Administrationshandbuch für vSphere Data Protection

vSphere Data Protection 6.1

Dieses Dokument unterstützt die Version sämtlicher darin aufgeführter Produkte sowie alle nachfolgenden Versionen, bis es durch eine neue Ausgabe ersetzt wird. Auf http://www.vmware.com/de/support/pubs können Sie überprüfen, ob neuere Ausgaben dieses Dokuments vorhanden sind.

EN-001795-00

vmware®

Die aktuelle technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support

Auf der VMware-Website finden sich auch die neuesten Produktupdates.

Sollten Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihr Feedback an:

docfeedback@vmware.com

Copyright © 2007 – 2015 VMware, Inc. Alle Rechte vorbehalten. Das geistige Eigentum und das Urheberrecht an diesem Produkt sind durch US-amerikanische und internationale Gesetze geschützt. VMware-Produkte sind durch ein oder mehrere Patente geschützt, die auf der folgenden Seite aufgeführt sind: http://www.vmware.com/de/go/patents.

VMware ist in den USA und/oder in anderen Ländern eine eingetragene Marke oder Marke von VMware, Inc. Alle anderen hierin aufgeführten Marken und Namen können Marken der jeweiligen Unternehmen sein.

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim / Lohhof
Tel: +49 89 3706 17000
Fax: +49 89 3706 17333
www.vmware.com/de

Inhalt

Informationen über dieses Handbuch

Das *Administratorhandbuch für vSphere Data Protection* beschreibt die Installation und das Management von Backups für kleine und mittelständische Unternehmen. Dieses Handbuch umfasst zudem Troubleshooting-Szenarios und Lösungsempfehlungen.

Zielgruppe

Dieses Handbuch richtet sich an Benutzer, die Backuplösungen mithilfe von vSphere® Data Protection (VDP) bereitstellen möchten. Die hierin enthaltenen Informationen sind für erfahrene Windows- oder Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und den Vorgängen von Rechenzentren vertraut sind.

Typographische Konventionen

VMware verwendet in diesem Dokument folgende typographische Konventionen:

Fettschrift	Für Bezeichnungen von Benutzeroberflächenelementen wie Bezeichnungen von Fenstern, Dialogfeldern, Schaltflächen, Feldern, Registerkarten, Schlüsselnamen und Menüpfaden (die vom Benutzer speziell ausgewählt oder angeklickt werden)
Kursiv	Für vollständige Publikationstitel, auf die im Text Bezug genommen wird
`Monospace-Schrift`	Verwendet für: ■ Systemausgaben (z. B. Fehlermeldungen und Skripte) ■ Systemcode ■ Pfad- und Dateinamen, Aufforderungen und Syntax ■ Befehle und Optionen
`Kursive Monospace-Schrift`	Für Variablen
`Fette Monospace-Schrift`	Für Benutzereingaben
[ ]	Eckige Klammern schließen optionale Werte ein.
|	Senkrechte Striche kennzeichnen alternative Möglichkeiten, d. h. **oder** .
{ }	Geschweifte Klammern schließen Inhalte ein, die der Benutzer angeben muss (x oder y oder z).
...	Auslassungspunkte verweisen auf unwichtige Informationen, die im Beispiel ausgelassen wurden.

VMware Technical Publications-Glossar

VMware Technical Publications stellt ein Glossar mit Begriffen zur Verfügung, die Ihnen möglicherweise nicht vertraut sind. Definitionen von Begriffen, wie sie in der technischen Dokumentation von VMware genutzt werden, finden Sie unter http://www.vmware.com/de/support/pubs.

Feedback zur Dokumentation

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Senden Sie Ihr Feedback an docfeedback@vmware.com.

Technischer Support und Schulungsressourcen

In den folgenden Abschnitten werden die für den technischen Support verfügbaren Ressourcen beschrieben. Die aktuellen Versionen weiterer VMware-Handbücher finden Sie unter http://www.vmware.com/de/support/pubs.

Online Support

Onlinesupport zur Anforderung technischer Unterstützung, zum Abruf Ihrer Produkt- und Vertragsdaten und zur Registrierung Ihrer Produkte finden Sie unter http://www.vmware/de/support/phone_support.html.

Supportangebote

VMware stellt ein umfangreiches Supportangebot bereit, um Ihre geschäftlichen Anforderungen zu erfüllen. Weitere Informationen finden Sie unter http://www.vmware.com/de/support/services.

VMware Professional Services

Die VMware Education Services-Kurse bieten umfangreiche Praxisübungen, Beispiele von Fallstudien und Kursmaterialien, die zur Verwendung als Referenztools bei der praktischen Arbeit vorgesehen sind. Kurse können vor Ort, im Unterrichtsraum und live online durchgeführt werden. Für Pilotprogramme vor Ort und die Implementierung von Best Practices unterstützt VMware Consulting Services Sie beim Bewerten, Planen, Erstellen und Managen Ihrer virtuellen Umgebung. Informationen zu Schulungen, Zertifizierungsprogrammen und Consulting Services finden Sie unter http://www.vmware.com/de/services.

Wissenswertes über vSphere Data Protection

1

In diesem Kapitel werden folgende Themen behandelt:

Einführung in vSphere Data Protection

vSphere Data Protection (VDP) ist eine robuste, einfach bereitzustellende, festplattenbasierte Backup- und Recovery-Lösung, die von EMC betrieben wird. VDP ist vollständig in VMware vCenter Server integriert und ermöglicht beim Speichern von Backups in deduplizierten Zielspeicherorten ein zentrales und effizientes Management von Backupjobs.

Die VMware vSphere Web Client-Schnittstelle wird zum Auswählen, Planen, Konfigurieren und Managen von Backups und Recoveries virtueller Maschinen verwendet.

Während eines Backups erstellt VDP einen stillgelegten Snapshot der virtuellen Maschine. Die Deduplizierung wird automatisch bei jedem Backupvorgang durchgeführt.

Die folgenden Begriffe werden im Kontext von Backup und Recovery in der gesamten vorliegenden Dokumentation verwendet.

- Ein **Datenspeicher** ist eine virtuelle Darstellung einer Kombination von zugrunde liegenden physischen Speicherressourcen im Rechenzentrum. Ein Datenspeicher ist der Speicherort (z. B. ein physisches Laufwerk, ein RAID oder SAN) für VM-Dateien.
- **Changed Block Tracking (CBT)**ist eine VMkernel-Funktion, die die Speicherblöcke virtueller Maschinen und ihre Änderungen im Laufe der Zeit nachverfolgt. Der VMkernel verfolgt Blockänderungen auf virtuellen Maschinen nach, was zu einer Verbesserung des Backupprozesses für VMware vStorage API-fähige Anwendungen führt.
- **Recovery auf Dateiebene** (File Level Recovery, FLR) ermöglicht lokalen Administratoren von geschützten virtuellen Maschinen, Backups für den lokalen Rechner zu durchsuchen und zu mounten. Ausgehend von diesen gemounteten Backups kann der Administrator dann einzelne Dateien wiederherstellen. Die Recovery auf Dateiebene wird mithilfe des VDP-Wiederherstellungsclients durchgesetzt.
- **VMware vStorage APIs for Data Protection (VADP)** ermöglicht, dass Backupsoftware zentralisierte Backups der virtuellen Maschine ohne Unterbrechung und Overhead durch laufende Backupaufgaben innerhalb jeder virtuellen Maschine durchführen kann.
- **Virtual Machine Disk (VMDK)** ist eine Datei oder ein Satz von Dateien, die bzw. der einem Gastbetriebssystem als physisches Laufwerk angezeigt wird. Diese Dateien können auf dem Hostrechner oder einem Remotedateisystem liegen.
- **Die VDP-Appliance** ist eine speziell entwickelte virtuelle Appliance für VDP.

Vorteile von VDP

vSphere Data Protection (VDP) bietet folgende Vorteile:

- Schnelle und effiziente Datensicherheit für alle virtuellen Maschinen, selbst für ausgeschaltete oder zwischen vSphere-Hosts migrierte virtuelle Maschinen
- Deutliche Reduzierung des durch Backupdaten belegten Festplattenspeichers durch patentierte Technologie zur Deduplizierung mit variabler Länge bei allen Backups
- Senkung der Kosten für das Backup virtueller Maschinen und Minimierung des Backupzeitfensters durch Changed Block Tracking (CBT) und Snapshots virtueller VMware-Maschinen
- Einfache Backups ohne die Installation von Drittanbieter-Agents auf jeder virtuellen Maschine
- Einfache geradlinige Installation als integrierte Komponente innerhalb von vSphere, die über ein Webportal gemanagt werden kann
- Direkter Zugriff auf die in vSphere Web Client integrierte VDP-Konfiguration
- Schutz von Backups mit Kontrollpunkt- und Rollbackmechanismus
- Vereinfachte Recovery von Windows- und Linux-Dateien mit vom Anwender initiierten Recoveries auf Dateiebene von einer webbasierten Schnittstelle aus

- Durch die Verwendung einer Notfallwiederherstellung bietet VDP eine Methode zur Wiederherstellung virtueller Maschinen, wenn vCenter Server nicht verfügbar ist oder der Benutzer über vSphere Web Client nicht auf die VDP-Benutzeroberfläche zugreifen kann.
- Durch Replikation können Sie einen Datenverlust bei einem Ausfall der VDP-Quell-Appliance vermeiden, weil Backupkopien auf einem Ziel verfügbar sind.
- Vorteile des Deduplizierungsspeichers

  Unternehmensdaten sind äußerst redundant. Dabei sind identische Dateien oder Daten innerhalb und über Systeme hinweg gespeichert (z. B. Betriebssystemdateien oder an mehrere Empfänger gesendete Dokumente). Bearbeitete Dateien weisen ebenfalls eine enorme Redundanz zu früheren Versionen auf. Herkömmliche Backupmethoden verstärken dies, da alle redundanten Daten immer wieder gespeichert werden. vSphere Data Protection nutzt patentierte Deduplizierungstechnologie zur Beseitigung von Redundanz auf Datei- und Subdatei-Datensegmentebene.
- Datensegmente mit variabler und fester Länge

  Ein Schlüsselfaktor bei der Beseitigung redundanter Daten auf Segment- (oder Subdatei-)Ebene ist die zum Ermitteln der Segmentgröße eingesetzte Methode. Segmente fester Blockgröße oder fester Länge werden im Allgemeinen von Snapshots und einigen Deduplizierungstechnologien genutzt. Leider können selbst durch geringfügige Änderungen am Dataset (z. B. das Einfügen von Daten am Dateianfang) alle Segmente fester Länge im Dataset geändert werden. vSphere Data Protection setzt eine intelligente Methode variabler Länge zur Ermittlung der Segmentgröße ein. Dabei werden die Daten zur Bestimmung logischer Grenzpunkte untersucht und die Effizienz erhöht.
- Ermittlung logischer Segmente

  VDP verwendet eine patentierte Methode zur Ermittlung der Segmentgröße, die darauf ausgelegt ist, systemübergreifend für optimale Effizienz zu sorgen. Mit dem VDP-Algorithmus wird die Binärstruktur eines Dataset analysiert, um die kontextabhängigen Segmentgrenzen zu bestimmen. Segmente variabler Länge sind im Durchschnitt 24 KB groß und werden durchschnittlich auf 12 KB komprimiert. Durch Analyse der Binärstruktur innerhalb der VMDK-Datei kann VDP für alle Dateitypen und -größen verwendet werden und sorgt für eine Deduplizierung der Daten.

VDP-Funktionen

Das Produkt vSphere Data Protection umfasst ab Version 6.0 alle Funktionen, die zuvor in VDP Advanced enthalten waren. Die VDP-Funktionen sind in vSphere Essentials Plus enthalten und ein spezieller Lizenzschlüssel ist nicht erforderlich. In der folgenden Tabelle werden VDP-Funktionen aufgeführt.

Tabelle 1-1. VDP-Funktionen

Komponente	VDP
Pro VDP-Appliance unterstützte virtuelle Maschinen	Bis zu 400
Anzahl der pro vCenter unterstützten Appliances	Bis zu 20
Größe des verfügbaren Speichers	0,5 TB, 1 TB, 2 TB, 4 TB und 8 TB
Unterstützung für Backups auf Image-Ebene	Ja
Unterstützung für Backups einzelner Festplatten	Ja
Unterstützung für Wiederherstellungsjobs auf Image-Ebene	Ja
Unterstützung für Replikationsjobs auf Image-Ebene	Ja
Unterstützung für direkte Recovery auf dem Host	Ja
Unterstützung für trennbare/erneut mountbare Datenpartitionen	Ja
Unterstützung für Recovery auf Dateiebene (File Level Recovery, FLR)	Ja, unterstützt LVM und EXT4 mit externen Proxys

Tabelle 1-1. VDP-Funktionen (Fortsetzung)

Komponente	VDP
Unterstützung für Backups auf Gastebene und Wiederherstellungen von Exchange Server-, SQL Server- und SharePoint Server-Rechnern	Ja
Unterstützung für Replikationen auf Anwendungsebene	Ja
Unterstützung für Backups direkt auf ein Data Domain-System	Ja
Fähigkeit zur Wiederherstellung auf granularem Level auf Microsoft-Servern	Ja
Unterstützung für automatische Backupverifizierung (ABV)	Ja
Unterstützung für externe Proxys	Ja (bis zu 24 virtuelle Maschinen gleichzeitig bei Bereitstellung der maximalen Anzahl von 8 externen Proxys)
Unterstützung für Customer Experience Improvement Program	Ja

Backups und Wiederherstellungen auf Image-Ebene

vSphere Data Protection erstellt Backups auf Image-Ebene, die in vStorage API for Data Protection (VADP) integriert sind, einer in vSphere festgelegten Funktion zum Offload des Backupverarbeitungsoverheads von der virtuellen Maschine auf die VDP-Appliance. Die VDP-Appliance kommuniziert mit vCenter Server, um einen Snapshot der .vmdk-Dateien einer virtuellen Maschine zu erstellen. Die Deduplizierung findet innerhalb der Appliance mithilfe patentierter Technologie zur Deduplizierung mit variabler Länge statt.

Zur Unterstützung des großen Umfangs und ständigen Wachstums vieler VMware-Umgebungen kann jede VDP-Appliance bis zu 8 virtuelle Maschinen gleichzeitig sichern, wenn der interne Proxy verwendet wird. Sie kann bis zu 24 virtuelle Maschinen gleichzeitig sichern, wenn die maximale Anzahl von 8 externen Proxys bei einer VDP-Appliance bereitgestellt ist.

Um eine höhere Effizienz bei Backups auf Image-Ebene zu erzielen, nutzt VDP die Changed Block Tracking(CBT)-Funktion. Hierdurch wird das Backupzeitfenster eines bestimmten VM-Image nicht nur deutlich verkürzt, zudem ist es möglich, eine große Anzahl virtueller Maschinen innerhalb eines bestimmten Backupzeitfensters zu verarbeiten.

Durch Nutzung der CBT-Funktion während Wiederherstellungen sorgt VDP für schnelle und effiziente Recoveries virtueller Maschinen an ihrem ursprünglichen Speicherort. Während eines Wiederherstellungsprozesses nutzt VDP die CBT-Funktion, um festzustellen, welche Blöcke seit dem letzten Backup geändert wurden. Durch CBT wird nicht nur die Datenübertragung innerhalb der vSphere-Umgebung während einer Recovery reduziert, sondern vor allem auch die Recovery-Zeit.

Zusätzlich bewertet VDP automatisch die Workload zwischen beiden Wiederherstellungsmethoden (vollständige Image-Wiederherstellung bzw. eine Recovery mit CBT) und setzt die entsprechende Methode um. Das Ergebnis: schnellste Wiederherstellungszeit. Dies ist in Szenarios nützlich, in denen die Änderungsrate seit dem letzten Backup auf einer wiederherzustellenden virtuellen Maschine sehr hoch ist und der Overhead einer CBT-Analyse kostspieliger wäre als eine direkte vollständige Image Recovery. VDP ermittelt, welche Methode zu den kürzesten Image-Recovery-Zeiten für virtuelle Maschinen in der Umgebung führt.

VDP unterstützt Backups von einer vCenter Server Appliance (VCSA) mithilfe eines integrierten Plattform Service Controllers.

Zur Erstellung eines Backups eines vCenter-Servers und einer vCenter Server Appliance (VCSA) mithilfe von externen Platform Services Controllern, führen Sie die in http://kb.vmware.com/kb/2110294 beschriebenen Schritte aus.

Backup und Wiederherstellung nur einer VMDK

Bei einem Backupjob „Vollständige Images“ werden alle Festplatten einer virtuellen Maschine (VM) in einem einzigen Image-Backup zusammengefasst. Backupjobs des Typs „Einzelne Festplatten“ ermöglichen es, nur die benötigten Festplatten auszuwählen. Bei einem Backup auf Image-Ebene einer VM mit nicht unterstützten Festplattentypen sind die nicht unterstützten Festplattentypen aufgrund der Snapshot-Beschränkungen nicht enthalten.

Beim Wiederherstellen einer VM stellt die VDP-Appliance die VM-Konfigurationsdatei (.vmx) wieder her, sodass letztendlich alle VMDKs aus der ursprünglichen VM erstellt werden. Falls ursprüngliche VMDKs nicht gesichert wurden, werden diese beim Wiederherstellungsprozess als provisorische VMDKs erstellt. Die VM ist in diesem Fall möglicherweise nicht voll funktionsfähig. Bei der Wiederherstellung kann jedoch auf die geschützten VMDKs zugegriffen werden.

Anweisungen zum Sichern einzelner Festplatten finden Sie unter „Erstellen eines Backupjobs auf einzelnen Festplatten“ auf Seite 128.

Backups und Wiederherstellungen auf Gastebene

VDP unterstützt Backups auf Gastebene für Microsoft SQL Server-, Exchange Server- und SharePoint Server-Rechner. Bei Backups auf Gastebene werden Client-Agents (VMware VDP for SQL Server Client, VMware VDP for Exchange Server Client oder VMware VDP for SharePoint Server Client) genauso auf den SQL Server-, Exchange Server- oder SharePoint Server-Rechnern installiert, wie Backup-Agents üblicherweise auf physischen Servern installiert werden.

Die Vorteile von VMware-Backups auf Gastebene:

- Zusätzliche Anwendungsunterstützung für Microsoft SQL Server-, Microsoft Exchange Server- oder SharePoint Server-Rechner innerhalb der virtuellen Maschinen
- Unterstützung für Backups und Wiederherstellungen ganzer Microsoft SQL Server-, Microsoft Exchange Server- bzw. SharePoint Server-Rechner oder ausgewählter Datenbanken
- Identische Backupmethoden für physische und virtuelle Maschinen

Zusätzliche Informationen zu Backups und Wiederherstellungen auf Gastebene finden Sie unter „VDP-Anwendungsunterstützung“ auf Seite 175.

Replikation

Durch Replikation können Sie einen Datenverlust bei einem Ausfall der VDP-Quell-Appliance vermeiden, weil Backupkopien auf dem Ziel verfügbar sind.

Replikationsjobs legen fest, welche Backups repliziert sowie wann und wo die Backups repliziert werden. Bei geplant oder ad hoc durchgeführten Replikationsjobs für Clients ohne Wiederherstellungspunkte wird der Client nur auf dem Zielserver repliziert. Mit VDP 6.0 oder höher erstellte Backups können auf eine andere VDP-Appliance, einen EMC Avamar-Server oder ein Data Domain-System repliziert werden. Wenn die VDP-Ziel-Appliance Version 5.8 oder früher ist, muss das Ziel VDP Advanced oder Replication Target Identity sein.

Zusätzliche Informationen zur Replikation finden Sie unter Kapitel 15, „Replikation“, auf Seite 151.

Recovery auf Dateiebene

Die Recovery auf Dateiebene (File Level Recovery, FLR) ermöglicht lokalen Administratoren von geschützten virtuellen Maschinen, Backups für den lokalen Rechner zu durchsuchen und zu mounten. Ausgehend von diesen gemounteten Backups kann der Administrator dann einzelne Dateien wiederherstellen. Die Recovery auf Dateiebene wird mithilfe des VDP-Wiederherstellungsclients durchgesetzt.

Zusätzliche Informationen zu FLR finden Sie unter Kapitel 16, „Verwenden der Wiederherstellung auf Dateiebene“, auf Seite 167.

Customer Experience Improvement Program

Das Customer Experience Improvement Program ist eine Option, die es Ihnen ermöglicht, verschlüsselte Konfigurations- und Nutzungsinformationen zur VDP-Umgebung zwecks Analyse an VMware-Server zu senden. Der Zweck des Customer Experience Improvement Program ist die Verbesserung der Qualität, Zuverlässigkeit und Funktionalität des VDP-Produkts. Standardmäßig ist das Customer Experience Improvement Program nicht aktiviert. Während der Installation können Sie das Customer Experience Improvement Program auf der Seite „Produktverbesserung“ im Dienstprogramm VDP-configure aktivieren. Sie können diese Option nach der Installation von VDP jederzeit in der Benutzeroberfläche aktivieren oder deaktivieren. Weitere Informationen finden Sie unter „Konfigurieren des Customer Experience Improvement Program“ auf Seite 58.

Architektur von VDP

VDP kann in jedem von vSphere unterstützen Speicher bereitgestellt werden. Zu unterstütztem Speicher gehören VMFS-, NFS- und VSAN-Datenspeicher. Das VDP-Management erfolgt mithilfe von vSphere Web Client.

Backupdaten werden dedupliziert und in den .vmdk-Dateien, aus denen sich die virtuelle VDP-Appliance zusammensetzt, oder auf einer unterstützten Data Domain-Appliance gespeichert.

Die folgende Abbildung zeigt die grundlegende Architektur des VDP:

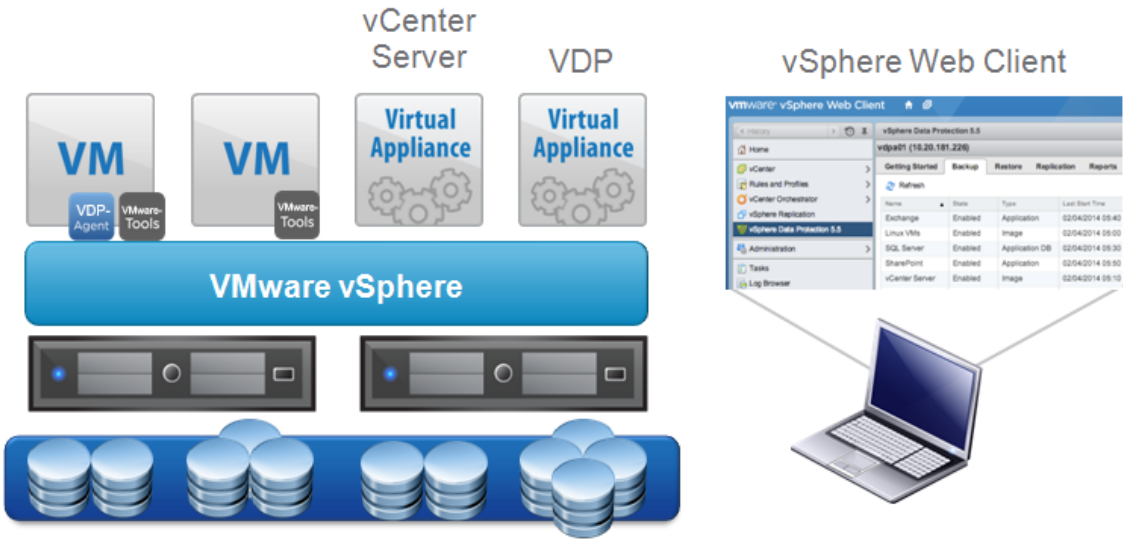


Abbildung 1-1. Allgemeine VDP-Architektur

Die allgemeine VDP-Architektur besteht aus folgenden Komponenten:

- vCenter Server 5.5 oder höher
- Virtuelle VDP-Appliance, die auf einem beliebigen vSphere-Host mit Version 5.1 oder höher installiert ist
- vSphere Web Client
- Anwendungsbackup-Agents

Die folgende Abbildung zeigt die detaillierte Architektur des VDP:

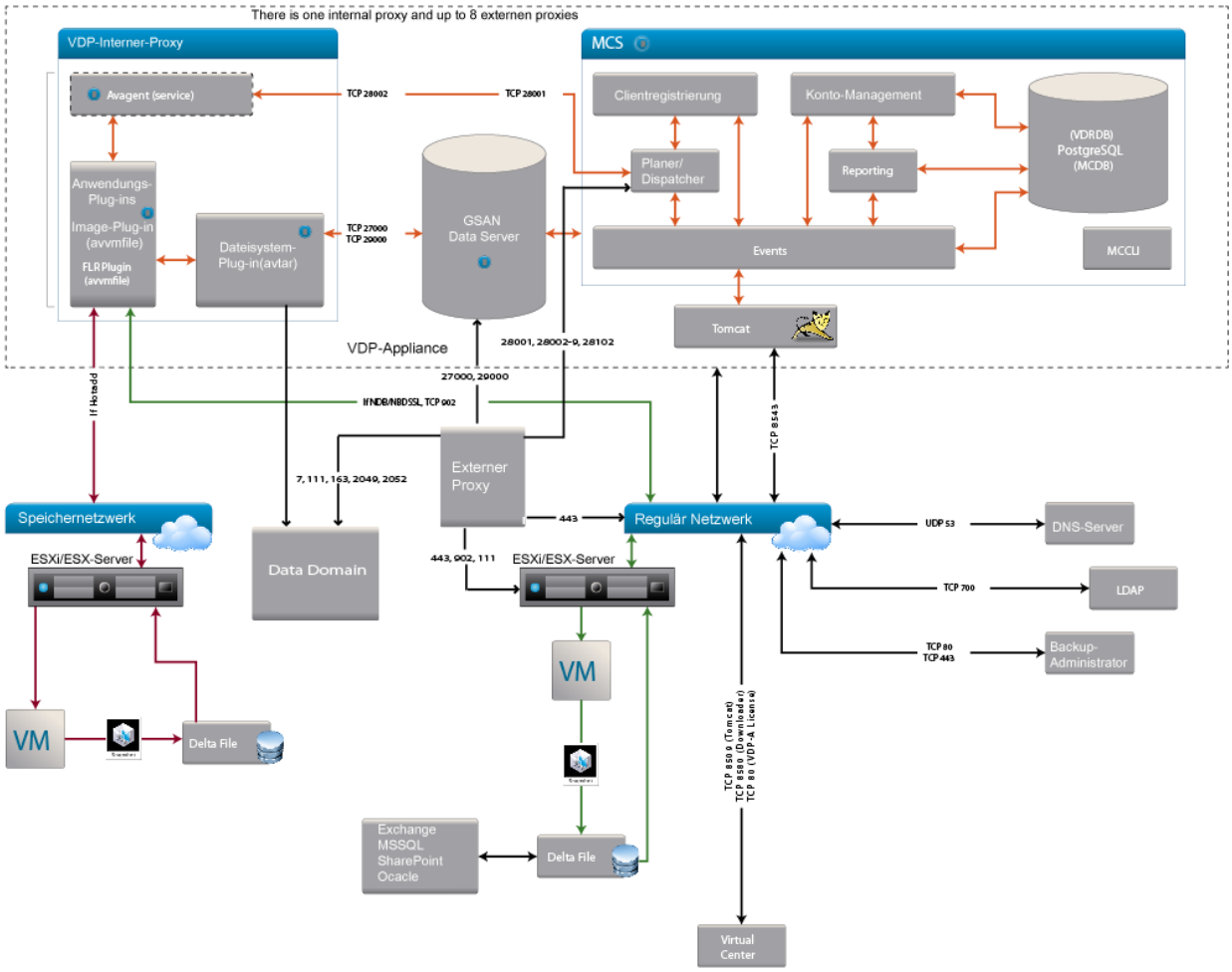


Abbildung 1-2. Detaillierte VDP-Architektur

Die detaillierte VDP-Architektur besteht aus folgenden wichtigen Komponenten:

- **MCS**: Der Management Console Server (MCS) ermöglicht eine zentralisierte Verwaltung, wie die Planung, Überwachung und das Management der VDP-Server. Außerdem betreibt er die vom Administrator verwendeten serverseitigen Prozesse. Die Prozesse umfassen alle Java Prozesse und Postgres (SQL)-Prozesse.

  Die entsprechende Protokolldatei für diese Komponente ist **/usr/local/Avamar/var/MC/server_log/mcserver.log** .

- **AvAgent** : Läuft als Dienst innerhalb der jeweiligen Proxy auf der VDP-Appliance. Er erstellt und pflegt die Kommunikation mit dem MCS. Der AvAgent prüft die MCS-Server alle 15 Sekunden auf eingehende Arbeitsaufträge. Als Reaktion auf einen Arbeitsauftrag, wie ein Backup oder eine Wiederherstellung, bringt der AvAgent das AvVcbImage hervor, welches wiederum AvTar aufruft.

  Die entsprechende Protokolldatei für diese Komponente ist **/usr/local/avamarclient/var-proxy-N/avagent.log** .

- **AvVcbImage** : Ermöglicht das Browsen, Sichern und Wiederherstellen von Dateien und Verzeichnissen auf dem vSphere Virtual Machine File System (VMFS).

  Die entsprechende Protokolldatei für diese Komponente ist **/usr/local/avamarclient/var-proxy-N/<JOBNAME>-<Zeit>-vmimagew.log** .

- **AvTar** : Der primäre Prozess für Sicherungen und Wiederherstellungen. AvTar kommuniziert mit GSAN.

  Die entsprechende Protokolldatei für diese Komponente ist **/usr/local/avamarclient/var-proxy-N/<JOBNAME>-<Zeit>-vmimagew_avtar.log** .

- **GSAN**: Das Global Storage Area Network (GSAN) ist eine Komponente der VDP-Appliance. Es wird auch als Datenserver oder Speicherserver bezeichnet.

  Die entsprechende Protokolldatei für diese Komponente ist **/data01/cur/gsan.log** .

VDP-Installation und -Konfiguration 2

In diesem Kapitel werden folgende Themen behandelt:

vSphere Data Protection-Kapazitätsanforderungen

Die Kapazitätsanforderungen für vSphere Data Protection (VDP) sind von verschiedenen Faktoren abhängig, z. B.:

- Anzahl der geschützten virtuellen Maschinen
- Datenmenge auf jeder geschützten virtuellen Maschine
- Typen der gesicherten Daten (z. B. Betriebssystemdateien, Dokumente und Datenbanken)
- Aufbewahrungsfrist für Backupdaten (täglich, wöchentlich, monatlich oder jährlich)
- Datenänderungsraten

HINWEIS Ausgehend von durchschnittlichen VM-Größen, Datentypen, Datenänderungsraten und einer Aufbewahrungs-Policy von 30 Tagen werden bei einer Kapazität von 1 TB an VDP-Backupdaten ca. 25 virtuelle Maschinen unterstützt.

Softwareanforderungen

Für VDP 6.1 ist folgende Software erforderlich:

- vCenter Server 5.5 oder höher

  VDP 6.1 unterstützt sowohl die Linux-basierte virtuelle vCenter Server-Appliance als auch den Windows-basierten vCenter Server.

- vSphere Web Client

  Unter dem folgenden Link finden Sie Informationen zum aktuellen vSphere-Webbrowsersupport:

  https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.install.doc%2FGUID-F6D456D7-C559-439D-8F34-4FCF533B7B42.html&resultof=%22web%22%20%22client%22

  Webbrowser müssen über Adobe Flash Player ab Version 11.3 verfügen, um auf die Funktionen von vSphere Web Client und VDP zuzugreifen.

- vSphere-Host 5.0 oder höher

Hardwareversionen und Migration

Durch die Hardwareversion der virtuellen Maschine werden virtuelle Maschinen an der Migration auf ältere Versionen, die auf neueren Versionen von vSphere-Hosts konfiguriert sind, gehindert. Wenn die VDP-Appliance zu einem vSphere-Host mit Version 5.1 oder früher migriert wird, ist sie nicht funktionstüchtig.

Kompatibilität und Performance von vSphere-Hosts und vSphere Flash Read Cache

Die VDP-Appliance wird als virtuelle Maschine mit Hardwareversion 7 bereitgestellt, was eine Abwärtskompatibilität mit vSphere 4.x-Hosts ermöglicht. Die von vSphere-Flashlesecache-unterstützten Festplatten sind nur auf vSphere 5.x- und höheren Hosts verfügbar, die erwarten, das eine VM die Hardwareversion 10 oder höher hat. Das Ergebnis ist, dass der Versuch, ein Backup auf Image-Ebene einer von vSphere-Flash-Lesecache-unterstützten Festplatte über die VDP-Appliance durchzuführen, dazu führt, dass die aktuelle Konfiguration die Appliance das NBD-Protokoll (Network Block Device) als Transportmodus verwenden lässt (anstelle von HotAdd), was sich negativ auf die Performance auswirkt.

Nicht unterstützte Festplattentypen

- Achten Sie bei der Backupplanung darauf, dass die Festplatten von VDP unterstützt werden. Momentan werden die folgenden virtuellen Hardware-Festplattentypen nicht von VDP unterstützt:
  - Independent
  - RDM Independent – Virtual Compatibility Mode
  - RDM Physical Compatibility Mode

Nicht unterstützte virtuelle Volumes

Die VDP-Appliance der Version 6.1 unterstützt keine Backups und Wiederherstellungen von virtuellen Maschinen auf virtuellen Volumes (VVOLs).

Systemanforderungen

Im folgenden Abschnitt werden die Systemanforderungen für VDP aufgeführt.

VDP-Systemanforderungen

VDP ist in den folgenden Konfigurationen verfügbar:

- 0,5 TB
- 1 TB
- 2 TB
- 4 TB
- 6 TB
- 8 TB

WICHTIGER HINWEIS Nachdem VDP bereitgestellt wurde, kann die Größe erhöht werden.

VDP stellt die folgenden minimalen Systemanforderungen:

Tabelle 2-2. Minimale Systemanforderungen für VDP

	0,5 TB	1 TB	2 TB	4 TB	6 TB	8 TB
Prozessoren	Mindestens vier 2-GHz-Prozessoren	Mindestens vier 2-GHz-Prozessoren	Mindestens vier 2-GHz-Prozessoren	Mindestens vier 2-GHz-Prozessoren	Mindestens vier 2-GHz-Prozessoren	Mindestens vier 2-GHz-Prozessoren
Speicher	4 GB	4 GB	4 GB	8 GB	10 GB	12 GB
Festplattenspeicher	873 GB	1.600 GB	3 TB	6 TB	9 TB	12 TB

IPv6-Anforderungen

DNS-Server, die VDP in einer IPv6-Umgebung verwenden, dürfen nur AAAA-Datensätze für Hostnamen enthalten. Der DNS-Server darf weder einen A- noch einen AAAA-Datensatz mit demselben Hostnamen enthalten.

Konfiguration vor der Installation

Vor der VDP-Installation müssen die folgenden vor der Installation abzuschließenden Schritte durchgeführt werden:

DNS-Konfiguration

Der DNS-Server muss in VDP und vCenter Vorwärts- und Rückwärtssuche (Forward und Reverse Lookup) unterstützen.

Bevor VDP bereitgestellt wird, muss dem DNS-Server für die IP-Adresse und die vollständig qualifizierten Domainnamen (Fully Qualified Domain Names, FQDN) der VDP-Appliance ein Eintrag hinzugefügt werden. Darüber hinaus sind zur DNS-Kommunikation VMware-Proxy-Nodes (Port 53) über TCP- und UDP-Protokolle erforderlich. Ein nicht ordnungsgemäß eingerichteter DNS kann zahlreiche Laufzeit- oder Konfigurationsprobleme nach sich ziehen.

Um eine ordnungsgemäße DNS-Konfiguration zu bestätigen, führen Sie die folgenden Befehle über die Eingabeaufforderung von vCenter Server aus:

- `nslookup` <*vollständig_qualifizierter_Domainname_von_VDP*>

  Der `nslookup`-Befehl gibt den vollständig qualifizierten Domainnamen der VDP-Appliance zurück.

- `nslookup` <*vollständig_qualifizierter_Domainname_von_vCenter*>

  Der `nslookup`-Befehl gibt den vollständig qualifizierten Domainnamen von vCenter Server zurück.

Wenn der `nslookup`-Befehl die richtigen Informationen zurückgibt, schließen Sie die Eingabeaufforderung. Wenn die `nslookup`-Befehle nicht die gewünschten Informationen zurückgeben, können Sie den VDP-Namen und die VDP-Adresse der Datei `/etc/hosts` in vCenter manuell hinzufügen.

Konfiguration von NTP

VDP nutzt VMware Tools zur Zeitsynchronisation über NTP. Sämtliche vSphere-Hosts und der vCenter Server-Rechner müssen über eine ordnungsgemäße NTP-Konfiguration verfügen. Die VDP-Appliance erhält die richtige Zeit über vSphere und darf nicht mit NTP konfiguriert werden.

ACHTUNG Wenn Sie NTP direkt auf der VDP-Appliance konfigurieren, führt dies zu Fehlern bei der Zeitsynchronisation.

Weitere Informationen zur NTP-Konfiguration finden Sie in der ESXi- und vCenter Server-Dokumentation.

vCenter-Ansicht „Hosts und Cluster"

Die VDP-Appliance kann mit Ordner- und Ressourcenansichten verwendet werden, die unter der Ansicht „Hosts und Cluster" erstellt wurden. Die Ansicht „Hosts und Cluster" in vSphere Web Client ermöglicht die Durchführung folgender Aufgaben:

- Konfigurieren von Benutzerkonten
- Erstellen eines Snapshot
- Mounten des ISO-Image
- Entfernen eines Snapshot
- Zurückkehren zu einem Snapshot
- Erweitern von Festplatten

- Konfigurieren der Systemeinstellungen für die VDP-Appliance
- Entfernen der VDP-Appliance aus dem vCenter-Bestand

Zugreifen auf die Ansicht „Hosts und Cluster“

1 Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

https://*<IP_Adresse_vCenter_Server>***:9443/vsphere-client/**

2 Melden Sie sich mit Administratorrechten an.

3 Wählen Sie **vCenter** > **Hosts und Cluster** aus.

Konfiguration des Benutzerkontos

Bevor das vCenter-Benutzerkonto oder der SSO-Admin-Benutzer mit VDP verwendet werden kann, müssen diese Benutzer als Administrator auf dem vCenter-Stammknoten hinzugefügt werden. Benutzer, die Berechtigungen von Gruppenrollen erben, sind nicht gültig.

HINWEIS In sicherheitssensiblen Umgebungen können Sie die zum Konfigurieren und Verwalten der VDP-Appliance erforderlichen vCenter-Benutzerkontorechte beschränken. Die Kategorien der einzelnen Kontoberechtigungen werden unter „Minimal erforderliche vCenter-Benutzerkontorechte“ auf Seite 213 aufgeführt.

Anhand der folgenden Schritte wird der VDP- oder SSO-Admin-Benutzer mit vSphere Web Client konfiguriert.

1 Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

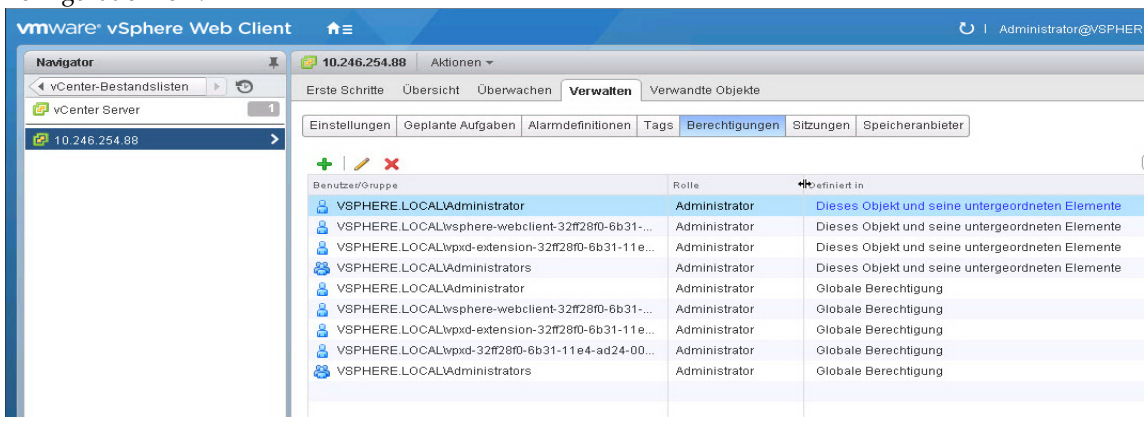
https://*<IP_Adresse_vCenter_Server>***:9443/vsphere-client/**

2 Melden Sie sich mit Administratorrechten an.

3 Wählen Sie **vCenter** > **Hosts und Cluster** aus.

4 Klicken Sie im linken Bereich der Seite auf „vCenter Server“.

WICHTIGER HINWEIS Achten Sie darauf, vCenter über die Stammebene der Baumstruktur auszuwählen (dargestellt unter „Hosts und Cluster“). Bei Auswahl der virtuellen vCenter-Maschine schlägt die Konfiguration fehl.



5 Klicken Sie auf die Registerkarte **Managen** und wählen Sie anschließend **Berechtigungen** aus.

6 Klicken Sie auf das Symbol **Berechtigung hinzufügen (+)**.

7 Klicken Sie auf **Hinzufügen**.

8 Wählen Sie in der Domain-Drop-down-Liste den Eintrag „Domain“, „Server“ oder „VSPHERE.LOCAL“ aus.

HINWEIS: Für vCenter Version 5.1 und früher lautet die Standarddomain „SYSTEM-DOMAIN“.

9 Wählen Sie den Benutzer aus, der VDP verwalten oder als SSO-Admin fungieren wird, und klicken Sie auf **Hinzufügen**.

10 Klicken Sie auf **OK**.

11 Wählen Sie aus der Liste **Zugewiesene Rolle** die Option **Administrator** aus.

12 Vergewissern Sie sich, dass das Kontrollkästchen **Auf untergeordnete Objekte übertragen** aktiviert ist.

13 Klicken Sie auf **OK**.

Navigieren Sie zu **Startseite > Administration > Rollenmanager** und klicken Sie auf die Rolle **Administrator**, um zu überprüfen, ob der Benutzer in der Liste der Administratoren aufgeführt ist. Der soeben hinzugefügte Benutzer sollte rechts neben der Rolle angezeigt werden.

WICHTIGER HINWEIS Wenn der VDP-Backupbenutzer, der das Dienstprogramm VDP-configure nutzt, zu einem Domainkonto gehört, verwenden Sie das Format „SYSTEM-DOMAIN\admin“ in VDP-configure. Wenn der Benutzername im Format „admin@SYSTEM-DOMAIN“ eingegeben wird, werden Aufgaben im Zusammenhang mit einem Backupjob möglicherweise nicht in den Aufgaben mit dem Status „Zuletzt ausgeführt“ angezeigt.

WICHTIGER HINWEIS Das Passwort für das Domainkonto darf keine Leerzeichen enthalten.

Best Practices für VDP

Die folgenden Best Practices sollten bei der Bereitstellung, Verwendung und dem Monitoring einer vSphere Data Protection(VDP)-Appliance befolgt werden.

Allgemeine Best Practices

- Stellen Sie die VDP-Appliance auf einem gemeinsam genutzten VMFS5-Dateisystem oder höheren System bereit, um Einschränkungen bezüglich der Blockgröße zu verhindern.
- Vergewissern Sie sich, dass alle virtuellen Maschinen mit Hardwareversion 7 oder höher ausgeführt werden, um Change Block Tracking (CBT) zu unterstützen.
- Installieren Sie VMware Tools auf jeder virtuellen Maschine, die von VDP gesichert wird. Mit VMware Tools wird eine zusätzliche Backupfunktion zur Verfügung gestellt, mit der vor dem Backup bestimmte Prozesse auf dem Gastbetriebssystem stillgelegt werden können. VMware Tools sind ebenfalls für bestimmte Funktionen bei der Wiederherstellung auf Dateiebene erforderlich.
- Wenn Sie das Netzwerk für die VDP-Appliance und vCenter konfigurieren, ändern Sie nicht die Informationen zur Netzwerkadresse, indem Sie NAT oder andere Konfigurationsmethoden verwenden (Firewalls, IDS oder TSNR). Wenn diese nicht unterstützten Methoden als Teil des virtuellen Netzwerks bereitgestellt werden, funktionieren einige VDP-Funktionen möglicherweise nicht wie vorgesehen.

Best Practices für die Bereitstellung

Folgendes sollte bei der Bereitstellung einer VDP-Appliance immer als Best Practice berücksichtigt werden:

- Erstellen Sie einen DNS-Datensatz für die VDP-Appliance, bevor Sie die Appliance bereitstellen. Vergewissern Sie sich, dass in DNS sowohl die Vorwärts- als auch die Rückwärtssuche (Forward und Reverse Lookup) aktiviert sind.
- Als einer der letzten Schritte wird bei der VDP-Bereitstellung optional eine Performanceanalyse für den Speicher ausgeführt. Überprüfen Sie mit dieser Analyse, ob der Speicher, auf dem VDP ausgeführt wird, die Performanceanforderungen erfüllt oder übertrifft. Die Fertigstellung der Analyse kann 30 Minuten bis hin zu mehreren Stunde dauern.
- Platzieren Sie die VDP-Appliance in einen anderen Datenspeicher als die geschützten VMs.
- Ziehen Sie bei der Planung von Backupjobs eine Staffelung der Startzeiten in Betracht.

- Wenn von Anwendungen, wie z. B. Datenbanken oder Exchange Server mit hohen Wechselraten, ein Backup durchgeführt wird, verschachteln (optimieren) Sie diese mit Image-Levelbackups einer anderen VM, als der VM für unstrukturierte Daten.

  Datenbanken gehören zu den strukturierten Daten und Image Backups gehören zu den unstrukturierten Daten. Datenbanken erzeugen mehr eindeutige Daten, die in einem niedrigen Deduplizierungsverhältnis resultieren, während Imagelevelbackups ein höheres Deduplizierungsverhältnis haben. Das Verschachteln von Imagelevelbackups zwischen zwei Anwendungsbackups belastet die Deduplizierungs-Engine weniger, was in einer besseren Backupperformance resultiert.

HINWEIS Grundsätzlich sollten Image-Levelbackups einer Anwendung oder VM mit hoher Wechselrate nicht durchgeführt werden, da die Snapshot-Verarbeitung aufwendig ist und die Performance beeinträchtigen kann.

- Berücksichtigen Sie andere Prozesse, die möglicherweise derzeit ausgeführt werden. Versuchen Sie, eine Replikation oder automatische Backupverifizierung nicht während der Ausführung von Backupjobs zu planen. Planen Sie, wenn möglich, diese Jobs so, dass sie nach Abschluss der Backupjobs und vor Öffnung des Wartungszeitfensters ausgeführt werden.
- Ein interner Proxy muss aktiviert sein und wird im Falle einer Notfallwiederherstellung automatisch aktiviert.

Best Practices für Hot-Add

Der Hot-Add-Transportmechanismus wird für schnellere Backups und Wiederherstellungen und eine geringe Anfälligkeit für Netzwerkrouting-, Firewall- und SSL-Zertifikatsprobleme empfohlen. Falls der Transportmechanismus des NBD (Network Block Device, Netzwerkblockgerät) statt eines Hot-Add eingesetzt wird, nimmt die Backupperformance ab.

Die folgenden Anforderungen müssen bei einer Festplatte erfüllt sein, die per Hot-Add gemountet werden soll:

- Bei Verwendung eines vSphere-Hosts der Version 5.0 muss der Host für Hot-Add lizenziert sein. vSphere-Hosts der Version 5.1 und höher beinhalten diese Funktion standardmäßig.
- Die VDP-Appliance wird auf einem vSphere-Host bereitgestellt, der über einen Pfad zum Speicher mit den für ein Backup vorgesehenen virtuellen Laufwerken verfügt.
- Die Hot-Add-Funktion wird nicht auf IDE-konfiguriertem virtuellen Laufwerken verwendet. I/O über das Netzwerk wirkt sich negativ auf die Performance aus. Verwenden Sie stattdessen virtuelle SCSI-Laufwerke.
- Die Gesamtkapazität des VMFS-Volume, auf dem sich VDP befindet, entspricht der Größe des größten virtuellen Laufwerks, das gesichert wird (der freie Speicherplatz kann unter dieser Größe liegen).
- Die Blockgröße des VMFS-Volume, auf dem sich VDP befindet, entspricht der Größe des größten virtuellen Laufwerks, das gesichert wird, oder liegt darüber.
- Die zu sichernde virtuelle Maschine darf nicht über eine unabhängige virtuelle Festplatte verfügen.
- Die virtuelle Maschine, die gesichert wird, befindet sich in demselben Rechenzentrum (vCenter Server-Containerobjekt) wie die VDP-Appliance. Der Hot-Add-Transport kann die Rechenzentrumsgrenze nicht überschreiten.
- Die virtuellen Maschinen und VMDKs auf dem vCenter Server-Rechner verfügen über denselben Namen wie diejenigen, die der virtuellen Maschine zugewiesen sind, die gesichert wird.
- Hot-Add funktioniert nicht bei virtuellen Maschinen, die vSphere Flash Read Cache (vFlash) verwenden.

Weitere Informationen zu den Hot-Add Best Practices finden Sie in folgendem Knowledgebase-Artikel:

http://kb.vmware.com/kb/2048138

Speicherkapazität für die erste VDP-Bereitstellung

Beim Bereitstellen einer neuen vSphere Data Protection (VDP)-Appliance wird die Appliance normalerweise in den ersten Wochen schnell aufgefüllt. Dies ist darauf zurückzuführen, dass fast jeder Client, der gesichert wird, einmalig vorkommende Daten umfasst. Die VDP-Deduplizierung lässt sich am effektivsten nutzen, wenn bereits andere ähnliche Clients gesichert oder dieselben Clients mindestens einmal gesichert wurden.

Nach dem ersten Backup werden von der Appliance während der folgenden Backups weniger einmalig vorkommende Daten gesichert. Wenn die ersten Backups abgeschlossen sind und die maximalen Aufbewahrungsfristen überschritten wurden, kann überlegt und gemessen werden, ob das System genauso viele neue Daten speichern kann, wie es täglich freigibt. Dies wird als Erreichen einer stabilen Kapazitätsauslastung bezeichnet. Eine stabile Kapazität sollte idealerweise bei 80 % liegen.

Dimensionierung

Über die vSphere Data Protection-Dimensionierung lassen sich anhand der folgenden Faktoren die VDP-Appliance-Größe und die Anzahl der erforderlichen Appliances ermitteln:

- Anzahl und Typ der virtuellen Maschinen (umfasst die VM Dateisystem- oder Datenbankdaten?)
- Datenmenge
- Aufbewahrungsfristen (täglich, wöchentlich, monatlich, jährlich)
- typische Änderungsrate

In der folgenden Tabelle sind beispielhafte Empfehlungen für die vSphere Data Protection-Dimensionierung angegeben:

Tabelle 2-3. Beispielhafte Empfehlungen für die vSphere Data Protection-Dimensionierung

Anzahl VMs	Datenspeicher pro Client	Aufbewahrungszeitraum: daily	Aufbewahrungszeitraum: weekly	Aufbewahrungszeitraum: monthly	Aufbewahrungszeitraum: yearly	Empfehlung
25	20	30	0	0	0	1–0,5 TB
25	20	30	4	12	7	1–2 TB
25	40	30	4	12	7	2–2 TB
50	20	30	0	0	0	1–1 TB
50	20	30	4	12	7	2–2 TB
50	40	30	4	12	7	3–2 TB
100	20	30	0	0	0	1–2 TB
100	20	30	4	12	7	3–2 TB
100	40	30	4	12	7	6–2 TB

Die oben stehenden Empfehlungen (beachten Sie, dass es lediglich Richtlinien sind) beruhen auf den folgenden Annahmen:

- Die virtuellen Maschinen enthalten hauptsächlich Dateisystemdaten. Wenn die virtuellen Maschinen hauptsächlich Datenbankdaten umfassen, fallen die Deduplizierungsraten niedriger aus.
- Die anfängliche Deduplizierungsrate für Dateisystemdaten beläuft sich auf 70 %.
- Die tägliche Deduplizierungsrate für Dateisystemdaten beläuft sich auf 99,7 %.
- Die jährliche Wachstumsrate beträgt 5 %.

WICHTIGER HINWEIS Wenn Sie in Bezug auf die Größe der bereitzustellenden Appliance unsicher sind, sollte besser ein größerer vSphere Data Protection-Datenspeicher verwendet werden. Sobald eine Anwendung bereitgestellt wurde, ist die Größe des Datenspeichers nicht mehr veränderbar.

Überwachen der VDP-Kapazität

Die VDP-Kapazität sollte proaktiv überwacht werden. Die VDP-Kapazität kann auf der VDP-Registerkarte **Berichte** über den Eintrag „Genutzte Kapazität“ angezeigt werden (der zur Bestimmung einer stabilen Kapazität verwendet wird). Weitere Informationen finden Sie unter „Anzeigen von Informationen über die Registerkarte „Berichte““ auf Seite 118.

Tabelle 2-4 beschreibt das VDP-Verhalten in Bezug auf wichtige Kapazitätsschwellenwerte:

Tabelle 2-4. Kapazitätsschwellenwerte

Schwellenwert	Wert	Verhalten
Kapazitätswarnung	80 %	VDP gibt ein Warnereignis aus.
Kapazitätsfehler	95 %	Für Backupjobs werden in vCenter keine Aufgaben generiert, wenn die Kapazitätsgrenze von 95 % überschritten wurde.
Grenzwert für Integritätsprüfung	95 %	Der Abschluss vorhandener Backups wird zugelassen, neue Backupvorgänge werden jedoch unterbrochen. VDP gibt Warnereignisse aus.
Serverbeschränkung durch Schreibschutz	100 %	VDP geht in den schreibgeschützten Modus über, in dem der Appliance-Status auf „Admin“ geändert wird, und lässt keine neuen Daten zu.

Sobald die Kapazitätsgrenze von 80 % überschritten wurde, wenden Sie für das Kapazitätsmanagement die folgenden Richtlinien an:

- Fügen Sie keine neuen virtuellen Maschinen als Backupclients hinzu.
- Entfernen Sie nicht benötigte Wiederherstellungspunkte.
- Löschjobs sind nicht länger erforderlich.
- Führen Sie eine Neubewertung der Aufbewahrungs-Policies durch, um festzustellen, ob Aufbewahrungs-Policies entschärft werden können.
- Erwägen Sie die Aufnahme zusätzlicher VDP-Appliances und verteilen Sie Backupjobs gleichmäßig auf mehrere Appliances.

VDP-Installation

Die Installation von vSphere Data Protection (VDP) wird in zwei Schritten abgeschlossen:

- „Bereitstellen der OVF-Vorlage“ auf Seite 29
- „Erstkonfiguration“ auf Seite 31

Bereitstellen der OVF-Vorlage

Voraussetzungen

- vSphere-Host 5.0 oder höher
- vCenter Server 5.5 oder höher
- Melden Sie sich bei vCenter Server über vSphere Web Client an, um die OVF-Vorlage bereitzustellen. Wenn Sie keine Verbindung zu vSphere Web Client herstellen können, vergewissern Sie sich, dass der vSphere Web Client-Service gestartet wurde.
- Die VDP-Appliance stellt über den Port 902 eine Verbindung zu einem vSphere-Host her. Ist eine Firewall zwischen der VDP-Appliance und dem vSphere-Host vorhanden, muss der Port 902 offen sein. Zusätzliche Informationen zur Portverwendung finden Sie unter Kapitel A, „Von VDP verwendete Ports“, auf Seite 209.
- Das VMware Client Integration-Plug-in muss in Ihrem Browser installiert sein. Falls dies noch nicht der Fall ist, kann es während des folgenden Verfahrens installiert werden.

Verfahren

1 Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

https://*<IP_Adresse_vCenter_Server>***:9443/vsphere-client/**

2 Melden Sie sich mit Administratorrechten an.

3 Wählen Sie **vCenter > Rechenzentren** aus.

4 Klicken Sie auf der Registerkarte **Objekte** auf **Aktionen > OVF-Vorlage bereitstellen.**

5 Lassen Sie bei Aufforderung das VMware Client Integration-Plug-in zu und installieren Sie es.

6 Wählen Sie die Quelle aus, auf der sich die VDP-Appliance befindet. Standardmäßig ist das Dialogfeld für den Dateinamen auf OVF-Pakete (*.ovf) eingestellt. Wählen Sie aus dem Drop-down-Feld rechts vom Dateinamen die Option **OVA-Pakete (*.ova)** aus.

7 Navigieren Sie zum Speicherort der .ova-Datei der VDP-Appliance. Vergewissern Sie sich, dass Sie die richtige Datei für den Datenspeicher auswählen. Klicken Sie auf **Öffnen**.

8 Nach Auswahl der .ova-Datei der VDP-Appliance klicken Sie auf **Weiter**.

9 Überprüfen Sie die Vorlagendetails und klicken Sie auf **Weiter**.

10 Lesen Sie auf dem Bildschirm „EULAs akzeptieren“ den Lizenzvertrag, klicken Sie auf **Akzeptieren** und dann auf **Weiter**.

11 Geben Sie im Bildschirm zum Auswählen von Namen und Ordner den Namen für die VDP-Appliance ein. Verwenden Sie beim Eingeben des Namens den vollständig qualifizierten Domainnamen (Fully Qualified Domain Name, FQDN), über den die VDP-Konfiguration nach der VDP-Appliance im vCenter-Bestand sucht. Ändern Sie den Namen der VDP-Appliance nicht mehr nach der Installation.

12 Klicken Sie auf den Ordner oder das Rechenzentrum, in dem Sie die VDP-Appliance bereitstellen möchten und klicken Sie dann auf **Weiter**.

13 Wählen Sie im Bildschirm zur Ressourcenauswahl den Host für die VDP-Appliance aus und klicken Sie auf **Weiter**.

14 Wählen Sie im Bildschirm zur Speicherauswahl das Format der virtuellen Laufwerke aus. Legen Sie dann den Speicherort für die VDP-Appliance fest. Klicken Sie auf **Weiter**.

15 Wählen Sie im Bildschirm zur Netzwerkeinrichtung das Zielnetzwerk für die VDP-Appliance aus und klicken Sie auf **Weiter**.

16 Geben Sie im Bildschirm zur Vorlagenanpassung Werte für **Standardgateway**, **DNS**, **Netzwerk 1 IP-Adresse** und **Netzwerk 1 Netzmaske** an. Vergewissern Sie sich, dass die IP-Adressen korrekt sind und dem Eintrag auf dem DNS-Server entsprechen. Wenn in diesem Dialogfeld falsche IP-Adressen angegeben werden, ist es erforderlich, die .ova-Datei neu bereitzustellen. Klicken Sie auf **Weiter**.

HINWEIS Die VDP-Appliance bietet keinen Support für DHCP. Eine statische IP-Adresse ist erforderlich.

17 Vergewissern Sie sich im Bildschirm „Bereit zur Fertigstellung“, dass sämtliche Bereitstellungsoptionen korrekt sind. Aktivieren Sie nach der Bereitstellung die Option **Einschalten** und klicken Sie auf **Fertig stellen**.

vCenter stellt die VDP-Appliance bereit und startet im Installationsmodus. Sie können das Fenster **Letzte Aufgaben** überwachen, um den Abschluss der Bereitstellung bestimmen zu können.

Erstkonfiguration

Voraussetzungen

- Vergewissern Sie sich, dass die `.ovf`-Vorlage von VDP erfolgreich bereitgestellt wurde. Weitere Informationen finden Sie unter „Bereitstellen der OVF-Vorlage" auf Seite 29.
- Sie müssen über vSphere Web Client bei vCenter Server angemeldet sein.
- Im Datenspeicher ist genügend freier Festplattenspeicher vorhanden. Wenn während der Erstkonfiguration der Appliance ein optionaler Performanceanalysetest ausgeführt wird, sind 41 GB Speicherplatz pro Festplatte pro Datenspeicher erforderlich. (Wenn sich beispielsweise drei Festplatten in demselben Datenspeicher befinden, sind 123 GB freier Speicherplatz erforderlich.) Wenn nicht genügend Speicherplatz verfügbar ist, meldet der Test für alle (optionalen) Lese-, Schreib- und Seek-Tests einen Wert von 0 und gibt abschließend über einen entsprechenden Status an, dass der Speicherplatz nicht ausreicht.

Verfahren

1 Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

https://<*IP_Adresse_vCenter_Server*>**:9443/vsphere-client/**

2 Melden Sie sich mit Administratorrechten an.

3 Wählen Sie **vCenter-Startseite > vCenter > VMs und Vorlagen** aus. Blenden Sie die vCenter-Struktur ein und wählen Sie die VDP-Appliance aus.

4 Öffnen Sie eine Konsolensitzung in der VDP-Appliance, indem Sie mit der rechten Maustaste auf die VDP-Appliance klicken und **Konsole öffnen** auswählen.

5 Nach dem Laden der Installationsdateien wird die Begrüßungsseite für das VDP-Menü angezeigt. Öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

https://<IP_Adresse_der_VDP_Appliance>**:8543/vdp-configure/**

Die VDP-Anmeldeseite wird angezeigt.

6 Geben Sie **root** in das Feld **Benutzer** und **changeme** in das Feld **Passwort** ein und klicken Sie dann auf **Anmelden**.

Die vSphere-Begrüßungsseite wird angezeigt.

7 Klicken Sie auf **Weiter**.

Das Dialogfeld „Netzwerkeinstellungen" wird standardmäßig angezeigt.

8 Bestätigen Sie die folgenden Netzwerk- und Serverinformationen für Ihre VDP-Appliance oder geben Sie diese ein. Vergewissern Sie sich, dass die Werte ordnungsgemäß ausgefüllt sind. Andernfalls schlägt die Installation fehl.

a Statische IPv4- oder IPv6-Adresse

b Netzmaske

c Gateway

d Primärer DNS

e Sekundärer DNS

f Hostname

g Domain

9 Klicken Sie auf **Weiter**.

Das Dialogfeld „Zeitzone" wird angezeigt.

10 Wählen Sie die entsprechende Zeitzone für Ihre VDP-Appliance aus und klicken Sie auf **Weiter**.

Das Dialogfeld „VDP-Anmeldedaten“ wird angezeigt.

11 Geben Sie das VDP-Appliance-Passwort unter Berücksichtigung der folgenden Kriterien in das Feld **Passwort** ein und bestätigen Sie das Passwort dann durch eine erneute Eingabe in das Feld **Passwort bestätigen**. Dieses Passwort wird als universelles Konfigurationspasswort verwendet.

Die vier Zeichenklassen lauten wie folgt:

- Großbuchstaben A–Z
- Kleinbuchstaben A–Z
- Zahlen 0–9
- Sonderzeichen (z. B. ~!@#,.)

Erstellen Sie das Passwort mithilfe der folgenden Kriterien:

- Bei Verwendung aller vier Zeichenklassen muss das Passwort mindestens 6 Zeichen lang sein.
- Bei Verwendung von drei Zeichenklassen muss das Passwort mindestens 7 Zeichen lang sein.
- Bei Verwendung von einer oder zwei Zeichenklassen muss das Passwort mindestens 8 Zeichen lang sein.

12 Klicken Sie auf **Weiter**.

Die Seite **vCenter-Registrierung** wird angezeigt.

13 Geben Sie Werte in die folgenden Felder ein:

- vCenter-Benutzername

  Wenn der Benutzer zu einem Domainkonto gehört, geben Sie den Namen ein, indem Sie das Format „SYSTEM-DOMAIN\admin“ verwenden.

ACHTUNG Wenn ein SSO-Admin-Benutzer als vCenter-Benutzername im Format <benutzername@vsphere.local> angegeben ist, werden Aufgaben mit Bezug zu VDP-Vorgängen nicht im vCenter-Fenster „Letzte Aufgaben“ von vSphere Web Client angezeigt. Damit Aufgaben im Fenster „Letzte Aufgaben“ angezeigt werden, geben Sie den SSO-Admin-Benutzer im Format <vsphere.local\benutzername> an.

- vCenter-Passwort
- vCenter-FQDN oder -IP-Adresse
- vCenter-HTTP-Port

  Der Standardport ist**80**. Wenn Sie nicht den Standard, sondern einen anderen Port benutzen, müssen Sie den Port in **/etc/firewall.base** öffnen und den **avfirewall** Service neu starten.

  Geben Sie einen benutzerdefinierten Wert für den HTTP-Port ein, wenn Sie über den HTTP-Port eine Verbindung zu vCenter herstellen müssen. Der HTTPS-Port hingegen wird für sämtliche andere Kommunikation verwendet.

- vCenter-HTTPS-Port

  Der Standardport ist**443**. Wenn Sie nicht den Standard, sondern einen anderen Port benutzen, müssen Sie den Port in **/etc/firewall.base** öffnen und den **avfirewall** Service neu starten.

  Wenn deaktiviert, aktivieren Sie zur SSO-Authentifizierung das Kontrollkästchen **vCenter zur SSO-Authentifizierung**.

HINWEIS Lassen Sie das Kontrollkästchen **vCenter zur SSO-Authentifizierung verwenden** aktiviert, wenn in vCenter SSO in der vCenter Server-Appliance integriert ist. Wenn Sie die Auswahl durch Deaktivierung des Kontrollkästchens aufheben, müssen Sie den vollständig qualifizierten Domainnamen oder die IP-Adresse des SSO-Servers eingeben und die Felder für den SSO-Port ausfüllen.

- Klicken Sie auf **Verbindung prüfen**.

  Die Meldung „Verbindung erfolgreich“ wird angezeigt. Wenn diese Meldung nicht angezeigt wird, führen Sie ein Troubleshooting Ihrer Einstellungen durch und wiederholen Sie diesen Schritt, bis eine Meldung „Erfolgreich“ angezeigt wird.

Wenn Sie die folgende Meldung auf der vCenter-Registrierungsseite erhalten, führen Sie die Schritte durch, die unter „Konfiguration des Benutzerkontos“ auf Seite 25 beschrieben sind:

```
Angegebener Benutzer ist entweder kein dedizierter VDP-Benutzer oder verfügt nicht
über ausreichende vCenter-Rechte zum Verwalten von VDP. Aktualisieren Sie Ihre
Benutzerrolle und versuchen Sie es erneut.
```

14 Klicken Sie auf **Weiter**, um zur Seite **Speicher erstellen** vorzugehen. Diese führt Sie durch die Auswahl des Speichertyps. Informationen zur Speicherkonfiguration und den abschließenden Schritten, die für das Abschließen des Assistenten für die Erstkonfiguration erforderlich sind, finden Sie unter „Erstellen von neuem Speicher“ auf Seite 78.

VDP-Appliance-Upgrades

3

Dieses Kapitel umfasst das folgende Thema:

Upgrade der VDP-Appliance

VDP 6.1 unterstützt die Durchführung eines Upgrades von früheren Versionen nicht. Zur Verwendung von VDP 6.1 müssen Sie zunächst die vorherige VDP-Version deinstallieren und dann die Version 6.1 installieren.

So deinstallieren Sie das VDP-Plug-in:

- Unter Windows Server 2012 oder Windows Server 2008 verwenden Sie **Programme und Funktionen**.
- Unter Windows Server 2003 verwenden Sie **Programme hinzufügen/entfernen**.

„VDP-Installation und -Konfiguration" auf Seite 21 bietet Informationen über die Installation und Konfiguration von VDP.

Konfiguration der VDP-Appliance nach der Installation

4

Dieses Kapitel umfasst folgende Themen:

Informationen über das Dienstprogramm VDP-configure

Während der Installation von vSphere Data Protection (VDP) wird das Dienstprogramm VDP-configure im Installationsmodus ausgeführt. Mit diesem Modus können Sie die anfänglichen Netzwerkeinstellungen, die Zeitzone, das VDP-Appliance-Passwort und die vCenter-Anmeldedaten eingeben. Mit dem Installationsmodus haben Sie außerdem die Möglichkeit, Speicher zu erstellen oder anzubinden und optional das Performance-Bewertungstool auszuführen. Nach der Erstinstallation wird das Dienstprogramm VDP-configure im Wartungsmodus ausgeführt und zeigt eine andere Benutzeroberfläche an.

Zum Zugreifen auf das Dienstprogramm VDP-configure öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

https://*<IP_Adresse_der_VDP_Appliance>***:8543/vdp-configure/**

Verwenden Sie den Benutzernamen und das Passwort der VDP-Appliance. Wenn Sie sich beim VDP-Konfigurationsdienstprogramm anmelden, wird ein Skript zur Systemintegritätsprüfung ausgeführt. Sie müssen auf den Abschluss der Systemintegritätsprüfung warten, bevor Sie Konfigurationsaufgaben von einer der Registerkarten des VDP-Konfigurationsdienstprogramms durchführen können.

HINWEIS Nach der Konfiguration der Appliance können Sie optional über das VDP-Konfigurationsdienstprogramm einen Performanceanalysetest ausführen. Für den Test sind 41 GB an Speicherplatz pro Festplatte pro Datenspeicher erforderlich. Wenn diese Menge an Speicherplatz nicht verfügbar ist, meldet das Dienstprogramm, dass der Speicherplatz nicht ausreicht, und der Performanceanalysetest wird nicht ausgeführt.

Führen Sie die folgenden Konfigurationsaufgaben mithilfe der Konfigurationsschnittstelle durch:

- „Speichermanagement" auf Seite 77: Hiermit können Sie Ihre Speicherkonfiguration anzeigen, ein Data Domain-System hinzufügen und bearbeiten sowie Festplattenspeicher auf einer VDP-Appliance hinzufügen oder erweitern.
- „Anzeigen des Status" auf Seite 39: Hiermit können Sie die Services anzeigen, die derzeit auf der VDP-Appliance ausgeführt werden oder beendet wurden.
- „Starten und Stoppen von Services" auf Seite 39: Hiermit können Sie ausgewählte Services auf der VDP-Appliance starten oder beenden.
- „Sammeln von VDP-Protokollen oder Diagnoseinformationen" auf Seite 40: Hiermit können Sie zwecks Troubleshooting aktuelle Protokolle von der VDP-Appliance herunterladen.
- „Ändern von Konfigurationseinstellungen" auf Seite 42: Hiermit können Sie Netzwerkeinstellungen anzeigen oder ändern, die vCenter-Registrierung konfigurieren, Systemeinstellungen (Zeitzoneninformationen und VDP-Anmeldedaten) anzeigen oder bearbeiten und den Proxydurchsatz anhand von Konfigurationsoptionen für externe und interne Proxys managen.
- „Rollback einer Appliance" auf Seite 43: Hiermit können Sie die VDP-Appliance in einem früheren bekannten und gültigen Status wiederherstellen.
- „Notfallwiederherstellung" auf Seite 44: Hiermit können Sie eine virtuelle Maschine direkt auf dem Host wiederherstellen, auf dem die VDP-Appliance ausgeführt wird. Dieses Verfahren zur Notfallwiederherstellung ist dann einzusetzen, wenn vCenter nicht verfügbar ist.
- „Managen des Proxydurchsatzes" auf Seite 71: Hiermit können Sie interne und externe Proxys managen. Sie können bis zu 8 externe virtuelle Proxymaschinen bereitstellen. Durch die Bereitstellung von 8 externen Proxys können Sie den Backupdurchsatz mithilfe der Hot-Add-Funktion verbessern und mehr gleichzeitige Backup- und Wiederherstellungsvorgänge ausführen.

Anzeigen des Status

Auf der Registerkarte **Konfiguration** werden alle für VDP erforderlichen Services sowie der aktuelle Status jedes Service aufgeführt. Tabelle 4-5 beschreibt die Services, die von VDP verwendet werden.

Tabelle 4-5. Beschreibung der auf der VDP-Appliance ausgeführten Services

Service	Beschreibung
Kernservices	Hierbei handelt es sich um die Services, die die Backup-Engine der VDP-Appliance beinhalten. Wenn diese Services deaktiviert sind, werden keine Backupjobs ausgeführt (weder geplant noch „On Demand“, also nach Bedarf). Außerdem können keine Wiederherstellungsaktivitäten initiiert werden.
Managementservices	Managementservices sollten nur auf Anweisungen des technischen Supports gestoppt werden.
Services für die Wiederherstellung auf Dateiebene	Hierbei handelt es sich um die Services, die das Management von Wiederherstellungsvorgängen auf Dateiebene unterstützen.
Backup-Recovery-Services	Hierbei handelt es sich um die Services, die Backup-Recoveries unterstützen.
Wartungsservices	Hierbei handelt es sich um die Services, die Wartungsaufgaben ausführen, z. B. wenn evaluiert wird, ob die Aufbewahrungsfristen von Backups abgelaufen sind. Die Wartungsservices sind die ersten 24–48 Stunden nach Bereitstellung der VDP-Appliance deaktiviert. Hierdurch entsteht ein größeres Backupzeitfenster für erste Backups.
Backupplaner	Beim Backupplaner handelt es sich um den Service, der geplante Backupjobs initiiert. Wenn der Backupplaner gestoppt wird, werden keine geplanten Backups ausgeführt. On-Demand-Backups können weiterhin initiiert werden.

HINWEIS Wenn einer dieser Services nicht mehr ausgeführt wird, löst dies einen Alarm auf dem vCenter Server-Rechner aus. Beim Neustart eines gestoppten Service wird der Alarm gelöscht. Das Auslösen oder Löschen von Alarmen kann sich bis zu 10 Minuten verzögern.

Folgende Statuswerte sind für diese Services möglich:

- Wird gestartet
- Start fehlgeschlagen
- Wird ausgeführt
- Wird gestoppt
- Stoppen fehlgeschlagen
- Gestoppt
- Ladevorgang wird durchgeführt – Status wird abgerufen
- Nicht wiederherstellbar (nur Kernservices)
- Wird wiederhergestellt (nur Managementservices)
- Wiederherstellung fehlgeschlagen (nur Managementservices)

Durch Klicken auf das Symbol „Aktualisieren“ wird die Statusanzeige aktualisiert.

Starten und Stoppen von Services

Auf dem Bildschirm „Status“ können Sie gestoppte Services neu starten, indem Sie auf **Starten** klicken, oder Sie können aktuell ausgeführte Services stoppen, indem Sie auf **Stoppen** klicken. Allgemein sollten laufende Services jedoch nur auf Anweisung des technischen Supports gestoppt werden.

Wenn Sie einen gestoppten Service entdecken, können Sie versuchen, diesen durch Klicken auf **Starten** neu zu starten. Mitunter sind jedoch zusätzliche Troubleshooting-Schritte erforderlich, damit der Service einwandfrei funktioniert.

Wenn alle Services gestoppt sind, starten Sie sie in der folgenden Reihenfolge neu:

1 Kernservices

2 Managementservices

3 Backupplaner

4 Wartungsservices

5 Services für die Wiederherstellung auf Dateiebene

6 Backup-Recovery-Services

Sammeln von VDP-Protokollen oder Diagnoseinformationen

Über die Registerkarte **Protokollsammlung** können Sie die VDP-Protokolldateien einzeln oder zusammen herunterladen. Auf der Registerkarte **Protokollsammlung** werden Protokolldateien in 4 Abschnitte gruppiert. Tabelle 4-6 beschreibt die Protokolldateien in jeder Gruppe.

Tabelle 4-6. Auf der Registerkarte „Protokollsammlung“ verfügbare Protokolldateien

Gruppe	Protokolldateien
Alle VDP-Appliance-Protokolle	Protokolldateien im Zusammenhang mit der VDP-Appliance
Clientprotokolle	Protokolldateien im Zusammenhang mit Microsoft-Anwendungen
Konfigurationen	VDP-Konfigurationsdateien von Proxys, Config Checker, Agents usw. Diese Konfigurationsdateien befinden sich in `/space/vdp/config`.
Protokolle externer Proxys	Protokolldateien von externen virtuellen Proxymaschinen Diese Protokolle sind nur sichtbar, wenn mindestens ein externer Proxy bereitgestellt wird.

HINWEIS Alle Protokolle werden unter `/space/vdp/logs` aufbewahrt.

Die Gruppe „Alle VDP-Appliance-Protokolle“ ist in die folgenden Untergruppen unterteilt, damit Sie nur bestimmte Protokolldateien herunterladen können:

Tabelle 4-7. In der Gruppe „Alle VDP-Appliance-Protokolle“ verfügbare Protokolldateien

Gruppe	Protokolldateien
VDP-Kernservice	Protokolldateien im Zusammenhang mit GSAN, VDP, AVI, dem System und DPN
Managementservice	Protokolldateien im Zusammenhang mit dem MC-Server
Dateisystemservice	Protokolldateien im Zusammenhang mit HFScheck
Service für die Wiederherstellung auf Dateiebene	Protokolldateien im Zusammenhang mit der Wiederherstellung auf Dateiebene
Replikation	Protokolldateien im Zusammenhang mit der Replikation und Replikations-Recovery
Image-Backup und -Wiederherstellung	Protokolldateien im Zusammenhang mit Backups und Wiederherstellungen

Verfahren

1 Öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

https://<*IP_Adresse_der_VDP_Appliance*>:8543/vdp-configure/

2 Melden Sie sich mit dem VDP-Benutzernamen und -Passwort an.

3 Wählen Sie auf der Registerkarte **Protokollsammlung** eine oder mehrere Optionen aus und klicken Sie auf **Download**, um Protokolldateien herunterzuladen:

- **Alle VDP-Appliance-Protokolle:** Wählen Sie diese Option aus und klicken Sie auf **Download**, um alle Protokolldateien von den VDP-Services in eine `ZIP`-Datei herunterzuladen.

  Das Dialogfeld für **Downloadspeicherort auswählen** wird angezeigt. Der Standardname für das Protokollbündel lautet `LogBundle.zip`.

  Benennen Sie die Datei mit einem eindeutigen Namen um. Das Protokollbündel ist in erster Linie dafür vorgesehen, VDP-Appliance-Protokolle an Supportmitarbeiter zu senden.

  - Um alle Protokolle unter einer bestimmten Überschrift aus der folgenden Liste herunterzuladen, aktivieren Sie das Kontrollkästchen neben der jeweiligen Überschrift und klicken Sie auf **Download**.
  - Um unter mehreren Überschriften aufgeführte Protokolldateien herunterzuladen, aktivieren Sie das Kontrollkästchen neben einer oder mehreren Protokolldateien und klicken Sie auf **Download**.

- **Clientprotokolle:** Wählen Sie die Option aus und klicken Sie auf **Download**, um eine aggregierte Textdatei mit allen Clientfehlerprotokollen herunterzuladen.
- **Konfigurationen:** Wählen Sie diese Option aus und klicken Sie auf **Download**, um ausschließlich VDP-Konfigurationsdateiinformationen herunterzuladen.

In der folgenden Tabelle finden Sie Informationen dazu, welche Protokolldateien Sie für das Troubleshooting der bereichsspezifischen Probleme herunterladen müssen:

Tabelle 4-8. Für das Troubleshooting der bereichsspezifischen Probleme herunterzuladende Protokolldateien

Troubleshooting-Bereich	Protokollgruppe	Speicherort auf Appliance	Relevante Protokolldateien zum Herunterladen
Upgrade	VDP-Kernservice -> AVI	/space/vdp/logs/avi_logs/server_log/	avinstaller.log.0
Image-Backup oder -Wiederherstellung	Protokolle zu Image-Backup und -Wiederherstellung und zum externen Proxy (wenn Sie einen externen Proxy verwenden)	■ /space/vdp/logs/image_proxy/avamarclient/ ■ /usr/local/avamarclient/var (bei einem externen Proxy)	■ *.log-Dateien (die auch als avtar-Protokolle bezeichnet werden und Informationen zum Backup enthalten) ■ *.alg-Dateien (enthält Informationen zum Arbeitsauftrag)
Replikation	Replikation	/space/vdp/logs/replicate/client/	■ *Replicate-avreplscript.log ■ *Replicate.log ■ *Replicate.alg
Recovery auf Dateiebene	Service für die Wiederherstellung auf Dateiebene	■ /usr/local/avamarclient/bin/logs ■ /space/vdp/logs/flr_proxy/ ■ /space/vdp/logs/vdp_logs/flr/server_logs/	■ flr-server.log ■ *.log ■ flr_debug.txt ■ flr_msg.txt ■ flr_out.txt
VDP-Plug-in	VDP-Kernservice -> VDP	/space/vdp/logs/vdp_logs/vdr/server_logs/	vdr_server.log
VDP-Konfigurationsdienstprogramm	VDP-Kernservice -> VDP	/space/vdp/logs/vdp_logs/vdr/server_logs/	vdr-configure.log
Integritätsprüfung	Dateisystemservice -> HFSCheck	/space/vdp/logs/hfscheck/	*.log

In der folgenden Tabelle finden Sie Informationen dazu, welche Protokolle Sie für das Troubleshooting der Backup- und Wiederherstellungsprobleme bei Microsoft-Anwendungen sammeln müssen:

Tabelle 4-9. Für das Troubleshooting der bereichsspezifischen Probleme herunterzuladende Protokolldateien

Plug-in	Speicherort der Protokolldateien	Relevante Protokolldateien zum Sammeln
SQL-VDP-Plug-in	■ Für eigenständige SQL-Bereitstellungen: C:\Programme\avp\var ■ Für SQL-Failover-Cluster: Der var-Ordner auf einem Freigabelaufwerk, der während der Clusterkonfiguration mithilfe des Windows Cluster Configuration Wizard (WCCW) angegeben wurde ■ Für SQL AlwaysOn-Cluster: Der var-Ordner, der während der Clusterkonfiguration mithilfe von WCCW angegeben wurde Wenn während der Clusterkonfiguration ein freigegebenes Laufwerk angegeben wurde, enthält das freigegebene Laufwerk die Protokolldateien aller Nodes. Wenn während der Clusterkonfiguration ein lokaler Ordner angegeben wurde, enthält jeder Cluster-Node die Protokolldateien.	■ Protokolle des SQL-VSS-Plug-ins ■ Avtar-Protokolle ■ Avagent-Protokolle ■ Windows-Anwendungs- und Systemeventanzeige Protokolle auf dem Client
SharePoint-VDP-Plug-in	C:\Programme\avp\var	■ Protokolle des SharePoint-VSS-Plug-ins ■ Avtar-Protokolle ■ Avagent-Protokolle ■ Windows-Anwendungs- und Systemeventanzeige Protokolle auf dem Client
HINWEIS ■ In einer SharePoint-Verbundfarm müssen Sie die Protokolle von jedem SharePoint Server-Node einschließlich aller SQL-Back-ends sammeln. ■ Wenn SharePoint Server entweder mit einem SQL-Failover- oder einem AlwaysOn-Cluster oder sowohl mit einem SQL-Failover- als auch einem AlwaysOn-Cluster verbunden ist, wird auch ein Satz Protokolle in dem freigegebenen var-Ordner generiert, der während der Clusterkonfiguration mithilfe von WCCW angegeben wurde.		
Exchange-VDP-Plug-in	■ Auf jedem VDP-Client: C:\Programme\avp\var ■ Der freigegebene var-Ordner, der im Windows Cluster Configuration Wizard für Exchange DAG angegeben wurde	■ Protokolle des Exchange-Plug-ins ■ Avtar-Protokolle ■ Avagent-Protokolle ■ Windows-Anwendungs- und Systemeventanzeige Protokolle auf dem Client

Ändern von Konfigurationseinstellungen

Wenn Sie nach der Installation auf das Dienstprogramm VDP-configure zugreifen, wird es im Wartungsmodus ausgeführt. Im Wartungsmodus können Sie durch Klicken auf die Registerkarte **Konfiguration** Einstellungen festlegen oder ändern, die während der Installation eingegeben wurden. Es ist möglich, Netzwerkeinstellungen und Systemeinstellungen zu konfigurieren sowie eine vCenter-Registrierung durchzuführen.

Netzwerkeinstellungen

Die folgenden Netzwerkeinstellungen können auf der Registerkarte **Konfiguration** konfiguriert werden.

HINWEIS Führen Sie beim Ändern von Netzwerkeinstellungen sofort nach der Änderung manuell eine Integritätsprüfung aus. Wird auf eine Integritätsprüfung verzichtet, kann dies während des Rollbacks auf einen vorherigen Kontrollpunkt zu einem VDP-Verbindungsfehler führen. Anweisungen finden Sie unter „Ausführen einer Integritätsprüfung" auf Seite 63.

- **Statische IPv4- oder IPv6-Adresse**: Die IPv4- oder IPv6-Einstellung der Schnittstelle
- **Netzmaske/Präfix**: Die Netzwerkmaske oder das Präfix der statischen IPv4- oder IPv6-Adresse
- **Gateway**: Die Gatewayadresse der statischen IPv4- oder IPv6-Adresse
- **Primärer DNS**: Zur DNS-Auflösung verwendeter primärer DNS-Server (Domain Name System)
- **Sekundärer DNS**: Zur DNS-Auflösung verwendeter sekundärer DNS-Server (Domain Name System)
- **Hostname**: Der eindeutige Name, unter dem ein Computer in einem Netzwerk bekannt ist (z. B. vdp-primary).
- **Domain**: Ein eindeutiger Name, der eine Website identifiziert (z. B. emc.com). Die *Domain* wird auch als *Domainname* bezeichnet.

vCenter Server-Registrierung

ACHTUNG Wenn der Hostname, das Passwort, der vollständig qualifizierte Domainname, die IP-Adresse oder die Portnummer von vCenter Server geändert wird, gehen alle mit der VDP-Appliance verbundenen Backupjobs, Replikationsjobs und Backupverifizierungsjobs verloren. Vorhandene Wiederherstellungspunkte bleiben zwar intakt, Sie müssen aber die Backupjobs und Replikationsjobs neu erstellen.

Bevor der Prozess ausgeführt wird, der die vCenter Server-Registrierung neu konfiguriert, müssen alle der folgenden Bedingungen erfüllt sein:

- Kein anderer Neukonfigurationsprozess wird ausgeführt (z. B. Passwort- oder Netzwerkneukonfiguration).
- Kein Backup-, Replikations- oder Wiederherstellungsjob wird ausgeführt.
- Es wird keine Integritätsprüfung ausgeführt.
- Alle Services werden auf der VDP-Appliance ausgeführt.

Führen Sie beim Ändern von Anmeldedaten für die vCenter-Registrierung sofort nach der Änderung manuell eine Integritätsprüfung aus. Wird auf eine Integritätsprüfung verzichtet, kann dies während des Rollbacks auf einen vorherigen Kontrollpunkt zu einem VDP-Verbindungsfehler führen. Anweisungen finden Sie unter „Ausführen einer Integritätsprüfung" auf Seite 63.

Rollback einer Appliance

Die VDP-Appliance kann inkonsistent oder instabil werden. In manchen Fällen kann das Dienstprogramm VDP-configure einen inkonsistenten oder instabilen Status erkennen und informiert Sie darüber unmittelbar nach der Anmeldung mithilfe einer Meldung, die der folgenden ähnelt:

> Ihre VDP-Appliance wurde offenbar nicht ordnungsgemäß heruntergefahren und benötigt wahrscheinlich ein Kontrollpunkt-Rollback, um die Datensicherheitsfunktion wiederherzustellen. Dieser Prozess kann über die Registerkarte „Rollback" initiiert werden.

ACHTUNG Standardmäßig bewahrt VDP zwei Systemkontrollpunkte. Wenn Sie ein Rollback auf einen Kontrollpunkt durchführen, gehen bei Abschluss des Rollbacks alle Backups und Konfigurationsänderungen seit der Erstellung des Kontrollpunkts verloren.

Der erste Kontrollpunkt wird bei der VDP-Installation erstellt. Nachfolgende Kontrollpunkte werden vom Wartungsservice erstellt. Dieser Service ist während der ersten 24–48 Stunden des VDP-Betriebs deaktiviert. Sollten Sie während dieses Zeitraums ein Rollback durchführen, wird die VDP-Appliance auf die Standardkonfiguration eingestellt und alle Backupkonfigurationen bzw. Backups gehen verloren.

HINWEIS Wenn zwischen einem Kontrollpunkt und einem Rollback VMware VDP for Exchange Server Clients oder VMware VDP for SQL Server Clients installiert wurden, müssen die Clients neu installiert werden.

Befolgen Sie das unten beschriebene Verfahren für das Rollback einer VDP-Appliance.

ACHTUNG Führen Sie ein Rollback nur auf den zuletzt validierten Kontrollpunkt durch.

Voraussetzung

Die VDP-Appliance muss installiert sein und das VDP-Appliance-Passwort ist erforderlich.

Verfahren

1 Öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

https://<*IP_Adresse_der_VDP_Appliance*>:8543/vdp-configure/

2 Melden Sie sich mit dem VDP-Benutzernamen und -Passwort an.

3 Klicken Sie auf die Registerkarte **Rollback**.

4 Klicken Sie auf das Sperrsymbol, um das VDP-Rollback zu ermöglichen.

5 Geben Sie das VDP-Appliance-Passwort ein und klicken Sie auf **OK**.

Das Sperrsymbol wechselt in den Status „entsperrt“.

6 Klicken Sie auf den Kontrollpunkt, für den ein Rollback durchgeführt werden soll.

7 Klicken Sie auf **VDP-Rollback auf ausgewählten Kontrollpunkt durchführen**.

Eine Warnmeldung wird angezeigt, in der die Folgen eines Rollback der VDP-Appliance erläutert werden.

8 Klicken Sie auf **Ja**.

Eine Informationsmeldung informiert Sie darüber, dass ein Rollback initiiert wurde.

9 Klicken Sie auf **OK**.

Die VDP-Appliance versucht, ein Rollback durchzuführen und zeigt Statusinformationen an. Eine Informationsmeldung informiert Sie außerdem darüber, ob das Rollback erfolgreich war oder fehlgeschlagen ist.

10 Klicken Sie auf **OK**.

Wenn das Rollback der VDP-Appliance nicht erfolgreich war, wenden Sie sich an den Customer Service.

Notfallwiederherstellung

VDP ist bei vielen Kernaufgaben auf vCenter Server angewiesen. Die Notfallwiederherstellung direkt auf dem Host bietet eine Methode zur Wiederherstellung virtueller Maschinen, wenn vCenter Server nicht verfügbar ist oder der Benutzer nicht über vSphere Web Client auf die VDP-Benutzeroberfläche zugreifen kann.

Bei einer Notfallwiederherstellung wird eine virtuelle Maschine direkt auf dem Host wiederhergestellt, auf dem die VDP-Appliance ausgeführt wird. Auf der Registerkarte **Notfallwiederherstellung** wird eine Liste der VMs angezeigt, die von der VDP-Appliance gesichert wurden. Diese virtuellen Maschinen können als neue virtuelle Maschinen auf dem Host wiederhergestellt werden, auf dem die VDP-Appliance ausgeführt wird.

Best Practices und Empfehlungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie einen Notfallwiederherstellungsvorgang durchführen:

- Die für eine Wiederherstellung vorgesehene virtuelle Maschine verfügt über eine virtuelle Hardwareversion, die vom Host unterstützt wird, auf dem die VDP-Appliance ausgeführt wird.
- Im Zieldatenspeicher ist ausreichend freier Speicherplatz für die gesamte virtuelle Maschine vorhanden.
- Der VMFS-Zieldatenspeicher, auf dem die virtuelle Maschine wiederhergestellt wird, unterstützt die VMDK-Dateigröße.
- Für die wiederhergestellten virtuellen Maschinen vom Host, auf dem die VDP-Appliance ausgeführt wird, ist eine Netzwerkverbindung verfügbar.

- Es gibt mindestens ein lokales Konto mit Administratorrechten auf dem Host, auf dem die VDP-Appliance ausgeführt wird.

Einschränkungen und nicht unterstützte Funktionen

- Der vSphere-Host, auf dem die Notfallwiederherstellung durchgeführt wird, kann nicht Teil des vCenter-Bestands sein. Ein vSphere-Host, der aktuell von vCenter Server gemanagt wird, muss vorübergehend von vCenter Server getrennt werden, um die Notfallwiederherstellung durchführen zu können. Um vCenter Server zu trennen, verwenden Sie den vSphere Client (nicht vSphere Web Client), der mit dem vSphere-Host direkt verbunden ist.
- Die Notfallwiederherstellung ermöglicht Ihnen ausschließlich die Wiederherstellung auf Stammhostebene im Bestand.
- Die Notfallwiederherstellung erfordert, dass der von VDP verwendete DNS-Server verfügbar ist und den vSphere-Zielhostnamen vollständig auflösen kann.
- Die Notfallwiederherstellung stellt die virtuelle Maschine im ausgeschalteten Zustand wieder her. Sie müssen sich manuell beim Host anmelden und die wiederhergestellte virtuelle Maschine einschalten.
- Die Notfallwiederherstellung stellt die virtuelle Maschine als neue virtuelle Maschine wieder her. Sie müssen dafür sorgen, dass es sich beim angegebenen Namen für die virtuelle Maschine nicht um ein Duplikat einer bereits vorhandenen virtuellen Maschine handelt.
- Die Notfallwiederherstellung führt keine MSapp-Clients auf.
- Ein interner Proxy wird im Falle einer Notfallwiederherstellung automatisch aktiviert. Wenn sowohl die internen als auch die externen Proxys aktiviert sind, müssen Sie den internen Proxy im Dienstprogramm VDP-configure deaktivieren, damit die Notfallwiederherstellung erfolgreich abgeschlossen werden kann.

Verfahren

1 Melden Sie sich, sofern noch nicht geschehen, beim vSphere Client des Hosts an und führen Sie auf der Registerkarte **Zusammenfassung** unter „Hostmanagement“ die folgenden Schritte durch:

   a Klicken Sie auf **Host von vCenter trennen**.

   b Klicken Sie auf **Ja**, wenn Sie zum Entfernen des Hosts aus vCenter aufgefordert werden.

2 Melden Sie sich beim Dienstprogramm VDP-configure an:

   https://<*IP_Adresse_der_VDP_Appliance***>:8543/vdp-configure/**

3 Klicken Sie auf die Registerkarte **Notfallwiederherstellung**.

   Durch VDP geschützte virtuelle Maschinen sind im Dialogfeld „Notfallwiederherstellung“ aufgeführt. Hier können Sie auf die folgenden Details über die virtuellen Maschinen zugreifen:

   - **Name**: Der Name der durch die VDP-Appliance geschützten virtuellen Maschinen. Durch Klicken auf die Erweiterungspfeile können Sie Datum und Uhrzeit der letzten Wiederherstellung der ausgewählten virtuellen Maschine festlegen.
   - **Letzter bekannter Pfad**: Der letzte bekannte Speicherort der virtuellen Maschine in der vCenter-Bestandsliste. Dieser Speicherort wird aktualisiert, wenn die virtuelle Maschine verlagert wird.
   - Details der Wiederherstellungsausführung:
     - **Client Name**: Der Name des virtuellen Maschinenclients, der wiederhergestellt wird.
     - **Status**: Der Status „Erfolgreich“ oder „Fehlgeschlagen“ der Wiederherstellung
     - **Startzeit**: Der Zeitpunkt, zu dem die Wiederherstellung gestartet wurde
     - **Abschlusszeit**: Der Zeitpunkt, zu dem die Wiederherstellung abgeschlossen wurde
     - **Übertragene Byte**: Die Anzahl an Byte, die während der Wiederherstellung übertragen wurde

4 Wählen Sie die virtuelle Maschine aus, die als Wiederherstellungspunkt dienen soll, und klicken Sie auf **Wiederherstellen**.

Das Dialogfeld „Hostanmeldedaten“ wird angezeigt.

5 Geben Sie im Dialogfeld „Hostanmeldedaten“ gültige Hostanmeldedaten ein:

- **ESXi-Hostname oder -IP-Adresse**: Geben Sie den Namen oder die IP-Adresse des vSphere-Hosts ein.
- **Port - 443**: Wird standardmäßig ausgefüllt.
- **Benutzername**: Geben Sie den Benutzernamen für den vSphere-Host ein. Der empfohlene Hostbenutzername ist „root“. Für alle anderen Hostbenutzernamen muss das Benutzerkonto über eine Berechtigung zum Erstellen von virtuellen Maschinen verfügen.
- **Passwort**: Geben Sie das Passwort für den vSphere-Host ein. Bei Eingabe ungültiger Hostanmeldedaten wird eine Fehlermeldung angezeigt, und es kann keine Verbindung zum Host hergestellt werden.

HINWEIS Wenn die ausgewählte virtuelle Maschine nicht erfolgreich von vCenter getrennt wurde, wird eine Fehlermeldung angezeigt und ein Fortfahren ist nicht möglich.

6 Klicken Sie auf **OK**.

Der Bildschirm „Backup wiederherstellen“ initiiert die Wiederherstellung mit dem neuen Namen und Ziel.

7 Im Dialogfeld „Backup wiederherstellen“ werden folgende Informationen angezeigt:

- **Clientname**: Der Name des Clients, auf dem die virtuelle Maschine wiederhergestellt wird
- **Backup**: Datum und Zeitstempel der Backups
- **Neuer Name**: Das Feld, in dem ein neuer Name eingegeben werden muss. Dabei darf es sich nicht um den Namen einer bereits vorhandenen virtuellen Maschine handeln.
- **Ziel**: Der Name des vSphere-Hosts
- **Datastore**: Eine Drop-down-Liste der als Ziele verfügbaren Datenspeicher

8 Geben Sie im Feld **Neuer Name** einen neuen Namen ein. Der Name muss eindeutig sein und darf bis zu 255 Zeichen umfassen. Die folgenden Zeichen sind für den Namen nicht zulässig: ~ ! @ $ ^ % { } [ ] | , ` ; # \ / : * ? < > ' " & . Zudem dürfen keine diakritischen Zeichen verwendet werden (z. B. â, é, ì, ü und ñ).

9 Wählen Sie einen Datenspeicher als Ziel für das Backup aus.

ACHTUNG Die Kapazitätsgröße des Datenspeichers wird aufgeführt. Achten Sie darauf, einen Datenspeicher auszuwählen, der über genug Festplattenspeicher für die Wiederherstellung verfügt. Bei unzureichendem Speicherplatz schlägt die Wiederherstellung fehl.

10 Klicken Sie auf **Wiederherstellen**.

11 Überprüfen Sie anhand des Fortschritts im Dialogfeld „Letzte Aufgaben“, ob die Wiederherstellung erfolgreich übermittelt wurde.

HINWEIS Die wiederhergestellte virtuelle Maschine wird im Bestand auf Ebene des vSphere-Hosts aufgeführt. Die Wiederherstellung in einem spezifischeren Bestandspfad wird nicht unterstützt.

Automatische Hosterkennung

Bei vSphere Data Protection der Version 5.5 und niedriger müssen Benutzer vor der Durchführung einer Notfallwiederherstellung den vSphere-Host identifizieren und trennen sowie die entsprechenden Werte auffüllen. Bei vSphere Data Protection der Version 5.8 und höher erkennt die Appliance automatisch den Host, bei dem sie aktuell registriert ist, und füllt den Hostnamen oder IP-Wert im Dialogfeld „Hostanmeldedaten“ vorab auf. Hierdurch werden die Benutzer entlastet, die womöglich über mehrere Hosts in einem Cluster verfügen und die den aktuellen, vorhandenen Host zwecks Trennung von vCenter identifizieren müssen.

Bei Folgendem handelt es sich um seltene Fälle, in denen die Appliance den aktuellen Host, bei dem die Appliance registriert ist, nicht erkennt und einen älteren Wert anzeigt:

- vCenter ist nicht verfügbar und nach der Migration der VDP-Appliance auf einen anderen Host unter einem HA-fähigen Clustering zeigt die Appliance den älteren Host an, bei dem sie registriert war.
- Sobald die Appliance auf einen anderen Host migriert wurde, ist vCenter nicht mehr verfügbar. In diesem Fall kann der neue Host nicht erkannt werden, da die Appliance ein gewisses Zeitfenster benötigt, um die Ereignisse von vCenter verarbeiten und aktualisieren zu können.

In beiden Fällen müssen Benutzer manuell festlegen, bei welcher Appliance der Host registriert ist.

Aktualisieren von Wiederherstellungspunkten

1 Melden Sie sich bei der URL von VDP-configure an:

https://<*IP_Adresse_der_VDP_Appliance*>**:8543/vdp-configure/**

2 Klicken Sie auf die Registerkarte **Notfallwiederherstellung**.

3 Klicken Sie auf **Aktualisieren**.

In der Ladeleiste werden die Wiederherstellungspunkte aktualisiert.

Erneutes Verbinden des Hosts mit vCenter

1 Stellen Sie vCenter wieder her. Anweisungen finden Sie unter „Wiederherstellungsvorgänge“ auf Seite 144.

HINWEIS vCenter im wiederhergestellten Zustand ist standardmäßig ausgeschaltet.

2 Schalten Sie vCenter nach Abschluss der vCenter-Wiederherstellung ein.

3 Melden Sie sich bei der vCenter-URL an, um sich zu vergewissern, dass alle Services ausgeführt werden:

https://<*IP_Adresse_vCenter*>**:5480**

Melden Sie sich bei einem Windows-basierten vCenter als Administrator für den Server an, auf dem vCenter Server ausgeführt wird, und überprüfen Sie, ob alle Windows-Services ausgeführt werden.

4 Melden Sie sich über vSphere Client beim wiederhergestellten vCenter an:

https://<*IP_Adresse_vCenter*>**:9443/vsphere-client/**

5 Fügen Sie über vSphere Client der vCenter-Wiederherstellung den vSphere-Host hinzu.

HINWEIS Nach der Wiederherstellung von vCenter kommt es beim Start der vCenter-Services u. U. zu einer Verzögerung von ca. 20 Minuten. Während dieser Verzögerung ist es nicht möglich, einen Backup- oder Wiederherstellungsprozess erfolgreich durchzuführen. Wiederholen Sie in diesem Fall Backup oder Wiederherstellung zu einem späteren Zeitpunkt.

Schützen der Kommunikation zwischen VDP und vCenter

5

Dieses Kapitel umfasst folgende Themen:

Ersetzen des VDP-Zertifikats

Das VDP-Zertifikat für den Port 8543 kann entweder durch ein neues selbst signiertes Zertifikat oder ein CA-signiertes Zertifikat ersetzt werden.

Gehen Sie zum Ersetzen des VDP-Zertifikats wie folgt vor:

1 Halten Sie die Services an, indem Sie den folgenden Befehl ausführen:

```
root@vdp#: emwebapp.sh --stop
```

2 Löschen Sie den **Tomcat**-Alias, indem Sie den folgenden Befehl ausführen:

```
root@vdp#:/usr/java/latest/bin/keytool -delete -alias tomcat
```

3 Erzeugen Sie ein SSL-Zertifikat, indem Sie den folgenden Befehl ausführen:

```
root@vdp#:/usr/java/latest/bin/keytool -genkeypair -v -alias tomcat -keyalg
RSA -sigalg SHA256withRSA -keystore /root/.keystore -storepass changeit
-keypass changeit -validity 3650 -dname "CN=vdp.vmware, OU=VDP, O=OrgName,
L=PUNE, S=MH, C=IN"
```

4 Um ein selbst signiertes Zertifikat zu verwenden, gehen Sie weiter zu Schritt 6.

5 Um ein selbst CA-signiertes Zertifikat zu verwenden, gehen Sie wie folgt vor:

   a Erzeugen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR), indem Sie den folgenden Befehl ausführen:

   ```
   root@vdp#:/usr/java/latest/bin/keytool -certreq -keyalg RSA -alias tomcat
   -file csrFileName.csr
   ```

   b Rufen Sie durch Verwendung des CSR-Inhalts das CA-signierte Zertifikat im **.p7b**-Format ab und speichern Sie das Zertifikat.

   c Importieren Sie die p7b-Datei des verketteten Zertifikats, indem Sie den folgenden Befehl ausführen:

   ```
   root@vdp#:/usr/java/latest/bin/keytool -import -alias tomcat -keystore
   /root/.keystore -file
   /<Pfad_zum_Zertifikat>/<Dateiname_des_Kettenzertifikats.p7b>
   ```

6 Überprüfen Sie, ob der Zertifikateintrag mit dem **Tomcat**-Alias im Keystore vorhanden ist, indem Sie den folgenden Befehl ausführen:

```
root@vdp#:/usr/java/latest/bin/keytool -list -v -keystore /root/.keystore
-storepass changeit -keypass changeit
```

7 Wenn der Zertifikateintrag im Keystore vorhanden ist, führen Sie das **addFingerprint.sh**-Script aus:

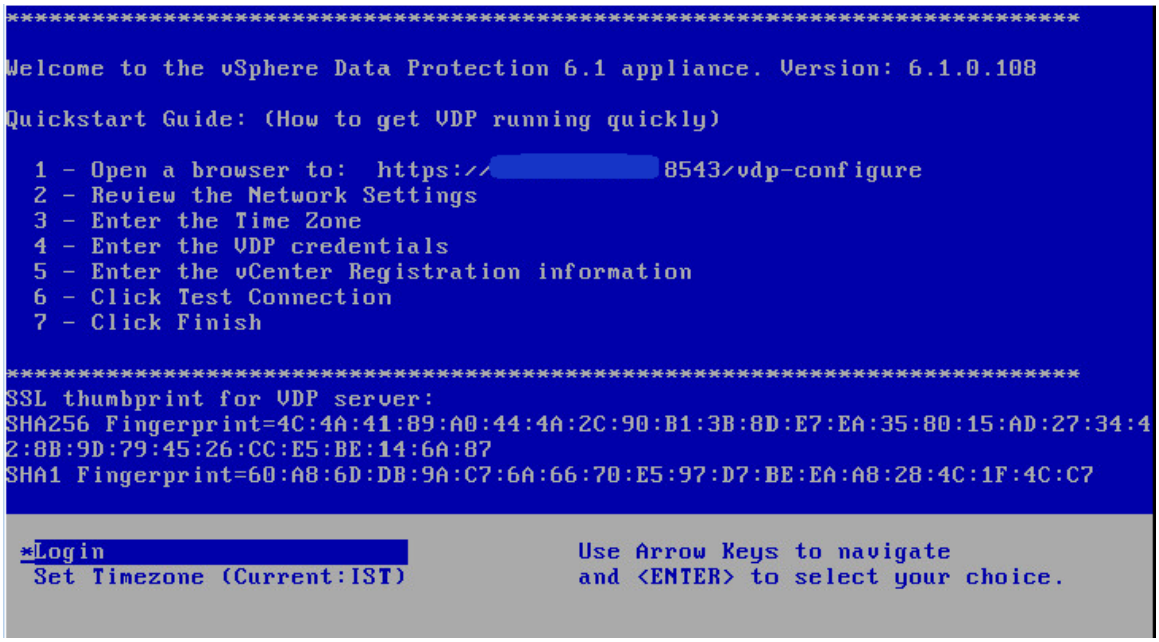
```
root@vdp#:./usr/local/avamar/bin/addFingerprint.sh
```

8 Starten Sie die Services, indem Sie den folgenden Befehl ausführen:

```
root@vdp#: emwebapp.sh --start
```

Authentifizieren des VDP-Servers für eine gesicherte Kommunikation

Um bei der Kommunikation mit dem VDP-Server Man-in-the-Middle-Angriffe (MTM) zu vermeiden und die von den Zertifikaten bereitgestellte Sicherheit vollständig zu nutzen, stellt VDP einen Fingerabdruck auf der Konsole bereit. In der folgenden Abbildung ist ein Beispielfingerabdruck dargestellt:



Stellen Sie beim Zugriff auf den VDP-Server über die URL **https://<vdp-ip>:8543/vdp-configure** sicher, dass das SSL-Zertifikat vom selben VDP-Server stammt und gültig ist. Wenn Sie überprüfen möchten, ob das SSL-Zertifikat gültig ist, stellen Sie sicher, dass der Fingerabdruck auf der Konsole und dem SSL-Zertifikat, das der Browser während des SSL-Handshake erhält, übereinstimmen. VDP verfügt über ein Standard-SSL-Zertifikat.

Zum Ändern des Standardzertifikats importieren Sie das neue Zertifikat als **privatekeyentry** in keytool an keystore.

Führen Sie nach dem Importieren des neuen Zertifikats die folgenden Schritte durch, um den aktualisierten Fingerabdruck auf der VDP-Konsole anzuzeigen:

1 Halten Sie Services mit dem folgenden Befehl an:

emwebapp.sh --stop

2 Führen Sie das Skript „addFingerprint.sh“ aus:

./usr/local/avamar/bin/addFingerprint.sh

3 Starten Sie Services mit dem folgenden Befehl:

emwebapp.sh -start

4 Starten Sie die VDP-Appliance neu.

Sichern der Kommunikation der VDP-Appliance mit dem vCenter-Server

Die VDP-Appliance kann HTTPS-Verbindungen mit dem vCenter-Server für verschiedene Zwecke mit oder ohne SSL-Zertifikatüberprüfung herstellen. Wird ein SSL-Zertifikat nicht überprüft, sind der vCenter-Server und die VDP-Appliance für Man-in-the-Middle-Angriffe anfällig. VDP unterstützt jetzt das Hochladen des vCenter-Serverzertifikats oder das Signieren des Zertifikats in den VDP-Zertifikat-Repositories während des Registrierungsprozesses beim vCenter-Server. Das Zertifikat wird dann verwendet, um den vCenter-Server in allen folgenden HTTPS-Verbindungen zu authentifizieren und ihm zu vertrauen, einschließlich Testverbindungen mit dem vCenter-Server, wodurch die VDP-Appliance gesichert wird.

Voraussetzungen

Laden Sie das vCenter-Zertifikat im Format **.p7b**, **.cer** oder **.crt** über die folgende URL herunter:

https://<*vCenter_IP_Adresse*>**/sdk**

Verfahren

- Für die Erstkonfiguration:
  a. Öffnen Sie den Assistenten für die Erstkonfiguration über die folgende URL:

     https:<*IP_Adresse_der_VDP_Appliance*>**:8543/vdp-configure/**

  b. Gehen Sie auf der Seite **vCenter-Registrierung** wie folgt vor:

     i. Geben Sie die vCenter-Informationen wie Anmeldedaten, Hostname oder IP-Adresse und Portnummern in die entsprechenden Felder ein.

     ii. Wählen Sie **vCenter-Zertifikat überprüfen** aus.

     Wenn Sie die Kommunikation der VDP-Appliance mit vCenter nicht sichern möchten, deaktivieren Sie **vCenter-Zertifikat überprüfen**. Bei Deaktivierung dieser Option wird das vCenter-Zertifikat nicht überprüft.

     iii. Klicken Sie auf **Hochladen** und wählen Sie das heruntergeladene vCenter-Zertifikat aus.

     iv. Klicken Sie auf **Verbindung prüfen**.

     Wenn das vCenter-Zertifikat gültig ist, wird die Verbindung mit vCenter hergestellt. Andernfalls schlägt die Verbindung fehl.

- Für die erneute vCenter-Registrierung:
  a. Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

     https:<*IP_Adresse_der_VDP_Appliance*>**:8543/vdp-configure/**

  b. Klicken Sie auf der Registerkarte **Konfiguration** auf das Symbol für die Einstellungen und wählen Sie **vCenter-Registrierung** aus.

     Der Assistent **vCenter-Registrierung** wird angezeigt.

  c. Wählen Sie auf der Seite **vCenter-Registrierung** die Option **Ich habe die Informationen überprüft. Ich möchte vCenter erneut konfigurieren.** aus und klicken Sie auf **Weiter**.

  d. Gehen Sie auf der Seite **vCenter-Konfiguration** wie folgt vor:

     i. Geben Sie die vCenter-Informationen wie Anmeldedaten, Hostname oder IP-Adresse und Portnummern in die entsprechenden Felder ein.

     ii. Wählen Sie **vCenter-Zertifikat überprüfen** aus.

     iii. Klicken Sie auf **Hochladen** und wählen Sie das heruntergeladene vCenter-Zertifikat aus.

     iv. Klicken Sie auf **Weiter**.

e Überprüfen Sie die Informationen auf der Seite **Bereit zur Fertigstellung** und klicken Sie auf **Fertig stellen**.

Wenn das vCenter-Zertifikat und andere Informationen gültig sind, wird die Verbindung mit vCenter hergestellt. Andernfalls schlägt die erneute Registrierung fehl.

Sichern der Proxykommunikation mit dem vCenter-Server

Standardmäßig führen der VDP-Server-Managementservice und Proxys beim Verbinden mit vCenter Server keine Validierung der SSL-Zertifikate durch. Dies macht vCenter Server ggf. gegenüber Man-in-the-Middle Exploits (MITM) anfällig, was zu einem unbefugten Zugriff auf vCenter Server führen kann. Mit der Konfiguration jedes Proxys zur Verwendung der SSL-Zertifikatauthentifizierung bei Verbindung mit vCenter Server wird diese Schwachstelle behoben.

Voraussetzungen

Vergewissern Sie sich, dass ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat auf vCenter Server installiert ist.

http://kb.vmware.com/kb/2034833 bietet Informationen über die Erstellung eines CA-signierten Zertifikats und dessen Installation auf dem vCenter-Server sowie die Implementierung des CA-signierten Zertifikats in einer vSphere 5.1- oder 5.5-Umgebung.

http://kb.vmware.com/kb/2111219 bietet Informationen über die Ersetzung der Standardzertifikate mit den CA-signierten SSL-Zertifikaten in einer vSphere 6.0-Umgebung.

Verfahren

1 Öffnen Sie eine Befehls-Shell und melden Sie sich beim Proxy als `root` an.

2 Kopieren Sie das vCenter-Server-Zertifikat in das Verzeichnis `/usr/local/avamarclient/bin` auf dem Proxy.

- Für einen Linux vCenter:
  - vCenter 5.x:
    - Serverzertifikat: `/etc/vmware-vpx/ssl/rui.crt`
    - Stammzertifikat: `/etc/vmware-vpx/ssl/rui-ca-cert.pem`
  - vCenter 6.0:
    - Serverzertifikat: `/etc/vmware-vpx/ssl/rui.crt`
    - Stammzertifikat: `/var/lib/vmware/vmca/root.cer`

  Führen Sie eine SCP des geeigneten vCenter-Zertifikats im Verzeichnis `/usr/local/avamarclient/bin` auf dem Proxy durch.

  Verwenden Sie im Falle eines selbst signierten Zertifikats nur das Serverzertifikat.

  Erstellen Sie im Falle eines CA-signierten Zertifikats ein verkettetes Zertifikat, indem Sie den folgenden Befehl ausführen:

  cat rui.crt root.cer > chain_cert.pem

- Für einen Windows vCenter:
  - vCenter 5.x:
    - Serverzertifikat: `C:\ProgramData\VMware\VMware VirtualCenter\SSL\rui.crt`
    - Stammzertifikat: `C:\ProgramData\VMware\VMware VirtualCenter\SSL\cacert.pem`
  - vCenter 6.0:

- Serverzertifikat: `C:\ProgramData\VMware\vCenterServer\cfg\vmware-vpx\ssl\rui.crt`
- Stammzertifikat: `C:\ProgramData\VMware\vCenterServer\data\vmca\root.cer`

Führen Sie eine SCP des geeigneten vCenter-Zertifikats im Verzeichnis `/usr/local/avamarclient/bin` auf dem Proxy durch.

Verwenden Sie im Falle eines selbst signierten Zertifikats nur das Serverzertifikat.

Erstellen Sie im Falle eines CA-signierten Zertifikats ein verkettetes Zertifikat, indem Sie den folgenden Befehl ausführen:

cat rui.crt root.cer > chain_cert.pem

HINWEIS Kopieren Sie bei Verwendung eines verketteten SSL-Zertifikats für vCenter die Datei **chain.pem**, die alle Zertifikate in der Kette enthält, in das Verzeichnis `/usr/local/avamarclient/bin` des Proxys.

3 Legen Sie die entsprechenden Betriebssystemberechtigungen fest, indem Sie Folgendes eingeben:

chmod 600 /usr/local/avamarclient/bin/<*certificate_file*>

wobei *certificate_file* entweder ein Serverzertifikat oder ein verkettetes Zertifikat ist.

4 Öffnen Sie `/usr/local/avamarclient/var/avvcbimageAll.cmd` in einem UNIX-Texteditor.

5 Fügen Sie den folgenden Inhalt am Ende der Datei hinzu:

--ssl_server_authentication_file=/usr/local/avamarclient/bin/<*certificate_file*>

wobei *certificate_file* entweder ein Serverzertifikat oder ein verkettetes Zertifikat ist.

HINWEIS Verwenden Sie **chain.pem** für ein verkettetes vCenter-SSL-Zertifikat.

6 Speichern Sie die Änderungen und schließen Sie `avvcbimageAll.cmd`.

7 Öffnen Sie `/usr/local/avamarclient/var/avvmwfileAll.cmd` in einem UNIX-Texteditor.

8 Fügen Sie den folgenden Inhalt am Ende der Datei hinzu:

--ssl_server_authentication_file=/usr/local/avamarclient/bin/<*certificate_file*>

wobei *certificate_file* entweder ein Serverzertifikat oder ein verkettetes Zertifikat ist.

HINWEIS Verwenden Sie **chain.pem** für ein verkettetes vCenter-SSL-Zertifikat.

9 Speichern Sie die Änderungen und schließen Sie `avvmwfileAll.cmd`.

10 Öffnen Sie `/etc/vmware/config` in einem UNIX-Texteditor.

11 Fügen Sie die folgenden Inhalte am Ende der Datei hinzu:

vix.enableSslCertificateCheck = "true"

vix.sslCertificateFile = "/usr/local/avamarclient/bin/<*certificate_file*>"

wobei *certificate_file* entweder ein Serverzertifikat oder ein verkettetes Zertifikat ist.

12 Speichern Sie die Änderungen und schließen Sie `/etc/vmware/config`.

13 Öffnen Sie `/usr/local/avamarclient/var/vddkconfig.ini` in einem UNIX-Texteditor.

14 Ändern Sie den Wert **vixDiskLib.linuxSSL.verifyCertificates** von **0** zu **1**.

15 Speichern Sie die Änderungen und schließen Sie `vddkconfig.ini`.

16 Vergewissern Sie sich, dass auf diesem Proxy derzeit weder Backup- noch Wiederherstellungsjobs ausgeführt werden.

17 Starten Sie die `avagent`- und `vmwareflr`-Services neu, indem Sie die folgenden Befehle ausführen:

service avagent-vmware restart

service vmwareflr restart

Ergebnis

Der Proxy verwendet und validiert SSL-Zertifikate beim Verbinden mit dem vCenter Server.

Wiederholen Sie dieses Verfahren für jeden Proxy, den Sie in der vCenter-Umgebung bereitstellen.

Konfigurieren von VDP

6

In diesem Kapitel werden folgende Themen behandelt:

Anmeldesicherheit

Zur Verstärkung der Sicherheit des VDP-Konfigurationsdienstprogramms wird das Programm nach 5 fehlgeschlagenen Anmeldeversuchen eines Benutzers für 5 Minuten gesperrt. Hierdurch werden in dieser Zeit sämtliche Anmeldeversuche verhindert. Vorhandene Sitzungen mit bestehenden Anmeldungen sind hiervon nicht betroffen.

Im Falle einer Sperre geschieht Folgendes:

- Das VDP-Konfigurationsdienstprogramm informiert den Benutzer während eines Anmeldeversuchs.
- Es wird ein vCenter-Ereignis in Bezug auf die Sperre erzeugt.
- In der Datei `vdp-configure.log` werden die Zeit, der Benutzer, die Quelladresse und die Anforderungsheader der fehlgeschlagenen Anmeldeversuche, die zu der Sperre geführt haben, erfasst.

  Melden Sie sich zum Anzeigen der Datei `vdp-configure.log` über den Terminal- oder Konsolenadministratorbenutzer und ein Standardpasswort bei der VDP-Appliance an.

Konfigurieren des Customer Experience Improvement Program

Das Customer Experience Improvement Program ist eine Option, die es Ihnen ermöglicht, verschlüsselte Konfigurations- und Nutzungsinformationen zur VDP-Umgebung zwecks Analyse an VMware-Server zu senden.

HINWEIS Das Customer Experience Improvement Program (PhoneHome) wird in einer reinen vSphere Data Protection-IPv6-Umgebung nicht unterstützt.

VDP sendet die folgenden Arten von Daten an VMware:

- Versionsinformationen für VDP und vSphere
- VDP-Zeitzone und -Verfügbarkeit
- Anzahl geschützter und ungeschützter VMs
- Menge der konfigurierten Kapazität
- Verwendung von Data Domain (wahr/falsch)
- Kapazitätsauslastung
- Anzahl von konfigurierten und registrierten internen und externen Proxys
- Anzahl der Arbeitsaufträge pro vom Benutzer konfigurierten Proxy
- Wartungs- und Managementstatus
- Datum des letzten gültigen Kontrollpunkts
- Verwendete Agents (SQL Server, Exchange, Exchange GLR/DAG und SharePoint)
- Letzter Integritätskontrollpunktstatus
- VDP-Status
- Details zu Jobfehlern mit Zeitstempel und Fehlercode
- Anzahl der fehlgeschlagenen Jobs für jeden Fehlercode

Während der VDP-Installation können Sie das Customer Experience Improvement Program auf der Seite „Produktverbesserung“ im VDP-Konfigurationsdienstprogramm aktivieren. Die Seite „Produktverbesserung“ umfasst das Kontrollkästchen **Customer Experience Improvement Program aktivieren**. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Das Customer Experience Improvement Program kann jederzeit nach der Installation aktiviert oder deaktiviert werden, indem Sie über einen Webbrowser auf das VDP-Dienstprogramm für die Konfiguration zugreifen.

Voraussetzungen

Bei Netzwerken, die von einer Firewall geschützt werden, müssen Sie möglicherweise das Netzwerk ändern, um Konnektivitätsprobleme zu vermeiden, wenn das Customer Experience Improvement Program versucht, Daten auf den VMware-Server hochzuladen. Damit die Firewall das Customer Experience Improvement Program nicht am Hochladen von Daten auf den VMware-Server hindert, öffnen Sie das Netzwerk für die folgenden VMware-Server:

- https://vcsa.vmware.com:443
- https://phtransfer.vmware.com:443

Verfahren

1 Öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

https://<**IP_Adresse**_der_VDP_Appliance>:8543/vdp-configure/

2 Melden Sie sich mit dem VDP-Benutzernamen und -Passwort an.

3 Klicken Sie auf der Registerkarte **Konfiguration** auf das Symbol und wählen Sie **Produktverbesserung** aus.

Die Seite **Produktverbesserung** wird angezeigt.

4 Aktivieren oder deaktivieren Sie das Customer Experience Improvement Program durch Aktivieren oder Deaktivieren des Kontrollkästchens **Customer Experience Improvement Program aktivieren**.

Konfigurieren und Monitoring

Über vSphere Web Client lassen sich neben Appliance- und Speicherinformationen auch Konfigurationsdetails für das Backupzeitfenster anzeigen und ändern. Darüber hinaus ist es möglich, die VDP-Appliance für eine geplante Sendung von E-Mail-Berichten zu konfigurieren.

Anzeigen der Backup-Appliance-Konfiguration

Die Backup-Appliance-Informationen bieten Daten zur Backup-Appliance, eine Speicherzusammenfassung und die Backupzeitfensterkonfiguration. Die Backup-Appliance-Informationen umfassen Folgendes:

- Anzeigename
- Produktname
- IP-Adresse
- Hauptversion (VDP-Versionsnummer)
- Nebenversion (Nutzung durch den technischen Support)
- Status
- Host
- vCenter Server
- VDP-Backupbenutzer
- VDP-Appliance-Zeit
- Zeitzone

Diese Optionen werden während der Installation der VDP-Appliance konfiguriert. Sie lassen sich über das Dienstprogramm VDP-configure bearbeiten. Zusätzliche Informationen finden Sie unter „Konfiguration der VDP-Appliance nach der Installation“ auf Seite 37.

Die VDP-Appliance-Speicherzusammenfassung umfasst Folgendes:

- **Kapazität**: Die Gesamtkapazität der VDP-Appliance
- **Freier Speicherplatz**: Die Menge des für Backups verfügbaren Speicherplatzes
- **Deduplizierte Größe**: Die von Backups im deduplizierten Format belegte Menge an Festplattenspeicher
- **Nicht deduplizierte Größe:** Die Menge an Festplattenspeicher, die die Backups beim Konvertieren in ein natives, nicht dedupliziertes Format belegen würden.

HINWEIS Klicken Sie zum Aktualisieren der Daten auf der Seite auf das Symbol zum Aktualisieren neben **Speicherzusammenfassung**.

Auf der linken Seite wird eine Farbcontainervariante zum Prüfen der VDP-Kapazität angezeigt:

- Wenn die genutzte Speicherkapazität unter 80 % liegt, ist der Container grün.
- Wenn die genutzte Speicherkapazität zwischen 80 % und 95 % liegt, ist der Container gelb. Es wird folgende Meldung angezeigt:

  `Der VDP-Speicher ist fast voll.`
- Wenn die genutzte Speicherkapazität zwischen 95 % und 100 % liegt, ist der Container rot. Es wird folgende Meldung angezeigt:

  `Der VDP-Speicher ist fast voll.`
- Wenn die genutzte Speicherkapazität bei 100 % liegt, ist der Container rot. Es wird folgende Meldung angezeigt:

  `Der VDP-Speicher ist voll.`

HINWEIS Wenn der VDP-Konfiguration ein Data Domain-System hinzugefügt wird, wird die Data Domain-Speicherzusammenfassung ebenfalls angezeigt.

In Abbildung 6-3 ist die Konfiguration des Backupzeitfensters dargestellt.

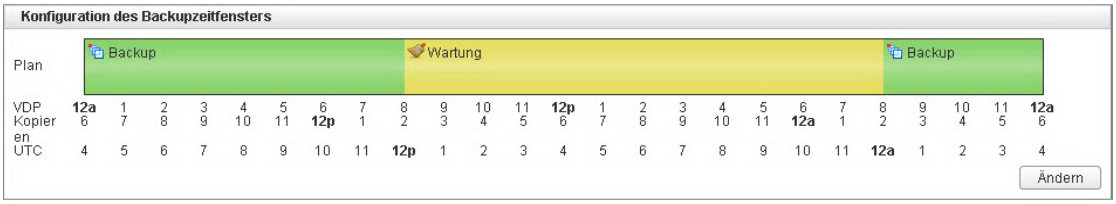


Abbildung 6-3. Konfiguration des Backupzeitfensters

Jeder 24 Stunden umfassende Tag ist in zwei Betriebszeitfenster unterteilt:

- **Backupzeitfenster:** Der Teil jedes Tags, der zur Durchführung von normal geplanten Backups reserviert ist.
- **Wartungszeitfenster:** Der Teil jedes Tags, der zur Ausführung routinemäßiger VDP-Wartungsaktivitäten wie Integritätsprüfungen reserviert ist. Sehen Sie von der Backupplanung bzw. Ausführung eines Vorgangs „Jetzt sichern“ ab, während sich VDP im Wartungsmodus befindet. Die Backupjobs werden zwar ausgeführt, sie belegen jedoch von VDP zur Wartung benötigte Ressourcen.

  Die Jobs, die beim Start oder während des Wartungszeitfensters ausgeführt werden, werden weiterhin ausgeführt.

HINWEIS Da das Ausfallzeitfenster nicht mehr vorhanden ist, werden Aktivitäten wie Integritätsprüfungen und die automatische Speicherbereinigung nun kontinuierlich im Wartungszeitfenster ausgeführt.

Bearbeiten des Backupzeitfensters

Sie können die zur Verarbeitung von Backupanforderungen verfügbare Zeit ändern.

Voraussetzungen

- VDP ist installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Verfahren

1 Stellen Sie eine Verbindung zur VDP-Appliance her. „Zugriff auf VDP" auf Seite 116 bietet Informationen dazu.

2 Wählen Sie in der VDP-Benutzeroberfläche die Registerkarte **Konfiguration** aus (standardmäßig befinden Sie sich in der Backup-Appliance-Ansicht).

3 Klicken Sie unten rechts in der Backup-Appliance-Ansicht auf die **Schaltfläche** Bearbeiten.

Die Optionen „Backupstartzeit" und „Backupdauer" werden angezeigt, wie in Abbildung 6-4 dargestellt:

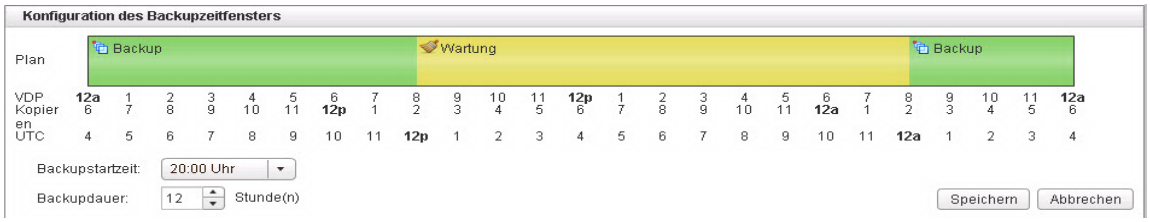


Abbildung 6-4. Backupzeitfensterkonfiguration im Bearbeitungsmodus

4 Wählen Sie die Startzeit für das Backupzeitfenster über den Drop-down-Pfeil.

5 Geben Sie die für das Backupzeitfenster gültige Dauer ein. Das minimale Backupzeitfenster beträgt 4 Stunden, das maximale Backupzeitfenster beträgt 16 Stunden.

6 Klicken Sie auf **Speichern**.

Über ein Dialogfeld werden Sie über die erfolgreiche Speicherung der Einstellungen informiert.

7 Klicken Sie auf **OK**.

VDP ändert die Konfiguration des Backupzeitfensters.

Konfigurieren von E-Mail-Benachrichtigungen und Berichten

VDP kann so konfiguriert werden, dass SMTP-E-Mail-Berichte an angegebene Empfänger gesendet werden. Wenn Sie E-Mail-Berichte aktiviert haben, werden E-Mail-Nachrichten mit den folgenden Informationen gesendet:

- Elemente, für die Ihre Aufmerksamkeit erforderlich ist
- VDP-Appliance-Status
- Zusammenfassung Backupjobs
- Zusammenfassung zu virtuellen Maschinen
- Replikationszusammenfassung
- Ungeschützte virtuelle Maschinen

HINWEIS Die E-Mail-Benachrichtigungsfunktion von VDP unterstützt weder Cc-/Bcc-Kopien noch SSL-Zertifikate.

Voraussetzungen

- VDP ist installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.
- Das E-Mail-Konto für E-Mail-Benachrichtigungen und Berichte muss vorhanden sein.

Verfahren

1 Stellen Sie eine Verbindung zur VDP-Appliance her. „Zugriff auf VDP" auf Seite 116 bietet Informationen dazu.

2 Wählen Sie in der VDP-Benutzeroberfläche die Registerkarte **Konfiguration** aus.

3 Wählen Sie **E-Mail** aus und klicken Sie auf **Bearbeiten**.

4 Geben Sie die folgenden Felder an:

- **E-Mail-Berichte aktivieren**: Aktivieren Sie diese Option, um E-Mail-Berichte zu aktivieren.
- **Postausgangsserver**: Geben Sie den Namen des SMTP-Servers ein, der zum Senden von E-Mails verwendet werden soll. Dieser Name kann als IP-Adresse, Hostname oder vollständig qualifizierter Domainname eingegeben werden. Die VDP-Appliance muss den von Ihnen eingegebenen Namen auflösen können.

  Der Standardport für nicht authentifizierte E-Mail-Server lautet 25. Der Standardport für authentifizierte E-Mail-Server lautet 587. Sie können einen anderen Port angeben, indem Sie dem Servernamen einen Doppelpunkt (:) und eine Portnummer anhängen. Um beispielsweise festzulegen, dass der Port 8025 für den Server „emailserver" verwendet werden soll, geben Sie Folgendes ein: emailserver:8025.
- (Optional) **Mein Server erfordert eine Anmeldung**: Wählen Sie diese Option aus, wenn für Ihren SMTP-Server eine Authentifizierung erforderlich ist.
- **Benutzername**: Geben Sie den Benutzernamen ein, mit dem Sie sich authentifizieren möchten.
- **Passwort**: Geben Sie das mit dem Benutzernamen verknüpfte Passwort ein.

  VDP validiert das Passwort nicht. Das von Ihnen eingegebene Passwort wird direkt an den E-Mail-Server übergeben.
- **Absenderadresse**: Geben Sie die E-Mail-Adresse ein, von der der E-Mail-Bericht stammen soll. Hier kann nur eine einzige Adresse festgelegt werden.
- **Empfängeradresse(n)**: Geben Sie eine durch Kommas getrennte Liste von bis zu 10 E-Mail-Adressen ein.
- **Sendezeit**: Wählen Sie aus der Drop-down-Liste den Zeitpunkt aus, zu dem VDP die Berichte per E-Mail versenden soll.
- **Sendetag(e)**: Wählen Sie die Tage aus, an denen die Berichte gesendet werden sollen.
- **Berichtgebietsschema**: Wählen Sie das Land für die E-Mail-Berichte aus.
- **CSV-Anhang aktivieren**: Wählen Sie diese Option aus, wenn Sie den E-Mail-Bericht als Anhang im CSV-Format erhalten möchten.
- **VDP-Alarm per E-Mail-Benachrichtigung aktivieren**: Wählen Sie diese Option aus, um den VDP-Alarm per E-Mail-Benachrichtigung zu aktivieren. Wenn Sie diese Option auswählen, sendet VDP eine E-Mail-Benachrichtigung, wenn der VDP-Alarm ausgelöst wird oder ein veröffentlichtes Ereignis den VDP-Alarmstatus von gelb zu rot ändert.

5 Klicken Sie auf die Schaltfläche **Speichern**.

6 Um Ihre E-Mail-Konfiguration zu testen, klicken Sie auf **Test-E-Mail senden**.

Anzeigen des Benutzeroberflächenprotokolls

Wenn Sie auf der Registerkarte **Konfiguration** auf **Protokoll** klicken, wird das Benutzeroberflächenprotokoll für VDP angezeigt. Hierbei handelt es sich um ein Übersichtsprotokoll, in dem die in der Benutzeroberfläche initiierten Aktivitäten aufgeführt und verschiedene wichtige Statuselemente identifiziert werden.

Klicken Sie auf **Ansicht exportieren**, um die auf dem Bildschirm angezeigten Details in einer Datei auf dem Rechner zu speichern, auf dem Ihr Browser ausgeführt wird.

Ausführlichere Protokolle können über das VDP-Konfigurationsdienstprogramm heruntergeladen werden. Anweisungen finden Sie unter „Sammeln von VDP-Protokollen oder Diagnoseinformationen" auf Seite 40.

Ausführen einer Integritätsprüfung

Durch Integritätsprüfungen wird die Datenintegrität im Deduplizierungsspeicher überprüft und bewahrt. Am Ende einer Integritätsprüfung steht ein Kontrollpunkt. Standardmäßig führt VDP jeden Tag eine Integritätsprüfung während des Wartungszeitfensters durch. Außerdem können Sie die Integritätsprüfung manuell starten.

ACHTUNG Wenn die VDP-Appliance einen Alarm ausgibt, wonach die letzte gültige Integritätsprüfung fehlgeschlagen oder veraltet ist, führen Sie eine manuelle Integritätsprüfung durch. Wenn Sie zulassen, dass die VDP-Appliance trotz veralteter Integritätsprüfung weiterhin Backups durchführt, besteht das Risiko eines potenziellen Verlusts von Backupdaten, sollte einmal ein Rollback auf den letzten validierten Kontrollpunkt erforderlich sein.

Eine Aufstellung aller VDP-Kontrollpunkte kann über das Dienstprogramm VDP-configure, Registerkarte **Rollback**, angezeigt werden. Zusätzliche Informationen finden Sie unter „Rollback einer Appliance" auf Seite 43.

Voraussetzungen

- VDP ist installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Verfahren

1. Stellen Sie eine Verbindung zur VDP-Appliance her. „Zugriff auf VDP" auf Seite 116 bietet Informationen dazu.
2. Klicken Sie auf der Registerkarte **Konfiguration** der VDP-Benutzeroberfläche auf das Symbol  und wählen Sie **Integritätsprüfung ausführen** aus.

   Über einen Bestätigungsbildschirm werden Sie gefragt, ob Sie eine manuelle Integritätsprüfung ausführen möchten.
3. Klicken Sie auf **Ja**.

   Über eine Meldung werden Sie informiert, dass die Integritätsprüfung initiiert wurde.
4. Klicken Sie auf **OK**.

   VDP startet die Integritätsprüfung.
5. Überwachen Sie den Fortschritt der Integritätsprüfung über das Fenster „Letzte Aufgaben".

HINWEIS Während der VDP-Integritätsprüfung wird der Wartungsservice gestoppt. Dies führt eventuell zu einem temporären VDP-Fehler. Warten Sie auf den Abschluss der Integritätsprüfung. Der Wartungsservice wird dann automatisch neu gestartet, und die VDP-Fehlermeldung wird nicht mehr angezeigt.

Überwachen der VDP-Aktivität

Sie können die Aktivitäten der VDP-Appliance mit einer der folgenden Methoden überwachen:

- „Anzeigen letzter Aufgaben" auf Seite 64 dargestellt.
- „Anzeigen von Alarmen" auf Seite 65
- „Anzeigen der Ereigniskonsole" auf Seite 66

Von VDP generierten Aufgaben, Ereignissen und Alarmen ist die Zeichenfolge „VDP:" vorangestellt. Manche Aufgaben und Events, die im Rahmen der VDP-Prozesse auftreten, werden jedoch von vCenter Server ausgeführt und haben kein Präfix.

Wenn VDP beispielsweise einen geplanten Backupjob für eine laufende virtuelle Maschine ausführt, werden die folgenden Aufgabeneinträge erstellt:

1 Snapshot der virtuellen Maschine erstellen (vCenter agiert auf der zu sichernden virtuellen Maschine)

2 VDP: Geplanter Backupjob (VDP startet den Backupjob)

3 Virtuelle Maschine neu konfigurieren (die VDP-Appliance fordert Services vom virtuellen Center an)

4 Snapshot entfernen (virtuelles Center agiert auf der virtuellen Maschine mit abgeschlossenem Backup)

Um ausschließlich VDP-generierte Aufgaben oder Ereignisse in der Aufgaben- bzw. Ereigniskonsole anzuzeigen, geben Sie „VDP**:"** im Feld **Filter** ein.

Anzeigen letzter Aufgaben

VDP generiert beim Ausführen der folgenden Vorgänge Aufgabeneinträge im Fenster „Letzte Aufgaben":

- Backups
- Automatische Backupverifizierung
- Wiederherstellungen
- Replikationen
- Replikations-Recovery
- VDP-Konfiguration
- Integritätsprüfungen

Durch Klicken auf einen Aufgabeneintrag im Fenster „Letzte Aufgaben" werden in dem unten auf dem Bildschirm vorhandenen Fenster Aufgabendetails angezeigt. Aufgabendetails können ebenfalls angezeigt werden, indem Sie auf der Registerkarte **Wird ausgeführt** unter **Letzte Aufgaben** auf den Link neben dem Symbol der virtuellen Maschine klicken.

Sie können die Aufgaben auch über den Aufgabenjobbereich **Wird ausgeführt** abbrechen, indem Sie auf das Symbol zum Abbrechen von Aufgaben klicken.

Anzeigen von Alarmen

In Tabelle 6-10 sind die Alarme aufgeführt, die die vSphere Data Protection(VDP)-Appliance auslösen kann:

Tabelle 6-10. vSphere Data Protection – Alarme

Alarmbezeichnung	Alarmbeschreibung
VDP: [001] Der letzte Kontrollpunkt für die VDP-Appliance ist veraltet.	Klicken Sie auf der Registerkarte **Konfiguration** der VDP-Benutzeroberfläche auf das Symbol „Alle Aktionen“ und wählen Sie „Integritätsprüfung ausführen“ aus.
VDP: [002] Die VDP-Appliance ist fast voll.	Der Speicherplatz der VDP-Appliance ist für zusätzliche Backups bald nicht mehr ausreichend. Zum Freigeben von Speicherplatz auf der Appliance können Sie unnötige oder ältere Backups manuell löschen und die Aufbewahrungs-Policies für Backupjobs ändern, um die Aufbewahrungszeit für Backups zu verkürzen.
VDP: [003] Die VDP-Appliance ist voll.	Der VDP-Speicher ist voll. Die Appliance wird im schreibgeschützten Modus ausgeführt, bis Sie zusätzlichen Speicherplatz bereitstellen. Sie können Speicherplatz freigeben, indem Sie unnötige oder ältere Backups löschen.
VDP: [004] Die Kapazitätsgrenze des VDP-Appliance-Datenspeichers ist fast erreicht.	Der Datenspeicher, in dem die VDP-Appliance ihre Festplatten bereitgestellt hat, nähert sich seiner maximalen Kapazitätsgrenze. Wenn die maximale Kapazitätsgrenze des Datenspeichers erreicht wurde, wird die VDP-Appliance angehalten. Die Appliance kann erst fortfahren, nachdem auf dem Datenspeicher zusätzlicher Speicherplatz zur Verfügung gestellt wurde.
VDP: [005] Kernservices werden nicht ausgeführt.	Starten Sie die Kernservices mithilfe des Dienstprogramms für die VDP-Konfiguration.
VDP: [006] Managementservices werden nicht ausgeführt.	Starten Sie die Managementservices mithilfe des Dienstprogramms für die VDP-Konfiguration.
VDP: [007] Dateisystemservices werden nicht ausgeführt (unterstützt von der VDP-Version 5.5 und niedriger).	Starten Sie die Dateisystemservices mithilfe des Dienstprogramms für die VDP-Konfiguration. HINWEIS: Dieser Alarm wird in VDP-Version 5.8 oder höher nicht unterstützt.
VDP: [008] Services für die Wiederherstellung auf Dateiebene werden nicht ausgeführt.	Starten Sie die Services für die Wiederherstellung auf Dateiebene mithilfe des Dienstprogramms VDP-configure.
VDP: [009] Wartungsservices werden nicht ausgeführt.	Starten Sie die Wartungsservices mithilfe des Dienstprogramms VDP-configure.
VDP: [010] Backupplaner wird nicht ausgeführt.	Starten Sie den Backupplaner mithilfe des Dienstprogramms VDP-configure.
VDP: [013] Grenzwert geschützter virtueller Maschinen überschritten.	Die unterstützte Anzahl geschützter virtueller Maschinen wurde überschritten.
VDP: [014] Backup-Recovery-Services werden nicht ausgeführt.	Starten Sie die Backup-Recovery-Services mithilfe des Dienstprogramms für die VDP-Konfiguration.
VDP: [015] Replikationsservices werden nicht ausgeführt.	Starten Sie die Replikationsservices mithilfe des Dienstprogramms für die VDP-Konfiguration.
VDP:[016] Der Data Domain-Speicher ist fast voll.	Der Data Domain-Speicher ist fast voll. Zum Freigeben von Speicherplatz im Data Domain-Speicher können Sie unnötige oder ältere Backups manuell löschen und die Aufbewahrungs-Policies für Backupjobs ändern, um die Aufbewahrungszeit für Backups zu verkürzen.
VDP:[017] Der Data Domain-Speicher ist voll.	Der Data Domain-Speicher ist voll. Sie können Speicherplatz freigeben, indem Sie unnötige oder ältere Backups manuell löschen.

Anzeigen der Ereigniskonsole

VDP kann Ereignisse der folgenden Typen generieren: Info, Fehler und Warnung. Im Folgenden sind Beispiele für diese Ereignistypen aufgeführt:

- **Info:** „VDP: Wichtiger VM-Backupjob erstellt."
- **Warnung:** „VDP: Clienthost 123 konnte dem Backupjob „Wichtige VMs" nicht hinzugefügt werden, da ..."
- **Error:** „VDP: Appliance von „Vollzugriff" zu „Schreibgeschützt" gewechselt."

VDP generiert Ereignisse bei allen Statusänderungen in der Appliance. Allgemein gilt, dass Statusänderungen, die die Funktionen der Appliance beeinträchtigen, als Fehler bezeichnet werden, während Statusänderungen, die die Funktionen verbessern, als Informationsmeldung bezeichnet werden. Beim Starten einer Integritätsprüfung generiert VDP beispielsweise ein Ereignis, das als Fehler bezeichnet ist, da die Appliance vor Ausführung der Integritätsprüfung auf den Status „Schreibgeschützt" gesetzt wurde. Nach der Integritätsprüfung generiert VDP ein als Informationsmeldung bezeichnetes Ereignis, da der Status der Appliance von „Schreibgeschützt" in „Vollzugriff" wechselt.

Durch Klicken auf einen Ereigniseintrag werden die Details zu diesem Ereignis angezeigt. Hierzu gehört ein Link zum **Anzeigen** verwandter Ereignisse.

Persistente und Pop-up-Meldungen zum Anzeigen des Kapazitätsauslastungsproblems

Wenn entweder die VDP-Appliance-Speicher- oder die Data Domain-Speichernutzung an einem kritischen Punkt ist, wird in vSphere Web Client eine Warnleiste mit einer Meldung angezeigt. Der Text und das Symbol in der Meldung hängen von der Menge der Speicherauslastung ab. Derselbe Text und dasselbe Symbol werden im Abschnitt **Speicherzusammenfassung** der Registerkarte **Konfiguration** angezeigt.

Sie können die Warnleiste über die Kontrolle zum Ausblenden/Einblenden unter der Warnleiste entweder aus- oder einblenden. Das Ausblenden und Einblenden der Warnleiste ist mit Einblende- und Größenänderungseffekten animiert.

Ein Symbol, das auf eine Meldung mit hohem Schweregrad hinweist, wird auf der linken Seite des Steuerelements zum Ausblenden/Einblenden angezeigt. Wenn Sie die Warnleiste ausgeblendet haben, wird das Symbol für die Meldung mit hohem Schweregrad angezeigt, damit Sie die Kapazitätswarnungen bestätigen können.

Außerdem enthält die Warnleiste auf der rechten Seite den Link **Konfiguration – Backup-Appliance**. Wenn Sie auf den Link klicken, wird der Bereich **Backup-Appliance** auf der Registerkarte **Konfiguration** angezeigt und der Link auf der Warnleiste wird ausgeblendet.

Wenn die Speicherauslastung nicht kritisch ist, werden die Warnleiste und das Steuerelement zum Ausblenden/Einblenden nicht angezeigt und sind nicht im Layout enthalten.

Wenn Sie die Größe des Webbrowserfensters anpassen, wird die Warnleiste gemäß Inhalt skaliert. Eine Kurzinformation wird in der Meldung angezeigt, wenn der Text gekürzt wird, damit er in die Leiste passt.

Verfahren zum Herunterfahren und Starten von VDP

Wenn Sie die VDP-Appliance herunterfahren müssen, verwenden Sie hierzu in vCenter Server Web Client die Aktion **Gastbetriebssystem herunterfahren**. Bei dieser Aktion wird die Appliance automatisch ordnungsgemäß heruntergefahren. Wenn die Appliance ohne die Aktion **Gastbetriebssystem herunterfahren** ausgeschaltet wird, sind Beschädigungen möglich. Das Herunterfahren und der Neustart der VDP-Appliance können bis zu 30 Minuten dauern. Der Status kann über die Konsole der virtuellen Maschine überwacht werden. Nach dem Herunterfahren einer Appliance können Sie diese über die Aktion **Einschalten** im vCenter Server Web Client neu starten.

Wenn die Appliance nicht ordnungsgemäß heruntergefahren wird, wird beim Neustart ein Rollback auf den letzten validierten Kontrollpunkt durchgeführt. Dies bedeutet, dass Änderungen an den Backupjobs oder Backups, die zwischen dem Kontrollpunkt und dem unerwarteten Herunterfahren-Vorgang durchgeführt wurden, verloren gehen. Hierbei handelt es sich um erwartetes Verhalten, mit dem eine Systembeschädigung aufgrund von unerwarteten Herunterfahren-Vorgängen ausgeschlossen wird. Zusätzliche Informationen finden Sie unter „Rollback einer Appliance" auf Seite 43.

Die VDP-Appliance ist auf einen 24x7-Betrieb ausgelegt, um so Wartungsvorgänge zu unterstützen und für Wiederherstellungsvorgänge verfügbar zu sein. Fahren Sie die VDP-Appliance nur herunter, wenn es dafür einen bestimmten Grund gibt.

HINWEIS Wenden Sie vor einem vCenter Server-Patch oder -Upgrade das Verfahren zum Herunterfahren von VDP an.

Proxys

7

In diesem Kapitel werden folgende Themen behandelt:

Proxyüberblick

In diesem Kapitel wird die Verwendung interner und externer Proxys in VDP-Appliances beschrieben.

Nach der Erstbereitstellung ist für eine VDP-Appliance lediglich ein interner Proxy konfiguriert. Im Anschluss an eine vollständige Bereitstellung der VDP-Appliance können Sie bis zu 8 externe Proxys über die Benutzeroberfläche für die VDP-Konfiguration bereitstellen. Wenn Sie einen externen Proxy für die VDP-Appliance konfigurieren, wird der interne Proxy während des Prozesses automatisch deaktiviert.

Überlegungen vor der Bereitstellung eines externen Proxys

Berücksichtigen Sie Folgendes, wenn Sie einen oder mehrere Proxys für eine Verwendung mit der VDP-Appliance bereitstellen:

- Die VDP-Appliance hat keinen Zugriff auf einen Datenspeicher, sodass eine Nutzung der Hot-Add-Transportmethode verhindert wird. Informationen zum Definieren der Best Practices für VMware Hot-Add aus Backupperspektive finden Sie im folgenden VMware-Knowledgebase-Artikel:

  http://kb.vmware.com/kb/1008072

- Eine größere Anzahl gleichzeitiger Backups ist erforderlich, was weder durch Ressourcen auf dem vSphere-Host noch durch die Performance des Datenspeichers eingeschränkt werden darf. Maximal werden 24 gleichzeitig ausgeführte Backupjobs unterstützt.

- Für eine Recovery auf Dateiebene (File Level Recovery, FLR) auf LVM- (Logical Volume Manager) oder EXT4-basierten Dateisystemen ist ein externer Proxy erforderlich.

Bereitstellung externer Proxys

Um Hot-Add während des Backupprozesses nutzen zu können, muss die Proxy-Appliance direkten Zugriff auf den Datenspeicher mit der Ziel-VM haben. Die Backup-Agent-Appliance nutzt den Datenspeicherzugriff von dem vSphere-Host, mit dem sie verbunden ist. Überprüfen Sie bei Bereitstellung des externen Proxys, ob die Appliance über den vSphere-Host Zugriff auf die gewünschten Datenspeicher hat.

Wenn die Proxy-Appliance keinen Zugriff auf den Datenspeicher mit der Ziel-VM hat, wird statt Hot-Add die Transportmethode NBD aufgerufen, wodurch sich u. U. die Backupgeschwindigkeit deutlich erhöht.

Anzahl der bereitzustellenden Proxys und Proxydurchsätze pro Proxy

Berücksichtigen Sie bei der Anzahl der bereitzustellenden Proxys und der Konfiguration der Anzahl der Proxydurchsätze pro Proxy die folgenden Best Practices:

Bei Verwendung eines Proxys

- Wenn ein externer Proxy mit der Standardkonfiguration für Speicher und CPUs bereitgestellt wird, sind sechs Proxydurchsätze bei der Ausführung von Backups optimal. Wenn die Proxydurchsätze pro Proxy auf eine höhere Zahl als sechs erhöht werden, führt dies zu einer Performanceverschlechterung.

- Eine CPU-Erhöhung auf Seiten des externen Proxys hat eine bessere Performance zur Folge als die Erhöhung des Speichers bei einem externen Proxy.

- Wenn die Konfiguration eines externen Proxys auf acht CPUs geändert wird, ist eine Ausführung von acht Proxydurchsätzen pro Proxy optimal. Dies gilt für Backups der Ebene 0 und Ebene 1. Bei dieser Konfiguration wird die Netzwerkbandbreite zum einschränkenden Faktor.

Bei Verwendung mehrerer externer Proxys für Backups der Ebene 0

- Durch Maximierung der Anzahl der bereitgestellten Proxys werden ggf. nicht die besten Performanceergebnisse erzielt.

- Wenn Sie die Anzahl der Proxy erhöhen, reduziert sich ggf. die optimale Anzahl von Proxydurchsätzen pro Proxy. Wenn beispielsweise zwei externe Proxys ausgeführt werden, lassen sich u. U. die besten Ergebnisse bei Ausführung von sechs Proxydurchsätzen pro Proxy beobachten. Wenn vier externe Proxys ausgeführt werden, lassen sich u. U. die besten Ergebnisse bei Ausführung von vier Proxydurchsätzen pro Proxy beobachten. Dies wird ggf. durch die Anzahl der Proxys pro vSphere-Host eingeschränkt.
- Bei der Durchführung mehrerer Backups ist es besser, die Anzahl der Proxydurchsätze pro Proxy zu erhöhen als die Anzahl der Proxys.

Bei Verwendung mehrerer externer Proxys für Backups der Ebene 1

Wenn Sie inkrementelle Backups für eine virtuelle Maschine (Backups der Ebene 1) ausführen, sollten Sie erwägen, die Anzahl der Proxys zu erhöhen. Die Ausführung von vier Proxydurchsätzen pro Proxy bietet eine bessere Performance als die Verwendung einer geringeren Anzahl von Proxys und die Ausführung von acht Proxydurchsätzen pro Proxy.

Erhöhung der Menge der auf der VDP-Appliance ausgeführten Backups

Nach der Ausführung der Backups müssen Sie ggf. die Menge der von der VDP-Appliance während eines bestimmten Zeitraums durchgeführten Backups erhöhen. Wenn die Menge der in einem bestimmten Zeitraum durchgeführten Backups erhöht wird, sollten die folgenden Best Practices berücksichtigt werden:

- Wenn die vSphere-Serverressourcen eine Einschränkung darstellen, führen Sie mehr Proxydurchsätze pro Proxy aus und reduzieren Sie die Anzahl der Proxys.
- Wenn die vSphere-Serverressourcen keine Einschränkung darstellen, erhöhen Sie die Anzahl der Proxys und behalten Sie die vier Proxydurchsätze pro Proxy bei.
- Wenn sechs bis acht externe Proxys zum Verarbeiten der gewünschten Backups erforderlich sind, erhöhen Sie die Anzahl der Proxydurchsätze pro Proxy und begrenzen Sie die Anzahl der bereitgestellten externen Proxys.

Reduzieren der gleichzeitig auf der VDP-Appliance ausgeführten Backups

Nach der Backupausführung auf der VDP-Appliance müssen Sie ggf. die Anzahl der gleichzeitig von der VDP-Appliance ausgeführten Backups reduzieren, um die Last für die Datenspeicher und zugehörigen Speicher zu begrenzen. Bei der Reduzierung der gleichzeitig von der VDP-Appliance ausgeführten Backups sollten die folgenden Best Practices berücksichtigt werden:

- Platzieren Sie die VDP-Appliance in einen Datenspeicher mit höherer Schreibperformance, wobei iSCSI NFS für den Datenspeicher vorzuziehen ist.
- Reduzieren Sie bei einer hohen Last auf den Datenspeicher, in dem sich während der Backups die geschützten virtuellen Maschinen befinden, die Anzahl der Proxys und die Anzahl der Proxydurchsätze pro Proxy auf höchstens vier. Hierdurch wird die Menge der Seek- und Lesevorgänge bei der Durchführung von Backups verringert.

Managen des Proxydurchsatzes

Der Assistent „Proxydurchsatz managen“ ermöglicht es, auf Grundlage Ihrer Infrastruktur die Anzahl der gleichzeitig durchführbaren Backups und Wiederherstellungen zu konfigurieren. Mithilfe des Assistenten „Proxydurchsatz managen“ können Sie Werte für interne und externe Proxys festlegen. Die VDP-Appliance unterstützt bis zu 8 externe Proxys und maximal sind 24 gleichzeitig ausgeführte Backupjobs möglich.

Weitere Informationen erhalten Sie unter „Anzahl der bereitzustellenden Proxys und Proxydurchsätze pro Proxy“ auf Seite 70.

ACHTUNG Bei der Anzahl, die Sie für das gleichzeitige Sichern und Wiederherstellen von Clients auswählen, handelt es sich um eine globale Einstellung. Diese Einstellung gilt für alle internen und externen Proxyeinstellungen.

Verfahren

1 Öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

https://<*IP_Adresse_der_VDP_Appliance*>:8543/vdp-configure/

2 Melden Sie sich mit dem VDP-Benutzernamen und -Passwort an.

3 Klicken Sie auf die Registerkarte **Konfiguration**.

4 Wählen Sie aus der Liste **Aktion** die Option **Proxydurchsatz managen** aus.

Die Seite „Proxy managen“ wird angezeigt.

5 Legen Sie die Anzahl (zwischen 1 und 8) der Backup- und Wiederherstellungsclients fest, die gleichzeitig ausgeführt werden sollen.

6 Klicken Sie auf **Weiter**.

Die Seite „Bereit zur Fertigstellung“ wird angezeigt.

7 Klicken Sie auf **Fertig stellen**, um die Änderungen zu übernehmen.

Unterstützung externer Proxys

VDP Advanced-Appliances der Version 5.5.6 und niedriger sind nur mit internen Proxys konfiguriert. Dabei werden die Proxyservices innerhalb der VDP-Appliance ausgeführt und sind für das Management von Jobanforderungen von der Appliance registriert. Externe Proxys können für VDP 6.0-Appliances konfiguriert werden.

HINWEIS Die VDP-Appliance mit externen Proxys unterstützt die Recovery auf Dateilevel (File Level Recovery, FLR) auf virtuellen Maschinen mit EXT4-Dateisystemen.

Best Practice für die Bereitstellung externer Proxys

HINWEIS Beim Konfigurieren der Appliance zur Verwendung externer Proxys werden die internen Proxys automatisch deaktiviert.

Der Hot-Add-Transport ist in der Regel schneller als Backups und Wiederherstellungen mit der Transportmethode NBD (Network Block Device, Netzwerkblockgerät).

Best Practices bei externen Proxys

- **Bereinigung verwaister Proxys**

  Externe Proxys, die bei der VDP-Appliance registriert, aber nicht länger im vCenter-Bestand vorhanden sind, gelten als verwaiste Proxys. Wenn die Proxy-VM im vCenter-Bestand verbleibt und die Warnung „Die virtuelle Maschine wurde entweder gelöscht oder sie wird derzeit nicht von vCenter gemanagt“ für den Proxy angezeigt wird, können Sie die Proxy-VM über das VDP-Konfigurationsdienstprogramm neu starten. Wenn das Problem fortbesteht, lässt sich der Hostname möglicherweise aufgrund einer falschen Netzwerkkonfiguration nicht auflösen. Um dieses Problem zu umgehen, löschen Sie den verwaisten Proxy und stellen Sie einen neuen Proxy bereit.

- Entfernung des ESXi-Hosts des Proxys aus vCenter

  Wenn der ESXi-Host eines externen Proxys aus vCenter entfernt wird, stuft die VDP-Appliance den Proxy bei dessen Auswahl im VDP-Konfigurationsdienstprogramm als verwaist ein und zeigt die Warnung „Die virtuelle Maschine wurde entweder gelöscht oder sie wird derzeit nicht von vCenter gemanagt“ an. Löschen Sie den Eintrag des verwaisten Proxys über das VDP-Konfigurationsdienstprogramm, solange der ESXi-Host nicht zu vCenter hinzugefügt wird.

- **vCenter-Wechsel**

  Wenn der ESXi-Host des Proxys nicht zusammen mit dem ESXi-Host von VDP in die neue vCenter-Version verschoben wird, wird dieser Proxy im VDP-Konfigurationsdienstprogramm als verwaist angezeigt. Löschen Sie den verwaisten Proxy über das VDP-Konfigurationsdienstprogramm, solange nicht geplant ist, den Host des Proxys in die neue vCenter-Version oder den VDP-Host zurück in die ursprüngliche vCenter-Version zu verschieben.

- **VDP-Rollback**

  Nach dem Rollback der VDP-Appliance auf einen früheren Kontrollpunkt werden alle externen Proxys, die nach der Erstellung des Kontrollpunkts hinzugefügt oder gelöscht wurden, im VDP-Konfigurationsdienstprogramm als verwaist angezeigt. Hinzugefügte externe Proxys können über das VDP-Konfigurationsdienstprogramm neu gestartet werden, um sie neu zu registrieren oder neu bereitzustellen. Löschen Sie bei gelöschten Proxys die Einträge mit verwaisten Proxys aus dem VDP-Konfigurationsdienstprogramm.

- **Kompletter VDP-Neuaufbau und Rollback**

  Wenn bei der VDP-Appliance Probleme aufgetreten sind, die einen kompletten Neuaufbau erforderlich gemacht haben, und ein Appliance-Rollback auf einen Kontrollpunkt von Data Domain durchgeführt wurde, ändern Sie das Appliance-Passwort sofort über das VDP-Konfigurationsdienstprogramm. Alle externen Proxy, die bereitgestellt wurden, bevor der Kontrollpunkt erstellt wurde, werden als verwaist angezeigt. Löschen Sie diese Waisen aus dem VDP-Konfigurationsdienstprogramm. Alle externen Proxys, die vor dem Kontrollpunktrollback auf der neu aufgebauten VDP-Appliance bereitgestellt wurden, werden mit der Warnung „Authentifizierung mit externem Proxy fehlgeschlagen“ angezeigt. Aktualisieren Sie das Proxypasswort nach der Änderung des VDP-Appliance-Passworts.

- **Bandbasierte Disaster Recovery von VDP**

  Wenn die VDP-Appliance nach einem schwerwiegenden Ereignis von Band wiederhergestellt wurde, löschen Sie die verwaisten externen Proxys über das VDP-Konfigurationsdienstprogramm und stellen Sie neue bereit.

- **Aktualisierung des Passworts**

  Wenn das VDP-Appliance-Passwort über das VDP-Konfigurationsdienstprogramm geändert wird, aktualisiert die VDP-Appliance das Passwort auf allen registrierten externen Proxys. Wenn ein Proxypasswort nicht aktualisiert wird, wird bei Auswahl des Proxys die Warnung „Authentifizierung mit externem Proxy fehlgeschlagen“ angezeigt. Sie können das Proxypasswort manuell über das VDP-Konfigurationsdienstprogramm aktualisieren.

- **Neustart des Proxys**

  Wenn zuvor registrierte externe Proxys im VDP-Konfigurationsdienstprogramm als nicht registriert angezeigt werden, starten Sie die Proxys neu. Hierdurch werden die Proxys aus- und wieder eingeschaltet und erneut bei der VDP-Appliance registriert.

- **Notfallwiederherstellung**

  Bei einer Notfallwiederherstellung der externen Proxys wird der interne Proxy automatisch aktiviert. Nachdem die Notfallwiederherstellung abgeschlossen wurde und alle ESXi-Hosts erneut mit vCenter verbunden wurden, können Sie entweder den internen Proxy oder alle externen Proxys löschen. Aktivieren Sie nicht sowohl interne als auch externe Proxys für Wiederherstellungsaktivitäten, die nicht der Notfallwiederherstellung dienen.

Einschränkungen

- Externe VDP-Proxys werden nur auf vSphere 5.1-Hosts und höher unterstützt.
- Das Limit für externe Proxys pro VDP-Appliance ist 8.
- Maximal sind 24 gleichzeitig ausgeführte Backupjobs möglich.

- Für eine Recovery auf Dateiebene (File Level Recovery, FLR) auf virtuellen Maschinen mit EXT4-Dateisystem ist die Verwendung eines externen Proxys erforderlich.

Hinzufügen eines externen Proxys

Der Assistent zum Hinzufügen von Proxys ermöglicht das Hinzufügen und Bereitstellen von bis zu 8 externen Proxys und deren Registrierung bei der VDP-Appliance über das VDP-Konfigurationsdienstprogramm.

Verfahren

1 Öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

https://<*IP_Adresse_der_VDP_Appliance*>:8543/vdp-configure/

2 Melden Sie sich mit dem VDP-Benutzernamen und -Passwort an.

3 Klicken Sie auf die Registerkarte **Konfiguration**.

4 Wählen Sie aus der Liste **Aktion** die Option zum **Hinzufügen von Proxys** aus.

Die Seite zum Hinzufügen von Proxys wird angezeigt.

5 Geben Sie auf der Seite „Host und Speicher“ die folgenden Anmeldedaten an und klicken Sie dann auf **Weiter**.

- **Host**: Wählen Sie einen Zielhost aus der Liste aus.
- **Storage**: Wählen Sie ein Zielspeichergerät aus der Liste aus.
- **Netzwerkverbindung**: Wählen Sie eine Netzwerkverbindung für die virtuelle Maschine aus der Liste aus.

6 Geben Sie auf der Seite „Netzwerk“ die folgenden Netzwerkeinstellungen an und klicken Sie dann auf **Weiter**.

- **Statische IPv4-Adresse**: Die IPv4- oder IPv6-Einstellung der Schnittstelle
- **Netzmaske**: Die Netzwerkmaske der statischen IPv4- oder IPv6-Adresse
- **Gateway**: Die Gatewayadresse der statischen IPv4- oder IPv6-Adresse
- **Primärer DNS**: Zur DNS-Auflösung verwendeter primärer DNS-Server (Domain Name System)
- **Sekundärer DNS**: Zur DNS-Auflösung verwendeter sekundärer DNS-Server (Domain Name System)

7 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung“ die Einstellungen für die Bereitstellung.

HINWEIS Sie können den Namen der externen Proxy-VM auf der Seite „Bereit zur Fertigstellung“ ändern.

8 Klicken Sie auf **Fertig stellen**, um den Proxy bereitzustellen.

Vergewissern Sie sich, dass der Proxy in den in Schritt 5 ausgewählten Datenspeicher bereitstellt. Wenn der Proxy nach erfolgreicher Bereitstellung in ein VMware vSphere Distributed Resource Scheduler™-Cluster (DRS) bereitstellt, kann das Cluster den Proxy mithilfe von Storage vMotion verschieben. Während des Migrationsvorgangs auf einen anderen Speicher sind die auf dem Proxy ausgeführten Jobs gefährdet. Hot-Add kann nicht für Proxys in einem DRS-Cluster verwendet werden. Daher müssen Sie eine manuelle DRS-Deaktivierung für den Proxy durchführen. Diese Szenario ist für die VDP-Appliance auch dann zutreffend, wenn ein interner Proxy verwendet wird.

Führen Sie die folgenden Schritte durch, um DRS für den Proxy manuell zu deaktivieren:

1 Wählen Sie auf dem Cluster, das den Proxy hostet, die Registerkarte **DRS** aus.

2 Klicken Sie auf die Optionen für die virtuelle Maschine.

3 Suchen Sie unter dem Level **Automatisierung** nach der virtuellen Proxymaschine und ändern Sie die Einstellung auf **Deaktivieren**.

Deaktivieren des internen Proxys

Wenn ein Benutzer einen Rollback-Vorgang als Kontrollpunkt während des Backups eines externen Proxys durchführt, wird nach Abschluss des Rollback der interne Proxy zusammen mit einer Warnmeldung, die den Benutzer zur Deaktivierung des internen Proxys auffordert, im VDP-Konfigurationsdienstprogramm angezeigt.

Verfahren

1 Wählen Sie im VDP-Konfigurationsdienstprogramm den internen Proxy aus der Liste **Proxys** aus.

2 Wählen Sie **Proxy managen** über das Symbol für Proxyaktionen aus.

Der Assistent „Internen Proxy managen“ wird angezeigt.

3 Aktivieren Sie das Kontrollkästchen **Internen Proxy deaktivieren** und klicken Sie auf **Weiter**.

4 Klicken Sie auf der Seite „Bereit zur Fertigstellung“ des Assistenten auf **Fertig stellen**, um die Änderungen zu übernehmen.

(Optional) Konfigurieren der Proxy-Zertifikatauthentifizierung

Standardmäßig führen Proxys beim Verbinden mit vCenter Server keine Validierung der SSL-Zertifikate durch. Dies macht vCenter Server ggf. gegenüber Man-in-the-Middle Exploits (MITM) anfällig, was zu einem unbefugten Zugriff auf vCenter Server führen kann. Mit der Konfiguration jedes Proxys zur Verwendung der SSL-Zertifikatauthentifizierung bei Verbindung mit vCenter Server wird diese Schwachstelle behoben. Unter Kapitel 5, „Schützen der Kommunikation zwischen VDP und vCenter“, auf Seite 49 finden Sie weitere Informationen.

Überwachen des Integritätsstatus externer Proxys

Kriterien für den Integritätsstatus

Der für den externen Proxy gemeldete Integritätsstatus basiert auf den folgenden Kriterien:

- Festplattenauslastung
  - **Warnung**: Jedes Dateisystem, dessen Kapazität zu mehr als 70 % belegt ist
  - **Kritische Warnung**: Jedes Dateisystem, dessen Kapazität zu mehr als 90 % belegt ist
- CPU-Last
  - **Warnung**: Die 15-minütige durchschnittliche Last liegt über einem Wert von 1,5.
  - **Kritische Warnung**: Die 15-minütige durchschnittliche Last liegt über einem Wert von 5,0.
- Speicherauslastung
  - **Warnung**: Die Auslastung liegt über 85 %.
  - **Kritische Warnung**: Die Auslastung liegt über 95 %.

Protokolle externer Proxys

Protokolle externer Proxys sind nur sichtbar, wenn mindestens ein externer Proxy konfiguriert ist. Wenn dieses Protokollbündel heruntergeladen wird, wird eine `.zip`-Datei in den Browser gestreamt. Die `.zip`-Datei enthält alle Protokolle der externen Proxys. Die internen Proxy sind von diesem Protokollbündel ausgeschlossen.

Informationen zum Herunterladen von Protokollen finden Sie unter „Sammeln von VDP-Protokollen oder Diagnoseinformationen“ auf Seite 40.

Speichermanagement

8

Dieses Kapitel umfasst folgende Themen:

Erstellen von neuem Speicher

Der Assistent für die Erstkonfiguration führt Sie durch die Auswahl des Speichertyps sowie die Gerätezuweisung auf VDP-Speicherfestplatten und bietet eine Option zur Ausführung des Performance-Bewertungstools.

Einschränkungen

Sie können die Appliance nicht auf einen neuen Host oder neuen Datenspeicher migrieren, während neuer Speicher erstellt wird.

Voraussetzungen

- Die VDP-Appliance wird bereitgestellt und Sie werden auf der Seite **Speicher erstellen** des Assistenten **Erste Konfiguration** angemeldet.
- Deaktivieren Sie unmittelbar nach der OVA-Bereitstellung vSphere HA auf der VDP-Appliance. Nach der Erstkonfiguration auf der VDP-Appliance, die das Erstellen eines Speichers einschließt, können Sie vSphere HA für die Appliance aktivieren.

Verfahren

1 Wählen Sie auf der Seite **Speicher erstellen** des Assistenten **Erste Konfiguration** die Option **Neuen Speicher erstellen** aus. Beim Erstellen eines neuen Speichers erstellt der Prozess einen neuen Speicher-Node in den ausgewählten Datenspeichern.

2 Wählen Sie eine der folgenden Kapazitätsoptionen aus und klicken Sie auf **Weiter**.

   - 0,5
   - 1
   - 2
   - 4
   - 6
   - 8

   Die Seite „Gerätezuweisung“ wird angezeigt. Wenn Sie neuen Speicher erstellen, ist die Anzahl der erforderlichen Festplatten bekannt.

3 Wählen Sie den Bereitstellungstyp aus der Drop-down-Liste **Bereitstellung** aus.

   - **Thick Lazy-Zeroed** (der Standard- und empfohlene Provisioning-Typ): Beim Thick Lazy-Zeroed Provisioning wird ein virtuelles Laufwerk in einem standardmäßigen Thick-Format erstellt. Der für das virtuelle Laufwerk erforderliche Speicherplatz wird beim Erstellen des virtuellen Laufwerks zugewiesen. Die auf dem physischen Gerät verbleibenden Daten werden während der Erstellung nicht gelöscht, sondern sie werden zu einem späteren Zeitpunkt beim ersten Schreibvorgang von der virtuellen Maschine nach Bedarf durch Nullbytes ersetzt („zeroed out“).
   - **Thick Eager-Zeroed**: Beim Thick Eager-Zeroed Provisioning wird eine Art virtuelles Thick-Laufwerk erstellt, das eingesetzt wird, wenn das Thema Datensicherheit wichtig ist. Der für das virtuelle Laufwerk erforderliche Speicherplatz wird beim Erstellen des virtuellen Laufwerks zugewiesen. Beim Erstellen eines virtuellen Laufwerks mithilfe von Thick Eager-Zeroed Provisioning auf einem Datenspeicher, auf dem bereits Daten vorhanden waren, werden diese alten Daten gelöscht und können nicht mehr wiederhergestellt werden. Die Erstellung von Laufwerken dauert in diesem Format mitunter wesentlich länger als die Erstellung anderer Typen.
   - **Thin**: Für eine Thin-Provisioning-Festplatte stellen Sie so viel Datenspeicherplatz bereit, wie die Festplatte basierend auf dem von Ihnen für die Festplattengröße eingegebenen Wert benötigt. Eine Thin-Provisioning-Festplatte beginnt mit einem kleinen Wert und nutzt nur so viel Datenspeicherplatz wie für die ersten Aufgaben erforderlich ist.

4 Nachdem allen Festplatten Datenspeichern zugewiesen wurden, klicken Sie auf **Weiter**.

Auf der Seite **Bereit zur Fertigstellung** können Sie eine Performanceanalyse der Speicherkonfiguration ausführen und auf **Weiter** klicken, um die Änderungen zu übernehmen. Obwohl es möglich ist, den Performanceanalysetest zu umgehen, wird eine Ausführung ausdrücklich empfohlen.

5 Wenn Sie auf **Weiter** klicken, werden Sie anhand einer Warnung darüber informiert, dass die Speicherkonfiguration beginnt und nicht rückgängig gemacht werden kann. Klicken Sie auf **Ja**, um fortzufahren.

Mögliche Ergebnisse sind „Erfolgreich“, „Fehlgeschlagen“ und „Bedingt erfolgreich“, wenn der Seek-Test ausgewählt wird (standardmäßig ausgeschlossen). Wenn alle Tests erfolgreich verlaufen, lautet das Ergebnis „Erfolgreich“. Wenn die Schreib- oder Lesetests nicht erfolgreich verlaufen, lautet das Ergebnis „Fehlgeschlagen“. Wenn der Seek-Test ausgewählt ist und die Schreib- und Lesetests erfolgreich verlaufen, der Seek-Test jedoch fehlschlägt, lautet das Ergebnis „Bedingt erfolgreich“.

a Wählen Sie zur Durchführung des Tests **Performanceanalyse für Speicherkonfiguration ausführen** aus, um sicherzustellen, dass die Speicherkonfiguration die minimalen Performanceerwartungen erfüllt. In Tabelle 8-11 sind die minimalen Performanceerwartungen aufgeführt.

Bei diesem Test werden Schreib-, Lese- und Seek-Performancetests der Festplatten durchgeführt. Abhängig von Ihrer Speicherkonfiguration kann der Abschluss der Performanceanalyse zwischen 30 Minuten und mehreren Stunden dauern.

b Wählen Sie **Bei Erfolg Appliance neu starten** aus, damit die Appliance nach einem erfolgreichen Test neu gestartet wird. Klicken Sie auf **Weiter**, um den Test zu starten.

Der Performanceanalyse-Test wird vom Server initiiert; der Browser kann während des Tests geschlossen werden.

- Bei erfolgreichem Test wird über eine Meldung angezeigt, dass die Konfiguration abgeschlossen wurde und die Appliance vom Server automatisch neu gestartet wird.
- Wenn der Test nur bedingt erfolgreich ist oder fehlschlägt, wird das Ergebnis der Performanceanalyse zwar angezeigt, aber die Appliance wird vom Server nicht automatisch neu gestartet. Zum Anzeigen der Testergebnisse müssen Sie sich erneut bei VDP-Configure anmelden und den Client manuell neu starten.

HINWEIS Wenn Sie nicht innerhalb von 59 Sekunden auf **Neu starten** klicken, werden die Services nach einem automatischen Neustart der Appliance gestartet. Nach dem Neustart der VDP-Appliance führt diese eine Reihe automatisierter Konfigurationsschritte aus. Bis zum Abschluss dieser Schritte können 30-45 Minuten oder mehr verstreichen.

Die Appliance wird unter den folgenden Umständen automatisch neu gestartet:

- Sie haben entschieden haben, am Ende des VDP-Konfigurationsassistenten eine Performanceanalyse durchzuführen.
- Sie haben im VDP-Konfigurationsassistenten das Kontrollkästchen für einen Neustart der VDP-Appliance nach erfolgreichen Tests aktiviert.
- Die Tests wurden erfolgreich durchgeführt.

Minimale Speicherperformance

Beim Konfigurieren der VDP-Appliance liefert der Performancetest abhängig von der Größe der bereitgestellten Appliance unterschiedliche Ergebnisse.

In Tabelle 8-11 sind die Mindesterwartungen für die Lese-, Schreib- und Seek-Performance nach VDP-Appliance-Größe aufgeführt.

Tabelle 8-11. Mindesterwartungen für Speicherperformance

VDP-Appliance-Größe (in TB)	Festplattengröße	Leseminimum	Schreibminimum	Seek-Minimum
Einziger Datenspeicher	256 GB	10 MB/s	20 MB/s	106 Seeks/s
0,5	256 GB	60 MB/s	30 MB/s	400 Seeks/s
1,0	512 GB	60 MB/s	30 MB/s	400 Seeks/s
2,0	1024 GB	60 MB/s	30 MB/s	400 Seeks/s
4,0	1024 GB	80 MB/s	40 MB/s	400 Seeks/s
6,0	1024 GB	80 MB/s	40 MB/s	400 Seeks/s
8,0	1024 GB	150 MB/s	120 MB/s	400 Seeks/s

Anbinden vorhandener VDP-Festplatten

Auf der Seite „Speicher erstellen“ des Assistenten für die Erstkonfiguration ist die Option **Vorhandene VDP-Festplatten anhängen** verfügbar. Diese Option ermöglicht Ihnen das Durchsuchen von Datenspeichern und die Auswahl der zuvor verwendeten VDP-Festplatten und fährt dann mit dem automatischen Anbinden der ausgewählten Festplatten an die neue VDP-Appliance fort. Diese Festplatten werden der neuen VDP-Appliance automatisch hinzugefügt.

ACHTUNG Versuchen Sie nicht, die verwendeten VDP-Festplatten manuell an die neue VDP-Appliance anzubinden, ohne die Schritte dieses Verfahrens verfolgt zu haben. Wenn Sie die verwendeten VDP-Festplatten importieren, werden nur die Wiederherstellungspunkte, aber weder die Backupjobs noch die Konfigurationsinformationen wie E-Mail-Berichte importiert. Sie müssen die Jobs erneut erstellen. Die importierten Wiederherstellungspunkte sind in der Domain **/REPLICATE/VDP_IMPORTS** vorhanden. Auf dem vSphere-Webclient werden die tatsächlichen Wiederherstellungspunkte in der Domain **/REPLICATE/VDP_IMPORTS** angezeigt. Wenn VDP eine unvollständige oder ungültige Speicherkonfiguration entdeckt, schlägt der Vorgang fehl.

Wenn Sie vorhandenen Speicher anbinden, ist die Auswahl einer Kapazitätsoption – im Gegensatz zur Erstellung von neuem Speicher – nicht erforderlich.

Die folgenden Änderungen treten auf, wenn zuvor verwendete VDP-Festplatten an die neue VDP-Appliance angebunden werden.

- Alle Backupjobs im Zusammenhang mit der zuvor verwendeten VDP werden gelöscht und müssen neu erstellt werden.
- Alle Replikationsjobs im Zusammenhang mit der zuvor verwendeten VDP werden gelöscht und müssen neu erstellt werden.
- Wiederherstellungspunkte im Zusammenhang mit der zuvor verwendeten VDP bleiben intakt. Die Wiederherstellungspunkte werden mit dem durch eine Folge zufälliger Buchstaben erweiterten Original-VM-Namen angezeigt.
- Auf der Seite „Wiederherstellungsoptionen festlegen“ des Assistenten „Backup wiederherstellen“ wird die Option **Am ursprünglichen Speicherort wiederherstellen** für die Wiederherstellungspunkte im Zusammenhang mit den zuvor verwendeten VDP-Festplatten deaktiviert.
- Das E-Mail-Reporting muss neu konfiguriert werden.

Voraussetzungen

- Vor der Anbindung von vorhandenem Speicher müssen Sie die VDP-Appliance, wie unter „VDP-Installation und -Konfiguration“ auf Seite 21 beschrieben, installieren und konfigurieren.
- Vergewissern Sie sich, dass sämtlicher VDP-Speicher, der an die VDP-Appliance angebunden werden soll, gesichert ist.

Verfahren

1 Wählen Sie auf der Seite „Speicher erstellen“ des Assistenten für die Erstkonfiguration die Option **Vorhandene VDP-Festplatten** anbinden aus und klicken Sie auf Weiter.

Das Dialogfeld „Gerätezuweisung“ wird angezeigt.

2 Klicken Sie auf die erste Ellipsenschaltfläche:

a Navigieren Sie zur ersten VMDK-Datei, die Sie anbinden möchten.

b Markieren Sie die VMDK-Datei und klicken Sie auf **Auswählen**.

HINWEIS Sie können festlegen, dass nur die Datenträger der zuvor verwendeten VDP-Appliance angebunden werden. Sie können die BS-Startpartition nicht auswählen. Falls Sie die primäre Laufwerkspartition von 200 GB (die Betriebssystemstartpartition) auswählen, wird eine Fehlermeldung angezeigt.

VMDK-Dateien können in beliebiger Reihenfolge angebunden werden. Nach Auswahl der ersten vmdk-Datei führt das System eine Analyse der Festplatte durch und definiert die Anzahl der auszuwählenden Festplatten.

HINWEIS Während des Anbindungsprozesses können Sie jederzeit auf **Zurücksetzen** klicken, um den Originalzustand des Dialogfelds „Gerätezuweisung“ wiederherzustellen.

3 Klicken Sie auf die Ellipsenschaltfläche, die der nächsten zu definierenden Festplatten entspricht:

a Navigieren Sie zur nächsten VMDK-Datei, die Sie anbinden möchten.

b Markieren Sie die VMDK-Datei und klicken Sie auf **Auswählen**.

Jede Festplatte wird vor dem Hinzufügen als übereinstimmende Festplatte validiert. Wenn die Validierung fehlschlägt, wird eine Fehlermeldung angezeigt. Platzieren Sie den Mauszeiger über der rot markierten Festplatte, um die Fehlermeldung anzuzeigen.

4 Wiederholen Sie Schritt 3 für alle verbleibenden Festplatten.

5 Nachdem alle Festplatten zugewiesen wurden, klicken Sie auf **Weiter**, um den kompletten Satz an Festplatten zu validieren.

Die Seite „Bereit zur Fertigstellung“ wird angezeigt.

6 Klicken Sie auf **Weiter**.

Auf dem System wird die folgende Meldung angezeigt:

Durch den folgenden Prozess wird die Speicherkonfiguration gestartet. Dies kann nicht rückgängig gemacht werden. Möchten Sie fortfahren?

7 Klicken Sie auf **Ja**.

Das System fordert Sie auf, das mit der zuvor verwendeten VDP-Appliance verknüpfte Root-Passwort anzugeben.

8 Geben Sie das Root-Passwort der zuvor verwendeten VDP-Appliance in die Textfelder **Passwort** und **Passwort bestätigen** ein und klicken Sie dann auf **OK**.

9 Klicken Sie auf **Fertig stellen**, um die Änderungen zu übernehmen und neu zu starten.

HINWEIS Nach einer erfolgreichen Speicherkonfiguration werden die Services nach einem automatischen Neustart des Systems gestartet. Nach dem Neustart der VDP-Appliance führt diese eine Reihe automatisierter Konfigurationsschritte aus. Bis zum Abschluss dieser Schritte können 30-45 Minuten oder mehr verstreichen.

Nach Abschluss der Konfiguration wird eine Integritätsprüfung gestartet.

Trennen und erneutes Anbinden von Speicher

Im folgenden Verfahren werden die durchzuführenden Schritte bei Beschädigung oder Verlust der primären Laufwerkspartition (die Betriebssystem-Startpartition) auf der VDP-Appliance erläutert, was zu einer nicht wiederherstellbaren VDP-Appliance führt.

Voraussetzungen

- Es ist mindestens ein validierter Kontrollpunkt auf der VDP-Appliance vorhanden, auf der die VMDK-Dateien getrennt und wieder neu angebunden werden.
- Eine neue VDP-Appliance wird bereitgestellt, die mit den älteren VMDK-Festplattendaten kompatibel ist (bei der VDP-Appliance muss es sich um eine identische Version der Festplattendaten oder um eine neuere Version handeln).
- Die VMDK-Dateien der vorherigen VDP-Appliance müssen sich auf einem Datenspeicher befinden, auf den die neu bereitgestellte VDP-Appliance zugreifen kann.

HINWEIS Während der erneuten Anbindung werden Sie zur Eingabe des Root-Passworts für die ältere VDP-Appliance aufgefordert.

Best Practices

- Erstellen Sie eine Backupkopie aller VMDK-Dateien, bevor diese erneut an die VDP-Appliance angebunden werden.
- Sofern möglich, sollten die VMDK-Dateien von der VDP-Appliance getrennt werden, nachdem die VDP-Appliance über die Aktion **Gastbetriebssystem herunterfahren** heruntergefahren wurde. Andernfalls können Sie die virtuelle Maschine im Notfall auch ausschalten.
- Notieren Sie sich vor dem Trennen einer VMDK-Datei von der VDP-Appliance den vollständigen Pfad und Namen der VMDK-Datei. Sie benötigen diese Informationen, wenn Sie die Festplatte erneut an die neu bereitgestellte VDP-Appliance anbinden.

Verfahren

1 Navigieren Sie in vSphere Client zur VDP-Appliance und führen Sie die Aktion **Gastbetriebssystem herunterfahren** auf der virtuellen Maschine aus.

HINWEIS Wenn die Option **Gastbetriebssystem herunterfahren** abgeblendet ist, navigieren Sie zu **vCenter > Hosts und Cluster**, klicken Sie mit der rechten Maustaste auf die VDP-Appliance und wählen Sie **VM ausschalten** aus.

2 Trennen Sie die VMDK-Dateien von der VDP-Appliance:

   a Melden Sie sich über vSphere Web Client als ein Benutzer an, der zum Bearbeiten von Hardwareeinstellungen berechtigt ist.

   b Navigieren Sie zu **vCenter > Hosts und Cluster**.

   c Klicken Sie in der Struktur auf der linken Seite so lange auf die Erweiterungspfeile, bis die VDP-Appliance angezeigt wird.

   d Klicken Sie mit der rechten Maustaste auf die VDP-Appliance und wählen Sie **Einstellungen bearbeiten** aus.

   Die Eigenschaften der virtuellen Maschine werden angezeigt. Die Registerkarte **Hardware** ist standardmäßig ausgewählt.

   Festplatte 1 ist immer die primäre, 200 GB umfassende Betriebssystem-Startpartition. Entfernen Sie Festplatte 1 nicht von der VDP-Appliance.

   e Klicken Sie auf Festplatte 2 in der Liste.

   f Notieren Sie sich den im Feld für die **Datenträgerdatei** angegebenen vollständigen Pfad und Namen der vmdk-Datei. Sie benötigen diese Informationen, wenn Sie die Festplatte erneut anbinden.

   g Klicken Sie auf **Remove**.

   h Wählen Sie unter „Optionen zum Entfernen“ die Option **Von virtueller Maschine entfernen** aus.

   i Führen Sie die zum Entfernen ausgewählte Option für jede Festplatte (2 bis *x*) in der Liste aus.

   j Nach dem Entfernen der Festplatten 2 bis *x* klicken Sie auf **OK**.

3 Wählen Sie auf der Seite „Speicher erstellen“ des Assistenten für die Erstkonfiguration die Option **Vorhandene VDP-Festplatten anbinden** aus und befolgen Sie die unter „Anbinden vorhandener VDP-Festplatten“ auf Seite 80 aufgeführten Schritte.

Anzeigen der Speicherkonfiguration

Die Registerkarte **Speicher** bietet eine Speicherzusammenfassung, Informationen zur Kapazitätsauslastung und Details zur Performanceanalyse.

Über die Schaltfläche **Kapazitätsauslastung** wird eine Seite mit Statusinformationen für den Datenspeicher aufgerufen:

- Ein graues horizontales Balkendiagramm neben dem Datenspeichersymbol zeigt in Prozent an, wie voll der Datenspeicher ist.
- Ein Kreisdiagramm enthält eine Aufschlüsselung des Speicherplatzes im Datenspeicher. Orange steht für die Speichermenge, die vom Datenspeicher verwendet wird. Grün steht für die Menge des freien Speicherplatzes im Datenspeicher. Blau steht für den Speicherplatz im Datenspeicher, der von anderen Anwendungen verwendet wird, die auf im Datenspeicher bereitgestellten virtuellen Maschinen ausgeführt werden.
- In einer Tabelle neben dem Kreisdiagramm werden der Name, die Größe, der Bereitstellungstyp und der vmdk-Dateiname der jeweiligen Datenpartition aufgeführt. Das folgende Beispiel enthält Informationen für eine Datenpartition namens Daten 01:

Daten 01	256 GiB	Thin	sample-vdp-241168_6..0.0.117_1.vmdk

  In diesem Beispiel steht der Wert 256 GiB für die maximale Größe, die verwendet werden kann.

Über die Schaltfläche **Performanceanalyse** wird eine Tabelle aufgerufen, die Statistiken aus einem Performanceanalysetest enthält.

Spalte	Beschreibung
Datenspeicher	Name des Datenspeichers.
Abgeschlossen am	Datum, an dem der Test abgeschlossen wurde.
Ergebnis	Ein Test kann eines der folgenden Ergebnisse anzeigen: ■ Nie ausführen ■ Erfolgreich ■ Fehlgeschlagen Wenn die Schreib- oder Lesetests nicht erfolgreich verlaufen, lautet das Ergebnis „Fehlgeschlagen“. ■ Bedingt erfolgreich Wenn die Schreib- und Lesetests erfolgreich verlaufen, der Seek-Test (optional) jedoch fehlschlägt, lautet das Ergebnis „Bedingt erfolgreich“.
Lesevorgang (MiB/s)	Megabyte pro Sekunde für den Lesetest.
Schreibvorgang (MiB/s)	Megabyte pro Sekunde für den Schreibtest.
Seek (Seeks/s)	Megabyte pro Sekunde für den Seek-Test.

Voraussetzungen

Die VDP-Speicherfestplatten sind auf die verfügbaren Datenspeicher verteilt, die Festplatten sind validiert, das System wurde neu gestartet, und die Systemservices sind betriebsbereit.

Verfahren

1 Melden Sie sich bei der URL von VDP-configure an:

https://<*IP_Adresse*_der_*VDP_Appliance*>**:8543/vdp-configure/**

2 Klicken Sie auf die Registerkarte **Speicher**.

Die Speicherzusammenfassung wird mit den verfügbaren Datenspeichern und der Menge des insgesamt nutzbaren Speichers sowie der für jeden Datenspeicher verfügbaren Speicherkapazität angezeigt.

HINWEIS Klicken Sie zum Aktualisieren der Daten auf der Seite auf das Symbol zum Aktualisieren neben **Speicherzusammenfassung**.

3 Um Statusinformationen zum Datenspeicher anzuzeigen, klicken Sie auf **Kapazitätsauslastung**. Diese Seite ist der Standard.

4 Um einen Performancetest durchzuführen, klicken Sie auf **Performanceanalyse**, wählen einen Datenspeicher in der Tabelle aus und klicken dann auf **Ausführen**.

Der Performanceanalysetest erstellt eine 256 GB große VMDK-Datei im Datenspeicher und führt Lese-, Schreib- und Seek-Tests durch, um die Datenspeicherperformance zu überprüfen.

Aktivieren des Seek-Tests

Der Seek-Test wurde entwickelt, um eine Seek-Performance des gewünschten Speichers zu erhalten. Das ist hauptsächlich nützlich, wenn der zugrunde liegende Speicher nicht per Thin Provisioning bereitgestellt wird. Da die meisten Feldimplementierung per Thin Provisioning bereitgestellte Volumes verwenden, können Seek-Testergebnisse verwirrend sein. Der Seek-Test ist nicht für virtuelle Umgebungen geeignet, daher ist dieser Test von den als Teil der DAT Test Suite ausgeführten Standardtests ausgeschlossen. Der Code ist dennoch vorhanden und der Seek-Test kann ausgeführt werden, wenn der Administrator diesen in die Konfigurationsdatei einschließt.

Wenn Sie den Seek-Test ausdrücklich ausführen möchten, müssen Sie zunächst die Konfigurationsdatei mithilfe der unten aufgeführten Anweisungen ändern. Dann können Sie das Performanceanalysetool ausführen, das den Seek-Test enthält.

Ändern der Konfigurationsdatei zum Aktivieren des Seek-Tests

1 Öffnen Sie über Putty eine SSH-Sitzung für die VDP-Appliance.

2 Öffnen Sie die Datei `/usr/local/vdr/etc/benchmark-settings.xml`, für die Schreibberechtigungen erforderlich sind.

3 Ändern Sie unter den Optionen <runSeekTest>false</runSeekTest> in <runSeekTest>true</runSeekTest>.

4 Speichern Sie die Datei und beenden Sie Putty.

5 Führen Sie die Performanceanalysesuite aus.

Data Domain-Integration

9

Dieses Kapitel umfasst folgende Themen:

Integration von VDP und Data Domain-Systemen

Die Integration von VDP und Data Domain-Systemen ermöglicht Folgendes:

- Verwendung von physischen Data Domain-Systemen als Backupziel für VDP-Backups
- Ziel von Backupdaten, das während der Erstellung eines Backupjobs festgelegt wird
- Transparente Benutzerinteraktion zum Backupziel (VDP oder Data Domain)

Übersicht über die Architektur

Ein Data Domain-System führt eine Deduplizierung über die Data Domain(DD)-Betriebssystemsoftware aus. Die quellbasierte VDP-Deduplizierung auf ein Data Domain-System wird durch die Verwendung der DD Boost-Bibliothek vereinfacht.

VDP verwendet die DD Boost-Bibliothek über eine API-basierte Integration, um auf im Data Domain-Dateisystem enthaltene Verzeichnisse, Dateien usw. zuzugreifen bzw. diese zu ändern. Dank der DD Boost-API erhält VDP einen Überblick über bestimmte Eigenschaften und Funktionen des Data Domain-Systems. Auf diese Weise kann VDP die in Data Domain-Systemen gespeicherten Backup-Images kontrollieren. VDP wird außerdem in die Lage versetzt, Wartungsaktivitäten zu managen und die Replikation auf Data Domain-Remotesystemen zu steuern.

DD Boost wird beim Hinzufügen eines Data Domain-Systems automatisch auf der VDP-Appliance installiert.

Abbildung 9-5 stellt eine Architekturübersicht über eine kombinierte, aus VDP und Data Domain bestehende Lösung dar. Durch die Integration von VDP und Data Domain können Sie festlegen, ob eine bestimmte Backup-Policy eine VDP-Appliance oder ein Data Domain-System zum Ziel hat.

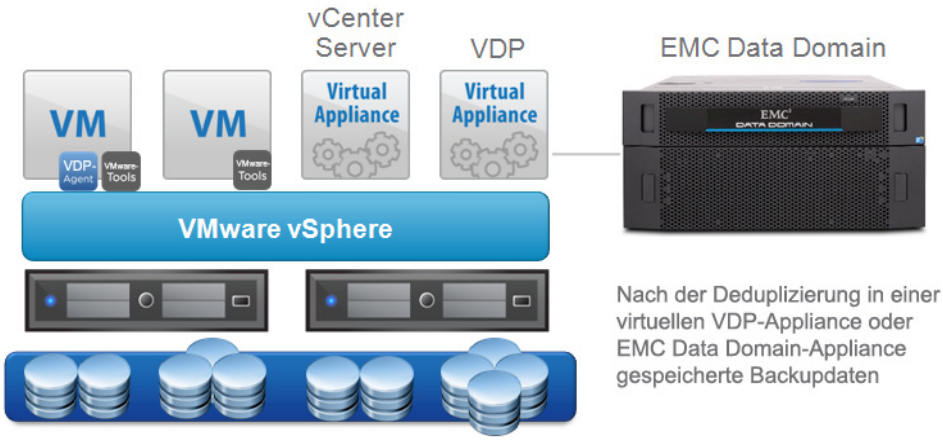


Abbildung 9-5. Lösung aus VDP und Data Domain

Wenn Sie die VDP-Appliance als Ziel für Backupspeicher auswählen, führt die VDP-Appliance eine Verarbeitung der Deduplizierungssegmente durch.

Wenn Sie ein Data Domain-System als Backupziel auswählen, werden Backupdaten an das Data Domain-System übertragen. Die erzeugten zugehörigen Metadaten werden zwecks Speicherung gleichzeitig an die VDP-Appliance gesendet. Über die Metadaten kann die VDP-Appliance Wiederherstellungsvorgänge vom Data Domain-System aus durchführen.

VDP-Clientunterstützung

Bei der Integration von VDP und Data Domain-System werden die folgenden Plug-ins unterstützt:

- VDP Plug-in for Exchange Server VSS
- VDP Plug-in for SharePoint Server VSS
- VDP Plug-in for SQL Server

Best Practices

Welche Einschränkungen bestehen bei VDP in Bezug auf ein angebundenes Data Domain-System?

VMware empfiehlt, bis zu 25 virtuelle Maschinen pro TB Kapazität auf einer VDP-Appliance zu schützen. Diese Variable ist von der Größe der virtuellen Maschinen, der typischen Änderungsrate und der auf jeder virtuellen Maschine vorhandenen Datenmenge abhängig. Vor diesem Hintergrund können Sie bis zu 200 virtuelle Maschinen pro VDP-Appliance mit Backup auf ein Data Domain-System schützen.

Da die Backupdaten auf dem Data Domain-System und nur die Backupjobmetadaten auf der VDP-Appliance gespeichert sind, sollten Sie eine 0,5 TB große VDP-Appliance für ein standardmäßiges Data Domain-System und eine 1 TB große VDP-Appliance für ein Data Domain-System mit 64 TB bereitstellen.

Die folgende Liste enthält die vorgeschlagene Anzahl von pro Data Domain-System bereitgestellten VDP-Appliances:

- 1 x VDP pro DD160 und DD620
- 1 x VDP pro DD2200
- 2 x VDP Advanced pro DD2500 und DD4xxx
- 3 x VDP pro DD7200 und DD990

Welche VDP-Appliance-Größe ist erforderlich, wenn alle Backups über Data Domain erfolgen sollen?

Wenn ein Data Domain-System an einer VDP-Appliance als Speichergerät angebunden ist, speichert die VDP-Appliance nur die Metadaten für Backups mit dem Data Domain-System als Ziel. Es wurde ermittelt, dass ein Data Domain-System mit 16 TB lediglich eine 0,5 TB große VDP-Appliance benötigt, wenn alle Backupdaten an das Data Domain-System gesendet werden. Wenn Backups ebenfalls an die VDP-Appliance gesendet werden, sollte die VDP-Appliance auf Grundlage der auf der VDP-Appliance zu speichernden Daten entsprechend vergrößert werden. Bei einem Data Domain-System mit 64 TB oder mehr können Sie eine 1 TB große VDP-Appliance je 64 TB an Data Domain-Systemspeicher bereitstellen, der voraussichtlich durch die Backupdaten belegt wird.

In meinen VMs sind zahlreiche Images, Bilder und PDF-Dateien vorhanden. Sollte ich die VDP-Appliance bzw. das Data Domain-System als Ziel für diese Backups festlegen?

Das Data Domain-System sorgt für eine bessere Deduplizierung bei Images, Bildern und PDF-Dateien als die standardmäßigen VDP-Appliance-Deduplizierungsalgorithmen.

Data Domain-Einschränkungen

Bei Folgendem handelt es sich um aktuelle Einschränkungen, die im Zusammenhang mit der Verwendung eines Data Domain-Systems mit einer VDP-Appliance definiert sind:

- Wenn eine VDP-Appliance an ein Data Domain-System angebunden ist, kann die Funktion „Vorhandenen Speicher importieren“ der VDP-Appliance nicht für VMDKs der VDP-Appliance mit angebundenem Data Domain-System verwendet werden.
- Es kann jeweils nur ein Data Domain-System an einer VDP-Appliance angebunden sein.

- Das Data Domain-System kann nicht aus der VDP Configuration-Benutzeroberfläche gelöscht werden. Verwenden Sie die unter „Löschen des Data Domain-Systems aus der VDP-Appliance" auf Seite 94 definierten manuellen Schritte, um ein Data Domain-System zu löschen.
- Wenn die Verbindung zwischen Data Domain und VDP unterbrochen ist, wird das Data Domain-System nicht von der VDP-Appliance überwacht. Verhaltensweisen, die auf einen Verbindungsverlust zwischen den Appliances hindeuten, sind u. a. fehlgeschlagene Integritätsprüfungen, `hfscheck`-Vorgänge oder Backups.
- Für das Data Domain-System oder die VDP-Appliance kann kein Upgrade durchgeführt werden, wenn ihre Verbindung zueinander unterbrochen ist.

Backup

Während eines Backups erzeugt die VDP-Appliance eine Backupanforderung für das Backupziel. Wenn die Backupanforderung die Option zum Verwenden eines Data Domain-Systems als Ziel umfasst, werden die Backupdaten auf dem Data Domain-System gespeichert. Metadaten werden auf der VDP-Appliance gespeichert.

Wiederherstellung

Der Prozess der Datenwiederherstellung ist für den Backupadministrator transparent. Der Backupadministrator nutzt die gleichen VDP-Recovery-Prozesse, die für aktuelle VDP-Implementierungen nativ sind.

Sicherheit – Verschlüsselung

Bei Verwendung einer VDP-Appliance mit einem angebundenen Data Domain-System sind 2 Backupdatenstreams möglich. Wenn die Backupdaten auf die VDP-Appliance geschrieben werden, findet immer eine „In-Flight"-Komprimierung und -Verschlüsselung der Backupdaten statt. Wenn die Backupdaten an das Data Domain-System weitergeleitet werden, werden die Backupdaten bei der Netzwerkübertragung an das Data Domain-System vom Dienstprogramm `ddboost` verschlüsselt.

Datenmigration

Backupdaten können nicht direkt von der VDP-Appliance zum Data Domain-System migriert werden.

Um das Data Domain-System und nicht die VDP-Appliance als Backupziel zum Sichern einer VM oder Appliance zu verwenden, bearbeiten Sie den Backupjob und definieren Sie das Ziel als Data Domain-System. Beginnen Sie dann, Backups auf das Data Domain-System durchzuführen. Wenn das Backupziel geändert und auf das Data Domain-System eingestellt wird, ist das nächste Backup ein komplettes Backup.

Im Anschluss an ein erfolgreiches Backup auf das Data Domain-System können vorherige Backups von der VDP-Appliance gelöscht werden. Weitere Informationen zum manuellen Löschen von Backups finden Sie unter „Löschen eines Backupjobs" auf Seite 130. Werden Backups nicht manuell gelöscht, laufen sie ab, sofern keine Intervention erfolgt.

Vor der Integration geltende Anforderungen

Schauen Sie sich vor der Integration eines Data Domain-Systems in eine VDP-Appliance die folgenden Themen an:

- „Netzwerkdurchsatz" auf Seite 89
- „Netzwerkkonfiguration" auf Seite 89
- „Konfiguration von NTP" auf Seite 90
- „Lizenzierung" auf Seite 90
- „Anforderungen an die Portverwendung und Firewalls" auf Seite 90

- „Kapazität" auf Seite 90
- „Data Domain-System-Streams" auf Seite 90
- „Vorhandene mit Data Domain verwendete Backupprodukte" auf Seite 91

HINWEIS In diesem Abschnitt wird davon ausgegangen, dass die VDP-Appliance und das Data Domain-System installiert und konfiguriert sind.

Netzwerkdurchsatz

Bei VDP können die VDP-Appliance und Data Domain-Systeme keine Verbindung über ein WAN (Wide Area Network) herstellen. Überprüfen Sie vor Verwendung dieser Konfiguration die Firewall-Portanforderungen des Data Domain-Systems. „Von VDP verwendete Ports" auf Seite 209 bietet Informationen dazu.

Sie können die VDP-Appliance-Replikation über ein WAN nutzen, um Daten von der VDP-Quell-Appliance und Data Domain-Quellsystemen auf VDP-Ziel-Appliances zu replizieren, sofern diese ebenfalls an ein Data Domain-System angebunden sind.

Vergewissern Sie sich vor der Integration eines Data Domain-Systems in eine VDP-Appliance darüber, dass die verfügbare Netzwerkbandbreite ausreichend ist. Um den maximal verfügbaren Durchsatz auf einem Data Domain-System (für Wiederherstellungen, Backups auf Ebene 0 und nachfolgende inkrementelle Backups nach einem Backup auf Ebene 0) zu erhalten, vergewissern Sie sich, dass die Netzwerkinfrastruktur mehr Bandbreite bereitstellt, als laut maximalem Durchsatz des Data Domain-Systems gefordert wird. Um den Netzwerkdurchsatz anzuzeigen, verwenden Sie den Befehl `system show performance` auf dem Data Domain-System:

```
system show performance [{hr | min | sec} [{hr | min | sec}]]
```

Beispiel:

```
system show performance 24 hr 10 min
```

Dieser Befehl zeigt die Systemperformance für die letzten 24 Stunden in 10-Minuten-Intervallen an. 1 Minute ist das Mindestintervall.

Netzwerkkonfiguration

Konfigurieren (oder überprüfen) Sie die folgende Netzwerkkonfiguration:

- Weisen Sie dem Data Domain-System einen vollständig qualifizierten Domainnamen (Fully Qualified Domain Name, FQDN) zu.
- Verwenden Sie einen vollständig qualifizierten Domain-Name (keine IP-Adresse), wenn Sie ein Data Domain-System registrieren. Hierdurch wird u. U. die Möglichkeit eingeschränkt, optimierten Deduplizierungsverkehr exklusiv über eine registrierte Schnittstelle weiterzuleiten.
- Vergewissern Sie sich, dass DNS auf dem Data Domain-System ordnungsgemäß konfiguriert ist.
- Vergewissern Sie sich, dass die DNS-Vorwärts- und -Rückwärtssuche zwischen folgenden Systemen funktioniert:
  - VDP-Appliance
  - Data Domain-System
  - Backup- und Wiederherstellungsclients
  - vCenter Server
  - vSphere-Hosts
- Verwenden Sie Hostdateien, um Hostnamen in nicht routbare IP-Adressen aufzulösen.
- Erstellen Sie keine sekundären Hostnamen zum Verknüpfen mit alternativen oder lokalen IP-Schnittstellen.

Konfiguration von NTP

Konfigurieren Sie die VDP-Appliance, vCenter Server, die vSphere-Hosts und die Data Domain-Systeme so, dass derselbe Network Time Protocol(NTP)-Server verwendet wird.

Lizenzierung

Vergewissern Sie sich, dass die Umgebung die Lizenzierungsanforderungen in Tabelle 9-12 erfüllt.

Tabelle 9-12. Lizenzierungsanforderungen

Produkt	Lizenzierungsanforderung
VDP-Appliance	Die VDP-Appliance setzt eine gültige vSphere-Hostlizenz voraus (mindestens Essentials Plus).
Data Domain-System	Die DD Boost-Lizenz muss auf dem Data Domain-System installiert sein.

Anforderungen an die Portverwendung und Firewalls

Um die Kommunikation zwischen der VDP-Appliance und den Data Domain-Systemen zu ermöglichen, lesen und implementieren Sie die unter „Von VDP verwendete Ports" auf Seite 209 beschriebenen Anforderungen an die Portverwendung und Firewalls.

Kapazität

Bewerten Sie Ihre Backupspeicheranforderungen sorgfältig, wenn Sie die Menge der auf dem Data Domain-System und der VDP-Appliance zu speichernden Daten berechnen. Schließen Sie Schätzungen von Daten ein, die von anderen Servern an das Data Domain-System gesendet werden.

Wenn das Data Domain-System seine maximale Speicherkapazität erreicht, sind auf das Data Domain-System so lange keine weiteren Backups möglich, bis zusätzliche Kapazität hinzugefügt wurde bzw. bis alte Backups gelöscht wurden oder abgelaufen sind.

Unter „Überwachen von Data Domain über die VDP-Appliance" auf Seite 102 erfahren Sie weitere Details zur Überwachung der Kapazität.

Data Domain-System-Streams

Jedes Data Domain-System hat einen weichen Grenzwert für die maximale Anzahl von Verbindungs- und Daten-Streams, die bei unveränderter Performance gleichzeitig unterhalten werden können. Die Anzahl der Streams hängt vom jeweiligen Data Domain-Systemmodell ab. DD990 kann beispielsweise 540 Backup-Streams unterstützen, DD620 hingegen 20 Backup-Streams.

Ändern des maximalen Stream-Werts

Standardmäßig ist die VDP-Appliance für die Verwendung eines maximalen Streamwerts von 16 konfiguriert.

Wenn Sie über die VDP-Appliance die Anzahl der mit einem Data Domain-System verbundenen Streams ändern müssen, führen Sie die folgenden Schritte aus. Die bei Verwendung dieser Schritte angewendeten Änderungen werden erst im Anschluss an nachfolgende Bearbeitungen oder dem Hinzufügen eines Data Domain-Systems zur VDP-Appliance wirksam.

1 Rufen Sie die Befehlszeile der VDP-Appliance auf (entweder mit SSH/Putty oder dem Terminal der Appliance) und geben Sie den folgenden Befehl ein:

cd /usr/local/vdr/etc/

2 Bearbeiten Sie die Datei `vdp-options.properties` mithilfe eines Dateieditors.

3 Fügen Sie das `com.vmware.vdp.option.datadomain.maxstreamsoverride=`*num* ein. *num* steht dabei für die maximale Stream-Anzahl für das Data Domain-System.

4 Speichern Sie die geänderte Datei.

5 Fügen Sie ein Data Domain-System hinzu oder bearbeiten Sie dieses. Räumen Sie fünf Minuten für die Ausführung des entsprechenden Prozesses ein.

Die Datei `ddrmaint read-ddr-info` sollte nun das Attribut „max-streams“ mit dem von Ihnen konfigurierten Wert enthalten.

Vorhandene mit Data Domain verwendete Backupprodukte

Data Domain-Systeme können Backup- und Archivierungssoftware von Drittanbietern verwenden. Die VDP-Appliance geht nicht davon aus, dass sie die alleinigen Eigentumsrechte am Data Domain-System besitzt. Achten Sie auf eine angemessene Dimensionierung, wenn das System zusammen mit anderen Softwareprodukten verwendet wird. Die VDP-Appliance nutzt nicht die nativen Snapshot- und Replikationsfunktionen des Data Domain-Systems.

Die Replikation erfolgt über die DD Boost-SDK-Bibliothek anhand von Kopier- und Cloningvorgängen. Allerdings greifen ggf. andere Produkte von Drittanbietern auf die nativen Snapshot- und Replikationsfunktionen des Data Domain-Systems zurück. In diesem Fall wird ein Snapshot eines gesamten Data Domain-Systems erstellt oder eine Replikation eines gesamten Data Domain-Systems umfasst die VDP-Appliance-Daten.

Vorbereiten des Data Domain-Systems auf die VDP-Integration

Achten Sie zur Unterstützung der Integration von VDP und des Data Domain-Systems darauf, dass die Umgebung die in Tabelle 9-13 aufgeführten Data Domain-Systemanforderungen erfüllt.

Tabelle 9-13. Data Domain-Systemanforderungen

Data Domain-Funktion oder -Spezifikation	Anforderung für die Verwendung mit der VDP-Appliance
Data Domain Operating System (DD OS)	Für eine VDP-Integration ist DD OS 5.4.0.8, DD OS 5.5.x oder höher erforderlich.
DD Boost	Für die VDP-Integration ist DD Boost 2.6.x erforderlich. Diese Software ermöglicht Backupservern die Kommunikation mit Speichersystemen, ohne dass Data Domain-Systeme hierzu eine Bandemulation durchführen müssen. DD Boost umfasst zwei Komponenten: eine Komponente, die auf dem Backupserver ausgeführt wird und eine Komponente, die auf dem Data Domain-System ausgeführt wird. Die Komponente, die auf dem Backupserver (DD Boost-Bibliotheken) ausgeführt wird, ist in die VDP-Appliance integriert. Die DD Boost-Software ist ein optionales Produkt, für das eine Lizenz erforderlich ist, damit es auf dem Data Domain-System betrieben werden kann.
Data Domain-Gerätetyp	Die VDP-Appliance bietet Unterstützung für alle Data Domain-Systeme, die die Ausführung der erforderlichen DD OS-Version unterstützen.
DD Boost-Benutzerkonto	Die DD Boost-Bibliothek nutzt einen eindeutigen Anmeldekontonamen, der auf dem Data Domain-System erstellt wurde. Dieser Kontoname ist als das DD Boost-Konto bekannt. Pro Data Domain-System existiert nur ein DD Boost-Konto. Wenn das Konto umbenannt und/oder das Passwort geändert wird, müssen diese Änderungen sofort durch Bearbeitung der Data Domain-Konfigurationsoptionen in der VDP-Appliance aktualisiert werden. Bleibt eine Aktualisierung der DD Boost-Kontoinformationen aus, kann dies möglicherweise zu Integritätsprüfungsfehlern und/oder Backup-/Wiederherstellungsproblemen führen. Das DD Boost-Konto muss über Administratorrechte verfügen.

Bevor der VDP-Konfiguration ein Data Domain-System hinzugefügt werden kann, muss das Data Domain-System vorbereitet werden, indem DD Boost aktiviert und ein DD Boost-Benutzerkonto für die VDP-Appliance erstellt wird. Letzteres dient für den Zugriff auf das Data Domain-System zwecks etwaiger Backup-, Wiederherstellungs- und Replikationsvorgänge.

So bereiten Sie das Data Domain-System vor:

1 Deaktivieren Sie DD Boost auf dem Data Domain-System, indem Sie sich bei der Befehlszeilenoberfläche als Administrator anmelden und den folgenden Befehl eingeben:

ddboost disable

2 Erstellen Sie ein DD Boost-Konto und -Passwort:

a Erstellen Sie mit folgendem Befehl ein Benutzerkonto mit Administratorrechten:

user add USER role admin

Dabei steht USER für den Benutzernamen des neuen Kontos.

b Legen Sie das neue Konto als DD Boost-Benutzer fest, indem Sie den folgenden Befehl eingeben:

ddboost set user-name USER

Dabei steht USER für den Benutzernamen des Kontos.

3 Geben Sie den folgenden Befehl ein, damit DD Boost die Änderungen zulässt:

ddboost enable

WICHTIGER HINWEIS Denken Sie bei einer Änderung des DD Boost-Kontonamens oder -Passworts daran, die Data Domain-Systemkonfiguration im VDP-Konfigurationsdienstprogramm zu bearbeiten. Anderenfalls schlagen alle Backups, Wiederherstellungen und Wartungsaktivitäten fehl.

Hinzufügen eines Data Domain-Systems

Ein Data Domain-System führt eine Deduplizierung über die Data Domain(DD)-Betriebssystemsoftware aus. Wenn Sie ein Data Domain-System als Backupziel auswählen, werden Backupdaten an das Data Domain-System übertragen. Nur ein Data Domain-System kann konfiguriert werden.

Verfahren

1 Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

https:<*IP_Adresse_der_VDP_Appliance*>**:8543/vdp-configure/**

2 Klicken Sie auf die Registerkarte **Speicher**.

Die Speicherzusammenfassung gibt statistische Daten über den insgesamt nutzbaren Speicher und die verfügbare Kapazität für das Data Domain-System sowie für jeden Datenspeicher wieder.

3 Wählen Sie aus der Liste **Aktion** die Option **Data Domain hinzufügen** aus.

Das Dialogfeld Hostkonfiguration wird angezeigt.

4 Legen Sie die Data Domain-Systeminformationen fest:

a Geben Sie im Feld **Vollständig qualifizierter Domainname oder IP von Data Domain** den vollständig qualifizierten Domainnamen oder die IP-Adresse des hinzuzufügenden Data Domain-Systems ein.

HINWEIS Verwenden Sie keine IP-Adresse bzw. keinen sekundären Hostnamen, die bzw. der mit alternativen oder lokalen IP-Schnittstellen verbunden ist. Dies kann die Fähigkeit der VDP-Appliance zur Weiterleitung von optimiertem Deduplizierungsdatenverkehr einschränken.

b Geben Sie im Feld **DDBoost-Benutzername** den Namen des DD Boost-Kontos für VDP ein, mit dem zwecks Backup-, Wiederherstellungs- und Replikationsvorgängen auf das Data Domain-System zugegriffen werden soll.

c Geben Sie im Feld **Passwort** das Passwort für das Konto ein, das VDP für den Zugriff auf das Data Domain-System zwecks Backup-, Wiederherstellungs- und Replikationsvorgängen verwenden soll.

d Wiederholen Sie Ihre Eingabe im Feld **Passwort bestätigen**, um das Passwort zu bestätigen.

e Aktivieren Sie das Kontrollkästchen **Kontrollpunktkopie aktivieren**, um die Unterstützung für Kontrollpunktbackups zu aktivieren. Hierdurch können VDP-Kontrollpunkte auf einem Data Domain-System (mit DD OS 5.3 oder höher) gespeichert werden. Diese Kontrollpunkte werden dann im Bedarfsfall zur Disaster Recovery eingesetzt.

5 Klicken Sie zum Konfigurieren von SNMP auf **Weiter**.

Das Dialogfeld „SNMP“ wird angezeigt. Die zu konfigurierenden SNMP-Optionen für die VDP- und Data Domain-Systemintegration umfassen Folgendes:

- Im Textfeld **Getter-/Setter-Portnummer** wird der Port auf dem Data Domain-System aufgeführt, über den SNMP-Objekte empfangen bzw. festgelegt werden. Der Standardwert ist 161.
- Im Textfeld **SNMP-Communityzeichenfolge** wird die von VDP für schreibgeschützten Zugriff auf das Data Domain-System verwendete Communityzeichenfolge aufgeführt.
- Im Textfeld **Trap-Portnummer** wird der Trap-Port aufgeführt. Der Standardwert ist 163.

6 Klicken Sie auf **Weiter**.

Das Dialogfeld „Bereit zur Fertigstellung“ wird angezeigt.

7 Klicken Sie auf **Hinzufügen**, um Ihre Data Domain-Konfiguration zu speichern.

Durch einen erfolgreichen Vorgang „Data Domain hinzufügen“ kommt es in der Benutzeroberfläche zu den folgenden Änderungen:

- Das System erstellt einen neuen Kontrollpunkt. Dies dauert ca. 10 Minuten.
- Die Data Domain-Informationen werden auf der VDP-Appliance in den folgenden Bereichen angezeigt:
  - Registerkarte **Backup**: Das Data Domain-System ist als Speicherziel im Assistenten „Neuen Backupjob erstellen“ verfügbar.
  - **Registerkarte** Wiederherstellen: Hier wird das Data Domain-System in der Spalte „Name“ des Assistenten „Backup wiederherstellen“ angezeigt.
  - Registerkarte **Berichte**: Hier werden Backupstatusberichte für das Data Domain-System bereitgestellt.
  - **Speicherzusammenfassung**: Hier werden statistische Daten über den insgesamt nutzbaren Speicher und die verfügbare Kapazität für das Data Domain-System angezeigt. Details finden Sie unter „Anzeigen der Speicherkonfiguration“ auf Seite 83.
  - **E-Mail-Reporting**: Hier wird eine Zusammenfassung der Data Domain-Konfiguration angezeigt.

HINWEIS Wenn der VDP-Konfiguration ein Data Domain-System hinzugefügt wird, erstellt die VDP-Appliance auf dem Data Domain-System für die VDP-Appliance ein MTree-Verzeichnis. „Mtree“ bezieht sich auf das innerhalb des DD Boost-Pfads erstellte Verzeichnis. Data Domain-Systeme unterstützen maximal 100 Mtree-Verzeichnisse. Nach dem Erreichen dieses Grenzwerts ist es nicht mehr möglich, der VDP-Konfiguration das Data Domain-System hinzuzufügen.

Bearbeiten des Data Domain-Systems

1 Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

https:<*IP_Adresse_der_VDP_Appliance*>**:8543/vdp-configure/**

2 Klicken Sie auf die Registerkarte **Speicher**.

Die Speicherzusammenfassung gibt statistische Daten über den insgesamt nutzbaren Speicher und die verfügbare Kapazität für das Data Domain-System sowie für jeden Datenspeicher wieder.

3 Wählen Sie aus der Liste **Aktion** die Option **Data Domain bearbeiten** aus.

Das Dialogfeld **Hostkonfiguration** wird angezeigt.

4 Bearbeiten Sie nach Bedarf die Einstellungen für das Data Domain-System. Unter „Hinzufügen eines Data Domain-Systems" auf Seite 92 erfahren Sie weitere Details zu den einzelnen Einstellungen des Dialogfelds.

5 Klicken Sie auf **Weiter**.

6 Klicken Sie nach der abgeschlossenen Bearbeitung auf **Fertig stellen**.

HINWEIS Wenn Sie den Hostnamen des Data Domain-Systems, den DD Boost-Benutzernamen oder das DD Boost-Passwort bearbeiten, erstellt das System automatisch einen neuen Kontrollpunkt. Dies dauert ca. 10 Minuten. Informationen zum Kontrollpunkt finden Sie unter „Rollback einer Appliance" auf Seite 43.

HINWEIS Bei einem Rollback auf einen Kontrollpunkt mit veraltetem Data Domain-Systemnamen oder veralteten DD Boost-Informationen schlägt das Rollback fehl.

Löschen des Data Domain-Systems aus der VDP-Appliance

Vor dem Löschen des Data Domain-Systems aus der VDP-Appliance ist Folgendes zu beachten:

- Sie müssen alle auf dem Data Domain-System gespeicherten Wiederherstellungspunkte mithilfe des VDP-Plug-ins in vSphere Web Client löschen.
- Es dürfen keinerlei Backupjobs in Bezug auf das Data Domain-System vorhanden sein. Sollten Backupjobs mit als Ziel konfiguriertem Data Domain-System existieren, müssen die Backupjobs entweder bearbeitet und auf ein neues Ziel eingestellt oder die Backupjobs gelöscht werden.
- Nach Prüfung der Wiederherstellungspunkte und Verifizierung der Backupjobs hat es sich als Best Practice bewährt, über die Registerkarte **Konfiguration** der VDP-Appliance eine Integritätsprüfung durchzuführen.
- Entfernen Sie mithilfe der Befehlszeilenoberfläche das Data Domain-System aus VDP. Ausführliche Anweisungen finden Sie unten.
- Nachdem das Data Domain-System gelöscht wurde, führen Sie eine weitere Integritätsprüfung von der VDP-Benutzeroberfläche aus durch, um zu überprüfen, ob das Data Domain-System gültig ist.

HINWEIS Der VMware-Knowledgebase-Artikel 2063806 liefert Informationen über das Löschen eines Data Domain-Systems. Hierbei handelt es sich um einen internen Artikel. Wenden Sie sich also hierfür an den technischen Support.

Verfahren

1 Bevor Sie das Data Domain-System löschen, entfernen Sie alle Wiederherstellungspunkte, die auf dem Data Domain-System gespeichert sind. Verwenden Sie vSphere Web Client zum Löschen von Wiederherstellungspunkten:

a Navigieren Sie zur Registerkarte **Wiederherstellen** des VDP-Plug-ins.

b Wählen Sie in der Navigationsleiste die Registerkarte **Manuelle Wiederherstellung** aus.

c Entfernen Sie für auf dem Data Domain-System gesicherte Clients sämtliche Wiederherstellungspunkte, bei denen der Speicherort angibt, dass sie auf dem Data Domain-Server gespeichert sind.

2 Vergewissern Sie sich, dass keine Backupjobs das Data Domain-System als Ziel verwenden. Wenn Backupjobs mit dem Data Domain-System als Ziel vorhanden sind, müssen Sie den Backupjob bearbeiten, um ein neues Ziel festzulegen, oder Sie müssen den Backupjob löschen.

3 Nach Prüfung der Wiederherstellungspunkte und Verifizierung der Backupjobs hat es sich als Best Practice bewährt, über die Registerkarte „Konfiguration“ des VDP-Plug-ins eine Integritätsprüfung durchzuführen.

4 Sobald die Integritätsprüfung und die Validierung der Integritätsprüfung abgeschlossen sind, entfernen Sie das Data Domain-System aus der VDP-Appliance. Verwenden Sie die Befehlszeile.

a Öffnen Sie eine SSH- oder Putty-Sitzung für die VDP-Appliance.

b Führen Sie den Befehl `status.dpn` aus und überprüfen Sie, ob `Last checkpoint` und Last hfscheck abgeschlossen wurden. Sollte dies nicht der Fall sein, wiederholen Sie diesen Schritt so lange, bis sie einen abgeschlossenen Status aufweisen.

c Führen Sie den Befehl `mccli server show-prop` aus. Mit diesem Befehl werden Ergebnisse wie die folgende Ausgabe angezeigt:

Attribute	Value
State	Full Access
Active sessions	0
Total capacity	575.9 GB
Capacity used	0 bytes
Server utilization	0.0%
Bytes protected	0 bytes
Bytes protected quota	Not configured
License expiration	Never
Time since Server initialization	1 days 20h:58m
Last checkpoint	2014-10-10 09:03:48 MDT
Last validated checkpoint	2014-10-09 09:02:16 MDT
System Name	gs-pod187.test.domain
System ID	1381255529@00:50:56:86:46:10
HFSAddr	gs-pod187.test.domain
HFSPort	27000

Die System-ID enthält eine Zahl, dann ein @-Zeichen und die MAC-Adresse der VDP-Appliance. Notieren Sie die Zahl vor dem @-Zeichen. Bei einem Data Domain-System wird diese Zahl als DPN-ID bezeichnet.

5 Führen Sie den folgenden Befehl aus:

ddrmaint has-backups –dpnid=*num* **–*ddr-server*=DDRSERVER** | grep ‘ hasbackups’

Dabei ist *num* die von Ihnen in Schritt c notierte DPN-ID und *DDRSERVER* ist entweder der Hostname oder die IP-Adresse des DDR-Servers. Achten Sie auf das Leerzeichen im `grep`-Befehl zwischen dem einfachen Anführungszeichen und dem Wort „hasbackups“.

Dieser Befehl zeigt eines der folgenden Ergebnisse an:

```
hasbackups="true"
```

oder

```
hasbackups="false"
```

6 Wenn `hasbackups='true'` als Information zurückgegeben wird, prüfen Sie, ob Schritt 1 und Schritt 2 wiederholt werden müssen. Nachdem Sie Schritt 1 und Schritt 2 wiederholt haben (oder sich vergewissert haben, dass die Schritte abgeschlossen wurden), wiederholen Sie Schritt 5.

7 Wenn Schritt 5 nach wie vor `'hasbackups=true'` zeigt, fahren Sie mit Schritt a fort. Andernfalls müssen Sie Schritt 11 ausführen.

Wenn Sie versucht haben, Backups über die VDP-Benutzeroberfläche aus dem Data Domain-System zu entfernen, und das Data Domain-System nach wie vor angibt, dass die Backupdaten vorhanden sind, müssen Sie die Data Domain-Datenpartition auf einer Linux-VM mounten, um das Datenverzeichnis zu bereinigen. Wenn keine Linux-VM verfügbar ist, können Sie die VDP-Appliance für die nächsten Schritte verwenden.

Standardmäßig werden alle Daten für Backups auf einem Data Domain-System unter einer LSU (Logical Storage Unit, logischen Speichereinheit) gespeichert. Die LSU für VDP heißt `Avamar-<DPNID>` und befindet sich unter `/data/col1`.

Wenn Sie über die Schnittstellen des Data Domain-Betriebssystems nicht auf das Dateisystem zugreifen können, müssen Sie der LSU Remotezugriff gewähren. Hierzu müssen Sie über die folgenden Schritte remote auf das Data Domain-System zugreifen:

a Öffnen Sie eine SSH- oder Putty-Sitzung für das Data Domain-System.

b Führen Sie den Befehl `nfs add /data/col1 <IP der Linux-VM>` aus.

Dieser Befehl sollte das folgende Ergebnis zurückgegeben: `NFS export for "/data/col1" added`.

Wenn der Befehl nicht das erwartete Ergebnis zurückgibt, können Sie `nfs help` eingeben, um eine Manpage des Befehls aufzurufen. Wenn der Befehl das erwartete Ergebnis zurückgibt, können Sie die SSH- oder Putty-Sitzung beenden.

c Öffnen Sie eine Putty- oder SSH-Sitzung für die Linux-VM, die in Schritt b als Root-Benutzer verwendet wurde.

d Führen Sie den Befehl `mkdir /mnt/DataDomain01` aus.

e Führen Sie den Befehl `mount <IP von DD>:/data/col1 /mnt/DataDomain01` aus.

f Führen Sie den Befehl `ls -ltr /mnt/DataDomain01/avamar-<DPNID>` aus. Dabei ist `DPNID` der in Schritt c notierte Wert. Die Ausgabe sollte Unterverzeichnisse anzeigen, in denen die VDP-Backups gespeichert werden.

g Führen Sie den Befehl `rm -rf /mnt/DataDomain01/avamar-<DPNID>/*` aus. Dabei ist `DPNID` der in Schritt c notierte Wert. Damit werden alle Daten aus den VDP-Backups entfernt.

8 Wiederholen Sie Schritt f, um zu überprüfen, ob alle Daten entfernt wurden.

9 Beenden Sie die virtuelle Linux-Maschine.

10 Öffnen Sie eine Putty- oder SSH-Sitzung für die VDP-Appliance.

11 Führen Sie den Befehl `mccli dd delete --name=<DD-IP oder -Hostname> --force=true` aus.

12 Nach dem Entfernen des Data Domain-Systems führen Sie eine Integritätsprüfung über die VDP-Benutzeroberfläche durch. Die alten Kontrollpunkte mit den Data Domain-Informationen sind nun ungültig.

Backups mit VDP und Data Domain

In den folgenden Themen werden VDP- und Data Domain-Systembackups beschrieben:

- Funktionsweise von Backups mit VDP und Data Domain-System
- Auswählen eines Data Domain-Ziels für Backups

Funktionsweise von Backups mit VDP und Data Domain

Während eines Backups sendet die VDP-Appliance eine Backupanforderung an vCenter Server. Wenn die Backupanforderung die Option zum Verwenden eines Data Domain-Systems als Ziel umfasst, werden die Backupdaten auf dem Data Domain-System gespeichert. Metadaten werden auf der VDP-Appliance gespeichert.

In den folgenden Themen finden Sie zusätzliche Details zur Funktionsweise von Backups mit VDP und Data Domain.

Speicherort von Backupdaten

Alle Daten für ein Backup werden unter einem einzigen dedizierten Mtree-Verzeichnis eines Data Domain-Systems gespeichert.

Management von Backupdaten mit der VDP-Appliance

Während eines Backups sendet die VDP-Appliance die Metadaten für das Backup vom Client an die VDP-Datenpartitionen. Dieser Prozess ermöglicht der VDP-Appliance das Management des Backups, obwohl die Daten auf einem Data Domain-System gespeichert sind.

Die VDP-Appliance speichert den ursprünglichen Pfad sowie den ursprünglichen Dateinamen einer Datei nicht auf dem Data Domain-System. Stattdessen nutzt die VDP-Appliance eindeutige Dateinamen auf dem Data Domain-System.

Unterstützte Backuptypen

Speichern Sie alle Backuptypen (komplett, differenziell, inkrementell) für einen Client auf demselben Ziel (VDP-Appliance oder Data Domain-System). Backuptypen sollten nicht über Ziele hinweg verteilt werden. Speichern Sie beispielsweise nicht das erste komplette Backup eines Clients auf der VDP-Appliance und nachfolgende differenzielle Backups auf dem Data Domain-System.

Abbrechen und Löschen von Backups

Wenn ein Backup während seiner Ausführung abgebrochen wird, löscht die VDP-Appliance während des nächsten VDP-Appliance-Prozesszyklus zur automatischen Speicherbereinigung die auf dem Data Domain-System geschriebenen Backupdaten.

Beim Löschen eines Backups in VDP wird das Backup während des nächsten VDP-Prozesszyklus zur automatischen Speicherbereinigung aus dem Data Domain-System gelöscht.

Unter „Löschen eines Backupjobs" auf Seite 130 finden Sie Anweisungen zum Abbrechen oder Löschen eines Backups.

Auswählen eines Data Domain-Ziels für Backups

Nach der Integration der VDP-Appliance und des Data Domain-Systems besteht bei jedem Backupziel für die VDP-Appliance die Möglichkeit, den Data Domain-Speicher als „Ziel“ im Workflow „Neuen Backupjob erstellen“ zu verwenden, wie in Abbildung 9-6 gezeigt.

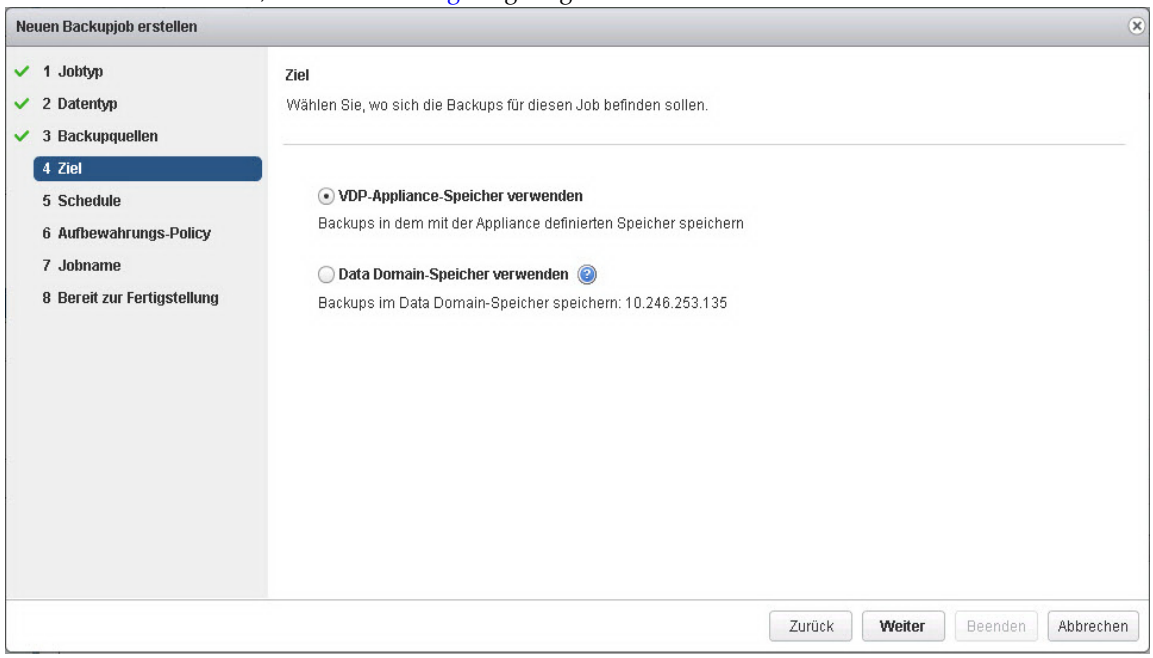


Abbildung 9-6. Assistent „Neuen Backupjob erstellen“ – Seite „Ziel“

Über den Assistenten zum Ändern eines Backupjobs können Sie das Ziel für einen Backupjob ändern. Weitere Informationen zum Bearbeiten von Backupjobs finden Sie unter „Bearbeiten eines Backupjobs“ auf Seite 130.

HINWEIS Wenn das Ziel eines Backupjobs geändert wird, ist das nächste Backup ein komplettes Backup. Unter dem neuen Ziel sind die Daten des vorherigen kompletten Backups nicht gespeichert.

Replikationskontrolle

Wenn eine VDP-Appliance mit einem angebundenen Data Domain-System Backupdaten repliziert, erfolgt die Replikation zwischen den Data Domain-Systemen. Allerdings werden Replikationsjobs mithilfe der VDP-Benutzeroberfläche konfiguriert.

Konfiguriert und überwacht wird die Replikation auf der VDP-Appliance. Die Replikationsaktivität kann durch Überprüfung der DD Boost-Aktivität auch über das Data Domain-System überwacht werden. Anweisungen zur Überwachung dieser Aktivität finden Sie im *DD OS-Administrationshandbuch*.

Verwenden Sie nicht die Data Domain-Replikationsfunktion, um eine Replikation der Daten zu initiieren, die von einer VDP-Appliance gesichert wurden. Bei Verwendung der Data Domain-Replikation verweisen die replizierten Daten nicht auf die verknüpfte VDP-Appliance, da die auf der VDP-Appliance gespeicherten Metadaten nicht repliziert wurden.

Replikationsdatenstrom

VDP repliziert die Daten direkt zwischen Data Domain-Systemen. Im Rahmen des Replikationsprozesses werden alle zu replizierenden Backups untersucht. Wenn dabei ermittelt wird, dass die Backupdaten auf einem Data Domain-System gespeichert sind, gibt der Prozess eine Anforderung aus, um die Daten mit DD Boost vom Data Domain-Quellsystem auf das Data Domain-Zielsystem zu replizieren. In diesem Fall sind die Data Domain-Systeme für die Replikation der Daten verantwortlich. Eine entsprechende Analyse erfolgt für jedes Backup, das repliziert wird.

Replikationsplanung

Die Replikation der VDP-Daten auf einem Data Domain-System erfolgt innerhalb der VDP-Replikationsplanung. Sie können die Replikation von Daten auf dem Data Domain-System nicht separat von der Replikation der Daten auf der VDP-Appliance planen.

Replikationskonfiguration

Zum Konfigurieren einer Replikation bei Verwendung eines Data Domain-Systems als Backupziel für VDP verwenden Sie das VDP-Plug-in in vSphere Web Client.

Weitere Informationen zum Konfigurieren einer VDP-Replikation finden Sie unter „Replikation“ auf Seite 151.

HINWEIS Wenn es sich im Replikationsfall bei der Quelle um eine an ein Data Domain-System angebundene VDP-Appliance handelt, muss an das Ziel (ob Avamar-Server oder VDP-Appliance) ebenfalls ein Data Domain-System angebunden sein.

Replikationsüberwachung mit VDP

Führen Sie zur Überwachung der Replikationsaktivität mit der VDP-Appliance, einschließlich Replikationsaktivitäten mit einem Data Domain-System, folgende Schritte durch:

1 Melden Sie sich in vSphere Web Client beim vSphere Data Protection-Plug-in an.

2 Klicken Sie auf die Registerkarte **Replikation**.

- Auf der Registerkarte **Replikation** werden alle Replikationsjobs, die letzte Ausführungszeit sowie die nächste geplante Ausführungszeit angezeigt.
- Beim Auswählen eines Replikationsjobs werden der Zielserver und die Clients, die im Abschnitt mit den Details zum Replikationsjobs enthalten sind, dargestellt.
- Wenn Sie die Spalte „Replikation“ auswählen, werden auf der Registerkarte **Berichte** für jeden geschützten Client der Replikationsjob und die letzte Ausführungszeit der Replikation angezeigt.

Überwachung serverbezogener Wartungsaktivitäten

Die VDP-Appliance führt die Systemwartungsvorgänge für Backupdaten auf dem Data Domain-System durch, darunter VDP-Integritätsprüfungen, Kontrollpunkte, Rollbacks, die automatische Speicherbereinigung und das sichere Löschen von Backups.

Das `ddrmaint`-Dienstprogramm implementiert für die VDP-Appliance alle erforderlichen Vorgänge auf dem Data Domain-System. Das `ddrmaint`-Dienstprogramm protokolliert sämtliche Wartungsaktivitäten auf der VDP-Appliance in der Datei `ddrmaint.log`. Die Protokolldatei befindet sich im Verzeichnis `/usr/local/avamar/var/ddrmaintlogs`.

Wenn die Protokolldatei `ddrmaint.log` eine Größe von 25 MB erreicht, kommt es zu einer Rotation der vorhandenen Protokollversion. Die vorhandene Protokolldatei `ddrmaint.log` wird in `ddrmaint.log.1` umbenannt und es wird eine neue Datei `ddrmaint.log` erstellt. Bei älteren Kopien von `ddrmaint.log.X` erhöht sich der Protokollzähler ebenfalls um einen Wert von eins. (Die Datei `ddrmaint.log.1` ändert sich zu `ddrmaint.log.2` usw.)

Wiederherstellen der Avamar-Kontrollpunktbackups von Data Domain-Systemen

Wenn Sie VDP-Kontrollpunktbackups auf einem Data Domain-System erstellt haben, können Sie bei einem Ausfall der ursprünglichen VDP-Appliance einen Kontrollpunkt auf eine neue VDP-Appliance wiederherstellen.

Annahmen für den Wiederherstellungsvorgang

Das Verfahren unter „Durchführen der Kontrollpunktwiederherstellung" auf Seite 100 erläutert, wie bei folgenden Annahmen eine Kontrollpunktwiederherstellung durchgeführt wird:

- Sie verfügen über einen gültigen Kontrollpunkt für eine VDP-Appliance auf einem Data Domain-Zielsystem.
- Die ausgefallene VDP-Appliance wurde ersetzt.
- Bei der als Ersatz verwendeten VDP-Appliance handelt es sich um eine neue Appliance ohne Backupdaten oder Metadaten.
- Die als Ersatz verwendete VDP-Appliance ist entweder genauso groß oder größer als die ursprüngliche VDP-Appliance.
- Die als Ersatz verwendete VDP-Appliance muss dieselbe Anzahl an Datenpartitionen aufweisen wie die ursprüngliche VDP-Appliance.
- Die als Ersatz verwendete VDP-Appliance muss denselben Hostnamen und dieselbe IP-Adresse verwenden wie die ursprüngliche VDP-Appliance.

Durchführen der Kontrollpunktwiederherstellung

So stellen Sie einen Kontrollpunkt von einem Data Domain-System auf eine neue VDP-Appliance wieder her:

1 Melden Sie sich bei der VDP-Appliance als Root an und fragen Sie über eine CLI-Eingabeaufforderung die für eine Wiederherstellung verfügbaren Kontrollpunkte ab, indem Sie den folgenden Befehl eingeben:

ddrmaint cp-backup-list --full --ddr-server=*Data_Domain_syste***m** *--ddr-user=***DD_Boost_user_name** *--ddr-password=DD_Boost_user_password*

Hierbei gilt:

- *Data_Domain_system* steht dabei für das Data Domain-System mit dem VDP-Appliance-Kontrollpunktbackup.
- *DD_Boost_user_name* steht dabei für das zur VDP- und Data Domain-Systemintegration verwendete DD Boost-Benutzerkonto.
- *DD_Boost_user_password* steht dabei für das zur VDP- und Data Domain-Systemintegration verwendete DD Boost-Benutzerkontopasswort.

Die Ausgabe ähnelt dem folgenden Beispiel:

```
================== Checkpoint ==================
VDP Advanced Name: a4dpe223d
VDP Advanced MTree/LSU: avamar-1346892530
Data Domain System Name: griffin-dd10.asl.lab.emc.com
VDP Advanced Client Path: /MC_SYSTEM/avamar-1346892530
VDP Advanced Client ID: 8b75468f70dc8ff0fa2e5118cec8ecdddf7fccee
Checkpoint Name: cp.20140919184604
Checkpoint Backup Date: 2014-09-19 11:51:12
Data Partitions: 6
Attached Data Domain systems: griffin-dd10.asl.lab.emc.com
```

2 Stellen Sie mit dem Befehl `cprestore` die auf der VDP-Appliance gespeicherten Backups anhand des Kontrollpunkts wieder her, der auf dem Data Domain-System vorhanden ist (Data Domain-Servername und -Anmeldedaten für das Data Domain-Zielsystem des standardmäßigen Backups erforderlich).

Der Befehl `cprestore` wird für den Wiederherstellungsvorgang verwendet. Der Befehl `cprestore` schließt die folgenden Aufgaben ab:

- `E`rstellen des NFS-Exports auf dem Data Domain-System
- `M`ounten des Data Domain-NFS-Exports auf der VDP-Appliance
- `K`opieren der auf der VDP-Appliance benötigten Backupdateien vom Backupkontrollpunkt des Data Domain-Systems in das entsprechende VDP-Appliance-Kontrollpunktverzeichnis jeder Datenpartition
- `R`ückgängigmachen von NFS-Mount- und -Exportvorgängen

Um die Backups auf dem Data Domain-System wiederherzustellen, geben Sie den folgenden Befehl in der VDP-Appliance ein:

/usr/local/avamar/bin/cprestore --hfscreatetime=*VDP_ID* **--ddr-server=***Data_Domain_system*
--ddr-user=*DD_Boost_user_name* **--cptag=***Checkpoint_name*

Hierbei gilt:

- *VDP_ID* wird anhand der Ausgabe von Schritt 1 ermittelt. Laut dem VDP-Appliance-Feld `MTree/LSU:avamar-1346892530` weist die `VDP_ID` den Wert `1346892530` auf.
- *Data_Domain_system* steht dabei für das Data Domain-System mit dem VDP-Appliance-Kontrollpunktbackup. Im vorherigen Beispiel einer Kontrollpunktausgabe lautet der Wert `griffin-dd10.asl.lab.emc.com`.
- *DD_Boost_user_name* steht dabei für das zur VDP- und Data Domain-Systemintegration verwendete DD Boost-Benutzerkonto. Im vorherigen Beispiel einer Kontrollpunktausgabe lautet der Wert `VDP`.
- *Checkpoint_name* steht für den Kontrollpunktnamen. Im vorherigen Beispiel einer Kontrollpunktausgabe lautet der Wert `cp.20140919184604`.

3 Stoppen Sie die VDP-Appliance durch Eingabe des folgenden Befehls:

dpnctl stop

Die Bestätigungsmeldung „Do you wish to shut down the local instance of EMS?“ wird angezeigt. Geben Sie **Y** ein.

4 Um ein Rollback zu initiieren, geben Sie den folgenden Befehl ein:

dpnctl start --force_rollback

Eine Meldung wird angezeigt und meldet, dass die Appliance heruntergefahren wurde. Eine Auswahlliste wird ebenfalls angezeigt.

5 Wählen Sie Option **3, „Select a specific checkpoint to which to roll back“**.

Warten Sie, bis das Rollback abgeschlossen ist. Je nach Datenmenge auf der VDP-Appliance kann das Rollback bis zu eine Stunde in Anspruch nehmen. Nach Abschluss des Rollbacks wird erneut die Eingabeaufforderung angezeigt.

6 Öffnen Sie die während des Rollbacks erstellte benutzerdefinierte temporäre Datei und vergewissern Sie sich, dass das Rollback erfolgreich und ohne Fehler abgeschlossen wurde.

7 Wenn der interne Proxy aktiviert ist, deaktivieren Sie ihn zunächst und aktivieren Sie ihn dann unter Verwendung des VDP-Konfigurationsdienstprogramms erneut.

8 Wenn verwaiste Proxys bestehen, also externe Proxys, die auf einer älteren VDP-Appliance bereitgestellt wurden, führen Sie die folgenden Schritte mit den VDP-Konfigurationsprogramm durch:

a Löschen Sie die verwaisten Proxys.

b Ändern Sie das Passwort für die VDP-Appliance.

c Fügen Sie die externen Proxys hinzu.

9 Erstellen Sie einen neuen Kontrollpunkt auf der VDP-Appliance:

a Wählen Sie auf der Registerkarte **VDP-Konfiguration** die Option Integritätsprüfung ausführen aus, um einen neuen Kontrollpunkt zu erstellen.

b Klicken Sie nach der Initiierung des Kontrollpunkts auf „OK“.

Überwachen von Data Domain über die VDP-Appliance

Verwenden Sie zum Überprüfen allgemeiner Informationen zur Kapazität eines an eine VDP-Appliance angebundenen Data Domain-Systems entweder vSphere Web Client oder das VDP-Konfigurationsdienstprogramm.

- Öffnen Sie in vSphere Web Client das VDP-Plug-in und navigieren Sie zur Registerkarte **Konfiguration**, um eine Kapazitätszusammenfassung für das Data Domain-System anzuzeigen.
- Öffnen Sie im VDP-Konfigurationsdienstprogramm die Registerkarte **Speicher**, um eine Speicherzusammenfassung für das Data Domain-System anzuzeigen.

HINWEIS Klicken Sie zum Aktualisieren der Daten auf der Seite auf das Symbol zum Aktualisieren neben **Speicherzusammenfassung**.

Wenn das Data Domain-System seine Kapazitätsgrenze erreicht, ist es möglich, anhand der Anweisungen unter „Wiedergewinnen von Speicher auf einem vollen Data Domain-System“ auf Seite 103 Speicherplatz auf dem Gerät wiederzugewinnen.

Tabelle 9-14. Kapazitätsschwellenwerte für Data Domain

Schwellenwert	Wert	Verhalten
Kapazitätswarnung	80 %	VDP gibt ein Warnereignis aus.
Kapazitätsfehler	95 %	Für Backupjobs werden in vCenter keine Aufgaben generiert, wenn die Data Domain-Kapazität über 95 % liegt.
Grenzwert für Integritätsprüfung	95 %	Der Abschluss vorhandener Backups wird zugelassen, neue Backupvorgänge werden jedoch unterbrochen. VDP gibt Fehlerevents für Data Domain aus.

HINWEIS Wenn das Data Domain-System 99 % seiner Kapazität erreicht, schlagen Wartungsvorgänge fehl. Als Best Practice wird empfohlen, die Data Domain-Kapazitätsauslastung auf 80 % zu beschränken.

Monitoring mithilfe des vSphere-Webclients

1 Öffnen Sie das VDP-Plug-in in vSphere Web Client

2 Auf der Registerkarte **Konfiguration** werden im Abschnitt **Speicherzusammenfassung** die folgenden Informationen angezeigt:

- Vollständig qualifizierter Domainname oder IP-Adresse des Data Domain-Systems
- Kapazität des Data Domain-Systems
- Freier Speicherplatz auf dem Data Domain-System
- Genutzte Kapazität auf dem Data Domain-System

3 Auf der linken Seite wird eine Farbcontainervariante zum Prüfen der Data Domain-Kapazität angezeigt:

- Wenn die genutzte Speicherkapazität unter 80 % liegt, ist der Container grün.
- Wenn die genutzte Speicherkapazität zwischen 80 % und 95 % liegt, ist der Container gelb. Es wird folgende Meldung angezeigt:

  ```
  Der Data Domain-Speicher ist fast voll.
  ```

- Wenn die genutzte Speicherkapazität zwischen 95 % und 100 % liegt, ist der Container rot. Es wird folgende Meldung angezeigt:

```
Der Data Domain-Speicher ist fast voll.
```

- Wenn die genutzte Speicherkapazität bei 100 % liegt, ist der Container rot. Es wird folgende Meldung angezeigt:

  ```
  Der Data Domain-Speicher ist voll.
  ```

Monitoring mithilfe des VDP-Konfigurationsdienstprogramms

1 Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

https://<*IP_Adresse*_der_*VDP_Appliance*>**:8543/vdp-configure/**

2 Auf der Registerkarte **Speicher** werden im Abschnitt **Speicherzusammenfassung** die folgenden Informationen angezeigt:

- DD-Hostname oder -IP-Adresse
- Insgesamt nutzbarer Speicher
- Verfügbarer Speicher
- Belegte Kapazität (in Prozent)

HINWEIS Klicken Sie zum Aktualisieren der Daten auf der Seite auf das Symbol zum Aktualisieren neben **Speicherzusammenfassung**.

3 Auf der linken Seite wird eine Farbcontainervariante zum Prüfen der Data Domain-Kapazität angezeigt:

- Wenn die genutzte Speicherkapazität unter 80 % liegt, ist der Container grün.
- Wenn die genutzte Speicherkapazität zwischen 80 % und 95 % liegt, ist der Container gelb. Es wird folgende Meldung angezeigt:

  ```
  Der Data Domain-Speicher ist fast voll.
  ```

- Wenn die genutzte Speicherkapazität zwischen 95 % und 100 % liegt, ist der Container rot. Es wird folgende Meldung angezeigt:

  ```
  Der Data Domain-Speicher ist fast voll.
  ```

- Wenn die genutzte Speicherkapazität bei 100 % liegt, ist der Container rot. Es wird folgende Meldung angezeigt:

  ```
  Der Data Domain-Speicher ist voll.
  ```

Wiedergewinnen von Speicher auf einem vollen Data Domain-System

Falls Sie den gesamten Speicherplatz auf einem Data Domain-System verwenden, können die folgenden Probleme auftreten:

- Backups schlagen fehl und starten ggf. nicht.
- Vorgänge, die Informationen auf dem Data Domain-System ändern, schlagen fehl, darunter das Löschen von Kontrollpunkten, aktiven Backups und abgelaufenen Backups während der Sammlung veralteter Daten. Diese Vorgänge schlagen ggf. fehl, weil es dabei zu Verzeichnisumbenennungen kommt, die auf einem vollen Data Domain-System nicht gestattet sind.

So gewinnen Sie belegten Speicher auf einem vollen Data Domain-System wieder:

1 Bestimmen Sie die Quelle der Daten, die den Speicher belegen. Die Daten können von einem bestimmten Client, von einer Gruppe von Clients, die einer bestimmten VDP-Appliance zugeordnet sind, oder von einem anderen Backupprodukt, das Daten auf dem Data Domain-System speichert, stammen.

2 Brechen Sie alle Backups ab, die gerade durchgeführt werden. Sie müssen dies über die Befehlszeile der VDP-Appliance durchführen.

   a Öffnen Sie eine SSH- oder Putty-Sitzung für die VDP-Appliance und führen Sie die folgenden Befehle aus:

   ```
   su - admin
   ssh-agent bash
   ssh-add .ssh/dpnid
   ```

   b Führen Sie den Befehl `mccli activity show` aus.

   Dieser Befehl gibt Ergebnisse zurück, die dem folgenden Ausgabebeispiel ähneln:

```
admin@gs-pod192:~/>: mccli activity show
0,23000,CLI command completed successfully.
ID              Status  Error Code Start Time          Elapsed   End Time          Type          Progress Bytes New Bytes Client
                        Domain
--------------- ------- ---------- -------------------- --------- ----------------- ------------- -------------- --------- ---------
9138660744236309 Running   0 2013-12-09 09:44 MST 00h:27m:25s 2013-12-10 09:44 MST On-Demand Backup 54.3 GB
                        4.2%      Win2008R2-GSClone /10.7.242.175/VirtualMachines
9138660744234709 Completed 0 2013-12-09 09:44 MST 00h:02m:51s 2013-12-09 09:47 MST On-Demand Backup 40.0 GB
                        <0.05%    GermanExchange    /10.7.242.175/VirtualMachines
9138660718256909 Completed 0 2013-12-09 09:39 MST 00h:01m:06s 2013-12-09 09:40 MST On-Demand Backup 40.0 GB
                        <0.05%    GermanExchange    /10.7.242.175/VirtualMachines
9138660744235609 Completed 02013-12-09 09:44 MST 00h:20m:37s 2013-12-09 10:04 MST On-Demand Backup 40.0 GB
                        2.6%      ActiveDirectory   /10.7.242.175/VirtualMachines \
```

   Um den Befehl auszuführen, der die laufende Backupjobs abbricht, müssen Sie das Appliance-Passwort kennen (unten als Wert „AppliancePassword“ eingegeben). Sie müssen sich außerdem die ID aller laufenden Jobs notieren.

   c Geben Sie den Befehl `mccli activity cancel --mcsuserid=`*`MCUser`* `--mcpasswd=`*`AppliancePassword`* `--id=XXXXX` ein. *`AppliancePassword`* steht dabei für das Appliance-Passwort und `XXXX` ist die ID des laufenden Jobs, der abgebrochen werden soll. Dieser Befehl gibt Ergebnisse zurück, die der folgenden Ausgabe ähneln:

   ```
   admin@gs-pod192:~/>: mccli activity cancel --mcsuserid=MCUser --mcspasswd=Test12345 --id=9138660744236309
   0,22205,Backup cancelled via console
   AttributWert
   -------------------------
   activity-id9138660744236309
   ```

3 Wiederholen Sie Schritt c für alle Jobs mit dem Status „Wird ausgeführt“.

4 Unterbrechen Sie Backups und Wiederherstellungen. Auf der VDP-Appliance kann dies durch Deaktivierung der Proxys über die Befehlszeile geschehen. Überprüfen Sie zusammen mit Anwendern, ob keine wichtigen Backups oder Wiederherstellungen anstehen, die vor der Ausführung dieser Befehle durchgeführt werden müssen.

   a Öffnen Sie eine SSH- oder Putty-Sitzung für die VDP-Appliance.

   b Führen Sie den Befehl `service avagent-vmware stop` aus.

5 Unterbrechen Sie die Serverwartungsvorgänge auf der VDP-Appliance.

   a Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

   https://<*IP_Adresse_der_VDP_Appliance*>**:8543/vdp-configure**

   b Wenn für die Wartungsservices der Status **Wird ausgeführt** angezeigt wird, klicken Sie auf die Schaltfläche **Stoppen**.

6 Löschen Sie die vorhandenen Verzeichnisse STAGING, DELETED oder cur/DELETED für die VDP-Appliance manuell aus dem Data Domain-System.

7 Verwenden Sie Data Domain Enterprise Manager, um den Data Domain-Dateisystembereinigungsvorgang zu initiieren.

   Durch diesen Prozess sollte genügend Speicherplatz freigegeben werden, damit die Servicewartungsvorgänge der VDP-Appliance für einen erfolgreichen Abschluss aktiviert werden können.

8 Starten Sie die Serverwartungsvorgänge auf der VDP-Appliance neu.

   a Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

   https://*<IP_Adresse_der_VDP_Appliance>***:8543/vdp-configure**

   b Wenn für die Wartungsservices der Status **Gestoppt** angezeigt wird, klicken Sie auf die Schaltfläche **Starten**.

9 Starten Sie die Proxys auf der VDP-Appliance neu, sodass Backups und Wiederherstellungen ausgeführt werden können.

   a Öffnen Sie eine SSH- oder Putty-Sitzung für die VDP-Appliance.

   b Führen Sie den Befehl `service avagent-vmware start` aus.

Häufige Probleme und Lösungen

In diesem Abschnitt sind häufige Probleme bei der Speicherung von VDP-Appliance-Backups auf einem Data Domain-System sowie deren Lösungen aufgeführt.

Backup schlägt fehl, wenn das Data Domain-System offline ist

Falls das Data Domain-System während der Initiierung eines Backups offline ist, kann es bis zu fünf Minuten oder länger dauern, bis das Backup fehlschlägt. Dieser Fehler tritt auf, weil nahezu alle DD Boost-Vorgänge über einen minimalen Timeout-Zeitraum von fünf Minuten verfügen.

Um eine Lösung für das fehlgeschlagene Backup zu finden, stellen Sie das Data Domain-System auf online und unternehmen Sie einen erneuten Backupversuch.

Rollback nach Löschung eines Data Domain-System

Wenn Sie nach Durchführung des unter „Löschen des Data Domain-Systems aus der VDP-Appliance" auf Seite 94 beschriebenen Verfahrens ein Rollback auf einen Kontrollpunkt durchführen, sollte durch das Rollback ein Status erreicht werden, bei dem das Data Domain-System aus der VDP-Appliance entfernt wird.

Damit das Data Domain-System wieder der VDP-Appliance hinzugefügt wird, verwenden Sie die VDP-Konfigurationsbenutzeroberfläche. Weitere Informationen finden Sie unter „Hinzufügen eines Data Domain-Systems" auf Seite 92.

Wenn Sie ein Rollback auf einen Kontrollpunkt durchführen, der vor der Löschung des Data Domain-Systems liegt, sollte das Data Domain-System nach wie vor angebunden und ordnungsgemäß konfiguriert sein. Um das Data Domain-System zu entfernen, befolgen Sie das unter „Löschen des Data Domain-Systems aus der VDP-Appliance" auf Seite 94 beschriebene Verfahren.

Wenn nach einem Rollback ein anderer Status vorliegt, setzen Sie sich am besten mit dem Support in Verbindung, um eine geeignete Lösung zu finden.

VDP-Festplattenerweiterung 10

Dieses Kapitel umfasst folgende Themen:

Voraussetzungen

Vergewissern Sie sich, dass Ihre Konfiguration die folgenden Anforderungen vor der Festplattenerweiterung erfüllt. Werden diese Schritte nicht abgeschlossen, kann dies zu einer VDP-Beschädigung führen und die Wiederherstellung von einem Clone oder VDP-Backup erforderlich machen.

- Vergewissern Sie sich, dass die an die CPU und den Speicher gestellten Mindestanforderungen für die neue Konfiguration erfüllt werden:
  - Die Mindestanzahl virtueller CPUs beträgt 4 für VDP-Kapazitätsoptionen von 2 TB, 4 TB, 6 TB und 8 TB.
  - Die Mindestspeichermenge pro VM hängt von der Kapazität ab:

Kapazitätsgröße	Erforderlicher Speicher
2 TB	6 GB
4 TB	8 GB
6 TB	10 GB
8 TB	12 GB

- Vergewissern Sie sich, dass sowohl CPU als auch Speicher-Hot-Add aktiviert sind. Die CPU- und Speicher-Hot-Add-Optionen sind im Falle einer einem Upgrade unterzogenen Appliance standardmäßig deaktiviert.

HINWEIS

- Wenn Sie über eine Essentials Plus-Lizenz verfügen, können Sie den erforderlichen Speicher nicht während des Betriebs hinzufügen („Hot-Plug“). Daher müssen Sie den Speicher, der VDP zugewiesen ist, manuell erhöhen. Zusätzliche Details finden Sie unter „Festplattenerweiterung mit Essentials Plus“ auf Seite 112.
- Vergewissern Sie sich, dass Ihnen für die Erweiterung Festplattenspeicher zur Verfügung steht. Sie können Ihren Festplattenspeicher über die Registerkarte **Speicher** prüfen. „Anzeigen der Speicherkonfiguration“ auf Seite 83 Siehe .
- Führen Sie die Festplattenerweiterung während des Backupzeitfensters durch, wenn keine Backupjobs oder anderen VDP-Aufgaben wie Wiederherstellungen oder Integritätsprüfungen ausgeführt werden. Vergewissern Sie sich vor einer Festplattenerweiterung, dass alle VDP-Services ausgeführt werden. Zusätzliche Details finden Sie unter „Starten und Stoppen von Services“ auf Seite 39.
- Vergewissern Sie sich, dass Sie in vCenter über Administratorrechte verfügen. Mithilfe der Informationen unter „Konfiguration des Benutzerkontos“ auf Seite 25 lässt sich feststellen, ob Sie über Administratorrechte für vCenter verfügen.
- Vergewissern Sie sich, dass die VMFS-Heap-Größe auf den richtigen Wert für die Menge des virtuellen mit dem vSphere-Host verbundenen Festplattenspeichers eingestellt ist. Zusätzliche Details finden Sie unter „Empfehlungen zur VMFS-Heap-Größe“ auf Seite 109.
- Notieren Sie sich vor dem Cloningvorgang die MAC-Adresse für die Appliance. Die MAC-Adresse wird später bei einem Speicherausfall verwendet.
- Erstellen Sie einen Clone oder ein Backup der VDP-Appliance und überprüfen Sie vor der Festplattenerweiterung die Gültigkeit des Clone bzw. Backups.

Empfehlungen zur VMFS-Heap-Größe

Die VMFS-Heap-Größe bestimmt die Menge des virtuellen Festplattenspeichers, der von den einzelnen vSphere-Hosts unterstützt wird. Wenn die Menge des virtuellen Festplattenspeichers die entsprechende Konfiguration für die VMFS-Heap-Größe übersteigt, kann Folgendes eintreten:

- Die virtuellen Maschinen verhalten sich unvorhersehbar.
- Es werden Fehlermeldungen angezeigt, wonach eine Zuweisung des Speichers nicht möglich ist.
- Die virtuellen Maschinen stürzen u. U. ab oder können nicht gestartet werden.

Vergewissern Sie sich vor der Festplattenerweiterung, dass die VMFS-Heap-Größe ordnungsgemäß für die neue virtuelle Laufwerkskapazität konfiguriert ist. Durch die Erhöhung der VMFS-Heap-Größe wird die Menge des dem vSphere-Host-Kernel zugewiesenen Speichers erhöht, und es ist ein Neustart des Systems erforderlich, damit die Änderungen wirksam werden.

VMFS3 und VMFS5 verwenden die gleichen Einstellungen und sind in Tabelle 10-15 definiert.

Tabelle 10-15. Einstellungen für die VMFS-Heap-Größe

Version/Build	Standardmäßige Heap-Menge	Standardmäßig zulässiger offener VMDK-Speicher pro Host	Minimale Heap-Menge	Maximale Heap-Menge	Maximaler Heap-Wert	Maximaler offener VMDK-Speicher pro Host
vSphere Host 5.0 Update 2 (914586) und niedriger	80 MB	8 TB	-	256 MB	255	25 TB
vSphere Host 5.0 Patch 5 (1024429) und höher	256 MB	60 TB	256 MB	640 MB	255	60 TB
vSphere Host 5.1 Patch 1 (914609) und niedriger	80 MB	8 TB	-	256 MB	255	25 TB
vSphere Host 5.1 Update 1 (1065491) und höher	256 MB	60 TB	256 MB	640 MB	255	60 TB

HINWEIS vSphere Host-Versionen ab 5.5 umfassen einen deutlich verbesserten Heap-Entfernungsprozess, sodass die größere, Speicher belegende Heap-Größe nicht erforderlich ist. vSphere 5.5 und höher unterstützt eine maximale Heap-Größe von 256 MB und ermöglicht Hosts den Zugriff auf den gesamten Adressbereich eines 64-TB-VMFS.

Im VMware-Knowledgebase-Artikel 1004424 werden die Schritte zum Ändern der VMFS-Heap-Größeneinstellungen beschrieben.

Durchführen einer Festplattenerweiterung

VDP ermöglicht die Erweiterung der Datenspeicherkapazität durch Verwendung des Assistenten **Speicher erweitern**. Die Festplattenerweiterung ermöglicht die Erweiterung des VDP-Speichers auf 1 TB, 2 TB, 4 TB, 6 TB oder 8 TB.

HINWEIS Sie können den Bereitstellungstyp nicht von Thin Provisioning in Thick Provisioning ändern. Die Festplatten erben den Bereitstellungstyp, der ihnen während der ersten Konfiguration zugewiesen wurde.

Beim Erweitern einer Thick-Eager-Zeroed-VMDK ist nur der erweiterte Teil vom Typ „Thick Lazy-Zeroed“.

VMware Knowledge Base Artikel 1035823 beschreibt die Schritte zur Erhöhung der VMDK Größe und Erstellung einer thick eager-zeroed VMDK.

Voraussetzung

Während der ersten Konfiguration werden die VDP-Speicherfestplatten validiert.

Verfahren

1 Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

https://<*IP_Adresse*_der_**VDP_Appliance**>:8543/vdp-configure/

2 Klicken Sie auf die Registerkarte **Speicher**.

Neben der Menge des insgesamt nutzbaren Speichers und der für jeden Datenspeicher verfügbaren Speicherkapazität werden im Bereich **Speicherzusammenfassung** die verfügbaren Datenspeicher angezeigt.

HINWEIS Klicken Sie zum Aktualisieren der Daten auf der Seite auf das Symbol zum Aktualisieren neben **Speicherzusammenfassung**.

3 Wählen Sie aus der Liste **Aktion** die Option **Speicher erweitern** aus.

Der Assistent Speicher erweitern wird angezeigt und zeigt die aktuelle Kapazität an.

4 Bestimmen Sie, ob Sie die Größe der Festplatten erweitern oder die Anzahl der Festplatten erhöhen.

HINWEIS Während der Erweiterung auf bis zu 2 TB bleibt die Anzahl der Festplatten bei 3, aber die Größe der vorhandenen Festplatten nimmt zu. Beim Erweitern von Festplatten sind die Steuerelemente zur Auswahl der Festplattenanzahl auf jedem Datenspeicher deaktiviert.

a Zum Vergrößern der Festplatten wählen Sie eine neue Kapazität aus der Liste aus. Sie können einen VDP-Speicher auf 1 TB, 2 TB, 4 TB, 6 TB oder 8 TB erweitern.

b Um Festplatten hinzuzufügen, erhöhen Sie die Anzahl an Festplatten in der Spalte Festplatten, bis die Gesamtanzahl der verfügbaren Speicherfestplatten zugewiesen ist. Sie können alle Festplatten einem einzigen Datenspeicher zuweisen oder die Festplatten auf mehrere Datenspeicher verteilen.

5 Klicken Sie auf **Weiter**.

Das Dialogfeld „Gerätezuweisung“ zeigt die Datenspeicher an, die zur Zuweisung zur Verfügung stehen, sowie die Anzahl der zuzuweisenden Festplatten.

Eine Warnmeldung wird angezeigt, wenn das System erkennt, dass eine Performanceanalyse fehlgeschlagen ist, nie ausgeführt wurde oder auf einem oder mehreren der ausgewählten Datenspeicher veraltet ist. Abhängig davon, ob Sie die Performanceanalyse auf dem ausgewählten Datenspeicher ausführen möchten oder nicht, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Ja**, um den Assistenten abzubrechen und die Performanceanalyse auf dem ausgewählten Datenspeicher auszuführen. Weitere Informationen zur Ausführung des Performanceanalysetools erhalten Sie unter „Performanceanalyse“ auf Seite 112.
- Klicken Sie auf **Nein**, um mit der Festplattenerweiterung fortzufahren.

6 Klicken Sie auf **Weiter**, um zur nächsten Seite des Assistenten „Speicher erweitern“ zu wechseln.

Im Dialogfeld „CPU und Speicher“ werden die Mindestanforderungen an CPU und Speicher zur aktuellen Konfiguration angezeigt.

7 Wählen Sie für jede virtuelle Maschine die Anzahl virtueller CPUs aus.

Maximal sind für eine VDP-VM 8 virtuelle CPUs zulässig.

8 Wählen Sie die Speichermenge aus, die der VDP-VM zugewiesen werden soll.

- Die Mindestspeichermenge pro VM hängt von der Kapazität ab:
  - Für 2 TB Kapazität sind 6 GB Speicher erforderlich.
  - Für 4 TB Kapazität sind 8 GB Speicher erforderlich.
  - Für 6 TB Kapazität sind 10 GB Speicher erforderlich.
  - Für 8 TB Kapazität sind 12 GB Speicher erforderlich.
- Die maximal zulässige Speichermenge für eine VDP-VM beträgt 64 GB.

9 Klicken Sie im Dialogfeld „Bereit zur Fertigstellung“ auf **Fertig stellen**, um die Änderungen zu übernehmen.

HINWEIS Im Anschluss an eine erfolgreiche Speicherkonfiguration erstellt das System automatisch einen Kontrollpunkt und führt eine Integritätsprüfung durch.

Anzeigen der Speicherkonfiguration

Nach Abschluss der Speichererweiterung können Sie auf der Registerkarte **Speicher** im Bereich **Speicherzusammenfassung** die Menge des insgesamt nutzbareren Speichers und die für jeden Datenspeicher verfügbare Speicherkapazität überprüfen.

Bekannte Einschränkung

Unmittelbar nach der Festplattenerweiterung wird ein Lastenausgleich durchgeführt; für die genutzte Kapazität werden dabei falsche Werte angezeigt. Die Werte werden jedoch korrekt angezeigt, nachdem die Ausführung des nächsten Wartungszeitfensters abgeschlossen wurde.

Verfahren

1 Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

https://<*IP_Adresse_der_VDP_Appliance*>**:8580/vdp-configure**

2 Klicken Sie auf die Registerkarte **Speicher**.

Im Bereich **Speicherzusammenfassung** wird der insgesamt nutzbare Speicher und die Speicherkapazität für jeden Datenspeicher angezeigt.

HINWEIS Klicken Sie zum Aktualisieren der Daten auf der Seite auf das Symbol zum Aktualisieren neben **Speicherzusammenfassung**.

Performanceanalyse

Beim Performanceanalysetest werden die Schreib-, Lese- und Seek-Performancetests durchgeführt. Während der Erstkonfiguration werden im Rahmen des Performanceanalysetests die Lese-, Schreib- und Seek-Funktionen der konfigurierten VDP-Festplatten bewertet. Nach der Erstellung messen die Tests die Performance der Datenspeicher, indem im jeweiligen Datenspeicher eine 256 GB große temporäre Festplatte erstellt wird.

Mögliche Testergebnisse sind:

- Unbekannt
- Fehlgeschlagen
- Erfolgreich

Ausführen des Performanceanalysetests

1 Melden Sie sich beim VDP-Konfigurationsdienstprogramm über die folgende URL an:

https://<*IP_Adresse_der_VDP_Appliance*>**:8543/vdp-configure**

2 Klicken Sie auf der Registerkarte **Speicher** auf **Performanceanalyse**.

Beim Performanceanalysetest wird eine temporäre Festplatte in den ausgewählten Datenspeichern erstellt. Die Tests werden dann auf dieser Festplatte ausgeführt. Die temporäre Festplatte wird nach Abschluss der Performanceanalyse automatisch entfernt.

3 Wählen Sie die Datenspeicher aus, auf denen der Performanceanalysetest ausgeführt wird.

4 Klicken Sie auf **Ausführen**, um die Performanceanalyse zu starten.

HINWEIS Sie können jederzeit auf **Abbrechen** klicken, um laufende Performanceanalysetests zu stoppen.

Festplattenerweiterung mit Essentials Plus

Wenn Sie über eine Essentials Plus-Lizenz verfügen, können Sie die Speicher-Hot-Add-Option nicht aktivieren. Daher müssen Sie den Speicher, der VDP zugewiesen ist, manuell an die Anforderungen der Zielkapazität anpassen.

HINWEIS Diese Einschränkung gilt für vSphere 5.x-Hosts. Sie müssen den erforderlichen Mindestspeicher für einen vSphere-Host unter Verwendung der in Tabelle 10-16 aufgeführten Speicheranforderungen manuell festlegen.

VDP stellt die folgenden, auf der Kapazitätsgröße basierenden Speicheranforderungen.

Tabelle 10-16. Speicheranforderungen für virtuelle Hardware

Kapazitätsgröße	Erforderlicher Speicher
2 TB	6 GB
4 TB	8 GB
6 TB	10 GB
8 TB	12 GB

Verfahren

So führen Sie eine Festplattenerweiterung mit einer Essentials Plus-Lizenz durch:

1 Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

https://<*IP_Adresse_vCenter_Server*>**:9443/vsphere-client/**

2 Fahren Sie die VDP-Appliance vor der Erweiterung herunter, indem Sie die Aktion **Gastbetriebssystem herunterfahren** auf der virtuellen Maschine ausführen.

Bei dieser Aktion wird die VDP-Appliance automatisch ordnungsgemäß heruntergefahren. Wenn die Appliance ohne die Aktion **Gastbetriebssystem herunterfahren** ausgeschaltet wird, sind Beschädigungen möglich. Das Herunterfahren und der Neustart der VDP-Appliance können bis zu 30 Minuten dauern. Der Status kann über die VM-Konsole überwacht werden.

3 Erhöhen Sie den der VDP-Appliance zugewiesenen Speicher mithilfe der in Tabelle 10-16 aufgeführten Anforderungen.

   a Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

   https://<IP_Adresse_vCenter_Server>**:9443/vsphere-client/**

   b Melden Sie sich in vSphere Web Client als ein Benutzer an, der zum Bearbeiten von Hardwareeinstellungen berechtigt ist.

   c Klicken Sie auf **vCenter > Hosts und Cluster**.

   d Klicken Sie in der Struktur auf der linken Seite so lange auf die Erweiterungspfeile, bis die VDP-Appliance angezeigt wird.

   e Klicken Sie mit der rechten Maustaste auf die VDP-Appliance und wählen Sie **Einstellungen bearbeiten** aus.

   f Klicken Sie auf die Registerkarte **Virtuelle Hardware**.

   g Erhöhen Sie die Speichermenge, indem Sie einen entsprechenden Wert im Feld **Speicher** eingeben.

   h Klicken Sie auf **OK**.

4 Um die VDP-Appliance neu zu starten, klicken Sie mit der rechten Maustaste auf die VDP-Appliance. Wählen Sie dann **Einschalten** aus.

11 Verwenden von VDP

In diesem Kapitel werden folgende Themen behandelt:

Zugriff auf VDP

Verwenden Sie vSphere Web Client für den Zugriff auf und das Management von VDP.

HINWEIS VDP kann nicht ohne vCenter Server verwendet werden. Im verknüpften Modus kann die VDP-Appliance nur mit dem vCenter Server-Rechner verwendet werden, mit dem die Appliance verknüpft ist. Wenn die VDP-Appliance nicht in vSphere Web Client angezeigt wird, entfernen Sie vCenter aus dem verknüpften Modus.

Voraussetzungen

Vor der Verwendung von VDP müssen Sie die VDP-Appliance, wie unter „VDP-Installation und -Konfiguration" auf Seite 21 beschrieben, installieren und konfigurieren.

Verfahren

1 Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

https://<*IP_Adresse_vCenter_Server*>:9443/vsphere-client/

2 Geben Sie auf der Seite mit den Anmeldedaten einen Administratorbenutzernamen und ein Passwort für vCenter ein und klicken Sie auf **Anmelden**. Das angegebene Benutzerkonto muss über Administratorrechte verfügen.

3 Wählen Sie in vSphere Web Client **VDP** aus.

4 Wählen Sie auf der **VDP-Begrüßungsseite** die VDP-Appliance aus und klicken Sie auf **Verbinden**.

Zugreifen auf die VDP-Appliance über die CLI

Aktuell können Benutzer über die vSphere Client-Konsole, SSH- oder Putty-Sitzungen auf die Befehlszeile der VDP-Appliance zugreifen. Ab VDP 5.8 und höher ist die Funktion zur Verwendung von SSH oder Putty zum Anmelden bei der VDP-Appliance mit dem Root-Benutzer nicht mehr verfügbar.

Um über SSH oder Putty auf die Appliance zuzugreifen, müssen Sie sich als Admin-Benutzer anmelden.

Ab VDP 5.8 und höher wurde außerdem das Standardpasswort für den Admin-Benutzer geändert. Dieses Passwort gilt nur, wenn sich der Benutzer vor Abschluss der Appliance-Konfiguration über die Benutzeroberfläche für die VDP-Konfiguration bei der VDP-Appliance anmeldet. In diesem Szenario lautet das Admin-Passwort: `88RttoTriz!!`

Nach Abschluss der Appliance-Konfiguration kann das neu konfigurierte Appliance-Passwort verwendet werden, um als Admin-Benutzer auf die Befehlszeile zuzugreifen.

Nützliche Befehle

Die folgende Tabelle listet einige der nützlichsten Befehle:

Tabelle 11-17. Nützliche VDP-Befehle

Befehl	Beschreibung
status.dpn	Anzeige des VDP Status.
dpnctl status	Anzeige des VDP-Service Status.
emwebapp.sh - - test	Prüfung des Status der VDP-Enterprise Manager Webapplikation.
capacity.sh	Analyse des Platzverbrauchs der letzten 30 Backupjobs und Anzeige der Größe der neuen Daten sowie des durch Garbage Collection entstandenen Platzes.
cplist	Anzeige des Checkpoint Status.
Mccli server show-prop	Anzeige der VDP-Appliance Eigenschaften, die mit denen im vSphere Webclient übereinstimmen.
mccli activity show	Anzeige der Backupjob Informationen. Jede Aktivität ist ein Backupjob aus einer einzigen virtuellen Maschine.

Tabelle 11-17. Nützliche VDP-Befehle

Befehl	Beschreibung
Mccli dd show-prop	Anzeige der Datendomain-Systemeigenschaften.
Mccli client show --domain=/vCenter FQDN oder IP/VirtualMachines --recursive=true	Auflistung der geschützten virtuellen Maschinen.
Mccli backup anzeigen --name=/vCenter FQDN oder IP/VirtualMachines/Name der virtuellen Maschine --recursive=true	Auflistung der Backups einer virtuellen Maschine.
mccli -help	Auflistung der verfügbaren Befehloptionen.

Wissenswertes über die VDP-Benutzeroberfläche

vSphere Web Client für vSphere Data Protection wird für das Konfigurieren und Managen von VDP verwendet.

Abbildung 11-7. vSphere Data Protection-Benutzeroberfläche

Die Benutzeroberfläche von vSphere Data Protection besteht aus sechs Registerkarten:

- **Erste Schritte**: Bietet einen Überblick über die VDP-Funktionen und Quicklinks zu den Themen „Herunterladen des Anwendungsbackupclients“, „Erstellen von Backupjobs“, „Überprüfen eines Backups“, „Wiederherstellen eines Backups“ und „Anzeigen eines Überblicks“.
- **Backup**: Enthält eine Liste der geplanten Backupjobs sowie Details zu jedem Backupjob. Sie können von dieser Seite aus auch Backupjobs erstellen und bearbeiten. Darüber hinaus bietet diese Seite die Möglichkeit, einen Backupjob unmittelbar auszuführen. Unter „Anzeigen von Informationen über die Registerkarte „Berichte““ auf Seite 118 finden Sie weitere Informationen.
- **Wiederherstellen**: Enthält eine Liste erfolgreicher Backups, die wiederhergestellt werden können. Unter „Wiederherstellungsvorgänge“ auf Seite 144 finden Sie weitere Informationen.
- **Replikation**: Enthält eine Liste erfolgreicher Backups, die repliziert werden können. Unter „Replikationsjobs“ auf Seite 152 finden Sie weitere Informationen.

- **Berichte**: Enthält Backupstatusberichte zu den virtuellen Maschinen auf dem vCenter Server-Rechner. Unter „Anzeigen von Informationen über die Registerkarte „Berichte““ auf Seite 118 finden Sie weitere Informationen.
- **Konfiguration:** Zeigt Informationen zur Konfiguration von VDP an und ermöglicht die Bearbeitung einiger dieser Einstellungen. Unter „Konfigurieren von VDP“ auf Seite 57 finden Sie weitere Informationen.

Wechseln zwischen VDP-Appliances

Jede vCenter Server-Installation unterstützt bis zu 20 VDP-Appliances. Sie können zwischen Appliances wechseln, indem Sie aus der Drop-down-Liste rechts neben der Option **Appliance wechseln** eine Appliance wählen.

HINWEIS Die VDP-Appliances in der Drop-down-Liste sind alphabetisch sortiert und das erste Element in der auf dem Bildschirm angezeigten Liste stimmt möglicherweise nicht mit der aktuellen Appliance überein. Bei dem auf dem VDP-Bildschirm links angezeigten Appliance-Namen handelt es sich um die aktuelle Appliance, und der Appliance-Name in der Dropdown-Liste ist der erste in der Liste der verfügbaren Appliances.

VDP-Benutzeroberfläche

Die VDP-Benutzeroberfläche umfasst die folgenden Funktionen:

- Backups auf Gastebene von Microsoft Exchange Server, SQL Server und SharePoint Server
- Vergrößern und Hinzufügen von Festplatten (Festplattenerweiterung)
- Backup auf einem Data Domain-System
- Granular Level Recovery (GLR)
- Verifizieren automatischer Backups

Diese Optionen werden unter „VDP-Anwendungsunterstützung“ auf Seite 176 beschrieben. Dort wird außerdem über die Durchführung von Backups und Wiederherstellungen auf Anwendungsebene informiert.

Anzeigen von Informationen über die Registerkarte „Berichte“

Auf der Registerkarte **Berichte** werden die folgenden Informationen angezeigt:

Appliance-Statusinformationen

- **Appliance-Status:** Der Status der VDP-Appliance
- **Status der Integritätsprüfung:** Klicken Sie auf den grünen Pfeil nach rechts, um die Integritätsprüfung zu initiieren. Der Statuswert lautet „Normal“ oder „Veraltet“.
  - „Normal“ gibt an, dass eine Integritätsprüfung in den letzten beiden Tagen erfolgreich abgeschlossen wurde.
  - „Veraltet“ gibt an, dass in den letzten beiden Tagen keine Integritätsprüfung stattgefunden hat bzw. erfolgreich abgeschlossen wurde.
- **Genutzte Kapazität:** Ein Prozentsatz der durch Backups belegten VDP-Gesamtkapazität
- **Genutzte DDR-Kapazität:** Ein Prozentsatz der vom Data Domain-System belegten Gesamtkapazität (falls zutreffend)
- **Aktuelle fehlgeschlagenes Backups:** Die Anzahl der virtuellen Maschinen, die im letzten abgeschlossenen Backupjob nicht gesichert wurden
- **Aktuelle fehlgeschlagene Backupverifizierungen**: Die Anzahl der Backupverifizierungsjobs, die zuletzt fehlgeschlagen sind

- **Aktuelle fehlgeschlagene Replikationen:** Die Anzahl der Replikationsjobs, die zuletzt fehlgeschlagen sind
- **Geschützte VMs insgesamt:** Die Gesamtanzahl der von der VDP-Appliance geschützten virtuellen Maschinen

HINWEIS Die VDP-Appliance unterstützt 400 virtuelle Maschinen. Wenn die maximale Anzahl zulässiger virtueller Maschinen überschritten wird, wird ein Alarm erzeugt und auf der Registerkarte **Protokoll** wird eine entsprechende Fehlermeldung angezeigt.

Aktualisieren

Sie können jederzeit auf die Schaltfläche **Aktualisieren** klicken, um die Daten auf der Registerkarte **Berichte** zu aktualisieren.

Registerkarte „Aufgabenfehler“

Auf der Registerkarte **Aufgabenfehler** werden Details zu den Jobs angezeigt, die in den letzten 72 Stunden fehlgeschlagen sind.

Fehlerzeit: Das Datum und die Uhrzeit des fehlgeschlagen Jobs

Ursache: Der Grund für den Jobfehler.

Client-/Quellname: Der mit vCenter verbundene Client

Jobname: Der Name des fehlgeschlagenen Jobs

Jobtyp: Der Typ des fehlgeschlagenen Jobs, z. B. „Geplantes Backup“ oder „Backup nach Bedarf“

Nächste Ausführungszeit: Das Datum und die Uhrzeit der nächsten geplanten Jobausführung

Protokoll anzeigen: Klicken Sie, um das Dialogfeld „Clientprotokoll zu Jobfehlern“ aufzurufen. Dort können Details zum Clientprotokoll angezeigt werden. Wenn keine Protokolldateien im Dialogfeld „Clientprotokoll“ verfügbar sind, wird ggf. eine von drei Fehlermeldungen angezeigt:

- Protokolldatei konnte nicht abgerufen werden. Dies kann in folgenden Fällen geschehen:
  - Managementservices wurden vor Kurzem gestartet.
  - Bei der regelmäßigen Protokollpflege wurden alte Protokolldateien entfernt.
  - Protokolle sind leer oder nicht vorhanden.
  - Es ist ein Fehler aufgetreten.
- Protokoll konnte nicht abgerufen werden. Protokolle werden regelmäßig 72 Stunden nach Fertigstellung des Jobs entfernt.
- Die abgerufene Protokolldatei ist leer.

HINWEIS Über die Registerkarte **Jobfehler** sind nicht alle Protokolle zu Replikationsquellen und -zielen verfügbar. Es ist jedoch möglich, die Replikationsprotokolle über das VDP-Konfigurationsdienstprogramm mithilfe des normalen Protokollbündels abzurufen. Weitere Informationen finden Sie unter „Sammeln von VDP-Protokollen oder Diagnoseinformationen“ auf Seite 40.

Symbol „Aktionen“ 

Sie können die folgenden Aufgaben über die Liste des Symbols „Aktionen“ rechts auf der Registerkarte **Aufgabenfehler** durchführen:

- **Aufgabe erneut ausführen**: Markieren Sie den fehlgeschlagenen Job und klicken Sie, um den fehlgeschlagenen Job erneut auszuführen. Die Funktion „Job erneut ausführen“ ist für Wiederherstellungsfehler nicht aktiviert.

HINWEIS Um ein Backup nur für den fehlgeschlagenen Client auszuführen, wählen Sie **Nur veraltete Quellen sichern** unter **Jetzt sichern** auf der Registerkarte **Backup** aus.

- **In CSV-Datei exportieren**: Klicken Sie, um die aktuelle Tabelle in eine kommagetrennte Datei (.CSV) zu exportieren.
- **Alle Spalten anzeigen**: Blenden Sie eine oder mehrere Spalten aus, indem Sie im Spaltennamen auf **X** klicken und klicken Sie dann auf **Alle Spalten anzeigen**, um die ausgeblendeten Spalten in der Benutzeroberfläche einzublenden.

Filter

Sie können die Details zu Jobfehlern durch Auswahl eines der folgenden Kriterien filtern oder anpassen. Es werden Informationen zu während der letzten 72 Stunden aufgetretenen Jobfehlern angezeigt.

- **Alle anzeigen:** Hierüber werden alle Jobfehlerinformationen für die virtuellen Maschinen angezeigt. **Alle anzeigen** ist die Standardeinstellung.
- **Error:** Hierüber werden die Jobfehlerinformationen nach Fehlermeldungen gefiltert.
- **Job:** Hierüber werden Jobfehlerinformationen für einen ausgewählten Job gefiltert.
- **Client:** Hierüber werden Jobfehlerinformationen für einen bestimmten Client gefiltert.

Registerkarte „Jobdetails“

Über die Registerkarte **Jobdetails** lässt sich zum einen der Jobtyp (Backups, Replikation oder Backupverifizierung) auswählen, zum anderen können Details zu einem ausgewählten Job angezeigt werden. „Backups“ ist der standardmäßige Jobtyp.

Jobdetails sind in drei Abschnitte gruppiert:

- **Clientinformationen**
  - **Client Name**: Der mit vCenter verbundene Client Normale VM-Clients und außer Betrieb genommene VM-Clients aus der Domain „Replizieren“ zeigen den Hash-Maskenwert an, angehängt an die replizierten, wiederhergestellten und importierten Namen.
  - **Geben Sie Folgendes ein**: Zeigt den Typ als Image, MS SQL Server, MS SharePoint Server oder MS Exchange Server an. Anwendungen (MS SQL Server, MS SharePoint Server oder MS Exchange Server) werden nur auf der VDP-Appliance unterstützt.
  - **Jobs**: Der Name des Jobs. Es werden mehrere Jobnamen angezeigt, wenn sich eine virtuelle Maschine in zwei unterschiedlichen Jobs befindet.
- **Letzte Ausführung**
  - **Jobname**: Der Name des Jobs
  - **Abschluss**: Das Datum und die Uhrzeit, zu denen der Job abgeschlossen wurde
  - **Ergebnis**: Ob der Job erfolgreich war, fehlgeschlagen ist, mit Ausnahmen erfolgreich war oder abgebrochen wurde.

    Wenn der Job erfolgreich mit Ausnahmen abgeschlossen wurde, klicken Sie auf den Link **Protokoll anzeigen**, um die Protokolle auf Informationen zu den Ausnahmen zu überprüfen.
- **Nächste Ausführung**
  - **Jobname**: Der Name des nächsten geplanten Job wird angezeigt. Wenn eine virtuelle Maschine in 2 verschiedenen Jobs mit unterschiedlichen Planungen vorhanden ist, wird der Name des nächsten geplanten Jobs angezeigt.
  - **Geplant**: Das Datum und die Uhrzeit der nächsten geplanten Jobausführung

Symbol „Aktionen“ 

Sie können die folgenden Aufgaben über die Liste des Symbols „Aktionen“ rechts auf der Registerkarte **Jobdetails** durchführen:

- **In CSV-Datei exportieren**: Klicken Sie, um die aktuelle Tabelle in eine kommagetrennte Datei (.CSV) zu exportieren.
- **Alle Spalten anzeigen**: Blenden Sie eine oder mehrere Spalten aus, indem Sie im Spaltennamen auf **X** klicken und klicken Sie dann auf **Alle Spalten anzeigen**, um die ausgeblendeten Spalten in der Benutzeroberfläche einzublenden.

Filter

Sie können die Jobdetails durch Auswahl eines der folgenden Kriterien filtern oder anpassen. Es werden Informationen zu während der letzten 72 Stunden aufgetretenen Jobfehlern angezeigt.

- **Alle anzeigen:** Hierüber werden alle Jobdetails für die virtuellen Maschinen angezeigt. **Alle anzeigen** ist die Standardeinstellung.
- **Client:** Hierüber werden Jobfehlerinformationen nach Client gefiltert.
- **Letzte Ausführung:** Hierüber werden die Jobdetails für den letzten ausgeführten Job gefiltert.
- **Nächste Ausführung:** Hierüber werden die Jobdetails für den nächsten geplanten Job gefiltert.

Registerkarte „Ungeschützte Clients“

- **Client Name**: Der Name des ungeschützten Clients
- **IP-Adresse:** Die IP-Adresse oder der Hostname des ungeschützten Clients
- **VM-Pfad:** Der Pfad, unter dem sich die virtuelle Maschine befindet

Symbol „Aktionen“ 

Sie können die folgende Aufgabe über die Liste des Symbols „Aktionen“ rechts auf der Registerkarte **Ungeschützte Clients** durchführen:

- **In CSV-Datei exportieren**: Klicken Sie, um die aktuelle Tabelle in eine kommagetrennte Datei (.CSV) zu exportieren.

Managen von Backups

12

In diesem Kapitel werden folgende Themen behandelt:

Backupjobs

Backupjobs umfassen mindestens eine virtuelle Maschine, die mit einer Backupplanung und bestimmten Aufbewahrungs-Policies verknüpft ist. Backupjobs werden mithilfe des Assistenten „Neuen Backupjob erstellen“ auf der Registerkarte **Backup** erstellt und bearbeitet.

Einschränkungen

- VDP führt kein Backup für die folgenden speziellen virtuellen Maschinen durch:
  - VDP-Appliances
  - vSphere Storage Appliances (VSA)
  - VMware Data Recovery(VDR)-Appliances
  - Vorlagen
  - sekundäre fehlertolerante Nodes
  - Proxys
  - Avamar Virtual Edition(AVE)-Server

  Mit dem Assistenten können Sie diese VMs auswählen. Wenn Sie den Assistenten durch Klicken auf **Fertig stellen** beenden, werden Sie über eine Warnung darüber informiert, dass diese speziellen virtuellen Maschinen dem Job nicht hinzugefügt wurden.
- Virtuelle Maschinen, deren Namen Sonderzeichen aufweisen, können Backupjobs nicht hinzugefügt werden. Die folgenden Zeichen sind nicht zulässig: ~!@$^%(){}[]|,`;#\/:*?<>'"&. Zudem dürfen keine diakritischen Zeichen verwendet werden (z. B. â, é, ì, ü und ñ).
- Die Verwendung von Snapshots zum Backup auf mit Bus-Sharing konfigurierten virtuellen Maschinen wird nicht unterstützt. Wenn SCSI-Bus-Sharing erforderlich, finden Sie weitere Informationen in folgendem Knowledgebase-Artikel: http://kb.vmware.com/kb/1006392.

Voraussetzungen

- VDP ist auf Ihrem vCenter Server-Rechner installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Auswählen der virtuellen Maschinen

Sie können Sammlungen virtueller Maschinen angeben, etwa alle virtuellen Maschinen eines Rechenzentrums, oder einzelne virtuelle Maschinen auswählen. Bei Auswahl eines kompletten Ressourcenpools, Hosts, Rechenzentrums oder Ordners sind alle neu hinzugefügten virtuellen Maschinen in diesem Container Teil nachfolgender Backups. Bei Auswahl einer einzigen virtuellen Maschine wird jede der virtuellen Maschine anschließend hinzugefügte Festplatte in das Backup aufgenommen. Wenn eine virtuelle Maschine aus dem ausgewählten Container in einen anderen, ursprünglich nicht ausgewählten Container verschoben wird, ist die virtuelle Maschine nicht länger Teil des Backups.

Es ist möglich, eine zu sichernde virtuelle Maschine manuell auszuwählen, damit die virtuelle Maschine auf jeden Fall gesichert wird, also auch, wenn sie verschoben wird.

Identifizieren außer Betrieb genommener virtueller Maschinen

Die folgenden Bedingungen führen dazu, dass ein VM-Client außer Betrieb genommen wird und nicht mehr als Kandidat für Backups, Wiederherstellungen oder Replikationsjobs zur Verfügung steht:

- **Host**: aus dem Bestand entfernt (dies geschieht ebenfalls, wenn ein übergeordneter Container eines Hosts entfernt wird, etwa ein Cluster, Hostordner, Rechenzentrum oder Rechenzentrumsordner)
- **Virtuelle Maschine**: Von Festplatte gelöscht
- **Virtuelle Maschine**: Aus dem Bestand entfernt

Die folgenden Bedingungen treten ein, wenn der VM-Client nicht außer Betrieb genommen ist und die untergeordnete virtuelle Maschine im Bestand verbleibt:

- **Ressourcenpool**: Aus dem Bestand entfernt
- **vApp**: Aus dem Bestand entfernt
- **Host**: Getrennt
- **Host**: Tritt in den Wartungsmodus ein
- **Host**: Wird heruntergefahren

Festlegen der Backupplanung

Auf der Seite „Planung“ des Assistenten Neuen Backupjob erstellen (Schritt 7 des unten beschriebenen Verfahrens) können Sie die Zeitintervalle festlegen, in denen die virtuellen Maschinen in Ihrem Backupjob gesichert werden. Die Backups werden so nah wie möglich am Startzeitpunkt des Backupzeitfensters ausgeführt. Die folgenden Zeitintervalle sind verfügbar: täglich, wöchentlich oder monatlich.

Festlegen der Aufbewahrungs-Policy

Aufbewahrungs-Policies für die VDP-Appliance werden einzeln pro Backupjob festgelegt. Jeder Wiederherstellungspunkt wird von einem Backupjob erstellt und wendet daher die Aufbewahrungs-Policy zum Zeitpunkt der Erstellung an. Wenn die Aufbewahrungs-Policy eines Backupjobs geändert wird, wirkt sich die neue Policy nur auf die neu erstellten Wiederherstellungspunkte aus. Zuvor erstellte Wiederherstellungspunkte behalten die vorherige Aufbewahrungs-Policy bei.

Geben Sie auf der Seite „Aufbewahrungs-Policy“ des Assistenten „Backupjob erstellen“ (Schritt 8) die Aufbewahrungsfrist für Backups an.

Die ersten drei Optionen – **Immer**, **Für** und Bis – werden auf alle Backups aller virtuellen Maschinen in der Gruppe gleichermaßen angewendet. Die vierte Option – **diese Planung** oder **benutzerdefinierter Aufbewahrungsplan** – gilt nur für Backups, denen intern spezielle Täglich-, Wöchentlich-, Monatlich- oder Jährlich-Tags zugewiesen wurden.

HINWEIS Der Standardwert zu **dieser Planung** ist 60 Tage. Der Standardwert zu **benutzerdefinierter Aufbewahrung** ist „Nie“.

Das erste Backup eines bestimmten Tages erhält ein Täglich-Tag. Wenn dieses Backup außerdem das erste Backup der Woche, des Monats und des Jahres ist, erhält das Backup auch die Wöchentlich-, Monatlich- und Jährlich-Tags. Die durch die Optionen **dieser Planung** bzw. benutzerdefinierter Aufbewahrungsplanung vorgegebenen Zeitintervalle gelten nur für Backups mit den internen Tags. Tabelle 12-18 beschreibt Optionen der Aufbewahrungs-Policy.

Tabelle 12-18. Optionen der Aufbewahrungs-Policy

Option	Beschreibung
Immer	Hierüber wird festgelegt, dass ein Backupjob niemals abläuft. Alle Backups für die virtuellen Maschinen in diesem Backupjob werden niemals gelöscht.
für	Hierüber wird eine bestimmte Anzahl an Tagen, Wochen, Monaten oder Jahren für den Backupjob festgelegt. Alle Backups für die virtuellen Maschinen in diesem Backupjob werden so lange gespeichert, bis das festgelegte Zeitintervall von ihrem Erstellungsdatum abgelaufen ist. Wenn Sie beispielsweise eine Aufbewahrungs-Policy von 30 Tagen für einen Backupjob festlegen, liegt das Ablaufdatum jedes ausgeführten Jobs 30 Tage in der Zukunft.
bis	Hierüber wird ein bestimmtes Ablaufdatum festgelegt. Alle Backups für die virtuellen Maschinen in diesem Backupjob werden zu dem im Feld **bis** angegebenen Datum gelöscht.

Tabelle 12-18. Optionen der Aufbewahrungs-Policy (Fortsetzung)

Option	Beschreibung
Diese Planung oder **benutzerdefinierter Aufbewahrungsplan**	Hierüber werden die Zeitintervalle für die Aufbewahrung von Backups festgelegt, denen interne Täglich-, Wöchentlich-, Monatlich- oder Jährlich-Tags zugewiesen wurden. Backups können mehrere dieser internen Tags aufweisen. Das Tag mit dem längsten Zeitintervall hat Vorrang. Wenn Sie beispielsweise Backups mit einem Wöchentlich-Tag für eine Aufbewahrung von 8 Wochen und Backups mit einem Monatlich-Tag für eine Aufbewahrung von 1 Monat festlegen, werden Backups mit zugewiesenen Wöchentlich- und Monatlich-Tags 8 Wochen lang aufbewahrt.

Erstellen von Backupjobs für vollständige Images

Voraussetzungen

- VDP ist auf Ihrem vCenter Server-Rechner installiert und konfiguriert.
- Die Festplatten werden von VDP unterstützt. Die folgenden virtuellen Hardware-Festplattentypen werden nicht von VDP unterstützt:
  - Independent
  - RDM Independent – Virtual Compatibility Mode
  - RDM Physical Compatibility Mode

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu.

2 Klicken Sie auf die Registerkarte **Backup**.

Auf der Registerkarte **Backup** wird eine Liste der erstellten Backupjobs angezeigt. Die Spalten in der Liste werden in der nachstehenden Tabelle beschrieben:

Tabelle 12-19. Spaltenbeschreibungen für die Registerkarte **Backup**

Spalte	Beschreibung
Name	Der Name des Backupjobs.
Status	Gibt an, ob der Backupjob aktiviert oder deaktiviert ist. Deaktivierte Backupjobs werden nicht ausgeführt.
Typ	Der Backuptyp, z. B. Anwendung oder Image.
Letzte Startzeit	Der letzte Zeitpunkt, zu dem der Backupjob gestartet wurde.
Dauer	Die Dauer bis zum Jobabschluss bei der letzten Ausführung.
Nächste Ausführungszeit	Der Zeitpunkt, zu dem der Backupjob für eine weitere Ausführung geplant ist.
Erfolgsanzahl	Die Anzahl virtueller Maschinen, die bei der letzten Ausführung des Backupjobs erfolgreich gesichert wurden. Diese Anzahl wird nach jedem Backupjob aktualisiert.
Fehleranzahl	Die Anzahl virtueller Maschinen, die bei der letzten Ausführung des Backupjobs nicht erfolgreich gesichert wurden. Diese Anzahl wird nach jedem Backupjob aktualisiert.

3 Wählen Sie im Menü **Backupjobaktionen** die Option **Neu** aus, um den Assistenten Neuen Backupjob erstellen auszuführen.

Sie können den Assistenten „Neuen Backupjob erstellen“ auch über die Registerkarte **Erste Schritte** ausführen. Klicken Sie hierzu unter „Standardaufgaben“ auf **Backupjob erstellen**.

4 Wählen Sie auf der Seite **Jobtyp** die Option **Gast-Images** aus und klicken Sie auf **Weiter**.

Die Option **Anwendungen** ermöglicht Ihnen das Erstellen von Backupjobs auf Microsoft Exchange Server-, Microsoft SQL Server- und Microsoft SharePoint Server-Rechnern. Einzelheiten finden Sie unter „VDP-Anwendungsunterstützung" auf Seite 175.

5 Klicken Sie auf der Seite **Datentyp** auf **Weiter**.

HINWEIS Durch die Auswahl der **Fallback to non-quiescence failure** Option können Backups als non-quiescence durchgeführt werden, im Falle einer quiescence Failure. Außerdem werden so die Wiederherstellungspunkte als crash-konsistent markiert.

6 Klicken Sie auf der Seite **Backupquellen** auf die Erweiterungspfeile, um die virtuellen Maschinen nach und nach anzuzeigen. Wählen Sie die Kontrollkästchen neben den Elementen aus, die dem Backupjob hinzugefügt werden sollen, und klicken Sie dann auf **Weiter**.

HINWEIS Wenn ein Data Domain-System als Backupziel konfiguriert ist, ist ein zusätzlicher Schritt zur Konfiguration des Ziels angezeigt. Wählen Sie entweder **lokalen Speicher** oder **Data Domain-Speicher** aus.

7 Wählen Sie auf der Seite **Planung** die Planung für den Backupjob aus und klicken Sie auf **Weiter**.

8 Wählen Sie auf der Seite **Aufbewahrungs-Policy** eine Aufbewahrungsfrist aus und klicken Sie auf **Weiter**. Die auswählbaren Aufbewahrungsfristen werden im Folgenden beschrieben.

- **Immer**: Alle Backups für die virtuellen Maschinen in diesem Backupjob laufen niemals ab.
- **Für**: Alle Backups für die virtuellen Maschinen in diesem Backupjob laufen ab, nachdem das festgelegte Zeitintervall von ihrem Erstellungsdatum verstrichen ist. Das Zeitintervall kann in Tagen, Wochen, Monaten oder Jahren angegeben werden.
- **Bis**: Alle Backups für die virtuellen Maschinen in diesem Backupjob laufen zu dem angegebenen Datum ab.
- **Diese Planung**: Hierüber werden die Zeitintervalle für die Aufbewahrung von Backups festgelegt, denen interne Tags zugewiesen wurden. Wenn Sie regelmäßig geplante tägliche Backups durchführen, wird einigen Backups automatisch einer der folgenden Aufbewahrungstypen zugewiesen:
  - **Täglich**: Das erste erfolgreich durchgeführte geplante Backup jedes Tags
  - **Wöchentlich**: Das erste erfolgreich durchgeführte geplante Backup jeder Woche
  - **Monatlich**: Das erste erfolgreich durchgeführte geplante Backup jedes Monats
  - **Jährlich**: Das erste erfolgreich durchgeführte geplante Backup jedes Jahrs

  Der Standardwert zu **dieser Planung** beträgt für Backupjobs nach Bedarf 60 Tage.

  Um Aufbewahrungstypen zuweisen zu können, beginnt jeder Tag um 00:00:01 GMT, jede Woche am Sonntag, jeder Monat am ersten Kalendertag des Monats und jedes Jahr am 1. Januar.

  Da Backups über mehr als eines dieser internen Tags verfügen können, hat das Tag mit dem längsten Zeitintervall Vorrang. Wenn Sie beispielsweise Backups mit einem Wöchentlich-Tag für eine Aufbewahrung von 8 Wochen und Backups mit einem Monatlich-Tag für eine Aufbewahrung von 1 Monat festlegen, werden Backups mit zugewiesenen Wöchentlich- und Monatlich-Tags 8 Wochen lang aufbewahrt.

ACHTUNG Nach dem Ablauf eines Backups entfernt die VDP-Appliance mit Beginn einer neuen Wartungsphase ihre Referenz zu den Backupdaten. Daher ist anschließend eine Wiederherstellung des abgelaufenen Backups nicht mehr möglich. Die VDP-Appliance bestimmt, ob die Backupdaten derzeit von einem anderen Wiederherstellungspunkt verwendet werden. Wenn das System feststellt, dass die Daten nicht verwendet werden, werden die Daten entfernt und es wird entsprechende Festplattenkapazität freigegeben.

9 Geben Sie auf der Seite **Name** einen Namen für den Backupjob ein und klicken Sie auf **Weiter**.

Der Name des Backupjobs muss eindeutig sein und darf bis zu 255 Zeichen umfassen. Die folgenden Zeichen sind für den Namen des Backupjobs nicht zulässig: ~!@$^%(){}[]|,`;#\/:*?<>'"&. Zudem dürfen keine diakritischen Zeichen verwendet werden (z. B. â, é, ì, ü und ñ).

10 Überprüfen Sie auf der Seite **Bereit zur Fertigstellung** die Zusammenfassung zum Backupjob und klicken Sie auf **Fertig stellen**.

In einem Informationsdialogfeld wird die erfolgreiche Erstellung des Backupjobs bestätigt. Der Backupvorgang kann einige Minuten dauern.

11 Klicken Sie auf **OK**.

Der neu erstellte Backupjob wird nun auf der Registerkarte **Backup** aufgeführt.

Erstellen eines Backupjobs auf einzelnen Festplatten

Bei einem Backupjob „Vollständiges Image“ werden alle Festplatten einer virtuellen Maschine in einem einzigen Image-Backup zusammengefasst. Backupjobs des Typs „Einzelne Festplatten“ ermöglichen es, nur die benötigten Festplatten auszuwählen. Mit dieser Funktion können Sie nach bestimmten Konfigurationskriterien filtern, etwa nach dem Betriebssystem oder nach der Archivierungs-Policy.

Nicht unterstützte Festplattentypen

Achten Sie bei der Planung von Backups einzelner Festplatten darauf, dass die Festplatten von VDP unterstützt werden. Momentan werden die folgenden virtuellen Hardware-Festplattentypen nicht von VDP unterstützt:

- Independent
- RDM Independent – Virtual Compatibility Mode
- RDM Physical Compatibility Mode
- Mit SCSI-Controller und aktiviertem Bus-Sharing verbundene virtuelle Laufwerke

HINWEIS Wenn eine virtuelle Maschine eine nicht unterstützte VMDK enthält, ist die VMDK abgeblendet und das zugehörige Kontrollkästchen ist nicht verfügbar.

Weitere Informationen zum Backup von nicht unterstützten Festplattentypen finden Sie unter „Backup und Wiederherstellung nur einer VMDK“ auf Seite 17.

Einschränkungen

Um ein Backup eines einzigen VMDK auf der virtuellen Maschine mit mehreren VMDKs durchzuführen, muss der Datenspeicher über genügend Speicherplatz für Snapshots von allen VMDKs auf der virtuellen Maschine verfügen. Obwohl mit dem Backupjob ein einziges VMDK gesichert werden soll, wird während des Backupprozesses ein Snapshot aller VMDKs auf der virtuellen Maschine erstellt.

Voraussetzungen

Die VDP-Appliance ist auf dem vCenter Server-Rechner installiert und konfiguriert.

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu.

2 Klicken Sie auf die Registerkarte **Backup** und dann unter **Backupjobaktionen** auf **Neu**, um den Assistenten „Neuen Backupjob erstellen“ zu starten.

HINWEIS Sie können den Assistenten „Neuen Backupjob erstellen“ auch über die Registerkarte **Erste Schritte** starten. Klicken Sie hierzu unter „Standardaufgaben“ auf **Backupjob erstellen**.

3 Zum Backup einzelner Festplatten virtueller Maschinen wählen Sie unter „Datentyp“ die Option **Einzelne Festplatten** aus und klicken Sie dann auf **Weiter**.

Auf der Seite „Virtuelle Maschinen“ wird eine Bestandsstruktur angezeigt. Die Struktur umfasst alle Objekte und virtuellen Maschinen auf dem vCenter Server-Rechner.

Klicken Sie auf den Erweiterungspfeil, um den Inhalt der Struktur nach und nach anzuzeigen. Wählen Sie die Kontrollkästchen neben den Elementen aus, die dem Backupjob hinzugefügt werden sollen, und klicken Sie dann auf **Weiter**.

4 Wählen Sie auf der Seite „Planung“ die Planung für den Job aus und klicken Sie auf **Weiter**.

5 Übernehmen Sie auf der Seite „Aufbewahrungs-Policy“ die standardmäßige Aufbewahrungs-Policy oder legen Sie eine alternative Aufbewahrungs-Policy fest. Klicken Sie dann auf **Weiter**.

6 Geben Sie auf der Seite „Name“ einen Backupjobnamen ein und klicken Sie auf **Weiter**.

Der Name des Backupjobs muss eindeutig sein und darf bis zu 255 Zeichen umfassen. Die folgenden Zeichen sind für den Namen des Backupjobs nicht zulässig: ~!@$^%(){}[]|,`;#\/:*?<>'"&. Zudem dürfen keine diakritischen Zeichen verwendet werden (z. B. â, é, ì, ü und ñ).

7 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung“ die Zusammenfassung zum Backupjob und klicken Sie auf **Fertig stellen**.

In einem Informationsdialogfeld wird die erfolgreiche Erstellung des Backupjobs bestätigt. Der Backupvorgang kann einige Minuten dauern.

8 Klicken Sie auf **OK**.

Der neu erstellte Backupjob wird nun auf der Registerkarte **Backup** aufgeführt.

Migration einzelner Festplatten

VMware Storage vMotion (SVMotion™) ist eine Komponente von VMware vSphere, die eine intuitive Benutzeroberfläche für die Livemigration von VMDK-Dateien bereitstellt, ohne Ausfallzeiten oder Unterbrechungen zu verursachen. Umfassende Informationen über die Migration mit vMotion und SVMotion finden Sie auf der Website des VMware vSphere-Dokumentationscenters:

http://pubs.vmware.com/vsphere-51/index.jsp.

Benutzern stehen zwei Möglichkeiten für die Migration einer virtuellen Maschine zwischen Datenspeichern offen:

- gleichzeitige Migration der kompletten virtuellen Maschine auf einen anderen Datenspeicher
- Migration einzelner Festplatten auf einen anderen Datenspeicher, wobei sich Festplatten einer virtuellen Maschine ggf. auf einem weiteren Datenspeicher befinden

Wenn eine komplette virtuelle Maschine migriert wird, führt die VDP-Appliance eine Aktualisierung der Backupjobs mit den neuen Speicherorten der geschützten VMDKs durch.

Ab VDP 6.0 und höheren Versionen erkennt VDP bei der Migration einzelner Festplatten (VMDK-Dateien) von einem Datenspeicher zu einem anderen die Änderung des Datenspeichers und sichert VMDK entsprechend während des nächsten Backups.

Anzeigen von Status- und Backupjobdetails

Auf der Registerkarte **Backup** wird eine Liste der mit VDP erstellten Backupjobs angezeigt. Durch Klicken auf einen Backupjob können Sie die Details des Jobs im Fenster „Backupjobdetails“ anzeigen:

- **Name**: Der Name des Backupjobs.
- **Status**: Gibt an, ob der Backupjob aktiviert oder deaktiviert ist.
- **Quellen:** Eine Liste der virtuellen Maschinen im Backupjob.
- **Veraltet**: Eine Liste aller virtuellen Maschinen, die bei der letzten Jobausführung nicht gesichert werden konnten.

Bearbeiten eines Backupjobs

Nachdem Sie einen Backupjob erstellt haben, können Sie ihn durch Markierung und Auswahl von **Backupjobaktionen** > **Bearbeiten** bearbeiten.

Klonen eines Backupjobs

Nachdem ein Backupjob erstellt wurde, können Sie ihn als Vorlage für die Erstellung eines anderen Jobs verwenden, indem Sie den Backupjob markieren und **Backupjobaktionen** > **Klonen** auswählen.

Beim Durchführen des Cloningvorgangs wird der Assistent zum Klonen von Backupjobs gestartet. Außerdem werden mit den Informationen aus dem ursprünglichen Job die ersten drei Seiten des Assistenten („Virtuelle Maschinen“, „Planung“ und „Aufbewahrungs-Policy“) ausgefüllt. Für den geklonten Job ist ein eindeutiger Name erforderlich. Mit Ausnahme des Datentyps (da ein Image-Backup nicht zu einem Backup einzelner Festplatten geändert werden kann und umgekehrt) können alle vom ursprünglichen Job kopierten Einstellungen geändert werden.

HINWEIS Sie können Backupjobs für vollständige Images und Backups einzelner Festplatten klonen.

Löschen eines Backupjobs

Sie können den Job löschen, indem Sie den Backupjob markieren und **Backupjobaktionen** > **Löschen** auswählen.

HINWEIS Wenn Sie auf der Registerkarte **Backup** die Option **Löschen** auswählen, wird nur der Job gelöscht. Zuvor vom Job erstellte Backups werden von VDP gemäß der Aufbewahrungs-Policy des Jobs aufbewahrt. Um Backups zu löschen, verwenden Sie auf der Registerkarte **Wiederherstellen** die Option **Löschen**.

Aktivieren oder Deaktivieren eines Backupjobs

Wenn ein Backupjob vorübergehend nicht mehr ausgeführt werden soll, können Sie ihn deaktivieren. Sie können deaktivierte Backupjobs bearbeiten und löschen. Mit VDP können deaktivierte Jobs erst nach ihrer Aktivierung ausgeführt werden.

Backupjobs können durch Markierung des Backupjobs und Auswahl von **Backupjobaktionen** > **Aktivieren/Deaktivieren** aktiviert bzw. deaktiviert werden.

Sofortiges Ausführen von vorhandenen Backupjobs

Backupjobs können über eine der folgenden Methoden sofort ausgeführt werden:

- Legen Sie fest, dass eine geschützte virtuelle Maschine gesichert werden soll.
- Legen Sie fest, dass ein vorhandener Backupjob ausgeführt werden soll.

Sofortiges Sichern einer geschützten virtuellen Maschine

1 Wählen Sie die geschützte virtuelle Maschine, die sofort gesichert werden soll, mit einer der folgenden Methoden aus:

- Klicken Sie mit der rechten Maustaste in einer Bestandsstruktur auf die virtuelle Maschine und wählen Sie **A**lle VDP-Aktionen > Jetzt sichern aus. Die virtuelle Maschine muss zu einem Backupjob gehören, damit diese Auswahlmöglichkeit angezeigt wird.
- Klicken Sie in der Bestandsstruktur auf die virtuelle Maschine und anschließend auf die Schaltfläche **Aktionen**. Wählen Sie **A**lle VDP-Aktionen > Jetzt sichern aus. Die virtuelle Maschine muss zu einem Backupjob gehören, damit diese Auswahlmöglichkeit angezeigt wird.
- Klicken Sie auf die virtuelle Maschine (auf der Registerkarte **Berichte**) und anschließend auf das unverankerte Symbol „Aktionen“. Wählen Sie dann **Jetzt sichern** aus.

Das Dialogfeld „Jetzt sichern“ wird angezeigt.

2 Wählen Sie die VDP-Appliance und den Backupjob aus und klicken Sie auf **OK**.

Über ein Informationsdialogfeld werden Sie informiert, dass der Backupjob initiiert wurde.

3 Klicken Sie auf **OK**.

VDP startet den Backupjob.

Sofortiges Ausführen eines Backupjobs

1 Klicken Sie in der VDP-Benutzeroberfläche auf der Registerkarte **Backup** auf den sofort auszuführenden Job.

Eine Mehrfachauswahl kann auf der Registerkarte **Backup** durch Klicken bei gedrückter Strg- oder Umschalttaste getroffen werden. Halten Sie die Strg-Taste gedrückt und klicken Sie auf mehrere bestimmte Backupjobs. Halten Sie die Umschalttaste gedrückt und klicken Sie auf einen Bereich von Backupjobs.

2 Klicken Sie auf **Jetzt sichern**.

Über eine Drop-down-Auswahl werden Ihnen folgende Optionen zur Verfügung gestellt:

- **Alle Quellen sichern**: Sichert alle virtuellen Maschinen im Backupjob
- **Nur veraltete Quellen sichern**: Sichert nur die virtuellen Maschinen, die bei der letzten Ausführung des Backupjobs nicht erfolgreich gesichert wurden.

3 Klicken Sie auf die sofort zu sichernden Quellen.

4 Klicken Sie auf **OK**, wenn eine Meldung über die Backupanforderung angezeigt wird.

VDP startet den Backupjob.

Mit der Option **Jetzt sichern** werden Backupjobs sofort initiiert, sofern VDP im „Backupzeitfenster“ bzw. „Wartungszeitfenster“ vorhanden ist.

Sperren und Entsperren eines Backups

Während Wartungsphasen überprüft VDP die Backups in der Appliance und bewertet, ob die Aufbewahrungsfrist der Backups abgelaufen ist. Ist sie abgelaufen, entfernt VDP das abgelaufene Backup aus der Appliance. Wenn VDP ein Backup nicht löschen soll, können Sie dieses sperren. VDP wird die Aufbewahrungsfrist zu diesem Backup erst dann wieder überprüfen, wenn es wieder entsperrt wird.

HINWEIS Die Daten in der VDP-Datenbank steuern den Status „Gesperrt“. Die VDP-Datenbank wird beim Import von Festplatten gelöscht (siehe „Anbinden vorhandener VDP-Festplatten“ auf Seite 80). Beim Import von Festplatten wird das ursprüngliche Ablaufdatum für gesperrte Backups neu zugewiesen und erhält den Status „Nie“. Diese Festplatten können daher nicht entsperrt werden.

HINWEIS Backups einzelner Festplatten können nicht gesperrt werden. Es können nur Backups für vollständige Images gesperrt werden.

Voraussetzungen

- VDP ist auf Ihrem vCenter Server-Rechner installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu.

2 Klicken Sie in der VDP-Benutzeroberfläche auf der Registerkarte **Wiederherstellen** auf den Erweiterungspfeil, der mit den in der Tabelle angezeigten Backups verknüpft ist, um nach dem zu sperrenden Backup zu suchen.

3 Wählen Sie das Kontrollkästchen neben dem Backup aus, das Sie sperren möchten.

4 Klicken Sie auf das Symbol **Sperren/Entsperren**.

Wird ein Backup gesperrt, so wird das Backupsymbol von einem Sperrsymbol überdeckt (). Das Backup ist nun gesperrt.

5 Wählen Sie zum Entsperren eines Backups erneut das Symbol **Sperren/Entsperren**.

Das überlagernde Sperrsymbol wird nicht mehr angezeigt und VDP überprüft das Ablaufdatum des Backup während der nächsten Wartungsphase.

Migrieren von Backupjobs von VDP zu Avamar

Mit VDP 6.1 können Sie Backupjobs und Backupverfizierungsjobs zu Avamar migrieren. Durch die Migration werden die Backupgruppe und die VM-Backupvalidierungsgruppe auf dem Avamar-Zielserver sichtbar und vollständig ausführbar.

Nach Abschluss der Migration geschieht Folgendes:

- Es gibt neue Einträge für Gruppen, Clients und zugehörige Einträge wie Datasets, Aufbewahrungen, Planungen usw. auf dem Avamar-Zielserver.
- Avamar kann dieselben Policies für den Schutz derselben VM-Clients wie VDP vor der Migration verwenden.

Richtlinien

- Die VDP-Migration ist ein einmaliger Prozess. Nach der Ausführung deaktiviert VDP weitere Migrationen.
- Beim Migrationsprozess werden nur die Details von Backupjobs und Backupverifizierungsjobs migriert.
- Für Anwendungsbackupjobs registrieren Sie die Anwendungsclients erneut auf dem Avamar-Server statt auf dem VDP-Server, um die neu migrierten Jobs ordnungsgemäß auszuführen.

Empfehlung

Sie replizieren alle vorhandenen Backups an den Avamar-Zielserver, bevor Sie die Migration durchführen.

Voraussetzungen

- Sie haben den vCenter-Quellclient beim Avamar-Zielserver registriert. Andernfalls können Sie die Migration nicht durchführen und die vCenter-Quelle manuell als neuen VMware vCenter Client auf dem Avamar-Zielserver hinzufügen.
- Sie haben VMware Image Proxy auf dem Ziel bereitgestellt und für das Arbeiten mit der vCenter-Quelle konfiguriert.

Verfahren

1 Öffnen Sie einen Webbrowser und geben Sie die folgende URL in die Adressleiste ein:

https://<IP_Adresse_der_VDP-Appliance>**:8543/vdp-configure/**

2 Geben Sie einen geeigneten VDP-Benutzernamen und ein Passwort in die entsprechenden Felder ein.

3 Überprüfen Sie die Informationen auf der Registerkarte **Avamar-Migration**.

Ein Migrationsverlauf in den Informationen weist darauf hin, dass VDP bereits migriert wurde und nicht erneut migriert werden kann.

4 Klicken Sie auf **Migrieren**.

Der Assistent für die **Migration** wird angezeigt.

5 Gehen Sie auf der Seite **Backupjobmigration** wie folgt vor:

   a Überprüfen Sie sorgfältig die Informationen zur Jobmigration und führen Sie erforderliche Aufgaben durch, um Fehler zu vermeiden.

   b Wählen Sie die relevante Option zum Aktivieren der Migration aus.

   c Klicken Sie auf **Weiter**.

6 Gehen Sie auf der Seite **Zielauswahl** wie folgt vor:

   a Geben Sie den Standort für den Avamar-Zielserver und die Serveranmeldeinformationen in die entsprechenden Felder ein.

   b Klicken Sie auf **Authentifizierung überprüfen**, um die Verbindung zwischen VDP und dem Avamar-Zielserver zu testen.

   c Klicken Sie auf **Weiter**.

7 Gehen Sie auf der Seite **Jobauswahl** wie folgt vor:

   a Wählen Sie aus den Tabellen auf den Registerkarten **Backupjobs** und **Backupverifizierungsjobs** die Jobs aus, die migriert werden sollen.

   Standardmäßig sind alle Jobs ausgewählt. Sie können alle Jobs aktivieren oder deaktivieren, indem Sie die Kontrollkästchen in der Tabellenkopfzeile aktivieren oder deaktivieren.

   b Klicken Sie auf **Weiter**.

8 Überprüfen Sie auf der Seite **Validierung** die Ergebnisse der Validierung und klicken Sie auf **Weiter**.

9 Überprüfen Sie auf der Seite **Bereit zur Fertigstellung** die Zusammenfassung der ausgewählten Jobs und klicken Sie auf **Migrieren**.

Nach Abschluss der Migration bemerken Sie den folgenden Status:

- VDP ist deaktiviert und auf der Registerkarte **Avamar-Migration** wird der Migrationsverlauf angezeigt.
- Im deaktivierten Status sind nur die folgenden VDP-Funktionen aktiviert:
  - Vollständige Image-Wiederherstellung
  - Festplattenwiederherstellung
  - Wiederherstellung auf Dateilevel
  - Notfallwiederherstellung
- vSphere Web Client und der VDP-Konfigurationsclient zeigen die Warnmeldungen an.
- Die Aufbewahrung der vorhandenen Backups bleibt gleich.

Sie können die folgenden zusätzlichen Schritte durchführen:

- Klicken Sie zum erneuten Aktivieren der deaktivierten Funktionen auf **Aktivieren**.
- Wenn Anwendungsbackupjobs vorhanden sind, die nicht auf dem Avamar-Zielserver registrierte Clients enthalten, müssen Sie diese Clients auf dem Avamar-Zielserver registrieren, um die neu migrierten Jobs ordnungsgemäß auszuführen. Zum Registrieren der Clients müssen Sie die Informationen im Dialogfeld **Benutzereingriffe** überprüfen, bevor Sie den Assistenten für die **Migration** schließen. Das Dialogfeld **Benutzereingriffe** enthält eine Liste der Clients und Domains, in denen Sie die Clients registrieren müssen. Klicken Sie zum Prüfen dieser Liste auf **Zielclients**.

Troubleshooting

- Nach Abschluss der Migration wird die Liste der fehlgeschlagenen Jobs angezeigt. Sie können die Migration entweder erneut versuchen oder beenden.
- Klicken Sie auf den Link **Weitere Informationen ...**, um zusätzliche Informationen zu den fehlgeschlagenen Jobs anzuzeigen.
- Weitere Informationen finden Sie in der Datei **avamar-migration.log**.

Automatische Backupverifizierung 13

In diesem Kapitel werden folgende Themen behandelt:

Informationen über die automatische Backupverifizierung

Bei der automatischen Backupverifizierung (ABV) handelt es sich um einen Mechanismus zur geplanten oder nach Bedarf durchgeführten Überprüfung von Backups, was für die Integrität von Wiederherstellungspunkten sorgt. ABV weist die folgenden Merkmale auf:

- Backups werden auf einer temporären virtuellen Maschine unter Verwendung folgender Benennungskonvention wiederhergestellt:

  VDP_VERIFICATION_<*VM-Name***> -<***eindeutige Nummer***>**

- Backups werden ohne Netzwerkkonflikte wiederhergestellt, da die Netzwerkschnittstellenkarte während des ABV-Vorgangs immer deaktiviert ist. Aufgrund der Deaktivierung der Netzwerkschnittstellenkarte ist es nicht möglich, einen Ping-Test durchzuführen.
- Nach Abschluss des Backupverifizierungsjobs werden temporäre virtuelle Maschinen, auch bezeichnet als *validierende VMs*, entfernt und aus dem Bestand gelöscht.
- Nur das letzte erfolgreiche komplette Image-Backup einer virtuellen Maschine wird verifiziert. Über das Fenster „Letzte Aufgaben“ und den Ereignisprotokollbericht wird gemeldet, welches Backup verifiziert wurde.

Einschränkungen

- Die Backupverifizierung wird für folgende Konfigurationen nicht unterstützt:
  - Einzelne VMDK-Backups.
  - Image-Backups von RDM-Festplatten (physischer Modus). Virtuell abhängige RDM-Festplatten werden unterstützt.
  - Anwendungsdatenbankbackups von Microsoft-Anwendungen (Exchange Server, SharePoint Server und SQL Server) werden nicht unterstützt.
  - Replizierte Backups.
  - Backups von importierten Festplatten.
- Die Verifizierung schlägt fehl, wenn der Pfad zum Zielhost geändert wird. Wenn der Host an einen neuen Ort verschoben wird, müssen Sie den Verifizierungsjob bearbeiten und den Zielhost erneut auswählen.
- Wenn der Name des Datenspeichers geändert wird, müssen Sie auch den Verifizierungsjob bearbeiten, um denselben oder einen anderen Datenspeicher erneut auszuwählen, bevor der Job wieder erfolgreich ausgeführt werden kann.
- In manchen Fällen wird die validierende VM nicht automatisch von VDP aus dem vCenter-Bestand gelöscht. In diesem Szenario müssen Sie die validierende VM manuell löschen.
- vSphere-Hosts vor Version 4.0 werden nicht als Zielhosts unterstützt, auf denen temporäre VMs wiederhergestellt werden.

Best Practices

Timing- und Ressourcenkonflikte

Sie können entsprechende Schritte unternehmen, um Timing- und Ressourcenkonflikte zu vermeiden, wenn Sie die Backupverifizierungsfunktion verwenden.

1. Wenn Sie VDP zum ersten Mal installieren, führen Sie erste komplette Backups durch.
2. Führen Sie nach der Durchführung der ersten Backups die ersten inkrementellen Backups durch.
3. Bestimmen Sie, wie lange es dauert, bis Backups ausgeführt werden, und planen Sie nach dem Abschluss der inkrementellen Backups auszuführende Backupverifizierungsjobs.

Auswählen des Ziels

Berücksichtigen Sie die folgenden Empfehlungen bei der Auswahl des Ziels:

- Führen Sie einen Lastenausgleich durch, wenn mehrere Verifizierungsjobs gleichzeitig ausgeführt werden sollen. Schränken Sie die Anzahl der Jobs auf fünf ein, wenn diese gleichzeitig ausgeführt werden.
- Vergewissern Sie sich, dass auf dem Host und dem Datenspeicher, auf dem die temporäre virtuelle Maschine wiederhergestellt wird, genügend Ressourcen verfügbar sind.

Allgemein

- Überprüfen Sie, ob VMware Tools zum Zeitpunkt des VM-Backups auf der virtuellen Maschine installiert ist.
- Stellen Sie das Heartbeat-Timeout-Intervall, abhängig von der Umgebung, auf seinen optimalen Wert ein. Bei manchen virtuellen Maschinen dauern Versand und Empfang des VMware Tools-Heartbeat länger als bei anderen.
- Überprüfen Sie regelmäßig die Verfügbarkeit des Zielhosts und eines Datenspeichers. Bearbeiten Sie den Job und konfigurieren Sie ggf. das Ziel neu. Wenn der Zielhost oder Datenspeicher nicht verfügbar ist, bearbeiten Sie den Job und wählen Sie ein neues Ziel.
- Führen Sie vor der Auswahl von „Verifizierungsskript“ als erweiterte Verifizierungsoption das Skript manuell auf dem Gast-BS aus, um seine ordnungsgemäße Ausführung zu überprüfen.

Erstellen eines neuen Backupverifizierungsjobs

Der Backupverifizierungsjob wird nach Bedarf oder im Rahmen einer Planung ausgeführt. Über den Abschnitt „Backupverifizierung“ der Registerkarte **Backup** können Sie Backupverifizierungsjobs erstellen und managen.

Voraussetzungen

- Es muss ein Backupjob oder ein Wiederherstellungspunkt vorhanden sein, bevor Sie einen Verifizierungsjob für eine virtuelle Maschine erstellen. Der Backupjob und der Wiederherstellungstyp müssen auf „Vollständiges Image“ eingestellt sein.
- VMware Tools muss zum Zeitpunkt des Backups auf den virtuellen Maschinen installiert sein. Wenn VMware Tools auf der validierenden VM nicht zu finden ist, schlägt die Heartbeat-Verifizierung fehl.
- Der ausgewählte Datenspeicher muss über ausreichend Speicherplatz verfügen.
- Wenn ein Verifizierungsskript verwendet werden soll, darf das Verifizierungsskript nicht von einer Verbindungsherstellung zu anderen VMs im Netzwerk abhängig sein.

Verfahren

1. Greifen Sie über einen Webbrowser auf VDP zu.
2. Klicken Sie auf die Registerkarte **Backup**.
3. Klicken Sie auf der Registerkarte **Backup** auf **Backupverifizierung**.
4. Wählen Sie aus dem Menü **Jobaktionen für Backupverifizierung** die Option **Neu** aus.

   Der Assistent „Neuen Backupverifizierungsjob erstellen“ wird auf der Seite „Virtuelle Maschinen“ geöffnet.
5. Wählen Sie auf der Seite „Virtuelle Maschinen“ eine virtuelle Maschine aus, für die ein Verifizierungsjob erstellt werden soll. Klicken Sie dann auf **Weiter**.

   - Pro Verifizierung können Sie nur eine virtuelle Maschine auswählen. Eine Mehrfachauswahl wird nicht unterstützt.

- Die virtuelle Maschine muss Teil eines vollständigen Image-Backupjobs sein oder sie kann über mehrere Wiederherstellungspunkte verfügen.
- Bei Bedarf lassen sich die virtuellen Maschinen nach Namen filtern.
- VMware Tools muss in den VM-Backups vorhanden sein. Anderenfalls schlägt der Verifizierungsjob fehl.

6 Wählen Sie auf der Seite „Verifizierungsoptionen“ eine Option aus:

- **Heartbeat-Verifizierung**: Hierbei handelt es sich um die Standardeinstellung zur Verifizierung eines Backups, unabhängig davon, ob die Skriptverifizierung ausgewählt ist. Durch die Heartbeat-Verifizierung wird geprüft, ob der VMware Tools-Heartbeat nach Einschalten der virtuellen Maschine innerhalb eines bestimmten Zeitrahmens empfangen wurde. Bei Empfang des VMware Tools-Heartbeat wurde das Gast-BS erfolgreich gestartet, und es befindet sich in einem einwandfreien Zustand.

HINWEIS Die Standardoption zur Verifizierung lautet **Gast-BS-Heartbeat**.

- **Skriptverifizierung**: Hierbei handelt es sich um die erweiterte Verifizierungsoption. Verwenden Sie die Skriptverifizierung, wenn Sie die virtuelle Maschine auf den Integritätsstatus von Anwendungen und Services überprüfen möchten, die auf dem Gastbetriebssystem ausgeführt wird. Das Skript muss vordefiniert und bereits auf dem Gast-BS vorhanden sein. Das Verifizierungsskript darf nicht von einer Verbindungsherstellung zu anderen virtuellen Maschinen im Netzwerk abhängig sein.

  Falls Sie ein Skript auf einem Gast-BS ausführen möchten, geben Sie die folgenden Informationen an:

  - **Benutzername**: Geben Sie die zum Anmelden beim Gastbetriebssystem verwendete Benutzer-ID ein.
  - **Passwort**: Geben Sie das zum Anmelden beim Gastbetriebssystem verwendete Passwort ein.
  - **Passwort bestätigen**: Geben Sie das Passwort erneut ein.
  - **Verifizierungsskript für Gast**: Geben Sie den vollständigen Pfad zum Speicherort des Skripts auf dem Gastbetriebssystem ein.

  Details zur Skriptkonfiguration finden Sie unter „Konfiguration des Verifizierungsskripts“ auf Seite 139.

7 Klicken Sie auf **Weiter**.

8 Wählen Sie auf der Seite „Ziel“ ein Ziel aus:

- **Zielpfad**: Der Zielhost muss mit der validierenden virtuellen Maschine kompatibel sein und der Zielhost muss über ausreichende Ressourcen verfügen, um die validierende virtuelle Maschine wiederherzustellen. Sie müssen einen eigenständigen Host oder einen Host innerhalb eines Clusters als Ziel auswählen, wo Backups vorübergehend zwecks Verifizierung wiederhergestellt werden. Ressourcenpools und vApps sind keine gültigen Ziele. vSphere-Hosts vor Version 4.0 werden nicht unterstützt.
- **Datastore**: Abhängig vom ausgewählten Host wird eine Liste mit Datenspeicher angezeigt. Es muss ein Datenspeicher zum Wiederherstellen der validierenden virtuellen Maschine ausgewählt werden. Vergewissern Sie sich, dass der ausgewählte Datenspeicher über ausreichend Speicherplatz verfügt.

9 Klicken Sie auf **Weiter**.

10 Wählen Sie auf der Seite „Planung“ die Planung für den Backupverifizierungsjob aus. Durch die auf dieser Seite festgelegten Einstellungen wird bestimmt, wie häufig und zu welcher Uhrzeit der Verifizierungsjob ausgeführt wird.

a **Planung für Backupverifizierung**: Geben Sie als Zeitintervalle täglich, wöchentlich oder monatlich an.

b **Startzeit auf Server**: Legen Sie die Zeit fest, zu der die Backupverifizierung am geplanten Tag stattfinden soll.

11 Klicken Sie auf **Weiter**.

12 Geben Sie auf der Seite „Jobname“ einen eindeutigen Namen für die Identifizierung des Verifizierungsjobs ein und klicken Sie auf **Weiter**.

Der Name des Verifizierungsjob kann sich aus beliebigen Buchstaben des Alphabets und Ziffern zusammensetzen. Als Sonderzeichen sind nur Leerzeichen, Unterstriche, Bindestriche und Punkte zulässig.

13 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung“ die Zusammenfassung des Backupverifizierungsjobs, den Sie erstellen. Bei Bedarf können Sie die Konfiguration des Jobs ändern, indem Sie auf der entsprechenden Seite auf **Zurück** klicken. Klicken Sie auf **Fertig stellen**, wenn Sie zum Speichern des Jobs bereit sind.

HINWEIS Sie können ebenfalls die Zusammenfassung des Backupverifizierungsjobs überprüfen, und zwar im Abschnitt „Backupverifizierung“ auf der Registerkarte „Wiederherstellen“.

14 Klicken Sie auf **OK**, wenn eine Meldung über die erfolgreiche Erstellung des Backupverifizierungsjobs angezeigt wird.

Konfiguration des Verifizierungsskripts

Sofern die Verwendung eines Verifizierungsskripts gewünscht wird, können hierzu die unterstützten Skriptformate .bat, .cmd, .sh und .exe eingesetzt werden. Eine gültige Skriptdatei wird per Doppelklick im Dateimanager oder in der Explorer-Ansicht ausgeführt. Wenn das Skript in einem nicht unterstützten Format vorliegt, müssen Sie die Ausführung des Skripts in einem unterstützten Format einschließen.

Ein Windows Power Shell-Skript (.ps1) kann beispielsweise nicht aufgerufen und direkt mit VDP ausgeführt werden, da das .ps-Format nicht unterstützt wird. Es ist jedoch möglich, das .ps-Skript über ein unterstütztes Format (z. B. .bat) aufzurufen und dann den vollständigen Pfad zum Speicherort des Skripts auf dem Gastbetriebssystem anzugeben. Achten Sie darauf, die Ausführungs-Policy vor der Ausführung des Skripts auf **Uneingeschränkt** einzustellen.

Das Skript muss 0 oder eine andere Ganzzahl zurückgeben. Bei Rückgabe von 0 war die Skriptverifizierung erfolgreich. Bei Rückgabe einer anderen Ganzzahl als 0 ist die Skriptverifizierung fehlgeschlagen.

Bearbeiten eines Backupverifizierungsjobs

Nach dem Erstellen von Backupverifizierungsjobs können Sie sie bei Bedarf bearbeiten.

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu.

2 Klicken Sie auf die Registerkarte **Backup**.

3 Klicken Sie auf der Registerkarte **Backup** auf **Backupverifizierung**.

4 Wählen Sie den Backupverifizierungsjob aus, den Sie bearbeiten möchten, und wählen Sie anschließend aus dem Menü **Jobaktionen für Backupverifizierung** die Option **Bearbeiten** aus.

Der Assistent „Backupverifizierungsjob wird bearbeitet: *job_name*“ wird auf der Seite „Virtuelle Maschinen“ geöffnet.

5 Durchlaufen Sie den Assistenten und nehmen Sie bei Bedarf Änderungen vor.

6 Wenn Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **Fertig stellen**.

7 Klicken Sie auf **OK**, wenn eine Meldung über die erfolgreiche Speicherung von Änderungen am Backupverifizierungsjobs angezeigt wird.

Klonen eines Backupverifizierungsjobs

Sobald ein Verifizierungsjob erstellt wurde, können Sie ihn als Vorlage für die Erstellung eines anderen Jobs verwenden, indem Sie den Verifizierungsjob markieren und **Jobaktionen für Backupverifizierung** > **Klonen** auswählen.

Beim Durchführen des Cloningvorgangs wird der Assistent zum Klonen von Backupverifizierungsjobs gestartet. Außerdem werden mit den Informationen aus dem ursprünglichen Job die ersten drei Seiten des Assistenten („Virtuelle Maschinen“, „Planung“ und „Aufbewahrungs-Policy“) ausgefüllt. Für den geklonten Job ist ein eindeutiger Name erforderlich.

Ausführen eines Backupverifizierungsjobs

Nach der Erstellung eines Backupverifizierungsjobs ist es möglich, eine Verifizierung zu starten, indem eine Verifizierung „nach Bedarf“ ausgeführt oder indem auf den planungsmäßigen Beginn des Backupverifizierungsjobs gewartet wird. Der vollständige Backupverifizierungszyklus lautet wie folgt:

- **Wiederherstellen**: Das neueste Backup für die ausgewählte virtuelle Maschine wird auf einer temporären virtuellen Maschine wiederhergestellt, die nach der Backupverifizierung gelöscht wird.
- **Einschalten**: Sobald die temporäre virtuelle Maschine wiederhergestellt wurde, wird sie so konfiguriert, dass die Netzwerkschnittstellenkarte vor dem Einschalten deaktiviert wird.
- **Startbetriebssystem**: Warten Sie darauf, dass nach dem Einschalten der virtuellen Maschine der Startvorgang für das Gastbetriebssystem vollständig abgeschlossen wurde.
- **Heartbeat-Verifizierung**: Nach dem Start des Gastbetriebssystems wartet die Appliance auf den Empfang des VMware Tools-Heartbeat von der wiederhergestellten virtuellen Maschine. Wenn kein Heartbeat empfangen wird, schlägt der Verifizierungsjob fehl, und das Backup befindet sich in keinem guten Zustand.
- **Verifizierungsskript**: Das Skript wird nur dann ausgeführt, wenn Sie sich für ein erweitertes Verifizierungslevel (Verifizierungsskript) entschieden haben. Über diese Funktion wird ein angepasstes Skript ausgeführt, das vom Benutzer zur Verifizierung des Status der auf dem Gast-BS ausgeführten Anwendungen definiert und festgelegt wurde.
- **Ausschalten**: Nachdem die Skriptverifizierung abgeschossen wurde, wird die virtuelle Maschine ausgeschaltet.
- **Virtuelle Maschine löschen**: In diesem letzten Schritt wird die wiederhergestellte virtuelle Maschine gelöscht und die Ergebnisse der Verifizierung werden von vCenter gemeldet (im Fenster „Letzte Aufgaben“ und im Ereignisprotokoll).

Verfahren

1. Greifen Sie über einen Webbrowser auf VDP zu.
2. Klicken Sie auf die Registerkarte **Backup**.
3. Klicken Sie auf der Registerkarte **Backup** auf **Backupverifizierung**.
4. Wählen Sie den Backupverifizierungsjob aus, den Sie ausführen möchten, und klicken Sie anschließend auf **Jetzt überprüfen**.
5. Klicken Sie auf **OK**, wenn eine Meldung über die erfolgreiche Ausgabe einer/mehrerer Anforderung(en) zur Backupverifizierung angezeigt wird.

Überwachen der Backupverifizierung

Nur das letzte erfolgreiche Backup einer virtuellen Maschine wird verifiziert. Sie können eine der nachstehenden Methoden verwenden, um die Ergebnisse des Verifizierungsjobs zu prüfen:

- vCenter-Aufgaben/-Ereignisse
- Registerkarte **Berichte**. Weitere Informationen finden Sie unter „Anzeigen von Informationen über die Registerkarte „Berichte““ auf Seite 118.
- E-Mail-Berichte. Weitere Informationen finden Sie unter „Konfigurieren von E-Mail-Benachrichtigungen und Berichten” auf Seite 61.
- Clientprotokolle. Clientprotokolle können unter h*ttps://<IP-Adresse oder Hostname von VDP>:8543/vdp-configure heruntergeladen werden.*

Aktivieren und Deaktivieren eines Backupverifizierungsjobs

Nach dem Erstellen von Backupverifizierungsjobs können Sie sie bei Bedarf aktivieren und deaktivieren. Wenn Sie einen Backupverifizierungsjob deaktivieren, wird er nicht mehr ausgeführt, bis Sie ihn wieder aktivieren.

Verfahren

1. Greifen Sie über einen Webbrowser auf VDP zu. Anweisungen finden Sie unter „Backupjobs” auf Seite 124.
2. Klicken Sie auf die Registerkarte **Backup**.
3. Klicken Sie auf der Registerkarte **Backup** auf **Backupverifizierung**.
4. Wählen Sie den Backupverifizierungsjob aus, den Sie aktivieren oder deaktivieren möchten, und wählen Sie aus dem Menü **Jobaktionen für Backupverifizierung** die Option **Aktivieren/Deaktivieren** aus.
5. Klicken Sie auf **OK**, wenn eine Meldung über die erfolgreiche Aktivierung oder Deaktivierung des Backupverifizierungsjobs angezeigt wird.

Löschen eines Backupverifizierungsjobs

Sie können Backupverifizierungsjobs löschen, wenn sie nicht länger benötigt werden.

Verfahren

1. Greifen Sie über einen Webbrowser auf VDP zu. Anweisungen finden Sie unter „Backupjobs” auf Seite 124.
2. Klicken Sie auf die Registerkarte **Backup**.
3. Klicken Sie auf der Registerkarte **Backup** auf **Backupverifizierung**.
4. Wählen Sie den Backupverifizierungsjob aus, den Sie löschen möchten, und wählen Sie aus dem Menü **Jobaktionen für Backupverifizierung** die Option **Löschen** aus.
5. Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob Sie den ausgewählten Job wirklich löschen möchten.
6. Klicken Sie auf **OK**, wenn eine Meldung über die erfolgreiche Löschung des Backupverifizierungsjobs angezeigt wird.

Managen von Wiederherstellungen 14

In diesem Kapitel wird folgendes Thema behandelt:

Wiederherstellungsvorgänge

Nachdem Sie die virtuellen Maschinen gesichert haben, können Sie die Backups entweder am ursprünglichen Speicherort oder an einem anderen Speicherort wiederherstellen.

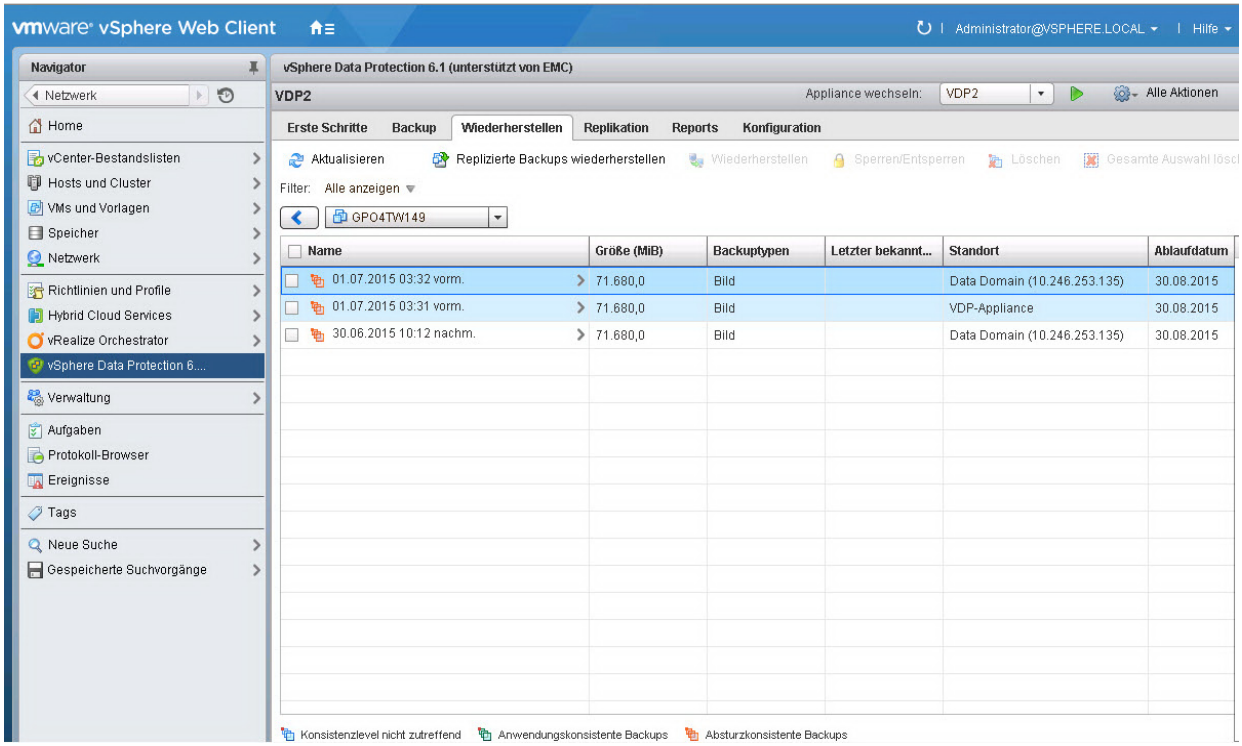
Wiederherstellungsvorgänge werden auf der Registerkarte **Wiederherstellen** durchgeführt. Auf der Registerkarte **Wiederherstellen** wird eine Liste der virtuellen Maschinen angezeigt, die von der VDP-Appliance gesichert wurden. Sie können durch die Liste von Backups navigieren und bestimmte Backups auswählen und wiederherstellen. In der Liste werden spezielle Symbole für absturzkonsistente und anwendungskonsistente Backups angezeigt.

Symbolrelevante Informationen finden Sie in der Legende im unteren linken Bereich der Seite. Notieren Sie sich vor der Auswahl eines wiederherzustellenden Backups die absturzkonsistenten Backups und das Ablaufdatum des Backups.

HINWEIS Die Erkennung der anwendungskonsistenten Backups gilt nur für die Windows-Clients. Die anwendungskonsistenten Backups auf den Linux-Clients werden mit dem Symbol **Konsistenzlevel nicht zutreffend** angezeigt.

Nach einer gewissen Zeit sind die auf der Registerkarte **Wiederherstellen** angezeigten Informationen veraltet. Zum Anzeigen der neuesten Informationen zu Backups, die für eine Wiederherstellung verfügbar sind, klicken Sie auf **Aktualisieren**.

In der folgenden Abbildung ist die Registerkarte **Wiederherstellen** dargestellt:



Einschränkungen

- Der Wiederherstellungsassistent lässt nicht die Auswahl mehrerer Wiederherstellungspunkte für denselben MSApp-Client zu. Es kann nur jeweils ein Wiederherstellungspunkt vom selben Client ausgewählt werden.
- Wenn für die Ziel-VM SCSI-Bus-Sharing konfiguriert ist, werden Wiederherstellungen auf diese virtuelle Maschine nicht unterstützt.

Auswahl wiederherzustellender Backups

Backups können mit den folgenden Optionen wiederhergestellt werden:

- Klicken Sie auf der Registerkarte **Erste Schritte** des VDP-Bildschirms auf **Backup wiederherstellen**.
- Wählen Sie auf der Registerkarte **Wiederherstellen** einen Wiederherstellungspunkt aus und klicken Sie auf **Wiederherstellen**.
- Klicken Sie in der vCenter-Bestandsliste mit der rechten Maustaste auf eine geschützte virtuelle Maschine und wählen Sie **Alle VDP-Aktionen > Wiederherstellungstest** aus. Auf der Seite „Backup auswählen“ wird eine Liste von Backups angezeigt.

Filtern der Backupliste

Die Liste der Backups, die wiederhergestellt werden können, kann mithilfe der Drop-down-Pfeile wie folgt gefiltert werden:

- **Backupdatum**: Gefiltert nach „Liegt vor“, „Liegt nach“, „Ist am“ oder „Ist nicht am”
- **Clientname**: Gefiltert nach **„**Enthält**“**, **„**Enthält nicht**“**, **„**Ist**“** oder **„**Ist nicht**“**
- **Speicherort**: Gefiltert nach dem Speicherort des Backups

Löschen Sie den Filter, indem Sie auf die Schaltfläche **Aktualisieren klicken** oder im Drop-down-Menü „Filter“ die Option Alle anzeigen auswählen.

Auf der Seite „Backup auswählen“ können Sie die wiederherzustellenden virtuellen Maschinen auswählen.

Wiederherstellungen bei vorhandenen Snapshots

In früheren VDP-Versionen konnten Benutzer Wiederherstellungen auf der ursprünglichen virtuellen Maschine durchführen, selbst wenn diese virtuelle Maschine Snapshots enthielt. Ab VDP 5.5 sind keine Snapshots mehr auf virtuellen Maschinen zulässig.

ACHTUNG Entfernen Sie vor der Durchführung von Wiederherstellungen alle Snapshots, die möglicherweise von der virtuellen Maschine stammen. Der Wiederherstellungsjob schlägt fehl, wenn die virtuelle Zielmaschine Snapshots enthält.

In den folgenden Knowledgebase-Artikeln finden Sie Informationen zum korrekten Einsatz von Snapshots:

- http://kb.vmware.com/kb/1025279
- https://community.emc.com/thread/145249?start=0&start=0

Wiederherstellen von Image-Backups am ursprünglichen Speicherort

Sie können Backups manuell wiederherstellen, indem Sie den Assistenten „Backup wiederherstellen“ verwenden.

Es gibt drei Szenarios, bei denen eine Wiederherstellung am ursprünglichen Speicherort nicht möglich ist, wenn einzelne Festplatten statt der gesamten virtuellen Maschine für die Wiederherstellung ausgewählt wurden:

- Die ursprüngliche Festplatte ist als „Unabhängig – Dauerhaft“ markiert.
- Die ursprüngliche Festplatte wurde aus der Ziel-VM entfernt.
- Die ursprüngliche Festplatte wurde von der Ziel-VM gelöscht.

HINWEIS Ein Wiederherstellungsjob für dieselbe(n) Festplatte(n) mit zwei unterschiedlichen Zeitstempeln ist nicht zulässig. Bei dem Versuch, eine mit zwei unterschiedlichen Zeitstempeln gesicherte Festplatte wiederherzustellen, wird eine Option zum Entfernen der doppelt vorhandenen Festplatte angezeigt. Die Wiederherstellung wird erst dann fortgesetzt, wenn die doppelt vorhandene Festplatte entfernt wurde.

Voraussetzungen

- VDP ist auf Ihrem vCenter Server-Rechner installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu.

2 Klicken Sie auf die Registerkarte **Wiederherstellen**.

3 Filtern Sie bei Bedarf die Backups, um Ihre Suche einzugrenzen.

4 Wählen Sie eine in der Spalte Name aufgeführte virtuelle Maschine aus. Beim Klicken auf eine virtuelle Maschine wird diese mit den durchgeführten Backups eingeblendet. Sie können ein oder mehrere Backups auswählen oder auf ein Backup klicken, um nach der wiederherzustellenden Festplatte zu suchen.

HINWEIS Der Name des Clients (der virtuellen Maschine) wird so umbenannt, das eine Zeichenfolge zufälliger Zeichen in der Domain **VDP_IMPORT** auf der Registerkarte **Wiederherstellen** angehängt wird, wenn während der Erstkonfiguration Speicher aus einer anderen VDP-Appliance importiert wird.

5 Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Elementen, um sie für die Wiederherstellung auszuwählen.

6 Klicken Sie auf **Wiederherstellen**, um den Assistenten „Backup wiederherstellen“ zu starten.

7 Gehen Sie auf der Seite **Backup auswählen** wie folgt vor:

   a Überprüfen Sie die Liste ausgewählter Backups auf absturzkonsistente Backups. Wenn Sie die absturzkonsistenten Backups nicht wiederherstellen möchten, entfernen Sie diese.

   b Klicken Sie auf **Weiter**.

8 Gehen Sie auf der Seite **Wiederherstellungsoptionen festlegen** wie folgt vor:

   a Behalten Sie die Aktivierung der Option **Am ursprünglichen Speicherort wiederherstellen** bei. Wenn die vmdk-Datei noch am ursprünglichen Speicherort vorhanden ist, wird sie überschrieben.

HINWEIS Wenn das virtuelle Laufwerk auf der ursprünglichen VM entfernt oder gelöscht wurde, ist die Option „Am ursprünglichen Speicherort wiederherstellen“ nicht zulässig. Die VMDK-Dateien müssen an einem neuen Speicherort wiederhergestellt werden.

   b Wenn Sie die virtuelle Maschine zusammen mit ihrer Konfiguration wiederherstellen möchten, wählen Sie **Virtuelle Maschine zusammen mit Konfiguration wiederherstellen** aus.

   c Klicken Sie auf **Weiter**.

9 Gehen Sie auf der Seite **Bereit zur Fertigstellung** wie folgt vor:

   a Überprüfen Sie die Zusammenfassung Ihrer Wiederherstellungsanforderung.

   In der Zusammenfassung werden die folgenden Informationen angezeigt:

   - Die Anzahl der Maschinen, die an ihrem ursprünglichen Standort ersetzt oder wiederhergestellt werden und die an einem neuen Standort erstellt oder wiederhergestellt werden
   - Ein Kontrollkästchen, mit dem Sie das Fortsetzen der Wiederherstellung bestätigen, wenn die Liste der ausgewählten wiederherzustellenden Backups absturzkonsistente Backups enthält

     Wenn Sie das Kontrollkästchen aktivieren, um die absturzkonsistente Wiederherstellung fortzusetzen, schlägt die Wiederherstellung manchmal fehl.

   Wenn Sie Wiederherstellungseinstellungen ändern möchten, klicken Sie entweder auf der Assistentenseite auf die Schaltfläche **Zurück** oder klicken Sie auf der linken Seite der Assistentenseite auf den Titel des entsprechenden nummerierten Schritts, um zur gewünschten Seite zu navigieren.

b Klicken Sie auf **Fertig stellen**, um mit dem Wiederherstellungsvorgang zu beginnen.

Eine Meldung wird angezeigt, in der angegeben ist, dass die Wiederherstellung erfolgreich initiiert wurde.

c Klicken Sie auf **OK**.

10 Überwachen Sie den Fortschritt der Wiederherstellung über das Fenster **Letzte Aufgaben**.

HINWEIS Bestätigen Sie bei Auswahl von **Verbindung der Netzwerkschnittstellenkarte wiederherstellen** die Netzwerkkonfiguration für die neu erstellte virtuelle Maschine. Es ist möglich, dass die Netzwerkschnittstellenkarte der neuen virtuellen Maschine dieselbe IP-Adresse wie die ursprüngliche virtuelle Maschine einsetzt, was zu Konflikten führt.

Wiederherstellen von Image-Backups an einem neuen Speicherort

Sie können Backups manuell wiederherstellen, indem Sie den Assistenten „Backup wiederherstellen“ verwenden. Im Assistenten Backup wiederherstellen können Sie auf der Seite „Wiederherstellungsoptionen festlegen“ angeben, wo das Image-Backup wiederhergestellt werden soll.

Voraussetzungen

- VDP ist auf Ihrem vCenter Server-Rechner installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu.

2 Klicken Sie auf die Registerkarte **Wiederherstellen**.

3 Filtern Sie bei Bedarf die Backups, um Ihre Suche einzugrenzen.

4 Wählen Sie eine in der Spalte Name aufgeführte virtuelle Maschine aus. Beim Klicken auf einen Client (eine virtuelle Maschine) wird diese(r) mit den durchgeführten Backups eingeblendet. Sie können ein oder mehrere Backups auswählen oder auf ein Backup klicken, um weiter per Drill-down zu der wiederherzustellenden Festplatte oder Anwendung zu gelangen.

HINWEIS Wenn der Speicher während der Erstkonfiguration von einer anderen VDP-Appliance importiert wurde, wird der in der Spalte „Name“ angezeigte Clientname durch eine Zeichenfolge zufälliger Buchstaben erweitert und somit umbenannt.

5 Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Elementen, um sie für die Wiederherstellung auszuwählen.

6 Klicken Sie auf **Wiederherstellen**, um den Assistenten „Backup wiederherstellen“ zu starten.

7 Klicken Sie auf der Seite **Backup auswählen** auf das wiederherzustellende Backup und dann auf **Weiter**.

8 Gehen Sie auf der Seite **Wiederherstellungsoptionen festlegen** wie folgt vor:

a Deaktivieren Sie das Kontrollkästchen **Am ursprünglichen Speicherort wiederherstellen**, um die Wiederherstellungsoptionen für jedes Backup, das Sie an einem neuen Speicherort wiederherstellen, festzulegen.

b Geben Sie die folgenden Felder an:

- **Neuer VM-Name**: Geben Sie einen neuen Namen für die wiederhergestellte VM ein.
- **Ziel**: Klicken Sie auf **Wählen** und wählen Sie das neue Ziel aus.
- **Datastore**: Wählen Sie den Datenspeicher aus, in dem die virtuelle Maschine wiederhergestellt wird.

c Klicken Sie auf **Weiter**.

9 Gehen Sie auf der Seite **Bereit zur Fertigstellung** wie folgt vor:

a Überprüfen Sie die Zusammenfassung Ihrer Wiederherstellungsanforderungen.

Diese Zusammenfassung gibt an, wie viele Maschinen ersetzt (oder an ihrem ursprünglichen Speicherort wiederhergestellt) und wie viele Maschinen erstellt (oder an einem neuen Speicherort wiederhergestellt) werden.

Wenn Sie Einstellungen für Ihre Wiederherstellungsanforderung ändern möchten, kehren Sie entweder über die Schaltfläche **Zurück** zum entsprechenden Bildschirm zurück oder klicken Sie links im Assistentenbildschirm auf die Überschrift des entsprechend nummerierten Schritts.

b Klicken Sie auf **Fertig stellen**, um mit dem Wiederherstellungsvorgang zu beginnen.

Eine Meldung wird angezeigt, in der angegeben ist, dass die Wiederherstellung erfolgreich initiiert wurde.

c Klicken Sie auf **OK**.

10 Überwachen Sie den Fortschritt der Wiederherstellung über das Fenster **Letzte Aufgaben**.

HINWEIS Bestätigen Sie bei Auswahl von **Verbindung der Netzwerkschnittstellenkarte wiederherstellen** die Netzwerkkonfiguration für die neu erstellte virtuelle Maschine. Es ist möglich, dass die Netzwerkschnittstellenkarte der neuen virtuellen Maschine dieselbe IP-Adresse wie die ursprüngliche virtuelle Maschine einsetzt, was zu Konflikten führt.

Deaktivieren der vMotion-Funktion vor der Durchführung von Wiederherstellungen an einem neuen Speicherort

vSphere vMotion ist eine Funktion zur Livemigration einer laufenden virtuellen Maschine von einem physischen Server zu einem anderen. Stellen Sie sicher, dass während der Durchführung von Backups oder Wiederherstellungen auf der VDP-Appliance keine vMotion-Vorgänge ausgeführt werden. „vMotion-Vorgänge sind während aktiver Backupvorgänge nicht zulässig" auf Seite 220 bietet Informationen dazu.

Deaktivieren Sie die vMotion-Funktion auf den VM- und Datenspeicherebenen, im Backupzeitfenster und vor der Durchführung einer Wiederherstellung an einem neuen Speicherort.

1 Greifen Sie über einen Webbrowser auf vSphere Web Client zu:

https://<IP_Adresse_vCenter_Server>**:9443/vsphere-client/**

2 Wählen Sie **vCenter** > **Hosts und Cluster** aus.

3 Wählen Sie auf der Registerkarte **DRS** die Option **Manuell** für alle DRS-Cluster aus, die im Menü auf der linken Seite aufgeführt sind.

4 Wählen Sie **Bestand** > **Datenspeicher** aus.

5 Gehen Sie für jeden Datenspeicher, auf dem sich VMs, Proxys und VDPs befinden, wie folgt vor:

a Wählen Sie den Datenspeicher aus.

b Wählen Sie **Edit Settings** aus.

c Klicken Sie im Menü links unter **Allgemein** auf **SDRS-Automatisierung**.

d Wählen Sie im rechten Fenster **Keine Automatisierung (manuell)** aus.

e Wählen Sie **Einstellungen der virtuellen Maschine** aus.

f Vergewissern Sie sich, dass bei allen VMs **Deaktiviert** oder **Manuell** für die SDRS-Automatisierung angezeigt wird.

Wiederherstellen von Backups auf einzelnen SCSI-Festplatten

Sie können Backups auf einzelne SCSI-Festplatten wiederherstellen, indem Sie den Assistenten „Backup wiederherstellen“ verwenden. Im Assistenten Backup wiederherstellen können Sie auf der Seite „Wiederherstellungsoptionen festlegen“ angeben, wo die einzelnen SCSI-Festplatten wiederhergestellt werden sollen.

HINWEIS SCSI-ID unterstützt nicht mehrere Wiederherstellungsanforderungen verschiedener VMs. Obwohl Sie mehrere Wiederherstellungsvorgänge initiieren können, ist nur die erste Wiederherstellung erfolgreich. Beim Wiederherstellen mehrerer Festplatten als neue Festplatten auf der ursprünglichen oder vorhandenen virtuellen Maschine müssen alle Festplatten von demselben Backup und derselben virtuellen Maschine stammen.

Voraussetzungen

- VDP ist auf Ihrem vCenter Server-Rechner installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu.

2 Klicken Sie auf die Registerkarte **Wiederherstellen**.

3 Filtern Sie bei Bedarf die Backups, um Ihre Suche einzugrenzen.

4 Wählen Sie eine in der Spalte Name aufgeführte virtuelle Maschine aus. Beim Klicken auf einen Client (eine virtuelle Maschine) wird diese(r) mit den durchgeführten Backups eingeblendet. Sie können ein oder mehrere Backups auswählen oder auf ein Backup klicken, um weiter per Drill-down zu der wiederherzustellenden Festplatte oder Anwendung zu gelangen.

HINWEIS Wenn der Speicher während der Erstkonfiguration von einer anderen VDP-Appliance importiert wurde, wird der in der Spalte „Name“ angezeigte Clientname durch eine Zeichenfolge zufälliger Buchstaben erweitert und somit umbenannt.

5 Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Elementen, um sie für die Wiederherstellung auszuwählen.

6 Klicken Sie auf **Wiederherstellen**, um den Assistenten „Backup wiederherstellen“ zu starten.

7 Klicken Sie auf der Seite **Backup auswählen** auf das wiederherzustellende Backup und dann auf **Weiter**.

8 Deaktivieren Sie auf der Seite **Wiederherstellungsoptionen festlegen** das Kontrollkästchen **Am ursprünglichen Speicherort wiederherstellen**, um die Wiederherstellungsoptionen für jedes Backup festzulegen, das Sie an einem neuen Speicherort wiederherstellen.

   a Geben Sie die folgenden Informationen ein:

   - **Ziel**: Klicken Sie zum Auswählen eines neuen Ziels auf **Wählen**. Sie können einen neuen Zielspeicherortcontainer (vApp, Ressourcenpool, Host oder Rechenzentrum) auswählen, wo das Backup wiederhergestellt wird. Sie können auch das Standardziel übernehmen. Dabei handelt es sich um den ursprünglichen Speicherort der vorhandenen virtuellen Maschine.
   - **Neuer VM-Name**: Das Feld **Neuer VM-Name** wird automatisch mit dem Namen der vorhandenen virtuellen Maschine aufgefüllt. Sie können dieses Feld ändern, um der virtuellen Maschine einen neuen Namen zu geben, wenn Sie in einem Container wiederherstellen. Beim Wiederherstellen auf einer vorhandenen virtuellen Maschine ist eine Änderung des Namens nicht möglich.
   - **Datastore**: Hier wird der Datenspeicher aufgeführt, auf dem sich derzeit die erste Festplatte befindet. Beim Wiederherstellen einer Festplatte auf einer vorhandenen virtuellen Maschine kann dieses Feld nicht bearbeitet werden. Wenn Sie eine Festplatte in einem neuen Container wiederherstellen, wählen Sie den Datenspeicher aus, auf dem die virtuelle Maschine wiederhergestellt wird.

- **Festplatten-ID**: Hier werden die als Wiederherstellungsziele verfügbaren SCSI-Festplatten-ID-Steckplätze aufgeführt. Die Liste zeigt nur leere SCSI-Steckplätze der SCSI-Controller, die aktuell mit der virtuellen Maschine verbunden sind. Wählen Sie aus der Liste einen Steckplatz für das virtuelle SCSI-Laufwerk als Wiederherstellungsziel aus.

  Sie können nicht auf IDE-konfigurierten virtuellen Laufwerken wiederherstellen. Es werden nur virtuelle SCSI-Laufwerke unterstützt. Auf einem SCSI-Controller sind maximal 15 Laufwerke zulässig. Steckplatz 7 ist reserviert und nicht verfügbar.

HINWEIS Der Assistent „Backup wiederherstellen“ fügt einen neuen Controller nicht automatisch hinzu, wenn nicht genügend SCSI-Steckplätze verfügbar sind. Sie müssen vor der Initiierung der Festplattenwiederherstellung einen neuen SCSI-Controller hinzufügen.

b Klicken Sie auf **Weiter**.

9 Gehen Sie auf der Seite **Bereit zur Fertigstellung** wie folgt vor:

a Überprüfen Sie die Zusammenfassung Ihrer Wiederherstellungsanforderungen.

Diese Zusammenfassung gibt an, wie viele Maschinen ersetzt (oder an ihrem ursprünglichen Speicherort wiederhergestellt) und wie viele Maschinen erstellt (oder an einem neuen Speicherort wiederhergestellt) werden.

Wenn Sie Einstellungen für Ihre Wiederherstellungsanforderung ändern möchten, kehren Sie entweder über die Schaltfläche **Zurück** zum entsprechenden Bildschirm zurück oder klicken Sie links im Assistentenbildschirm auf die Überschrift des entsprechend nummerierten Schritts.

b Klicken Sie auf **Fertig stellen**, um mit dem Wiederherstellungsvorgang zu beginnen.

Eine Meldung wird angezeigt, in der angegeben ist, dass die Wiederherstellung erfolgreich initiiert wurde.

c Klicken Sie auf **OK**.

10 Überwachen Sie den Fortschritt der Wiederherstellung über das Fenster **Letzte Aufgaben**.

Löschen eines Backups von der Registerkarte „Wiederherstellen“

VDP löscht Backups entsprechend den Aufbewahrungs-Policies, die für die Backupjobs festgelegt wurden. Sie können Backups allerdings auch manuell über die Registerkarte **Wiederherstellen** löschen. Wählen Sie hierzu die zu löschenden Backupjobs aus und klicken Sie auf das Symbol **Löschen**.

Löschen aller ausgewählten Backups von der Registerkarte „Wiederherstellen“

1 Wählen Sie auf der Registerkarte **Manuelle Wiederherstellung** die Backups aus, die aus der Liste der Backups gelöscht werden sollen. Klicken Sie dann auf **Gesamte Auswahl löschen**.

2 Klicken Sie auf **Aktualisieren**, um die Daten auf der Registerkarte **Wiederherstellen** zu aktualisieren.

Replikation 15

In diesem Kapitel werden folgende Themen behandelt:

Replikationsjobs

Durch Replikation können Sie einen Datenverlust bei einem Ausfall der VDP-Quell-Appliance vermeiden, weil Backupkopien auf dem Ziel verfügbar sind. Replikationsjobs legen fest, welche Backups repliziert sowie wann und wo die Backups repliziert werden. Bei geplant oder ad hoc durchgeführten Replikationsjobs für Clients ohne Wiederherstellungspunkte wird der Client nur auf dem Zielserver repliziert. Mit der VDP-Appliance erstellte Backups können auf eine andere VDP-Appliance, einen Avamar-Server oder ein Data Domain-System repliziert werden.

Replikationskompatibilität

In Tabelle 15-20 und Tabelle 15-21 ist angegeben, welche Backups repliziert werden können, je nachdem, welches VDP-Produkt zur Backuperstellung verwendet wurde.

Die folgenden Abkürzungen werden in diesen Tabellen verwendet:

- **VDP-A**: VDP Advanced-Appliance
- **RTI**: Replication Target Identity

WICHTIGER HINWEIS VDP Advanced gilt für VDP 5.8 und niedriger. RTI gilt nur für VDP 5.8.

- **DD**: Data Domain-System
- **N**: Nein, das Ziel wird nicht unterstützt.
- **J**: Ja, das Ziel wird unterstützt.
- **(E)**: Empfohlener
- **(NE)**: Nicht empfohlen
- **(HP)**: Hash-Passwort

Tabelle 15-20. Replikationsquellmatrix – Teil 1

Mit diesem Produkt erstellte Backups	können auf diese Ziele repliziert werden ...														
	VDP 5.1.x	VDP 5.5.1.x	VDP 5.5.5.x	VDP-A 5.5.5.x	VDP-A 5.5.5.x + DD	VDP 5.5.6.x	VDP-A 5.5.6.x	VDP-A 5.5.6.x + DD	VDP 5.8.x	VDP-A 5.8.x	VDP-A 5.8.x + DD	VDP 6.0.x	VDP 6.0.x + DD	VDP 6.1.x	VDP 6.1.x + DD
VDP 5.5.1.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
VDP 5.5.1.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
VDP 5.5.5.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
VDP-A 5.5.5.x	N	N	N	J (E)	J (E)	N	J	J	N	J (HP)	J (HP)	J (HP)	J (HP)	J (HP)	J (HP)
VDP-A 5.5.5.x + DD	N	N	N	N	J (E)	N	N	J	N	N	J (HP)	N	J (HP)	N	J (HP)
VDP 5.5.6.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
VDP-A 5.5.6.x	N	N	N	J	J	N	J	J	N	J (HP)	J (HP)	J (HP)	J (HP)	J (HP)	J (HP)
VDP-A 5.5.6.x + DD	N	N	N	N	J	N	N	J	N	N	J (HP)	N	J (HP)	N	J (HP)
VDP 5.8.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
VDP-A 5.8.x	N	N	N	J	J	N	J	J	N	J (E)	J	J (E)	J	J (E)	J
VDP-A 5.8.x + DD	N	N	N	N	J	N	N	J	N	N	J (E)	N	J (E)	N	J (E)
RTI 5.8.x	N	N	N	J	J	N	J	J	N	J (E)	J	J (E)	J	J (E)	J

Tabelle 15-20. Replikationsquellmatrix – Teil 1 (Fortsetzung)

Mit diesem Produkt erstellte Backups	können auf diese Ziele repliziert werden ...														
	VDP 5.1.x	VDP 5.5.1.x	VDP 5.5.5.x	VDP-A 5.5.5.x	VDP-A 5.5.5.x + DD	VDP 5.5.6.x	VDP-A 5.5.6.x	VDP-A 5.5.6.x + DD	VDP 5.8.x	VDP-A 5.8.x	VDP-A 5.8.x + DD	VDP 6.0.x	VDP 6.0.x + DD	VDP 6.1.x	VDP 6.1.x + DD
RTI 5.8.x + DD	N	N	N	N	J	N	N	J	N	N	J (E)	N	J (E)	N	J (E)
VDP 6.0.x	N	N	N	J	J (E)	N	J	J (E)	N	J	J (E)	J	J (E)	J	J (E)
VDP 6.0.x + DD	N	N	N	N	J	N	N	J	N	N	J	N	J	N	J
VDP 6.1.x	N	N	N	J	J (E)	N	J	J (E)	N	J	J (E)	J	J (E)	J	J (E)
VDP 6.1.x + DD	N	N	N	N	J	N	N	J	N	N	J	N	J	N	J

Tabelle 15-21. Replikationsquellmatrix – Teil 2

Mit diesem Produkt erstellte Backups	können auf diese Ziele repliziert werden ...									
	RTI 5.8.x	RTI 5.8.x + DD	VDP 6.0.x	VDP 6.0.x + DD	Avamar SP1 6.1.1.87	Avamar SP2 6.1.2.47	Avamar 7.0.0.427	Avamar 7.0.1.56	Avamar 7.1.x.x	Avamar 7.1.x.x + DD
VDP 5.1.x	N	N	N	N	N	N	N	N	N	N
VDP 5.5.1.x	N	N	N	N	J	J	J	J	J	J
VDP 5.5.5.x	N	N	N	N	J	J	J	J (E)	J	J
VDP-A 5.5.5.x	J (HP)	J	J	N	J	J	J (E)	J (E)	J	J
VDP-A 5.5.5.x + DD	N	J (HP)	N	J (HP)	J (NE)	J (NE)	J (NE)	J (NE)	J	J
VDP 5.5.6.x	N	N	N	N	J	J	J (E)	J	J	J
VDP-A 5.5.6.x	J (HP)	J (HP)	J (HP)	N	J	J	J (E)	J (E)	J	J
VDP-A 5.5.6.x + DD	N	J (HP)	N	J (HP)	J (NE)	J (NE)	J (NE)	J (NE)	J	J
VDP 5.8.x	N	N	N	N	J	J	J	J	J (E)	J
VDP-A 5.8.x	J (E)	J	J (HP)	N	J	J	J	J	J (E)	J
VDP-A 5.8.x + DD	N	J (E)	N	J (HP)	J (NE)	J (NE)	J (NE)	J	J	J
RTI 5.8.x	J (E)	J	J (HP)	N	J	J	J	J	J (E)	J
RTI 5.8.x + DD	N	J (E)	N	J (HP)	J (NE)	J (NE)	J (NE)	J (NE)	J (NE)	J (E)
VDP 6.0.x	J	J (E)	J (HP)	J (E)	J (HP)	J (HP)	J (HP)	J (HP)	J (HP)	N
VDP 6.0.x + DD	N	J	N	J (HP)	N	N	N	N	N	J (HP)

Tabelle 15-21. Replikationsquellmatrix – Teil 2

Mit diesem Produkt erstellte Backups	können auf diese Ziele repliziert werden ...									
	RTI 5.8.x	RTI 5.8.x + DD	VDP 6.0.x	VDP 6.0.x + DD	Avamar SP1 6.1.1.87	Avamar SP2 6.1.2.47	Avamar 7.0.0.427	Avamar 7.0.1.56	Avamar 7.1.x.x	Avamar 7.1.x.x + DD
VDP 6.1.x	Y	J (E)	J (HP)	J (E)	J (HP)	J (HP)	J (HP)	J (HP)	J (HP)	N
VDP 6.1.x + DD	N	J	N	J (HP)	N	N	N	N	N	J (HP)

Replikation und Data Domain

Falls die VDP-Quell-Appliance über ein Data Domain-System als Backupziel verfügt, muss die als Replikationsziel vorgesehene VDP-Appliance ebenfalls über ein Data Domain-System verfügen. Ebenso muss der Avamar-Server bei der Replikation von VDP auf einen Avamar-Server über ein Data Domain-System verfügen.

HINWEIS Data Domain Boost 2.6 sowie Data Domain 5.4.1.1 oder höher, 5.5x und 5.6 werden unterstützt.

Der Replikationsjob schlägt fehl, wenn Data Domain- und Avamar-Backupziele zu einem einzigen Replikationsjob kombiniert werden. Entweder müssen alle Data Domain-Clients oder alle Avamar-Clients als Backupziele konfiguriert werden.

Best Practices für die Replikation

- Da nur abgeschlossene Clientbackups repliziert werden, sollten Replikationen nur in Zeiträumen mit geringen Backupaktivitäten geplant werden. So wird ermöglicht, dass die größtmögliche Anzahl an Clientbackups während der Replikationssitzungen repliziert wird.
- Wenn Sie die Benutzer-ID oder das Passwort für das Root-Konto auf dem Replikationszielserver ändern, müssen Sie die Benutzer-ID und das Passwort auf dem Quellserver mit dem neuen Passwort aktualisieren.
- Über das Management von Replikationszielen können Sie die Informationen für einen oder mehrere Replikationsjobs, die mit demselben Replikationszielserver verknüpft sind, aktualisieren.
- Die Replikation von dynamischen oder nicht-statischen Daten wird nicht unterstützt. Daher müssen Sie die Replikation während einer geringen Backupaktivität durchführen.
- Mehrere Clients können nicht gleichzeitig repliziert und/oder wiederhergestellt werden, wenn gleichzeitig mehrere Backup- und/oder Wiederherstellungsvorgänge durchgeführt werden.
- Obgleich die Replikation zwischen Servern unterschiedlicher Versionen unterstützt wird, stellen Sie sicher, dass die VDP-Version auf dem Zielserver entweder gleich oder höher ist, als die VDP-Version auf dem Quell-Server.
- Beim Erstellen der Replikationsjob-Policy, optimieren Sie die Größe der Replikationsgruppe, sodass alle Clients bei jeder planmäßigen Replikation erfolgreich repliziert werden. Wenn die Gruppe sehr groß ist, nimmt die Replikation mehr Zeit in Anspruch. Daher teilen Sie die Gruppe in zwei kleinere Gruppen auf, die Sie unabhängig voneinander planen können.
- Mehrere Replikationsjobs, die Teil eines Jobs für verschiedene VMs sind, können nicht parallel ausgeführt werden. Um diese Einstellung zu ändern, fügen Sie der Datei **/usr/local/vdr/etc/vdp-options.properties** die folgende Eigenschaft zu **com.vmware.vdp.option.replicate.maxtreams**.

  Zum Beispiel: com.vmware.vdp.option.replicate.maxstreams=8

Einschränkungen

- Wird ein Replikationsjob gestartet, können nur im Ruhezustand befindliche, statische Daten verarbeitet werden, die sich auf dem Quellserver befinden. Daher werden alle Vorgänge, bei denen Daten auf den Quellserver geschrieben werden und die noch nicht vollständig abgeschlossen sind (z. B. ein laufender Backupjob), bei diesem Replikationsjob nicht berücksichtigt. Die Daten werden jedoch bei der nächsten Replikation repliziert.
- Auf der VDP-Quell-Appliance erhöht sich die zum Durchsuchen der einzelnen Clients erforderliche Zeit mit der Backupanzahl für replizierte Clients.
- Importierte Image-Backups können nicht repliziert werden.

  Für importierte Backups verschiebt der Importvorgang die Clients und Konten von ihrem aktuellen Kontopfad zu /REPLICATE/VDP_IMPORTS/. Der Name der Domain auf diesem Level enthält einen Zeitstempel, der an das Ende des Namens angehängt wird. Der Importvorgang löscht außerdem alle Jobs. Zum Replizieren dieser Backups müssen Sie replizierte Backups für den Typ und dann importierte Backups auswählen.

Festlegen von Backuptypen für einen Replikationsjob

Sie legen die Aufbewahrungs-Policy und die Backupplanung fest, wenn Sie Backups erstellen. Bedenken Sie diese Faktoren, wenn Sie die Backuptypen festlegen, die Sie für den Replikationsjob verwenden möchten.

- Aufbewahrungs-Policy. Nähere Informationen finden Sie unter „Festlegen der Aufbewahrungs-Policy" auf Seite 125.
- On-Demand-Backup oder geplante Backuptypen:
  - Falls ein beliebiger Backupjob mithilfe der Option **Jetzt sichern** ausgeführt wird, wird er als On-Demand-Backup betrachtet und keinem Backuptyp zugeordnet. Zum Replizieren dieses Backups müssen Sie den Backuptyp **Benutzerinitiiert** (Schritt 6 des Assistenten „Neuen Replikationsjob erstellen") auswählen.
  - Legen Sie zur Planung des Backups die Planungsoptionen fest (Schritt 10 des Assistenten „Neuen Replikationsjob erstellen").

Erstellen eines Replikationsjobs

Erstellen Sie Replikationsjobs über den Assistenten „Neuen Replikationsjob erstellen".

HINWEIS Clients oder Wiederherstellungspunkte, die bereits von einem anderen Quellserver repliziert wurden, sind im Assistenten „Neuen Replikationsjob erstellen" verfügbar.

Voraussetzungen

- VDP ist auf Ihrem vCenter Server-Rechner installiert und konfiguriert.
- Sie sind bei vSphere Web Client angemeldet und mit der VDP-Appliance verbunden.

Verfahren

1. Greifen Sie über einen Webbrowser auf VDP zu. Anweisungen finden Sie unter „Zugriff auf VDP" auf Seite 116.
2. Klicken Sie auf die Registerkarte **Replikation**.

Auf der Registerkarte **Replikation** wird eine Liste der erstellten Replikationsjobs angezeigt. In der folgenden Tabelle sind die Spalten und die dazugehörigen Beschreibungen aufgeführt.

Tabelle 15-22. Spaltenbeschreibungen für die Registerkarte **Replikation**

Spalte	Beschreibung
Name	Der Name des Replikationsjobs.
Status	Der Status des Replikationsjobs.
Ziel	Der Speicherort, an dem die Clientbackups repliziert werden.
Letzte Ausführungszeit	Der letzte Zeitpunkt, zu dem der Replikationsjob ausgeführt wurde.
Dauer	Die Dauer bis zum Replikationsabschluss bei der letzten Jobausführung.
Nächste Ausführungszeit	Der Zeitpunkt, zu dem der Replikationsjob für eine weitere Ausführung geplant ist.
Anzahl Clients	Die Anzahl der Clients, deren Backups im Job geschützt und repliziert werden. Dieser Wert wird nur geändert, wenn der Benutzer mithilfe der Funktion „Bearbeiten“ Clients hinzufügt oder aus einem Replikationsjob entfernt.

3 Wählen Sie im Menü **Replikationsjobaktionen** die Option **Neu** aus, um den Assistenten „Neuen Replikationsjob erstellen“ zu starten.

4 Legen Sie auf der Seite „Typ auswählen“ fest, ob Gast-Images (lokale Backups) oder replizierte Backups repliziert werden sollen. Klicken Sie dann auf **Weiter**.

Die Seite „Typ auswählen“ wird angezeigt. Auf dieser Seite werden die entsprechenden Clients basierend auf dem von Ihnen ausgewählten Replikationstyp angezeigt.

Beim Typ „Replizierte Backups“:

- Die VDP-Appliance zeigt replizierte Backups und wiederhergestellte Backupclients als Optionen für die Replikation auf einen anderen Zielserver an.
- In der Clienttabelle wird der Quellpfad in der Spalte „Quellpfad“ und nicht unter „Letzter bekannter Pfad“ angezeigt.

HINWEIS Es sind sowohl Gast-Images als auch Optionen für Anwendungsbackups verfügbar.

5 Führen Sie auf der Seite Clients auswählen eine der folgenden Aufgaben aus:

- Um alle Clientbackups zu replizieren, klicken Sie auf **Alle Clients** und dann auf **Weiter**.
- Um Backups nur von bestimmten Clients zu replizieren, klicken Sie auf **Clients einzeln auswählen** und wählen Sie dann den Typ aus der Liste **Typ** aus. Zu den Optionen gehören Image, MS SQL Server, MS Exchange Server und MS SharePoint Server.

HINWEIS Sowohl reguläre als auch außer Betrieb genommene VM-Backups werden für die Replikation unterstützt. Wenn eine außer Betrieb genommene virtuelle Maschine wieder als reguläre virtuelle Maschine hinzugefügt wird, wird die virtuelle Maschine zweimal unter demselben Namen in der Systemliste aufgeführt. An den Namen der stillgelegten virtuellen Maschine ist ein Suffix angehängt. Achten Sie also bei der Auswahl der Clients darauf, die reguläre virtuelle Maschine ohne Suffix auszuwählen.

Bei Aktivierung der Option **Clients einzeln auswählen** können Sie einen oder mehrere Clients auswählen. Falls gewünscht, lassen sich die Clients vor der Auswahl filtern. So filtern Sie Clients:

a Klicken Sie neben **Filter** auf **Alle anzeigen** und wählen Sie dann **Client** aus.

Um nach Clientnamen zu filtern, wählen Sie **Name** aus. Die folgenden Informationen werden für vCenter Client angezeigt.

- **Name:** Mit den Filtern „Ist“, „Ist nicht“, „Enthält“ oder „Enthält nicht“ kann der Clientname abgerufen werden.

- **Status:** Mögliche Werte sind „Eingeschaltet“, „Ausgeschaltet“, „Unterbrochen“, „Aktiviert“ oder „Nicht aktiviert“.
- **Clienttyp**: Der Clienttyp

b Klicken Sie auf **Weiter**.

Die Seite **Backupauswahl** wird angezeigt. Auf dieser Seite können Sie die Anzahl der bei der Jobausführung replizierten Backups begrenzen. Ohne Auswahl von Backupoptionen werden alle Backups für die ausgewählten virtuellen Maschinen repliziert.

6 Gehen Sie auf der Seite **Backupauswahl** des Assistenten **Neuen Replikationsjob erstellen** wie folgt vor:

a Wählen Sie einen **Backuptyp** aus:

Täglich: Es werden ausschließlich tägliche Backups repliziert.

Wöchentlich: Es werden einmal ausschließlich wöchentliche Backups repliziert.

Monatlich: Es werden ausschließlich monatliche Backups repliziert.

Jährlich: Es werden ausschließlich jährliche Backups repliziert.

Benutzerinitiiert: Es werden ausschließlich vom Benutzer initiierte Backups repliziert.

HINWEIS Bei benutzerinitiierten Backups bleiben erweiterte Aufbewahrungsoptionen nicht erhalten. Diese Backups müssen als separater Backuptyp gekennzeichnet werden.

b Wählen Sie eine Einstellung für **Maximal pro Client zu replizierende Backups** aus:

Keine Begrenzung: Ist diese Option ausgewählt, werden alle vorhandenen Backups für einen Client repliziert, der das Kriterium **Backuptyp** erfüllt. Die Anzahl an Backups ist unbegrenzt.

Anzahl an Backups: Ist diese Option ausgewählt, folgen die zu replizierenden Backups einer chronologischen Reihenfolge. Unabhängig davon, ob es sich um ein On-Demand-Backup oder ein geplantes Backup handelt, wird das letzte Backup ausgewählt. Die maximale Anzahl von Backups beträgt 999.

c Legen Sie die **Datenbeschränkungen** fest:

Ohne: Alle Backups, die die Kriterien **Backuptyp** und **Maximal pro Client zu replizierende Backups** erfüllen, werden repliziert. Es gibt keine anderen Einschränkungen.

Letzte: Wählen Sie eine Zahl und eine Zeiteinheit aus. Diese Option schränkt die Auswahl von Backups ein, indem nur Backups eingeschlossen werden, die während der festgelegten Anzahl an Tagen, Wochen, Monaten oder Jahren erstellt wurden.

Nach Bereich: Wählen Sie unter **Von** und **Bis** jeweils ein Datum und eine Uhrzeit aus. Sie können dies ab einem bestimmten Datum, bis zu einem Datum oder zwischen zwei Daten festlegen.

d Klicken Sie auf **Weiter**.

Die Seite **Destination** wird angezeigt. Auf dieser Seite werden Verbindungsinformationen für das Ziel angegeben, auf dem die Clientbackups repliziert werden.

Sie können einen Avamar-Server als Replikationsziel verwenden. Geben Sie hierzu auf der Seite „Ziel“ die IP-Adresse, den Port sowie die Anmeldedaten für den Avamar-Server an.

HINWEIS Wenn Sie den Namen des VM-Clients ändern, wird der umbenannte Client in VDP in der Spalte „Name“ des Assistenten „Neuen Replikationsjob erstellen“ angezeigt. Bei Replikation eines umbenannten VM-Clients mit einem Avamar-Server oder Avamar Virtual Edition (AVE) als Ziel wird der geänderte Name nicht in Avamar widergespiegelt. Auf dem Avamar-Server wird der ältere Name angezeigt, der schon vor der Namensänderung registriert wurde. Dies ist ein bekanntes Problem.

7 Geben Sie auf der Seite **Ziel** des Assistenten „Neuen Replikationsjob erstellen“ die folgenden Informationen an:

HINWEIS Alle Referenzen zum **Ziel** beziehen sich entweder auf den Avamar-Server oder die VDP-Appliance, auf die die Backupdaten repliziert werden.

- **Hostname oder IP**: Der Hostname oder die IP-Adresse des Ziels
- Port**:** Die Portnummer, über die VDP mit dem Ziel kommuniziert. Der Standardwert lautet 29000. Dabei handelt es sich um den Standardport für SSL-verschlüsselte Replikationen.
- **Benutzername**: Der zum Anmelden beim Ziel verwendete Benutzername
- **Passwort**: Das zum Anmelden beim Ziel verwendete Passwort
- **Pfad:** Der eindeutige Name, der die Domain identifiziert und für mehrmandantenfähige Konfigurationen verwendet wird. Details zur mehrmandantenfähigen Konfiguration finden Sie unter „Mehrmandantenfähigkeit" auf Seite 164.

Zur Replikation und Wiederherstellung replizierter Backups verwenden Sie den Benutzernamen **repluser**. Die Anmeldedaten des Benutzernamens **repluser** werden mit dem Root-Benutzer synchron gehalten.

8 Klicken Sie auf **Authentifizierung überprüfen**, um die Verbindung zwischen VDP und dem Ziel zu testen.

9 Klicken Sie auf **Weiter**.

Die Seite **Schedule** wird angezeigt. Auf dieser Seite wird angegeben, wie häufig und zu welcher Tageszeit Backups repliziert werden.

10 Gehen Sie auf der Seite **Planung** des Assistenten „Neuen Replikationsjob erstellen" wie folgt vor:

a Wählen Sie eine der folgenden Planungsoptionen:

- **Täglich**: Wählen Sie diese Option aus, damit die Backups jeden Tag repliziert werden.
- **Wöchentlich am**: Wählen Sie diese Option aus, um einen Tag festzulegen, an dem die Backups jede Woche repliziert werden.
- **Am ... jedes Monats:** Wählen Sie diese Option aus, um eine Zahl und einen Tag festzulegen, an dem die Backups jeden Monat repliziert werden.

b Wählen Sie **Startzeit auf Server** aus, um den Zeitpunkt für die Replikation am geplanten Tag anzugeben.

Best Practice: Da nur abgeschlossene Clientbackups repliziert werden, sollten Replikationen nur in Zeiträumen mit geringen Backupaktivitäten geplant werden. So wird ermöglicht, dass die größtmögliche Anzahl an Clientbackups während der Replikationssitzungen repliziert wird.

c Klicken Sie auf **Weiter**.

Die Seite „Aufbewahrung" wird angezeigt. Auf dieser Seite wird angegeben, wann replizierte Backups auf dem Zielrechner ablaufen.

11 Gehen Sie auf der Seite **Aufbewahrung** des Assistenten „Neuen Replikationsjob erstellen" wie folgt vor:

a Um das aktuelle Ablaufdatum der einzelnen Backups zu verwenden, wählen Sie **Aktuellen Ablauf für alle Backups beibehalten** aus.

b Um die Ablaufdaten auf Grundlage des Backuptyps festzulegen, wählen Sie **Ablauf nach Backuptyp festlegen** und für jeden Typ die gewünschte Zahl von Tagen, Wochen, Monaten oder Jahren aus.

c Um den Replikationsjob auf unbestimmte Zeit aufzubewahren, wählen Sie **Immer beibehalten** aus.

d Klicken Sie auf **Weiter**.

Die Seite „Name" wird angezeigt. Auf dieser Seite wird der Replikationsjob benannt.

12 Gehen Sie auf der Seite **Name** des Assistenten „Neuen Replikationsjob erstellen" wie folgt vor:

a Geben Sie einen Namen für den Replikationsjob ein.

Der Name des Replikationsjobs muss eindeutig sein und darf bis zu 255 Zeichen umfassen. Die folgenden Zeichen sind für den Jobnamen nicht zulässig: ~!@$^%(){}[]|,`;#\/:*?<>'"&. Zudem dürfen keine diakritischen Zeichen verwendet werden (z. B. â, é, ì, ü und ñ).

b Klicken Sie auf **Weiter**.

Die Seite „Bereit zur Fertigstellung“ wird angezeigt. Auf dieser Seite kann vor dem Speichern eine Zusammenfassung des Replikationsjobs, den Sie erstellen, überprüft werden.

13 Gehen Sie auf der Seite **Bereit zur Fertigstellung** des Assistenten „Neuen Replikationsjob erstellen“ wie folgt vor:

a Überprüfen Sie die Informationen.

b Klicken Sie auf **Fertig stellen**, um den Job zu erstellen.

Managen von Zielen

Sie können vorhandene Replikationsjobs über die Registerkarte **Replikation** auswählen und dann mithilfe des drei Schritte umfassenden Assistenten „Ziel managen“ die zielbezogenen Verbindungsinformationen für all diese Jobs ändern.

Best Practice

Alle Replikationsjobs, die mit demselben spezifischen Replikationszielserver verknüpft sind, sollten aktualisiert werden, statt eine Kombination von Replikationsjobs mit verschiedenen Zielservern auszuwählen.

Verfahren

1 Greifen Sie über einen Webbrowser auf VDP zu. Anweisungen finden Sie unter „Zugriff auf VDP“ auf Seite 116.

2 Klicken Sie auf die Registerkarte **Replikation**.

Auf der Registerkarte **Replikation** wird eine Liste der erstellten Replikationsjobs angezeigt.

3 Markieren Sie den Replikationsjob und wählen Sie **Replikationsjobaktionen > Ziel managen** aus.

Der Assistent „Ziel managen“ wird angezeigt.

4 Klicken Sie auf der Seite „Replikationsjobs“ auf den Replikationsjob, um das mit diesem verknüpfte Ziel zu aktualisieren. Klicken Sie dann auf **Weiter**. Sie können mehrere Jobs auswählen.

5 Geben Sie auf der Seite **Ziel** des Assistenten „Ziel managen“ die folgenden Informationen an:

HINWEIS Alle Referenzen zum **Ziel** beziehen sich entweder auf den Avamar-Server oder die VDP-Appliance, auf die die Backupdaten repliziert werden.

- **Hostname oder IP**: Der Hostname oder die IP-Adresse des Ziels
- Port**:** Die Portnummer, über die VDP mit dem Ziel kommuniziert. Es ist ausschließlich der Port 29000 zulässig. Diese Port ist der Standardport für SSL-verschlüsselte Replikationen.
- **Benutzername**: Der zum Anmelden beim Ziel verwendete Benutzername
- **Passwort**: Das zum Anmelden beim Ziel verwendete Passwort
- **Pfad:** Der eindeutige Namen, der die Domain identifiziert. Dieses Feld wird für mehrmandantenfähige Konfigurationen verwendet. Details zur mehrmandantenfähigen Konfiguration finden Sie unter „Mehrmandantenfähigkeit“ auf Seite 164.

Zur Replikation und Wiederherstellung replizierter Backups verwenden Sie den Benutzernamen **repluser**. Die Anmeldedaten des Benutzernamens **repluser** werden mit dem Root-Benutzer synchron gehalten.

6 Klicken Sie auf **Authentifizierung überprüfen**, um die Verbindung zwischen VDP und dem Ziel zu testen.

7 Klicken Sie auf **Weiter**.

8 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung“ das Ziel, das den ausgewählten Replikationsjobs zugewiesen wird. Klicken Sie auf **Fertig stellen**, um den Replikationsjob zu aktualisieren, oder auf **Zurück**, um Änderungen vorzunehmen.

Bearbeiten eines Replikationsjobs

Sie können einen Replikationsjob bearbeiten, indem Sie ihn markieren und **Replikationsjobaktionen** > **Bearbeiten** auswählen.

Klonen eines Replikationsjobs

Sie können einen Replikationsjob als Vorlage für die Erstellung eines anderen Jobs verwenden. Markieren Sie hierzu den Replikationsjob und wählen Sie **Replikationsjobaktionen** > **Klonen** aus.

Durch die Durchführung des Cloningvorgangs wird der Assistent zum Klonen von Replikationsjobs gestartet. Außerdem werden die Informationen aus dem ursprünglichen Job zum automatischen Auffüllen verwendet. Für den geklonten Job ist ein eindeutiger Name erforderlich. Sie können beliebige aus dem ursprünglichen Job kopierte Einstellungen ändern.

Löschen eines Replikationsjobs

Sie können einen Replikationsjob löschen, indem Sie ihn markieren und **Replikationsjobaktionen** > **Löschen** auswählen.

HINWEIS Sie können mehrere Replikationsjobs zum Löschen auswählen. Durch Löschen eines Replikationsjobs wird die Anzahl der mit einem bestimmten Replikationsziel verbundenen Replikationsjobs verringert. Wenn die Replikationsjobs, die gelöscht werden, zu Replikationszielen ohne verbundene Replikationsjobs führen, erhalten Sie die Möglichkeit, die Replikationsziele als Teil der Löschanforderung zu entfernen.

Aktivieren oder Deaktivieren eines Replikationsjobs

Wenn ein Replikationsjob vorübergehend nicht mehr ausgeführt werden soll, können Sie ihn deaktivieren. Sie können deaktivierte Replikationsjobs bearbeiten und löschen. Mit VDP können deaktivierte Jobs erst nach ihrer Aktivierung ausgeführt werden.

Replikationsjobs können durch Markierung des Replikationsjobs und Auswahl von **Replikationsjobaktionen** > **Aktivieren/Deaktivieren** aktiviert bzw. deaktiviert werden.

Anzeigen von Status- und Replikationsjobdetails

Auf der Registerkarte **Replikation** wird eine Liste der mit VDP erstellten Replikationsjobs angezeigt. Die Details zum Replikationsjob können durch Klicken auf den Job aufgerufen werden. Die Details werden im Fenster „Replikationsjobdetails“ angezeigt:

- **Name:** Der Name des Replikationsjobs.
- **Status:** Der Status des Replikationsjobs.
- **Ziel:** Replikationsort der im Job angegebenen Backups
- **Clients:** Eine Liste der Clients, deren Backups vom Job repliziert werden
- **Letzte Ausführungszeit:** Der letzte Zeitpunkt, zu dem der Replikationsjob ausgeführt wurde.
- **Dauer**: Die Dauer bis zum Replikationsabschluss bei der letzten Jobausführung.
- **Nächste Ausführungszeit:** Das Datum und die Uhrzeit der nächsten geplanten Jobausführung

Sofortiges Ausführen von vorhandenen Replikationsjobs

Es ist möglich, einen Replikationsjob sofort auszuführen, indem Sie den Job markieren und auf **Jetzt replizieren** klicken.

Replikation zurück auf die Quelle

Ein Replikationsjob kann so konfiguriert werden, dass Backupdaten von einer VDP-Appliance auf eine andere VDP-Appliance repliziert werden.

Node-Struktur für wiederhergestellte Backups

Wenn eine gültige Recovery-Aktion mithilfe des Quellservers erstmalig initiiert wird, erstellt die Recovery-Aktion den Quellserver-Node unter dem Link /REPLICATE. Alle wiederhergestellten Backups werden auf der Registerkarte **Wiederherstellen** der VDP-Quell-Appliance unter diesem Link /REPLICATE angezeigt.

Im Anschluss an eine erfolgreiche Replikation von der VDP-Quell-Appliance auf einen Replikationszielserver wird der vollständig qualifizierte Domainname bei einer Recovery vom Replikationsquellserver für die auf einem Zielserver befindlichen replizierten Backups unter dem Link /REPLICATE auf der Registerkarte **Wiederherstellen** angezeigt. Wiederhergestellte Backups geben nicht den vollständig qualifizierten Domainnamen des Zielservers wieder, anhand dessen die Wiederherstellung erfolgt ist.

Node-Struktur erneut replizierter Backups

Wenn ein Benutzer ein repliziertes Backup repliziert, wird der Replikationsquell-Node nicht unter dem Link /REPLICATE auf dem Replikationszielserver angezeigt.

Nach einer erfolgreichen Replikation replizierter Backups werden auf der Registerkarte **Wiederherstellen** des nachfolgenden Zielservers Informationen zum übergeordneten Quellserver (auf dem Quellserver, auf dem die virtuelle Maschine ursprünglich gesichert wurde) unter dem Link /REPLICATE auf der Registerkarte **Wiederherstellen** angezeigt.

Im Anschluss an eine erfolgreiche Replikation replizierter Backups von Server B auf Server C (wo die virtuelle Maschine ursprünglich mithilfe von Server A gesichert wurde) werden auf der Registerkarte **Wiederherstellen** der VDP-Appliance von Server C die Informationen zu Server A unter dem Link /REPLICATE angezeigt. Es werden also keine Informationen für den tatsächlichen Replikationsquellserver B dargestellt.

Replikationsziele

Es folgen Beispiele für Fälle, in denen ein Replikationsziel erforderlich ist:

- Ein Backup, das auf der lokalen VDP-Appliance vorhanden ist, wird auf ein Remotereplikationsziel repliziert. Das Backup wird dann von der lokalen Appliance entfernt oder gelöscht. Mit der Funktion zur **Replikation zurück auf die Quelle** können Sie die Backups durchsuchen, die sich auf einem Remoteziel befinden. Außerdem können Sie bestimmte Backups wiederherstellen, indem Sie sie zurück auf die lokale Appliance kopieren. Nachdem für das Backup eine Recovery auf der lokalen Appliance durchgeführt wurde, kann es mit dem üblichen Prozess wiederhergestellt werden.
- Es muss eine neue VDP-Appliance installiert werden, um eine beschädigte VDP zu ersetzen. Für bestimmte Backups, die bereits auf ein Replikationsziel repliziert wurden, muss eine Recovery durchgeführt werden. Mit der Funktion zur **Replikation zurück auf die Quelle** können Sie eine Verbindung zu einem Replikationsziel herstellen, die dort vorhandenen Backups durchsuchen und eine Recovery für bestimmte Backups durchführen, indem Sie sie zurück auf die lokale Appliance kopieren. Nachdem für das Backup eine Recovery auf der neuen VDP-Appliance durchgeführt wurde, kann es mit dem üblichen Prozess wiederhergestellt werden.

HINWEIS Der Recovery-Assistent ist auf dem Avamar-Server nicht verfügbar. Eine Replikation zurück zur Quelle ist auf dem Avamar-Server nicht möglich.

Replikations-Recovery-Kompatibilität

In Tabelle 15-23 sind die unterstützten Replikations-Recovery-Ziel- und Replikations-Recovery-Quellserver aufgeführt.

Tabelle 15-23. Kompatibilitätsmatrix für Replikations-Recoveries

Replikations-Recovery-Ziel (Recovery von)	Replikations-Recovery-Quelle (Recovery nach)				
	VDP 5.8	VDP Advanced 5.8	VDP Advanced 5.8 Target Identity	VDP 6.0	VDP 6.1
VDP 5.8.0.x	Nein	Nein	Nein	Ja	Ja
VDP Advanced 5.8.0.x	Nein	Ja	Ja	Ja	Ja
VDP Replication Target Identity 5.8.0.x	Nein	Ja	Ja	Ja	Ja
VDP 5.5.1.356	Nein	Nein	Nein	Nein	Nein
VDP 5.5.5.180	Nein	Nein	Nein	Nein	Nein
VDP Advanced 5.5.5.180	Nein	Ja	Ja	Ja	Ja
VDP 5.5.6.56	Nein	Nein	Nein	Nein	Nein
VDP Advanced 5.5.6.56	Nein	Ja	Ja	Ja	Ja
Avamar Server 7.0.x	Ja	Ja	Ja	Ja	Ja
Avamar Virtual Edition (AVE) 6.0.x	Ja	Ja	Ja	Ja	Ja
Avamar Server/AVE 7.1.x	Ja	Ja	Ja	Ja	Ja
AVE 7.2.x	Ja	Ja	Ja	Ja	Ja
VDP 6.0	Nein	Ja	Ja	Ja	Ja
VDP 6.1	Nein	Ja	Ja	Ja	Ja

WICHTIGER HINWEIS VDP Advanced gilt für die Versionen 5.8 und niedriger. Replication Target Identity gilt nur für VDP 5.8.

Aktivieren oder Deaktivieren der Replikations-Recovery

Bei VDP der Version 5.5 und höher wird der Port 29000 verwendet, wenn von einer VDP-Appliance auf ein Replikationsziel wie ein Avamar-Speicherserver- oder Data Domain-System repliziert wird.

Um die Funktion zur Replikations-Recovery zu aktivieren, muss der Port 29000 auf dem Replikationsquellserver offen sein. Durch Öffnen des Ports 29000 sind replizierte Backups auf dem Replikationsziel zulässig. Wenn der Port 29000 geschlossen ist, wird die Replikations-Recovery deaktiviert und Sie sind nicht in der Lage, das Ziel als gültiges Replikations-Recovery-Ziel zu verifizieren.

Standardmäßig ist auf einer VDP-Appliance der Port 29000 offen. Verfahren zum Öffnen und Schließen des Ports 29000 finden Sie in der Dokumentation standardmäßiger Linux-Server.

Replikations-Recovery

Auf einer neu installierten VDP-Version können Sie mit dem Assistenten „Neuen Replikationsjob erstellen“ ein Ziel festlegen (eine Maschine, auf die die Backups repliziert wurden). Nach dem Hinzufügen des Ziels können Sie für beliebige replizierte Backups eine Recovery oder Wiederherstellung durchführen.

HINWEIS Bei der aktuellen Implementierung der Replikations-Recovery wird im Fall einer Umbenennung eines VM-Clients auf der lokalen VDP-Appliance diese Namensänderung nicht auf Backups auf einer als Replikationsziel verwendeten VDP Advanced-Remote-Appliance weiterverteilt. Der neue VM-Name wird zwar bei den lokalen Wiederherstellungspunkten widergespiegelt, aber nicht am Ziel.

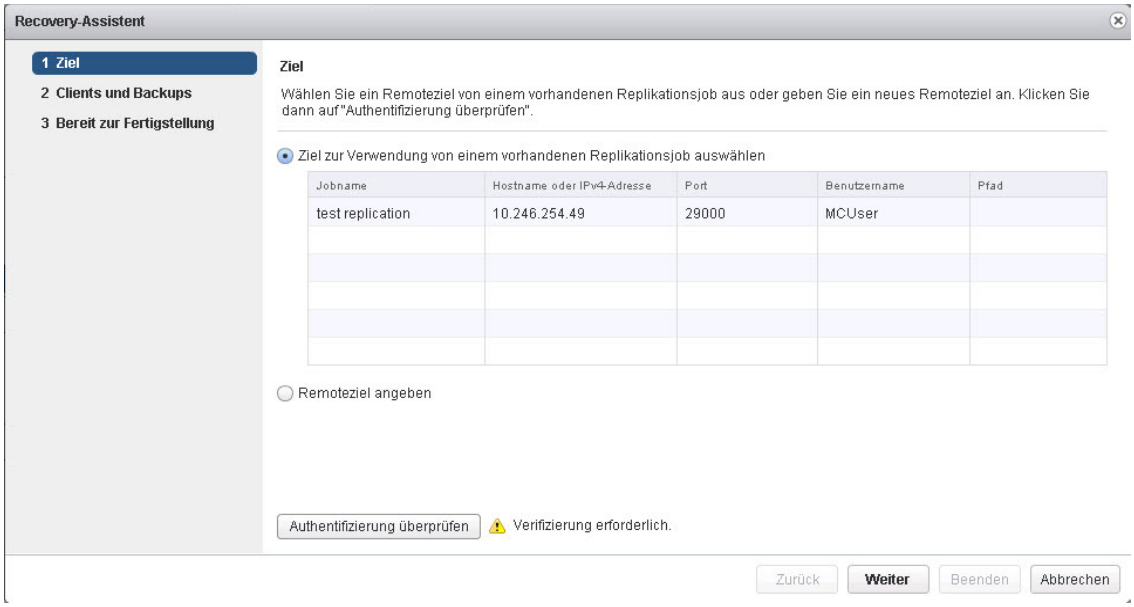
Die Option zur **Auswahl eines Replikationsziels** ist nach einer vCenter Server-Änderung deaktiviert und wird erst dann wieder aktiviert, wenn ein neuer Replikationsjob im Anschluss an die vCenter Server-Änderung erstellt wurde.

1 Greifen Sie über einen Webbrowser auf VDP zu. Anweisungen finden Sie unter „Zugriff auf VDP" auf Seite 116.

2 Klicken Sie auf die Registerkarte **Wiederherstellen**.

3 Klicken Sie auf der Registerkarte **Wiederherstellen** auf **Replizierte Backups wiederherstellen**.

Der Recovery-Assistent wird angezeigt.



4 Wählen Sie auf der Seite „Ziel" eine der folgenden Optionen aus:

- **Ziel zur Verwendung von einem vorhandenen Replikationsjob auswählen**
- **Remoteziel angeben**

5 Klicken Sie auf **Authentifizierung überprüfen**.

6 Wählen Sie auf der Seite „Clients und Backups" einen Remoteclient und Backups aus, für die eine Recovery zurück auf diese Appliance durchgeführt werden soll. Ein Client lässt sich einblenden, indem Sie auf den Pfeil klicken und so die zugehörigen Backups anzeigen.

7 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung" die wiederherzustellenden Elemente.

8 Klicken Sie auf **Fertig stellen**, um die Recovery-Anforderung zu starten, oder auf **Zurück**, um zum vorherigen Bildschirm zurückkehren, sofern Änderungen erforderlich sind.

Mehrmandantenfähigkeit

In VDP wird die Mehrmandantenfähigkeit unterstützt, sodass auf einer einzigen VDP-Appliance separate Konten für mehrere Kunden oder Organisationen vorhanden sein können. Jeder Kunde oder jede Organisation kann auf die VDP-Appliance replizieren und über die Funktion für die Replikations-Recovery auf die eigenen replizierten Daten zugreifen. Auf die replizierten Daten für einen bestimmten Kunden bzw. eine bestimmte Organisation kann nur über die Kontoanmeldedaten des jeweiligen Kunden bzw. der jeweiligen Organisation zugegriffen werden. Integrierte Anmeldedaten mit vollständigen Berechtigungen wie „root" und „repluser" haben Zugriff auf alle replizierte Daten. Diese Anmeldedaten sollten nicht an einzelne Kunden oder Organisationen weitergegeben werden. Die replizierten Daten für ein Konto werden von den replizierten Daten für alle anderen Konten isoliert.

VDP, VDP Replication Target (nur in VDP 5.8 verfügbar), Avamar (Version 7.1 oder höher empfohlen) und Avamar Virtual Edition (Version 7.1 oder höher empfohlen) sind unterstützte Ziele in Bezug auf die Mehrmandantenfähigkeit.

Sie können mehrmandantenfähige Konten erstellen, indem Sie das Skript `create_av_domain.rb` verwenden, das auf allen VDP-Appliances verfügbar ist. Das Skript `create_av_domain.rb` definiert die folgenden Parameter:

```
Verwendung: create_av_domain.rb

-c, --company=<Unternehmensname>        (erforderlich)
-d, --department=<Abteilungsname>       (optional)
-u, --username=<Benutzername>           (erforderlich)
-p, --password=<Benutzerpasswort>       (erforderlich)
-h, --help
```

Der Wert „company“ sollte den Namen der Firma oder Organisation des Kunden enthalten. Der optionale Wert „department“ ermöglicht die Einrichtung mehrerer Konten, für die derselbe company-Wert verwendet wird. Die department-Werte sind dabei aber jeweils eindeutig. Ein Konto besteht aus der Kombination der Werte „company“ und „department“. Jedes Konto besitzt einen eigenen isolierten Bucket, der replizierte Daten aufnehmen kann. Die Parameter „username“ und „password“ definieren die Anmeldedaten für den Zugriff auf ein Konto. Um für ein einziges Konto mehr als einen Satz an Zugriffsanmeldedaten zu erstellen, können Sie das Skript `create_av_domain.rb` mehrfach mit identischen Werten für „company“ und „department“, aber unterschiedlichen Werten für „username“ und „password“ ausführen.

Befolgen Sie diese Schritte, um das Skript `create_av_domain.rb` auszuführen:

1 Melden Sie sich (per ssh) beim Replikationszielserver als Admin-Benutzer an.

2 Führen Sie den folgenden Befehl aus und geben Sie das Root-Passwort an:

su – root

3 Wechseln Sie in das folgende Verzeichnis:

cd /usr/local/vdr/configure/bin

4 Führen Sie den folgenden Befehl aus und geben Sie entsprechende Werte für das Konto an, das erstellt wird:

./create_av_domain.rb --company=<*Unternehmensname*> **--department=**<*Abteilungsname*> **--username=**<*Benutzername*> **--password=**<*Benutzerpasswort*>

Beispiel:

./create_av_domain.rb --company=Acme--department=Marketing --username=fred --password=topsecret

Nachdem Sie das Konto erstellt haben, geben Sie die Kontoinformationen ein, wenn Sie ein Replikationsziel auf der VDP-Appliance definieren. Für die Seite „Replikationsziel“ sind ein Hostname oder eine IP-Adresse für das Remoteziel, die Benutzeranmeldedaten (Benutzername und Passwort) sowie ein Pfadwert erforderlich. Bei dem Pfadwert handelt es sich um die Konto-ID, die aus den beim Einrichten des Kontos mit dem Skript `create_av_domain.rb` angegebenen Werten „company“ und „department“ besteht. Die Werte „company“ und „department“ sind durch einen einzigen Schrägstrich voneinander getrennt. Im Beispiel oben lautet der Pfadwert **Acme/Marketing**.

Verwenden der Wiederherstellung auf Dateiebene 16

In diesem Kapitel werden folgende Themen behandelt:

Einführung zum VDP-Wiederherstellungsclient

VDP erstellt Backups gesamter virtueller Maschinen. Diese Backups können mithilfe der VDP-Benutzeroberfläche über vSphere Web Client in Gänze wiederhergestellt werden. Wenn jedoch nur bestimmte Dateien von diesen virtuellen Maschinen wiederhergestellt werden sollen, verwenden Sie den Wiederherstellungsclient für VDP (Zugriff über einen Webbrowser). Dies wird als Wiederherstellung auf Dateiebene bezeichnet.

Der Wiederherstellungsclient ermöglicht es, bestimmte VM-Backups als Dateisysteme zu mounten und anschließend das Dateisystem nach den wiederherzustellenden Dateien zu durchsuchen.

Der Service „Wiederherstellungsclient“ ist nur für die virtuellen Maschinen verfügbar, deren Backups von VDP gemanagt werden. Dazu müssen Sie entweder über die vCenter-Konsole oder eine andere Remoteverbindung bei einer der von VDP gesicherten virtuellen Maschinen angemeldet sein.

HINWEIS Nehmen Sie zur Durchführung einer Recovery auf Dateiebene mit den Wiederherstellungspunkten, die von einer zuvor verwendeten VDP-Festplatte importiert wurden, mindestens ein VM-Backup unter Verwendung des neuen VDP vor.

ACHTUNG Informationen zu den von vSphere 6.0 unterstützten Webbrowsern finden Sie unter „Softwareanforderungen“ auf Seite 22. Internet Explorer 10 wird nicht unterstützt und führt beim Wiederherstellungsclient zu unzuverlässigen Ergebnissen.

LVM- und EXT-Unterstützung

Folgendes ist bei der Erwägung von durch Logical Volume Manager (LVM) gemanagten logischen Volumes und EXT-Dateisystemen zu bedenken:

- Ein physisches Volume (.vmdk) muss genau einem logischen Volume zugeordnet sein.
- Es werden ausschließlich ext2- und ext3-Formatierungen (primäre Partition mit Master Boot Record (MBR) und eigenständige Partition ohne MBR) unterstützt.
- LVM und ext4 werden nur mit einem externen Proxy unterstützt.

Einschränkungen bei der Wiederherstellung auf Dateiebene

Für FLR gelten folgende Beschränkungen:

- VMware Tools muss auf der virtuellen Zielmaschine installiert sein. Vergewissern Sie sich, dass auf allen virtuellen Maschinen die neueste VMware Tools-Version ausgeführt wird, um für optimale Ergebnisse zu sorgen. Ältere Versionen verursachen bekanntermaßen Fehler, wenn während der Wiederherstellung auf Dateiebene ein Suchvorgang durchgeführt wird.
- Sie können die symbolischen Links nicht durchsuchen oder wiederherstellen.
- Das Durchsuchen eines bestimmten Verzeichnisses innerhalb eines Backup- oder Wiederherstellungsziels ist auf insgesamt 5.000 Dateien bzw. Ordner beschränkt.
- Es ist nicht möglich, innerhalb desselben Wiederherstellungsvorgangs mehr als 5.000 Ordner oder Dateien wiederherzustellen.
- Beim Erstellen von Partitionen müssen zunächst die Indexe niedrigerer Ordnung aufgefüllt werden. Sie können keine einzelne Partition erstellen und diese in den Partitionsindex 2, 3 oder 4 platzieren. Sie müssen die Partition in den Partitionsindex 1 platzieren.
- Eine Recovery auf Dateilevel ist nicht möglich, wenn sich die VM hinter NAT (Network Address Translation) befindet.
- Wenn die Netzwerk-Appliance NAT verwendet und den gesamten VDP-Datenverkehr über einen Proxy oder eine Firewall sendet, zeigt die Recovery auf Dateilevel in einer Fehlermeldung an, dass der Client in VDP nicht gefunden werden kann.

- Die Recovery auf Dateilevel schlägt fehl, wenn Sie eine ältere Version von VMware-Tools verwenden. Stellen Sie sicher, dass Sie die neueste Version von VMware-Tools auf den virtuellen Zielmaschinen installieren.
- ACLs können nicht wiederhergestellt werden.
- Sie können sich nicht beim Wiederherstellungsclient auf einer virtuellen Maschine anmelden, wenn die virtuelle Maschine aus einem Backup wiederhergestellt wurde. Die Authentifizierung schlägt fehl, da die UUID (Universal Unique Identifier) der wiederhergestellten virtuellen Maschine unterschiedlich ist.

  Workaround: Sichern Sie die neue virtuelle Maschine und melden Sie sich über den Modus **Erweiterte Anmeldung** beim Wiederherstellungsclient an. „Erweiterte Anmeldung" auf Seite 170 bietet Informationen dazu.
- Eine Recovery auf Dateilevel ist nicht möglich für Novell NSS-Volumes.

Nicht unterstützte VMDK-Konfigurationen

Bei der Recovery auf Dateiebene werden die folgenden virtuellen Laufwerkskonfigurationen (VMDK) nicht unterstützt:

- Unformatierte Festplatten
- Dynamische Festplatten (Windows)
- GPT-Festplatten (GUID Partition Table)
- Erweiterte Partitionen (Typen: 05h, 0Fh, 85h, C5h, D5h)
- Virtuelle Laufwerke mit mehr als einer Partition
- Zwei oder mehr einer Partition zugeordnete virtuelle Laufwerke
- Verschlüsselte Ordner oder Dateien
- SCSI-Festplatten werden nur unterstützt, wenn Dateien oder Ordner auf der ursprünglichen virtuellen Maschine wiederhergestellt werden.
- Null-Byte-Dateien
- Komprimierte Partitionen

HINWEIS In einigen Fällen (insbesondere bei erweiterten Partitionen) können Sie das komplette Backup-Image auf einer temporären virtuellen Maschine wiederherstellen und anschließend ausgewählte Ordner oder Dateien nach Bedarf kopieren.

Nicht unterstützte Windows-Konfigurationen

Die Recovery auf Dateiebene bietet keine Unterstützung für die folgenden Windows 8- und Windows Server 2012-Konfigurationen:

- Deduplicated New Technology File System (NTFS)
- Resilient File System (ReFS)
- Extensible Firmware Interface (EFI) Boot Loader

Anmelden beim Wiederherstellungsclient

Der Wiederherstellungsclient wird im Modus „Standard" oder „Erweitert" betrieben. Dateien eines Windows-Backups lassen sich nur auf einem Windows-Rechner wiederherstellen, Dateien eines Linux-Backups nur auf einem Linux-Rechner.

HINWEIS Falls Sie versuchen, sich über eine Windows 7-VM beim Wiederherstellungsclient anzumelden, müssen Sie die UAC-Einstellungen (User Account Control, Benutzerkontensteuerung) auf die am wenigsten einschränkenden Einstellungen für FLR einstellen, damit dies funktioniert.

Standardanmeldung

Bei der Standardanmeldung stellen Sie über eine mit VDP gesicherte virtuelle Maschine eine Verbindung zum Wiederherstellungsclient her. Melden Sie sich beim Wiederherstellungsclient mit den lokalen Administrator-Anmeldedaten der virtuellen Maschine an, bei der Sie angemeldet sind, wie in Abbildung 16-8 gezeigt.

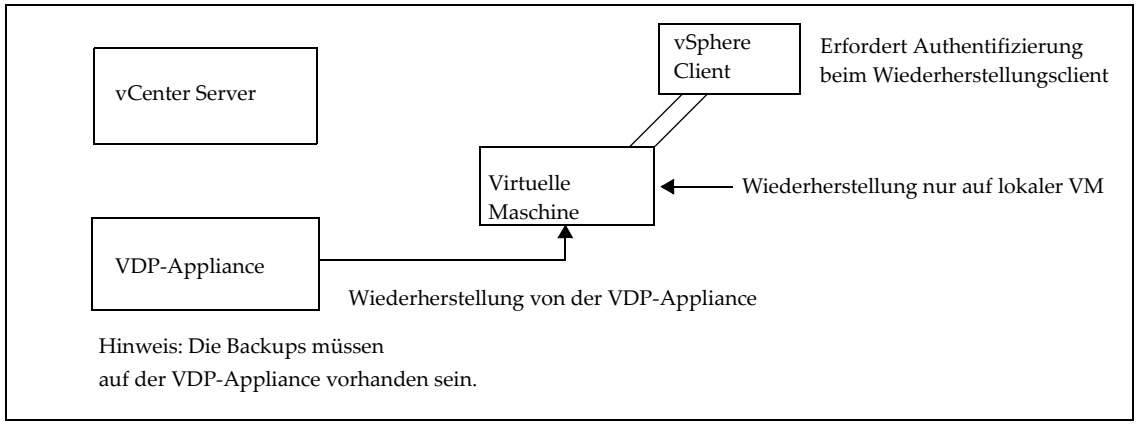


Abbildung 16-8. Recovery auf Dateiebene – Standardanmeldung

Anweisungen zur Anmeldung finden Sie unter „Verwenden des Wiederherstellungsclients im Modus „Standardanmeldung““ auf Seite 171.

Bei der Standardanmeldung zeigt der Wiederherstellungsclient nur Backups zur lokalen virtuellen Maschine an. Wenn Sie z. B. im Standardmodus von einem Windows-Host namens „WS44“ beim Wiederherstellungsclient angemeldet sind, können Sie nur die Backups von „WS44“ mounten und durchsuchen.

Erweiterte Anmeldung

Bei der erweiterten Anmeldung stellen Sie über eine mit VDP gesicherte virtuelle Maschine eine Verbindung zum Wiederherstellungsclient her. Melden Sie sich beim Wiederherstellungsclient mit den lokalen Administrator-Anmeldedaten der virtuellen Maschine, bei der Sie angemeldet sind, sowie mit den Administrator-Anmeldedaten für die Registrierung der VDP-Appliance bei vCenter Server an (siehe Abbildung 16-9).

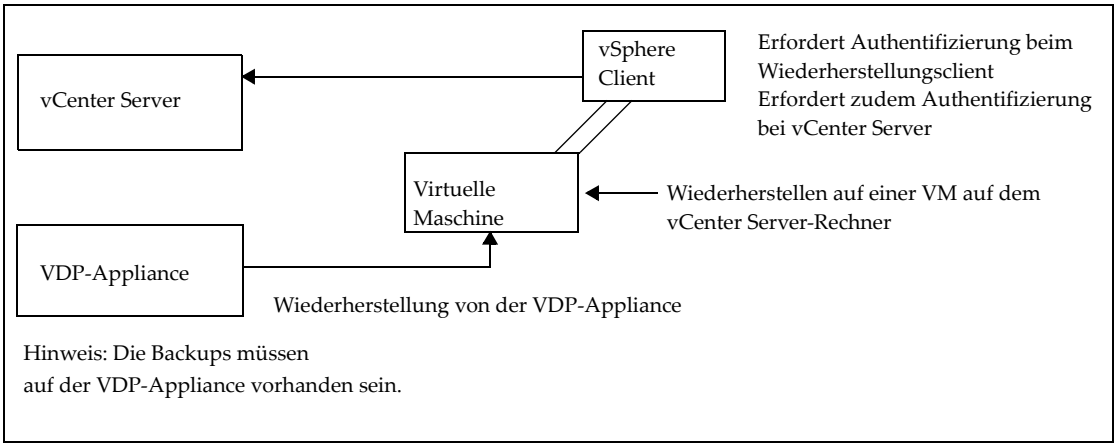


Abbildung 16-9. Recovery auf Dateiebene – erweiterte Anmeldung

Anweisungen zur Anmeldung finden Sie unter „Verwenden des Wiederherstellungsclients im Modus „Erweiterte Anmeldung““ auf Seite 172.

Nachdem eine Verbindung zum Wiederherstellungsclient hergestellt wurde, ist es möglich, Dateien von einer beliebigen, mit VDP gesicherten virtuellen Maschine aus zu mounten, zu durchsuchen und wiederherzustellen. Alle Wiederherstellungsdateien werden auf der virtuellen Maschine wiederhergestellt, bei der Sie derzeit angemeldet sind.

Zur erweiterten Anmeldung bei der Recovery auf Dateilevel müssen dieselben vCenter-Benutzeranmeldedaten verwendet werden, die während der Installation der VDP-Appliance angegeben wurden. Zusätzliche Informationen finden Sie unter „VDP-Installation" auf Seite 29.

Mounten von Backups

Nach erfolgreicher Anmeldung wird das Dialogfeld Gemountete Backups managen standardmäßig mit allen zum Mounten verfügbaren Backups angezeigt. Das Format dieses Dialogfelds hängt von der Art der Anmeldung ab.

- Bei einer Standardanmeldung werden im Dialogfeld alle zum Mounten verfügbaren Backups des Clients angezeigt, bei dem Sie angemeldet sind.
- Bei einer erweiterten Anmeldung werden im Dialogfeld alle auf VDP gesicherten Clients angezeigt. Unter jedem Client ist eine Liste aller zum Mounten verfügbaren Backups vorhanden.

HINWEIS Sie können bis zu 254 vmdk-Datei-Images mithilfe der unten rechts im Dialogfeld angezeigten Schaltflächen **Mounten**, **Unmounten** bzw. **Alle** unmounten mounten.

Filtern von Backups

Das Dialogfeld Gemountete Backups managen bietet die Möglichkeit, alle Backups anzuzeigen oder die Liste der Backups zu filtern. Die Liste kann wie folgt gefiltert werden:

- **Alle Wiederherstellungspunkte** – Es werden alle Backups angezeigt.
- **Datum der Wiederherstellungspunkte** – Es werden nur die in einem angegebenen Datumsbereich liegenden Backups angezeigt.
- **VM-Name** – Es werden nur Backups von Hosts angezeigt, deren Anzeigename den im Filterfeld eingegebenen Text enthält. (Diese Option ist bei der Standardanmeldung nicht verfügbar, da nur die Backups angezeigt werden, die zu der virtuellen Maschine gehören, bei der Sie angemeldet sind.)

Navigieren gemounteter Backups

Nach dem Mounten von Backups ist es möglich, über die Strukturanzeige auf der linken Seite der Wiederherstellungsclient-Benutzeroberfläche durch den Backupinhalt zu navigieren. Die Darstellung der Struktur ist davon abhängig, ob die Standardanmeldung oder die erweiterte Anmeldung verwendet wurde.

Ausführen von Wiederherstellungen auf Dateiebene

Über den Hauptbildschirm des Wiederherstellungsclients können Sie bestimmte Dateien wiederherstellen, indem Sie durch die Dateisystemstruktur in der linken Spalte navigieren und dann auf Verzeichnisse in der Struktur oder auf Dateien oder Verzeichnisse in der rechten Spalte klicken.

Verwenden des Wiederherstellungsclients im Modus „Standardanmeldung"

Verwenden Sie den Wiederherstellungsclient, um auf einer virtuellen Windows- oder Linux-Maschine im Modus „Standardanmeldung" auf einzelne Dateien aus Wiederherstellungspunkten für diese Maschine zuzugreifen, statt die gesamte virtuelle Maschine wiederherzustellen.

Voraussetzungen

- Überprüfen Sie, ob vSphere Data Protection (VDP) auf Ihrem vCenter Server installiert und konfiguriert ist.

- Bei der Standardanmeldung können Sie sich nur beim Wiederherstellungsclient von einer virtuellen Maschine anmelden, die von VDP gesichert wurde.
- VMware Tools muss auf der virtuellen Maschine installiert sein, um Wiederherstellungen auf Dateiebene von Backups durchzuführen. Eine Liste der Betriebssysteme mit VMware Tools-Unterstützung finden Sie auf der VMware-Website.

Verfahren

1 Greifen Sie auf den mit VDP gesicherten lokalen Host mit Remotedesktop oder vSphere Web Client zu.

2 Greifen Sie auf den VDP-Wiederherstellungsclient zu:

https://<*IP_Adresse_der_VDP_Appliance*>**:8543/flr**

3 Geben Sie auf der Seite mit den **Anmeldedaten** unter **Lokale Anmeldedaten** den **Benutzernamen** und das **Passwort** für den lokalen Host an und klicken Sie auf **Anmelden**.

Das Dialogfeld **Gemountete Backups managen** wird angezeigt, indem alle Wiederherstellungspunkte für den Client, auf den Sie zugreifen, ausgeführt werden.

4 Wählen Sie den Mount-Punkt aus, der wiederhergestellt werden soll, und klicken Sie auf **Mount**.

Nach Abschluss des Mount-Vorgangs wird das Laufwerksymbol als grünes Netzlaufwerk angezeigt  .

5 Klicken Sie auf **Schließen**.

6 Navigieren Sie im Fenster **Gemountete Backups** zu den wiederherzustellenden Ordnern und Dateien und wählen Sie diese aus.

7 Klicken Sie auf **Ausgewählte Dateien wiederherstellen**.

8 Navigieren Sie im Dialogfeld **Ziel auswählen** zum wiederherzustellenden Laufwerk und Zielordner und wählen Sie diese aus.

9 **Klicken Sie auf** Wiederherstellen.

Das Bestätigungsdialogfeld „Wiederherstellung initiieren?“ wird angezeigt.

10 Klicken Sie auf **Ja**.

Ein Dialogfeld zur erfolgreichen Initiierung wird angezeigt.

11 Klicken Sie auf **OK**.

12 Wählen Sie die Registerkarte **Wiederherstellungen überwachen**, um den Status der Wiederherstellung anzuzeigen und den erfolgreichen Abschluss der Wiederherstellung sicherzustellen.

Verwenden des Wiederherstellungsclients im Modus „Erweiterte Anmeldung“

Verwenden Sie den Wiederherstellungsclient auf einer virtuellen Windows- oder Linux-Maschine im Modus „Erweiterte Anmeldung“, um zur Recovery auf Dateilevel auf eine virtuelle Maschine eines vCenter Server-Rechners mit Wiederherstellungspunkten zuzugreifen.

Voraussetzungen

- Überprüfen Sie, ob VDP auf dem vCenter Server-Rechner installiert und konfiguriert ist.
- Zur erweiterten Anmeldung bei der Recovery auf Dateilevel müssen dieselben vCenter-Benutzeranmeldedaten verwendet werden, die während der Installation der VDP-Appliance angegeben wurden. Zusätzliche Informationen finden Sie unter „VDP-Installation“ auf Seite 29.
- VMware Tools muss auf der virtuellen Maschine installiert sein, um Wiederherstellungen auf Dateiebene von Backups durchzuführen. Eine Liste der Betriebssysteme mit VMware Tools-Unterstützung finden Sie auf der VMware-Website.

Verfahren

1 Führen Sie mithilfe von Remotedesktop eine Remoteanmeldung durch oder greifen Sie mit vSphere Web Client auf eine virtuelle Maschine zu.

2 Greifen Sie auf den VDP-Wiederherstellungsclient zu:

https://*<IP_Adresse_der_VDP_Appliance>***:8543/flr**

3 Geben Sie auf der Seite mit den **Anmeldedaten** unter **Lokale Anmeldedaten** den **Benutzernamen** und das **Passwort** für den lokalen Host an. Geben Sie im Feld **vCenter-Anmeldedaten** den **Benutzernamen** und das **Passwort** des vCenter-Administrators an und klicken Sie auf **Anmelden**.

Das Dialogfeld **Gemountete Backups managen** wird angezeigt. Dort werden alle Wiederherstellungspunkte für alle Clients desselben Typs aufgeführt, die auf VDP gesichert wurden.

4 Wählen Sie den Mount-Punkt aus, der wiederhergestellt werden soll, und klicken Sie auf **Mount**.

Nach Abschluss des Mount-Vorgangs wird das Laufwerksymbol als grünes Netzlaufwerk angezeigt  .

5 Klicken Sie auf **Schließen**.

6 Navigieren Sie im Fenster **Gemountete Backups** zu der virtuellen Maschine, den Ordnern und Dateien für die Recovery und wählen Sie diese aus.

7 Klicken Sie auf **Ausgewählte Dateien wiederherstellen**.

8 Navigieren Sie im Dialogfeld **Ziel auswählen** zum Laufwerk und Zielordner für die Recovery und wählen Sie diese aus.

9 **Klicken Sie auf** Wiederherstellen.

Das Bestätigungsdialogfeld „Wiederherstellung initiieren?“ wird angezeigt.

10 Klicken Sie auf **Ja**.

Ein Dialogfeld zur erfolgreichen Initiierung wird angezeigt.

11 Klicken Sie auf **OK**.

12 Wählen Sie die Registerkarte **Wiederherstellungen überwachen**, um den Status der Wiederherstellung anzuzeigen und den erfolgreichen Abschluss der Wiederherstellung sicherzustellen.

Überwachen von Wiederherstellungen

Klicken Sie zum Überwachen aktueller und zurückliegender Aktivitäten des Wiederherstellungsclients auf die Schaltfläche **Wiederherstellungen überwachen**. Auf dem Bildschirm zur Wiederherstellungsüberwachung werden Informationen zu aktuellen und vor kurzem abgeschlossenen Wiederherstellungsvorgängen angezeigt.

Die Spalten in dieser Tabelle lassen sich durch Klicken auf die Spaltenüberschrift sortieren. Durch mehrmaliges Klicken auf eine Tabellenüberschrift wird die Sortierreihenfolge umgekehrt, und über einen Pfeil nach oben bzw. nach unten wird angegeben, ob die Sortierreihenfolge auf- oder absteigend ist.

Standardmäßig werden unter **Wiederherstellungen überwachen** alle Jobs angezeigt, die derzeit verarbeitet werden oder die während der aktuellen Sitzung abgeschlossen wurden. Wenn Sie Jobs anzeigen möchten, die während einer vorherigen Sitzung abgeschlossen wurden oder fehlgeschlagen sind, wählen Sie **Abgeschlossene Aktivitäten anzeigen** aus. Alle zuvor abgeschlossenen und fehlgeschlagenen Job werden zusammen mit ausgeführten und ausstehenden Jobs angezeigt.

VDP-Anwendungsunterstützung 17

In diesem Kapitel werden folgende Themen behandelt:

VDP-Anwendungsunterstützung

VDP unterstützt granulare Backups und Recoveries auf Gastebene für Microsoft Exchange Server, SQL Server und SharePoint Server. Zur Unterstützung von Backups auf Gastebene ist ein VDP-Client auf den Exchange Server-, SharePoint Server- und SQL Server-Rechnern installiert.

Installieren von Anwendungs-Agents

Informationen zum Installieren von Anwendungs-Agents finden Sie in den folgenden anwendungsspezifischen Anweisungen:

- „Installieren von VDP for SQL Server Client" auf Seite 178
- „Installieren von VDP for Exchange Server Client" auf Seite 188
- „Installieren von VDP for SharePoint Server Client" auf Seite 202

Überprüfen der Einstellung zur Benutzerkontensteuerung unter Microsoft Windows

Mit der Funktion UAC (User Account Control, Benutzerkontensteuerung) wird die Anwendungssoftware auf Standardbenutzerrechte beschränkt. Für bestimmte Aufgaben, z. B. Installieren von Software, sind Administratorrechte erforderlich. UAC ist standardmäßig aktiviert.

Wenn Sie einen VDP-Client oder ein Plug-in-Installationsprogramm ohne Administratorrechte auf einem Computer starten, auf dem UAC aktiviert ist, wird die Software nicht korrekt installiert. Sie können die UAC-Funktion deaktivieren oder umgehen. Die Installationsverfahren in diesem Kapitel beschreiben eine Methode zum Umgehen der UAC-Funktion. Weitere Methoden und zusätzliche Informationen finden Sie in der Microsoft-Dokumentation.

Installieren von VDP-Clients bei aktivierter Benutzerkontensteuerung

Bei dem Versuch, VDP-Clients mit aktivierter Benutzerkontensteuerung zu installieren, wird bei der Installation der folgende Fehler angezeigt:

Der VMware VDP for <*Microsoft Application*> Server kann nicht installiert werden. Vergewissern Sie sich, dass Sie als Administrator angemeldet sind und dass alle Installationsvoraussetzungen erfüllt wurden.

Um dieses Problem zu beheben, müssen Sie das Installationsprogramm mit Administratorrechten ausführen, indem Sie die folgenden Schritte durchführen:

1 Klicken Sie unter Windows mit der rechten Maustaste auf das Symbol für die Eingabeaufforderung und wählen Sie **Als Administrator ausführen** aus.

2 Legen Sie im Fenster für die Eingabeaufforderung per Verzeichniswechsel den Speicherort des Installationspakets als Arbeitsverzeichnis fest, indem Sie den folgenden Pfad eingeben:

cd *install_path*

Dabei steht *install_path* für den vollständigen Pfad des temporären Verzeichnisses mit dem Installationspaket.

3 Geben Sie den folgenden Befehl ein, um das Installationsprogramm zu starten:

msiexec /i VMwareVDPExchange-windows-x86_64-<*version*>**.msi**
msiexec /i VMwareVDPMoss-windows-x86_64-<*version*>**.msi**
msiexec /i VMwareVDPSQL-windows-x86_64-<*version*>**.msi**
msiexec /i VMwareVDPSQL-windows-x86_32-<*version*>**.msi**

Dabei steht *version* für die VDP-Client-Version.

Sichern und Wiederherstellen von Microsoft SQL Server

VDP unterstützt erweiterte Backup- und Wiederherstellungsoptionen für Microsoft SQL Server.

In diesem Abschnitt werden folgende Themen behandelt:

Microsoft SQL Server-Optionen

Die folgenden Optionen werden für Microsoft SQL Server unterstützt:

- Backup ausgewählter SQL Server-Rechner
- Auswahl vollständiger Datenbankinstanzen für Backups
- Auswahl einzelner Datenbanken für Backups
- Unterstützung für komplette, differenzielle oder inkrementelle Backups
- Unterstützung zur Verwendung von inkrementellen Backups nach kompletten Backups
- Unterstützung für Multistreaming-Backups (bis zu sechs Streams)
- Unterstützung für Datenbankbackups im einfachen Modus (Überspringen inkrementeller Backups)
- Wiederherstellung am ursprünglichen oder an einem anderen Speicherort
- Wiederherstellung einer Datenbank in der ursprünglichen Instanz mithilfe des angegebenen Pfads
- Wiederherstellung einer Datenbank in einer anderen Instanz mithilfe des angegebenen Pfads

Hardwareanforderungen

Tabelle 17-24 umfasst die Hardwareanforderungen für Microsoft SQL Server.

Tabelle 17-24. Hardwareanforderungen für Microsoft SQL Server

Anforderung	Minimum
Speicher (RAM)	512 MB (2 GB empfohlen)
Festplattenspeicher	Für die Softwareinstallation ist 1 Gigabyte permanenter Festplattenspeicher erforderlich. Die Microsoft SQL Server-Software erfordert außerdem zusätzlich 12 MB permanenten Festplattenspeicher je 64 MB physischen Arbeitsspeichers. Der Speicherplatz wird für lokale Cachedateien benötigt.

Microsoft SQL Server-Unterstützung

VDP unterstützt die folgenden SQL Server-Versionen:

- SQL Server-Failover-Cluster für die folgenden SQL-Versionen:
  - SQL Server 2014
  - SQL Server 2012
  - SQL Server 2008, 2008 R2
  - SQL Server 2005
- SQL AlwaysOn-Cluster für die folgenden SQL-Versionen:
  - SQL Server 2014

- SQL Server 2012
- SQL Server 2014
  - SQL Server 2014 (x86/x64) unter Windows Server 2012
  - SQL Server 2014 (x86/x64) unter Windows Server 2008 SP2 oder höher
  - SQL Server 2014 (x86/x64) unter Windows Server 2008 R2 SP1 oder höher
- SQL Server 2012 (x86/x64) unter Windows Server 2012
- SQL Server 2012 (x86) unter Windows Server 2008 SP2 oder höher
- SQL Server 2012 (x64) unter Windows Server 2008 R2 SP1 oder höher
- SQL Server 2008 R2 und höher unter:
  - Windows Server 2008 oder höher (x86/x64)
  - Windows Server 2008 R2 (x64)
  - Windows Server 2012
- SQL Server 2008 SP1 oder höher unter:
  - Windows Server 2008 SP1 oder höher (x86/x64)
  - Windows Server 2008 R2 (x64)
  - Windows Server 2012
- SQL Server 2005 SP3 unter:
  - Windows Server 2008 SP1 oder höher (x86/x64)
  - Windows Server 2008 R2 (x64)
- SQL Server 2005 SP2 unter Windows Server 2008 (x86/x64)

Installieren von VDP for SQL Server Client

Zur Unterstützung von Backups auf Gastebene muss VDP for SQL Server Client auf jedem SQL Server-Rechner installiert werden, damit Backups und Wiederherstellungen unterstützt werden.

Zur Installation von VDP for SQL Server Client in einem Cluster installieren Sie VDP for SQL Server Client auf jedem Node, registrieren Sie jeden Node und konfigurieren Sie dann den VDP-Clusterclient. So installieren Sie VDP for SQL Server Client in einem Cluster:

1 Installieren Sie VDP for SQL Server Client auf jedem Node im Cluster unter dem gleichen Ordner.

   Beim Installationsvorgang wird die Software installiert und anschließend jeder Node im Cluster bei der VDP-Appliance registriert und darauf aktiviert.

2 Konfigurieren Sie die VDP-Appliance mithilfe des VMware VDP Windows Cluster Configuration Wizard.

Voraussetzungen

- Vor der Verwendung von VDP müssen Sie die VDP-Appliance, wie unter „VDP-Installation und -Konfiguration" auf Seite 21 beschrieben, installieren und konfigurieren und Sie müssen über Administratorrechte auf dem SQL Server-Rechner verfügen.
- Folgende Software muss auf dem SQL Server-Rechner installiert sein:
  - .NET 4.0
  - SQL Server-Installationskomponente
  - Clienttools SDK

Verfahren

1 Greifen Sie auf jedem SQL Server-Client auf vSphere Web Client zu:

https://<*IP_Adresse_vCenter_Server*>:9443/vsphere-client/

2 Geben Sie auf der Seite mit den Anmeldedaten einen Administratorbenutzernamen und ein Passwort für vCenter ein und klicken Sie auf **Anmelden**.

3 Wählen Sie in vSphere Web Client **VDP** aus.

4 Wählen Sie auf der VDP-Begrüßungsseite die VDP-Appliance aus und klicken Sie auf **Verbinden**.

5 Klicken Sie auf die Registerkarte **Konfiguration**.

6 Klicken Sie unter **Clientdownloads** auf **Microsoft SQL Server 32 Bit** oder **Microsoft SQL Server 64 Bit** (abhängig von der Version des SQL Server-Clients).

7 Je nach dem von Ihnen verwendeten Browser können Sie die `.msi`-Datei speichern oder ausführen. Sobald Sie die `.msi`-Datei ausführen, wird der Setup-Assistent von VMware VDP for SQL Server gestartet. Klicken Sie auf **Weiter**.

8 Lesen Sie sich auf der Seite „Endbenutzer-Lizenzvertrag“ den Lizenztext durch und klicken Sie, sofern Sie zustimmen möchten, auf **Ich akzeptiere die Bedingungen des Lizenzvertrags** und dann auf **Weiter**.

9 Geben Sie auf der Seite mit den Appliance-Registrierungsinformationen den Namen der für das SQL Server-Backup vorgesehenen VDP-Appliance ein und klicken Sie auf **Weiter**.

10 Klicken Sie auf der Seite „VMware VDP for SQL Server kann jetzt installiert werden“ auf **Installieren**.

11 Klicken Sie auf der Seite „Der Setup-Assistent von VMware VDP for SQL Server wurde fertiggestellt“ auf **Fertig stellen**.

Wiederholen Sie dieses Verfahren für zusätzliche SQL Server.

Konfigurieren des Clusterclients in einem Failover-Cluster

Der VDP-Clusterclient in einem Failover-Cluster ermöglicht das Backup und die Wiederherstellung von SQL Server-Daten in dem gemeinsamen Speicher des Clusters unabhängig davon, welcher Node die Daten zum Backup- oder Wiederherstellungszeitpunkt managt. Der VMware VDP Windows Cluster Configuration Wizard enthält alle notwendigen Schritte zur Konfiguration des Clusterclients für das SQL Server-Plug-in in einem Failover-Cluster.

Verfahren

1 Melden Sie sich als Domainadministrator beim aktiven Node im Cluster an. Das Konto muss ebenfalls ein Mitglied der lokalen Administratorgruppe jedes Cluster-Node sein.

2 Starten Sie den VMware VDP Windows Cluster Configuration Wizard:

- Öffnen Sie unter Windows Server 2012 den **Start**bildschirm und wählen Sie **VMware VDP Windows Cluster Configuration Wizard** aus.
- Öffnen Sie unter Windows Server 2008 das Menü **Start** und wählen Sie **Programme > VMware VDP > VMware VDP Windows Cluster Configuration Wizard** aus.

3 **Klicken Sie auf der Seite Willkommen** auf Weiter.

4 Wählen Sie auf der Seite **Plug-ins** die Option **SQL** aus und klicken Sie auf **Weiter**.

Die Seite „Cluster-Nodes“ wird mit einer Liste der Nodes und ihrer Status angezeigt.

5 Vergewissern Sie sich auf der Seite **Cluster-Nodes**, dass die Umgebung die folgenden Anforderungen erfüllt und klicken Sie auf **Weiter**:

- Laut Status sind alle SQL Server-Nodes aktiv.
- Der Installationsstatus der Windows-Clientsoftware für jeden Node ist „Installiert“.

- Der Installationsstatus des SQL Server-Plug-ins auf jedem Node ist „Installiert“.

6 Wählen Sie auf der Seite **Vorgänge** die Option **Neuen Clusterclient für alle Nodes konfigurieren** aus und klicken Sie auf **Weiter**.

7 Vergewissern Sie sich auf der Seite **Voraussetzungen**, dass die Umgebung alle Voraussetzungen erfüllt.

Durch ein Häkchen neben einer Voraussetzung wird angegeben, dass die Umgebung die Voraussetzung erfüllt.

Wenn die Umgebung eine Voraussetzung nicht erfüllt, beenden Sie den Assistenten, beheben Sie das Problem und starten Sie den Assistenten dann erneut.

8 Wählen Sie die von der Umgebung verwendete IP-Version aus und klicken Sie auf **Weiter**.

9 Gehen Sie auf der Seite **SQL-Einstellungen** wie folgt vor:

a Wählen Sie die Clustergruppe, den Clusterdienst oder die Clusterrolle für den Clusterclient aus der Liste aus:

- Wählen Sie unter Windows Server 2012 die Clusterrolle für den Clusterclient aus der Liste mit der **Clusterrolle für den Clusterclient** aus.
- Wählen Sie unter Windows Server 2008 den Clusterdienst für den Clusterclient aus der Liste mit dem **Clusterdienst für den Clusterclient** aus.

b Wählen Sie das gemeinsam genutzte Volume für den Clusterclient aus der Liste mit dem gemeinsam genutzten Volume für den Clusterclient aus.

c Klicken Sie auf **Weiter**.

10 Geben Sie auf der Seite **Servereinstellungen** die Einstellungen für die VDP-Appliance an:

a Geben Sie entweder den DNS-Namen der VDP-Appliance in das Feld **Name** oder die IP-Adresse in das Feld **IPv4-/IPv6-Adresse** ein.

b Geben Sie den Datenport für die Kommunikation zwischen VDP-Client und -Server in das Feld **Portnummer** ein.

HINWEIS Standardmäßig nutzt der VDP-Client den Port 28001 zur Kommunikation mit der VDP-Appliance.

c Geben Sie den Namen des Ordners oder Volume in das Feld **var-Verzeichnis von Clusterclient** ein oder klicken Sie auf **Durchsuchen**, um einen Ordner oder ein Volume auszuwählen.

Dieser Ordner bzw. dieses Volume speichert die Clientkonfigurations- und Protokolldateien. Alle Nodes im Cluster müssen über Schreibzugriff für diesen Ordner bzw. dieses Volume verfügen.

HINWEIS Wählen Sie statt eines Remotepfadnamens im Netzwerk ein Volume aus, das zu dem Cluster gehört.

d Klicken Sie auf **Weiter**.

11 Überprüfen Sie auf der Seite **Zusammenfassung** die Konfigurationseinstellungen und klicken Sie auf **Konfigurieren**.

Die Seite **Progress** stellt den Status der Konfiguration bereit.

12 Überprüfen Sie die Informationen auf der Seite **Ergebnisse** und klicken Sie auf **Schließen**.

Konfigurieren des Clusterclients für eine AlwaysOn-Verfügbarkeitsgruppe

Der VDP-Clusterclient für eine AlwaysOn-Verfügbarkeitsgruppe ermöglicht das Backup und die Wiederherstellung von SQL Server-Datenbanken in einer Verfügbarkeitsgruppe. Der VMware VDP Windows Cluster Configuration Wizard enthält alle notwendigen Schritte zur Konfiguration des VDP-Clusterclients für das SQL Server-Plug-in in einer AlwaysOn-Verfügbarkeitsgruppe.

Verfahren

1 Melden Sie sich als Domainadministrator bei einem Cluster-Node an. Das Konto muss ebenfalls ein Mitglied der lokalen Administratorgruppe jedes Cluster-Node sein.

2 Starten Sie den VMware VDP Windows Cluster Configuration Wizard:

- Öffnen Sie unter Windows Server 2012 den **Start**bildschirm und wählen Sie **VMware VDP Windows Cluster Configuration Wizard** aus.
- Öffnen Sie unter Windows Server 2008 das Menü **Start** und wählen Sie **Programme > VMware VDP > VMware VDP Windows Cluster Configuration Wizard** aus.

3 **Klicken Sie auf der Seite Willkommen** auf Weiter.

4 Wählen Sie auf der Seite **Plug-ins** die Option **SQL AlwaysOn** aus und klicken Sie auf **Weiter**.

5 Gehen Sie auf der Seite **Cluster-Nodes** wie folgt vor:

a Vergewissern Sie sich, dass die Umgebung die folgenden Anforderungen erfüllt:

- Laut Status sind alle SQL Server-Nodes aktiv.
- Der Installationsstatus der Windows-Clientsoftware für jeden Node ist „Installiert“.
- Der Installationsstatus des SQL Server-Plug-ins auf jedem Node ist „Installiert“.

b Klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite **Vorgänge** die Option **Neuen Clusterclient für alle Nodes konfigurieren** aus und klicken Sie auf **Weiter**.

7 Vergewissern Sie sich auf der Seite **Voraussetzungen**, dass die Umgebung alle Voraussetzungen erfüllt.

Durch ein Häkchen neben einer Voraussetzung wird angegeben, dass die Umgebung die Voraussetzung erfüllt.

Wenn die Umgebung eine Voraussetzung nicht erfüllt, beenden Sie den Assistenten, beheben Sie das Problem und starten Sie den Assistenten erneut.

8 Wählen Sie die von der Umgebung verwendete IP-Version aus und klicken Sie auf **Weiter**.

9 Gehen Sie auf der Seite **SQL AlwaysOn-Einstellungen** wie folgt vor:

a Wählen Sie die Clustergruppe, den Clusterdienst oder die Clusterrolle für den Clusterclient aus der Liste aus:

- Wählen Sie unter Windows Server 2012 die Clusterrolle für den Clusterclient aus der Liste mit der Clusterrolle für den Clusterclient aus.
- Wählen Sie unter Windows Server 2008 den Clusterdienst für den Clusterclient aus der Liste mit dem Clusterdienst für den Clusterclient aus.

Der Name des Clusterclients wird im Feld **Clusterclientname** angezeigt.

HINWEIS Sie müssen einen Verfügbarkeitsgruppen-Listener für jede Verfügbarkeitsgruppe konfigurieren. Konfigurieren Sie Clusterclients nicht für Verfügbarkeitsgruppen ohne Listener.

b Klicken Sie auf **Weiter**.

10 Geben Sie auf der Seite **Servereinstellungen** die Einstellungen für die VDP-Appliance an:

a Geben Sie entweder den DNS-Namen der VDP-Appliance in das Feld **Name** oder die IP-Adresse in das Feld **IPv4-/IPv6-Adresse** ein.

b Geben Sie den Datenport für die Kommunikation zwischen VDP-Client und -Server in das Feld **Portnummer** ein.

HINWEIS Standardmäßig nutzt die VDP-Appliance den Port 28001 zur Kommunikation.

c Geben Sie den Namen des Ordners oder Volume in das Feld **var-Verzeichnis von Clusterclient** ein oder klicken Sie auf **Durchsuchen**, um einen Ordner oder ein Volume auszuwählen.

Dieser Ordner bzw. dieses Volume speichert die Clientkonfigurations- und Protokolldateien. Alle Nodes im Cluster müssen über Schreibzugriff für diesen Ordner bzw. dieses Volume verfügen.

HINWEIS Wählen Sie statt eines Remotepfadnamens im Netzwerk ein Volume aus, das zu dem Cluster gehört.

d Klicken Sie auf **Weiter**.

11 Überprüfen Sie auf der Seite **Zusammenfassung** die Konfigurationseinstellungen und klicken Sie auf **Konfigurieren**.

Die Seite **Progress** stellt den Status der Konfiguration bereit.

12 Überprüfen Sie die Informationen auf der Seite **Ergebnisse** und klicken Sie auf **Schließen**.

Erstellen von Backupjobs für Microsoft SQL Server

VMware VDP for SQL Server Client muss auf jedem SQL Server installiert werden, der für Backups verfügbar ist. Zusätzliche Informationen zur Clientinstallation finden Sie unter „Installieren von VDP for SQL Server Client“ auf Seite 178.

1 Wählen Sie in vSphere Web Client die Registerkarte **Backup** aus.

2 Klicken Sie auf der Registerkarte **Backup** auf **Backupjobaktionen** und wählen Sie **Neu** aus, um den Assistenten **Neuen Backupjob erstellen** zu starten.

Wählen Sie auf der Seite „Jobtyp“ des Assistenten die Option **Anwendungen** aus. Mit dieser Option können Sie den kompletten Server oder ausgewählte Datenbanken sichern.

Sichern von Anwendungen

Wenn Sie auf der Seite „Jobtyp“ **Anwendungen** auswählen, können Sie wahlweise Anwendungsserver oder individuelle Datenbanken sichern.

1 Wählen Sie auf der Seite **Jobtyp** des Assistenten **Neuen Backupjob erstellen** die Option **Anwendungen** aus und klicken Sie auf **Weiter**.

2 Wählen Sie auf der Seite **Datentyp** eine der folgenden Optionen aus und klicken Sie auf **Weiter**:

- **Kompletter Server**: Über diese Option können Sie ganze Anwendungsserver sichern.
- **Ausgewählte Datenbanken**: Mit dieser Option können Sie einzelne Anwendungsserverdatenbanken sichern.

3 Klicken Sie auf der Seite **Backupquellen** auf den Pfeil neben einer der folgenden Backupquellen, um die Liste zu erweitern:

- **Microsoft SQL Server**: Wählen Sie diese Option für ein SQL Server-Backup aus.
- **Microsoft SQL-Failover-Cluster**: Wählen Sie diese Option für ein SQL-Failover-Clusterbackup aus.
- **Microsoft SQL AlwaysOn-Cluster**: Wählen Sie diese Option für ein Backup der SQL AlwaysOn-Verfügbarkeitsgruppe aus.

4 Führen Sie einen der folgenden Schritte aus:

- Falls Sie einen kompletten Server sichern möchten, aktivieren Sie das Kontrollkästchen neben dem zu sichernden SQL Server und klicken Sie dann auf **Weiter**.

  HINWEIS Als Best Practice gilt die Auswahl nur eines SQL Server-Rechners pro Backupjob.

- Falls Sie ausgewählte Datenbanken sichern möchten, klicken Sie auf den Pfeil neben einem SQL Server und führen Sie ein Drill-down durch, bis Sie die Datenbank- oder Speichergruppe auswählen können, die Sie sichern möchten. Klicken Sie dann auf **Weiter**.

5 Wählen Sie auf der Seite **Backupoptionen** den Backuptyp **Komplett**, **Differenziell** oder **Inkrementell** aus. Die konfigurierbaren Optionen hängen von Ihrer Auswahl ab.

- **Komplett**: Über die Option **Komplett** wird die gesamte Datenbank gesichert, einschließlich aller Objekte, Systemtabellen und Daten. Die Optionen für komplette Backups werden wie folgt beschrieben:
  - **Inkrementelles Backup nach komplettem Backup erzwingen**: Durch Aktivieren oder Deaktivieren dieses Kontrollkästchens wird festgelegt, ob ein inkrementelles Backup mit den zwischen kompletten Backups durchgeführten Transaktionen erzwungen werden soll. Hierdurch wird eine Point-in-Time Recovery an einem Punkt zwischen kompletten Backups erstellt.

    Verwenden Sie diese Option nicht für Datenbanken, die das einfache Recovery-Modell nutzen, da diese Datenbanken Backups von Transaktionsprotokollen nicht unterstützen. Hierzu gehören Systemdatenbanken wie Master- und msdb-Datenbanken.

    Für einfache Recovery-Modelldatenbanken verwenden Sie die Option **Für einfache Recovery-Modelldatenbanken**.

  - **Multi-Stream-Backup aktivieren**: Es können entweder mehrere Datenbanken parallel mit einem Stream pro Datenbank oder eine einzige Datenbank mit mehreren parallelen Streams gesichert werden. Wenn Sie sich dafür entscheiden, eine einzige Datenbank mit mehreren parallelen Streams zu sichern, können Sie die minimale Größe jedes Stream während des Backups angeben.

    Nach Festlegung der minimalen Stream-Größe können Sie die zum Sichern der Datenbank verwendete Stream-Anzahl mithilfe der folgenden Gleichung berechnen:

    Datenbankgröße/minimale Stream-Größe = Stream-Anzahl

    Wenn eine Datenbank beispielsweise 1.280 MB groß und als minimale Stream-Größe die Standardeinstellung von 256 MB ausgewählt ist, beträgt die zum Durchführen eines kompletten Backups verwendete Stream-Anzahl 5, wie in der folgenden Gleichung zu sehen ist:

    1.280 MB/256 = 5

    Bei Transaktionsprotokollen und differenziellen Backups wird die Stream-Anzahl anhand der Größe der zu sichernden Daten und nicht anhand der Datenbankgesamtgröße berechnet. Wenn die Datenbankgröße unter der minimalen Stream-Größe liegt, wird in VDP ein Single Stream zum Sichern der Datenbank verwendet.

    Wenn Sie die Stream-Anzahl für eine Datenbank auf Grundlage der minimalen Stream-Größe berechnen und diese Anzahl die maximale für das Backup konfigurierte Stream-Anzahl übersteigt, erfolgt das Backup der Datenbank nur mit der maximalen Stream-Anzahl.

  - **Für einfache Recovery-Modelldatenbanken**: Durch diese Option wird festgelegt, wie VDP inkrementelle Backups (Backups von Transaktionsprotokollen) von Datenbanken verarbeitet, die das einfache Recovery-Modell ohne Unterstützung für Backups von Transaktionsprotokollen verwenden:

    Inkrementell mit Warnung überspringen (Standardeinstellung): Beim Auswählen von Datenbanken mit unterschiedlichen Recovery-Modellen für das Backup sind im Backup keine Datenbanken mit einfachem Recovery-Modell enthalten. Das Backup wird mit Ausnahmen abgeschlossen, und es wird eine Fehlermeldung in das Protokoll geschrieben. Wenn ausschließlich Datenbanken mit dem einfachen Recovery-Modell für das Backup ausgewählt werden, schlägt das Backup fehl.

    Inkrementell mit Warnung überspringen: Beim Auswählen von Datenbanken mit unterschiedlichen Recovery-Modellen für das Backup sind im Backup keine Datenbanken mit einfachem Recovery-Modell enthalten. Das Backup wird erfolgreich abgeschlossen, und es wird für jede Datenbank mit einfachem Recovery-Modell eine Warnung in das Protokoll geschrieben. Wenn ausschließlich Datenbanken mit dem einfachen Recovery-Modell für das Backup ausgewählt werden, schlägt das Backup fehl.

Inkrementell auf komplett hochstufen: Bei Datenbanken mit einfachem Recovery-Modell wird statt eines Backups von Transaktionsprotokollen automatisch ein komplettes Backup durchgeführt.

- **Datenbankprotokoll kürzen**: Durch diese Option wird das Verhalten beim Kürzen von Datenbanktransaktionsprotokollen gesteuert. Die folgenden Optionen stehen u. a. zum Kürzen zur Verfügung:

  Nur für inkrementelles Backup (Standardeinstellung): Das Datenbanktransaktionsprotokoll wird gekürzt, wenn der Backuptyp auf inkrementell festgelegt ist (Transaktionsprotokoll). Das Protokoll wird nicht gekürzt, wenn für den Backuptyp die Option „Komplett“ oder „Differenziell“ ausgewählt ist.

  Für alle Backuptypen: Das Datenbanktransaktionsprotokoll wird unabhängig vom Backuptyp gekürzt. Durch diese Einstellung wird die Kette von Protokollbackups durchbrochen. Sie sollte nur bei einem auf „Komplett“ eingestellten Backuptyp verwendet werden.

  Nie: Das Datenbanktransaktionsprotokoll wird unter keinen Umständen gekürzt.

- **Authentifizierungsmethode:** Die Authentifizierungsmethode legt fest, ob für die SQL Server-Verbindung eine NT-Authentifizierung oder SQL Server-Authentifizierung verwendet wird. Wenn Sie die SQL Server-Authentifizierung auswählen, geben Sie den Benutzernamen und das Passwort für die SQL Server-Anmeldung an.

- **Verfügbarkeitsgruppenreplikat für Backup:** Es gibt 4 Optionen:

  Primär: Falls ausgewählt, wird das Backup auf dem primären Replikat der ausgewählten AlwaysOn-Verfügbarkeitsgruppe ausgeführt.

  Sekundär bevorzugen: Falls ausgewählt, wird das Backup auf dem sekundären Replikat der ausgewählten AlwaysOn-Verfügbarkeitsgruppe ausgeführt. Wenn kein sekundäres Replikat verfügbar ist, wird das Backup auf dem primären Replikat durchgeführt.

  Nur sekundär: Falls ausgewählt, wird das Backup auf dem sekundären Replikat der ausgewählten AlwaysOn-Verfügbarkeitsgruppe ausgeführt. Wenn kein sekundäres Replikat verfügbar ist, wird der Backupvorgang unterbrochen und eine entsprechende Fehlermeldung in die Protokolldatei geschrieben.

  SQL Server definiert: Falls ausgewählt, wird das Backup auf dem primären oder sekundären Replikat auf Basis der SQL Server-Konfiguration ausgeführt. Wenn „Automated_Backup_Preference“ auf „none“ eingestellt ist, wird das Backup auf dem primären Replikat ausgeführt.

- **Differenziell** oder **Inkrementell**: Mit der Option **Differenziell** werden alle Daten gesichert, die sich seit dem letzten kompletten Backup geändert haben. Über die Option **Inkrementell** werden nur die Transaktionsprotokolle gesichert. Die einzige Konfigurationsoption, die sich von einem kompletten Backup unterscheidet, ist das Erzwingen eines kompletten Backups statt eines inkrementellen Backups.

  - **Komplettes Backup erzwingen**: Durch Aktivieren oder Deaktivieren des Kontrollkästchens wird festgelegt, ob ein komplettes Backup durchgeführt wird, wenn VDP eine Protokolllücke entdeckt oder kein vorheriges komplettes Backup vorhanden ist, aus dem ein Backup von Transaktionsprotokollen (inkrementell) oder ein differenzielles Backup angewendet werden kann. Tatsächlich wird durch diese Option bei Bedarf die Erstellung eines kompletten Backups automatisiert.

    Wenn Sie **Differenziell** oder **Inkrementell** auswählen, sollte diese Option aktiviert bleiben (Standardeinstellung). Andernfalls ist eine Wiederherstellung von Daten bei nicht vorhandenem komplettem Backup in VDP u. U. nicht möglich.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite **Planung** die Backupplanung und die Startzeit für den Backupjob aus und klicken Sie auf **Weiter**.

Weitere Informationen zum Konfigurieren der Planung finden Sie unter „Festlegen der Backupplanung" auf Seite 125.

8 Legen Sie mithilfe der Optionen auf der Seite **Aufbewahrungs-Policy** fest, wie lange das Backup aufbewahrt werden soll. Klicken Sie dann auf **Weiter**.

Weitere Informationen zum Konfigurieren der Aufbewahrungs-Policy finden Sie unter „Festlegen der Aufbewahrungs-Policy" auf Seite 125.

9 Geben Sie auf der Seite **Name** einen Namen für den Backupjob ein und klicken Sie auf **Weiter**.

10 Überprüfen Sie auf der Seite **Bereit zur Fertigstellung** die Zusammenfassung zum Backupjob und klicken Sie auf **Fertig stellen**.

11 Klicken Sie auf **OK**, wenn eine Bestätigung über die erfolgreiche Erstellung des Backupjobs angezeigt wird.

Wiederherstellen von Microsoft SQL Server-Backups

Sobald Backups auf Microsoft SQL Server-Rechnern ausgeführt wurden, ist es möglich, diese Backups an ihrem ursprünglichen Speicherort oder an einem anderen Speicherort wiederherzustellen.

Verfahren

1 Wählen Sie in vSphere Web Client die Registerkarte **Wiederherstellen** aus.

2 Wählen Sie das wiederherzustellende Backup aus. Die Auswahl mehrerer SQL Server-Rechner ist zwar möglich, allerdings kann nur ein Wiederherstellungspunkt pro SQL Server ausgewählt werden.

3 Klicken Sie auf **Wiederherstellen**.

4 Wählen Sie auf der Seite **Backup auswählen** den wiederherzustellenden Backupjob aus und klicken Sie auf **Weiter**.

5 Gehen Sie auf der Seite **Wiederherstellungsoptionen auswählen** wie folgt vor:

a Führen Sie einen der folgenden Schritte aus:

- Lassen Sie die Option **Am ursprünglichen Speicherort wiederherstellen** ausgewählt (die Standardeinstellung), um das Backup an seinem ursprünglichen Speicherort wiederherzustellen.
- Deaktivieren Sie die Option **Am ursprünglichen Speicherort wiederherstellen**, um das Backup an einem anderen Speicherort wiederherzustellen, und gehen Sie dann folgendermaßen vor:

  i Klicken Sie auf **Auswählen**, um den Zielclient auszuwählen.

  ii Geben Sie im Feld **SQL-Instanz** den Namen der SQL-Instanz ein. Bei der Verwendung von „lokal" muss dies in Klammern stehen.

  iii Geben Sie im Feld **Speicherpfad** den vorhandenen vollständigen Windows-Pfad ein, an dem die Datenbankdateien wiederhergestellt werden.

  Wenn der Speicherpfad nicht vorhanden ist, wird er nicht erstellt, und die Wiederherstellung schlägt fehl.

  iv Geben Sie im Feld **Protokolldateipfad** den vorhandenen vollständigen Windows-Pfad ein, an dem die Protokolldateien wiederhergestellt werden.

b Falls Sie erweiterte Optionen festlegen möchten, klicken Sie auf den Pfeil neben **Erweiterte Optionen**, um die Liste zu erweitern. Die Optionen werden im Folgenden beschrieben:

- **Verwenden von SQL REPLACE:** Durch diese Option wird festgelegt, dass SQL Server die ggf. erforderlichen Datenbanken und zugehörigen Dateien erstellen soll, selbst wenn bereits eine andere Datenbank oder Datei desselben Namens vorhanden ist.

Hierdurch wird die SQL Server-Sicherheitsprüfung außer Kraft gesetzt, die ein versehentliches Überschreiben einer anderen Datenbank oder Datei verhindern soll. Diese Sicherheitsprüfung wird im Microsoft Transact-SQL-Referenzhandbuch im Abschnitt über den RESTORE-Befehl beschrieben.

- **Nur auf primärem Replikat wiederherstellen**: Mit diesem Kontrollkästchen wird das Flag `--recover-primary-only` gesetzt und damit die automatische Recovery sekundärer Replikate deaktiviert und die Recovery ausschließlich auf dem primären Replikat durchgeführt. Standardmäßig ist das Kontrollkästchen deaktiviert, sodass die Recovery nur auf dem primären Replikat durchgeführt wird. Diese Option ist nur für Datenbanken aktiviert, die sich in einer AlwaysOn-Verfügbarkeitsgruppe befinden.

HINWEIS Nachdem eine Datenbank ausschließlich auf dem primären Replikat wiederhergestellt wurde, liegt die entsprechende Datenbank auf dem sekundären Replikat in einem Status „Wiederherstellen“ vor.

- **Protokollfragmentbackup:** Für ein Protokollfragmentbackup während des Wiederherstellungsprozesses muss die Datenbank online geschaltet sein und entweder das vollständige oder massenprotokollierte Recovery-Modell verwenden. Die Durchführung eines Protokollfragmentbackups für die Systemdatenbanken ist nicht möglich, da diese Datenbanken das einfache Recovery-Modell nutzen (z. B. Master- und msdb-Datenbanken).

  Wählen Sie nicht die Option „Protokollfragmentbackup“ aus, wenn Sie eine umgeleitete Wiederherstellung auf einer anderen SQL Server-Instanz durchführen.

- **Systemdatenbanken wiederherstellen**: Es ist nur selten erforderlich, ausschließlich Systemdatenbanken wiederherzustellen. Im Falle einer Beschädigung von einer oder mehreren Systemdatenbanken kann dies jedoch vonnöten sein.

  Es ist wahrscheinlicher, dass Sie Systemdatenbanken gleichzeitig mit Benutzerdatenbanken wiederherstellen müssen. Wenn Sie sowohl die System- als auch die Benutzerdatenbanken zur Wiederherstellung auswählen, werden zuerst die Systemdatenbanken wiederhergestellt.

  Beim Wiederherstellen von Systemdatenbanken werden die Datenbanken von VDP Microsoft SQL Server Client automatisch in der richtigen Reihenfolge (Master, msdb, dann das Modell) wiederhergestellt, und die SQL Server-Dienste werden gemanagt.

- **Authentifizierungsmethode**: Die Authentifizierungsmethode legt fest, ob für die SQL Server-Verbindung eine NT-Authentifizierung oder SQL Server-Authentifizierung verwendet wird. Wenn Sie die SQL Server-Authentifizierung auswählen, geben Sie den Benutzernamen und das Passwort für die SQL Server-Anmeldung an.

- **Recovery-Vorgang**: Wählen Sie den geeigneten Wert – **RECOVERY** oder **KEINE RECOVERY**, wenn Sie die Wiederherstellung in einer SQL AlwaysOn-Clusterumgebung durchführen.

c Klicken Sie auf **Weiter**.

6 Überprüfen Sie auf der Seite **Bereit zur Fertigstellung** die Wiederherstellungsanforderungen und klicken Sie auf **Fertig stellen**.

7 Klicken Sie in der Meldung, in der angegeben ist, dass die Wiederherstellung erfolgreich initiiert wurde, auf **OK**.

8 Überwachen Sie den Fortschritt der Wiederherstellung über das Fenster **Letzte Aufgaben**.

Überwachen der Clientaktivität

Sie können Aufgaben und Ereignisse für sämtliche Clientaktivitäten überwachen, indem Sie Clientprotokolle zusammenstellen und analysieren. Bei den Clientprotokollen handelt es sich um MSApp-bezogene Protokolle. (MSApp steht für Microsoft Application, also Microsoft-Anwendungen.) Das aggregierte Clientprotokoll umfasst alle Jobs des Typs „Replikation“, „Backup“, „Wiederherstellung“ bzw. „Automatische Backupverifizierung“ (ABV), die mit Ausnahmen abgeschlossen wurden oder fehlgeschlagen sind. Weitere Informationen erhalten Sie unter „Sammeln von VDP-Protokollen oder Diagnoseinformationen“ auf Seite 40.

Deinstallieren von VDP Plug-in for SQL Server

So deinstallieren Sie VDP Plug-in for SQL Server:

- Unter Windows Server 2012 oder Windows Server 2008 verwenden Sie **Programme und Funktionen**.
- Unter Windows Server 2003 verwenden Sie **Programme hinzufügen/entfernen**.

Sichern und Wiederherstellen von Microsoft Exchange Server

In diesem Abschnitt werden folgende Themen behandelt:

Microsoft Exchange Server-Optionen

VDP unterstützt die erweiterten Backup- und Wiederherstellungsoptionen für Microsoft Exchange Server.

- Backup ausgewählter Exchange Server-Rechner
- Backup ausgewählter einzelner Exchange-Datenbanken oder -Speichergruppen
- Funktion zur Durchführung inkrementeller Backups
- Unterstützung für Multistreaming-Backups (bis zu zehn Streams)
- Unterstützung für die Umlaufprotokollierung (Hochstufen, Umlauf und Überspringen)
- Funktion zur Exchange-Wiederherstellung am ursprünglichen oder an einem anderen Speicherort
- Option zum Unterbinden der Wiedergabe von Protokollen während der Wiederherstellung
- Recovery-Speichergruppe (Recovery Storage Group, RSG)/Wiederherstellungsdatenbank (Recovery Database, RDB)
- Granular Level Restores

Microsoft Exchange Server-Unterstützung

Tabelle 17-25 führt die Microsoft Exchange Server-Versionen und Betriebssysteme auf, die vom VDP-Plug-in für Microsoft Exchange unterstützt werden.

Tabelle 17-25. Unterstützte Microsoft Exchange Server-Versionen und Betriebssysteme

Exchange Server-Version	Betriebssysteme
■ Exchange Server 2013 ■ Exchange Server 2013 Database Availability Group (DAG)	■ Windows Server 2012 (x64) ■ Windows Server 2012 R2 (x64) ■ Windows Server 2008 R2 (x64)
■ Exchange Server 2010 SP3 ■ Exchange Server 2010 Database Availability Group (DAG)	■ Windows Server 2012 (x64) ■ Windows Server 2008 R2 (x64) ■ Windows Server 2008 SP2 (x64)
■ Exchange Server 2007 SP3	■ Windows Server 2008 R2 (x64) ■ Windows Server 2008 SP2 (x64)

Microsoft .NET Framework 4-Anforderung

Das Exchange Server VSS-Plug-in erfordert die Installation von Microsoft .NET Framework 4 auf jedem Server in der Exchange Server-Gesamtstruktur. Suchen Sie im Microsoft Download Center nach „Microsoft .NET Framework 4“, um Downloads und zusätzliche Informationen zu finden.

Hardwareanforderungen

Tabelle 17-26 führt die Hardwareanforderungen für das VDP-Plug-in für Microsoft Exchange Server auf.

Tabelle 17-26. Hardwareanforderungen für Microsoft Exchange Server

Anforderung	Minimum
Speicher (RAM)	64 MB
Festplattenspeicher	Für die Softwareinstallation sind mindestens 100 MB permanenter Festplattenspeicher erforderlich, 1 GB wird empfohlen. Die lokalen Cachedateien erfordern außerdem zusätzlich 12 MB permanenten Festplattenspeicher je 64 MB physischen Arbeitsspeichers.

Nicht unterstützte Microsoft Exchange Server

Cluster von Microsoft Exchange Server 2007 (SCC, CCR und SCR) werden nicht mit dem VDP-Plug-in für Microsoft Exchange Server-Rechner unterstützt.

Installieren von VDP for Exchange Server Client

Zur Unterstützung von Backups auf Gastebene muss VMware vSphere Data Protection (VDP) for Exchange Server Client auf jedem Exchange Server-Rechner installiert werden, damit Backups und Wiederherstellungen unterstützt werden.

Voraussetzungen

Vor der Verwendung von VDP müssen Sie die VDP-Appliance, wie unter „VDP-Installation und -Konfiguration“ auf Seite 21 beschrieben, installieren und konfigurieren und Sie müssen über Administratorrechte auf dem Exchange Server-Rechner verfügen.

Verfahren

1 Greifen Sie auf jedem Exchange Server-Client auf vSphere Web Client zu:

https://<*IP_Adresse_vCenter_Server*>:9443/vsphere-client/

2 Geben Sie auf der Seite mit den Anmeldedaten einen Administratorbenutzernamen und ein Passwort für vCenter ein und klicken Sie anschließend auf **Anmelden**.

3 Wählen Sie in vSphere Web Client **VDP** aus.

4 Wählen Sie auf der VDP-Begrüßungsseite die VDP-Appliance aus und klicken Sie auf **Verbinden**.

5 Klicken Sie auf die Registerkarte **Konfiguration**.

6 Klicken Sie unter **Clientdownloads** auf **Microsoft Exchange Server 64 Bit**.

7 Je nach dem von Ihnen verwendeten Browser können Sie die `.msi`-Datei speichern oder ausführen. Sobald Sie die `.msi`-Datei ausführen, wird der Setup-Assistent von VMware VDP for Exchange Server gestartet. Klicken Sie auf **Weiter**.

8 Lesen Sie sich auf der Seite **Endbenutzer-Lizenzvereinbarung** den Lizenztext durch und klicken Sie, sofern Sie zustimmen möchten, auf **Ich akzeptiere die Bedingungen des Lizenzvertrags** und dann auf **Weiter**.

9 Geben Sie auf der Seite **Appliance-Registrierungsinformationen** die IP-Adresse oder den vollständig qualifizierten Domainnamen der für das Exchange Server-Backup vorgesehenen VDP-Appliance ein und klicken Sie auf **Weiter**.

10 (Optional) Wählen Sie die Option zum Installieren des **Exchange Server GLR**-Plug-ins aus, wenn Sie den Server für granulare Recovery verwenden möchten.

HINWEIS Wenn Sie die Option „Exchange Server GLR“ auswählen, müssen Sie den Microsoft Exchange Server neu starten.

11 Klicken Sie auf der Seite **VMware VDP for Exchange Server kann jetzt installiert werden** auf **Installieren**.

12 Klicken Sie auf der Seite **Der Setup-Assistent von VMware VDP for Exchange Server wurde fertiggestellt** auf **Fertig stellen**.

Wenn Sie das Kontrollkästchen **VDP Exchange Backup User Configuration Tool** ausgewählt haben, fahren Sie mit dem Abschnitt „Verwenden des VMware Exchange Backup User Configuration Tool“ auf Seite 191 fort.

Wenn Sie nicht das Kontrollkästchen**VDP Exchange Backup Configuration Tool** ausgewählt haben, fahren Sie mit dem Abschnitt „Manuelles Konfigurieren des VDP-Backupdiensts“ auf Seite 192 fort.

Wiederholen Sie dieses Verfahren für zusätzliche Exchange Server-Rechner.

Installieren in einer DAG- oder Clusterumgebung

Verfahren

1 Exchange for VDP umfasst ein einziges, eigenständiges Installationsprogramm. Installieren Sie das VDP for Exchange Client-Plug-in auf jedem Microsoft Exchange Server-Rechner mit Mailbox-Serverrolle.

Um einen Server zwecks Recovery auf granularer Ebene (Granular Level Recovery, GLR) einzusetzen, wählen Sie die Optionen zur Installation des Exchange GLR-Plug-ins und des Exchange VSS-Plug-ins aus. In einer DAG-Umgebung sollten Sie mindestens einen Server für eine Recovery auf granularer Ebene konfigurieren.

HINWEIS Nach der Installation des Exchange GLR-Plug-ins müssen Sie den Exchange Server neu starten.

2 Registrieren Sie jeden Exchange Server als Client bei der VDP-Appliance.

3 Erstellen und konfigurieren Sie das VMwareVDPBackupUser-Konto.

4 Verwenden Sie den VMware VDP Windows Cluster Configuration Wizard, um den Exchange DAG Client bzw. den VDP-Clusterclient zu konfigurieren.

Konfigurieren eines Exchange DAG Client

Die Konfiguration eines Exchange DAG Client ermöglicht die Durchführung föderierter Datenbankbackups in einer Exchange Server 2013- oder Exchange Server 2010 DAG-Umgebung.

Voraussetzungen

Vergewissern Sie sich, dass die DAG-Clusterumgebung die folgenden Voraussetzungen erfüllt, bevor Sie den Exchange DAG Client konfigurieren.

- Der VDP Windows Client wurde installiert.
- Das VDP Backup-Plug-in für Exchange DAG wurde installiert.
- Die DAG-Gruppe ist vorhanden, wenn der DAG-Client für die Nodes bereits konfiguriert wurde.
- Für die Zuweisung zu dem neuen VDP Exchange DAG Client ist eine unbenutzte statische IP-Adresse verfügbar.
- Die Rechnerkonten für alle Cluster-Nodes müssen über einen Vollzugriff auf die SMB-Share verfügen.
- Das föderierte Exchange DAG-Backup muss über eine erstellte Netzwerk-Share verfügen (zur Verwendung als `var`-Verzeichnis).

Verfahren

1 Melden Sie sich mit dem VMwareVDPBackupUser-Konto bei einem Exchange Server in der DAG-Umgebung an.

2 Starten Sie den VMware VDP Windows Cluster Configuration Wizard:

- Öffnen Sie unter Windows Server 2012 den **Start**bildschirm und wählen Sie **VMware VDP Windows Cluster Configuration Wizard** aus.
- Öffnen Sie unter Windows Server 2008 das Menü **Start** und wählen Sie **Programme > VMware VDP > VMware VDP Windows Cluster Configuration Wizard** aus.

3 **Klicken Sie auf der Seite Willkommen** auf Weiter.

4 Wählen Sie auf der Seite **Plug-ins** die Option **Exchange DAG** aus und klicken Sie auf **Weiter**.

5 Gehen Sie auf der Seite **DAG-Nodes** wie folgt vor:

a Vergewissern Sie sich, dass die Umgebung die folgenden Anforderungen erfüllt:

- Laut Status sind alle Exchange Server aktiv.
- Der Installationsstatus der Windows-Clientsoftware für jeden Server ist „Installiert“.
- Der Installationsstatus des Exchange VSS-Plug-ins auf jedem Server ist „Installiert“.

b Klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite **Vorgänge** die Option **Neuen DAG-Client für alle Nodes konfigurieren** aus und klicken Sie auf **Weiter**.

7 Gehen Sie auf der Seite **Voraussetzungen** wie folgt vor:

a Vergewissern Sie sich, dass die Umgebung alle Voraussetzungen erfüllt.

Durch ein Häkchen neben einer Voraussetzung wird angegeben, dass die Umgebung die Voraussetzung erfüllt.

Wenn die Umgebung eine Voraussetzung nicht erfüllt, beenden Sie den Assistenten, beheben Sie das Problem und starten Sie den Assistenten erneut.

b Wählen Sie die Internetprotokollversion – IPv4 oder IPv6 – aus, die in der Umgebung verwendet wird.

c Klicken Sie auf **Weiter**.

8 Geben Sie auf der Seite **DAG-Clienteinstellungen** die Clienteinstellungen für die Clustergruppe für den DAG-Client an:

a Wählen Sie das Netzwerk aus der Netzwerkliste aus.

b Geben Sie die IP-Adresse für die Clustergruppe des DAG-Clients in das Feld **Exchange DAG Client IPv4-/IPv6-Adresse** ein. Die IP-Adresse muss eindeutig sein und darf noch nicht verwendet worden sein. Verwenden Sie nicht die DAG-IP-Adresse.

c Geben Sie die Netzwerkmaske für die Clustergruppe des DAG-Clients in das Feld **Exchange DAG-Client-IP-Subnetzmaske** ein.

d Klicken Sie auf **Weiter**.

9 Gehen Sie auf der Seite mit den Benutzereinstellungen wie folgt vor:

a Wählen Sie eines der folgenden Anmeldekonten aus:

- Lokales Systemkonto
- Dieses Konto (unter Angabe des Kontonamens und Passworts für das VMwareVDPBackupUser-Konto)

b Klicken Sie auf **Weiter**.

10 Geben Sie auf der Seite **Servereinstellungen** die Einstellungen für die VDP-Appliance an:

a Geben Sie entweder den DNS-Namen der VDP-Appliance in das Feld **Name** oder die IP-Adresse in das Feld **IPv4-/IPv6-Adresse** ein.

b Geben Sie den Namen der VDP-Domain für den Exchange DAG-Client in das Feld **VDP-Clientdomain für den DAG-Client** ein.

c Geben Sie den Datenport für die Kommunikation zwischen VDP-Client und -Server in das Feld **Portnummer** ein.

d Geben Sie den Pfad zum `var`-Ordner für den Clusterclient in das Feld **var-Verzeichnis von Clusterclient** ein oder klicken Sie auf **Durchsuchen**, um einen Speicherort auszuwählen.

Im `var`-Ordner werden die Exchange DAG Client-Konfiguration und -Protokolldateien gespeichert. Das VMwareVDPBackupUser-Konto und alle Nodes im Cluster müssen über Schreibzugriff auf diesen Speicherort verfügen.

HINWEIS Wählen Sie ein Volume aus, auf den alle Server in der DAG-Umgebung zugreifen können.

e Klicken Sie auf **Weiter**.

11 Prüfen Sie auf der Seite **Zusammenfassung** die Einstellungen, die Sie im Assistenten angegeben haben und klicken Sie auf **Konfigurieren**.

Die Seite **Progress** stellt den Status der Konfiguration bereit.

12 Überprüfen Sie die Informationen auf der Seite **Ergebnisse** und klicken Sie auf **Schließen**.

Verwenden des VMware Exchange Backup User Configuration Tool

Wenn das Kontrollkästchen **Exchange Backup User Configuration Utility starten** während der VMware VDP for Exchange Server Client-Installation aktiviert wird, wird das VMware Exchange Backup User Configuration Tool nach Abschluss der Installation automatisch gestartet.

VMwareVDPBackupUser-Konto

Für VDP Microsoft Exchange Server Client wird ein direkter Exchange Server-Zugriff benötigt. Ein spezielles Benutzerkonto, VMwareVDPBackupUser, ist erforderlich, um VDP die entsprechenden Domain- und Administratorberechtigungen bereitzustellen. Dieses Benutzerkonto wird durch das VDP Exchange Backup User Configuration Tool konfiguriert, das standardmäßig nach der VDP Microsoft Exchange Server Client-Installation ausgeführt wird.

HINWEIS Der VDP-Backup-Agent-Dienst muss nicht länger unter diesem Konto ausgeführt werden und auch der Benutzer muss nicht mehr das Kontrollkästchen **Backup-Agent konfigurieren** aktivieren. Wenn der VDP-Backup-Agent zur Ausführung unter dem lokalen Systemkonto konfiguriert ist, muss der Benutzer beim Erstellen von Backupjobs oder Durchführen von Backup- und Wiederherstellungsvorgängen Anmeldedaten eingeben.

VMwareVDPBackupUser ist durch Folgendes konfiguriert:

- Das Benutzerkonto wird hinzugefügt und für die entsprechenden Active Directory-, Exchange- und Gruppenkonten aktiviert. Das Benutzerkonto wird den folgenden Gruppen hinzugefügt:
  - Sicherungsoperatoren
  - Domänenbenutzer
  - Domänenadministrator (für Exchange Server 2007)
  - Exchange Server-Rechner
  - Exchange-Organisationsverwaltung (in Microsoft Exchange-Sicherheitsgruppen) für Exchange Server 2010 und 2013
  - Exchange-Organisationsadministratoren für Exchange Server 2007

- Eine Mailbox wird erstellt, aktiviert und für das Benutzerkonto getestet.
- Ein Benutzerkonto wird in der Exchange-Domain und dann auf jedem Exchange Server-Rechner mit VDP Microsoft Exchange Server Client konfiguriert und aktiviert. VDP-Backupdienste müssen zur Verwendung des VMwareVDPBackupUser-Kontos konfiguriert werden.

Voraussetzungen

- Vor der Verwendung von VDP müssen Sie die VDP-Appliance, wie unter „VDP-Installation und -Konfiguration" auf Seite 21 beschrieben, installieren und konfigurieren.
- Das Kontrollkästchen **Exchange Backup User Configuration Utility starten** muss während der VMware VDP for Exchange Server Client-Installation aktiviert werden. Wenn der Benutzer das Kontrollkästchen nicht bei der Installation aktiviert, kann der Benutzer das VMware Exchange Backup User Configuration Tool über folgenden Speicherort manuell starten:

  x:\programme\avp\bin\vmbackupusercfg.exe
- .NET 4.0 muss auf dem Exchange Server installiert sein:

Verfahren

1. Wählen Sie im VMware Exchange Backup User Configuration Tool abhängig vom Status des Benutzers, den Sie konfigurieren, die Option **Neuer Benutzer** oder **Vorhandener Benutzer** aus.
2. Geben Sie im Feld **Benutzername** einen Benutzernamen zum VMwareVDPBackupUser-Konto ein. Bei Bedarf können Sie den Standardnamen VMwareVDPBackupUser verwenden.
3. Geben Sie im Feld **Passwort** ein Passwort für das Konto ein.
4. Geben Sie das Passwort im Feld **Passwort bestätigen** erneut ein.
5. Wählen Sie im Feld **Exchange Server** den Namen des Exchange Server-Rechners aus, auf dem VDP Microsoft Exchange Server Client installiert wurde.
6. Wählen Sie im Feld **Speichergruppe** (nur für Exchange Server 2007 aktiv) den Speichergruppennamen aus.
7. Wählen Sie im Feld **Mailboxspeicher** die Mailboxdatenbank für das VMwareVDPBackupUser-Konto aus.
8. Klicken Sie auf **Prüfen**, um die neuen Benutzereinstellungen zu testen. Falls der Benutzer in Active Directory nicht vorhanden ist, schlägt die Prüfung fehl.
9. Klicken Sie auf **Services konfigurieren**.
10. Im Meldungsprotokoll wird eine Liste verschiedener Tests aufgeführt, die bestanden wurden oder erfolgreich waren. Wenn alle Prüfungen erfolgreich abgeschlossen wurden, klicken Sie auf **Schließen**.

Manuelles Konfigurieren des VDP-Backupdiensts

Wenn das VDP Exchange Backup User Configuration Tool schon ausgeführt wurde, ist das VMwareVDPBackupUser-Konto bereits erstellt. Die folgenden Schritte dienen der manuellen Konfiguration des VMwareVDPBackupUser-Kontos zur Ausführung des VDP-Backupdiensts.

- Vor der Verwendung von VDP müssen Sie die VDP-Appliance, wie unter „VDP-Installation und -Konfiguration" auf Seite 21 beschrieben, installieren und konfigurieren.
- Das VMwareVDPBackupUser-Konto wurde durch den Start des Exchange Backup User Configuration Utility erstellt.

Verfahren

1. Melden Sie sich bei Exchange Server als VMwareVDPBackupUser oder als ein anderer Benutzer mit Administratorrechten an.
2. Starten Sie die Dienstanwendung, indem Sie **Start** > **Programme** > **Verwaltung** > **Dienste** auswählen.

3 Klicken Sie im Fenster „Dienste“ in der Liste „Dienste“ mit der rechten Maustaste auf **Backup-Agent** und wählen Sie **Eigenschaften** aus.

4 Klicken Sie im Dialogfeld mit den Backup-Agent-Eigenschaften auf die Registerkarte **Anmelden**.

5 Wählen Sie die Schaltfläche **Dieses Konto** aus und geben Sie den vom VDP Exchange Backup User Configuration Tool erstellten Benutzernamen (standardmäßig VMwareVDPBackupUser) an.

6 Geben Sie das Passwort für das VMwareVDPBackupUser-Konto in die entsprechenden Felder zur **Passworteingabe** und **Passwortbestätigung** ein und klicken Sie auf **OK**.

7 Klicken Sie in der Liste „Dienste“ mit der rechten Maustaste auf den Dienst „Backup Agent“ und wählen Sie **Neu starten**.

HINWEIS Wenn GLR installiert ist, müssen Sie diesen Vorgang im „VMware VDP Exchange GLR Service“ ebenfalls wiederholen.

Erstellen von Backupjobs für Microsoft Exchange Server

Auf Microsoft Exchange Server-Clients muss VMware VDP Microsoft Exchange Server Client installiert sein, um für Backups verfügbar zu sein. Zusätzliche Informationen zur Clientinstallation finden Sie unter „Installieren von VDP for Exchange Server Client“ auf Seite 188.

1 Wählen Sie in vSphere Web Client die Registerkarte **Backup** aus.

2 Klicken Sie auf der Registerkarte **Backup** auf **Backupjobaktionen** und wählen Sie **Neu** aus, um den Assistenten **Neuen Backupjob erstellen** zu starten.

3 Wählen Sie auf der Seite „Jobtyp“ des Assistenten die Option **Anwendungen** aus. Mit dieser Option können Sie den kompletten Server oder ausgewählte Datenbanken sichern.

Der von Ihnen ausgewählte Jobtyp legt die Optionen fest, aus denen Sie ab diesem Zeitpunkt auswählen können. Befolgen Sie auf Grundlage Ihrer Auswahl die Anweisungen im entsprechenden nachstehenden Abschnitt.

Sichern von Anwendungen

Wenn Sie auf der Seite „Jobtyp“ **Anwendungen** auswählen, können Sie wahlweise Anwendungsserver oder individuelle Datenbanken sichern.

1 Wählen Sie auf der Seite **Jobtyp** des Assistenten zum Erstellen eines neuen Backupjobs die Option **Anwendungen** aus und klicken Sie auf **Weiter**.

2 Wählen Sie auf der Seite **Datentyp** eine der folgenden Optionen aus und klicken Sie auf **Weiter**:

- **Kompletter Server**: Über diese Option können Sie ganze Anwendungsserver sichern.
- **Ausgewählte Datenbanken**: Mit dieser Option können Sie einzelne Anwendungsserverdatenbanken sichern.

3 Klicken Sie auf der Seite **Backupquellen** auf den Pfeil neben **Microsoft Exchange Server**, um die Liste zu erweitern.

4 Führen Sie einen der folgenden Schritte aus:

HINWEIS Als Best Practice gilt die Auswahl nur eines Exchange Server-Rechners pro Backupjob.

- Falls Sie einen kompletten Server sichern möchten, klicken Sie auf das Kontrollkästchen neben dem zu sichernden Exchange Server und klicken Sie auf **Weiter**.
- Falls Sie ausgewählte Datenbanken sichern möchten, klicken Sie auf den Pfeil neben einem Exchange Server und führen Sie ein Drill-down durch, bis Sie die Datenbank- oder Speichergruppe auswählen können, die Sie sichern möchten. Klicken Sie dann auf **Weiter**. Wenn der Client als lokales Systemkonto ausgeführt wird, muss der Benutzer Exchange-Administrator-Anmeldedaten angeben, um einen Exchange Server-Drill-down durchführen zu können.

HINWEIS Falls das Backupziel ein Exchange 2007 Server ist, können Sie keine individuelle Datenbank auswählen und müssen stattdessen eine Speichergruppe auswählen.

5 Gehen Sie auf der Seite **Backupoptionen** wie folgt vor:

a Wählen Sie **Komplett** oder **Inkrementell** als Backuptyp aus. Inkrementelle Backups werden automatisch auf komplette Backups hochgestuft, sofern kein komplettes Backup vorhanden ist.

HINWEIS Wenn der Client als lokales Systemkonto ausgeführt wird, muss der Benutzer Exchange-Administrator-Anmeldedaten angeben. Bei einer Ausführung ohne lokales Systemkonto sind keine Anmeldedaten erforderlich.

Falls Sie **Inkrementell** auswählen, können Sie Umlaufprotokollierungsoptionen festlegen. Die Umlaufprotokollierung ermöglicht es Ihnen, die Anzahl von Transaktionsprotokollen auf dem System zu verringern. Für heterogene Umgebungen, in denen nicht für alle Speichergruppen bzw. Datenbanken die Umlaufprotokollierung aktiviert ist, können Sie eine dieser Einstellungen auswählen, um die Art und Weise der Verarbeitung inkrementeller Backups durch VDP festzulegen.

- **Promote** (Standardeinstellung): Durch diese Option wird ein inkrementelles Backup auf ein komplettes Backup hochgestuft, wenn für eine Datenbank im Saveset die Umlaufprotokollierung aktiviert wurde. Sämtliche Datenbanken werden gesichert, unabhängig davon, ob für sie die Umlaufprotokollierung aktiviert wurde. Wenn für eine oder mehrere Datenbanken die Umlaufprotokollierung aktiviert wurde, werden etwaige inkrementelle Backups aller Datenbanken im Saveset auf ein komplettes Backup hochgestuft.
- **Circular**: Durch diese Option werden alle inkrementellen Backups von sämtlichen Datenbanken mit aktivierter Umlaufprotokollierung auf ein komplettes Backup hochgestuft und alle Datenbanken ohne aktivierte Umlaufprotokollierung werden übersprungen.
- **Skip**: Durch diese Option wird ein inkrementelles Backup aller Datenbanken mit deaktivierter Umlaufprotokollierung durchgeführt und alle Datenbanken mit aktivierter Umlaufprotokollierung werden übersprungen.

b (Nur für DAG-Cluster verfügbar) Geben Sie im Listenfeld mit der **bevorzugten Serverreihenfolge** die Priorität der zum Sichern von Exchange-Datenbanken zu verwendenden Server an. Geben Sie den Servernamen und nicht den vollständig qualifizierten Domainnamen an. Mehrere Einträge müssen durch Komma getrennt werden. Wenn Sie keine Liste festlegen, fügt das Exchange VSS-Plug-in alle in der DAG vorhandenen Server der Liste alphabetisch sortiert hinzu.

c (Nur für DAG-Cluster verfügbar) Wählen Sie aus der Liste zum **Festlegen der vorzugsweise zu sichernden Datenbanktypen** den Typ der zu sichernden Datenbank aus:

- Wählen Sie **Passiv bevorzugt** aus, um eine passive Kopie jeder Datenbank zu sichern, sofern eine einwandfreie passive Kopie verfügbar ist. Wenn keine einwandfreie passive Kopie verfügbar ist, führt die VDP-Appliance ein Backup der aktiven Kopie durch.
- Wählen Sie **Aktiv**, damit ausschließlich die aktive Kopie einer jeden Datenbank gesichert wird.
- Wählen Sie **Passiv**, damit ausschließlich die passive Kopie einer jeden Datenbank gesichert wird. Wenn keine einwandfreie passive Kopie verfügbar ist, ist die Datenbank nicht im Backup enthalten.

6 Wählen Sie die Option **Multi-Stream-Backup aktivieren** aus, wenn Sie die parallele Verarbeitung von Backupjobs mithilfe mehrerer Prozessoren ermöglichen möchten. Legen Sie die Anzahl der zu verwendenden Streams mithilfe des Schiebereglers fest.

Es können bis zu zehn Streams verwendet werden. Jeder Stream erfordert einen separaten Prozessorkern. Durch Nutzung mehrerer Prozessoren lässt sich die Backupperformance steigern.

7 Klicken Sie auf **Weiter**.

8 Wählen Sie auf der Seite **Planung** die Backupplanung und die Startzeit für den Backupjob aus und klicken Sie auf **Weiter**.

Weitere Informationen zum Konfigurieren der Planung finden Sie unter „Festlegen der Backupplanung" auf Seite 125.

9 Legen Sie mithilfe der Optionen auf der Seite **Aufbewahrungs-Policy** fest, wie lange das Backup aufbewahrt werden soll. Klicken Sie dann auf **Weiter**.

Weitere Informationen zum Konfigurieren der Aufbewahrungs-Policy finden Sie unter „Festlegen der Aufbewahrungs-Policy" auf Seite 125.

10 Geben Sie auf der Seite **Name** einen Namen für den Backupjob ein und klicken Sie auf **Weiter**.

11 Überprüfen Sie auf der Seite **Bereit zur Fertigstellung** die Zusammenfassung zum Backupjob und klicken Sie dann auf **Fertig stellen**.

12 Klicken Sie auf **OK**, wenn eine Bestätigung über die erfolgreiche Erstellung des Backupjobs angezeigt wird.

Wiederherstellen von Microsoft Exchange Server-Backups

Nachdem Backups auf Microsoft Exchange Server-Rechnern ausgeführt wurden, ist es möglich, diese Backups an ihrem ursprünglichen Speicherort oder an einem anderen Speicherort wiederherzustellen.

ACHTUNG Der Microsoft Exchange Server-Zielrechner muss hinsichtlich Exchange Server-Version und Service Pack mit dem Exchange Server-Rechner, auf dem das Backup durchgeführt wurde, übereinstimmen. Anderenfalls schlägt die Wiederherstellung fehl.

Verfahren

1 Wählen Sie in vSphere Web Client die Registerkarte **Wiederherstellen** aus.

2 Klicken Sie auf den Client, dessen Backup Sie wiederherstellen möchten.

3 Klicken Sie auf das wiederherzustellende Backup.

4 Aktivieren Sie das Kontrollkästchen **Exchange-Informationsspeicher**, um den gesamten Inhalt des Backups wiederherzustellen.

5 Nachdem Sie alle Ziele ausgewählt haben, klicken Sie auf die Schaltfläche **Wiederherstellen**.

HINWEIS Wenn der Client als lokales Systemkonto ausgeführt wird, muss der Benutzer Exchange-Administrator-Anmeldedaten angeben. Bei einer Ausführung ohne lokales Systemkonto sind keine Anmeldedaten erforderlich.

6 Auf der Seite **Wiederherstellungsoptionen auswählen** ist die Option **Am ursprünglichen Speicherort wiederherstellen** die Standardeinstellung, die nicht geändert werden kann.

7 (Optional) Zur Recovery auf granularer Ebene (Granular Level Recovery, GLR) gehen Sie auf der Seite „Wiederherstellungsoptionen auswählen" wie folgt vor:

- **Restore to Original Location**: Deaktivieren Sie dieses Kontrollkästchen, wenn Sie einen anderen Client auswählen möchten, auf dem die RDB erstellt werden soll oder wenn Sie in ein anderes Postfach wiederherstellen möchten.
- **Zielclient**: Hierbei handelt es sich um den Exchange Server, auf dem die RDB erstellt und aus dem Backup gemountet wird. Der Client muss ein Exchange Server mit installiertem VDP Exchange GLR-Plug-in sein.
- **Zielpostfach**: Stellen Sie hier die E-Mail-Adresse des Postfachs ein, in der die ausgewählten Postfächer wiederhergestellt werden sollen.

8 Falls Sie erweiterte Optionen festlegen möchten, klicken Sie auf den Pfeil neben **Erweiterte Optionen**, um die Liste zu erweitern.

Geben Sie die folgenden Optionen an:

- **Allow database overwrite**: Erzwingt, dass alle vorhandenen Datenbanken überschrieben werden, die den- oder dieselben Namen im Wiederherstellungsjob aufweisen. Wenn diese Option aktiviert ist, wird das interne Exchange Server-Flag zum Zulassen von Dateiwiederherstellungen geändert.
- **Restore into RSG/RDB**: Wiederherstellungsspeichergruppen (Restore Storage Groups, RSG) werden in Exchange Server 2007 und Recovery-Datenbanken (Recovery Databases, RDB) in Exchange Server 2010 und Exchange Server 2013 verwendet. RSG/RDB dienen der Wiederherstellung in einer RSG/RDB statt in einer Produktionsdatenbank. Falls Sie **In RSG/RDB wiederherstellen** auswählen, können Sie die folgenden Optionen konfigurieren:
  - **Overwrite existing RSG/RDB**: Überschreibt alle vorhandenen RSG/RDB. Setzen Sie diese Option mit Vorsicht ein.
  - **RSG/RDB name**: Hierbei handelt es sich um den für die Wiederherstellung verwendeten RSG-/RDB-Namen. Sofern noch keine RSG/RDB mit dem angegebenen Namen vorhanden ist, wird diese erstellt. Wenn bereits eine RSG/RDB mit dem angegebenen Namen vorhanden ist, verwenden Sie zum Überschreiben die Option **Vorhandene RSG/RDB überschreiben**.
  - **RSG/RDB database path**: Der Pfad, unter dem die RSG-/RDB-Datenbankdatei wiederhergestellt wird (Beispiel: `C:\myrdb`). Hierbei handelt es sich um ein optionales Feld. Der Standardspeicherort wird verwendet, sofern dieses Feld leer gelassen wird.
  - **RSG/RDB log path**: Der Pfad, unter dem die RSG-/RDB-Protokolldatei wiederhergestellt wird (Beispiel: `C:\myrdb`). Hierbei handelt es sich um ein optionales Feld. Der Standardspeicherort wird verwendet, sofern dieses Feld leer gelassen wird.
- Sie können festlegen, dass Transaktionsprotokolle wiederhergestellt, aber nicht wiedergegeben werden, indem Sie das Kontrollkästchen **Transaktionsprotokolle nicht wiedergeben** aktivieren oder deaktivieren. Bei Auswahl dieser Option ist es Ihnen möglich, zusätzliche Transaktionsprotokolle vor dem Mounten der Datenbank manuell zu kopieren.
- Wenn während der Wiederherstellung Protokolldateikonflikte auftreten, geben Sie über das Feld **Protokollpfade verschieben** einen Speicherort an, in den die vorhandenen Protokolldateien vor der Wiederherstellung verschoben werden sollen. Wenn Sie keinen Pfad für die Protokolldateien angeben und es Lücken im Transaktionsprotokoll gibt, werden die aktuellen Transaktionsprotokolle im Zuge des Wiederherstellungsprozesses automatisch in einen Unterordner mit der Bezeichnung `logs_Uhrzeit_Datum` verschoben. Die Werte für Uhrzeit und Datum entsprechen der Uhrzeit und dem Datum der Wiederherstellung. Der Unterordner befindet sich im Transaktionsprotokoll-Ordner für die Datenbank oder Speichergruppe. Diese Protokolle können bei Bedarf zum Analysieren des Wiederherstellungsvorgangs oder bis zum Eintreten des Fehlers angewendet werden.
- Informationen zu den Wiederherstellungsoptionen für Exchange DAG-Clusterkonfigurationen finden Sie unter „Unterbrechen der Replikation in einer DAG oder einem Cluster" auf Seite 197.

9 Überprüfen Sie auf der Seite **Bereit zur Fertigstellung** die Wiederherstellungsanforderungen und klicken Sie auf **Fertig stellen**.

10 Klicken Sie in der Meldung, in der angegeben ist, dass die Wiederherstellung erfolgreich initiiert wurde, auf **OK**.

11 Überwachen Sie den Fortschritt der Wiederherstellung über das Fenster **Letzte Aufgaben**.

Unterbrechen der Replikation in einer DAG oder einem Cluster

Die VDP-Appliance unterbricht während einer Wiederherstellung die Replikation von aktiven Datenbanken oder Speichergruppen in passive Datenbanken oder Speichergruppen, wenn Sie während einer Wiederherstellung das Kontrollkästchen **Replikationsunterbrechung automatisieren** aktivieren.

Sie können die Replikation in passive Datenbanken oder Speichergruppen unterbrechen, indem Sie die Exchange-Verwaltungsshell vor der Wiederherstellung verwenden.

Verfahren

Geben Sie in Exchange Server 2013 oder 2010 den folgenden Befehl in die Exchange-Verwaltungsshell auf einem beliebigen Server in der DAG ein, um vor einer Wiederherstellung die Replikation in passive Datenbanken oder Speichergruppen zu unterbrechen:

suspend-MailboxDatabaseCopy -Identity *database***I**

Dabei steht `database` für den Namen der Datenbank und `server` für den Namen des DAG-Servers mit der passiven Kopie.

Überwachen der Clientaktivität

Sie können Aufgaben und Ereignisse für sämtliche Clientaktivitäten überwachen, indem Sie Clientprotokolle zusammenstellen und analysieren. Bei den Clientprotokollen handelt es sich um MSApp-bezogene Protokolle. (MSApp steht für Microsoft Application, also Microsoft-Anwendungen.) Das aggregierte Clientprotokoll umfasst alle Jobs des Typs „Replikation“, „Backup“, „Wiederherstellung“ bzw. „Automatische Backupverifizierung“ (ABV), die mit Ausnahmen abgeschlossen wurden oder fehlgeschlagen sind. Weitere Informationen erhalten Sie unter „Sammeln von VDP-Protokollen oder Diagnoseinformationen“ auf Seite 40.

Deinstallieren des Exchange Server-Plug-ins

Verwenden Sie zum Deinstallieren des Exchange Server-Plug-ins **Programme und Funktionen**.

Bei der Deinstallation des Exchange Server-Plug-ins wird das Exchange Server GLR-Plug-in automatisch deinstalliert. Nach der Deinstallation des Exchange Server-Plug-ins müssen Sie den Computer neu starten.

Granular Level Recovery auf Microsoft Exchange Server-Rechnern

Das VDP Plug-in for Exchange Granular Level Recovery (GLR) mountet ein temporäres virtuelles Laufwerk auf dem Zielserver und stellt aus einem Backup eine Exchange Server-Datenbank oder -Speichergruppe in einer Wiederherstellungsdatenbank (Recovery Database, RDB) oder Recovery-Speichergruppe (Recovery Storage Group, RSG) auf dem virtuellen Laufwerk wieder her.

Beachten Sie Folgendes:

- GLR in VDP unterstützt nur die Recovery auf Mailboxebene. GLR wird auf der Ebene einzelner Elemente nicht unterstützt.
- Bei dem Backup muss es sich um ein komplettes Backup mit dem VMware VDP Exchange Server-Plug-in handeln.
- Sie können GLR-Vorgänge für Backups ausführen, die Öffentliche Ordner-Datenbanken enthalten, Sie können GLR jedoch nicht zum Durchsuchen oder Wiederherstellen aus der Öffentliche Ordner-Datenbank selbst verwenden.

Systemanforderungen für GLR

Beim GLR-Prozess mit dem VDP Plug-in for Exchange Server GLR gelten zusätzlich zu den grundlegenden Anforderungen für Backup und Wiederherstellung weitere Computerhardware- und Ressourcenanforderungen. Tabelle 17-27 beschreibt die Systemanforderungen für das VDP Plug-in for Exchange Server GLR.

Tabelle 17-27. Systemanforderungen für GLR

Anforderung	Minimum
Speicher (RAM)	Das VDP Plug-in for Exchange Server GLR erfordert zusätzlichen Arbeitsspeicher (RAM). Beginnen Sie mit 1 GB RAM. Die erforderliche zusätzliche Speichermenge bzw. die Gesamtspeichermenge richtet sich nach der aktuellen Systemperformance mit dem vorhandenen Arbeitsspeicher: ■ Wenn die Ressourcen bereits ausgelastet sind und die Performance bei normalen Vorgängen des VDP Plug-in for Exchange Server VSS langsam ist, müssen Sie wesentlich mehr Arbeitsspeicher hinzufügen, damit die Vorgänge des VDP Plug-in for Exchange Server GLR unterstützt werden. ■ Wenn die Performance derzeit bei normalen Vorgängen des VDP Plug-in for Exchange Server VSS ausreichend ist, ist zusätzlicher Arbeitsspeicher u. U. nicht erforderlich, um Vorgänge des VDP Plug-in for Exchange Server GLR zu unterstützen.
Festplattenspeicher	Um einen Festplatten-Stagingbereich bereitzustellen, der die Exchange Server-Datenbank und -Protokolldateien enthält, ist zusätzlicher Festplattenspeicher erforderlich.

HINWEIS Ferner müssen Sie die neuesten MAPI-Client-Bibliotheken und CDO 1.2.1 von der Microsoft-Website herunterladen und die Bibliotheken und CDO auf jedem Exchange Server-Rechner mit dem Exchange Server GLR-Plug-in installieren. Einige Funktionen funktionieren möglicherweise erst, wenn Sie die neuesten Versionen installiert haben.

Multistreaming-Anforderungen

Für Multistreaming gelten zusätzlich zu den grundlegenden Anforderungen für das VDP Plug-in for Exchange Server VSS weitere Computerhardware- und Ressourcenanforderungen. Außerdem gibt es mehrere Konfigurationsempfehlungen für Multistreaming.

Tabelle 17-28 führt die Hardware- und Softwareanforderungen für Multistreaming auf.

Tabelle 17-28. Multistreaming-Anforderungen

Hardware und Software	Empfehlung
CPU	Mindestens ein Prozessorkern pro Stream
Speicher (RAM)	48 GB oder mehr
Festplatte	1 Festplattenlaufwerk für Betriebssystem/Exchange Server-Installation 1 bis 2 Festplattenlaufwerke oder RAID-Laufwerksgruppe für jede Exchange Server-Datenbank 7.200 U/min oder schnellere Festplattenlaufwerke
Netzwerkadapter	1 GB
Betriebssystem	Windows Server 2008 SP2 oder höher

Exchange Server-Konfigurationsanforderungen für Multistreaming

Mit Multistreaming verbraucht VDP wesentlich mehr CPU während Backups. Dieser zusätzliche CPU-Verbrauch auf einem aktiven Exchange Server-Rechner kann die Performance beeinträchtigen und sich auf den Anwender auswirken.

Sorgen Sie dafür, dass die Exchange Server-Umgebung den folgenden Anforderungen für Multistreaming entspricht:

- Platzieren Sie jede Datenbank auf einem separaten physischen Laufwerk. Platzieren Sie die Datenbankdatei falls möglich bei jeder Datenbank auf einer Festplatte und die Transaktionsprotokolle auf einer separaten Festplatte.
- Die besten Ergebnisse erzielen Sie, wenn jede Datenbank oder Speichergruppe ungefähr dieselbe Größe hat.

Wenn Sie Multistreaming-Optionen für ein Backup festlegen, geben Sie für jedes Laufwerk im Backup-Set höchstens einen Backup-Stream an. Beispiel:

- Wenn Sie zwei Datenbanken sichern und sich jede Datenbank auf einer eigenen Festplatte befindet, legen Sie maximal zwei Streams fest.
- Wenn Sie zwei Datenbanken sichern und sich jede Datenbank samt zugehörigen Protokollen auf zwei Festplatten (also insgesamt vier Festplatten) befindet, legen Sie maximal vier Streams fest.

VSS-Anforderungen

Das VDP Plug-in for Exchange Server VSS verwendet Microsoft Volume Shadow Copy Service(VSS)-Technologie zur Durchführung von Backups. VSS ist ein Framework, das die Durchführung von Volume-Backups ermöglicht, während Anwendungen in einem System in das Volume schreiben.

Unterstützte VSS Provider und Writer

Das Exchange Server VSS Plug-in verwendet den Microsoft Software Shadow Copy Provider und die folgenden VSS Writer:

- Microsoft Exchange Server Store VSS Writer
- Microsoft Exchange Server Replication VSS Writer

Das Exchange Server VSS-Plug-in unterstützt keine Hardwareprovider.

Volume-Anforderungen für VSS-Snapshots

Das Microsoft-VSS-Framework unterstützt bis zu 64 Volumes in einem VSS-Snapshot. Wenn Sie einen Dataset erstellen oder ein On-Demand-Backup durchführen, sollten Sie nicht mehr als 64 Volumes einschließen. Wenn Sie mehr als 64 Volumes in einem Snapshot einschließen, schlägt das Backup fehl und das Ereignisprotokoll führt den folgenden Fehler auf:

`VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED.`

Das VSS-Framework beschränkt die Anzahl der Schattenkopien auf 64 pro Volume. Wenn die Anzahl der Schattenkopien in einem Volume 64 übersteigt, schlägt das Backup fehl und das Ereignisprotokoll führt den folgenden Fehler auf:

`VSS_E_MAXIMUM_NUMBER_OF_SNAPSHOTS_REACHED.`

Aktivieren von GLR-Protokolldateien vor der Durchführung eines GLR

Mit GLR-Protokolldateien können Sie granulare Wiederherstellungen verfolgen und debuggen. Mithilfe der folgenden Schritte können Sie GLR-Protokolldateien aktivieren:

1 Erstellen Sie mithilfe eines Texteditors die Befehlsdatei im Ordner `C:\Programme\avp\var`, wobei `C:\Progamme\avp` der Installationsordner ist.

2 Speichern und schließen Sie die Befehlsdatei.

In Tabelle 17-29 sind die VDP-Protokolldateien aufgeführt, die Sie für die Nachverfolgung und das Debugging von GLR aktivieren können.

Tabelle 17-29. VDP-Protokolldateien

Protokolldatei	Inhalte	Flag zur Debuggingaktivierung	Befehlsdatei für Flags
`Axionfs.log`	Verfolgungs- und Debugginginformationen für AvFS-Dateisystemaufrufe	`--debug x19=327680`	`axionfs.cmd`
`avmapi.log`	Verfolgungs- und Debugginginformationen für MAPI-Aufrufe	`--debug`	`avmapi.cmd`
`avexglr_plugin.log`	Verfolgungs- und Debugginginformationen zur RDB- und RSG-Erstellung, zum Mounten, Durchsuchen und Wiederherstellen	`--debug`	`avexchglr.cmd`

Tabelle 17-29. VDP-Protokolldateien

`Aveexchglrsvc.log`	Verfolgungs- und Debugginginformationen zur RDB- und RSG-Erstellung, zum Mounten, Durchsuchen und Wiederherstellen	`--debug`	`aveexchglrsvc.cmd`
`ps_exec.log`	Verfolgungs- und Debugginginformationen zur Ausführung von PowerShell-Befehlen auf dem Exchange Server-Client	`--debug`	`ps_exec.cmd`

Sichern von Exchange Server-Datenbanken

Anweisungen zum Sichern von Exchange Server-Datenbanken finden Sie unter „Sichern von Anwendungen" auf Seite 182.

Wiederherstellen einzelner Mailboxen

HINWEIS Sie müssen alle RDBs auf dem Exchange Server-Zielrechner (2010 oder 2013) manuell löschen, bevor Sie eine granulare Recovery (Granular Level Recovery, GLR) durchführen. Beim GLR-Prozess werden RSGs auf Exchange Server 2007-Zielservern automatisch gelöscht.

Wenn Sie einzelne Mailboxen gesichert haben, können Sie individuelle Mailboxen aus der wiederherzustellenden Datenbank extrahieren und durchsuchen. Die ausgewählten Elemente werden aus der VDP-Appliance in einem Ordner für wiederhergestellte Elemente im ursprünglichen Postfach wiederhergestellt. Anschließend können Sie die Elemente durchsuchen und die Elemente, die Sie behalten möchten, auswählen. Anweisungen zum Wiederherstellen eines Backups auf granularer Ebene finden Sie unter „Wiederherstellen von Microsoft Exchange Server-Backups" auf Seite 195.

Das virtuelle Laufwerk wird automatisch ungemountet und die RDB oder RSG wird nach Abschluss der Wiederherstellung vom Zielserver für die GLR gelöscht. Exchange Server 2007 wird automatisch gelöscht. Exchange Server 2010 und 2013 müssen Sie vor der Durchführung einer GLR löschen.

Verfahren

1 Wählen Sie in vSphere Web Client die Registerkarte **Wiederherstellen** aus.

2 Wählen Sie das wiederherzustellende Backup aus und klicken Sie auf das Symbol **Wiederherstellen**, um den Assistenten „Backup wiederherstellen" zu starten.

   Die Seite „Backup auswählen" wird angezeigt.

3 Klicken Sie auf den Client, dessen Backup Sie wiederherstellen möchten.

4 Klicken Sie auf das wiederherzustellende Backup.

5 Wählen Sie die Wiederherstellung auf einer beliebigen Ebene in der Hierarchie aus. Bei der Wiederherstellung wird von einer GLR ausgegangen, wenn die Wiederherstellungsziele sich auf der Mailboxebene befinden.

   - Bei Microsoft Exchange 2007 Server-Rechnern sieht die Backuphierarchie folgendermaßen aus:

     Exchange Server-Name - > Backupdatum - > Exchange-Informationsspeicher - > Speichergruppen - > Datenbanken - > Mailboxen.

   - Bei Microsoft Exchange 2010- oder 2013-Servern sieht die Backuphierarchie folgendermaßen aus:

     Exchange Server-Name - > Backupdatum - > Exchange-Informationsspeicher - > Datenbanken - > Mailboxen.

6 Wenn alle Ziele ausgewählt wurden, klicken Sie auf die Schaltfläche **Wiederherstellen**.

HINWEIS Wenn der Client als lokales Systemkonto ausgeführt wird, muss der Benutzer Exchange-Administrator-Anmeldedaten angeben. Bei einer Clientausführung ohne lokales Systemkonto sind keine Anmeldedaten erforderlich.

7 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung“ die Wiederherstellungsanforderungen und klicken Sie auf **Fertig stellen**.

8 Klicken Sie auf **OK**, wenn eine Meldung angezeigt wird, dass Ihre Wiederherstellung erfolgreich initiiert wurde.

9 Überwachen Sie den Fortschritt der Wiederherstellung über das Fenster „Letzte Aufgaben“.

Sichern und Wiederherstellen von Microsoft SharePoint Server

VDP unterstützt Backups und Wiederherstellungen von Microsoft SharePoint Server-Rechnern. Derzeit wird nur ein SharePoint Server-System pro Farm unterstützt.

HINWEIS Wenn nur die SharePoint Server-Konfiguration oder Administratordatenbank wiederhergestellt wird, kann dies zu einer Beschädigung der SharePoint Server-Anwendung führen. Wenn Sie nicht nur Inhaltsdatenbanken wiederherstellen, müssen Sie daher das gesamte Backup wiederherstellen.

Hardwareanforderungen

Tabelle 17-30 führt die Hardwareanforderungen für Microsoft SharePoint Server auf.

Tabelle 17-30. Hardwareanforderungen für Microsoft SharePoint Server

Anforderung	Minimum
Speicher (RAM)	2 GB
Dateisysteme	NTFS

Unterstützte Microsoft SharePoint Server-Versionen

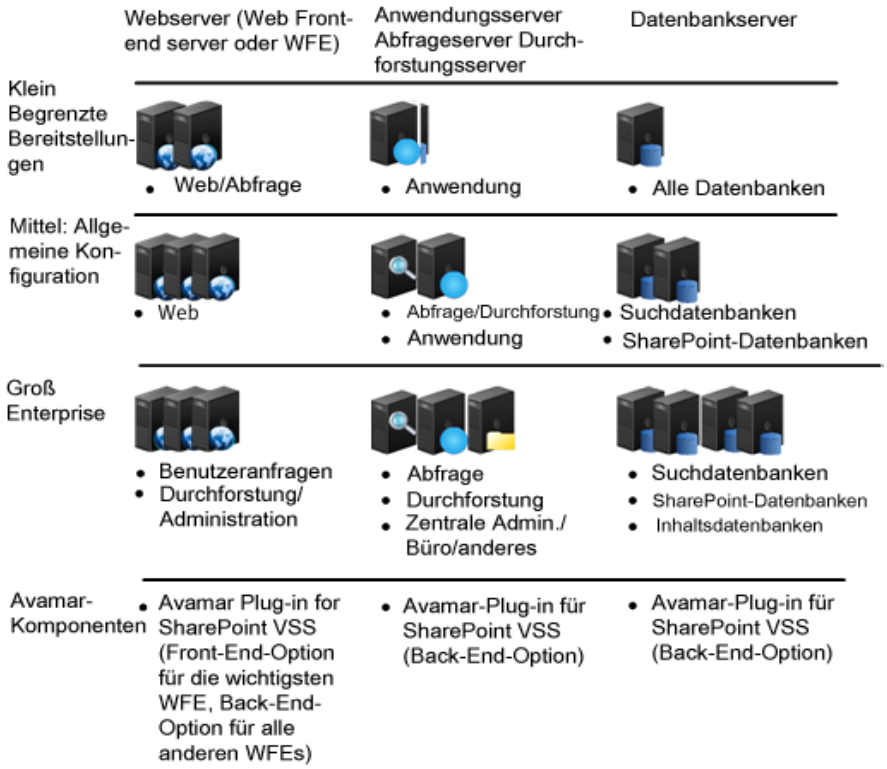
VDP unterstützt die folgenden Microsoft SharePoint Server-Versionen:

- SharePoint Server 2007 SP2 oder höher:
  - Windows Server 2008 R2
  - Windows Server 2008
- SharePoint Server 2010, 2010 SP1:
  - Windows Server 2008 SP2
  - Windows Server 2008 R2
- SharePoint Server 2013:
  - Windows Server 2012
  - Windows Server 2008 R2 SP1 oder höher
- SharePoint Server 2013 SP1:
  - Windows Server 2012 R2

Installieren von VDP for SharePoint Server Client

Installieren Sie das VDP-Client-Plug-in auf jedem SharePoint Server-Rechner in der Farm. Eine SharePoint-Farm ist eine Gruppe von SharePoint Servern, die zusammenarbeiten und eine Reihe von grundlegenden SharePoint Serverdiensten bereitstellen, die einen einzigen Standort unterstützen.

Die folgende Abbildung zeigt SharePoint Topologien für kleine, mittlere und große Farmen:



SharePoint Topologien**Einschränkungen**

Der SharePoint Server VSS Writer muss mit dem Administratorkonto der SharePoint Server-Farm ausgeführt werden.

Voraussetzungen

- Die VDP-Appliance muss, wie unter „VDP-Installation und -Konfiguration" auf Seite 21 beschrieben, installiert und konfiguriert sein.
- Sie benötigen lokale Administratorrechte für jeden SharePoint Server-Rechner.

Verfahren

1. Greifen Sie auf jedem SharePoint Server-Client auf vSphere Web Client zu:

   https://<*IP_Adresse_vCenter_Server***>:9443/vsphere-client/**

2. Geben Sie auf der Seite mit den **Anmeldedaten** einen Administratorbenutzernamen und ein Passwort für vCenter ein und klicken Sie auf **Anmelden**.
3. Wählen Sie in vSphere Web Client **VDP** aus.
4. Wählen Sie auf der **VDP-Begrüßungsseite** die VDP-Appliance aus und klicken Sie auf **Verbinden**.
5. Klicken Sie auf die Registerkarte **Konfiguration**.
6. Klicken Sie unter **Clientdownloads** auf **Microsoft SharePoint Server 64 Bit**. Je nach dem von Ihnen verwendeten Browser können Sie die `.msi`-Datei speichern oder ausführen.

   Der Setup-Assistent von VMware VDP for SharePoint Server wird gestartet.

7 Klicken Sie auf **Weiter**.

8 Lesen Sie sich auf der Seite **Endbenutzer-Lizenzvereinbarung** den Lizenztext durch und klicken Sie, sofern Sie zustimmen möchten, auf **Ich akzeptiere die Bedingungen des Lizenzvertrags** und dann auf **Weiter**.

9 Geben Sie auf der Seite mit den Appliance-**Anmeldedaten** die IP-Adresse oder den Namen der für das SharePoint Server-Backup vorgesehenen VDP-Appliance ein. Klicken Sie auf **Weiter**.

10 Klicken Sie auf der Seite **VMware VDP for SharePoint Server kann jetzt installiert werden** auf **Installieren**.

11 Legen Sie während der Installation fest, ob der für die Installation ausgewählte Server als primärer Backupserver (Front-end) fungieren soll oder ob er ein weiterer Mitgliedsserver der SharePoint Server-Farm (Back-end) ist.

HINWEIS Der Front-end-Server kann auf einem Farmserver installiert werden und es muss sich um einen Web-Front-end- oder Anwendungsserver handeln.

12 Klicken Sie auf der Seite **Der Setup-Assistent von VMware VDP for SharePoint Server wurde fertig gestellt** auf **Fertig stellen**.

Erstellen von Backupjobs für Microsoft SharePoint Server

Nach der Installation von VDP for SharePoint Server Client stehen die SharePoint-VM-Clients für Backups zur Verfügung.

1 Klicken Sie in vSphere Web Client auf die Registerkarte **Backup**.

2 Klicken Sie auf der Registerkarte **Backup** auf **Backupjobaktionen** und wählen Sie **Neu** aus, um den Assistenten **Neuen Backupjob erstellen** zu starten.

3 Wählen Sie auf der Seite „Jobtyp“ des Assistenten die Option **Anwendungen aus.** Diese Option sichert die SharePoint Server-Anwendung, die auf der virtuellen Maschine ausgeführt wird.

4 Klicken Sie auf **Weiter** und befolgen Sie die nachstehenden Anweisungen.

Sichern von Anwendungen

Es kann nur der gesamte SharePoint Server-Anwendungsserver gesichert werden. Das Backup einzelner Datenbanken wird in der aktuellen Version nicht unterstützt.

1 Wählen Sie auf der Seite **Datentyp** die Option **Kompletter Server** aus und klicken Sie auf **Weiter**.

2 Gehen Sie auf der Seite **Backupquellen** wie folgt vor:

   a Klicken Sie auf den Pfeil neben **Microsoft SharePoint Server**, um die Liste zu erweitern.

   b Wählen Sie das Kontrollkästchen neben dem zu sichernden SharePoint Server-Rechner aus.

   c Klicken Sie auf **Weiter**.

3 Führen Sie auf der Seite **Backupoptionen** ggf. einen Bildlauf nach unten durch, um den als Front-end installierten SharePoint Server zu finden:

   a Geben Sie im Abschnitt **Farmadministrator-Anmeldedaten** die **Anmelde-ID** und das **Anmeldepasswort** des Administrators ein.

   b Wählen Sie die Option **Multi-Stream-Backup aktivieren** aus, wenn mehrere Ausführungs-Threads während des Backups möglich sein sollen. Legen Sie die Anzahl der zu verwendenden Streams mithilfe des Schiebereglers fest und wählen Sie im Menü **Gruppieren nach** die Option **Datenbank** oder **Volume** aus.

   c Klicken Sie auf **Weiter**.

4 Wählen Sie auf der Seite **Planung** die Backupplanung und die Startzeit für den Backupjob aus und klicken Sie auf **Weiter**.

5 Legen Sie mithilfe der Optionen auf der Seite **Aufbewahrungs-Policy** fest, wie lange das Backup aufbewahrt werden soll. Klicken Sie dann auf **Weiter**.

6 Geben Sie auf der Seite **Name** einen Namen für den Backupjob ein und klicken Sie auf **Weiter**.

7 Überprüfen Sie Ihre Auswahl auf der Seite **Bereit zur Fertigstellung**.

Wenn die Einstellungen korrekt sind, klicken Sie auf **Fertig stellen**. Sind die Einstellungen nicht korrekt, klicken Sie auf **Zurück**, um zur entsprechenden Seite im Assistenten zu navigieren.

Wiederherstellen von Microsoft SharePoint Server-Backups

Nachdem Backups auf SharePoint Server-Rechnern ausgeführt wurden, ist es möglich, diese Backups an ihrem ursprünglichen Speicherort oder an einem anderen Speicherort wiederherzustellen.

1 Klicken Sie in vSphere Web Client auf die Registerkarte **Wiederherstellen**.

2 Wählen Sie das wiederherzustellende Backup aus und klicken Sie auf das Symbol **Wiederherstellen**.

3 Wählen Sie auf der Seite **Backup auswählen** den Backupjob aus, den Sie wiederherstellen möchten. Die Auswahl mehrerer SharePoint Server-Rechner ist zwar möglich, allerdings kann nur ein Wiederherstellungspunkt pro Server ausgewählt werden. Erstellen (oder bestätigen) Sie die Backupjobs für die Wiederherstellung und klicken Sie auf **Weiter**.

4 Gehen Sie auf der Seite **Wiederherstellungsoptionen auswählen** wie folgt vor:

a Führen Sie einen der folgenden Schritte aus:

- Lassen Sie die Option **Am ursprünglichen Speicherort wiederherstellen** ausgewählt (die Standardeinstellung), um das Backup an seinem ursprünglichen Speicherort wiederherzustellen.
- Deaktivieren Sie die Option **Am ursprünglichen Speicherort wiederherstellen**, um das Backup an einem anderen Speicherort wiederherzustellen. Klicken Sie auf **Auswählen**, um ein Ziel auszuwählen, und geben Sie den vollständigen Windows-Pfad zum Speicherort auf dem Ziel an, an dem das Backup wiederhergestellt wird.

b Um erweiterte Optionen festzulegen, klicken Sie auf den Pfeil neben **Erweiterte Optionen**, um die Liste zu erweitern.

- **Anmelde-ID**: Geben Sie die Anmelde-ID des SharePoint Server-Administrators ein. Das Format lautet wie folgt: **DOMAIN\benutzer**.
- **Anmeldepasswort**: Geben Sie das zum Anmelden beim Zielclient verwendete Passwort des Farmadministrators ein.
- **Anwendungspool** (optional) Geben Sie für SharePoint Server 2013 den Namen eines vorhandenen Anwendungspools ein, in den die Search Service Application wiederhergestellt wird.
- **Verschlüsselungsmethode**: Wählen Sie eine Verschlüsselungsmethode aus der Liste aus.
- **Erweiterte Optionen** (nur Support): Geben Sie in dieses Feld nichts ein. Es ist ausschließlich zur Verwendung durch den EMC Support bestimmt.

c Klicken Sie auf **Weiter**.

5 Überprüfen Sie Ihre Auswahl auf der Seite **Bereit zur Fertigstellung**. Ist sie korrekt, klicken Sie auf **Fertig stellen**. Sind die Einstellungen nicht korrekt, klicken Sie auf **Zurück**, um die richtige Konfiguration zu erstellen.

6 Klicken Sie in der Meldung, in der angegeben ist, dass die Wiederherstellung erfolgreich initiiert wurde, auf **OK**.

7 Überwachen Sie den Fortschritt der Wiederherstellung über das Fenster **Letzte Aufgaben**.

Überwachen der Clientaktivität

Sie können Aufgaben und Ereignisse für sämtliche Clientaktivitäten überwachen, indem Sie Clientprotokolle zusammenstellen und analysieren. Bei den Clientprotokollen handelt es sich um MSApp-bezogene Protokolle. (MSApp steht für Microsoft Application, also Microsoft-Anwendungen.) Das aggregierte Clientprotokoll umfasst alle Jobs des Typs „Replikation“, „Backup“, „Wiederherstellung“ bzw. „Automatische Backupverifizierung“ (ABV), die mit Ausnahmen abgeschlossen wurden oder fehlgeschlagen sind. Weitere Informationen erhalten Sie unter „Sammeln von VDP-Protokollen oder Diagnoseinformationen” auf Seite 40.

Deinstallieren von VDP Plug-in for SharePoint Server

Um auf einer Windows Server 2008- oder Windows Server 2012-Installation VDP Plug-in for SharePoint Server zu deinstallieren, verwenden Sie **Programme und Funktionen**.

VDP Disaster Recovery 18

In diesem Kapitel wird folgendes Thema behandelt:

Grundlegende Disaster Recovery

Im Notfall können Sie die Daten oder die VDP-Appliance über verschiedene Methoden wiederherstellen.

- Verwenden der VDP-Kontrollpunkte

  VDP verfügt über robuste Speicher- und Managementfunktionen für Backups. Bei einem Ausfall ist als erste Maßnahme ein Rollback auf einen bekannten validierten Kontrollpunkt durchzuführen (siehe „Rollback einer Appliance" auf Seite 43).

- Verwenden der Data Domain-Kontrollpunktkopie

  Wenn Sie die Data Domain-Integration in der Umgebung verwenden, können Sie die Kontrollpunktkopiefunktion verwenden, um die fehlgeschlagene VDP-Appliance wiederherzustellen. Die Kontrollpunktkopie erstellt ein Backup der VDP-Kontrollpunkte auf Data Domain. Sie können diese Kontrollpunkte verwenden, um die VDP-Appliance bei einem Ausfall wiederherzustellen. „Wiederherstellen der Avamar-Kontrollpunktbackups von Data Domain-Systemen" auf Seite 100 bietet Informationen dazu.

- Trennen und erneutes Anbinden von VDP-Speicher

  Im Fall eines reinen Appliance-Betriebssystem-Festplattenausfalls oder einer Beschädigung können Sie VDP erneut bereitstellen und Datenfestplatten der fehlgeschlagenen VDP erneut anbinden. „Trennen und erneutes Anbinden von Speicher" auf Seite 81 bietet Informationen dazu.

- Verwenden der Replikation

  Sie können die Replikationsfunktion von VDP verwenden, um Daten im Notfall wiederherzustellen. Sie können die Backups auf eine Remote-VDP-Appliance replizieren. Damit können Sie die Daten von der sekundären VDP-Appliance im Notfall auf der primären VDP-Appliance wiederherstellen. „Replikation" auf Seite 151 bietet Informationen dazu.

Von VDP verwendete Ports

A

In Tabelle A-31 sind die von VDP verwendeten Ports aufgeführt.

Tabelle A-31. Von VDP verwendete Ports

Produkt	Port	Protokoll	Quelle	Ziel	Zweck
VDP	7	TCP	VDP	Data Domain-System	ECHO-Service Erforderlich zum Registrieren eines Data Domain-Systems
VDP	21	TCP	VDP	FTP-Server	FTP
VDP	22	TCP	User	VDP	SSH-Zugriff (Secure Shell) zum Debuggen
VDP	23	TCP	VDP	Intern	Intern
VDP	25	TCP	VDP	EMC Customer Service	SFTP
VDP	53	TCP/UDP	VDP	DNS-Server	Für Namensauflösung erforderlich
VDP	67	UDP	DHCP-Server	VDP	DHCP
VDP	68	UDP	VDP	DHCP-Server	DHCP
VDP	69	TCP	Interner Switch	VDP	TFTP
VDP	80	TCP	VDP	vCenter	HTTP für die Lizenzierung
VDP	88	TCP/UDP	VDP	Key Distribution Center (KDC)	SMTP
VDP	111	TCP/UDP	VDP	vSphere-Host	Zugriff auf die RPC-Port-Mapper-Funktion Erforderlich, wenn Backups auf einem Data Domain-System gespeichert sind
VDP	123	TCP/UDP	NTP-Zeitserver	VDP	NTP
VDP	161	TCP	Data Domain-System	VDP	Getter-/Setter-Port für SNMP-Objekte von einem Data Domain-System Erforderlich zum Speichern von Avamar Clientbackups auf einem Data Domain-System
VDP	162	TCP/UDP	VDP	SNMP-Agent	SNMP-Traps
VDP	163	TCP	VDP	SNMP-Service auf Data Domain	MC SNMP Manager
VDP	389	TCP/UDP	VDP	LDAP	LDAP

Tabelle A-31. Von VDP verwendete Ports

Produkt	Port	Protokoll	Quelle	Ziel	Zweck
VDP	443	TCP	VDP	vCenter oder SSO	https
VDP	464	TCP/UDP	VDP	vCenter	Kerberos
VDP	514	UDP	Utility-Node- oder Single-Node-Server	VDP	SYSLOG
VDP	700	TCP	VDP LDAP	Active Directory	Loginmgr tool
VDP	703	TCP	Avamar-Server-Nodes	VDP	AKM-Service
VDP	902	TCP	VDP	VMware ESX-Serverproxy	VMware ESX-Serverproxyservice
VDP	2049	TCP/UDP	VDP	NFS-Daemon auf Data Domain-System	NFS-Daemon auf Data Domain-System
VDP	2052	TCP/UDP	VDP	NFS-Mount-Prozess auf Data Domain-System	NFS-Mount-Prozess auf Data Domain-System
VDP	2888	TCP	Avamar Extended Retention – Medienzugriffs-Node	VDP	AVDTO Erforderlich für den Support von Avamar Extended Retention
VDP	3008	TCP	VDP	Aktiver Archivierungsservice auf Data Domain-System	Aktiver Archivierungsservice auf Data Domain-System
VDP	5480	TCP	VDP	Externer Proxy	Externer Proxy
VDP	5489	TCP	VDP	Avamar-Proxy	Proxyservice
VDP	5555	TCP	■ Utility-Node, auf dem Avamar Client Manager ausgeführt wird ■ PostgreSQL-Administratorclientcomputer	VDP	PostgreSQL-Administratorserver
VDP	5568	TCP	Avamar Extended Retention – Medienzugriffs-Node	VDP	PostgreSQL
VDP	5671	TCP	■ Localhost ■ Andere Avamar-Utility-Nodes ■ Avamar Extended Retention-Computer ■ EMC Backup and Recovery Manager-Computer	VDP	RabbitMQ

Tabelle A-31. Von VDP verwendete Ports

Produkt	Port	Protokoll	Quelle	Ziel	Zweck
VDP	6667	TCP	Avamar Extended Retention – Medienzugriffs-Node	VDP	Archivierungsserviceevent
VDP	7.000	TCP	Avamar Extended Retention – Medienzugriffs-Node	VDP	Apache Tomcat
VDP	7443	TCP	Avamar Extended Retention – Medienzugriffs-Node	VDP	Apache Tomcat
VDP	7444	TCP	VDP	VMware vCenter	VMware vCenter-Kommunikationsport
VDP	7778	TCP	Avamar-Administratormanagementkonsole	VDP	RMI
VDP	7779	TCP	Avamar-Administratormanagementkonsole	VDP	RMI
VDP	7780	TCP	Avamar-Administratormanagementkonsole	VDP	RMI
VDP	7781	TCP	Avamar-Administratormanagementkonsole	VDP	RMI
VDP	7937–9936	TCP/UDP	VDP	NetWorker-Server	NetWorker-Service
VDP	8080	TCP	VDP	NetWorker-Server	Kommunikationsport für NetWorker-Server
VDP	8105	TCP	Clientcomputer	VDP	Apache Tomcat
VDP	8109	TCP	Clientcomputer	VDP	Apache Tomcat
VDP	8181	TCP	Clientcomputer	VDP	HTTP
VDP	8444	TCP	Webbrow‑serclients	VDP	HTTPS
VDP	8505	TCP	Utility-Node- oder Single-Node-Server	VDP	Apache Tomcat
VDP	8509	TCP	Utility-Node- oder Single-Node-Server	VDP	Apache Tomcat-AJP-Connector
VDP	8543	TCP	vSphere Web Client	VDP	Redirect for Tomcat
VDP	8580	TCP	vCenter	VDP	VDP Downloader
VDP	9443	TCP	vCenter	VDP	VDP Web Services
VDP	19000	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN
VDP	19500	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN
VDP	20.000	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN

Tabelle A-31. Von VDP verwendete Ports

Produkt	Port	Protokoll	Quelle	Ziel	Zweck
VDP	20500	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN
VDP	25000	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN
VDP	25500	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN
VDP	26000	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN
VDP	26500	TCP/UDP	Avamar-Server-Nodes	VDP	GSAN
VDP	27000	TCP	VDP	vCenter	Licensing communication
Hinweis: VDP setzt zur Lizenzierung voraus, dass der Port 27000 offen ist. Port 27000 ist für die vCenter-Kommunikation nicht erforderlich.					
VDP	27500	TCP	Avamar-Server-Nodes oder Replikatorquell-Node	VDP	Avamar-Server
VDP	28001	TCP	Clientcomputer, VMWare-Proxy	VDP	Avamar-Server-CLI, MCS
VDP	28002–28011	TCP	Avamar Extended Retention – Medienzugriffs-Node	VDP	Support für Avamar Extended Retention
VDP	28009	TCP	VMware-Proxy	VDP	avagent
VDP	29000	TCP	Clientcomputer	VDP	Avamar-Server-SSL
VDP	30001	TCP	Clientcomputer VMware-Proxy	VDP	MCS
VDP	30002	TCP	VDP	Clientcomputer	Erforderlich für Client- oder Avagent-Verbindungen
VDP	30003	TCP	Clientcomputer	VDP	MCS
VDP	30102–30109	TCP	VMware-Proxy	VDP	avagent
VDP	61617	TCP	Avamar Extended Retention – Medienzugriffs-Node	VDP	Apache ActiveMQ-SSL
VDP	61619	TCP	VDP	Client, auf dem EMC Backup and Recovery Manager ausgeführt wird	Erforderlich zum Zulassen der Kommunikation mit EMC Backup and Recovery Manager

Minimal erforderliche vCenter-Benutzerkontorechte

B

Informationen zum Konfigurieren von VDP-Benutzern oder SSO-Admin-Benutzern mit vSphere Web Client finden Sie unter „Konfiguration des Benutzerkontos“ auf Seite 25. In sicherheitssensiblen Umgebungen können Sie die zum Konfigurieren und Verwalten der VDP-Appliance erforderlichen vCenter-Benutzerkontorechte auf folgende Kategorien beschränken:

Alarme

- Erstellen
- Ändern

Datenspeicher

- Speicherplatz zuweisen
- Datenspeicher durchsuchen
- Datenspeicher konfigurieren (für VSAN-Unterstützung)
- Spezielle Dateivorgänge
- Datenspeicher verschieben
- Datenspeicher entfernen
- Datei entfernen
- Datenspeicher umbenennen

Erweiterung

- Erweiterung registrieren
- Erweiterungen aktualisieren

Ordner

- Ordner anlegen

Global

- Aufgabe abbrechen
- Methoden deaktivieren
- Methoden aktivieren
- Lizenzen
- Ereignis protokollieren
- Benutzerdefinierte Attribute managen
- Einstellungen

Netzwerk

- Netzwerk zuweisen
- Konfigurieren

Ressource

- Virtuelle Maschine dem Ressourcenpool zuweisen

Sitzungen

- Sitzung validieren

Aufgaben

- Aufgabe erstellen
- Aufgabe aktualisieren

Virtuelle Maschine > Konfiguration

- Vorhandene Festplatte hinzufügen
- Neue Festplatte hinzufügen
- Gerät hinzufügen oder entfernen
- Advanced
- CPU-Anzahl ändern
- Ressource ändern
- Festplattenwechsel nachverfolgen
- Festplatten-Leasing
- Virtuelles Laufwerk erweitern
- Host-USB-Gerät
- Speicher
- Geräteeinstellung ändern
- Raw-Gerät
- Von Pfad neu laden
- Festplatte entfernen
- Umbenennen
- Gastinformationen zurücksetzen
- Anmerkung festlegen
- Einstellungen
- Auslagerungsdatei platzieren
- VM-Kompatibilität aktualisieren

Virtuelle Maschine > Gastvorgänge

- Änderungen Gastvorgänge
- Programmausführung Gastvorgänge
- Abfragen Gastvorgänge

Virtuelle Maschine > Interaktion

- Konsoleninteraktion
- Geräteverbindung
- Management von Gastbetriebssystem durch VIX API
- Ausschalten
- Einschalten
- Zurücksetzen
- VMware Tools-Installation

Virtuelle Maschine > Bestand

- Neu erstellen
- Registrieren
- Entfernen
- Registrierung aufheben

Virtuelle Maschine > Provisioning

- Festplattenzugriff zulassen
- Schreibgeschützten Festplattenzugriff zulassen
- VM-Download zulassen
- Als Vorlage markieren

Virtuelle Maschine > Snapshot-Management

- Snapshot erstellen
- Snapshot entfernen
- Zu Snapshot zurückkehren

vApp

- Export
- Import
- vApp-Anwendungskonfiguration

VDP-Troubleshooting

C

In diesem Kapitel werden folgende Troubleshooting-Themen behandelt:

Troubleshooting der VDP-Appliance-Installation

Gehen Sie bei Problemen im Zusammenhang mit der Installation der vSphere Data Protection(VDP)-Appliance wie folgt vor:

- Vergewissern Sie sich, dass sämtliche Software die Softwaremindestanforderungen erfüllt. Weitere Informationen finden Sie unter „Softwareanforderungen" auf Seite 22.
- Vergewissern Sie sich, dass sämtliche Hardware die Hardwaremindestanforderungen erfüllt. Weitere Informationen finden Sie unter „Systemanforderungen" auf Seite 23.
- Vergewissern Sie sich, dass die DNS-Konfiguration für die VDP-Appliance ordnungsgemäß durchgeführt wurde. Weitere Informationen finden Sie unter „Konfiguration vor der Installation" auf Seite 24.

Troubleshooting des Installationsprogrammpakets

Upgradebezogene Protokolle, die beim Troubleshooting verwendet werden können, finden Sie in der Datei `avinstaller.log.0` im Protokollbündel.

Troubleshooting des VDP-Managements

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme beim Management von VDP identifiziert und behoben werden können.

Die VDP-Appliance reagiert nicht. Bitte versuchen Sie es erneut

Wenn bisher eine VDP-Verbindung hergestellt werden konnte und diese Meldung angezeigt wird, überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass der Benutzername oder das Passwort, der bzw. das zur VDP-Validierung bei vCenter Server verwendet wird, nicht geändert wurde. Nur ein Benutzerkonto und Passwort werden zur VDP-Validierung verwendet. Dies wird durch das Dienstprogramm VDP-configure konfiguriert. Zusätzliche Informationen finden Sie unter „vCenter Server-Registrierung" auf Seite 43.
- Vergewissern Sie sich, dass die Netzwerkeinstellungen für die IP- und DNS-Konfiguration seit der VDP-Erstinstallation nicht geändert wurden. Zusätzliche Informationen finden Sie unter „DNS-Konfiguration" auf Seite 24.

Das VDP-Plug-in antwortet nicht.

Wenn das VDP-Plug-in in der vCenter-Benutzeroberfläche die Meldung **Das VDP-Plug-in antwortet nicht** anzeigt, ist meistens ein oder mehr Services der VDP-Appliance oder die gesamte VDP-Appliance inaktiv.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1 Pingen Sie die VDP-Appliance von einer Remotemaschine an, indem Sie den folgenden Befehl ausführen:

ping <IP_Adresse_der_VDP_Appliance>

Wenn in der Ausgabe ein Meldungsverlust von 100 % angezeigt wird, ist die VDP-Appliance entweder inaktiv oder nicht erreichbar. Starten Sie die VDP-Appliance, indem Sie sich bei vCenter Server anmelden, der diese VDP-Appliance managt, oder die Netzwerkprobleme beheben.

2 Öffnen Sie das VDP-Konfigurationsdienstprogramm über die folgende URL:

https://<IP_Adresse_der_VDP_Appliance>**:8543/vdp-configure/**

Wenn diese Seite nicht ordnungsgemäß angezeigt wird, wurde der Tomcat-Anwendungsserver angehalten. Melden Sie sich bei der VDP-Appliance über den SSH-Client (Putty) an und starten Sie den Tomcat-Service neu, indem Sie den folgenden Befehl ausführen:

emwebapp.sh -restart

Troubleshooting des VDP-Backups

Die folgenden Troubleshooting-Themen beschreiben, wie gängige Probleme mit Backups identifiziert und behoben werden können.

Backupjobdaten werden geladen

Diese Meldung kann über längere Zeit (bis zu fünf Minuten) angezeigt werden, wenn eine große Anzahl virtueller Maschinen (ca. 100 virtuelle Maschinen) für einen einzigen Backupjob ausgewählt wird. Diese Meldung kann auch bei Aktionen zum Sperren/Entsperren, Aktualisieren oder Löschen für große Jobs angezeigt werden. Wenn sehr große Jobs ausgewählt werden, handelt es sich hierbei um erwartetes Verhalten. Im Hinblick auf diese Meldung sind keine Maßnahmen erforderlich. Nach Abschluss der Aktion wird sie nicht mehr angezeigt. Dies kann bis zu fünf Minuten dauern.

Client {Clientname} konnte beim Erstellen des Backupjobs {Backupjobname} der VDP-Appliance nicht hinzugefügt werden

Dieser Fehler kann auftreten, wenn ein doppelter Clientname im vApp-Container bzw. auf dem vSphere-Host vorhanden ist. In diesem Fall wird nur ein Backupjob hinzugefügt. Korrigieren Sie etwaig vorhandene doppelte Clientnamen.

Die folgenden Elemente konnten nicht gefunden werden und wurden nicht ausgewählt: {Clientname}

Dieser Fehler kann auftreten, wenn ein Auffinden der gesicherten virtuellen Maschinen während der Bearbeitung eines Backupjobs nicht möglich ist. Dies ist ein bekanntes Problem.

VMDK-Backupjob schlägt automatisch fehl, wenn eine einzelne VMDK an einen anderen Datenspeicher migriert wird

Während einer Migration einer einzelnen VMDK von einem Datenspeicher zu einem anderen versucht VDP, alle Backupjobs zu aktualisieren, die die migrierte Festplatte enthalten. In einigen Fällen kann VDP nicht genau bestimmen, wohin die vom Backupjob verwiesene Festplatte migriert wurde. In diesem Fall wird der Backupjob nicht aktualisiert. Eine Instanz dieses Problems tritt auf, wenn sich der Festplattenordnername im neuen Datenspeicher von dem Ordner im ursprünglichen Datenspeicher unterscheidet. Wenn VDP nicht bestimmen kann, wohin die VMDK migriert wurde, sendet VDP eine vCenter-Warnmeldung mit der Mitteilung, dass der Backupjob möglicherweise nicht mehr genau ist.

Wenn die VDP-Appliance heruntergefahren wird oder der Service `emwebapp.sh` zum Zeitpunkt der VMDK-Migration angehalten wird, kann VDP die Migration nicht erkennen. Die Backupjobs werden nicht aktualisiert. Wenn Backupjobs nicht synchronisiert sind, wird keine Warnmeldung an vCenter gesendet. Wenn ein Backupjob nicht mit dem Standort der VMDK synchronisiert ist, wird der Backupjob weiterhin erfolgreich abgeschlossen, sichert aber die migrierte Festplatte nicht mehr.

Sie können dieses Problem lösen, indem Sie den Backupjob aktualisieren. Fügen Sie dann die migrierte VMDK erneut zum Backupjob hinzu, indem Sie das VDP vCenter-Plug-in verwenden.

Backup schlägt fehl, wenn die VDP-Datenspeicherkapazität unzureichend ist

Geplante Backups schlagen bei zu 92 % abgeschlossenem Vorgang fehl, wenn die Datenspeicherkapazität nicht ausreicht. Wenn der VDP-Datenspeicher mit Thin Provisioning konfiguriert ist und die maximale Kapazität nicht erreicht wurde, fügen Sie zusätzliche Speicherressourcen hinzu.

Backup schlägt fehl, wenn für eine virtuelle Maschine VMware Fault Tolerance aktiviert ist

Wenn für eine virtuelle Maschine VMware Fault Tolerance aktiviert ist, schlägt das Backup fehl. Hierbei handelt es sich um erwartetes Verhalten. VDP unterstützt kein Backup von virtuellen Maschinen mit aktivierter VMware Fault Tolerance.

Wenn virtuelle Maschinen in oder aus verschiedenen Clustergruppen verschoben werden, gehen damit verknüpfte Backupquellen u. U. verloren

Wenn Hosts in Cluster mit der Option zum Aufbewahren der Ressourcenpools und vApps verschoben werden, werden die Container neu erstellt und nicht kopiert. Daher handelt es sich nicht länger um denselben Container, auch wenn der Name identisch ist. Validieren Sie nach dem Verschieben von Hosts in und aus Clustern alle Backupjobs, die Container schützen, oder erstellen Sie diese neu.

Nach einem unerwarteten Herunterfahren-Vorgang gehen aktuelle Backupjobs und Backups verloren

Bei jedem unerwarteten Herunterfahren führt die VDP-Appliance ein Rollback auf den zuletzt validierten Kontrollpunkt aus. Hierbei handelt es sich um erwartetes Verhalten. Zusätzliche Informationen finden Sie unter „Rollback einer Appliance" auf Seite 43.

vMotion-Vorgänge sind während aktiver Backupvorgänge nicht zulässig

vSphere vMotion ist eine Funktion, mit der die Livemigration aktiver virtueller Maschinen von einem physischen Server zu einem anderen ermöglicht wird. vMotion-Vorgänge dürfen während aktiver Backupvorgänge nicht auf der VDP-Appliance ausgeführt werden. Hierbei handelt es sich um erwartetes Verhalten. Warten Sie auf den Abschluss aller Backupvorgänge, bevor Sie einen vMotion-Vorgang ausführen.

Wenn während der Durchführung von Backups automatisierte oder gespeicherte vMotion-Vorgänge durchgeführt werden, schlagen manchmal einige der Backups bzw. die Löschung von Snapshots fehl. Führen Sie in diesem Fall die folgenden Schritte aus:

1 Warten Sie bis zum Abschluss der Migration.

2 Führen Sie Backups der fehlgeschlagenen VMs durch die Verwendung von **Backup > Name des Backupjobs > Jetzt sichern** aus.

HINWEIS Verwenden Sie für die Backups nicht **Berichte > Aufgabenfehler > Aufgabe erneut ausführen**.

Backups schlagen bei Verwendung bestimmter Zeichen in den Namen von virtuellen Maschinen, Datenspeichern, Ordnern oder Rechenzentren fehl

Wenn in den Namen von virtuellen Maschinen, Datenspeichern, Ordnern oder Rechenzentren Sonderzeichen enthalten sind, wird die `.vmx`-Datei nicht in das Backup eingeschlossen. Im Folgenden werden die Sonderzeichen (im Format einer Zeichen-/Escape-Sequenz) aufgeführt, die ein Backup der `.vmx`-Datei verhindern:

- & %26
- + %2B
- / %2F
- = %3D
- ? %3F
- % %25
- \ %5C
- ~ %7E
-] %5D

Die Option „Erneut ausführen" des Symbols „Aktionen" führt Backups für alle Clients aus, nicht nur für die fehlgeschlagenen Clientbackups

Wenn ein Clientbackup in einem Backupjob fehlschlägt und Sie die Option **Job erneut ausführen** über das Symbol „Aktionen" auf der Registerkarte **Berichte** verwenden, um das fehlgeschlagene Backup erneut auszuführen, führt das System ein Backup aller Clients im Backupjob aus.

Um ein Backup nur für den fehlgeschlagenen Client auszuführen, wählen Sie **Nur veraltete Quellen sichern** unter **Jetzt sichern** auf der Registerkarte **Backup** aus.

Startfehler beim Job „Jetzt sichern“

Wenn Sie einen **Jetzt sichern**-Job an einen VDP-Appliance-Speicher oder einen Data Domain-Speicher durchführen, der zu mehr als 95 % gefüllt ist, wird eine Fehlermeldung in vSphere Web Client angezeigt, in der angegeben ist, dass das Backup nicht möglich ist.

Troubleshooting der VDP-Backupperformance

Die folgenden Troubleshooting-Themen beschreiben, wie gängige Backupperformance Probleme identifiziert und behoben werden können.

Prüfen Sie die Leistung des Festplatten-Subsystems, auf dem der Backup Datensatz gespeichert ist

Führen Sie das Performance Analyse Tool auf der **Appliance https://VDP IP/hostname:8543/vdp-Konfigurationsseite** aus, um zu prüfen, ob die Datenspeicher, auf dem die VDP-Backups gespeichert sind, die für VDP empfohlenen lesen/schreiben Mindestwerte erfüllen. Die folgende Tabelle zeigt die erforderlichen lesen/schreiben Mindestwerte für VDP:

Tabelle C-32. Lesen/schreiben Mindestwerte für VDP

VDP-Appliance Größe	Festplattengröße	Lese-Mindestwert	Schreib-Mindestwert
0,5 TB	256 GB	60 MB/s	30 MB/s
1,0 TB	512 GB	60 MB/s	30 MB/s
2,0 TB	1024 GB	60 MB/s	30 MB/s
4,0 TB	1024 GB	80 MB/s	40 MB/s
6,0 TB	1024 GB	80 MB/s	40 MB/s
8,0 TB	1024 GB	150 MB/s	120 MB/s

Prüfen Sie, ob die Backups den Hotadd Transportmodus, jedoch nicht den NBD Tansportmodus verwenden

Der HotAdd-Transportmechanismus ermöglicht schnellere Backups und Wiederherstellungen und ist dabei weniger anfällig für Netzwerkrouting-, Firewall- und SSL-Zertifikatsprobleme. Falls der Transportmechanismus des NBD (Network Block Device, Netzwerkblockgerät) statt eines HotAdd eingesetzt wird, nimmt die Backupperformance ab.

Prüfen Sie bei Verwendung des NBD Transportmodus, ob Netzwerkengpässe bestehen

Wenn Sie den HotAdd-Transportmechanismus nicht verwenden können, stellen Sie sicher, dass keine Netzwerkprobleme bestehen und auch keine anderweitigen Probleme mit der ESXi Server Netzwerkkonfiguration, die langsame Backups verursachen.

Troubleshooting der VDP-Wiederherstellungen

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme mit Wiederherstellungen identifiziert und behoben werden können.

Registerkarte „Wiederherstellen“ wird mit der Meldung „Backups werden geladen“ angezeigt und wird nur langsam geladen

Das Laden der Backups auf der Registerkarte **Wiederherstellen** dauert normalerweise zwei Sekunden pro VM-Backup. Hierbei handelt es sich um erwartetes Verhalten.

Registerkarte „Wiederherstellen“ wird nur langsam geladen oder aktualisiert

Bei einer großen Anzahl virtueller Maschinen wird die Registerkarte **Wiederherstellen** möglicherweise nur langsam geladen oder aktualisiert. In Tests mit 100 virtuellen Maschinen hat dies bis zu viereinhalb Minuten gedauert.

Das Einschalten der VM schlägt fehl, wenn die gesicherte virtuelle Maschine mit DVS verbunden war und an einen anderen ESX wiederhergestellt wurde

Wenn Sie eine virtuelle Maschine nach dem Wiederherstellen einschalten, gibt vCenter einen PowerOnFailure-Fehler wie den folgenden zurück:

```
DRS findet keinen Host zum Einschalten oder Migrieren der virtuellen Maschine.
Netzwerkschnittstelle 'Netzwerkadapter 1' verwendet Netzwerk '77 d3 02 50 5f 76
ca d7-db f9 42 6c 0f 6f 87 1f', auf das nicht zugegriffen werden kann.
```

Zu dieser Fehlermeldung kommt es, wenn die Umgebung, in der Sie die virtuelle Maschine wiederherstellen, nicht über die Netzwerkverbindung verfügt, die beim Sichern der virtuellen Maschine vorhanden war. Nehmen wir beispielsweise an, ein Benutzer sichert eine virtuelle Maschine, die mit einem verteilten vSwitch verbunden ist. Dann stellt der Benutzer die virtuelle Maschine auf einem ESX-Host wieder her, der Teil eines DRS-Clusters (Distributed Resource Scheduler) ist. Der vSwitch ist im DRS-Cluster nicht vorhanden. Daher schlägt das Einschalten der virtuellen Maschine fehl.

Sie können dieses Problem umgehen, indem Sie die Einstellungen der virtuellen Maschine bearbeiten und die Netzwerkverbindung auf den Netzwerkadapter festlegen. Schalten Sie dann die virtuelle Maschine ein.

Bei Wiederherstellungen auf Festplattenebene steht keine Option zur Angabe der Zieldatenspeicher zur Verfügung

Wenn auf Festplattenebene an einem neuen Speicherort wiederhergestellt werden soll, steht keine Option zur Verfügung, um die Zieldatenspeicher für die einzelnen Festplatten der virtuellen Maschine anzugeben. Derzeit werden mit VDP alle Festplatten der virtuellen Maschine, einschließlich der während des Backups ausgelassenen Festplatten, auf dem angegebenen Zieldatenspeicher wiederhergestellt.

Geben Sie zum Umgehen dieses Problems einen Zieldatenspeicher an, der über genügend freien Speicherplatz für alle Festplatten der virtuellen Maschine, einschließlich der während des Backups ausgelassenen Festplatten, verfügt.

Gelöschte Festplatten werden beim Wiederherstellen am ursprünglichen Speicherort übersprungen

Wenn die Ziel-VM nicht länger über denselben Festplattenspeicherplatz wie die ursprünglich gesicherte virtuelle Maschine verfügt (sofern die Festplatten von der virtuellen Maschine entfernt oder gelöscht wurden), schlägt die Wiederherstellung der fehlenden Festplatte der virtuellen Maschine bei Durchführung des Vorgangs „Am ursprünglichen Speicherort wiederherstellen“ nach Auswahl eines Wiederherstellungspunkt-Zeitstempels im Fenster „Wiederherstellen“ automatisch fehl.

Als Workaround sind die Festplatten am ursprünglichen Speicherort wiederherzustellen, nachdem der virtuellen Maschine die fehlende Festplatte manuell hinzugefügt wurde. Sorgen Sie dafür, dass die Festplatte die gleiche Größe wie beim Backup der virtuellen Maschine aufweist.

Sollte dieser Workaround fehlgeschlagen, stellen Sie zum Erstellen einer neuen virtuellen Maschine die Festplatte an einem neuen Speicherort wieder her. Trennen Sie bei Abschluss der Wiederherstellungsaufgabe die wiederhergestellten Festplatten von der neuen virtuellen Maschine, und binden Sie sie an die erforderliche virtuelle Maschine an.

Namenskonflikt beim Wiederherstellen einer Festplatte auf eine bestehende virtuelle Maschine

Die Wiederherstellung einer Festplatte auf eine bestehende VM kann aufgrund eines Namenskonflikts fehlschlagen. Es kommt zu diesem Konflikt, wenn eine bestehende VMDK-Festplatte in demselben Datenspeicher vorhanden ist, in dem die neue Festplatte wiederhergestellt wird.

Um dieses Problem zu umgehen, benennen Sie vorhandene Festplatten um, die den Namenkonflikt verursachen, oder entfernen Sie diese.

Zeitstempeldetails für Wiederherstellungspunkte einer Notfallwiederherstellung werden nicht angezeigt

Beim Navigieren durch die Wiederherstellungspunkte auf der Registerkarte **Notfallwiederherstellung** des Dienstprogramms VDP-configure werden u. U. keine Zeitstempeldetails für Wiederherstellungspunkte angezeigt. Dieses Problem tritt auf, wenn UTC als Zeitzone definiert ist.

Führen Sie die folgende Schritte aus, um die UTC-Zeitzone zu ändern:

1 Öffnen Sie das VDP-Konfigurationsdienstprogramm.

2 Wählen Sie auf der Registerkarte **Konfiguration** die Option **Zeitzone ändern** aus.

3 Wählen Sie eine andere Zeitzone als die UTC-Zeitzone aus und klicken Sie auf **Speichern**.

4 Klicken Sie auf **Änderungen anwenden**.

5 Melden Sie sich nach dem Neustart der Webservices beim VDP-Konfigurationsdienstprogramm an und überprüfen Sie den Zeitstempel.

Troubleshooting der VDP-Replikationsjobs

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme mit Wiederherstellungen identifiziert und behoben werden können.

Informationen zur letzten erfolgreichen und letzten fehlgeschlagenen Replikation nicht Teil des E-Mail-Berichts

Die planungsmäßig und ad hoc erstellten E-Mail-Berichte, die nach Abschluss eines Replikationsjobs generiert werden, weisen unter „Zusammenfassung Replikationsjobs“ keine Informationen zur letzten erfolgreichen und letzten fehlgeschlagenen Replikation auf.

Sie sind nicht in der Lage, aus VDP Informationen zu erfolgreichen und fehlgeschlagenen Replikationsjobs zu beziehen.

Fehler bei fehlgeschlagenem Replikationsjob

Wenn sich der Zielserver im Status „Normal“ oder „Vollzugriff“ befindet, wird der Status des Zielservers von der VDP-Appliance korrekt gemeldet. Wenn sich der Zielserver im Status „Admin“, „Schreibgeschützt“ oder „Synchron“ befindet, gibt die VDP-Appliance bei fehlgeschlagenem Replikationsjob einen sonstigen Fehler aus.

Wenn der Zielserver zu mehr als 95 % gefüllt ist und Sie einen **Jetzt replizieren**-Job nicht starten können, wird eine Warnmeldung hinsichtlich des Kapazitätsproblems angezeigt. Auf ähnliche Weise können replizierte Backups nicht an eine VDP-Appliance oder einen Data Domain-Speicher repliziert werden, wenn mehr als 95 % der Kapazität des Speichers gefüllt ist. Eine Warnmeldung hinsichtlich des Kapazitätsproblems wird angezeigt.

Bei falschem Reporting von Ausführungsfehlern kann der Benutzer den Status des Zielservers nicht bestimmen.

Fortschritt des Replikationsjobs anscheinend auf unbestimmte Zeit in einem unvollständigen Status

Der VDP-Aufgabenbereich gibt einen sonstigen Fehler für den Replikationsjob aus und ist nicht in der Lage, zwecks Replikation die Sitzung mit Servern zu initiieren. Eine mögliche Ursache für diesen Fehler: Der Kernmanagementservice wird nicht mehr für den Zielserver ausgeführt.

Prüfen Sie die Managementservices und starten Sie den Kernservice neu, sofern er nicht ausgeführt wird. Versuchen Sie dann, den Replikationsjob erneut auszuführen.

Mehrere in einem Job erstellte Replikationsjobs für verschiedene VMs werden nacheinander und nicht parallel ausgeführt

Replikationsaktivitäten für mehrere virtuelle Maschinen sollten parallel verarbeitet werden. Dieses sequenzielle Verhalten tritt nur auf, wenn bereits ein anderer Replikationsjob mit denselben Clients ausgeführt wird. In diesem Fall wartet die Clientreplikationsaufgabe auf den Abschluss des bereits laufenden Replikationsjobs.

Als Workaround für dieses Problem müssen Sie die Eigenschaft`com.vmware.vdp.option.replicate.maxtreams` der Datei `/usr/local/vdr/etc/vdp-options.properties` hinzufügen. Der Standardwert ist 1. Nachdem Sie die Standardeinstellung beim Hinzufügen oder Bearbeiten der Eigenschaft geändert haben, legt die Appliance den neuen Wert als maximal zulässige Anzahl gleichzeitig ablaufender Prozesse für einen Replikationsjob fest.

Troubleshooting der VDP-Integritätsprüfung

Nach dem Starten einer Integritätsprüfung kann es zu einer Verzögerung von einigen Sekunden kommen, bevor die Aufgabe „VDP: Integritätsprüfung“ auf der Aufgabenregisterkarte **Wird ausgeführt** unter „Letzte Aufgaben“ angezeigt wird. Auch beim Abbrechen einer Integritätsprüfung kann es zu einer Verzögerung von einigen Sekunden kommen, bevor die Aufgabe schließlich abgebrochen wird.

In manchen Fällen (zum Beispiel bei einem Fortschritt der Integritätsprüfung von über 90 %) kann es dazu kommen, dass die Integritätsprüfung vor dem Abbrechen abgeschlossen wird. Auch wenn die Integritätsprüfung erfolgreich abgeschlossen wurde, zeigt die Aufgabenkonsole möglicherweise dennoch einen Fehler an, laut dem die Integritätsprüfung abgebrochen wurde.

Falls Sie wissen, dass der Status der Integritätsprüfung der Appliance (der auf der Registerkarte **Berichte** angezeigt wird) vor dem Start der Integritätsprüfung „Veraltet“ lautete, können Sie sich unmittelbar nach dem Abbrechen des Jobs den Status ansehen und überprüfen, ob das Abbrechen erfolgreich war. Falls der Status der Integritätsprüfung „Normal“ lautet, war die Überprüfung erfolgreich. Falls der Status „Veraltet“ lautet, wurde die Überprüfung abgebrochen.

Troubleshooting der automatischen Backupverifizierung

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme bei der automatischen Backupverifizierung identifiziert und behoben werden können.

Fehlschlag der automatischen Backupverifizierung nach Umbenennung des Datenspeichers

Dieser Fehler kann auftreten, wenn der Zieldatenspeicher umbenannt oder außerhalb von VDP verschoben wird.

Bearbeiten Sie den Job und wählen Sie den umbenannten bzw. verschobenen Zieldatenspeicher als neues Ziel aus. Anweisungen finden Sie unter „Bearbeiten eines Backupverifizierungsjobs“ auf Seite 139.

Mindestens ein ABV-Job mit Fehler „Virtuelle Maschine konnte nicht erstellt werden“ fehlgeschlagen, sodass eine verwaiste VM im vCenter-Bestand zurückgelassen wurde

ABV hat die Überprüfung einer wiederhergestellten VM auf einem Host ausgelöst, der eine frühere Version aufweist und daher nicht mit der zum Erstellen der VM verwendeten Version kompatibel ist. Die Tatsache, dass hierdurch eine verwaiste VM zurückgelassen wird, ist beabsichtigt. Denn dies ist erforderlich, damit Administratoren in einer solchen Situation ein ordnungsgemäßes Troubleshooting bei einem Problem im Zusammenhang mit Wiederherstellungen durchführen können.

Löschen Sie die temporären virtuellen Maschinen manuell, die in vCenter bzw. dem Datenspeicherbestand verbleiben, oder heben Sie deren Registrierung auf.

Bei Abbruch eines ABV-Jobs bleibt eine VDP_VERIFICATION_XXXX-VM auf dem Zielhost zurück

Sie können dieses Problem umgehen, indem Sie im Anschluss an einen ABV-Jobabbruch nach übrig gebliebenen VDP_VERIFICATION_*-VMs auf dem Zielhost suchen und diese manuell entfernen.

Verfügbarer Speicher auf Datenspeicher für angeforderte Aktionen unzureichend

ABV-Jobs oder geplante Jobs schlagen mit Fehlermeldungen in den Protokollen fehl (mitunter mit tatsächlichem Datenverlust), sodass Datenspeicheraktionen aufgrund von unzureichendem Speicher nicht abgeschlossen werden konnten.

Geben Sie Speicher in den Datenspeichern frei und versuchen Sie, den fehlgeschlagenen ABV-Job erneut auszuführen. Führen Sie routinemäßiges Speicherplatzmanagement für Datenspeicher durch, um zu verhindern, dass Speicherplatz knapp wird, insbesondere bevor sich geplante Jobs auf die Nutzung des Datenspeicherplatzes auswirken.

Troubleshooting des Wiederherstellungsclients (Recovery auf Dateiebene)

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme mit dem Wiederherstellungsclient identifiziert und behoben werden können.

Anmeldung fehlgeschlagen, kann virtuelle Maschine nicht unter *10.100.1.10* in vCenter finden

Dieser Fehler kann auftreten, wenn Sie versuchen, sich von einem nicht von VDP gesicherten Host aus mit dem Wiederherstellungsclient zu verbinden.

Melden Sie sich bei einer virtuellen Maschine an, die von VDP gesichert wurde, und verbinden Sie sich dann mit dem Wiederherstellungsclient.

Anmeldung fehlgeschlagen, kann virtuelle Maschine nicht in vCenter finden

Wenn Sie sich nach einer Wiederherstellung auf Dateiebene bei der virtuellen Quellmaschine anmelden, schlägt der Anmeldevorgang mit folgendem Fehler fehl:

```
Anmeldung fehlgeschlagen. Virtuelle Maschine kann nicht in vCenter gefunden
            werden.
```

Dieser Fehler kann auftreten, wenn Sie ein VM-Image auf einer neuen virtuellen Maschine ohne angeschlossene NIC wiederherstellen. In diesem Fall kann sich die FLR-Komponente für einen kurzen Zeitraum nach abgeschlossener Wiederherstellung nicht bei der virtuellen Quellmaschine anmelden. Um dieses Problem zu umgehen, warten Sie im Anschluss an die Wiederherstellung einige Minuten, bevor Sie sich bei der virtuellen Quellmaschine anmelden.

Der Wiederherstellungsvorgang schlägt fehl, und der Fehlercode lautet *10007*.

Sollte der Wiederherstellungsvorgang fehlschlagen und der Fehlercode 1007 „Aktivität fehlgeschlagen – Clientfehler“ lauten, kann dies daran liegen, dass Sie ein schreibgeschütztes Ziel (zum Beispiel ein CD-Laufwerk) oder ein Wechselmediengerät ausgewählt haben, in dem sich kein Medium befindet (zum Beispiel ein Diskettenlaufwerk).

Versuchen Sie die Wiederherstellung erneut an einem neuen Ziel durchzuführen, oder vergewissern Sie sich, dass Ihr Zielgerät beschreibbar ist.

Beim Mounten einer Recovery auf Dateiebene wird nur die letzte Partition angezeigt, wenn die VMDK-Datei mehrere Partitionen enthält

Der Wiederherstellungsclient unterstützt keine erweiterten Volumes. Hierbei handelt es sich um erwartetes Verhalten. Führen Sie eine Recovery auf Image-Ebene durch und kopieren Sie die erforderlichen Dateien manuell.

Beim Mounten einer Recovery auf Dateiebene ist das Mounten nicht unterstützter Partitionen nicht möglich

Die folgenden Festplattenformate werden vom Wiederherstellungsclient nicht unterstützt. Es handelt sich um erwartetes Verhalten, wenn der Mount-Vorgang des Wiederherstellungsclients fehlschlägt.

- Unformatierte Festplatte
- Erweiterte Partitionen (Typen: 05h, 0Fh, 85h, C5h, D5h)
- Dynamische Festplatten (Windows)/Multi-Laufwerkspartitionen (aus 2 oder mehr virtuellen Laufwerken bestehende Partitionen)
- Dedupliziertes NTFS
- Resilient File System (ReFS)
- EFI Boot Loader
- Verschlüsselte Partitionen
- Komprimierte Partitionen

Führen Sie eine Wiederherstellung auf Image-Ebene durch und kopieren Sie die erforderlichen Dateien manuell.

Symbolische Links werden im Wiederherstellungsclient nicht angezeigt

Der Wiederherstellungsclient unterstützt nicht die Anzeige symbolischer Links.

Nach dem Import von VMs Fehlschlag der FLR-Anmeldung bei vor dem Import gesicherten VMs

Nehmen Sie zur Durchführung einer Recovery auf Dateiebene mit den Wiederherstellungspunkten, die von einer zuvor verwendeten VDP-Festplatte importiert wurden, mindestens ein VM-Backup unter Verwendung des neuen VDP vor.

Einschränkungen durch verschachtelte Container

Beim Wiederherstellen eines VMware-Containers, der andere Container enthält (also eine Struktur mit verschachtelten Containern ist), stellt die VDP-Appliance lediglich die höchste Hierarchieebene wieder her. (vApp-1 umfasst beispielsweise mehrere virtuelle Maschinen; in vApp-1 verschachtelt ist ein Container mit der Bezeichnung vApp-2, der ebenfalls mehrere virtuelle Maschinen enthält.) Für diese Einschränkung gibt es zwei Zwischenlösungen:

- Verflachen der Containerstruktur.
- Hinzufügen beider v-Apps (vApp-1 und vApp-2) als separate Containerentitäten, damit sie getrennt voneinander gesichert werden können. Stellen Sie zunächst vApp-1 und dann vApp-2 in vApp-1 wieder her.

Troubleshooting der VDP-Lizenzierung

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme mit der Lizensierung identifiziert und behoben werden können.

Trotz lizenziertem Host werden Lizenzverletzungsereignisse generiert

Bei der Lizenzierung von Hosts in einem Cluster müssen alle Hosts im Cluster lizenziert werden. Anderweitig werden alle Hosts als Hosts betrachtet, die gegen die Lizenzvereinbarung verstoßen. Aufgrund der Beschaffenheit von Clustern gibt es keine Möglichkeit zu bestimmen, zu welchem Host eine VM zu einem bestimmten Zeitpunkt gehört. Daher müssen für das gesamte Cluster gültige Lizenzen vorhanden sein. Der Administrator ist dafür verantwortlich, Lizenzschlüssel ordnungsgemäß zuzuweisen.

Die Evaluierungslizenz läuft ab und das System wird heruntergestuft (nicht einsatzfähig)

Die VDP-Appliance fährt wesentliche Services absichtlich herunter, wann immer die Lizenzanforderungen nicht erfüllt sind. Hierzu kann es kommen, wenn eine Evaluierungslizenz abläuft.

Für alle geschäftskritischen Daten sollte keine Evaluierungs-Appliance verwendet werden. Dies wird nur als Möglichkeit zum Experimentieren mit der VDP Advanced-Appliance betrachtet, die als Wegwerf-Appliance betrachtet werden sollte.

Falls Sie jedoch seitdem einen permanenten vSphere Data Protection-Lizenzschlüssel gekauft haben, gibt es einen Mechanismus zur Wiederherstellung der Appliance. Die folgenden Schritte müssen zwischen den einstündigen Intervallen ausgeführt werden, zu denen das System die Deaktivierung von Hauptservices erzwingt.

1 Starten Sie alle Services mithilfe des VDP-Konfigurationsdienstprogramms neu.

2 Greifen Sie über vSphere Web Client auf die VDP-Appliance zu.

   a Navigieren Sie zum Lizenzzuweisungs-Portlet auf der Registerkarte **Konfiguration**.

   b Fügen Sie dem System den neuen, permanenten Lizenzschlüssel hinzu.

Über diesen Prozess wird für die Appliance ein Upgrade auf einen permanenten Status durchgeführt und die Services sollten funktionsbereit bleiben.

HINWEIS Falls Sie über mehrere Evaluierungs-Appliances verfügen, die auf diese Weise wiederhergestellt werden müssen, müssen Sie den oben erläuterten Prozess auf jeder Appliance wiederholen. Sie können den permanenten Lizenzschlüssel einfach entfernen und erneut hinzufügen, um die Aktualisierung zu erzwingen.

Sie können auch den Lizenzschlüssel einmalig installieren und 24 Stunden warten, bis das Lizenzaudit durchgeführt wird. Beim Lizenzaudit wird das Vorhandensein eines permanenten Lizenzschlüssels erkannt und die Appliance wird über ihren Evaluierungslizenzschlüssel aktualisiert. Sie müssen die Services mithilfe des VDP-Konfigurationsdienstprogramms neu starten.

Troubleshooting der VDP-Appliance

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme mit der VDP-Appliance identifiziert und behoben werden können.

Die VMware VDP für Exchange Serverclients bzw. VMware VDP für SQL Serverclients sind nicht länger bei der VDP-Appliance registriert.

Dieses Problem kann auftreten, wenn die VDP-Appliance umbenannt wurde oder wenn die Clients installiert wurden und kein neuer Kontrollpunkt erstellt und dann ein Rollback durchgeführt wurde. Um dieses Problem zu umgehen, installieren Sie alle VDP SQL Server- und Exchange Server-Clients erneut.

Wenn ein Backupjob mehr als einen SQL Server oder Exchange Server umfasst und die Server identische Datenbankpfade aufweisen, wird bei Auswahl einer Datenbank in einer Serverinstanz, aber nicht in der anderen Instanz mit demselben Pfad, die zweite Instanz mit demselben Pfad ebenfalls gesichert.

Dieses Problem lässt sich beheben, indem entweder pro Backupjob nur ein Exchange Server- oder SQL Server-Rechner eingeschlossen wird oder darauf geachtet wird, dass alle Datenbankpfade eindeutig sind.

Ein oder mehrere Clients können nicht wiederhergestellt werden; der Client ist inaktiv und es gibt keine vergleichbaren Clients, auf denen eine Wiederherstellung vorgenommen werden kann

Dieses Problem kann auftreten, wenn ein Benutzer versucht, den Wiederherstellungsassistenten ohne Auswahl eines Wiederherstellungspunkts aufzurufen, oder wenn ein Wiederherstellungspunkt für einen nicht registrierten Client vorhanden ist. In beiden Fällen ist eine Wiederherstellung nicht möglich, wenn ein inaktiver Client vorliegt und kein vergleichbarer Zielclient in der Umgebung vorhanden ist.

Gastbetriebssystem der VDP-Appliance (Linux) wechselt in schreibgeschützten Status

Das Linux-Gastbetriebssystem wechselt beim Auftreten aller folgenden Symptome in einen schreibgeschützten Status:

1 Es kann kein Kontakt hergestellt werden oder der Status der Services kann nicht geprüft werden, wie in der folgenden Meldung gezeigt:

```
root@ldummyxxx:/usr/local/#: dpnctl status
/bin/chown: changing ownership of '/usr/local/avamar/var/log': Read-only file system
dpnctl: ERROR: running as user "root" - problem opening log file "/usr/local/avamar/var/log/dpnctl.log" (-rw-rw-r--) -
dpnctl: ERROR: traceback on exit:
dpnctl_util: pen_log_file (/usr/local/avamar/bin/dpnctl line YYY)
```

2 Melden Sie sich bei der VDP-configure-Benutzeroberfläche an.

3 Über den vCenter Server-Webclient kann keine Verbindung zum VDP-Plug-in hergestellt werden.

Weitere Informationen über Dateisysteme, die in einen schreibgeschützten Status wechseln können, finden Sie im folgenden VMware-Knowledgebase-Artikel: http://kb.vmware.com/kb/51306

Starten Sie die Appliance neu, bevor Sie sich an den technischen Support wenden. Hierdurch wird das Problem möglicherweise behoben.

Troubleshooting vom VDP Microsoft Exchange Server

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme Exchange Server identifiziert und behoben werden können.

Nicht gemountete oder Offlinedatenbanken werden übersprungen

Eine Datenbank, die während eines Backups nicht gemountet oder offline ist, wird übersprungen. Im Allgemeinen ist dies kein Problem, da nicht gemountete Datenbanken nicht in Produktionsumgebungen verwendet werden.

Backups schlagen beim Mischen von Laufwerksbuchstaben und Volumes fehl

Wenn Sie Exchange Server so konfigurieren, dass über unterschiedliche Pfade, z. B. das Volume `G:\` und `C:\MOUNT-PUNKT`, auf dieselben Datenbankdateien verwiesen wird, schlagen Backups ggf. fehl.

Zur Vermeidung dieses Backupfehlers konfigurieren Sie die Exchange Server-Datenbanken so, dass sie mit demselben Pfad auf die Datenbankdateien verweisen. Wenn sich beispielsweise drei Datenbanken, DB1, DB2 und DB3, unter demselben Pfad auf Laufwerk `G:\` oder `C:\`*`Mount-Punkt`* befinden, verwenden Sie einen – aber nicht beide – der folgenden Beispielpfade:

- `G:\DB1`, `G:\DB2`, `G:\DB3`
- `C:\`*`Mount-Punkt`*`\DB1`, *`C:`*`\Mount-Punkt\`*`DB2`*, `C:\`Mount-Punkt\DB3

Wiederherstellung auf RDB schlägt fehl oder führt zu nicht mehr einsatzfähiger RDB

VDP verwendet die von Microsoft empfohlenen Wartezeiten für die RDB-Stabilisierung in Exchange Server 2013, bevor die Wiederherstellung startet. Die Wiederherstellung schlägt entweder fehl oder führt zu einer nicht mehr einsatzfähigen RDB, falls die Wartezeit bei der Stabilisierung überschritten wird. Sie können die Wartezeit erhöhen, damit mehr Zeit für die Stabilisierung der RDB zur Verfügung steht.

So erhöhen Sie die Wartezeit für die RDB-Stabilisierung:

1 Erstellen Sie mithilfe eines Texteditors die Datei `avexchglr.cmd` im Ordner `C:\Programme\avp\var`, wobei `C:\Progamme\avp` der Installationsordner ist.

2 Geben Sie folgenden Text in die Befehlsdatei ein:

--rdb_stabilize_wait=*n*

wobei *n* die Wartezeit in Sekunden ist. Der Standardwert ist 60 Sekunden.

3 Speichern und schließen Sie die Datei.

Wiederherstellungsanforderungen werden nicht erfüllt

Beim Wiederherstellen einer Exchange Server-Datenbank muss der Exchange Server-Zielrechner hinsichtlich Exchange Server-Version und Service Pack mit dem Exchange Server-Rechner, auf dem das Backup durchgeführt wurde, übereinstimmen.

Wenn die Exchange Server-Version auf den Ziel- und Quellservern nicht übereinstimmt, schlägt die Wiederherstellung fehl.

Protokolldateien werden beim Entdecken von Lücken entfernt

Wenn während einer normalen Wiederherstellung eine Lücke im Transaktionsprotokoll entdeckt wird, werden alle vorhandenen Protokolldateien in einen Ordner namens logs_TIME_DATE verschoben. TIME und DATE stehen dabei für die jeweilige Uhrzeit und das jeweilige Datum der Wiederherstellung. Der Ordner wird als ein Unterordner im Transaktionsprotokoll-Dateipfad der Exchange Server 2007-Speichergruppe bzw. der Exchange Server 2010-Datenbank angelegt. Diese Protokolle können bei Bedarf zum Analysieren des Wiederherstellungsvorgangs oder bis zum Eintreten des Fehlers angewendet werden.

Exchange Server 2007-Datenbanken werden nach der Wiederherstellung gemountet

Vor Wiederherstellungsbeginn werden über VDP alle Datenbanken in einer Speichergruppe ungemountet, selbst wenn die Datenbanken nicht zur Wiederherstellung ausgewählt sind. Nach Abschluss der Wiederherstellung versucht VDP, alle vorhandenen – auch zuvor nicht gemountete – Datenbanken in der Speichergruppe zu mounten. VDP versucht nicht, nicht auf der Festplatte vorhandene Datenbanken zu mounten, selbst wenn diese im Active Directory vorhanden sind.

Die selektive Wiederherstellung von Datenbanken aus einem älteren Backup schlägt u. U. fehl

Wenn Sie versuchen, ausgewählte Datenbanken aus einem älteren Backup wiederherzustellen, obwohl neuere Backups vorhanden sind, schlägt die Wiederherstellung möglicherweise fehl. Löschen Sie in einem solchen Fall die im Protokollordnerpfad erstellte Datei `restore.env` sowie alle Protokolldateien unter diesem Pfad und führen Sie die Wiederherstellung erneut durch. Prüfen Sie außerdem die Ereignisprotokolle über die Ereignisanzeige, wenn eine oder mehrere Datenbanken gemountet werden.

Troubleshooting vom VDP Microsoft SQL Server

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme mit dem SQL Server identifiziert und behoben werden können.

Nicht alle Datenbanken sind in SQL Server 2012 sichtbar

Dieses Problem lässt sich beheben, indem der Gruppe der SQL Server-Administratoren das Dienstkonto des Windows-Systems hinzugefügt wird:

1 Blenden Sie in SQL Server Management Studio den Knoten „Sicherheit“ und dann den Knoten „Anmeldungen“ für die Instanz ein.

2 Klicken Sie mit der rechten Maustaste auf das Konto NT AUTHORITY\SYSTEM und wählen Sie **Eigenschaften** aus.

Das Dialogfeld „Anmeldungseigenschaften“ wird angezeigt.

3 Wählen Sie die Seite **Serverrollen** aus der Liste aus und aktivieren Sie das Kontrollkästchen neben dem Benutzer „sysadmin“.

4 Klicken Sie auf **OK**.

Das Backup einer Datenbank schlägt fehl, wenn diese aktuell wiederhergestellt wird

Microsoft SQL Server bietet keine Unterstützung für Backups, wenn sich die Datenbank in einem Wiederherstellungsstatus befindet.

Eine SQL Server-Wiederherstellung mit aktivierter Option „Protokollfragmentbackup“ schlägt fehl

Dieses Problem kann auftreten, wenn die letzte Wiederherstellung nach dem letzten kompletten Backup durchgeführt wurde. Führen Sie vor der Wiederherstellung ein komplettes Backup für die Datenbank durch.

Die Wiederherstellung kann außerdem fehlschlagen, wenn die Wiederherstellungsoption **Protokollfragmentbackup** aktiviert und die Datenbank nicht vorhanden oder offline ist. Deaktivieren Sie in diesem Fall die Option **Protokollfragmentbackup**.

Troubleshooting vom VDP Microsoft SharePoint Server

Die folgenden Troubleshooting-Themen beschreiben, wie einige gängige Probleme mit dem SharePoint Server identifiziert und behoben werden können.

SharePoint-Jobs für umgeleitete Wiederherstellung mit erfolgreichem Status, selbst wenn einige Datenbanken nicht wiederhergestellt werden können

Wenn eine IP-Adresse statt eines Servernamens verwendet wird, kann bei einer umgeleiteten Wiederherstellung ein Teil der SharePoint-Farm nicht wiederhergestellt werden, auch wenn die Benutzeroberfläche einen erfolgreichen Vorgang angibt.

Verwenden Sie den Servernamen und nicht eine IP-Adresse, wenn ein Alias für eine umgeleitete Wiederherstellung der gesamten oder eines Teil einer SharePoint-Farm erstellt wird.

Troubleshooting von Problemen mit der Speicherkapazität

Bewerten Sie sorgfältig Ihre Backupspeicheranforderungen, wenn Sie die Menge der auf der VDP-Appliance und dem Data Domain-System zu speichernden Daten auswerten. Schließen Sie Schätzungen der Daten ein, die andere Server an die VDP-Appliance und das Data Domain-System gesendet haben, beispielsweise durch Replikationsjobs von anderen VDP-Appliances, durch Freigeben desselben Data Domain-Systems für andere VDP-Appliances und so weiter.

Wenn Sie eine neue VDP-Appliance bereitstellen, füllt sich der Speicher in den ersten Wochen schnell, da jeder Client, den Sie sichern, eindeutige Daten enthält. Die VDP-Deduplizierung lässt sich effektiver nutzen, wenn bereits andere ähnliche Clients gesichert oder dieselben Clients mindestens einmal gesichert wurden.

Nach dem ersten Backup werden von der VDP-Appliance während der folgenden Backups weniger einmalig vorkommende Daten gesichert. Wenn die ersten Backups, die lokalen Backups und die Backups von anderen Servern die Aufbewahrungsfristen überschreiten, können Sie die Fähigkeit des Systems messen, etwa so viele neue Daten zu speichern wie jeden Tag freigesetzt werden. Dieser Prozess wird als Erreichen einer stabilen Kapazitätsauslastung bezeichnet. Die ideale stabile Kapazität liegt bei 80 %.

Monitoring der lokalen VDP-Speicherkapazität

Sie müssen die VDP-Speicherkapazität über die folgenden Methoden proaktiv überwachen:

- Verwenden Sie den vSphere-Webclient:

  „Anzeigen der Backup-Appliance-Konfiguration" auf Seite 59 bietet Informationen dazu.

  Sie können die Kapazität auch anzeigen, indem Sie die unter „Anzeigen von Informationen über die Registerkarte „Berichte"" auf Seite 118 beschriebenen Schritte durchführen.

- Verwenden Sie das VDP-Konfigurationsdienstprogramm.

  „Anzeigen der Speicherkonfiguration" auf Seite 83 bietet Informationen dazu.

- Konfigurieren und überwachen Sie E-Mail-Benachrichtigungen und Berichte.

  „Konfigurieren von E-Mail-Benachrichtigungen und Berichten" auf Seite 61 bietet Informationen dazu.

Monitoring der Data Domain-Speicherkapazität

Sie können die Speicherkapazität des Data Domain-Systems mithilfe der folgenden Methoden überwachen:

- Verwenden Sie den vSphere-Webclient:

  „Monitoring mithilfe des vSphere-Webclients" auf Seite 102 bietet Informationen dazu.

- Verwenden Sie das VDP-Konfigurationsdienstprogramm.

  „Monitoring mithilfe des VDP-Konfigurationsdienstprogramms" auf Seite 103 bietet Informationen dazu.

- Konfigurieren und überwachen Sie E-Mail-Benachrichtigungen und Berichte.

  „Konfigurieren von E-Mail-Benachrichtigungen und Berichten" auf Seite 61 bietet Informationen dazu.

Monitoring von Kapazitätsproblemen

Kapazitätsprobleme beginnen, wenn der Speicher der VDP-Appliance, des Data Domain-Systems oder beider nahezu ausgeschöpft ist. Sie können Kapazitätsprobleme mithilfe der folgenden Methoden überwachen:

- Die Alarme von Kapazitätsproblemen werden auf vCenter ausgelöst. Sie können die Alarme auf dem vSphere-Client oder dem vSphere-Webclient anzeigen.
- Sie können VDP-Alarm-E-Mail-Benachrichtigungen aktivieren, um E-Mails zu erhalten, wenn ein VDP-Alarm ausgelöst wird. „Konfigurieren von E-Mail-Benachrichtigungen und Berichten" auf Seite 61 bietet Informationen dazu. Ein VDP-Alarm enthält auch die Alarme zu den Kapazitätsproblemen.

Auswirkung von Kapazitätsproblemen

Wenn die Speicherkapazität der VDP-Appliance, des Data Domain-Systems oder beider 80 % überschreitet:

- Der gelbe Alarm `Der VDP-/Data Domain-Speicher ist fast voll.` wird ausgelöst.
- Die Warnmeldung wird in der Warnleiste und im Abschnitt **Speicherzusammenfassung** auf dem vSphere-Webclient und im VDP-Konfigurationsdienstprogramm angezeigt.

Wenn die Speicherkapazität der VDP-Appliance, des Data Domain-Systems oder beider 95% überschreitet:

- Der rote Alarm `Der VDP-/Data Domain-Speicher ist fast voll.` wird ausgelöst.

- Die Fehlermeldung wird in der Warnleiste und im Abschnitt **Speicherzusammenfassung** auf dem vSphere-Webclient und im VDP-Konfigurationsdienstprogramm angezeigt.
- Die Jobs „Jetzt sichern“ und „Replizierte Backups wiederherstellen“ können jetzt nicht mehr auf der VDP-Appliance und dem Data Domain-System durchgeführt werden.

Wenn die Speicherkapazität der VDP-Appliance, des Data Domain-Systems oder beider 100 % erreicht:

- Der rote Alarm `Der VDP-/Data Domain-Speicher ist voll.` wird ausgelöst.
- Die Fehlermeldung wird in der Warnleiste und im Abschnitt **Speicherzusammenfassung** auf dem vSphere-Webclient und im VDP-Konfigurationsdienstprogramm angezeigt.
- Die aktuellen Backups auf der VDP-Appliance und dem Data Domain-System schlagen fehl.
- Sie können keine neuen Backups auf der VDP-Appliance und dem Data Domain-System durchführen.
- Die Replikation von Daten an die VDP-Appliance und das Data Domain-System schlägt fehl.
- Vorgänge, die Informationen auf dem Data Domain-System ändern, schlagen fehl. Zu diesen Vorgängen gehören das Löschen von Kontrollpunkten, aktiven Backups und abgelaufenen Backups während der automatischen Speicherbereinigung. Diese Vorgänge können fehlschlagen, weil es dabei zu Verzeichnisumbenennungen kommt, die auf einem vollen Data Domain-System nicht gestattet sind.
- Die VDP-Appliance befindet sich im Status „Admin“.

Allgemeine Schritte für das Freigeben von Speicherplatz

Sie müssen die folgenden Schritte durchführen, um vorab Speicherplatz freizugeben und so das Erreichen der maximalen Kapazität zu vermeiden. Führen Sie die folgenden Schritte durch, wenn die Speicherkapazität 80 % überschreitet:

- Fügen Sie keine virtuellen Maschinen als Backupclients hinzu.
- Entfernen Sie nicht benötigte Wiederherstellungspunkte.
- Löschen Sie unerwünschte Jobs.
- Werten Sie Aufbewahrungs-Policies neu aus, um Aufbewahrungsfristen zu verkürzen.
- Fügen Sie VDP-Appliances hinzu und verteilen Sie die Backupjobs gleichmäßig über mehrere Appliances.
- Wenn Sie der VDP-Appliance kein Data Domain-System hinzugefügt haben, fügen Sie eins hinzu und verteilen Sie die Backupjobs gleichmäßig zwischen der VDP-Appliance und dem Data Domain-System.
- Erweitern Sie die lokale VDP-Speicherfestplatte. „VDP-Festplattenerweiterung“ auf Seite 107 bietet Informationen dazu.
- Wenn das Data Domain-System seine Kapazitätsgrenze erreicht, führen Sie die unter „Wiedergewinnen von Speicher auf einem vollen Data Domain-System“ auf Seite 103 beschriebenen Schritte durch, um Speicherplatz zurückzugewinnen.

Zugreifen auf VDP-Knowledgebase-Artikel

Zusätzliche Troubleshooting-Informationen sind über die VDP-Knowledgebase-Artikel unter folgender Adresse verfügbar.

http://www.vmware.com/selfservice/microsites/microsite.do

Wählen Sie **Products** > **VMware vSphere Data Protection** Category > **Troubleshooting** aus.

Index

W

Z