IBM Spectrum Protect for Virtual Environments
Version 8.1.6

Data Protection for Microsoft Hyper-V Installations- und Benutzerhandbuch

IBM Spectrum Protect for Virtual Environments
Version 8.1.6

Data Protection for Microsoft Hyper-V Installations- und Benutzerhandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 267 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

Diese Veröffentlichung enthält Übersichts- und Planungsinformationen sowie Benutzeranweisungen für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Zielgruppe dieser Veröffentlichung

Diese Veröffentlichung ist für Administratoren und Benutzer bestimmt, die für die Implementierung einer Sicherungslösung mit IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V in einer der unterstützten Umgebungen verantwortlich sind.

In dieser Veröffentlichung wird vorausgesetzt, dass Sie über Kenntnisse bezüglich der folgenden Anwendungen verfügen:

- Microsoft Windows Server 2016 mit installierter Hyper-V-Rolle
- Microsoft Windows Server 2012 oder 2012 R2 mit installierter Hyper-V-Rolle
- IBM Spectrum Protect-Client für Sichern/Archivieren
- IBM Spectrum Protect-Server

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 für Version 8.1.6

In IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Version 8.1.6 werden neue Funktionen und Aktualisierungen eingeführt.

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

Die folgenden Funktionen und Aktualisierungen sind für dieses Release neu:

In-Guest-Anwendungen schützen

Verwenden Sie Data Protection for Microsoft Hyper-V, um Microsoft Exchange Server und Microsoft SQL Server zu schützen, die innerhalb von Hyper-V-VM-Gastmaschinen in einer Microsoft Hyper-V-Umgebung ausgeführt werden.

Sie können anwendungskonsistente Sicherungen der VMs erstellen, die Microsoft Exchange Server- oder Microsoft SQL Server-Daten hosten. Anschließend können Sie bestimmte Anwendungssicherungen von den VMs zurückschreiben.

Weitere Informationen siehe:

- „Microsoft Exchange Server-Daten in Hyper-V-Umgebungen schützen" auf Seite 105
- „Microsoft SQL Server-Daten in Hyper-V-Umgebungen schützen" auf Seite 123
- „INCLUDE.VMTSMVSS" auf Seite 194

Konfiguration von Data Protection for Microsoft Hyper-V mit der Data Protection for Microsoft Hyper-V-Verwaltungskonsole oder einem PowerShell-Cmdlet überprüfen

Um Ihnen die Behebung von Konfigurationsproblemen zu erleichtern, können Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole oder das PowerShell-Cmdlet **Test-DpHvConfiguration** zum Überprüfen einer Data Protection for Microsoft Hyper-V-Konfiguration verwenden.

Weitere Informationen siehe:

- „Konfiguration von Data Protection for Microsoft Hyper-V überprüfen" auf Seite 85
- „Beispiele für Data Protection for Microsoft Hyper-V-Cmdlets" auf Seite 157

Umgebung konfigurieren, in der die virtuellen Maschinen mehrerer Tenants auf demselben Server gehostet werden

Wenn Sie Data Protection for Microsoft Hyper-V mit dem Konfigurationsassistenten konfigurieren, wird eine Standardnamenskonvention für die automatisch erstellten Knoten verwendet.

Wenn Sie jedoch eine Speicherumgebung unterstützen möchten, in der die virtuellen Maschinen (VMs) mehrerer Tenants auf demselben Server gehostet werden, müssen Sie den Standardknotennamen ein Präfix, ein Suffix oder beides hinzufügen.

Anweisungen finden Sie in „Knotennamen anpassen" auf Seite 23.

VM-Platten mit einer Größe von bis zu 8 TB sichern

Sie können jetzt VM-Platten (VHDX) mit einer Größe von bis zu 8 TB sichern. Verwenden Sie die Option `vmmaxvirtualdisks`, um die maximale Größe von VHDX-Platten anzugeben, die in Sicherungsoperationen eingeschlossen werden sollen. Geben Sie mit der Option `vmskipmaxvirtualdisks` an, ob bei VMs, die die maximale VHDX-Größe überschreiten, die Sicherung übersprungen werden oder die Sicherungsoperation fehlschlagen soll.

Weitere Informationen finden Sie unter:

- „Vmmaxvirtualdisks" auf Seite 213
- „Vmskipmaxvirtualdisks" auf Seite 216

VM-Platten bei Sicherungsoperationen unter Windows Server 2012 ein- oder ausschließen

Für Hyper-V-Hosts unter Windows Server 2012-Betriebssystemen können Sie jetzt VM-Platten (VHDX) für Sicherungsoperationen auswählen.

Informationen zum Auswählen von VM-Platten für Ad-hoc-Sicherungsoperationen finden Sie in „Ad-hoc-Sicherung einer virtuellen Maschine ausführen" auf Seite 91.

Informationen zum Auswählen von VM-Platten durch Ändern von Einstellungen in der Optionsdatei (`dsm.opt`) oder in der Befehlszeilenschnittstelle enthalten die folgenden Abschnitte:

- „`Exclude.vmdisk`" auf Seite 186
- „`Include.vmdisk`" auf Seite 191
- „`Domain.vmfull`" auf Seite 183
- „**`Backup VM`**" auf Seite 166
- „Ad-hoc-Sicherung einer virtuellen Maschine ausführen" auf Seite 91

Diese Funktion war zuvor nur unter Windows Server 2016 verfügbar.

In einer Clusterumgebung von Flexibilität beim Upgrade profitieren

In Umgebungen mit mehreren Clustern und Hosts können Sie einen gestaffelten Zeitplan für das Upgrade von Data Protection for Microsoft Hyper-V verwenden. Wenn Sie auf einem der Cluster oder Hosts eine neuere Produktversion installieren, können frühere Versionen der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der PowerShell-Cmdlets eine Verbindung zu der neueren Version herstellen. Dadurch haben Sie mehr Zeit, um ein Upgrade für Ihre Umgebung durchzuführen.

Weitere Informationen finden Sie in „Kompatibilität mit verschiedenen Versionen" auf Seite 19.

Für mehr Sicherheit Zertifikate akzeptieren

Um zu mehr Sicherheit in Ihrer Umgebung beizutragen, werden Sie zum Akzeptieren von Sicherheitszertifikaten aufgefordert, wenn Sie eine Verbindung zu neuen Hyper-V-Hosts herstellen.

Weitere Informationen siehe:

- „Data Protection for Microsoft Hyper-V-Verwaltungskonsole starten" auf Seite 75
- „Verwendung von PowerShell-Cmdlets mit Data Protection for Microsoft Hyper-V vorbereiten" auf Seite 151

Zusätzliche Installationsoptionen sind verfügbar

Bei einer Standardinstallation werden alle Komponenten von Data Protection for Microsoft Hyper-V installiert. Sie können jedoch erweiterte Installa-

tionsoptionen verwenden, um nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole oder nur die Einheit zum Versetzen von Daten zu installieren.

- Installieren Sie für die Fernverwaltung von Data Protection for Microsoft Hyper-V nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole. Anweisungen finden Sie in „Nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installieren" auf Seite 30.
- Installieren Sie für Sicherungs- und Zurückschreibungsoperationen und Zurückschreibungsoperationen mit In-Guest-Anwendungsschutz nur die Einheit zum Versetzen von Daten. Anweisungen finden Sie in „Nur die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten installieren" auf Seite 32.

Die separate Installation von Recovery Agent ist nicht mehr verfügbar. Recovery Agent ist in der Installation der Einheit zum Versetzen von Daten enthalten.

Eine Liste der neuen Funktionen und Aktualisierungen für das aktuelle und vorherige Release der Version 8.1 finden Sie in Aktualisierungen für Data Protection for Microsoft Hyper-V.

Kapitel 1. Schutz für virtuelle Microsoft Hyper-V-Maschinen

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ist ein lizenziertes Produkt, das Speicherverwaltungsservices für virtuelle Maschinen (VMs) in einer Microsoft Hyper-V-Umgebung zur Verfügung stellt.

Data Protection for Microsoft Hyper-V nutzt den IBM Spectrum Protect-Client für Sichern/Archivieren, um virtuelle Hyper-V-Maschinen unter den folgenden Betriebssystemen zu schützen:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Virtuelle Hyper-V-Maschinen sichern

Data Protection for Microsoft Hyper-V erstellt eine Sicherung 'Immer inkrementell - Vollständig' oder 'Immer inkrementell - Inkrementell' von Hyper-V-VMs (VM - virtuelle Maschine). Von der VM wird eine konsistente Momentaufnahme erstellt und die VM wird auf dem IBM Spectrum Protect-Server gesichert.

Sie können Hyper-V-VMs sichern, die sich auf einer lokalen Platte, einer an ein SAN angeschlossenen Platte oder einem freigegebenen Clustervolume (Cluster Shared Volume, CSV) befinden. Sie können beispielsweise VMs sichern, die auf CSVs in einer Hyper-V-Clusterumgebung oder auf SMB-Dateifreigaben (SMB - Server Message Block) auf einem fernen System gespeichert sind. Sie können jedes Gastbetriebssystem sichern, das vom Hyper-V-Server auf fernen freigegebenen Verzeichnissen unterstützt wird, unabhängig davon, ob IBM Spectrum Protect diese direkt unterstützt.

Die folgenden Sicherungstypen werden für Microsoft Hyper-V-VMs mit virtuellen Platten im VHDX-Plattenformat unterstützt:

Sicherung 'Immer inkrementell - Vollständig'
Erstellt eine Sicherung von Momentaufnahmeplattendaten auf dem IBM Spectrum Protect-Server.

Sicherung 'Immer inkrementell - Inkrementell'
Erstellt eine Momentaufnahme der Blöcke, die sich seit der letzten Sicherung 'Immer inkrementell - Vollständig' oder 'Immer inkrementell - Inkrementell' geändert haben.

Wenn Sie den Hyper-V-Host unter dem Betriebssystem Windows Server 2012 oder Windows Server 2012 R2 ausführen, wird Microsoft Volume Shadow Copy Service (VSS) verwendet, um eine konsistente Momentaufnahme der VM zu erstellen. Die zwischen den Sicherungen an der VM vorgenommenen Änderungen werden in einer Momentaufnahmedifferenzierungsdatei protokolliert.

Wenn Sie den Hyper-V-Host unter dem Betriebssystem Windows Server 2016 oder höher ausführen, werden Momentaufnahmen mithilfe einer Windows-API erstellt und die zwischen den Sicherungsoperationen an einer VHDX-Platte vorgenommen Änderungen werden mit RCT (Resilient Change Tracking) verfolgt.

Sicherungen virtueller Maschinen mit Volume Shadow Copy Service (VSS)

Bei Hyper-V-Sicherungen unter Windows Server 2012 und 2012 R2 wird Microsoft Volume Shadow Copy Service (VSS) verwendet, um während Sicherungsoperationen konsistente Momentaufnahmen von virtuellen Maschinen (VMs) zu erstellen.

Bei einer anfänglichen Sicherungsoperation 'Immer inkrementell - Vollständig' erstellt der Client eine Momentaufnahme der Festplatte der virtuellen Maschine (VHDX) und sendet den Inhalt an den IBM Spectrum Protect-Server. Änderungen, die nach der anfänglichen Momentaufnahme auftreten, werden in einer Momentaufnahmedifferenzierungsdatei (`.avhdx`) gespeichert. Bei nachfolgenden Sicherungsoperationen 'Immer inkrementell - Inkrementell' werden nur die Daten gesichert, die sich seit der letzten Sicherung geändert haben.

Wenn Sie eine Sicherung 'Immer inkrementell - Inkrementell' ausführen, bevor Sie eine Sicherung 'Immer inkrementell - Vollständig' erstellen, führt der Client eine Sicherung 'Immer inkrementell - Vollständig' aus.

Verarbeitung von Momentaufnahmen bei VSS-Sicherungen

Bei jeder VM-Sicherung wird eine neue Momentaufnahmedifferenzierungsdatei (`.avhdx`) erstellt, um die Änderungen an der VM zu verfolgen, die nach der Sicherungsoperation auftreten. Diese Differenzierungsmomentaufnahme wird auf dem Hyper-V-Host gespeichert, um die Schreibvorgänge für die nächste inkrementelle Sicherung zu erfassen.

In vorherigen Releases von Data Protection for Microsoft Hyper-V konnte eine Momentaufnahme nur eine einzige VM enthalten. Dieses Verhalten konnte bei Clustersicherungsoperationen Konkurrenzsituationen bei der Planung verursachen, weil zu viele Momentaufnahmen erstellt werden mussten. Mithilfe der Option `vmmaxpersnapshot`, die in Data Protection for Microsoft Hyper-V Version 8.1.2 eingeführt wurde, können Sie die Anzahl der für eine Sicherungsoperation erstellten Momentaufnahmen reduzieren, indem Sie mehrere VMs in einer einzigen Momentaufnahme gruppieren. Weitere Informationen finden Sie in „Geplante VM-Sicherungen für Windows Server 2012- und 2012 R2-Cluster optimieren" auf Seite 72.

Sicherungen virtueller Maschinen mit Resilient Change Tracking (RCT)

Bei Hyper-V-Sicherungen unter Microsoft Windows Server 2016 oder höheren Versionen wird das Feature Resilient Change Tracking (RCT) zum Sichern von virtuellen Maschinen (VMs) verwendet.

RCT ist ein Feature, das integrierte Funktionalität zur Überwachung geänderter Blöcke für Hyper-V-VM-Platten bereitstellt. Data Protection for Microsoft Hyper-V verwendet RCT, um Änderungen an einer VM-Platte (VHDX) zu verfolgen, die zwischen Sicherungsoperationen vorgenommen werden. Die Änderungen werden auf der Datenblockebene verfolgt. Nur Blöcke, die sich seit der letzten Sicherungsoperation geändert haben, sind Kandidaten für die nächste Sicherung 'Immer inkrementell - Inkrementell'.

Windows Server 2016 bietet außerdem die Möglichkeit, Sicherungsmomentaufnahmen (auch als Prüfpunkte bezeichnet) direkt zu erstellen, d. h. ohne Verwendung von Microsoft Volume Shadow Copy Service (VSS). (VSS wird jedoch noch immer

innerhalb von Windows-Gast-VMs verwendet, um die VMs für anwendungskonsistente Sicherungen in den Quiescemodus zu versetzen.)

Sie können mehrere VMs in einer einzigen Momentaufnahme gruppieren. Wird jedoch eine Gast-VM, die Anwendungen hostet, für Anwendungsschutz aktiviert, wird die VM-Momentaufnahme einzeln erstellt. Weitere Informationen zum Anwendungsschutz finden Sie in Kapitel 6, „In-Guest-Anwendungen schützen", auf Seite 105.

Für VM-Sicherungsoperationen mit RCT muss die Hyper-V-VM die Version 6.2 oder höher aufweisen.

Wenn Ihre VM unter dem Betriebssystem Windows Server 2012 R2 oder früher erstellt und später auf einen Host-Server mit Windows Server 2016 versetzt wurde (oder wenn der Host-Server auf Windows Server 2016 aktualisiert wurde), müssen Sie die VM offline setzen und ein Upgrade für die VM-Version durchführen, damit sie gesichert werden kann. Sie können die VM-Version mit dem Hyper-V-Manager oder dem Cmdlet **Update-VMVersion** aktualisieren.

In Data Protection for Microsoft Hyper-V Version 8.1.0 wird VSS verwendet, um VMs in der Hyper-V-Umgebung unter Windows Server 2016 zu sichern. Ab Version 8.1.2 wird für alle Hyper-V-VM-Sicherungsoperationen in Umgebungen mit Windows Server 2016 oder höher RCT verwendet. Wenn Sie ein Upgrade von Version 8.1.0 durchführen, wird eine Sicherung 'Immer inkrementell - Vollständig' ausgeführt, wenn Sie Ihre VMs unter Windows Server 2016 zum ersten Mal mit Data Protection for Microsoft Hyper-V Version 8.1.6 sichern, da in den VSS-Sicherungen früherer Versionen keine RCT-Informationen zur Überwachung von Änderungen enthalten sind.

Nachdem Sie eine VM mit RCT gesichert haben, können Sie nicht mehr Data Protection for Microsoft Hyper-V Version 8.1.0 verwenden, um VSS-Sicherungen für diese VM auszuführen.

Verarbeitung von Momentaufnahmen bei RCT-Sicherungen

Während einer Sicherungsoperation 'Immer inkrementell - Vollständig' für eine VM wird eine Momentaufnahme der VM-Platte erstellt und der Inhalt der Momentaufnahme wird auf dem IBM Spectrum Protect-Server gesichert. Die Momentaufnahme wird automatisch gelöscht, nachdem die Sicherungsoperation abgeschlossen ist.

Während der nächsten Sicherung 'Immer inkrementell - Inkrementell' wird eine neue Momentaufnahme erstellt und anhand der RCT-Informationen zur Überwachung von Änderungen aus der vorherigen Sicherungsoperation überprüft, um festzustellen, welche Daten sich geändert haben. Nur die geänderten Blöcke werden auf dem IBM Spectrum Protect-Server gesichert.

Nach der Sicherungsoperation wird die Momentaufnahme von Hyper-V mit der VM zusammengeführt und die Momentaufnahmedifferenzierungsdatei (`.avhdx`) wird automatisch gelöscht. Dieser Prozess unterscheidet sich von der VSS-Momentaufnahmeverarbeitung unter den Betriebssystemen Windows Server 2012 und 2012 R2, bei der die Momentaufnahmedifferenzierungsdatei zum Speichern von inkrementellen Änderungen auf der VM aufbewahrt wird.

Alle Momentaufnahmen, die Sie manuell oder mit einem anderen Sicherungsprodukt erstellen, wirken sich nicht auf die Sicherungskette aus, die vom RCT-Prozess erstellt wird. Sie können vor oder nach einer RCT-Sicherungsoperation in Data Pro-

tection for Microsoft Hyper-V Momentaufnahmen manuell oder mit Sicherungsprodukten anderer Anbieter erstellen. Die nächste inkrementelle Sicherungsoperation in Data Protection for Microsoft Hyper-V basiert dennoch auf den RCT-Informationen zur Überwachung von Änderungen aus der vorherigen Sicherungsoperation.

Verfügbare Funktionen für RCT-Sicherungen

Die meisten Data Protection for Microsoft Hyper-V-Funktionen, die unter Windows Server 2012 und 2012 R2 bereitgestellt werden, sind auch unter Windows Server 2016 verfügbar.

Momentaufnahmeoperationen unterscheiden sich jedoch bei VSS- und RCT-Sicherungen. Weitere Informationen finden Sie in „Verarbeitung von Momentaufnahmen bei RCT-Sicherungen" auf Seite 3.

Die Unterstützung für Host-Failover mit freigegebenen Clustervolumes (Cluster Shared Volumes, CSVs) ist gegenüber Version 8.1.0 und früheren Versionen unverändert; die Ausführung einer VM-Sicherung während eines schrittweisen Upgrades eines Betriebssystems für einen Hyper-V-Cluster wird jedoch nicht unterstützt.

Abfrage von RCT-Sicherungen

Sie können den Befehl **query VM** verwenden, um Informationen zu einer VM anzuzeigen, die auf dem IBM Spectrum Protect-Server gesichert wurde. Geben Sie den Parameter `-detail` mit dem Befehl **query vm** an, um ausführliche Informationen zu der Sicherungsoperation anzuzeigen. Weitere Informationen finden Sie in „**Query VM**" auf Seite 174.

Sie können auch den Befehl **backup vm -preview** verwenden, um die VM-Plattenpositionen anzuzeigen, die für den Befehl **backup vm** verwendet werden können. Weitere Informationen finden Sie in „**Backup VM**" auf Seite 166.

Zugehörige Konzepte:

„Upgrade für Data Protection for Microsoft Hyper-V durchführen" auf Seite 19

„Einschränkungen bei Hyper-V-Sicherungsoperationen" auf Seite 12

„Sicherungen virtueller Maschinen mit Volume Shadow Copy Service (VSS)" auf Seite 2

Zugehörige Tasks:

„Von VSS-Sicherungen auf RCT-Sicherungen migrieren" auf Seite 26

Zugehörige Verweise:

Anhang A, „Fehlerbehebung", auf Seite 235

Virtuelle Hyper-V-Maschinen zurückschreiben

Zum Zurückschreiben von virtuellen Hyper-V-Maschinen sind mehrere Methoden verfügbar. Sie können eine vollständige virtuelle Maschine zurückschreiben, eine vollständige virtuelle Maschine an eine alternative Position zurückschreiben oder einzelne Dateien aus einer virtuellen Maschine (VM) zurückschreiben.

Vollständige VM-Zurückschreibung

Vollständige Hyper-V-VM zurückschreiben
Jede Hyper-V-VM-Sicherung wird als Einheit von dem IBM Spectrum Protect-Server zurückgeschrieben. Sie können alle Gastbetriebssysteme zurückschreiben, die vom Hyper-V-Server gehostet

werden, unabhängig davon, ob das Gastbetriebssystem von IBM Spectrum Protect unterstützt wird.

Bei einer Zurückschreibungsoperation in Data Protection for Microsoft Hyper-V ist sichergestellt, dass derselbe Block auf der Produktionsplatte nur einmal zurückgeschrieben wird. Ältere Sicherungsversionen verfallen entsprechend der Verwaltungsklassenmaßnahme des IBM Spectrum Protect-Servers, die der virtuellen Maschine zugeordnet wurde.

Vollständige Hyper-V-VM an eine alternative Position zurückschreiben
Beim Zurückschreiben einer Hyper-V-VM können Sie einen alternativen VM-Namen, eine alternative Position auf dem Hyper-V-Host oder beides verwenden. Sie können eine Hyper-V-VM auch mithilfe der Data Protection for Microsoft Hyper-V-Verwaltungskonsole auf einen anderen Hyper-V-Host zurückschreiben. Müssen Sie die Befehlszeile zum Zurückschreiben einer VM auf einen anderen Host verwenden, müssen Sie die Zurückschreibungsoperation von dem Hyper-V-Host aus ausführen, auf den die VM zurückgeschrieben wird.

Dateien mit der Schnittstelle für Dateizurückschreibung zurückschreiben
Verwenden Sie die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung, um eine Datei oder mehrere Dateien über eine webbasierte Schnittstelle zurückzuschreiben. Dateieigner können mit minimaler Administratorunterstützung Dateien in einer VM-Sicherung suchen und zurückschreiben. Zudem können Help-Desk-Mitarbeiter die Schnittstelle für Dateizurückschreibung verwenden, um Dateien anstelle der Dateieigner zurückzuschreiben.

Weitere Informationen finden Sie in Kapitel 5, „Einführung in Dateizurückschreibungsoperationen", auf Seite 99.

Dateien mit Recovery Agent zurückschreiben
Verwenden Sie diese Zurückschreibungsmethode nur, wenn Sie In-Guest-Mountoperationen ausführen möchten. Dateien werden manuell von einer bereitgestellten Platte der virtuellen Maschine kopiert, auf die über ein iSCSI-Ziel oder eine iSCSI-Partition zugegriffen wird (iSCSI - Internet Small Computer System Interface). Für diese Methode muss IBM Spectrum Protect Recovery Agent installiert sein.

Weitere Informationen finden Sie in Kapitel 10, „Bereitstellung und Dateizurückschreibung", auf Seite 219.

Benutzerschnittstellen für Hyper-V-Operationen

Sie können mehrere Benutzerschnittstellen verwenden, um Data Protection for Microsoft Hyper-V-Operationen auszuführen. Die Einheit zum Versetzen von Daten muss auf dem Hyper-V-Host-Server oder auf jedem Host in einem Cluster installiert werden.

Die folgenden Benutzerschnittstellen sind für Data Protection for Microsoft Hyper-V-Operationen verfügbar:

Data Protection for Microsoft Hyper-V-Verwaltungskonsole
Eine grafische Benutzerschnittstelle (Graphical User Interface - GUI), mit der Sie tägliche Sicherungsmanagementtasks ausführen können, z. B. die

Sicherungen virtueller Maschinen (VMs) verwalten, VM-Sicherungen überwachen, Ad-hoc-Sicherungs- und Zurückschreibungsoperationen ausführen und die Konfiguration aktualisieren.

IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung
Eine webbasierte Schnittstelle, mit der Dateieigner oder Help-Desk-Mitarbeiter mit minimaler Administratorunterstützung eine oder mehrere Dateien aus einer VM-Sicherung zurückschreiben können. Der Administrator stellt eine URL für die Schnittstelle für Dateizurückschreibung bereit.

Einheit zum Versetzen von Daten
Eine Komponente, die auch als Client für Sichern/Archivieren bekannt ist und die bei Sicherungs- und Zurückschreibungsoperationen Daten auf den IBM Spectrum Protect-Server und von diesem Server versetzt.

Die Einheit zum Versetzen von Daten umfasst eine Befehlszeilenschnittstelle (**dsmc**-Befehle), die Sie für Sicherungs-, Abfrage-, Zurückschreibungs- und andere Operationen verwenden können.

Data Protection for Microsoft Hyper-V-Cmdlets
Windows PowerShell-Cmdlets, die Ihnen helfen, Data Protection for Microsoft Hyper-V-Operationen mit PowerShell-Scripts zu automatisieren.

IBM Spectrum Protect Recovery Agent
Ein Agent, der Funktionalität für virtuelle Bereitstellung und Dateizurückschreibung zur Verfügung stellt.

Die folgenden Abbildungen enthalten allgemeine Übersichten über Data Protection for Microsoft Hyper-V in den Umgebungen Windows Server 2016 oder höher und Windows Server 2012.

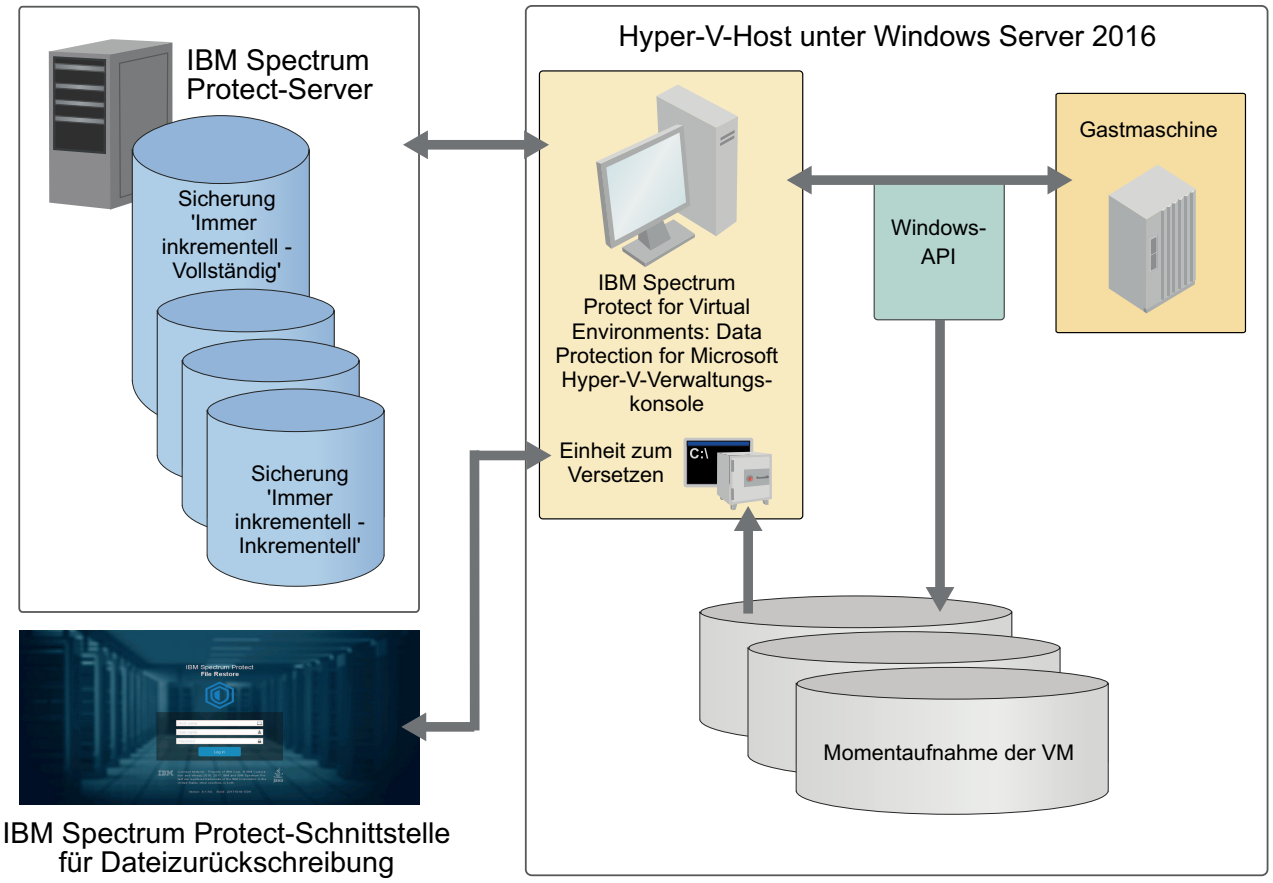


Abbildung 1. Allgemeine Übersicht über Data Protection for Microsoft Hyper-V in der Umgebung Windows Server 2016

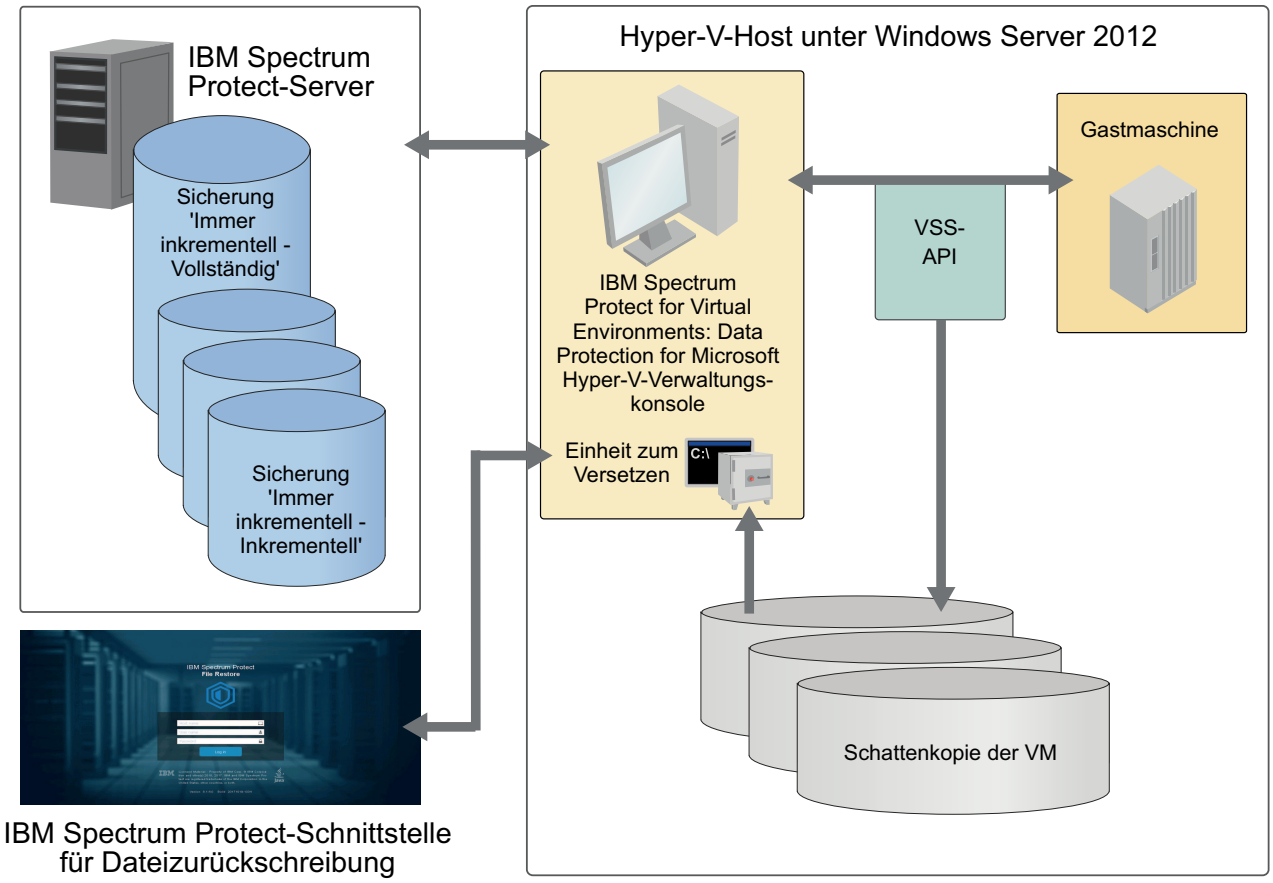


Abbildung 2. Allgemeine Übersicht über Data Protection for Microsoft Hyper-V in der Umgebung Windows Server 2012

Verwendung von IBM Spectrum Protect-Knoten in Data Protection for Microsoft Hyper-V

Data Protection for Microsoft Hyper-V kommuniziert bei Sicherungs-, Zurückschreibungs- und Mountoperationen über IBM Spectrum Protect-Knoten mit VMs.

Ein Knoten ist ein System, auf dem die Einheit zum Versetzen von Daten, Data Protection for Microsoft Hyper-V oder ein anderer Anwendungsclient installiert ist. Dieses System ist beim IBM Spectrum Protect-Server registriert. Jeder Knoten hat einen eindeutigen Namen (Knotennamen), mit dem der Server das System identifiziert. Kommunikation, Speichermaßnahme, Berechtigung und Zugriff für VM-Daten werden auf der Basis eines Knotens definiert.

In einer Data Protection for Microsoft Hyper-V-Umgebung besteht die einfachste Knotenkonfiguration aus zwei Knoten: dem *Knoten der Einheit zum Versetzen von Daten* und dem *Zielknoten*.

- Der Knoten der Einheit zum Versetzen von Daten stellt eine bestimmte Einheit zum Versetzen von Daten dar, die Daten von einem System auf ein anderes "versetzt". Unter diesem Knoten werden auf dem IBM Spectrum Protect-Server keine Daten gespeichert.
- Der Zielknoten ist der Knotenname, unter dem VM-Daten auf dem IBM Spectrum Protect-Server gespeichert werden.

In einer Clusterumgebung besteht die Knotenkonfiguration aus einem Zielknoten, der dem Namen des Clusters zugeordnet ist, und einem Knoten der Einheit zum Versetzen von Daten für jeden Host im Cluster.

Für Mountoperationen ist ein Mount-Proxy-Knotenpaar für jedes Hostsystem erforderlich. Ein Mount-Proxy-Knoten stellt das Linux- oder Windows-Proxy-System dar, das über eine iSCSI-Verbindung auf die bereitgestellten VM-Platten zugreift. Diese Knoten bewirken, dass die Dateisysteme auf den bereitgestellten VM-Platten als Mountpunkte auf dem Proxy-System zugänglich sind. Anschließend können Sie mit der Schnittstelle für Dateizurückschreibung einzelne Dateien zurückschreiben oder den Recovery Agent verwenden, um die Dateien durch Kopieren von den Mountpunkten auf Ihre lokale Platte abzurufen. Mount-Proxy-Knoten werden paarweise erstellt und werden vom Hyper-V-Hostknoten für jedes Windows- oder Linux-System benötigt, das als Proxy fungiert.

Zur Vereinfachung der Konfiguration erstellt der Data Protection for Microsoft Hyper-V-Konfigurationsassistent automatisch die verschiedenen Knoten, die für Sicherungs-, Zurückschreibungs- und Dateizurückschreibungsoperationen erforderlich sind. Außerdem führt der Konfigurationsassistent die folgenden Aktionen aus: Er registriert die Knoten auf dem IBM Spectrum Protect-Server, erstellt die notwendigen Proxy-Beziehungen und die lokalen Optionsdateien, konfiguriert die Services für den Knoten der Einheit zum Versetzen von Daten auf lokalen Windows-Hosts und startet diese Services.

Welche Typen von Knoten erstellt werden, ist von Ihrer Hyper-V-Umgebung abhängig sowie davon, ob Sie das Feature für Dateizurückschreibung aktiviert haben. Die Namen der Knoten, die erstellt werden, entsprechen einer bestimmten Namenskonvention, die auf dem Cluster- oder Hostnamen und dem Knotentyp basiert. Benutzerdefinierte Knotennamen können nicht verwendet werden.

Wenn Sie ein Upgrade von Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher durchführen und die Knoten bereits auf dem IBM Spectrum Protect-Server definiert sind, müssen Sie die Knotennamen auf dem Server aktualisieren. Weitere Informationen finden Sie in „Knoten auf dem IBM Spectrum Protect-Server umbenennen” auf Seite 20.

Die folgende Tabelle enthält einen Vergleich der verschiedenen Knotentypen in der Data Protection for Microsoft Hyper-V-Umgebung.

Tabelle 1. Typen der vom Konfigurationsassistenten konfigurierten Knoten

Knotentyp	**Namenskonvention**	**Beschreibung**
Zielknoten	Für einen eigenständigen Host: *Hostname*_HV_TGT Für einen Cluster: *Clustername*_HV_TGT	Der Knotenname, unter dem alle VM-Sicherungen auf dem IBM Spectrum Protect-Server gespeichert werden. Für Cluster werden VMs in einem einzigen Container auf dem IBM Spectrum Protect-Server unter einem einzigen Knotennamen (Clusterknoten) gespeichert, unabhängig von dem Host im Cluster, von dem sie gesichert werden.

Tabelle 1. Typen der vom Konfigurationsassistenten konfigurierten Knoten (Forts.)

Knotentyp	Namenskonvention	Beschreibung
Knoten der Einheit zum Versetzen von Daten	*Hostname*_HV_DM	Der Knoten, der Daten unter dem Zielknoten auf dem IBM Spectrum Protect-Server sichert. Unter dem Knoten der Einheit zum Versetzen von Daten werden keine Daten gespeichert. Für Cluster wird ein Knoten der Einheit zum Versetzen von Daten für jeden Host im Cluster erstellt.
Windows-Mount-Proxy-Knoten	*Hostname*_HV_MP_WIN	Einer der beiden Knoten in einem Mount-Proxy-Knotenpaar, das für Mountoperationen für die Schnittstelle für Dateizurückschreibung erforderlich ist. Für Cluster wird ein Windows-Mount-Proxy-Knoten für jeden Host im Cluster erstellt.
Linux-Mount-Proxy-Knoten	*Hostname*_HV_MP_LNX	Einer der beiden Knoten in einem Mount-Proxy-Knotenpaar, das für Mountoperationen für die Schnittstelle für Dateizurückschreibung erforderlich ist. Für Cluster wird ein Linux-Mount-Proxy-Knoten für jeden Host im Cluster erstellt.

Sie können den Standardknotennamen auch wie folgt ein Präfix und ein Suffix hinzufügen: *Präfix_Hostname*_HV_TGT_*Suffix*. Anweisungen finden Sie in „Knotennamen anpassen" auf Seite 23.

Maßnahmenverwaltung auf der Ebene der virtuellen Maschine

Die Speicheranforderungen für Sicherungen virtueller Hyper-V-Maschinen werden durch die Verwaltungsklassen des IBM Spectrum Protect-Servers festgelegt.

Sie können für unterschiedliche virtuelle Maschinen unterschiedliche Maßnahmen festlegen. Obwohl die Standardverwaltungsklasse die Speichermerkmale aller Hyper-V-Sicherungen festlegt, können Sie die Standardverwaltungsklasse überschreiben oder eine Verwaltungsklasse angeben, die für die Hyper-V-Steuerdateien verwendet werden soll.

Sie können die Standardverwaltungsklasse für Sicherungen virtueller Hyper-V-Maschinen mit der Option `vmmc` ändern. Sie können die Standardverwaltungsklasse für Hyper-V-Steuerdateien mit der Option `vmctlmc` ändern.

Zugehörige Verweise:

„`Vmmc`" auf Seite 215

„`Vmctlmc`" auf Seite 208

Sicherungsstrategie 'Immer inkrementell'

Eine Sicherungsstrategie 'Immer inkrementell' minimiert die Fenster zum Durchführen von Sicherungen und ermöglicht gleichzeitig eine schnellere Wiederherstellung Ihrer Daten.

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V bietet eine Sicherungsstrategie mit dem Namen 'Immer inkrementell'. Bei dieser Sicherungslösung ist nur eine einzige erste Gesamtsicherung erforderlich. Anschließend findet eine (für immer) fortlaufende Folge von inkrementellen Sicherungen statt. Die Sicherungslösung 'Immer inkrementell' bietet die folgenden Vorteile:

- Das Datenvolumen, das über das Netz übertragen wird, verringert sich.
- Die Datenzunahme verringert sich, weil alle inkrementellen Sicherungen ausschließlich diejenigen Blöcke enthalten, die sich seit der vorherigen Sicherung geändert haben.
- Ein Vergleich mit dem Sicherungsziel ist nicht erforderlich, da nur geänderte Blöcke angegeben werden.
- Die Auswirkung auf das Clientsystem wird minimiert.
- Das Fenster zum Durchführen von Sicherungen wird kürzer.
- Es ist nicht erforderlich, mit einem separaten Zeitplan eine erste Gesamtsicherung zu planen: Bei der ersten Ausführung einer immer inkrementellen Sicherung wird standardmäßig eine immer inkrementelle vollständige Sicherung ausgeführt.

Darüber hinaus ist der Zurückschreibungsprozess optimiert, da nur die letzten Versionen von Blöcken zurückgeschrieben werden, die zu einer zurückgeschriebenen Sicherung gehören. Da derselbe Bereich auf der Produktionsplatte nur ein einziges Mal wiederhergestellt wird, wird nicht mehrmals in denselben Block geschrieben. Infolge dieser Vorteile ist 'Immer inkrementell' die bevorzugte Sicherungsstrategie.

Momentaufnahmeverwaltung mit Windows PowerShell

Auf einem Microsoft Hyper-V-System können Sie Windows PowerShell „cmdlets" verwenden, um Momentaufnahmen, die mit IBM Spectrum Protect für eine virtuelle Hyper-V-Maschine erstellt wurden, zu entfernen (widerrufen).

Sie können diese Cmdlets nur auf dem Hyper-V-System verwenden. Sie können keine Momentaufnahmen vom Microsoft System Center Virtual Machine Manager entfernen.

Hyper-V-Systeme geben Warnnachrichten aus, um Sie vom Bearbeiten virtueller Festplatten, die Momentaufnahmen enthalten, oder virtueller Festplatten, denen eine Kette voneinander abweichender (immer inkrementeller) Momentaufnahmen zugeordnet ist, abzuhalten. Verwenden Sie stattdessen die Cmdlets zum Verwalten von Momentaufnahmen, um das Risiko eines Datenverlusts zu minimieren.

Eine Liste der für Hyper-V verfügbaren Cmdlets finden Sie unter http://technet.microsoft.com/en-us/library/hh848559.aspx und in den Informationen zu den verfügbaren Cmdlets. Verwenden Sie das Cmdlet **Get-VMSnapshot** mit dem Parameter **-SnapshotType Recovery** zum Abrufen von Momentaufnahmen, die einer virtuellen Maschine (VM) zugeordnet sind. Verwenden Sie das Cmdlet **Remove-VMSnapshot** zum Entfernen einer Momentaufnahme. Beim Entfernen einer Momentaufnahme werden die Informationen, die die Momentaufnahme in die Mo-

mentaufnahmedifferenzdatei (die AVHDX-Datei) geschrieben hat, wieder auf der Festplatte (die VHDX-Datei) der VM eingefügt.

Sind mehrere Typen von Momentaufnahmen für eine VM vorhanden, können Sie die Ergebnisse nach Momentaufnahmetyp filtern, wenn Sie eine Momentaufnahme entfernen. Führen Sie beispielsweise das folgende Cmdlet aus, um nur die Momentaufnahmen mit dem Momentaufnahmetyp "recovery" zu entfernen:

```
get-vmsnapshot * | where snapshottype -eq recovery | remove-vmsnapshot
```

Einschränkungen bei Hyper-V-Sicherungsoperationen

Lesen Sie die Beschreibung der Einschränkungen, bevor Sie eine Hyper-V-Sicherungsoperation starten. Einige Einschränkungen gelten für alle Hyper-V-Sicherungsoperationen, andere nur für Hyper-V-Sicherungen unter Windows Server 2012 oder 2012 R2 oder Windows Server 2016.

Einschränkungen bei allen Hyper-V-Sicherungen

Sie können auf einem Host nicht mehrere Sicherungs- oder Zurückschreibungsoperationen gleichzeitig ausführen. Wenn Sie beispielsweise zwei oder mehr Befehle **backup vm** oder **restore vm** gleichzeitig auf einem Host ausführen, schlägt eine der Sicherungs- oder Zurückschreibungsoperationen mit einer Fehlernachricht fehl. Ab Data Protection for Microsoft Hyper-V Version 8.1.6 stellt die Data Protection for Microsoft Hyper-V-Verwaltungskonsole Sicherungs- und Zurückschreibungstasks, die an denselben Host übergeben werden, in eine Warteschlange. Nur jeweils eine Sicherungs- oder Zurückschreibungstask ist auf einem Host aktiv und weitere Sicherungs- oder Zurückschreibungstasks befinden sich im Status 'Anstehend', bis die aktive Task beendet ist. Dann wird die nächste anstehende Task zur aktiven Task.

Data Protection for Microsoft Hyper-V unterstützt Sicherungsoperationen des Typs 'Immer inkrementell - Vollständig' und 'Immer inkrementell - Inkrementell' für Microsoft Hyper-V-VMs (VM - virtuelle Maschine), die das VHDX-Plattenformat aufweisen müssen. Falls Sie Hyper-V-VMs im VHD-Plattenformat sichern müssen: Verwenden Sie den Client für Sichern/Archivieren mit Version 7.1 (ohne Data Protection for Microsoft Hyper-V), um eine Imagesicherung der vollständigen VM zu erstellen. Geben Sie den Befehl **dsmc backup vm VM-Name -vmbackuptype=hypervfull -mode=full** des Clients für Sichern/Archivieren mit Version 7.1 aus, um eine Imagesicherung aller Objekte auf einer VHD- oder VHDX-Platte einer virtuellen Microsoft Hyper-V-Maschine zu erstellen. Konvertieren Sie optional `.vhd`-Dateien in das `.vhdx`-Format. Gehen Sie dabei gemäß den Anweisungen vor, die in der Microsoft-Dokumentation verfügbar sind.

Die Data Protection for Microsoft Hyper-V-Unterstützung für VM-Sicherungsoperationen ist auf VM-Namen und Namen von Hyper-V-Hosts oder Clustern beschränkt, die ausschließlich englische 7-Bit-ASCII-Zeichen enthalten. VM-Namen und Namen von Hyper-V-Hosts oder Clustern, die Zeichen aus anderen Sprachen verwenden, werden derzeit nicht unterstützt. Weitere Zeichenbeschränkungen sind in „Nicht unterstützte Zeichen in Namen von virtuellen Maschinen, Hyper-V-Hosts oder Clustern” auf Seite 236 aufgelistet.

Der Microsoft Windows-Dienst WMI (Windows Management Instrumentation, **winmgmt**) muss auf den Systemen ausgeführt werden, auf denen Data Protection for Microsoft Hyper-V, der IBM Spectrum Protect-Client für Sichern/Archivieren und

IBM Spectrum Protect Recovery Agent installiert sind. Operationen schlagen fehl, wenn der Dienst WMI nicht ausgeführt wird. Schalten Sie deshalb den Dienst WMI nicht aus.

Stellen Sie sicher, dass keine Exchange Server-Datenbanken auf RDM-Platten (Raw Device Mapped) im Modus für physische Kompatibilität, auf unabhängigen Platten oder auf Platten gespeichert sind, die über In-Guest-iSCSI direkt an die Gastmaschine angeschlossen sind.

Sie können keine VM mit einer gemeinsam genutzten virtuellen Festplatte sichern.

Momentaufnahmedifferenzsicherungsoperationen werden in der Hyper-V-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 Einheit zum Versetzen von Daten von Data Protection for Microsoft Hyper-V installiert ist.

Einschränkungen nur bei VSS-Sicherungen unter Windows Server 2012 und 2012 R2

Data Protection for Microsoft Hyper-V sichert keine VMs mit angeschlossenen physischen Platten (Durchgriffsplatten wie iSCSI-Platten). Diese Einschränkung tritt auf, weil Data Protection for Microsoft Hyper-V den Volume Shadow Copy Service (VSS) für Sicherungsoperationen verwendet und VSS keine Momentaufnahme der physischen Platten erstellen kann. Wenn Sie versuchen, eine VM mit angeschlossenen physischen Platten zu sichern, schlägt die Sicherungsoperation für die VM mit der physischen Platte fehl; die Sicherungsoperationen für andere VMs werden jedoch fortgesetzt.

Hyper-V-Konfigurationen unter dem Betriebssystem Windows Server 2012 R2 sind nicht mit Windows Server 2012 kompatibel. Deshalb schlägt eine Zurückschreibungsoperation von Windows Server 2012 R2 nach Windows Server 2012 fehl. Eine Zurückschreibungsoperation von Windows Server 2012 nach Windows Server 2012 R2 verläuft dagegen erfolgreich. Weitere Informationen finden Sie in der Microsoft Knowledge Base. Suchen Sie nach dem Artikel 2868279.

Einschränkungen nur bei RCT-Sicherungen unter Windows Server 2016 oder höher

Sie können eine VM-Sicherungsoperation nicht während eines schrittweisen Upgrades eines Betriebssystems für einen Hyper-V-Cluster ausführen.

Falls Data Protection for Microsoft Hyper-V die Informationen zur Überwachung von Änderungen nicht abrufen kann, wird eine Sicherung 'Immer inkrementell - Vollständig' ausgeführt.

Data Protection for Microsoft Hyper-V kann keine anwendungskonsistente Momentaufnahme einer VM erstellen, die sich im Status `Paused` befindet. Von einer VM im Status `Paused` kann nur eine absturzkonsistente Momentaufnahme erstellt werden. Definieren Sie beispielsweise die folgende Option in der Datei `dsm.opt`:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM-Name 1 1
```

Sie können Data Protection for Microsoft Hyper-V nicht unter Nano Server für Windows Server 2016 installieren. Sie können jedoch Data Protection for Microsoft Hyper-V unter Windows Server 2016 verwenden, um absturzkonsistente Sicherungen von Gast-VMs mit Nano Server zu erstellen.

Aktuelle Informationen zu bekannten Problemen und Einschränkungen finden Sie in Technote 1993768.

Dokumentationsressourcen

Die Software IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V stellt mehrere Komponenten zur Verfügung, mit deren Hilfe Sie Ihre virtuellen Maschinen schützen können. Infolgedessen werden mehrere Dokumentationsressourcen bereitgestellt, die Ihnen bei der Ausführung bestimmter Tasks helfen.

Tabelle 2. Data Protection for Microsoft Hyper-V-Dokumentationressourcen

Dokumentation	Inhalt	Position
IBM Spectrum Protect for Virtual Environments Data Protection for Microsoft Hyper-V Installations- und Benutzerhandbuch	Übersichtsinformationen, Strategieplanung, Installation, Konfiguration, Sicherungs- und Zurückschreibungsszenarios und Befehlszeilenreferenz.	IBM Knowledge Center unter https://www.ibm.com/support/knowledgecenter/SSERB6_8.1.6/ve.user/r_pdf_ve.html
Onlinehilfe für die GUI der Data Protection for Microsoft Hyper-V-Verwaltungskonsole	Sicherungs- und Zurückschreibungstasks im Zusammenhang mit virtuellen Hyper-V-Gastmaschinen, Konfiguration, Sicherungsmanagement und Sicherungsüberwachung.	Starten Sie die virtuellen Maschinen anhand einer der folgenden Methoden: • Auf dem Windows-System klicken Sie auf **Start** > **IBM Spectrum Protect** > **DP for Hyper-V-Verwaltungskonsole**. • Öffnen Sie ein Fenster mit Administratorbefehlseingabeaufforderung und geben Sie den folgenden Befehl ein: `"C:\Programme\IBM\SpectrumProtect\DPHyperV\DpHv.msc"` Greifen Sie mit einer der folgenden Methoden auf den Hilfetext zu: • Klicken Sie auf das Hilfesymbol ("?") in der Schnittstelle. • In der Menüleiste klicken Sie auf **Hilfe** > **Hilfe zu Data Protection for Microsoft Hyper-V**. Sie können auch die Taste F1 drücken, um die Onlinehilfe zu öffnen.
Onlinehilfe für die IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung	Einzelne Dateien und Ordner aus einer VM-Sicherung zurückschreiben.	Starten Sie die Schnittstelle für Dateizurückschreibung über die URL, die vom Dateizurückschreibungsadministrator bereitgestellt wird. Greifen Sie auf die Hilfe zu, indem Sie auf **Hilfe** > **Produktdokumentation** klicken.

Tabelle 2. Data Protection for Microsoft Hyper-V-Dokumentationressourcen (Forts.)

Dokumentation	Inhalt	Position
Onlinehilfe für den Befehlszeilenclient der Einheit zum Versetzen von Daten	Sicherungs- und Zurückschreibungstasks im Zusammenhang mit virtuellen Hyper-V-Gastmaschinen.	Starten Sie den Befehlszeilenclient der Einheit zum Versetzen von Daten anhand einer der folgenden Methoden: • Auf dem Windows-System rufen Sie **Start** > **IBM Spectrum Protect** > **Befehlszeile für Sichern/ Archivieren** auf. • Öffnen Sie ein Fenster mit Administratorbefehlseingabeaufforderung und wechseln Sie in das Installationsverzeichnis des Clients für Sichern/Archivieren (`cd "C:\ Programme\tivoli\tsm\baclient"`). Führen Sie **`dsmc.exe`** aus. Greifen Sie mit einer der folgenden Methoden auf den Hilfetext zu: • Nachdem Sie den Befehlszeilenclient gestartet haben, geben Sie bei der Eingabeaufforderung `Protect>` den Befehl **`help`** ein, um das Inhaltsverzeichnis der Hilfe anzuzeigen. • Um die Hilfe in einem eigenen Fenster anzuzeigen, öffnen Sie ein Fenster mit Administratorbefehlseingabeaufforderung und wechseln Sie in das Installationsverzeichnis des Clients für Sichern/Archivieren (`cd "C:\ Programme\tivoli\tsm\baclient"`). Führen Sie **`dsmc.exe help`** aus, um das Inhaltsverzeichnis der Hilfe anzuzeigen. Sie können dem Befehl auch einen Abschnittstitel anfügen, um die Hilfe zu einem Thema anzuzeigen. Mit `dsmc help options` wird beispielsweise der Hilfeabschnitt angezeigt, in dem die Verwendung von Clientoptionen beschrieben wird, und mit `dsmc help backup vm` wird die Hilfe für den Befehl **`backup vm`** angezeigt.

Kapitel 2. Data Protection for Microsoft Hyper-V installieren und aktualisieren

Die Installation von IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V umfasst Tasks für die Planung, die Installation und das Upgrade.

Installation von Data Protection for Microsoft Hyper-V planen

Bevor Sie Data Protection for Microsoft Hyper-V installieren, sollten Sie wissen, welche Features installiert werden, und die Systemvoraussetzungen lesen.

Features, die installiert werden

Alle Features für Data Protection for Microsoft Hyper-V sind Bestandteil der Installationssuite.

Die folgenden Komponenten werden bei einer Standardinstallation von Data Protection for Microsoft Hyper-V installiert:

- IBM Spectrum Protect-Einheit zum Versetzen von Daten
- Data Protection for Microsoft Hyper-V-Verwaltungskonsole
- IBM Spectrum Protect-Feature für Dateizurückschreibung
- PowerShell-Cmdlets von Data Protection for Microsoft Hyper-V
- IBM Spectrum Protect Recovery Agent
- IBM Spectrum Protect-Web-Server
- IBM Spectrum Protect Java™ Virtual Machine (JVM)

Sie müssen keines dieser Features mit den zugehörigen Unterstützungspaketen separat installieren. Installationsanweisungen finden Sie in „Data Protection for Microsoft Hyper-V installieren" auf Seite 28.

Wenn Sie nur die Einheit zum Versetzen von Daten für Zurückschreibungsoperationen mit In-Guest-Anwendungsschutz installieren möchten, finden Sie weitere Informationen in „Nur die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten installieren" auf Seite 32. Recovery Agent ist in der Installation der Einheit zum Versetzen von Daten enthalten. Sie können IBM Spectrum Protect Recovery Agent nicht mehr separat installieren.

Wenn Sie Data Protection for Microsoft Hyper-V über Fernzugriff verwalten möchten, installieren Sie nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole auf einem separaten Windows-Host. Weitere Informationen finden Sie in „Nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installieren" auf Seite 30. Die PowerShell-Cmdlets sind Bestandteil dieser Installation.

Sie können Data Protection for Microsoft Hyper-V auch auf Hyper-V-Hosts unter Windows Server-Betriebssystemen installieren, die mit der Server Core-Option installiert wurden. Anschließend können Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole auf einem anderen Windows Server oder Windows 10-Client installieren, um Data Protection for Microsoft Hyper-V über Fernzugriff zu verwalten. Weitere Informationen finden Sie in „Data Protection for Microsoft Hyper-V auf Windows Server Core-Systemen installieren und konfigurieren" auf Seite 35

35.

Systemvoraussetzungen feststellen

Für Data Protection for Microsoft Hyper-V gelten Mindestanforderungen in Bezug auf Hardware, Plattenspeicherplatz, Hauptspeicher und Software.

In der folgenden Tabelle sind die Hardwaremindestvoraussetzungen beschrieben, die für die Installation von Data Protection for Microsoft Hyper-V erforderlich sind.

Tabelle 3. Hardwaremindestvoraussetzungen für Data Protection for Microsoft Hyper-V

Komponente	Mindestvoraussetzung	Bevorzugt
System	x64-Prozessor	Nicht zutreffend
Hauptspeicher	4 GB RAM	16 GB RAM
Verfügbarer Speicherplatz auf der Festplatte	2 GB	3,5 GB
NIC-Karte	1 NIC - 100 MB/s	1 NIC - 10 Gb/s

Für Data Protection for Microsoft Hyper-V muss die Hyper-V-Rolle auf dem System mit Microsoft Windows Server 2012, 2012 R2 oder 2016 installiert sein. Das eigenständige Produkt Hyper-V Server, das nur den Windows-Hypervisor enthält, wird ebenfalls unterstützt.

Zur Sicherstellung der Zuverlässigkeit und Leistung auf einem System mit Windows Server 2012 oder 2012 R2 verwenden Sie einen VSS-Hardware-Provider anstelle eines Software-Providers.

Sie können Data Protection for Microsoft Hyper-V nicht unter Nano Server für Windows Server 2016 installieren. Sie können jedoch Data Protection for Microsoft Hyper-V unter Windows Server 2016 verwenden, um absturzkonsistente Sicherungen von Gast-VMs mit Nano Server zu erstellen.

Details zu den Hardware- und Softwarevoraussetzungen für Data Protection for Microsoft Hyper-V enthält die Technote 2017394.

Ausführliche Informationen zu den Softwarevoraussetzungen für den Anwendungsschutz der VMs, die Microsoft Exchange Server oder Microsoft SQL Server hosten, finden Sie in der Technote 2017347.

Informationen zu den Voraussetzungen für das Feature für Dateizurückschreibung finden Sie in „Voraussetzungen für die Dateizurückschreibung” auf Seite 100.

Erforderliche Kommunikationsports

Vor der Installation von Data Protection for Microsoft Hyper-V müssen Sie sicherstellen, dass bestimmte Kommunikationsports in der Firewall offen sind.

Die folgenden TCP-Ports werden von Data Protection for Microsoft Hyper-V verwendet. Diese Ports müssen in der Firewall jedes Computers offen sein.

Tabelle 4. Erforderliche Kommunikationsports für Data Protection for Microsoft Hyper-V

Computer	Funktion	Eingehende TCP-Ports	Abgehende TCP-Ports
Hyper-V-Host	Alle	1581, 1582, 3260, 9081	135, 445, 1500, 1581, 9081
Windows-VM	Dateizurückschreibung, Anwendungsschutz	135, 445	Trifft nicht zu
Linux-Mount-Proxy	Dateizurückschreibung	1581	22, 1581, 3260
Linux-VM	Dateizurückschreibung	22	Trifft nicht zu

Die folgende Tabelle zeigt, welche Ports von welchen Komponenten verwendet werden.

Tabelle 5. Verwendete Kommunikationsports nach Komponenten

Komponente	TCP-Ports
SSH	22
WMI	135, 445
IBM Spectrum Protect-Server	1500
Clientakzeptor (CAD)	1581, 1582
iSCSI	3260
REST-API	9081

Einschränkung: Der Windows-Mount-Proxy auf dem Hyper-V-Host und der Linux-Mount-Proxy müssen sich in demselben Teilnetz befinden, damit iSCSI-Datenverkehr unterstützt wird.

Wenn diese Ports während der Konfiguration geändert werden, müssen die Firewallregeln aktualisiert werden.

Upgrade für Data Protection for Microsoft Hyper-V durchführen

Informieren Sie sich über die Tasks, die Sie ausführen müssen, bevor Sie ein Upgrade von einer Vorgängerversion auf Data Protection for Microsoft Hyper-V Version 8.1.6 durchführen.

Kompatibilität mit verschiedenen Versionen

In Umgebungen mit mehreren Clustern und Hosts ist Data Protection for Microsoft Hyper-V mit späteren Versionen kompatibel.

Wenn Sie Data Protection for Microsoft Hyper-V auf mehreren Clustern und Hosts in Ihrer Umgebung implementieren, sind die installierten Produktversionen mit späteren Versionen kompatibel. Genauer gesagt, wenn neue Versionen von Data Protection for Microsoft Hyper-V in Ihrer Umgebung eingeführt werden, können frühere Versionen der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der PowerShell-Cmdlets eine Verbindung zu den neueren Versionen herstellen. Dank dieser Kompatibilität haben Sie genügend Zeit, um alle Data Protection for Microsoft Hyper-V-Implementierungen auf die neuesten Versionen zu aktualisieren.

Eine Data Protection for Microsoft Hyper-V-Verwaltungskonsole oder ein PowerShell-Cmdlet kann jedoch keine Verbindung zu einer früheren Version von Data

Protection for Microsoft Hyper-V herstellen. Sie werden in einer Nachricht aufgefordert, entweder die frühere Implementierung auf eine neuere Version zu aktualisieren oder die Verwaltungskonsole oder das PowerShell-Cmdlet zu verwenden, die bzw. das mit der früheren Implementierung bereitgestellt wird.

Beispiel

In der folgenden Tabelle ist die Kompatibilität zwischen Data Protection for Microsoft Hyper-V Version 8.1.4 und Version 8.1.6 für Umgebungen dargestellt, in denen Data Protection for Microsoft Hyper-V auf mehreren Clustern oder Hosts implementiert ist.

Data Protection for Microsoft Hyper-V Version 8.1.4 und Version 8.1.6 sind auf unterschiedlichen Clustern in der Umgebung installiert.

Tabelle 6. Kompatibilitätsbeispiele

Version der Data Protection for Microsoft Hyper-V-Verwaltungskonsole oder des Cmdlets	Data Protection for Microsoft Hyper-V-Version	Kompatibel?
Version 8.1.4	Version 8.1.6	Ja. Alle Operationen funktionieren so, als ob eine Verbindung zu einer Implementierung mit Version 8.1.4 bestünde.
Version 8.1.6	Version 8.1.4	Nein. Aktualisieren Sie die Implementierung der Version 8.1.4 auf die neuere Version oder verwenden Sie die Verwaltungskonsole oder die PowerShell-Cmdlets, die mit der früheren Implementierung bereitgestellt werden.

Knoten auf dem IBM Spectrum Protect-Server umbenennen

Bevor Sie für Ihre Umgebung ein Upgrade von Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher auf Version 8.1.6 durchführen, müssen Sie und der IBM Spectrum Protect-Serveradministrator die Knoten auf dem Server umbenennen.

Informationen zu diesem Vorgang

Wenn Sie die vorhandenen Knotennamen auf dem IBM Spectrum Protect-Server umbenennen, müssen Sie die Namenskonvention verwenden, die in Schritt 1 auf Seite 21 beschrieben ist.

Einschränkung: Wenn Sie den Konfigurationsassistenten für die Konfiguration von Data Protection for Microsoft Hyper-V verwenden, müssen Sie die Konfiguration ausführen, bevor Sie ältere Sicherungen der virtuellen Maschine (VM), die mit Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher erstellt wurden, zurückschreiben können. Andernfalls können Sie ältere VM-Sicherungen nicht über die Data Protection for Microsoft Hyper-V-Verwaltungskonsole zurückschreiben.

Wenn Sie Data Protection for Microsoft Hyper-V manuell konfigurieren und die Befehlszeile der Einheit zum Versetzen von Daten zum Zurückschreiben von VMs

verwenden, sind die älteren Knotennamen noch aktiv, bis Sie den Konfigurationsassistenten ausführen.

Vorgehensweise

Der IBM Spectrum Protect-Serveradministrator führt die folgenden Schritte aus:

1. Verwenden Sie den Serverbefehl **RENAME NODE**, um den vorhandenen Hyper-V-Knotennamen (der durch die Option asnodename angegeben ist) in einen neuen Zielknotennamen umzubenennen, der den folgenden Namenskonventionen entspricht:
   - Für eine Umgebung mit eigenständigem Hyper-V-Host: *Hostname*_HV_TGT
   - Für eine Clusterumgebung: *Clustername*_HV_TGT

   Beispiel: Für einen Cluster mit dem Clusterknotennamen Cluster1 lautet der neue Zielknotenname Cluster1_HV_TGT oder *Präfix*_Cluster1_HV_TGT_*Suffix*.

   Sie können dem Standardknotennamen auch ein Präfix und ein Suffix hinzufügen. Beispiele sind *Präfix_Hostname*_HV_TGT_*Suffix* oder *Präfix_Clustername*_HV_TGT_*Suffix*.

   Anweisungen zum Hinzufügen eines Präfixes und eines Suffixes zum Knotennamen finden Sie in „Knotennamen anpassen" auf Seite 23.

   Einschränkung: Sie können keine Knotennamen verwenden, die diesen Namenskonventionen nicht entsprechen. Wenn Sie den Data Protection for Microsoft Hyper-V-Konfigurationsassistenten ausführen, werden der neue Zielknoten und die zugehörigen Knoten der Einheit zum Versetzen von Daten, die den neuen Namenskonventionen entsprechen, automatisch auf dem IBM Spectrum Protect-Server registriert. Zudem werden die erforderlichen Windows-Dienste auf dem lokalen Windows-Host konfiguriert.
2. Verwenden Sie den Serverbefehl **UPDATE SCHEDULE**, um vorhandene Zeitpläne mit den folgenden erforderlichen Parametern zu aktualisieren:
   - Geben Sie die Parameter ACTION=BACKUP und SUBACTION=VM in der Zeitplandefinition an.
   - Aktualisieren Sie die Optionszeichenfolge wie folgt:
     - Für einen eigenständigen Hostnamen: `options='-asnodename=Hostname_HV_TGT -domain.vmfull="all-vm"'` oder `options='-asnodename=Präfix_Hostname_HV_TGT_Suffix -domain.vmfull="all-vm"'`
     - Für einen Clusternamen: `options='-asnodename=Clustername_HV_TGT -domain.vmfull="all-vm"'` oder `options='-asnodename=Präfix_Clustername_HV_TGT_Suffix -domain.vmfull="all-vm"'`

   Weitere Informationen finden Sie in „Sicherungszeitpläne für einen Host oder eine Clustermaschine verwalten" auf Seite 86.
3. Optional: Aktualisieren Sie die Knotenreplikationsparameter, indem Sie den Befehl REPLICATE NODE auf dem IBM Spectrum Protect-Server ausgeben:
   - Für einen eigenständigen Host replizieren Sie Daten auf dem Knoten *Hostname*_HV_TGT oder *Präfix_Hostname*_HV_TGT_*Suffix*.
   - Für einen Cluster replizieren Sie Daten auf dem Knoten *Clustername*_HV_TGT oder *Präfix_Clustername*_HV_TGT_*Suffix*.

Führen Sie die folgenden Tasks auf einem Hyper-V-Host aus:

4. Führen Sie auf einem eigenständigen Host bzw. auf allen Hosts in einem Cluster ein Upgrade von Data Protection for Microsoft Hyper-V auf Version 8.1.6 durch.

   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V installieren" auf Seite 28.
5. Führen Sie den Konfigurationsassistenten auf dem Hyper-V-Host aus. Für Cluster führen Sie den Assistenten auf einem der Hosts im Cluster aus, in der Regel auf Ihrem lokalen Windows-Host.

   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.
6. Ordnen Sie dem neuen Zielknotennamen einen Zeitplan zu. Verwenden Sie dazu das Fenster **Sicherungsmanagement** in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole.

   Anweisungen finden Sie in „Sicherungszeitpläne für einen Host oder eine Clustermaschine verwalten" auf Seite 86.
7. Überprüfen Sie Ihre Konfiguration, indem Sie Sicherungs- und Zurückschreibungsoperationen in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole ausführen.

   Anweisungen finden Sie in den folgenden Themen:
   - „Ad-hoc-Sicherung einer virtuellen Maschine ausführen" auf Seite 91
   - „Virtuelle Maschine zurückschreiben" auf Seite 93
8. Führen Sie die folgenden Bereinigungstasks aus, nachdem die Konfiguration überprüft wurde:
   - Der IBM Spectrum Protect-Serveradministrator löscht die alten Knoten der Einheit zum Versetzen von Daten mithilfe des Serverbefehls **REMOVE NODE**.
   - Der Hyper-V-Administrator entfernt die Services, die für den alten Clusterknoten und die alten Knoten der Einheit zum Versetzen von Daten erstellt wurden, indem er den Befehl **dsmcutil remove** auf dem eigenständigen Host oder auf jedem Host in einem Cluster ausführt.

     Weitere Informationen enthält die Beschreibung des Befehls **REMove** in Dsmcutil-Befehle: Erforderliche Optionen und Beispiele.

Ergebnisse

Sie können Ihre Hyper-V-VMs mit Data Protection for Microsoft Hyper-V schützen.

Tipps zum Anzeigen des Sicherungsprotokolls: Das Protokoll für Sicherungen, die vor der Knotenaktualisierung ausgeführt wurden, ist nicht mehr verfügbar. Jedoch können alle Sicherungen noch über den Assistenten **Zurückschreiben** oder die Befehlszeile zurückgeschrieben werden. Nach der Knotenaktualisierung ist das Sicherungsprotokoll für die erste Sicherungsoperation und nachfolgende Sicherungsoperationen verfügbar.

Sofort nach der Knotenaktualisierung können Sie in Clusterkonfigurationen VM-Sicherungen nur in der Clustersicht, nicht in der Hostsicht anzeigen und zurückschreiben. Die Hostsicht enthält nur die VMs, deren Eigner dieser Hostknoten ist. Nach der Knotenaktualisierung ist der Hostknoten nicht mehr der Eigner der Sicherungen. Nachdem erfolgreiche Sicherungen ausgeführt wurden, können die VMs wieder von der Hostsicht aus gesichert und zurückgeschrieben werden.

Nächste Schritte

In einigen Situationen muss mindestens eine der beiden folgenden Tasks ausgeführt werden:

- Der IBM Spectrum Protect-Serveradministrator überprüft, ob dem Zielknoten die Proxy-Berechtigung für den Knoten der Einheit zum Versetzen von Daten erteilt wurde. Dazu gibt er den Serverbefehl **QUERY PROXY NODE** aus.
- Der Hyper-V-Administrator startet den Clientakzeptorservice auf dem Hyper-V-Host erneut.

Der IBM Spectrum Protect-Serveradministrator führt den Zeitplan aus, damit die Sicherungsinformationen für die aktualisierten Knoten korrekt angezeigt werden können.

Zugehörige Konzepte:

„Verwendung von IBM Spectrum Protect-Knoten in Data Protection for Microsoft Hyper-V" auf Seite 8

Knotennamen anpassen

Sie können den Standardknotennamen ein Präfix, ein Suffix oder beides hinzufügen. Auf diese Weise können Sie die Knotennamen anpassen, die vom Konfigurationsassistenten automatisch generiert werden.

Informationen zu diesem Vorgang

Wenn Sie den Konfigurationsassistenten für die Konfiguration von Data Protection for Microsoft Hyper-V verwenden, entsprechen die erstellten Knoten den folgenden Standardnamenskonventionen:

*Hostname*_HV_TGT (oder *Clustername*_HV_TGT für Cluster)

*Hostname*_HV_DM

*Hostname*_HV_MP_WIN (wenn das Feature für Dateizurückschreibung aktiviert ist)

*Hostname*_HV_MP_LNX (wenn das Feature für Dateizurückschreibung aktiviert ist)

Sie können die Knotennamen jedoch anpassen. Beispielsweise müssen Sie die Knotennamen möglicherweise anpassen, um eine Multi-Tenant-Umgebung zu unterstützen, in der die virtuellen Maschinen mehrerer Tenants auf demselben Server gehostet werden. Zur Unterscheidung der Knoten auf der Basis des Tenants können Sie den Standardknotennamen ein Präfix, ein Suffix oder beides hinzufügen.

Sie können die Knotennamen für eine neue oder eine vorhandene Data Protection for Microsoft Hyper-V-Konfiguration anpassen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Knotennamen anzupassen:

1. Erstellen Sie eine Textdatei mit dem Namen `hvConfig.props` im Verzeichnis `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI` auf dem Hyper-V-Host, der sich in einer eigenständigen Umgebung oder Clusterumgebung befindet.
2. Editieren Sie die Datei `hvConfig.props` und fügen Sie der Datei die folgenden beiden Anweisungen hinzu:

```
node_prefix=Präfix
node_suffix=Suffix
```

Dabei ist *Präfix* die Textzeichenfolge, die Sie am Anfang des Knotennamens hinzufügen möchten, und *Suffix* ist die Textzeichenfolge, die Sie am Ende des Knotennamens anfügen möchten.

Sie können nur das Präfix, nur das Suffix oder sowohl ein Präfix als auch ein Suffix angeben. Die Gesamtlänge des Knotennamens (einschließlich des Präfix und des Suffix) darf 64 Zeichen nicht überschreiten.

Wenn Sie die Textzeichenfolge leer lassen oder die Anweisung entfernen, bleiben die Standardknotennamen unverändert. Wenn Sie weder ein Präfix noch ein Suffix verwenden möchten, erstellen Sie die Datei `hvConfig.props` nicht.

Die sich ergebenden angepassten Knotennamen entsprechen dem folgenden Muster:

*Präfix_Hostname*_HV_TGT_*Suffix* (oder *Präfix_Clustername*_HV_TGT_*Suffix* für Cluster)

*Präfix_Hostname*_HV_DM_*Suffix*

*Präfix_Hostname*_HV_MP_WIN_*Suffix* (wenn das Feature für Dateizurückschreibung aktiviert ist)

*Präfix_Hostname*_HV_MP_LNX_*Suffix* (wenn das Feature für Dateizurückschreibung aktiviert ist)

3. Für eine Clusterumgebung erstellen Sie die Datei `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\hvConfig.props` auf jedem Host im Cluster und geben Sie auf jedem Host dieselben Eigenschaften an.

   Wichtig: Alle Hosts im Cluster müssen über diese Datei verfügen, bevor Sie den Konfigurationsassistenten ausführen können.

4. Wenn Sie Data Protection for Microsoft Hyper-V zuvor mit den Standardknotennamen konfiguriert haben, müssen Sie die Knoten auf dem IBM Spectrum Protect-Server umbenennen.

   Anweisungen finden Sie in „Knoten auf dem IBM Spectrum Protect-Server umbenennen” auf Seite 20.

5. Führen Sie den Konfigurationsassistenten auf dem Hyper-V-Host aus. Das Präfix, das Suffix oder beides werden der Namenskonvention der Knoten hinzugefügt.

Ergebnisse

Beispiel: Sie möchten den Data Protection for Microsoft Hyper-V-Knotennamen das Präfix "SP" und das Suffix "DEPT1" hinzufügen. Sie haben der Datei `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\hvConfig.props` die folgenden Anweisungen hinzugefügt:

```
node_prefix=SP
node_suffix=DEPT1
```

Für einen eigenständigen Host mit dem Namen MYHOST werden die folgenden Knoten erstellt, wenn Sie den Konfigurationsassistenten ausführen (falls das Feature für Dateizurückschreibung aktiviert ist):

```
SP_MYHOST_HV_TGT_DEPT1
SP_MYHOST_HV_DM_DEPT1
SP_MYHOST_HV_MP_WIN_DEPT1
SP_MYHOST_HV_MP_LNX_DEPT1
```

Sind ein Cluster mit dem Clusternamen MYCLUSTER sowie die Hosts HOSTA und HOSTB vorhanden, werden die folgenden Knoten erstellt (falls das Feature für Dateizurückschreibung aktiviert ist):

```
SP_MYCLUSTER_HV_TGT_DEPT1
SP_HOSTA_HV_DM_DEPT1
SP_HOSTA_HV_MP_WIN_DEPT1
SP_HOSTA_HV_MP_LNX_DEPT1
SP_HOSTB_HV_DM_DEPT1
SP_HOSTB_HV_MP_WIN_DEPT1
SP_HOSTB_HV_MP_LNX_DEPT1
```

Nächste Schritte

Sie können die Werte für die Parameter **node_prefix** und **node_suffix** überprüfen, indem Sie das Windows PowerShell-Cmdlet **Get-DpHvHostConfiguration** ausführen.

Geben Sie bei einer PowerShell-Eingabeaufforderung beispielsweise das folgende Cmdlet aus:

```
PS C:\Users\administrator> Get-DpHvHostConfiguration -Session $session
```

Zugehörige Konzepte:

„Verwendung von IBM Spectrum Protect-Knoten in Data Protection for Microsoft Hyper-V" auf Seite 8

Upgradehinweise für RCT-Sicherungen

Lesen Sie die Hinweise zu Sicherungsoperationen für virtuelle Maschinen (VMs) unter Windows Server 2016, bevor Sie ein Upgrade auf Data Protection for Microsoft Hyper-V Version 8.1.2 oder höher durchführen.

- Wenn Sie Ihre Hyper-V-Umgebung von Windows Server 2012 oder 2012 R2 auf Windows Server 2016 aktualisieren, wird die VM-Version der virtuellen Maschinen nicht automatisch aktualisiert. Der Hyper-V-Administrator muss die VMs auf die neue Version aktualisieren, nachdem für die Umgebung ein Upgrade auf Windows Server 2016 durchgeführt wurde. Data Protection for Microsoft Hyper-V Version 8.1.2 oder höher sichert nur VMs, die auf die neue VM-Version aktualisiert wurden.

  Stellen Sie sicher, dass die Gast-VM offline ist, wenn Sie die VM-Version aktualisieren. Sie können die VM-Version mit dem Hyper-V-Manager oder mit dem Cmdlet Update-VMVersion aktualisieren.
- Für VM-Sicherungsoperationen mit Resilient Change Tracking (RCT) muss die Hyper-V-VM die Version 6.2 oder höher aufweisen.

  In Data Protection for Microsoft Hyper-V Version 8.1.0 und früheren Versionen werden weiterhin frühere VM-Versionen unter Verwendung der VSS-Sicherungsmethode unterstützt.

Zugehörige Tasks:

„Von VSS-Sicherungen auf RCT-Sicherungen migrieren" auf Seite 26

Von VSS-Sicherungen auf RCT-Sicherungen migrieren

Wenn Sie das Sicherungsfeature Resilient Change Tracking (RCT) in Data Protection for Microsoft Hyper-V Version 8.1.2 oder höher nutzen möchten, müssen Sie Ihre Sicherungsoperationen für virtuelle Maschinen (VMs) von Microsoft Volume Shadow Copy Service (VSS) auf RCT migrieren.

Vorbereitende Schritte

- Stellen Sie sicher, dass die Hyper-V-VM die Version 6.2 oder höher aufweist. Sie können die VM-Version mit dem Hyper-V-Manager oder mit dem Cmdlet Get-VM feststellen.
- Wenn Sie Ihre Hyper-V-Umgebung von Windows Server 2012 oder 2012 R2 auf Windows Server 2016 migrieren, wird die VM-Version der Hyper-V-VMs nicht automatisch aktualisiert. Sie müssen die VMs auf die neue Version aktualisieren, damit sie von Data Protection for Microsoft Hyper-V gesichert werden können.

  Stellen Sie sicher, dass Sie die Gast-VM offline setzen, bevor Sie die VM-Version der VM aktualisieren. Sie können die VM-Version mit dem Hyper-V-Manager oder mit dem Cmdlet Update-VMVersion aktualisieren.

Vorgehensweise

Gehen Sie wie folgt vor, um VSS-Sicherungen auf RCT zu migrieren:

1. Installieren und konfigurieren Sie Data Protection for Microsoft Hyper-V Version 8.1.6 auf dem Hyper-V-Host-Server unter dem Betriebssystem Windows Server 2016.
2. Führen Sie eine Sicherungsoperation 'Immer inkrementell - Vollständig' für Ihre VMs aus.

   Für alle Data Protection for Microsoft Hyper-V-Sicherungsoperationen in der Umgebung mit Windows Server 2016 oder höher werden RCT-Sicherungen verwendet.

Ergebnisse

- Da in den vorherigen VSS-Sicherungen keine RCT-Informationen zur Überwachung von Änderungen vorhanden sind, wird bei der ersten Sicherung einer VM mit Data Protection for Microsoft Hyper-V Version 8.1.6 eine Sicherung 'Immer inkrementell - Vollständig' erstellt.
- Nach der Erstsicherung einer VM mit RCT werden die VSS-Sicherungen inaktiviert.
- Mit Data Protection for Microsoft Hyper-V Version 8.1.6 können Sie weiterhin VMs zurückschreiben, die unter Windows Server 2016 in Version 8.1.0 gesichert wurden. Bei nachfolgenden Sicherungen von VMs wird RCT verwendet.

Zugehörige Konzepte:

„Sicherungen virtueller Maschinen mit Resilient Change Tracking (RCT)" auf Seite 2

„Sicherungen virtueller Maschinen mit Volume Shadow Copy Service (VSS)" auf Seite 2

Data Protection for Microsoft Hyper-V-Komponenten installieren

Führen Sie eine Standardinstallation aus, um alle Data Protection for Microsoft Hyper-V-Komponenten zu installieren. Anschließend können Sie separate Komponenten für Ihren Anwendungsfall nach Bedarf installieren.

Installationspaket herunterladen und extrahieren

Bevor Sie Data Protection for Microsoft Hyper-V installieren können, müssen Sie das Installationspaket herunterladen und die Installationsdateien aus dem Paket extrahieren.

Vorbereitende Schritte

Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie unter IBM Spectrum Protect for Virtual Environments - IBM Support.

Vorgehensweise

1. Laden Sie das Data Protection for Microsoft Hyper-V-Paket von IBM Passport Advantage oder Fix Central herunter.
2. Extrahieren Sie die komprimierte Installationsdatei, die Sie heruntergeladen haben:
   a. Kopieren Sie das heruntergeladene, komprimierte Installationspaket auf eine lokale Platte oder in eine Netzfreigabe. Stellen Sie sicher, dass Sie die Installationsdateien in ein leeres Verzeichnis extrahieren (*Extraktionsordner*).
   b. Doppelklicken Sie auf dem komprimierten Installationspaket, um die Installationsdateien in dasselbe Verzeichnis zu extrahieren.

      Standardmäßig werden die dekomprimierten Dateien im aktuellen Plattenlaufwerk im Verzeichnis *Extraktionsordner*\TSMHYPERV_WIN gespeichert.

      Wenn das Installationsprogramm Dateien aus einem anderen Versuch zur Installation von Data Protection for Microsoft Hyper-V in diesem Verzeichnis erkennt, müssen Sie angeben, ob die alten Dateien überschrieben werden sollen. Wenn eine Systemanfrage in Bezug auf das Überschreiben von Dateien angezeigt wird, geben Sie die Option für 'Immer überschreiben' ein, um die vorhandenen Dateien zu überschreiben. Diese Auswahl stellt sicher, dass nur die Dateien aus der aktuellen Installation verwendet werden.

Ergebnisse

Das Data Protection for Microsoft Hyper-V-Installationsprogramm (spinstall.exe) befindet sich im Verzeichnis *Extraktionsordner*\TSMHYPERV_WIN.

Nächste Schritte

Data Protection for Microsoft Hyper-V installieren.

Data Protection for Microsoft Hyper-V mit dem Installationsassistenten installieren

Verwenden Sie den Installationsassistenten, um eine Standardinstallation von Data Protection for Microsoft Hyper-V auszuführen oder um die verfügbaren Komponenten separat zu installieren.

Data Protection for Microsoft Hyper-V installieren

Anweisungen für eine Standardinstallation der Software IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V werden bereitgestellt.

Vorbereitende Schritte

Stellen Sie in einer Clusterumgebung sicher, dass Sie das Data Protection for Microsoft Hyper-V-Paket auf jedem Host im Cluster installieren.

Auf jedem Host, auf dem Data Protection for Microsoft Hyper-V installiert ist, müssen Sie sicherstellen, dass der HTTPS-Port, der für die Kommunikation mit Data Protection for Microsoft Hyper-V verwendet wird, in der Firewall offen ist. Wenn nicht anders angegeben, wird die Standardportnummer 9081 verwendet. .

Bei einem Upgrade von Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher führen Sie die Tasks in „Knoten auf dem IBM Spectrum Protect-Server umbenennen" auf Seite 20 aus.

Stellen Sie sicher, dass Sie das Installationspaket gemäß der Beschreibung in „Installationspaket herunterladen und extrahieren" auf Seite 27 heruntergeladen und extrahiert haben.

Informationen zu diesem Vorgang

Eine Standardinstallation umfasst alle Features von Data Protection for Microsoft Hyper-V einschließlich Einheit zum Versetzen von Daten, Data Protection for Microsoft Hyper-V-Verwaltungskonsole, PowerShell-Cmdlets und IBM Spectrum Protect Recovery Agent.

Wenn Sie nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole für die Fernverwaltung installieren möchten, finden Sie weitere Informationen in „Nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installieren" auf Seite 30. Die PowerShell-Cmdlets sind Bestandteil dieser Installation.

Wenn Sie nur die Einheit zum Versetzen von Daten für Zurückschreibungsoperationen mit In-Guest-Anwendungsschutz installieren möchten, finden Sie weitere Informationen in „Nur die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten installieren" auf Seite 32. Recovery Agent ist in der Installation der Einheit zum Versetzen von Daten enthalten.

Einschränkung: Unter dem Betriebssystem Windows inaktiviert das Data Protection for Microsoft Hyper-V-Installationsprogramm die Funktion für automatische Bereitstellung (Automount) mit dem Befehl **diskpart** automatisch. Diese Aktion ist erforderlich, damit in der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung die korrekten Laufwerkzuordnungen angezeigt und die vom System reservierte Platte ausgeblendet wird.

Wenn Sie nicht die Ausführung von Dateizurückschreibungsoperationen planen oder wenn es Sie nicht stört, dass in der Schnittstelle für Dateizurückschreibung falsche Laufwerkzuordnungen und die vom System reservierte Platte angezeigt werden, können Sie die Funktion Automount nach dem Abschluss der Installation aktivieren.

Vorgehensweise

Führen Sie die folgenden Schritte auf einem einzelnen Hyper-V-Host oder auf jedem Host in einem Cluster aus:

1. „Installationspaket herunterladen und extrahieren" auf Seite 27.
2. Doppelklicken Sie auf der Datei `spinstall.exe`, um das Installationsprogramm zu starten. Wählen Sie die Sprache für den Installationsprozess aus und klicken Sie anschließend auf **Weiter**.
3. Klicken Sie auf der Seite **Willkommen beim InstallShield-Assistenten für IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V** auf **Weiter**.
4. Lesen Sie auf der Seite **Lizenzvereinbarung** die Bedingungen der Lizenzvereinbarung. Klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken Sie auf **Weiter**. Wenn Sie die Bedingungen der Lizenzvereinbarung nicht akzeptieren, wird die Installation beendet und Sie müssen auf **Abbrechen** klicken, um den Installationsassistenten zu verlassen.
5. Auf der Seite **Aktuellen Zielordner ändern** akzeptieren Sie die Standardinstallationsposition oder geben Sie eine andere Installationsposition an. Klicken Sie auf **Weiter**.
6. Auf der Seite **Installationstyp** klicken Sie auf **Standardinstallation**. Der Installationsprozess beginnt sofort. Sie können Ihre Auswahl nicht mehr ändern, nachdem der Installationsprozess begonnen hat.

   Tipp: Der Installationsprozess kann einige Minuten dauern, während die Pakete für Data Protection for Microsoft Hyper-V, JVM, Einheit zum Versetzen von Daten, Web-Server, Framework und Recovery Agent installiert werden.
7. Auf der Seite **Installationsassistent abgeschlossen** klicken Sie auf **Fertigstellen**, um den Installationsassistenten zu verlassen. Die Data Protection for Microsoft Hyper-V-Verwaltungskonsole wird sofort gestartet, nachdem der Assistent geschlossen wurde.

   Wenn Sie den Konfigurationsassistenten zu diesem Zeitpunkt nicht starten möchten, wählen Sie das Feld **Data Protection for Microsoft Hyper-V-Verwaltungskonsole jetzt starten** ab und klicken Sie auf **Fertigstellen**, um den Assistenten zu verlassen.

Ergebnisse

Data Protection for Microsoft Hyper-V ist installiert.

Die folgenden installierten Komponenten werden unter **Programme und Funktionen** in der Systemsteuerung des Windows-Betriebssystems angezeigt:

- IBM Spectrum Protect-Client
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V-Lizenz

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Suite
- IBM Spectrum Protect for Virtual Environments: Framework
- IBM Spectrum Protect for Virtual Environments: Recovery Agent
- IBM Spectrum Protect JVM
- IBM Spectrum Protect WebServer

Nächste Schritte

Bevor Sie versuchen, Sicherungs- oder Zurückschreibungsoperationen auszuführen oder die Schnittstelle für Dateizurückschreibung zu verwenden, führen Sie die Tasks in Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren aus.

Bevor Sie versuchen, die Sicherung einer virtuellen Hyper-V-Maschine bereitzustellen, um eine Datei zurückzuschreiben, führen Sie die Tasks in „IBM Spectrum Protect Recovery Agent-GUI konfigurieren" auf Seite 60 aus.

Nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installieren

Sie können auf einem Windows-Host nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole für die Fernverwaltung von Data Protection for Microsoft Hyper-V installieren.

Vorbereitende Schritte

Stellen Sie sicher, dass der HTTPS-Port, der für die Kommunikation mit der Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwendet wird, in der Firewall offen ist. Der Standardport ist 9081, wenn Sie keinen anderen Port verwenden. Weitere Informationen finden Sie in „Erforderliche Kommunikationsports" auf Seite 18.

Stellen Sie sicher, dass Sie das Installationspaket gemäß der Beschreibung in „Installationspaket herunterladen und extrahieren" auf Seite 27 heruntergeladen und extrahiert haben.

Informationen zu diesem Vorgang

Diese Installation umfasst nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole, die Data Protection for Microsoft Hyper-V PowerShell-Cmdlets und die Data Protection for Microsoft Hyper-V-Lizenzdatei.

Einschränkung: Unter dem Betriebssystem Windows inaktiviert das Data Protection for Microsoft Hyper-V-Installationsprogramm die Funktion für automatische Bereitstellung (Automount) mit dem Befehl **diskpart** automatisch. Diese Aktion ist erforderlich, damit in der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung die korrekten Laufwerkzuordnungen angezeigt und die vom System reservierte Platte ausgeblendet wird.

Wenn Sie nicht die Ausführung von Dateizurückschreibungsoperationen planen oder wenn es Sie nicht stört, dass in der Schnittstelle für Dateizurückschreibung falsche Laufwerkzuordnungen und die vom System reservierte Platte angezeigt werden, können Sie die Funktion Automount nach dem Abschluss der Installation aktivieren.

Vorgehensweise

Führen Sie die folgenden Schritte auf dem Windows-Computer aus, den Sie für die Fernverwaltung von Data Protection for Microsoft Hyper-V verwenden möchten.

1. „Installationspaket herunterladen und extrahieren" auf Seite 27.
2. Doppelklicken Sie auf der Datei `spinstall.exe`, um das Installationsprogramm zu starten. Wählen Sie die Sprache für den Installationsprozess aus und klicken Sie anschließend auf **Weiter**.
3. Klicken Sie auf der Seite **Willkommen beim InstallShield-Assistenten für IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V** auf **Weiter**.
4. Lesen Sie auf der Seite **Lizenzvereinbarung** die Bedingungen der Lizenzvereinbarung. Klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken Sie auf **Weiter**. Wenn Sie die Bedingungen der Lizenzvereinbarung nicht akzeptieren, wird die Installation beendet und Sie müssen auf **Abbrechen** klicken, um den Installationsassistenten zu verlassen.
5. Auf der Seite **Aktuellen Zielordner ändern** akzeptieren Sie die Standardinstallationsposition oder geben Sie eine andere Installationsposition an. Klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite **Installationstyp** auf **Erweiterte Installation**.
7. Auf der Seite **Erweiterte Installation** klicken Sie auf **Nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installieren**. Der Installationsprozess beginnt sofort. Sie können Ihre Auswahl nicht mehr ändern, nachdem der Installationsprozess begonnen hat.

   Tipp: Der Installationsprozess kann einige Minuten dauern, während die erforderlichen Pakete installiert werden.
8. Auf der Seite **Installationsassistent abgeschlossen** klicken Sie auf **Fertigstellen**, um den Installationsassistenten zu verlassen. Die Data Protection for Microsoft Hyper-V-Verwaltungskonsole wird sofort gestartet, nachdem der Assistent geschlossen wurde.

   Wenn Sie den Konfigurationsassistenten zu diesem Zeitpunkt nicht starten möchten, wählen Sie das Feld **Data Protection for Microsoft Hyper-V-Verwaltungskonsole jetzt starten** ab und klicken Sie auf **Fertigstellen**, um den Assistenten zu verlassen.

Ergebnisse

Data Protection for Microsoft Hyper-V-Verwaltungskonsole ist installiert.

Die folgenden installierten Komponenten werden unter **Programme und Funktionen** in der Systemsteuerung des Windows-Betriebssystems angezeigt:

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V-Lizenz
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Suite

Nächste Schritte

Konfigurieren Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole, indem Sie die folgenden Schritte ausführen:

1. Wenn der Konfigurationsassistent nicht automatisch geöffnet wird, starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole, indem Sie auf **Start** > **IBM Spectrum Protect** > **DP for Hyper-V-Verwaltungskonsole** klicken.
2. Geben Sie im Fenster **Verbindung zu Data Protection for Hyper-V herstellen** den Hostnamen und die Berechtigungsnachweise des eigenständigen Hosts oder des Hosts im Cluster ein, den Sie verwalten möchten.
3. Führen Sie die Tasks in Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren aus.

Mit dem Cmdlet **Set-DpHvMmcLoginPreferences** können Sie auch den bevorzugten Host für die Anmeldung angeben. Weitere Informationen finden Sie in Kapitel 7, „Virtuelle Maschinen mithilfe von Windows PowerShell-Cmdlets schützen", auf Seite 151.

Zugehörige Tasks:

„Data Protection for Microsoft Hyper-V auf Windows Server Core-Systemen installieren und konfigurieren" auf Seite 35

Nur die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten installieren

Sie können die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten installieren, um Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen (VMs) sowie Zurückschreibungsoperationen mit In-Guest-Anwendungsschutz auszuführen. Bei dieser Installation wird auch der Windows-Mount-Proxy für Dateizurückschreibungsoperationen installiert.

Vorbereitende Schritte

- Stellen Sie sicher, dass die Kommunikationsports in der Firewall offen sind. Eine Liste der Ports, die offen sein müssen, finden Sie in „Erforderliche Kommunikationsports" auf Seite 18.
- Stellen Sie sicher, dass Sie das Installationspaket gemäß der Beschreibung in „Installationspaket herunterladen und extrahieren" auf Seite 27 heruntergeladen und extrahiert haben.
- Wenn Sie die Einheit zum Versetzen von Daten installieren, um In-Guest-Anwendungen zu schützen, stellen Sie sicher, dass Sie vor der Installation der Einheit zum Versetzen von Daten die Anweisungen in den folgenden Themen befolgen:
  - „Software installieren und für den Anwendungsschutz von Microsoft Exchange Server konfigurieren" auf Seite 105
  - „Software installieren und für den Anwendungsschutz von Microsoft SQL Server konfigurieren" auf Seite 124

Informationen zu diesem Vorgang

Die Installation der Einheit zum Versetzen von Daten umfasst die Einheit zum Versetzen von Daten. Diese wird für VM-Sicherungs- und -Zurückschreibungsoperationen sowie für Zurückschreibungsoperationen mit In-Guest-Anwendungsschutz verwendet. Diese Installation beinhaltet außerdem den Mount-Proxy für Dateizurückschreibungsoperationen. Auch Recovery Agent ist in der Installation enthalten.

Einschränkung: Unter dem Betriebssystem Windows inaktiviert das Data Protection for Microsoft Hyper-V-Installationsprogramm die Funktion für automatische Bereitstellung (Automount) mit dem Befehl **diskpart** automatisch. Diese Aktion ist

erforderlich, damit in der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung die korrekten Laufwerkzuordnungen angezeigt und die vom System reservierte Platte ausgeblendet wird.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Windows-Mount-Proxy-Maschine oder auf der Gast-VM aus, die Anwendungsdaten hostet:

1. „Installationspaket herunterladen und extrahieren" auf Seite 27.
2. Doppelklicken Sie auf der Datei `spinstall.exe`, um das Installationsprogramm zu starten. Wählen Sie die Sprache für den Installationsprozess aus und klicken Sie anschließend auf **Weiter**.
3. Klicken Sie auf der Seite **Willkommen beim InstallShield-Assistenten für IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V** auf **Weiter**.
4. Lesen Sie auf der Seite **Lizenzvereinbarung** die Bedingungen der Lizenzvereinbarung. Klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken Sie auf **Weiter**. Wenn Sie die Bedingungen der Lizenzvereinbarung nicht akzeptieren, wird die Installation beendet und Sie müssen auf **Abbrechen** klicken, um den Installationsassistenten zu verlassen.
5. Auf der Seite **Aktuellen Zielordner ändern** akzeptieren Sie die Standardinstallationsposition oder geben Sie eine andere Installationsposition an. Klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite **Installationstyp** auf **Erweiterte Installation**.
7. Auf der Seite **Erweiterte Installation** klicken Sie auf **Feature der Einheit zum Versetzen von Daten oder Mount-Proxy installieren**. Der Installationsprozess beginnt sofort. Sie können Ihre Auswahl nicht mehr ändern, nachdem der Installationsprozess begonnen hat.

   Tipp: Der Installationsprozess kann einige Minuten dauern, während die erforderlichen Pakete installiert werden.
8. Auf der Seite **Installationsassistent abgeschlossen** klicken Sie auf **Fertigstellen**, um den Installationsassistenten zu verlassen.

Ergebnisse

Die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten ist installiert.

Die folgenden installierten Komponenten werden unter **Programme und Funktionen** in der Systemsteuerung des Windows-Betriebssystems angezeigt:

- IBM Spectrum Protect-Client
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V-Lizenz
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Suite
- IBM Spectrum Protect for Virtual Environments: Framework
- IBM Spectrum Protect for Virtual Environments: Recovery Agent
- IBM Spectrum Protect JVM
- IBM Spectrum Protect WebServer

Nächste Schritte

Weitere Informationen zum Installieren der Software und zum Konfigurieren der Software für Anwendungsschutz finden Sie in einem der folgenden Themen:

- „Software installieren und für den Anwendungsschutz von Microsoft Exchange Server konfigurieren" auf Seite 105
- „Software installieren und für den Anwendungsschutz von Microsoft SQL Server konfigurieren" auf Seite 124

Data Protection for Microsoft Hyper-V im unbeaufsichtigten Modus installieren

Sie können alle Features von Data Protection for Microsoft Hyper-V und der Einheit zum Versetzen von Daten im unbeaufsichtigten Modus auf einem einzelnen System installieren.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie das Installationspaket gemäß der Beschreibung in „Installationspaket herunterladen und extrahieren" auf Seite 27 heruntergeladen und extrahiert haben.

Informationen zu diesem Vorgang

Einschränkung: Alle Features werden an ihrer Standardposition installiert. Sie können die Features von Data Protection for Microsoft Hyper-V und der Einheit zum Versetzen von Daten im unbeaufsichtigten Modus nur an der Standardposition installieren.

Vorgehensweise

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

   ```
   cd Extraktionsordner\TSMHYPERV_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 angeze
   Akzeptieren Sie diese Warnung,
   damit die Registrierung ausgeführt werden kann.
   Möchten Sie den Treiber für virtuelle Datenträger jetzt registrieren?
   ```

   Geben Sie zur Fortsetzung der IBM Spectrum Protect Recovery Agent-Operationen **Ja** ein, um den Treiber für virtuelle Datenträger zu registrieren.

Data Protection for Microsoft Hyper-V auf Windows Server Core-Systemen installieren und konfigurieren

Sie können Data Protection for Microsoft Hyper-V auf Hyper-V-Hosts unter Windows Server-Betriebssystemen installieren und konfigurieren, die mit der Server Core-Option installiert wurden.

Vorbereitende Schritte

Auf jedem Host, auf dem Data Protection for Microsoft Hyper-V installiert ist, müssen Sie sicherstellen, dass der HTTPS-Port, der für die Kommunikation mit Data Protection for Microsoft Hyper-V verwendet wird, in der Firewall offen ist. Wenn nicht anders angegeben, wird die Standardportnummer 9081 verwendet.

Informationen zu diesem Vorgang

Da lokale Benutzerschnittstellen unter Server Core nicht unterstützt werden, müssen Sie Data Protection for Microsoft Hyper-V im unbeaufsichtigten Modus auf einem eigenständigen Host oder auf jedem Host in einem Cluster installieren.

Sie müssen Data Protection for Microsoft Hyper-V mithilfe der Data Protection for Microsoft Hyper-V-Verwaltungskonsole aus einer anderen Implementierung verwalten und dabei auf einen eigenständigen Host oder einen Host in einem Cluster verweisen.

Vorgehensweise

1. Führen Sie eine unbeaufsichtigte Installation von Data Protection for Microsoft Hyper-V auf einem eigenständigen Host oder auf allen Hosts in einem Cluster aus.

   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V im unbeaufsichtigten Modus installieren" auf Seite 34.
2. Für die ferne Verwaltung von Data Protection for Microsoft Hyper-V müssen Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole separat unter einem anderen Windows Server- oder Windows 10-Betriebssystem installieren.

   Anweisungen finden Sie in „Nur die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installieren" auf Seite 30.
3. Wenn der Konfigurationsassistent nicht automatisch geöffnet wird, starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole, indem Sie auf **Start** > **IBM Spectrum Protect** > **DP for Hyper-V-Verwaltungskonsole** klicken.
4. Im Fenster **Verbindung zu Data Protection for Hyper-V herstellen** geben Sie den Hostnamen und die Berechtigungsnachweise für den eigenständigen Host oder den Host im Cluster ein, den Sie verwalten möchten.
5. Konfigurieren Sie Data Protection for Microsoft Hyper-V mit dem Assistenten.

Ergebnisse

Sie können die Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwenden, um die täglichen Data Protection for Microsoft Hyper-V-Operationen auf einem eigenständigen Host oder in einem Cluster unter einem Betriebssystem, das mit der Server Core-Option installiert wurde, über Fernzugriff zu verwalten.

Nächste Schritte

Mit dem Cmdlet **Set-DpHvMmcLoginPreferences** können Sie auch den bevorzugten Host für die Anmeldung angeben. Weitere Informationen finden Sie in Kapitel 7, „Virtuelle Maschinen mithilfe von Windows PowerShell-Cmdlets schützen", auf Seite 151.

Zugehörige Konzepte:

Kapitel 4, „Daten mit der Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwalten", auf Seite 75

Zugehörige Tasks:

„Andere Portnummer als die Standardportnummer für Data Protection for Microsoft Hyper-V-Operationen konfigurieren" auf Seite 71

Data Protection for Microsoft Hyper-V deinstallieren

Der Prozess zum Deinstallieren von IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ist für eine Neuinstallation und für eine Version, für die ein Upgrade durchgeführt wurde, identisch.

Vorbereitende Schritte

Einschränkung: Sie können IBM Spectrum Protect Recovery Agent im Rahmen der Deinstallation der IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Suite deinstallieren. Sie können Recovery Agent auch separat deinstallieren. Sie müssen die Bereitstellung aller virtuellen Datenträger aufheben, bevor Sie IBM Spectrum Protect Recovery Agent deinstallieren. Andernfalls kann die Bereitstellung dieser bereitgestellten virtuellen Datenträger nach der erneuten Installation von Recovery Agent nicht aufgehoben werden.

Vorgehensweise

1. Öffnen Sie die **Systemsteuerung** und klicken Sie auf **Programm deinstallieren**.
2. Deinstallieren Sie die IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Suite:
   a. Auf der Seite **Programm deinstallieren oder ändern** wählen Sie **IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Suite** aus und klicken Sie auf **Deinstallieren**.
   b. Auf der Seite **Programm entfernen** des **InstallShield-Assistenten** klicken Sie auf **Entfernen**.

      Tipp: Der Deinstallationsprozess kann einige Minuten dauern.
   c. Klicken Sie auf **Fertigstellen** auf der Seite **InstallShield-Assistent abgeschlossen**, wenn die Deinstallation beendet ist. Klicken Sie auf das Symbol **Aktualisieren**, um die Liste der Programme zu aktualisieren.
3. Deinstallieren Sie die Data Protection for Microsoft Hyper-V-Lizenz:
   a. Auf der Seite **Programm deinstallieren oder ändern** wählen Sie **IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V-Lizenz** aus und klicken Sie auf **Deinstallieren**.
   b. Klicken Sie bei der entsprechenden Aufforderung auf **Ja**.
4. Deinstallieren Sie den IBM Spectrum Protect-Web-Server:
   a. Auf der Seite **Programm deinstallieren oder ändern** wählen Sie **IBM Spectrum Protect Web Server** aus und klicken Sie auf **Deinstallieren**.
   b. Klicken Sie bei der entsprechenden Aufforderung auf **Ja**.

5. Deinstallieren Sie IBM Spectrum Protect Java Virtual Machine (JVM):
   a. Auf der Seite **Programm deinstallieren oder ändern** wählen Sie **IBM Spectrum Protect JVM** aus und klicken Sie auf **Deinstallieren**.
   b. Klicken Sie bei der entsprechenden Aufforderung auf **Ja**.

Nächste Schritte

Sie müssen das Feature für Dateizurückschreibung separat entfernen. Weitere Informationen finden Sie in „Feature für Dateizurückschreibung entfernen" auf Seite 42.

Linux-Mount-Proxy-Feature installieren

Befolgen Sie die Anweisungen, um auf Linux-Gast-VMs (VM = virtuelle Maschine) das Mount-Proxy-Feature für die Verwendung bei Dateizurückschreibungsoperationen zu installieren.

Upgrade des Linux-Mount-Proxy-Features von einer älteren Version durchführen

Wenn das Mount-Proxy-Feature bereits auf der virtuellen Linux-Maschine installiert ist, können Sie ein Upgrade auf den Linux-Mount-Proxy von Data Protection for Microsoft Hyper-V Version 8.1.6 durchführen.

Vorgehensweise

Verwenden Sie eine der folgenden Methoden, um ein Upgrade für das Mount-Proxy-Feature durchzuführen:

- Aktualisieren Sie das Mount-Proxy-Feature direkt, indem Sie die Version 8.1.6 des Linux-Pakets für die Einheit zum Versetzen von Daten installieren.

  Anweisungen dazu finden Sie in einem der folgenden Themen:
  - „Mount-Proxy-Feature auf Linux-Systemen installieren" auf Seite 38
  - „Linux-Mount-Proxy-Feature im unbeaufsichtigten Modus installieren" auf Seite 40
- Ist die Version 8.1.4 des Linux-Mount-Proxys installiert, deinstallieren Sie diese Version, bevor Sie die Version 8.1.6 des Linux-Pakets installieren. Sie können das Paket der Version 8.1.4 deinstallieren, indem Sie die folgenden Befehle ausgeben.

```
rpm -e TIVsm-BAcit.x86_64 TIVsm-BA.x86_64
rpm -e TIVsm-APIcit.x86_64 TIVsm-API64.x86_64
rpm -e gskcrypt64.linux.x86_64.rpm gskssl64.linux.x86_64
```

Nächste Schritte

Nach dem Upgrade müssen Sie das Kennwort für den Linux-Mount-Proxy nur zurücksetzen, wenn Sie den Konfigurationsassistenten in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole auf dem Hyper-V-Host erneut starten oder die verschlüsselten Kennwortdateien im Verzeichnis `/etc/adsm` löschen.

Auch ein Neustart des Linux-Systems ist nach dem Upgrade nicht erforderlich. Geben Sie einfach den Befehl **kill -9** aus, um einen eventuell vorhandenen **dsmcad**-Prozess der Version 8.1.4 zu stoppen. Anschließend starten Sie den **dsmcad**-Prozess erneut, um den Clientakzeptor für Version 8.1.6 zu starten.

Mount-Proxy-Feature auf Linux-Systemen installieren

Wenn Sie planen, Dateizurückschreibungsoperationen auf Linux-Gast-VMs (VM = virtuelle Maschine) auszuführen, müssen Sie das Mount-Proxy-Feature auf Linux-Systemen installieren, indem Sie das Data Protection for Microsoft Hyper-V-Paket der Einheit zum Versetzen von Daten für Linux verwenden.

Vorbereitende Schritte

Wenn Sie ein Upgrade von einer älteren Version des Linux-Mount-Proxys durchführen, sollten Sie die Informationen in „Upgrade des Linux-Mount-Proxy-Features von einer älteren Version durchführen" auf Seite 37 lesen.

Informationen zu diesem Vorgang

Für Mountoperationen in der Schnittstelle für Dateizurückschreibung ist ein Mount-Proxy-Knoten erforderlich. Der Mount-Proxy-Knoten bewirkt, dass die Dateisysteme auf den bereitgestellten VM-Platten von VM-Sicherungen als Mountpunkte für Dateizurückschreibungsoperationen zugänglich sind.

Die Linux-Mount-Proxy-Software ist Bestandteil des Linux-Pakets für die Einheit zum Versetzen von Daten. Sie ist nicht in dem standardmäßigen Data Protection for Microsoft Hyper-V-Installationspaket für Windows enthalten. Sie müssen das Linux-Paket separat herunterladen und installieren.

Vorgehensweise

Als Rootbenutzer installieren Sie das Mount-Proxy-Feature, indem Sie die folgenden Schritte durchführen:

1. Laden Sie das Installationspaket herunter und extrahieren Sie es:
   a. Laden Sie das Installationspaket für die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten unter Linux von einer der folgenden Websites herunter:
      - Passport Advantage
      - Fix Central

      Das Downloadpaket heißt in der Regel `8.x.x.x-TSM4HYPERV.tar.gz`. Für die Version 8.1.6 hat das Paket beispielsweise den Namen `8.1.6.0-TSM4HYPERV.tar.gz`.

      Tipp: Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.
   b. Kopieren Sie das Linux-Paket für die Einheit zum Versetzen von Daten an die Position, an der Sie die Installationsdateien speichern möchten. Erstellen Sie beispielsweise das folgende Verzeichnis und kopieren Sie das Installationspaket in das Verzeichnis:

      ```
      /extract_folder
      ```
   c. Wechseln Sie in das Verzeichnis mit dem Installationspaket. Beispiel:

      ```
      cd /extract_folder
      ```
   d. Extrahieren Sie die Installationsdateien aus dem Installationspaket, indem Sie den folgenden Befehl ausgeben:

      ```
      tar -xvzf 8.1.6.0-TSM4HYPERV.tar.gz
      ```

      Die Installationsdateien werden in das Verzeichnis `CD` extrahiert. Die Installationsdateien werden beispielsweise in dem folgenden Verzeichnis gespeichert:

```
/extract_folder/CD
```

2. Wechseln Sie in das Verzeichnis, das die Installationsdateien enthält. Geben Sie beispielsweise den folgenden Befehl aus:
   ```
   cd /extract_folder/CD/Linux/DataProtectionForHyperV
   ```
3. Starten Sie den Data Protection for Microsoft Hyper-V-Installationsassistenten, indem Sie den folgenden Befehl ausgeben:
   ```
   ./install-Linux.bin
   ```
4. Wählen Sie die Sprache für den Installationsprozess aus und klicken Sie auf **OK**.
5. Führen Sie auf den einzelnen Seiten des Installationsassistenten die folgenden Aktionen aus.

Seite	Aktion
Willkommen	Klicken Sie auf **Weiter**.
Softwarelizenzvereinbarung	Akzeptieren Sie die Softwarelizenzvereinbarung und klicken Sie auf **Weiter**.
Gefundenes Installationsverzeichnis	Überprüfen Sie das Installationsverzeichnis (`/opt/tivoli/tsm/DPHyperV`) und klicken Sie auf **Weiter**.
Angepasst	Stellen Sie sicher, dass **Data Protection for Hyper-V-Einheit zum Versetzen von Daten** markiert ist, und klicken Sie auf **Weiter**.
Zusammenfassung der Installationsvorbereitungen	Überprüfen Sie die Installationszusammenfassung. Zum Fortsetzen der Installation klicken Sie auf **Installieren**.
Überprüfen Sie diese Informationen, bevor Sie fortfahren	Klicken Sie auf **Weiter**.
Installation abgeschlossen	Klicken Sie auf **Fertig**.

Ergebnisse

Tipp: Wenn Sie den Installationsassistenten nicht ausführen möchten, können Sie das Mount-Proxy-Feature mithilfe einer der folgenden Methoden installieren:

- Zum Installieren über die Konsole geben Sie den folgenden Befehl aus:
  ```
  ./install-Linux.bin -i console
  ```
- Informationen zur Installation im unbeaufsichtigten Modus finden Sie in „Linux-Mount-Proxy-Feature im unbeaufsichtigten Modus installieren" auf Seite 40.

Nächste Schritte

Konfigurieren Sie den Linux-Mount-Proxy für Dateizurückschreibungsoperationen. Anweisungen finden Sie in „Linux-Mount-Proxy für Dateizurückschreibungsoperationen konfigurieren" auf Seite 54.

Zugehörige Tasks:

„Mount-Proxy-Feature auf Linux-Systemen deinstallieren" auf Seite 41

Linux-Mount-Proxy-Feature im unbeaufsichtigten Modus installieren

Wenn Sie planen, Dateizurückschreibungsoperationen auf Linux-Gast-VMs (VM = virtuelle Maschine) auszuführen, müssen Sie das Mount-Proxy-Feature auf Linux-Systemen installieren, indem Sie das Data Protection for Microsoft Hyper-V-Paket der Einheit zum Versetzen von Daten für Linux verwenden. Wenn Sie das Mount-Proxy-Feature nicht interaktiv installieren möchten, können Sie die Installation im unbeaufsichtigten Modus ausführen.

Vorbereitende Schritte

Wenn Sie ein Upgrade von einer älteren Version des Linux-Mount-Proxys durchführen, sollten Sie die Informationen in „Upgrade des Linux-Mount-Proxy-Features von einer älteren Version durchführen" auf Seite 37 lesen.

Informationen zu diesem Vorgang

Für Mountoperationen in der Schnittstelle für Dateizurückschreibung ist ein Mount-Proxy-Knoten erforderlich. Der Mount-Proxy-Knoten bewirkt, dass die Dateisysteme auf den bereitgestellten VM-Platten von VM-Sicherungen als Mountpunkte für Dateizurückschreibungsoperationen zugänglich sind.

Die Linux-Mount-Proxy-Software ist Bestandteil des Linux-Pakets für die Einheit zum Versetzen von Daten. Sie ist nicht in dem standardmäßigen Data Protection for Microsoft Hyper-V-Installationspaket für Windows enthalten. Sie müssen das Linux-Paket separat herunterladen und installieren.

Vorgehensweise

Als Rootbenutzer führen Sie die folgenden Schritte auf der Linux-Gast-VM aus:

1. Laden Sie das Installationspaket herunter und extrahieren Sie es:
   a. Laden Sie das Installationspaket für die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten unter Linux von einer der folgenden Websites herunter:
      - Passport Advantage
      - Fix Central

      Das Downloadpaket heißt in der Regel `8.x.x.x-TSM4HYPERV.tar.gz`. Für die Version 8.1.6 hat das Paket beispielsweise den Namen `8.1.6.0-TSM4HYPERV.tar.gz`.

      Tipp: Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.
   b. Kopieren Sie das Linux-Paket für die Einheit zum Versetzen von Daten an die Position, an der Sie die Installationsdateien speichern möchten. Erstellen Sie beispielsweise das folgende Verzeichnis und kopieren Sie das Installationspaket in das Verzeichnis:

      ```
      /extract_folder
      ```
   c. Wechseln Sie in das Verzeichnis mit dem Installationspaket. Beispiel:

      ```
      cd /extract_folder
      ```
   d. Extrahieren Sie die Installationsdateien aus dem Installationspaket, indem Sie den folgenden Befehl ausgeben:

      ```
      tar -xvzf 8.1.6.0-TSM4HYPERV.tar.gz
      ```

Die Installationsdateien werden in das Verzeichnis `CD` extrahiert. Die Installationsdateien werden beispielsweise in dem folgenden Verzeichnis gespeichert:

`/extract_folder/CD`

2. Wechseln Sie in das Verzeichnis, das die Installationsdatei enthält. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   cd /extract_folder/CD/Linux/DataProtectionForHyperV
   ```

3. Verwenden Sie eine der folgenden Methoden, um den Mount-Proxy im unbeaufsichtigten Modus zu installieren:
   - Für die Standardinstallation geben Sie den folgenden Befehl aus:

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

   - Wenn Sie eine angepasste Installation verwenden möchten, führen Sie die folgenden Schritte aus:
     a. Editieren Sie die Datei `installer.properties` und geben Sie die jeweiligen Werte ein:
        - Entfernen Sie das Nummernzeichen (#) aus der Anweisung `LICENSE_ACCEPTED=TRUE`.
        - Ändern Sie im Parameter `USER_INSTALL_DIR=` den Standardinstallationspfad in den angepassten Pfad.
        - Stellen Sie sicher, dass das Nummernzeichen (#) aus der Anweisung `CHOSEN_INSTALL_SET=Custom` entfernt wurde.

     b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

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

Nächste Schritte

Konfigurieren Sie den Linux-Mount-Proxy für Dateizurückschreibungsoperationen. Anweisungen finden Sie in „Linux-Mount-Proxy für Dateizurückschreibungsoperationen konfigurieren” auf Seite 54.

Zugehörige Tasks:

„Mount-Proxy-Feature auf Linux-Systemen installieren” auf Seite 38

Mount-Proxy-Feature auf Linux-Systemen deinstallieren

Wenn Sie keine Dateizurückschreibungsoperationen auf Linux-Gast-VMs (VM = virtuelle Maschine) mehr ausführen müssen, können Sie das Mount-Proxy-Feature auf dem Linux-Mount-Proxy-System deinstallieren.

Vorbereitende Schritte

Führen Sie den Deinstallationsprozess als Rootbenutzer aus. Das Rootbenutzerprofil muss als Quelle verwendet werden. Wenn Sie mit dem Befehl **su** zum Root wechseln, müssen Sie den Befehl **su -** verwenden, um das Rootprofil als Quelle zu verwenden.

Informationen zu diesem Vorgang

Bei der Deinstallation des Linux-Mount-Proxy-Features entspricht der Typ der ausgeführten Deinstallation standardmäßig dem Typ der ursprünglichen Installation. Zum Verwenden eines anderen Deinstallationsprozesses geben Sie den korrekten Parameter an. Wenn Sie beispielsweise den unbeaufsichtigten Installationsprozess verwendet haben, können Sie für die Deinstallation den Installationsassistenten

verwenden, indem Sie den Parameter **–i swing** angeben.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das Linux-Mount-Proxy-Feature zu entfernen:

1. Wechseln Sie in das Verzeichnis, das das Deinstallationsprogramm enthält. Geben Sie beispielsweise den folgenden Befehl aus, um zur Standardposition des Deinstallationsprogramms zu wechseln:

   ```
   cd /opt/tivoli/tsm/DPHyperV/_uninst/DPHyperV
   ```

2. Je nach dem Typ der Installation verwenden Sie eine der folgenden Methoden, um den Linux-Mount-Proxy zu deinstallieren:
   - Zum Deinstallieren des Linux-Mount-Proxys über den Installationsassistenten geben Sie den folgenden Befehl aus:

     ```
     ./Uninstall_Data_Protection_for_Hyper-V –I swing
     ```

   - Zum Deinstallieren des Linux-Mount-Proxys über die Konsole geben Sie den folgenden Befehl aus:

     ```
     ./Uninstall_Data_Protection_for_Hyper-V -i console
     ```

   - Zum Deinstallieren des Linux-Mount-Proxys im unbeaufsichtigten Modus geben Sie den folgenden Befehl aus:

     ```
     ./Uninstall_Data_Protection_for_Hyper-V -i silent
     ```

Zugehörige Tasks:

„Feature für Dateizurückschreibung entfernen"

Feature für Dateizurückschreibung entfernen

Wenn Sie keine Dateizurückschreibungsoperationen mehr ausführen möchten, können Sie das Feature für Dateizurückschreibung entfernen, indem Sie eine Konfigurationsdatei aktualisieren. Wenn Sie Data Protection for Microsoft Hyper-V deinstallieren, müssen Sie dieselbe Konfigurationsdatei aktualisieren, um das Feature für Dateizurückschreibung zu entfernen.

Informationen zu diesem Vorgang

Zum Entfernen der Services, die zum Feature für Dateizurückschreibung gehören, müssen Sie die Datei `frConfig.props` aktualisieren und die Services entfernen, die zu den Mount-Proxy-Knoten gehören.

Vorgehensweise

Führen Sie die folgenden Schritte auf dem Hyper-V-Host oder -Cluster aus:

1. Editieren Sie die Datei `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\frConfig.props` manuell und ändern Sie die folgende Option:

   ```
   enable_filerestore=true
   ```

   Ändern Sie die Option wie dargestellt:

   ```
   enable_filerestore=false
   ```

2. Öffnen Sie **Dienste** in der Systemsteuerung des Windows-Betriebssystems und entfernen Sie die Services, die zu dem Mount-Proxy-Knoten gehören. Normalerweise heißen die Services `TSM CAD - `*`Hostname`*`_HV_MP_`*`Plattform`* und `TSM Agent - `*`Hostname`*`_HV_MP_`*`Plattform`*.

3. Entfernen Sie die Mount-Proxy-Knoten auf dem IBM Spectrum Protect-Server mit dem Befehl REMOVE NODE.

Ergebnisse

Das Feature für Dateizurückschreibung wird vom Hyper-V-Host oder -Cluster entfernt. Es ist nicht erforderlich, die Services für die Derby-Datenbank von IBM Spectrum Protect for Virtual Environments oder für den IBM Spectrum Protect-Web-Server erneut zu starten.

Nächste Schritte

Falls Sie Dateizurückschreibungsoperationen auf einer virtuellen Linux-Gastmaschine ausgeführt haben, müssen Sie das Linux-Mount-Proxy-Feature deinstallieren. Anweisungen finden Sie in „Mount-Proxy-Feature auf Linux-Systemen deinstallieren" auf Seite 41.

Kapitel 3. Data Protection for Microsoft Hyper-V konfigurieren

Nach der erfolgreichen Installation der Software IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V müssen Sie Data Protection for Microsoft Hyper-V konfigurieren, bevor Sie Sicherungs- und Zurückschreibungsoperationen ausführen. Wenn Sie Mountoperationen auf Gast-VMs mit IBM Spectrum Protect Recovery Agent ausführen möchten, müssen Sie auch Recovery Agent konfigurieren.

Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren

Sie können den Konfigurationsassistenten für die Erstkonfiguration oder für die Aktualisierung der Konfiguration von Data Protection for Microsoft Hyper-V in einer Umgebung mit einem eigenständigen Hyper-V-Host oder einer Clusterumgebung verwenden. Außerdem können Sie Data Protection for Microsoft Hyper-V mit diesem Assistenten für Dateizurückschreibungsoperationen aktivieren.

Vorbereitende Schritte

- Wenn Sie ein Upgrade von Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher durchführen und Knoten vorhanden sind, die bereits auf dem IBM Spectrum Protect-Server definiert sind, führen Sie die Tasks in „Knoten auf dem IBM Spectrum Protect-Server umbenennen" auf Seite 20 aus.
- Der Hyper-V-Host, auf dem Data Protection for Microsoft Hyper-V installiert ist, muss über Netzkonnektivität zu dem IBM Spectrum Protect-Server verfügen, der zum Speichern von Sicherungen virtueller Maschinen (VMs) verwendet wird.
- Zur Verbesserung der Leistung sollten Sie mindestens eine 10-Gb-Verbindung zwischen den Hyper-V-Hosts und dem IBM Spectrum Protect-Server verwenden.
- Sie benötigen die Anmeldeberechtigungsnachweise für das Konto des IBM Spectrum Protect-Serveradministrators.
- Sie müssen eine Verbindung zu einem sicheren IBM Spectrum Protect-Server herstellen, der SSL-Kommunikation verwendet (SSL = Secure Sockets Layer). Während der Ausführung des Konfigurationsassistenten wird automatisch ein Sicherheitszertifikat heruntergeladen.
- Stellen Sie in einer Clusterumgebung sicher, dass Sie das Data Protection for Microsoft Hyper-V-Paket auf jedem Host im Cluster installieren. Nachdem das Paket auf allen Hosts installiert wurde, führen Sie den Konfigurationsassistenten auf einem der Hosts im Cluster aus. Der Konfigurationsassistent stellt eine Verbindung zu jedem Host her, um die Konfiguration auszuführen.

  Alle Knoten, auf denen die Software Data Protection for Microsoft Hyper-V nicht installiert ist, werden bei der Clusterkonfiguration übergangen. Dies wirkt sich nicht auf die Konfiguration der übrigen Knoten aus, auf denen sie Software installiert ist. Wenn Sie dem Cluster zu einem späteren Zeitpunkt einen Knoten hinzufügen, installieren Sie Data Protection for Microsoft Hyper-V auf diesem Knoten und führen Sie den Konfigurationsassistenten für diesen Knoten aus (entweder lokal oder von einem beliebigen anderen Knoten des Clusters aus).
- Auf jedem Host, auf dem Data Protection for Microsoft Hyper-V installiert ist, müssen Sie sicherstellen, dass der HTTPS-Port, der für die Kommunikation mit Data Protection for Microsoft Hyper-V verwendet wird, in der Firewall offen ist. Wenn nicht anders angegeben, wird die Standardportnummer 9081 verwendet.

- Der Konfigurationsassistent legt die zu verwendenden Knotennamen auf der Basis des Host- oder Clusternamens fest. Sie können die Standardknotennamen verwenden oder die Knotennamen anpassen, indem Sie Präfixe und Suffixe hinzufügen. Zum Anpassen der Knotennamen müssen Sie die in „Knotennamen anpassen" auf Seite 23 beschriebenen Schritte durchführen, bevor Sie den Konfigurationsassistenten ausführen.

Informationen zu diesem Vorgang

Zur Vereinfachung der Konfiguration erstellt der Konfigurationsassistent automatisch die Knoten, die für Sicherungs-, für Zurückschreibungs- und optional für Dateizurückschreibungsoperationen erforderlich sind. Darüber hinaus registriert der Konfigurationsassistent die Knoten auf dem IBM Spectrum Protect-Server und konfiguriert die Services auf dem lokalen Windows-Host.

Weitere Informationen zu den Knotentypen, die für Data Protection for Microsoft Hyper-V verwendet werden, finden Sie in „Verwendung von IBM Spectrum Protect-Knoten in Data Protection for Microsoft Hyper-V" auf Seite 8.

Vorgehensweise

Führen Sie die folgenden Schritte auf dem Hyper-V-Host aus, um Data Protection for Microsoft Hyper-V zu konfigurieren. Für eine Clusterumgebung führen Sie die folgenden Schritte auf einem beliebigen Host im Cluster aus, auf dem Data Protection for Microsoft Hyper-V installiert ist.

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole, indem Sie auf **Start** > **IBM Spectrum Protect** > **DP for Hyper-V-Verwaltungskonsole** klicken.

   Geben Sie alternativ den folgenden Befehl bei der Eingabeaufforderung aus:

   ```
   "C:\Programme\IBM\SpectrumProtect\DPHyperV\DpHv.msc"
   ```

2. Bei der Aufforderung melden Sie sich bei der Data Protection for Microsoft Hyper-V-Verwaltungskonsole an. Geben Sie die Berechtigungsnachweise ein, mit denen Sie sich auch bei dem Hyper-V-Host anmelden.

   Das Konto, das Sie verwenden, muss der lokalen Administratorgruppe auf der Maschine angehören, damit Hyper-V- und Clusteroperationen ausgeführt werden können.

3. Wenn Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole zum ersten Mal konfigurieren, wird der Konfigurationsassistent automatisch geöffnet.

   Wenn Sie die vorhandene Konfiguration ändern, klicken Sie in einer Umgebung mit einem eigenständigen Host auf **Konfigurieren** im Aktionsfenster. In einer Clusterumgebung wählen Sie einen Clusterknoten im Navigationsfenster aus und klicken Sie auf **Konfigurieren**.

4. Bearbeiten Sie jede Seite des Assistenten und klicken Sie dann auf **Weiter**, um die nächste Seite aufzurufen.

Seite	Aktion
Einführung	Klicken Sie auf **Weiter**, um den Assistenten zu starten.

Seite	Aktion
Sicherungsserver	Geben Sie Informationen zu dem IBM Spectrum Protect-Server ein, auf dem VM-Sicherungen gespeichert werden. **Adresse des Sicherungsservers** Der Hostname oder die IP-Adresse des IBM Spectrum Protect-Servers. **SSL-Port des Sicherungsservers** Geben Sie die Portnummer für den Server-Port an, der Verwaltungsverbindungen unter Verwendung des SSL-Protokolls mit aktiviertem TLS 1.2 zulässt. Die Standardportnummer wird bereitgestellt. Akzeptieren Sie die Standardportnummer, wenn Ihr Server nicht für die Verwendung eines anderen Ports konfiguriert ist. **Verwaltungsberechtigungsnachweise** Der Benutzername und das Kennwort des IBM Spectrum Protect-Serveradministrators. Der Administrator muss über Systemberechtigung verfügen und Clientknoten auf dem Server registrieren können.
Zertifikat akzeptieren	Dieses Fenster wird nur angezeigt, wenn Sie zum ersten Mal eine Verbindung zum IBM Spectrum Protect-Server herstellen oder wenn das vorhandene Sicherheitszertifikat nicht mehr gültig ist. Klicken Sie auf **Akzeptieren**, damit das Zertifikat automatisch heruntergeladen und importiert wird. Wenn Sie eine Verbindung zu einem Server mit Version 8.1.1 oder einer früheren Stufe der Version 8 bzw. zu einem Server mit Version 7.1.7 oder früher herstellen und der Downloadprozess fehlschlägt, finden Sie weitere Informationen in „Sicherheitseinstellungen für die Verbindung zu einem IBM Spectrum Protect-Server mit Version 8.1.1 oder früher bzw. mit Version 7.1.7 oder früher konfigurieren" auf Seite 51.

Seite	Aktion
Cluster- und Hostkonfiguration	Die folgenden Optionen sind verfügbar: **Maßnahmendomäne** Wählen Sie eine Maßnahmendomäne in der Liste aus. Die Maßnahmendomäne enthält Regeln, die festlegen, wie lange VM-Sicherungen auf dem IBM Spectrum Protect-Server aufbewahrt werden und wie viele Versionen der VM-Sicherung gespeichert werden. Die Standardmaßnahmendomäne ist STANDARD. **Name des Zielknotens** Zeigt den Knotennamen an, unter dem VM-Sicherungen auf dem IBM Spectrum Protect-Server gespeichert werden. Für Cluster werden alle VM-Sicherungen unter dem Zielknoten gespeichert; unabhängig davon, welcher Knoten im Cluster die Sicherung ausführt. **Knotendefinitionen** Zeigt die Knotendefinition(en) für den eigenständigen Host oder für die Hosts im Cluster an. Informationen zu den Knotentypen finden Sie in Tabelle 1 auf Seite 9. **Dateizurückschreibung aktivieren** Wählen Sie dieses Feld aus, wenn Sie die Webschnittstelle für Dateizurückschreibung verwenden möchten, um einzelne Dateien aus einer VM-Sicherung zurückzuschreiben. Wenn Sie dieses Kontrollkästchen auswählen, wird das Mount-Proxy-Knotenpaar für jeden Host automatisch der Liste hinzugefügt. Dieses Knotenpaar stellt die Linux- und Windows-Proxy-Systeme dar, die über eine iSCSI-Verbindung auf die bereitgestellten VM-Platten zugreifen. Diese Knoten bewirken, dass die Dateisysteme auf den bereitgestellten VM-Platten als Mountpunkte für Dateizurückschreibungsoperationen zugänglich sind. Bei der Erstkonfiguration ist **Dateizurückschreibung aktivieren** standardmäßig markiert. **Einstellungen für Dateizurückschreibung** Klicken Sie auf diese Schaltfläche, um die Berechtigungsnachweise für den Dateizurückschreibungsadministrator einzugeben.

Seite	Aktion
Einstellungen für Dateizurückschreibung	Dieses Fenster wird nur angezeigt, wenn Sie das Feature für Dateizurückschreibung aktiviert haben. Geben Sie die Berechtigungsnachweise für den Dateizurückschreibungsadministrator ein. Das Konto muss ein Windows-Domänenbenutzerkonto mit lokaler Administratorberechtigung für alle VMs sein.
Zusammenfassung	Überprüfen Sie die Einstellungen und klicken Sie auf **Weiter**, um die Konfiguration auszuführen.
Ergebnisse	Die Ergebnisse der Konfiguration werden angezeigt. Wenn die Konfiguration nicht erfolgreich verlaufen ist, wird eine Liste mit Fehlern angezeigt. Beheben Sie die Fehler und führen Sie die Konfiguration erneut aus. Wenn das Feature für Dateizurückschreibung erfolgreich konfiguriert wurde, werden in der Ergebnistabelle der Dateizurückschreibung Informationen zum Host, zum Linux-Mount-Proxy und zu URLs für die Dateizurückschreibung angezeigt. Sie können auf **Kopieren** klicken, um alle Informationen in die Zwischenablage zu kopieren. Sie müssen die Anweisungen in „Umgebung für Dateizurückschreibungsoperationen aktivieren" auf Seite 52 ausführen, um die Konfiguration der Dateizurückschreibung abzuschließen.

Ergebnisse

Wenn der Assistent erfolgreich ausgeführt wurde, können Sie Sicherungs- und Zurückschreibungsoperationen über die Eingabeaufforderung, über Powershell-Cmdlets oder über die Data Protection for Microsoft Hyper-V-Verwaltungskonsole ausführen.

Für mehr Bedienungskomfort können Sie die Schnittstelle für Dateizurückschreibung auch öffnen, indem Sie auf **Dateizurückschreibung** im Fenster **Aktionen** klicken.

Nächste Schritte

Sie können die Konfiguration überprüfen, indem Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole oder das PowerShell-Cmdlet **`Test-DpHvConfiguration`** ausführen. Weitere Informationen siehe:

- „Konfiguration von Data Protection for Microsoft Hyper-V überprüfen" auf Seite 85
- „Beispiele für Data Protection for Microsoft Hyper-V-Cmdlets" auf Seite 157

Mit dem Cmdlet **Set-DpHvMmcLoginPreferences** können Sie auch den bevorzugten Host für die Anmeldung angeben. Weitere Informationen finden Sie in Kapitel 7, „Virtuelle Maschinen mithilfe von Windows PowerShell-Cmdlets schützen", auf Seite 151.

War das Feature für Dateizurückschreibung bei der Konfiguration von Data Protection for Microsoft Hyper-V aktiviert und haben Sie den Konfigurationsassistenten nach der Erstkonfiguration erneut ausgeführt, muss das Kennwort des Linux-Mount-Proxy-Knotens zurückgesetzt werden. Verwenden Sie zum Zurücksetzen des Kennworts eine der folgenden Methoden:

Methode 1

Der IBM Spectrum Protect-Administrator führt auf dem Linux-Mount-Proxy den Befehl **dsmc** aus und gibt bei der entsprechenden Aufforderung die Benutzer-ID und das Kennwort des IBM Spectrum Protect-Administrators ein.

Methode 2

Führen Sie die folgenden Schritte aus:

1. Der IBM Spectrum Protect-Administrator setzt das Kennwort des Linux-Mount-Proxy-Knotens zurück, indem er den Serverbefehl UPDATE NODE auf der IBM Spectrum Protect-Serverkonsole ausführt.
2. Der Eigner des Linux-Mount-Proxy-Knotens führt den Befehl **dsmc** auf dem Linux-Mount-Proxy aus. Bei der entsprechenden Aufforderung gibt der Eigner die standardmäßige ID für den Linux-Mount-Proxy-Knoten und das neue Kennwort für den Linux-Mount-Proxy-Knoten ein (diese Informationen hat er beim IBM Spectrum Protect-Serveradministrator angefordert).

Zugehörige Tasks:

„Andere Portnummer als die Standardportnummer für Data Protection for Microsoft Hyper-V-Operationen konfigurieren" auf Seite 71

Sicherheitseinstellungen für Data Protection for Microsoft Hyper-V konfigurieren

Die Einstellungen, die für eine sichere Verbindung zum IBM Spectrum Protect-Server benötigt werden, sind von der Version des Servers abhängig, zu dem Sie eine Verbindung herstellen.

Informationen zu diesem Vorgang

IBM Spectrum Protect-Server mit Version 8.1.2 oder höher und mit Version 7.1.8 stellen ein verbessertes Sicherheitsprotokoll zur Verfügung, das die gesamte Kommunikation zwischen dem Server und den Clients mit Transport Layer Security (TLS) 1.2 verschlüsselt. Data Protection for Microsoft Hyper-V und der Server werden automatisch so konfiguriert, dass sie das Protokoll Secure Sockets Layer (SSL) für die Kommunikation miteinander verwenden. Zertifikate werden automatisch verteilt.

Wenn Sie den Konfigurationsassistenten verwenden, um Data Protection for Microsoft Hyper-V zu konfigurieren, werden Sie aufgefordert, das Sicherheitszertifikat zu akzeptieren. Für den Abruf und Import des Zertifikats sind keine manuellen Schritte erforderlich. Weitere Informationen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.

Wenn Sie eine Verbindung zu IBM Spectrum Protect-Servern mit früheren Versionen herstellen und der automatische Downloadprozess für das Zertifikat fehlschlägt, müssen Sie das Zertifikat manuell herunterladen und importieren, bevor Sie den Konfigurationsassistenten ausführen. Weitere Informationen finden Sie in „Sicherheitseinstellungen für die Verbindung zu einem IBM Spectrum Protect-Server mit Version 8.1.1 oder früher bzw. mit Version 7.1.7 oder früher konfigurieren".

Sicherheitseinstellungen für die Verbindung zu einem IBM Spectrum Protect-Server mit Version 8.1.1 oder früher bzw. mit Version 7.1.7 oder früher konfigurieren

Sie können Data Protection for Microsoft Hyper-V für die Kommunikation mit einem IBM Spectrum Protect-Server der Version 8.1.1 oder früher bzw. der Version 7.1.7 oder früher über das Protokoll Transport Layer Security (TLS) aktivieren.

Informationen zu diesem Vorgang

Wenn der Server für die Verwendung von SSL mit aktiviertem TLS 1.2 konfiguriert ist, wird automatisch ein Truststore mit einem Zertifikat erstellt, wenn im Konfigurationsassistenten das Sicherheitszertifikat akzeptiert wird. Wenn jedoch der automatische Downloadprozess fehlschlägt, müssen Sie den Truststore manuell erstellen und den Konfigurationsassistenten erneut ausführen.

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

Dieses Tool befindet sich im Verzeichnis `C:\Programme\Common Files\Tivoli\TSM\jvm80406\jre\bin`. Diese Position kann sich je nach der von Ihnen verwendeten Version der Java-Software ändern.

Vorgehensweise

Führen Sie die folgenden Schritte auf einem eigenständigen Hyper-V-Host aus. In einer Clusterumgebung führen Sie die folgenden Schritte für jeden Host im Cluster aus.

1. Fordern Sie das notwendige Zertifikat vom IBM Spectrum Protect-Serveradministrator an und laden Sie es an eine Position auf Ihrem Host herunter, z. B. in das Verzeichnis `c:\cert`.
2. Wechseln Sie bei der Eingabeaufforderung in das Truststore-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

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

   Wenn dieser Ordner nicht vorhanden ist, erstellen Sie ihn.
3. Importieren Sie das Zertifikat mit dem folgenden Befehl:

   ```
   "C:\Programme\Common Files\Tivoli\TSM\jvm80406\jre\bin\keytool.exe"
   -importcert -alias mein-Zertifikat -file "Name-der-Zertifikatsdatei"
   -keystore tsm-ve-truststore.jks -storepass Kennwort
   ```

   Hierbei gilt Folgendes:

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

-file "*Name-der-Zertifikatsdatei***"**
Der Name der Datei, die das selbst signierte Serverzertifikat oder das Stammzertifikat der Zertifizierungsstelle enthält. Beispiel: `"C:\cert\cert256.arm"`.

-storepass *Kennwort*
Das Schlüsselspeicherkennwort. Stellen Sie sicher, dass Sie sich dieses Kennwort für die zukünftige Verwendung merken.

4. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V-Verwaltungskonsole starten" auf Seite 75.
5. Klicken Sie auf **Konfigurieren**, um den Konfigurationsassistenten zu öffnen.
6. Geben Sie auf der Seite **Sicherungsserver** die Portnummer im Feld **SSL-Port des Sicherungsservers** an. Dieser Port ist der Server-Port, der Verwaltungsverbindungen unter Verwendung von SSL mit aktiviertem TLS 1.2 zulässt.
7. Führen Sie den Assistenten vollständig aus.

Ergebnisse

Wenn der Assistent erfolgreich ausgeführt wurde, können Sie Sicherungs- und Zurückschreibungsoperationen über die Eingabeaufforderung, über Powershell-Cmdlets oder über die Data Protection for Microsoft Hyper-V-Verwaltungskonsole ausführen.

Umgebung für Dateizurückschreibungsoperationen aktivieren

Wenn das Feature für Dateizurückschreibung von einem Administrator aktiviert wurde, können Dateieigner mit minimaler Unterstützung Dateien zurückschreiben.

Informationen zu diesem Vorgang

Wenn Sie das Feature für Dateizurückschreibung mit dem Konfigurationsassistenten aktivieren, wird die für Dateizurückschreibungsoperationen erforderliche Software auf dem Knoten der Einheit zum Versetzen von Daten auf einem eigenständigen Hyper-V-Host oder auf jedem Host in einem Cluster installiert.

In einer Clusterumgebung ist die Dateizurückschreibungssoftware auf jedem Host im Cluster unabhängig von den anderen Hosts. Damit der Dateieigner sich bei der Schnittstelle für Dateizurückschreibung anmelden kann, sind in der URL für die Dateizurückschreibung der Name des Hosts und der Name der virtuellen Maschine (VM) erforderlich, die die Daten des Dateieigners enthält.

Vorgehensweise

1. Zum Starten des Konfigurationsassistenten wählen Sie einen Host oder Cluster im Navigationsfenster aus und klicken Sie auf **Konfigurieren**.
2. Befolgen Sie die Anweisungen auf jeder Seite des Assistenten. Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.
   a. Wenn das Fenster **Cluster- und Hostkonfiguration** angezeigt wird, wählen Sie das Kontrollkästchen **Dateizurückschreibung aktivieren** aus.
   b. Wenn Sie die Dateizurückschreibung zum ersten Mal aktivieren, werden Sie aufgefordert, die Berechtigungsnachweise für den Dateizurückschreibungs-

administrator einzugeben. Das Administratorkonto muss ein Windows-Domänenbenutzerkonto mit lokaler Administratorberechtigung für alle VMs sein.

3. Optional: Wenn Sie planen, Dateizurückschreibungsoperationen auf Linux-Gast-VMs auszuführen, klicken Sie in der Ergebnistabelle der Dateizurückschreibung auf der Seite **Ergebnisse** auf **Kopieren**, um die URL für die Dateizurückschreibung und die Optionen für den Linux-Mount-Proxy in die Zwischenablage zu kopieren. Sie können die Mount-Proxy-Optionen in die Datei `dsm.sys` einfügen, wenn Sie den Linux-Mount-Proxy konfigurieren.

   Sie können diese Dateizurückschreibungsinformationen auch nach der Konfiguration jederzeit abrufen, indem Sie im Fenster **Aktionen** auf **Eigenschaften** klicken.

   Weitere Informationen zur Konfiguration des Linux-Mount-Proxys finden Sie in „Linux-Mount-Proxy für Dateizurückschreibungsoperationen konfigurieren" auf Seite 54.
4. Schließen Sie die Konfiguration im Assistenten ab.
5. Überprüfen Sie, ob Sie auf die Schnittstelle für Dateizurückschreibung zugreifen können, indem Sie eine VM im Fenster **Ergebnisse** auswählen und auf **Dateizurückschreibung** im Fenster **Aktionen** klicken.
6. Erstellen Sie die angepasste URL für jeden Dateieigner auf der Basis der folgenden Schablone für die URL der Dateizurückschreibung:

   ```
   https://<DPHV-Host>:9081/FileRestoreUI/login?vmName=<Name_der_Gast-VM>
   &vmHost=<Host_der_Gast-VM>&vmPlatform=<Plattform_der_Gast-VM>
   ```

   Hierbei gilt Folgendes:

   DPHV-Host
   Der Hyper-V-Host, auf dem Sie Data Protection for Microsoft Hyper-V installiert und konfiguriert haben.

   Name_der_Gast-VM
   Der Name der Gast-VM, die Daten für den Dateieigner enthält.

   Host_der_Gast-VM
   Der Name des VM-Hosts, von dem die Gast-VM gehostet wird. Der Wert für *Host_der_Gast-VM* kann der Computername, die IP-Adresse oder der DNS-Name sein.

   Plattform_der_Gast-VM
   Das Betriebssystem der Gast-VM. Geben Sie einen der folgenden Werte an: **LINUX** oder **WINDOWS**.

   Beispiel: Wenn Data Protection for Microsoft Hyper-V auf einem Hyper-V-Host mit dem Namen `Cluster1` installiert ist und die Daten des Dateieigners sich auf einer Windows-Gast-VM mit dem Namen `MyVM-Win2k26` auf dem VM-Host `HostB` befinden, lautet die Dateizurückschreibungs-URL wie folgt:

   ```
   https://Cluster1:9081/FileRestoreUI/login?vmName=MyVM-Win2k26
   &vmHost=HostB&vmPlatform=WINDOWS
   ```

   Direktaufruf: Sie können die URL für die Dateizurückschreibung auch abrufen, indem Sie einen Host und eine VM auswählen und auf **Dateizurückschreibung** im Fenster **Aktionen** klicken. Sie können die URL-Adresse kopieren, die im Web-Browser angezeigt wird.

   Tipp: Wenn Sie nicht die Standardportnummer verwenden, ersetzen Sie den Port 9081 durch den Port, den Sie konfiguriert haben. Informationen zum Anzeigen der Portnummern, die in Verwendung sind, finden Sie in „Andere Port-

nummer als die Standardportnummer für Data Protection for Microsoft Hyper-V-Operationen konfigurieren" auf Seite 71.

7. Verteilen Sie die URLs für die Dateizurückschreibung anhand der folgenden Szenarios:
   - Für das Help-Desk-Modell sendet der Hyper-V- oder Dateizurückschreibungsadministrator eine angepasste URL an jeden Dateieigner.
   - Für das Self-Service-Modell sendet der Hyper-V- oder Dateizurückschreibungsadministrator Anweisungen an die Dateieigner, sodass diese ihre jeweiligen Dateizurückschreibungs-URLs selbst erstellen können. Sie können die Informationen zur URL aus Schritt 6 auf Seite 53 in Ihren Anweisungen für die Dateieigner verwenden.

   Tipp: Bei einem Failover können VMs jederzeit von anderen Hosts in einem Cluster übernommen werden. In dieser Situation müssen Sie dem Dateieigner eine neue URL mit der aktualisierten Gast-VM senden oder der Dateieigner muss mit Ihnen in Kontakt treten, um festzustellen, von welchem Host die VM gehostet wird.

Ergebnisse

Die Dateieigner sind in der Lage, sich bei der Schnittstelle für Dateizurückschreibung anzumelden und einzelne Dateien und Ordner zurückzuschreiben.

Linux-Mount-Proxy für Dateizurückschreibungsoperationen konfigurieren

Zur Vorbereitung einer virtuellen Linux-Gastmaschine (virtuelle Maschine = VM) für Dateizurückschreibungsoperationen müssen Sie den Linux-Mount-Proxy konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die folgenden Tasks ausführen:

1. Den Konfigurationsassistenten von Data Protection for Microsoft Hyper-V auf dem Hyper-V-Host oder -Cluster ausführen, um das Feature für Dateizurückschreibung zu aktivieren. Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.
2. Den Mount-Proxy auf einem Linux-System installieren. Anweisungen finden Sie in „Mount-Proxy-Feature auf Linux-Systemen installieren" auf Seite 38.

Informationen zu diesem Vorgang

Wenn Sie das Feature für Dateizurückschreibung mit dem Konfigurationsassistenten aktivieren, wird das Mount-Proxy-Knotenpaar für einen eigenständigen Host oder für jeden Host in einem Cluster automatisch beim IBM Spectrum Protect-Server registriert. Zudem werden die Proxy-Beziehungen definiert. Zum Aktivieren der Gast-VM für Dateizurückschreibungsoperationen müssen Sie den Linux-Mount-Proxy konfigurieren, indem Sie die Optionen für den Linux-Mount-Proxy, die vom Konfigurationsassistenten bereitgestellt werden, der Datei `dsm.sys` hinzufügen.

Mit der folgenden Prozedur wird der Mount-Proxy-Knoten eingerichtet, indem die Mount-Proxy-Knotenoptionen aktualisiert werden und die Konnektivität zum IBM Spectrum Protect-Server überprüft wird.

Vorgehensweise

Führen Sie die folgenden Schritte auf dem Linux-Mount-Proxy-System aus:

1. Wenn die Clientbenutzeroptionsdatei (`dsm.opt`) sich nicht im Installationsverzeichnis (`opt/tivoli/tsm/client/ba/bin`) befindet, erstellen Sie die Datei mit einem Texteditor.
2. Öffnen Sie die Datei `dsm.opt` mit einem Texteditor und fügen Sie der Datei die folgende Anweisung hinzu:

   ```
   servername MPNODE_Hostname_HV_MP_LNX
   ```

   Dabei ist ist *Hostname* der Name des Windows Hyper-V-Hosts.

   Stellen Sie sicher, dass diese Anweisung die einzige Anweisung in der Datei ist. Speichern Sie Ihre Aktualisierungen und schließen Sie die Datei.
3. Öffnen Sie die Datei `dsm.sys` mit einem Texteditor. Kopieren Sie die Mount-Proxy-Optionen aus dem Fenster **Optionen für den Linux-Mount-Proxy** des Konfigurationsassistenten und fügen Sie sie in die Datei ein.

   Fügen Sie beispielsweise die folgende Zeilengruppe in die Datei `dsm.sys` ein:

   ```
   SERVERNAME           MPNODE_Hostname_HV_MP_LNX
   NODename             Hostname_HV_MP_LNX
   PASSWORDAccess       generate
   TCPServeraddress     Adresse_des_Sicherungsservers
   TCPPort              1500
   HTTPPort             1581 ** Muss für jeden Knoten eindeutig sein
   COMMMethod           tcpip
   ERRORLOGName         dsmerror.Hostname_HV_MP_LNX.log
   ```

   Dabei ist *Hostname* der Name des Hyper-V-Hosts und *Adresse_des_Sicherungsservers* ist der Hostname oder die IP-Adresse des IBM Spectrum Protect-Servers, auf dem die VMs gesichert werden.

   Speichern Sie Ihre Änderungen und schließen Sie die Datei `dsm.sys`.
4. Starten Sie auf dem Mount-Proxy-System eine Befehlszeilensitzung mit den Befehlszeilenparametern `-asnodename` und `-optfile`:

   ```
   dsmc -asnodename=Hyper-V-Zielknoten -optfile=dsm.opt
   ```

   Dabei ist *Hyper-V-Zielknoten* der Hyper-V-Knotenname, unter dem Ihre VM-Sicherungen gespeichert werden. Der Hyper-V-Zielknoten entspricht der folgenden Namenskonvention:

   - Für eine Umgebung mit einem eigenständigen Host: *Hostname*_HV_TGT
   - Für eine Clusterumgebung: *Clustername*_HV_TGT

   Bei der ursprünglichen Anmeldung werden Sie aufgefordert, eine Benutzer-ID und ein Kennwort einzugeben. Geben Sie Ihre IBM Spectrum Protect-Serveradministrator-ID und das zugehörige Kennwort ein.

   Nach der ursprünglichen Anmeldung wird ein neues Kennwort generiert und gespeichert, sodass Sie nicht mehr zur Eingabe des Kennworts aufgefordert werden.

   Um sicherzustellen, dass Sie nicht zur Eingabe des Kennworts aufgefordert werden, führen Sie den Befehl **dsmc** erneut aus. Wenn Sie zur Eingabe des Kennworts aufgefordert werden, stellen Sie sicher, dass die Option `passwordaccess generate` in der Datei `dsm.sys` definiert ist. Anschließend wiederholen Sie Schritt 4.
5. Überprüfen Sie die Verbindung zum IBM Spectrum Protect-Server, indem Sie den folgenden Befehl ausgeben:

   ```
   dsmc query session
   ```

Dieser Befehl zeigt Informationen zu Ihrer Sitzung an, darunter den aktuellen Knotennamen, die Startzeit der Sitzung, die Serverinformationen und die Informationen zur Serververbindung.

6. Richten Sie den Clientakzeptorservice (CAD) ein, indem Sie die folgenden Aktionen ausführen:
   a. Definieren Sie die folgende Umgebungsvariable in der Datei `/etc/init.d/dsmcad`:

      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
      ```

   b. Das Installationsprogramm erstellt ein Startscript für den Clientakzeptor (`dsmcad`) im Verzeichnis `/etc/init.d`. Der Clientakzeptor muss gestartet werden, damit er Scheduler-Tasks verwalten kann.

      Stellen Sie sicher, dass Sie mit der Rootbenutzer-ID angemeldet sind, und verwenden Sie anschließend den folgenden Befehl, um den Clientakzeptor zu starten:

      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
      service dsmcad start
      ```

      Wenn der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden soll, fügen Sie den Service wie folgt bei einer Shelleingabeaufforderung hinzu:

      ```
      # chkconfig --add dsmcad
      ```

Nächste Schritte

Überprüfen Sie, ob der Linux-Mount-Proxy-Knoten korrekt eingerichtet ist:

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole auf dem Hyper-V-Host oder im Cluster.
2. Wählen Sie eine Linux-VM aus und klicken Sie im Fenster **Aktionen** auf **Dateizurückschreibung**, um die Schnittstelle für Dateizurückschreibung aufzurufen.
3. Überprüfen Sie, ob Sie Dateizurückschreibungsoperationen für die Linux-Gast-VM ausführen können.

War das Feature für Dateizurückschreibung bei der Konfiguration von Data Protection for Microsoft Hyper-V aktiviert und haben Sie den Konfigurationsassistenten nach der Erstkonfiguration erneut ausgeführt, muss das Kennwort des Linux-Mount-Proxy-Knotens zurückgesetzt werden. Verwenden Sie zum Zurücksetzen des Kennworts eine der folgenden Methoden:

Methode 1

Der IBM Spectrum Protect-Administrator führt auf dem Linux-Mount-Proxy den Befehl **dsmc** aus und gibt bei der entsprechenden Aufforderung die Benutzer-ID und das Kennwort des IBM Spectrum Protect-Administrators ein.

Methode 2

Führen Sie die folgenden Schritte aus:

1. Der IBM Spectrum Protect-Administrator setzt das Kennwort des Linux-Mount-Proxy-Knotens zurück, indem er den Serverbefehl UPDATE NODE auf der IBM Spectrum Protect-Serverkonsole ausführt.
2. Der Eigner des Linux-Mount-Proxy-Knotens führt den Befehl **dsmc** auf dem Linux-Mount-Proxy aus. Bei der entsprechenden Aufforderung gibt der Eigner die standardmäßige ID für den Linux-Mount-Proxy-

Knoten und das neue Kennwort für den Linux-Mount-Proxy-Knoten ein (diese Informationen hat er beim IBM Spectrum Protect-Serveradministrator angefordert).

Optionen für Dateizurückschreibungsoperationen ändern

Ändern Sie die Optionen in der Datei `frConfig.props`, damit Administratoren die Dateizurückschreibungsoperationen konfigurieren und steuern können.

Informationen zu diesem Vorgang

Führen Sie diese Schritte auf dem System aus, auf dem die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installiert ist.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis, in dem sich die Datei `frConfig.props` 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. Informationen zu den Optionen, die möglicherweise geändert werden müssen, finden Sie in „Optionen für Dateizurückschreibungsoperationen".
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 Dateizurückschreibungsoperationen

Die Optionen in der Datei `frConfig.props` steuern die Konfiguration, Unterstützung und Zurückschreibungsverarbeitung für Dateizurückschreibungsoperationen.

backup_info_duration_hours=*Anz_Std*
Geben Sie die Zeit in Stunden an, während der Informationen zu kürzlich ausgeführten Sicherungsaktivitäten in der lokalen Derby-Datenbank von Data Protection for Microsoft Hyper-V aufbewahrt werden. Der Maximalwert ist 14 Tage (336 Stunden). Der Standardwert ist eine Woche (168 Stunden).

enable_contact_info=false | true
Geben Sie an, ob Kontaktinformationen für den Administrator bereitgestellt werden sollen, die Dateieigner verwenden können, um in der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung Unterstützung anzufordern.

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 für die 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
- Fenster **Produktinformation** im Hilfemenü
- Link zu Unterstützungsinformationen in den Schnittstellennachrichten

Mit dem Assistenten der Data Protection for Microsoft Hyper-V-Verwaltungskonsole können Sie die Option **enable_filerestore** überschreiben, jedoch nur mit dem Wert **true**. Wenn Sie das Feature für Dateizurückschreibung inaktivieren möchten, müssen Sie die Option manuell auf **false** setzen.

Data Protection for Microsoft Hyper-V-Protokollaktivität konfigurieren

Ändern Sie die Optionen in der Datei FRLog.config, damit Administratoren die Formatierung und Protokollierung von Inhalt für Operationen der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der Dateizurückschreibung konfigurieren und steuern können.

Vorbereitende Schritte

Die Datei FRLog.config wird generiert, wenn zum ersten Mal auf die Data Protection for Microsoft Hyper-V-Verwaltungskonsole oder die Schnittstelle für Dateizurückschreibung zugegriffen wird.

Informationen zu diesem Vorgang

Führen Sie diese Schritte auf dem System aus, auf dem die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installiert ist.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis, in dem sich die Datei FRLog.config 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. Informationen zu den Optionen, die möglicherweise geändert werden müssen, finden Sie in „Optionen für die Data Protection for Microsoft Hyper-V-Protokollaktivität".
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** > **System und Sicherheit** > **Verwaltung** > **Dienste**.
   b. Klicken Sie mit der rechten Maustaste auf **IBM Spectrum Protect for Virtual Environments Web Server** und klicken Sie auf **Neu starten**.

Ergebnisse

Die Einstellungen werden auf den Inhalt und das Format der Protokollinformationen für Operationen der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der Dateizurückschreibung angewendet.

Optionen für die Data Protection for Microsoft Hyper-V-Protokollaktivität

Die FRLog.config-Optionen steuern den Inhalt und das Format der Protokollinformationen für Operationen der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der Dateizurückschreibung.

Mit den folgenden Optionen werden Informationen für Tasks der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der Dateizurückschreibung 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 für Services der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der Dateizurückschreibung in der Datei `fr_api.log` protokolliert. Diese Services sind interne API-Services, die zur Aktivität der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der Dateizurückschreibung 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` 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 *Installationsverzeichnis*`/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs`.

FR.API.LOG=ON | OFF
Geben Sie an, ob die Protokollierung für Services der Data Protection for Microsoft Hyper-V-Verwaltungskonsole und der Dateizurückschreibung aktiviert werden soll.

- Zum Aktivieren der Protokollierung geben Sie ON an. Der Standardwert ist ON.
- Zum Inaktivieren der Protokollierung geben Sie OFF an.

IBM Spectrum Protect Recovery Agent-GUI konfigurieren

Sie müssen die IBM Spectrum Protect Recovery Agent-GUI für Mount- und Dateizurückschreibungsoperationen einrichten.

Vorbereitende Schritte

Diese Konfigurationstasks müssen abgeschlossen sein, bevor Sie die IBM Spectrum Protect Recovery Agent-GUI verwenden.

Vorgehensweise

1. Melden Sie sich bei dem System an, auf das Dateien zurückgeschrieben werden sollen. IBM Spectrum Protect Recovery Agent muss auf dem System installiert sein.
2. Klicken Sie auf **IBM Spectrum Protect-Server auswählen** in der IBM Spectrum Protect Recovery Agent-GUI, um eine Verbindung zu dem IBM Spectrum Protect-Server herzustellen.

   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 auf dem Zielknoten befindlichen Sicherungen virtueller Maschinen zu verwenden. Der Proxy-Knoten ist ein Knoten, dem "Proxy"-Berechtigung für die Ausführung von Operationen für den Zielknoten erteilt wird.

Normalerweise verwenden Sie 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 Sicherungen virtueller Maschinen 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 die IBM Spectrum Protect-Seite zu verlassen.

Bei Verwendung dieser Methode kennt der Benutzer von IBM Spectrum Protect 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 bestimmter virtueller Maschinen auf dem Zielknoten begrenzt ist.

Normalerweise wird diesem Knoten mit dem Befehl `set access` Zugriff von dem Zielknoten erteilt, der Eigner der Sicherungen virtueller Maschinen ist.

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

Der folgende Befehl gibt beispielsweise 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 Sicherungen virtueller Maschinen 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 die IBM Spectrum Protect-Seite zu verlassen.

Mit dieser Methode können Sie eine vollständige Liste gesicherter virtueller Maschinen anzeigen. Sie können jedoch nur die Sicherungen virtueller Maschinen zurückschreiben, für die dem Knoten der Zugriff erteilt wurde. Außerdem sind die Momentaufnahmedaten nicht vor dem Verfall auf dem Server geschützt.

Direkt Wählen Sie diese Option aus, um sich direkt beim Zielknoten zu authentifizieren (der Knoten, auf dem sich die Sicherungen virtueller Maschinen 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 Sicherungen virtueller Maschinen 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 die IBM Spectrum Protect-Seite zu verlassen.

Kennwortzugriff 'generate' verwenden
Wenn diese Option ausgewählt und das Kennwortfeld leer ist, authentifiziert sich IBM Spectrum Protect Recovery Agent mit einem bestehenden Kennwort, das im Kennwortspeicher 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 im Kennwortspeicher gespeichert. Wählen Sie deshalb das Kontrollkästchen **Kennwortzugriff 'generate' verwenden** aus und geben Sie kein Kennwort ein.

Weitere Informationen zum Kennwortspeicher finden Sie in Sicherer Kennwortspeicher.

IBM Spectrum Protect 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 IBM Spectrum Protect Recovery Agent, der auf dem Sicherungs-Proxy-Host ausgeführt wird, speichert Datenänderungen auf einem virtuellen Datenträger im Schreibcache. Standardmäßig ist der Schreibcache aktiviert und die maximale Cachegröße beträgt 90 % des verfügbaren Speicherbereichs 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.

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.

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

Voraussetzung: 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. Diese Option ist standardmäßig abgewählt. 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. 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 Mountsitzungen 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. IBM Spectrum Protect 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 den folgenden 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.

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 Si-

cherheitsprotokolle 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`

iSCSI-Einheit manuell konfigurieren

Sie müssen das Windows-System konfigurieren, das während 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:

- Bei einer iSCSI-Bereitstellung wird auf dem IBM Spectrum Protect Recovery Agent-System ein iSCSI-Ziel erstellt. Sie können von jedem System aus eine Verbindung zum iSCSI-Ziel herstellen, um einen Datenträger zu erstellen, der die Sicherungsdaten enthält. Außerdem können Sie dann diesen Datenträger von einem anderen System bereitstellen.
- Der iSCSI-Initiator ist auf jedem System erforderlich, das mit dem iSCSI-Ziel verbunden werden muss.
- Stellen Sie sicher, dass auf dem System, auf dem die Daten zurückgeschrieben werden sollen, ein iSCSI-Initiator installiert ist.
- Der Microsoft-iSCSI-Initiator wird auf dem IBM Spectrum Protect Recovery Agent-System nicht benötigt.

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 einzige 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 die folgenden Tasks aus, um das Windows-System zu konfigurieren, das während einer iSCSI-Mountoperation verwendet wird:

Vorgehensweise

1. Öffnen Sie auf dem IBM Spectrum Protect Recovery Agent-System Port `3260` in der LAN-Firewall und in der Firewall des Windows-Clients. Notieren Sie den iSCSI-Initiatornamen auf dem System, auf dem die 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 IBM Spectrum Protect Recovery Agent (iSCSI-Ziel) installiert ist:

a. Starten Sie die IBM Spectrum Protect 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.

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 IBM Spectrum Protect 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. Wählen Sie auf dem Initiatorsystem die Optionen **Systemsteuerung** > **Verwaltung** > **Computerverwaltung** > **Speicher** > **Datenträgerverwaltung** aus.

      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. Führen Sie die folgenden Tasks aus, nachdem die Datei zurückgeschrieben wurde:

   a. Trennen Sie über den Dialog **iSCSI-Initiator-Eigenschaften** die Verbindung zu jedem iSCSI-Ziel.

   b. Heben Sie die Bereitstellung des Datenträgers aus Schritt 2 auf, indem Sie den Datenträger in der IBM Spectrum Protect Recovery Agent-GUI auswählen und auf **Bereitstellung aufheben** klicken.

Erweiterte Konfiguration

Verwenden Sie erweiterte Konfigurationstasks, um die Konfiguration von Data Protection for Microsoft Hyper-V noch weiter anzupassen.

Andere Portnummer als die Standardportnummer für Data Protection for Microsoft Hyper-V-Operationen konfigurieren

Wenn Sie nicht die Standardportnummern für die Services des Data Protection for Microsoft Hyper-V-Web-Servers oder der -REST-API verwenden möchten, können Sie mithilfe von Windows Powershell-Cmdlets andere Portnummern konfigurieren.

Informationen zu diesem Vorgang

Die Standardportnummer, die dem Web-Server zugeordnet ist, stellt Services für die Data Protection for Microsoft Hyper-V-Verwaltungskonsole, für die Schnittstelle für Dateizurückschreibung und für Powershell-Cmdlets zur Verfügung.

Führen Sie die Schritte in der folgenden Prozedur aus, um die Portnummer zu ändern.

Vorgehensweise

1. Starten Sie Powershell anhand der Anweisungen in „Verwendung von PowerShell-Cmdlets mit Data Protection for Microsoft Hyper-V vorbereiten" auf Seite 151.
2. Optional: Zeigen Sie die verwendeten Portnummern an, indem Sie die folgenden Cmdlets ausführen:
   - Zum Anzeigen des Web-Server-Ports verwenden Sie das Cmdlet **Show-DpHvHttpsPort**.
   - Zum Anzeigen des REST-API-Ports verwenden Sie das Cmdlet **Show-DpHvMmcLoginPreferences**.

     Dieses Cmdlet zeigt die Anmeldevorgaben einschließlich der REST-API-Portnummer für die Data Protection for Microsoft Hyper-V-Verwaltungskonsole an. Die Vorgaben werden bei der ersten Ausführung der Verwaltungskonsole erstellt. Wenn Sie dieses Cmdlet ausführen, bevor die Verwaltungskonsole zum ersten Mal ausgeführt wurde, werden keine Informationen zurückgegeben.
3. Verwenden Sie die folgenden Cmdlets, um die Standardportnummern zu ändern:
   - Zum Ändern des Web-Server-Ports verwenden Sie das Cmdlet **Set-DpHvHttpsPort**. Soll beispielsweise die Web-Server-Portnummer in 9082 geändert werden, verwenden Sie das folgende Cmdlet:

     ```
     Set-DpHvHttpsPort -httpsPort 9082
     ```

     Alle Hosts in einem Cluster müssen denselben HTTPS-Port verwenden.
   - Zum Ändern des REST-API-Ports verwenden Sie das Cmdlet **Set-DpHvMmcLoginPreferences**. Soll beispielsweise die REST-API-Portnummer in 9082 geändert werden, verwenden Sie das folgende Cmdlet:

     ```
     Set-DpHvMmcLoginPreferences -RestApiPort 9082
     ```

   Tipp: Weitere Beispiele können Sie mit dem Befehl **Get-Help** *Cmdlet-Name* aufrufen.

Geplante VM-Sicherungen für Windows Server 2012- und 2012 R2-Cluster optimieren

Ab Data Protection for Microsoft Hyper-V Version 8.1.2 können Sie mehr virtuelle Maschinen (VMs) parallel und über mehrere Knoten in einem Cluster hinweg sichern. Bei einer Sicherungsoperation für einen Clusterknoten wird der Momentaufnahmeversuch bei Datenträgern mit Momentaufnahmen, die mit einer wiederherstellbaren Bedingung fehlschlagen sind, immer wiederholt. Sie können auch die Anzahl der VMs in einer Momentaufnahme optimieren, um die Workload einer Momentaufnahme für den Hyper-V-Host zu reduzieren.

Sie können die folgenden Optionen verwenden, um die Erstellung von Momentaufnahmen während der Sicherung zu optimieren:

- Mit der Option `vmmaxparallel` können Sie steuern, wie viele VMs parallel an den IBM Spectrum Protect-Server gesendet werden. Die Einstellung für diese Option wirkt sich sehr stark auf die Leistung aus.
- Mit der Option `vmmaxpersnapshot` können Sie steuern, wie viele VMs in jede der Momentaufnahmen eingeschlossen werden können, die während der Sicherungsoperation erstellt werden.

Überprüfen und optimieren Sie die Werte für diese beiden Optionen für die Umgebung, bevor Sie einen Cluster sichern.

Verwenden Sie den folgenden allgemeinen Ansatz für die Optimierung Ihrer Clustersicherungsoperationen:

1. Planen Sie die Verwendung eines IBM Spectrum Protect-Servers mit geeigneter Kapazität und Konfiguration, der Container-Pools nutzt. Informationen zur Ermittlung der geeigneten Serverkapazität finden Sie in IBM Spectrum Protect Blueprints.
2. Beginnen Sie mit den Standardwerten für die Optionen `vmmaxpersnapshot` und `vmmaxparallel`.
3. Führen Sie den Sicherungszeitplan aus und notieren Sie die Ergebnisse. Notieren Sie beispielsweise, ob die Sicherungen innerhalb des Zeitplanfensters abgeschlossen wurden oder ob zu viele Momentaufnahmewiederholungen aufgetreten sind.
4. Passen Sie den Wert für die Option `vmmaxparallel` an Ihre Umgebung an. Setzen Sie den Wert beispielsweise auf 10.
5. Setzen Sie den Wert für `vmmaxpersnapshot` auf einen Wert, mit dem die Anzahl der Wiederholungsversuche minimiert wird. Die Wiederholungsversuche werden in den Statistikdaten für die Sicherung aufgelistet.

   Wenn Sie die Anzahl der VMs pro Momentaufnahme verringern, erhöht sich die Anzahl der Momentaufnahmen, die für die Ausführung einer Sicherungsoperation erforderlich sind. Diese größere Anzahl der Momentaufnahmen kann bei Clustersicherungsoperationen von VMs auf CSVs zu Verzögerungen führen. Die Verzögerung tritt auf, weil nicht mehrere Momentaufnahmen gleichzeitig erstellt werden können und die Sicherungsoperationen anderer Knoten in dem Zeitplan sich während der Momentaufnahmeerstellung verzögern. Wenn Sie die Anzahl der VMs in einer Momentaufnahme erhöhen, verringert sich die Anzahl der Momentaufnahmen, die für eine Sicherungsoperation erstellt werden.

   Beachten Sie die folgenden Faktoren, wenn Sie die Anzahl der VMs festlegen, die in eine Momentaufnahme eingeschlossen werden sollen:

- Die Erstellung einer Momentaufnahme mit mehr VMs dauert länger und erhöht die Systembelastung. Eine größere Anzahl an VMs bedeutet, dass die Momentaufnahme länger bestehen bleibt. Dies kann die Systemleistung beeinträchtigen.
- Die Kombination der Optionen `vmmaxpersnapshot` und `vmmaxparallel` legt fest, wie viele Momentaufnahmen bei einer Sicherungsoperation erstellt werden. Die Option `vmmaxparallel` gibt an, wie viele VMs gleichzeitig gesichert werden können. Data Protection for Microsoft Hyper-V erstellt die Anzahl an Momentaufnahmen, die für die Einhaltung der Einstellung für `vmmaxparallel` erforderlich sind.

  Die VMs werden auf der Basis der Datenträger sortiert und ausgewählt, die für die Erstellung der Momentaufnahme für die VMs benötigt werden. Eine Momentaufnahme wird für eine Gruppe von VMs erstellt, die eine Gruppe von Datenträgern gemeinsam nutzen. Daher variiert die Anzahl der Momentaufnahmen je nach den Datenträgern, die von den VMs verwendet werden. Die Anzahl der VMs pro Momentaufnahme überschreitet niemals den Wert für die Option `vmmaxpersnapshot`.

  Die folgende Tabelle enthält Beispiele für die Anzahl der VMs, die mit verschiedenen Einstellungen für `vmmaxpersnapshot` und `vmmaxparallel` pro Momentaufnahme verarbeitet werden können. In diesen Beispielen wird vorausgesetzt, dass alle VMs sich auf demselben Datenträger befinden.

Tabelle 7. Anzahl der Momentaufnahmen und VMs (auf demselben Datenträger), die mit den Einstellungen für `vmmaxpersnapshot` und `vmmaxparallel` verarbeitet werden

Einstellung für `vmmaxpersnapshot`	**Einstellung für `vmmaxparallel`**	**Anzahl der erstellten Momentaufnahmen**
10	20	Es werden zwei Momentaufnahmen mit jeweils 10 VMs erstellt. Wenn die Anzahl der VMs, die verarbeitet werden, kleiner als die Einstellung für `vmmaxparallel` ist, wird eine weitere Momentaufnahme erstellt.
20	20	Es wird eine Momentaufnahme erstellt, die 20 VMs enthält.
20	10	Es wird eine Momentaufnahme erstellt, die 20 VMs enthält, und aufgrund der Einstellung für `vmmaxparallel` werden 10 VMs bei der ersten Ausführung gesichert. Die übrigen 10 VMs werden bei der zweiten Ausführung gesichert. (Eine zweite Momentaufnahme ist nicht erforderlich.)

Sie können auch mit der Option `vmmaxsnapshotretry` die maximale Anzahl der Wiederholungen einer Momentaufnahmeoperation für eine VM angeben, wenn die anfängliche Momentaufnahme mit einer wiederherstellbaren Bedingung fehlschlägt.

Zugehörige Konzepte:

„Einschränkungen bei Hyper-V-Sicherungsoperationen" auf Seite 12

Zugehörige Verweise:

„`Vmmaxpersnapshot`" auf Seite 210

„`Vmmaxsnapshotretry`" auf Seite 212

„`Vmmaxparallel`" auf Seite 209

Kapitel 4. Daten mit der Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwalten

Die Data Protection for Microsoft Hyper-V-Verwaltungskonsole stellt eine einzige Umgebung zur Verfügung, die Ihnen hilft, die täglichen Data Protection for Microsoft Hyper-V-Operationen zu verwalten.

Mit der Data Protection for Microsoft Hyper-V-Verwaltungskonsole können Sie Adhoc-Sicherungs- und Zurückschreibungsoperationen starten und aktuelle Sicherungsinformationen für alle virtuellen Maschinen (VMs) anzeigen, die sich auf einem Hyper-V-Host oder in einem Cluster befinden.

Diese Informationen umfassen die Kennzeichnung von VMs, bei denen die Gefahr besteht, dass sie ungeschützt sind, weil die VM noch nie gesichert wurde oder weil eine Sicherung nicht in dem Zeitintervall ausgeführt wurde, das in der Maßnahme bei Gefährdung festgelegt ist. Die Maßnahme bei Gefährdung gilt nur für VMs, die zuvor gesichert wurden.

Tipp: Sie können auch den Konfigurationsassistenten verwenden, um die Konfiguration von Data Protection for Microsoft Hyper-V zu erstellen oder zu aktualisieren. Weitere Informationen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.

Data Protection for Microsoft Hyper-V-Verwaltungskonsole starten

Zur Verwaltung der Routineoperationen für Data Protection for Microsoft Hyper-V starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole und geben Sie Ihre Anmeldeberechtigungsnachweise ein.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole, indem Sie auf **Start** > **IBM Spectrum Protect** > **DP for Hyper-V-Verwaltungskonsole** klicken.

   Geben Sie alternativ den folgenden Befehl bei der Eingabeaufforderung aus:

   ```
   "C:\Programme\IBM\SpectrumProtect\DPHyperV\DpHv.msc"
   ```

2. Bei der Aufforderung melden Sie sich bei der Data Protection for Microsoft Hyper-V-Verwaltungskonsole an. Geben Sie die Berechtigungsnachweise ein, mit denen Sie sich auch bei dem Hyper-V-Host anmelden.

   Das Konto, das Sie verwenden, muss der lokalen Administratorgruppe auf dem Computer angehören, damit Hyper-V- und Clusteroperationen ausgeführt werden können.

   Tipp: Wenn Sie Data Protection for Microsoft Hyper-V noch nicht konfiguriert haben oder wenn die Konfiguration unvollständig ist, wird automatisch der Konfigurationsassistent angezeigt. Weitere Informationen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.

3. Wird das Sicherheitszertifikat des Hosts, zu dem Sie eine Verbindung herstellen, nicht erkannt oder befindet es sich nicht auf dem Server, auf dem die Data Protection for Microsoft Hyper-V-Verwaltungskonsole installiert ist, werden Sie aufgefordert, ein neues Zertifikat zu installieren.

Führen Sie die folgenden Schritte für einen eigenständigen Host oder für jeden Host in einem Cluster aus:

a. Im Fenster **Verbindung zu <Hostname> wird geschützt** klicken Sie auf **Zertifikat anzeigen**.

   Wenn Sie eine der anderen Optionen auswählen - z. B. **Ja**, um die Zertifikatswarnung für die aktuelle Sitzung zu ignorieren, **Nein**, um die Verbindung zu stoppen, oder **Bei Verbindungen zu diesem Computer nicht mehr fragen**, um alle zukünftigen Zertifikatswarnungen zu ignorieren - können Sie keine Verbindung zu Data Protection for Microsoft Hyper-V herstellen.

b. Klicken Sie auf der Registerkarte **Allgemein** des Fensters **Zertifikat** auf **Zertifikat installieren**.

c. Wählen Sie auf der Begrüßungsseite des Fensters **Zertifikatimport-Assistent** eine Speicherposition aus (**Aktueller Benutzer** oder **Lokale Maschine**) und klicken Sie auf **Weiter**.

d. Auf der Seite **Zertifikatspeicher** klicken Sie auf **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie auf **Durchsuchen**.

e. Wählen Sie im Fenster **Zertifikatspeicher auswählen** die Option **Vertrauenswürdige Stammzertifizierungsstellen** aus und klicken Sie auf **OK**.

f. Klicken Sie auf der Seite **Zertifikatspeicher** auf **Weiter**.

g. Überprüfen Sie die ausgewählten Einträge auf der Seite **Fertigstellen des Assistenten** und klicken Sie auf **Fertigstellen**.

h. Klicken Sie im Fenster mit der **Sicherheitswarnung** auf **Ja**, um das Zertifikat zu installieren.

i. Klicken Sie im Bestätigungsfenster auf **OK**.

Wenn Sie das Zertifikat ablehnen, können Sie keine Verbindung zu Data Protection for Microsoft Hyper-V herstellen.

Nächste Schritte

Sie können die Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwenden, um Ihre Sicherungen virtueller Maschinen zu verwalten und deren Status zu überwachen.

Nach einem Inaktivitätszeitraum kann eine Zeitlimitüberschreitung bei Ihrer Verbindung zu der Data Protection for Microsoft Hyper-V-Verwaltungskonsole auftreten. Wenn eine Zeitlimitüberschreitung auftritt, werden Sie aufgefordert, Ihre Berechtigungsnachweise in das Fenster **Verbindung wiederherstellen - Sitzung ist abgelaufen** einzugeben.

Tipp für die Ausführung in einer angepassten Konsole: Sie können die Data Protection for Microsoft Hyper-V-Verwaltungskonsole einer angepassten Microsoft Management Console hinzufügen, sodass sie beispielsweise zusammen mit dem Hyper-V-Manager und dem Failovercluster-Manager in einer einzigen Konsole ausgeführt werden kann.

1. Starten Sie eine leere Microsoft Management Console, indem Sie den Befehl **mmc** bei einer Eingabeaufforderung ausgeben.
2. Klicken Sie auf **Datei** > **Snap-In hinzufügen/entfernen**.
3. Wählen Sie **Data Protection for Microsoft Hyper-V** aus und klicken Sie auf **Hinzufügen**.
4. Wählen Sie weitere Snap-ins aus und fügen Sie sie hinzu, z. B. den **Hyper-V-Manager** und den **Failovercluster-Manager**.

5. Klicken Sie auf **Datei** > **Speichern unter**, um der `.msc`-Datei einen Namen zuzuordnen und sie zu speichern.
6. Zum Starten der angepassten Konsole führen Sie die `.msc`-Datei aus, die Sie gespeichert haben.

In der Data Protection for Microsoft Hyper-V-Verwaltungskonsole navigieren

Verwenden Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole für das Routinemanagement von Sicherungsoperationen. Sie können Sicherungsoperationen für virtuelle Maschinen überwachen, Sicherungs- und Zurückschreibungsoperationen ausführen und die Konfiguration aktualisieren.

Die Data Protection for Microsoft Hyper-V-Verwaltungskonsole enthält drei Hauptarbeitsbereiche: das Navigationsfenster, das Ergebnisfenster und das Aktionsfenster. Informationen zu diesen Arbeitsbereichen wird bereitgestellt.

Navigationsfenster

Das Navigationsfenster auf der linken Seite ist mit **Data Protection for Hyper-V** bezeichnet und enthält eine Baumstruktursicht, die die Cluster oder Hosts in der Hyper-V-Umgebung anzeigt. In der Clustersicht stellen die untergeordneten Knoten des Clusterknotens die Hosts in dem Cluster dar.

Wenn Sie im Navigationsfenster einen Host oder Cluster auswählen, werden der Sicherungsstatus der virtuellen Maschinen (VMs) auf dem ausgewählten Host bzw. in dem ausgewählten Cluster und das Protokoll der Zeitplanausführungen in den Sichten **Virtuelle Maschinen** und **Zeitplanprotokoll** im Ergebnisfenster angezeigt. Außerdem wird die Liste der verfügbaren Aktion für den ausgewählten Cluster oder Host bzw. die ausgewählte VM im Aktionsfenster rechts in der Verwaltungskonsole angezeigt.

Ergebnisfenster

Im Ergebnisfenster, das sich in der Mitte der Data Protection for Microsoft Hyper-V-Verwaltungskonsole befindet, werden ausführliche Informationen zu den Sicherungen virtueller Maschinen und zum Sicherungszeitplanprotokoll für einen ausgewählten Cluster oder Host angezeigt.

Der Arbeitsbereich enthält zwei Sichten, die mit **Virtuelle Maschinen** und **Zeitplanprotokoll** bezeichnet sind. Klicken Sie auf die entsprechende Registerkarte im Ergebnisfenster, um die jeweilige Sicht anzuzeigen.

Sicht 'Virtuelle Maschinen'

In der Sicht **Virtuelle Maschinen** im Ergebnisfenster werden der Datenschutzstatus jeder virtuellen Maschine (VM) in einem Cluster oder auf einem Host und das Sicherungsprotokoll für die einzelnen VMs angezeigt.

Sie können einen VM-Namen oder einen Teil eines VM-Namens in das Filterfeld eingeben, um nur VMs anzuzeigen, deren Name diese Textzeichenfolge enthält. Sie können auch auf **Aktualisieren** klicken, um den Inhalt in den Tabellen zu aktualisieren.

VM-Tabelle

Oben in der Sicht 'Virtuelle Maschinen' werden die Tabelle der VMs auf einem Host oder in einem Cluster sowie Details zur letzten Sicherungsoperation für jede VM angezeigt. Die folgenden Daten werden in der Tabelle angezeigt.

Tabelle 8. Beschreibung der Spalten in der VM-Tabelle

Spalte	Beschreibung
Name	Der Name der VM.
Host	Wenn ein Cluster im Navigationsfenster ausgewählt ist, der Name des aktuellen aktiven Hosts für die VM. Auch wenn der VM-Status **Gelöscht** lautet, wird der Hostname angezeigt. Wurde für die Umgebung jedoch ein Upgrade von Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher durchgeführt, ist das Feld leer, bis VM-Sicherungen mit Version 8.1.6 ausgeführt werden.
Status	Der Datenschutzstatus der VM. Eine VM kann einen der folgenden Status haben: **Gefährdet** Die letzte Sicherungsoperation wurde nicht innerhalb des Zeitlimits ausgeführt, das durch die Maßnahme bei Gefährdung angegeben ist. **Keine Sicherung** Die VM ist für Sicherungsoperationen konfiguriert; es wurde jedoch noch keine Sicherung ausgeführt. **Normal** Eine Sicherungsoperation wurde innerhalb des Zeitlimits ausgeführt, das durch die Maßnahme bei Gefährdung angegeben ist. **Ignoriert** Die Maßnahme bei Gefährdung ist so definiert, dass Warnungen bei Gefährdung für die VM unterdrückt werden. **Gelöscht** Die VM wurde aus der Hyper-V-Umgebung gelöscht; ihre Sicherung ist jedoch für die Zurückschreibung verfügbar.
Letzte Sicherung	Das Datum der letzten erfolgreichen Sicherungsoperation.
Übertragene Daten	Das Volumen der Daten, die während der Sicherungsoperation an den IBM Spectrum Protect-Server gesendet wurden.
Dauer	Die Länge der Zeit, die die Ausführung der Sicherungsoperation in Anspruch genommen hat.

Tabelle 8. Beschreibung der Spalten in der VM-Tabelle (Forts.)

Spalte	Beschreibung
Sicherungstyp	Der Typ der Sicherungsoperation, die ausgeführt wurde (vollständig oder inkrementell).
Zeitplan	Der Name des Zeitplans, der bei der letzten erfolgreichen Sicherungsoperation ausgeführt wurde.

Tabelle 'Sicherungsprotokoll'

In der Tabelle **Sicherungsprotokoll** werden die Details zu vorherigen geplanten oder Ad-hoc-Sicherungstasks für eine einzelne virtuelle Maschine (VM) angezeigt, die Sie in der VM-Tabelle ausgewählt haben. Wenn Sie mehrere VMs ausgewählt haben, werden keine Daten in der Tabelle **Sicherungsprotokoll** angezeigt.

Die Anzahl der Sicherungstasks, die in der Tabelle **Sicherungsprotokoll** angezeigt werden, ist von der Anzahl der Tage abhängig, die durch den Befehl **SET EVENTRETENTION** auf dem IBM Spectrum Protect-Server definiert wurden.

Die folgenden Daten werden in der Tabelle angezeigt.

Tabelle 9. Beschreibung der Spalten in der Tabelle **Sicherungsprotokoll**

Spalte	Beschreibung
Letzte Ausführungszeit	Der tatsächliche Startzeitpunkt (Datum und Zeit) der letzten Sicherungsausführung.
Status	Der Status der Sicherungsoperation. **Erfolgreich** Die Sicherungsoperation wurde erfolgreich ausgeführt. **Fehlgeschlagen** Bei der Sicherungsoperation ist ein Fehler aufgetreten und sie wurde nicht ausgeführt. **In Bearbeitung** Eine Sicherungsoperation ist in Bearbeitung.
Dauer	Die Dauer der Sicherungsoperation.
Fehlercode	Wenn die Sicherungsoperation fehlgeschlagen ist, wird ein Fehlercode angezeigt. Wenn die Sicherungsoperation erfolgreich ausgeführt wurde, wird eine Null (0) angezeigt.
Übertragene Daten	Das Volumen der Daten, die während der Sicherungsoperation an den IBM Spectrum Protect-Server gesendet wurden.

Tabelle 9. Beschreibung der Spalten in der Tabelle **Sicherungsprotokoll** *(Forts.)*

Spalte	Beschreibung
Sicherungstyp	Der Typ der Sicherungsoperation, die für die VM ausgeführt wurde: **Inkrementell** Sichert die Blöcke, die sich seit der letzten (vollständigen oder inkrementellen) Sicherung geändert haben. **Vollständig** Sichert eine Momentaufnahme der gesamten VM.
Sicherungshost	Der Host, auf dem sich die Einheit zum Versetzen von Daten für die VM befand, als sie gesichert wurde. Für Cluster kann dieser Host der Einheit zum Versetzen von Daten sich durch Failover-Clustering ändern.

Tabelle 'Tasks'

In der Tabelle **Tasks** wird eine Liste der letzten Tasks angezeigt, die seit dem Start der Data Protection for Microsoft Hyper-V-Verwaltungskonsole gestartet wurden.

Weitere Informationen finden Sie in „Tabelle 'Tasks'“ auf Seite 83.

Sicht 'Zeitplanprotokoll'

In der Sicht **Zeitplanprotokoll** im Ergebnisfenster wird das Ausführungsprotokoll für die Sicherungszeitpläne angezeigt, die einem Hyper-V-Host oder Cluster zugeordnet sind.

Sie können auf **Aktualisieren** klicken, um den Inhalt in den Tabellen zu aktualisieren.

Tabelle 'Zeitplanprotokoll'

In der Tabelle 'Zeitplanprotokoll' wird das Protokoll der Sicherungszeitpläne für den Host oder Cluster angezeigt.

Die Anzahl der aufgelisteten Sicherungsprotokolleinträge ist von der Anzahl der Tage abhängig, die durch den Befehl **SET EVENTRETENTION** auf dem IBM Spectrum Protect-Server definiert sind.

Die folgenden Daten werden in der Tabelle 'Zeitplanprotokoll' angezeigt.

Tabelle 10. Beschreibung der Spalten in der Tabelle 'Zeitplanprotokoll'

Spalte	Beschreibung
Startzeit des Zeitplans	Der tatsächliche Zeitpunkt (Datum und Zeit), an dem der Zeitplan gestartet wurde. Wurde ein Zeitplan versäumt, wird die geplante Startzeit angezeigt.
Name	Der Name des Zeitplans.

Tabelle 10. Beschreibung der Spalten in der Tabelle 'Zeitplanprotokoll' (Forts.)

Spalte	Beschreibung
Status	Der Status des Zeitplans basiert auf allen Einheiten zum Versetzen von Daten, die dem Zeitplan zugeordnet sind. Die folgenden Status sind möglich: **Erfolgreich** Der Zeitplan wurde für alle Einheiten zum Versetzen von Daten vollständig ausgeführt. Die Details zu den einzelnen VMs, die gesichert oder nicht gesichert wurden, werden in der zweiten Tabelle angezeigt. **Fehlgeschlagen** Der Zeitplan wurde auf mindestens einer Einheit zum Versetzen von Daten nicht vollständig ausgeführt. **In Bearbeitung** Der Zeitplan wurde auf allen Einheiten zum Versetzen von Daten gestartet und die Ausführung ist noch nicht abgeschlossen. **Versäumt** Der Start des Zeitplans ist auf mindestens einer Einheit zum Versetzen von Daten innerhalb des Startfensters fehlgeschlagen.
VM erfolgreich	Die Anzahl der VMs, die bei der Zeitplanausführung erfolgreich gesichert wurden.
VM-Fehler	Die Anzahl der VMs, deren Sicherung bei der Zeitplanausführung fehlgeschlagen ist. Wenn der Zeitplan versäumt wurde oder fehlgeschlagen ist, wird ein Strich angezeigt.
Dauer	Die Länge der Zeit, die die Zeitplanausführung in Anspruch genommen hat. Die Dauer wird vom Start der ersten Zeitplanaktivität bis zum Ende der letzten Zeitplanaktivität gemessen. Wenn der Zeitplan versäumt wurde oder fehlgeschlagen ist, wird ein Strich angezeigt.

Tabelle 'Zeitplandetail'

Wenn Sie einen Zeitplaneintrag in der Tabelle 'Zeitplanprotokoll' auswählen, wird in der Tabelle **Zeitplandetail** die Liste der virtuellen Maschinen (VMs) angezeigt, die bei der ausgewählten Zeitplanausführung gesichert wurden.

Wenn einem Zeitplan mehrere Knoten zugeordnet sind, spiegelt die angezeigte Anzahl der virtuellen Maschinen (VMs) die Informationen von allen Knoten der Einheit zum Versetzen von Daten für diese Zeitplanausführung wider.

Sie können einen VM-Namen oder einen Teil eines VM-Namens in das Filterfeld eingeben, um nur VMs anzuzeigen, deren Name diese Textzeichenfolge enthält.

Die folgenden Daten werden in der Tabelle angezeigt.

Tabelle 11. Beschreibung der Spalten in der Tabelle **Zeitplandetail**

Spalte	Beschreibung
Name	Der Name der VM.
Status	Der Sicherungsstatus der VM. **Erfolgreich** Die VM wurde erfolgreich gesichert. **Fehlgeschlagen** Die Sicherung der VM ist fehlgeschlagen.
Startzeit	Der Zeitpunkt (Datum und Zeit), an dem die VM-Sicherungsoperation gestartet wurde.
Ursache	Wenn die VM-Sicherung fehlgeschlagen ist, wird ein Fehlercode bereitgestellt. Wenn die Sicherungsoperation erfolgreich war, wird eine Null (0) angezeigt.
Dauer	Die Dauer der Sicherungsoperation.
Übertragene Daten	Das Volumen der Daten, die während der Sicherungsoperation an den IBM Spectrum Protect-Server gesendet wurden.
Sicherungstyp	Der Typ der Sicherungsoperation, die für die VM ausgeführt wurde: **Inkrementell** Sichert die Blöcke, die sich seit der letzten (vollständigen oder inkrementellen) Sicherung geändert haben. **Vollständig** Sichert eine Momentaufnahme der gesamten VM.
Sicherungshost	Der Host, auf dem sich die Einheit zum Versetzen von Daten befindet, die zum Ausführen der VM-Sicherungsoperation verwendet wird. Für Cluster kann dieser Host der Einheit zum Versetzen von Daten sich durch Failover-Clustering ändern.

Tabelle 'Tasks'

In der Tabelle **Tasks** wird eine Liste der letzten Tasks angezeigt, die seit dem Start der Data Protection for Microsoft Hyper-V-Verwaltungskonsole gestartet wurden.

Weitere Informationen finden Sie in „Tabelle 'Tasks'" auf Seite 83.

Tabelle 'Tasks'

In der Tabelle **Tasks** wird die Liste der kürzlich ausgeführten Sicherungs- oder Zurückschreibungstasks angezeigt, die gestartet wurden, seit Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole gestartet haben.

In der Sicht **Virtuelle Maschinen** und in der Sicht **Zeitplanprotokoll** wird dieselbe Liste von Tasks angezeigt. Sie können Tasks mit langer Laufzeit, z. B. Sicherungs- oder Zurückschreibungsoperationen, überwachen.

Sie können außerdem die folgenden Aktionen ausführen:

Stoppen
Eine aktive Task abbrechen.

Kopieren
Die Ergebnisse der ausgewählten Tasks in die Zwischenablage kopieren.

Beendete entfernen
Alle beendeten Tasks aus der Tabelle entfernen. Aktive Tasks werden nicht entfernt.

Die folgenden Daten werden in der Tabelle **Tasks** angezeigt.

Tabelle 12. Beschreibung der Spalten in der Tabelle **Tasks**

Spalte	Beschreibung
Host	Der Host, auf dem die Task ausgeführt wird.
Task	Der Typ der Task, die ausgeführt wird (**Sichern** oder **Zurückschreiben**).
Status	Der Status der Task (**Aktiv**, **Erfolgreich** oder **Fehlgeschlagen**).
Startzeit	Der Startzeitpunkt (Datum und Zeit) der Task.
Dauer	Die Länge der Zeit, die die Ausführung der Task in Anspruch genommen hat, oder die Länge der Zeit, während der die Task aktiv ist.
Nachrichten	Wenn die Task fehlgeschlagen ist, werden die zugehörigen Fehlernachrichten angezeigt. Wenn die Task erfolgreich ausgeführt wurde, werden keine Nachrichten angezeigt. In dem Nachrichtenfeld werden auch Statusnachrichten für eine Task angezeigt, die in Bearbeitung ist.

Aktionsfenster

Im Fenster **Aktionen** auf der rechten Seite der Data Protection for Microsoft Hyper-V-Verwaltungskonsole wird die Liste der verfügbaren Aktionen für das im Navigationsfenster ausgewählte Element und die im Ergebnisfenster ausgewählten VMs angezeigt.

Das Aktionsfenster enthält einen Abschnitt für einen Host oder Cluster und einen Abschnitt für eine VM.

Auf der Host- oder Clusterebene anwendbare Aktionen

Abmelden
Sich bei Data Protection for Microsoft Hyper-V abmelden.

Verbindung herstellen
Sich bei Data Protection for Microsoft Hyper-V anmelden.

Sicherungsmanagement
Einem einzelnen Hyper-V-Host oder einer Clusterumgebung einen Sicherungszeitplan zuordnen.

Konfigurieren
Den Konfigurationsassistenten öffnen, um die Konfiguration von Data Protection for Microsoft Hyper-V zu aktualisieren.

Eigenschaften
Die aktuelle Konfiguration für Data Protection for Microsoft Hyper-V anzeigen. Klicken Sie auf **Konfigurieren**, um die Konfiguration zu aktualisieren.

Anzeigen > Anpassen
Die Informationen anpassen, die in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole angezeigt werden.

Aktualisieren
Den Inhalt in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole aktualisieren.

Hilfe Die Onlinehilfe für die Data Protection for Microsoft Hyper-V-Verwaltungskonsole öffnen.

Auf der VM-Ebene anwendbare Aktionen

Sichern
Eine VM oder mehrere VMs sichern.

Zurückschreiben
Eine einzelne VM mit dem Assistenten **Zurückschreiben** zurückschreiben.

Dateizurückschreibung
Die Schnittstelle für Dateizurückschreibung in einem Web-Browser öffnen. Nur verfügbar, wenn Sie das Feature für Dateizurückschreibung aktiviert haben.

Als gefährdet definieren
Die Maßnahme bei Gefährdung für eine VM oder mehrere VMs definieren.

Hilfe Die Onlinehilfe für die Data Protection for Microsoft Hyper-V-Verwaltungskonsole öffnen.

Konfiguration von Data Protection for Microsoft Hyper-V überprüfen

Nachdem Sie den Konfigurationsassistenten ausgeführt haben, können Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwenden, um die Konfiguration der während des Konfigurationsprozesses erstellten Knoten zu überprüfen. Durch Überprüfen der Knotenkonfiguration können Sie dazu beitragen, potenzielle Probleme bei Systemoperationen zu vermeiden.

Informationen zu diesem Vorgang

Wenn Sie die Konfiguration der Knoten überprüfen, werden die folgenden Typen von Informationen angezeigt:

- Informationen zum Knoten der Einheit zum Versetzen von Daten wie der Hostname, das Betriebssystem und die Position des Fehlerprotokolls
- Wenn das Feature für Dateizurückschreibung aktiviert ist: Informationen zu den Mount-Proxy-Knoten wie der Hostname, das Betriebssystem, die Position des Fehlerprotokolls, der Status von Recovery Agent und der iSCSI-Status der Mount-Proxy-Knoten

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
2. Wählen Sie im Navigationsfenster einen Cluster oder Host aus.
3. Klicken Sie im Fenster **Aktionen** auf **Eigenschaften**.
4. Wählen Sie im Fenster **Eigenschaften** die Seite **Knoten überprüfen** aus, um die Knoteninformationen anzuzeigen.

   Die Daten, die auf der Seite **Allgemein** und auf der Seite **Knoten überprüfen** angezeigt werden, sind von dem Knoten abhängig, den Sie im Navigationsfenster ausgewählt haben. Wenn Sie einen Clusterknoten ausgewählt haben, werden Informationen zu allen gültigen Knoten im Cluster angezeigt. Wenn Sie einen Host ausgewählt haben, werden nur die Daten angezeigt, die zu dem Host gehören.
5. Wählen Sie einen Knoten, den Sie überprüfen möchten, im Feld **Knoteninformationen** aus und klicken Sie auf **Knoten überprüfen**.

   Tipp: Wenn Sie einen Linux-Mount-Proxy-Knoten ausgewählt haben, ist die Schaltfläche **Knoten überprüfen** inaktiviert. Zum Anzeigen von Linux-Mount-Proxy-Informationen wählen Sie den Windows-Mount-Proxy-Knoten (normalerweise der nächste Eintrag in der Liste) aus und klicken Sie auf **Knoten überprüfen**. Wählen Sie anschließend erneut den Linux-Mount-Proxy-Knoten im Feld **Knoteninformationen** aus, um die Linux-Mount-Proxy-Informationen im Feld **Statusdetails** anzuzeigen.
6. Überprüfen Sie die Ergebnisse im Feld **Statusdetails** und beheben Sie alle Probleme, die bei der Überprüfung festgestellt werden.

   Tipp: Sie können die Ergebnisse in der Zwischenablage speichern, indem Sie den Inhalt im Feld **Statusdetails** hervorheben und die Tastenkombination **Strg+C** drücken. Anschließend können Sie den Inhalt in ein Textdokument einfügen und dieses für Referenzzwecke speichern.
7. Zum Schließen des Fensters **Eigenschaften** klicken Sie auf **Schließen**.

Nächste Schritte

Nachdem Sie alle Konfigurationsprobleme behoben haben, können Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole erneut starten und die Konfiguration erneut überprüfen.

Tipp: Sie können die Konfiguration auch mit dem PowerShell-Cmdlet **Test-DpHvConfiguration** überprüfen. Weitere Informationen finden Sie in „Beispiele für Data Protection for Microsoft Hyper-V-Cmdlets" auf Seite 157.

Sicherungszeitpläne für einen Host oder eine Clustermaschine verwalten

Sie können einen Zeitplan auswählen, um anzugeben, wie oft und wann virtuelle Maschinen (VMs) auf einem Hyper-V-Host oder in einem Cluster automatisch gesichert werden sollen.

Informationen zu diesem Vorgang

Zeitpläne werden vom IBM Spectrum Protect-Serveradministrator definiert, um VMs automatisch zu sichern.

Damit Zeitpläne für Data Protection for Microsoft Hyper-V verwendet werden können, muss der IBM Spectrum Protect-Serveradministrator eine Liste von Zeitplänen speziell für die Sicherung von Hyper-V-VMs definieren. Die Zeitplandefinition muss die folgenden Parameter und Optionen beinhalten:

- In der Optionszeichenfolge muss die Option `-domain.vmfull="all-vm"` angegeben werden. Für die Option `-domain.vmfull` sind keine weiteren Parameter erforderlich.
- Der Zeitplan muss die Parameter ACTION=BACKUP und SUBACTION=VM enthalten.

Beispiel: Der Administrator definiert einen Zeitplan mit dem folgenden Serverbefehl **DEFINE SCHEDULE**:

```
define schedule Name_der_Hyper-V-Domäne Zeitplanname
description=Zeitplanbeschreibung action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=hypervfull
-mode=IFIncremental -domain.vmfull="all-vm"'
```

Der Hyper-V-Administrator ordnet dem Zeitplan anschließend eine Einheit zum Versetzen von Daten zu. Dazu verwendet er das Fenster **Sicherungsmanagement**. Die Option `-asnodename=` wird der Zeitplandefinition automatisch hinzugefügt. Beispiel: Für einen eigenständigen Host wird die folgende Option hinzugefügt:

```
-asnodename=Hyper-V-Host_HV_TGT
```

Für eine Clusterumgebung wird die folgende Option hinzugefügt:

```
-asnodename=Clustername_hv_tgt
```

Je nach der Systemkonfiguration kann der Knotenname auch ein Präfix und ein Suffix enthalten. Weitere Informationen finden Sie in „Knotennamen anpassen" auf Seite 23.

Tipp: Der Serveradministrator kann auch das IBM Spectrum Protect Operations Center verwenden, um den Hyper-V-Zeitplan zu definieren.

Wenn einige VMs ausgeschlossen werden müssen, geben Sie den Parameter `-vm` in der Optionszeichenfolge für die Option `-domain.vmfull` an. Beispiel: Zum Sichern aller VMs mit Ausnahme der VM mit dem Namen `TestVm1`, die ausgeschlossen werden soll, geben Sie die folgende Option in der Optionszeichenfolge an:

```
-domain.vmfull="all-vm;-vm=TestVm1"
```

Wenn Sie eine einzige VM bei geplanten Sicherungsoperationen einschließen müssen, geben Sie die folgende Option in der Optionszeichenfolge an:

```
-domain.vmfull="vm=TestVM1"
```

Sie definieren die Sicherungsmaßnahme für einen Host oder Cluster, indem Sie dem Host oder Cluster einen Sicherungszeitplan zuordnen. Sie können die Zeitplanzuordnung für einen Host oder Cluster auch aufheben.

In einer Clusterumgebung wird der ausgewählte Zeitplan für alle Hosts in dem Cluster angewendet. Es ist nicht möglich, den Hosts, die zu einem Cluster gehören, unterschiedliche Zeitpläne zuzuordnen.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
2. Klicken Sie im Navigationsfenster auf einen eigenständigen Host oder einen Cluster.
3. Klicken Sie im Fenster **Aktionen** auf **Sicherungsmanagement**.

   In einer Tabelle wird eine Zusammenfassung des Zeitplans angezeigt. Die folgenden Eigenschaften von Zeitplänen werden angezeigt:

   Zeitplanname
   Der Name des Zeitplans.

   Wiederholungen
   Wie oft der Zeitplan wiederholt wird.

   Hostnamen
   Eine Liste der Hosts, die den Knoten der Einheit zum Versetzen von Daten entsprechen, welche dem Zeitplan zugeordnet sind.

   Beschreibung
   Eine Beschreibung des Zeitplans.
4. Wählen Sie einen Zeitplan im Fenster **Sicherungsmanagement** aus und führen Sie eine der folgenden Aktionen aus.
   - Klicken Sie auf **Zeitplan zuordnen**, um den ausgewählten Zeitplan dem Cluster oder Host zuzuordnen und das Fenster zu aktualisieren.

     Wird ein Zeitplan einem Cluster oder Host zugeordnet, wird mit der Option `-asnodename` in der Optionszeichenfolge in der Zeitplandefinition der Zielknoten (*Hostname*_HV_TGT oder *Clustername*_HV_TGT) angegeben. Nur die relevanten Zeitpläne für diesen Zielknoten oder Zeitpläne, die keinen anderen Zielknoten zugeordnet sind, werden angezeigt.

     Der Zielknotenname kann auch ein Präfix und ein Suffix enthalten. Beispiele sind *Präfix_Hostname*_HV_TGT_*Suffix* oder *Präfix_Clustername*_HV_TGT_*Suffix*.
   - Klicken Sie auf **Zuordnung des Zeitplans aufheben**, um die ausgewählte Zeitplanzuordnung für den Cluster oder Host zu entfernen.

Wenn Sie die Zeitplanzuordnung für den Cluster oder Host entfernen, wird die Option `asnodename` aus der Optionszeichenfolge in der Zeitplandefinition entfernt und die zu dem Cluster oder Host gehörigen Knoten werden aus der Zuordnung entfernt.

5. Klicken Sie auf **Schließen**, um das Fenster zu schließen.

Maßnahme bei Gefährdung für eine virtuelle Maschine definieren

Bei virtuellen Hyper-V-Maschinen (virtuelle Maschinen = VMs) kann aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen die Gefahr bestehen, dass sie ungeschützt sind. Sie können eine Maßnahme für eine VM definieren, die angibt, ob die VM als gefährdet angezeigt wird, wenn eine Sicherungsoperation in einem angegebenen Zeitintervall nicht ausgeführt wurde.

Informationen zu diesem Vorgang

Standardmäßig verwendet jede VM die Maßnahme, die für den IBM Spectrum Protect-Server definiert wurde. Sie können für mindestens eine VM, die in der Cluster- oder Hostsicht in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole ausgewählt wurde, die Standardmaßnahme verwenden, eine angepasste Maßnahme definieren oder die Maßnahme ignorieren.

In der Spalte **Status** im Fenster **Virtuelle Maschinen** wird der Datenschutzstatus jeder VM auf dem Host oder in dem Cluster angezeigt. Die folgenden Datenschutzstatus sind möglich.

Gefährdet
Die letzte Sicherungsoperation wurde nicht innerhalb des Zeitlimits ausgeführt, das durch die Maßnahme bei Gefährdung angegeben ist.

Keine Sicherung
Die VM ist für Sicherungsoperationen konfiguriert; es wurde jedoch noch keine Sicherung ausgeführt.

Normal
Eine Sicherungsoperation wurde innerhalb des Zeitlimits ausgeführt, das durch die Maßnahme bei Gefährdung angegeben ist.

Ignoriert
Die Maßnahme bei Gefährdung ist so definiert, dass Warnungen bei Gefährdung für die VM unterdrückt werden.

Gelöscht
Die VM wurde aus der Hyper-V-Umgebung gelöscht; ihre Sicherung ist jedoch für die Zurückschreibung verfügbar.

Sie können nur VMs, die gesichert wurden, eine Maßnahme bei Gefährdung zuordnen. Wurde eine VM noch nie gesichert, ist die Aktion 'Als gefährdet definieren' inaktiviert.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die standardmäßige Maßnahme bei Gefährdung zu verwenden, für bestimmte VMs eine angepasste Maßnahme bei Gefährdung auszuwählen oder die Maßnahme bei Gefährdung für bestimmte VMs zu ignorieren:

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.

2. Klicken Sie im Navigationsfenster auf einen Host oder Cluster und klicken Sie in der VM-Tabelle auf mindestens eine VM.
3. Klicken Sie auf **Aktion** > **Als gefährdet definieren**.
4. Führen Sie im Fenster **Als gefährdet definieren** eine der folgenden Aktionen aus.

Aktion	Schritt
Standardmäßige Maßnahme bei Gefährdung verwenden	Klicken Sie auf **Standard**, um die Standarddauer von 1 Tag zu akzeptieren.
Warnungen bei Gefährdung für die VM unterdrücken	Klicken Sie auf **Ignorieren**.
Angepasste Maßnahme bei Gefährdung definieren	Klicken Sie auf **Angepasst** und verwenden Sie die Schiebeleiste, um das Zeitintervall seit der letzten Sicherung zu definieren. Der Standardwert ist 6 Stunden.

5. Klicken Sie auf **Als gefährdet definieren**, um Ihre Einstellung zu speichern.
6. Zum Schließen des Fensters klicken Sie auf **Schließen**.

Ergebnisse

Ist die Maßnahme bei Gefährdung für eine VM auf **Standard** oder **Angepasst** gesetzt, wird der Status **Gefährdet** für die VM angezeigt, wenn eine Sicherungsoperation innerhalb des von der Maßnahme definierten Zeitlimits nicht ausgeführt wurde. Wurde die VM noch nie gesichert, wird sie ebenfalls als gefährdet angesehen und der Status **Keine Sicherung** wird angezeigt.

Ist die Maßnahme bei Gefährdung für eine VM auf **Ignorieren** gesetzt, wird unabhängig vom Status der Sicherung der Risikostatus **Ignoriert** für die VM angezeigt.

Zeitplanprotokoll für einen Hyper-V-Host oder Cluster anzeigen

Sie können das Ausführungsprotokoll für die Sicherungszeitpläne anzeigen, die einem Hyper-V-Host oder Cluster zugeordnet sind. Dieses Protokoll umfasst den Zeitpunkt (Datum und Zeit), zu dem ein Zeitplan ausgeführt wurde, den Status der Zeitplanausführung und die Anzahl der virtuellen Maschinen (VMs), die erfolgreich gesichert wurden bzw. deren Sicherung fehlgeschlagen ist.

Informationen zu diesem Vorgang

Die Anzahl der Ausführungen, die für einen Zeitplan angezeigt werden, ist von der Anzahl der Tage abhängig, die durch den Befehl **SET EVENTRETENTION** auf dem IBM Spectrum Protect-Server definiert wurden.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
2. Klicken Sie im Navigationsfenster auf einen Host oder Cluster und klicken Sie auf die Registerkarte **Zeitplanprotokoll**.

   Sie können das Ausführungsprotokoll für alle Sicherungszeitpläne anzeigen, die dem Cluster oder Host zugeordnet sind. Sie können außerdem einen Zeitplan auswählen, um in der Tabelle **Zeitplandetail** den Sicherungsstatus für die VMs anzuzeigen, die diesem Zeitplan zugeordnet sind.

   Informationen dazu finden Sie in „Sicht 'Zeitplanprotokoll'" auf Seite 80.

Zugehörige Informationen:

SET EVENTRETENTION (Aufbewahrungszeitraum für Ereignissätze definieren)

Sicherungsstatus und Sicherungsprotokoll einer virtuellen Maschine anzeigen

Sie können den Status geplanter Sicherungen virtueller Maschinen (VMs) auf einem Host oder in einem Cluster anzeigen, um die VMs zu identifizieren, die möglicherweise Aufmerksamkeit erfordern. Sie können außerdem das Sicherungsprotokoll für einzelne VMs anzeigen.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
2. Klicken Sie im Navigationsfenster auf einen Host oder Cluster.
3. Klicken Sie auf die Registerkarte **Virtuelle Maschinen**.
4. In der VM-Tabelle wird der Status der letzten geplanten Sicherungsoperationen für VMs auf dem Host oder in dem Cluster angezeigt.

   Lautet der Status einer VM **Gefährdet**, gibt dies an, dass eine der letzten geplanten Sicherungen versäumt oder mit Fehlern beendet wurde.
5. Zum Anzeigen des Sicherungsprotokolls für eine VM wählen Sie die VM in der VM-Tabelle aus.

   Das Sicherungsprotokoll für diese VM wird in der Tabelle **Sicherungsprotokoll** angezeigt.

   Die Anzahl der Sicherungstasks, die in der Tabelle **Sicherungsprotokoll** angezeigt werden, ist von der Anzahl der Tage abhängig, die durch den Befehl **SET EVENTRETENTION** auf dem IBM Spectrum Protect-Server definiert wurden.

   Weitere Informationen finden Sie in „Sicht 'Virtuelle Maschinen'" auf Seite 77.

   Tipp: Wenn Sie einen Befehl der Einheit zum Versetzen von Daten (**dsmc**) verwenden, um auf Informationen zu VM-Sicherungen zuzugreifen, geben Sie die folgenden Optionen mit dem **dsmc**-Befehl an:

   - Geben Sie für Cluster die folgenden Optionen an:

     ```
     -optfile=Hostname_HV_DM.opt
     -asnodename=Clustername_HV_TGT
     ```

   - Geben Sie für einen eigenständigen Host die folgenden Optionen an:

     ```
     -optfile=Hostname_HV_DM.opt
     -asnodename=Hostname_HV_TGT
     ```

   Je nach der Systemkonfiguration kann der Knotenname auch ein Präfix und ein Suffix enthalten. In diesem Fall geben Sie die folgenden Optionen mit dem **dsmc**-Befehl an:

   - Geben Sie für Cluster die folgenden Optionen an:

     ```
     -optfile=Präfix_Hostname_HV_DM_Suffix.opt
     -asnodename=Präfix_Clustername_HV_TGT_Suffix
     ```

   - Geben Sie für einen eigenständigen Host die folgenden Optionen an:

     ```
     -optfile=Präfix_Hostname_HV_DM_Suffix.opt
     -asnodename=Präfix_Hostname_HV_TGT_Suffix
     ```

   Verwenden Sie beispielsweise die folgende Befehlssyntax, um Informationen zu VM-Sicherungen auf dem IBM Spectrum Protect-Server abzufragen:

```
dsmc query vm VM-Name -optfile=Hostname_HV_DM.opt -asnodename=Clustername_HV_TGT
```

Wenn Sie die Optionen `-asnodename` und `-optfile` nicht im Befehl **dsmc query vm** angeben, stimmt die Ausgabe des Befehls nicht mit den VM-Sicherungsergebnissen in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole überein.

Nächste Schritte

Wenn Sie eine gefährdete VM sichern möchten, ohne auf die Ausführung des Zeitplans zu warten, wählen Sie die VM aus und klicken Sie im Fenster **Aktionen** auf **Sichern**.

Zugehörige Tasks:

„Knotennamen anpassen" auf Seite 23

Zugehörige Informationen:

SET EVENTRETENTION (Aufbewahrungszeitraum für Ereignissätze definieren)

Ad-hoc-Sicherung einer virtuellen Maschine ausführen

Wenn Sie eine Ad-hoc-Sicherung einer virtuellen Maschine (VM) starten, beginnt die Sicherungsoperation sofort; es wird nicht auf die Ausführung eines Zeitplans gewartet.

Informationen zu diesem Vorgang

Normalerweise werden die VMs auf dem Hyper-V-Host oder im Cluster gesichert, wenn ein Zeitplan ausgeführt wird. Sie können jedoch eine Ad-hoc-Sicherung starten, wenn Sie feststellen, dass ein Sicherungszeitplan versäumt wurde, oder wenn eine VM-Sicherung mit Fehlern beendet wurde. Sie können außerdem eine Ad-hoc-Sicherung einer VM starten, die bei geplanten Sicherungsservices ausgeschlossen ist.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
2. Klicken Sie im Navigationsfenster auf einen Host oder Cluster.
3. Klicken Sie in der VM-Tabelle in der Sicht **Virtuelle Maschinen** auf eine VM. Klicken Sie beispielsweise auf eine VM, deren Datenschutzstatus **Gefährdet** lautet.
4. Klicken Sie im VM-Abschnitt des Fensters **Aktionen** auf **Sichern**.
5. Füllen Sie die folgenden Felder im Fenster **Ad-hoc-Sicherung** aus:

Option	Beschreibung
Sicherungstyp	Wählen Sie den Typ der auszuführenden Sicherung aus: **Inkrementell** Sichert die Blöcke, die sich seit der vorherigen (vollständigen oder inkrementellen) Sicherung geändert haben. Die letzte inkrementelle Sicherung wird an die vorhergehende Sicherung angefügt. Ist für diese virtuelle Maschine keine vollständige Sicherung vorhanden, wird automatisch eine vollständige Sicherung ausgeführt. Sie müssen daher nicht überprüfen, ob eine vollständige Sicherung vorhanden ist. **Vollständig** Sichert eine Momentaufnahme der gesamten VM. Nachdem die vollständige Sicherung ausgeführt wurde, müssen Sie keine weiteren vollständigen Sicherungen erstellen.
Datenkonsistenz	Nur für Hyper-V-Hosts oder Cluster unter Betriebssystemen Windows Server 2016 verfügbar. Wählen Sie den Typ der Momentaufnahme und die Anzahl der Wiederholungsversuche aus, die bei Sicherungsoperationen verwendet werden: **Immer anwendungskonsistent** Es werden zwei Momentaufnahmen im Quiescemodus versucht, um anwendungskonsistente Sicherungen zu erstellen, bevor die Sicherung fehlschlägt. **Anwendungskonsistenz versuchen** Es wird eine Momentaufnahme im Quiescemodus versucht. Als letzter Versuch wird eine maschinenkonsistente Momentaufnahme ohne Quiesce erstellt. **Nur maschinenkonsistent** Es wird nur eine Momentaufnahme ohne Quiesce für VMs versucht, für die niemals eine Momentaufnahme im Quiescemodus ausgeführt werden kann.
Plattenschutz	Wählen Sie die VM-Platten aus, die bei Sicherungen eingeschlossen werden sollen. Die Platten werden über die Plattennummern angegeben. Sie können alle Platten in der VM, nur Platte 1 oder alle Platten außer Platte 1 sichern. Die Platte 1 enthält normalerweise das Betriebssystem.

6. Klicken Sie auf **Sichern**, um die Sicherungsoperation zu starten und das Fenster zu schließen.

Ergebnisse

Die Sicherungsoperation, die Sie gestartet haben, wird in der Taskliste unten in der Sicht **Virtuelle Maschinen** oder in der Sicht **Zeitplanprotokoll** angezeigt.

Virtuelle Maschine zurückschreiben

Sie können eine virtuelle Maschine (VM) aus einer Sicherung zurückschreiben, die sich auf einem IBM Spectrum Protect-Server befindet.

Informationen zu diesem Vorgang

Während der Zurückschreibungsoperation wird die VM heruntergefahren und gelöscht, bevor sie aus der VM-Sicherung zurückgeschrieben wird, die auf dem IBM Spectrum Protect-Server gespeichert ist. Anschließend wird die VM von der Zurückschreibungsoperation erneut erstellt, und zwar so, dass ihr Inhalt und ihre Konfiguration mit dem Stand zum Zeitpunkt der Sicherung übereinstimmen. Obwohl die VM vor dem Löschen heruntergefahren wird, empfiehlt es sich, sie vor dem Start der Zurückschreibungsoperation manuell herunterzufahren, damit alle aktiven Anwendungsaktivitäten ordnungsgemäß abgeschlossen werden.

Sie können die Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwenden, um Daten in eine neue VM zurückzuschreiben oder die vorhandene VM durch die zurückgeschriebenen Daten zu ersetzen.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
2. Klicken Sie im Navigationsfenster in der Cluster- oder Hostsicht auf einen Host.
3. Wählen Sie in der VM-Tabelle in der Sicht **Virtuelle Maschinen** eine VM aus. Klicken Sie beispielsweise auf eine VM, deren Datenschutzstatus **Normal** lautet.

   Tipp: Wenn Sie eine gelöschte VM zurückschreiben müssen, deren Sicherung noch auf dem IBM Spectrum Protect-Server verfügbar ist, wählen Sie eine VM mit dem Status **Gelöscht** aus.
4. Klicken Sie im Fenster **Aktionen** auf **Zurückschreiben**.
5. Füllen Sie die folgenden Seiten im Assistenten **Zurückschreiben** je nach Bedarf aus. Welche Seiten bereitgestellt werden, ist von den Optionen abhängig, die Sie im Assistenten auswählen.

Assistentenseite	Aktion
Einführung	Klicken Sie auf **Weiter**, um den Assistenten zu starten.

Assistentenseite	Aktion
Zurückschreibungspunkt auswählen	Für die im Kalender hervorgehobenen Tage sind Zurückschreibungspunkte verfügbar. Zurückschreibungspunkte sind VM-Sicherungen, die für Zurückschreibungsoperationen verfügbar sind. Für einige VMs sind mehrere Zurückschreibungspunkte pro Tag vorhanden. Wählen Sie ein Datum und einen Zurückschreibungspunkt in der Liste **Verfügbare Zurückschreibungspunkte** aus. Die Größe der VM ist neben einem verfügbaren Zurückschreibungspunkt angegeben. Die VM wird mit dem Status zurückgeschrieben, den sie bei der Sicherung hatte.

Assistentenseite	Aktion
Optionen auswählen	Mit den Daten des ausgewählten Zurückschreibungspunkts können Sie eine VM erstellen oder die vorhandene VM ersetzen. Die folgenden Optionen sind verfügbar: **Neue virtuelle Maschine erstellen** Eine VM mit den Daten des ausgewählten Zurückschreibungspunkts erstellen. Diese Option ist der Standardwert. **Vorhandene virtuelle Maschine ersetzen** Die vorhandene VM durch die Daten des ausgewählten Zurückschreibungspunkts ersetzen. Die VM-IDs bleiben unverändert. **Name der virtuellen Maschine** Wenn Sie eine VM erstellen, ist der Standardname für die neue VM der ursprüngliche VM-Name, an den das Datum der Zurückschreibungsoperation angehängt wird. Wenn Sie nicht den Standardnamen verwenden möchten, geben Sie einen VM-Namen in das Eingabefeld ein, der noch nicht von einer anderen VM auf dem Hyper-V-Host oder im Cluster verwendet wird. Wenn Sie eine vorhandene VM ersetzen, wird der ursprüngliche VM-Name angezeigt. Sie können diesen Namen nicht aktualisieren. **Virtuelle Maschine zurückschreiben auf** Wenn Sie eine VM erstellen, wählen Sie einen Host aus, auf den die VM zurückgeschrieben werden kann. Wenn Sie eine vorhandene VM ersetzen, wird die VM auf den Host zurückgeschrieben, der der Eigner der VM ist. Dieses Feld ist nicht auswählbar.
Speicher auswählen	Die Seite wird nur angezeigt, wenn Sie mit den Daten aus dem Zurückschreibungspunkt eine VM erstellen. Geben Sie die Position auf dem Host ein, an der Sie die VM erstellen möchten. Die Standardposition ist `C:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines`.
Zusammenfassung	Überprüfen Sie die Optionen, die Sie im Assistenten ausgewählt haben. Klicken Sie auf **Weiter**, um die Zurückschreibungsoperation zu starten.

Assistentenseite	Aktion
Ergebnisse	Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

Ergebnisse

Die Zurückschreibungsoperation, die Sie gestartet haben, wird in der Taskliste unten in der Sicht **Virtuelle Maschinen** oder in der Sicht **Zeitplanprotokoll** angezeigt.

Wenn die Zurückschreibungsoperation beendet ist, wurde die VM an der von Ihnen ausgewählten Position zurückgeschrieben.

Nächste Schritte

Wenn Sie eine gelöschte VM zurückgeschrieben haben oder wenn Sie eine VM mit einem neuen VM-Namen zurückgeschrieben haben, müssen Sie die zurückgeschriebene VM mit Microsoft Failover Cluster Manager, mit System Center Virtual Machine Manager oder mit PowerShell-Cmdlets für Hochverfügbarkeit konfigurieren. Informationen zur Konfiguration einer VM für Hochverfügbarkeit finden Sie in der Microsoft-Dokumentation.

Bewährte Verfahren für Data Protection for Microsoft Hyper-V

Sie können bewährte Verfahren befolgen, um von den Funktionen zu profitieren, die Ihnen bei der Verwaltung von Data Protection for Microsoft Hyper-V-Operationen helfen können.

Virtuelle Maschinen bei geplanten Sicherungsoperationen ausschließen

Wenn für eine virtuelle Maschine (VM) gerade Wartungsoperationen ausgeführt werden oder es sich um eine Test-VM handelt, die nicht regelmäßig gesichert werden muss, können Sie sie bei geplanten Sicherungsoperationen ausschließen. Anstatt die Clientoptionsdatei (`dsm.opt`) auf jeder Einheit zum Versetzen von Daten zu aktualisieren, ist es möglicherweise sinnvoll, die VMs in der Zeitplandefinition auf dem IBM Spectrum Protect-Server auszuschließen.

Der IBM Spectrum Protect-Serveradministrator kann diese Task ausführen, indem er der Optionszeichenfolge in der Zeitplandefinition auf einem Server den Parameter `-vm=`*VM-Name1,VM-Name2* hinzufügt.

Beispiel: Der Administrator hat den folgenden Zeitplan auf dem IBM Spectrum Protect-Server definiert:

```
define schedule Name_der_Hyper-V-Domäne Zeitplanname
description=Zeitplanbeschreibung action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=Hyper-V-Host_hv_tgt -mode=IFIncremental
-domain.vmfull="all-vm"'
```

Soll eine VM mit dem Namen `testvm1` bei geplanten Sicherungsoperationen ausgeschlossen werden, aktualisieren Sie die Option `-domain.vmfull` in der Zeitplandefinition wie folgt:

```
define schedule Name_der_Hyper-V-Domäne Zeitplanname
description=Zeitplanbeschreibung action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=Hyper-V-Host_hv_tgt -mode=IFIncremental
-domain.vmfull="all-vm;-vm=testvm1"'
```

Soll mindestens eine VM ausgeschlossen werden, deren Name mit `testvm` beginnt, aktualisieren Sie die Option `-domain.vmfull` in der Zeitplandefinition wie folgt:

```
define schedule Name_der_Hyper-V-Domäne Zeitplanname
description=Zeitplanbeschreibung action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=Hyper-V-Host_hv_tgt -mode=IFIncremental
-domain.vmfull="all-vm;-vm=testvm*"'
```

Weitere Informationen zu der Option `-domain.vmfull` finden Sie in „Domain.vmfull" auf Seite 183.

Tipp: Je nach der Systemkonfiguration kann der Knotenname auch ein Präfix und ein Suffix enthalten. Weitere Informationen finden Sie in „Knotennamen anpassen" auf Seite 23.

Virtuelle Maschinen erneut an Verwaltungsklassen binden

Wenn Sie die Verwaltungsklasse außer Kraft setzen müssen, an die virtuelle Maschinen (VMs) durch die Option `vmmc` in der Clientoptionsdatei gebunden sind, können Sie die Option `include.vm` verwenden, um die VMs an eine neue Verwaltungsklasse zu binden.

In einer Clusterumgebung müssen Sie die Option `include.vm` in der Optionsdatei (`dsm.opt`) auf allen Hosts definieren.

Ein Beispiel: Sie möchten die VMs in Ihrer Testumgebung zwar sichern, aber die Sicherungen der Test-VMs sollen nicht so lange aufbewahrt werden wie in der Verwaltungsklasse STANDARD angegeben. In diesem Fall können Sie die Test-VMs an eine Verwaltungsklasse mit einer kürzeren Aufbewahrungsdauer für Sicherungen binden.

Fügen Sie der Clientoptionsdatei (`dsm.opt`) beispielsweise die folgende Anweisung hinzu, um alle VMs, deren Name mit `testvm` beginnt, an die Verwaltungsklasse `NONPRODMC` zu binden:

```
include.vm vmtest* NONPRODMC
```

Weitere Informationen und Beispiele zu der Option `include.vm` finden Sie in „Vmmc" auf Seite 215.

Kapitel 5. Einführung in Dateizurückschreibungsoperationen

Die Schnittstelle für Dateizurückschreibung ist verfügbar, um Dateien über eine webbasierte Schnittstelle mit minimaler Administratorunterstützung zurückzuschreiben. Nachdem das Feature für Dateizurückschreibung konfiguriert wurde, sendet der Administrator die Dateizurückschreibungs-URL an die Dateieigner oder die Help-Desk-Mitarbeiter, damit diese in der Lage sind, Dateien zu suchen und zurückzuschreiben.

In der webbasierten Schnittstelle ist keine Dateimanageranwendung für das manuelle Kopieren der Dateien erforderlich. Wenn ein Dateieigner eine Datei zurückschreibt, gibt er einen Zurückschreibungspunkt an, sucht die Datei bzw. navigiert zu der Datei und startet die Zurückschreibungsoperation.

Wenn die Konfiguration vollständig ist, wird keine Administratorinteraktion benötigt, um auf Dateien zuzugreifen oder Dateien zurückzuschreiben. Während des Konfigurationsprozesses erteilt der Administrator dem Dateieigner Zugriff auf die virtuelle Maschine (VM), die die Daten des Dateieigners enthält. Der Zugriff auf die Daten erfolgt mit lokalen VM-Berechtigungsnachweisen, sodass Administratoren die Ressourcen für die Dateizurückschreibung überwachen können. Es ist nicht erforderlich, Dateieignerberechtigungen zu verwalten.

In der Schnittstelle für Dateizurückschreibung können alle Benutzer Demovideos anzeigen, um sich mit der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung vertraut zu machen. Die Videos *Dateien suchen und zurückschreiben* und *Zurückschreibungen überwachen* werden angezeigt, wenn Benutzer sich zum ersten Mal bei der Schnittstelle für Dateizurückschreibung anmelden. Die Videos sind nur in Englisch verfügbar.

„Dateizurückschreibungstasks"

„Sich anmelden, um Dateien zurückzuschreiben" auf Seite 102

Dateizurückschreibungstasks

Verschiedene Benutzertypen richten das Feature für Dateizurückschreibung ein und verwenden es. Dateieigner, Help-Desk-Mitarbeiter und Administratoren sind für unterschiedliche Gruppen von Tasks verantwortlich.

Dateieigner

Der Dateieigner pflegt Geschäftsdaten wie Textdokumente, Arbeitsblätter und Präsentationsdateien auf virtuellen Maschinen (VMs).

Der Dateieigner führt die folgenden Tasks aus, um einzelne Dateien und Ordner zurückzuschreiben:

- „Sich anmelden, um Dateien zurückzuschreiben" auf Seite 102
- „Dateien aus einer Sicherung der virtuellen Maschine zurückschreiben" auf Seite 103

Help-Desk-Mitarbeiter

Mitarbeiter in der Help-Desk-Umgebung unterstützen Dateieigner bei der Zurückschreibung ihrer Daten.

Die Help-Desk-Mitarbeiter stellen die speziellen Dateizurückschreibungs-URLs für die Dateieigner bereit oder schreiben anstelle der Dateieigner Dateien zurück.

Die Help-Desk-Mitarbeiter führen die folgenden Tasks aus:

- Dateizurückschreibungs-URL vom Dateizurückschreibungsadministrator oder von der Data Protection for Microsoft Hyper-V-Verwaltungskonsole abrufen. Weitere Informationen finden Sie in Schritt 5 in „Umgebung für Dateizurückschreibungsoperationen aktivieren" auf Seite 52.
- „Sich anmelden, um Dateien zurückzuschreiben" auf Seite 102
- „Dateien aus einer Sicherung der virtuellen Maschine zurückschreiben" auf Seite 103

Dateizurückschreibungsadministrator

Der Administrator installiert Software, plant VM-Sicherungsoperationen auf dem IBM Spectrum Protect-Server und verwaltet Benutzerkonten und -berechtigungen in der in the Microsoft Hyper-V-Umgebung.

Der Administrator führt die folgenden Tasks aus, um die Umgebung für Dateizurückschreibung einzurichten:

1. „Umgebung für Dateizurückschreibungsoperationen aktivieren" auf Seite 52
2. Führen Sie die folgenden Tasks aus, wenn Sie erwarten, dass Dateieigner Dateizurückschreibungsoperationen auf Linux-Gast-VMs ausführen:
   a. „Linux-Mount-Proxy-Feature installieren" auf Seite 37
   b. „Linux-Mount-Proxy für Dateizurückschreibungsoperationen konfigurieren" auf Seite 54
3. Überprüfen Sie, ob Sicherungsoperationen wie erwartet ausgeführt werden: Warten Sie, bis eine geplante Sicherung ausgeführt wurde, oder führen Sie eine Ad-hoc-Sicherungsoperation einer VM aus.

Nachdem die Umgebung für Dateizurückschreibungsoperationen vorbereitet wurde, kann der Administrator die folgenden optionalen Tasks ausführen:

- „Optionen für Dateizurückschreibungsoperationen ändern" auf Seite 57
- „Data Protection for Microsoft Hyper-V-Protokollaktivität konfigurieren" auf Seite 59

Wenn Sie keine Dateizurückschreibungsoperationen mehr verwenden müssen, können Sie das Feature anhand der folgenden Anweisungen entfernen:

„Feature für Dateizurückschreibung entfernen" auf Seite 42

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 IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V auf einem Hyper-V-Hostsystem installiert sein.

Der Web-Service für Dateizurückschreibung und die zugrunde liegende Data Protection for Microsoft Hyper-V-Umgebung müssen installiert, konfiguriert und be-

triebsbereit sein, einschließlich der Einheiten zum Versetzen von Daten, die als Mount-Proxy agieren, und der ISCI-Services.

Hyper-V-Administratoren müssen den Dateieignern eine URL bereitstellen, mit der diese eine Verbindung zu der Webschnittstelle für Dateizurückschreibung herstellen können. Wenn Sie den Konfigurationsassistenten verwenden, um Data Protection for Microsoft Hyper-V zu konfigurieren und das Feature für Dateizurückschreibung zu aktivieren, wird die URL bei Abschluss des Assistenten bereitgestellt. Weitere Informationen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.

Voraussetzungen für virtuelle Hyper-V-Maschinen

Die folgenden Voraussetzungen gelten für virtuelle Hyper-V-Maschinen, die die zurückzuschreibenden Dateien enthalten:

- Die virtuelle Maschine (VM) muss während der Dateizurückschreibungsoperation aktiv sein.
- Die Windows-VM muss derselben Windows-Domäne angehören wie der Hyper-V-Host, auf dem der IBM Spectrum Protect-Client für Sichern/Archivieren installiert ist.
- Wenn eine VM aus einer Windows-Domäne gelöscht und zu einem späteren Zeitpunkt zurückgeschrieben wird, muss die VM wieder in die Domäne eingebunden werden, damit die Domänenvertrauensbeziehung sichergestellt ist. Versuchen Sie nicht, eine Dateizurückschreibung aus der VM auszuführen, bis die Domänenvertrauensbeziehung wiederhergestellt ist.
- 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.
- Für Linux-Gast-VMs ist für die VM die lokale Benutzerauthentifizierung erforderlich. Die Authentifizierung über die Windows-Domäne, über Lightweight Directory Access Protocol (LDAP), über Kerberos oder über andere Netzauthentifizierungsmethoden ist nicht verfügbar.
- Für Linux-Gast-VMs unter dem Betriebssystem Red Hat Enterprise Linux 6 muss die Option `ChallengeResponseAuthentication` in der Konfigurationsdatei des Dämons **sshd** (`/etc/ssh/sshd_config`) auf YES gesetzt oder auskommentiert sein. Sie können eine der folgenden Anweisungen angeben:

  ```
  ChallengeResponseAuthentication yes
  #ChallengeResponseAuthentication no
  ```

  Starten Sie den Dämon **sshd** nach der Änderung dieser Option erneut.

Voraussetzungen für die Einheit zum Versetzen von Daten

Eine spezielle Einheit zum Versetzen von Daten (Client für Sichern/Archivieren) ist auf dem Hyper-V-Hostsystem installiert, die Daten von einem System auf ein anderes "versetzt".

Das Hyper-V-Hostsystem muss derselben Windows-Domäne angehören wie die VM, 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 VM-Platten zugreift. Dieses System

bewirkt, dass die Dateisysteme auf den bereitgestellten VM-Platten als Zurückschreibungspunkte in der Schnittstelle für Dateizurückschreibung zugänglich sind.

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

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:

- Ein Windows-Domänenbenutzer mit lokaler Administratorberechtigung ist erforderlich, um die Netzfreigabe zu erstellen und auf sie zuzugreifen. Der Administrator gibt diese Berechtigungsnachweise im Data Protection for Microsoft Hyper-V-Konfigurationsassistenten ein, um die Umgebung für Dateizurückschreibungsoperationen zu aktivieren.
- Ein Dateieigner greift mit den Berechtigungsnachweisen eines Windows-Domänenbenutzers auf die ferne VM zu, die die zurückzuschreibenden Dateien enthält. Diese Berechtigungsnachweise werden bei der Anmeldung in die Schnittstelle für Dateizurückschreibung eingegeben. Mit den Berechtigungsnachweisen des Domänenbenutzers wird überprüft, ob der Dateieigner berechtigt ist, sich bei der fernen VM anzumelden und Dateien auf der fernen VM zurückzuschreiben. Für diese Berechtigungsnachweise sind keine besonderen Berechtigungen erforderlich.
- Wenn ein Dateieigner ein Windows-Domänenbenutzerkonto verwendet, das den Zugriff auf bestimmte Computer beschränkt (anstatt Zugriff auf alle Computer in der Domäne zu gewähren), müssen Sie sicherstellen, 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

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

Sich anmelden, um Dateien zurückzuschreiben

Sie können sich bei der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung anmelden, um Ihre Dateien mit minimaler Unterstützung durch den Administrator zurückzuschreiben.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die URL der Schnittstelle für Dateizurückschreibung von Ihrem Administrator anfordern.

Informationen zu diesem Vorgang

Wenn Sie sich bei dieser Schnittstelle anmelden, können Sie Ihre Dateien nach Belieben suchen und zurückschreiben.

Vorgehensweise

1. Greifen Sie auf die Schnittstelle für Dateizurückschreibung zu, indem Sie einen Web-Browser öffnen und die URL eingeben, die Sie von Ihrem Administrator erhalten haben.
2. Geben Sie den Netznamen oder die IP-Adresse der virtuellen Maschine (VM) an, die Ihre Dateien enthält. Beispiel: `myhost.mycompany.com`.
3. Geben Sie das Benutzerkonto ein, das Sie für den Zugriff auf Ihre Dateien verwenden.
   - Verwenden Sie für Windows-Gastbetriebssysteme das Format `Windows-Domänenname\Benutzername`.
   - Verwenden Sie für Linux-Gastbetriebssysteme den Benutzernamen, mit dem Sie sich bei der Linux-Gast-VM anmelden.
4. Geben Sie das Kennwort des Benutzerkontos ein und klicken Sie auf **Anmelden**.

Zugehörige Tasks:

„Dateien aus einer Sicherung der virtuellen Maschine zurückschreiben"

Dateien aus einer Sicherung der virtuellen Maschine zurückschreiben

Suchen Sie Ihre Dateien und schreiben Sie sie an eine bevorzugte Position zurück.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie bei der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung angemeldet sind. Damit Sie Dateien zurückschreiben können, muss es eine Sicherung geben.

Informationen zu diesem Vorgang

Es werden nur die Dateien und Verzeichnisse angezeigt, für die Sie unter dem Betriebssystem die Berechtigung zum Anzeigen haben.

Vorgehensweise

1. Wählen Sie eine Sicherung aus, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf ein Datum im Kalender.
   b. Wählen Sie gegebenenfalls eine Uhrzeit im Feld **Verfügbare Sicherungen** aus.
   c. Klicken Sie auf **Sicherung auswählen**.

   Die Platten oder Verzeichnisse der virtuellen Maschine werden in der Tabelle angezeigt.
2. Optional: Wenn Sie nicht die Standardsicherung verwenden möchten, wählen Sie eine andere Sicherung aus, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf den Kalender.
   b. Klicken Sie auf ein Datum im Kalender.
   c. Wählen Sie gegebenenfalls eine Uhrzeit aus.
   d. Klicken Sie auf **Sicherung ändern**.

Einschränkung: Wenn Sie Sicherungsdatum oder -uhrzeit ändern, geht Ihre bisherige Dateiauswahl verloren. Allerdings wird die neue Sicherung in das Verzeichnis geladen, das Sie zuvor untersucht haben. Wenn dieses Verzeichnis nicht verfügbar ist, wird die Sicherung in das Hauptverzeichnis geladen.

Die Platten oder Verzeichnisse der virtuellen Maschine werden in der Tabelle angezeigt.

3. Führen Sie die folgenden Schritte aus, um Dateien für das Zurückschreiben auszuwählen:
   a. Klicken Sie auf eine Platte oder ein Verzeichnis in der Tabelle, damit die Unterverzeichnisse und Dateien angezeigt werden.
   b. Optional: Wenn Sie im aktuellen Verzeichnis und in dessen Unterverzeichnissen nach einer Datei suchen möchten, geben Sie im Feld **Suchen** einen Namen ein und drücken Sie die **Eingabetaste**. Die Ergebnisse werden in der Reihenfolge angezeigt, in der sie gefunden werden.
   c. Wählen Sie mindestens eine Datei/ein Verzeichnis für das Zurückschreiben aus. Wenn Sie ein Verzeichnis ohne Inhalt auswählen, wird das leere Verzeichnis nicht zurückgeschrieben.
4. Wählen Sie aus, wohin Dateien zurückgeschrieben werden sollen.
   - Wenn Dateien und Verzeichnisse an ihre ursprüngliche Position zurückgeschrieben werden sollen, wählen Sie **Zurückschreibungsziel** > **Ursprüngliche Position** aus.
   - Wenn Dateien und Verzeichnisse an eine andere Position zurückgeschrieben werden sollen, wählen Sie **Zurückschreibungsziel** > **Alternative Position** aus.
5. Wenn Sie das Auswählen beendet haben, klicken Sie auf **Zurückschreiben**. Wenn Sie Dateien in ein alternatives Verzeichnis zurückschreiben, wählen Sie ein bestehendes Verzeichnis auf Ihrer virtuellen Maschine aus oder erstellen Sie ein Verzeichnis für die zurückzuschreibenden Dateien. Klicken Sie dann auf **Zurückschreiben**. Wenn es bereits eine Datei mit demselben Namen gibt, werden das ursprüngliche Änderungsdatum und die ursprüngliche Änderungsuhrzeit der zurückgeschriebenen Datei dem Dateinamen hinzugefügt. Nachfolgende Zurückschreibungen derselben Datei enthalten eine Zahl (_*N*) hinter dem ursprünglichen Änderungsdatum und der ursprünglichen Änderungsuhrzeit. Beispiel: `t2.2015-03-07-07-28-03_1.txt`

Nächste Schritte

Klicken Sie auf das Symbol für Zurückschreiben (), um Informationen zu aktiven und vor Kurzem durchgeführten Zurückschreibungen anzuzeigen. Standardmäßig werden Informationen nach dem Abschluss einer Zurückschreibung 7 Tage lang aufbewahrt.

Wenn eine Zurückschreibung mit einem Fehler oder einer Warnung abgeschlossen wird, rufen Sie zusätzliche Informationen durch Klicken auf **Details** auf. Wenn Sie die Fehler- oder Warnungsinformationen speichern möchten, klicken Sie auf **Exportieren** und speichern Sie die Informationen im CSV-Format.

Kapitel 6. In-Guest-Anwendungen schützen

Sie können Data Protection for Microsoft Hyper-V zum Schützen von Microsoft Exchange Servern und Microsoft SQL Servern verwenden, die innerhalb von virtuellen Gastmaschinen in einer Microsoft Hyper-V-Umgebung ausgeführt werden.

Microsoft Exchange Server-Daten in Hyper-V-Umgebungen schützen

Für Microsoft Exchange Server-Workloads, die in einer Hyper-V-Gast-VM (VM = virtuelle Maschine) ausgeführt werden, können Sie anwendungskonsistente Sicherungen der Gast-VM erstellen. Anschließend können Sie eine Sicherung auf Datenbankebene oder Mailboxebene wiederherstellen, falls die ursprüngliche Datenbank oder Mailbox beschädigt oder nicht mehr vorhanden ist.

Die folgenden Produkte arbeiten zusammen, um Microsoft Exchange Server-Daten in einer Hyper-V-Umgebung zu schützen:

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Version 8.1.6
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Exchange Server Version 8.1.6

Diese Softwareangebote arbeiten zusammen, um Microsoft Exchange Server-Daten in einer Hyper-V-Umgebung zu schützen, wenn keine anderen Softwareprodukte zum Sichern von Microsoft Exchange Server-Daten verwendet werden.

Informationen zu den Berechtigungen, die zum Sichern und Zurückschreiben von Anwendungsdaten für Microsoft Exchange Server erforderlich sind, enthält die Technote 1647986.

Informationen zu den Softwarevoraussetzungen für den Anwendungsschutz von Microsoft Exchange Server finden Sie in der Technote 2017347. .

Software installieren und für den Anwendungsschutz von Microsoft Exchange Server konfigurieren

Zum Schützen einer Gast-VM (VM = virtuelle Maschine), die Microsoft Exchange Server-Daten hostet, müssen Sie Installations- und Konfigurationsschritte auf dem Hyper-V-Host und der Gast-VM ausführen. Verwenden Sie die schrittweisen Anleitungen, um Ihre Umgebung für den In-Guest-Anwendungsschutz einzurichten.

Vorbereitende Schritte

Überprüfen Sie die Softwarevoraussetzungen in der Technote 2017347.

Informationen zu diesem Vorgang

In der folgenden Tabelle sind die Namen aufgelistet, die in den Beispielen in den folgenden Tasks verwendet werden:

Typ des Namens	Beispiel
Name des Hyper-V-Hosts oder -Clusters	Kingston5

Typ des Namens	Beispiel
Name der Gast-VM, die Microsoft Exchange Server hostet	Kingston40

Führen Sie die folgenden Schritte aus, um Data Protection for Microsoft Hyper-V und Data Protection for Microsoft Exchange Server zu installieren, einzurichten und für den Schutz von Microsoft Exchange Server-Daten auf VM-Gastmaschinen zu konfigurieren.

Vorgehensweise

1. „Schritt 1 (Hyper-V-Host): Data Protection for Microsoft Hyper-V installieren und konfigurieren".
2. „Schritt 2 (Gast-VM): Data Protection for Microsoft Exchange Server installieren und konfigurieren" auf Seite 107.
3. „Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren" auf Seite 109.
4. „Schritt 4 (Gast-VM): Datenbank zurückschreiben" auf Seite 112.
5. „Optional: Anwendungsschutz nach einer Namensänderung der virtuellen Maschine konfigurieren" auf Seite 113

Schritt 1 (Hyper-V-Host): Data Protection for Microsoft Hyper-V installieren und konfigurieren

Installieren und konfigurieren Sie Data Protection for Microsoft Hyper-V und stellen Sie sicher, dass Sie die Gast-VM (VM = virtuelle Maschine), die Microsoft Exchange Server-Daten hostet, erfolgreich sichern können.

Vorbereitende Schritte

Wenn Sie ein Upgrade von Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher durchführen, benennen Sie die vorhandenen Hyper-V-Knotennamen auf dem IBM Spectrum Protect-Server in *Clustername_hv_tgt* für einen Cluster oder *Hostname_hv_tgt* für einen eigenständigen Host um. Der Hyper-V-Knotenname ist der Knotenname, der durch die Option `asnodename` angegeben wird.

Nennen Sie beispielsweise den Hyper-V-Knoten auf dem Server in `KINGSTON_HV_TGT` um. Weitere Informationen finden Sie in „Knoten auf dem IBM Spectrum Protect-Server umbenennen" auf Seite 20.

Stellen Sie sicher, dass die Kommunikationsports wie in „Erforderliche Kommunikationsports" auf Seite 18 beschrieben offen sind.

Vorgehensweise

Führen Sie die folgenden Tasks auf dem Hyper-V-Host oder -Cluster aus:

1. Installieren Sie Data Protection for Microsoft Hyper-V.

   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V installieren" auf Seite 28.
2. Konfigurieren Sie Data Protection for Microsoft Hyper-V, indem Sie den Konfigurationsassistenten ausführen.

   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.

Hinweis: Notieren Sie sich den Zielknotennamen, der auf der Assistentenseite **Cluster und Hosts** oder nach Klicken auf **Aktionen** > **Eigenschaften** in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole angezeigt wird. Der Zielknotenname endet auf `_HV_TGT`. Der Zielknotenname ist erforderlich, wenn Sie den Konfigurationsassistenten in Data Protection for Microsoft Exchange Server ausführen.

3. Sichern Sie mit der Data Protection for Microsoft Hyper-V-Verwaltungskonsole die VM, die Microsoft Exchange Server hostet.

   Anweisungen finden Sie in „Ad-hoc-Sicherung einer virtuellen Maschine ausführen" auf Seite 91.

4. Optional: Sichern Sie eine passive Kopie einer Datenbank, die zu einer Exchange Server-Datenbankverfügbarkeitsgruppe (DAG) gehört. Geben Sie die Option `vmpreferdagpassive yes` mit dem Befehl **`dsmc backup vm`** an.

   Durch die Sicherung der passiven Kopie verringern sich in der Regel die Auswirkungen auf die Leistung bei der aktiven Kopie in der Produktionsdatenbank. Ist keine gültige passive Kopie verfügbar, wird die aktive Datenbankkopie gesichert.

Nächste Schritte

Wenn die VM erfolgreich gesichert wurde, fahren Sie mit „Schritt 2 (Gast-VM): Data Protection for Microsoft Exchange Server installieren und konfigurieren" fort.

Zugehörige Informationen:

Vmpreferdagpassive

Schritt 2 (Gast-VM): Data Protection for Microsoft Exchange Server installieren und konfigurieren

Damit sichergestellt ist, dass Sie Datenbanken mit Data Protection for Microsoft Exchange Server sichern können, führen Sie die Schritte für die Installation und Konfiguration von Data Protection for Microsoft Exchange Server und für die Sicherung einer Microsoft Exchange Server-Datenbank aus.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Prozedur in „Schritt 1 (Hyper-V-Host): Data Protection for Microsoft Hyper-V installieren und konfigurieren" auf Seite 106 ausgeführt haben.

Stellen Sie sicher, dass Microsoft Exchange Server-Datenbanken und -Mailboxen auf virtuellen Hyper-V-Platten gehostet werden.

Stellen Sie sicher, dass keine Microsoft Exchange Server-Datenbank auf physischen Festplatten, auf unabhängigen Platten oder auf Platten gehostet wird, die durch In-Guest-iSCSI direkt an die Gastmaschine angeschlossen sind.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Gast-VM (VM = virtuelle Maschine) aus, die Microsoft Exchange Server-Daten hostet:

1. Installieren Sie Data Protection for Microsoft Exchange Server.

   Wichtig: Führen Sie den Data Protection for Microsoft Exchange Server-Konfigurationsassistenten erst in Schritt 3 auf Seite 108 aus.

Installationsanweisungen finden Sie in der Produktdokumentation zu IBM Spectrum Protect for Mail.

2. Installieren Sie das Feature der Einheit zum Versetzen von Daten aus dem Data Protection for Microsoft Hyper-V-Installationspaket.

   Wählen Sie im Installationsassistenten die Option für die erweiterte Installation aus und klicken Sie anschließend auf **Feature der Einheit zum Versetzen von Daten oder Mount-Proxy installieren**, um die Unterstützung für Anwendungsschutz zu installieren.

   Weitere Informationen finden Sie in „Nur die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten installieren" auf Seite 32.

3. Öffnen Sie die Data Protection for Microsoft Exchange Server-Verwaltungskonsole, indem Sie auf **Start** > **DP for Exchange-Verwaltungskonsole** klicken. Der Konfigurationsassistent wird automatisch geöffnet.

   Wenn der Konfigurationsassistent nicht automatisch gestartet wird, rufen Sie die Baumstruktursicht in der Verwaltungskonsole auf und klicken Sie auf **IBM Spectrum Protect** > **Dashboard** > **Verwalten** > **Konfiguration** > **Assistenten**. Klicken Sie doppelt auf **IBM Spectrum Protect-Konfigurationsassistent**.

4. Auf der Seite **IBM Spectrum Protect-Knotennamen** des Konfigurationsassistenten geben Sie den Knotennamen des VSS-Anforderers, Data Protection for Microsoft Exchange Server, und des Hyper-V-Zielknotens in die jeweiligen Felder ein. Stellen Sie sicher, dass das Kontrollkästchen **DP Exchange-VSS-Unterstützung nicht konfigurieren** abgewählt ist.

   In der folgenden Tabelle sind beispielsweise die Knotennamen aufgelistet, die in den Konfigurationsanweisungen verwendet werden.

Feldname	Beispiele für Knotennamen
VSS-Anforderer	KINGSTON40_VSS
Data Protection for Exchange	KINGSTON40_EXC
Hyper-V-Zielknoten	KINGSTON5_HV_TGT

5. Auf der Seite **IBM Spectrum Protect-Servereinstellungen** des Konfigurationsassistenten führen Sie einen der folgenden Schritte aus:
   - Wenn der IBM Spectrum Protect-Server mit dem Assistenten konfiguriert werden soll, wählen Sie **Überprüfen** oder **Editieren** aus und aktualisieren Sie das Makro nach Bedarf.
   - Wenn der Server manuell konfiguriert werden soll, führen Sie die folgenden Schritte aus:
     a. Auf der letzten Assistentenseite klicken Sie auf den Link, der die Makrodatei öffnet.
     b. Aktualisieren Sie die Makrodatei und führen Sie sie aus. Sie können auch die entsprechenden Befehle aus dem Makro ausführen und diese nach Bedarf für Ihre Umgebung anpassen.

        Angenommen, eine Maßnahmendomäne mit dem Namen `fcm_pdexc` wurde für Ihre Verwendung definiert. Führen Sie im Ordner `C:\Programme\Tivoli\TSM\baclient` den Befehl **dsmadmc** aus und geben Sie die folgenden Befehle aus:

```
register node KINGSTON40_VSS T_3_m_p_P_w userid=KINGSTON40_VSS
update node KINGSTON40_VSS T_3_m_p_P_w backdelete=yes forcep=yes

register node KINGSTON40_EXC T_3_m_p_P_w domain=fcm_pdexc
 userid=KINGSTON40_EXC
update node KINGSTON40_EXC T_3_m_p_P_w backdelete=yes domain=fcm_pdexc
 forcep=yes
```

```
grant proxynode target=KINGSTON40_EXC agent=KINGSTON40_VSS
```

Die Option `forcep=yes` erzwingt die Zurücksetzung des Kennworts beim ersten Zugriff.

In einigen Fällen wird die folgende Fehlernachricht angezeigt, wenn Sie den Befehl **dsmadmc** ausführen:

```
ANS1592E SSL-Protokoll konnte nicht initialisiert werden
```

Wenn diese Nachricht angezeigt wird, stellen Sie sicher, dass die Option `sessionsecurity` für das Konto des IBM Spectrum Protect-Serveradministrators, das Sie verwenden, auf **transitional** gesetzt ist.

Geben Sie beispielsweise den folgenden Befehl auf einem fernen Computer aus, der auf den IBM Spectrum Protect-Server zugreifen kann:

```
update admin myAdmin sessionsecurity=transitional
```

6. Führen Sie den Konfigurationsassistenten vollständig aus.
7. Sichern Sie eine Datenbank von der Data Protection for Microsoft Exchange Server-Verwaltungskonsole aus:
   a. Klicken Sie im Fenster **Aktionen** auf **Sicherungsmethode** > **VSS**.
   b. Klicken Sie im Fenster **Aktionen** auf **Sicherungsziel** > **TSM**.
   c. Klicken Sie im Fenster **Aktionen** auf **Vollständige Sicherung**.
8. Optional: Aktualisieren Sie manuell die Mailboxprotokollinformationen, um sicherzustellen, dass konsistente Positionsinformationen für das Mailboxprotokoll und die Mailboxen in der Datenbanksicherung vorhanden sind.

   Anweisungen finden Sie in „Mailboxinformationen in Microsoft Exchange Server-Sicherungen aktualisieren" auf Seite 116.

Nächste Schritte

Nachdem die VSS-Sicherung erfolgreich ausgeführt wurde, fahren Sie mit „Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren" fort.

Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren

Konfigurieren Sie Data Protection for Microsoft Hyper-V für den Schutz der Gast-VM (VM = virtuelle Maschine), die Microsoft Exchange Server-Daten hostet. Sichern Sie die VM und überprüfen Sie, ob die Sicherungsoperation erfolgreich ausgeführt wurde.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Prozedur in „Schritt 2 (Gast-VM): Data Protection for Microsoft Exchange Server installieren und konfigurieren" auf Seite 107 ausgeführt haben.

Stellen Sie sicher, dass die virtuellen Festplatten (VHDXs), die die Microsoft Exchange Server-Datenbank hosten, nicht bei der VM-Sicherungsoperation ausgeschlossen werden. Anweisungen finden Sie in „Sicherstellen, dass Microsoft Exchange Server-Datenträger bei Sicherungen virtueller Maschinen nicht ausgeschlossen sind" auf Seite 117.

Optional: Die Integration Services oder die Schnittstelle für Gastdienste wird während einer Sicherungsoperation automatisch für die Gast-VM aktiviert. Eine manuelle Aktivierung ist nicht erforderlich. Wenn Sie jedoch den aktuellen Status über-

prüfen oder den Service **Gastdienste** explizit aktivieren möchten, verwenden Sie eine der folgenden Methoden auf dem Hyper-V-Host oder -Cluster:

- Über den Hyper-V Manager:
  1. Klicken Sie mit der rechten Maustaste auf die VM und klicken Sie auf **Einstellungen** > **Integration Services**.
  2. Im Fenster **Integration Services** stellen Sie sicher, dass das Kontrollkästchen **Gastdienste** ausgewählt ist.
- Geben Sie als Administrator die folgenden Befehle bei einer PowerShell-Eingabeaufforderung aus:

```
Get-VMIntegrationService -VMName Kingston40
Enable-VMIntegrationService -VMName Kingston40 -Name "Schnittstelle für Gastdienste"
```

Informationen zu diesem Vorgang

Data Protection for Microsoft Hyper-V stellt Anwendungskonsistenz zur Verfügung, wenn Sie VMs sichern, die Microsoft Exchange Server hosten. Mit diesen Sicherungen können Sie die VM in einem konsistenten Zustand wiederherstellen.

Sollen aus diesem Sicherungstyp nur ausgewählte Datenbanken oder Mailboxen zurückgeschrieben werden, ohne dass die gesamte VM wiederhergestellt werden muss, müssen zum Zeitpunkt der VM-Momentaufnahme und -Sicherung Informationen zum Zustand des Microsoft Exchange Servers aufbewahrt werden. Diese Informationen werden im Rahmen der Interaktionen von Microsoft Volume Shadow Copy Services (VSS) erfasst, die während einer VM-Momentaufnahme ausgeführt werden.

Damit Data Protection for Microsoft Hyper-V die Microsoft VSS-Metadaten für Microsoft Exchange Server erfasst, müssen Sie Data Protection for Microsoft Hyper-V so konfigurieren, dass diese Informationen während Sicherungsoperationen von der VM abgerufen werden.

Vorgehensweise

Führen Sie die folgenden Schritte auf dem Hyper-V-Host oder -Cluster aus, wenn keine anderslautenden Anweisungen angegeben sind:

1. Vom Ordner `baclient` aus definieren Sie die Windows-Berechtigungsnachweise für die Gast-VM, die Microsoft Exchange Server hostet:
   - Zum Definieren von Berechtigungsnachweisen für eine bestimmte VM geben Sie den folgenden Befehl im Ordner `baclient` bei der Eingabeaufforderung aus:

     ```
     dsmc set password -type=vmguest Name_der_Gast-VM "Admin-ID_der_Gastmaschine" Admin-Kennwort_de
     -optfile=dsm.Hostname_HV_DM.opt
     ```

   - Zum Definieren von Berechtigungsnachweisen für alle VMs, für die keine speziellen Berechtigungsnachweise definiert sind, geben Sie den folgenden Befehl aus:

     ```
     dsmc set password -type=vmguest allvm "Admin-ID_der_Gastmaschine" Admin-Kennwort_der_Gastmasch
     -optfile=dsm.Hostname_HV_DM.opt
     ```

   Hierbei gilt Folgendes:

   VM-Name
   Der Name der Gast-VM, die Microsoft Exchange Server hostet. Der Name ist der VM-Name, der im Hyper-V-Manager angezeigt wird.

Admin-ID_der_Gastmaschine
Die Administrator-ID für die Gast-VM. Die *Admin-ID_der_Gastmaschine* kann ein Windows-Domänenkonto oder ein lokales Konto sein. Beispiel:

- Verwenden Sie für ein Domänenkonto das Format *Domäne\Benutzername*.
- Verwenden Sie für ein lokales Konto das Format *Benutzername*.

Admin-Kennwort_der_Gastmaschine
Das Kennwort für die Administrator-ID für die Gast-VM.

Hyper-V-Hostname
Der Name des Hyper-V-Hosts oder -Clusters.

Beispiel:

```
dsmc set password -type=vmguest Kingston40 "world\alan" "@lanPwd!"
-optfile=dsm.KINGSTON5_HV_DM.opt
```

Die Konten, die im Befehl **set password** verwendet werden, müssen sowohl auf dem Hyper-V-Host oder -Cluster als auch auf der Gast-VM gültig sein, die Exchange Server-Daten hostet.

Mit dem Befehl **dsmc set password** werden die Berechtigungsnachweise der Gast-VM verschlüsselt auf dem System gespeichert, auf dem sich die Einheit zum Versetzen von Daten befindet. Für die Administrator-ID und das Kennwort der Gast-VM sind die folgenden Mindestberechtigungen erforderlich:

Sicherungsberechtigungen: Microsoft Exchange Server 2013 und 2016: Berechtigungen für Organisationsverwaltung (Zugehörigkeit zur Verwaltungsrollengruppe, Organisationsverwaltung).

2. Vom Ordner `baclient` aus konfigurieren Sie die Optionsdatei der Einheit zum Versetzen von Daten für Anwendungsschutz:
   a. Öffnen Sie die Optionsdatei der Einheit zum Versetzen von Daten (`dsm.`*`Hostname`*`_HV_DM.opt`) zum Editieren. Geben Sie beispielsweise den folgenden Befehl aus:

      ```
      notepad dsm.KINGSTON5_HV_DM.opt
      ```

   b. Fügen Sie die Option `include.vmtsmvss` *Name_der_Gast-VM* hinzu. Der Parameter *Name_der_Gast-VM* kann Platzhalterzeichen enthalten. Beispiel:

      ```
      include.vmtsmvss Kingston40
      ```

3. Führen Sie die folgenden Schritte auf der Gast-VM aus, um die Anzeige von Datenbanksicherungen in Data Protection for Microsoft Exchange Server zu ermöglichen.
   a. Generieren Sie die Berechtigungsnachweisdatei auf der Gastmaschine, indem Sie den folgenden Befehl bei einer PowerShell-Eingabeaufforderung ausführen und bei der entsprechenden Aufforderung den Domänenbenutzernamen (*Domänenname\Benutzername*) und das Kennwort eingeben.

      ```
      Get-Credential | Export-Clixml -Path
      'C:\Programme\Tivoli\TSM\baclient\dsmcreds.xml'
      ```

      Der Domänenbenutzer muss über die Exchange-Zurückschreibungsberechtigung verfügen.

   b. Überprüfen Sie die Berechtigungsnachweise, indem Sie die folgenden Befehle über eine Exchange-Verwaltungsshell auf der Gast-VM ausführen:

      ```
      $cred = Import-CliXml -Path 'C:\Programme\Tivoli\TSM \baclient\
        dsmcreds.xml'
      $Session = New-PSSession -Credential $cred -ConfigurationName
        Microsoft.Exchange -ConnectionUri http://Exchange Server-Name/
        PowerShell?serializationLevel=Full -Authentication Kerberos
      Import-PSSession -Session $Session
      Get-MailboxDatabase -Server <Exchange Server-Name>
      ```

Die Liste der Mailboxdatenbanken wird korrekt angezeigt.

4. Vom Ordner `baclient` auf dem Hyper-V-Host aus sichern Sie die Gast-VM, indem Sie den Befehl **dsmc backup vm** ausgeben: Beispiel:

```
dsmc backup vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt
-asnode=KINGSTON5_HV_TGT
```

5. Überprüfen Sie die Sicherungsoperation, indem Sie den Befehl **dsmc query vm** ausführen. Bei VM-Namen muss die Groß-/Kleinschreibung beachtet werden.

   Geben Sie beispielsweise den folgenden Befehl im Ordner `baclient` aus:

```
dsmc query vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt
-asnode=KINGSTON5_HV_TGT -detail
```

   Die Ausgabe umfasst einen ähnlichen Text wie in dem folgenden Beispiel (möglicherweise ist bei Ihnen jedoch eine andere Version von Microsoft Exchange Server installiert):

```
Art des Anwendungsschutzes: TSM VSS
Geschützte Anwendung(en): Microsoft Exchange Server 2016
```

6. Vom Ordner `baclient` aus verwenden Sie den Befehl **dsmc set access**, um dem VSS-Knoten auf der Gast-VM den Zugriff auf die VM-Sicherung und ihre Zurückschreibung zu gestatten. Geben Sie beispielsweise den folgenden Befehl aus:

```
dsmc set access backup -type=vm Kingston40 kingston40_vss -nodename=
KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
```

   Geben Sie den folgenden Befehl **dsmc query access** aus, um die VM-Sicherungen anzuzeigen, auf die der Knoten Zugriff hat. Beispiel:

```
dsmc query access -nodename=KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
```

Nächste Schritte

Wenn die Sicherungsoperation erfolgreich ausgeführt wurde, fahren Sie mit „Schritt 4 (Gast-VM): Datenbank zurückschreiben" fort.

Zugehörige Verweise:

„**Backup VM**" auf Seite 166

„INCLUDE.VMTSMVSS" auf Seite 194

Zugehörige Informationen:

Set Access

Set Password

Schritt 4 (Gast-VM): Datenbank zurückschreiben

Schreiben Sie eine Datenbank mit Data Protection for Microsoft Exchange Server zurück, um zu überprüfen, ob Sie den Anwendungsschutz korrekt konfiguriert haben.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Prozedur in „Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren" auf Seite 109 ausgeführt haben.

Stellen Sie sicher, dass die folgenden erforderlichen Services auf der Gast-VM (VM = virtuelle Maschine) aktiv sind:

1. Bei der Eingabeaufforderung geben Sie den folgenden Befehl aus:

```
services.msc
```

2. Lokalisieren Sie den **IBM Spectrum Protect Recovery Agent-Service** in der Liste der Services und starten Sie den Service bei Bedarf.
3. Lokalisieren Sie den **Microsoft iSCSI-Initiator-Dienst** in der Liste der Services. Gegebenenfalls ändern Sie den Starttyp in **Automatisch** und starten Sie den Service.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Gast-VM aus:

1. Starten Sie die Data Protection for Microsoft Exchange Server-Verwaltungskonsole.
2. Wählen Sie eine **Exchange Server**-Instanz in der Baumstruktur aus.
3. Rufen Sie die Registerkarte **Wiederherstellen** auf und klicken Sie auf **Aktualisieren**.
4. Wählen Sie einen Datenbankeintrag mit der Sicherungsmethode **VMVSS** aus.
5. Klicken Sie im Fenster **Aktionen** auf **Zurückschreiben**.
6. Wenn die Zurückschreibungsoperation beendet ist, überprüfen Sie die Datenbank und eventuelle zugehörige Mailboxen.

Nächste Schritte

Sie können jetzt Sicherungen verwalten und bei Bedarf Daten wiederherstellen. Weitere Informationen siehe:

- „Sicherungsoperationen verwalten" auf Seite 115
- „Daten zurückschreiben" auf Seite 118

Wenn Sie den Namen der Gast-VM ändern, nachdem Sie die Konfigurationsschritte für Anwendungsschutz ausgeführt haben, müssen Sie die Software mit dem neuen VM-Namen neu konfigurieren. Anweisungen finden Sie in „Optional: Anwendungsschutz nach einer Namensänderung der virtuellen Maschine konfigurieren".

Optional: Anwendungsschutz nach einer Namensänderung der virtuellen Maschine konfigurieren

Wenn Sie den Namen der Gast-VM (VM = virtuelle Maschine) geändert haben, nachdem Sie die Anwendungsschutzkonfiguration ausgeführt haben, müssen Sie Data Protection for Microsoft Hyper-V mit der umbenannten Gast-VM neu konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Software installiert und für den Schutz von Gast-VMs konfiguriert haben, die Microsoft Exchange Server hosten.

Informationen zu diesem Vorgang

Führen Sie diese Task nur aus, wenn Sie den Namen einer Gast-VM geändert haben, die durch Anwendungsschutz geschützt ist.

Vorgehensweise

1. Geben Sie auf der Einheit zum Versetzen von Daten auf dem Hyper-V-Host oder -Cluster den folgenden Befehl aus:

```
dsmc set password –type=vmguest neuer_Anzeigename_der_VM-Gastmaschine
Admin-ID_der_Gastmaschine Admin-Kennwort_der_Gastmaschine
```

Hierbei gilt Folgendes:

neuer_Anzeigename_der_VM-Gastmaschine
Der Name der neuen Gast-VM, die Microsoft Exchange Server hostet. Der Name ist der VM-Name, der im Hyper-V-Manager angezeigt wird.

Admin-ID_der_Gastmaschine
Die Administrator-ID für die neue Gast-VM. *Admin-ID_der_Gastmaschine* muss ein Windows-Domänenkonto oder ein lokales Konto sein. Beispiel:

- Verwenden Sie für ein Domänenkonto das Format *Domäne\Benutzername*.
- Verwenden Sie für ein lokales Konto das Format *Benutzername*.

Admin-Kennwort_der_Gastmaschine
Das Kennwort für die Administrator-ID für die neue Gast-VM.

2. Aktualisieren Sie in der Optionsdatei der Einheit zum Versetzen von Daten (`dsm.Hostname_HV_DM.opt`) die Option `include.vmtsmvss` wie folgt:

   ```
   include.vmtsmvss neuer_Anzeigename_der_VM-Gastmaschine
   ```

   Dabei ist *neuer_Anzeigename_der_VM-Gastmaschine* der Anzeigename der neuen Gast-VM im Hyper-V-Manager. Sie können Platzhalterzeichen verwenden.
3. Vom Ordner `baclient` auf der Einheit zum Versetzen von Daten aus sichern Sie die neue Gast-VM, indem Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwenden oder den folgenden Befehl bei der Eingabeaufforderung ausgeben:

   ```
   dsmc backup vm neuer_Anzeigename_der_VM-Gastmaschine -optfile=dsm.Hostname_HV_DM.opt
   -asnode=Hostname_HV_TGT
   ```
4. Vom Ordner `baclient` aus verwenden Sie den Befehl **dsmc set access**, um dem VSS-Knoten auf der neuen Gast-VM den Zugriff auf die VM-Sicherung und ihre Zurückschreibung zu gestatten. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   dsmc set access backup –type=VM neuer_Anzeigename_der_VM-Gastmaschine VSS-Anfordererknoten
   -optfile=dsm.Hostname_HV_DM.opt
   ```

   Hierbei gilt Folgendes:

   neuer_Anzeigename_der_VM-Gastmaschine
   Der Anzeigename der neuen Gast-VM im Hyper-V-Manager.

   VSS-Anfordererknoten
   Der Name des VSS-Anforderers, der in Data Protection for Microsoft Exchange Server konfiguriert wurde.

   Hostname
   Der Name des Hyper-V-Hosts oder -Clusters, auf dem Data Protection for Microsoft Hyper-V installiert ist.
5. Optional: Da der VSS-Anfordererknoten bereits Zugriff auf die VMs hat, die unter dem alten VM-Namen gesichert wurden, werden in der Data Protection for Microsoft Exchange Server-Verwaltungskonsole die VMVSS-Datenbanken angezeigt, die für die alte VM und die neue VM gesichert wurden.

   Wenn Sie nicht möchten, dass Zugriff auf die VM-Sicherungen mit dem alten VM-Namen besteht, müssen Sie den Zugriff auf die alten VM-Sicherungen löschen. Geben Sie den folgenden Befehl auf der Einheit zum Versetzen von Daten auf dem Hyper-V-Host aus:

   ```
   dsmc del access -optfile=dsm.Hostname_HV_DM.opt -asnode=Hostname_HV_TGT
   ```

Eine Zugriffsliste wird angezeigt. Geben Sie den Index für den Eintrag an, der aus der Zugriffsliste gelöscht werden soll.

Wenn Sie Speicherbereich auf dem IBM Spectrum Protect-Server einsparen wollen, können Sie den Dateibereich löschen, der die Sicherungsdaten für die alte VM enthält. Geben Sie dazu den Befehl **dsmc delete filespace** aus.

Wichtig: Wenn Sie einen Dateibereich löschen, werden alle Sicherungsversionen in diesem Dateibereich gelöscht und die Daten können nicht mehr zurückgeschrieben werden. Stellen Sie sicher, dass die alten VM-Sicherungen veraltet sind, bevor Sie sie löschen.

Sicherungsoperationen verwalten

Nachdem Sie die Umgebung für den Schutz von Microsoft Exchange Server-Daten konfiguriert haben, können Sie Sicherungen für virtuelle Maschinen (VMs) planen. Außerdem können Sie separat die Mailboxinformationen in Exchange Server-Datenbanksicherungen auf der VM aktualisieren.

Sicherungen virtueller Maschinen planen

Planen Sie Sicherungen virtueller Maschinen (VMs), damit sichergestellt ist, dass Ihre Daten regelmäßig geschützt werden.

Vorbereitende Schritte

Bevor Sie VMs sichern, die Microsoft Exchange Server-Datenbanken hosten, müssen Sie die Datenbanken bereitstellen.

Standardmäßig beträgt die maximale Größe, die für eine virtuelle Festplatte (VHDX) bei einer Sicherungsoperation zulässig ist, 2 TB. Mit der Option `vmmaxvirtualdisks` können Sie die maximale Größe jedoch auf 8 TB erweitern. Weitere Informationen finden Sie in „Vmmaxvirtualdisks" auf Seite 213.

Informationen zu diesem Vorgang

Während der Sicherungsverarbeitung übergeht Data Protection for Microsoft Hyper-V eine Microsoft Exchange Server-Gastdatenbank in einer Datenbankverfügbarkeitsgruppe (Database Availability Group - DAG), deren Bereitstellung aufgehoben wurde, die beschädigt bzw. ausgesetzt ist oder die sich nicht in einwandfreiem Zustand befindet. Datenbanken in solchen ungültigen Status werden bei VM-Sicherungen ausgeschlossen und sind nicht für die Zurückschreibung verfügbar.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.
2. Klicken Sie im Navigationsfenster auf einen eigenständigen Host oder einen Cluster.
3. Klicken Sie im Fenster **Aktionen** auf **Sicherungsmanagement**.
4. Wählen Sie einen Zeitplan im Fenster **Sicherungsmanagement** aus und klicken Sie auf **Zeitplan zuordnen**.
5. Zum Schließen des Fensters klicken Sie auf **Schließen**.
6. Stellen Sie sicher, dass die Quelle für den Zeitplan die VMs umfasst, die Microsoft Exchange Server hosten.
7. Stellen Sie sicher, dass einer der folgenden Services aktiv ist:

- Wenn Sie einen Scheduler verwenden, der von einem Clientakzeptor (CAD) verwaltet wird, stellen Sie sicher, dass der Clientakzeptorservice auf der Einheit zum Versetzen von Daten aktiv ist.
- Wenn Sie einen eigenständigen Scheduler verwenden, stellen Sie sicher, dass der Scheduler-Service aktiv ist.

Zugehörige Tasks:

„Sicherungszeitpläne für einen Host oder eine Clustermaschine verwalten" auf Seite 86

Mailboxinformationen in Microsoft Exchange Server-Sicherungen aktualisieren

Wenn Sie eine virtuelle Maschine (VM) sichern, die Microsoft Exchange Server-Daten hostet, wird automatisch das Mailboxprotokoll mit der VM-Sicherung hochgeladen, wenn Data Protection for Microsoft Exchange Server auf der VM erkannt wird.

Informationen zu diesem Vorgang

Mailboxprotokollinformationen werden bei Sicherungsoperationen für Exchange Server-Datenbanken nur dann automatisch aktualisiert, wenn Data Protection for Microsoft Exchange Server auf der VM installiert ist. Der automatische Upload des Mailboxprotokolls kann auch durch Angabe der Option `VMBACKUPMAILBOXHISTORY No` in der Datei `dsm.opt` inaktiviert werden.

Sie können die Mailboxprotokollinformationen manuell aktualisieren, indem Sie die Data Protection for Microsoft Exchange Server-Befehlszeilenschnittstelle verwenden.

Tipp: Führen Sie diese Task aus, bevor Sie die VMs sichern, die Microsoft Exchange Server enthalten. Auf diese Weise können Sie sicherstellen, dass Sie über konsistente Positionsinformationen für das Mailboxprotokoll und die Mailboxen in Datenbanksicherungen verfügen.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Gast-VM aus, die Exchange Server-Daten hostet:

1. Geben Sie den Befehl **backup /UpdateMailboxInfoOnly** wie im folgenden Beispiel dargestellt aus, um nur die Mailboxprotokollinformationen in Exchange Server-Datenbanksicherungen zu aktualisieren:

   ```
   tdpexcc backup DB1 full /UpdateMailboxInfoOnly
   ```

   Dabei ist `DB1` der Datenbankname und `full` ist der Typ der Datenbanksicherung.

   Tipp: Geben Sie einen Stern (*) als Datenbanknamen an, um die Informationen für alle Mailboxen in der Exchange-Organisation zu aktualisieren.
2. Optional: Führen Sie die folgenden Schritte aus, um zu überprüfen, ob die Mailboxinformationen korrekt aktualisiert wurden.
   a. Überprüfen Sie die Mailboxinformationen für Datenbanksicherungen auf dem IBM Spectrum Protect-Server, indem Sie den Befehl **query /SHOWMAILBOXInfo** wie im folgenden Beispiel dargestellt ausgeben:

      ```
      tdpexcc query tsm /showmailboxinfo
      ```

b. Starten Sie die Microsoft Management Console (MMC) und prüfen Sie in der Sicht **Mailboxzurückschreibung** oder **Browser für Mailboxzurückschreibung** die Liste der aktualisierten Mailboxen, die für die Zurückschreibung verfügbar sind.

Sicherungen überprüfen

Nachdem Sie eine Sicherung erstellt haben, überprüfen Sie, ob Sie die Sicherungen virtueller Maschinen und die Datenbanksicherungen über die Data Protection for Microsoft Exchange Server-Schnittstelle abfragen können.

Vorgehensweise

1. In der Microsoft Management Console (MMC) wählen Sie einen Microsoft Exchange Server aus.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**.
3. Wählen Sie **Anzeigen** > **Datenbanken** aus. Eine Liste der Microsoft Exchange Server-Datenbanksicherungen, die zurückgeschrieben werden können, wird angezeigt.

   Für Microsoft Exchange Server-Datenbanken, die mit Data Protection for Microsoft Hyper-V gesichert werden, ist die Sicherungsmethode `vmvss` angegeben.

Sicherstellen, dass Microsoft Exchange Server-Datenträger bei Sicherungen virtueller Maschinen nicht ausgeschlossen sind

Die Datenträger auf virtuellen Hyper-V-Festplatten (VHDXs) müssen die Microsoft Exchange Server-Datenbanken enthalten, die nicht bei der Data Protection for Microsoft Hyper-V-Sicherungsverarbeitung ausgeschlossen sind.

Vorbereitende Schritte

Stellen Sie sicher, dass die Datenbanken sich nicht auf den folgenden Plattentypen befinden:

- Physischen Platten
- Unabhängigen Platten
- Platten, die über iSCSI direkt an das Gastbetriebssystem angeschlossen sind

Vorgehensweise

1. Stellen Sie sicher, dass eventuell vorhandene Anweisungen `EXCLUDE.VMDISK` in der Optionsdatei auf der Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten, die zum Sichern der virtuellen Maschine (VM) verwendet wird, nicht versehentlich VHDXs ausschließen, die Datenträger mit Microsoft Exchange Server-Dateien, -Dateibereichen, -Datenbanken und -Mailboxen enthalten.

   Beispiel:

   - Die Datei `kingston40.vhdx` enthält den logischen Datenträger `C:`.
   - Die Datei `kingston40.vhdx` enthält die logischen Datenträger `E:` und `F:`.
   - Die Plattenposition (IDE-Controllernummer und Einheitenposition) für `kingston40_1.vhdx` ist `IDE 1 0`.
   - Die Plattenposition für `kingston40_2.vhdx` ist `IDE 1 1`.
   - Die zu sichernden Microsoft Exchange Server-Datenbankdateien befinden sich auf den Laufwerken `E:` und `F:`.

2. Vergewissern Sie sich, dass in keiner Anweisung `kingston40_2.vhdx` bei der VM-Sicherung ausgeschlossen wird, indem Sie sicherstellen, dass die Einheit zum Versetzen von Daten nicht die folgenden oder ähnliche Anweisungen enthält:

   ```
   EXCLUDE.VMDISK KINGSTON40 "IDE 1 1"
   EXCLUDE.VMDISK * "IDE 1 1"
   ```

   Wenn Sie alternativ die meisten Festplatten ausschließen, müssen Sie die VM-Platten explizit einschließen, indem Sie eine der folgenden Anweisungen verwenden:

   ```
   INCLUDE.VMDISK KINGSTON40 "IDE 1 1"
   INCLUDE.VMDISK * "IDE 1 1"
   ```

   Einschluss- und Ausschlussanweisungen werden in der Reihenfolge, in der sie in der Datei `dsm.opt` angezeigt werden, von unten nach oben verarbeitet. Geben Sie die Anweisungen in der richtigen Reihenfolge ein, um das gewünschte Ziel zu erreichen.

   Sie können den Ausschluss und Einschluss einer VM-Platte über die Befehlszeilenschnittstelle angeben:

   ```
   dsmc backup vm „KINGSTON40:-vmdisk=IDE 1 1" -asnode=KINGSTON5_HV_TGT
   ```

Zugehörige Verweise:

„Exclude.vmdisk" auf Seite 186

„Include.vmdisk" auf Seite 191

Daten zurückschreiben

Nachdem Sie eine virtuelle Maschine mit aktiviertem Anwendungsschutz gesichert haben, können Sie eine Datenbank oder Mailbox wiederherstellen, falls das ursprüngliche Objekt nicht mehr vorhanden oder beschädigt ist.

Bei einer Wiederherstellungsoperation wird eine vollständige Sicherung der Microsoft Exchange Server-Datenbank oder -Mailbox aus der Data Protection for Microsoft Hyper-V-Sicherung zurückgeschrieben.

Wenn Sie die gesamte virtuelle Maschine (VM) zurückschreiben, werden alle Microsoft Exchange Server-Datenbanken und -Mailboxen auf der VM zurückgeschrieben und mit dem Stand der VM-Sicherung wiederhergestellt.

Microsoft iSCSI-Initiator-Dienst starten

Mit dem iSCSI-Protokoll werden die Platten bereitgestellt, die für eine Wiederherstellungsoperation verwendet werden. Stellen Sie sicher, dass der Microsoft iSCSI-Initiator-Dienst gestartet ist und auf dem System, auf das die Daten zurückgeschrieben werden sollen, auf den Starttyp 'Automatisch' gesetzt ist.

Vorgehensweise

Führen Sie die folgenden Schritte im Windows-Fenster **Dienste** aus.

1. In der Liste **Dienste** klicken Sie mit der rechten Maustaste auf **Microsoft iSCSI-Initiator-Dienst**.
2. Klicken Sie auf **Eigenschaften**.
3. Definieren Sie auf der Registerkarte **Allgemein** die folgenden Optionen:
   a. Wählen Sie in der Liste **Starttyp** die Option **Automatisch** aus.
   b. Klicken Sie auf **Starten** und klicken Sie anschließend auf **OK**.

Ergebnisse

In der Liste **Dienste** wird für den **Microsoft iSCSI-Initiator-Dienst** der Status **Gestartet** und der Starttyp **Automatisch** angezeigt.

Datenbanksicherungen mithilfe der grafischen Benutzerschnittstelle zurückschreiben

Zum Wiederherstellen einer vollständigen Microsoft Exchange Server-Datenbanksicherung aus einer Sicherung einer virtuellen Maschine (VM) können Sie die grafische Data Protection for Microsoft Exchange Server-Benutzerschnittstelle verwenden.

Vorbereitende Schritte

Stellen Sie sicher, dass der Microsoft iSCSI-Initiator-Dienst aktiv ist, bevor Sie eine Microsoft Exchange Server-Datenbank mit der Sicherungsmethode "VMVSS" zurückschreiben. Ist der Dienst nicht aktiv, starten Sie ihn. Anweisungen finden Sie in „Microsoft iSCSI-Initiator-Dienst starten" auf Seite 118.

Vorgehensweise

1. Zum Starten einer vollständigen Datenbankwiederherstellung aus einer VM starten Sie die Data Protection for Microsoft Exchange Server Management Console (MMC).
2. Im Navigationsfenster erweitern Sie den Knoten **Daten schützen und wiederherstellen** und wählen Sie einen Microsoft Exchange Server-Server aus.
3. Auf der Registerkarte **Wiederherstellen** wählen Sie **Datenbankzurückschreibung** aus. Alle Sicherungen einschließlich aller Datenbanksicherungen aus einer VM-Sicherung werden aufgelistet.
4. Wählen Sie eine vollständige Datenbanksicherung für die Zurückschreibung aus.
5. Klicken Sie im Fenster **Aktionen** auf **Zurückschreiben**.

Sicherungen einer anderen virtuellen Maschine zurückschreiben

Mit Data Protection for Microsoft Exchange Server können Sie auf Sicherungen einer anderen virtuellen Maschine (VM) auf dem IBM Spectrum Protect-Server zugreifen und die Sicherung zurückschreiben.

Informationen zu diesem Vorgang

Sie können Datenbank- und Mailboxsicherungen auf einen anderen DAG-Knoten (Database Availability Group - Datenbankverfügbarkeitsgruppe) als den ursprünglichen Sicherungsknoten zurückschreiben.

Im folgenden Szenario wird vorausgesetzt, dass Exchange-VMs sich in Ihrer virtuellen Umgebung befinden: `vm1` und `vm2`.

Sie möchten es Data Protection for Microsoft Exchange Server auf `vm2` ermöglichen, auf Datenbank- und Mailboxsicherungen auf `vm1` und `vm2` zuzugreifen und sie zurückzuschreiben.

Vorgehensweise

1. Konfigurieren Sie den eigenständigen Anwendungsschutz, um Microsoft Exchange Server-Daten auf `vm1` und `vm2` zu schützen.

   Anweisungen finden Sie in den folgenden Themen:

- „Schritt 1 (Hyper-V-Host): Data Protection for Microsoft Hyper-V installieren und konfigurieren" auf Seite 106
- „Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren" auf Seite 109

2. Auf dem Hyper-V-Host sichern Sie `vm1` und `vm2`, indem Sie den Befehl **`dsmc backup vm`** in der Befehlszeilenschnittstelle der Einheit zum Versetzen von Daten ausgeben.
3. Auf `vm2` installieren Sie Data Protection for Microsoft Exchange Server und konfigurieren Sie die Software für Exchange Server-Datenschutz in einer Hyper-V-Umgebung.

   Anweisungen finden Sie in „Schritt 2 (Gast-VM): Data Protection for Microsoft Exchange Server installieren und konfigurieren" auf Seite 107.
4. Geben Sie auf dem Hyper-V-Host den Befehl **`set access`** wie im folgenden Beispiel aus, um Data Protection for Microsoft Exchange Server auf `vm2` den Zugriff auf Sicherungen auf `vm1` und `vm2` zu gestatten:

   ```
   dsmc set access backup -type=vm vm1 vm2_vss
   dsmc set access backup -type=vm vm2 vm2_vss
   ```
5. Schreiben Sie Datenbank- oder Mailboxsicherungen auf `vm1` oder `vm2` zurück.

Mailboxdaten zurückschreiben

Data Protection for Microsoft Exchange Server sichert Mailboxdaten auf der Datenbankebene und kann außerdem einzelne Mailboxeinträge aus der Datenbanksicherung zurückschreiben.

Anweisungen zum Zurückschreiben von Mailboxdaten, zum Zurückschreiben von verlagerten und gelöschten Mailboxen und zum interaktiven Zurückschreiben von Mailboxnachrichten mit dem Browser für Mailboxzurückschreibung finden Sie in der Produktdokumentation zu IBM Spectrum Protect for Mail.

Daten mithilfe der Befehlszeilenschnittstelle zurückschreiben

Wenn Sie die Data Protection for Microsoft Exchange Server-Befehlszeilenschnittstelle bevorzugen, können Sie diese verwenden, um eine vollständige Wiederherstellung einer Microsoft Exchange Server-Datenbank aus einer virtuellen Maschine zu starten.

Vorbereitende Schritte

Stellen Sie sicher, dass der Microsoft iSCSI-Initiator-Dienst aktiv ist, bevor Sie eine Microsoft Exchange Server-Datenbank mit dem Sicherungstyp "VMVSS" zurückschreiben. Ist der Dienst nicht aktiv, starten Sie ihn. Anweisungen finden Sie in „Microsoft iSCSI-Initiator-Dienst starten" auf Seite 118.

Vorgehensweise

1. Geben Sie den Befehl **`query`** aus, um die vollständigen Datenbanksicherungen abzufragen. In dem folgenden Beispiel werden alle Sicherungen für die Microsoft Exchange Server-Datenbank mit dem Namen `exc_db10` abgefragt.

```
tdpexcc q tsm exc_db10

IBM Spectrum Protect for Mail:
Data Protection for Microsoft Exchange Server
Version 8, Release 1, Stufe 6.0 (C) Copyright
IBM Corporation 1997, 2018. All rights reserved.

...

IBM Spectrum Protect-Server wird nach einer Liste der
Datensicherungen abgefragt, bitte warten....

Verbindung zu IBM Spectrum Protect-Server als Knoten 'KINGSTON40_EXC' wird hergestellt...
Verbindung zum lokalen DSM-Agenten 'exc' wird hergestellt...
Ausweichknoten 'KINGSTON40_EXC' wird verwendet...

 Exchange Server : exc

 Datenbank : exc_db10

 Sicherungsdatum Größe S Typ  Pos  Objektname
-------------------- ---- - ----  --- ----------------------
15.07.2018 19:17:26 5,40 B A full  Srv 20180715191726 (VMVSS)

Die Operation wurde erfolgreich ausgeführt. (rc = 0)
```

2. Zum Zurückschreiben der Datenbank ohne Anwenden der Transaktionsprotokolle geben Sie den folgenden Befehl aus:

   ```
   TDPEXCC RESTore Datenbankname FULL /BACKUPDEstination=TSM
    /BACKUPMethod=VMVSS
   ```

   Die folgende Beispielausgabe entsteht, wenn Sie den Befehl für die Microsoft Exchange Server-Datenbank mit dem Namen exc_db10 ausgeben.

   ```
   TDPEXCC RESTore exc_db10 FULL /BACKUPDEstination=TSM /BACKUPMethod=VMVSS

   IBM Spectrum Protect for Mail:
   Data Protection for Microsoft Exchange Server
   Version 8, Release 1, Stufe 6.0 (C) Copyright
   IBM Corporation 1997, 2018. All rights reserved.

   Verbindung zu IBM Spectrum Protect-Server als Knoten 'KINGSTON40_EXC' wird hergestellt...

   Verbindung zum lokalen DSM-Agenten 'exc' wird hergestellt...
   Ausweichknoten 'KINGSTON40_EXC' wird verwendet...

   Microsoft Exchange-Zurückschreibung wird gestartet...
   Beginn der VSS-Zurückschreibung von 'exc_db10'...

   'exc_db10' wird über Kopie auf Dateiebene aus Momentaufnahme(n) zurückgeschrieben.
   Diese Operation kann einige Zeit dauern. Bitte warten

   ...

   Die Operation wurde erfolgreich ausgeführt. (rc = 0)
   ```

   Sie können die Datenbank an eine andere Position zurückschreiben, indem Sie den Parameter **/INTODB** hinzufügen. Beispiel:

   ```
   TDPEXCC RESTore TestDB1 FULL /INTODB=Test2
    /BACKUPDEstination=TSM /BACKUPMethod=VMVSS
   ```

Nächste Schritte

Sie können inaktive Sicherungen über die Data Protection for Microsoft Exchange Server-Befehlszeilenschnittstelle mit dem Befehl **TDPEXCC** zurückschreiben. Bei der Ausgabe des Befehls **restore** geben Sie den Datenbankobjektnamen für die jeweilige Sicherung an.

Zum Abrufen des Datenbankobjektnamens geben Sie den folgenden Befehl aus:

```
tdpexcc q tsm DB-Name full /all
```

Wenn Sie über den Wert für den Datenbankobjektnamen verfügen, geben Sie den Datenbankobjektnamen im Parameter */OBJect=Objektname* des Befehls **TDPEXCC restore** an, wobei *Objektname* der Datenbankobjektname ist. Beispiel:

```
TDPEXCC RESTore db44 FULL /OBJect=20180715191726 /BACKUPDEstination=TSM
 /BACKUPMethod=VMVSS
```

Daten mithilfe von Windows PowerShell-Cmdlets zurückschreiben

Wenn Sie Windows PowerShell-Cmdlets bevorzugen, können Sie diese mit Data Protection for Microsoft Exchange Server verwenden, um eine vollständige Wiederherstellung einer Microsoft Exchange Server-Datenbank aus einer virtuellen Maschine zu starten.

Vorbereitende Schritte

Stellen Sie sicher, dass der Microsoft iSCSI-Initiator-Dienst aktiv ist, bevor Sie eine Microsoft Exchange Server-Datenbank mit dem Sicherungstyp "VMVSS" zurückschreiben. Ist der Dienst nicht aktiv, starten Sie ihn. Anweisungen finden Sie in „Microsoft iSCSI-Initiator-Dienst starten” auf Seite 118.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Gast-VM aus:

1. Geben Sie das Cmdlet **query** aus, um die vollständigen Datenbanksicherungen abzufragen. Geben Sie beispielsweise den folgenden Befehl ein, um alle vollständigen Datenbanksicherungen abzufragen:

   ```
   Get-DpExcBackup -Name * -FromExcServer *
   ```

2. Geben Sie das Cmdlet für Datenbankzurückschreibung aus. Beispiel:

   ```
   Restore-DpExcBackup -Name ExchDb01 -Full
    -BACKUPDESTINATION TSM -FROMEXCSERVer PALADIN20
    -INTODB Zwen
   ```

3. Geben Sie die Cmdlets für Zurückschreibung mit dem Parameter **intodb** aus, um die Daten an eine andere Position zurückzuschreiben. Beispiel:

   ```
   Restore-DpExcBackup -Name ExchDb01 -Full
    -BACKUPDESTINATION TSM -FROMEXCSERVer PALADIN20
    -OBJect 20140923100738 -INTODB ExchDb01_altRdb
   ```

Informationen zum IBM Spectrum Protect-Dateibereich

Möglicherweise ist es niemals erforderlich, dass Ihnen die Dateinamen oder Speicherpositionen für die Dateien Ihrer virtuellen Maschine (VM) bekannt sein müssen. Falls die zugrunde liegende Dateistruktur Sie jedoch interessiert: Data Protection for Microsoft Hyper-V-Sicherungen werden unter dem Knotennamen des Hyper-V-Zielknotens (z. B. `KINGSTON5_HV_TGT`) auf dem IBM Spectrum Protect-Server gespeichert.

Das folgende Beispiel zeigt die Dateibereichsinformationen für die VM mit dem Namen `Kingston40`.

```
Protect: ORION>q file KINGSTON5_HV_TGT f=d

Knotenname:  KINGSTON5_HV_TGT
Dateibereichsname: \VMFULL-kingston40
Hexadezimaler Dateibereichsname:
FSID: 61
Kollokationsgruppenname:
Plattform: TDP Hyper-V
Dateibereichstyp: API:TSMVM
Ist Dateibereich Unicode?: Nein
Kapazität: 0 KB
Auslastung in %: 0,0
Startdatum/-zeit der letzten Sicherung: 13.03.2018 21:29:17
Tage seit Start der letzten Sicherung: 31
Enddatum/-zeit der letzten vollständigen NAS-Imagesicherung:
Tage seit der letzten vollständigen NAS-Imagesicherung:
Datum/Zeit der letzten Sicherung des Clients (UTC):
Datum/Zeit der letzten Archivierung des Clients (UTC):
Startdatum/-zeit der letzten Replikation:
Tage seit dem Start der letzten Replikation:
Enddatum/-zeit der letzten Replikation:
Tage seit dem Ende der letzten Replikation:
Replikationsregel für Sicherungsdaten: DEFAULT
Replikationsstatus für Sicherungsdaten: Aktiviert
Replikationsregel für Archivierungsdaten: DEFAULT
Replikationsstatus für Archivierungsdaten: Aktiviert
Replikationsregel für speicherverwaltete Daten: DEFAULT
Replikationsstatus für speicherverwaltete Daten: Aktiviert
Typ für Gefährdung: Standardintervall
Gefährdungsintervall:
```

Microsoft SQL Server-Daten in Hyper-V-Umgebungen schützen

Für Microsoft SQL Server-Workloads, die in einer Hyper-V-Gast-VM (VM = virtuelle Maschine) ausgeführt werden, können Sie anwendungskonsistente Sicherungen der Gast-VM erstellen. Anschließend können Sie eine Sicherung auf Datenbankebene wiederherstellen, falls die ursprüngliche Datenbank beschädigt oder nicht mehr vorhanden ist.

Die folgenden Produkte arbeiten zusammen, um Microsoft SQL Server-Daten in einer Hyper-V-Umgebung zu schützen:

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V Version 8.1.6
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft SQL Server Version 8.1.6

Informationen zu den Berechtigungen, die zum Sichern und Zurückschreiben von Anwendungsdaten für Microsoft SQL Server erforderlich sind, enthält die Technote 1647995.

Informationen zu den Softwarevoraussetzungen für den Anwendungsschutz von Microsoft SQL Server finden Sie in der Technote 2017347. .

Software installieren und für den Anwendungsschutz von Microsoft SQL Server konfigurieren

Zum Schützen einer Gast-VM (VM = virtuelle Maschine), die Microsoft SQL Server-Daten hostet, müssen Sie Installations- und Konfigurationsschritte auf dem Hyper-V-Host und der Gast-VM ausführen. Verwenden Sie die schrittweisen Anleitungen, um Ihre Umgebung für den In-Guest-Anwendungsschutz einzurichten.

Vorbereitende Schritte

Überprüfen Sie die Softwarevoraussetzungen in der Technote 2017347.

Informationen zu diesem Vorgang

In der folgenden Tabelle sind die Namen aufgelistet, die in den Beispielen in den folgenden Tasks verwendet werden:

Typ des Namens	Beispiel
Name des Hyper-V-Hosts oder -Clusters	Kingston5
Name der Gast-VM, die Microsoft SQL Server hostet	Kingston40

Führen Sie die folgenden Schritte aus, um Data Protection for Microsoft Hyper-V und Data Protection for Microsoft SQL Server zu installieren, einzurichten und für den Schutz von Microsoft SQL Server-Daten auf VM-Gastmaschinen zu konfigurieren.

Vorgehensweise

1. „Schritt 1 (Hyper-V-Host): Data Protection for Microsoft Hyper-V installieren und konfigurieren".
2. „Schritt 2 (Gast-VM): Data Protection for Microsoft SQL Server installieren und konfigurieren" auf Seite 125.
3. „Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren" auf Seite 128.
4. „Schritt 4 (Gast-VM): Datenbank zurückschreiben" auf Seite 131.
5. „Optional: Anwendungsschutz nach einer Namensänderung der virtuellen Maschine konfigurieren" auf Seite 132

Schritt 1 (Hyper-V-Host): Data Protection for Microsoft Hyper-V installieren und konfigurieren

Installieren und konfigurieren Sie Data Protection for Microsoft Hyper-V und stellen Sie sicher, dass Sie die Gast-VM (VM = virtuelle Maschine), die Microsoft SQL Server-Daten hostet, erfolgreich sichern können.

Vorbereitende Schritte

Wenn Sie ein Upgrade von Data Protection for Microsoft Hyper-V Version 8.1.2 oder früher durchführen, benennen Sie die vorhandenen Hyper-V-Knotennamen auf dem IBM Spectrum Protect-Server in *Clustername_hv_tgt* für einen Cluster oder *Hostname_hv_tgt* für einen eigenständigen Host um. Der Hyper-V-Knotenname ist der Knotenname, der durch die Option `asnodename` angegeben wird.

Nennen Sie beispielsweise den Hyper-V-Knoten auf dem Server in `KINGSTON_HV_TGT` um. Weitere Informationen finden Sie in „Knoten auf dem IBM Spectrum Protect-Server umbenennen" auf Seite 20.

Stellen Sie sicher, dass die Kommunikationsports wie in „Erforderliche Kommunikationsports" auf Seite 18 beschrieben offen sind.

Vorgehensweise

Führen Sie die folgenden Tasks auf dem Hyper-V-Host oder -Cluster aus:

1. Installieren Sie Data Protection for Microsoft Hyper-V.

   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V installieren" auf Seite 28.
2. Konfigurieren Sie Data Protection for Microsoft Hyper-V, indem Sie den Konfigurationsassistenten ausführen.

   Anweisungen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren" auf Seite 45.

   Hinweis: Notieren Sie sich den Zielknotennamen, der auf der Assistentenseite **Cluster und Hosts** oder nach Klicken auf **Aktionen** > **Eigenschaften** in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole angezeigt wird. Der Zielknotenname endet auf `_HV_TGT`. Der Zielknotenname ist erforderlich, wenn Sie den Konfigurationsassistenten in Data Protection for Microsoft SQL Server ausführen. .
3. Sichern Sie mit der Data Protection for Microsoft Hyper-V-Verwaltungskonsole die VM, die Microsoft SQL Server hostet.

   Anweisungen finden Sie in „Ad-hoc-Sicherung einer virtuellen Maschine ausführen" auf Seite 91.

Nächste Schritte

Wenn die VM erfolgreich gesichert wurde, fahren Sie mit „Schritt 2 (Gast-VM): Data Protection for Microsoft SQL Server installieren und konfigurieren" fort.

Schritt 2 (Gast-VM): Data Protection for Microsoft SQL Server installieren und konfigurieren

Damit sichergestellt ist, dass Sie Datenbanken mit Data Protection for Microsoft SQL Server sichern können, führen Sie die Schritte für die Installation und Konfiguration von Data Protection for Microsoft SQL Server und für die Sicherung einer Microsoft SQL Server-Datenbank aus.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Prozedur in „Schritt 1 (Hyper-V-Host): Data Protection for Microsoft Hyper-V installieren und konfigurieren" auf Seite 124 ausgeführt haben.

Stellen Sie sicher, dass Microsoft SQL Server-Datenbanken auf virtuellen Hyper-V-Platten gehostet werden.

Stellen Sie sicher, dass keine Microsoft SQL Server-Datenbank auf physischen Platten, auf unabhängigen Platten oder auf Platten gehostet wird, die durch In-Guest-iSCSI direkt an die Gastmaschine angeschlossen sind.

Stellen Sie sicher, dass Microsoft SQL Server-Datenbanken sich auf einem Einzelserver befinden und nicht an irgendeinem Clustering-Typ teilnehmen, z. B. an Failover-Clustern, AlwaysOn-Verfügbarkeitsgruppen oder AlwaysOn-Failover-Cluster-Instanzen.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Gast-VM (VM = virtuelle Maschine) aus, die Microsoft SQL Server-Daten hostet:

1. Installieren Sie Data Protection for Microsoft SQL Server.

   Wichtig: Führen Sie den Data Protection for Microsoft SQL Server-Konfigurationsassistenten erst in Schritt 3 aus.

   Installationsanweisungen finden Sie in der Produktdokumentation zu IBM Spectrum Protect for Databases.
2. Installieren Sie das Feature der Einheit zum Versetzen von Daten aus dem Data Protection for Microsoft Hyper-V-Installationspaket.

   Wählen Sie im Installationsassistenten die Option für die erweiterte Installation aus und klicken Sie anschließend auf **Feature der Einheit zum Versetzen von Daten oder Mount-Proxy installieren**, um die Unterstützung für Anwendungsschutz zu installieren.

   Weitere Informationen finden Sie in „Nur die Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten installieren" auf Seite 32.
3. Öffnen Sie die Data Protection for Microsoft SQL Server-Verwaltungskonsole, indem Sie auf **Start** > **DP for SQL-Verwaltungskonsole** klicken. Der Konfigurationsassistent wird automatisch geöffnet.

   Wenn der Konfigurationsassistent nicht automatisch gestartet wird, rufen Sie die Baumstruktursicht in der Verwaltungskonsole auf und klicken Sie auf **IBM Spectrum Protect** > **Dashboard** > **Verwalten** > **Konfiguration** > **Assistenten**. Klicken Sie doppelt auf **IBM Spectrum Protect-Konfigurationsassistent**.
4. Auf der Seite **IBM Spectrum Protect-Knotennamen** des Konfigurationsassistenten geben Sie den Knotennamen des VSS-Anforderers, Data Protection for Microsoft SQL Server, und des Hyper-V-Zielknotens in die jeweiligen Felder ein. Stellen Sie sicher, dass das Kontrollkästchen **DP-SQL-VSS-Unterstützung nicht konfigurieren** abgewählt ist.

   In der folgenden Tabelle sind beispielsweise die Knotennamen aufgelistet, die in den Konfigurationsanweisungen verwendet werden.

Feldname	Beispiele für Knotennamen
VSS-Anforderer	KINGSTON40_VSS
Data Protection for SQL	KINGSTON40_SQL
Hyper-V-Zielknoten	KINGSTON5_HV_TGT

5. Auf der Seite **IBM Spectrum Protect-Servereinstellungen** des Konfigurationsassistenten führen Sie einen der folgenden Schritte aus:
   - Wenn der IBM Spectrum Protect-Server mit dem Assistenten konfiguriert werden soll, wählen Sie **Überprüfen** oder **Editieren** aus und aktualisieren Sie das Makro nach Bedarf.
   - Wenn der Server manuell konfiguriert werden soll, führen Sie die folgenden Schritte aus:
     a. Auf der letzten Assistentenseite klicken Sie auf den Link, der die Makrodatei öffnet.

b. Aktualisieren Sie die Makrodatei und führen Sie sie aus. Sie können auch die entsprechenden Befehle aus dem Makro ausführen und diese nach Bedarf für Ihre Umgebung anpassen.

   Angenommen, eine Maßnahmendomäne mit dem Namen `fcm_pdsql` wurde für Ihre Verwendung definiert. Führen Sie im Ordner `C:\Programme\Tivoli\TSM\baclient` den Befehl **dsmadmc** aus und geben Sie die folgenden Befehle aus:

   ```
   register node KINGSTON40_VSS T_3_m_p_P_w userid=KINGSTON40_VSS
   update node KINGSTON40_VSS T_3_m_p_P_w backdelete=yes forcep=yes
   ```

   ```
   register node KINGSTON40_SQL T_3_m_p_P_w domain=fcm_pdsql
    userid=KINGSTON40_SQL
   update node KINGSTON40_SQL T_3_m_p_P_w backdelete=yes domain=fcm_pdsql
    forcep=yes
   ```

   ```
   grant proxynode target=KINGSTON40_SQL agent=KINGSTON40_VSS
   ```

   Die Option `forcep=yes` erzwingt die Zurücksetzung des Kennworts beim ersten Zugriff.

In einigen Fällen wird die folgende Fehlernachricht angezeigt, wenn Sie den Befehl **dsmadmc** ausführen:

```
ANS1592E SSL-Protokoll konnte nicht initialisiert werden
```

Wenn diese Nachricht angezeigt wird, stellen Sie sicher, dass die Option `sessionsecurity` für das Konto des IBM Spectrum Protect-Serveradministrators, das Sie verwenden, auf **transitional** gesetzt ist.

Geben Sie beispielsweise den folgenden Befehl auf einem fernen Computer aus, der auf den IBM Spectrum Protect-Server zugreifen kann:

```
update admin myAdmin sessionsecurity=transitional
```

6. Führen Sie den Konfigurationsassistenten vollständig aus.
7. Stellen Sie sicher, dass die Maßnahmen so definiert sind, dass genügend Versionen von Microsoft SQL Server-Protokollen und VM-Sicherungen aufbewahrt werden.

   Anweisungen finden Sie in „Versionen von Sicherungen verwalten" auf Seite 135.
8. Sichern Sie eine Datenbank von der Data Protection for Microsoft SQL Server-Verwaltungskonsole aus:
   a. Klicken Sie im Fenster **Aktionen** auf **Sicherungsmethode** > **VSS**.
   b. Klicken Sie im Fenster **Aktionen** auf **Sicherungsziel** > **TSM**.
   c. Klicken Sie im Fenster **Aktionen** auf **Vollständige Sicherung**.

Nächste Schritte

Nachdem die VSS-Sicherung erfolgreich ausgeführt wurde, fahren Sie mit „Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren" auf Seite 128 fort.

Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren

Konfigurieren Sie Data Protection for Microsoft Hyper-V für den Schutz der Gast-VM (VM = virtuelle Maschine), die Microsoft SQL Server-Daten hostet. Sichern Sie die VM und überprüfen Sie, ob die Sicherungsoperation erfolgreich ausgeführt wurde.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Prozedur in „Schritt 2 (Gast-VM): Data Protection for Microsoft SQL Server installieren und konfigurieren" auf Seite 125 ausgeführt haben.

Stellen Sie sicher, dass die virtuellen Festplatten (VHDXs), die die Microsoft Exchange Server-Datenbank hosten, nicht bei der VM-Sicherungsoperation ausgeschlossen werden. Anweisungen finden Sie in „Sicherstellen, dass Microsoft SQL Server-Datenträger bei Sicherungen virtueller Maschinen nicht ausgeschlossen sind" auf Seite 136.

Optional: Die Integration Services oder die Schnittstelle für Gastdienste wird während einer Sicherungsoperation automatisch für die Gast-VM aktiviert. Eine manuelle Aktivierung ist nicht erforderlich. Wenn Sie jedoch den aktuellen Status überprüfen oder den Service **Gastdienste** explizit aktivieren möchten, verwenden Sie eine der folgenden Methoden auf dem Hyper-V-Host oder -Cluster:

- Über den Hyper-V Manager:
  1. Klicken Sie mit der rechten Maustaste auf die VM und klicken Sie auf **Einstellungen** > **Integration Services**.
  2. Im Fenster **Integration Services** stellen Sie sicher, dass das Kontrollkästchen **Gastdienste** ausgewählt ist.
- Geben Sie als Administrator die folgenden Befehle bei einer PowerShell-Eingabeaufforderung aus:

```
Get-VMIntegrationService -VMName Kingston40
Enable-VMIntegrationService -VMName Kingston40 -Name "Schnittstelle für Gastdienste"
```

Informationen zu diesem Vorgang

Data Protection for Microsoft Hyper-V stellt Anwendungskonsistenz zur Verfügung, wenn Sie VMs sichern, die Microsoft SQL Server hosten. Mit diesen Sicherungen können Sie die VM in einem konsistenten Zustand wiederherstellen.

Sollen aus diesem Sicherungstyp nur ausgewählte Datenbanken zurückgeschrieben werden, ohne dass die gesamte VM wiederhergestellt werden muss, müssen zum Zeitpunkt der VM-Momentaufnahme und -Sicherung Informationen zum Zustand des Microsoft SQL Servers aufbewahrt werden. Diese Informationen werden im Rahmen der Interaktionen von Microsoft Volume Shadow Copy Services (VSS) erfasst, die während einer VM-Momentaufnahme ausgeführt werden.

Damit Data Protection for Microsoft Hyper-V die Microsoft VSS-Metadaten für Microsoft SQL Server erfasst, müssen Sie Data Protection for Microsoft Hyper-V so konfigurieren, dass diese Informationen während Sicherungsoperationen von der VM abgerufen werden.

Vorgehensweise

Führen Sie die folgenden Schritte auf dem Hyper-V-Host oder -Cluster aus:

1. Vom Ordner baclient aus definieren Sie die Windows-Berechtigungsnachweise für die Gast-VM, die Microsoft SQL Server hostet:
   - Zum Definieren von Berechtigungsnachweisen für eine bestimmte VM geben Sie den folgenden Befehl im Ordner baclient bei der Eingabeaufforderung aus:

     ```
     dsmc set password -type=vmguest Name_der_Gast-VM "Admin-ID_der_Gastmaschine" Admin-Kennwort_
     -optfile=dsm.Hostname_HV_DM.opt
     ```

   - Zum Definieren von Berechtigungsnachweisen für alle VMs, für die keine speziellen Berechtigungsnachweise definiert sind, geben Sie den folgenden Befehl aus:

     ```
     dsmc set password -type=vmguest allvm "Admin-ID_der_Gastmaschine" Admin-Kennwort_der_Gastmas
     -optfile=dsm.Hostname_HV_DM.opt
     ```

   Hierbei gilt Folgendes:

   VM-Name
   Der Name der Gast-VM, die Microsoft SQL Server hostet. Der Name ist der VM-Name, der im Hyper-V-Manager angezeigt wird.

   Admin-ID_der_Gastmaschine
   Die Administrator-ID für die Gast-VM. Die *Admin-ID_der_Gastmaschine* kann ein Windows-Domänenkonto oder ein lokales Konto sein. Beispiel:
   - Verwenden Sie für ein Domänenkonto das Format *Domäne\Benutzername*.
   - Verwenden Sie für ein lokales Konto das Format *Benutzername*.

   Admin-Kennwort_der_Gastmaschine
   Das Kennwort für die Administrator-ID für die Gast-VM.

   Hostname
   Der Name des Hyper-V-Hosts oder -Clusters.

   Beispiel:

   ```
   dsmc set password -type=vmguest Kingston40 "world\alan" "@lanPwd!"
   -optfile=dsm.KINGSTON5_HV_DM.opt
   ```

   Die Konten, die im Befehl **set password** verwendet werden, müssen sowohl auf dem Hyper-V-Host oder -Cluster als auch auf der Gast-VM gültig sein, die SQL Server-Daten hostet.

   Einschränkung: Die Anmeldeberechtigungsnachweise (Benutzername und Kennwort) für die Gast-VM müssen mit den Berechtigungsnachweisen für den Hyper-V-Host übereinstimmen.

   Mit dem Befehl **dsmc set password** werden die Berechtigungsnachweise der Gast-VM verschlüsselt auf dem System gespeichert, auf dem sich die Einheit zum Versetzen von Daten befindet. Für die Administrator-ID und das Kennwort der Gast-VM sind die folgenden Mindestberechtigungen erforderlich:

   Sicherungsberechtigungen
   Benutzer mit der Datenbankrolle db_backupoperator haben die Berechtigung zum Ausführen der eigenständigen Anwendungsdatensicherung. Gehört der Benutzer zu der festen Serverrolle sysadmin von SQL Server, kann er alle Datenbanken der Microsoft SQL Server-Instanz sichern. Der Benutzer kann außerdem die Datenbanken sichern, deren Eigner er ist, auch wenn er nicht über Sicherungsberechtigungen für eine bestimmte Datenbank verfügt. Der Benutzer der Gast-VM muss die Berechtigung besitzen, Volumeschattenkopien zu erstellen und SQL Server-Protokolle abzuschneiden.

Zurückschreibungsberechtigungen

Wenn die Datenbank vorhanden ist, können Sie die Zurückschreibungsoperation ausführen, wenn Sie zu der festen Serverrolle `dbcreator` gehören oder wenn Sie der Eigner der Datenbank sind. Benutzer mit der festen Serverrolle sysadmin für Microsoft SQL Server verfügen über die Berechtigung zum Zurückschreiben einer Datenbank aus beliebigen Sicherungssätzen. Bei anderen Benutzern ist die Berechtigung davon abhängig, ob die Datenbank vorhanden ist.

2. Vom Ordner `baclient` aus konfigurieren Sie die Optionsdatei der Einheit zum Versetzen von Daten für Anwendungsschutz:
   a. Öffnen Sie die Optionsdatei der Einheit zum Versetzen von Daten (`dsm.`*`Hostname`*`_HV_DM.opt`) zum Editieren. Geben Sie beispielsweise den folgenden Befehl aus:

      ```
      notepad dsm.KINGSTON5_HV_DM.opt
      ```

   b. Fügen Sie die Option `include.vmtsmvss` *Name_der_Gast-VM* hinzu. Der Parameter *Name_der_Gast-VM* kann Platzhalterzeichen enthalten. Beispiel:

      ```
      include.vmtsmvss Kingston40
      ```

      Wenn Sie alternativ planen, die SQL Server-Protokolle manuell beizubehalten und die SQL Server-Transaktionen nach der Zurückschreibung der VM bis zu einem bestimmten Prüfpunkt zurückzuschreiben, geben Sie die folgenden Optionen an, um das SQL Server-Protokoll nicht abzuschneiden:

      ```
      include.vmtsmvss Kingston40 OPTions=KEEPSqllog
      ```

3. Vom Ordner `baclient` aus sichern Sie die Gast-VM, indem Sie den Befehl **dsmc backup vm** ausgeben: Beispiel:

   ```
   dsmc backup vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt
   -asnode=KINGSTON5_HV_TGT
   ```

4. Überprüfen Sie die Sicherungsoperation, indem Sie den Befehl **dsmc query vm** ausführen. Bei VM-Namen muss die Groß-/Kleinschreibung beachtet werden.

   Geben Sie beispielsweise den folgenden Befehl im Ordner `baclient` aus:

   ```
   dsmc query vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt
   -asnode=KINGSTON5_HV_TGT -detail
   ```

   Die Ausgabe umfasst einen ähnlichen Text wie in dem folgenden Beispiel (möglicherweise ist bei Ihnen jedoch eine andere Version von Microsoft SQL Server installiert):

   ```
   Art des Anwendungsschutzes: TSM VSS
   Geschützte Anwendung(en): Microsoft SQL Server 2017
   ```

5. Vom Ordner `baclient` aus verwenden Sie den Befehl **dsmc set access**, um dem VSS-Knoten auf der Gast-VM den Zugriff auf die VM-Sicherung und ihre Zurückschreibung zu gestatten. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   dsmc set access backup -type=vm Kingston40 kingston40_vss
   -nodename=KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
   ```

   Geben Sie den folgenden Befehl **dsmc query access** aus, um die VM-Sicherungen anzuzeigen, auf die der Knoten Zugriff hat. Beispiel:

   ```
   dsmc query access -nodename=KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
   ```

Nächste Schritte

Wenn die Sicherungsoperation erfolgreich ausgeführt wurde, fahren Sie mit „Schritt 4 (Gast-VM): Datenbank zurückschreiben" auf Seite 131 fort.

Zugehörige Verweise:

„**Backup VM**" auf Seite 166
„INCLUDE.VMTSMVSS" auf Seite 194

Zugehörige Informationen:

Set Access

Set Password

Schritt 4 (Gast-VM): Datenbank zurückschreiben

Schreiben Sie eine Datenbank mit Data Protection for Microsoft SQL Server zurück, um zu überprüfen, ob Sie den Anwendungsschutz korrekt konfiguriert haben.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Prozedur in „Schritt 3 (Hyper-V-Host): Data Protection for Microsoft Hyper-V für Anwendungsschutz konfigurieren" auf Seite 128 ausgeführt haben.

Stellen Sie sicher, dass die erforderlichen Services auf der Gast-VM (VM = virtuelle Maschine) aktiv sind:

1. Bei der Eingabeaufforderung geben Sie den folgenden Befehl aus:
   ```
   services.msc
   ```
2. Lokalisieren Sie den **IBM Spectrum Protect Recovery Agent-Service** in der Liste der Services und starten Sie den Service bei Bedarf.
3. Lokalisieren Sie den **Microsoft iSCSI-Initiator-Dienst** in der Liste der Services. Gegebenenfalls ändern Sie den Starttyp in **Automatisch** und starten Sie den Service.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Gast-VM aus:

1. Starten Sie die Data Protection for Microsoft SQL Server-Verwaltungskonsole.
2. Wählen Sie eine **SQL Server**-Instanz in der Baumstruktur aus.
3. Rufen Sie die Registerkarte **Wiederherstellen** auf und klicken Sie auf **Aktualisieren**.
4. Wählen Sie einen Datenbankeintrag mit der Sicherungsmethode **VMVSS** aus.
5. Klicken Sie im Fenster **Aktionen** auf **An alternative Position zurückschreiben**. Geben Sie einen neuen Datenbanknamen und eine neue Position für die Zurückschreibung der Datenbank an.
6. Klicken Sie im Fenster **Aktionen** auf **Zurückschreiben**.
7. Wenn die Zurückschreibungsoperation beendet ist, überprüfen Sie die Datenbank und eventuelle zugehörige Tabellen.

Nächste Schritte

Sie können jetzt Sicherungen verwalten und bei Bedarf Daten wiederherstellen. Weitere Informationen siehe:

- „Sicherungsoperationen verwalten" auf Seite 133
- „Daten zurückschreiben" auf Seite 137

Wenn Sie den Namen der Gast-VM ändern, nachdem Sie die Konfigurationsschritte für Anwendungsschutz ausgeführt haben, müssen Sie die Software mit dem neuen VM-Namen neu konfigurieren. Anweisungen finden Sie in „Optional: Anwen-

dungsschutz nach einer Namensänderung der virtuellen Maschine konfigurieren".

Optional: Anwendungsschutz nach einer Namensänderung der virtuellen Maschine konfigurieren

Wenn Sie den Namen der Gast-VM (VM = virtuelle Maschine) geändert haben, nachdem Sie die Anwendungsschutzkonfiguration ausgeführt haben, müssen Sie Data Protection for Microsoft Hyper-V mit der umbenannten Gast-VM neu konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die Software installiert und für den Schutz von Gast-VMs konfiguriert haben, die Microsoft SQL Server hosten.

Informationen zu diesem Vorgang

Führen Sie diese Task nur aus, wenn Sie den Namen einer Gast-VM geändert haben, die durch Anwendungsschutz geschützt ist.

Vorgehensweise

1. Geben Sie auf der Einheit zum Versetzen von Daten auf dem Hyper-V-Host oder -Cluster den folgenden Befehl aus:

   ```
   dsmc set password –type=vmguest neuer_Anzeigename_der_VM-Gastmaschine Admin-ID_der_Gastmaschine
   Admin-Kennwort_der_Gastmaschine
   ```

   Hierbei gilt Folgendes:

   neuer_Anzeigename_der_VM-Gastmaschine
   Der Name der neuen Gast-VM, die Microsoft SQL Server hostet. Der Name ist der VM-Name, der im Hyper-V-Manager angezeigt wird.

   Admin-ID_der_Gastmaschine
   Die Administrator-ID für die neue Gast-VM. *Admin-ID_der_Gastmaschine* muss ein Windows-Domänenkonto oder ein lokales Konto sein. Beispiel:

   - Verwenden Sie für ein Domänenkonto das Format *Domäne\Benutzername*.
   - Verwenden Sie für ein lokales Konto das Format *Benutzername*.

   Admin-Kennwort_der_Gastmaschine
   Das Kennwort für die Administrator-ID für die neue Gast-VM.

2. Aktualisieren Sie in der Optionsdatei der Einheit zum Versetzen von Daten (`dsm.`*`Hostname`*`_HV_DM.opt`) die Option `include.vmtsmvss` wie folgt:

   ```
   include.vmtsmvss neuer_Anzeigename_der_VM-Gastmaschine
   ```

   Dabei ist *neuer_Anzeigename_der_VM-Gastmaschine* der Anzeigename der neuen Gast-VM im Hyper-V-Manager. Sie können Platzhalterzeichen verwenden.

3. Vom Ordner `baclient` auf der Einheit zum Versetzen von Daten aus sichern Sie die neue Gast-VM, indem Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole verwenden oder den folgenden Befehl bei der Eingabeaufforderung ausgeben:

   ```
   dsmc backup vm neuer_Anzeigename_der_VM-Gastmaschine -optfile=dsm.Hostname_HV_DM.opt
   -asnode=Hostname_HV_TGT
   ```

4. Vom Ordner `baclient` aus verwenden Sie den Befehl **`dsmc set access`**, um dem VSS-Knoten auf der neuen Gast-VM den Zugriff auf die VM-Sicherung und ihre Zurückschreibung zu gestatten. Geben Sie beispielsweise den folgenden Befehl aus:

```
dsmc set access backup –type=VM neuer_Anzeigename_der_VM-Gastmaschine VSS-Anfordererknoten
-optfile=dsm.Hostname_HV_DM.opt
```

Hierbei gilt Folgendes:

neuer_Anzeigename_der_VM-Gastmaschine
Der Anzeigename der neuen Gast-VM im Hyper-V-Manager.

VSS-Anfordererknoten
Der Name des VSS-Anforderers, der in Data Protection for Microsoft SQL Server konfiguriert wurde.

Hostname
Der Name des Hyper-V-Hosts oder -Clusters, auf dem Data Protection for Microsoft Hyper-V installiert ist.

5. Optional: Da der VSS-Anfordererknoten bereits Zugriff auf die VMs hat, die unter dem alten VM-Namen gesichert wurden, werden in der Data Protection for Microsoft SQL Server-Verwaltungskonsole die VMVSS-Datenbanken angezeigt, die für die alte VM und die neue VM gesichert wurden.

   Wenn Sie nicht möchten, dass Zugriff auf die VM-Sicherungen mit dem alten VM-Namen besteht, müssen Sie den Zugriff auf die alten VM-Sicherungen löschen. Geben Sie den folgenden Befehl auf der Einheit zum Versetzen von Daten auf dem Hyper-V-Host aus:

   ```
   dsmc del access -optfile=dsm.Hostname_HV_DM.opt -asnode=Hostname_HV_TGT
   ```

   Eine Zugriffsliste wird angezeigt. Geben Sie den Index für den Eintrag an, der aus der Zugriffsliste gelöscht werden soll.

   Wenn Sie Speicherbereich auf dem IBM Spectrum Protect-Server einsparen wollen, können Sie den Dateibereich löschen, der die Sicherungsdaten für die alte VM enthält. Geben Sie dazu den Befehl **dsmc delete filespace** aus.

   Wichtig: Wenn Sie einen Dateibereich löschen, werden alle Sicherungsversionen in diesem Dateibereich gelöscht und die Daten können nicht mehr zurückgeschrieben werden. Stellen Sie sicher, dass die alten VM-Sicherungen veraltet sind, bevor Sie sie löschen.

Sicherungsoperationen verwalten

Nachdem Sie die Umgebung für den Schutz von Microsoft SQL Server-Daten konfiguriert haben, können Sie Sicherungen planen. Sie können Zeitpläne für eine Operation zur Sicherung von virtuellen Maschinen (VMs) und eine Operation zur Sicherung von Microsoft SQL Server-Protokollen definieren.

Sicherungen virtueller Maschinen planen

Planen Sie Sicherungen virtueller Maschinen (VMs), damit sichergestellt ist, dass Ihre Daten regelmäßig geschützt werden.

Vorbereitende Schritte

Standardmäßig beträgt die maximale Größe, die für eine virtuelle Festplatte (VHDX) bei einer Sicherungsoperation zulässig ist, 2 TB. Mit der Option `vmmaxvirtualdisks` können Sie die maximale Größe jedoch auf 8 TB erweitern. Weitere Informationen finden Sie in „Vmmaxvirtualdisks" auf Seite 213.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft Hyper-V-Verwaltungskonsole.

2. Klicken Sie im Navigationsfenster auf einen eigenständigen Host oder einen Cluster.
3. Klicken Sie im Fenster **Aktionen** auf **Sicherungsmanagement**.
4. Wählen Sie einen Zeitplan im Fenster **Sicherungsmanagement** aus und klicken Sie auf **Zeitplan zuordnen**.
5. Zum Schließen des Fensters klicken Sie auf **Schließen**.
6. Stellen Sie sicher, dass die Quelle für den Zeitplan die VMs umfasst, die Microsoft SQL Server hosten.
7. Stellen Sie sicher, dass einer der folgenden Services aktiv ist:
   - Wenn Sie einen Scheduler verwenden, der von einem Clientakzeptor (CAD) verwaltet wird, stellen Sie sicher, dass der Clientakzeptorservice auf der Einheit zum Versetzen von Daten aktiv ist.
   - Wenn Sie einen eigenständigen Scheduler verwenden, stellen Sie sicher, dass der Scheduler-Service aktiv ist.

Microsoft SQL Server-Protokollsicherungen planen

Nachdem der Zeitplan für die Sicherung der virtuellen Maschine erstellt wurde, können Sie den Zeitplan für die Microsoft SQL Server-Protokollsicherung erstellen.

Informationen zu diesem Vorgang

Durch die Sicherung von SQL Server-Protokollen wird ein differenzierteres Niveau von Wiederherstellungspunkten zur Verfügung gestellt. Möglicherweise ist die Sicherung von SQL Server-Protokollen für Sie nicht erforderlich, wenn Sie aufgrund der Häufigkeit Ihrer Sicherungen über genügend Wiederherstellungspunkte verfügen, und unter der Voraussetzung, dass Sie für die Sicherung nicht die Option `INCLUDE.VMTSMVSS VM-Anzeigename OPTions=KEEPSqllog` angegeben haben.

Vorgehensweise

1. Starten Sie die Data Protection for Microsoft SQL Server-Benutzerschnittstelle von der virtuellen Maschine (VM) aus, die Microsoft SQL Server hostet.
2. Im Navigationsfenster erweitern Sie den Knoten **Verwalten**.
3. Unter dem Knoten **Verwalten** klicken Sie mit der rechten Maustaste auf **Zeitplanung** > **Planungsassistent**.
4. Öffnen Sie den **Planungsassistenten**, um den Zeitplannamen und die Planzeit anzugeben.
5. Auf der Seite **Geplante Task definieren** wählen Sie **Befehlszeile** aus.
6. Klicken Sie auf das Symbol, um die SQL Server-Schablone auszuwählen. Klicken Sie auf **Weiter**.
7. Verwenden Sie die Befehlszeilenschnittstelle und die SQL Server-Schablone, um die Datenbankprotokollsicherung anzugeben, beispielsweise wie folgt:

   ```
   tdpsqlc backup * log /truncate=yes 2>&1
   ```

   Tipp: Sie können Microsoft SQL Server-Sicherungen auch mithilfe des zentralen Zeitplanungsservice von IBM Spectrum Protect planen. Mit diesem Service können Sie einen Sicherungszeitplan für alle Microsoft SQL Server-Instanzen auf einer VM erstellen.

Sicherungen überprüfen

Nachdem Sie eine Sicherung erstellt haben, überprüfen Sie, ob Sie die Sicherungen virtueller Maschinen und die Datenbanksicherungen über die Data Protection for Microsoft SQL Server-Schnittstelle abfragen können.

Vorgehensweise

1. In der Microsoft Management Console (MMC) wählen Sie einen Microsoft SQL Server aus.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**.
3. Wählen Sie **Anzeigen** > **Datenbanken** aus. Eine Liste der Microsoft SQL Server-Datenbanken, die zurückgeschrieben werden können, wird angezeigt.

   Für Microsoft SQL Server-Datenbanken, die mit Data Protection for Microsoft Hyper-V gesichert werden, ist die Sicherungsmethode `vmvss` angegeben.

   Für Microsoft SQL Server-Protokolle, die mit Data Protection for Microsoft SQL Server gesichert werden, ist die Sicherungsmethode `Legacy` angegeben.

Versionen von Sicherungen verwalten

Mithilfe von Data Protection for Microsoft SQL Server können Sie den Verfall von Sicherungen verwalten. Sie können die Anzahl der aufzubewahrenden Momentaufnahmen und den Aufbewahrungszeitraum für Momentaufnahmen angeben.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Aufbewahrung für Microsoft SQL Server-Sicherungen zu definieren. Bei dieser Prozedur wird vorausgesetzt, dass Sicherungen 30 Tage lang aufbewahrt werden sollen.

Vorgehensweise

1. Definieren Sie die Aufbewahrungsparameter in der Verwaltungsklasse, die für Sicherungen virtueller Maschinen (VMs) verwendet wird. Beispiel:

   ```
   Extraversionen aufbewahren = 30
   Einzige Version aufbewahren = 30
   Versionen bestehender Daten = nolimit
   Versionen gelöschter Daten = nolimit
   ```

   Verwenden Sie die Option `vmmc` in der Optionsdatei der Einheit zum Versetzen von Daten, um die Verwaltungsklasse anzugeben, die für VM-Sicherungen verwendet wird.

   Geplante VM-Sicherungen sind Data Protection for Microsoft Hyper-V zugeordnet.
2. Definieren Sie die Aufbewahrungsparameter in der Verwaltungsklasse, die für Microsoft SQL Server-Sicherungen verwendet wird. Beispiel:

   ```
   Extraversionen aufbewahren = 0
   Einzige Version aufbewahren = 1
   Versionen bestehender Daten = nolimit
   Versionen gelöschter Daten = nolimit
   ```

   Geben Sie die Verwaltungsklasse für die Microsoft SQL Server-Sicherungen in der Datei `dsm.opt` an, die vom Data Protection for Microsoft SQL Server-Agenten verwendet wird. Siehe hierzu die folgenden `INCLUDE`-Optionen:

   ```
   INCLUDE *:\...\*log Name_der_Verwaltungsklasse
   INCLUDE *:\...\log\..\* Name_der_Verwaltungsklasse
   ```

3. Während Data Protection for Microsoft SQL Server auf der VM ausgeführt wird, geben Sie den Befehl **inactivate** aus, um explizit alle aktiven Protokollsicherungen für alle Datenbanken auf dem Microsoft SQL Server zu inaktivieren. Beispiel:

   ```
   tdpsqlc inactivate * log=* /OLDERTHAN=30
   ```

   Von Data Protection for Microsoft SQL Server erstellte Protokollsicherungen müssen explizit inaktiviert werden, da die vollständigen Datenbanksicherungen von Data Protection for Microsoft Hyper-V ausgeführt werden. Diese Konfiguration umfasst eine eintägige Karenzzeit nach der Inaktivierung der Microsoft SQL Server-Protokollsicherungen, bevor der IBM Spectrum Protect-Server die Sicherungen löscht.

   Tipp: Sie können Protokollsicherungen nur auf dem Server aufbewahren, wenn die zugehörigen vollständigen Datenbanksicherungen aufbewahrt werden. Setzen Sie in der Verwaltungsklasse den Wert für **RETONLY** für Protokollsicherungen auf den gleichen Wert wie den Parameter **RETEXTRA** für vollständige Datenbanksicherungen.

Sicherstellen, dass Microsoft SQL Server-Datenträger bei Sicherungen virtueller Maschinen nicht ausgeschlossen sind

Die Datenträger auf virtuellen Hyper-V-Festplatten (VHDXs) müssen die Microsoft SQL Server-Datenbanken enthalten, die nicht bei der Data Protection for Microsoft Hyper-V-Sicherungsverarbeitung ausgeschlossen sind.

Vorbereitende Schritte

Stellen Sie sicher, dass die Datenbanken sich nicht auf den folgenden Plattentypen befinden:

- Physischen Platten
- Unabhängigen Platten
- Platten, die über iSCSI direkt an das Gastbetriebssystem angeschlossen sind

Vorgehensweise

1. Stellen Sie sicher, dass eventuell vorhandene Anweisungen `EXCLUDE.VMDISK` auf der Data Protection for Microsoft Hyper-V-Einheit zum Versetzen von Daten, die zum Sichern der virtuellen Maschine (VM) verwendet wird, nicht versehentlich VHDXs ausschließen, die Datenträger mit Microsoft SQL Server-Dateien, -Dateibereichen und -Datenbanken enthalten.

   Beispiel:

   - `kingston40.vhdx` enthält den logischen Datenträger `C:`.
   - `kingston40.vhdx` enthält die logischen Datenträger `E:` und F:.
   - Die Plattenposition (IDE-Controllernummer und Einheitenposition) für `kingston40_1.vhdx` ist `IDE 1 0`.
   - Die Plattenposition für `kingston40_2.vhdx` ist `IDE 1 1`.
   - Die zu sichernden Microsoft SQL Server-Datenbankdateien befinden sich auf den Laufwerken `E:` und `F:`.

2. Vergewissern Sie sich, dass in keiner Anweisung `kingston40_2.vhdx` bei der VM-Sicherung ausgeschlossen wird, indem Sie sicherstellen, dass die Einheit zum Versetzen von Daten nicht die folgenden oder ähnliche Anweisungen enthält:

   ```
   EXCLUDE.VMDISK KINGSTON40 "IDE 1 1"EXCLUDE.VMDISK * "IDE 1 1"
   ```

Wenn Sie alternativ die meisten Festplatten ausschließen, müssen Sie die VM-Platten explizit einschließen, indem Sie eine der folgenden Anweisungen verwenden:

```
INCLUDE.VMDISK KINGSTON40 "IDE 1 1"INCLUDE.VMDISK * "IDE 1 1"
```

Einschluss- und Ausschlussanweisungen werden in der Reihenfolge, in der sie in der Datei `dsm.opt` angezeigt werden, von unten nach oben verarbeitet. Geben Sie die Anweisungen in der richtigen Reihenfolge ein, um das gewünschte Ziel zu erreichen.

Sie können den Ausschluss und Einschluss einer VM-Platte über die Befehlszeilenschnittstelle angeben:

```
dsmc backup vm „KINGSTON40:-vmdisk=IDE 1 1" -asnode=KINGSTON5_HV_TGT
```

Zugehörige Verweise:

„Exclude.vmdisk" auf Seite 186

„Include.vmdisk" auf Seite 191

Daten zurückschreiben

Nachdem Sie eine virtuelle Maschine mit aktiviertem Anwendungsschutz gesichert haben, können Sie eine Datenbank wiederherstellen, falls das ursprüngliche Objekt nicht mehr vorhanden oder beschädigt ist.

Mit einer Wiederherstellungsoperation wird eine vollständige Sicherung der Microsoft SQL Server-Datenbank aus der Data Protection for Microsoft Hyper-V-Sicherung zurückgeschrieben.

Wenn Sie die gesamte virtuelle Maschine (VM) zurückschreiben, werden alle Microsoft SQL Server-Datenbanken auf der VM zurückgeschrieben und mit dem Stand der VM-Sicherung wiederhergestellt. In diesem Szenario können Sie Sicherungen, die nach diesem Zeitpunkt erstellt wurden, weder zurückschreiben noch wiederherstellen.

Microsoft iSCSI-Initiator-Dienst starten

Mit dem iSCSI-Protokoll werden die Platten bereitgestellt, die für eine Wiederherstellungsoperation verwendet werden. Stellen Sie sicher, dass der Microsoft iSCSI-Initiator-Dienst gestartet ist und auf dem System, auf das die Daten zurückgeschrieben werden sollen, auf den Starttyp 'Automatisch' gesetzt ist.

Vorgehensweise

Führen Sie die folgenden Schritte im Windows-Fenster **Dienste** aus.

1. In der Liste **Dienste** klicken Sie mit der rechten Maustaste auf **Microsoft iSCSI-Initiator-Dienst**.
2. Klicken Sie auf **Eigenschaften**.
3. Definieren Sie auf der Registerkarte **Allgemein** die folgenden Optionen:
   a. Wählen Sie in der Liste **Starttyp** die Option **Automatisch** aus.
   b. Klicken Sie auf **Starten** und klicken Sie anschließend auf **OK**.

Ergebnisse

In der Liste **Dienste** wird für den **Microsoft iSCSI-Initiator-Dienst** der Status **Gestartet** und der Starttyp **Automatisch** angezeigt.

Datenbanksicherungen mithilfe der grafischen Benutzerschnittstelle zurückschreiben

Zum Wiederherstellen einer vollständigen Microsoft SQL Server-Datenbanksicherung aus einer Sicherung einer virtuellen Maschine (VM) können Sie die grafische Data Protection for Microsoft SQL Server-Benutzerschnittstelle verwenden.

Vorbereitende Schritte

Stellen Sie sicher, dass der Microsoft iSCSI-Initiator-Dienst aktiv ist, bevor Sie eine Microsoft SQL Server-Datenbank mit dem Sicherungstyp "VMVSS" zurückschreiben. Ist der Dienst nicht aktiv, starten Sie ihn. Anweisungen finden Sie in „Microsoft iSCSI-Initiator-Dienst starten" auf Seite 137.

Vorgehensweise

1. Zum Starten einer vollständigen Datenbankwiederherstellung aus einer VM starten Sie die Data Protection for Microsoft SQL Server Management Console (MMC).
2. Im Navigationsfenster erweitern Sie den Knoten **Daten schützen und wiederherstellen** und wählen Sie einen Microsoft SQL Server-Server aus.
3. Auf der Registerkarte **Wiederherstellen** wählen Sie **Datenbankzurückschreibung** aus. Alle Sicherungen einschließlich aller Datenbanksicherungen aus einer VM-Sicherung werden aufgelistet.
4. Wählen Sie eine vollständige Datenbanksicherung für die Zurückschreibung aus.
5. Klicken Sie im Fenster **Aktionen** auf **Zurückschreiben**.

Daten mithilfe der Befehlszeilenschnittstelle zurückschreiben

Wenn Sie die Data Protection for Microsoft SQL Server-Befehlszeilenschnittstelle bevorzugen, können Sie diese verwenden, um eine vollständige Wiederherstellung einer Microsoft SQL Server-Datenbank aus einer virtuellen Maschine (VM) zu starten.

Vorbereitende Schritte

Stellen Sie sicher, dass der Microsoft iSCSI-Initiator-Dienst aktiv ist, bevor Sie eine Microsoft SQL Server-Datenbank mit dem Sicherungstyp "VMVSS" zurückschreiben. Ist der Dienst nicht aktiv, starten Sie ihn. Anweisungen finden Sie in „Microsoft iSCSI-Initiator-Dienst starten" auf Seite 137.

Vorgehensweise

1. Geben Sie den Befehl **query** aus, um die vollständigen Datenbanksicherungen und Protokollsicherungen abzufragen. In dem folgenden Beispiel werden alle Sicherungen für die Microsoft SQL Server-Datenbank mit dem Namen `sql_db10` abgefragt.

```
tdpsqlc q tsm sql_db10

IBM Spectrum Protect for Databases:
Data Protection for Microsoft SQL Server
Version 8, Release 1, Stufe 6.0
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.

Verbindung zu IBM Spectrum Protect-Server als Knoten 'KINGSTON40_SQL' wird hergestellt...

IBM Spectrum Protect-Server wird nach Sicherungen abgefragt....

Angaben zum Sicherungsobjekt
-------------------------

SQL Server-Name   ..................... SQL40
SQL-Datenbankname ..................... sql_db10
Sicherungsmethode ..................... VMVSS
Sicherungsposition..................... Srv
Sicherungsobjekttyp.................... Vollständig
Stammverzeichnis für Mountpunkte .........
Status des Sicherungsobjekts ............. Aktiv
Datum/Zeit der Sicherungserstellung ...... 12.07.2018 13:08:45
Sicherungsgröße ....................... 17,00 MB
Sicherung komprimiert..................... Ja
Verschlüsselungstyp der Sicherung......... Keiner
Sicherung clientseitig dedupliziert....... Ja
Sicherung unterstützt Sofortzurückschreib. Nein
Name des Datenbankobjekts ................ 20180712130845
Zugeordnete Verwaltungsklasse ............ STANDARD
Sicherung geändert.....................


Die Operation wurde erfolgreich ausgeführt. (rc = 0)
```

2. Zum Zurückschreiben der Datenbank ohne Anwenden der Transaktionsprotokolle geben Sie den folgenden Befehl aus:

   `tdpsqlc restore` *`Datenbankname`* `/backupMethod=vmvss`

   Das folgende Beispiel zeigt die Ausgabe des Befehls, wenn Sie die Microsoft SQL Server-Datenbank mit dem Namen `sql_db10` angeben.

```
tdpsqlc restore sql_db10 /backupmethod=vmvss /sqlserver=sql40
/fromsqlserver=sql40 /recovery=no

IBM Spectrum Protect for Databases:
Data Protection for Microsoft SQL Server
Version 8, Release 1, Stufe 6.0
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.

Verbindung zu SQL Server wird hergestellt, bitte warten...

IBM Spectrum Protect-Server wird nach Sicherungen abgefragt....

Verbindung zu IBM Spectrum Protect-Server als Knoten 'KINGSTON40_SQL' wird hergestellt...
Verbindung zum lokalen DSM-Agenten 'SQL40' wird hergestellt...
Ausweichknoten 'KINGSTON40_SQL' wird verwendet...
SQL-Datenbankzurückschreibung wird gestartet...

Beginn der VSS-Zurückschreibung von 'sql_db10'...

'sql_db10' wird über Kopie auf Dateiebene aus Momentaufnahme(n) zurückgeschrieben. Dieser
 Prozess kann einige Zeit dauern. Bitte warten

Geprüfte/Abgeschlossene/Fehlgeschlagene Dateien: [ 2 / 2 / 0 ] Gesamtsumme Byte: 3146070

VSS-Zurückschreibungsoperation mit RC = 0 beendet
 Geprüfte Dateien : 2
 Beendete Dateien : 2
 Fehlgeschlagene Dateien : 0
 Gesamtsumme Byte : 3146070
 Gesamtsumme LAN-unabhängiger Byte : 0

Die Operation wurde erfolgreich ausgeführt. (rc = 0)
```

3. Nachdem die Operation für die vollständige Datenbankzurückschreibung erfolgreich ausgeführt wurde, geben Sie den Befehl zum Zurückschreiben der Protokolle aus. Sollen beispielsweise alle Protokolle auf der Basis der zurückgeschriebenen Microsoft SQL-Datenbank `sql_db10` zurückgeschrieben werden, geben Sie den folgenden Befehl aus.

   ```
   tdpsqlc restore databasename log=* /sqlsever=sql40 /fromserver=sql40
   /recovery=yes
   ```

   Sie können auch die Option `/stopat` verwenden, um einen differenzierteren Zeitpunkt anzugeben.

```
tdpsqlc restore sql_db10 log=* /sqlserver=sql40
/fromsqlserver=sql40 /recovery=yes


IBM Spectrum Protect for Databases:
Data Protection for Microsoft SQL Server
Version 8, Release 1, Stufe 6.0
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.

Verbindung zu SQL Server wird hergestellt, bitte warten...
SQL-Datenbankzurückschreibung wird gestartet...
Verbindung zu IBM Spectrum Protect-Server als Knoten 'KINGSTON40_SQL' wird hergestellt...
IBM Spectrum Protect-Server wird nach einer Liste
der Datenbanksicherungen abgefragt, bitte warten...

Beginn der Protokollzurückschreibung von Sicherungsobjekt sql_db10\20180712130845\00000DB0,
1 von 3, in Datenbank sql_db10 ...

Beginn der Protokollzurückschreibung von Sicherungsobjekt sql_db10\20180712130845\00000DB0,
2 von 3, in Datenbank sql_db10 ....

Geprüfte Datenbanksicherungen: 3
Für Zurückschreibung angeforderte DB-Sicherungen: 3
Zurückgeschriebene Datenbanksicherungen: 3
Übersprungene Datenbanksicherungen: 0
Durchsatzrate: 134,32 Kb/Sek
Übertragene Byte: 385.536
Übertragene LAN-unabhängige Byte: 0
Abgelaufene Verarbeitungszeit: 2,80 Sek.
Die Operation wurde erfolgreich ausgeführt. (rc = 0)
```

Nächste Schritte

Sie können inaktive Sicherungen über die Data Protection for Microsoft SQL Server-Befehlszeilenschnittstelle mit dem Befehl **TDPSQLC** zurückschreiben. Bei der Ausgabe des Befehls **restore** geben Sie den Datenbankobjektnamen für die jeweilige Sicherung an.

Zum Abrufen des Datenbankobjektnamens geben Sie den folgenden Befehl aus:

```
tdpsqlc q tsm DB-Name full /all
```

Wenn Sie über den Wert für den Datenbankobjektnamen verfügen, geben Sie den Datenbankobjektnamen im Parameter */OBJect=Objektname* des Befehls **TDPSQLC restore** an, wobei *Objektname* der Datenbankobjektname ist. Beispiel:

```
tdpsqlc restore db44 /object=20180712130845 /backupdestination=tsm
 /backupmethod=vmvss
```

Microsoft SQL Server-Protokollsicherungen zurückschreiben

Nachdem die vollständige Datenbank erfolgreich zurückgeschrieben wurde, können Sie Data Protection for Microsoft SQL Server verwenden, um Transaktionsprotokolle zurückzuschreiben.

Vorgehensweise

Führen Sie die folgenden Schritte auf der Gast-VM aus:

1. Starten Sie die Microsoft Management Console (MMC) für Data Protection for Microsoft SQL Server.
2. Wählen Sie einen Microsoft SQL Server aus und klicken Sie auf die Registerkarte **Wiederherstellen**.
3. Stellen Sie sicher, dass die Option **Automatische Auswahl** auf Falsch gesetzt ist.

4. Ändern Sie die Option **Wiederherstellung ausführen** in `Wahr`.
5. Wählen Sie die Protokolle aus, die wiederhergestellt werden sollen.
6. Klicken Sie auf **Zurückschreiben**.

Verlagerte und gelöschte Datenbanken zurückschreiben

Für die Sicherungslösung zum Zurückschreiben von Datenbanken und Protokolldateien, die nach einer Sicherung einer virtuellen Maschine (VM) verlagert und gelöscht wurden, sind Data Protection for Microsoft Hyper-V und Data Protection for Microsoft SQL Server erforderlich.

Vorbereitende Schritte

Entscheiden Sie, wo die Datenbank- und Protokolldateidaten zurückgeschrieben werden sollen.

Informationen zu diesem Vorgang

Wenn Sie die Sicherungen zurückschreiben und eine Operation für die vollständige Datenbankzurückschreibung aus der Sicherung ausführen, schreibt Data Protection for Microsoft Hyper-V die Dateien an ihre ursprüngliche Position zurück.

Wurden Datenbank- oder Protokolldateien während des Sicherungszyklus verlagert, schreibt Data Protection for Microsoft SQL Server die Dateien an ihre ursprüngliche Position zurück.

Wurden während des Sicherungszyklus Datenbanken oder Protokolldateien erstellt, erstellt Data Protection for Microsoft SQL Server die neuen Dateien erneut. Wurden während des Sicherungszyklus Datenbank- oder Protokolldateien gelöscht, werden diese Dateien nicht zurückgeschrieben.

Vorgehensweise

1. Verwenden Sie Data Protection for Microsoft Hyper-V, um die VM zu sichern. Betrachten Sie das folgende Beispiel.

   Sie sichern um 14 Uhr die VM `kingston40`, die die Microsoft SQL Server-Datenbank `moose` enthält. Um 14 Uhr besteht die Microsoft SQL Server-Datenbank aus den folgenden Dateien:

   - `C:\sqldbs\moose\moose.mdf`
   - `C:\sqldbs\moose\moose_log.ldf`
2. Verlagern Sie eine Datenbanksicherung an eine alternative Position. Betrachten Sie das folgende Beispiel. Sie möchten die Datenbank `moose` um 18 Uhr an die folgende Position verlagern:
   - `E:\sqldbs\moose\moose.mdf`
   - `F:\sqldbs\moose\moose_log.ldf`
3. Fügen Sie der Datenbanksicherung Dateien hinzu. Betrachten Sie das folgende Beispiel. Sie möchten der Datenbank `moose` um 19 Uhr zwei neue Dateien hinzufügen. Die Datenbank besteht jetzt aus den folgenden Dateien:
   - `E:\sqldbs\moose\moose.mdf`
   - `F:\sqldbs\moose\moose_log.ldf`
   - `E:\sqldbs\moose\moose2.ndf`
   - `F:\sqldbs\moose\moose2_log.ldf`

4. Verwenden Sie Data Protection for Microsoft SQL Server, um eine Protokollsicherung auszuführen. Betrachten Sie das folgende Beispiel. Sie starten um 21 Uhr eine Protokollsicherung.
5. Schreiben Sie die Datenbanksicherung zurück. Betrachten Sie das folgende Beispiel.

   Sie möchten die gesamte Datenbank `moose` zurückschreiben.

   - Sie schreiben die gesamte Datenbank aus der Data Protection for Microsoft Hyper-V-Sicherung mit **runrecovery**=`false` zurück.
   - Um 21 Uhr schreiben Sie die Protokollsicherung zurück und wenden sie an.

   Die Datenbank `moose` wird an die folgende Position zurückgeschrieben:

   - `C:\sqldbs\moose\moose.mdf`
   - `C:\sqldbs\moose\moose_log.ldf`
   - `E:\sqldbs\moose\moose2.ndf`
   - `F:\sqldbs\moose\moose2_log.ldf`

   Bei der vollständigen VM-Zurückschreibung werden die Dateien an ihre ursprüngliche Position zurückgeschrieben. Bei der Anwendung der Protokollsicherung werden die Dateien zurückgeschrieben, die nach der Verlagerung hinzugefügt wurden.

Beispielscript zur Überprüfung von vollständigen Sicherungen virtueller Maschinen

Prüfen Sie vor dem Sichern von Microsoft SQL Server-Protokollen, ob Sie über eine gültige vollständige Sicherung der virtuellen Maschine (VM) verfügen. Eine der Prozeduren für die Prüfung auf das Vorhandensein einer vollständigen VM-Sicherung besteht darin, einen Zeitplan für die Ausführung eines Scripts zu erstellen.

Das folgende Beispielscript prüft, ob die Instanz einer vollständigen Sicherung vorhanden ist, und führt anschließend die Microsoft SQL Server-Protokollsicherungen aus, wenn eine vollständige VM-Sicherung vorhanden ist. Dieses Script kann mit einem Scheduler-Service wie dem IBM Spectrum Protect-Scheduler verwendet werden.

```
@echo off
dsmc q vm sql01_SQL -detail -asnode=datacenter01 | find /c
 „Wiederherstellung auf Datenbankebene" > c:\temp.txt
SET /p VAR=<c:\temp.txt

if %VAR% == „1" (
tdpsqlc back * log
) ELSE (
echo „Keine vollständige Sicherung vorhanden"
set ERRORLEVEL=1
)
```

Dieses Script generiert die folgende Ausgabe:

```
IBM Spectrum Protect for Databases:
Data Protection for Microsoft SQL Server
Version 8, Release 1, Stufe 6.0
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.

Verbindung zu SQL Server wird hergestellt, bitte warten...
SQL-Datenbanksicherung wird gestartet...
Verbindung zu IBM Spectrum Protect-Server als Knoten 'SQL01_SQL' wird hergestellt...
Ausweichknoten 'SQL01_SQL' wird verwendet...
ACO5458W Die Einstellung für 'backup delete' des IBM Spectrum Protect-Servers für Knoten (SQL01_SQL)
ist auf NO gesetzt. Damit die Operation ordnungsgemäß ausgeführt werden kann, muss diese Einstellung auf YES ges
Beginn der Protokollsicherung für Datenbankmodell, 1 von 2.
Gesamt: 0 Gelesen: 87808 Geschrieben: 87808 Rate: 32,54 KB/s
Name des Datenbankobjekts: 20180703011509\000007CC
Sicherung des Modells wurde erfolgreich ausgeführt.
Beginn der Protokollsicherung für Datenbank sqldb test2, 2 von 2.
Gesamt: 0 Gelesen: 88832 Geschrieben: 88832 Rate: 132,44 KB/s
Name des Datenbankobjekts: 20180703011511\000007CC
Sicherung von sqldb test2 wurde erfolgreich ausgeführt.
Ausgewählte SQL-Sicherungen: 4
Versuchte SQL-Sicherungen: 2
Beendete SQL-Sicherungen: 2
Ausgeschlossene SQL-Sicherungen: 2
Deduplizierte SQL-Datenbanken: 0
Durchsatzrate: 51,85 Kb/Sek
Gesamtzahl überprüfter Byte: 176.640
Gesamtzahl übertragener Byte: 176.640
Gesamtzahl übertragener LAN-unabhängiger Byte: 0
Gesamtzahl Byte vor Deduplizierung: 0
Gesamtzahl Byte nach Deduplizierung: 0
Daten komprimiert um: 0%
Reduzierung durch Deduplizierung: 0,00%
Gesamtverhältnis der Datenreduktion: 0,00%
Abgelaufene Verarbeitungszeit: 3,33 Sek
Die Operation wurde erfolgreich ausgeführt. (rc = 0)
```

Sie können auch das IBM Spectrum Protect-Aktivitätenprotokoll und die erweiterte Übersichtstabelle auf dem IBM Spectrum Protect-Server verwenden, um festzustellen, ob VM-Sicherungen erfolgreich sind.

Informationen zum IBM Spectrum Protect-Dateibereich

Möglicherweise ist es niemals erforderlich, dass Ihnen die Dateinamen oder Speicherpositionen für die Dateien Ihrer virtuellen Maschine (VM) bekannt sein müssen. Falls die zugrunde liegende Dateistruktur Sie jedoch interessiert: Data Protection for Microsoft Hyper-V-Sicherungen werden unter dem Knotennamen des Hyper-V-Zielknotens (z. B. `KINGSTON5_HV_TGT`) auf dem IBM Spectrum Protect-Server gespeichert.

Das folgende Beispiel zeigt die Dateibereichsinformationen für die virtuelle Maschine mit dem Namen `kingston40`.

```
Protect: ORION>q file KINGSTON5_HV_TGT f=d

Knotenname:  KINGSTON5_HV_TGT
Dateibereichsname: \VMFULL-kingston40
Hexadezimaler Dateibereichsname:
FSID: 61
Kollokationsgruppenname:
Plattform: TDP Hyper-V
Dateibereichstyp: API:TSMVM
Ist Dateibereich Unicode?: Nein
Kapazität: 0 KB
Auslastung in %: 0,0
Startdatum/-zeit der letzten Sicherung: 13.03.2018 21:29:17
Tage seit Start der letzten Sicherung: 31
Enddatum/-zeit der letzten vollständigen NAS-Imagesicherung:
Tage seit der letzten vollständigen NAS-Imagesicherung:
Datum/Zeit der letzten Sicherung des Clients (UTC):
Datum/Zeit der letzten Archivierung des Clients (UTC):
Startdatum/-zeit der letzten Replikation:
Tage seit dem Start der letzten Replikation:
Enddatum/-zeit der letzten Replikation:
Tage seit dem Ende der letzten Replikation:
Replikationsregel für Sicherungsdaten: DEFAULT
Replikationsstatus für Sicherungsdaten: Aktiviert
Replikationsregel für Archivierungsdaten: DEFAULT
Replikationsstatus für Archivierungsdaten: Aktiviert
Replikationsregel für speicherverwaltete Daten: DEFAULT
Replikationsstatus für speicherverwaltete Daten: Aktiviert
Typ für Gefährdung: Standardintervall
Gefährdungsintervall:
```

Fehlerbehebung für Anwendungsschutz von virtuellen Gastmaschinen

Ist Data Protection for Microsoft Hyper-V für Anwendungsschutz von virtuellen Maschinen (VMs) konfiguriert, die Anwendungsdaten hosten, und tritt bei VM-Sicherungsoperationen ein Problem auf, versuchen Sie, das Problem in Ihrer Umgebung zu reproduzieren.

Bei Sicherungen mit Anwendungsschutz erstellte Momentaufnahmen, die unterbrochen wurden, können nicht gelöscht werden

Ist Data Protection for Microsoft Hyper-V für den Anwendungsschutz von VMs konfiguriert, die Anwendungsdaten hosten, können Sie eine Sicherung mit Anwendungsschutz für eine VM ausführen, indem Sie den Befehl `dsmc backup vm` *VM-Name* ausgeben. Wenn Sie die Sicherungsoperation jedoch mithilfe der Tastenkombination **Strg + C** abbrechen, wird die von der Sicherungsoperation erstellte Momentaufnahme nicht automatisch entfernt. Darüber hinaus kann die Momentaufnahme nicht mit dem Hyper-V-Manager entfernt werden.

Zur Behebung dieses Problems müssen Sie die Momentaufnahme manuell entfernen, indem Sie das Cmdlet **Get-VMSnapshot** mit dem Parameter **-SnapshotType Recovery** und anschließend das Cmdlet **Remove-VMSnapshot** ausführen, um die Momentaufnahme zu entfernen. Weitere Informationen finden Sie in „Momentaufnahmeverwaltung mit Windows PowerShell" auf Seite 11.

Nachricht ANS4063W wird während einer Sicherung mit Anwendungsschutz für eine Microsoft Exchange Server-Datenbank generiert

Wurde die Berechtigungsnachweisdatei auf der Gast-VM nicht generiert, bevor die Gast-VM von der Einheit zum Versetzen von Daten gesichert wird, wird die Nachricht ANS4063W generiert.

```
ANS4063W Der IBM Spectrum Protect-Anwendungsschutz kann die
Anwendungsmetadatei 'APPPROTECTIONDBINFO.XML' nicht von der folgenden VM kopieren:
'<Name_Name>'.
Die Zurückschreibung einer einzelnen Datenbank aus dieser Sicherung wird nicht unterstützt.
Überprüfen Sie den Zustand der Anwendungsausgabeprogramme und -datenbanken.
```

Führen Sie die folgenden Schritte aus, um das Problem zu beheben:

1. Generieren Sie in der Gast-VM die Berechtigungsnachweisdatei in der Gastmaschine, indem Sie den folgenden Befehl bei einer PowerShell-Eingabeaufforderung ausführen und bei der entsprechenden Aufforderung den Domänenbenutzernamen (*Domänenname\Benutzername*) und das Kennwort eingeben:

   ```
   Get-Credential | Export-Clixml -Path 'C:\Programme\Tivoli\TSM\baclient\
   dsmcreds.xml'
   ```

   Der Domänenbenutzer muss über die Exchange-Zurückschreibungsberechtigung verfügen.
2. Überprüfen Sie die Berechtigungsnachweise, indem Sie die folgenden Befehle über eine Exchange-Verwaltungsshell auf der Gast-VM ausführen:

   ```
   $cred = Import-CliXml -Path 'C:\Programme\Tivoli\TSM \baclient\
     dsmcreds.xml'
   $Session = New-PSSession -Credential $cred -ConfigurationName Microsoft.Exchange
     -ConnectionUri http://Exchange Server-Name/PowerShell?serializationLevel=
     Full -Authentication Kerberos
   Import-PSSession -Session $Session
   Get-MailboxDatabase -Server <Exchange Server-Name>
   ```

3. Sichern Sie die Gast-VM auf der Einheit zum Versetzen von Daten auf dem Hyper-V-Host oder -Cluster mithilfe von Data Protection for Microsoft Hyper-V.

   Anweisungen finden Sie in „Ad-hoc-Sicherung einer virtuellen Maschine ausführen" auf Seite 91.

Zugehörige Tasks:

„Fehlerbehebung für VSS-Sicherungs- und -Zurückschreibungsoperationen auf virtuellen Gastmaschinen"

Fehlerbehebung für VSS-Sicherungs- und -Zurückschreibungsoperationen auf virtuellen Gastmaschinen

Wenn bei der Sicherungs- oder Zurückschreibungsverarbeitung mit Volume Shadow Copy Service (VSS) auf einer Gast-VM (VM = virtuelle Maschine) ein Problem auftritt, versuchen Sie, das Problem in Ihrer Umgebung zu reproduzieren.

Informationen zu diesem Vorgang

Wenn ein Problem vorliegt, dass Sie durch Reproduktion des Problems oder mithilfe der folgenden Informationen nicht beheben können, wenden Sie sich an den IBM Support.

VSS-Writer-Service verursacht das Fehlschlagen einer VM-Sicherung

Sie können jeden VSS-Writer, der das Fehlschlagen einer VM-Sicherung verursacht, übergehen und bei der Sicherung ausschließen.

Informationen zu diesem Vorgang

Der VSS-Writer befindet sich vor einer VM-Sicherung in einem stabilen Zustand und es liegen für ihn keine Fehler vor. Während der VM-Sicherungsverarbeitung kann bei einem VSS-Writer ein Fehler auftreten, der bewirkt, dass die gesamte VM-Sicherung fehlschlägt.

Beispiel: Der VSS-Writer Microsoft Forefront Protection ist auf einer Gast-VM installiert, die VM-Sicherung schlägt fehl und der Status des VSS-Writers ändert sich in `Fehler mit Wiederholungsaktion`, `Warten auf Beendigung` oder einen anderen Status als `Stabil`. Führen Sie die folgenden Schritte aus, um den Writer-Service bei der VM-Sicherung auszuschließen.

Vorgehensweise

1. Listen Sie im VSS-Verwaltungsbefehlszeilentool auf der Gast-VM die VSS-Writer auf, indem Sie den Befehl **`vssadmin list writers`** ausgeben. Im folgenden Befehlsbeispiel wird der `Microsoft Forefront Protection VSS Writer`-Service durch Writer-Namen, ID und Instanz-ID angegeben:

   ```
   Writer-Name: 'FSCVSSWriter'
      Writer-ID: {68124191-7787-401a-8afa-12d9d7ccc6ee}
      Writer-Instanz-ID: {f4cc5385-39a5-463b-8ab4-aafb2b35e21e}
      Status: [1] Stabil
      Letzter Fehler: Kein Fehler
   ```

2. Fügen Sie in der Optionsdatei der Einheit zum Versetzen von Daten, `dsm.opt` oder `dsm.sys`, die Option `EXCLUDE.VMSYSTEMSERVICE` gefolgt vom *Writer-Namen* hinzu, wie im folgenden Beispiel dargestellt.

   ```
   EXCLUDE.VMSYSTEMSERVICE FSCVSSWriter
   ```

   Tipp: Wenn die Maschine der Einheit zum Versetzen von Daten sich auf einem Linux-System befindet, ist `dsm.sys` die Optionsdatei. Wenn die Gast-VM und die Maschine der Einheit zum Versetzen von Daten unterschiedliche Sprachengruppen verwenden, geben Sie die *Writer-ID* oder die *Writer-Instanz-ID* anstelle des *Writer-Namens* an.
   Beispiel:

   ```
   EXCLUDE.VMSYSTEMSERVICE {68124191-7787-401a-8afa-12d9d7ccc6ee}
   ```

Ergebnisse

Die VM-Sicherung wird selbst dann erfolgreich beendet, wenn der `Microsoft Forefront Protection VSS Writer`-Service auf der Gast-VM ausgeführt wird.

Keine Anwendungsschutzdatei APPPROTECTIONDBINFO.XML und keine Warnungen für übersprungene Datenbanken

Unter bestimmten Bedingungen wird eine Exchange Server-Datenbank, deren Bereitstellung aufgehoben wurde, während einer Sicherungsoperation übersprungen, ohne dass eine Warnung ausgegeben wird.

Informationen zu diesem Vorgang

Angenommen, die folgenden Bedingungen sind während einer VM-Sicherung einer Gast-VM mit Microsoft Exchange Server erfüllt:

- Der Exchange Server gehört nicht zu einer Datenbankverfügbarkeitsgruppe (Database Availability Group - DAG).
- Die Bereitstellung aller Exchange Server-Datenbanken wurde aufgehoben.

In diesem Fall wird die folgende Warnung generiert:

```
ANS4063W Der IBM Spectrum Protect-Anwendungsschutz kann die
Anwendungsmetadatei 'APPPROTECTIONDBINFO.XML' nicht von der folgenden VM kopieren: '<Name_Name>'.
Die Zurückschreibung einer einzelnen Datenbank aus dieser Sicherung wird nicht unterstützt.

ANS4063W Der IBM Spectrum Protect-Anwendungsschutz kann die
Anwendungsmetadatei '_____L' nicht von der folgenden VM kopieren: '<VM-Name>'.
Die Zurückschreibung einer einzelnen Datenbank aus dieser Sicherung wird nicht unterstützt.
```

In dieser Situation ist die VM-Sicherung nur für die vollständige VM-Zurückschreibung verfügbar. Die Zurückschreibung einer einzelnen Datenbank aus dieser VM-Sicherung ist nicht verfügbar.

Zur Vermeidung dieser Situation müssen Sie die Exchange Server-Datenbanken bereitstellen, bevor Sie die VM-Sicherungsoperation starten.

Wenn die Bereitstellung von Exchange Server-DAG-Datenbanken oder Exchange Server-Datenbanken aufgehoben wird, wird bei einer VM-Sicherungsoperation einer Gast-VM die folgende Warnung generiert:

```
ANS2234W Das Zurückschreiben aus einer Sicherung der virtuellen Maschine ist für
die abgehängte Datenbank <Datenbank> nicht verfügbar
```

Bei einer Exchange Server-Datenbank, deren Bereitstellung aufgehoben wurde und die kein Mitglied einer DAG ist, kann IBM Spectrum Protect nicht erkennen, dass die Bereitstellung der Datenbanken aufgehoben wurde. Daher wird die Warnung ANS4063W anstelle von ANS2234W generiert.

Transaktionsfehler durch das Mischen von deduplizierten und nicht deduplizierten Daten in derselben Transaktion

Unter bestimmten Bedingungen tritt ein Transaktionsfehler auf, wenn deduplizierte und nicht deduplizierte Daten in derselben Transaktion gemischt werden.

Informationen zu diesem Vorgang

Wenn die Datendeduplizierung aktiviert ist, kann bei einer Data Protection for Microsoft Hyper-V-Sicherung einer VM mit Anwendungsschutz der folgende Fehler in der Datei `dsmerror.log` generiert werden:

```
ANS0246E 'dsmEndTxn' ausgeben und dann eine neue Transaktionssitzung beginnen.
ANS5250E Es wurde ein unerwarteter Fehler festgestellt.
   IBM Spectrum Protect-Funktionsname : vmSendViaFile()
   IBM Spectrum Protect-Funktion      : Datei konnte nicht gesendet werden
                        /tmp/tsmvmbackup/fullvm/vmtsmvss/member1/IIS CONFIG WRITER.XML
   IBM Spectrum Protect-Rückkehrcode  : 2070
   IBM Spectrum Protect-Datei         : vmmigration.cpp (1383)
```

Dieser Fehler ist behebbar und kann ignoriert werden. Der Fehler tritt auf, wenn Data Protection for Microsoft Hyper-V versucht, die XML-Datei (die aufgrund ihrer geringen Größe bei der Deduplizierung ausgeschlossen wurde) in derselben Transaktion wie die deduplizierten Daten zu senden. Data Protection for Microsoft Hyper-V sendet die XML-Datei, die in der Fehlernachricht angegeben ist, in einer neuen Transaktion erneut.

Für PowerShell ist bei Datenbankzurückschreibungsoperationen möglicherweise kein Speicher mehr verfügbar

Wenn Sie Microsoft Exchange Server-Datenbanken mit der Data Protection for Microsoft Exchange Server-Verwaltungskonsole zurückschreiben, kann bei Windows PowerShell der folgende Fehler auftreten:

```
APPCRASH
Nicht verfügbar
0
powershell.exe
10.0.14409.1005
584a185c
tsmapi64.dll
8.1.6.14
5af94075
c00000fd
000000000022df88
```

Der Ausnahmecode `0xc00000fd` gibt an, dass eine Stapelüberlaufausnahme aufgetreten ist. Zur Behebung dieses Problems erhöhen Sie den maximalen Speicher, der für PowerShell zugeordnet wird, mithilfe der Quote **MaxMemoryPerShellMB**.

Details zum Ändern des Werts der Quote **MaxMemoryPerShellMB** mit dem Editor für Gruppenmaßnahmen (**gpedit.msc**) oder mit PowerShell finden Sie in https://msdn.microsoft.com/en-us/library/ee309367(v=vs.85).aspx. Der Standardwert ist 150; der bevorzugte Wert ist jedoch 1024.

Kapitel 7. Virtuelle Maschinen mithilfe von Windows PowerShell-Cmdlets schützen

Sie können Data Protection for Microsoft Hyper-V-Operationen mithilfe von Microsoft Windows PowerShell-Cmdlets (Version 3.0 oder höher) ausführen.

Informationen zu diesem Vorgang

Informationen zur Vorbereitung für die Verwendung von Powershell-Cmdlets, die Liste der verfügbaren Cmdlets und allgemeine Tasks unter Verwendung dieser Cmdlets werden bereitgestellt.

Einschränkung: Die PowerShell-Cmdlets interagieren mit der Data Protection for Microsoft Hyper-V-REST-API, um Ihre virtuellen Maschinen zu schützen. Sie können nicht direkt mit der REST-API interagieren. Sie müssen die bereitgestellten Powershell-Cmdlets verwenden, um Data Protection for Microsoft Hyper-V-Operationen auszuführen.

Verwendung von PowerShell-Cmdlets mit Data Protection for Microsoft Hyper-V vorbereiten

Data Protection for Microsoft Hyper-V umfasst eine Reihe von Windows PowerShell-Cmdlets, die Ihnen bei der Verwaltung von Data Protection for Microsoft Hyper-V-Operationen in Ihrer Umgebung helfen.

Vorbereitende Schritte

Stellen Sie sicher, dass Microsoft Windows PowerShell 3 oder höher auf dem System verfügbar ist, auf dem Data Protection for Microsoft Hyper-V installiert ist. Geben Sie den folgenden Befehl in einer Powershell-Sitzung ein, um die installierte Powershell-Version anzuzeigen:

```
PS C:\> $PSVersionTable.PSVersion
```

Die Zahl in der Spalte `Major` ist die Powershell-Version.

Informationen zu diesem Vorgang

Sie können die Cmdlets interaktiv über die Powershell-Befehlszeile ausführen oder in Scripts für die Automatisierung von Data Protection for Microsoft Hyper-V-Operationen einfügen.

Sie müssen die folgenden Schritte ausführen, bevor Sie die Cmdlets verwenden.

Vorgehensweise

1. Starten Sie eine Microsoft Windows PowerShell- oder Microsoft Windows PowerShell ISE-Sitzung mit Administratorberechtigung:
   a. Klicken Sie auf **Start** > **Alle Programme** > **Zubehör** > **Windows PowerShell**.
   b. Klicken Sie mit der rechten Maustaste auf **Windows PowerShell** und klicken Sie auf **Als Administrator ausführen**.

2. Überprüfen Sie, ob die Ausführungsmaßnahme auf `RemoteSigned` gesetzt ist, indem Sie den folgenden Befehl ausgeben:

   ```
   PS C:\> Get-ExecutionPolicy
   ```

   Wird eine andere Maßnahme angezeigt, setzen Sie die Ausführungsmaßnahme auf `RemoteSigned`, indem Sie den folgenden Befehl ausgeben:

   ```
   PS C:\> Set-ExecutionPolicy RemoteSigned
   ```

   Tipp: Der Befehl **Set-ExecutionPolicy** muss nur einmal ausgeführt werden.

3. Importieren Sie das Powershell-Modul für Data Protection for Microsoft Hyper-V, um die Cmdlets verfügbar zu machen:

   ```
   PS C:\> Import-Module "C:\Programme\IBM\SpectrumProtect\DPHyperV\dphvModule.dll"
   ```

4. Authentifizieren Sie sich bei Data Protection for Microsoft Hyper-V, indem Sie das Cmdlet 'session' verwenden:

   ```
   $cred = Get-Credential -UserName Benutzername -message "credential"
   $session = New-DpHvSession -ComputerName Computername -Credential $cred
   ```

   Hierbei gilt Folgendes:

   Benutzername
   : Gibt das Konto an, mit dem Sie sich bei dem Windows-System anmelden, auf dem Data Protection for Microsoft Hyper-V installiert ist.

   Computername
   : Gibt den Namen des Servers an, auf dem Data Protection for Microsoft Hyper-V installiert ist.

5. Wird das Sicherheitszertifikat des Hosts, zu dem Sie eine Verbindung herstellen, nicht erkannt oder befindet es sich nicht auf dem lokalen Server (auf dem die PowerShell-Cmdlets installiert sind), schlägt das Cmdlet für die Sitzung fehl. Sie müssen das Cmdlet **New-DpHvSession** erneut ausführen. Dabei müssen Sie einen der folgenden Parameter angeben: Entweder den Parameter **-Force**, damit das Zertifikat ignoriert wird, oder den Parameter **-CertificatePrompt**, damit eine Eingabeaufforderung für die Installation eines neuen Zertifikats angezeigt wird.

   Führen Sie beispielsweise das folgende Cmdlet für die Sitzung aus:

   ```
   $cred = Get-Credential -UserName Benutzername -message "credential"
   $session = New-DpHvSession -ComputerName Computername -Credential $cred
   -CertificatePrompt
   ```

   Führen Sie bei der entsprechenden Aufforderung die folgenden Schritte für einen eigenständigen Host oder für jeden Host in einem Cluster aus:

   a. Im Fenster **Verbindung zu <Hostname> wird geschützt** klicken Sie auf **Zertifikat anzeigen**.

      Wenn Sie eine der anderen Optionen auswählen - z. B. **Ja**, um die Zertifikatswarnung für die aktuelle Sitzung zu ignorieren, **Nein**, um die Verbindung zu stoppen, oder **Bei Verbindungen zu diesem Computer nicht mehr fragen**, um alle zukünftigen Zertifikatswarnungen zu ignorieren - können Sie keine Verbindung zu Data Protection for Microsoft Hyper-V herstellen.

   b. Klicken Sie auf der Registerkarte **Allgemein** des Fensters **Zertifikat** auf **Zertifikat installieren**.

   c. Wählen Sie auf der Begrüßungsseite des Fensters **Zertifikatimport-Assistent** eine Speicherposition aus (**Aktueller Benutzer** oder **Lokale Maschine**) und klicken Sie auf **Weiter**.

   d. Auf der Seite **Zertifikatspeicher** klicken Sie auf **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie auf **Durchsuchen**.

e. Wählen Sie im Fenster **Zertifikatspeicher auswählen** die Option **Vertrauenswürdige Stammzertifizierungsstellen** aus und klicken Sie auf **OK**.

f. Klicken Sie auf der Seite **Zertifikatspeicher** auf **Weiter**.

g. Überprüfen Sie die ausgewählten Einträge auf der Seite **Fertigstellen des Assistenten** und klicken Sie auf **Fertigstellen**.

h. Klicken Sie im Fenster mit der **Sicherheitswarnung** auf **Ja**, um das Zertifikat zu installieren.

i. Klicken Sie im Bestätigungsfenster auf **OK**.

Wenn Sie das Zertifikat ablehnen, können Sie nur dann eine Verbindung zu Data Protection for Microsoft Hyper-V herstellen, wenn Sie den Parameter **-Force** verwenden.

6. Lesen Sie die Liste der verfügbaren Cmdlets in „PowerShell-Cmdlets für Data Protection for Microsoft Hyper-V".
7. Optional: Lesen Sie die Onlinehilfe für jedes Cmdlet. Weitere Informationen finden Sie in „Hilfeinformationen für PowerShell-Cmdlets abrufen" auf Seite 156.

Nächste Schritte

Informationen zur Erstellung, Ausführung, Überwachung und Fehlerbehebung für Scripts mit Cmdlets enthält die Dokumentation zu Windows PowerShell 3.0 oder höher. Weitere Informationen zu Cmdlets, konsistenten Benennungsmustern, Parametern, Argumenten und der Syntax in Windows PowerShell finden Sie in Microsoft TechNet: Erste Schritte mit Windows PowerShell.

PowerShell-Cmdlets für Data Protection for Microsoft Hyper-V

Informieren Sie sich über die Data Protection for Microsoft Hyper-V-Cmdlets, die Sie verwenden können, um die Daten Ihrer virtuellen Maschinen (VMs) zu schützen.

In der folgenden Tabelle sind die Cmdlets aufgeführt, die für Data Protection for Microsoft Hyper-V verfügbar sind.

Tabelle 13. PowerShell-Cmdlets für Data Protection for Microsoft Hyper-V

Cmdlet-Name	Beschreibung
Backup-DpHvVm	Eine Hyper-V-VM sichern. Zugehöriger Befehl: **dsmc backup vm**
Get-DpHvBackup	Informationen zu einer VM-Sicherung anzeigen. Zugehöriger Befehl: **dsmc query vm**
Get-DpHvBackupSchedule	Eine Liste der auswählbaren Sicherungszeitpläne für die VMs auf dem Hyper-V-Host oder im Cluster anzeigen. Ein auswählbarer Zeitplan muss vom IBM Spectrum Protect-Serveradministrator für eine Domäne definiert werden, die das Ziel für Hyper-V-VMs ist. Die Zeitplandefinition muss die folgenden Parameter und Optionen beinhalten: • In der Optionszeichenfolge muss die Option `-domain.vmfull="all-vm"` angegeben werden. • Der Zeitplan muss die Parameter ACTION=BACKUP und SUBACTION=VM enthalten.

Tabelle 13. PowerShell-Cmdlets für Data Protection for Microsoft Hyper-V (Forts.)

Cmdlet-Name	Beschreibung
Get-DpHvHostConfiguration	Die Konfigurationsinformationen für den Hyper-V-Host auf dem IBM Spectrum Protect-Server anzeigen.
Get-DpHvLastSuccessfulBackup	Informationen zu den letzten VM-Sicherungsoperationen anzeigen, die auf einem Host oder in einem Cluster ausgeführt wurden. Die folgenden Informationen werden zurückgegeben: der Gefährdungsstatus der VM-Sicherung; das Sicherungsdatum; die Dauer der Sicherung; das Volumen der übertragenen Daten; der Typ der Sicherung; der Host, zu dem die VM gehört (für Cluster); der Name des ausgeführten Zeitplans.
Get-DpHvPolicyDomain	Eine Liste der Maßnahmendomänen auf dem IBM Spectrum Protect-Server anzeigen. Zugehöriger Befehl: **dsmadmc q domain**
Get-DpHvScheduleHistory	Eine Liste der ausgeführten Zeitpläne anzeigen. Zu jedem zurückgegebenen Zeitplan können die Startzeit der Ausführung, der Name des Zeitplans, der Status des Zeitplans, die Anzahl der gesicherten oder nicht gesicherten VMs und die Dauer der Zeitplanausführung angegeben sein.
Get-DpHvScheduleHistoryDetail	Informationen zu jeder VM anzeigen, die bei einer Zeitplanausführung gesichert wurde. Zu jeder zurückgegebenen Sicherungstask können der Name der VM, der Status der Sicherung, die Startzeit der Sicherung und die Fehlercodes für die fehlgeschlagenen Sicherungen angegeben sein.
Get-DpHvTask	Allgemeine Informationen zu abgeschlossen und aktiven Tasks anzeigen.
Get-DpHvVvm	Informationen zu dem VM-Bestand auf dem Hyper-V-Host anzeigen. Zugehöriger Befehl: **dsmc show vm**
Get-DpHvVMAtRisk	Die aktuelle Maßnahme bei Gefährdung für die VM anzeigen. Die Maßnahme bei Gefährdung legt fest, wann eine VM-Sicherung als gefährdet angezeigt wird, wenn eine Sicherungsoperation in einem angegebenen Zeitintervall nicht ausgeführt wurde. Die Maßnahme bei Gefährdung besteht aus einem Typ für Gefährdung. Der Typ für Gefährdung ist eine Zahl und kann 0 (BYPASS), 1 (CUSTOM) oder 2 (DEFAULT) lauten. Angepasste Typen für Gefährdung verfügen über ein Gefährdungsintervall in Stunden.

Tabelle 13. PowerShell-Cmdlets für Data Protection for Microsoft Hyper-V (Forts.)

Cmdlet-Name	Beschreibung
Get-DpHvVMBackupHistory	Das Sicherungsprotokoll für eine VM von der erweiterten Übersichtstabelle auf dem IBM Spectrum Protect-Server aus anzeigen. Zu jeder zurückgegebenen Sicherungstask können die folgenden Informationen angegeben sein: die letzte Ausführungszeit einer Sicherung; der Status der Sicherung; die Dauer der Sicherung; das Volumen der übertragenen Daten; der Host, zu dem die VM gehört (für Cluster); die zurückgegebenen Fehlercodes.
Get-DpHvVmBackupTaskHistory	Das Protokoll der VM-Sicherungstasks anzeigen, das lokal in Data Protection for Microsoft Hyper-V gespeichert ist.
Get-DpHvVmRestoreTaskHistory	Das Protokoll der VM-Zurückschreibungstasks anzeigen, das lokal in Data Protection for Microsoft Hyper-V gespeichert ist.
New-DpHvFsInfo	Erstellt ein Objekt `FsInfo`, das mit dem Cmdlet **Set-DpHvVmAtRisk** verwendet wird. Das Objekt `FsInfo` gibt die IBM Spectrum Protect-Dateibereichs-ID und den Namen der VM an, für die die Maßnahme bei Gefährdung definiert werden soll.
New-DpHvNodeInfo	Erstellt ein Objekt `NodeInfo`, das mit dem Cmdlet **Set-DpHvHostConfiguration** verwendet wird. Das Objekt `NodeInfo` gibt den Knotennamen und den Knotentyp auf dem Hyper-V-Host an.
New-DpHvSession	Sich bei Data Protection for Microsoft Hyper-V authentifizieren und eine Powershell-Cmdlet-Sitzung starten.
Receive-DpHvTask	Die Sicherungs- oder Zurückschreibungstask überwachen.
Remove-DpHvSession	Die Sitzung mit Data Protection for Microsoft Hyper-V schließen.
Restore-DpHvVm	Eine Hyper-V-VM zurückschreiben. Zugehöriger Befehl: **dsmc restore vm**
Set-DpHvBackupSchedule	Einem Zeitplan eine Einheit zum Versetzen von Daten auf einem Hyper-V-Host oder in einem Cluster zuordnen. Sie können einem Zeitplan einen Knoten zuordnen, die Zuordnung zwischen einem Zeitplan und einem Knoten aufheben und einem Zeitplan einen Zielknoten zuordnen.
Set-DpHvHostConfiguration	Den Hyper-V-Host für Data Protection for Microsoft Hyper-V-Operationen konfigurieren.
Set-DpHvHttpsPort	Den HTTPS-Port definieren, der für den IBM Spectrum Protect-Web-Server verwendet wird.
Set-DpHvMmcLoginPreferences	Die Vorgaben für die Data Protection for Microsoft Hyper-V-Verwaltungskonsole definieren.

Tabelle 13. PowerShell-Cmdlets für Data Protection for Microsoft Hyper-V (Forts.)

Cmdlet-Name	Beschreibung
Set-DpHvVmAtRisk	Die Maßnahme bei Gefährdung für eine VM oder mehrere VMs definieren. Die Maßnahme bei Gefährdung legt fest, wann eine VM-Sicherung als gefährdet angezeigt wird, wenn eine Sicherungsoperation in einem angegebenen Zeitintervall nicht ausgeführt wurde. Die Maßnahme bei Gefährdung besteht aus einem Typ für Gefährdung. Der Typ für Gefährdung ist eine Zahl und kann 0 (BYPASS), 1 (CUSTOM) oder 2 (DEFAULT) lauten. Angepasste Typen für Gefährdung verfügen über ein Gefährdungsintervall in Stunden.
Set-ServerConnection	Informationen zur IBM Spectrum Protect-Serververbindung auf dem Hyper-V-Host speichern und die Verbindung zum Server überprüfen.
Show-DpHvHttpsPort	Die Portinformationen für den IBM Spectrum Protect-Web-Server anzeigen.
Show-DpHvMmcLoginPreferences	Die Vorgaben für die Data Protection for Microsoft Hyper-V-Verwaltungskonsole anzeigen.
Stop-DpHvTask	Eine Sicherungs- oder Zurückschreibungstask abbrechen.
Test-DpHvConfiguration	Die Konfiguration für Data Protection for Microsoft Hyper-V überprüfen.
Test-DomainCredentials	Die Berechtigungsnachweise für den Windows-Domänenbenutzer überprüfen.

Die Liste der allgemeinen Tasks für die Cmdlets finden Sie in „Beispiele für Data Protection for Microsoft Hyper-V-Cmdlets" auf Seite 157.

Hilfeinformationen für PowerShell-Cmdlets abrufen

Für die Powershell-Cmdlets wird Onlinehilfe bereitgestellt. Führen Sie das Cmdlet **Get-Help** mit dem Namen des Cmdlets aus, um detaillierte Informationen zu einem bestimmten Cmdlet anzuzeigen:

```
Get-Help Cmdlet-Name
```

Beispiel:

```
Get-Help Backup-DpHvVm
```

Die folgenden Beispiele beziehen sich auf das Cmdlet **Backup-DpHvVm**. Geben Sie Folgendes ein, um Beispiele für Cmdlets anzuzeigen:

```
Get-Help Backup-DpHvVm -examples
```

Für detaillierte Informationen geben Sie Folgendes ein:

```
Get-Help Backup-DpHvVm -detailed
```

Wenn technische Informationen angezeigt werden sollen, geben Sie Folgendes ein:

```
Get-Help Backup-DpHvVm -full
```

Onlineproduktinformationen werden mit der folgenden Eingabe angezeigt:

```
Get-Help Backup-DpHvVm -online
```

Wenn Sie Informationen zu einem bestimmten Parameter wünschen, z. B. **IFINCREMENTAL**, geben Sie Folgendes ein:

```
help Backup-DpHvVm -Parameter IFINCREMENTAL
```

Soll die Hilfe in einem separaten Fenster angezeigt werden, geben Sie den Parameter **-ShowWindow** mit dem Befehl **help** an.

Beispiele für Data Protection for Microsoft Hyper-V-Cmdlets

Für Data Protection for Microsoft Hyper-V-Cmdlets werden Beispiele bereitgestellt, um Sie beim Schutz Ihrer virtuellen Hyper-V-Maschinen (virtuelle Maschinen = VMs) zu unterstützen.

Stellen Sie sicher, dass Sie die Schritte in „Verwendung von PowerShell-Cmdlets mit Data Protection for Microsoft Hyper-V vorbereiten" auf Seite 151 ausführen, bevor Sie die Cmdlets verwenden.

Für gängige Data Protection for Microsoft Hyper-V-Tasks werden Beispiele bereitgestellt.

Tipps:

- Für jedes Cmdlet gibt es Parameter. Geben Sie zum Anzeigen der Parameter den folgenden Befehl **help** aus:

  ```
  help Cmdlet-Name -ShowWindow
  ```

- Für die Cmdlets ist Onlinehilfe verfügbar. Weitere Informationen finden Sie in „Hilfeinformationen für PowerShell-Cmdlets abrufen" auf Seite 156.

Beispiel 1: Mindestens eine VM sichern

Führen Sie eine Sicherung 'Immer inkrementell - Inkrementell' für eine VM oder mehrere VMs aus.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred$vmList = @("vm1","vm2")
$task = Backup-DpHvVm -Session $session -VmName $vmList -mode IFINCREMENTAL
$taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
while ("running" -eq $taskInfo.taskState) {
    start-sleep -seconds 30
    $taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
    if ($taskInfo.hasMoreData) {
        $results = Receive-DpHvTask -Session $session -TaskId $task.taskId
        write-verbose -verbose ("Started {0} Duration {1:g} Transferred
            {2:N2} MB" -f $results.startTime, ((Get-Date)-$results.startTime),
            ($results.totalBytesTransferred/1MB))
    }
}

$results = Receive-DpHvTask -Session $session -TaskId $task.taskId
$results

Remove-DpHvSession -Session $session
```

In diesem Beispiel werden folgende Aktionen ausgeführt: eine Powershell-Cmdlet-Sitzung mit Data Protection for Microsoft Hyper-V starten, die VMs sichern, die VM-Sicherung abfragen, den Sicherungsjob überwachen und die Sitzung beenden, wenn die Sicherung abgeschlossen ist.

Beispiel 2: VM-Sicherung abfragen

Fragen Sie den IBM Spectrum Protect-Serverdateibereich ab und zeigen Sie allgemeine Informationen zu allen VM-Sicherungen an.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred$bks = Get-DpHvBackup -Sessio
$bks
Remove-DpHvSession -Session $session
```

Beispiel 3: Prüfen, ob ein Hyper-V-Host für Data Protection for Microsoft Hyper-V-Operationen konfiguriert ist

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
Get-DpHvHostConfiguration -Session $session
Remove-DpHvSession -Session $session
```

Beispiel 4: Informationen zur IBM Spectrum Protect-Serververbindung auf dem Hyper-V-Host speichern und die Verbindung überprüfen

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
Set-ServerConnection -Session $session -SPServerName Servername -SPAdmin
  Administratorname -SPAdminPwd Administratorkennwort -SPServerSSLPort Port
Remove-DpHvSession -Session $session
```

Beispiel 5: Maßnahmeninformationen auf dem IBM Spectrum Protect-Server anzeigen

Zeigen Sie Informationen wie den Domänennamen, die Standardverwaltungsklasse, die Beschreibung und den Aufbewahrungszeitraum für Sicherungen sowie Archivierungen an:

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
Get-DpHvPolicyDomain -Session $session
Remove-DpHvSession -Session $session
```

Beispiel 6: Hyper-V-Host für Data Protection for Microsoft Hyper-V-Operationen konfigurieren

Im folgenden Beispiel wird ein Hyper-V-Host durch Ausführung der folgenden Tasks konfiguriert:

- Den Zielknoten (Clusterknoten) registrieren.
- Den Knoten der Einheit zum Versetzen von Daten registrieren und für Sicherungsoperationen konfigurieren (die Optionsdatei konfigurieren und den Clientakzeptor- sowie den Scheduler-Service erstellen).
- Die Umgebung für die Dateizurückschreibung konfigurieren, falls angefordert (die Windows- und Linux-Mount-Proxy-Knoten registrieren und die Optionsdatei sowie den Clientakzeptorservice erstellen). Wenn das Feature für Dateizurückschreibung aktiviert wird, müssen die Berechtigungsnachweise für die Dateizurückschreibung der Domänenbenutzer und das zugehörige Kennwort sein.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
Set-ServerConnection -Session $session -SPServerName Servername -SPAdmin
  Administratorname -SPAdminPwd Administratorkennwort -SPServerSSLPort Port
$nodesList = @(New-DpHvNodeInfo -NodeName Knotenname -NodeType Knotentyp)
```

```
Set-DpHvHostConfiguration -Session $session -PolicyDomain Name_der_Maßnahmendomäne
  -RegisterTargetNode -TargetNode Zielknoten -NodeList $nodesList -EnableFR
  -FRDomainUser Domänenname\Benutzername -FRDomainPwd Kennwort
Remove-DpHvSession -Session $session
```

Beispiel 7: VM-Bestand auf dem Hyper-V-Host anzeigen

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
$vms = Get-DpHvVm -Session $session
$vms
Remove-DpHvSession -Session $session
```

Beispiel 8: Sicherungsstatus von VMs auf einem Host oder in einem Cluster anzeigen

In dem folgenden Beispiel werden Informationen zu den letzten VM-Sicherungen auf einem Host oder in einem Cluster zurückgegeben.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
$lastBackups = Get-DpHvLastSuccessfulBackup -Session $session
$vmName = $lastBackups | select -first 1 -ExpandProperty name
$vmBackupHistory = Get-DpHvVMBackupHistory -Session $session -vmName $vmName
$vmBackupHistory
Remove-DpHvSession -Session $session
```

Beispiel 9: Maßnahme bei Gefährdung für eine VM definieren

Die Maßnahme bei Gefährdung legt fest, dass bei einer VM die Gefahr besteht, dass sie ungeschützt ist, wenn eine geplante Sicherungsoperation innerhalb eines angegebenen Zeitintervalls nicht ausgeführt wird.

Im ersten Teil des folgenden Beispiels werden Gefährdungsinformationen für alle gesicherten VMs angezeigt. Im zweiten Teil des Beispiels wird der Gefährdungswert für alle VMs, die mit "SQL" beginnen, in 12 Stunden geändert.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred

$lastBackups = Get-DpHvLastSuccessfulBackup -Session $session

# 1 - Aktuellen Gefährdungswert für alle VMs anzeigen

$i = 0
$atRiskList = @()
foreach ($backup in $lastBackups) {
  $activity = "Checking at risk value for {0}" -f $backup.name
  Write-Progress -activity $activity -status "Progress:" -percentcomplete
    ($i++/$lastBackups.count*100)
  $atRisk = Get-DpHvVmAtRisk -session $session -VmName $backup.name
  $atRiskList += [pscustomobject]@{VM=$backup.name;AtRiskType=
    $atRisk.AtRiskType;AtRiskInterval=$atRisk.AtRiskInterval}
}
$atRiskList | Out-GridView -Title "VM Risk Status" -PassThru

# 2 - Gefährdungswert für alle VMs, die mit SQL beginnen, auf das angepasste Intervall
# von 12 Stunden setzen

$sqlVms = $lastBackups | where name -like "sql*"
$fsList = @()
foreach ($vm in $sqlVms) {
   $fsList += New-DpHvFsInfo -vmName $vm.Name -fsId $vm.FileSpaceId
}
```

```
Set-DpHvVmAtRisk -session $session -AtRiskType CUSTOM -AtRiskInterval 12
   -FsList $fsList

Remove-DpHvSession -Session $sess
```

Beispiel 10: Protokoll der Zeitplanausführungen anzeigen

Im folgenden Beispiel wird eine Zusammenfassung der geplanten Aktivität gefolgt von den Details der letzten geplanten Aktivität angezeigt.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
$schedHistory = Get-DpHvScheduleHistory -Session $session
$sh = $schedHistory | Sort-Object actualstarttime -Descending | Select-Object
  -First 1
$schedHistoryDetail = Get-DpHvScheduleHistoryDetail -Session $session -ScheduleName
  $sh.Name -StartTime $sh.ActualStartTime -EndTime $sh.EndTime -NodeList
    $sh.NodeList

#"Zusammenfassung des Zeitplanprotokolls"
$schedHistory |
    select actualstarttime,name,status,vmsucceeded,vmfailures,duration,nodelist |
    sort actualstarttime -desc | ft -AutoSize

#"Details zu der letzten geplanten Aktivität"
$schedHistoryDetail |
    select starttime,datamover,targetnode,name,status,duration,datatransmitted,
    backuptype| ft -AutoSize

Remove-DpHvSession -Session $session
```

Beispiel 11: Zeitplan zu einer Einheit zum Versetzen von Daten auf einem Host oder in einem Cluster zuordnen

Sie können eine Zeitplanzuordnung überprüfen, indem Sie den Befehl QUERY ASSOCIATION auf dem IBM Spectrum Protect-Server ausführen.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
# Liste der Zeitpläne vom IBM Spectrum Protect-Server abrufen
$scheduleList = Get-DpHvBackupSchedule -Session $session
$scheduleList | format-table -autosize

# Zeitplan zu einem Knoten der Einheit zum Versetzen von Daten zuordnen
Set-DpHvBackupSchedule -Session $sess -ScheduleName "sched0" -Operation define
  -DmNodesList hyperv1_HV_DM

# Zeitplanzuordnung entfernen
Set-DpHvBackupSchedule -Session $sess -ScheduleName "sched0" -Operation remove
  -DmNodesList hyperv1_HV_DM

Remove-DpHvSession -Session $sess
```

Beispiel 12: Mindestens eine VM zurückschreiben

Schreiben Sie mehrere VMs unter Angabe der `Sicherungs-IDs` unter einem neuen Namen an ein neues Zurückschreibungsziel zurück.

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred
# Eine VM mit Standardparametern zurückschreiben
$task = Restore-DpHvVm -Session $session -vmname "vm1"
$taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
while ("running" -eq $taskInfo.taskState) {
    start-sleep -seconds 30
    $taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
```

```
    if ($taskInfo.hasMoreData) {
        $results = Receive-DpHvTask -Session $session -TaskId $task.taskId
        write-verbose -verbose ("Started {0} Duration {1:g} Transferred
            {2:N2} MB" -f $results.startTime, ((Get-Date)-$results.startTime),
            ($results.totalBytesTransferred/1MB))
    }
}

$results = Receive-DpHvTask -Session $session -TaskId $task.taskId
$results

# Mehrere VMs zurückschreiben
$task = Restore-DpHvVm -Session $session -vmname vm1,vm2 -backupId 111111,222222
 -newVmName vm1_restored,vm2_restored -targethPath c:\restored,c:\restored
$taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
while ("running" -eq $taskInfo.taskState) {
    start-sleep -seconds 30
    $taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
    if ($taskInfo.hasMoreData) {
        $results = Receive-DpHvTask -Session $session -TaskId $task.taskId
        write-verbose -verbose ("Started {0} Duration {1:g} Transferred
            {2:N2} MB" -f $results.startTime, ((Get-Date)-$results.startTime),
            ($results.totalBytesTransferred/1MB))
    }
}
$results = Receive-DpHvTask -Session $session -taskId $task.taskId
$results

# Zurückschreibungsprotokoll für VMs abrufen
$vmRestoreHistory = Get-DpHvVmRestoreTaskHistory -Session $session
$vmRestoreHistory

Remove-DpHvSession -Session $session
```

Beispiel 13: Konfiguration von Data Protection for Microsoft Hyper-V überprüfen

Nachdem Sie den Konfigurationsassistenten ausgeführt haben, können Sie mit dem Cmdlet **Test-DpHvConfiguration** die folgenden Konfigurationsinformationen anzeigen:

- Informationen zum Standardknoten der Einheit zum Versetzen von Daten wie den Computernamen, das Betriebssystem und die Position des Fehlerprotokolls
- Informationen zu den Standard-Mount-Proxy-Knoten wie den Computernamen, das Betriebssystem, die Position des Fehlerprotokolls, den Status von Recovery Agent und den iSCSI-Status der Mount-Proxy-Knoten

```
$cred = Get-Credential -Message 'Enter credentials' -UserName Benutzername
$session = New-DpHvSession -ComputerName Computername -Credential $cred

$out1 = Test-DpHvConfiguration -session $session -nodetype DMNODE
$out2 = Test-DpHvConfiguration -session $session -nodetype MPNODE

Remove-DpHvSession -Session $session
```

Zugehörige Verweise:

„PowerShell-Cmdlets für Data Protection for Microsoft Hyper-V" auf Seite 153

Kapitel 8. Befehlsreferenz

Die folgenden Abschnitte enthalten ausführliche Informationen über alle Clientbefehle, die für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V-Operationen verwendet werden.

Geben Sie diese Befehle im Befehlszeilenclient für Sichern/Archivieren von IBM Spectrum Protect aus. Starten Sie den Befehlszeilenclient mit einer der folgenden Methoden auf dem Windows-System:

- Rufen Sie **Start** > **Apps nach Name** > **IBM Spectrum Protect** > **Befehlszeile für Sichern/Archivieren** auf.
- Öffnen Sie eine Administratorbefehlseingabeaufforderung und wechseln Sie in das Installationsverzeichnis des Clients für Sichern/Archivieren (**cd** `"C:\Programme\tivoli\tsm\baclient"`). Führen Sie **dsmc.exe** aus.

Um diese Tasks in der IBM Spectrum Protect-GUI (Graphical User Interface - grafische Benutzerschnittstelle) für Sichern/Archivieren auszuführen, starten Sie den Client für die GUI für Sichern/Archivieren mit einer der folgenden Methoden auf dem Windows-System:

- Rufen Sie **Start** > **Apps nach Name** > **IBM Spectrum Protect** > **GUI für Sichern/Archivieren** auf.
- Öffnen Sie eine Administratorbefehlseingabeaufforderung und wechseln Sie in das Installationsverzeichnis des Clients für Sichern/Archivieren (**cd** `"C:\Programme\tivoli\tsm\baclient"`). Führen Sie **dsm.exe** aus.

Greifen Sie mit einer der folgenden Methoden auf die entsprechende GUI-Taskhilfe zu:

- Wählen Sie das Hilfesymbol aus und klicken Sie auf **Hilfethemen** oder 'Einführung'.
- Sie können auch die Taste F1 drücken, um die Hilfe **Hilfethemen** zu öffnen.

Syntaxdiagramme lesen

Folgen Sie beim Lesen eines Syntaxdiagramms zum Eingeben eines Befehls der Linie. Lesen Sie von links nach rechts und von oben nach unten.

- Das Symbol ►►— zeigt den Anfang eines Syntaxdiagramms an.
- Das Symbol —► am Ende einer Zeile zeigt an, dass das Syntaxdiagramm in der nächsten Zeile fortgesetzt wird.
- Das Symbol ►— am Anfang einer Zeile zeigt an, dass ein Syntaxdiagramm aus der vorherigen Zeile fortgesetzt wird.
- Das Symbol —►◄ zeigt das Ende eines Syntaxdiagramms an.

Syntaxelemente, beispielsweise Schlüsselwörter und Variable, können sich befinden:

- Auf der Linie (erforderliches Element)
- Über der Linie (Standardelement)
- Unter der Linie (optionales Element)

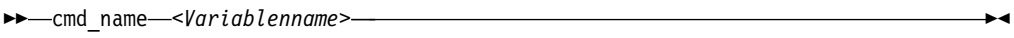
Symbole

Geben Sie diese Symbole *exakt* so ein, wie sie im Syntaxdiagramm stehen.

- * Stern
- *{ }* Geschweifte Klammern
- *:* Doppelpunkt
- *,* Komma
- = Gleichheitszeichen
- - Bindestrich
- *()* Runde Klammern
- . Punkt
- Leerzeichen
- ” Anführungszeichen
- ’ Hochkomma

Variable

Elemente in Kursivdruck, beispielsweise <*Variablenname*>, stehen für Variablen. In diesem Beispiel können Sie einen <*Variablennamen*> angeben, wenn Sie den Befehl **cmd_name** eingeben.



Wiederholung

Ein Pfeil, der nach links zurückgeht, bedeutet, dass das Element wiederholt werden kann. Ein Zeichen innerhalb des Pfeils bedeutet, dass Sie die sich wiederholenden Elemente mit diesem Zeichen voneinander trennen müssen.

Eine Fußnote (1) bei dem Pfeil nennt die maximale Anzahl an Wiederholungen für das Element.

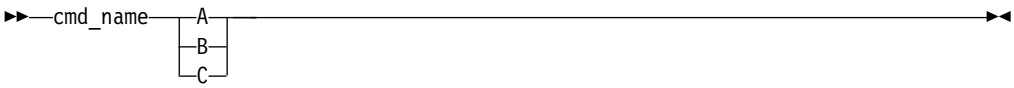
Anmerkungen:

1 Geben Sie *wiederholen* maximal 5-mal an.

Erforderliche Auswahlmöglichkeiten

Wenn mindestens zwei Elemente übereinander dargestellt werden, von denen sich eines auf der Linie befindet, *müssen* Sie ein Element angeben.

In diesem Beispiel müssen Sie A, B oder C auswählen.



Optionale Auswahlmöglichkeiten

Wenn sich ein Element *unter* der Linie befindet, handelt es sich um ein optionales Element. Im ersten Beispiel können Sie A oder gar nichts auswählen.

Wenn mindestens zwei Elemente übereinander dargestellt werden, die sich alle unter der Linie befinden, handelt es sich ausschließlich um optionale Elemente. Im zweiten Beispiel können Sie A, B, C oder gar nichts auswählen.

Wiederholt anwendbare Auswahlmöglichkeiten

Übereinander dargestellte Elemente, gefolgt von einem Pfeil, der nach links zurückgeht, bedeuten, dass Sie mehrere Elemente auswählen können, in manchen Fällen auch, dass Sie ein einzelnes Element wiederholen können.

In diesem Beispiel können Sie jede Kombination von A, B und C auswählen.

Standardwerte

Standardwerte befinden sich über der Linie. Der Standardwert wird ausgewählt, wenn Sie ihn nicht überschreiben. Sie können ihn aber auch explizit auswählen. Sie können den Standardwert überschreiben, indem Sie eine der unterhalb der Linie aufgeführten Optionen einbeziehen.

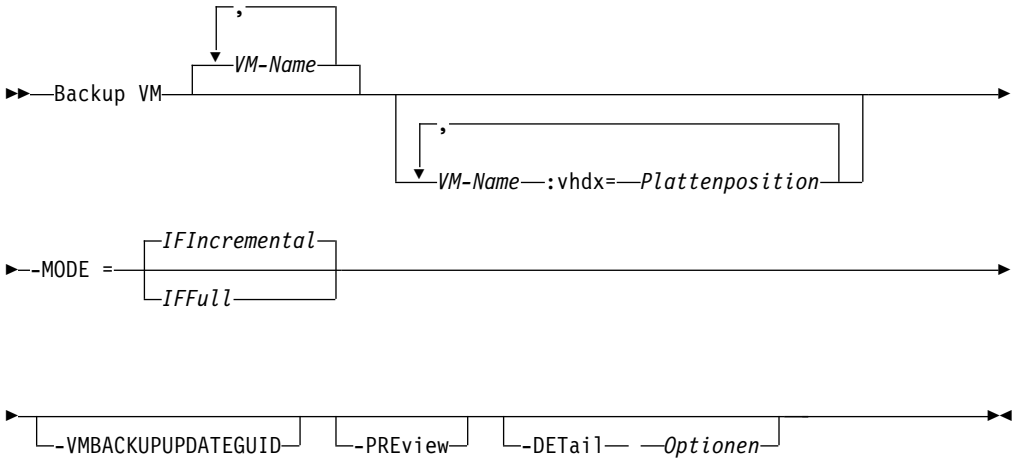
In diesem Beispiel ist A der Standardwert. Wählen Sie B oder C aus, um A zu überschreiben.

Backup VM

Verwenden Sie den Befehl **backup vm**, um virtuelle Hyper-V-Maschinen zu sichern.

Sie können Hyper-V-Gastmaschinen sichern, die auf einer lokalen Platte, einer an ein SAN angeschlossenen Platte oder einem freigegebenen Clustervolume (Cluster Shared Volume, CSV) gespeichert sind. Sie können auch Gastmaschinen sichern, die auf einer fernen Dateiserverfreigabe gespeichert sind. Ferne Dateiserverfreigaben müssen sich auf einem System mit Windows Server 2012 oder höher befinden. Außerdem muss es sich bei fernen Dateifreigaben um Server Message Block (SMB) 3.0 mit File Server VSS Agent Service (Dateiserver-VSS-Agent-Dienst) handeln, installiert auf dem Server.

Syntax



Parameter

VM-Name

Gibt den Namen der virtuellen Maschine an, die gesichert werden soll. Wenn Sie mehrere Namen virtueller Maschinen angeben, müssen Sie die Namen durch Kommas trennen (`vm1,VM2,Vm5`) oder die Option `domain.vmfull` verwenden. Bei den Namen muss die Groß-/Kleinschreibung beachtet werden. Sie muss der Schreibung entsprechen, die auf dem Hyper-V-Host in der Sicht **Hyper-V-Manager** > **Virtuelle Maschinen** angezeigt wird.

Platzhalterzeichen können in den Namen virtueller Maschinen verwendet werden.

VM-Name:**vhdx=***Plattenposition*

Dieser Parameter gibt die Festplatte der virtuellen Maschine (VHDX) an, die in Sicherungsoperationen für virtuelle Hyper-V-Maschinen eingeschlossen werden soll.

Die Variable *VM-Name* gibt den Namen der zu sichernden VM an. Für die Auswahl von VM-Namen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) steht für eine beliebige Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zei-

chen.
Das Schlüsselwort **:vhdx=***Plattenposition* gibt die Position der VM-Platte an, die in die Sicherungsoperation eingeschlossen werden soll. Die Plattenposition wird im Format "*Controllertyp Controllernummer Plattenpositionsnummer_im_Controller*" angegeben. Der Controllertyp muss "SCSI" oder "IDE" sein. Beispiel:

```
dsmc backup vm "vm1:VHDX=IDE 1 0"
```

Sie können die Informationen zur Plattenposition in **Hyper-V Manager** abrufen. Klicken Sie in der Sicht **Virtuelle Maschinen** mit der rechten Maustaste auf eine virtuelle Maschine und mit der linken Maustaste auf **Einstellungen**. Machen Sie im Abschnitt **Hardware** des Fensters **Einstellungen** den IDE-Controller oder den SCI-Controller ausfindig und klicken Sie auf **Festplatte**, um die Einstellungen der Festplatte anzuzeigen. Die Controllernummer und die Plattenposition werden im Feld **Controller** bzw. **Speicherort** angezeigt. Sie können die Informationen zur Plattenposition auch durch Ausführen des Windows PowerShell-Cmdlets **Get-VMHardDiskDrive** abrufen.
Sie können eine VM-Platte von Sicherungsoperationen ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort **vhdx=** angeben. Verwenden Sie beispielsweise **-vhdx=**, um eine VM-Platte bei der Sicherungsoperation einer VM auszuschließen:

```
dsmc backup vm "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

Wenn Sie mehrere einzuschließende oder auszuschließende VM-Platten angeben, müssen das Schlüsselwort **vhdx=** bzw. **-vhdx=** und die zugehörigen Werte durch Doppelpunkte ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
dsmc backup vm "*:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

Wenn Sie mehrere VM-Namen und VM-Platten angeben, müssen der VM-Name und die zugehörigen Werte durch Semikolons ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
dsmc backup vm "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1;vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

-MODE
Sie müssen den Sicherungsmodus, der beim Sichern einer virtuellen Maschine verwendet werden soll, angeben, indem Sie in der Befehlszeile den Parameter **-mode** hinzufügen. Die folgenden Modi können angegeben werden:

IFFull Modus 'Immer inkrementell - Vollständig'. In diesem Modus wird eine Momentaufnahme aller auf den Platten einer virtuellen Maschine belegten Blöcke auf dem Server gesichert. Die Sicherung bezieht Konfigurationsdaten und alle Platten ein.

IFIncremental
Immer inkrementell - Inkrementell. In diesem Modus wird eine Momentaufnahme der Blöcke erstellt, die sich seit der letzten (vollständigen oder inkrementellen) Sicherungsoperation 'Immer inkrementell' geändert haben. Die Sicherung umfasst Konfigurationsinformationen und alle Platten. Dieser Wert ist der Standardwert.

-VMBACKUPUPDATEGUID
Diese Option aktualisiert die global eindeutige ID (GUID) für die zu sichernde virtuelle Maschine. Dieser Parameter ist nur für die Verwendung im folgenden Szenario vorgesehen:

Sie möchten eine bereits gesicherte virtuelle Maschine mit dem Namen ORION zurückschreiben. Vor dem Herunterfahren und Ersetzen der Kopie von ORION, die in Ihrer Produktionsumgebung ausgeführt wird, möchten Sie jedoch die Konfiguration der zurückgeschriebenen virtuellen Maschine prüfen, bevor Sie sie zum Ersetzen der vorhandenen virtuellen Maschine ORION verwenden.

1. Sie schreiben die virtuelle Maschine ORION zurück und geben ihr einen neuen Namen: `dsmc restore vm Orion -vmname=Orion2`
2. Sie aktualisieren und prüfen die virtuelle Maschine ORION2 und stellen fest, dass sie zum Ersetzen der vorhandenen virtuellen Maschine mit dem Namen ORION verwendet werden kann.
3. Sie schalten ORION aus und löschen sie.
4. Sie benennen ORION2 in ORION um.
5. Bei der nächsten Sicherung von ORION mit einer Sicherung 'Immer inkrementell - Vollständig' oder 'Immer inkrementell - Inkrementell' fügen Sie dem Befehl **backup vm** den Parameter **-VMBACKUPUPDATEGUID** hinzu. Diese Option aktualisiert die GUID auf dem IBM Spectrum Protect-Server, sodass die neue GUID den gespeicherten Sicherungen für die virtuelle Maschine ORION zugeordnet wird. Die Teilsicherungskette bleibt erhalten. Vorhandene Sicherungen müssen nicht gelöscht und durch neue Sicherungen ersetzt werden.

-PREView

Dieser Parameter zeigt weitere Informationen zu einer virtuelle Maschine an, einschließlich der Kennsätze der virtuellen Festplatten, die sich in der virtuellen Maschine befinden.

Wenn Sie die Option `-preview` ausgeben, wird die Sicherungsoperation nicht gestartet. Zum Starten der Sicherungsoperation müssen Sie den Befehl 'backup' ohne die Option `-preview` ausgeben.

Sie können sowohl die Option `-preview` als auch die Option `-detail` im Befehl angeben, um Informationen zu den Unterplatten anzuzeigen, die bei der Ausführung der Sicherung eingeschlossen werden. Eine Unterplatte ist die AVHDX-Datei, die generiert wird, wenn eine Momentaufnahme einer VHDX-Datei erstellt wird.

-DETail

Dieser Parameter zeigt ausführliche Informationen über eine virtuelle Maschine an. Verwenden Sie diese Option mit `-preview`, um weitere Details über die in die Sicherungsoperation einbezogenen Platten anzuzeigen.

Wenn Sie die Option `-detail` ausgeben, wird die Sicherungsoperation nicht gestartet. Zum Starten der Sicherungsoperation müssen Sie den Befehl 'backup' ohne die Option `-detail` ausgeben.

Rückkehrcodes für Sicherungsoperationen für virtuelle Maschinen

Bei der Beendigung von Sicherungsoperationen für virtuelle Maschinen können die Rückkehrcodes ausgegeben werden, die in der folgenden Tabelle enthalten sind.

Tabelle 14. Rückkehrcodes für VM-Sicherungsbefehle

Rückkehrcode	Beschreibung
0	Ein Befehl zum Sichern einer oder mehrerer virtueller Maschinen wurde erfolgreich ausgeführt.

Tabelle 14. Rückkehrcodes für VM-Sicherungsbefehle (Forts.)

Rückkehrcode	Beschreibung
8	Ein Befehl zum Sichern mehrerer virtueller Maschinen wurde nur für einige der virtuellen Maschinen, für die der Befehl galt, erfolgreich ausgeführt. Der Protokolldatei können Sie den Verarbeitungsstatus jeder der virtuellen Maschinen entnehmen, für die der Befehl galt.
12	Gibt an, dass eine der folgenden Fehlerbedingungen aufgetreten ist: • Durch den Sicherungsbefehl konnte keine der virtuellen Maschinen gesichert werden, die Ziele der Sicherungsoperation waren. • Der Sicherungsbefehl ist fehlgeschlagen und wurde gestoppt, bevor alle angegebenen virtuellen Maschinen überprüft wurden. Untersuchen Sie die Protokolldatei, um die Fehlerursache festzustellen.

Beispielbefehle

1. Mit dem folgenden Befehl wird eine Sicherung 'Immer inkrementell - Inkrementell' einer virtuellen Hyper-V-Maschine mit dem Namen "VM1" erstellt:

   ```
   dsmc backup vm VM1 -mode=ifincremental
   ```

2. Für Windows Server 2016 oder Betriebssysteme einer höheren Version: Mit dem folgenden Befehl werden eine IDE-Platte (mit Controllernummer 1 und Plattenposition 0) und eine SCSI-Platte (mit Controllernummer 0 und Plattenposition 1) bei einer RCT-Sicherung des Typs 'Immer inkrementell - Inkrementell' der virtuellen Maschine "vm2" ausgeschlossen:

   ```
   dsmc backup vm "vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1" -mode=ifincremental
   ```

3. Für Windows Server 2016 oder Betriebssysteme einer höheren Version: Mit dem folgenden Befehl wird die Voranzeige einer RCT-Sicherung des Typs 'Immer inkrementell - Inkrementell' der virtuellen Maschine "VM05" angezeigt:

   ```
   dsmc backup vm VM05 -mode=ifincremental -preview
   ```

   In der Befehlsausgabe führt der Parameter `-preview` zur Anzeige der VHDX-Kennsätze in der virtuellen Maschine. Wird der Parameter `-detail` mit dem Parameter `-preview` angegeben, werden keine zusätzlichen Informationen für Hyper-V-RCT-Sicherungen angezeigt.

```
Befehl 'Backup VM' gestartet. Gesamtzahl zu verarbeitender VMs: 1

  1. VM-Name: VM05

        Domänenschlüsselwort: VM05
        Modus:                Immer inkrementell - Inkrementell
        Name des Zielknotens: NODE14
        Knotenname der Einheit zum Versetzen von Daten: NODE14
        Clusterressource:     Nein

        Platte[1]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05.vhdx
        Kapazität:            15,00 GB
        Größe:                10,91 GB
        Status:               Eingeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  0
        Controllerposition:   IDE 0 0

        Platte[2]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05_Disk2.vhdx
        Kapazität:            2,00 GB
        Größe:                132,00 MB
        Status:               Eingeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  0
        Controllerposition:   SCSI 0 1

Gesamtzahl verarbeiteter virtueller Maschinen: 1
```

4. Für Windows Server 2012 oder 2012 R2: Mit dem folgenden Befehl wird eine Sicherung des Typs 'Immer inkrementell - Inkrementell' der virtuellen Hyper-V-Maschine "VM03" gestartet:

   ```
   dsmc backup vm VM03 -mode=ifincremental -preview
   ```

   In der Befehlsausgabe führt der Parameter `-preview` zur Anzeige der VHDX-Kennsätze in der virtuellen Maschine:

   ```
   1. VM-Name: VM03

          Domänenschlüsselwort: all-vm
          Modus:                Immer inkrementell - Inkrementell
          Name des Zielknotens: NODE14_HV_DM
          Knotenname der Einheit zum Versetzen von Daten: NODE14_HV_DM
          Clusterressource:     Nein

          Platte[1]
          Name: \\NODE14\d$\Hyper-V\VM03\VM03\Virtual Hard Disks\VM03.vhdx
          Kapazität:            64,00 GB
          Größe:                28,91 GB
          Status:               Ausgeschlossen
          Plattentyp:           VHDX
          Anzahl Unterplatten:  1
   ```

   Wird der Parameter `-detail` mit dem Parameter `-preview` angegeben, werden die VHDX-Kennsätze und ihre Unterplatten angezeigt. Die folgende Beispielausgabe ist abgekürzt, um nur Informationen zu einer einzigen virtuellen Maschine und einer einzigen Platte anzuzeigen:

```
1. VM-Name: VM03

        Domänenschlüsselwort: all-vm
        Modus:                Immer inkrementell - Inkrementell
        Name des Zielknotens: NODE14_HV_DM
        Knotenname der Einheit zum Versetzen von Daten: NODE14_HV_DM
        Clusterressource:     Nein

        Platte[1]
        Name: \\NODE14\d$\Hyper-V\VM03\VM03\Virtual Hard Disks\VM03.vhdx
        Kapazität:            64,00 GB
        Größe:                28,91 GB
        Status:               Ausgeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  1

        Unterplatte[1]
        Name: \\NODE14\d$\Hyper-V\VM03\VM03\Virtual Hard Disks\
              VM03_94F6257B-5C61-45F1-BD62-3323DCF26954.avhdx
        Kapazität:            64,00 GB
        Größe:                180,00 MB
        Status:               Ausgeschlossen
        Plattentyp:           AVHDX
```

Beispiele für Optionsdatei

Die Option `domain.vmfull` wird für die Verarbeitung bestimmter virtueller Maschinen verwendet. Im folgenden Beispiel wird die Option `domain.vmfull` wie folgt angegeben:

```
domain.vmfull VM04,VM05
```

Mit dem folgenden Befehl wird eine Voranzeige einer vollständigen Sicherung der virtuellen Maschinen angezeigt, die durch die Option `domain.vmfull` angegeben sind. Mit dem Befehl werden Voranzeigeinformationen zu jeder virtuellen Maschine angezeigt:

```
dsmc backup vm -mode=iffull -preview
```

Die folgende Ausgabe wird unter Windows Server 2016 und Betriebssystemen einer höheren Version angezeigt:

```
Befehl 'Backup VM' gestartet. Gesamtzahl zu verarbeitender VMs: 2

  1. VM-Name: VM04

        Domänenschlüsselwort: VM04
        Modus:                Immer inkrementell - Vollständig
        Name des Zielknotens: NODE14
        Knotenname der Einheit zum Versetzen von Daten: NODE14
        Clusterressource:     Nein

        Platte[1]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM04\Virtual Hard Disks\VM04.vhdx
        Kapazität:            36,00 GB
        Größe:                9,16 GB
        Status:               Eingeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  0
        Controllerposition:   IDE 0 0

  2. VM-Name: VM05

        Domänenschlüsselwort: VM05
        Modus:                Immer inkrementell - Vollständig
        Name des Zielknotens: NODE14
```

```
        Knotenname der Einheit zum Versetzen von Daten: NODE14
        Clusterressource:     Nein

        Platte[1]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05.vhdx
        Kapazität:            15,00 GB
        Größe:                10,91 GB
        Status:               Eingeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  0
        Controllerposition:   IDE 0 0

        Platte[2]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05_Disk2.vhdx
        Kapazität:            2,00 GB
        Größe:                132,00 MB
        Status:               Eingeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  0
        Controllerposition:   SCSI 0 1

Gesamtzahl verarbeiteter virtueller Maschinen: 2
```

Die folgende Ausgabe wird unter Windows Server 2012 und 2012 R2 angezeigt:

```
Befehl 'Backup VM' gestartet. Gesamtzahl zu verarbeitender VMs: 2

  1. VM-Name: VM04

        Domänenschlüsselwort: all-vm
        Modus:                Immer inkrementell - Inkrementell
        Name des Zielknotens: NODE14_HV_DM
        Knotenname der Einheit zum Versetzen von Daten: NODE14_HV_DM
        Clusterressource:     Nein

        Platte[1]
        Name: \\NODE14\d$\Hyper-V\VM04\VM04\Virtual Hard Disks\VM04.vhdx
        Kapazität:            64,00 GB
        Größe:                28,91 GB
        Status:               Ausgeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  1

        Unterplatte[1]
        Name: \\NODE14\d$\Hyper-V\VM04\VM04\Virtual Hard Disks\
              VM04_94F6257B-5C61-45F1-BD62-3323DCF26954.avhdx
        Kapazität:            64,00 GB
        Größe:                180,00 MB
        Status:               Ausgeschlossen
        Plattentyp:           AVHDX
  2. VM-Name: VM05

        Domänenschlüsselwort: all-vm
        Modus:                Immer inkrementell - Inkrementell
        Name des Zielknotens: NODE14_HV_DM
        Knotenname der Einheit zum Versetzen von Daten: NODE14_HV_DM
        Clusterressource:     Nein

        Platte[1]
        Name: \\NODE14\d$\Hyper-V\disks\Windows 10.vhdx
        Kapazität:            20,00 GB
        Größe:                18,75 GB
        Status:               Ausgeschlossen
        Plattentyp:           VHDX
        Anzahl Unterplatten:  1

        Unterplatte[1]
```

```
                Name: \\NODE14\d$\Hyper-V\disks\
                      Windows 10_15F8A5AA-C104-4C74-8F68-B57B27592F8A.avhdx
                Kapazität:            20,00 GB
                Größe:                112,00 MB
                Status:               Ausgeschlossen
                Plattentyp:           AVHDX
                Platte[2]
                Name: \\NODE14\e$\Hyper-V\disks\Windows10_disk2\Windows10_disk2.vhdx
                Kapazität:            5,00 GB
                Größe:                5,00 GB
                Status:               Ausgeschlossen
                Plattentyp:           VHDX
                Anzahl Unterplatten:  1

                Unterplatte[1]
                Name: \\NODE14\e$\Hyper-V\disks\Windows10_disk2\
                      Windows10_disk2_15F8A5AA-C104-4C74-8F68-B57B27592F8A.avhdx
                Kapazität:            5,00 GB
                Größe:                4,00 MB
                Status:               Ausgeschlossen
                Plattentyp:           AVHDX
                Platte[3]
                Name: \\NODE14\e$\Hyper-V\disks\Windows10_disk2\Windows10_disk5.vhdx
                Kapazität:            1,00 GB
                Größe:                1,00 GB
                Status:               Eingeschlossen
                Plattentyp:           VHDX
                Anzahl Unterplatten:  1

                Unterplatte[1]
                Name: \\NODE14\e$\Hyper-V\disks\Windows10_disk2\
                      Windows10_disk5_15F8A5AA-C104-4C74-8F68-B57B27592F8A.avhdx
                Kapazität:            1,00 GB
                Größe:                4,00 MB
                Status:               Eingeschlossen
                Plattentyp:           AVHDX
Gesamtzahl verarbeiteter virtueller Maschinen: 2ANS1900I Rückkehrcode ist 0.
ANS1901I Höchster Rückkehrcode war 0.
```

Links zu Informationen zum Sichern virtueller Hyper-V-Maschinen

- „Detail" auf Seite 183
- „Domain.vmfull" auf Seite 183
- „Mbobjrefreshthresh" auf Seite 200
- „Mbpctrefreshthresh" auf Seite 201
- „Mode" auf Seite 199
- „**Query VM**" auf Seite 174
- „**Restore VM**" auf Seite 178

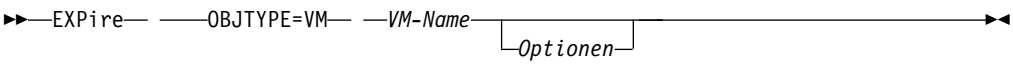
Expire

Verwenden Sie den Befehl **expire**, um die aktuelle Sicherung einer virtuellen Maschine (VM) auf dem IBM Spectrum Protect-Server zu inaktivieren.

Wenn Sie im interaktiven Modus arbeiten, werden Sie durch eine Eingabeaufforderung informiert, bevor Objekte verfallen.

Der Befehl **expire** entfernt die VM nicht vom lokalen Host. Wenn Sie eine VM verfallen lassen, die noch auf Ihrem lokalen Host vorhanden ist, wird die VM bei der nächsten inkrementellen Sicherung erneut gesichert, wenn Sie die VM nicht bei der Sicherungsverarbeitung ausschließen.

Syntax



Parameter

OBJTYPE=VM VM-Name

VM-Name gibt den Namen einer VM an. Die aktive Sicherung für die angegebene VM wird auf dem IBM Spectrum Protect-Server als verfallen markiert. Der VM-Name darf keine Platzhalterzeichen enthalten.

Wird objtype=VM angegeben, markiert der Befehl 'expire' nur vollständige VM-Sicherungen (MODE=IFFULL) für die im Parameter VM-Name angegebene VM als verfallen.

Tabelle 15. Befehl 'expire': zugehörige Optionen

Option	Verwendung in
dateformat „Dateformat" auf Seite 181	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
noprompt „Noprompt" auf Seite 202	Nur Befehlszeile.
numberformat „Numberformat" auf Seite 202	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
pick „Pick" auf Seite 203	Nur Befehlszeile.
timeformat „Timeformat" auf Seite 206	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiel

Task Die aktuelle Sicherung der VM mit dem Namen vm_test inaktivieren.

Befehl: `dsmc expire –objtype=VM vm_test`

Query VM

Verwenden Sie den Befehl **query VM**, um die erfolgreichen Sicherungen von virtuellen Maschinen (VMs) aufzulisten und zu verifizieren.

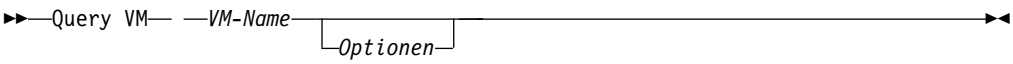
Query VM für virtuelle Microsoft Hyper-V-Maschinen

Verwenden Sie den Befehl **query vm**, um festzustellen, welche virtuellen Hyper-V-Maschinen gesichert wurden.

Unterstützte Clients

Dieser Befehl ist auf Windows-Clients gültig, die auf einem Hyper-V-Hostsystem installiert sind.

Syntax



Parameter

VM-Name

Gibt den Hostnamen der virtuellen Maschine an, die abgefragt werden soll. Beim Namen der virtuellen Maschine muss die Groß-/Kleinschreibung beachtet werden. Wenn Sie einen VM-Namen in dem Befehl angeben, darf der Name keine Platzhalterzeichen enthalten.

Wenn Sie den Namen der virtuellen Maschine nicht angeben, zeigt der Befehl alle VM-Sicherungen auf dem IBM Spectrum Protect-Server an.

Tabelle 16. Befehl Query VM: Zugehörige Optionen für Abfragen virtueller Hyper-V-Maschinen

Option	Verwendung
`detail`	Befehlszeile. Zeigt die Details zu jeder Platte (Kennsatz, Name) und ihren Status (geschützt oder ausgeschlossen) sowie Leistungsstatistik für immer inkrementelle Sicherungen an.
`inactive`	Befehlszeile
`pitdate`	Befehlszeile
`pittime`	Befehlszeile

Beispiele

Task Alle virtuellen Maschinen auflisten, die von Data Protection for Microsoft Hyper-V auf dem Hyper-V-Host gesichert wurden.

```
dsmc query vm
```

Beispiele für Query VM (Hyper-V)

Das folgende Beispiel zeigt einen Befehl **query VM**, mit dem Übersichtsdaten zu allen virtuellen Hyper-V-Maschinen angezeigt, die gesichert wurden.

```
dsmc query vm

VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe        Typ      A/I Position  Virtuelle Maschine
---  ------------------  ----------  -----------  ------  --- --------  ---------------
  1  19.03.2017 17:54:34  STANDARD       17,00 GB  IFFULL    A  SERVER    DeptA_VM05
  2  20.03.2017 01:51:34  STANDARD       15,00 GB  IFINCR    A  SERVER    DeptA_VM_W2k08R2
  3  20.03.2017 01:46:19  STANDARD       36,00 GB  IFFULL    A  SERVER    DeptA_VM04
```

Mit dem folgenden Befehl **query VM** mit der Option `-detail` werden detaillierte Informationen zu virtuellen Hyper-V-Maschinen angezeigt, die gesichert wurden. Die detaillierte Ausgabe umfasst den Typ der ausgeführten Sicherung, die Größe der virtuellen Maschine, Informationen zu ihren Platten und statistische Daten.

```
dsmc query vm -detail

VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe        Typ      A/I Position  Virtuelle Maschine
---  ------------------  ----------  -----------  ------   --- --------  ---------------
  1  19.03.2017 17:54:34  STANDARD       17,00 GB  IFFULL    A  SERVER    DeptA_VM05
       Größe dieser Teilsicherung: nicht zutreffend
       Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
       Zusätzliches Datenvolumen: 0
       IBM Spectrum Protect-Objektfragmentierung: 0
       Sicherung ist dargestellt durch: 99 IBM Spectrum Protect-Objekte
       Art des Anwendungsschutzes: nicht zutreffend
       Die Sicherung ist komprimiert: Nein
       Die Sicherung ist dedupliziert: Nein
       Momentaufnahmetyp: Hyper-V RCT - anwendungskonsistent
       Platte[1]Name: DeptA_VM05.vhdx
       Platte[1]Position: IDE 0 0
       Platte[1]Status: Geschützt
       Platte[2]Name: DeptA_VM05_Disk2.vhdx
       Platte[2]Position: SCSI 0 1
       Platte[2]Status: Geschützt
       Platte[3]Name:  Platte 7 2,00 GB Bus 0 LUN 4 Ziel 0
       Platte[3]Position: SCSI 0 0
       Platte[3]Status: übersprungen: Physische Platte
       Platte[4]Name:  Platte 8 2,50 GB Bus 0 LUN 5 Ziel 0
       Platte[4]Position: SCSI 0 2
       Platte[4]Status: Übersprungen: Physische Platte
  2  20.03.2017 01:51:34  STANDARD       15,00 GB  IFINCR    A  SERVER    DeptA_VM_W2k08R2
       Größe dieser Teilsicherung: 544,00 KB
       Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
       Zusätzliches Datenvolumen: 0
       IBM Spectrum Protect-Objektfragmentierung: 2
       Sicherung ist dargestellt durch: 37 IBM Spectrum Protect-Objekte
       Art des Anwendungsschutzes: nicht zutreffend
       Die Sicherung ist komprimiert: Nein
       Die Sicherung ist dedupliziert: Nein
       Momentaufnahmetyp: Hyper-V RCT - absturzkonsistent
       Platte[1]Name: DeptA_VM_W2k08R2.vhdx
       Platte[1]Position: IDE 0 0
       Platte[1]Status: Geschützt
  3  20.03.2017 01:46:19  STANDARD       36,00 GB  IFFULL    A  SERVER    DeptA_VM04
       Größe dieser Teilsicherung: nicht zutreffend
       Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
       Zusätzliches Datenvolumen: 0
       IBM Spectrum Protect-Objektfragmentierung: 0
       Sicherung ist dargestellt durch: 79 IBM Spectrum Protect-Objekte
       Art des Anwendungsschutzes: nicht zutreffend
       Die Sicherung ist komprimiert: Nein
       Die Sicherung ist dedupliziert: Nein
       Momentaufnahmetyp: Hyper-V RCT - anwendungskonsistent
       Platte[1]Name: DeptA_VM04.vhdx
       Platte[1]Position: IDE 0 0
       Platte[1]Status: Geschützt
--------------------------------------------------------------------------------
       Alle Durchschnittswerte werden nur für oben angezeigte immer inkrementelle Sicherungen berechnet.
       Durchschnittsgröße der Teilsicherung: 544,00 KB
       Durchschnittliche Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
       Durchschnittsaufwand für zusätzliche Daten: 0
       Durchschnittliche Objektfragmentierung: 0
       Durchschnittliche Anzahl Objekte pro Sicherung: 71
```

Die detaillierte Ausgabe umfasst auch den Momentaufnahmetyp und Datenträgerinformationen wie die folgenden:

Momentaufnahmetyp
Der Typ der Momentaufnahme, der während der VM-Sicherungsoperation erstellt wurde:

Hyper-V RCT - anwendungskonsistent
Eine Momentaufnahme im Quiescemodus, die mit Hyper-V Resilient Change Tracking (RCT) unter Windows Server 2016 erstellt wurde.

Hyper-V RCT - absturzkonsistent
Eine Momentaufnahme ohne Quiesce, die mit Hyper-V RCT unter Windows Server 2016 erstellt wurde.

Hyper-V VSS
Eine Momentaufnahme, die mit dem Volumeschattenkopiedienst (Volume Shadow Copy Service, VSS) unter Windows Server 2012 oder Windows Server 2012 R2 erstellt wurde.

Platte[*n*]Position
Die Plattenposition der VM-Platte *n*; dabei ist *n* eine Zahl. Die Plattenposition besteht aus dem Plattencontrollertyp ("IDE" oder "SCSI") gefolgt von der Controllernummer und der Einheitenpositionsnummer.

Platte[*n*]Status
Der Sicherungsstatus der VM-Platte *n*; dabei ist *n* eine Zahl.

Geschützt
Gibt an, dass die Daten auf der VM-Platte gesichert werden.

Übersprungen: Nach Benutzer ausgeschlossen
Gibt an, dass die VM-Platte während Sicherungsoperationen wie durch die Option `exclude.vmdisk` angegeben ausgeschlossen wird.

Übersprungen: Physische Platte
Gibt an, dass es sich bei der VM-Platte um eine physische Platte (Durchgriffsplatte) handelt, deren Daten nicht gesichert werden. Es werden nur die Plattenkonfigurationsinformationen gesichert.

Das folgende Beispiel zeigt die Syntax, die verwendet werden muss, um die detaillierte Ausgabe für eine bestimmte virtuelle Maschine mit dem Namen `DeptA_VM_W2k08R2` aufzulisten.

```
dsmc query vm DeptA_VM_W2k08R2 -detail

VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe        Typ      A/I Position  Virtuelle Maschine
---  ------------------  ----------  -----------  ------  --- --------  ---------------
  1  20.03.2017 01:51:34  STANDARD       15,00 GB  IFINCR    A  SERVER    DeptA_VM_W2k08R2
       Größe dieser Teilsicherung: 544,00 KB
       Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
       Zusätzliches Datenvolumen: 0
       IBM Spectrum Protect-Objektfragmentierung: 2
       Sicherung ist dargestellt durch: 37 IBM Spectrum Protect-Objekte
       Art des Anwendungsschutzes: nicht zutreffend
       Die Sicherung ist komprimiert: Nein
       Die Sicherung ist dedupliziert: Nein
       Momentaufnahmetyp: Hyper-V RCT - absturzkonsistent
       Platte[1]Name: Jimmy_VM_Windows2008R2.vhdx
       Platte[1]Position: IDE 0 0
       Platte[1]Status: Geschützt
--------------------------------------------------------------------------------
       Alle Durchschnittswerte werden nur für oben angezeigte immer inkrementelle Sicherungen berechnet.
       Durchschnittsgröße der Teilsicherung: 544,00 KB
       Durchschnittliche Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
       Durchschnittsaufwand für zusätzliche Daten: 0
       Durchschnittliche Objektfragmentierung: 2
       Durchschnittliche Anzahl Objekte pro Sicherung: 37
```

Zugehörige Verweise:

„Exclude.vmdisk" auf Seite 186

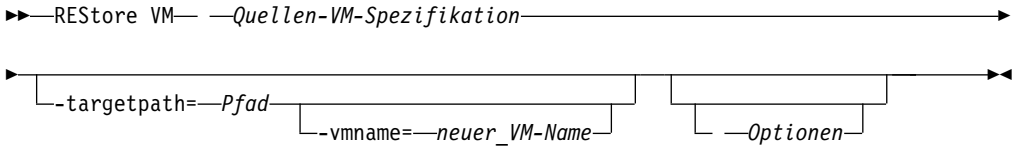
„Vmprocessvmwithphysdisks" auf Seite 215

Restore VM

Mit dem Befehl **restore vm** können Sie eine virtuelle Microsoft Hyper-V-Maschine zurückschreiben, die zuvor von IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V gesichert wurde.

Wenn die virtuelle Maschine, die Sie zurückschreiben, auf dem Hyper-V-Host-Server vorhanden ist, wird sie heruntergefahren und gelöscht, bevor sie aus dem Image zurückgeschrieben wird, das auf dem IBM Spectrum Protect-Server gespeichert ist. Bei der Operation 'Restore VM' wird dann die virtuelle Maschine so erstellt, dass ihr Inhalt und ihre Konfiguration mit dem Stand zum Zeitpunkt der Sicherung übereinstimmen. Obwohl die virtuelle Maschine vor dem Löschen heruntergefahren wird, empfiehlt es sich, sie vor der Ausführung des Befehls **Restore VM** manuell herunterzufahren, damit alle aktiven Anwendungsaktivitäten ordnungsgemäß abgeschlossen werden.

Syntax



Parameter

Der Parameter ***Quellen-VM-Spezifikation*** ist erforderlich. Die übrigen Parameter sind optional. Bestimmen Sie anhand der folgenden Szenarios die zu verwendenden Parameter:

- Verwenden Sie nur den Parameter ***Quellen-VM-Spezifikation***, um die virtuelle Maschine unter dem ursprünglichen VM-Namen in den ursprünglichen Pfad zurückzuschreiben. Die virtuelle Maschine wird mit ihrer ursprünglichen Hyper-V-GUID zurückgeschrieben.
- Verwenden Sie die Parameter ***Quellen-VM-Spezifikation*** und **-targetpath**, um die virtuelle Maschine unter dem ursprünglichen VM-Namen in einen Alternativpfad zurückzuschreiben. Die virtuelle Maschine mit mit einer neuen Hyper-V-GUID in den angegebenen Pfad zurückgeschrieben. Die virtuelle Maschine im ursprünglichen Pfad wird nicht gelöscht.
- Verwenden Sie die Parameter ***Quellen-VM-Spezifikation***, **-targetpath** und **-vmname**, um die virtuelle Maschine unter einem neuen VM-Namen in einen Alternativpfad zurückzuschreiben. Die virtuelle Maschine wird mit dem neuen Namen und einer neuen Hyper-V-GUID in den angegebenen Pfad zurückgeschrieben. Die virtuelle Maschine mit dem ursprünglichen Namen im ursprünglichen Pfad wird nicht gelöscht.

Der Parameter **-vmname** ist nur für die Zurückschreibung virtueller Maschinen gültig, die in den Modi `iffull` oder `ifincremental` gesichert wurden. Dieser Parameter wird bei virtuellen Maschinen ignoriert, die mit den in vorherigen Produktreleases bereitgestellten Modi `full` oder `incremental` gesichert wurden.

Quellen-VM-Spezifikation
Gibt den Namen der virtuellen Maschine an, die zurückgeschrieben werden soll. Beim Namen der virtuellen Maschine muss die Groß-/Kleinschreibung beachtet werden. Im Namen der virtuellen Maschine können keine Platzhalterzeichen verwendet werden.

-targetpath=*Pfad*
Gibt den Pfad an, in den die virtuelle Maschine zurückgeschrieben werden soll.

Dieser Parameter ist erforderlich, wenn der Parameter **-vmname** verwendet wird; andernfalls ist er optional. Verwenden Sie diesen Parameter, um die virtuelle Maschine in einen Alternativpfad zurückzuschreiben.

-vmname=*neuer_VM-Name*
Gibt einen neuen Namen für die virtuelle Maschine an. Der Name kann 1-100 Zeichen enthalten. Die folgenden Zeichen sind nicht gültig: `\ / : ; , * ? " ' < > |`

Für diesen Parameter ist der Parameter **-targetpath** erforderlich.

Tabelle 17. Befehl 'Restore VM': zugehörige Optionen beim Zurückschreiben virtueller Hyper-V-Maschinen

Option	Verwendung in
`inactive`	Befehlszeile
`pick`	Befehlszeile
`pitdate`	Befehlszeile
`pittime`	Befehlszeile
`replace`	Befehlszeile, Clientoptionsdatei oder Clientvorgabeneditor.
`vmbackdir`	Befehlszeile, Clientoptionsdatei.

Beispiele

Task Zurückschreibung der neuesten Sicherungsversion einer virtuellen Maschine mit dem Namen 'myVM'.

```
dsmc restore vm myvm
```

Anmerkung: Wenn Sie eine gelöschte VM zurückgeschrieben haben oder wenn Sie eine VM mit einem neuen VM-Namen zurückgeschrieben haben, müssen Sie die zurückgeschriebene VM mit Microsoft Failover Cluster Manager, mit System Center Virtual Machine Manager oder mit PowerShell-Cmdlets für Hochverfügbarkeit konfigurieren. Informationen zur Konfiguration einer VM für Hochverfügbarkeit finden Sie in der Microsoft-Dokumentation.

Kapitel 9. Optionsreferenz

Die folgenden Abschnitte enthalten ausführliche Informationen über alle Clientoptionen, die für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V-Operationen verwendet werden.

Zu jeder Option werden die folgenden Informationen bereitgestellt:

- eine Beschreibung
- ein Syntaxdiagramm
- ausführliche Beschreibungen der Parameter
- Beispiele für die Verwendung der Option in der Clientoptionsdatei (falls zutreffend)
- Beispiele für die Verwendung der Option in der Befehlszeile (falls zutreffend)

Optionen mit dem Befehlszeilenbeispiel **Trifft nicht zu** können nicht in der Befehlszeile oder in geplanten Befehlen verwendet werden.

Dateformat

Die Option `dateformat` gibt das Format an, das beim Anzeigen und Eingeben von Datumsangaben verwendet werden soll.

Verwenden sie diese Option zum Ändern des Standarddatumsformats für die Sprache des von Ihnen verwendeten Nachrichtenrepositorys.

Standardmäßig erhalten der Client für Sichern/Archivieren und der Verwaltungsclient Formatinformationen aus der Definition der Ländereinstellung, die aktiv war, als der Client gestartet wurde. Entnehmen Sie Details zum Definieren Ihrer Ländereinstellung der Dokumentation zu Ihrem lokalen System.

Sie können die Option `dateformat` mit dem Befehl **`expire`** verwenden.

Wenn Sie mit einem Befehl die Option `dateformat` angeben, muss sie sich vor den Optionen `fromdate` und `pitdate` befinden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option angeben auf der Registerkarte **Ländereinstellungen**, Dropdown-Liste **Datumsformat** des Vorgabeneditors.

Syntax

Parameter

Formatnummer
Zeigt das Datum in einem der folgenden Formate an. Wählen Sie die Nummer des gewünschten Datumsformats aus:
1 MM/TT/JJJJ

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:
- Englisch (Vereinigte Staaten)
- Chinesisch (traditionell)
- Koreanisch

2 TT-MM-JJJJ

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:
- Portugiesisch (Brasilien)
- Italienisch

3 JJJJ-MM-TT

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:
- Japanisch
- Chinesisch (vereinfacht)
- Polnisch

4 TT.MM.JJJJ

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:
- Deutsch
- Französisch
- Spanisch
- Tschechisch
- Russisch

5 JJJJ.MM.TT

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:
- Ungarisch

6 JJJJ/MM/TT

7 TT/MM/JJJJ

Beispiele

Optionsdatei:

```
dateformat 3
```

Befehlszeile:

```
-date=3
```

Diese Option ist gültig in der Anfangsbefehlszeile und im interaktiven Modus. Wenn Sie diese Option im interaktiven Modus verwenden, wirkt sie sich nur auf den Befehl aus, mit dem sie angegeben wird. Nachdem dieser Befehl ausgeführt wurde, wird der Wert auf den Wert zurückgesetzt, der zu Beginn der interaktiven Sitzung gültig war. Dies ist der Wert aus der Datei dsm.opt, falls er nicht von der Anfangsbefehlszeile oder durch eine vom Server erzwungene Option überschrieben wurde.

Weitere Hinweise zur Angabe von Datums- und Zeitformaten

Das Datums- oder Zeitformat, das Sie mit dieser Option angeben, muss verwendet werden, wenn Optionen verwendet werden, deren Eingabe aus Datums- und Zeitangaben besteht. Beispiele sind: `totime`, `fromtime`, `todate`, `fromdate` und `pittime`.

Wenn Sie beispielsweise die Option `timeformat` als `TIMEFORMAT 4` angeben, muss der Wert, den Sie für die Option `fromtime` oder `totime` angeben, als Zeit angegeben werden, wie z. B. `12:24:00pm`. Die Angabe `13:24:00` wäre nicht gültig, da `TIMEFORMAT 4` als Angabe für die Stunde eine ganze Zahl, die kleiner-gleich 12 ist, erfordert. Wenn in einer Option für die Stunde Werte bis zu 24 angegeben und Kommas als Trennzeichen verwendet werden sollen, müssen Sie `TIMEFORMAT 2` angeben.

Detail

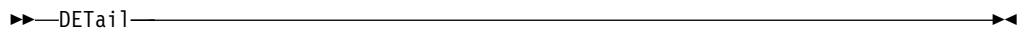
Verwenden Sie die Option `detail` zum Anzeigen von Informationen zur Verwaltungsklasse, zum Dateibereich und zur Sicherung.

Verwenden Sie `detail` mit dem Befehl **query vm** zum Anzeigen der folgenden Statistikdaten:

- Die durchschnittliche Zahl an IBM Spectrum Protect-Objekten, die zum Beschreiben eines einzelnen Megablocks benötigt wird. Dabei werden alle Megablöcke in einer Sicherung berücksichtigt.
- Die durchschnittliche Zahl an IBM Spectrum Protect-Objekten, die zum Beschreiben eines einzelnen Megablocks für alle Megablöcke in einem Dateibereich benötigt wird.
- Die Anzahl der Sicherungen, die seit der Erstellung der letzten Gesamtsicherung von den Produktionsplatten erstellt wurden.

Die für **query vm** zurückgegebenen Werte können Ihnen bei der Optimierung der heuristischen Verfahren helfen (siehe die Optionen `Mbobjrefreshthresh` und `Mbpctrefreshthresh`), um den Werteauslöser für die Aktualisierung von Megablöcken zu optimieren.

Syntax



Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc query vm -detail
```

Domain.vmfull

Die Option `domain.vmfull` gibt die Imagegesamtsicherungsoperationen für virtuelle Maschinen eingeschlossen werden sollen.

Domain.vmfull für virtuelle Microsoft Hyper-V-Maschinen

Verwenden Sie für Hyper-V-VM-Sicherungen die Option `domain.vmfull`, um anzugeben, welche Hyper-V-VMs verarbeitet werden, wenn Sie einen Befehl **backup vm** ausführen, ohne Hyper-V-VM-Namen anzugeben.

Sie können die zu verarbeitenden VMs mit einer der folgenden Methoden angeben:

- Verwenden Sie die Option `VM=` und geben Sie den Namen einer virtuellen Maschine an.
- Geben Sie eine durch Kommas getrennte Liste mit den Namen der virtuellen Maschinen an.
- Verwenden Sie eine Syntax mit Platzhalterzeichen, um die virtuellen Maschinen zu verarbeiten, die dem Namensmuster entsprechen.

- Verwenden Sie die Option *VM-Name*:vhdx=, um die VM-Festplatte (VHDX) anzugeben, die bei der Hyper-V-Sicherungsoperation einer VM ein- oder ausgeschlossen werden soll.
- Verwenden Sie den Parameter `all-vm` auf Domänenebene. Sie können auch eine oder mehrere virtuelle Maschinen mithilfe des Schlüsselworts `VM=` einschließen oder VMs mithilfe der Syntax `-VM=` ausschließen.

Die mit der Option `domain.vmfull` angegebenen virtuellen Maschinen werden nur verarbeitet, wenn der Befehl **backup vm** ohne Angabe einer virtuellen Maschine oder eine Liste virtueller Maschinen in die Befehlszeile eingegeben wird.

Achtung: Bei Microsoft Hyper-V-Operationen ist **all-vm** der einzige gültige Parameter auf Domänenebene für die Option `domain.vmfull`. Sie können auch virtuelle Maschinen mit dem Schlüsselwort `VM=` einschließen oder mit der Syntax `-VM=` ausschließen.

Unterstützte Clients

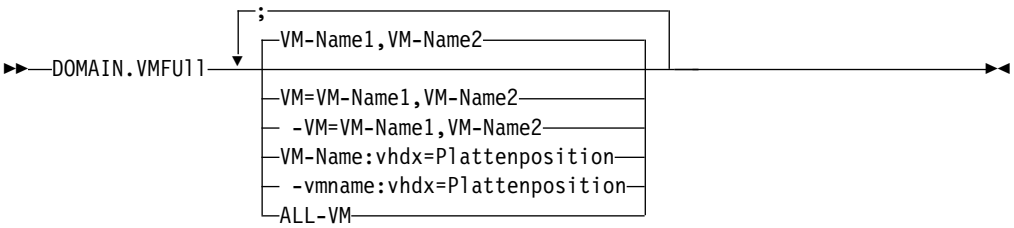
Diese Option kann für unterstützte Windows-Clients verwendet werden. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Definieren Sie diese Option in den Clientoptionen, über die Befehlszeile oder mithilfe der Registerkarte **VM-Sicherung** im Profileditor.

Einschränkung: Der Parameter *VM-Name*:vhdx=*VHDX-Position* kann nicht im Profileditor festgelegt werden. Schließen Sie diese Einstellung in die Optionsdatei oder in die Befehlszeile ein, wenn Sie einen Befehl **backup vm** ausführen:

Syntax für virtuelle Microsoft Hyper-V-Maschinen



Syntaxregeln: Mehrere Schlüsselwörter müssen jeweils durch ein Semikolon voneinander getrennt werden. Hinter den Semikolons dürfen keine Leerzeichen stehen. Mehrere Maschinen- oder Domänennamen müssen durch Kommas und ohne Leerzeichen getrennt werden. Beispiele finden Sie bei `vm=`*`VM-Name`*.

Parameter

VM-Name

Definiert den Namen der virtuellen Maschine, die verarbeitet werden soll. Sie können eine Liste mit Hostnamen virtueller Maschinen angeben. Trennen Sie die Namen jeweils durch ein Komma voneinander (`vm1,VM2,Vm5`). Bei den Namen muss die Groß-/Kleinschreibung beachtet werden und die Groß-/Kleinschreibung muss mit der Schreibweise übereinstimmen, die auf dem Hyper-V-Host in der Sicht **Hyper-V-Manager** > **Virtuelle Maschinen** angezeigt wird.

vm=*VM-Name*

Das Schlüsselwort vm= gibt an, dass die nächste Gruppe von Werten eine Liste mit Namen virtueller Maschinen ist. Das Schlüsselwort vm= ist der Standardwert und ist nicht erforderlich.

In diesem Beispiel ist vm= nicht angegeben und die Maschinennamen sind durch Kommas getrennt.

```
domain.vmfull my_vm1,my_vm2
```

Wenn Sie mehrere Schlüsselwörter angeben, wie beispielsweise vm= und -vm=, müssen die Werte, auf die sich die Schlüsselwörter beziehen, durch Semikolons und ohne Zwischenleerschritte getrennt werden:

```
domain.vmfull vm=my_vm1;vm=my_vm2
domain.vmfull -vm=my_vm3;-vm=my_vm4
```

Für die Auswahl von Namen virtueller Maschinen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen. Beispiele:

- Alle Dateien ausschließen, deren Hostname die Zeichenfolge „test" enthält: -vm=*test*
- Alle virtuellen Maschinen mit Namen wie den folgenden einschließen: „test20", „test25", „test29", „test2A":

  ```
  vm=test2?
  ```

Sie können eine virtuelle Maschine von einer Sicherungsoperation ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort vm= angeben. Beispielsweise wird -vm für den Ausschluss einer bestimmten Maschine oder mehrerer Maschinen von einer Sicherung auf Domänenebene (wie beispielsweise ALL-VM) verwendet. Wenn „vm1" der Name einer virtuellen Maschine ist, können Sie alle virtuellen Maschinen in der Domäne sichern, die virtuelle Maschine „vm1" jedoch von der Sicherung ausschließen. Definieren Sie die folgende Option:

```
domain.vmfull all-vm;-vm=vm1
```

Sie können mit dem Ausschlussoperator (-) keine Domäne ausschließen, beispielsweise ALL-VM. Der Ausschlussoperator funktioniert nur auf der Ebene der Namen der virtuellen Maschinen.

VM-Name*:vhdx=*VHDX-Position

Diese Option gibt die Festplatte der virtuellen Maschine (VHDX) an, die bei Sicherungsoperationen für virtuelle Hyper-V-Maschinen eingeschlossen werden soll.

Die Variable *VM-Name* gibt den Namen der zu sichernden virtuellen Maschine an. Für die Auswahl von Namen virtueller Maschinen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen.

Das Schlüsselwort :vhdx=*Plattenposition* gibt die Position der Platte der virtuellen Maschine an, die in die Sicherungsoperation eingeschlossen werden soll. Die Plattenposition, die durch die Variable *Plattenposition* angegeben wird, muss mit "SCSI" oder "IDE" beginnen, gefolgt von der Controllernummer und der Einheitenpositionsnummer. Beispiel:

```
domain.vmfull "vm1:VHDX=IDE 1 0"
domain.vmfull "vm*:VHDX=SCSI 0 1"
domain.vmfull "vm?:VHDX=SCSI 0 1"
```

Sie können eine virtuelle Maschine von Sicherungsoperationen ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort vhdx= angeben. Verwenden Sie beispielsweise -vhdx=, um eine VM-Platte von der Sicherungsoperation für eine virtuelle Maschine auszuschließen. Beispiel:

```
domain.vmfull "vm1:-VHDX=IDE 1 0"
```

Wenn Sie mehrere einzuschließende oder auszuschließende Platten virtueller Maschinen angeben, müssen das Schlüsselwort vhdx= bzw. -vhdx= und die zugehörigen Werte durch Doppelpunkte ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
domain.vmfull "vm1:vhdx=IDE 1 0:vhdx=SCSI 0 1"
```

Wenn Sie mehrere Namen virtueller Maschinen und Platten virtueller Maschinen angeben, müssen der VM-Name und die zugehörigen Werte durch Semikolons ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"
domain.vmfull "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1;vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

all-vm
Diese Option gibt an, dass bei einer Operation **backup vm** alle virtuellen Hyper-V-Maschinen verarbeitet werden, die dem Hyper-V-Host bekannt sind.

Beispiele für virtuelle Microsoft Hyper-V-Maschinen

Optionsdatei:

Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull   all-vm
```

Alle virtuellen Maschinen mit Ausnahme der Maschinen mit dem Namenssuffix _test in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull all-vm;-vm=*_test
```

Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen, jedoch die virtuellen Maschinen testvm1 und testmvm2 ausschließen.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

IDE-Platten (mit Controller 1 und Plattenposition 0) und SCSI-Platten (mit Controller 0 und Plattenposition 1) in Hyper-V-Sicherungsoperationen für die virtuellen Maschinen vm1 und vm2 einschließen.

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"
```

Einschränkung: Sie können die Option all-vm nicht zusammen mit der Option *VM-Name:***-vhdx=** in einer einzigen Domänenspezifikation in der Optionsdatei oder in der Befehlszeile verwenden. Beispielsweise ist domain1 = all-vm:-VHDX=SCSI 0 0 nicht gültig.

Exclude.vmdisk

Mit der Option EXCLUDE.VMDISK wird eine Platte einer virtuellen Maschine von Sicherungsoperationen ausgeschlossen.

Die Option EXCLUDE.VMDISK gibt den Kennsatz einer VM-Platte an, die von einer Operation **backup vm** ausgeschlossen werden soll. Wenn Sie im Befehl **backup vm** eine Platte ausschließen, überschreiben die Befehlszeilenparameter alle Anweisungen EXCLUDE.VMDISK in der Optionsdatei.

EXCLUDE.VMDISK für virtuelle Microsoft Hyper-V-Maschinen

Verwenden Sie die Option EXCLUDE.VMDISK, um eine Platte einer virtuellen Maschine bei Hyper-V-Sicherungsoperationen auszuschließen.

Unterstützte Clients

Diese Option kann für alle unterstützten Windows-Clients verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Befehlszeilenparameter überschreiben Anweisungen in der Optionsdatei.

Syntax

Parameter

VM-Name

Gibt den Namen der VM an, die eine Platte enthält, die von einer Operation **backup vm** ausgeschlossen werden soll. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung EXCLUDE.VMDISK können Sie nur einen einzigen VM-Namen angeben. Geben Sie weitere Anweisungen EXCLUDE.VMDISK für jede VM-Platte an, die ausgeschlossen werden soll.

Der VM-Name kann einen Stern (*) enthalten, der einer beliebigen Zeichenfolge entspricht, und ein Fragezeichen (?), das einem beliebigen einzelnen Zeichen entspricht. Wenn der VM-Name Leerzeichen enthält, schließen Sie ihn in Anführungszeichen („ ”) ein.

Tipp: Wenn der VM-Name Sonderzeichen enthält, wie beispielsweise eckige Klammern ([oder]), wird der VM-Name möglicherweise nicht korrekt abgeglichen. Wenn ein VM-Name Sonderzeichen enthält, stellen Sie die Sonderzeichen mithilfe von Fragezeichen (?) dar.

Um beispielsweise eine Platte einer virtuellen SCSI-Maschine von der Sicherung einer VM mit dem Namen "Windows VM3 [2012R2]" auszuschließen, verwenden Sie in der Optionsdatei die folgende Syntax:

```
EXCLUDE.VMDISK "Windows VM3 ?2012R2?" "SCSI 0 1"
```

Plattenposition

Geben Sie die Position der Festplatte der virtuellen Maschine (VHDX) an, die bei Hyper-V-Sicherungsoperationen ausgeschlossen werden soll. Die Plattenpositionsbezeichnung muss mit "SCSI" oder "IDE" beginnen, gefolgt von der Controllernummer und der Einheitenpositionsnummer. Platzhalterzeichen sind nicht zulässig.

Tipp: Verwenden Sie den Befehl **backup vm** mit der Option -preview, um die Position der Platten in einer bestimmten VM zu bestimmen. Informationen zur Syntax finden Sie in der Beschreibung des Befehls "**Backup VM**".

Beispiele

Optionsdatei

Die Windows-Systemplatte von allen virtuellen Maschinen, deren Name mit `WinVM` beginnt, mit der folgenden Anweisung in der Optionsdatei ausschließen:

```
exclude.vmdisk WinVM* "IDE 0 0"
```

Die virtuelle Maschine `vm1` enthält eine Platte der virtuellen Maschine mit dem Contollertyp IDE, der Controllernummer 1 und der Einheitenposition 0. Um diese virtuelle Maschine von Operationen **backup vm** auszuschließen, geben Sie in der Optionsdatei die folgende Anweisung an:

```
EXCLUDE.VMDISK vm1 "IDE 1 0"
```

Die virtuelle Maschine `vm2` enthält eine Platte der virtuellen Maschine mit dem Contollertyp SCSI, der Controllernummer 0 und der Einheitenposition 1. Schließen Sie diese Platte von Sicherungsoperationen aus, indem Sie in der Optionsdatei die folgende Anweisung angeben:

```
EXCLUDE.VMDISK vm2 "SCSI 0 1"
```

Befehlszeile:

Die Befehlszeilenbeispiele zeigen die Verwendung des Ausschlussoperators (-) vor dem Schlüsselwort `vhdx=`, um anzugeben, dass die Platte ausgeschlossen werden soll.

Schließen Sie eine IDE-Platte (mit der Controllernummer 1 und der Einheitenposition 0) von der Sicherungsoperation für die virtuelle Maschine `vm1` aus:

```
dsmc backup vm "vm1:-vhdx=IDE 1 0"
```

Schließen Sie eine SCSI-Platte (mit der Controllernummer 0 und der Einheitenposition 1) von der Sicherungsoperation für die virtuelle Maschine `vm2` aus:

```
dsmc backup vm "vm2:-vhdx=SCSI 0 1"
```

Einschränkung: Sie können die Option `all-vm` nicht zusammen mit der Option *VM-Name:*`-vhdx=` in der Befehlszeile oder in der Optionsdatei verwenden.

Tipps für die Zurückschreibung von Hyper-V-VMs mit ausgeschlossenen Platten

Während einer VM-Zurückschreibungsoperation wird eine Informationsnachricht angezeigt, die angibt, dass eine VM-Platte nicht zurückgeschrieben wird, da sie von der Sicherungsoperation ausgeschlossen war. Bei der Zurückschreibungsoperation wird auch geprüft, ob die ursprüngliche Plattendatei noch im Zurückschreibungszielordner vorhanden ist. Wenn die ursprüngliche Plattendatei noch vorhanden ist, wird sie wieder mit der zurückgeschriebenen VM verbunden. Andernfalls wird eine leere Plattendatei mit denselben Attributen (wie beispielsweise Dateiname, Plattengröße und Blockgröße) erstellt und die leere Plattendatei mit der zurückgeschriebenen VM verbunden.

Nach einer Zurückschreibungsoperation stimmt die Controller- und Datenträgerreihenfolge in der zurückgeschriebenen VM mit der in der ursprünglichen VM weiterhin überein. Sie müssen die Plattenposition in der Option `EXCLUDE.VMDISK` nicht für zukünftige Sicherungsoperationen der zurückgeschriebenen VM anpassen.

Wenn Sie jedoch einen SCSI-Controller manuell entfernen, werden die Nummern aller nachfolgenden SCSI-Controller geändert. Wenn Sie beispielsweise "SCSI 0" entfernen, wird der nächste SCSI-Controller (der zuvor "SCSI 1" war) zu "SCSI 0". In diesem Fall müssen Sie die VM-Plattenposition in der Option `EXCLUDE.VMDISK` aktualisieren.

Die Plattenpositionsinformationen, wie beispielsweise "SCSI 0 0", werden in Nachrichten für Sicherungs-, Zurückschreibungs- und Abfrageoperationen angezeigt.

Zugehörige Verweise:

„**Backup VM**" auf Seite 166

„**Restore VM**" auf Seite 178

„Domain.vmfull" auf Seite 183

„Include.vmdisk" auf Seite 191

Inactive

Verwenden Sie die Option `inactive`, um sowohl aktive als auch inaktive Objekte anzuzeigen.

Sie können die Option `inactive` mit den Befehlen **query vm** und **restore vm** verwenden.

Wichtig: Wenn Sie die Option `inactive` während einer Zurückschreibungsoperation verwenden, verwenden Sie auch die Option `pick`, da alle Versionen in einer unbestimmten Reihenfolge zurückgeschrieben werden. Diese Option wird implizit verwendet, wenn `pitdate` verwendet wird.

Syntax

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore vm VM1 -inactive
```

Include.vm

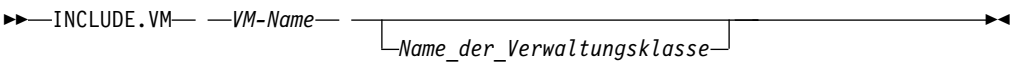
Diese Option überschreibt die mit der Option `vmmc` angegebene Verwaltungsklasse.

Die mit der Option `vmmc` angegebene Verwaltungsklasse findet auf alle Sicherungen Anwendung. Sie können die Option `include.vm` verwenden, um diese Verwaltungsklasse für eine oder mehrere virtuelle Maschinen zu überschreiben. Die Option `include.vm` wirkt sich nicht auf die Verwaltungsklasse aus, die durch die Option `vmctlmc` angegeben ist. Mit der Option `vmctlmc` werden gesicherte Steuerdateien virtueller Maschinen an eine bestimmte Verwaltungsklasse gebunden.

Optionsdatei

Geben Sie diese Option in der Clientoptionsdatei an.

Syntax



Parameter

VM-Name
Erforderlicher Parameter. Gibt den Namen einer virtuellen Maschine an, die an die angegebene Verwaltungsklasse gebunden werden soll. In jeder Anweisung `include.vm` kann nur eine einzige virtuelle Maschine angegeben werden. Sie können jedoch beliebig viele Anweisungen `include.vm` angeben, um jede virtuelle Maschine an eine bestimmte Verwaltungsklasse zu binden.

Sie können im Namen der virtuellen Maschine Platzhalterzeichen verwenden. Ein Stern (*) steht für eine beliebige Zeichenfolge. Ein Fragezeichen (?) steht für ein einzelnes Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, muss er in doppelte Anführungszeichen (") eingeschlossen werden.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, geben Sie beim Angeben des Namens das Fragezeichen als Platzhalterzeichen für die Sonderzeichen ein.

Name_der_Verwaltungsklasse
Optionaler Parameter. Gibt die Verwaltungsklasse an, die beim Sichern der angegebenen virtuellen Maschine verwendet werden soll. Wenn dieser Parameter nicht angegeben wird, wird standardmäßig die globale Verwaltungsklasse für virtuelle Maschinen verwendet, die mit der Option `vmmc` angegeben wird.

Beispiele

Nehmen Sie an, dass die folgenden Verwaltungsklassen auf dem IBM Spectrum Protect-Server vorhanden und aktiv sind:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

Beispiel 1

Die folgende Anweisung `include.vm` in der Clientoptionsdatei bindet alle virtuellen Maschinen, deren Name mit VMTEST beginnt, an die Verwaltungsklasse MCFORTESTVMS:

```
include.vm vmtest* MCFORTESTVMS
```

Beispiel 2

Die folgende Anweisung `include.vm` in der Clientoptionsdatei bindet eine virtuelle Maschine mit dem Namen WHOPPER VM1 [PRODUCTION] an die Verwaltungsklasse mit dem Namen MCFORPRODVMS:

```
include.vm "WHOPPER VM1 ?PRODUCTION?" MCFORPRODVMS
```

Der Name der virtuellen Maschine muss in Anführungszeichen eingeschlossen werden, da er Leerzeichen enthält. Außerdem wurde das Fragezeichen als Platzhalterzeichen für die Sonderzeichen im Namen der virtuellen Maschine verwendet.

Beispiel 3

Die folgende Anweisung `include.vm` in der Clientoptionsdatei bindet eine virtuelle Maschine mit dem Namen VM1 an eine Verwaltungsklasse mit dem Namen MCUNIQUEVM:

```
include.vm VM1 MCUNIQUEVM
```

Zugehörige Verweise:

„Vmmc" auf Seite 215

Include.vmdisk

Mit der Option `INCLUDE.VMDISK` wird eine Platte einer virtuellen Maschine (VM) in Sicherungsoperationen eingeschlossen. Wenn Sie nicht mindestens einen Plattenkennsatz angeben, werden alle Platten in der VM gesichert.

Die Option `INCLUDE.VMDISK` gibt den Kennsatz einer VM-Platte an, die in eine Operation **backup vm** eingeschlossen werden soll. Wenn Sie im Befehl **backup vm** eine Platte einschließen, überschreiben die Befehlszeilenparameter alle Anweisungen `INCLUDE.VMDISK` in der Optionsdatei.

INCLUDE.VMDISK für virtuelle Microsoft Hyper-V-Maschinen

Verwenden Sie die Option `INCLUDE.VMDISK`, um eine VM-Platte bei Hyper-V-Sicherungsoperationen einzuschließen.

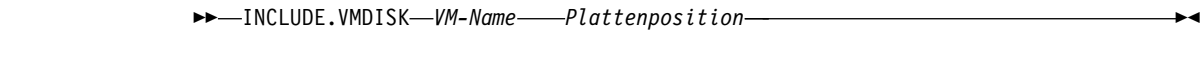
Unterstützte Clients

Diese Option kann für alle unterstützten Windows-Clients verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Befehlszeilenparameter überschreiben Anweisungen in der Optionsdatei.

Syntax



Parameter

VM-Name

Gibt den Namen der VM an, die eine Platte enthält, die in eine Operation **backup vm** eingeschlossen werden soll. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung `INCLUDE.VMDISK` können Sie nur einen einzigen VM-Namen angeben. Geben Sie weitere Anweisungen `INCLUDE.VMDISK` für jede VM-Platte an, die eingeschlossen werden soll.

Der VM-Name kann einen Stern (*) enthalten, der einer beliebigen Zeichenfolge entspricht, und ein Fragezeichen (?), das einem beliebigen einzelnen Zeichen entspricht. Wenn der VM-Name Leerzeichen enthält, schließen Sie ihn in Anführungszeichen („ ") ein.

Tipp: Wenn der VM-Name Sonderzeichen enthält, wie beispielsweise eckige Klammern ([oder]), wird der VM-Name möglicherweise nicht korrekt abgeglichen. Wenn ein VM-Name Sonderzeichen enthält, stellen Sie die Sonderzeichen mithilfe von Fragezeichen (?) dar.

Um beispielsweise eine SCSI-VM-Platte in die Sicherung einer virtuellen Maschine mit dem Namen "Windows VM3 [2012R2]" einzuschließen, verwenden Sie in der Optionsdatei die folgende Syntax:

```
INCLUDE.VMDISK "Windows VM3 ?2012R2?" "SCSI 0 1"
```

Plattenposition

Geben Sie die Position der VM-Platte an, die bei einer Hyper-V-Sicherungsoperation eingeschlossen werden soll. Die Plattenpositionsbezeichnung muss mit "SCSI" oder "IDE" beginnen, gefolgt von der Controllernummer und der Einheitenpositionsnummer. Platzhalterzeichen sind nicht zulässig.

Tipp: Verwenden Sie den Befehl **backup vm** mit der Option -preview, um die Position der Platten in einer bestimmten VM zu bestimmen. Informationen zur Syntax finden Sie in der Beschreibung des Befehls "**Backup VM**".

Beispiele

Optionsdatei

Die virtuelle Maschine vm1 enthält eine IDE-VM-Platte (VHDX) mit der Controllernummer 1 und der Einheitenposition 0. Um diese VHDX in Operationen **backup vm** einzuschließen, geben Sie in der Optionsdatei die folgende Anweisung an:

```
INCLUDE.VMDISK vm1 "IDE 1 0"
```

Die virtuelle Maschine vm2 enthält eine SCSI-VM-Platte mit Controllernummer 0 und Einheitenposition 1. Schließen Sie diese VHDX in Sicherungsoperationen ein, indem Sie in der Optionsdatei die folgende Anweisung angeben:

```
INCLUDE.VMDISK vm2 "SCSI 0 1"
```

Befehlszeile:

Schließen Sie eine einzelne IDE-Platte (mit der Controllernummer 1 und der Einheitenposition 0) in die Sicherungsoperation für die virtuelle Maschine vm1 ein:

```
dsmc backup vm "vm1:vhdx=IDE 1 0"
```

Schließen Sie eine SCSI-Platte (mit der Controllernummer 0 und der Einheitenposition 1) in die Sicherungsoperation für die virtuelle Maschine vm2 ein:

```
dsmc backup vm "vm2:vhdx=SCSI 0 1"
```

Zugehörige Verweise:

„**Backup VM**" auf Seite 166

„**Restore VM**" auf Seite 178

„Domain.vmfull" auf Seite 183

„Exclude.vmdisk" auf Seite 186

INCLUDE.VMSNAPSHOTATTEMPTS

Bestimmen Sie mithilfe der Option INCLUDE.VMSNAPSHOTATTEMPTS die Gesamtzahl Versuche, eine Momentaufnahme für eine Sicherungsoperation für eine virtuelle Maschine (VM) zu erstellen, die aufgrund eines Momentaufnahmefehlers fehlschlägt.

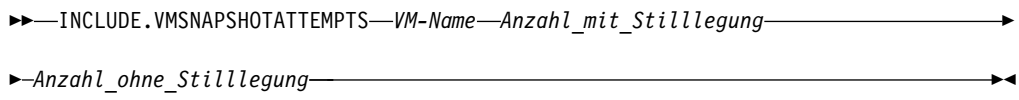
Unterstützte Clients

Diese Option kann für unterstützte Windows-Clients verwendet werden, die für die Sicherung von VMs auf Hyper-V-Hosts konfiguriert sind, die unter Windows Server 2016-Betriebssystemen ausgeführt werden.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. In der Befehlszeile ist sie nicht gültig.

Syntax



Parameter

VM-Name

Ein erforderlicher positionsgebundener Parameter, der den Namen der virtuellen Maschine angibt, für die die Gesamtzahl Versuche zur Erstellung einer Momentaufnahme ausgeführt werden soll, wenn ein Sicherungsversuch aufgrund eines Momentaufnahmefehlers fehlschlägt. Der Name ist der Anzeigename der virtuellen Maschine.

In einer Anweisung INCLUDE.VMSNAPSHOTATTEMPTS kann nur jeweils eine virtuelle Maschine angegeben werden. Sie können jedoch mit den folgenden Methoden die Gesamtzahl der Momentaufnahmeversuche für andere virtuelle Maschinen konfigurieren:

- Geben Sie für jede virtuelle Maschine, für die diese Option gelten soll, so viele Anweisungen INCLUDE.VMSNAPSHOTATTEMPTS an. wie Wiederholungsversuche zur Erstellung von Momentaufnahmen, die fehlgeschlagen sind, erforderlich sind.
- Verwenden Sie Platzhalterzeichen für den Parameterwert *VM-Name*, um Namen virtueller Maschinen anzugeben, die mit dem Platzhalterzeichenmuster übereinstimmen. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) steht für ein einzelnes Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen (") ein.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, ersetzen Sie die Sonderzeichen durch das Platzhalterzeichen ? (Fragezeichen), wenn Sie den Namen der virtuellen Maschine angeben.

Anzahl_mit_Stilllegung

Ein positionsgebundener Parameter, der die folgende Aktion angibt:

Für Hyper-V-RCT-Sicherungsoperationen:

Der Parameter *Anzahl_mit_Stilllegung* gibt an, wie oft versucht werden soll, Momentaufnahmen mit Stilllegung zu erstellen, um anwendungskonsistente Sicherungen zu erstellen.

Sie können einen Wert im Bereich von 0 bis 10 angeben. Der Standardwert ist 2.

Anzahl_ohne_Stilllegung

Für Hyper-V-RCT-Sicherungsoperationen:

Die Option *Anzahl_ohne_Stilllegung* gibt die Anzahl Versuche zur Erstellung von Momentaufnahmen ohne Stilllegung an, nachdem die angegebene Anzahl Versuche, die in der Option *Anzahl_mit_Stilllegung* angegeben ist, ausgeführt wurde.

Sie können einen Wert im Bereich von 0 bis 10 angeben. Der Standardwert ist 0.

Wichtig: Wenn dieser Parameter auf eine VM-Sicherung angewendet wird, wird die Sicherung als absturzkonsistent betrachtet. Demzufolge sind Betriebssystem-, Dateisystem- und Anwendungskonsistenz nicht garantiert. Ein Eintrag `include.vmsnapshotattempts 0 0` ist nicht gültig. Für Sicherungsoperationen ist mindestens eine Momentaufnahme erforderlich.

Beispiele

Beispiele für Hyper-V:

Beispiel 1

Geben Sie die folgende Anweisung in der Clientoptionsdatei an, um insgesamt zwei Versuche zur Erstellung einer Momentaufnahme mit absturzkonsistenten Sicherungen für alle Hyper-V-VMs auszuführen, deren Namen mit `LinuxVM` beginnen:

```
INCLUDE.VMSNAPSHOTATTEMPTS LinuxVM* 0 2
```

Beispiel 2

Geben Sie die folgende Anweisung in der Clientoptionsdatei an, um drei Versuche zur Erstellung einer Momentaufnahme für die virtuelle Maschine VM1 auszuführen: zwei Versuche zur Erstellung einer anwendungskonsistenten Momentaufnahme und - wenn diese fehlschlagen - ein Versuch zur Erstellung einer absturzkonsistenten Momentaufnahme:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM1 2 1
```

INCLUDE.VMTSMVSS

Verwenden Sie die Option `INCLUDE.VMTSMVSS` zur Aktivierung von Anwendungsschutz während Sicherungsoperationen virtueller Gastmaschinen (virtuelle Maschine = VM), die Anwendungsdaten hosten.

Mit der Option `INCLUDE.VMTSMVSS` werden Anwendungen auf der Gast-VM darüber benachrichtigt, dass eine Sicherung bevorsteht. Durch diese Option ist es möglich, dass die Anwendung Transaktionsprotokolle abschneidet und Transaktionen festschreibt, so dass sie nach Beendigung der Sicherung in einem konsistenten Zustand fortfahren kann. Ein optionaler Parameter kann angegeben werden, um das Abschneiden von Microsoft SQL Server-Transaktionsprotokollen zu unterdrücken.

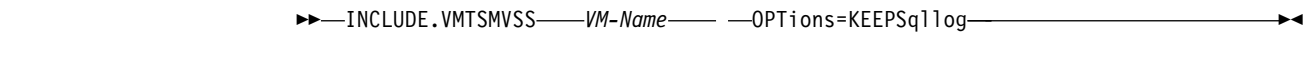
Wenn eine VM durch diese Option eingeschlossen ist, wird Anwendungsschutz bereitgestellt. Das heißt, die Einheit zum Versetzen von Daten blockiert (freeze) die VSS-Writer, gibt sie frei (thaw) und schneidet optional die Anwendungsprotokolle ab. Wenn eine VM nicht durch diese Option geschützt ist, wird Anwendungsschutz von Hyper-V bereitgestellt. Hyper-V blockiert die VSS-Writer und gibt sie frei, aber Anwendungsprotokolle werden nicht abgeschnitten.

Wichtig: Vor der Ausführung von Sicherungen mit Anwendungsschutz müssen Sie sicherstellen, dass sich die Anwendungsdatenbank (z. B. die Microsoft SQL Server-Datenbank oder die Microsoft Exchange Server-Datenbank) auf einem nicht bootenden Laufwerk (beliebiges Laufwerk außer dem Bootlaufwerk) befindet, falls eine **diskshadow revert**-Operation während der Zurückschreibung erforderlich ist.

Optionsdatei

Definieren Sie diese Option in der Optionsdatei der Einheit zum Versetzen von Daten. Diese Option kann nicht vom Profileditor und nicht in der Befehlszeile angegeben werden.

Syntax



Parameter

VM-Name
Gibt den Namen der VM an, die die Anwendungen enthält, die in den Quiescemodus versetzt werden sollen. Der Name ist der VM-Anzeigename im Hyper-V-Manager. Geben Sie eine einzige VM pro Anweisung `INCLUDE.VMTSMVSS` an. Soll beispielsweise eine VM mit dem Namen Windows VM3 [2012R2] eingeschlossen werden, verwenden Sie die folgende Syntax in der Optionsdatei:

```
INCLUDE.VMTSMVSS "Windows VM3 [2012R2]"
```

Verwenden Sie einen Stern als Platzhalterzeichen (`INCLUDE.VMTSMVSS *`), um alle VMs mit dieser Option zu schützen. Sie können auch Fragezeichen als Platzhalterzeichen für beliebige einzelne Zeichen verwenden. Mit der Angabe `INCLUDE.VMTSMVSS vm??` werden z. B. alle VMs geschützt, deren Namen 'vm' gefolgt von zwei beliebigen weiteren Zeichen lauten (vm10, vm11, vm17 usw.).

Tipp: Wenn der VM-Name Sonderzeichen enthält, wie beispielsweise eckige Klammern ([oder]), wird der VM-Name möglicherweise nicht korrekt abgeglichen. Enthält ein VM-Name Sonderzeichen, können Sie das Fragezeichen (?) verwenden, um die Sonderzeichen im VM-Namen abzugleichen.

Für diesen Parameter gibt es keinen Standardwert. Sie müssen VMs, die geschützt werden sollen, in mindestens einer Anweisung `INCLUDE.VMTSMVSS` angeben, um den Anwendungsschutz zu aktivieren. Stellen Sie sicher, dass Sie keine Platte in einer VM (mit der Option `EXCLUDE.VMDISK`) ausschließen, wenn die Platte Anwendungsdaten enthält, die geschützt werden sollen.

OPTions=KEEPSqllog
Nur für Microsoft SQL Server: Ist der Parameter `OPTions KEEPSqllog` in einer Anweisung `INCLUDE.VMTSMVSS` angegeben, verhindert er, dass SQL Server-Protokolle abgeschnitten werden, wenn eine Einheit zum Versetzen von Daten, die

auf einem Knoten einer Einheit zum Versetzen von Daten installiert ist, eine VM sichert, auf der ein SQL Server ausgeführt wird.

Die Angabe dieses Parameters ermöglicht dem SQL Server-Administrator das manuelle Sichern und ggf. Abschneiden der SQL Server-Protokolle, sodass sie beibehalten und für die Zurückschreibung von SQL-Transaktionen bis zu einem bestimmten Prüfpunkt verwendet werden können, nachdem die VM zurückgeschrieben wurde.

Wenn diese Option angegeben wird, wird das SQL-Protokoll nicht abgeschnitten und die folgende Nachricht wird angezeigt und auf dem Server protokolliert:

```
ANS4179I Der IBM Spectrum Protect-Anwendungsschutz
hat die Microsoft SQL Server-Protokolle auf der virtuellen Maschine 'VM' nicht abgeschnitten.
```

Sie können die Option `OPTIONS=KEEPSQLLOG` entfernen, um das Abschneiden der SQL-Protokolle bei Beendigung einer Sicherung zu ermöglichen.

Anmerkung: Der Client sichert nicht die SQL-Protokolldateien. Der SQL-Administrator muss die Protokolldateien sichern, damit sie nach dem Zurückschreiben der Datenbank angewendet werden können.

Beispiele

Optionsdatei

Anwendungsschutz für eine VM mit dem Namen 'vm_example' konfigurieren:

```
INCLUDE.VMTSMVSS vm_example
```

Für SQL Server: Anwendungsschutz für vm11, vm12 und vm15 konfigurieren:

```
INCLUDE.VMTSMVSS vm11
INCLUDE.VMTSMVSS vm12
INCLUDE.VMTSMVSS vm15 options=keepsqllog
```

Befehlszeile

Nicht gültig. Diese Option kann nicht in der Befehlszeile angegeben werden.

Zugehörige Konzepte:

„Hinweise zu Schattenkopien für die Zurückschreibung einer Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten” auf Seite 197

Zugehörige Verweise:

Exclude.vmdisk

Include.vmdisk

„INCLUDE.VMSNAPSHOTATTEMPTS” auf Seite 193

Hinweise zu Schattenkopien für die Zurückschreibung einer Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten

Für Windows-VMs (VM = virtuelle Maschine) gelten Einschränkungen hinsichtlich Schattenkopien, wenn Sie versuchen, eine Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten zurückzuschreiben.

Im Schattenspeicher kann der Speicherbereich knapp werden

Wenn Sie versuchen, eine vollständige VM-Zurückschreibung einer Sicherung mit Anwendungsschutz auszuführen, ist die Momentaufnahme des Systemproviders auf der zurückgeschriebenen VM vorhanden. Während die Anwendung Daten auf die Platte schreibt, wächst der Schattenspeicherbereich, bis nicht mehr genügend Plattenspeicher verfügbar ist.

Wenn Anwendungsschutz während einer Sicherung verwendet wurde, darf im Allgemeinen nur die Zurückschreibung mit Anwendungsschutz für die Zurückschreibung einer Datenbank verwendet werden. Wenn Sie die Anwendung zurückschreiben, wird der Datenträger automatisch zurückgesetzt. Wenn Sie jedoch die vollständige VM zurückschreiben müssen, müssen Sie die Schattenkopie entweder manuell zurücksetzen oder löschen.

Stellen Sie nach der Zurückschreibung der gesamten virtuellen Maschine sicher, dass die Zurückschreibung erfolgreich war und die Daten nicht beschädigt sind. Wenn die Daten nicht beschädigt sind, löschen Sie die Schattenkopie. Wenn die Daten beschädigt sind, setzen Sie die Schattenkopie zurück, um die Datenintegrität wiederherzustellen.

Sie können die Schattenkopie, die gelöscht oder zurückgesetzt werden soll, mithilfe der Datei `dsmShadowCopyID.txt` im Stammverzeichnis jedes zurückgeschriebenen Datenträgers bestimmen. Diese Datei enthält die Momentaufnahme-IDs der Schattenkopien, die während der Versuche zur Erstellung einer Momentaufnahme erstellt wurden. Mit dem **diskshadow**-Befehl **delete shadows** können Sie diese IDs löschen; mit dem Befehl **revert** können Sie die Schattenkopie zurücksetzen. Nachdem das Löschen oder Zurücksetzen abgeschlossen ist, können Sie auch die Datei `dsmShadowCopyID.txt` löschen.

Wichtig: Damit die Zurücksetzungsoperation erfolgreich verläuft, darf die Anwendungsdatenbank, z. B. die Microsoft SQL Server-Datenbank oder die Microsoft Exchange Server-Datenbank, sich nicht auf einem Bootlaufwerk befinden.

Schattenkopie muss während einer Zurückschreibung mit Anwendungsschutz auf dem zurückgeschriebenen Datenträger verfügbar sein

In einigen Fällen wird bei einer Sicherungsoperation mit Anwendungsschutz möglicherweise Volume Shadow Copy Service (VSS) verwendet, um vor dem Start einer VM-Sicherung eine anwendungskonsistente Schattenkopie zu erstellen. Alle Änderungen, die nach der Erstellung der Schattenkopie vorgenommen werden, werden im Schattenspeicher gespeichert.

Eine Datenbankzurückschreibung schlägt eventuell fehl, wenn die Schattenkopie während der Zurückschreibung einer Anwendung nicht verfügbar ist. Die Schattenkopie wird während der Zurückschreibung verwendet, um den zurückgeschrie-

benen Datenträger in einen anwendungskonsistenten Status zurückzusetzen. Wenn die Schattenkopie nicht verfügbar ist, befinden die zurückgeschriebenen Daten sich in einem inkonsistenten Status.

Die folgenden Situationen können dazu führen, dass die Schattenkopie nicht verfügbar ist:

- In der Regel ist der Schattenspeicher Bestandteil eines Datenträgers. Manchmal ist der Schattenspeicherbereich jedoch standardmäßig oder manuell so konfiguriert, dass er sich auf einem anderen Datenträger befindet. In diesem Fall kann die Datenbankzurückschreibung fehlschlagen, weil die Schattenkopie, die während der VM-Sicherungsoperation erstellt wurde, bei der Zurückschreibung nicht verfügbar ist.
- Der Schattenspeicher ist nicht verfügbar, weil der Datenträger mit dem Schattenspeicher bei der Sicherung ausgeschlossen wurde.

Für dieses Problem sind die folgenden Problemumgehungen verfügbar:

- Fügen Sie mit dem Befehl **vssadmin add shadowstorage** für jeden auf der Gast-VM verfügbaren Datenträger die Zuordnung für den Schattenkopiespeicher hinzu, bevor Sie eine VM-Sicherung ausführen. Geben Sie beispielsweise den folgenden Befehl aus, um die Schattenspeicherposition für den Datenträger `E:` auf dem Datenträger `E:` zu definieren:

  ```
  vssadmin add shadowstorage /for=E: /on=E: /maxsize=unbounded
  ```

  Wichtig: Der Befehl **vssadmin add shadowstorage** schlägt möglicherweise fehl, wenn VSS-Momentaufnahmen für die VM vorhanden sind. Sie müssen die VSS-Momentaufnahmen mit der Anwendung löschen, mit der sie erstellt wurden.

  Wurde beispielsweise von IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server eine VSS-Sicherung einer Exchange-Datenbank mit dem Sicherungsziel LOCAL erstellt, verwenden Sie die Anwendung Data Protection for Microsoft Exchange Server, um die VSS-Sicherung zu löschen. Ist eine nicht identifizierte VSS-Momentaufnahme vorhanden, verwenden Sie den **diskshadow**-Befehl **delete shadows** von Windows, um die VSS-Momentaufnahme zu löschen.

  Stellen Sie außerdem sicher, dass der Datenträger, der den Schattenspeicher enthält, nicht bei Sicherungsoperationen ausgeschlossen ist.
- Setzen Sie Momentaufnahmen manuell zurück, um die Anwendungskonsistenz der Datenbankdateien zu erzielen:
  1. Stellen Sie mit IBM Spectrum Protect Recovery Agent alle Platten in der VM-Sicherung bereit.
  2. Starten Sie den **diskshadow**-Befehl von Windows im interaktiven Modus.
  3. Geben Sie im interaktiven **diskshadow**-Modus den folgenden Befehl aus:

     ```
     list shadows all
     ```
  4. Lokalisieren Sie die Datei `dsmShadowCopyID.txt` im Stammverzeichnis jedes bereitgestellten Laufwerks. Diese Datei enthält die global eindeutige ID (GUID) der VSS-Schattenkopie, die für die Zurücksetzungsoperation für den Datenträger erforderlich ist.
  5. Öffnen Sie die Datei `dsmShadowCopyID.txt` und ermitteln Sie die GUID des Datenträgers, auf dem die Datenbankdateien sich befinden.
  6. Geben Sie im interaktiven **diskshadow**-Modus den folgenden Befehl aus:

     ```
     revert GUID
     ```

Dabei ist *GUID* die GUID der Momentaufnahme, die in der Datei `dsmShadowCopyID.txt` angegeben war.

Damit die Zurücksetzungsoperation erfolgreich verläuft, darf die Anwendungsdatenbank sich nicht auf einem Bootlaufwerk befinden.

Mode

Verwenden Sie die Option 'mode' zum Angeben des Sicherungsmodus, der bei der Durchführung bestimmter Sicherungsoperationen verwendet werden soll.

Sie können die Option `mode` mit dem Befehl **backup vm** verwenden. Dieser Parameter gibt an, ob eine Imagegesamtsicherung, eine immer inkrementelle vollständige Sicherung oder eine immer inkrementelle Teilsicherung virtueller Hyper-V-Maschinen durchgeführt werden soll.

Die Option `mode` hat keine Auswirkungen beim Sichern einer logischen Roheinheit.

Syntax

Parameter

IFIncremental
Gibt an, dass Sie eine immer inkrementelle Teilsicherung einer virtuellen Hyper-V-Maschine durchführen möchten. Bei einer immer inkrementellen Teilsicherung werden nur die seit der letzten Sicherung geänderten Plattenblöcke gesichert. Dies ist der Standardsicherungsmodus.

Dieser Sicherungsmodus kann nicht zum Sichern einer virtuellen Maschine verwendet werden, wenn der Client für das Verschlüsseln der Sicherungsdaten konfiguriert ist.

IFFull
Gibt an, dass Sie eine immer inkrementelle vollständige Sicherung einer virtuellen Hyper-V-Maschine durchführen möchten. Bei einer immer inkrementellen vollständigen Sicherung werden alle auf den Platten einer virtuellen Maschine belegten Blöcke gesichert. Standardmäßig wird bei der ersten Sicherung einer virtuellen Hyper-V-Maschine eine immer inkrementelle vollständige Sicherung (`mode=iffull`) durchgeführt, selbst wenn Sie `mode=ifincremental` angeben (oder die Option `mode` ihren Standardwert verwenden lassen). Bei nachfolgenden Sicherungen wird standardmäßig der Wert `mode=ifincremental` angenommen.

Dieser Sicherungsmodus kann nicht zum Sichern einer virtuellen Maschine verwendet werden, wenn der Client für das Verschlüsseln der Sicherungsdaten konfiguriert ist.

Beispiele

Task Durchführung einer immer inkrementellen vollständigen VM-Sicherung einer virtuellen Windows Hyper-V-Maschine mit dem Namen `msvm1`

```
dsmc backup vm msvm1 -mode=iffull
```

Task Durchführung einer immer inkrementellen Teilsicherung einer virtuellen Windows Hyper-V-Maschine mit dem Namen `msvm1`

```
dsmc backup vm msvm1 -mode=ifincremental
```

Zugehörige Verweise:

„**Backup VM**" auf Seite 166

Mbobjrefreshthresh

Bei der Option mbobjrefreshthresh handelt es sich um eine Zahl zum Definieren des Schwellenwerts für die Megablockobjektaktualisierung. Wenn die Anzahl der IBM Spectrum Protect-Objekte, die zum Beschreiben eines beliebigen 128-MB-Megablocks benötigt werden, diesen Wert überschreitet, wird der gesamte Megablock aktualisiert und die Objekte, die bei vorherigen Sicherungen zur Darstellung dieses Bereichs verwendet wurden, werden als verfallen markiert.

Wenn Sie eine virtuelle Maschine sichern, werden die Daten auf dem IBM Spectrum Protect-Server in 128-MB-Einheiten gespeichert, die als *Megablöcke* bezeichnet werden. Wenn ein Bereich auf der Produktionsplatte geändert und eine neue Teilsicherung durchgeführt wird, wird für die Darstellung der Änderungen an den zuvor gesicherten Daten ein neuer Megablock erstellt. Da mit jeder Teilsicherung ein neuer Megablock erstellt werden kann, können die Megablöcke schließlich die Leistung der IBM Spectrum Protect-Datenbank und damit auch die Leistung der meisten IBM Spectrum Protect-Operationen negativ beeinflussen.

Verwenden Sie diese Option bei der Schätzung von IBM Spectrum Protect-Objekten, die Produktionsdaten für jede Sicherung einer virtuellen Maschine darstellen. Sobald beispielsweise die Anzahl der IBM Spectrum Protect-Objekte diesen Wert überschreitet, wird der Megablock aktualisiert. Diese Aktion bedeutet, dass der gesamte 128-MB-Block auf den IBM Spectrum Protect-Server kopiert und als einzelnes IBM Spectrum Protect-Objekt dargestellt wird. Der Mindestwert ist 2; der Maximalwert ist 8192. Der Standardwert ist 50.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann sich auch auf dem Server in einer Clientoptionsgruppe befinden. Sie ist nicht in der Befehlszeile gültig.

Syntax

Parameter

Der Mindestwert, den Sie angeben können, ist 2 Megablöcke, der Höchstwert 8192 Megablöcke. Der Standardwert ist 50 Megablöcke.

Beispiele

Geben Sie diese Option an, um eine Megablockaktualisierung auszulösen, wenn die Anzahl der Objekte, die für die Darstellung eines aktualisierten Megablocks benötigt wird, 20 Objekte überschreitet:

```
MBOBJREFRESHTHRESH 20
```

Mbpctrefreshthresh

Bei der Option mbpctrefreshthresh handelt es sich um eine Zahl zum Definieren des Schwellenwerts für die Megablockprozentsatzaktualisierung. Wenn der Prozentsatz der IBM Spectrum Protect-Objekte, die zum Beschreiben eines beliebigen 128-MB-Megablocks benötigt werden, diesen Wert übersteigt, wird der gesamte Megablock aktualisiert und die Objekte, die bei vorherigen Sicherungen zur Darstellung dieses Bereichs verwendet wurden, werden als verfallen markiert.

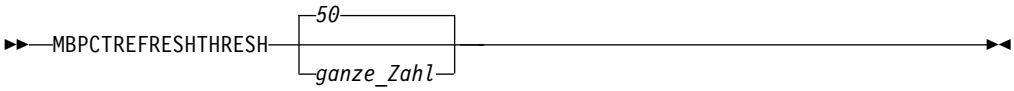
Wenn Sie eine virtuelle Maschine sichern, werden Daten auf dem IBM Spectrum Protect-Server in 128-MB-Einheiten gespeichert, die als *Megablöcke* bezeichnet werden. Wenn ein Bereich auf der Produktionsplatte geändert und eine neue Teilsicherung durchgeführt wird, wird für die Darstellung der Änderungen an den zuvor gesicherten Daten ein neuer Megablock erstellt. Da mit jeder Teilsicherung ein neuer Megablock erstellt werden kann, können die Megablöcke schließlich die Leistung der IBM Spectrum Protect-Datenbank und damit auch die Leistung der meisten IBM Spectrum Protect-Operationen negativ beeinflussen.

Verwenden Sie diese Option beim Abschätzen des Umfangs von zusätzlichen Daten, die für jede virtuelle Maschine gesichert werden. Wenn beispielsweise ein 128-MB-Block einer Produktionsplatte zu einem höheren als dem angegebenen Prozentsatz geändert wird, wird der gesamte 128-MB-Block auf den IBM Spectrum Protect-Server kopiert. Der Block wird als einzelnes IBM Spectrum Protect-Objekt dargestellt.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann sich auch auf dem Server in einer Clientoptionsgruppe befinden. Sie ist nicht in der Befehlszeile gültig.

Syntax



Parameter

Der Mindestwert, den Sie angeben können, ist 1 Prozent, der Höchstwert 99 Prozent. Der Standardwert ist 50 Prozent.

Beispiele

Geben Sie diese Option an, um eine Megablockaktualisierung auszulösen, wenn 50 Prozent (oder mehr) der Objekte in einem Megablock auf einer Produktionsplatte geändert wurden:

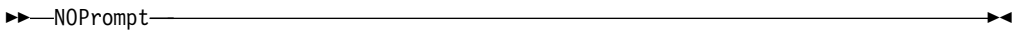
```
MBPCTREFRESHTHRESHOLD 50
```

Noprompt

Die Option noprompt unterdrückt die Bestätigungsaufforderung des Befehls **expire**.

Verwenden Sie die Option noprompt mit dem Befehl **expire**.

Syntax



Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc expire -noprompt c:\home\project\*
```

Numberformat

Die Option numberformat gibt das Format an, das zum Anzeigen von Zahlen verwendet werden soll.

Verwenden Sie diese Option zum Ändern des Standardzahlenformats für die Sprache des Nachrichtenrepositorys, das Sie verwenden.

Standardmäßig werden die Formatinformationen der Ländereinstellungsdefinition entnommen, die aktiv war, als der Client aufgerufen wurde. Entnehmen Sie Details zum Definieren Ihrer Ländereinstellung der Dokumentation zu Ihrem lokalen System.

Sie können die Option numberformat nur mit dem Befehl **expire** verwenden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option angeben auf der Registerkarte **Ländereinstellungen**, Feld **Zahlenformat** des Vorgabeneditors.

Syntax

Parameter

Zahl
Zeigt Zahlen in einem der folgenden Formate an. Geben Sie die Nummer (0–6) an, die für das gewünschte Zahlenformat steht.

0 Das in der Ländereinstellung angegebene Format wird verwendet. Dies ist der Standardwert (gilt nicht für Mac OS X).

1 1,000.00

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Englisch (Vereinigte Staaten)
- Japanisch
- Chinesisch (traditionell)
- Chinesisch (vereinfacht)
- Koreanisch

2 1,000,00

3 1 000,00

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Französisch
- Tschechisch
- Ungarisch
- Polnisch
- Russisch

4 1 000.00

5 1.000,00

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Portugiesisch (Brasilien)
- Deutsch
- Italienisch
- Spanisch

6 1'000,00

Beispiele

Optionsdatei:

```
num 4
```

Befehlszeile:

```
-numberformat=4
```

Diese Option ist gültig in der Anfangsbefehlszeile und im interaktiven Modus. Wenn Sie diese Option im interaktiven Modus verwenden, wirkt sie sich nur auf den Befehl aus, mit dem sie angegeben wird. Nachdem dieser Befehl ausgeführt wurde, wird der Wert auf den Wert zurückgesetzt, der zu Beginn der interaktiven Sitzung gültig war. Dies ist der Wert aus der Datei dsm.opt, falls er nicht von der Anfangsbefehlszeile oder durch eine vom Server erzwungene Option überschrieben wurde.

Pick

Die Option `pick` erstellt eine Liste von Sicherungsversionen oder Archivierungskopien, die der von Ihnen eingegebenen Dateispezifikation entsprechen.

In der Liste können Sie auswählen, welche Versionen verarbeitet werden sollen. Wenn Sie zusätzlich die Option `inactive` verwenden, werden sowohl aktive als auch inaktive Objekte angezeigt.

Verwenden Sie die Option `pick` mit dem Befehl **`restore vm`**.

Syntax

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore vm vmfin* -pick -inactive
```

Pitdate

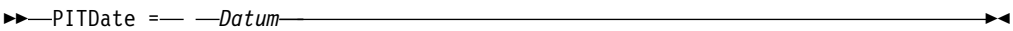
Verwenden Sie die Option `pitdate` mit der Option `pittime`, um einen Zeitpunkt für das Anzeigen oder Zurückschreiben der neuesten Version Ihrer Sicherungen festzulegen.

Es werden Dateien verarbeitet, die *zu oder vor* dem von Ihnen angegebenen Zeitpunkt (Datum und Uhrzeit) gesichert und nicht *vor* diesem Zeitpunkt gelöscht wurden. Nach diesem Zeitpunkt erstellte Sicherungsversionen werden ignoriert.

Verwenden Sie die Option `pitdate` mit den Befehlen **`query vm`** und **`restore vm`**.

Wenn `pitdate` verwendet wird, werden die Optionen `inactive` und `latest` implizit verwendet.

Syntax



Parameter

Datum
Gibt das entsprechende Datum an.

Beispiele

Befehlszeile:

```
dsmc restore vm vmfin3 -pitdate=02/21/2014
```

Pittime

Verwenden Sie die Option `pittime` mit der Option `pitdate`, um einen Zeitpunkt für das Anzeigen oder Zurückschreiben der neuesten Version Ihrer Sicherungen festzulegen.

Es werden Dateien verarbeitet, die *zu oder vor* dem von Ihnen angegebenen Zeitpunkt (Datum und Uhrzeit) gesichert und nicht *vor* diesem Zeitpunkt gelöscht wurden. Nach diesem Zeitpunkt erstellte Sicherungsversionen werden ignoriert. Diese Option wird ignoriert, wenn Sie nicht die Option `pitdate` angeben,

Verwenden Sie die Option `pittime` mit den Befehlen **`query vm`** und **`restore vm`**.

Syntax

Parameter

Uhrzeit
Gibt eine Uhrzeit an einem angegebenen Datum an. Wenn Sie keine Uhrzeit angeben, wird standardmäßig 23:59:59 Uhr verwendet.

Beispiele

Befehlszeile:

```
dsmc query vm vmfin1 -pitt=06:00:00 -pitd=02/03/2014
```

Skipsystemexclude

Mit der Option `skipsystemexclude` können Sie angeben, wie Ausschlussanweisungen für bestimmte Betriebssystemdateien, die der IBM Spectrum Protect for Virtual Environments-Client standardmäßig überspringt, verarbeitet werden.

Bestimmte Windows-Betriebssystemdateien, die für die Systemwiederherstellung während Sicherungsoperationen für virtuelle Maschinen normalerweise nicht erforderlich sind, werden von IBM Spectrum Protect for Virtual Environments-Clients standardmäßig übersprungen. Hierzu können Windows-Systemdateien, temporäre Internetdateien und Dateien im Papierkorb gehören.

Mit dieser Option können Sie die Verarbeitung von Ausschlussanweisungen für diese Betriebssystemdateien überspringen. Durch die Nichtverarbeitung dieser Ausschlussanweisungen kann sich die erforderliche Sicherungszeit für virtuelle Maschinen verringern.

Unterstützte Clients

Diese Option ist nur für IBM Spectrum Protect for Virtual Environments-Clients unter Windows-Betriebssystemen gültig.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (`dsm.opt`) und in der Befehlszeile gültig. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

Parameter

Yes
Geben Sie diesen Parameter an, um die Verarbeitung von Ausschlussanweisungen für bestimmte Windows-Betriebssystemdateien während VM-Sicherungsoperationen zu überspringen. Dieser Parameter ist der Standardwert.

No Geben Sie diesen Parameter an, um Ausschlussanweisungen für Windows-Betriebssystemdateien zu verarbeiten. Wenn Sie diesen Parameter auswählen und eine Dateisicherung des Hyper-V-Hosts ausführen, werden die Betriebssystemdateien ausgeschlossen.

Beispiele

Optionsdatei

```
SKIPSYSTemexclude yes
```

Befehlszeile:

```
dsmc backup vm -SKIPSYST=yes

dsmc incr -skipsyst=no
```

Timeformat

Die Option `timeformat` gibt das Format an, in dem die Systemzeit angezeigt und eingegeben werden soll.

Verwenden Sie diese Option zum Ändern des Standardzeitformats für die Sprache des von Ihnen verwendeten Nachrichtenrepositorys.

Standardmäßig werden die Formatinformationen der Ländereinstellungsdefinition entnommen, die aktiv war, als der Client aufgerufen wurde. Entnehmen Sie Details zum Definieren Ihrer Ländereinstellung der Dokumentation zu Ihrem lokalen System.

Sie können die Option `timeformat` nur mit dem Befehl **`expire`** verwenden.

Wenn Sie mit einem Befehl die Option `timeformat` angeben, muss sie sich vor den Optionen `fromtime`, `pittime` und `totime` befinden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option angeben auf der Registerkarte **Ländereinstellungen**, Feld **Zeitformat** des Vorgabeneditors.

Syntax

Parameter

Formatnummer
Zeigt die Uhrzeit in einem der hier aufgelisteten Formate an. Wählen Sie die Formatnummer aus, die für das gewünschte Format steht. Wenn Sie mit einem Befehl die Option `timeformat` angeben, muss sie sich vor der Option `pittime` befinden.

1 23:00:00
2 23,00,00
3 23.00.00
4 12:00:00 A/P
5 A/P 12:00:00

Beispiele

Optionsdatei:

```
timeformat 4
```

Befehlszeile:

```
-time=3
```

Diese Option ist gültig in der Anfangsbefehlszeile und im interaktiven Modus. Wenn Sie diese Option im interaktiven Modus verwenden, wirkt sie sich nur auf den Befehl aus, mit dem sie angegeben wird. Nachdem dieser Befehl ausgeführt wurde, wird der Wert auf den Wert zurückgesetzt, der zu Beginn der interaktiven Sitzung gültig war. Dies ist der Wert aus der Datei dsm.opt, falls er nicht von der Anfangsbefehlszeile oder durch eine vom Server erzwungene Option überschrieben wurde.

Weitere Hinweise zur Angabe von Datums- und Zeitformaten

Das Datums- oder Zeitformat, das Sie mit dieser Option angeben, muss verwendet werden, wenn Optionen verwendet werden, deren Eingabe aus Datums- und Zeitangaben besteht. Beispiele sind: `totime`, `fromtime`, `todate`, `fromdate` und `pittime`.

Wenn Sie beispielsweise die Option `timeformat` als `TIMEFORMAT 4` angeben, muss der Wert, den Sie für die Option `fromtime` oder `totime` angeben, als Zeit angegeben werden, wie z. B. `12:24:00pm`. Die Angabe `13:24:00` wäre nicht gültig, da `TIMEFORMAT 4` als Angabe für die Stunde eine ganze Zahl, die kleiner-gleich 12 ist, erfordert. Wenn in einer Option für die Stunde Werte bis zu 24 angegeben und Kommas als Trennzeichen verwendet werden sollen, müssen Sie `TIMEFORMAT 2` angeben.

Vmbackdir

Die Option `vmbackdir` gibt die temporäre Plattenposition an, an der der Client Steuerdateien speichert, die während VM-Gesamtsicherungen und vollständiger VM-Zurückschreibungen virtueller Microsoft Hyper-V-Maschinen erstellt werden.

Wenn ein Client auf einem Knoten einer Einheit zum Versetzen von Daten eine VM-Gesamtsicherung einer virtuellen Maschine startet, erstellt der Client Metadaten in Dateien, die der gesicherten virtuellen Maschine und deren Daten zugeordnet sind. Die Dateien, die die Metadaten enthalten, werden als *Steuerdateien* bezeichnet.

Während VM-Gesamtsicherungsoperationen werden die Metadaten auf einer Platte auf dem Knoten der Einheit zum Versetzen von Daten gespeichert, bis die Sicherung beendet ist und sowohl die Daten der virtuellen Maschine als auch die Steuerdateien im Serverspeicher gespeichert sind. Während einer vollständigen VM-Zurückschreibung werden die Steuerdateien vom Server kopiert und temporär auf der Platte der Einheit zum Versetzen von Daten gespeichert, wo sie beim Zurückschreiben der virtuellen Maschine und ihrer Daten verwendet werden. Nach dem Ende einer Sicherungs- oder Zurückschreibungsoperation werden die Steuerdateien nicht mehr benötigt und der Client löscht sie an ihrer temporären Plattenposition.

Das mit dieser Option angegebene Verzeichnis muss sich auf einem Laufwerk befinden, das genug freien Speicherplatz enthält, um die Steuerinformationen einer VM-Gesamtsicherung aufzunehmen.

Optionsdatei

Legen Sie diese Option in der Clientoptionsdatei fest oder geben Sie sie in der Befehlszeile als Option des Befehls **backup vm** oder **restore vm** an.

Syntax

Parameter

Verzeichnis
Gibt den Pfad an, unter dem die Steuerdateien auf dem Sicherungsserver gespeichert werden.

Der Standardwert ist `c:\mnt\tsmvmbackup\fullvm\`

Beispiele

Optionsdatei:

```
VMBACKD c:\mnt\tsmvmbackup\
```

Befehlszeile:

```
dsmc backup vm -VMBACKUPT=fullvm -VMBACKD=G:\virtuelle_maschine\
steuerdateien\

dsmc restore vm -VMBACKUPT=fullvm -VMBACKD=G:\san_temp\
```

Vmctlmc

Diese Option gibt die Verwaltungsklasse an, die beim Sichern von Steuerdateien virtueller Maschinen verwendet werden soll.

Standardmäßig sind Steuerdateien virtueller Maschinen an die Standardverwaltungsklasse gebunden. Mit der Option `vmmc` kann eine andere Verwaltungsklasse angegeben werden, an die Daten und Steuerdateien virtueller Maschinen gebunden werden. Die Option `vmctlmc` setzt die Standardverwaltungsklasse und die Option `vmmc` für die Steuerdateien virtueller Maschinen außer Kraft.

Unter bestimmten Bedingungen kann es wünschenswert oder notwendig sein, die Steuerdateien an eine andere Verwaltungsklasse als die Datendateien zu binden.

Die Option `vmctlmc` ist erforderlich, wenn Datendateien virtueller Maschinen auf Band gesichert werden. Steuerdateien virtueller Maschinen müssen in einem plattenbasierten Speicherpool gesichert werden, der nicht auf Band umgelagert wird. Der Speicherpool kann sich aus Datenträgern mit wahlfreiem Zugriff und sequenziellen FILE-Datenträgern zusammensetzen; bei dem Speicherpool kann es sich auch um einen deduplizierten Pool handeln. Verwenden Sie die Option `vmctlmc`, um eine Verwaltungsklasse anzugeben, die Daten in einem solchen Speicherpool speichert.

Einschränkung: Die mit der Option `vmctlmc` angegebene Verwaltungsklasse bestimmt nur den Zielspeicherpool für Steuerdateien virtueller Maschinen. Die Aufbewahrungsdauer der Steuerdateien wird durch die Option `vmmc`, falls angegeben, oder durch die Standardverwaltungsklasse bestimmt. Die Aufbewahrungsdauer für die Steuerdateien virtueller Maschinen stimmt immer mit der Aufbewahrungsdauer für die Datendateien virtueller Maschinen überein.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei dsm.opt ein.

Syntax

Parameter

Klassenname
Gibt eine Verwaltungsklasse für das Sichern von Steuerdateien virtueller Maschinen an. Wenn Sie diese Option nicht definieren, wird die mit der Option vmmc angegebene Verwaltungsklasse verwendet. Wenn Sie diese Option nicht definieren und die Option vmmc nicht definiert ist, wird die Standardverwaltungsklasse des Knotens verwendet.

Beispiele

Optionsdatei:

```
vmctlmc diskonlymc
```

Befehlszeile:
Trifft nicht zu.

Vmmaxparallel

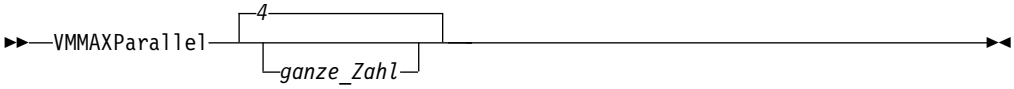
Diese Option wird zum Konfigurieren paralleler Sicherungen verschiedener virtueller Maschinen unter Verwendung einer Einzelinstanz des Clients für Sichern/Archivieren verwendet. Die Option vmmaxparallel gibt die maximale Anzahl virtueller Maschinen an, die zu jeder Zeit auf dem Server gesichert werden können.

Diese Option ist nur für Hyper-V-Sicherungsoperationen unter den Betriebssystemen Windows Server 2012 und 2012 R2 gültig.

Optionsdatei

Diese Option ist gültig in der Clientoptionsdatei (dsm.opt) oder in der Befehlszeile für **Backup VM**. Sie kann sich auch auf dem Server in einer Clientoptionsgruppe befinden. Sie kann nicht im Vorgabeneditor festgelegt werden.

Syntax



Parameter

ganze_Zahl
Gibt die maximale Anzahl virtueller Maschinen an, die zu jeder Zeit während einer parallelen Sicherungsoperation gesichert werden können. Der Standardwert ist 4. Der Maximalwert ist 50.

Tipp: Wenn Sie die clientseitige Datendeduplizierung verwenden, wird eine Deduplizierungssitzung für jede VM gestartet. Diese Deduplizierungssitzung zählt nicht zu den vmmaxparallel-Sitzungen.

Der Serverparameter MAXNUMMP gibt die maximale Anzahl an Mountpunkten an, die ein Knoten auf dem Server verwenden darf, wenn FILE oder TAPE das Kopienziel des Speicherpools ist. MAXNUMMP muss größer-gleich der Einstellung für VMMAXPARALLEL sein. Wenn mehrere Instanzen des Clients Dateien sichern oder wenn ein einzelner Client parallele Sicherungen ausführt, sind unter Umständen zusätzliche Mountpunkte erforderlich. Wenn die Anzahl der angeforderten Mountpunkte den Wert für MAXNUMMP überschreitet, gibt der Server einen Fehler aus (ANS0266I). Als Reaktion auf den Fehler reduziert der Client den Wert für VMMAXPARALLEL auf die durch MAXNUMMP angegebene Anzahl und setzt die Sicherung mit der reduzierten Sitzungszahl fort. Werden weitere Fehler ANS0266I festgestellt, reduziert der Client VMMAXPARALLEL um 1 und versucht, die Sicherung fortzusetzen. Wenn der Wert für VMMAXPARALLEL auf 1 verringert wird und der Client weitere Fehler ANS0266I empfängt, beendet der Client die Sicherung und gibt den folgenden Fehler aus:
ANS5228E Eine VM-Sicherungsoperation ist fehlgeschlagen, weil VMMAXPARALLEL auf 1 reduziert wurde und der Client noch immer keinen Servermountpunkt abrufen kann.
Wenden Sie sich an Ihren Serveradministrator, wenn Sie einen höheren als den derzeit festgelegten Wert für MAXNUMMP benötigen, damit Ihr Knoten zusätzliche parallele Sicherungssitzungen unterstützen kann.

Beispiele

Optionsdatei

```
VMMAXP 10
```

Befehlszeile

```
dsmc backup vm -vmmaxp=10
```

Zugehörige Verweise:

„**Backup VM**" auf Seite 166

„Domain.vmfull" auf Seite 183

Vmmaxpersnapshot

Mithilfe der Option vmmaxpersnapshot können Sie die maximale Anzahl virtueller Maschinen (VMs) angeben, die in eine Hyper-V-Momentaufnahme eingeschlossen werden sollen. Die VMs in der Momentaufnahme werden auf dem IBM Spectrum Protect-Server gesichert.

Indem die Anzahl virtueller Maschinen in einer Momentaufnahme erhöht wird, können Sie die Anzahl Momentaufnahmen, die für eine Sicherungsoperation erstellt werden, reduzieren. Dadurch werden Konkurrenzsituationen bei der Planung, die während Clustersicherungsoperationen für virtuelle Maschinen auf freigegebenen Clusterdatenträgern (CSVs = Clustered Shared Volumes) auftreten, reduziert.

Die Erstellung einer Momentaufnahme mit vielen virtuellen Maschinen dauert länger und erhöht die Systembelastung. Eine größere Anzahl virtueller Maschinen bedeutet, dass die Momentaufnahme länger bestehen bleibt, was Auswirkungen auf die Leistung haben kann.

Diese Option ist nur für Hyper-V-Sicherungsoperationen unter Betriebssystemen Windows Server 2012 und 2012 R2 gültig.

Unterstützte Clients

Diese Option ist für alle unterstützten Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (`dsm.opt`) und in der Befehlszeile für den Befehl **`Backup VM`** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

Parameter

ganze_Zahl

Gibt die maximale Anzahl VMs an, die in eine Hyper-V-Momentaufnahme eingeschlossen werden können. Der Standardwert ist 20. Der Maximalwert ist 100. Der Mindestwert ist 1.

Wenn einige VMs auf lokalen Datenträgern und einige VMs auf freigegebenen Clusterdatenträgern (CSVs) gespeichert sind, ist die Anzahl VMs in einer Momentaufnahme unter Umständen kleiner als die Einstellung für `vmmaxpersnapshot`. Eine Momentaufnahme kann nicht gleichzeitig VMs auf lokalen Datenträgern und VMs auf CSV-Datenträgern enthalten.

Um zu verhindern, dass eine Momentaufnahme erstellt wird, die sich über mehrere Datenträger erstreckt, kann die Anzahl VMs in einer Momentaufnahme kleiner als die maximale Anzahl sein, wenn sich die VMs auf unterschiedlichen Datenträgern befinden. Beispiel: Vier VMs befinden sich auf Datenträger A und eine VM befindet sich auf Datenträger B. Es wird eine Momentaufnahme mit nur vier VMs (von Datenträger A) erstellt, obwohl die maximale Einstellung fünf ist. Für Datenträger B wird eine zweite Momentaufnahme erstellt.

Beispiele

Optionsdatei

```
vmmaxpersnapshot 10
```

Befehlszeile

```
dsmc backup vm -vmmaxpers=10
```

Zugehörige Konzepte:

„Geplante VM-Sicherungen für Windows Server 2012- und 2012 R2-Cluster optimieren" auf Seite 72

Zugehörige Verweise:

„Vmmaxsnapshotretry" auf Seite 212

Vmmaxsnapshotretry

Verwenden Sie die Option vmmaxsnapshotretry, um die maximale Anzahl Wiederholungen einer Momentaufnahmeoperation für eine virtuelle Maschine (VM) anzugeben, wenn die erste Momentaufnahmeoperation mit einer wiederherstellbaren Bedingung fehlschlägt.

Wenn während einer VM-Sicherung eine Momentaufnahmeoperation für eine VM aufgrund einer temporären Bedingung fehlschlägt, versucht Data Protection for Microsoft Hyper-V automatisch, die Momentaufnahmeoperation zu wiederholen, bis die durch die Option vmmaxsnapshotretry angegebene Anzahl Wiederholungen erreicht ist. Wenn die Momentaufnahmeoperation immer noch fehlschlägt, nachdem die maximale Anzahl Wiederholungen erreicht ist, wird nicht erneut versucht, die Momentaufnahmeoperation für die VM auszuführen, und der Sicherungsversuch schlägt fehl.

Eine wiederherstellbare Bedingung kann beispielsweise durch zwei Sicherungsanforderungen verursacht werden, die etwa zu derselben Zeit gestartet werden, um VMs zu sichern, die sich auf demselben Datenträger befinden. Eine der Sicherungsoperationen meldet, dass die Momentaufnahmeoperation fehlgeschlagen ist, da die Sicherung nicht gestartet werden kann, während eine andere Sicherung für dieselbe VM aktiv ist. In diesem Fall versucht Data Protection for Microsoft Hyper-V, die Momentaufnahmeoperation zu wiederholen, nachdem die erste VM-Sicherung abgeschlossen ist.

Wenn der ursprüngliche Fehler nicht behebbar ist, wird nicht versucht, eine Momentaufnahmeoperation auszuführen. Wenn beispielsweise während des ersten Momentaufnahmeprozesses ein Fehler beim VSS-Writer auftritt, wird die Sicherungsverarbeitung gestoppt und Data Protection for Microsoft Hyper-V versucht nicht, die Momentaufnahmeoperation zu wiederholen.

Diese Option ist nur für Hyper-V-Sicherungsoperationen unter Betriebssystemen Windows Server 2012 und 2012 R2 gültig.

Unterstützte Clients

Diese Option ist für alle unterstützten Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für den Befehl **Backup VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

Parameter

ganze_Zahl
Gibt die maximale Anzahl Wiederholungen der Momentaufnahmeoperation für eine VM an, wenn der erste Versuch zur Erstellung einer Momentaufnahme

mit einer wiederherstellbaren Bedingung fehlschlägt. Der Standardwert ist 20. Der Maximalwert ist 30. Der Mindestwert ist 1.

Wenn beispielsweise die Option `vmmaxsnapshotretry` auf 12 gesetzt ist, versucht Data Protection for Microsoft Hyper-V bis zu 12 Mal, die Momentaufnahmeoperation zu wiederholen, nachdem die erste Momentaufnahmeoperation während einer VM-Sicherungsoperation fehlgeschlagen ist. Wenn die Momentaufnahmeoperation immer noch fehlschlägt, nachdem die 12 Wiederholungen ausgeführt wurden, wird nicht versucht, weitere Wiederholungen auszuführen, und der Sicherungsversuch schlägt fehl.

Vor dem nächsten Wiederholungsversuch für eine Momentaufnahmeoperation müssen mindestens 10 Minuten verstreichen. Die Zeit zwischen Versuchen verlängert sich, wenn die fehlgeschlagene VM Teil einer Momentaufnahme für VMs ist, die gerade gesichert werden. Die Sicherungsoperation für die anderen VMs muss abgeschlossen sein und die Momentaufnahme von der Sicherungsoperation entfernt werden, bevor ein Wiederholungsversuch erfolgen kann.

Beispiele

Optionsdatei

```
vmmaxsna 12
```

Befehlszeile

```
dsmc backup vm -vmmaxsna=12
```

Zugehörige Konzepte:

„Geplante VM-Sicherungen für Windows Server 2012- und 2012 R2-Cluster optimieren" auf Seite 72

Zugehörige Verweise:

„Vmmaxpersnapshot" auf Seite 210

Vmmaxvirtualdisks

Die Option `vmmaxvirtualdisks` gibt die maximale Größe von Platten virtueller Hyper-V-Maschinen (VHDX) an, die bei einer Sicherungsoperation eingeschlossen werden sollen.

Verwenden Sie die Option `vmmaxvirtualdisks` mit der Option `vmskipmaxvirtualdisks`, um anzugeben, wie die Einheit zum Versetzen von Daten während einer Sicherungsoperation große Platten virtueller Maschinen (VM-Platten) verarbeitet:

- Definieren Sie die Option `vmmaxvirtualdisks`, um die maximale Größe von VM-Platten anzugeben, die eingeschlossen werden sollen.
- Definieren Sie die Option `vmskipmaxvirtualdisks`, um anzugeben, dass die VM-Platten, die die maximale Größe nicht überschreiten, gesichert (und die übrigen VM-Platten ausgeschlossen) werden sollen oder dass die Operation fehlschlagen soll.

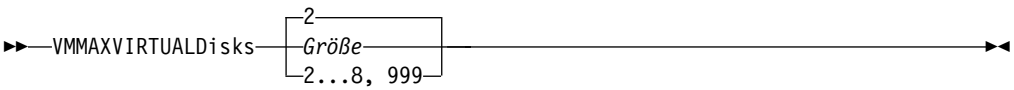
Unterstützte Clients

Diese Option ist für unterstützte Windows-Clients gültig, die als Einheiten zum Versetzen von Daten agieren und virtuelle Hyper-V-Maschinen sichern.

Optionsdatei

Definieren Sie die Option vmmaxvirtualdisks in der Clientoptionsdatei (dsm.opt). Sie können diese Option auch als Befehlszeilenparameter im Befehl **backup vm** angeben.

Syntax



Parameter

Größe

Gibt die maximale Größe der VM-Platten in Terabyte (TB) an, die in eine Sicherungsoperation eingeschlossen werden sollen. Der Bereich ist eine ganze Zahl von 2 bis 8; der Standardwert ist 2. Der Maximalwert ist 8 TB (äquivalent zu 8192 GB).

Geben Sie 999 an, um sicherzustellen, dass die Größe der VM-Platten, die bei Sicherungsoperationen eingeschlossen sind, immer die maximale Größe ist. Dieser Wert ist die einfachste Methode, um sicherzustellen, dass immer der Maximalwert definiert ist. Mit diesem Wert entfällt die kontinuierliche Änderung der Optionsdatei.

Wenn Sie außerdem die Option vmskipmaxvirtualdisks yes angeben, werden VM-Platten, die der angegebenen maximalen Größe entsprechen oder kleiner sind, gesichert, während VM-Platten, die größer als die angegebene maximale Größe sind, ausgeschlossen werden.

Wenn Sie außerdem die Option vmskipmaxvirtualdisks no angeben, schlagen Sicherungsoperationen fehl, wenn die Größe einer VM-Platte die angegebene maximale Größe überschreitet.

Beispiele

Optionsdatei:

```
vmmaxvirtualdisks 3
```

Befehlszeile:

VM-Platten sichern, die maximal 5 TB groß sind, und VM-Platten ausschließen, die größer als 5 TB sind:

```
backup vm VM1 -vmmaxvirtualdisks=5 -vmskipmaxvirtualdisks=yes
```

VM-Platten sichern, die maximal 3 TB groß sind, und die Sicherung fehlschlagen lassen, wenn eine VM-Platte größer als 3 TB ist:

```
backup vm VM1 -vmmaxvirtualdisks=3 -vmskipmaxvirtualdisks=no
```

VM-Platten sichern, die maximal 8 TB groß sind, und VM-Platten ausschließen, die größer als 8 TB sind:

```
backup vm VM1 -vmmaxvirtualdisks=8 -vmskipmaxvirtualdisks=yes
```

Oder:

```
backup vm VM1 -vmmaxvirtualdisks=999 -vmskipmaxvirtualdisks=yes
```

Vmmc

Verwenden Sie die Option vmmc zum Speichern von Sicherungen virtueller Maschinen unter Verwendung einer anderen als der Standardverwaltungsklasse.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie in der Befehlszeile ein.

Syntax

Parameter

Verwaltungsklassenname
Gibt eine Verwaltungsklasse für die gesicherten Daten virtueller Maschinen an. Wenn Sie diese Option nicht definieren, wird die Standardverwaltungsklasse des Knotens verwendet.

Beispiele

Task: Ausführen einer Sicherung der virtuellen Maschine mit dem Namen myVirtualMachine und Speichern der Sicherung entsprechend der Verwaltungsklasse mit dem Namen myManagmentClass.

```
dsmc backup vm "myVirtualMachine" -vmmc=myManagmentClass
```

Vmprocessvmwithphysdisks

Mithilfe der Option vmprocessvmwithphysdisks können Sie steuern, ob Hyper-V-RCT-Sicherungen einer virtuellen Maschine (VM) verarbeitet werden, wenn für die VM eine oder mehrere physische Platten (Durchgriffsplatten) bereitgestellt werden.

Eine virtuelle Maschine (VM) kann auf den Speicher auf einer physischen Platte zugreifen, die direkt mit dem Hyper-V-Server verbunden ist. Diese physische Platte wird als *Durchgriff*splatte bezeichnet.

Wenn Sie diese Option auf yes setzen, werden die Daten auf allen physischen Platten von Sicherungsoperationen ausgeschlossen, die Konfigurationsinformationen für die physischen Platten werden jedoch bei der VM-Sicherung gespeichert. Bei einer Zurückschreibungsoperation können Sie die Konfiguration der physischen Platten zurückschreiben, indem Sie die Option vmskipphysdisks no festlegen. Wenn die ursprünglichen physischen Platten verfügbar sind, werden sie wieder mit der zurückgeschriebenen VM verbunden.

Diese Option ist nur für RCT-Sicherungen unter Windows Server 2016 gültig. Diese Option ist nicht für Hyper-V-VSS-Sicherungen unter Windows Server 2012 oder Windows Server 2012 R2 gültig.

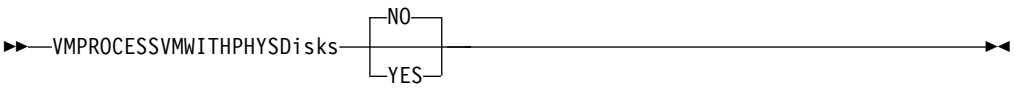
Unterstützte Clients

Diese Option ist für Clients unter Windows Server 2016 oder Betriebssystemen einer höheren Version gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) ein oder geben Sie sie als Befehlszeilenparameter im Befehl **backup vm** an.

Syntax



Parameter

No Die Sicherungsoperation der VM schlägt fehl, wenn eine oder mehrere physische Platten erkannt werden. Dies ist der Standardwert.

Yes
VMs, die eine oder mehrere physische Platten enthalten, werden gesichert. Mit dieser Option wird die Konfiguration der physischen Platten gesichert, ohne die Daten auf den physischen Platten zu sichern.

Beispiele

Optionsdatei:

```
VMPROCESSVMWITHPHYSDISKS Yes
```

Befehlszeile:

```
dsmc backup vm vmlocal -vmprocessvmwithphysd=yes
```

Zugehörige Verweise:

„Vmskipphysdisks" auf Seite 217

Vmskipmaxvirtualdisks

Die Option `vmskipmaxvirtualdisks` gibt an, wie Platten virtueller Maschinen (VM-Platten), die die maximale Plattengröße überschreiten, bei Sicherungsoperationen verarbeitet werden.

Verwenden Sie die Option `vmskipmaxvirtualdisks` mit der Option `vmmaxvirtualdisks`, um anzugeben, wie die Einheit zum Versetzen von Daten große VM-Platten während einer Sicherungsoperation verarbeitet:

- Definieren Sie die Option `vmskipmaxvirtualdisks`, um anzugeben, dass die VM-Platten, die die maximale Größe nicht überschreiten, gesichert (und die übrigen VM-Platten ausgeschlossen) werden sollen oder dass die Operation fehlschlagen soll.
- Definieren Sie die Option `vmmaxvirtualdisks`, um die maximale Größe von VM-Platten anzugeben, die eingeschlossen werden sollen.

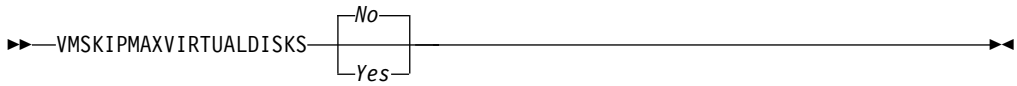
Unterstützte Clients

Diese Option ist für alle unterstützten Windows-Clients gültig, die als Einheiten zum Versetzen von Daten agieren und virtuelle Hyper-V-Maschinen sichern.

Optionsdatei

Definieren Sie die Option vmskipmaxvirtualdisks in der Clientoptionsdatei (dsm.opt). Sie können diese Option auch als Befehlszeilenparameter im Befehl **backup vm** angeben.

Syntax



Parameter

No Gibt an, dass Sicherungsoperationen fehlschlagen, wenn eine virtuelle Maschine mindestens eine VM-Platte enthält, die die maximale Größe überschreitet. Dies ist die Standardeinstellung.

Yes
Gibt an, dass bei Sicherungsoperationen VM-Platten eingeschlossen werden, die die maximale Größe nicht überschreiten, und VM-Platten ausgeschlossen werden, die die maximale Größe überschreiten.

Beispiele

Optionsdatei:

```
vmskipmaxvirtualdisks yes
```

Befehlszeile:

Angeben, dass eine Sicherungsoperation fehlschlagen soll, wenn eine VM-Platte größer als 2 TB ist:

```
backup vm VM1 -vmskipmaxvirtualdisks=no
```

Angeben, dass eine Sicherungsoperation fehlschlagen soll, wenn eine VM-Platte größer als 5 TB ist:

```
backup vm VM1 -vmskipmaxvirtualdisks=no -vmmaxvirtualdisks=5
```

VM-Platten sichern, die maximal 8 TB groß sind, und VM-Platten ausschließen, die größer als 8 TB sind:

```
backup vm VM1 -vmskipvirtualdisks=yes -vmmaxvirtualdisks=8
```

Vmskipphysdisks

Mithilfe der Option vmskipphysdisks können Sie Konfigurationsinformationen für physische Platten (Durchgriffsplatten), die einer virtuellen Hyper-V-Maschine zugeordnet sind, zurückschreiben, wenn die Nummern logischer Einheiten (LUNs), die den Datenträgern auf den physischen Platten zugeordnet sind, verfügbar sind.

Da physische Platten nicht in eine VM-Momentaufnahme eingeschlossen sind, können nur die Konfigurationsinformationen, aber nicht die Daten auf den Datenträgern zurückgeschrieben werden.

Diese Option ist nur für die Zurückschreibung virtueller Hyper-V-Maschinen unter Windows Server 2016 gültig. Diese Option ist nicht für Hyper-V-Hosts unter Windows Server 2012 oder Windows Server 2012 R2 gültig.

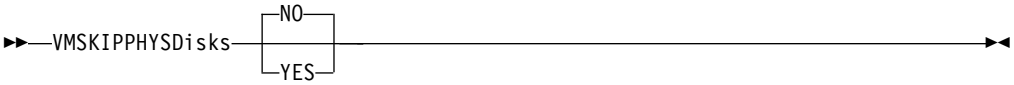
Unterstützte Clients

Diese Option ist für Clients unter Windows Server 2016 oder Betriebssystemen einer höheren Version gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) ein oder geben Sie sie als Befehlszeilenparameter im Befehl **`restore vm`** an.

Syntax



Parameter

`NO` Wenn die ursprünglichen physischen Platten verfügbar sind, geben Sie diesen Wert an, um die Konfigurationsinformationen für die physischen Platten, die mit der Option `vmprocessvmwithphysdisks yes` gesichert wurden, zurückzuschreiben. Die ursprünglichen physischen Platten werden wieder mit der zurückgeschriebenen VM verbunden. Wenn die ursprünglichen physischen Platten nicht lokalisiert werden können, schlägt die Zurückschreibungsoperation fehl. Dies ist der Standardwert.

`YES`
Geben Sie diesen Wert an, wenn Sie eine VM zurückschreiben müssen, die mit der Option `vmprocessvmwithphysdisks yes` gesichert wurde, und die ursprünglichen physischen Platten nicht lokalisiert werden können. Diese Einstellung hat zur Folge, dass der Client Versuche, die physischen Platten zu lokalisieren, überspringt und die Konfigurationsinformationen für die physischen Platten nicht zurückschreibt.

Beispiele

Optionsdatei:

```
VMSKIPPHYSDISKS YES
```

Befehlszeile:

```
dsmc restore vm vm123 -vmskipphysd=yes
```

Zugehörige Verweise:

„Vmprocessvmwithphysdisks" auf Seite 215

Kapitel 10. Bereitstellung und Dateizurückschreibung

Konfigurationen von IBM Spectrum Protect Recovery Agent

IBM Spectrum Protect Recovery Agent stellt eine Vielfalt von Konfigurationen für die Ausführung von Dateizurückschreibungen und für die Bereitstellung von Platten-/Blockeinheiten zur Verfügung.

Off-Host-Dateizurückschreibung

Für diese Konfiguration ist es nicht erforderlich, dass IBM Spectrum Protect Recovery Agent auf jeder virtuellen Gastmaschine installiert ist. Stattdessen ist eine Off-Host-Instanz für die Dateizurückschreibung mehrerer virtueller Maschinen verantwortlich. Mit dieser Konfiguration macht der Bereitstellungsprozess einen virtuellen Datenträger aus einer ausgewählten Plattenpartition verfügbar. Bei GPT-Platten muss die gesamte Platte verfügbar gemacht werden, damit die Partitionen verfügbar sind, und die Platte muss über iSCSI verbunden sein. Verwenden Sie die Recovery Agent-GUI, um diese Task auszuführen.

Sie müssen einen Knoten registrieren, der dem Recovery Agent zugeordnet ist. Dem Recovery Agent-Knoten muss die Proxy-Berechtigung erteilt werden, damit er auf den bzw. die Datenknoten mit den gespeicherten Momentaufnahmen zugreifen kann. Wenn eine Momentaufnahme für den Off-Host-Server bereitgestellt wird, kann der virtuelle Datenträger über das Netz gemeinsam genutzt werden, um ihn für die virtuelle Gastmaschine zugänglich zu machen. Alternativ können Sie auch die Dateien mit einer beliebigen Dateifreigabemethode vom bereitgestellten Datenträger auf die virtuelle Gastmaschine kopieren.

- Schrittweise Anleitungen für die Zurückschreibung sind unter „Eine oder mehrere Dateien zurückschreiben" auf Seite 224 beschrieben.

In-Guest-Dateizurückschreibung

Für diese Konfigurationen muss IBM Spectrum Protect Recovery Agent auf jeder virtuellen Gastmaschine installiert sein. Der Mount- und Zurückschreibungsprozess wird für eine Einzelpartition von der gesicherten Platte ausgeführt.

Dem IBM Spectrum Protect Recovery Agent-Knotennamen wird mit dem Befehl **dsmc set access** des IBM Spectrum Protect-Clients für Sichern/Archivieren in der Regel nur Zugriff auf die virtuelle Maschine erteilt, auf der er ausgeführt wird. Der Zurückschreibungsprozess wird normalerweise von einem Benutzer eingeleitet, der sich bei der Gastmaschine der virtuellen Maschine anmeldet.

Stellen Sie bei diesen Konfigurationen sicher, dass die speziellen Anforderungen an das Betriebssystem der virtuellen Gastmaschine mit den unterstützten Versionen von IBM Spectrum Protect Recovery Agent verglichen werden. Wenn ein bestimmtes Betriebssystem nicht unterstützt wird, stellen Sie fest, ob auch die Konfiguration für die Off-Host-Bereitstellung von Platten-/Blockeinheiten für die Dateizurückschreibung verwendet werden kann. Verwenden Sie zur Ausführung dieser Task die IBM Spectrum Protect Recovery Agent-GUI.

- Planungsinformationen und betriebssystembasierte Richtlinien finden Sie in Kapitel 10, „Bereitstellung und Dateizurückschreibung".

- Schrittweise Zurückschreibungsanweisungen finden Sie unter „Eine oder mehrere Dateien zurückschreiben" auf Seite 224.

Off-Host-iSCSI-Ziel

Bei dieser Konfiguration wird ein iSCSI-Ziel aus der Instanz des Off-Host-IBM Spectrum Protect Recovery Agent verfügbar gemacht und manuell ein In-Guest-iSCSI-Initiator für den Zugriff auf die Plattenmomentaufnahme verwendet. Diese Konfiguration erfordert es, dass ein iSCSI-Initiator auf der virtuellen Gastmaschine installiert ist. Anders als bei der Off-Host-Dateizurückschreibung, bei der eine einzelne Plattenpartition verfügbar gemacht wird, wird bei dieser Methode eine iSCSI-LUN verfügbar gemacht. Verwenden Sie zur Ausführung dieser Task die IBM Spectrum Protect Recovery Agent-GUI.

In dieser Konfiguration gibt der Benutzer den iSCSI-Initiatornamen der virtuellen Gastmaschine für das System an, auf dem auf die iSCSI-Einheit zugegriffen wird. Nachdem eine Plattenmomentaufnahme bereitgestellt wurde, kann sie unter Verwendung des iSCSI-Initiators auf der virtuellen Gastmaschine erkannt und dort angemeldet werden.

Wenn Sie eine virtuelle Maschine sichern, die GPT-Platten (GPT - GUID Partition Table) enthält, und den Datenträger in der GPT-Platte bereitstellen möchten, gehen Sie wie folgt vor:

1. Stellen Sie die GPT-Platte als iSCSI-Ziel bereit.
2. Verwenden Sie den Microsoft-iSCSI-Initiator, um sich bei dem Ziel anzumelden.
3. Öffnen Sie die Windows-Datenträgerverwaltung, um die Platte zu suchen, und versetzen Sie die Platte in den Onlinestatus. Sie können dann den Datenträger in der GPT-Platte anzeigen.

- Planungsinformationen und betriebssystembasierte Richtlinien finden Sie in Kapitel 10, „Bereitstellung und Dateizurückschreibung", auf Seite 219.
- Schrittweise Zurückschreibungsanweisungen stehen unter „Eine oder mehrere Dateien zurückschreiben" auf Seite 224 zur Verfügung.

Übersicht über die Momentaufnahmebereitstellung

Mit IBM Spectrum Protect Recovery Agent können Sie eine Momentaufnahme bereitstellen und die Momentaufnahme für die Ausführung einer Datenwiederherstellung verwenden.

Stellen Sie Momentaufnahmen über die IBM Spectrum Protect Recovery Agent-GUI bereit. Verwenden Sie für die Installation und Ausführung von Recovery Agent ein System, das über ein LAN mit dem IBM Spectrum Protect-Server verbunden ist. Die Operationen der Komponente Recovery Agent können Sie in einem LAN-unabhängigen Pfad nicht verwenden.

Beachten Sie die folgenden Situationen bei der Ausführung von Mountoperationen:

- Ist IBM Spectrum Protect Recovery Agent auf einer Gastmaschine installiert, können Sie keine Mountoperation für ein Dateisystem oder eine Platte starten, während die Gastmaschine gesichert wird. Sie müssen vor der Ausführung einer Mountoperation entweder auf das Ende der Sicherung warten oder die Sicherung abbrechen. Diese Operationen sind nicht zulässig, weil der Sperrmechanismus für eine gesamte virtuelle Maschine gilt.
- Beim Anzeigen des Momentaufnahmesicherungsbestands handelt es sich bei der Betriebssystemversion der virtuellen Maschine um die Version, die bei der ur-

sprünglichen Erstellung der virtuellen Maschine angegeben wurde. Deshalb spiegelt Recovery Agent möglicherweise nicht das aktuelle Betriebssystem wider.

- Ein Datenträger wird instabil, wenn eine Mountoperation durch einen Netzausfall unterbrochen wird. Eine Nachricht wird an das Ereignisprotokoll ausgegeben. Nachdem die Netzverbindung wiederhergestellt wurde, wird eine weitere Nachricht an das Ereignisprotokoll ausgegeben. Diese Nachrichten werden nicht an die Recovery Agent-GUI ausgegeben.

Es werden maximal 20 iSCSI-Sitzungen unterstützt. Dieselbe Momentaufnahme kann mehrmals bereitgestellt werden. Wenn Sie eine Momentaufnahme aus demselben Bandspeicherpool unter Verwendung mehrerer Instanzen von Recovery Agent bereitstellen, wird eine der folgenden Aktionen ausgeführt:

- Die zweite Recovery Agent-Instanz wird geblockt, bis die erste Instanz beendet ist.
- Die zweite Recovery Agent-Instanz kann die Aktivität der ersten Instanz unterbrechen. Beispielsweise kann sie einen Dateikopierprozess der ersten Instanz unterbrechen.
- Recovery Agent kann keine Verbindung zu mehreren Servern oder Knoten gleichzeitig herstellen.

Vermeiden Sie daher parallele Recovery Agent-Sitzungen für denselben Banddatenträger.

Mountrichtlinien

Momentaufnahmen können entweder im schreibgeschützten Modus oder im Schreib-/Lesemodus bereitgestellt werden. Im Schreib-/Lesemodus speichert Recovery Agent Änderungen an Daten im Speicher. Wird der Service erneut gestartet, gehen die Änderungen verloren.

Recovery Agent wird in einem der beiden folgenden Modi ausgeführt:

Kein Benutzer ist angemeldet
Recovery Agent wird als Service ausgeführt.

Benutzer ist angemeldet
Recovery Agent wird weiterhin als Service ausgeführt, bis Sie Recovery Agent starten und die GUI verwenden. Wenn Sie Recovery Agent und die GUI schließen, wird der Service erneut gestartet. Sie können Recovery Agent und die GUI nur verwenden, wenn Sie mit Anmeldeberechtigungsnachweisen für Administratoren angemeldet sind. Nur eine einzige Kopie von Recovery Agent kann jeweils aktiv sein.

Wenn bereitgestellte Datenträger vorhanden sind und Mount über das Startmenü gestartet wird, wird die folgende Nachricht angezeigt:

```
Einige Momentaufnahmen werden momentan
bereitgestellt. Wenn Sie fortfahren, wird die Bereitstellung dieser Momentaufnahmen aufgehoben. Beachten
Sie, dass eine Anwendung instabil werden kann, wenn ein bereitgestellter Datenträger momentan von
der Anwendung verwendet wird. Fortfahren?
```

Wenn **Ja** angeklickt wird, wird die Bereitstellung der bereitgestellten Datenträger aufgehoben, auch wenn sie im Gebrauch sind.

Einschränkung: Wenn Momentaufnahmen als iSCSI-Ziele bereitgestellt werden und eine Momentaufnahme einer dynamischen Platte für das Originalsystem bereitgestellt wird, sind die UUIDs doppelt vorhanden. Ebenso sind doppelte GUIDs

vorhanden, wenn eine Momentaufnahme einer GPT-Platte für das Originalsystem bereitgestellt wird. Machen Sie, um diese Duplizierung zu vermeiden, dynamische Platten und GPT-Platten für ein anderes System als das Originalsystem verfügbar. Stellen Sie beispielsweise diese Plattentypen für ein Proxy-System bereit, es sei denn, die ursprünglichen Platten sind nicht mehr vorhanden.

Übersicht über die Dateizurückschreibung

Verwenden Sie IBM Spectrum Protect Recovery Agent für effiziente Dateizurückschreibungsoperationen und zum Minimieren der Ausfallzeit, indem Sie Momentaufnahmen auf virtuellen Datenträgern bereitstellen.

IBM Spectrum Protect Recovery Agent kann für die folgenden Tasks verwendet werden:

- Wiederherstellen von verloren gegangenen oder beschädigten Dateien aus einer Sicherung
- Bereitstellen eines Datenträgers einer virtuellen Gastmaschine und Erstellen eines Archivs der Dateien der virtuellen Gastmaschine
- Bereitstellen von Datenbankanwendungen für Stapelberichte

Der virtuelle Datenträger kann mit Hilfe eines beliebigen Dateimanagers, wie z. B. Windows Explorer, angezeigt werden. Die Verzeichnisse und Dateien in der Momentaufnahme können wie jede andere Datei angezeigt und verwaltet werden. Wenn Sie die Dateien editieren und Ihre Änderungen speichern, gehen Ihre Änderungen verloren, sobald Sie die Bereitstellung des Datenträgers aufheben, da die geänderten Daten im Speicher verbleiben und nie auf Platte gespeichert werden. Da die Änderungen in den Speicher geschrieben werden, kann IBM Spectrum Protect Recovery Agent sehr viel Arbeitsspeicher verwenden, wenn der Schreib-/Lesemodus verwendet wird.

Sie können die geänderten Dateien vor dem Aufheben der Bereitstellung des Datenträgers auf einen anderen Datenträger kopieren.

Die Standard-Mountoption *schreibgeschützt* ist die bevorzugte Methode, wenn ein bereitgestellter Datenträger nicht änderbar sein soll. Für eine Archivierungsanwendung kann zum Beispiel der Schreibzugriff auf den archivierten Datenträger erforderlich sein.

IBM Spectrum Protect Recovery Agent stellt Momentaufnahmen vom IBM Spectrum Protect-Server bereit. Klicken Sie in der IBM Spectrum Protect Recovery Agent-GUI auf **Entfernen**, um eine bestehende Verbindung zu dem IBM Spectrum Protect-Server zu beenden. Sie müssen alle bestehenden Verbindungen entfernen, bevor Sie eine neue Verbindung zu einem anderen Server oder anderen Knoten aufbauen können. Heben Sie die Bereitstellung aller Datenträger auf, bevor Sie auf **Entfernen** klicken. Die Operation zum Entfernen schlägt fehl, wenn aktive Mount- und Zurückschreibungssitzungen auf den Mountmaschinen vorhanden sind. Sie können die Verbindung zu einem Server nicht entfernen, während Sie eine Dateizurückschreibung von diesem Server ausführen. Sie müssen zuerst die Bereitstellung für alle virtuellen Einheiten aufheben und alle Zurückschreibungssitzungen stoppen, bevor Sie die Verbindung zu einem Server trennen. Andernfalls wird die Verbindung nicht entfernt.

Sie müssen die Bereitstellung aller virtuellen Datenträger aufheben, bevor Sie IBM Spectrum Protect Recovery Agent deinstallieren. Andernfalls kann die Bereitstel-

lung dieser bereitgestellten virtuellen Datenträger nach der erneuten Installation von IBM Spectrum Protect Recovery Agent nicht aufgehoben werden.

Die Zurückschreibung von Dateiinformationen für eine Momentaufnahme auf Blockebene ist ein Prozess mit wahlfreiem Zugriff. Dies kann zu einer langsamen Verarbeitung führen, wenn eine Einheit mit sequenziellem Zugriff (zum Beispiel ein Band) verwendet wird. Zum Ausführen einer Dateizurückschreibung von Daten, die auf Band gespeichert sind, empfiehlt es sich möglicherweise, die Daten zunächst auf eine Platte oder in einen Dateispeicher zu versetzen. Geben Sie auf dem Verwaltungsbefehlszeilenclient des IBM Spectrum Protect-Servers (`dsmadmc`) den Befehl **`QUERY OCCUPANCY`** aus, um zu ermitteln, wo die Daten gespeichert sind. Geben Sie dann den Befehl **`MOVE NODEDATA`** aus, um die Daten auf die Platte oder in den Dateispeicher zu versetzen.

Die Bereitstellung einer Momentaufnahme aus demselben Bandspeicherpool durch zwei Instanzen von Mount kann zu einem der folgenden Ergebnisse führen:

- Die zweite Mountinstanz wird geblockt, bis die erste Instanz beendet ist.
- Beide Mountinstanzen sind erfolgreich, aber die Leistung ist schlecht.

Wenn Sie Daten aus einem gespiegelten Datenträger zurückschreiben, stellen Sie nur eine der Platten bereit, die den gespiegelten Datenträger enthalten. Werden beide Platten bereitgestellt, versucht Windows, die Platten zu resynchronisieren. Beide Platten enthalten jedoch unterschiedliche Zeitmarken, wenn sie bereitgestellt werden. Infolgedessen werden alle Daten von einer Platte auf die andere Platte kopiert. Dieses Datenvolumen kann vom virtuellen Datenträger nicht aufgenommen werden. Wenn Sie Daten von einem Datenträger wiederherstellen müssen, der sich über zwei Platten erstreckt, und diese Platten einen gespiegelten Datenträger enthalten, gehen Sie folgendermaßen vor:

1. Stellen Sie die beiden Platten bereit.
2. Stellen Sie mit dem iSCSI-Initiator eine Verbindung zur ersten Platte her.
3. Importieren Sie diese Platte mit dem Windows Disk Manager. Ignorieren Sie alle Nachrichten, die sich auf die Synchronisation beziehen.
4. Löschen Sie die gespiegelte Partition von der ersten (d.h. importierten) Platte.
5. Stellen Sie mit dem iSCSI-Initiator eine Verbindung zur zweiten Platte her.
6. Importieren Sie die zweite Platte mit dem Windows Disk Manager.

Beide Datenträger sind nun verfügbar.

Einschränkung: Ändern Sie das IBM Spectrum Protect-Knotenkennwort nicht, während eine Dateizurückschreibung aus Momentaufnahmen ausgeführt wird, die auf diesem Knoten gespeichert sind.

Richtlinien für die Dateizurückschreibung

Sie können IBM Spectrum Protect Recovery Agent verwenden, um Dateien effizient zurückzuschreiben und die Ausfallzeit zu minimieren, indem Sie Momentaufnahmen auf virtuellen Datenträgern bereitstellen. Die Dateizurückschreibung wird aus Momentaufnahmen von NTFS-, FAT- oder FAT32-Datenträgern unterstützt.

Die Bereitstellungsfunktion kann nicht verwendet werden, um eine Momentaufnahme von Partitionen aus einer dynamischen oder einer GPT-basierten Platte als virtuellen Datenträger bereitzustellen. Nur Partitionen aus einer MBR-basierten Platte/Basisplatte können als virtuelle Datenträger bereitgestellt werden. Die Dateizurückschreibung von einer GPT-Platte, einer dynamischen Platte oder einer ande-

ren Nicht-MBR- oder Nicht-Basisplatte ist möglich, indem ein virtuelles iSCSI-Ziel erstellt und unter Verwendung eines iSCSI-Initiators mit Ihrem System verbunden wird.

Wenn Sie eine Dateizurückschreibung für Daten auf dynamischen Platten ausführen, muss die Momentaufnahme für einen Server bereitgestellt werden, auf dem im Vergleich zu dem Knoten, auf dem die Momentaufnahme erstellt wurde, dieselbe oder eine neuere Version von Windows ausgeführt wird. Auf Dateien auf der dynamischen Platte kann indirekt von Knoten, auf denen ältere Versionen von Windows ausgeführt werden, zugegriffen werden, indem ein Laufwerk auf den älteren Knoten einem freigegebenen CIFS-Verzeichnis zugeordnet wird, in dem die Momentaufnahme bereitgestellt wird.

Wichtig: Die ACL-Werte, die den Ordnern und Dateien zugeordnet sind, die in einer Dateizurückschreibungsoperation zurückgeschrieben werden, werden nicht in die zurückgeschriebenen Dateien übertragen. Um ACL-Werte beizubehalten, verwenden Sie den Befehl **XCOPY**, wenn Dateien vom Ziel kopiert werden.

Eine oder mehrere Dateien zurückschreiben

Sie können eine einzige Datei (oder mehrere Dateien) einer virtuellen Maschine zurückschreiben, die im IBM Spectrum Protect-Serverspeicher gesichert wurde(n).

Vorbereitende Schritte

Wenn Ihre Zurückschreibungsoperation mit einem In-Guest-iSCSI-Initiator auf die Momentaufnahme der Platte einer virtuellen Maschine zugreift, müssen zunächst die folgenden Bedingungen erfüllt sein:

- Die iSCSI-Einheit ist konfiguriert und das iSCSI-Initiatorprogramm wird ausgeführt.
- Port `3260` ist in der LAN-Firewall zwischen dem System, auf dem die IBM Spectrum Protect Recovery Agent-GUI installiert ist, und dem Initiatorsystem offen.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Platte einer gesicherten virtuellen Maschine bereitzustellen und den bereitgestellten Datenträger für eine Dateizurückschreibungsoperation zu exportieren:

Vorgehensweise

1. Starten Sie die IBM Spectrum Protect Recovery Agent-GUI.
   Rufen Sie auf dem Windows-System **Start** > **Apps nach Name** > **IBM Spectrum Protect** > **IBM Spectrum Protect Recovery Agent** auf.
   Die IBM Spectrum Protect Recovery Agent-GUI kann entweder auf der virtuellen Gastmaschine oder auf einem separaten Host installiert sein.
2. Stellen Sie eine Verbindung zu dem IBM Spectrum Protect-Server her, indem Sie auf **IBM Spectrum Protect-Server auswählen** klicken. Auf dem Zielknoten befinden sich die Sicherungen. Sie können die Zugriffsebene für die Daten des Zielknotens steuern, indem Sie einen anderen Knotennamen im Abschnitt `Knotenzugriffsmethode` angeben.
3. Wählen Sie eine virtuelle Maschine in der Liste aus.

   Tipp: Sie können Ihre virtuelle Maschine schnell finden, indem Sie die ersten Buchstaben des Maschinennamens in den Editierteil des Listenfensters einge-

ben. Die Liste zeigt nur die Maschinen an, die mit den eingegebenen Buchstaben übereinstimmen. Bei Maschinennamen muss die Groß-/Kleinschreibung beachtet werden.

Eine virtuelle Maschine kann in der Liste angezeigt werden, aber wenn sie ausgewählt wird, ist die Momentaufnahmenliste möglicherweise leer. Diese Situation tritt aus einem der folgenden Gründe auf:

- Für diese virtuelle Maschine wurde keine Momentaufnahme erfolgreich erstellt.
- Die Option **Von Knoten** wurde verwendet und der angegebene Knoten ist nicht berechtigt, die ausgewählte virtuelle Maschine zurückzuschreiben.

4. Stellen Sie die Momentaufnahme über eine iSCSI-Verbindung bereit:
   a. Klicken Sie in der IBM Spectrum Protect Recovery Agent-GUI auf **Bereitstellen**.
   b. Klicken Sie im Dialog **Bereitstellungsziel auswählen** auf **Bereitstellung als iSCSI-Ziel**.
   c. Geben Sie den Namen des Ziels ein. Dieser Name muss für jede Bereitstellung eindeutig sein.
   d. Geben Sie den iSCSI-Initiatornamen ein.
   Der iSCSI-Initiatorname wird in der Registerkarte **Konfiguration** im Dialog **iSCSI-Initiator-Eigenschaften** angezeigt. Beispiel:
   ```
   iqn.1991-05.com.microsoft:hostname
   ```
5. Führen Sie die folgenden Schritte auf dem Zielsystem aus, auf dem der iSCSI-Initiator installiert ist:
   a. Klicken Sie auf die Registerkarte **Ziele**.
   b. Geben Sie im Abschnitt **Schnell verbinden** die IP-Adresse oder den Hostnamen des Systems an, auf dem die IBM Spectrum Protect Recovery Agent-GUI installiert ist.
   c. Klicken Sie auf **Schnell verbinden**.
   d. Wählen Sie im Dialog **Schnell verbinden** im Feld **Erkannte Ziele** die IP-Adresse oder den Hostnamen aus und klicken Sie auf **Verbinden**.
   e. Wenn **Status - Verbunden** angezeigt wird, klicken Sie auf **Fertig**.
   f. Rufen Sie **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.
6. Wählen Sie das bevorzugte Momentaufnahmedatum aus. Es wird eine Liste von Platten virtueller Maschinen angezeigt, die in der ausgewählten Momentaufnahme gesichert sind. Wählen Sie eine Platte aus und klicken Sie auf **Bereitstellen**.

7. Wählen Sie im Dialog `Bereitstellungsziel auswählen` die Option **Virtuellen Datenträger aus ausgewählter Partition erstellen** aus. Eine Liste der Partitionen, die auf der ausgewählten Platte verfügbar sind, wird angezeigt. Für jede Partition werden die Größe, der Kennsatz und der Dateisystemtyp angezeigt.
   - Handelt es sich bei der Platte nicht um eine MBR-basierte Platte, wird eine Fehlernachricht angezeigt.
   - Standardmäßig werden nur Partitionen angezeigt, die für die Dateizurückschreibung verwendet werden können.
   - Sollen alle Partitionen angezeigt werden, die auf der ursprünglichen Platte vorhanden waren, inaktivieren Sie das Kontrollkästchen **Nur Partitionen anzeigen, die bereitgestellt werden können**.
8. Wählen Sie die erforderliche Partition aus. Partitionen, die mit nicht unterstützten Dateisystemen formatiert wurden, können nicht ausgewählt werden.
9. Geben Sie einen Laufwerkbuchstaben oder einen leeren Ordner als Mountpunkt für den virtuellen Datenträger an.
10. Klicken Sie auf **OK**, um einen virtuellen Datenträger zu erstellen, der zur Wiederherstellung der Dateien verwendet werden kann.
11. Wenn der virtuelle Datenträger erstellt wurde, verwenden Sie Windows Explorer, um die Dateien an die gewünschte Position zu kopieren.

    Tipp: Die ACL-Werte, die den Ordnern und Dateien zugeordnet sind, die in einer Dateizurückschreibungsoperation zurückgeschrieben werden, werden nicht in die zurückgeschriebenen Dateien übertragen. Um ACL-Werte beizubehalten, verwenden Sie den Befehl **`XCOPY`**, wenn Dateien vom Ziel kopiert werden.

Zugehörige Tasks:

„IBM Spectrum Protect Recovery Agent-GUI konfigurieren" auf Seite 60

„iSCSI-Einheit manuell konfigurieren" auf Seite 69

Kapitel 11. IBM Spectrum Protect Recovery Agent-Befehle

Die Recovery Agent-Befehlszeilenschnittstelle (Command-Line Interface - CLI) kann als Befehlszeilen-API zu IBM Spectrum Protect Recovery Agent angesehen werden. Änderungen, die über die Recovery Agent-CLI an IBM Spectrum Protect Recovery Agent vorgenommen werden, werden sofort wirksam.

Mit der Recovery Agent-CLI können Sie nur ein einziges System verwalten, auf dem IBM Spectrum Protect Recovery Agent ausgeführt wird.

Klicken Sie auf einem Windows-System auf **Start** > **Apps nach Name** > **IBM Spectrum Protect** > **Recovery Agent-CLI**.

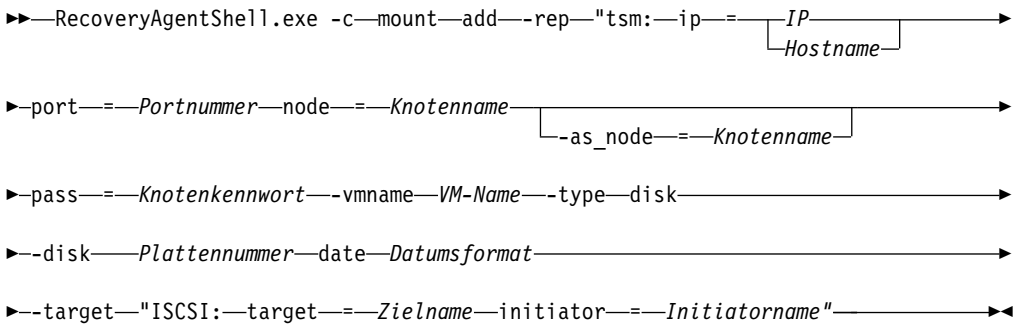
Mount

Mit dem Befehl **mount** können Sie verschiedene IBM Spectrum Protect Recovery Agent-Tasks ausführen.

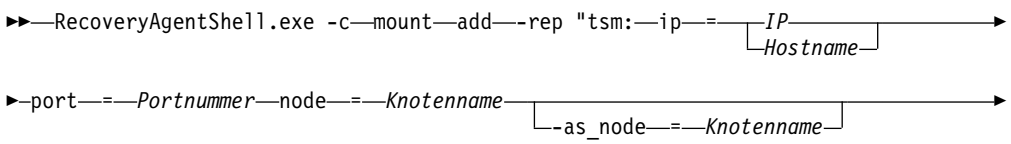
Die Recovery Agent-CLI kann zum Bereitstellen (**mount add**) und Aufheben der Bereitstellung (**mount del**) von Datenträgern und Platten sowie zum Anzeigen einer Liste bereitgestellter Datenträger (**mount view**) verwendet werden. Für die Verwendung des Befehls **mount** muss IBM Spectrum Protect Recovery Agent aktiv sein. Verwenden Sie den Befehl **set_connection**, um eine RecoveryAgentShell.exe mit der Mountanwendung zu verbinden.

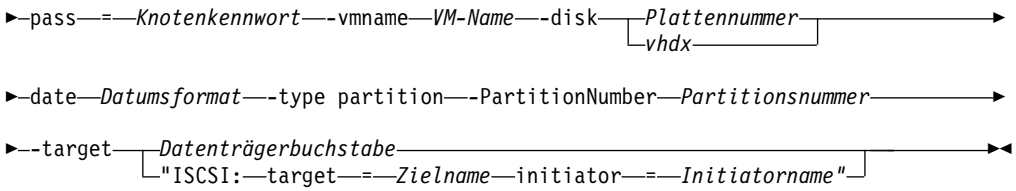
Die Bereitstellung bzw. Aufhebung der Bereitstellung von Momentaufnahmen erfolgt auf dem System, auf dem IBM Spectrum Protect Recovery Agent ausgeführt wird.

Syntax für das Bereitstellen einer Platte



Syntax für das Bereitstellen einer Partition





Befehlstypen

add Verwenden Sie diesen Befehlstyp, um eine Platte oder einen Datenträger mit einer Momentaufnahme auf dem System bereitzustellen, auf dem IBM Spectrum Protect Recovery Agent ausgeführt wird.

In der folgenden Liste sind die Tags und Parameter für den Befehlstyp **add** aufgeführt:

-target
Dieser Tag ist erforderlich. Mit diesem Tag können Sie die folgenden Ziele angeben:

- Virtueller Datenträger - nur für eine Partitionsbereitstellung
- Analysepunkt - nur für eine Partitionsbereitstellung
- iSCSI-Ziel

-rep Dieser Tag ist erforderlich. Verwenden Sie ihn, um den IBM Spectrum Protect-Server anzugeben, auf dem die Momentaufnahmen gespeichert sind, und den IBM Spectrum Protect-Knoten anzugeben, der Zugriff auf die Sicherungen hat. Beispiel:

```
tsm: ip=<IP/Hostname> port=<Portnummer>
 node=<Knotenname> pass=<Knotenkennwort>
```

Sie können auch die Optionen `as_node` und `from_node` angeben. Wenn das Feld für das `Kennwort` leer ist, versucht IBM Spectrum Protect Recovery Agent, das Kennwort für den gespeicherten Knoten zu verwenden.

-type Dieser Tag ist erforderlich. Verwenden Sie ihn, um anzugeben, dass eine Platte oder eine Partition bereitgestellt werden soll. Die Optionen sind:

-type disk

-type partition

-VMname
Dieser Tag ist erforderlich. Verwenden Sie ihn, um den Namen der Maschine anzugeben, die die Quelle der Momentaufnahme ist. Beim angegebenen Wert muss die Groß-/Kleinschreibung beachtet werden.

-disk Dieser Tag ist erforderlich. Verwenden Sie ihn, um die Nummer der bereitzustellenden Platte der gesicherten Quellenmaschine anzugeben.

-date Dieser Tag ist erforderlich. Verwenden Sie ihn, um das Datum der Momentaufnahme anzugeben, die bereitgestellt werden soll. Das Datumsformat lautet `jjjj-Mmm-tt hh:mm:ss`. Beispiel:

```
-date "2013-Apr-12 22:42:52 AM"
```

Zum Anzeigen der aktiven (oder letzten) Momentaufnahme geben Sie `Letzte Momentaufnahme` an.

-PartitionNumber
Dieser Tag ist optional. Hat der Tag `-type` den Wert `partition`, geben Sie die Nummer der Partition ein, die bereitgestellt werden soll.

-ro|-fw
Verwenden Sie diesen Tag, um anzugeben, ob der bereitgestellte Datenträger schreibgeschützt ist (**-ro**) oder über imitierten Schreibzugriff (**-fw**) verfügt.

-disk Dieser Tag ist erforderlich. Verwenden Sie ihn, um die Nummer der bereitzustellenden Platte der gesicherten Quellenmaschine anzugeben.

-ExpireProtect
Dieser Tag ist optional. 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. Sie können einen der folgenden Werte angeben:

Yes Geben Sie `Yes` an, um die Momentaufnahme vor dem Verfall zu schützen. Dieser Wert ist der Standardwert. Die Momentaufnahme auf dem IBM Spectrum Protect-Server wird gesperrt und die Momentaufnahme ist während der Mountoperation vor dem Verfall geschützt.

No Geben Sie `No` an, um den Verfallsschutz zu inaktivieren. 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 Angabe von `No`, um den Sperrversuch und dieses Fehlschlagen zu verhindern.

dump Verwenden Sie diesen Befehlstyp, um eine Liste aller verfügbaren Sicherungen für die Bereitstellung abzurufen.

In der folgenden Liste sind die Tags und Parameter für den Befehlstyp **dump** aufgeführt:

-rep Dieser Tag ist erforderlich. Verwenden Sie diesen Tag, um den IBM Spectrum Protect-Server anzugeben, auf dem die Momentaufnahmen gespeichert sind, und den IBM Spectrum Protect-Knoten anzugeben, der Zugriff auf die Sicherungen hat. Beispiel:

```
tsm: ip=<IP/Hostname> port=<Portnummer>
node=<Knotenname> pass=<Knotenkennwort>
```

-file Dieser Tag ist optional. Verwenden Sie diesen Tag, um den Namen einer Datei zur Speicherung des Speicherauszugstextes anzugeben. Wenn dieser Tag nicht angegeben wird, wird der Speicherauszugstext nur an stdout ausgegeben.

remove

Verwenden Sie diesen Typ, um die Verbindung zu dem IBM Spectrum Protect-Server zu entfernen. Eine Verbindung kann nicht entfernt werden, wenn sie im Gebrauch ist, beispielsweise wenn bereitgestellte Datenträger vorhanden sind.

Die folgende Liste enthält den Tag für den Befehlstyp **remove**:

-rep - Dieser Tag ist erforderlich. Verwenden Sie diesen Tag, um die IBM Spectrum Protect-Serververbindung anzugeben, die entfernt werden soll.

view Mit diesem Typ zeigen Sie eine Liste aller bereitgestellten Momentaufnahmen an. Dieser Typ hat keine Tags.

Beispielbefehle

In den folgenden Beispielen wird der Tag **-target** verwendet:

- In dem folgenden Beispiel ist *V:* das Bereitstellungsziel für den virtuellen Datenträger:

  ```
  -target "V:"
  ```

- In dem folgenden Beispiel wird ein Analysepunkt als Bereitstellungsziel für den Datenträger angegeben:

  ```
  -target "C:\SNOWBIRD@FASTBACK\SnowbirtK\Snowbird\K\\"
  ```

- In dem folgenden Beispiel wird ein iSCSI-Ziel angegeben:

  ```
  -target "ISCSI: target=<Zielname> initiator=<Initiatorname>"
  ```

In diesem Beispiel befindet sich eine Momentaufnahme der virtuellen Maschine mit dem Namen VM-03ent auf einem IBM Spectrum Protect-Server mit der IP-Adresse IP 10.10.10.01. Die Platte mit der Nummer 1 dieser Momentaufnahme wird auf dem System bereitgestellt, auf dem IBM Spectrum Protect Recovery Agent ausgeführt wird. Der folgende Befehl zeigt, wie der Typ **add** angegeben wird, um eine Platte bereitzustellen:

```
mount add -rep "tsm: ip=10.10.10.01 port=1500 node=tsm-ba pass=Kennwort"
-target "iscsi: target=test1 initiator=Initiatorname" -type disk
-vmname VM-03ENT -disk 1 -date "2014-Jan-21 10:46:57 AM -ExpireProtect=Yes"
```

Die folgenden Beispiele zeigen, wie der Typ 'dump' angegeben wird:

- Alle verfügbaren gesicherten virtuellen Maschinen auflisten.

  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListVM [–file <Dateiname und Pfad>]
  ```

- Alle verfügbaren Plattenmomentaufnahmen einer virtuellen Maschine auflisten.

  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListSnapshots -VMName P [-file <Dateiname und Pfad>]
  ```

- Alle verfügbaren Partitionen einer Plattenmomentaufnahme auflisten.

  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListPartitions -VMName P -disk P -date P [-file <Dateiname und Pfad>]
  ```

Im folgenden Beispiel wird die Verbindung zu dem IBM Spectrum Protect-Server (10.10.10.01) unter Verwendung des Knotens NodeName entfernt:

```
mount remove -rep "tsm: NodeName@ip"
```

Im folgenden Beispiel wird der Typ **view** verwendet:

```
mount view
```

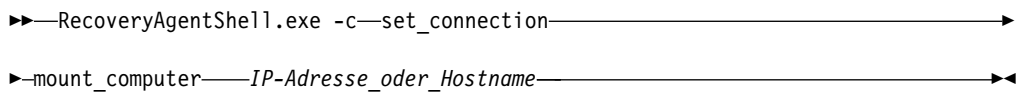
Links für die Bereitstellung einer Hyper-V-Momentaufnahme

- „**Set_connection**"
- „**Help**" auf Seite 232

Set_connection

Mit dem Befehl **set_connection** wird die Verbindung von der Recovery Agent-CLI zu einer angegebenen IBM Spectrum Protect Recovery Agent-Instanz definiert.

Syntax



Befehlstyp

mount_computer

Verwenden Sie diesen Befehlstyp zum Festlegen der Verbindung zwischen der Recovery Agent-CLI und dem System, auf dem IBM Spectrum Protect Recovery Agent installiert ist.

Die folgende Liste enthält die Parameter für den Befehlstyp **mount_computer**:

IP-Adresse_oder_Hostname

Diese Variable ist erforderlich. Geben Sie die IP-Adresse oder den Hostnamen des Systems an, auf dem IBM Spectrum Protect Recovery Agent installiert ist.

Beispielbefehle

Im folgenden Beispiel wird die Recovery Agent-CLI für die Verwendung von IBM Spectrum Protect Recovery Agent auf dem Host *Computername* definiert.

```
set_connection mount_computer Computername
```

Links für das Einrichten einer Verbindung

- „**Mount**" auf Seite 227
- „**Help**" auf Seite 232

Help

Mit dem Befehl **help** wird die Hilfe für alle unterstützten Befehle der Recovery Agent-CLI angezeigt.

Syntax

```
►►—RecoveryAgentShell.exe -c—-h—Befehl————————————————————————————►◄
```

Befehlstag

-h Verwenden Sie diesen Befehlstag zum Anzeigen von Hilfeinformationen.

Die folgende Liste enthält den Parameter für den Befehlstyp **mount_computer**:

Befehl Diese Variable ist erforderlich. Geben Sie den Recovery Agent-Befehl an, für den Sie Hilfeinformationen benötigen.

Beispielbefehle

Im folgenden Beispiel wird die Recovery Agent-CLI für die Verwendung von IBM Spectrum Protect Recovery Agent auf dem Host *Computername* definiert.

```
set_connection mount_computer Computername
```

Links für das Einrichten einer Verbindung

- „**Mount**" auf Seite 227
- „**Set_connection**" auf Seite 231

Rückkehrcodes der Recovery Agent-Befehlszeilenschnittstelle

Anhand von Rückkehrcodes können Sie die Ergebnisse für Operationen der Recovery Agent-Befehlszeilenschnittstelle (Command Line Interface - CLI) ermitteln.

Verwenden Sie die folgenden Rückkehrcodes, um den Status Ihrer Operationen in der Recovery Agent-CLI zu überprüfen.

Tabelle 18. Rückkehrcodes der Recovery Agent-CLI

Rückkehrcode	Wert	Beschreibung
0	FBC_MSG_MOUNT_SUCCESS	Der Befehl wurde erfolgreich an die Bereitstellung von Data Protection for Microsoft Hyper-V übergeben.
0	FBC_MSG_DISMOUNT_SUCCESS	Die Bereitstellung einer Momentaufnahme wurde erfolgreich aufgehoben.
0	FBC_MSG_VIEW_SUCCESS	Die Anzeigeoperation wurde erfolgreich ausgeführt.
0	FBC_MSG_DUMP_SUCCESS	Die Speicherauszugsoperation wurde erfolgreich ausgeführt.
0	FBC_MSG_REMOVE_SUCCESS	Die Operation zum Entfernen wurde erfolgreich ausgeführt.
1	FBC_MSG_MOUNT_FAIL	Die Bereitstellung ist fehlgeschlagen (Details enthalten die Bereitstellungsprotokolle).

Tabelle 18. Rückkehrcodes der Recovery Agent-CLI (Forts.)

Rückkehr-code	Wert	Beschreibung
2	FBC_MSG_MOUNT_DRIVER_ERROR	Beim Bereitstellungstreiber trat ein Fehler auf.
3	FBC_MSG_VOLUME_LETTER_BUSY	Der Datenträgerbuchstabe oder Analysepunkt wird verwendet.
4	FBC_MSG_MOUNT_WRONG_ PARA-METERS	Dem Befehl mount wurden falsche Parameter zugewiesen (Details enthalten die Bereitstellungsprotokolle).
5	FBC_MSG_MOUNT_ALREADY_ MOUNTED	Der Job wurde auf dem angeforderten Ziel bereits bereitgestellt.
6	FBC_MSG_MOUNT_WRONG_ PERMISSIONS	Die Berechtigungen sind unzureichend.
7	FBC_MSG_MOUNT_NETWORK_ DRIVE	Die Bereitstellung auf einem über das Netz zugeordneten Datenträger ist nicht möglich.
8	FBC_MSG_MOUNT_LOCKED_BY_ SERVER	Die Momentaufnahme wurde durch den Server gesperrt.
9	FBC_MSG_CAN_NOT_CHANGE_ REPOSITORY	Das Repository kann nicht geändert werden.
11	FBC_MSG_DISMOUNT_FAIL	Das Aufheben der Bereitstellung für eine bereitgestellte Momentaufnahme ist fehlgeschlagen.
13	FBC_MSG_VIEW_FAIL	Das Abrufen der Liste mit virtuellen Datenträgern ist fehlgeschlagen.
15	FBC_MSG_DUMP_FAIL	Die Listenerstellung durch den Speicherauszugsbefehl ist fehlgeschlagen.
16	FBC_MSG_CONNECTION_FAILED	Die Verbindung zur Bereitstellung von Data Protection for Microsoft Hyper-V wurde getrennt.
17	FBC_MSG_CONNECTION_TIMEOUT	Es trat eine Zeitlimitüberschreitung für die Operation auf.
18	FBC_MSG_MOUNT_FAILED_TO_ FIND_REPOSITORY	Es wurde kein gültiges Repository mit Momentaufnahmen gefunden.
19	FBC_MSG_MOUNT_JOB_NOT_ FOUND	Die angeforderte Momentaufnahme wurde nicht gefunden.
20	FBC_MSG_MOUNT_JOB_FOLDER_ NOT_FOUND	Die angeforderten Momentaufnahmedaten wurden nicht gefunden.
22	FBC_MSG_CAN_NOT_REMOVE_ REPOSITORY	Das ausgewählte Repository kann nicht entfernt werden.
23	FBC_MSG_REPOSITORY_GOT_ MOUNTS	Das Repository enthält bereitgestellte Momentaufnahmen.
38	FBC_MSG_MOUNT_NOT_WRITABLE_ VOLUME	Der Bereitstellungsdatenträger ist nicht beschreibbar.
39	FBC_MSG_NO_TSM_REPOSITORY	Es wurde kein IBM Spectrum Protect-Repository gefunden.

Tabelle 18. Rückkehrcodes der Recovery Agent-CLI (Forts.)

Rückkehr-code	Wert	Beschreibung
40	FBC_MSG_MOUNT_NOT_ALLOWED_ AS_READONLY	Die Bereitstellung des iSCSI-Ziels im Lesezugriff ist nicht zulässig.
41	FBC_MSG_RESOURCE_BUSY_IN_ TAPE_MODE	Data Protection for Microsoft Hyper-V wird im Bandmodus ausgeführt - der Datenträger ist ausgelastet.
42	FBC_MSG_DISK_TYPE_NOT_ SUPPORTED	Die Partitionierungsoperation wird bei diesem Plattentyp nicht unterstützt.
43	FBC_MSG_MOUNT_INITIALIZING	Die Operation ist fehlgeschlagen, die Bereitstellung von Data Protection for Microsoft Hyper-V wird gegenwärtig initialisiert. Wiederholen Sie die Aktion zu einem späteren Zeitpunkt.
44	FBC_MSG_CANNOT_LOCK_ SNAPSHOT	Die Momentaufnahme kann während dieser Operation nicht vor einem Verfall geschützt werden. Die Dokumentation enthält ausführliche Informationen.

Anhang A. Fehlerbehebung

Lösungen für Probleme mit Data Protection for Microsoft Hyper-V werden bereitgestellt.

Die folgenden Themen sind verfügbar:

- „Protokolldateien suchen"
- „Fehlerbehebung mit PowerShell-Cmdlets"
- „Sicherung der virtuellen Maschine schlägt fehl und der Fehler 0x800705B4 wird im Hyper-V-Ereignisprotokoll angezeigt"
- „Nicht unterstützte Zeichen in Namen von virtuellen Maschinen, Hyper-V-Hosts oder Clustern" auf Seite 236
- „In der Schnittstelle für Dateizurückschreibung wird eine falsche Laufwerkzuordnung und die vom System reservierte Platte angezeigt" auf Seite 236
- „Es kann keine SSL-Verbindung hergestellt werden" auf Seite 236
- „SSL-Zertifikat für den Agenten ist nicht gültig" auf Seite 237
- „VM-Sicherungs- oder -Zurückschreibungsoperation kann nicht gestartet werden, wenn eine andere VM-Operation in Bearbeitung ist" auf Seite 237

Protokolldateien suchen

Informationen zu den Data Protection for Microsoft Hyper-V-Protokolldateien enthalten die folgenden Themen:

- „Optionen für die Data Protection for Microsoft Hyper-V-Protokollaktivität" auf Seite 59
- „Traceoptionen für Data Protection for Microsoft Hyper-V" auf Seite 239

Fehlerbehebung mit PowerShell-Cmdlets

Für die Data Protection for Microsoft Hyper-V-Operationen können Sie eine Fehlerbehebung mithilfe von Powershell-Cmdlets ausführen. Weitere Informationen finden Sie in „Fehlerbehebung für Data Protection for Microsoft Hyper-V-Operationen" auf Seite 238.

Sicherung der virtuellen Maschine schlägt fehl und der Fehler `0x800705B4` wird im Hyper-V-Ereignisprotokoll angezeigt

Bei VM-Sicherungsoperationen unter Windows Server 2016 kann dieser Fehler auftreten, wenn Sie eine vollständige RCT-Sicherung (RCT - Resilient Change Tracking) einer virtuellen Maschine (VM) mit vielen VM-Platten ausführen. Entweder überschreitet die Momentaufnahmeoperation das Zeitlimit oder im Dateibereich auf dem Server ist nicht mehr genügend Speicherplatz verfügbar.

Suchen Sie im Hyper-V-Ereignisprotokoll nach dem Fehler `0x800705B4`, wenn die VM-Sicherungsoperation fehlschlägt. Ist dieser Fehler vorhanden, führen Sie die folgenden Schritte aus, um die Leistung der Momentaufnahmeoperation zu verbessern:

1. Stellen Sie sicher, dass die Hyper-V-VM eine VM der zweiten Generation ist.
2. Stellen Sie sicher, dass nur SCSI-Platten an die VM der zweiten Generation angeschlossen sind (anstelle einer Kombination aus SCSI- und IDE-Platten).

3. Versetzen Sie den Hyper-V-Momentaufnahmeordner von seiner Standardposition (`C:\ProgramData\Microsoft\Windows\Hyper-V\Snapshots`) auf ein schnelleres Laufwerk, das nicht das Windows-Systemlaufwerk ist (z. B. das Laufwerk `D:`).

Nicht unterstützte Zeichen in Namen von virtuellen Maschinen, Hyper-V-Hosts oder Clustern

In Data Protection for Microsoft Hyper-V wird die Sicherung von virtuellen Maschinen und Hyper-V-Hosts oder Clustern nicht unterstützt, deren Name eines der folgenden Zeichen enthält:

`"`	Anführungszeichen
`'`	Hochkomma
`:`	Doppelpunkt
`;`	Semikolon
`*`	Stern
`?`	Fragezeichen
`,`	Komma
`<`	Kleiner-als-Zeichen
`>`	Größer-als-Zeichen
`/`	Schrägstrich
`\`	Umgekehrter Schrägstrich
`|`	Vertikaler Balken

In der Schnittstelle für Dateizurückschreibung wird eine falsche Laufwerkzuordnung und die vom System reservierte Platte angezeigt

Stellen Sie sicher, dass die Windows-Funktion für automatische Bereitstellung (Automount) nicht aktiviert ist.

Standardmäßig inaktiviert das Data Protection for Microsoft Hyper-V-Installationsprogramm die Funktion Automount mit dem Befehl **`diskpart`** automatisch. Diese Aktion ist erforderlich, damit in der IBM Spectrum Protect-Schnittstelle für Dateizurückschreibung die korrekten Laufwerkzuordnungen angezeigt und die vom System reservierte Platte ausgeblendet wird.

Die Funktion Automount wurde höchstwahrscheinlich nach der Installation von Data Protection for Microsoft Hyper-V aktiviert. Verwenden Sie den Befehl **`diskpart`**, um die Funktion Automount zu inaktivieren.

Es kann keine SSL-Verbindung hergestellt werden

Die folgende Nachricht kann in der Data Protection for Microsoft Hyper-V-Verwaltungskonsole angezeigt werden, wenn das SSL-Zertifikat auf irgendeine Weise ungültig ist, z. B. wenn Sie Data Protection for Microsoft Hyper-V erneut installiert haben und das alte SSL-Zertifikat nicht gelöscht wurde.

```
GVM6065E Die SSL-Verbindung konnte nicht hergestellt werden. Das IBM
Spectrum Protect-SSL-Zertifikat fehlt. Überprüfen Sie 'TSM-ve-trustore.jks'
auf ein gültiges IBM Spectrum Protect-Zertifikat RC=215
```

Löschen Sie alle Dateien im Ordner `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\truststores`. Starten Sie anschließend die Data Protection for Microsoft Hyper-V-Verwaltungskonsole erneut und führen Sie den Konfigurationsassistenten aus. Akzeptieren Sie bei der entsprechenden Aufforderung das Sicherheitszertifikat.

SSL-Zertifikat für den Agenten ist nicht gültig

Möglicherweise empfangen Sie einen SSL-Verbindungsfehler, wenn das Sicherheitszertifikat für den fernen Clientagenten nicht gültig oder nicht aktuell ist.

Wurden beispielsweise die Zertifikatsdateien (`dsmcert.sth`, `dsmcert.idx` und `dsmcert.kdb`) im Verzeichnis `C:\Programme\Tivoli\TSM\baclient` gelöscht oder beschädigt, wird die folgende Nachricht im Fehlerprotokoll der Einheit zum Versetzen von Daten (`dsmerror.`*`Hostname`*`_HV_DM.log`) angezeigt:

```
ANS1592E SSL-Protokoll konnte nicht initialisiert werden.
```

Die Methode, die Sie für die Behebung dieses Problems verwenden, ist von der Version des IBM Spectrum Protect-Servers abhängig, zu dem Sie eine Verbindung herstellen:

- Wenn Sie eine Verbindung zu einem IBM Spectrum Protect-Server mit Version 8.1.2 oder höher bzw. mit Version 7.1.8 oder einer höheren Stufe der Version 7 herstellen, führen Sie einen der folgenden Schritte aus:
  - Stoppen Sie den Clientakzeptorservice auf dem Knoten der Einheit zum Versetzen von Daten und dem Mount-Proxy-Knoten (falls die Dateizurückschreibung aktiviert ist) und führen Sie den Data Protection for Microsoft Hyper-V-Konfigurationsassistenten auf dem eigenständigen Host oder auf einem beliebigen Host in einem Cluster erneut aus.

    Weitere Informationen finden Sie in „Data Protection for Microsoft Hyper-V mit dem Assistenten konfigurieren” auf Seite 45.
  - Aktualisieren Sie die Knotendefinition auf dem IBM Spectrum Protect-Server, indem Sie den Parameter SESSIONSECURITY=TRANSITIONAL angeben. Das Sicherheitszertifikat wird erneut erstellt, wenn Sie sich von der Data Protection for Microsoft Hyper-V-Verwaltungskonsole aus beim IBM Spectrum Protect-Server anmelden.

    Weitere Informationen finden Sie in UPDATE NODE.
- Wenn Sie eine Verbindung zu einem IBM Spectrum Protect-Server mit Version 8.1.1 oder einer früheren Stufe der Version 8 bzw. zu einem Server mit Version 7.1.7 oder früher herstellen, finden Sie in Dsmcutil-Befehle: Erforderliche Optionen und Beispiele weitere Informationen.

VM-Sicherungs- oder -Zurückschreibungsoperation kann nicht gestartet werden, wenn eine andere VM-Operation in Bearbeitung ist

Die folgende Nachricht wird angezeigt, wenn eine Sicherungs- oder Zurückschreibungsoperation gestartet wird, wenn eine andere VM-Operation in Bearbeitung ist:

```
ANS5176W Die angeforderte VM-Operation kann nicht ausgeführt werden, da
bereits eine Sicherungs- oder Zurückschreibungsoperation für eine virtuelle
Maschine ausgeführt wird. Wiederholen Sie die Operation, nachdem die erste
Operation beendet wurde.
```

Diese Nachricht wird in den folgenden Situationen angezeigt:

- Sie haben eine Sicherungs- oder Zurückschreibungsoperation für eine VM gestartet und auf demselben Host ist bereits eine andere Sicherungs- oder Zurückschreibungsoperation in Bearbeitung.
- Sie haben eine Sicherungs- oder Zurückschreibungsoperation für eine VM gestartet und auf demselben Host ist eine andere geplante Sicherung einer beliebigen VM aktiv. Möglicherweise hat auch ein anderer Benutzer die Operation von einer anderen Position aus gestartet.

Wenn diese Nachricht angezeigt wird, warten Sie, bis die aktive Operation beendet ist. Starten Sie anschließend Ihre Sicherungs- oder Zurückschreibungsoperation erneut.

Zugehörige Verweise:

„Fehlerbehebung für Anwendungsschutz von virtuellen Gastmaschinen" auf Seite 145

Fehlerbehebung für Data Protection for Microsoft Hyper-V-Operationen

Sie können Diagnoseinformationen abrufen, um Probleme bei Data Protection for Microsoft Hyper-V zu beheben, indem Sie Microsoft Windows PowerShell-Cmdlet-Befehle ausführen.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie Ihre Umgebung für die Verwendung von Powershell-Cmdlets vorbereiten. Weitere Informationen finden Sie in „Verwendung von PowerShell-Cmdlets mit Data Protection for Microsoft Hyper-V vorbereiten" auf Seite 151.

Vorgehensweise

Führen Sie die folgenden Schritte auf dem System aus, auf dem Data Protection for Microsoft Hyper-V installiert ist.

1. Zeigen Sie Protokolldateiinformationen in einem Powershell-Viewer an, indem Sie den folgenden Befehl ausgeben:

   ```
   PS C:\> Show-DpHvApiLogEntries
   ```

   Mit einer der folgenden Aktionen können Sie Protokollinformationen im Powershell-Viewer untersuchen und gemeinsam nutzen:
   - Geben Sie einen Begriff ein, um die Ergebnisse zu filtern.
   - Klicken Sie auf das Feld zum Hinzufügen von Kriterien, um die Informationen mit detaillierteren Angaben zu filtern.
   - Klicken Sie auf mindestens eine Zeile, um ihren Inhalt zu speichern oder für die gemeinsame Nutzung zu kopieren.
2. Zeigen Sie die Traceinformationen aus einer Tracedatei an, indem Sie den folgenden Befehl ausgeben:

   ```
   PS C:\> Show-DpHvApiTraceEntries
   ```
3. Wenn Sie Protokolle zusammenstellen müssen, um detaillierte Diagnoseinformationen zu überprüfen oder sie an den IBM Support zu senden, speichern Sie die Protokolle in einer komprimierten Datei, indem Sie den folgenden Befehl ausgeben:

   ```
   PS C:\> Get-DpHvProblemDeterminationInfo -review
   ```

Standardmäßig wird mit diesem Befehl die Datei `DpHvProblemDetermination.zip` auf dem Desktop gespeichert.

Tipp: Wenn dieser Befehl in der Standardschnittstelle "PowerShell" einen Fehler zurückgibt, starten Sie die Schnittstelle "PowerShell ISE" als Administrator. Anschließend führen Sie den Befehl erneut aus.

4. Optional: Für jedes Data Protection for Microsoft Hyper-V-Cmdlet gibt es Parameter. Geben Sie zum Anzeigen der Parameter den folgenden Befehl **help** aus:

   ```
   help Cmdlet-Name -ShowWindow
   ```

Zugehörige Verweise:

„Optionen für die Data Protection for Microsoft Hyper-V-Protokollaktivität" auf Seite 59

„Traceoptionen für Data Protection for Microsoft Hyper-V"

Traceoptionen für Data Protection for Microsoft Hyper-V

Das Definieren von Tracing-Optionen in der Datei `FRLog.config` unterstützt Sie beim Beheben von Fehlern, die bei Data Protection for Microsoft Hyper-V- und Dateizurückschreibungsoperationen auftreten können.

Ändern Sie die Optionen in der Datei `FRLog.config` mit einem Texteditor im Administratormodus. Die Datei `FRLog.config` befindet sich im folgenden Verzeichnis:

```
C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI
```

FR.API.TRACE=ON | OFF
Geben Sie an, ob die API-Aktivität mit der empfohlenen Detaillierungsebene verfolgt werden soll.

Anmerkung: Die folgenden Werte werden ebenfalls unterstützt und geben die minimale, empfohlene und höchste Detaillierungsebene an: DEBUG, TRACE, ALL.

API_MAX_TRACE_FILES=*Anzahl*
Geben Sie die maximale Anzahl an Tracedateien an, die erstellt oder verwendet werden sollen. Der Standardwert ist 8.

API_MAX_TRACE_FILE_SIZE=*Anzahl*
Geben Sie die maximale Größe jeder Tracedatei in KB an. Der Standardwert ist 8192 KB.

API_TRACE_FILE_NAME=*Name_der_API-Tracedatei*
Geben Sie den Namen der API-Tracedatei an. Der Standardwert ist `fr_api-.trace`.

API_TRACE_FILE_LOCATION=*Position_der_API-Tracedatei*
Geben Sie die Position der API-Tracedatei an. Geben Sie die Position mit einem Schrägstrich (/) an. Die Standardposition ist *Installationsverzeichnis*`/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs`.

Anhang B. Data Protection for Microsoft Hyper-V-Nachrichten

Für die von Data Protection for Microsoft Hyper-V ausgegebenen Nachrichten werden Erläuterungen und vorgeschlagene Aktionen bereitgestellt.

Nachrichten, die mit dem Präfix GVM beginnen, sind in aufsteigender numerischer Reihenfolge aufgeführt. Für einige Nachrichten sind die Erläuterung und die Benutzeraktion in der Nachricht selbst enthalten.

Einige Nachrichten, die mit dem Präfix GVM beginnen, werden auch mit IBM Spectrum Protect for Virtual Environments: Data Protection for VMware gemeinsam genutzt.

Nachrichten, die mit dem Präfix ANS beginnen, finden Sie in ANS-Nachrichten 0000-9999.

GVM5900E Die Operation ist mit dem Rückkehrcode *Rückkehrcode* fehlgeschlagen.

GVM5901E Ein interner Fehler ist aufgetreten: *Fehlertyp*

GVM5902E Es konnte keine Verbindung zum IBM Spectrum Protect-Server hergestellt werden.

Erläuterung: Der Server ist möglicherweise nicht aktiv.

Benutzeraktion: Überprüfen Sie die Netzverbindung mit der Servermaschine. Stellen Sie sicher, dass der Server aktiv ist, und melden Sie sich erneut an.

GVM5903W Sollen diese Daten wirklich gelöscht werden?

Erläuterung: Sie können die Daten nach dem Löschen nicht wiederherstellen. Stellen Sie vor dem Löschen der Daten sicher, dass sie nicht benötigt werden.

Benutzeraktion: Klicken Sie auf 'OK', um die Daten zu löschen, oder klicken Sie auf 'Abbrechen', um diese Aktion abzubrechen.

GVM5904W Die Verbindung zum IBM Spectrum Protect-Server hat das zulässige Zeitlimit überschritten.

Erläuterung: Mögliche Ursachen sind Operationen mit langer Laufzeit, ein Problem auf dem Server oder ein Kommunikationsfehler.

Benutzeraktion: Handelt es sich um eine Operation mit langer Laufzeit, ist die Operation möglicherweise beendet oder bald beendet. Bevor Sie die Operation wiederholen, stellen Sie fest, ob das erwartete Ergebnis eingetreten ist. Überprüfen Sie das Aktivitätenprotokoll des IBM Spectrum Protect-Servers auf Fehler, die sich auf die Operation beziehen. Die Verwendung eines SSL-Ports ohne Auswahl von SSL kann diesen Fehler verursachen.

GVM5905W Die virtuelle Maschine *VM-Name* ist vorhanden. Soll sie überschrieben werden?

GVM5906W Die virtuelle Maschine *VM-Name* ist aktiv. Stellen Sie sicher, dass das System ausgeschaltet ist. Klicken Sie dann auf 'OK', um fortzufahren.

GVM5907I Eine Serververbindung mit dem Namen *Servername* wurde erfolgreich erstellt. Klicken Sie auf 'OK', um fortzufahren.

GVM5908W Es wurde keine IBM Spectrum Protect-Serverdefinition gefunden.

Erläuterung: Für einen IBM Spectrum Protect-Server muss eine Verbindung definiert werden, bevor Serveroperationen oder -abfragen ausgeführt werden.

Benutzeraktion: Führen Sie folgende Schritte aus, um einen Server zu definieren:

1. Klicken Sie auf die Registerkarte 'Konfiguration'.
2. Klicken Sie auf den Aktionslink 'Konfigurationseinstellungen editieren'.
3. Klicken Sie auf die Registerkarte 'IBM Spectrum Protect-Serverberechtigungsnachweise'.

GVM5909I Die virtuelle Maschine *VM-Name* erstreckt sich über mehrere Datenspeicher. Sie kann nur an ihre ursprüngliche Position zurückgeschrieben werden.

GVM5910E Beim Schreiben in die Serverdatenbankdatei 'tsmserver.props' ist ein Fehler aufgetreten.

Erläuterung: Die Serverdefinition konnte nicht in die Datei 'tsmserver.props' geschrieben werden.

Benutzeraktion: Die Datei muss sich im Installationsverzeichnis von Data Protection for Virtual Environments befinden. Bevor Sie die Aktion wiederholen, stellen Sie sicher, dass die Datei vorhanden und nicht schreibgeschützt ist.

GVM5911E Es konnte keine Verbindung zum vCenter-Server hergestellt werden.

Erläuterung: Der Server ist möglicherweise nicht aktiv.

Benutzeraktion: Dies kann auf ein Netzproblem hindeuten. Stellen Sie sicher, dass der Server aktiv ist und auf die Maschine zugegriffen werden kann. Wiederholen Sie die Aktion.

GVM5912I Die Verbindung zum vCenter-Server wurde hergestellt.

GVM5913E Der VMCLI-Konfigurationsbefehl 'inquire' ist fehlgeschlagen. Die folgenden Nachrichten beschreiben den Fehler.

Erläuterung: Die Derby-Datenbank ist möglicherweise nicht aktiv.

Benutzeraktion: Korrigieren Sie den Fehler. Wiederholen Sie die Aktion.

GVM5914I Der VMCLI-Konfigurationsbefehl 'inquire' wurde erfolgreich ausgeführt.

GVM5915E Es konnte nicht festgestellt werden, welche Produkte installiert sind.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Korrigieren Sie den Fehler. Wiederholen Sie die Aktion.

GVM5916I Es wurde erfolgreich festgestellt, welche Produkte installiert sind.

GVM5917E Mehrere Zurückschreibungspunkte wurden ausgewählt, aber sie befinden sich nicht im selben Datencenter.

Erläuterung: Die Auswahl von Zurückschreibungspunkten aus verschiedenen Datencentern ist nicht zulässig. Alle Zurückschreibungspunkte müssen sich im selben Datencenter befinden.

Benutzeraktion: Wählen Sie die Zurückschreibungspunkte aus demselben Datencenter aus oder wählen Sie nur einen einzigen Zurückschreibungspunkt aus.

GVM5918E Mehrere Zurückschreibungspunkte wurden ausgewählt, aber sie stammen nicht aus derselben Sicherung.

Erläuterung: Die Auswahl von Zurückschreibungspunkten aus verschiedenen Sicherungen ist nicht zulässig. Alle Zurückschreibungspunkte müssen sich in derselben Sicherung befinden.

Benutzeraktion: Für Zurückschreibungen aus IBM Spectrum Snapshot müssen alle Zurückschreibungspunkte aus derselben Sicherung stammen. Sie können nicht mehrere virtuelle Maschinen zurückschreiben, die aus verschiedenen Sicherungen stammen.

GVM5919E Eine zentrale Konfigurationsdatei fehlt: vmcliConfiguration.xml.

Erläuterung: Die Datei vmcliConfiguration.xml ist für den Betrieb der GUI erforderlich; sie wurde jedoch beim Start der GUI-Sitzung nicht gefunden. Dieser ungewöhnliche Fehler kann durch ein Installationsproblem oder durch das manuelle Editieren der Datei verursacht werden.

Benutzeraktion: Stellen Sie sicher, dass die Datei sich im korrekten Verzeichnis befindet, über die korrekten Zugriffsberechtigungen verfügt und eine gültige Syntax für ihren Inhalt aufweist. Wiederholen Sie den Zugriff auf die GUI.

GVM5920E Ungültiger Tag mode in Datei vmcliConfiguration.xml.

Erläuterung: Der XML-Tag mode in der Datei vmcliConfiguration.xml ist für den Betrieb der GUI erforderlich; er fehlt jedoch oder hat einen falschen Wert. Dieser Fehler kann durch ein Installationsproblem oder durch das manuelle Editieren der Datei verursacht werden.

Benutzeraktion: Stellen Sie sicher, dass der Tag mit einem gültigen Wert angegeben wird. Wiederholen Sie den Zugriff auf die GUI.

GVM5921E Ungültiger Tag enable_direct_start in Datei vmcliConfiguration.xml.

Erläuterung: Der XML-Tag enable_direct_start in der Datei vmcliConfiguration.xml ist für den Betrieb der GUI erforderlich; er fehlt jedoch oder hat einen falschen Wert. Dieser Fehler kann durch ein Installationsproblem oder durch das manuelle Editieren der Datei verursacht werden.

Benutzeraktion: Stellen Sie sicher, dass der Tag mit einem gültigen Wert angegeben wird. Wiederholen Sie den Zugriff auf die GUI.

GVM5922E Ungültiger URL-Tag für den angegebenen Tag mode in der Datei vmcliConfiguration.xml.

Erläuterung: In der Datei vmcliConfiguration.xml ist der URL-Tag, der dem angegebenen Tag mode entspricht, für den Betrieb der GUI erforderlich; er fehlt jedoch oder hat einen falschen Wert. Dieser Fehler kann durch ein Installationsproblem oder durch das manuelle Editieren der Datei verursacht werden.

Benutzeraktion: Stellen Sie sicher, dass der korrekte URL-Tag mit einem gültigen Wert für den angegebenen Modus angegeben wird. Wiederholen Sie den Zugriff auf die GUI.

GVM5923E Ungültiger Tag VMCLIPath in Datei vmcliConfiguration.xml.

Erläuterung: Der XML-Tag VMCLIPath in der Datei vmcliConfiguration.xml ist für den Betrieb der GUI erforderlich; er fehlt jedoch oder hat einen falschen Wert. Dieser Fehler kann durch ein Installationsproblem oder durch das manuelle Editieren der Datei verursacht werden.

Benutzeraktion: Stellen Sie sicher, dass der Tag mit einem gültigen Wert angegeben wird. Wiederholen Sie den Zugriff auf die GUI.

GVM5924E Ungültiger Tag interruptDelay in Datei vmcliConfiguration.xml.

Erläuterung: Der XML-Tag interruptDelay in der Datei vmcliConfiguration.xml ist für den Betrieb der GUI erforderlich; er fehlt jedoch oder hat einen falschen Wert. Dieser Fehler kann durch ein Installationsproblem oder durch das manuelle Editieren der Datei verursacht werden.

Benutzeraktion: Stellen Sie sicher, dass der Tag mit einem gültigen Wert angegeben wird. Wiederholen Sie den Zugriff auf die GUI.

GVM5925E Der eingegebene VM-Name *VM-Name* **steht in Konflikt mit einer vorhandenen virtuellen Maschine. Geben Sie einen anderen Namen ein.**

GVM5926E Beim Verarbeiten der Anforderung an den Web-Server ist ein Fehler aufgetreten. Bleibt dieser Fehler bestehen, überprüfen Sie die Netzverbindung zum Web-Server und stellen Sie sicher, dass der Web-Server aktiv ist.
Detail: *Ausnahme*
Ausnahmebedingungsnachricht

GVM5927E Die Ausführung einer Anforderung für den Server hat zu lange gedauert. Bleibt dieser Fehler bestehen, überprüfen Sie die Netzverbindung zum Web-Server und stellen Sie sicher, dass der Web-Server aktiv ist.

GVM5928E Beim Verarbeiten der Antwort vom Web-Server ist ein Fehler aufgetreten.
Detail: *Fehler*

GVM5929E Beim Erstellen der Web-Server-Anforderung ist ein Fehler aufgetreten. Bleibt dieser Fehler bestehen, überprüfen Sie die Netzverbindung zum Web-Server und stellen Sie sicher, dass der Web-Server aktiv ist.
Fehler: *Nachricht*

GVM5930E Keine übereinstimmende Einheitenklasse gefunden. Kehren Sie zur Quellenseite zurück und treffen Sie erneut eine Auswahl.

GVM5931E Kein übereinstimmender Proxy-Knoten gefunden. Kehren Sie zur Quellenseite zurück und treffen Sie erneut eine Auswahl.

GVM5932E Es sind keine ESX-Proxy-Hosts verfügbar.

GVM5933I Kennwort wurde erfolgreich definiert.

GVM5934E Die Festlegung des Kennworts ist fehlgeschlagen.
Fehler: *Nachricht*

Erläuterung: Das Kennwort ist möglicherweise nicht korrekt oder der Server ist nicht aktiv.

Benutzeraktion: Stellen Sie sicher, dass das Kennwort korrekt ist, und wiederholen Sie dann die Aktion. Oder überprüfen Sie die Netzverbindung zur Servermaschine und stellen Sie sicher, dass der Server aktiv ist, und wiederholen Sie dann die Aktion.

GVM5935E Das Abrufen der verwalteten Domäne ist fehlgeschlagen.
Fehler: *Nachricht*

GVM5936E Mehrere Zurückschreibungspunkte wurden ausgewählt, aber sie haben nicht denselben Sicherungstyp.

Erläuterung: Die Auswahl von Zurückschreibungspunkten verschiedener Typen ist nicht zulässig. Alle

Zurückschreibungspunkte müssen sich entweder auf einem IBM Spectrum Protect-Server oder in dem IBM Spectrum Snapshot-Repository befinden.

Benutzeraktion: Wählen Sie denselben Typ von Zurückschreibungspunkten aus oder wählen Sie nur einen einzelnen Zurückschreibungspunkt aus.

GVM5937E Sicherungs-ID ist Null.

Erläuterung: Ein interner Fehler ist aufgetreten.

Benutzeraktion: Aktualisieren Sie die Tabelle und führen Sie die Aktion erneut aus.

GVM5938E Task-ID ist Null.

Erläuterung: Ein interner Fehler ist aufgetreten.

Benutzeraktion: Aktualisieren Sie die Tabelle und führen Sie die Aktion erneut aus.

GVM5939E Ein Popup-Fenster konnte nicht geöffnet werden.

Erläuterung: Ein interner Fehler ist aufgetreten.

Benutzeraktion: Wiederholen Sie die Aktion.

GVM5940E Name der virtuellen Maschine ist Null.

Erläuterung: Ein interner Fehler ist aufgetreten.

Benutzeraktion: Aktualisieren Sie die Tabelle und führen Sie die Aktion erneut aus.

GVM5941E Datenspeicher ist nicht vorhanden.

Erläuterung: Ein interner Fehler ist aufgetreten.

Benutzeraktion: Aktualisieren Sie die Tabelle und führen Sie die Aktion erneut aus.

GVM5942I Es wurde keine Auswahl getroffen. Die gesamte virtuelle Maschine wird zugeordnet.

Erläuterung: Es wurde keine Auswahl getroffen.

Benutzeraktion: Fahren Sie mit der Aktion fort oder brechen Sie die Aktion ab.

GVM5943I Domäne wurde erfolgreich definiert.

GVM5944E Die Festlegung der Domäne ist fehlgeschlagen.
Fehler: *Nachricht*

Erläuterung: Der Server ist möglicherweise nicht aktiv.

Die Berechtigungen für das Dateiverzeichnis sind möglicherweise nicht korrekt.

Benutzeraktion: Überprüfen Sie die Netzverbindung mit der Servermaschine. Stellen Sie sicher, dass der Server aktiv ist, und wiederholen Sie dann die Aktion.

Überprüfen Sie die Berechtigungen des Verzeichnisses, das in SystemErr.log angegeben ist.

GVM5945E Der Zeitplan erfordert die Verwendung der folgenden Datencenter, die sich nicht in der aktiven Domäne befinden.
Datencenter: *Liste*
Aktion: Dieser Zeitplan kann nicht aktualisiert werden. Aktualisieren Sie stattdessen das Domänenkonstrukt, um die Datencenter einzuschließen, oder erstellen Sie einen neuen Zeitplan ohne Abhängigkeit von diesen Datencentern.
Detail: Die Zeitplandefinition lautet wie folgt:
Zeitplanzusammenfassung: *Zusammenfassung*

GVM5946E Der Zeitplan erfordert die Verwendung der folgenden Datencenter, die dem System nicht bekannt sind.
Datencenter: *Liste*
Aktion: Dieser Zeitplan kann nicht aktualisiert werden. Erstellen Sie stattdessen einen neuen Zeitplan ohne Abhängigkeit von diesen Datencentern.
Detail: Die Zeitplandefinition lautet wie folgt:
Zeitplanzusammenfassung: *Zusammenfassung*

GVM5947E Der Zeitplan erfordert die Verwendung der folgenden Hosts, die dem System nicht bekannt sind.
Hosts: *Liste*
Aktion: Dieser Zeitplan kann nicht aktualisiert werden. Erstellen Sie stattdessen einen neuen Zeitplan ohne Abhängigkeit von diesen Hosts.
Detail: Die Zeitplandefinition lautet wie folgt:
Zeitplanzusammenfassung: *Zusammenfassung*

GVM5948E Der Zeitplan erfordert die Verwendung der folgenden Datenspeicher, die dem System nicht bekannt sind.
Datenspeicher: *Liste*
Aktion: Dieser Zeitplan kann nicht aktualisiert werden. Erstellen Sie stattdessen einen neuen Zeitplan ohne Abhängigkeit von diesen Datenspeichern.
Detail: Die Zeitplandefinition lautet wie folgt:
Zeitplanzusammenfassung: *Zusammenfassung*

GVM5949E **Der Zeitplan erfordert die Verwendung der folgenden virtuellen Maschinen, die dem System nicht bekannt sind.**
Virtuelle Maschinen: *Liste*
Aktion: Dieser Zeitplan kann nicht aktualisiert werden. Erstellen Sie stattdessen einen neuen Zeitplan ohne Abhängigkeit von diesen virtuellen Maschinen.
Detail: Die Zeitplandefinition lautet wie folgt:
Zeitplanzusammenfassung: *Zusammenfassung*

GVM5950I **Kennwort wurde erfolgreich definiert.**
Warnung: *Nachricht*

Erläuterung: Das Kennwort wurde erfolgreich mit einer Warnung definiert.

Benutzeraktion: Führen Sie die in der Warnung beschriebene Aktion aus.

GVM5951E **Beim Erstellen der Web-Server-Anforderung ist ein Fehler aufgetreten. Bleibt dieser Fehler bestehen, überprüfen Sie die Netzverbindung zum Web-Server und stellen Sie sicher, dass der Web-Server aktiv ist.**
Fehler: *Fehler*

GVM5952E **Der folgende Befehl erfordert die Bestätigung vom Server: ""***Befehl***""**

Erläuterung: Ein Befehl wurde ausgegeben und eine Antwort wurde erwartet. Einige Befehle erfordern eine Bestätigung, die nicht über die Data Protection for Virtual Environments-GUI ausgegeben werden kann.

Benutzeraktion: Geben Sie den Befehl in der Befehlszeile aus.

GVM5953E **Der folgende Befehl ist dem Server nicht bekannt: ""***Befehl***""**

Erläuterung: Ein unbekannter Befehl wurde an den Server ausgegeben. Der Befehl ist möglicherweise für die Serverversion und -plattform nicht gültig oder die Befehlssyntax ist möglicherweise falsch.

Benutzeraktion: Stellen Sie sicher, dass der Befehl für die Serverversion und -plattform gültig ist und die Befehlssyntax korrekt ist.

GVM5954E **Die Syntax des folgenden Befehls ist falsch: ""***Befehl***"".**

Erläuterung: Siehe Nachricht.

Benutzeraktion: Korrigieren Sie die Syntax und geben Sie den Befehl in der Befehlszeile aus. Das Aktivitätenprotokoll des IBM Spectrum Protect-Servers zeigt alle Befehle, die vor und nach diesem Befehl ausgegeben wurden.

GVM5955E **Ein interner Serverfehler ist aufgetreten.**

Erläuterung: Siehe Nachricht.

Benutzeraktion: Wiederholen Sie den Befehl. Bleibt der Fehler bestehen, verständigen Sie die Kundenunterstützung. Sie werden möglicherweise aufgefordert, Traceinformationen und Informationen zu den Aktionen bereitzustellen, die vor dem Auftreten des Fehlers ausgeführt wurden.

GVM5956E **Während der Verarbeitung der Anforderung verfügte der Server über keinen Speicher mehr. Schließen Sie alle nicht erforderlichen Prozesse auf dem IBM Spectrum Protect-Server und wiederholen Sie die Operation.**

Erläuterung: Siehe Nachricht.

Benutzeraktion: Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5957E **Das Datenbankwiederherstellungsprotokoll ist voll.**

Erläuterung: Siehe Nachricht.

Benutzeraktion: Bevor Sie die Aktion wiederholen, erweitern Sie das Wiederherstellungsprotokoll oder sichern Sie die IBM Spectrum Protect-Serverdatenbank. Ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5958E **Die Serverdatenbank ist voll.**

Erläuterung: Siehe Nachricht.

Benutzeraktion: Bevor Sie die Aktion wiederholen, erweitern Sie die Serverdatenbank. Ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5959E **Der Server verfügt über keinen Speicherbereich mehr.**

Erläuterung: Siehe Nachricht.

Benutzeraktion: Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5960E **Sie sind nicht berechtigt, diese Aktion auszuführen. Ein Administrator mit Systemberechtigung kann Ihre Berechtigungsstufe ändern, um die Ausführung dieser Aktion zu ermöglichen.**

GVM5961E Das Objekt, auf das zugegriffen werden soll, ist auf dem Server nicht vorhanden.

GVM5962E Das Objekt, auf das zugegriffen werden soll, wird gegenwärtig von einer anderen Sitzung oder einem anderen Prozess verwendet. Wiederholen Sie die Aktion zu einem späteren Zeitpunkt.

GVM5963E Auf das Objekt, das entfernt werden soll, wird von einem anderen Objekt verwiesen, das für den Server definiert ist. Entfernen Sie das andere Objekt, bevor Sie dieses Objekt entfernen.

GVM5964E Das Objekt, auf das zugegriffen oder das entfernt werden soll, ist nicht verfügbar.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5965E Während der Verarbeitung der Anforderung hat der Server einen E/A-Fehler entdeckt. Weitere Informationen enthält das Ereignis- oder Fehlerprotokoll des Betriebssystems.

GVM5966E Die Aktion ist fehlgeschlagen, da die Transaktion nicht festgeschrieben werden konnte.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Wiederholen Sie die Aktion zu einem späteren Zeitpunkt. Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5967E Die Aktion ist aufgrund eines Ressourcensperrenkonflikts fehlgeschlagen.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Wiederholen Sie die Aktion zu einem späteren Zeitpunkt. Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5968E Die Aktion ist aufgrund eines Moduskonflikts fehlgeschlagen.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Wiederholen Sie die Aktion zu einem späteren Zeitpunkt. Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5969E Die Aktion ist fehlgeschlagen, da der Server keinen neuen Thread starten konnte.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Wiederholen Sie die Aktion zu einem späteren Zeitpunkt. Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5970E Der Server ist für die Ausführung dieser Aktion nicht lizenziert. Wurde eine Lizenz gekauft, verwenden Sie die Befehlszeile, um die Lizenz zu registrieren.

GVM5971E Das angegebene Ziel ist nicht gültig.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Geben Sie ein anderes Ziel ein oder aktualisieren Sie die Konfiguration mit einem gültigen Ziel und wiederholen Sie die Aktion.

GVM5972E Die angegebene Eingabedatei kann nicht geöffnet werden. Überprüfen Sie den Dateinamen und die Verzeichnisberechtigungen und wiederholen Sie die Aktion.

GVM5973E Die angegebene Ausgabedatei kann nicht geöffnet werden. Überprüfen Sie den Dateinamen und die Verzeichnisberechtigungen und wiederholen Sie die Aktion.

GVM5974E Beim Schreiben in die angegebene Ausgabedatei ist ein Fehler aufgetreten.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Überprüfen Sie das Dateisystem, um sicherzustellen, dass genügend Speicherbereich vorhanden ist. Überprüfen Sie das Ereignis- oder Fehlerprotokoll des Betriebssystems auf weitere Informationen.

GVM5975E Der angegebene Administrator ist für diesen Server nicht definiert.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Stellen Sie sicher, dass der Administratorname korrekt eingegeben wurde. Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5976E Die SQL-Anweisung konnte nicht verarbeitet werden.

Erläuterung: Während der Verarbeitung der SQL-Anweisung ist eine Ausnahmebedingung aufgetreten. Mögliche Ausnahmebedingungen sind Division durch Null, mathematischer Überlauf, temporärer Tabellenspeicherbereich nicht verfügbar und Datentypfehler.

Benutzeraktion: Korrigieren Sie die SQL-Abfrage und wiederholen Sie die Aktion.

GVM5977E Diese Operation ist mit diesem Objekt nicht zulässig.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5978E Die Tabelle wurde in der Serverdatenbank nicht gefunden.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5979E Der angegebene Dateibereichsname ist mit dem Dateibereichstyp nicht kompatibel.

Erläuterung: Unicode-Dateibereichsnamen sind mit Nicht-Unicode-Namen nicht kompatibel.

Benutzeraktion: Geben Sie einen Dateibereichsnamen mit dem korrekten Typ ein und wiederholen Sie die Aktion.

GVM5980E Die angegebene TCP/IP-Adresse ist nicht gültig. Überprüfen Sie die TCP/IP-Adresse und wiederholen Sie dann die Aktion.

GVM5981E Es wurden keine Objekte gefunden, die den Suchbedingungen entsprechen.

GVM5982E Ihre Verwaltungs-ID auf diesem Server ist gesperrt. Ein Administrator mit Systemberechtigung kann Ihre ID entsperren.

GVM5983E Während der Ausführung der Aktion ist die Verbindung zum Server verloren gegangen.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Dies kann auf ein Netzproblem hindeuten. Stellen Sie sicher, dass der Server aktiv ist und auf die Maschine zugegriffen werden kann. Wiederholen Sie die Aktion.

GVM5984E Ihre ID oder Ihr Kennwort ist für diesen Server nicht gültig.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Geben Sie eine gültige ID oder ein gültiges Kennwort für Ihren IBM Spectrum Protect-Server ein.

GVM5985E Ihr Kennwort ist auf diesem Server abgelaufen.

Erläuterung: Ihr IBM Spectrum Protect-Kennwort ist abgelaufen.

Benutzeraktion: Setzen Sie Ihr Kennwort auf dem IBM Spectrum Protect-Server zurück oder bitten Sie den Administrator Ihres IBM Spectrum Protect-Servers, das Kennwort zurückzusetzen.

GVM5986E Der Server kann keine neuen Sitzungen akzeptieren. Sind Sitzungen für diesen Server inaktiviert, geben Sie den Befehl ENABLE SESSIONS in der Befehlszeile aus.

GVM5987E Während der Verarbeitung der Anforderung ist ein Kommunikationsfehler aufgetreten. Wiederholen Sie die Aktion zu einem späteren Zeitpunkt.

GVM5988E Während der Verarbeitung der Anforderung hat die Verwaltungs-API einen internen Fehler entdeckt.

GVM5989E Die Verwaltungs-API kann das vom Server gesendete Befehlsdokument nicht verarbeiten.

Erläuterung: Das XML-Befehlsdokument konnte nicht syntaktisch analysiert werden. Entweder konnte die Datei nicht gelesen werden oder die Datei ist beschädigt.

Benutzeraktion: Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5990E Der folgende Befehl enthält einen oder mehrere ungültige Parameter: ""*Befehl*"".

Erläuterung: Die Data Protection for Virtual Environments-GUI hat versucht, einen Befehl auszuführen, aber der Aufruf an die API enthielt einen oder mehrere ungültige Parameter.

Benutzeraktion: Überprüfen Sie die Parameter in dem Befehl. Haben Sie Text in ein Feld eingegeben, können

Sie den Fehler möglicherweise in den Parametern finden und korrigieren. Die Anzeige des Aktivitätenprotokolls kann bei der Bestimmung der Fehlerursache helfen. Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5991E Während der Verarbeitung der Anforderung hat die Verwaltungs-API ungültige Parameter entdeckt.

Erläuterung: Ein Befehl wurde über die Verwaltungs-API ausgeführt, aber einer der Parameter war für eine API-Methode ungültig.

Benutzeraktion: Dies ist normalerweise ein interner Fehler, aber er kann durch ungewöhnliche Parameter verursacht werden. Beispielsweise können Zeichen wie < > & den Fehler verursachen. Überprüfen Sie die Parameter in dem Befehl. Haben Sie Text in ein Feld eingegeben, können Sie den Fehler möglicherweise in den Parametern finden und korrigieren.

GVM5992E Die Berechtigungsstufe des Administrators auf diesem Server kann nicht bestimmt werden.

Erläuterung: Siehe Nachricht.

Benutzeraktion: Verwenden Sie eine andere Administrator-ID. Bevor Sie die Aktion wiederholen, ziehen Sie den Administrator des IBM Spectrum Protect-Servers zu Rate.

GVM5993E Ein Objekt mit dem angegebenen Namen ist bereits auf dem Server vorhanden. Geben Sie einen anderen Namen ein.

GVM5994E Die Version des Servers wird von der Data Protection for Virtual Environments-GUI nicht unterstützt.

GVM5995E Es ist ein interner Fehler aufgetreten.

Erläuterung: Die Operation ist nach einem internen Fehler fehlgeschlagen.

Benutzeraktion: Die Operation wiederholen. Bleibt der Fehler bestehen, verständigen Sie die Kundenunterstützung. Sie werden möglicherweise aufgefordert, Traceinformationen und Informationen zu den Aktionen bereitzustellen, die vor dem Auftreten des Fehlers ausgeführt wurden.

GVM5996E Die Operation ist fehlgeschlagen. Das Protokoll enthält ausführliche Informationen.

GVM5997E Falsches Format für Enddatum und -zeit. Geben Sie das Enddatum und die Endzeit im Format jjjjMMttHHmmss ein.

GVM5998E Die Beschreibung der Sicherungstask wurde nicht in einer Datei erstellt. Wiederholen Sie die Aktion.

Erläuterung: Auf der Seite 'Allgemein' des Sicherungsassistenten können Sie Ihre Sicherungstask allgemein beschreiben.

GVM5999E Der eingegebene ESXHOST-Name ist zu lang. Geben Sie einen kürzeren Namen ein.

GVM6000E Falsche Sicherungs-ID. Wiederholen Sie die Aktion.

GVM6001E Bei der Verarbeitung der Sicherungsobjektdatei ist ein Fehler aufgetreten. Wiederholen Sie die Aktion zu einem späteren Zeitpunkt.

Erläuterung: Wenn Sie im Sicherungsassistenten auf 'Übergeben' klicken, wird die Objektliste in einer Datei gespeichert. Bei der Verarbeitung dieser Datei ist ein Fehler aufgetreten.

GVM6002E Es wurde kein Sicherungsobjekt ausgewählt. Sie müssen einen Quellenknoten für die Sicherung auswählen.

Erläuterung: Um eine Sicherungstask einzuleiten, müssen Sie ein Objekt auf der Quellenseite des Sicherungsassistenten auswählen.

GVM6003E Falsches Format für Startdatum und -zeit. Geben Sie das Startdatum und die Startzeit im Format jjjjMMttHHmmss ein.

GVM6004I Sicherungstask *Taskname* wurde gestartet; soll diese Task jetzt überwacht werden?

GVM6005I Sicherungstask wurde erfolgreich gelöscht.

GVM6006E Löschen der Sicherungstask ist fehlgeschlagen. Überprüfen Sie das Protokoll auf weitere Details.

GVM6007I **Zurückschreibungstask** *Task-ID* **wurde erfolgreich gestartet; soll diese Task jetzt überwacht werden?**

GVM6008E *Fehler oder Warnung*

GVM6009I **Bereitgestelltes Sicherungsobjekt konnte nicht zurückgeschrieben werden.**

GVM6010I **Ergebnis der Zuordnung ist** *Status* **(Task-ID:** *Task-ID* **). Die Ereignisliste enthält Details.**

GVM6011I **Ergebnis der Aufhebung der Zuordnung ist** *Status* **(Task-ID:** *Task-ID* **). Die Ereignisliste enthält Details.**

GVM6012I **Der Befehl wurde erfolgreich an den IBM Spectrum Protect-Server übergeben.**
Detail: *Servernachrichten*

GVM6013E **Der Befehl, der an den IBM Spectrum Protect-Server übergeben wurde, ist fehlgeschlagen.**
Fehler: *Fehlercode*
Fehlernachrichten

Erläuterung: Die Ursache des Problems ist im Nachrichtentext angegeben.

Benutzeraktion: Lösen Sie das Problem auf der Basis der im Nachrichtentext angegebenen Informationen. Wiederholen Sie dann die Aktion.

GVM6014E **Keine IBM Spectrum Protect-Serververbindung vorhanden. Konfigurieren Sie den IBM Spectrum Protect-Server in der Konfigurationsanzeige.**

GVM6015E **Die ausgewählten Einträge können sich nur unter EINEM Datencenter befinden.**

GVM6018E **Die virtuelle Maschine** *VM-Name* **ist vorhanden. Löschen Sie zuerst die virtuelle Maschine, bevor Sie sie zurückschreiben.**

GVM6019E **Die virtuelle Zielmaschine** *VM-Name* **ist aktiv. Schließen Sie die virtuelle Maschine, bevor Sie virtuelle Platten auf sie zurückschreiben.**

GVM6020E **Einige der ausgewählten virtuellen Platten sind auf der virtuellen Zielmaschine vorhanden. Entfernen Sie diese virtuellen Platten auf der virtuellen Zielmaschine, bevor auf die Maschine zurückgeschrieben wird.**

GVM6021E **Ein VMCLI-Befehl ist fehlgeschlagen.**
Fehler: *Fehlernachrichten*

Erläuterung: Die Ursache des Problems ist im Nachrichtentext angegeben.

Benutzeraktion: Lösen Sie das Problem auf der Basis der im Nachrichtentext angegebenen Informationen. Wiederholen Sie dann die Aktion.

GVM6023E **Ein Befehl, der an den IBM Spectrum Protect-Server übergeben wurde, ist fehlgeschlagen.**
Fehler: *Fehlernachrichten*

Erläuterung: Die Ursache des Problems ist im Nachrichtentext angegeben.

Benutzeraktion: Lösen Sie das Problem auf der Basis der im Nachrichtentext angegebenen Informationen. Wiederholen Sie dann die Aktion.

GVM6024E **Die Datei mit dem Format 'summary.date.log' kann in dem folgenden Pfad nicht gefunden werden:** *Pfad*

GVM6025E **Der IBM Spectrum Snapshot-Installationspfad kann mit dem VMCLI-Befehl 'inquire_config' nicht gefunden werden.**

GVM6026E **Ein VMCLI-Befehl zum Abrufen der Version von ist fehlgeschlagen.**

GVM6027I **Sicherungstask** *Task-ID* **wurde gestartet; soll diese Task jetzt überwacht werden?**

GVM6028E **Der Data Protection for Virtual Environments-Web-Server konnte nicht angesprochen werden.**

Erläuterung: Die Data Protection for Virtual Environments-GUI hat versucht, Kontakt zu ihrem Web-Server aufzunehmen. Die Operation war nicht erfolgreich.

Benutzeraktion: Führen Sie einen oder mehrere der folgenden Schritte aus, um den Fehler zu bestimmen:

- Stellen Sie sicher, dass der Data Protection for Virtual Environments-Web-Server aktiv ist.
- Stellen Sie sicher, dass die Web-Servermaschine aktiv ist.
- Stellen Sie sicher, dass über das Netz auf die Web-Servermaschine zugegriffen werden kann.

Schließen Sie die Data Protection for Virtual Environments-GUI. Starten Sie die GUI erneut, nachdem der Fehler behoben wurde.

GVM6029I **Der Befehl wurde erfolgreich an den Server übergeben.**

GVM6030E **Im Datencenter** *Datencentername* **wurde kein Host gefunden. Wählen Sie ein anderes Datencenter für die Zurückschreibung aus.**

GVM6031W **Der Zeitplan enthält nicht alle erforderlichen Parameter. Er kann im Eigenschaftennotizbuch nicht angezeigt werden.**

Erläuterung: Dieser Zeitplan wurde möglicherweise außerhalb der Data Protection for Virtual Environments-GUI erstellt oder geändert.

Benutzeraktion: Dieser Zeitplan muss außerhalb der Data Protection for Virtual Environments-GUI geändert werden.

GVM6032W **Es sind eine oder mehrere virtuelle Maschinen vorhanden. Soll die Zurückschreibungsoperation fortgesetzt und sollen die vorhandenen virtuellen Maschinen überschrieben werden?**

GVM6033E **Die angegebene Administrator-ID hat keine ausreichenden Berechtigungen.**

Erläuterung: Für die von Ihnen versuchte Operation ist eine IBM Spectrum Protect-Serveradministrator-ID erforderlich, die mindestens über unbeschränkte Maßnahmenberechtigung verfügt.

Benutzeraktion: Bitten Sie den IBM Spectrum Protect-Serveradministrator, Ihrer Administrator-ID die unbeschränkte Maßnahmenberechtigung zu erteilen. Oder verwenden Sie eine alternative ID mit dieser Berechtigung und versuchen sie es erneut.

GVM6034E **Der Knotenname** *Knotenname* **wird bereits verwendet. Wählen Sie einen anderen Knotennamen.**

Erläuterung: Der ausgewählte Knotenname ist auf dem Server bereits vorhanden. Wählen Sie einen anderen Namen.

Benutzeraktion: Wählen Sie einen anderen Knotennamen aus. Wenn Sie diesen Knoten wiederverwenden wollen, inaktivieren Sie das Kontrollkästchen 'Knoten registrieren'.

GVM6035E **Der Knotenname** *Knotenname* **ist auf dem Server nicht definiert. Stellen Sie sicher, dass der eingegebene Knotenname auf dem Server existiert.**

Erläuterung: Der eingegebene Knotenname existiert nicht auf dem Server. Da Sie nicht das Kontrollkästchen 'Knoten registrieren' ausgewählt haben, muss der Name, den Sie eingeben, zuvor definiert worden sein und auf dem Server existieren.

Benutzeraktion: Überprüfen Sie den Knotennamen, den Sie verwenden sollen, und geben Sie ihn erneut ein. Wenn Sie diesen Knoten registrieren möchten, wählen Sie das Kontrollkästchen 'Knoten registrieren' aus.

GVM6036E **Die Kennwörter im Eingabefeld und im Prüffeld stimmen nicht überein. Wiederholen Sie die Aktion.**

Erläuterung: Die eingegebenen neuen Kennwörter stimmen nicht überein.

Benutzeraktion: Löschen Sie den Inhalt der Felder und geben Sie dasselbe Kennwort in beide Kennwortfelder ein.

GVM6037W **Wählen Sie mindestens ein zu verwaltendes Datencenter aus.**

Erläuterung: Mindestens ein Datencenter muss ausgewählt werden.

Benutzeraktion: Fügen Sie der Liste der verwalteten Datencenter mindestens ein Datencenter hinzu.

GVM6038W **Für mindestens einen Knoten wurde kein Kennwort festgelegt. Stellen Sie sicher, dass für alle Knoten ein Kennwort festgelegt wurde.**

Erläuterung: Wenn für einen Knoten das Kontrollkästchen 'Knoten registrieren' aktiviert wurde, muss für den Knoten ein Kennwort festgelegt werden.

Benutzeraktion: Weisen Sie Knoten, die registriert werden sollen, ein Kennwort zu.

GVM6039I **Es wurde kein Datencenterknoten gefunden, der** *Datencentername* **zugeordnet ist. Wählen Sie in der Liste einen Datencenterknoten aus, der** *Datencentername* **zugeordnet werden soll. Wählen Sie nichts aus, wenn der Konfigurationsassistent einen neuen Datencenterknoten dafür erstellen soll.**

GVM6040I **Möchten Sie wirklich fortfahren, ohne eine IBM Spectrum Protect-Administrator-ID einzugeben?**
Ohne IBM Spectrum Protect-Verwaltungszugriff wird der Assistent weder Knotennamen prüfen noch Knoten registrieren. Stattdessen wird nach Beendigung des Assistenten eine Makrodatei für Sie generiert, die Sie Ihrem IBM Spectrum Protect-Administrator zur Ausführung übergeben sollten.

GVM6041I **Diese Task wurde übersprungen, weil sie nicht erforderlich war oder weil eine vorausgesetzte Task fehlgeschlagen ist.**

GVM6042E **Beim Schreiben in die Scriptdatei** *Dateipfad* **trat ein Fehler auf.**

Erläuterung: Bei dem Versuch, in die durch den Pfad angegebene Datei zu schreiben, wurde ein Fehler festgestellt.

Benutzeraktion: Wiederholen Sie die Operation.

GVM6043I **Die verwalteten Datencenter haben sich geändert. Prüfen oder ändern Sie Ihre aktuellen Zuordnungen auf der Seite der Einheit zum Versetzen von Daten.**

GVM6044I **Für die Konfiguration des vCenter-Knotens** *vCenter-Knoten* **und des VMCLI-Knotens** *VMCLI-Knoten* **wurden keine Datencenterknoten gefunden. Der Assistent generiert eine Standardgruppe der Datencenterknoten für Sie.**

GVM6045E **Das eingegebene Kennwort ist nicht zulässig. Wählen Sie ein anderes Kennwort.**

Erläuterung: Der IBM Spectrum Protect-Server hat das ausgewählte Kennwort nicht akzeptiert. Möglicherweise entsprach das Kennwort nicht bestimmten Kennwortregeln.

Benutzeraktion: Versuchen Sie es mit einem anderen Kennwort.

GVM6046W **Das Abwählen dieses Kontrollkästchens bedeutet, dass Sie einen Knotennamen verwenden, der auf dem IBM Spectrum Protect-Server bereits definiert ist UND für Ihre Konfiguration verwendet werden soll. Da dieser Assistent ohne Verwaltungszugriff arbeitet, kann er nicht prüfen, ob der Knoten bereits existiert. Sie sollten nur fortfahren, wenn Sie verstehen, was Sie tun.**

Erläuterung: Da Sie den Konfigurationsassistenten ohne eine IBM Spectrum Protect-Administrator-ID verwenden, sollten Sie sehr vorsichtig sein. Die Makroscriptdatei, die am Ende der Ausführung des Konfigurationsassistenten generiert wird, könnte Fehler enthalten, da die Werte nicht überprüft werden.

Benutzeraktion: Es wird ausdrücklich empfohlen, den Konfigurationsassistenten mit einer korrekten IBM Spectrum Protect-Administrator-ID zu verwenden.

GVM6047W **Der IBM Spectrum Protect-Knoten** *Knoten* **wurde bereits angegeben. Wenn Sie einen anderen als den Standardnamen verwenden möchten, editieren Sie dieses Feld noch einmal. Wenn Sie dieselbe Einheit zum Versetzen von Daten für mehrere Datencenter verwenden möchten, geben Sie dies über die Konfigurationseinstellungen an.**

Erläuterung: Der Knoten wird bereits in dieser Konfiguration verwendet.

Benutzeraktion: Verwenden Sie einen anderen Knotennamen.

GVM6048W **Der IBM Spectrum Protect-Knoten** *Knoten* **enthält ungültige Zeichen oder überschreitet 64 Zeichen. Wählen Sie einen anderen Namen und editieren Sie dieses Feld noch einmal.**

Erläuterung: Der Knotenname ist ungültig oder länger als 64 Zeichen.

Benutzeraktion: Verwenden Sie einen anderen Knotennamen.

GVM6049E **Das eingegebene Kennwort ist auf diesem Server nicht zulässig, weil es ungültige Zeichen enthält. Gültige Zeichen sind:** *Gültige Zeichen*

Erläuterung: Der IBM Spectrum Protect-Server hat das ausgewählte Kennwort nicht akzeptiert, weil es ungültige Zeichen enthält.

Benutzeraktion: Versuchen Sie es mit einem anderen Kennwort, das nur gültige Zeichen enthält.

GVM6050E **Das eingegebene Kennwort ist auf diesem Server aus dem unten genannten Grund nicht zulässig. Wählen Sie ein anderes Kennwort.**
Fehler: *Nachricht*

Erläuterung: Der IBM Spectrum Protect-Server hat das ausgewählte Kennwort nicht akzeptiert. Warum das Kennwort nicht gültig ist, kann der Nachricht entnommen werden.

Benutzeraktion: Versuchen Sie es mit einem anderen,

den Regeln entsprechenden Kennwort.

GVM6051E Der Filter wurde geändert. Wählen Sie 'Filter anwenden' aus, bevor Sie fortfahren.

Erläuterung: Ein Filtermuster muss übernommen werden, nachdem es geändert wurde.

Benutzeraktion: Klicken Sie auf die Schaltfläche 'Filter anwenden'.

GVM6052E Wählen Sie zur Fortsetzung mindestens einen Eintrag aus einem Datencenter aus.

Erläuterung: Zur Durchführung einer Sicherung muss ein Host, ein Host-Cluster oder eine virtuelle Maschine ausgewählt werden.

Benutzeraktion: Wählen Sie einen Eintrag unter einem Datencenter aus.

GVM6053E Ihre Auswahl überschreitet die für Sicherungen erlaubte Grenze von 512 Zeichen. Ändern Sie Ihre Auswahl.

Erläuterung: Für das Auflisten der ausgewählten Einträge werden mehr als die erlaubten 512 Zeichen benötigt. Wenn Hosts nur partiell ausgewählt werden, werden außerdem Zeichen benötigt zum Auflisten der virtuellen Maschinen, die von der Sicherung ausgeschlossen werden.

Benutzeraktion: Erstellen Sie mehrere Sicherungstasks mit weniger ausgewählten Einträgen pro Task.

GVM6054I Bei Änderung des Kontrollkästchens für neu hinzugefügte virtuelle Maschinen werden alle ausgewählten Einträge für Host-Cluster, Hosts und virtuelle Maschinen abgewählt. Klicken Sie auf OK, um fortzufahren, oder auf 'Abbrechen', um die ausgewählten Einträge beizubehalten.

Erläuterung: Der Status des Kontrollkästchens für neu hinzugefügte virtuelle Maschinen hat erhebliche Auswirkungen darauf, welche Einträge in der Quellenanzeige ausgewählt werden dürfen. Daher werden die ausgewählten Einträge abgewählt, wenn sich der Status ändert.

Benutzeraktion: Wählen Sie OK aus, um fortzufahren, oder wählen Sie 'Abbrechen' aus, um alle ausgewählten Einträge beizubehalten.

GVM6055E Für den Datencenterknoten *Name des Datencenterknotens* **enthält die vmcli-Konfigurationsdatei keinen zugeordneten IBM Spectrum Protect-Knoten.**

Erläuterung: Für den Datencenterknoten muss in der Konfigurationsdatei vmcliprofile ein entsprechender IBM Spectrum Protect-Knoten aufgeführt sein.

Benutzeraktion: Korrigieren Sie den Fehler, indem Sie in der Registerkarte 'Konfiguration' der GUI 'Konfiguration editieren' auswählen, um die Zuordnung für das Datencenter zu aktualisieren. Beheben Sie außerdem alle weiteren Konfigurationsfehler, die in der Registerkarte 'Konfiguration' aufgelistet werden.

GVM6056E Der IBM Spectrum Protect-Datencenterknoten *Name des Datencenterknotens* **ist in der vmcli-Konfigurationsdatei dem vCenter-Datencenternamen** *Datencentername* **zugeordnet, aber** *Datencentername* **ist im vCenter nicht vorhanden.**

Erläuterung: Der vCenter-Datencentername ist in der vmcli-Konfigurationsdatei mit dem Namen vmcliprofile einem Datencenterknoten zugeordnet, aber der Datencentername ist im vCenter nicht vorhanden.

Benutzeraktion: Korrigieren Sie den Fehler, indem Sie in der Registerkarte 'Konfiguration' der GUI 'Konfiguration editieren' auswählen, um die Zuordnung für das Datencenter zu aktualisieren. Beheben Sie außerdem alle weiteren Konfigurationsfehler, die in der Registerkarte 'Konfiguration' aufgelistet werden.

GVM6057E Sie haben Einträge aus mehreren Datencentern ausgewählt: *Datencenterliste***. Dies ist nicht zulässig. Alle ausgewählten Einträge müssen aus einem einzigen Datencenter stammen.**

Erläuterung: Eine Sicherungstask unterstützt nur Einträge aus einem einzigen Datencenter. Falls es sich um eine bestehende Task handelt, ist dieses Problem möglicherweise auf Änderungen an der vCenter-Konfiguration nach dem Erstellen der Task zurückzuführen.

Benutzeraktion: Prüfen und korrigieren Sie die ausgewählten Einträge, sodass sich alle ausgewählten Einträge unter demselben Datencenter befinden.

GVM6058E Die ausgewählten Einträge *Eintragsliste* **werden unter dem Datencenter** *Datencentername* **im vCenter nicht gefunden. Prüfen Sie sie und wählen Sie sie ab.**

Erläuterung: Ursprünglich ausgewählte Einträge werden unter dem der Sicherungstask zugeordneten Datencenter nicht mehr gefunden. Dies kann durch Änderungen an der vCenter-Konfiguration verursacht worden sein.

Benutzeraktion: Prüfen Sie, ob sich die Einträge jetzt unter einem anderen Datencenter befinden. Wählen Sie die nicht gefundenen Einträge ab und treffen Sie eine neue Auswahl unter dem anderen Datencenter oder erstellen Sie eine neue Sicherungstask für diese Einträge.

GVM6062E **Das eingegebene Kennwort ist auf diesem Server nicht zulässig, weil es zu kurz ist. Kennwörter müssen aus mindestens** *Mindestkennwortlänge* **Zeichen bestehen.**

Erläuterung: Der IBM Spectrum Protect-Server hat das ausgewählte Kennwort nicht akzeptiert, weil es zu kurz ist.

Benutzeraktion: Versuchen Sie es mit einem Kennwort, das länger als die erforderliche Mindestlänge ist.

GVM6063E *Komponente* **ist eine ältere Version und wird deshalb in der GUI inaktiviert. Sie können die GUI nur für** *Komponente* **verwenden.**

GVM6064E **In den aktuellen Einstellungen wurde eine Abweichung bei Einträgen für den IBM Spectrum Protect-Server erkannt. Von der GUI verwendete Definition des IBM Spectrum Protect-Servers:**
Server1
IBM Spectrum Protect-Server, auf dem Sicherungen gespeichert werden:
Server2
Klicken Sie auf ""Serverdefinition zurücksetzen"", um die IBM Spectrum Protect-Definition zu löschen und neue Berechtigungsnachweise einzugeben. Sie können auch auf ""Umgebung rekonfigurieren"" klicken, um den Konfigurationsassistenten für das Rekonfigurieren Ihrer Data Protection for Virtual Environments-Umgebung zu starten.

Erläuterung: IBM Spectrum Protect hat eine Abweichung der IBM Spectrum Protect-Servereinträge zwischen der Datei vmcliprofile und der IBM Spectrum Protect-Serververbindung der aktuellen GUI erkannt.

Benutzeraktion: Wählen Sie eine der beiden verfügbaren Aktionen aus. Sie können entweder die IBM Spectrum Protect-Serverdefinition/Berechtigungsnachweise zurücksetzen ODER mit dem Konfigurationsassistenten eine neue Umgebung konfigurieren.

GVM6065E **Die SSL-Verbindung konnte nicht hergestellt werden. Das IBM Spectrum Protect-SSL-Zertifikat fehlt. Überprüfen Sie 'TSM-ve-truststore.jks' auf ein gültiges IBM Spectrum Protect-Zertifikat.**

Erläuterung: Der IBM Spectrum Protect-Server hat die SSL-Verbindung nicht akzeptiert. Der SSL-Schlüsselspeicher befindet sich nicht an der Standardposition oder enthält kein IBM Spectrum Protect-Zertifikat.

Benutzeraktion: Überprüfen Sie 'TSM-ve-truststore.jks' auf ein gültiges Zertifikat und stellen Sie sicher, dass sich 'TSM-ve-truststore.jks' an der korrekten Standardposition befindet.

GVM6066E **Das eingegebene Kennwort ist auf diesem Server nicht zulässig, weil es zu lang ist. Kennwörter dürfen aus maximal** *max. Kennwortlänge* **Zeichen bestehen.**

Erläuterung: Der IBM Spectrum Protect-Server hat das ausgewählte Kennwort nicht akzeptiert, weil es zu lang ist.

Benutzeraktion: Versuchen Sie es mit einem Kennwort, das kürzer als die zulässige maximale Länge ist.

GVM6067E **Die SSL-Verbindung konnte nicht hergestellt werden. Das IBM Spectrum Protect-SSL-Zertifikat ist ungültig.**

Erläuterung: Der IBM Spectrum Protect-Server hat die SSL-Verbindung nicht akzeptiert. 'TSM-ve-truststore.jks' enthält ein ungültiges IBM Spectrum Protect-SSL-Zertifikat.

Benutzeraktion: Fordern Sie ein neues gültiges IBM Spectrum Protect-SSL-Zertifikat vom IBM Spectrum Protect-Server an und stellen Sie es in 'TSM-ve-truststore.jks'.

GVM6068E **Die Nicht-SSL-Verbindung konnte nicht hergestellt werden. Diese IBM Spectrum Protect-Administrator-ID erfordert eine IBM Spectrum Protect-SSL-Verbindung.**

Erläuterung: Der IBM Spectrum Protect-Server hat die Nicht-SSL-Verbindung nicht akzeptiert. Der IBM Spectrum Protect-Server erfordert die Verwendung von SSL mit dieser Administrator-ID.

Benutzeraktion: Verwenden Sie SSL mit dieser Administrator-ID. Stellen Sie sicher, dass 'TSM-ve-truststore.jks' mit einem gültigen SSL-Zertifikat für den IBM Spectrum Protect-Server an der Standardposition installiert ist.

GVM6069E **Aufgrund Ihrer ausgewählten Einträge wurden für die Definition der Sicherungstask** *Anzahl* **Zeichen benötigt. Damit wird der Grenzwert von 512 Zeichen überschritten. Dies kann durch eine lange Ausschlussliste mit virtuellen Maschinen verursacht werden. Diese Liste enthält alle virtuellen Maschinen unter Host(s), die nicht ausgewählt wurden. Wählen Sie entweder mehr virtuelle Maschinen unter den ausgewählten Hosts aus oder wählen Sie das Kontrollkästchen für neu hinzugefügte virtuelle Maschinen ab.**

Erläuterung: Wenn das Kontrollkästchen für neu hin-

zugefügte virtuelle Maschinen ausgewählt ist, muss die resultierende Sicherungstask alle nicht ausgewählten virtuellen Maschinen für Hosts auflisten, die partiell ausgewählt wurden. Die Definition der Sicherungstask hat eine Begrenzung von 512 Zeichen und die Kombination aus ausgewählten Einträgen und ausgeschlossenen virtuellen Maschinen überschreitet diesen Grenzwert.

Benutzeraktion: Wählen Sie das Kontrollkästchen für neu hinzugefügte virtuelle Maschinen ab oder erstellen Sie mehrere Sicherungstasks mit weniger ausgewählten Einträgen pro Task.

GVM6070E **Aufgrund Ihrer Auswahl von virtuellen Maschinen wurden für die Definition der Sicherungstask** *Anzahl* **Zeichen benötigt. Damit wird der Grenzwert von 512 Zeichen überschritten. Erstellen Sie entweder mehrere Sicherungstasks mit weniger virtuellen Maschinen pro Task oder wählen Sie das Kontrollkästchen für neu hinzugefügte virtuelle Maschinen aus und wählen Sie gesamte Hosts mit nur wenigen nicht ausgewählten virtuellen Maschinen aus.**

Erläuterung: Die Definition der Sicherungstask hat eine Begrenzung von 512 Zeichen und die Gesamtzahl der Zeichen für die ausgewählten Einträge überschreitet diesen Grenzwert.

Benutzeraktion: Erstellen Sie mehrere Sicherungstasks mit weniger ausgewählten virtuellen Maschinen pro Task oder wählen Sie das Kontrollkästchen für neu hinzugefügte virtuelle Maschinen aus und wählen Sie dann Hosts anstelle von einzelnen virtuellen Maschinen aus (falls gewünscht, können Sie eine geringe Anzahl virtueller Maschinen pro Host abwählen).

GVM6071E **Es ist keine Proxy-Beziehung des Knotens der Einheit zum Versetzen von Daten für den Datencenterknoten** *Name des Datencenterknotens* **vorhanden. Überprüfen Sie die Beziehungen der Einheit zum Versetzen von Daten auf der Registerkarte 'Konfiguration' oder auf dem IBM Spectrum Protect-Server.**

GVM6072E **Es ist kein Datencenterknoten für das Datencenter** *Datencentername* **definiert. Überprüfen Sie die Knotenkonfiguration auf der Registerkarte 'Konfiguration'.**

GVM6073I **Knoten** *Knotenname* **ist derzeit gesperrt. Wenn Sie fortfahren, versucht der Konfigurationsassistent, diesen Knoten zu entsperren.**

GVM6074E **Es konnte keine Verbindung zum IBM Spectrum Protect-Server (***Adresse:Port***) hergestellt werden. Überprüfen Sie, ob die Serveradresse und der Admin-Port** *Server- oder Admin-Port* **korrekt sind.**

Erläuterung: Möglicherweise ist der Server nicht aktiv oder der angegebene Admin-Port oder Server-Admin-Port ist falsch.

Benutzeraktion: Überprüfen Sie die Netzverbindung mit der IBM Spectrum Protect-Servermaschine. Stellen Sie sicher, dass der Server aktiv ist, und melden Sie sich erneut an. Überprüfen Sie außerdem, ob die Informationen zur Serveradresse und zum Admin-Port korrekt sind.

GVM6075E **Der vCenter-Benutzername oder das zugehörige Kennwort ist nicht gültig. Wiederholen Sie die Aktion.**

Erläuterung: Der vCenter-Benutzername oder das zugehörige Kennwort ist nicht gültig.

Benutzeraktion: Geben Sie den Benutzernamen oder das Kennwort erneut ein.

GVM6076E **Die Berechtigung zum Ausführen dieser Operation wurde verweigert. Bitte geben Sie einen anderen Benutzernamen an.**

Erläuterung: Der vCenter-Benutzername ist nicht gültig.

Benutzeraktion: Geben Sie einen anderen Benutzernamen ein.

GVM6077I **Eine Administrator-ID und ein Kennwort sind für IBM Spectrum Protect derzeit nicht festgelegt. Das Fehlen dieser Informationen schränkt die Aktionen ein, die Sie in der GUI ausführen können. Klicken Sie auf 'OK', um in der Konfigurationseinstellungsanzeige eine ID und ein Kennwort einzugeben. Klicken Sie auf 'Abbrechen', um ohne Verwendung einer ID und eines Kennworts fortzufahren.**

GVM6078W **Sie haben eine Administrator-ID ausgewählt, die weniger Berechtigungen hat als die aktuelle ID. Sind Sie sicher, dass Sie diese ID ändern möchten?**
Aktuelle IBM Spectrum Protect-Berechtigungsstufe: *Aktuelle Stufe*
Neue IBM Spectrum Protect-Berechtigungsstufe: *Neue Stufe*
Aktuelle Rolle: *Aktuelle Rolle*
Neue Rolle: *Neue Rolle*
Klicken Sie auf 'OK', um diese Ände-

rungen zu akzeptieren, oder auf 'Abbrechen', um die Anzeige ohne Änderungen zu verlassen.

GVM6079I **Dies sind die aktuelle und die neue Rolle für IBM Spectrum Protect-Administrator-IDs. Überprüfen und bestätigen Sie diese Änderungen.**
Aktuelle IBM Spectrum Protect-Berechtigungsstufe: *Aktuelle Stufe*
Neue IBM Spectrum Protect-Berechtigungsstufe: *Neue Stufe*
Aktuelle Rolle: *Aktuelle Rolle*
Neue Rolle: *Neue Rolle*
Klicken Sie auf 'OK', um diese Änderungen zu akzeptieren, oder auf 'Abbrechen', um die Anzeige ohne Änderungen zu verlassen.

GVM6080I **Die ID wurde ohne Sichern geändert. Die vorherige ID wird geladen.**

GVM6081I **Ihre aktuelle Rolle in der Benutzerschnittstelle erlaubt nicht das Entsperren oder Zurücksetzen des VMCLI-Knotens. Um Änderungen vornehmen zu können, rufen Sie die Seite 'Serverberechtigungsnachweise' auf und geben Sie eine IBM Spectrum Protect-Administrator-ID und ein Kennwort ein, das über die erforderlichen Berechtigungen zum Aktualisieren des VMCLI-Knotens verfügt. Wählen Sie OK aus, um diese Berechtigungsnachweise zu speichern. Öffnen Sie dann erneut das Notizbuch mit den Konfigurationseinstellungen und aktualisieren Sie den VMCLI-Knoten.**

GVM6082I **Ihre aktuelle Rolle in der Benutzerschnittstelle erlaubt nicht das Aufrufen anderer Anzeigen. Wählen Sie OK aus, um diese Berechtigungsnachweise zu speichern. Öffnen Sie dann erneut das Notizbuch mit den Konfigurationseinstellungen und nehmen Sie andere Aktualisierungen vor.**

GVM6083I **Ein oder mehrere Datencenter enthalten nicht englische Zeichen. Die Domäne wird entsprechend angepasst.**

GVM6084E **Das Datencenter** *Datencentername* **kann der Domäne nicht hinzugefügt werden, da es nicht englische Zeichen enthält.**

Erläuterung: Datencenter, die nicht englische Zeichen enthalten, werden derzeit nicht unterstützt. Daher können Sie nicht der Domäne hinzugefügt werden.

Benutzeraktion: Das Datencenter wird der Domäne nicht hinzugefügt.

GVM6085W **Der Knoten** *Knotenname* **ist bereits auf dem Server vorhanden. Soll der Knoten in** *Neuer Knotenname* **umbenannt werden?**

Erläuterung: Der Knotenname ist bereits auf dem IBM Spectrum Protect-Server registriert.

Benutzeraktion: Klicken Sie auf 'Ja', um den Knoten umzubenennen. Klicken Sie auf 'Nein', um andere Änderungen vorzunehmen. Beispiel: 'Knoten registrieren' abwählen, Knoten manuell umbenennen.

GVM6086W **Die Namen der folgenden virtuellen Maschinen für den Host** *Hostname* **enthalten nicht unterstützte Zeichen:** *Ungültige Namen virtueller Maschinen***. Daher werden diese virtuellen Maschinen unabhängig von Ihren ausgewählten Einträgen nicht gesichert. Sie müssen diese virtuellen Maschinen umbenennen, damit sie gesichert werden.**

Erläuterung: Die folgenden Zeichen werden in Namen virtueller Maschinen nicht unterstützt: „" ' : ; * ? , < > / |

Benutzeraktion: Benennen Sie die angegebenen virtuellen Maschinen um und entfernen Sie nicht unterstützte Zeichen aus ihren Namen.

GVM6087E **Die Namen der folgenden Host-Cluster enthalten nicht unterstützte Zeichen:** *Ungültige Host-Cluster***. Diese Host-Cluster können nicht für die Sicherung ausgewählt werden, weil sie nicht unterstützte Zeichen enthalten. Benennen Sie diese Host-Cluster um oder entfernen Sie sie aus der Auswahl.**

Erläuterung: Die folgenden Zeichen werden in Namen von Host-Clustern nicht unterstützt: „" ' : ; * ? , < > / |

Benutzeraktion: Benennen Sie die angegebenen Host-Cluster um und entfernen Sie nicht unterstützte Zeichen aus ihren Namen. Oder entfernen Sie sie aus Ihrer Sicherungsauswahl.

GVM6088E **Auf der Basis Ihrer ausgewählten Einträge wurde eine leere Liste virtueller Maschinen für die Sicherung erstellt. Dieses Problem kann auftreten, weil die Namen aller ausgewählten virtuellen Maschinen nicht unterstützte Zeichen enthalten. Überprüfen Sie, ob Sie virtuelle Maschinen ausgewählt haben, deren Namen nicht unterstützte Zeichen enthalten.**

Erläuterung: Die folgenden Zeichen werden in Namen virtueller Maschinen nicht unterstützt: „" ' : ; * ? , < > / | . Die Namen virtueller Maschinen, die diese Zeichen enthalten, werden automatisch aus der Definition der Sicherungstask entfernt. Dieses Entfernen kann eine leere Taskdefinition verursachen.

Benutzeraktion: Benennen Sie die angegebenen virtuellen Maschinen um und entfernen Sie nicht unterstützte Zeichen aus ihren Namen. Oder wählen Sie andere virtuelle Maschinen für die Sicherung aus.

GVM6089E **Das Filtermuster kann nicht angewendet werden, weil es nicht unterstützte Zeichen enthält. Ändern Sie das Muster, indem Sie die nicht unterstützten Zeichen entfernen, und wenden Sie den Filter anschließend erneut an.**

Erläuterung: Die folgenden Zeichen werden im Filtermuster nicht unterstützt: „" ' : ; < > / |

Benutzeraktion: Ändern Sie das Filtermuster, indem Sie die nicht unterstützten Zeichen entfernen, und wenden Sie den Filter anschließend erneut an.

GVM6090E **Für die Ausführung dieser Operation ist kein temporärer Datenspeicher verfügbar. Dieser temporäre Datenspeicher ist neben dem Datenspeicher für das Zurückschreibungsziel erforderlich.**

Erläuterung: Für diese Operation ist ein Datenspeicher für die Verwendung als temporäres Zurückschreibungsziel erforderlich. Dieser temporäre Datenspeicher muss von demselben ESX-Host stammen wie der Datenspeicher, der als tatsächliches Zurückschreibungsziel verwendet wird. Bei dem temporären Datenspeicher darf es sich jedoch nicht um den Datenspeicher handeln, der auch als tatsächliches Zurückschreibungsziel verwendet wird.

Benutzeraktion: Fügen Sie dem ESX-Zielhost einen Datenspeicher hinzu. Wählen Sie diesen Datenspeicher anschließend als temporäres Zurückschreibungsziel aus.

GVM6091E **Beim Erstellen der opt-Datei ist ein Fehler aufgetreten:** *Dateiname***.**

Erläuterung: Bei dem Versuch, in die Datei zu schreiben, wurde ein Fehler festgestellt.

Benutzeraktion: Wiederholen Sie die Operation.

GVM6092E **Die Erstellung von** *Service* **ist fehlgeschlagen. Für den Knoten der Einheit zum Versetzen von Daten** *Knotenname* **wurden keine Services erstellt.**

Erläuterung: Bei dem Versuch, den IBM Spectrum Protect-Service für den angegebenen Knoten der Einheit zum Versetzen von Daten zu erstellen, ist ein Fehler aufgetreten.

Benutzeraktion: Überprüfen Sie die Umgebung und stellen Sie sicher, dass der Benutzer über ordnungsgemäße Berechtigungen verfügt, bevor Sie die Operation wiederholen.

GVM6093E **Die Erstellung der Firewall für** *Service* **ist fehlgeschlagen. Fügen Sie manuell Firewallregeln für die installierten Services hinzu.**

Erläuterung: Bei dem Versuch, eine Firewallregel für die angegebene ausführbare Datei hinzuzufügen, ist ein Fehler aufgetreten.

Benutzeraktion: Überprüfen Sie die Umgebung und stellen Sie sicher, dass der Benutzer über ordnungsgemäße Berechtigungen verfügt, bevor Sie die Operation wiederholen. Sie können auch manuell Firewallregeln für den IBM Spectrum Protect-Clientakzeptor, IBM Spectrum Protect-Agent und IBM Spectrum Protect-Scheduler hinzufügen.

GVM6094W **Die lokalen Services wurden erfolgreich eingerichtet; sie konnten jedoch den Firewallzugriff für die folgenden ausführbaren Dateien nicht prüfen:**
agentExe
cadExe
schedExe
Falls Probleme in Bezug auf lokale Services auftreten, überprüfen Sie, ob Firewallzugriff für diese ausführbaren Dateien verfügbar ist.

Erläuterung: Möglicherweise ist die Microsoft-Firewall inaktiviert oder eine andere Firewall wird verwendet.

Benutzeraktion: Überprüfen Sie die Umgebung und fügen Sie bei Bedarf manuell Regeln für den IBM Spectrum Protect-Clientakzeptor, IBM Spectrum Protect-Agent und IBM Spectrum Protect-Scheduler hinzu.

GVM6095E **Der Knoten der Einheit zum Versetzen von Daten** *Knotenname* **wurde erfolgreich auf dem Server registriert; es wurden jedoch keine Services erstellt.**

Erläuterung: Bei dem Versuch, Services für den angegebenen Knoten zu erstellen, ist ein Fehler aufgetreten.

Benutzeraktion: Überprüfen Sie die Umgebung und stellen Sie sicher, dass der Benutzer über ordnungsgemäße Berechtigungen verfügt, bevor Sie die Operation wiederholen.

GVM6096E **Ursachencode** *Ursache*
Dieser Fehler wurde von der IBM Spectrum Protect-Einheit zum Versetzen von Daten zurückgemeldet. Es ist keine weitere Beschreibung verfügbar. Weitere Informationen finden Sie im Fehlerprotokoll *Fehlerprotokoll* **auf der Hostmaschine der Einheit zum Versetzen von Daten,** *Hostname***, unter der Adresse '***Adresse***'.**

Erläuterung: Bei der Einheit zum Versetzen von Daten ist ein Fehler mit dem zurückgemeldeten Ursachencode aufgetreten.

Benutzeraktion: Melden Sie sich bei der angegebenen Hostmaschine an und überprüfen Sie das Fehlerprotokoll auf weitere Informationen.

GVM6097W **Der Scanzeitplan** *Zeitplanname* **wurde erfolgreich auf dem Server definiert und dem Knoten** *Knotenname* **zugeordnet; es wurden jedoch keine Services erstellt, um den Zeitplan auszuführen.**
Detail: *Fehler*

Erläuterung: In einem der folgenden Schritte wurde ein Fehler festgestellt, als versucht wurde, IBM Spectrum Protect-Services für den VMCLI-Knoten zu erstellen.

1. Optionsdatei für den VMCLI-Knoten erstellen.
2. Kennwort für den VMCLI-Knoten für den nächsten Schritt auf ein temporäres Kennwort setzen.
3. IBM Spectrum Protect-Konfigurationsdienstprogramm für Client-Service zum Erstellen der Services ausführen.
4. IBM Spectrum Protect-Konfigurationsdienstprogramm für Client-Service zum Starten des Clientakzeptorservice ausführen.
5. VMCLI-Knotenkennwort zurücksetzen.

Benutzeraktion: Löschen Sie den Zeitplan und erstellen Sie ihn erneut, um die Services automatisch zu konfigurieren, oder konfigurieren Sie die Services manuell. Überprüfen Sie die Umgebung und stellen Sie sicher, dass der Benutzer über ordnungsgemäße Berechtigungen verfügt, bevor Sie die Operation wiederholen.

GVM6098W **Scanzeitplan** *Zeitplanname* **wurde erfolgreich auf dem Server definiert und dem Knoten** *Knotenname* **zugeordnet. IBM Spectrum Protect-Services zur Ausführung des Zeitplans wurden erstellt. Das Zurücksetzen des VMCLI-Knotenkennworts ist jedoch fehlgeschlagen.**
Detail: *Fehler*

Erläuterung: Bei dem Versuch, das VMCLI-Knotenkennwort zurückzusetzen, wurde ein Fehler festgestellt.

Benutzeraktion: Verwenden Sie die Konfigurationseinstellungen, um das VMCLI-Knotenkennwort zurückzusetzen.

GVM6099W **Warnung: Wenn diese Task abgebrochen wird, gehen alle erstellten Daten auf den virtuellen Maschinen, die nicht vollständig zurückgeschrieben sind, verloren und die virtuellen Maschinen werden aus dem ESX-Host entfernt.**
Soll diese Task wirklich abgebrochen werden?

Erläuterung: Ein Befehl zum Abbrechen der Task wird übergeben. Führen Sie eine Aktualisierung durch, um den Fortschritt des Abbruchs anzuzeigen.

Benutzeraktion: Brechen Sie die ausgewählte Task ab oder erlauben Sie die Fortsetzung der Taskverarbeitung.

GVM6100W **Bei einer Operation zum Aufheben der Bereitstellung werden die iSCSI-Platten entfernt, jedoch nicht die VM oder ihre Daten. Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, bevor Sie mit der Aufhebung der Bereitstellung fortfahren:**
-Die bereitgestellte iSCSI-Platte wurde wiederhergestellt.
-Storage vMotion hat die Umlagerung der virtuellen Maschine in einen lokalen Datenspeicher abgeschlossen.
Ist die Wiederherstellungsoperation fehlgeschlagen und möchten Sie die VM und ihre Daten löschen sowie die Bereitstellung aller iSCSI-Ziele aufheben, klicken Sie auf 'Bereitstellung aufheben und löschen'. 'Bereitstellung aufheben und löschen' ist eine zerstörerische Aktion, durch die die VM und ihre Daten unabhängig vom Erfolg oder Misserfolg der Instant Restore-Operation gelöscht werden.
Möchten Sie auf der Basis dieser Informationen die Bereitstellung der VMs aufheben, die für Instant Restore ausgewählt sind?

Erläuterung: Bei einer Operation zum Aufheben der Bereitstellung werden die iSCSI-Platten entfernt, jedoch

nicht die VM oder ihre Daten. Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, bevor Sie mit der Aufhebung der Bereitstellung fortfahren: Die bereitgestellte iSCSI-Platte wurde wiederhergestellt, Storage vMotion hat die Umlagerung der virtuellen Maschine in einen lokalen Datenspeicher abgeschlossen. Ist die Wiederherstellungsoperation fehlgeschlagen und möchten Sie die VM und ihre Daten löschen sowie die Bereitstellung aller iSCSI-Ziele aufheben, klicken Sie auf 'Bereitstellung aufheben und löschen'. 'Bereitstellung aufheben und löschen' ist eine zerstörerische Aktion, durch die die VM und ihre Daten unabhängig vom Erfolg oder Misserfolg der Instant Restore-Operation gelöscht werden.

Benutzeraktion: Klicken Sie auf 'Bereitstellung aufheben', um die Bereitstellung der virtuellen Maschinen aufzuheben, die für die Instant Restore-Operation ausgewählt sind. Klicken Sie auf 'Bereitstellung aufheben und löschen', um die Bereitstellung der virtuellen Maschinen aufzuheben, die für die Instant Restore-Operation ausgewählt sind, diese virtuellen Maschinen aus dem ESX-Host zu entfernen und zu überprüfen, ob Storage vMotion aktiv ist.

GVM6101W **Bei einer Operation zum Aufheben der Bereitstellung gehen alle erstellten Daten auf den virtuellen Maschinen verloren und die virtuellen Maschinen werden aus dem ESX-Host entfernt. Soll die Bereitstellung der ausgewählten Instant Access-VMs aufgehoben werden?**

Erläuterung: Alle erstellten Daten auf den virtuellen Maschinen gehen verloren und die virtuellen Maschinen werden aus dem ESX-Host entfernt.

Benutzeraktion: Klicken Sie auf 'Bereitstellung aufheben', um die Bereitstellung der Instant Access-VMs aufzuheben (die Instant Access-VMs zu bereinigen).

GVM6102E **Die Auswahl mehrerer virtueller Maschinen mit unterschiedlichem Zurückschreibungstyp ist nicht zulässig.**

Erläuterung: Die Zurückschreibung mehrerer virtueller Maschinen mit unterschiedlichem Zurückschreibungstyp wird nicht unterstützt.

Benutzeraktion: Wählen Sie virtuelle Maschinen mit demselben Zurückschreibungstyp aus.

GVM6103I **Bereinigungstask** *Task-ID* **wurde erfolgreich gestartet; soll diese Task jetzt überwacht werden?**

GVM6104W **Soll diese Task wirklich abgebrochen werden?**

Erläuterung: Ein Befehl zum Abbrechen der Task wird übergeben. Führen Sie eine Aktualisierung durch, um den Fortschritt des Abbruchs anzuzeigen.

Benutzeraktion: Brechen Sie die ausgewählte Task ab oder erlauben Sie die Fortsetzung der Taskverarbeitung.

GVM6105I **Ihre aktuelle Rolle in der Benutzerschnittstelle erlaubt nicht das Anzeigen des Notizbuchs mit den Sicherungseigenschaften.**

GVM6106I **Ihre aktuelle Rolle in der Benutzerschnittstelle erlaubt nicht das Editieren von Knoten. Um Änderungen vornehmen zu können, öffnen Sie das Notizbuch 'Konfigurationseinstellungen'. Rufen Sie die Seite 'Serverberechtigungsnachweise' auf und geben Sie eine IBM Spectrum Protect-Administrator-ID mit dem zugehörigen Kennwort ein, die über die erforderlichen Berechtigungen zum Aktualisieren von Knoten verfügt.**

GVM6107E **Ursachencode** *Ursache*
Dieser Fehler wurde von der IBM Spectrum Protect-Einheit zum Versetzen von Daten zurückgemeldet. Es ist keine weitere Beschreibung verfügbar. Weitere Informationen finden Sie im Fehlerprotokoll 'dsmerror.log' auf der Hostmaschine der Einheit zum Versetzen von Daten.

Erläuterung: Bei der Einheit zum Versetzen von Daten ist ein Fehler mit dem zurückgemeldeten Ursachencode aufgetreten.

Benutzeraktion: Melden Sie sich bei der Hostmaschine an, auf der die Einheit zum Versetzen von Daten sich befindet, und überprüfen Sie das Fehlerprotokoll auf weitere Informationen.

GVM6108W **Anmeldeinformationen für vCenter erforderlich.**

Erläuterung: Für die Installation neuer lokaler Services für die Einheit zum Versetzen von Daten sind vCenter-Berechtigungsnachweise erforderlich.

Benutzeraktion: Geben Sie vCenter-Berechtigungsnachweise ein, um fortzufahren.

GVM6109E Sie haben nicht die erforderlichen Berechtigungen für den Zugriff auf die GUI.

Erläuterung: Für den Zugriff auf GUI-Inhalte muss der Benutzer die notwendigen vSphere-Berechtigungen haben.

Benutzeraktion: Fügen Sie die erforderlichen Berechtigungen für den Benutzer hinzu.

GVM6110E Sie haben nicht die erforderlichen Berechtigungen für den Zugriff auf die GUI.

Erläuterung: Für den Zugriff auf GUI-Inhalte muss der Benutzer die notwendigen vSphere-Berechtigungen haben.

Benutzeraktion: Fügen Sie die erforderlichen Berechtigungen für den Benutzer hinzu.

GVM6111I Ein neues Datencenter (*Name*) wurde erkannt. Rufen Sie die Seite 'Knoten der Einheit zum Versetzen von Daten' auf und fügen Sie einen Datencenterknoten für dieses Datencenter hinzu.

GVM6112W Die folgenden Freigaben und Bereitstellungen werden entfernt und die zugehörigen Daten sind für den Endbenutzer nicht mehr zugänglich. Bereitstellung der ausgewählten Freigaben und Bereitstellungen aufheben? *Bereitstellungen*

Erläuterung: Die ausgewählten Freigaben und Bereitstellungen werden entfernt.

Benutzeraktion: Klicken Sie auf 'Bereitstellung aufheben', um die Bereitstellung der Bereitstellungen und Freigaben aufzuheben (diese zu bereinigen).

GVM6113I Die Task *Task-ID* zum Aufheben der Bereitstellung wurde erfolgreich gestartet. Möchten Sie diese Task jetzt überwachen?

GVM6114W Bei der Löschoperation für die Optionsdatei ist ein Fehler aufgetreten: *Dateiname***.**

Erläuterung: Bei der Löschoperation ist ein Fehler aufgetreten. Dieser Fehler kann beispielsweise durch ungenügende Benutzerberechtigungen verursacht werden oder die Datei ist nicht mehr vorhanden.

Benutzeraktion: Stellen Sie sicher, dass die Optionsdatei gelöscht wurde. Ist diese Datei noch vorhanden, löschen Sie sie manuell.

GVM6115W Die Entfernungsoperation für den IBM Spectrum Protect-Service *Service* ist fehlgeschlagen.

Erläuterung: Ein Fehler hat verhindert, dass der IBM Spectrum Protect-Service entfernt wurde.

Benutzeraktion: Überprüfen Sie die Umgebung und stellen Sie sicher, dass der Benutzer über ausreichende Berechtigungen für die Ausführung dieser Operation verfügt. Wiederholen Sie anschließend die Operation.

GVM6116E Der iSCSI-Service für den Mount-Proxy-Knoten *Knotenname* konnte nicht gestartet werden.

Erläuterung: Beim Versuch, den iSCSI-Service für den angegebenen Mount-Proxy-Knoten zu starten, ist ein Fehler aufgetreten.

Benutzeraktion: Starten Sie den iSCSI-Service manuell.

GVM6117E Die Verbindung zum IBM Spectrum Protect-Server war nicht erfolgreich, weil entweder die Serverberechtigungsnachweise ungültig sind oder ein SSL-Zertifikat erforderlich ist, aber nicht abgerufen werden konnte.

Erläuterung: Für die Herstellung der Verbindung zum Server sind eine korrekte Serverbenutzer-ID und ein korrektes Kennwort sowie ein SSL-Zertifikat für den IBM Spectrum Protect-Server erforderlich.

Benutzeraktion: Rufen Sie die Notizbuchseite 'Konfiguration > Tasks > IBM Spectrum Protect-Konfiguration editieren > Serverberechtigungsnachweise' auf. Stellen Sie sicher, dass die Anmeldeberechtigungsnachweise korrekt sind, dass die korrekte Portnummer für den IBM Spectrum Protect-Administratorport angegeben ist und dass das Kontrollkästchen 'SSL verwenden...' ausgewählt ist. Das Zertifikat des Servers muss abgerufen und ein Truststore erstellt werden. Die entsprechende Prozedur ist unter dem Link 'Weitere Informationen...' dokumentiert.

GVM6118E Sie haben Organisations-VDCs aus mehreren Provider-VDCs ausgewählt. Für Sicherungstasks müssen alle ausgewählten Organisations-VDCs zu demselben Provider-VDC gehören. Ändern Sie die ausgewählten Einträge und wiederholen Sie die Operation.

GVM6119E Die folgenden vCloud-Ressourcen (vApp, Organisation, Organisations-vDC) sind für die Auswahl ungültig, da ihre Namen nicht unterstützte Zeichen enthalten: *Ressourcenliste*

Erläuterung: Für die Erstellung von Sicherungstasks dürfen die Namen von vCloud-Ressourcen keines der folgenden Zeichen enthalten: „" ' : ; * ? , < > / | .

Benutzeraktion: Benennen Sie die angegebenen Ressourcen um und entfernen Sie nicht unterstützte Zeichen aus ihren Namen. Oder entfernen Sie sie aus Ihrer Sicherungsauswahl.

GVM6120E **Sie haben eine vApp aus einem anderen Organisations-VDC ausgewählt. Für Zurückschreibungstasks müssen alle ausgewählten vApps zu demselben Organisations-VDC gehören. Ändern Sie die ausgewählten Einträge und wiederholen Sie die Operation.**

GVM6121E **Die vApp** *vApp-Name* **ist vorhanden. Wählen Sie einen anderen vApp-Namen als Ziel der Zurückschreibung aus.**

GVM6122E **Aufgrund Ihrer Auswahl der zu sichernden Einträge wurden für die Definition der Sicherungstask** *Anzahl* **Zeichen benötigt. Damit wird der Grenzwert von 512 Zeichen überschritten. Erstellen Sie mehrere Sicherungstasks mit weniger Einträgen pro Task.**

Erläuterung: Die Definition der Sicherungstask hat eine Begrenzung von 512 Zeichen und die Gesamtzahl der Zeichen für die ausgewählten Einträge überschreitet diesen Grenzwert.

Benutzeraktion: Erstellen Sie mehrere Sicherungstasks mit weniger Einträgen pro Task.

GVM6123E **Der Organisations-VDC-Knoten kann nicht eingeschlossen werden, da der zugehörige Provider-VDC-Knoten nicht eingeschlossen ist. Wählen Sie zuerst das Kontrollkästchen 'Einschließen' für den Provider-VDC-Knoten aus und wiederholen Sie dann die Operation.**

GVM6124E **Der Knotenname** *Knotenname* **wird bereits verwendet. Wählen Sie das Kontrollkästchen 'Knoten registrieren' ab oder wählen Sie einen anderen Knotennamen aus.**

Erläuterung: Der ausgewählte Knotenname ist auf dem Server bereits vorhanden. Verzichten Sie auf die Registrierung oder verwenden Sie einen anderen Namen.

Benutzeraktion: Wählen Sie einen anderen Knotennamen aus. Wenn Sie diesen vorhandenen Knoten wiederverwenden wollen, inaktivieren Sie das Kontrollkästchen 'Knoten registrieren'.

GVM6125W **Soll der Knoten der Einheit zum Versetzen von Daten,** *Knotenname***, wirklich entfernt werden?**

GVM6126W **Der IBM Spectrum Protect-Knoten** *Knoten* **wurde bereits verwendet. Wenn Sie einen anderen als den Standardnamen verwenden möchten, editieren Sie dieses Feld noch einmal.**

Erläuterung: Der Knoten wird bereits in dieser Konfiguration verwendet.

Benutzeraktion: Verwenden Sie einen anderen Knotennamen.

GVM6127E **Der Organisations-VDC-Knoten kann nicht registriert werden, da das zugehörige Provider-VDC nicht gültig ist.**

GVM6128E **Der Organisations-VDC-Name** *OVDC-Name* **ist ungültig. Informationen zu unterstützten Zeichen finden Sie im IBM Spectrum Protect-Referenzhandbuch für Administratoren im Abschnitt zur Benennung von IBM Spectrum Protect-Objekten.**

GVM6129I **Diese Task wurde übersprungen, weil sie nicht notwendig war. Es ist keine weitere Aktion erforderlich.**

GVM6130W **Die Internet Explorer-Version** *Version* **wird nicht unterstützt; verwenden Sie eine unterstützte Version oder einen anderen Browser. Möglicherweise treten Probleme bei Darstellung und Funktion auf, wenn Sie diesen nicht unterstützten Browser weiterhin verwenden.**

Erläuterung: Aufgrund von Unterschieden bei der Internet Explorer-Implementierung je nach Versionsnummer werden nur bestimmte Versionen unterstützt. Die Verwendung eines auf Standards basierenden Browsers wie Mozilla Firefox wird empfohlen. Wenn Sie jedoch vom vSphere-Client aus auf die GUI als Plug-in zugreifen, können Sie nur den Internet Explorer-Browser verwenden, der auf dem System mit der vSphere-Client-Installation installiert ist.

Benutzeraktion: Verwenden Sie eine unterstützte Version von Internet Explorer oder einen anderen Browser. Die unterstützten Browserversionen sind in der Onlinehilfe dokumentiert.

GVM6131W **Der Browser *Version* wird nicht unterstützt; verwenden Sie einen unterstützten Browser. Möglicherweise treten Probleme bei Darstellung und Funktion auf, wenn Sie diesen nicht unterstützten Browser weiterhin verwenden.**

Erläuterung: Aufgrund von Unterschieden bei Browserimplementierungen werden nur bestimmte Versionen unterstützt.

Benutzeraktion: Verwenden Sie einen unterstützten Browser. Die unterstützten Browserversionen sind in der Onlinehilfe dokumentiert.

GVM6132E **Mindestens eine der virtuellen Maschinen, die Sie für die Zurückschreibung an eine alternative Position ausgewählt haben, ist bereits im Datencenter vorhanden. Daher ist die Zurückschreibung nicht zulässig. Soll die Zurückschreibung an eine alternative Position erfolgen, wenn die virtuelle Zielmaschine bereits vorhanden ist, wählen Sie nur eine virtuelle Maschine für die Zurückschreibungsoperation aus und wählen Sie einen neuen Namen für die virtuelle Zielmaschine aus. Doppelte VM:** *VM-Name*

Erläuterung: Bei der Zurückschreibung an eine alternative Position darf die virtuelle Zielmaschine noch nicht vorhanden sein.

Benutzeraktion: Verwenden Sie den Assistenten für die Zurückschreibung einzelner virtueller Maschinen, damit Sie die virtuelle Zielmaschine umbenennen können.

GVM6133W **Zieldatenspeicher nicht gefunden; wählen Sie einen anderen Zieldatenspeicher aus.**

GVM6134E **Der Benutzer *Benutzername* ist für keines der verwalteten Datencenter berechtigt. Wenden Sie sich an Ihren Systemadministrator.**

GVM6135E **Sie haben nicht die erforderlichen Berechtigungen zum Anzeigen virtueller Maschinen für dieses Ereignis.**

GVM6136E **Sie haben nicht die erforderlichen Berechtigungen zum Anzeigen von Zurückschreibungspunkten für diese virtuelle Maschine.**

GVM6137E **Sie haben nicht die erforderlichen Berechtigungen zum Anzeigen einiger zugeordneter Punkte.**

GVM6138E **Sie haben nicht die erforderlichen Berechtigungen zum Anzeigen von Zurückschreibungspunkten für diesen Datenspeicher.**

GVM6139E **Sie haben nicht die erforderlichen Berechtigungen zum Aufheben der Zuordnung für den Zurückschreibungspunkt.**

GVM6140E **Bei der Verarbeitung von Benutzerberechtigungen ist ein Fehler aufgetreten. Wenden Sie sich an Ihren Systemadministrator.**

GVM6141I **Einige Datencenter werden aufgrund von Berechtigungsanforderungen nicht angezeigt.**

GVM6142E **Sie haben keine Berechtigungen zum Abbrechen dieser Task.**

GVM6143I **Die Task befindet sich noch im Anfangszustand; aktualisieren Sie die Task und wiederholen Sie den Abbruch.**

GVM6147I **Einige Datencenter sind nicht verfügbar, weil mindestens ein anderes Datencenter denselben Namen hat. Mehrere Datencenter mit demselben Namen werden nicht unterstützt.**

GVM6148E **Die Berechtigungsnachweise für die Windows-Domäne sind falsch. Öffnen Sie den Konfigurationsassistenten, rufen Sie die Seite 'Dateizurückschreibung' auf und geben Sie die Berechtigungsnachweise erneut ein.**

Erläuterung: Die Berechtigungsnachweise für die Windows-Domäne, die auf der Seite 'Dateizurückschreibung' im Konfigurationsassistenten eingegeben wurden, sind falsch.

Systemaktion: Die Verarbeitung wird gestoppt.

Benutzeraktion: Führen Sie den Konfigurationsassistenten erneut aus und geben Sie die korrekten Berechtigungsnachweise für die Windows-Domäne ein.

GVM6149E **Diese Aktion kann nicht ausgeführt werden, da kein VMCLI-Knoten definiert ist. Zum Beheben des Fehlers verwenden Sie den Konfigurationsassistenten, um den VMCLI-Knoten zu definieren und die anderen Schritte im Assistenten durchzuführen.**

GVM6150E **Diese Aktion kann nicht ausgeführt werden, da kein vCloud Director-Knoten definiert ist. Zum Beheben des Fehlers verwenden Sie den Konfigurationsassistenten, um den vCloud Director-Knoten zu definieren und die anderen Schritte im Assistenten durchzuführen.**

GVM6151E **Diese Aktion kann nicht ausgeführt werden, da die Verbindung zu dem IBM Spectrum Protect-Server nicht betriebsbereit ist. Beheben Sie das Verbindungsproblem und wiederholen Sie diese Aktion.**

GVM6152E **Diese Task erfordert die Verwendung des Provider-VDC-Knotens** *Name des Provider-VDC-Knotens* **in IBM Spectrum Protect, aber dieser Knoten ist im vCloud Director keinem bekannten Provider-VDC zugeordnet.**
Diese Task darf nicht aktualisiert werden. Erstellen Sie stattdessen eine neue Task ohne Abhängigkeit von diesem Provider-VDC.

GVM6153E **Die unten aufgelisteten Organisations-VDCs wurden ausgewählt, sind jedoch nicht für den IBM Spectrum Protect-Server konfiguriert. Sie müssen diese ausgewählten Einträge entfernen, um diese Aktion ausführen zu können.**
Org.-VDC-Name

GVM6154I **Ihre aktuelle Rolle in der Benutzerschnittstelle erlaubt nicht das Anzeigen von Knotendetails.**

GVM6155E **Beim Herstellen der Verbindung zu dem IBM Spectrum Protect-Server** *Servername* **ist ein Fehler aufgetreten. Entweder ist Ihre Administrator-ID bzw. Ihr Kennwort nicht gültig oder die TCPPORT-Nummer wurde statt der TCPADMINPORT- oder SSLTCPADMINPORT-Nummer im Feld für den Administratorport eingegeben.**

Erläuterung: Siehe Nachricht.

Benutzeraktion: Starten Sie den Konfigurationseditor über die Registerkarte 'Konfiguration' und geben Sie eine gültige ID oder ein gültiges Kennwort für Ihren IBM Spectrum Protect-Server ein.

GVM6156E **Das Kennwort für die Benutzer-ID mit Administratorberechtigung** *Administrator-ID* **ist auf dem IBM Spectrum Protect-Server** *Servername* **abgelaufen.**

Erläuterung: Ihr IBM Spectrum Protect-Administratorkennwort ist abgelaufen.

Benutzeraktion: Bitten Sie Ihren IBM Spectrum Protect-Serveradministrator, das Kennwort für die Benutzer-ID mit Administratorberechtigung zurückzusetzen.

GVM6157E **Die Portnummer für den IBM Spectrum Protect-Server,** *TCP-Port***, ist falsch. Der erwartete Wert für diesen Port ist** *TCP-Port aus Abfrage***, der Wert der Option TCPPORT. Verwenden Sie den Konfigurationsassistenten, um den erwarteten Wert einzugeben.**

Erläuterung: Der Wert, der in das Feld für den IBM Spectrum Protect-Serverport eingegeben wird, muss mit der Option TCPPORT auf dem IBM Spectrum Protect-Server übereinstimmen.

Benutzeraktion: Verwenden Sie den Konfigurationsassistenten, um im Feld für den IBM Spectrum Protect-Serverport den korrekten Wert anzugeben.

GVM6159E **Bei der Verarbeitung eines VMCLI-Befehls ist ein Fehler aufgetreten und die Sitzung mit der grafischen Benutzerschnittstelle wird geschlossen. Melden Sie sich erneut an und wiederholen Sie die Operation. Bleibt der Fehler bestehen, wenden Sie sich an Ihren Administrator.**

GVM6160E **Beim Schreiben in die Konfigurationsdatei frConfig.props ist ein Fehler aufgetreten.**

Erläuterung: Die Datei frConfig.props enthält Konfigurationsoptionen für die Verarbeitung der Zurückschreibung auf Dateiebene. Mögliche Ursachen für diesen Fehler sind u. a. die folgenden Situationen:

- Die Datei frConfig.props befindet sich nicht im Data Protection for Virtual Environments-Installationsverzeichnis.
- Die Datei frConfig.props file ist schreibgeschützt.

Systemaktion: Die Verarbeitung wird gestoppt.

Benutzeraktion: Stellen Sie sicher, dass die Datei im Data Protection for Virtual Environments-Installationsverzeichnis vorhanden und nicht schreibgeschützt ist.

GVM6161E Das lokale Mount-Proxy-Knotenpaar kann nicht entfernt werden, während das Feature für Zurückschreibung auf Dateiebene aktiviert ist.

Erläuterung: Für die Verarbeitung der Zurückschreibung auf Dateiebene ist ein lokaler Mount-Proxy-Knoten erforderlich.

Benutzeraktion: Inaktivieren Sie das Feature für Zurückschreibung auf Dateiebene. Anschließend können Sie das Mount-Proxy-Knotenpaar bei Bedarf entfernen.

GVM6162E Beim Lesen der Konfigurationsdatei frConfig.props ist ein Fehler aufgetreten.

Erläuterung: Die Datei frConfig.props enthält Konfigurationsoptionen für die Verarbeitung der Zurückschreibung auf Dateiebene. Die Datei kann nicht gelesen werden. Eine häufige Ursache für diesen Fehler ist, dass die Datei lesegeschützt ist.

Systemaktion: Die Verarbeitung wird gestoppt.

Benutzeraktion: Stellen Sie sicher, dass die Datei nicht lesegeschützt ist.

GVM6164W Die Verbindung zum IBM Spectrum Protect-Server war nicht erfolgreich, weil ein Sicherheitszertifikat erforderlich ist.

Erläuterung: Für sichere Verbindungen zum IBM Spectrum Protect-Server muss die Verbindung mit einem SSL-Zertifikat hergestellt werden. Für den ausgewählten IBM Spectrum Protect-Server wurde kein Zertifikat gefunden.

Benutzeraktion: Wurde diese Nachricht nicht bei Verwendung des Konfigurationsassistenten angezeigt, muss das Zertifikat abgerufen und mithilfe der im Hilfetext dokumentierten Prozedur muss ein Truststore erstellt werden.

GVM6165E Der angegebene Zielknoten '*Knotenname*' entspricht nicht dem in der Benutzersitzung gespeicherten Knoten '*Knotenname*'.

Erläuterung: Der Eingabezielknoten für die Konfigurationshostoperation entspricht nicht dem in der verbundenen Sitzung gespeicherten Zielknoten.

Benutzeraktion: Wiederholen Sie die Operation mit dem korrekten Zielknotennamen.

GVM6166E Eine Benutzersitzung ist ungültig oder kein zu akzeptierendes SSL-Zertifikat.

Erläuterung: Die einleitende IBM Spectrum Protect-Serververbindung stellt fest, dass ein SSL-Zertifikat benötigt wird und dass die Operation mit derselben Verbindung erneut aufgerufen werden muss. In diesem Fall ist die Verbindung null oder ungültig.

Benutzeraktion: Stellen Sie sicher, dass der zweite Operationsaufruf zum Akzeptieren des Zertifikats dieselbe einleitende Verbindung verwendet.

GVM6167E Ein Windows-Mount-Proxy-Knoten und ein Linux-Mount-Proxy-Knoten sind zur Aktivierung der Dateizurückschreibung erforderlich.

Erläuterung: Für die Hostkonfigurationsoperation wurde entweder nur ein Mount-Proxy-Knoten oder kein Proxy-Knoten angegeben.

Benutzeraktion: Wiederholen Sie die Operation mit einer Knotenliste, die einen Windows-Mount-Proxy-Knoten und einen Linux-Mount-Proxy-Knoten enthält.

GVM6168E Hostkonfiguration fehlgeschlagen. Weitere Informationen finden Sie in der Taskliste.

Erläuterung: Die Konfiguration des Hosts besteht aus den folgenden Tasks: Zielknoten registrieren, Einheit zum Versetzen von Daten registrieren und Services für Sicherung und Zurückschreibung erstellen, Mount-Proxy-Knoten registrieren und Services für Zurückschreibung auf Dateibene erstellen. Bei einer dieser Tasks ist ein Fehler aufgetreten.

Benutzeraktion: Beheben Sie den Fehler und wiederholen Sie die Operation.

GVM6169E Unerwarteter Fehler während der Konfiguration auf dem IBM Spectrum Protect-Server aufgetreten.

Erläuterung: Mögliche Ursachen für diesen Fehler sind u. a. die folgenden Situationen:

- Unbekannter Fehler während des Herstellens der Verbindung zum IBM Spectrum Protect-Server aufgetreten.
- Unbekannter Fehler während des Schreibens in die Datenbankdatei des Servers (tsmserver.props) aufgetreten.

Benutzeraktion: Überprüfen Sie die Netzverbindung mit der IBM Spectrum Protect-Servermaschine. Stellen Sie sicher, dass der Server aktiv ist, und melden Sie sich erneut an. Überprüfen Sie außerdem, ob die Informationen zum Server-Port korrekt sind.

GVM6170E Unerwarteter Fehler: Maßnahmendomäne für Knoten '*Knotenname*' kann nicht abgerufen werden.

Erläuterung: Der Zielknoten ist auf dem IBM Spectrum Protect-Server nicht vorhanden oder während der Knotenabfrage ist ein interner Fehler aufgetreten.

Benutzeraktion: Führen Sie den Konfigurationsassistenten aus, um den Zielknoten zu registrieren, oder ak-

tualisieren Sie den Knoten mit einer anderen Maßnahmendomäne.

GVM6171E Unerwarteter Fehler: Zeitplan '*Zeitplanname*' ist auf dem IBM Spectrum Protect-Server nicht vorhanden.

Erläuterung: Der Zeitplan wurde möglicherweise während der Operation versehentlich gelöscht.

Benutzeraktion: Wählen Sie einen anderen Zeitplan aus.

GVM6172E '*Domänenname*' ist keine gültige Windows-Domäne.

Erläuterung: LOCALHOST oder der Computername sind keine gültigen Domänen.

Benutzeraktion: Geben Sie eine gültige Domäne ein.

GVM6173E Die Domäne fehlt im Benutzernamen.

Erläuterung: Der von Ihnen eingegebene Benutzername gehört zu keiner Domäne.

Benutzeraktion: Stellen Sie sicher, dass der Benutzername das Format DOMAIN\UserName hat.

GVM6174E Die folgenden Adressen können nicht erreicht werden: *HTTP-URL*, *HTTPS-URL*. Überprüfen Sie, ob der TSM-Clientakzeptor (CAD) betriebsbereit ist.

Erläuterung: Der CAD-Service ist für die Einheit zum Versetzen von Daten nicht aktiv.

Systemaktion: Die Operation kann ohne eine Verbindung zum CAD-Service der Einheit zum Versetzen von Daten nicht fortgesetzt werden.

Benutzeraktion: Stellen Sie sicher, dass der CAD-Service der Einheit zum Versetzen von Daten aktiv ist und dass auf dem Knoten die richtigen Proxy-Beziehungen eingerichtet sind.

GVM6175E Der TCP-Port aus der HTTP-Antwort kann nicht abgerufen werden. Überprüfen Sie, ob der TSM-Clientakzeptor (CAD) betriebsbereit ist.

Erläuterung: Der CAD-Service ist für die Einheit zum Versetzen von Daten nicht aktiv.

Systemaktion: Die Operation kann ohne eine Verbindung zum CAD-Service der Einheit zum Versetzen von Daten nicht fortgesetzt werden.

Benutzeraktion: Stellen Sie sicher, dass der CAD-Service der Einheit zum Versetzen von Daten aktiv ist und dass auf dem Knoten die richtigen Proxy-Beziehungen eingerichtet sind.

GVM6176E Der TCP-Port aus der HTTP-Antwort kann nicht geparst oder gefunden werden.

Erläuterung: Der HTTP-Datenstrom vom Agenten enthält nicht die TCP-Portnummer.

Systemaktion: Die Operation kann ohne eine Verbindung zum CAD-Service der Einheit zum Versetzen von Daten nicht fortgesetzt werden.

Benutzeraktion: Stellen Sie sicher, dass der CAD-Service der Einheit zum Versetzen von Daten aktiv ist und dass auf dem Knoten die richtigen Proxy-Beziehungen eingerichtet sind.

GVM6177E Beim Parsing der Zeichenfolge für den TCP-Port ist eine Ausnahme aufgetreten: *TCP-Port*.

Erläuterung: Der HTTP-Datenstrom vom Agenten hat eine ungültige TCP-Portnummer zurückgegeben.

Systemaktion: Die Operation kann ohne eine Verbindung zum CAD-Service der Einheit zum Versetzen von Daten nicht fortgesetzt werden.

Benutzeraktion: Stellen Sie sicher, dass der CAD-Service der Einheit zum Versetzen von Daten aktiv ist und dass auf dem Knoten die richtigen Proxy-Beziehungen eingerichtet sind.

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 Verordnungen, 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

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Programmnummer: 5725-X00

Gedruckt in Deutschland