diese Option ausgewählt wird,

ist es nicht möglich, mehrere Momentaufnahmen bereitzustellen oder eine Instant Restore-Operation auszuführen.

VTL Die Momentaufnahme wird aus einem virtuellen Offline-Bandarchiv bereitgestellt. Parallele Mountsitzungen für dasselbe virtuelle Bandarchiv werden unterstützt.

Anmerkung: Wenn der Speichertyp geändert wird, müssen Sie den Service erneut starten, damit die Änderungen wirksam werden.

Verfallsschutz inaktivieren
Während einer Mountoperation wird die Momentaufnahme auf dem IBM Spectrum Protect-Server gesperrt, um zu verhindern, dass sie während der Operation verfällt. Ein Verfall ist möglich, weil der bereitgestellten Momentaufnahmefolge eine weitere Momentaufnahme hinzugefügt wird. Dieser Wert gibt an, ob der Verfallsschutz während der Mountoperation inaktiviert werden soll.

- Wenn die Momentaufnahme vor dem Verfall geschützt werden soll, wählen Sie diese Option nicht aus. Die Momentaufnahme auf dem IBM Spectrum Protect-Server wird gesperrt und die Momentaufnahme ist während der Mountoperation vor dem Verfall geschützt.
- Wählen Sie diese Option aus, um den Verfallsschutz zu inaktivieren. Diese Option ist standardmäßig ausgewählt. Die Momentaufnahme auf dem IBM Spectrum Protect-Server wird nicht gesperrt und die Momentaufnahme ist nicht vor dem Verfall während der Mountoperation geschützt. Die Folge ist, dass die Momentaufnahme während der Mountoperation verfallen kann. Dieser Verfall kann zu nicht erwarteten Ergebnissen führen und den Mountpunkt beeinträchtigen. Der Mountpunkt kann beispielsweise nicht mehr verwendbar sein oder Fehler enthalten. Der Verfall wirkt sich jedoch nicht auf die aktuell aktive Kopie aus. Die aktive Kopie kann während einer Operation nicht verfallen.

  Wenn die Momentaufnahme auf einem Zielreplikationsserver gespeichert ist, kann sie nicht gesperrt werden, weil sie sich im Lesezugriffsmodus befindet. Ein Sperrversuch durch den Server bewirkt, dass die Mountoperation fehlschlägt. Inaktivieren Sie den Verfallsschutz durch Auswahl dieser Option, um den Sperrversuch und diesen Fehlschlag zu verhindern.

Größe für Vorauslesen (in 16-KB-Blöcken)
Geben Sie die Anzahl zusätzlicher Datenblöcke an, die von der Speichereinheit abgerufen werden, nachdem eine Leseanforderung an einen einzelnen Block gesendet wurde. Die Standardwerte lauten wie folgt:

- Platte oder Datei: 64
- Band: 1024
- VTL: 64

Der Maximalwert für alle Einheiten ist 1024.

Cachegröße für Vorauslesen (in Blöcken)
Geben Sie die Größe des Cache an, in dem die zusätzlichen Datenblöcke gespeichert werden. Die Standardwerte lauten wie folgt:

- Platte oder Datei: 10.000
- Band: 75.000
- VTL: 10.000

Da jede Momentaufnahme einen eigenen Cache hat, müssen Sie unbedingt planen, wie viele Momentaufnahmen gleichzeitig bereitgestellt oder zurückgeschrieben werden. Die kumulative Cachegröße kann 75.000 Blöcke nicht überschreiten.

Zeitlimit für Treiber (Sekunden)
Dieser Wert gibt die Zeit für die Verarbeitung der Datenanforderungen vom Dateisystemtreiber an. Wird die Verarbeitung nicht rechtzeitig beendet, wird die Anforderung abgebrochen und ein Fehler an den Dateisystemtreiber zurückgegeben. Ziehen Sie die Erhöhung dieses Werts in Betracht, wenn Zeitlimitüberschreitungen auftreten. Zeitlimitüberschreitungen können beispielsweise auftreten, wenn das Netz langsam ist, die Speichereinheit ausgelastet ist oder mehrere Mount- oder Instant Restore-Sitzungen verarbeitet werden. Die Standardwerte lauten wie folgt:

- Platte oder Datei: 60
- Band: 180
- VTL: 60

Klicken Sie auf **OK**, um Ihre Änderungen zu sichern und die **Einstellungen** zu verlassen.

4. Stellen Sie sicher, dass jeder IBM Spectrum Protect-Serverknoten (der mit den Optionen `Als Knotenname` und `Von Knoten` angegeben wurde) das Löschen von Sicherungen zulässt. Recovery Agent erstellt während Operationen nicht verwendete temporäre Objekte. Diese Objekte können mit der Serveroption `BACKDELete=Yes` entfernt werden, damit sie sich nicht auf dem Knoten anhäufen.
   a. Melden Sie sich beim IBM Spectrum Protect-Server an und starten Sie eine Verwaltungsclientsitzung im Befehlszeilenmodus:
      ```
      dsmadmc -id=admin -password=admin -dataonly=yes
      ```
   b. Geben Sie diesen Befehl ein:
      ```
      Query Node <Knotenname> Format=Detailed
      ```
      Stellen Sie sicher, dass die Befehlsausgabe für jeden Knoten die folgende Anweisung enthält:
      ```
      Sicherung löschen?: Ja
      ```
      Wenn diese Anweisung nicht eingeschlossen ist, aktualisieren Sie jeden Knoten mit diesem Befehl:
      ```
      UPDate Node <Knotenname> BACKDELete=Yes
      ```
      Führen Sie den Befehl `Query Node` für jeden Knoten erneut aus, um sicherzustellen, dass jeder Knoten das Löschen von Sicherungen zulässt.

5. Wenn Sie den Recovery Agent in einem iSCSI-Netz einsetzen und der Recovery Agent keine Einheit zum Versetzen von Daten verwendet, rufen Sie die Datei `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` auf und geben Sie den Tag `[IMOUNT]` und den Parameter **`Target IP`** an:

   ```
   [IMOUNT config]
   Target IP=<IP-Adresse der Netzkarte auf dem System,
   das die iSCSI-Ziele verfügbar macht>
   ```

   Beispiel:

   ```
   [Allgemeine config]
   Param1
   Param2
   ...
   [IMount config]
   Target IP=9.11.153.39
   ```

   Nach der Hinzufügung oder Änderung des Parameters 'Target IP' starten Sie die Recovery Agent-GUI oder Recovery Agent-CLI erneut.

Sichere Kommunikation zwischen Recovery Agent und dem IBM Spectrum Protect-Server aktivieren

Wenn der IBM Spectrum Protect-Server für die Verwendung des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) konfiguriert ist, können Sie Recovery Agent für die Kommunikation mit dem Server über dieses Protokoll aktivieren.

Vorbereitende Schritte

Beachten Sie die folgenden Voraussetzungen, bevor Sie die Konfiguration für sichere Kommunikation mit dem Server starten:

- Jeder Server, der für SSL aktiviert ist, muss über ein eindeutiges Zertifikat verfügen. Bei dem Zertifikat kann es sich um einen der folgenden Typen handeln:
  - Ein vom Server selbst signiertes Zertifikat.
  - Ein Zertifikat, das von einer unabhängigen Zertifizierungsstelle (Certificate Authority - CA) ausgestellt wurde. Das CA-Zertifikat kann von einem Unternehmen wie Symantec oder Thawte stammen oder ein internes Zertifikat sein, das innerhalb Ihres Unternehmens verwaltet wird.
- Unter Leistungsaspekten empfiehlt es sich, SSL oder TLS nur für Sitzungen zu verwenden, in denen Sicherheit erforderlich ist. Ziehen Sie die Hinzufügung weiterer Prozessorressourcen auf dem Serversystem für die höheren Anforderungen in Betracht.
- Damit ein Client eine Verbindung zu einem Server herstellen kann, der TLS Version 1.2 verwendet, muss der Algorithmus der Zertifikatssignatur Secure Hash Algorithm 1 (SHA-1) oder höher sein. Wenn Sie ein selbst signiertes Zertifikat für einen Server mit TSL V1.2 nutzen, müssen Sie das Zertifikat `cert256.arm` verwenden. Ihr IBM Spectrum Protect-Administrator muss möglicherweise das Standardzertifikat auf dem Server ändern.
- Fügen Sie die Option **`SSLDISABLELEGACYtls yes`** in der Datei `C:\windows\system32\fb.opt` oder `C:\Windows\SysWOW64\fb.opt` hinzu, um Sicherheitsprotokolle mit geringerer Sicherheit als TLS 1.2 zu inaktivieren. TLS 1.2 oder höher trägt dazu bei, Attacken durch böswillige Programme zu verhindern.

Sichere Kommunikation unter Verwendung eines selbst signierten Zertifikats des IBM Spectrum Protect-Servers aktivieren

Wenn der IBM Spectrum Protect-Server ein selbst signiertes Zertifikat verwendet, müssen Sie eine Kopie dieses Zertifikats beim Serveradministrator anfordern. Außerdem müssen Sie Recovery Agent für die Kommunikation mit dem Server unter Verwendung des SSL- oder TLS-Protokolls konfigurieren.

Informationen zu diesem Vorgang

Jeder Server generiert ein eigenes Zertifikat. Server mit Version 6.3 und höher generieren Dateien mit dem Namen `cert256.arm`, wenn der Server TLS 1.2 oder höher verwendet, oder `cert.arm`, wenn der Server eine frühere Version von SSL oder TLS verwendet. Server mit früheren Versionen als Version 6.3 generieren Dateien mit dem Namen `cert.arm` unabhängig vom Protokoll. Sie müssen das Zertifikat auswählen, das als Standardwert auf dem Server definiert ist.

Die Zertifikatsdatei wird auf der Server-Workstation im Serverinstanzverzeichnis gespeichert. Beispiel: `C:\IBM\tivoli\tsm\server\bin\cert256.arm`. Ist die Zertifikatsdatei nicht vorhanden, wird sie erstellt, wenn diese Optionen angegeben sind und der Server erneut gestartet wird.

Vorgehensweise

Gehen Sie wie folgt vor, um die SSL- oder TLS-Kommunikation zwischen Recovery Agent und Server unter Verwendung eines selbst signierten Zertifikats zu aktivieren:

1. Hängen Sie den GSKit-Binärpfad und den Bibliothekspfad an die Umgebungsvariable PATH auf dem Client an. Beispiel:

   ```
   set PATH=C:\Programme\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Programme\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. Wenn Sie SSL oder TLS zum ersten Mal auf dem Client konfigurieren, müssen Sie die lokale Schlüsseldatenbank des Clients, dsmcert.kdb, erstellen. Führen Sie im Verzeichnis `C:\Windows\SysWOW64` den Befehl **gsk8capicmd_64** aus, wie im folgenden Beispiel dargestellt:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw Kennwort -stash
   ```

   Das Kennwort, das Sie bereitstellen, wird zur Verschlüsselung der Schlüsseldatenbank verwendet. Das Kennwort wird automatisch in verschlüsselter Form in der Stashdatei (dsmcert.sth) gespeichert. Die Stashdatei wird vom Client zum Abrufen des Kennworts für die Schlüsseldatenbank verwendet.

3. Fordern Sie das selbst signierte Serverzertifikat an.
4. Importieren Sie das Zertifikat in die Datenbank dsmcert.kdb. Sie müssen das Zertifikat für jeden Client in dsmcert.kdb importieren. Führen Sie im Verzeichnis `C:\Windows\SysWOW64` den Befehl **gsk8capicmd_64** aus, wie im folgenden Beispiel dargestellt:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Selbst signierter Schlüssel des Servers Servername"
   -file Pfad_zu_Zertifikat -format ascii -trust enable
   ```

   Der Datenbank dsmcert.kdb können mehrere Serverzertifikate hinzugefügt werden, sodass der Client eine Verbindung zu verschiedenen Servern herstellen kann. Die Bezeichnungen für verschiedene Zertifikate müssen unterschiedlich sein. Verwenden Sie aussagekräftige Namen für die Bezeichnungen.

Wichtig: Damit die Wiederherstellung des Servers nach einem Katastrophenfall möglich ist, generiert der Server automatisch ein neues Zertifikat, wenn das Zertifikat nicht mehr vorhanden ist. Auf jedem Client muss dann das neue Zertifikat importiert werden.

5. Nachdem das Serverzertifikat der Datenbank dsmcert.kdb hinzugefügt wurde, fügen Sie die Option `ssl yes` der Datei `C:\Windows\SysWOW64\fb.opt` hinzu und aktualisieren Sie den Wert der Option `tcpport`.

   Wichtig:

   Der Server ist normalerweise so konfiguriert, dass für SSL- und TLS-Verbindungen ein anderer Port als für Nicht-SSL- und Nicht-TLS-Verbindungen verwendet wird. Geben Sie keine Nicht-SSL- oder Nicht-TLS-Portnummer als Wert für die Option `tcpport` an. Wenn der Wert für `tcpport` falsch ist, kann Recovery Agent keine Verbindung zum Server herstellen.

   Mit einem Recovery Agent, der für SSL oder TLS aktiviert ist, können Sie keine Verbindung zu einem Nicht-SSL- oder Nicht-TLS-Port herstellen. Ebenso können Sie mit einem Recovery Agent, der nicht für SSL oder TLS aktiviert ist, keine Verbindung zu einem SSL- oder TLS-Port herstellen.

6. Definieren Sie die korrekten SSL- oder TLS-Ports in den folgenden Recovery Agent-Konfigurationsdateien:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Sichere Kommunikation unter Verwendung eines Zertifikats eines Drittanbieters aktivieren

Wenn der IBM Spectrum Protect-Server eine unabhängige Zertifizierungsstelle (Certificate Authority - CA) verwendet, müssen Sie das CA-Stammzertifikat anfordern.

Informationen zu diesem Vorgang

Wenn das Zertifikat von einer Zertifizierungsstelle wie Symantec oder Thawte ausgestellt wurde, ist der Client für SSL oder TLS bereit und Sie können die folgenden Konfigurationsschritte überspringen. Eine Liste der vorinstallierten CA-Stammzertifikate finden Sie, wenn Sie im IBM Knowledge Center nach **Stammzertifikate von Zertifizierungsstellen** suchen.

Wenn das Zertifikat nicht von einem vorinstallierten Stammzertifikat ausgestellt wurde oder ein internes CA-Zertifikat ist, das innerhalb Ihres Unternehmens verwaltet wird, müssen Sie Recovery Agent für die Kommunikation mit dem Server unter Verwendung des SSL- oder TLS-Protokolls konfigurieren.

Vorgehensweise

Gehen Sie wie folgt vor, um die SSL- oder TLS-Kommunikation zwischen Recovery Agent und Server unter Verwendung eines CA-Zertifikats zu aktivieren:

1. Hängen Sie den GSKit-Binärpfad und den Bibliothekspfad an die Umgebungsvariable PATH an. Beispiel:

```
set PATH=C:\Programme\Common Files\Tivoli\TSM\api64\gsk8\bin\;
    C:\Programme\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```

2. Wenn Sie SSL oder TLS zum ersten Mal auf dem Client konfigurieren, müssen Sie die lokale Schlüsseldatenbank des Clients, dsmcert.kdb, erstellen. Führen Sie für Clients im Verzeichnis `C:\Windows\SysWOW64` den Befehl **gsk8capicmd_64** aus, wie im folgenden Beispiel dargestellt:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw Kennwort -stash
   ```

   Das Kennwort, das Sie bereitstellen, wird zur Verschlüsselung der Schlüsseldatenbank verwendet. Das Kennwort wird automatisch in verschlüsselter Form in der Stashdatei (dsmcert.sth) gespeichert. Die Stashdatei wird vom Client zum Abrufen des Kennworts für die Schlüsseldatenbank verwendet.
3. Fordern Sie das CA-Zertifikat an.
4. Importieren Sie das Zertifikat in die Datenbank dsmcert.kdb. Sie müssen das Zertifikat für jeden Client in dsmcert.kdb importieren. Führen Sie für Clients im Verzeichnis `C:\Windows\SysWOW64` den Befehl **gsk8capicmd_64** aus, wie im folgenden Beispiel dargestellt:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Zertifizierungsstelle XYZ"
   -file Pfad_zu_CA-Stammzertifikat -format ascii -trust enable
   ```

   Der Datenbank dsmcert.kdb können mehrere Serverzertifikate hinzugefügt werden, sodass der Client eine Verbindung zu verschiedenen Servern herstellen kann. Die Bezeichnungen für verschiedene Zertifikate müssen unterschiedlich sein. Verwenden Sie aussagekräftige Namen für die Bezeichnungen.

   Wichtig: Damit die Wiederherstellung des Servers nach einem Katastrophenfall möglich ist, generiert der Server automatisch ein neues Zertifikat, wenn das Zertifikat nicht mehr vorhanden ist. Auf jedem Client muss dann das neue Zertifikat importiert werden.
5. Nachdem das Serverzertifikat der Datenbank dsmcert.kdb hinzugefügt wurde, fügen Sie die Option `ssl yes` der Datei `C:\Windows\SysWOW64\fb.opt` hinzu und aktualisieren Sie den Wert der Option `tcpport`.

   Wichtig:

   Der Server ist normalerweise so konfiguriert, dass für SSL- und TLS-Verbindungen ein anderer Port als für Nicht-SSL- und Nicht-TLS-Verbindungen verwendet wird. Geben Sie keine Nicht-SSL- oder Nicht-TLS-Portnummer als Wert für die Option `tcpport` an. Wenn der Wert für `tcpport` falsch ist, kann Recovery Agent keine Verbindung zum Server herstellen.

   Mit einem Recovery Agent, der für SSL oder TLS aktiviert ist, können Sie keine Verbindung zu einem Nicht-SSL- oder Nicht-TLS-Port herstellen. Ebenso können Sie mit einem Recovery Agent, der nicht für SSL oder TLS aktiviert ist, keine Verbindung zu einem SSL- oder TLS-Port herstellen.
6. Definieren Sie die korrekten SSL- oder TLS-Ports in den folgenden Recovery Agent-Konfigurationsdateien:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Ländereinstellungen

Ländereinstellungen geben die Sprache an, die für Schnittstellen, Nachrichten und Onlinehilfe verwendet wird.

Data Protection for VMware-GUIs

Die Bezeichnung „Data Protection for VMware-GUI" bezieht sich auf die folgenden GUIs:

- Data Protection for VMware vSphere-GUI, auf die Sie in einem Web-Browser zugreifen
- IBM Spectrum Protect vSphere-Client-Plug-in in der vSphere-Web-Client-GUI

Die Data Protection for VMware-GUIs unterstützen nicht die Ausführung in einer Umgebung, in der die Ländereinstellungen auf den Prozessoren für die Ausführung der folgenden Komponenten inkonsistent sind: der Data Protection for VMware-GUI, des VMware vSphere-Clients und des IBM Spectrum Protect-Servers.

Geben Sie dieselbe Ländereinstellung auf den Systemen an, die die Data Protection for VMware-GUI, den VMware vSphere-Client und den IBM Spectrum Protect-Server ausführen.

Beim ersten Zugriff auf eine Hilfetextseite für eine Data Protection for VMware-GUI über den Link zu weiteren Informationen wird der Hilfetext in der Sprache angezeigt, die durch die Ländereinstellung des Systems angegeben wird, das die Data Protection for VMware-GUI ausführt. Beim ersten Zugriff auf die Hilfe wird der Hilfetext nicht in der Sprache angezeigt, die durch die Ländereinstellung des VMware vSphere-Clients angegeben wird. In dieser Situation klicken Sie auf mindestens zwei Links innerhalb der Hilfe, nachdem die Hilfetextseite für die Data Protection for VMware-GUI angezeigt wird, und schließen Sie anschließend die Hilfe. Beim nächsten Start der Hilfe über den Link zu weiteren Informationen wird der Hilfetext in der Sprache angezeigt, die durch die Ländereinstellung des VMware vSphere-Clients angegeben ist.

IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung

Die Sprache des Inhalts und der Nachrichten der Schnittstelle ist durch die Spracheinstellung des Web-Browsers festgelegt, der auf die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung zugreift.

Für Fehlernachrichten, die in der Datei `fr_api.log` protokolliert werden, verwendet die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung die Sprache, die durch die Ländereinstellung des Systems angegeben wird, das die Data Protection for VMware vSphere-GUI ausführt.

Protokolldateiaktivität

Data Protection for VMware erstellt und ändert mehrere Protokolldateien bei Installations-, Sicherungs-, Mount- und Zurückschreibungsoperationen.

Data Protection for VMware-Protokolldateien sind einfache Textdateien mit der Dateierweiterung `.sf`.

Windows Protokolle werden in dem folgenden Verzeichnis abgelegt:
`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`

Die Verzeichnisse enthalten für jede Data Protection for VMware-Komponente ein Unterverzeichnis. Das Unterverzeichnis für Recovery Agent ist beispielsweise `\mount`, das Unterverzeichnis für die Recovery Agent-Befehlszeilenschnittstelle heißt `\shell`.
Über das Menü **Windows** > **Start** können Sie nach Protokolldateien suchen. Wählen Sie hierzu die Optionen **Systemsteuerung** > **Suchen** aus und geben Sie `*.log` ein.

Linux Protokolle werden in den beiden folgenden Pfaden abgelegt:
`<Benutzerausgangsverzeichnis>/tivoli/tsm/ve/mount/log`
`/opt/tivoli/tsm/TDPVMware/mount/engine/var`
Sie können nach Protokolldateien suchen, indem Sie den folgenden Befehl eingeben:

```
find /opt/tivoli/ -name "*.log"
```

Wichtig: Bei jedem Start einer Installation werden vorhandene Protokolldateien überschrieben. Falls bei der Installation ein Problem auftritt und Sie das Produkt erneut installieren müssen, rufen Sie die vorhandene Datei `TDPVMwareInstallation.log` aus dem Verzeichnis `%allusersprofile%` ab, bevor Sie den Installationsversuch wiederholen.

Anmerkung: Während der Data Protection for VMware-Service aktiv ist, verbleiben mehrere Protokolldateien im geöffneten Status. Aus diesem Grund zeigen einige Dateimanager nicht den aktuellen Status dieser Dateien, sondern möglicherweise die Dateigröße null an. Das Auswählen oder Öffnen einer dieser Dateien erzwingt die Aktualisierung der Dateiinformationen durch den Dateimanager.

Recovery Agent-Protokolldateien

Die Recovery Agent-Protokolldatei ist `TDP_FOR_VMWARE_MOUNT`*`nnn`*`.sf`. Die Protokolldatei mit den aktuellsten Daten ist die mit der Nummer *040* gespeicherte Protokolldatei (`TDP_FOR_VMWARE_MOUNT040.sf`). Wenn eine Protokolldatei den Grenzwert für die maximale Größe erreicht, wird eine neue Protokolldatei erstellt. Der Protokolldateiname ist identisch, nur die Nummer der Protokolldatei wird um eins verringert. Das heißt, die Daten in der Protokolldatei mit der Nummer *040* werden in eine Protokolldatei mit der Nummer *039* kopiert. Die Protokolldatei mit der Nummer *040* enthält die neuesten Protokolldateidaten. Wenn die Datei mit der Nummer *040* erneut die maximale Dateigröße erreicht, wird der Inhalt der Datei mit der Nummer *039* in eine Datei mit der Nummer *038* kopiert und die Informationen in der Datei mit der Nummer *040* werden wieder in die Datei mit der Nummer *039* kopiert.

Protokolldateien der Data Protection for VMware-GUI

Die Data Protection for VMware vSphere-GUI stellt Protokolldateien in das folgende Verzeichnis:

Windows `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Achten Sie beim Zusammenstellen von Protokolldateien darauf, dass die komprimierte Datei alle Unterverzeichnisse enthält.

Data Protection for VMware-Befehlszeilenschnittstelle-Protokolldateien

Die Data Protection for VMware-Befehlszeilenschnittstelle legt Protokolldateien im folgenden Verzeichnis ab:

Windows `C:\Programme\IBM\SpectrumProtect\Framework\VEGUI\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/logs`

Achten Sie beim Zusammenstellen von Protokolldateien darauf, dass die komprimierte Datei alle Unterverzeichnisse enthält.

Protokolldateien der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung

Die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung protokolliert Fehlernachrichten in den Dateien `fr_api.log`, `fr_gui.log` und `messages.log`. Diese Dateien befinden sich in dem folgenden Standardverzeichnis:

Windows `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Sie können den Namen und die Position der Datei `fr_api.log` ändern, indem Sie die Optionen `API_LOG_FILE_NAME` und `API_LOG_FILE_LOCATION` in der Protokollaktivitätsdatei für die Dateizurückschreibung (`FRLog.config`) definieren.

Dateizurückschreibungsoperationen werden auch vom IBM Spectrum Protect-Server protokolliert. Sie können diese Nachrichten mit einem Verwaltungsbefehlszeilenclient des Servers durchsuchen.

- Geben Sie den folgenden Befehl an Ihrer Workstation ein, um eine Verwaltungsclientsitzung im Befehlszeilenmodus zu starten:

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  Wenn Sie den Befehl **DSMADMC** wie dargestellt mit den Optionen **-ID** und **-PASSWORD** eingeben, werden Sie nicht zur Eingabe einer Benutzer-ID und eines Kennworts aufgefordert.
- Wenn Sie die erweiterte SQL-Übersichtstabelle nach Ergebnissen zu Dateizurückschreibungsoperationen durchsuchen möchten, geben Sie den Befehl **select** auf dem Verwaltungsbefehlszeilenclient aus:

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  ```

  Sie können die Suche eingrenzen, indem Sie mindestens eines der folgenden Kriterien in die Anweisung SELECT einschließen:

  - `* ENTITY='`*`KNOTENNAME_DER_EINHEIT_ZUM_VERSETZEN_VON_DATEN`*`'`
  - `* AS_ENTITY='`*`DATENCENTERKNOTENNAME`*`'`
  - `* SUB_ENTITY='`*`VM-HOSTNAME`*`'`
  - `* START_TIME='`*`jjjj-MM-tt HH:mm:ss`*`'`

  Beispiel:

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
  and START_TIME>'2017-03-11 17:30:00'
  ```

  Das Kriterium `START_TIME` unterstützt Abfragen mit den folgenden Operatoren: gleich (=), kleiner als (<) oder größer als (>).

- Wenn Sie die SQL-Aktivitätenprotokolltabelle nach Ereignissen zu Dateizurückschreibungsoperationen durchsuchen möchten, geben Sie den Befehl **select** auf dem Verwaltungsbefehlszeilenclient aus:

  ```
  select * from ACTLOG
  ```

  Sie können die Suche eingrenzen, indem Sie mindestens eines der folgenden Kriterien in die Anweisung SELECT einschließen:

  – `* NODENAME='`*`DATENCENTERKNOTENNAME`*`'`

  – `* DATE_TIME='`*`jjjj-MM-tt HH:mm:ss`*`'`

  Beispiel:

  ```
  select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
  ```

Geben Sie *KNOTENNAME_DER_EINHEIT_ZUM_VERSETZEN_VON_DATEN* und *DATENCENTERKNOTENNAME* in Großbuchstaben an.

Das Kriterium `DATE_TIME` unterstützt Abfragen mit den folgenden Operatoren: gleich (=), kleiner als (<) oder größer als (>).

Services für Data Protection for VMware starten und ausführen

Standardmäßig wird Recovery Agent unter dem lokalen Systemkonto gestartet, wenn das Windows-Betriebssystem gestartet wird.

Recovery Agent-Services unter Microsoft Windows ausführen

Wenn Sie Recovery Agent über das Windows-Menü 'Start' starten, wird der Service automatisch gestoppt. Wenn Recovery Agent nach dem Start über das Menü 'Start' beendet wird, wird der Service automatisch gestartet. Außerdem stellt der Service für diese Betriebssysteme keine grafische Benutzerschnittstelle (GUI) zur Verfügung. Zur Verwendung der GUI rufen Sie das Windows-Menü 'Start' auf und wählen Sie **Alle Programme** > **IBM Spectrum Protect** > **Data Protection for VMware** > **Recovery Agent** aus.

Data Protection for VMware-Befehlszeilenschnittstelle

Mit der folgenden Task können Sie prüfen, ob die Data Protection for VMware-Befehlszeilenschnittstelle aktiv ist:

Windows Wählen Sie **Start** > **Systemsteuerung** > **Verwaltung** > **Dienste** aus und prüfen Sie, ob für `Data Protection for VMware-Befehlszeilenschnittstelle` der Status `Gestartet` angegeben ist.

Linux Wechseln Sie in das Verzeichnis scripts (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) und geben Sie den folgenden Befehl aus:

```
./vmclid status
```

- Ist der Dämon nicht aktiv, geben Sie den folgenden Befehl aus, um ihn manuell zu starten:

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  Zum Starten und Stoppen des Dämons können auch die folgenden INIT-Scripts verwendet werden:

  ```
  ./vmclid stop
  ./vmclid start
  ```

Anhang A. Erweiterte Konfigurationstasks

Sie müssen jede Komponente unter Verwendung der verfügbaren Anwendungsschnittstellen manuell konfigurieren und prüfen.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, bevor Sie mit dieser Task fortfahren:

- Für die Registrierung der Knoten muss ein IBM Spectrum Protect-Server verfügbar sein.
- Die Data Protection for VMware vSphere-GUI ist auf einem System installiert, das die Betriebssystemvoraussetzungen erfüllt. Zu den folgenden Systemen muss Netzkonnektivität bestehen:
  - vStorage-Sicherungsserver
  - IBM Spectrum Protect-Server
  - vCenter-Server

Vorgehensweise

1. Melden Sie sich beim IBM Spectrum Protect-Server an und führen Sie die Tasks aus, die unter „IBM Spectrum Protect-Knoten in einer vSphere-Umgebung definieren" auf Seite 96 beschrieben sind.
2. Melden Sie sich beim vStorage-Sicherungsserver an und führen Sie die Tasks aus, die unter „Knoten der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI definieren" auf Seite 97 beschrieben sind.
3. Melden Sie sich bei dem System an, auf dem die Data Protection for VMware vSphere-GUI installiert ist, und führen Sie die Tasks aus, die unter „Data Protection for VMware-Befehlszeilenschnittstelle in einer vSphere-Umgebung konfigurieren" auf Seite 104 beschrieben sind.
4. Starten Sie auf dem System, auf dem die Data Protection for VMware vSphere-GUI installiert ist, den vSphere-Client und melden Sie sich beim vCenter an. Falls der vSphere-Client bereits aktiv ist, müssen Sie ihn stoppen und erneut starten.
5. Wechseln Sie im vSphere-Client in das Ausgangsverzeichnis. Klicken Sie auf das Symbol für die Data Protection for VMware vSphere-GUI im Fenster für Lösungen und Anwendungen (Solutions and Applications).

   Tipp: Wird das Symbol nicht angezeigt, wurde die Data Protection for VMware vSphere-GUI nicht registriert oder es ist ein Verbindungsfehler aufgetreten.

   a. Rufen Sie im Menü des vSphere-Clients **Plug-ins** > **Manage Plug-ins (Plug-ins verwalten)** auf, um den Plug-in-Manager zu starten.
   b. Wenn Sie die Data Protection for VMware vSphere-GUI lokalisieren können und ein Verbindungsfehler aufgetreten ist, überprüfen Sie die Konnektivität zu der Maschine, auf der die Data Protection for VMware vSphere-GUI installiert ist. Geben Sie dazu den Befehl `ping` aus.

Ergebnisse

Die Data Protection for VMware vSphere-GUI ist nun für Sicherungs- und Zurückschreibungsoperationen bereit.

IBM Spectrum Protect-Knoten in einer vSphere-Umgebung definieren

In dieser Prozedur wird beschrieben, wie Sie in einer vSphere-Umgebung Knoten manuell beim IBM Spectrum Protect-Server registrieren und diesen Knoten die Proxy-Berechtigung erteilen.

Vorbereitende Schritte

Wichtig:

Informationen zu diesem Vorgang

Alle Schritte in dieser Prozedur werden auf dem IBM Spectrum Protect-Server ausgeführt.

Tipp: Diese Task kann auch mit dem Konfigurationsassistenten oder dem Notizbuch 'Konfiguration editieren' der Data Protection for VMware vSphere-GUI ausgeführt werden. Starten Sie die Data Protection for VMware vSphere-GUI, indem Sie einen Web-Browser öffnen und zum GUI-Web-Server wechseln. Beispiel:

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

Melden Sie sich mit dem vCenter-Benutzernamen und -Kennwort an.

- Navigieren Sie bei einer Erstkonfiguration zu **Konfiguration** > **Konfigurationsassistenten ausführen**.
- Navigieren Sie bei einer vorhandenen Konfiguration zu **Konfiguration** > **Konfiguration editieren**.

Vorgehensweise

1. Melden Sie sich beim IBM Spectrum Protect-Server an und starten Sie eine Verwaltungsclientsitzung im Befehlszeilenmodus:

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. Geben Sie den Befehl `REGister Node` aus, um die folgenden Knoten beim IBM Spectrum Protect-Server zu registrieren:
   a. Knoten, der das VMware vCenter darstellt (vCenter-Knoten):

      ```
      REGister Node MY_VCNODE <Kennwort für MY_VCNODE>
      ```

   b. Knoten für die Kommunikation zwischen IBM Spectrum Protect und der Data Protection for VMware vSphere-GUI (VMCLI-Knoten):

      ```
      REGister Node MY_VMCLINODE <Kennwort für MY_VMCLINODE>
      ```

   c. Knoten, der das Datencenter darstellt und auf dem die VM-Daten gespeichert werden (Datencenterknoten):

      ```
      REGister Node MY_DCNODE <Kennwort für MY_DCNODE>
      ```

   d. Knoten, der Daten von einem System auf ein anderes System 'versetzt' (Knoten der Einheit zum Versetzen von Daten):

      ```
      REGister Node MY_DMNODE <Kennwort für MY_DMNODE>
      ```

   Achtung: Verwenden Sie während der Registrierung von Knoten beim IBM Spectrum Protect-Server nicht den Parameter `userid`.
3. Geben Sie den Befehl `GRant PROXynode` aus, um die Proxy-Beziehungen für diese Knoten zu definieren:

Hinweis: Zielknoten sind Eigner der Daten. Agentenknoten können im Namen der Zielknoten agieren. Wenn einem Zielknoten die Proxyberechtigung erteilt wird, kann ein Agentenknoten Sicherungs- und Zurückschreibungsoperationen für den Zielknoten ausführen.

a. Erteilen Sie dem vCenter-Knoten die Proxyberechtigung, indem Sie den folgenden Befehl ausgeben:

   ```
   GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
   ```

   Dieser Befehl erteilt den Knoten MY_DCNODE und MY_VMCLINODE die Berechtigung, virtuelle Maschinen im Namen des Knotens MY_VCNODE zu sichern und zurückzuschreiben.

b. Erteilen Sie dem Datencenterknoten die Proxyberechtigung, indem Sie den folgenden Befehl ausgeben:

   ```
   GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
   ```

   Dieser Befehl erteilt den Knoten MY_VMCLINODE und MY_DMNODE die Berechtigung, virtuelle Maschinen im Namen des Knotens MY_DCNODE zu sichern und zurückzuschreiben.

c. (Optional) Erteilen Sie weiteren Datencenterknoten oder Knoten der Einheit zum Versetzen von Daten in Ihrer Umgebung die Proxyberechtigung.

d. Prüfen Sie die Proxy-Beziehungen, indem Sie den IBM Spectrum Protect-Serverbefehl Query PROXynode ausgeben. Die erwartete Befehlsausgabe lautet: Die erwartete Befehlsausgabe lautet:

   ```
   Target Node       Agent Node
   --------------    ------------------------------
   MY_VCNODE           MY_DCNODE  MY_VMCLINODE
   MY_DCNODE           MY_VMCLINODE  MY_DMNODE
   ```

Nächste Schritte

Nachdem Sie die IBM Spectrum Protect-Knoten erfolgreich definiert haben, müssen Sie in der nächsten manuellen Konfigurationstask die Knoten der Einheit zum Versetzen von Daten definieren. Dies ist im Abschnitt „Knoten der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI definieren" beschrieben.

Knoten der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI definieren

Wenn Sie in einer vSphere-Umgebung Sicherungsarbeitslast auf einen vStorage-Sicherungsserver auslagern, können Sie mit dem Assistenten für die Einheit zum Versetzen von Daten eine Reihe von Knoten der Einheit zum Versetzen von Daten definieren, damit die Operation ausgeführt wird und die Daten auf den IBM Spectrum Protect-Server versetzt werden.

Vorbereitende Schritte

Zum Definieren von Knoten der Einheit zum Versetzen von Daten müssen Sie die Konfiguration ändern, die erforderlichen Services starten und die Konfiguration überprüfen.

Sie können diese Tasks mit der Plug-in-GUI ausführen. Diese vereinfacht und beschleunigt die Erstellung einer Reihe von Knoten der Einheit zum Versetzen von Daten. Alternativ können Sie die Arbeit manuell ausführen. Weitere Informationen

dazu finden Sie in „Knoten der Einheit zum Versetzen von Daten in einer vSphere-Umgebung manuell definieren" auf Seite 99.

In einer Data Protection for VMware-Standardumgebung wird für jeden Knoten der Einheit zum Versetzen von Daten eine separate Datei `dsm.opt` (Windows) bzw. Zeilengruppe in der Datei `dsm.sys` (Linux) verwendet. Wenn mehrere Knoten der Einheit zum Versetzen von Daten auf einem vStorage-Sicherungsserver für die Datendeduplizierung verwendet werden und diese Knoten berechtigt sind, Daten für denselben Datencenterknoten zu versetzen, muss jede Datei `dsm.opt` bzw. jede Zeilengruppe in der Datei `dsm.sys` einen anderen Wert für die Option `dedupcachepath` aufweisen.

Ein physischer Knoten der Einheit zum Versetzen von Daten verwendet normalerweise das SAN, um Daten zu sichern und zurückzuschreiben. Falls Sie den Knoten der Einheit zum Versetzen von Daten für den direkten Zugriff auf die Speicherdatenträger konfigurieren, inaktivieren Sie die automatische Laufwerkzuordnung. Ist sie nicht inaktiviert, beschädigt der Client auf dem Knoten für die Einheit zum Versetzen von Daten möglicherweise das Raw Data Mapping (RDM) der virtuellen Platten. Falls das RDM der virtuellen Platten beschädigt ist, schlagen Sicherungen fehl.

Einschränkung: Data Protection for VMware unterstützt keine Zeitpläne, bei denen der vStorage-Sicherungsserver (der als Einheit zum Versetzen von Daten verwendet wird) sich selbst sichert. Stellen Sie sicher, dass der vStorage-Sicherungsserver aus seinen eigenen Zeitplänen ausgeschlossen ist. Verwenden Sie für die Sicherung einer virtuellen Maschine, die einen vStorage-Sicherungsserver enthält, einen anderen vStorage-Sicherungsserver.

Wenn Sie eine der oben genannten Anpassungen vornehmen müssen, lesen Sie das Thema "Knoten der Einheit zum Versetzen von Daten in einer vSphere-Umgebung manuell definieren".

Informationen zu diesem Vorgang

Verwenden Sie das vSphere-Plug-in, um die Knoten der Einheit zum Versetzen von Daten zu konfigurieren.

Vorgehensweise

1. Im vSphere-Plug-in wählen Sie IBM Spectrum Protect aus.
2. Auf der Registerkarte **Konfigurieren** wählen Sie **Einheiten zum Versetzen von Daten** aus.
3. In der Anzeige **Einheit zum Versetzen von Daten hinzufügen** wählen Sie im Dropdown-Menü ein Datencenter aus.
4. Editieren Sie die folgenden Felder nach Bedarf:
   - **Name der Einheit zum Versetzen von Daten**: Ein Knotenname, der bereits mit einem vorgeschlagenen Namen ausgefüllt ist. Der Vorschlag basiert auf dem Knotenpräfix, dem Datencenterknotennamen, dem Namen der Einheit zum Versetzen von Daten und einer sich erhöhenden Nummer.
   - **Hostname der Einheit zum Versetzen von Daten**
   - **vCenter-Benutzer**, bereits mit dem Namen des Benutzers ausgefüllt, der das Plug-in registriert hat.
   - **vCenter-Kennwort**

   Klicken Sie auf **Hinzufügen**, wenn die Einstellungen fertig sind.

5. In der Anzeige **Ergebnisse** wird Folgendes angezeigt:
   - Der Name der konfigurierten Einheit zum Versetzen von Daten.
   - Die Position der Optionsdatei. Sie können die Einheit zum Versetzen von Daten konfigurieren, indem Sie diese Datei editieren.
   - Die Position der Protokolldateien.
   - Die Standardoptionen, die verwendet wurden.
6. Sie können jetzt die Einheit zum Versetzen von Daten mithilfe der Registerkarte **IBM Spectrum Protect > Konfigurieren > Einheiten zum Versetzen von Daten** testen. Sie können die Installation auch überprüfen, indem Sie die Einheit zum Versetzen von Daten auswählen und auf die Option für Überprüfen klicken oder indem Sie bei der nächsten Hinzufügung einer Einheit zum Versetzen von Daten den Status prüfen.
7. Sie können die Einheit zum Versetzen von Daten einem Zeitplan hinzufügen, indem Sie die Registerkarte **IBM Spectrum Protect > Zeitpläne** verwenden.

Knoten der Einheit zum Versetzen von Daten in einer vSphere-Umgebung manuell definieren

Wenn Sie in einer vSphere-Umgebung Sicherungsarbeitslast auf einen vStorage-Sicherungsserver auslagern, können Sie manuell die Knoten der Einheit zum Versetzen von Daten definieren, damit die Operation ausgeführt wird und die Daten auf den IBM Spectrum Protect-Server versetzt werden.

Vorbereitende Schritte

Ein physischer Knoten der Einheit zum Versetzen von Daten verwendet normalerweise das SAN, um Daten zu sichern und zurückzuschreiben. Falls Sie Knoten der Einheit zum Versetzen von Daten für den direkten Zugriff auf die Speicherdatenträger konfigurieren, inaktivieren Sie die automatische Laufwerkzuordnung. Ist sie nicht inaktiviert, beschädigt der Client auf dem Knoten für die Einheit zum Versetzen von Daten möglicherweise das Raw Data Mapping (RDM) der virtuellen Platten. Falls das RDM der virtuellen Platten beschädigt ist, schlagen Sicherungen fehl.

Erforderliche Services: Für die Einheit zum Versetzen von Daten ist der Clientakzeptorservice, der ferne Clientagent-Service und der Scheduler-Service erforderlich, wie in den folgenden Schritten beschrieben. Wenn Sie eine Einheit zum Versetzen von Daten aus einem Datencenter entfernen, deinstallieren und löschen Sie diese Services für die Einheit zum Versetzen von Daten.

Wichtig: Ist die Einheit zum Versetzen von Daten auf demselben Windows-System wie die Data Protection for VMware vSphere-GUI installiert und wurde bei der Konfiguration der Einheit zum Versetzen von Daten **Services erstellen** ausgewählt, sind die folgenden Schritte nicht erforderlich.

In einer Data Protection for VMware-Standardumgebung wird für jeden Knoten der Einheit zum Versetzen von Daten eine separate Datei `dsm.opt` (Windows) bzw. Zeilengruppe in der Datei `dsm.sys` (Linux) verwendet. Wenn mehrere Knoten der Einheit zum Versetzen von Daten auf einem vStorage-Sicherungsserver für die Datendeduplizierung verwendet werden und diese Knoten berechtigt sind, Daten für denselben Datencenterknoten zu versetzen, muss jede Datei `dsm.opt` bzw. jede Zeilengruppe in der Datei `dsm.sys` einen anderen Wert für die Option `dedupcachepath` aufweisen. Die besten Ergebnisse werden erzielt, wenn Sie eine unterschiedliche

Option schedlogname und errorlogname für jede Datei dsm.opt bzw. für jede Zeilengruppe in der Datei dsm.sys angeben. Die Mindestgruppe der erforderlichen Optionen ist in Schritt 2 angegeben.

Ein physischer Knoten der Einheit zum Versetzen von Daten verwendet normalerweise das SAN, um Daten zu sichern und zurückzuschreiben. Falls Sie den Knoten der Einheit zum Versetzen von Daten für den direkten Zugriff auf die Speicherdatenträger konfigurieren, inaktivieren Sie die automatische Laufwerkzuordnung. Ist sie nicht inaktiviert, beschädigt der Client auf dem Knoten für die Einheit zum Versetzen von Daten möglicherweise das Raw Data Mapping (RDM) der virtuellen Platten. Falls das RDM der virtuellen Platten beschädigt ist, schlagen Sicherungen fehl.

Einschränkung: Data Protection for VMware unterstützt keine Zeitpläne, bei denen der vStorage-Sicherungsserver (der als Einheit zum Versetzen von Daten verwendet wird) sich selbst sichert. Stellen Sie sicher, dass der vStorage-Sicherungsserver aus seinen eigenen Zeitplänen ausgeschlossen ist. Verwenden Sie für die Sicherung einer virtuellen Maschine, die einen vStorage-Sicherungsserver enthält, einen anderen vStorage-Sicherungsserver.

Informationen zu diesem Vorgang

Tipp: Alle Schritte in dieser Prozedur werden auf dem vStorage-Sicherungsserver ausgeführt.

Vorgehensweise

1. Linux Stellen Sie sicher, dass die Java-Software auf der Zielmaschine installiert ist.
2. Linux Definieren Sie die relevanten Umgebungsvariablen.
   a. Stellen Sie sicher, dass die Umgebungsvariable JAVA_HOME korrekt exportiert wird:
      ```
      export JAVA_HOME=<Inst-Verz-für-jre-oder-jdk>
      ```
   b. Stellen Sie sicher, dass die Umgebungsvariable PATH korrekt exportiert wird:
      ```
      export PATH=$PATH:$JAVA_HOME/jre/bin
      ```
   c. Stellen Sie sicher, dass die Umgebungsvariable LD_LIBRARY_PATH korrekt exportiert wird. Überprüfen Sie, ob sie auf das Clientinstallationsverzeichnis und die gemeinsam genutzte Java-Bibliothek libjvm.so gesetzt ist bzw. definieren Sie sie entsprechend:

      Für IBM Java:
      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic
      ```
      Für Oracle Java:
      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server
      ```
3. Erstellen Sie die Optionsdatei dsm.opt oder dsm.sys an der folgenden Position:
   - **Windows:** C:\Programme\Tivoli\TSM\baclient
   - **Linux:** /opt/tivoli/tsm/client/ba/bin
4. Kopieren Sie die Optionen aus der Beispieloptionsdatei für die Einheit zum Versetzen von Daten in die Datei dsm.opt oder dsm.sys. Gehen Sie wie folgt vor, um die Beispieldatei für die Einheit zum Versetzen von Daten zu lokalisieren:
   - Öffnen Sie einen Web-Browser und geben Sie die Adresse des GUI-Web-Servers ein. Beispiel:
     ```
     https://guihost.mycompany.com:9081/TsmVMwareUI/
     ```

- Melden Sie sich mit dem vCenter-Benutzernamen und -Kennwort an und stellen Sie sicher, dass **Konfigurationsmodus** ausgewählt ist.
- Rufen Sie im Konfigurationsassistenten die Seite **Knoten der Einheit zum Versetzen von Daten** auf.
- Lokalisieren Sie die gewünschte Einheit zum Versetzen von Daten und klicken Sie auf **Anzeigen**.
- Kopieren Sie die Beispieloptionen aus der Registerkarte **Windows** oder **Linux** in die Optionsdatei.

Sie können diese Optionen bei Bedarf für Ihre Umgebung aktualisieren.

Eine Beschreibung der Optionen finden Sie in Optionsreferenz.

Stellen Sie für Instant Access-, Instant Restore- oder Mountoperationen (Dateizurückschreibungsoperationen) sicher, dass Sie der Optionsdatei der Einheit zum Versetzen von Daten die Option `VMISCSISERVERADDRESS` hinzufügen. Geben Sie die IP-Adresse der Netzkarte des iSCSI-Servers auf dem vStorage-Sicherungsserver an, die bei Instant-Operationen für die iSCSI-Datenübertragung verwendet wird. Die physische Netzschnittstellenkarte (NIC), die an die iSCSI-Einheit auf dem ESX-Host gebunden wird, muss sich in demselben Teilnetz wie die NIC auf dem vStorage-Sicherungsserver befinden, die für die iSCSI-Übertragung verwendet wird.

5. Geben Sie den folgenden Befehl aus, um den VMware vCenter-Benutzer und das zugehörige Kennwort für den Knoten der Einheit zum Versetzen von Daten festzulegen:

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <Administrator> <Kennwort1>
   ```

6. Führen Sie die folgenden Tasks aus, um den Clientakzeptorservice und den Scheduler-Service der Einheit zum Versetzen von Daten zu konfigurieren:

   - Windows Bei dieser Prozedur wird der Konfigurationsassistent der IBM Spectrum Protect-Client-GUI verwendet, um den Clientakzeptorservice und den Scheduler-Service zu konfigurieren. Standardmäßig wird auch der ferne Clientagent-Service mithilfe des Assistenten konfiguriert. Falls Sie für diese Task das IBM Spectrum Protect-Konfigurationsdienstprogramm für Client-Service (**dsmcutil**) verwenden, müssen Sie sicherstellen, dass Sie auch den fernen Clientagent-Service installieren.

     Starten Sie den Konfigurationsassistenten des IBM Spectrum Protect-Clients über das Menü 'Datei', indem Sie die Optionen **Dienstprogramme** > **Setup-Assistent** auswählen:

     – Wählen Sie die Option **TSM-Web-Client konfigurieren** aus. Geben Sie die Informationen wie angefordert ein.

       a. Wählen Sie bei der Option für den `Startzeitpunkt des Service` die Einstellung für das automatische Starten beim Windows-Start aus.

       b. Wählen Sie bei der Option für das `Starten des Service nach dem Abschluss dieses Assistenten` die Einstellung **Ja** aus.

     Rufen Sie nach der erfolgreichen Ausführung der Operation wieder die Begrüßungsseite des Assistenten auf und fahren Sie mit Schritt b fort.

     Tipp: Wenn Sie auf derselben Maschine mehrere Knoten der Einheit zum Versetzen von Daten konfigurieren, müssen Sie für jede Clientakzeptorinstanz einen unterschiedlichen Portwert angeben.

     – Wählen Sie die Option `TSM-Client-Scheduler konfigurieren` aus. Geben Sie die Informationen wie angefordert ein.

a. Stellen Sie bei der Eingabe des Schedulernamens sicher, dass Sie die Option **Clientakzeptordämon zum Verwalten des Schedulers verwenden** auswählen.
b. Wählen Sie bei der Option für den `Startzeitpunkt des Service` die Einstellung für das automatische Starten beim Windows-Start aus.
c. Wählen Sie bei der Option für das `Starten des Service nach dem Abschluss dieses Assistenten` die Einstellung **Ja** aus.

- Linux **Führen Sie für die Einheit zum Versetzen von Daten unter Linux die folgenden Schritte aus:**
  a. Das Installationsprogramm erstellt ein Startscript für den Clientakzeptor (`dsmcad`) in `/etc/init.d`. Überprüfen bzw. definieren Sie die relevanten Umgebungsvariablen in der Datei `/etc/init.d/dsmcad`.
  b. Geben Sie die folgenden Optionen in der Datei `dsm.sys` in der Zeilengruppe für den Knoten der Einheit zum Versetzen von Daten an:
     – Geben Sie die Option `managedservices` mit diesen Parametern an:

       ```
       managedservices schedule webclient
       ```

       Diese Einstellung weist den Clientakzeptor an, sowohl den Web-Client als auch den Scheduler zu verwalten.
     – (Optional) Falls Sie Zeitplan- und Fehlerinformationen an andere Protokolldateien als die Standarddateien weiterleiten wollen, geben Sie die Optionen `schedlogname` und `errorlogname` mit dem vollständig qualifizierten Pfad- und Dateinamen der Position an, an der die Protokolldaten gespeichert werden sollen. Beispiel:

       ```
       schedlogname /vmsched/dsmsched_dm.log
       errorlogname /vmsched/dsmerror_dm.log
       ```
  c. Starten Sie den Clientakzeptorservice:

     Der Clientakzeptor muss gestartet werden, bevor er Scheduler-Tasks oder den Web-Client verwalten kann. Führen Sie die folgenden Schritte als Rootbenutzer aus:

     1) Konfigurieren Sie den Clientakzeptorservice und den Scheduler-Service der Einheit zum Versetzen von Daten so, dass sie als vStorage-Sicherungsserver agieren.
     2) Starten Sie den Clientakzeptor, indem Sie den folgenden Befehl ausgeben:

        ```
        service dsmcad start
        ```

        Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet wird, fügen Sie den Service wie folgt an einer Shelleingabeaufforderung hinzu:

        ```
        # chkconfig --add dsmcad
        ```

        Tipp: Wenn Sie den Befehl **dsmc** direkt in der Linux-Befehlszeile ausführen möchten, müssen Sie die in Schritt 2 beschriebenen entsprechenden Umgebungsvariablen auch auf die Befehlsshell anwenden.

7. Starten Sie eine Befehlszeilensitzung der Einheit zum Versetzen von Daten mit den Befehlszeilenparametern `-asnodename` und `-optfile`:

   ```
   dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
   ```

   Stellen Sie sicher, dass Ihr Kennwort nach der ersten Anmeldung nicht von Ihnen angefordert wird.

Achtung: Um ein Fehlschlagen des IBM Spectrum Protect-Schedulers zu verhindern, müssen Sie sicherstellen, dass die Option `asnodename` nicht in der Datei `dsm.opt` (Windows) bzw. der Zeilengruppe in der Datei `dsm.sys` (Linux) festgelegt ist. Der Scheduler fragt den IBM Spectrum Protect nach Zeitplänen ab, die `nodename` (Knoten der Einheit zum Versetzen von Daten) und nicht `asnodename` (Datencenterknoten) zugeordnet sind. Falls `asnodename` in `dsm.opt` bzw. `dsm.sys` festgelegt ist, werden Zeitpläne abgefragt, die `asnodename` (und nicht `nodename`) zugeordnet sind. Die Planung von Operationen schlägt daher fehl.

Führen Sie die folgenden Tasks aus:

a. Geben Sie den folgenden Befehl aus, um die Verbindung zum IBM Spectrum Protect-Server zu prüfen:

   ```
   dsmc query session
   ```

   Dieser Befehl zeigt Informationen zur Sitzung an. Hierzu gehören der aktuelle Knotenname, der Zeitpunkt des Sitzungsaufbaus, Serverinformationen und Serververbindungsdaten.

b. Geben Sie den folgenden Befehl aus, um zu prüfen, ob Sie eine virtuelle Maschine sichern können:

   ```
   dsmc backup vm vm1
   ```

   In den Schritten 5b und 5d ist `vm1` der Name der VM.

c. Geben Sie den folgenden Befehl aus, um zu prüfen, ob die Sicherung erfolgreich ausgeführt wurde:

   ```
   dsmc query vm "*"
   ```

d. Geben Sie den folgenden Befehl aus, um zu prüfen, ob die virtuelle Maschine zurückgeschrieben werden kann:

   ```
   dsmc restore vm vm1 -vmname=vm1-restore
   ```

8. Prüfen Sie, ob der Clientakzeptor und der Agent ordnungsgemäß konfiguriert sind:

   a. Geben Sie in einem Web-Browser die Adresse des IBM Spectrum Protect vSphere-Client-Plug-ins ein. Beispiel:

      ```
      https://guihost.mycompany.com/vsphere-client/
      ```

   b. Melden Sie sich mit dem vCenter-Benutzernamen und -Kennwort an.

   c. Klicken Sie im vSphere-Web-Client auf **IBM Spectrum Protect** > **Konfigurieren** > **Einheiten zum Versetzen von Daten**.

   d. Stellen Sie sicher, dass in der Spalte **Status** für die Einheit zum Versetzen von Daten der Status **Verifiziert** angezeigt wird. Wird **Fehlgeschlagen** angezeigt, bewegen Sie den Mauszeiger über den Status, um die Fehlernachricht anzuzeigen.

   Tipp: Wenn die IP-Adresse auf dem System, auf dem die Data Protection for VMware vSphere-GUI installiert ist, geändert wird, müssen Sie Folgendes ausführen:

   a. Konfigurieren Sie den Clientakzeptor erneut, damit die Data Protection for VMware vSphere-GUI für Operationen aktiviert wird. Andernfalls ist für die Data Protection for VMware vSphere-GUI im Plug-in-Manager der Status 'Inaktiviert' angegeben.

Data Protection for VMware-Befehlszeilenschnittstelle in einer vSphere-Umgebung konfigurieren

Aktualisieren Sie das Profil der Data Protection for VMware-Befehlszeilenschnittstelle auf dem System, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

Vorbereitende Schritte

Das Profil (`vmcliprofile`) befindet sich auf dem System, auf dem die Data Protection for VMware vSphere-GUI installiert ist, im folgenden Verzeichnis:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 Bit: `C:\Programme\IBM\SpectrumProtect\Framework\VEGUI\scripts`

Informationen zu diesem Vorgang

Alle Schritte in dieser Prozedur werden auf dem System ausgeführt, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

Tipp: Diese Task kann auch mit dem Konfigurationsassistenten oder dem Konfigurationsnotizbuch der Data Protection for VMware vSphere-GUI ausgeführt werden. Rufen Sie das Fenster **Konfiguration** in der Data Protection for VMware vSphere-GUI auf und klicken Sie auf **Konfigurationsassistenten ausführen** oder **Konfiguration editieren**.

Vorgehensweise

1. Aktualisieren Sie das Profil mit den folgenden Einstellungen:

   VE_TSMCLI_NODE_NAME
   Geben Sie den Knoten an, der die Data Protection for VMware-Befehlszeilenschnittstelle mit dem IBM Spectrum Protect-Server und dem Agentenknoten (`MY_VMCLINODE`) verbindet.

   Einschränkung: Der VMCLI-Knoten unterstützt bei der Kommunikation mit dem IBM Spectrum Protect weder das SSL-Protokoll noch die LDAP-Authentifizierung.

   VE_VCENTER_NODE_NAME
   Geben Sie den virtuellen Knoten an, der ein vCenter darstellt (`MY_VCNODE`).

   VE_DATACENTER_NAME
   Geben Sie den virtuellen Knoten an, der einem Datencenter zugeordnet ist. Die korrekte Syntax lautet:
   `Datencentername::Datencenterknotenname`
   - Beim Wert für `Datencentername` muss die Groß-/Kleinschreibung beachtet werden.
   - Denken Sie daran, diesen Parameter für jedes Datencenter in Ihrer Umgebung festzulegen (`MY_DCNODE`).
   - Die Data Protection for VMware vSphere-GUI unterstützt keine Datencenter mit identischem Namen im vCenter.

VE_TSM_SERVER_NAME
Geben Sie den Hostnamen oder die IP-Adresse des IBM Spectrum Protect-Servers an.

VE_TSM_SERVER_PORT
Geben Sie den Portnamen an, der für den IBM Spectrum Protect-Server verwendet werden soll. Der Standardwert ist `1500`.

Nachfolgend ein Beispielprofil mit diesen Einstellungen:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

2. Definieren Sie das Kennwort für den VMCLI-Knoten in der Datei `pwd.txt`. Dieses Kennwort gilt für den Knoten, der eine Verbindung von der Data Protection for VMware-Befehlszeilenschnittstelle zu dem IBM Spectrum Protect-Server und dem Knoten der Einheit zum Versetzen von Daten herstellt. Er wird durch den Profilparameter VE_TSMCLI_NODE_NAME angegeben.
   a. Geben Sie den Befehl `echo` aus, um eine Textdatei zu erstellen, die das Kennwort enthält:

      Linux `echo password1 > pwd.txt`

      Windows `echo password1> pwd.txt`

      Windows Zwischen dem Kennwort (`password1`) und dem Größer-als-Zeichen (`>`) darf kein Leerzeichen stehen.
   b. Geben Sie den folgenden vmcli-Befehl aus, um das Kennwort für den VMCLI-Knoten festzulegen:
      `vmcli -f set_password -I pwd.txt`

      Wichtig:

      - Linux Sie müssen den Befehl `vmcli -f set_password` als Benutzer tdpvmware und nicht als Root ausgeben.
      - Linux Windows Wenn Sie die Erstellung von Anwendungsschutzberichten planen, müssen Sie den Parameter **`-type VMGuest`** verwenden, um anzugeben, dass das Kennwort für eine VM gilt. Beispiel:

        ```
        vmcli -f set_password -type VMGuest -I password.txt
        ```

3. Prüfen Sie, ob die Data Protection for VMware-Befehlszeilenschnittstelle aktiv ist:

   Windows Klicken Sie auf **Start** > **Systemsteuerung** > **Verwaltung** > **Dienste** und prüfen Sie, ob für `Data Protection for VMware-Befehlszeilenschnittstelle` der Status `Gestartet` angegeben ist.

   Linux Wechseln Sie in das Verzeichnis scripts (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) und geben Sie den folgenden Befehl aus:

   ```
   ./vmclid status
   ```

   - Falls der Dämon aktiv ist, fahren Sie mit Schritt 4 fort.
   - Ist der Dämon nicht aktiv, geben Sie den folgenden Befehl aus, um ihn manuell zu starten:

     ```
     /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
     ```

     Zum Starten und Stoppen des Dämons können auch die folgenden INIT-Scripts verwendet werden:

```
./vmclid stop
./vmclid start
```

4. Geben Sie den folgenden vmcli-Befehl aus, um zu prüfen, ob die Data Protection for VMware-Befehlszeilenschnittstelle die IBM Spectrum Protect-Knotenkonfiguration erkennt:

   ```
   vmcli -f inquire_config -t TSM
   ```

5. Vergewissern Sie sich durch eine Prüfung der Knoten, dass keine Konfigurationsfehler aufgetreten sind:
   a. Starten Sie die Data Protection for VMware vSphere-GUI, indem Sie im vSphere-Clientfenster für Lösungen und Anwendungen (Solutions and Applications) auf das Symbol klicken.
   b. Rufen Sie das Fenster **Konfiguration** auf.
   c. Wählen Sie in der Tabelle einen Knoten aus und klicken Sie auf **Ausgewählten Knoten prüfen**. Die Statusinformationen werden im Teilfenster **Statusdetails** angezeigt.

Nächste Schritte

Linux Windows Nachdem Sie die drei manuellen Konfigurationstasks ausgeführt haben, die im vorliegenden Abschnitt beschrieben sind, können Sie Folgendes ausführen:

1. „IBM Spectrum Protect-Knoten in einer vSphere-Umgebung definieren" auf Seite 96
2. „Knoten der Einheit zum Versetzen von Daten mit der vSphere-Plug-in-GUI definieren" auf Seite 97

Zum Sichern Ihrer VM-Daten sind keine weiteren Konfigurationstasks erforderlich.

Prüfliste für die Konfiguration der vSphere-Umgebung mit der Befehlszeilenschnittstelle

Verwenden Sie diese Prozedur, um Data Protection for VMware in einer vSphere-Umgebung ausschließlichen mit einer Befehlszeilenschnittstelle zu konfigurieren.

Vorgehensweise

Führen Sie Schritt 1 und Schritt 2 auf dem IBM Spectrum Protect-Server aus.

1. Registrieren Sie die folgenden Knoten beim IBM Spectrum Protect-Server:
   a. Knoten, der das VMware vCenter darstellt (vCenter-Knoten):

      ```
      REGister Node MY_VCNODE <Kennwort für MY_VCNODE>
      ```

   b. Knoten für die Kommunikation zwischen IBM Spectrum Protect und der Data Protection for VMware vSphere-GUI (VMCLI-Knoten):

      ```
      REGister Node MY_VMCLINODE <Kennwort für MY_VMCLINODE>
      ```

   c. Knoten, der das Datencenter darstellt und auf dem die VM-Daten gespeichert werden (Datencenterknoten):

      ```
      REGister Node MY_DCNODE <Kennwort für MY_DCNODE>
      ```

   d. Knoten, der Daten von einem System auf ein anderes System 'versetzt' (Knoten der Einheit zum Versetzen von Daten):

      ```
      REGister Node MY_DMNODE <Kennwort für MY_DMNODE>
      ```

2. Definieren Sie die Proxy-Beziehungen für diese Knoten:
   a. Erteilen Sie dem vCenter-Knoten die Proxyberechtigung, indem Sie den folgenden Befehl ausgeben:

```
GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

Dieser Befehl erteilt den Knoten MY_DCNODE und MY_VMCLINODE die Berechtigung, virtuelle Maschinen im Namen des Knotens MY_VCNODE zu sichern und zurückzuschreiben.

b. Erteilen Sie dem Datencenterknoten die Proxyberechtigung, indem Sie den folgenden Befehl ausgeben:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Dieser Befehl erteilt den Knoten MY_VMCLINODE und MY_DMNODE die Berechtigung, virtuelle Maschinen im Namen des Knotens MY_DCNODE zu sichern und zurückzuschreiben.

c. (Optional) Erteilen Sie weiteren Datencenterknoten oder Knoten der Einheit zum Versetzen von Daten in Ihrer Umgebung die Proxyberechtigung.

d. Prüfen Sie die Proxy-Beziehungen, indem Sie den IBM Spectrum Protect-Serverbefehl Query PROXynode ausgeben. Die erwartete Befehlsausgabe lautet:

```
Target Node       Agent Node
--------------    ------------------------------
MY_VCNODE               MY_DCNODE  MY_VMCLINODE
MY_DCNODE            MY_VMCLINODE  MY_DMNODE
```

Führen Sie die Schritte 3 bis 9 auf dem vStorage-Sicherungsserver aus.

3. Legen Sie die entsprechenden Werte für die folgenden Optionen der Einheit zum Versetzen von Daten fest:

   - Windows Geben Sie diese Optionen in der Optionsdatei dsm.opt an.
   - Linux Geben Sie diese Optionen in der Datei dsm.sys in der Zeilengruppe für den Knoten der Einheit zum Versetzen von Daten an.

```
NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPORT
COMMMETHOD
HTTPPORT
```

Anmerkung: Die Option HTTPPORT ist nur dann erforderlich, wenn mehrere Clientakzeptorservices verwendet werden. Sind beispielsweise zwei Knoten der Einheit zum Versetzen von Daten (und zwei Clientakzeptordämonservices) vorhanden, muss in der Optionsdatei für jeden Knoten der Einheit zum Versetzen von Daten ein anderer Wert für HTTPPORT angegeben sein.
Beispiel für eine Datei dsm.dm.opt mit diesen Optionen:

```
NODename MY_DMNODE
PASSWORDAccess generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort 1500
COMMMethod tcpip
HTTPPORT 1583
```

4. Geben Sie den folgenden Befehl aus, um die Verbindung zum IBM Spectrum Protect-Server zu prüfen:
   `dsmc query session`
5. Geben Sie den folgenden Befehl aus, um den VMware vCenter-Benutzer und das zugehörige Kennwort für den Knoten der Einheit zum Versetzen von Daten festzulegen:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <Administrator> <Kennwort1>`
6. Richten Sie die folgenden IBM Spectrum Protect-Services ein:
   - Windows
     a. Installieren Sie den Scheduler-Service:
        ```
        dsmcutil install scheduler /name:"TSM Central Scheduler Service"
        /node:MY_DMNODE   /password:MY_DMNODEPWD /startnow:no /autostart:no
        ```
     b. Installieren Sie den Clientakzeptordämon:
        ```
        dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
        ```
     c. Installieren Sie den fernen Clientagent-Service:
        ```
        dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /partnername:"TSM CAD - MY_DMNODE" /startnow:no
        ```
   - Linux Geben Sie die Option `managedservices` in der Datei `dsm.sys` in der Zeilengruppe für den Knoten der Einheit zum Versetzen von Daten an:
     Achten Sie darauf, die Parameter `schedule` und `webclient` anzugeben:
     ```
     managedservices schedule webclient
     ```
     Diese Einstellung weist den Clientakzeptor an, sowohl den Web-Client als auch den Scheduler zu verwalten.
7. Linux Legen Sie die folgende Umgebungsvariable in der Datei `/etc/init.d/dsmcad` fest, um den Clientakzeptorservice und den Scheduler-Service der Einheit zum Versetzen von Daten so zu konfigurieren, dass sie als vStorage-Sicherungsserver agieren:
   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
   ```
8. Linux Starten Sie den Clientakzeptorservice: Das Installationsprogramm erstellt ein Startscript für den Clientakzeptordämon (`dsmcad`) in `/etc/init.d`. Der Clientakzeptordämon muss gestartet werden, bevor er Scheduler-Tasks oder den Web-Client verwalten kann. Geben Sie den folgenden Befehl als Root aus, um den Dämon zu starten:
   ```
   service dsmcad start
   ```
   Damit der Clientakzeptordämon nach einem Systemwiederanlauf automatisch gestartet wird, fügen Sie den Service wie folgt an einer Shelleingabeaufforderung hinzu:
   ```
   # chkconfig --add dsmcad
   ```
9. Prüfen Sie, ob die IBM Spectrum Protect-Services korrekt konfiguriert sind:
   a. Melden Sie sich bei einem fernen System an.
   b. Stellen Sie in einem Web-Browser eine Verbindung zum System `HOST1` mit dem folgenden Wert für Adresse und Port her:
      `http://HOST1.xyz.yourcompany.com:1581`

Führen Sie Schritt 10 auf dem System aus, auf dem die Data Protection for VMware vSphere-GUI installiert ist.

10. Legen Sie die entsprechenden Werte für die folgenden Optionen im Profil der Data Protection for VMware-Befehlszeilenschnittstelle (`vmcliprofile`) fest:

```
VE_TSMCLI_NODE_NAME
VE_VCENTER_NODE_NAME
VE_DATACENTER_NAME
VE_TSM_SERVER_NAME
VE_TSM_SERVER_PORT
```

Nachfolgend ein Beispielprofil mit diesen Optionen:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

Das Profil befindet sich in den folgenden Verzeichnissen:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 Bit: `C:\Programme\IBM\SpectrumProtect\Framework\VEGUI\scripts`

a. Legen Sie das Kennwort für den VMCLI-Knoten fest:
   1) Geben Sie den Befehl `echo` aus, um eine Textdatei zu erstellen, die das Kennwort enthält:

      Linux

      ```
      echo password1 > pwd.txt
      ```

      Windows

      ```
      echo password1> pwd.txt
      ```

   2) Geben Sie den folgenden vmcli-Befehl aus, um das Kennwort für den VMCLI-Knoten festzulegen:

      Wichtig: Linux Sie müssen diesen Befehl als Benutzer tdpvmware und nicht als Root ausgeben.

      ```
      vmcli -f set_password -I pwd.txt
      ```

b. Prüfen Sie, ob die Data Protection for VMware-Befehlszeilenschnittstelle aktiv ist:

   Windows Geben Sie den folgenden Befehl in einer Windows-Eingabeaufforderung aus:
   `net start`

   Linux Geben Sie den folgenden Befehl aus:
   `./vmclid status`

c. Geben Sie den folgenden vmcli-Befehl aus, um zu prüfen, ob die Data Protection for VMware-Befehlszeilenschnittstelle die IBM Spectrum Protect-Knotenkonfiguration erkennt:

   ```
   vmcli -f inquire_config -t TSM
   ```

Richtlinien für die Bandkonfiguration

Lesen Sie die folgenden Richtlinien, bevor Sie versuchen, Sicherungsoperationen in Bandspeicher auszuführen.

Sicherung auf Band vorbereiten

Linux Windows Bevor Sie versuchen, eine Sicherung auf Band durchzuführen, müssen die folgenden Parameter auf dem IBM Spectrum Protect-Server für Ihre Bandsicherungen festgelegt werden:

1. Definieren Sie die Verwaltungsklasse:

   ```
   define mgmtclass <Domänenname> <Maßnahmengruppenname> <Verwaltungsklassenname>
   ```

   Beispiel:

   ```
   define mgmtclass tape tape DISK
   ```

2. Definieren Sie die Kopiengruppe:

   ```
   define copygroup <Domänenname> <Maßnahmengruppenname> <Verwaltungsklassenname>
   destination=<Speicherpoolname>
   ```

   Beispiel:

   ```
   define copygroup tape tape DISK destination=Diskpool
   ```

3. Aktivieren Sie die Maßnahmengruppe:

   ```
   activate policyset <Domänenname> <Maßnahmengruppenname>
   ```

   Beispiel:

   ```
   activate policyset tape tape
   ```

Bei der Konfiguration von Sicherungen auf physischen Bändern sind zusätzliche Konfigurationsanforderungen zu beachten. Sie müssen immer IBM Spectrum Protect-Metadaten (Steuerdateien) auf Platte und die tatsächlichen Sicherungsdaten der virtuellen Maschine auf Band speichern.

- Verwenden Sie die Option VMMC, um die VMware-Sicherungen (und die VMware-Steuerdateien) mit einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zu speichern.
- Verwenden Sie die Option VMCTLMC, um die Verwaltungsklasse anzugeben, die speziell für VMware-Steuerdateien während VMware-Sicherungen verwendet werden soll. Die angegebene Verwaltungsklasse überschreibt die Standardverwaltungsklasse. Sie überschreibt auch die mit der Option VMMC angegebene Verwaltungsklasse. Die VMCTLMC-Verwaltungsklasse muss einen Plattenspeicherpool ohne Umlagerung auf Band angeben.
- Die Option VMMC wird immer verwendet, um die Aufbewahrungsdauer für VM-Sicherungen zu steuern. Diese Option gilt für Platten- und Bandkonfigurationen. VMCTLMC wird nicht für die Aufbewahrungsdauer der Steuerdateien verwendet. Die Steuerdateien und Datendateien sind Teil derselben Gruppierung und sie verfallen zusammen auf der Basis der Aufbewahrungsmaßnahme der Option VMMC. Werden beide Optionen definiert, wird VMMC für Datendateien und VMCTLMC für Steuerdateien verwendet.

Einschränkung: Bei Zurückschreibungsoperationen, die Speicheragenten in LAN-unabhängigen Konfigurationen verwenden, werden möglicherweise Dateien aus einem Kopienspeicherpool zurückgeschrieben, obwohl die Daten auch aus einem primären Speicherpool abgerufen werden könnten. Dies könnte vorkommen, wenn es sich um eine Zurückschreibungsanforderung für eine bestimmte Datei handelt oder die Zurückschreibungsanforderung nicht die Methode ohne Abfrage verwendet und die primäre Kopie der Datei in einem Speicherpool gespeichert ist, auf den nicht über einen LAN-unabhängigen Pfad zugegriffen werden kann. Dies kann auch andere Vorgänge als Zurückschreibungen betreffen, wie zum Beispiel Data Protection for VMware-Sicherungsoperationen. In einer Data Protection for VMware-Umgebung ist die Platte die bevorzugte Speichermethode für Steuerdateien virtueller Maschinen, sodass zum Zurückschreiben der Datei während einer inkrementellen Sicherung keine Bereitstellung erforderlich ist. Diese Steuerdateien virtueller Maschinen sollten nicht nur auf Platten gespeichert sondern auch nicht in einem Kopienspeicherpool gesichert werden, der über einen LAN-unabhängigen Pfad verfügbar ist. In diesem Fall wird eine Bandbereitstellung verwendet, um die Dateien während einer LAN-unabhängigen inkrementellen Sicherung von einem Data Protection for VMware-Client zurückzuschreiben.

Wenn die IBM Spectrum Protect-Serverumgebung die Umlagerung von Platte auf Band verwendet, beachten Sie vor der Umlagerung die folgenden Richtlinien:

- Setzen Sie den Wert für MIGDELAY des Plattenspeicherpools auf einen Wert, der die meisten Mountanforderungen von der Platte unterstützt. Typische Verwendungsmuster geben an, dass ein hoher Prozentsatz einzelner Dateiwiederherstellungen innerhalb weniger Tage erfolgt, z. B. gewöhnlich 3 - 5 Tage nach der letzten Änderung einer Datei. Aus diesem Grund sollten Sie Daten für diesen kurzen Zeitraum auf der Platte speichern, um Wiederherstellungsoperationen zu optimieren.

  Wird außerdem die clientseitige Deduplizierung mit dem Plattenspeicherpool verwendet, definieren Sie die Option MIGDELAY, die häufige vollständige Sicherungen von virtuellen Maschinen berücksichtigt. Lagern Sie Daten erst dann aus dem deduplizierten Speicherpool auf Band um, wenn mindestens zwei vollständige Sicherungen für eine virtuelle Maschine ausgeführt wurden. Wenn Daten auf Band versetzt werden, werden sie nicht mehr dedupliziert. Werden beispielsweise vollständige Sicherungen wöchentlich ausgeführt, sollten Sie den Wert für MIGDELAY auf mindestens 10 Tage setzen. Mit dieser Einstellung wird sichergestellt, dass jede vollständige Sicherung doppelte Daten aus der vorherigen Sicherung identifiziert und verwendet, bevor sie auf Band versetzt werden.
- Verwenden Sie einen Speicherpool mit der Einheitenklasse FILE anstelle eines Speicherpools mit der Einheitenklasse DISK. Ein typischer Wert für eine Datenträgergröße, die durch den Parameter MAXCAPACITY der Einheitenklasse angegeben wird, ist 8 GB bis 16 GB. Ziehen Sie für den zugeordneten Speicherpool die Anwendung der Kollokation nach Dateibereich in Betracht. Jede virtuelle Maschine, die gesichert wird, wird als separater Dateibereich auf dem IBM Spectrum Protect-Server dargestellt. Bei der Kollokation nach Dateibereich werden die Daten aus mehreren inkrementellen Sicherungen für eine bestimmte virtuelle Maschine auf demselben Datenträger (Plattendatei) gesichert. Bei der Umlagerung auf Band positioniert die Kollokation nach Dateibereich mehrere inkrementelle Sicherungen für eine bestimmte virtuelle Maschine zusammen auf einem physischen Band.

Verwenden Sie den Dialog **Einstellungen**, um den Wert für den Bandmodus zu definieren.

Eine Sicherungsoperation wird unterbrochen, wenn eine Mount- oder Instant Restore-Operation denselben Bandspeicher benötigt, der gleichzeitig von der Sicherungsoperation verwendet wird.

iSCSI-Einheit auf einem Linux-System manuell konfigurieren

Linux

In dieser Prozedur wird die Konfiguration eines Linux-Systems beschrieben, das bei einer iSCSI-Mountoperation verwendet wird. Die VM-Momentaufnahme aus dem IBM Spectrum Protect-Serverspeicher wird bereitgestellt.

Vorbereitende Schritte

Während einer iSCSI-Bereitstellung wird ein iSCSI-Ziel auf dem Recovery Agent-System erstellt. Microsoft iSCSI Initiator ist auf dem Recovery Agent-System nicht erforderlich.

Tipp: Open-iSCSI Initiator wird mit Red Hat Enterprise Linux und SUSE Linux Enterprise Server zur Verfügung gestellt.

Überprüfen Sie die folgenden iSCSI-Voraussetzungen, bevor Sie mit dieser Task fortfahren:

- Sie können von jedem System aus eine Verbindung zu dem iSCSI-Ziel herstellen, um einen Datenträger zu erstellen, der die Sicherungsdaten enthält. Sie können diesen Datenträger von einem anderen System aus bereitstellen.
- Ein iSCSI-Initiator ist auf jedem System erforderlich, das eine Verbindung zu dem iSCSI-Ziel herstellen muss.
- Ein iSCSI-Initiator muss auf dem System installiert sein, auf dem die Daten zurückgeschrieben werden sollen.
- Falls sich ein Datenträger auf mehrere Platten erstreckt, müssen Sie alle erforderlichen Platten bereitstellen. Bei Verwendung von Spiegeldatenträgern stellen Sie nur eine der gespiegelten Platten bereit. Die Bereitstellung von nur einer Platte verhindert eine zeitaufwendige Synchronisationsoperation.

Informationen zu diesem Vorgang

Führen Sie diese Schritte aus, um das Linux-System zu konfigurieren, das bei einer iSCSI-Mountoperation verwendet wird:

Vorgehensweise

1. Notieren Sie sich den iSCSI-Initiatornamen auf dem System, auf dem Daten zurückgeschrieben werden sollen. Sie finden den iSCSI-Initiatornamen in der Datei `/etc/iscsi/initiatorname.iscsi`. Ist der Wert von `InitiatorName=` leer, erstellen Sie einen Initiatornamen mit dem folgenden Befehl:

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   Das folgende Beispiel zeigt einen Initiatornamen:

   ```
   iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

2. Fügen Sie den Initiatornamen der Datei `/etc/iscsi/initiatorname.iscsi` hinzu.
   a. Editieren Sie die Datei `/etc/iscsi/initiatorname.iscsi` mit dem Befehl **vi**. Beispiel:

```
twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
```

b. Aktualisieren Sie den Parameter **InitiatorName=** mit dem Initiatornamen. Beispiel:

```
InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

3. Führen Sie die folgenden Schritte auf dem System aus, auf dem Recovery Agent (oder das iSCSI-Ziel) installiert ist:
   a. Starten Sie Recovery Agent. Geben Sie in den Dialogen `IBM Spectrum Protect-Server auswählen` und `Momentaufnahme auswählen` die entsprechenden Informationen an und klicken Sie auf **Bereitstellen**.
   b. Wählen Sie im Dialog `Mountziel auswählen` die Option `Als iSCSI-Ziel bereitstellen` aus.
   c. Erstellen Sie einen Zielnamen. Achten Sie darauf, dass der Name eindeutig ist und dass Sie ihn von dem System aus erkennen können, auf dem der iSCSI-Initiator ausgeführt wird. Beispiel:

      ```
      iscsi-mount-tsm4ve
      ```

   d. Geben Sie den in Schritt 1 notierten iSCSI-Initiatornamen ein und klicken Sie auf **OK**.
   e. Prüfen Sie, ob der soeben bereitgestellte Datenträger im Feld `Bereitgestellte Datenträger` angezeigt wird.
4. Suchen Sie auf dem in Schritt 1 ausgewählten Initiatorsystem nach dem iSCSI-Initiatorprogramm und starten Sie es:
   a. Prüfen Sie, ob der iSCSI-Service ausgeführt wird, indem Sie den folgenden Befehl ausgeben:
      Red Hat Enterprise Linux:

      ```
      service iscsi status
      ```

      SUSE Linux Enterprise Server:

      ```
      service open-iscsi status
      ```

      Falls der Service nicht aktiv ist, geben Sie den folgenden Befehl aus, um den Service zu starten:
      Red Hat Enterprise Linux:

      ```
      service iscsi start
      ```

      SUSE Linux Enterprise Server:

      ```
      service open-iscsi start
      ```

   b. Stellen Sie die Verbindung zum iSCSI-Ziel her, indem Sie den folgenden Befehl ausgeben:

      ```
      iscsiadm -m discovery -t sendtargets -p <IP-Adresse/Hostname des
      Recovery
      Agent-Systems> --login
      ```

   c. Stellen Sie sicher, dass eine neue Roheinheit verfügbar ist, indem Sie den folgenden Befehl ausgeben:

      ```
      fdisk -l
      ```

5. Stellen Sie das Dateisystem bereit:
   Geben Sie die folgenden Befehle für einen Datenträger aus, der kein LVM-Datenträger ist. In diesem Beispiel ist `/dev/sdb1` die neue Einheit:

   ```
   mkdir /mountdir
   mount /dev/sdb1 /mountdir
   ```

   Führen Sie für einen LVM-Datenträger die folgenden Tasks auf der Linux-Gastmaschine aus:

a. Stellen Sie sicher, dass das Script `vgimportclone` auf dem Linux-System verfügbar ist. Dieses Script ist nicht im Lieferumfang des LVM-Basispakets (Standard) enthalten. Folglich müssen Sie möglicherweise das LVM-Paket auf eine Version aktualisieren, die dieses Script bereitstellt.

b. Geben Sie den Befehl **vgimportclone** aus und geben Sie den Namen einer neuen Basisdatenträgergruppe an (`VolGroupSnap01`). Beispiel:

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```

c. Geben Sie den Befehl **lvchange** aus, um den logischen Datenträger als aktiv zu markieren. Beispiel:

```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```

d. Geben Sie diese Befehle aus, um den Datenträger bereitzustellen:

```
mkdir /mountdir
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```

6. Nach dem Abschluss der Dateizurückschreibungsoperation geben Sie diese Befehle aus:

- Geben Sie bei einem Datenträger, der kein LVM-Datenträger ist, die folgenden Befehle aus:

  a. Bereitstellung des Dateisystems aufheben:

  ```
  umount /dev/sdb1 /mountdir
  ```

  b. Den Datenträger entfernen. Ist der Datenträger Bestandteil einer Datenträgergruppe, entfernen Sie den Datenträger zunächst aus der Datenträgergruppe, indem Sie den folgenden Befehl ausgeben:

  ```
  vgreduce <Ihre_Datenträgergruppe> /dev/sdb1
  ```

  Anschließend geben Sie diesen Befehl aus, um den Datenträger zu entfernen:

  ```
  pvremove /dev/sdb1
  ```

  c. Bei einem einzelnen Ziel abmelden:

  ```
  iscsiadm --mode node --targetname <Zielname> --logout
  ```

  d. Bei allen Zielen abmelden:

  ```
  iscsiadm --mode node --logout
  ```

- Führen Sie für einen LVM-Datenträger die folgenden Tasks auf der Linux-Gastmaschine aus:

  a. Bereitstellung des Dateisystems aufheben:

  ```
  unmount /mountdir
  ```

  b. Den logischen Datenträger entfernen:

  ```
  lvm lvremove LogVol00
  ```

  c. Die Datenträgergruppe entfernen:

  ```
  lvm vgremove VolGroupSnap01
  ```

  d. Bei einem einzelnen Ziel abmelden:

  ```
  iscsiadm --mode node --targetname <Zielname> --logout
  ```

  e. Bei allen Zielen abmelden:

  ```
  iscsiadm --mode node --logout
  ```

iSCSI-Einheit auf einem Windows-System manuell konfigurieren

Windows

In dieser Prozedur wird die Konfiguration eines Windows-Systems beschrieben, das bei einer iSCSI-Mountoperation verwendet wird. Die Momentaufnahme wird aus dem IBM Spectrum Protect-Serverspeicher bereitgestellt.

Vorbereitende Schritte

Überprüfen Sie die folgenden iSCSI-Voraussetzungen, bevor Sie mit dieser Task fortfahren:

- Während einer iSCSI-Bereitstellung wird ein iSCSI-Ziel auf dem Recovery Agent-System erstellt. Sie können von jedem System aus eine Verbindung zu dem iSCSI-Ziel herstellen, um einen Datenträger zu erstellen, der die Sicherungsdaten enthält. Außerdem können Sie diesen Datenträger anschließend von einem anderen System aus bereitstellen.
- Ein iSCSI-Initiator ist auf jedem System erforderlich, das eine Verbindung zu dem iSCSI-Ziel herstellen muss.
- Stellen Sie sicher, dass ein iSCSI-Initiator auf dem System installiert ist, auf dem die Daten zurückgeschrieben werden sollen.
- Microsoft iSCSI Initiator ist auf dem Recovery Agent-System nicht erforderlich.

Überprüfen Sie die folgenden Platten- und Datenträgervoraussetzungen, bevor Sie mit dieser Task fortfahren:

- Falls sich ein Datenträger auf mehrere Platten erstreckt, müssen Sie alle erforderlichen Platten bereitstellen. Bei Verwendung von Spiegeldatenträgern stellen Sie nur eine der gespiegelten Platten bereit. Die Bereitstellung von nur einer Platte verhindert eine zeitaufwendige Synchronisationsoperation.
- Falls mehrere dynamische Platten auf dem Sicherungssystem verwendet wurden, sind diese Platten derselben Gruppe zugeordnet. Der Windows Disk Manager sieht daher möglicherweise einige Platten als fehlend an und gibt eine Fehlernachricht aus, wenn Sie nur eine Platte bereitstellen. Ignorieren Sie diese Nachricht. Die Daten auf der gesicherten Platte sind dennoch zugänglich, sofern sich nicht einige Daten auf der anderen Platte befinden. Dieses Problem können Sie lösen, indem Sie alle dynamischen Platten bereitstellen.

Informationen zu diesem Vorgang

Führen Sie diese Tasks aus, um das Windows-System zu konfigurieren, das bei einer iSCSI-Mountoperation verwendet wird:

Vorgehensweise

1. Auf dem Recovery Agent-System öffnen Sie den Port `3260` in der LAN-Firewall und in der Firewall des Windows-Clients. Notieren Sie sich den iSCSI-Initiatornamen auf dem System, auf dem Daten zurückgeschrieben werden sollen.

   Der iSCSI-Initiatorname wird im Konfigurationsfenster für den iSCSI-Initiator in der Systemsteuerung angezeigt. Beispiel:

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. Führen Sie die folgenden Tasks auf dem System aus, auf dem Recovery Agent (iSCSI-Ziel) installiert ist:

a. Starten Sie die Recovery Agent-GUI. Geben Sie in den Dialogen **IBM Spectrum Protect-Server auswählen** und **Momentaufnahme auswählen** die entsprechenden Informationen an und klicken Sie auf **Bereitstellen**.

b. Wählen Sie im Dialog **Mountziel auswählen** die Option **Als iSCSI-Ziel bereitstellen** aus.

c. Erstellen Sie einen Zielnamen. Achten Sie darauf, dass der Name eindeutig ist und dass Sie ihn von dem System aus erkennen können, auf dem der iSCSI-Initiator ausgeführt wird. Beispiel:

```
iscsi-mount-tsm4ve
```

d. Geben Sie den in Schritt 1 notierten iSCSI-Initiatornamen ein und klicken Sie auf **OK**.

e. Prüfen Sie, ob der soeben bereitgestellte Datenträger im Feld **Bereitgestellte Datenträger** angezeigt wird.

f. Wenn Sie den Recovery Agent in einem iSCSI-Netz einsetzen und der Recovery Agent keine Einheit zum Versetzen von Daten verwendet, rufen Sie die Datei `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` auf und geben Sie den Tag `[IMOUNT]` und den Parameter **`Target IP`** an:

```
[IMOUNT config]
Target IP=<IP-Adresse der Netzkarte auf dem System,
das die iSCSI-Ziele verfügbar macht>
```

Beispiel:

```
[Allgemeine config]
Param1
Param2
...
[IMount config]
Target IP=9.11.153.39
```

Nach der Hinzufügung oder Änderung des Parameters 'Target IP' starten Sie die Recovery Agent-GUI oder Recovery Agent-CLI erneut.

3. Suchen Sie auf dem in Schritt 1 ausgewählten Initiatorsystem nach dem iSCSI-Initiatorprogramm und starten Sie es:

a. Stellen Sie eine Verbindung zum iSCSI-Ziel her:

1) Geben Sie auf der Registerkarte 'Ziele' die TCP/IP-Adresse der in Schritt 2 verwendeten Recovery Agent-Instanz (iSCSI-Ziel) im Dialog **Ziel:** ein. Klicken Sie auf **Schnell verbinden**.

2) Im Dialog **Schnell verbinden** wird ein Ziel angezeigt, dessen Name mit dem in Schritt 2c angegebenen Zielnamen identisch ist. Falls noch keine Verbindung besteht, wählen Sie dieses Ziel aus und klicken Sie auf **Verbinden**.

b. Rufen Sie auf dem Initiatorsystem **Systemsteuerung** > **Verwaltung** > **Computerverwaltung** > **Speicher** > **Datenträgerverwaltung** auf.

1) Falls das bereitgestellte iSCSI-Ziel mit **Typ=Fremd** angezeigt wird, klicken Sie mit der rechten Maustaste auf **Fremde Datenträger** und wählen Sie **Fremde Datenträger importieren** aus. **Fremde Datenträgergruppe** ist ausgewählt. Klicken Sie auf **OK**.

2) In der nächsten Anzeige sind der Typ, die Bedingung und die Größe der fremden Platte angegeben. Klicken Sie auf **OK** und warten Sie, bis die Platte importiert wurde.

3) Drücken Sie nach Abschluss des Plattenimports die Taste **F5** (Aktualisieren). Die bereitgestellte iSCSI-Momentaufnahme ist sichtbar und enthält einen zugeordneten Laufwerkbuchstaben. Falls Laufwerkbuchstaben

nicht automatisch zugeordnet werden, klicken Sie mit der rechten Maustaste auf die erforderliche Partition und wählen Sie **Laufwerkbuchstabe oder -pfad ändern** aus. Klicken Sie auf **Hinzufügen** und wählen Sie einen Laufwerkbuchstaben aus.

4. Öffnen Sie Windows Explorer (oder ein anderes Dienstprogramm) und durchsuchen Sie die bereitgestellte Momentaufnahme für eine Dateizurückschreibungsoperation.
5. Nach der Zurückschreibung der Datei führen Sie die folgenden Tasks aus:
   a. Trennen Sie die Verbindung zu jedem iSCSI-Ziel mithilfe des Dialogs **iSCSI-Initiatoreigenschaften**.
   b. Heben Sie die Bereitstellung des Datenträgers aus Schritt 2 auf, indem Sie den Datenträger in der Recovery Agent-GUI auswählen und auf **Bereitstellung aufheben** klicken.

Mount-Proxy-Knoten auf einem Linux-System manuell konfigurieren

Linux

Führen Sie diese Task aus, um einen Mount-Proxy-Knoten einem fernen Linux-System hinzuzufügen.

Vorbereitende Schritte

In einer standardmäßigen Data Protection for VMware vSphere-GUI-Umgebung wird eine separate Zeilengruppe in der Datei `dsm.sys` für jeden Mount-Proxy-Knoten verwendet. Alle Schritte in dieser Prozedur werden unter Verwendung der Einheit zum Versetzen von Daten ausgeführt, die auf dem Sicherungsserver installiert ist.

Informationen zu diesem Vorgang

Mit dieser Task werden die Mount-Proxy-Knoten konfiguriert, indem die Optionen der Einheit zum Versetzen von Daten aktualisiert werden und die Konnektivität zum IBM Spectrum Protect-Server überprüft wird.

Vorgehensweise

1. Geben Sie diese Optionen in der Datei `dsm.sys` in der Zeilengruppe für den Mount-Proxy-Knoten an.

   NODENAME
   Geben Sie den Namen eines zuvor definierten Mount-Proxy-Knotens an. Diesem Knoten werden IBM Spectrum Protect-Zeitpläne zugeordnet.

   PASSWORDACCESS
   Geben Sie GENERATE an, damit das Kennwort automatisch generiert wird (und keine Benutzereingabeaufforderung ausgegeben wird).

   MANAGEDSERVICES
   Geben Sie diese Option an, um den Clientakzeptor anzuweisen, sowohl den Web-Client als auch den Scheduler zu verwalten (`schedule webclient`).

   TCPSERVERADDRESS
   Geben Sie die TCP/IP-Adresse für den IBM Spectrum Protect-Server an.

TCPPORT
Geben Sie die TCP/IP-Portadresse für den IBM Spectrum Protect-Server an.

COMMMETHOD
Geben Sie die Übertragungsmethode an, die vom IBM Spectrum Protect-Server verwendet werden soll. Für Mount-Proxy-Knoten müssen Sie TCP/IP als Übertragungsmethode angeben. Falls eine andere Methode angegeben wird, schlagen Operationen fehl.

HTTPPORT
Diese Option gibt eine TCP/IP-Portadresse an und muss nur angegeben werden, wenn mehrere Clientakzeptorservices (CAD) verwendet werden. Sind beispielsweise zwei Mount-Proxy-Knoten (und zwei CAD-Services) vorhanden, muss in der Optionsdatei für jeden Mount-Proxy-Knoten ein anderer Wert für `HTTPPORT` angegeben sein.

Einschränkung: Aktivieren Sie nicht die Option für LAN-Unabhängigkeit (`ENABLELANFREE YES`) in der Datei `dsm.sys`. Diese Option wird für Mount-Proxy-Knoten nicht unterstützt.
Nachfolgend ein Beispiel für eine Datei dsm.sys mit diesen Einstellungen:

```
Servername     tsm_server1
  NODename datacenter1_MP_LNX
  PASSWORDAccess generate
  MANAGEDServices schedule webclient
  TCPServeraddress tsmserver.myco.com
  TCPPort 1500
  COMMMethod tcpip
  HTTPPORT 1583
```

2. Geben Sie den folgenden Befehl aus, um den VMware vCenter-Benutzer und das zugehörige Kennwort für den Mount-Proxy-Knoten festzulegen:
`dsmc set password -type=vm vcenter.mycompany.xyz.com <Administrator> <Kennwort1>`
3. Starten Sie eine Befehlszeilensitzung der Einheit zum Versetzen von Daten mit den Befehlszeilenparametern `-asnodename` und `-optfile`:
`dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
Stellen Sie sicher, dass Ihr Kennwort nach der ersten Anmeldung nicht von Ihnen angefordert wird.

   Achtung: Um ein Fehlschlagen des IBM Spectrum Protect-Schedulers zu verhindern, müssen Sie sicherstellen, dass die Option `asnodename` in der Zeilengruppe der Datei `dsm.sys` (Linux) nicht angegeben ist. Der Scheduler fragt den IBM Spectrum Protect-Server nach Zeitplänen ab, die `nodename` (dem Mount-Proxy-Knoten) und nicht `asnodename` (dem Datencenterknoten) zugeordnet sind. Ist `asnodename` in `dsm.sys` definiert, werden Zeitpläne abgefragt, die `asnodename` (und nicht `nodename`) zugeordnet sind. Die Planung von Operationen schlägt daher fehl.
4. Geben Sie den folgenden Befehl aus, um die Verbindung zum IBM Spectrum Protect-Server zu prüfen:
`dsmc query session`
Dieser Befehl zeigt Informationen zur Sitzung an. Hierzu gehören der aktuelle Knotenname, der Zeitpunkt des Sitzungsaufbaus, Serverinformationen und Serververbindungsdaten.
5. Führen Sie die folgenden Tasks aus, um den Clientakzeptorservice (CAD) und den Scheduler-Service der Einheit zum Versetzen von Daten zu konfigurieren:
   - Geben Sie die folgenden Optionen in der Datei `dsm.sys` in der Zeilengruppe für den Mount-Proxy-Knoten ein:

– Geben Sie die Option `managedservices` mit diesen Parametern an:

```
managedservices schedule webclient
```

Diese Einstellung weist den Clientakzeptor an, sowohl den Web-Client als auch den Scheduler zu verwalten.

– Sollen Zeitplan- und Fehlerinformationen in andere Protokolldateien als die Standarddateien übertragen werden, geben Sie die Optionen `schedlogname` und `errorlogname` an. Jede Option muss den vollständig qualifizierten Pfad und Namen der Datei enthalten, in der die Protokolldaten gespeichert werden sollen. Beispiel:

```
schedlogname /vmsched/dsmsched_mp_lnx.log
errorlogname /vmsched/dsmerror_mp_lnx.log
```

- Sollen der Clientakzeptorservice und der Scheduler-Service der Einheit zum Versetzen von Daten so konfiguriert werden, dass sie als Sicherungsserver agieren, definieren Sie die folgende Umgebungsvariable in der Datei `/etc/init.d/dsmcad`:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```

- Starten Sie den Clientakzeptorservice:

  Das Installationsprogramm erstellt ein Startscript für den Clientakzeptordämon (`dsmcad`) in `/etc/init.d`. Der Clientakzeptordämon muss gestartet werden, bevor er Scheduler-Tasks oder den Web-Client verwalten kann. Geben Sie den folgenden Befehl als Root aus, um den Dämon zu starten:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
service dsmcad start
```

  Damit der Clientakzeptordämon nach einem Systemwiederanlauf automatisch gestartet wird, fügen Sie den Service wie folgt an einer Shelleingabeaufforderung hinzu:

```
# chkconfig --add dsmcad
```

6. Prüfen Sie, ob der Clientakzeptor und der Agent ordnungsgemäß konfiguriert sind:
   a. Melden Sie sich bei einem fernen System an.
   b. Stellen Sie in einem Web-Browser eine Verbindung zum System `HOST1` mit dem folgenden Wert für Adresse und Port her:

```
http://HOST1.xyz.yourcompany.com:1581
```

Mount-Proxy-Knoten auf einem fernen Windows-System manuell konfigurieren

Windows

Führen Sie diese Task aus, um einen Mount-Proxy-Knoten einem fernen Windows-System hinzuzufügen. Diese Task ist erforderlich, wenn Sie Ihrer Umgebung einen zweiten Windows-Mount-Proxy-Knoten hinzufügen möchten.

Vorbereitende Schritte

Stellen Sie sicher, dass der primäre Windows-Mount-Proxy-Knoten konfiguriert ist, bevor Sie diese Task fortsetzen.

Informationen zu diesem Vorgang

Führen Sie diese Schritte auf dem fernen Windows-Mount-Proxy-System aus:

Vorgehensweise

1. Installieren Sie die folgenden Produkte auf dem fernen Windows-Mount-Proxy-System:
   - Recovery Agent
   - IBM Spectrum Protect-Einheit zum Versetzen von Daten

   Beide Produkte befinden sich im Download-Image von IBM Spectrum Protect for Virtual Environments. Schrittweise Installationsanweisungen sind im IBM Knowledge Center unter dem folgenden Link verfügbar:
   „Data Protection for VMware-Komponenten auf Windows-Systemen installieren" auf Seite 25
2. Rufen Sie den Inhalt der Beispieloptionsdatei von dem erstellten Windows-Mount-Proxy-Knoten ab und fügen Sie ihn der Optionsdatei auf dem fernen Windows-Mount-Proxy-System hinzu:
   a. Auf dem primären Windows-Mount-Proxy-System rufen Sie das Fenster **Konfiguration** in der Data Protection for VMware vSphere-GUI auf.
   b. Klicken Sie auf **TSM-Konfiguration editieren** in der Liste **Tasks**. Möglicherweise dauert es einige Momente, bis das Konfigurationsnotizbuch geladen ist.
   c. Rufen Sie die Seite **Mount-Proxy-Knotenpaare** auf.
   d. In der Tabellenspalte für den Primärknoten rufen Sie den Windows-Mount-Proxy-Knoten mit der anstehenden Position aus und klicken Sie auf **Einstellungen anzeigen**.
   e. Kopieren Sie den Inhalt der Beispieldatei `dsm.opt`, der im Dialog **Mount-Proxy-Einstellungen** angezeigt wird.
   f. Fügen Sie den Inhalt der Beispieldatei `dsm.opt` in die Optionsdatei auf dem fernen Windows-Mount-Proxy-System ein (bzw. fügen Sie ihn hinzu). Benennen Sie die Optionsdatei unter Verwendung einer Namenskonvention, die auf die Rolle des Knotens als ferner Mount-Proxy-Knoten hinweist. Beispiel: `dsm.REMOTE1_MP_WIN.opt`.

   Einschränkung: Aktivieren Sie nicht die Option für LAN-Unabhängigkeit (`ENABLELANFREE YES`) in der Optionsdatei. Diese Option wird für Mount-Proxy-Knoten nicht unterstützt.
3. Geben Sie den folgenden Befehl der Einheit zum Versetzen von Daten aus, um den VMware vCenter-Benutzer und das zugehörige Kennwort für den Mount-Proxy-Knoten festzulegen:

   Tipp: Zum Starten der dsmc-Befehlszeile öffnen Sie das Windows-Menü **Start** und wählen Sie **Programme→ IBM Spectrum Protect → Befehlszeile für Client für Sichern/Archivieren** aus.

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <Administrator> <Kennwort1>
   -optfile=dsm.REMOTE1_MP_WIN.opt
   ```
4. Geben Sie den folgenden Befehl aus, um die Verbindung zum IBM Spectrum Protect-Server zu prüfen:

   ```
   dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
   ```

Dieser Befehl zeigt Informationen zur Sitzung an. Hierzu gehören der aktuelle Knotenname, der Zeitpunkt des Sitzungsaufbaus, Serverinformationen und Serververbindungsdaten.

5. Führen Sie die folgenden Schritte aus, um den Clientakzeptorservice (CAD) und den Scheduler-Service der Einheit zum Versetzen von Daten zu konfigurieren:
   In diesem Schritt wird der Konfigurationsassistent der IBM Spectrum Protect-Client-GUI verwendet, um den CAD- und Scheduler-Service zu konfigurieren. Der ferne Clientagent-Service wird standardmäßig ebenfalls mithilfe des Assistenten konfiguriert. Falls Sie für diese Task das Konfigurationsdienstprogramm des Client-Service von IBM Spectrum Protect (`dsmcutil`) verwenden, müssen Sie auch den fernen Clientagent-Service installieren.
   Starten Sie den Konfigurationsassistenten des IBM Spectrum Protect-Clients über das Menü 'Datei', indem Sie die Optionen **Dienstprogramme > Setup-Assistent** auswählen:
   a. Wählen Sie die Option `TSM-Web-Client konfigurieren` aus. Geben Sie die Informationen wie angefordert ein.
      1) Wählen Sie bei der Option für den `Startzeitpunkt des Service` die Einstellung für das automatische Starten beim Windows-Start aus.
      2) Wählen Sie bei der Option für das `Starten des Service nach dem Abschluss dieses Assistenten` die Einstellung `Ja` aus.

      Rufen Sie nach der erfolgreichen Ausführung der Operation wieder die Begrüßungsseite des Assistenten auf und fahren Sie mit Schritt b fort.

      Tipp: Falls Sie mehrere Mount-Proxy-Knoten auf demselben System konfigurieren, müssen Sie für jede Clientakzeptorinstanz einen anderen Portwert angeben.
   b. Wählen Sie die Option `TSM-Client-Scheduler konfigurieren` aus. Geben Sie die Informationen wie angefordert ein.
      1) Stellen Sie bei der Eingabe des Schedulernamens sicher, dass Sie die Option `Clientakzeptordämon zum Verwalten des Schedulers verwenden` auswählen.
      2) Wählen Sie bei der Option für den `Startzeitpunkt des Service` die Einstellung für das automatische Starten beim Windows-Start aus.
      3) Wählen Sie bei der Option für das `Starten des Service nach dem Abschluss dieses Assistenten` die Einstellung `Ja` aus.
6. Prüfen Sie, ob der Clientakzeptor und der Agent ordnungsgemäß konfiguriert sind. Stellen Sie in einem Web-Browser eine Verbindung zum System `HOST1` mit dem folgenden Wert für Adresse und Port her:
   `http://HOST1.xyz.yourcompany.com:1581`

Mehrere Clientakzeptorservices auf einem Linux-System manuell konfigurieren

Unter bestimmten Bedingungen kann es sinnvoll sein, mehrere dsmcad-Services auf einem einzigen Linux-Client-Host zu verwenden.

Informationen zu diesem Vorgang

Mit dieser Task werden mehrere dsmcad-Instanzen eingerichtet, die ausgeführt und beim Systemstart automatisch gestartet werden:

Vorgehensweise

1. Erstellen Sie zwei eindeutige Knotenzeilengruppen in der Datei dsm.sys (diese Datei befindet sich standardmäßig in /opt/tivoli/tsm/client/ba/bin/):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
  COMMMethod         TCPip
  TCPPort 1500
  TCPServeraddress   localhost
  nodename           node1
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
  managedservices    webclient sched
  httpport           1581
  passwordaccess     generate

SErvername node2
  COMMMethod         TCPip
  TCPPort 1500
  TCPServeraddress   localhost
  nodename           node2
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
  managedservices    webclient sched
  httpport           1582
  passwordaccess     generate
```

   Tipp: Es empfiehlt sich möglicherweise, bestimmte Include-/Exclude-Optionen anzugeben, um diese Knoten voneinander zu unterscheiden. Andernfalls werden eventuell dieselben Daten von beiden Knotennamen gesichert.

2. Erstellen Sie zwei dsm.opt-Dateien, je eine für jeden Knoten (diese Dateien befinden sich standardmäßig in /opt/tivoli/tsm/client/ba/bin):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Aktivieren Sie passwordaccess generate, indem Sie sich bei beiden Knoten mit den Berechtigungsnachweisen anmelden:

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Erstellen Sie zwei Kopien des standardmäßigen Initialisierungsscripts rc.dsmcad (dieses Script befindet sich standardmäßig in /opt/tivoli/tsm/client/ba/bin):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Editieren Sie rc.dsmcad-node1:
   a. Ändern Sie diese Zeile für Red Hat Enterprise Linux-Distributionen:

```
daemon $DSMCAD_BIN
```

      In diese Zeile:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

b. Ändern Sie diese Zeile für SUSE Linux Enterprise Server-Distributionen:

```
startproc $DSMCAD_BIN
```

In diese Zeile:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

6. Editieren Sie rc.dsmcad-node2:
   a. Ändern Sie diese Zeile für Red Hat Enterprise Linux-Distributionen:

```
daemon $DSMCAD_BIN
```

In diese Zeile:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

   b. Ändern Sie diese Zeile für SUSE Linux Enterprise Server-Distributionen:

```
startproc $DSMCAD_BIN
```

In diese Zeile:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

7. Erstellen Sie neue Links in `/etc/init.d/`, um auf die beiden neuen rc.dsmcad-Initialisierungsscripts zu verweisen. Über diese Links kann der Linux-Initialisierungsservice die dsmcad-Services beim Systemstart starten:

```
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
# ls -la dsm*
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

8. Registrieren Sie die beiden neuen rc-Scripts mit **chkconfig**:

```
# chkconfig --add dsmcad-node1
# chkconfig --add dsmcad-node2
```

9. Testen Sie die Konfiguration mit dem Befehl **service dsmcad start**, um sicherzustellen, dass die Scripts ohne Probleme geladen und gestartet werden:

```
# service dsmcad-node1 start
Starting dsmcad-node1:                                     [  OK  ]
# service dsmcad-node2 start
Starting dsmcad-node2:                                     [  OK  ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

Der Befehlstext wird in diesem Beispiel in zwei Zeilen dargestellt, um die Seitenformatierung zu berücksichtigen.

10. Starten Sie das System erneut und überprüfen Sie, ob die beiden dsmcad-Instanzen automatisch gestartet wurden:

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

Der Befehlstext wird in diesem Beispiel in zwei Zeilen dargestellt, um die Seitenformatierung zu berücksichtigen.

VMCLI-Konfigurationsdatei ändern

Die VMCLI-Konfigurationsdatei (`vmcliConfiguration.xml`) enthält Einstellungen für die Data Protection for VMware vSphere-GUI.

Während des Data Protection for VMware-Installationsprozesses muss ein Benutzer die IP-Adresse eines vCenter-Servers bereitstellen und angeben, ob der Zugriff auf die GUI über einen Web-Browser aktiviert werden soll. Nach der Installation kann die IP-Adresse des Servers und die GUI-Zugriffsmethode jedoch nicht mehr vom Installationsprogramm geändert werden.

Zum Aktualisieren dieser Einstellungen können Sie die VMCLI-Konfigurationsdatei (`vmcliConfiguration.xml`) manuell editieren. Diese Datei wird während der Installation an den folgenden Positionen erstellt:
Auf Windows-Systemen:
`C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI`
Auf Linux-Systemen:
`/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/`

Wenn Sie die Angabe ändern möchten, die festlegt, ob der Zugriff auf die GUI über einen Web-Browser aktiviert werden soll, geben Sie einen der folgenden Werte in den Parameter **<enable_direct_start></enable_direct_start>** ein:

- *yes* Auf die GUI kann direkt mit einem Web-Browser zugegriffen werden. Beispiel:

  ```
  <enable_direct_start>yes</enable_direct_start>
  ```

- *no* Auf die GUI kann nicht direkt mit einem Web-Browser zugegriffen werden. Beispiel:

  ```
  <enable_direct_start>no</enable_direct_start>
  ```

Zum Verwenden der GUI für vSphere-Schutz geben Sie den folgenden Wert im Parameter **<mode></mode>** an:

- *vcenter* Die GUI wird für vSphere-Schutz verwendet. Beispiel:

  ```
  <mode>vcenter</mode>
  ```

Wenn Sie die IP-Adresse des vCenter-Servers ändern möchten, stellen Sie sicher, dass **<mode>vcenter</mode>** festgelegt ist, und geben Sie anschließend die IP-Adresse in den Parameter **<vcenter_url></vcenter_url>** ein. Beispiel:

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

Der Wert `https://` am Anfang der IP-Adresse des vCenter-Servers ist erforderlich. Der Wert `/sdk` am Ende der IP-Adresse des vCenter-Servers ist erforderlich.

Beispiele für die Datei `vmcliConfiguration.xml`

Die folgende Datei `vmcliConfiguration.xml` ist für vSphere-Schutz konfiguriert und der Web-Browser-Zugriff für die GUI ist aktiviert:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
 <VMCLIPath>C:\Programme\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
  <interruptDelay>900000</interruptDelay>
  <mode>vcenter</mode>
  <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
  <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

Anhang B. Auf eine Sicherungsstrategie 'Immer inkrementell - Inkrementell' migrieren

Mit dem hier beschriebenen Verfahren können Sie bestehende Sicherungszeitpläne, -maßnahmen und Knoten der Einheit zum Versetzen von Daten auf die Verwendung einer Sicherungsstrategie 'Immer inkrementell' migrieren.

Vorbereitende Schritte

Sie können die Sicherungsstrategie 'Immer inkrementell - Vollständig' verwenden, die in Data Protection for VMware Version 6.2 und 6.3 implementiert war. Wenn Sie weiterhin die Sicherungsstrategie 'Immer inkrementell - Vollständig' verwenden möchten, ist keine Änderung Ihrer Maßnahme oder Zeitpläne erforderlich. Sie müssen lediglich sicherstellen, dass Sie für die Knoten der Einheit zum Versetzen von Daten ein Upgrade auf Version 6.4 (oder höher) durchführen, wie in der folgenden Prozedur beschrieben. Wenn Sie jedoch die Sicherungsstrategie 'Immer inkrementell - Inkrementell' verwenden möchten, müssen Sie nicht nur die Knoten der Einheit zum Versetzen von Daten auf Version 6.4 (oder höher) aktualisieren, sondern auch die Zeitpläne und Maßnahme für diejenigen Knoten der Einheit zum Versetzen von Daten aktualisieren, die auf diese Sicherungsstrategie 'Immer inkrementell - Inkrementell' migriert werden sollen.

Zum Migrieren vorhandener Data Protection for VMware-Zeitpläne auf eine Sicherungsstrategie des Typs 'Immer inkrementell - Inkrementell' müssen Sie die Tasks ausführen, die in dieser Prozedur dokumentiert sind.

Wichtig:

- Obwohl einige Tasks in sich abgeschlossen sind, müssen letztendlich alle Anwendungen und Komponenten aktualisiert werden, um optimal von den Vorteilen der Strategie 'Immer inkrementell - Inkrementell' zu profitieren. Diese Veröffentlichung enthält alle Informationen, die Sie für jede einzelne Task benötigen.
- Für die Ausführung des gesamten Migrationsprozesses gibt es mehrere Methoden. Bei den in dieser Veröffentlichung dokumentierten Methoden handelt es sich jedoch um effiziente Methoden für typische Data Protection for VMware-Umgebungen.
- Der Zeitplan, der in dieser Prozedur migriert werden soll, wurde mit dem Sicherungsassistenten der Data Protection for VMware vSphere-GUI erstellt. Falls der zu migrierende Zeitplan manuell erstellt wurde, müssen die in dieser Prozedur angegebenen Zeitplanänderungen ebenfalls manuell vorgenommen werden.

Informationen zu diesem Vorgang

Vorgehensweise

1. Führen Sie für alle vStorage-Sicherungsserver, die ein einzelnes vCenter schützen, ein Upgrade durch. Stellen Sie sicher, dass dieses Upgrade für alle Knoten der Einheit zum Versetzen von Daten gleichzeitig vorgenommen wird.
   - Dieses Upgrade erfordert die Installation der IBM Spectrum Protect-Einheit zum Versetzen von Daten Version 6.4 (oder höher) auf dem vStorage-Sicherungsserver.
   - Da es sich um in sich abgeschlossene Tasks handelt, müssen Sie Schritt 2 oder Schritt 3 nicht unmittelbar nach Schritt 1 ausführen. Nachdem Sie für

die Knoten der Einheit zum Versetzen von Daten das Upgrade durchgeführt haben, können Sie weiterhin virtuelle Maschinen in Ihrer vorhandenen Umgebung sichern. Sie können Schritt 2 und Schritt 3 ausführen, sobald sich eine günstigere Gelegenheit ergibt.

Tipp: Falls in Ihrer Umgebung mehrere vStorage-Sicherungsserver eingesetzt werden, kann es sinnvoll sein, zunächst nur für einen der Server ein Upgrade durchzuführen. Anschließend können Sie prüfen, ob der Server erfolgreich betrieben wird, bevor Sie das Upgrade der übrigen vStorage-Sicherungsserver durchführen.

2. Aktualisieren Sie die Sicherungsmaßnahme und die Sicherungszeitpläne, um Sicherungen des Typs 'Immer inkrementell - Inkrementell' zu implementieren: Führen Sie die folgenden Tasks für die Sicherungsmaßnahme auf dem IBM Spectrum Protect-Server aus, indem Sie im Verwaltungsbefehlszeilenclient (`dsmadmc`) Befehle ausgeben:
   a. Erstellen Sie eine Verwaltungsklasse für die entsprechende Domäne und Maßnahmengruppe für Ihre Sicherungen des Typs 'Immer inkrementell - Inkrementell'. Im vorliegenden Beispiel wird die Verwaltungsklasse `mgmt_ifincr28` für die Domäne `domain1` und die Maßnahmengruppe `prodbackups` erstellt. Mit dem Namen der Verwaltungsklasse wird eine Sicherungsstrategie 'Immer inkrementell - Inkrementell' beschrieben, mit der 28 Sicherungsversionen aufbewahrt werden:

      ```
      define mgmtclass domain1 prodbackups mgmt_ifincr28
      description="Aufbewahrung von 28 Sicherungsversionen"
      ```

   b. Erstellen Sie eine Sicherungskopiengruppe für Ihre Sicherungen des Typs 'Immer inkrementell - Inkrementell'. Im vorliegenden Beispiel wird eine Standardsicherungskopiengruppe für die Domäne `domain1`, die Maßnahmengruppe `prodbackups` und die Verwaltungsklasse `mgmt_ifincr28` erstellt:

      ```
      define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
      ```

      Die Einträge `standard type=backup` sind Standardwerte und müssen nicht unbedingt angegeben werden. Im vorliegenden Beispiel sollen sie lediglich veranschaulichen, dass der Kopiengruppenname `STANDARD` lautet und die Kopiengruppe den Typ `backup` (anstelle von `archive`) hat.

   c. Aktualisieren Sie die Sicherungskopiengruppe mit den gewünschten Einstellungen für Version, Aufbewahrungsdauer und Verfall:

      Hinweis: In Data Protection for VMware Version 6.2 und 6.3 basieren Version, Aufbewahrungsdauer und Verfall einer Sicherung auf der Granularitätsstufe der Sicherungskette. Diese Methode bedeutet, dass trotz der Erstellung von Sicherungen des Typs 'Immer inkrementell - Vollständig' und des Typs 'Immer inkrementell - Inkrementell' (im Rahmen der Sicherungsstrategie 'Immer inkrementell - Vollständig' aus Version 6.2 und 6.3) für den Versionsverfall ausschließlich vollständige Sicherungen berücksichtigt werden. In Data Protection for VMware Version 6.4 (oder höher) basieren Version, Aufbewahrungsdauer und Verfall einer Sicherung auf der Granularitätsstufe einer einzelnen Sicherung. Diese Methode bedeutet, dass beim Versionsverfall sowohl Sicherungen des Typs 'Immer inkrementell - Vollständig' als auch Sicherungen des Typs 'Immer inkrementell - Inkrementell' berücksichtigt werden.

      Der Parameter `verexists` gibt an, wie viele VM-Sicherungsversionen maximal auf dem Server aufbewahrt werden sollen. Wenn eine Sicherungsoperation des Typs 'Immer inkrementell - Inkrementell' dazu führt, dass diese Anzahl überschritten wird, markiert der Server die älteste im Serverspeicher vorhandene Sicherungsversion als verfallen. Im vorliegenden Beispiel ist

verexists=28 angegeben. Dieser Wert bedeutet, dass maximal 28 Versionen der VM-Sicherung auf dem Server aufbewahrt werden.

Der Parameter retextra gibt an, wie viele Tage eine VM-Sicherungsversion maximal aufbewahrt wird, bevor die Version inaktiv wird. Im vorliegenden Beispiel ist retextra=nolimit angegeben. Dieser Wert bedeutet, dass die maximale Anzahl von inaktiven VM-Sicherungsversionen unbegrenzt aufbewahrt wird. Bei Angabe von verexists wird der Wert für nolimit jedoch durch den Wert für verexists überlagert. Im vorliegenden Beispiel werden daher maximal 28 inaktive VM-Sicherungsversionen auf dem Server aufbewahrt.

Basierend auf den in diesem Schritt beschriebenen Einstellungen wird die Sicherungskopiengruppe wie folgt aktualisiert.

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

In diesem Beispiel besteht die vorhandene Umgebung von Data Protection for VMware Version 6.3 aus den folgenden Hosts und Zeitplänen:

- Ein ESX-Cluster (esxcluster) enthält zwei ESX-Hosts (esxhost1, esxhost2).
- Mit dem Zeitplan bup_esxcluster_full wird eine wöchentliche Sicherung des Typs 'Immer inkrementell - Vollständig' jedes ESX-Hosts mit dem Knoten der Einheit zum Versetzen von Daten namens dm1 ausgeführt.
- Mit dem Zeitplan bup_esxcluster_incr wird eine tägliche Sicherung des Typs 'Immer inkrementell - Inkrementell' jedes ESX-Hosts mit dem Knoten der Einheit zum Versetzen von Daten namens dm2 ausgeführt.

Führen Sie die folgenden Tasks für die Sicherungszeitpläne in der Data Protection for VMware vSphere-GUI aus:

a. Starten Sie die Data Protection for VMware vSphere-GUI, indem Sie im vSphere-Clientfenster für Lösungen und Anwendungen (Solutions and Applications) auf das Symbol klicken.
b. Klicken Sie im Fenster **Einführung** auf die Registerkarte **Sichern**, um das Fenster **Sicherungszeitpläne verwalten** zu öffnen.
c. Lokalisieren Sie den Sicherungszeitplan (für Sicherungen des Typs 'Immer inkrementell - Vollständig' oder 'Immer inkrementell - Inkrementell'), der aktualisiert werden muss. In der vorliegenden Prozedur wird der Zeitplan für 'Immer inkrementell - Vollständig', bup_esxcluster_full, verwendet.
d. Klicken Sie mit der rechten Maustaste auf den Zeitplan und wählen Sie **Eigenschaften** aus.
e. Rufen Sie die Seite **Zeitplan** auf und geben Sie **Inkrementell** in der Dropdown-Liste **Sicherungsstrategie** an.
f. Klicken Sie auf **OK**, um Ihre Aktualisierung zu speichern.
g. Lokalisieren Sie den Sicherungszeitplan für Sicherungen des Typs 'Immer inkrementell - Inkrementell'. Klicken Sie mit der rechten Maustaste auf den Zeitplan und wählen Sie **Löschen** aus. Da der Zeitplan bup_esxcluster_full für 'Immer inkrementell - Vollständig' in 'Immer inkrementell - Inkrementell' geändert wurde, wird dieser Zeitplan für 'Immer inkrementell - Inkrementell' nicht mehr benötigt.

3. Da Sie jetzt über einen Zeitplan für Sicherungen des Typs 'Immer inkrementell - Inkrementell' verfügen, können Sie die Anzahl der Knoten der Einheit zum Versetzen von Daten reduzieren, indem Sie sie konsolidieren:
Im vorliegenden Beispiel werden zwei Knoten der Einheit zum Versetzen von Daten in einem einzigen Knoten der Einheit zum Versetzen von Daten konsolidiert.

a. Öffnen Sie auf dem vStorage-Sicherungsserver eine Eingabeaufforderung und wechseln Sie in das Verzeichnis, in dem sich die Optionsdatei für den Knoten `dm1` befindet.
b. Aktualisieren Sie diese Datei in einem Texteditor (z. B. 'Editor') mit den folgenden Optionen:
   1) Geben Sie `vmmaxparallel` an, um die Anzahl der virtuellen Maschinen zu steuern, die gleichzeitig durch `dm1` gesichert werden:

      ```
      vmmaxparallel=2
      ```

      Der Standardwert und der Mindestwert ist 1. Der Maximalwert ist 50.

      Tipp: Setzen Sie für jeden Knoten der Einheit zum Versetzen von Daten, den Sie entfernen, den Wert für `vmmaxparallel` um 1 herauf.

      Alternativ können Sie auch `vmlimitperhost` angeben, um die Anzahl der virtuellen Maschinen zu steuern, die gleichzeitig durch den Knoten `dm1` aus demselben ESX-Host gesichert werden:

      ```
      vmlimitperhost=1
      ```

      Diese Option ist hilfreich, wenn Sie verhindern wollen, dass ein Host überlastet wird. Der Standardwert ist 0 (keine Begrenzung). Der Mindestwert ist 1. Der Maximalwert ist 50.
c. Melden Sie sich beim IBM Spectrum Protect-Server an. Verwenden Sie den Verwaltungsbefehlszeilenclient (`dsmadmc`), um die maximale Anzahl gleichzeitiger VM-Sicherungssitzungen anzugeben, die eine Verbindung zum Server herstellen können. Beispiel:

   ```
   maxsessions=4
   ```

   Der Standardwert ist 25. Der Mindestwert ist 2.

4. Prüfen Sie, ob die aktualisierten Knoten der Einheiten zum Versetzen von Daten ordnungsgemäß arbeiten:
   a. Starten Sie die Data Protection for VMware vSphere-GUI, indem Sie im vSphere-Client im Fenster für Lösungen und Anwendungen (Solutions and Applications) auf das Symbol klicken.
   b. Klicken Sie im Fenster **Einführung** auf die Registerkarte **Konfiguration**, um die Seite **Konfigurationsstatus** anzuzeigen.
   c. Wählen Sie auf der Seite **Konfigurationsstatus** das vCenter aus, das Sie in Schritt 1 geschützt haben. Klicken Sie auf einen Knoten der Einheit zum Versetzen von Daten, um seine Statusinformationen im Teilfenster **Statusdetails** anzuzeigen. Wenn für einen Knoten eine Warnung oder ein Fehler angezeigt wird, klicken Sie auf diesen Knoten und beheben Sie das Problem unter Zuhilfenahme der Informationen im Teilfenster **Statusdetails**. Wählen Sie anschließend den Knoten aus und klicken Sie auf **Ausgewählten Knoten prüfen**, um festzustellen, ob das Problem gelöst wurde. Klicken Sie auf 'Aktualisieren', um alle Knoten erneut zu testen.

Ergebnisse

Nach dem erfolgreichen Abschluss aller Tasks ist die Umgebung für die Verwendung in einer Sicherungsstrategie 'Immer inkrementell - Inkrementell' bereit.

Einschränkungen: Nachdem Sie Zeitpläne für Sicherungen des Typs 'Immer inkrementell - Vollständig' auf Sicherungen des Typs 'Immer inkrementell - Inkrementell' migriert haben, müssen Sie die folgenden Einschränkungen beachten:

- Die erneute Änderung der migrierten Zeitpläne in Sicherungen des Typs 'Immer inkrementell - Vollständig' pro VM (Dateibereich) wird nicht unterstützt.
- Die Verwendung einer früheren Version der IBM Spectrum Protect-Einheit zum Versetzen von Daten mit einem migrierten Dateibereich wird nicht unterstützt.
- Wenn ein Dateibereich (mindestens) eine Sicherung des Typs 'Immer inkrementell - Inkrementell' enthält, wird eine Sicherung des Typs 'Immer inkrementell - Vollständig' nicht unterstützt.

Beispiel für die Versionssteuerung mit dem Parameter `verexists`

In diesem Beispiel für die Migration eines Zeitplans verwendet Data Protection for VMware Version 6.3 die beiden folgenden Sicherungszeitpläne:

- `-mode=full`: Eine wöchentliche Sicherung des Typs 'Immer inkrementell - Vollständig' wird geplant (sonntags) und auf dem Server werden maximal vier VM-Sicherungsversionen aufbewahrt (`verexists=4`).
- `-mode=incr`: An jedem Werktag wird eine Sicherung des Typs 'Immer inkrementell - Inkrementell' geplant (Montag bis Samstag).

In einem Zeitraum von vier Wochen werden 28 Sicherungen erstellt:

- Vier Sicherungen des Typs 'Immer inkrementell - Vollständig' (eine wöchentliche vollständige Sicherung multipliziert mit vier Wochen)
- 24 Sicherungen des Typs 'Immer inkrementell - Inkrementell' (inkrementelle Sicherungen an sechs Werktagen multipliziert mit vier Wochen)

Da Data Protection for VMware Version 6.3 lediglich vollständige Sicherungen bei der Zählung berücksichtigt, bewahrt die Einstellung `verexists=4` alle 28 Sicherungen auf.

Erstellen Sie den folgenden Zeitplan, um dasselbe Schutzniveau mit Data Protection for VMware Version 6.4 (oder höher) und der Sicherungsstrategie 'Immer inkrementell - Inkrementell' zur Verfügung zu stellen:
`-mode=iffull`: Eine tägliche Sicherung des Typs 'Immer inkrementell - Vollständig' wird geplant und der Parameter `verexists` wird auf 28 gesetzt.
In einem Zeitraum von vier Wochen werden 28 Sicherungen erstellt:

- Eine Sicherung des Typs 'Immer inkrementell - Vollständig' (Erstsicherung multipliziert mit einem Tag)
- 27 Sicherungen des Typs 'Immer inkrementell - Inkrementell' (tägliche immer inkrementelle Sicherungen multipliziert mit 27 Tagen)

Da Data Protection for VMware Version 6.4 (oder höher) sowohl Sicherungen des Typs 'Immer inkrementell - Vollständig' als auch Sicherungen des Typs 'Immer inkrementell - Inkrementell' bei der Zählung berücksichtigt, werden mit dem Wert `verexists=28` alle 28 Sicherungen aufbewahrt.

Anhang C. 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 IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Website "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 ihrer Tochtergesellschaften in den USA und anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

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.

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 und/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 nicht weitergeben, anzeigen oder 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 nicht vervielfältigen, weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Rechte

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 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 genutzten 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, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

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

Ein Glossar mit Begriffen und Definitionen für die IBM Spectrum Protect-Produktfamilie ist verfügbar.

Siehe das Glossar für IBM Spectrum Protect.

Index

K

L

M

N

P

R

S

T

U

V

W

Z

Programmnummer: 5725-X00

Gedruckt in Deutschland