Administratorhandbuch für vSphere Data Protection

vSphere Data Protection 5.1

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.

DE-000846-00

vmware®

Die neueste 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

VMware, Inc.
Freisinger Str. 3
D-85716 Unterschleißheim / Lohhof
www.vmware.com/de

Inhaltsverzeichnis

1 Wissenswertes über vSphere Data Protection 7
- Einführung in vSphere Data Protection 8
- Backups auf Image-Ebene und Wiederherstellungen 8
- Recovery auf Dateiebene 9
- Vorteile des Deduplizierungsspeichers 9
  - Datensegmente mit variabler und fester Länge 9
  - Ermittlung logischer Segmente 10
- Architektur von vSphere Data Protection 10

2 Installieren und Konfigurieren von vSphere Data Protection 11
- Dimensionierung von vSphere Data Protection 12
- Softwareanforderungen 12
- Systemanforderungen 13
- Spezifikationen von vSphere Data Protection 13
- Konfiguration vor der Installation 14
  - DNS-Konfiguration 14
  - Konfiguration von NTP 14
  - Konfiguration des Benutzerkontos 14
  - Bereitstellen der OVF-Vorlage 15
  - Voraussetzungen 15
  - Verfahren 15
- Installation und Konfiguration von vSphere Data Protection 16
  - Voraussetzungen 16
  - Verfahren 16
- Konfiguration nach der Installation 17
  - Registerkarte „Status“ 18
  - Registerkarte „Konfiguration“ 19
  - Registerkarte „Rollback“ 20
  - Registerkarte „Upgrade“ 20
  - Verwenden von VDP Configure 20
- Aktualisieren der vSphere Data Protection Appliance 21
  - Erstellen eines Snapshot der vSphere Data Protection Appliance 21
  - Installieren des Upgrades 22
  - Entfernen von Snapshots 23

3 Verwenden von vSphere Data Protection 25
- Wissenswertes über die vSphere Data Protection-Benutzeroberfläche 26
  - Registerkarte „Erste Schritte“ 26
  - Registerkarte „Backup“ 27
  - Registerkarte „Wiederherstellen“ 28
  - Registerkarte „Berichte“ 28
  - Registerkarte „Konfiguration“ 28
- Zugreifen auf vSphere Data Protection 29
- Wechseln zwischen vSphere Data Protection Appliances 29

Erstellen von Backup-Jobs 29
Virtuelle Maschinen 29
Planung 30
Aufbewahrungs-Policy 30
Bereit zur Fertigstellung 30
Verwenden des Backup-Job-Assistenten 30
Jetzt sichern 31
Wiederherstellen virtueller Maschinen 31
Backup auswählen 31
Wiederherstellungsoptionen festlegen 32
Wiederherstellen virtueller Maschinen aus Backups 32
Anzeigen des Fortschritts von Wiederherstellungsjobs 33
Sperren von Backup-Jobs 33
Anzeigen von Berichten 33
Filtern auf der Registerkarte „Berichte“ 33
Managen der Konfiguration 34
Anzeigen und Bearbeiten von Backup-Appliance-Details 34
Konfiguration des Backup-Zeitfensters 34
Ändern der Einstellungen für das Wartungsfenster 36
Manuelles Ausführen einer Integritätsprüfung 37
Konfigurieren der E-Mail-Benachrichtigung 37
Verwenden von Kontrollpunkten und Rollback 38
Verwenden der Recovery auf Dateiebene 39
Unterstützte Konfigurationen bei der Recovery auf Dateiebene: 39
Einschränkungen der Recovery auf Dateiebene 39
Anmeldeoptionen 40
Verwenden des Wiederherstellungsclients im Modus „Standardanmeldung“ 41
Verwenden des Wiederherstellungsclients im Modus „Erweiterte Anmeldung“ 41
Verfahren zum Herunterfahren und Starten von vSphere Data Protection 42

4 Kapazitätsmanagement mit vSphere Data Protection 43
Auswirkung durch die Auswahl von Thin- oder Thick-Provisioning-Festplatten 44
Voraussetzungen 44
Verfahren 44
Auswirkung der Speicherkapazität auf die erste vSphere Data Protection-Bereitstellung 45
Überwachen der vSphere Data Protection-Kapazität 45
Kapazitätsschwellwerte von vSphere Data Protection 45
Kapazitätsmanagement 45

5 vSphere Data Protection-Troubleshooting 47
Installation der vSphere Data Protection Appliance 48
vSphere Data Protection-Backups 48
vSphere Data Protection-Wiederherstellungen 49
Recovery auf Dateiebene 50
vSphere Data Protection-Reporting 50

6 Von vSphere Data Protection verwendete Ports 51

7 Disaster Recovery von vSphere Data Protection 53

Index 55

Informationen über dieses Handbuch

Das Administratorhandbuch für vSphere Data Protection enthält Informationen zur Installation und zum Management von Backups für kleine und mittelständische Unternehmen.

Zielgruppe

Dieses Handbuch richtet sich an Benutzer, die Backup-Lösungen mithilfe von vSphere Data Protection 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.

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 zur technischen Unterstützung verfügbaren Ressourcen beschrieben. Die aktuellen Versionen weiterer VMware-Handbücher finden Sie unter http://www.vmware.com/de/support/pubs.

Online-Support

Online-Support 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.

Support-Angebote

VMware stellt ein umfangreiches Support-Angebot 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

vSphere Data Protection (VDP) ist eine robuste, einfach bereitzustellende festplattenbasierte Backup- und Recovery-Lösung. vSphere Data Protection ist voll in VMware vCenter Server integriert und ermöglicht beim Speichern von Backups in dedupliziertem Zielspeicher das zentrale und effiziente Management von Backup-Jobs.

Die Vorteile von vSphere Data Protection:

- schnelle und effiziente Data Protection für alle virtuellen Maschinen, selbst für ausgeschaltete oder zwischen physischen Hosts verlagerte VMs
- deutliche Reduzierung des belegten Festplattenspeichers durch Backup-Daten mit intelligenter Deduplizierungsfunktion bei allen Backups
- Senkung der Kosten für das Backup virtueller Maschinen und Minimierung des Backup-Zeitfensters 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 die vSphere Web Client-Standardversion integrierte vSphere Data Protection-Konfiguration
- Schutz von Backups mit Kontrollpunkt- und Rollback-Mechanismus
- vereinfachte Recovery von Windows- und Linux-Dateien mit vom Anwender initiierten Recoveries auf Dateiebene von einer webbasierten Schnittstelle aus

In diesem Kapitel werden folgende Themen behandelt:

- „Einführung in vSphere Data Protection“ auf Seite 8
- „Backups auf Image-Ebene und Wiederherstellungen“ auf Seite 8
- „Recovery auf Dateiebene“ auf Seite 9
- „Vorteile des Deduplizierungsspeichers“ auf Seite 9
- „Architektur von vSphere Data Protection“ auf Seite 10

Einführung in vSphere Data Protection

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

Während eines Backup erstellt vSphere Data Protection einen stillgelegten Snapshot der virtuellen Maschine. Die Deduplizierung wird automatisch bei jedem Backup-Vorgang 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 Backup-Prozesses für VMware vStorage API-fähige Anwendungen führt.
- **VMware vStorage APIs for Data Protection (VADP)** ermöglicht, dass Backup-Software zentrale VM-Backups durchführen kann, und zwar ohne Unterbrechung und Overhead durch laufende Backup-Aufgaben innerhalb jeder virtuellen Maschine.
- **Virtual Machine Disk (VMDK)** ist eine Datei oder ein Satz von Dateien, die bzw. der einem Gastbetriebssystem als physisches Festplattenlaufwerk angezeigt wird. Diese Dateien können auf dem Hostrechner oder einem Remote-Dateisystem liegen.
- **Die vSphere Data Protection Appliance** ist eine speziell entwickelte virtuelle Appliance für vSphere Data Protection.

Backups auf Image-Ebene und Wiederherstellungen

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 Backup-Verarbeitungs-Overhead von der virtuellen Maschine auf die vSphere Data Protection Appliance. Die Appliance kommuniziert mit vCenter Server, um einen VMDK-Snapshot der 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 vSphere Data Protection Appliance auf acht virtuelle Maschinen gleichzeitig sichern, um die Data-Protection-Workload-Kapazität zu erweitern.

Für mehr Effizienz von Backups auf Image-Ebene nutzt vSphere Data Protection die VADP-Funktion Changed Block Tracking (CBT). CBT ist eine VMware-Funktion, die es vSphere Data Protection ermöglicht, nur die seit dem letzten Backup geänderten Festplattenblöcke zu sichern. Hierdurch lässt sich zum einen die Backup-Zeit einer bestimmten virtuellen Maschine deutlich reduzieren, zum anderen wird eine Möglichkeit geschaffen, eine große Anzahl von virtuellen Maschinen innerhalb eines vorgegebenen Backup-Zeitfensters zu verarbeiten.

Durch Nutzung der CBT-Funktion sorgt vSphere Data Protection bei der Wiederherstellung virtueller Maschinen an ihrem ursprünglichen Speicherort für schnelle und effiziente Recoveries. Während eines Wiederherstellungsprozesses stellt vSphere Data Protection eine Abfrage an VADP, um die seit dem letzten Backup geänderten Blöcke zu bestimmen. Daraufhin werden während einer Recovery nur diese Blöcke wiederhergestellt bzw. ersetzt. So wird nicht nur die Datenübertragung innerhalb der vSphere-Umgebung während einer Recovery reduziert, sondern vor allem auch die Recovery Time Objective (RTO).

Zusätzlich bewertet vSphere Data Protection automatisch den Workload zwischen beiden Wiederherstellungsmethoden (vollständige Image-Wiederherstellung bzw. eine Recovery mit CBT) und setzt die entsprechende Methode um. Das Ergebnis: schnellste Wiederherstellungszeiten. 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. vSphere Data Protection entscheidet auf intelligente Weise, welche Bereitstellungsmethode bei bestimmten Szenarios oder Umgebungen zu schnelleren VM-Image-Recovery-Zeiten führt.

Die Vorteile von VMware Image Backups:

- vollständige, vom Gastbetriebssystem unabhängige Image Backups virtueller Maschinen
- Nutzung der effizienten Übertragungsmethode SCSI Hot-Add, sofern verfügbar und ordnungsgemäß lizenziert; hierdurch kein Kopieren des gesamten VMDK-Image über das Netzwerk
- Möglichkeit zur Recovery auf Dateiebene von Backups auf Image-Ebene
- Deduplizierung innerhalb der und über alle von der vSphere Data Protection Appliance geschützten .vmdk-Dateien hinweg
- schnellere Backups und Wiederherstellungen durch Changed Block Tracking (CBT)
- Minimierung des Netzwerkverkehrs durch Deduplizierung und Komprimierung von Daten
- Beseitigung der Notwendigkeit zum Management von Backup Agents auf jeder virtuellen Maschine
- höherer Durchsatz durch Unterstützung für gleichzeitige Backup- und Recovery-Vorgänge

WICHTIGER HINWEIS Best Practice für VM-Image-Backups ist die Installation von VMware Tools auf jeder virtuellen Maschine. Mit VMware Tools wird eine zusätzliche Backup-Funktion zur Verfügung gestellt, mit der vor dem Backup bestimmte Prozesse auf dem Gastbetriebssystem stillgelegt werden können.

Recovery auf Dateiebene

Die Recovery auf Dateiebene 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 Wiederherstellungsclients für vSphere Data Protection durchgesetzt.

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 Backup-Methoden 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 Ineffizienzen beseitigt.

Ermittlung logischer Segmente

vSphere Data Protection verwendet eine patentierte Methode zur Ermittlung der Segmentgröße, die darauf ausgelegt ist, systemübergreifend für optimale Effizienz zu sorgen. Mit dem vSphere Data Protection-Algorithmus wird die Binärstruktur des Dataset analysiert (alle Nullen und Einsen eines Dataset), um die kontextabhängigen Segmentgrenzen zu bestimmen. Segmente variabler Länge sind im Durchschnitt 24 KB groß und werden durchschnittlich auf 12 KB komprimiert.

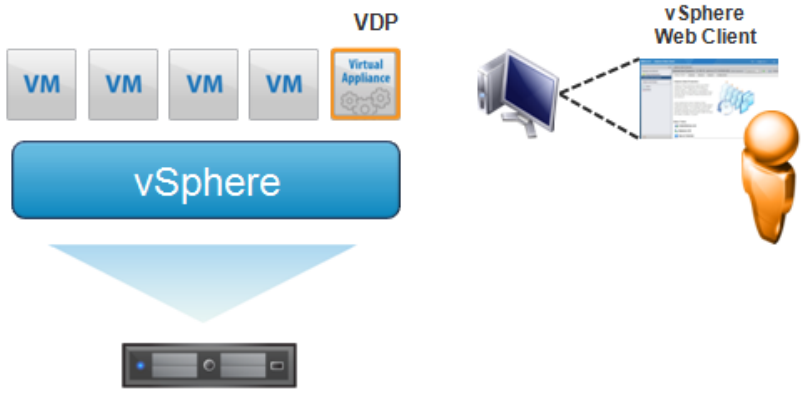
Durch Analyse der Binärstruktur innerhalb der VMDK-Dateien kann vSphere Data Protection für alle Dateitypen und -größen verwendet werden und sorgt für eine intelligente Deduplizierung der Daten.

Architektur von vSphere Data Protection

vSphere Data Protection (VDP) verwendet vSphere Web Client und eine vSphere Data Protection Appliance, um Backups in dedupliziertem Speicher zu sichern.

vSphere Data Protection besteht aus einer Reihe von Komponenten, die auf verschiedenen Maschinen ausgeführt werden (siehe nachfolgende Abbildung).

- vSphere 5.1
- vSphere Data Protection Appliance (installiert auf ESX/ESXi 4.x oder 5.x)
- vSphere Web Client



Installieren und Konfigurieren von vSphere Data Protection

2

In diesem Kapitel werden folgende Themen behandelt:

- „Dimensionierung von vSphere Data Protection“ auf Seite 12
- „Softwareanforderungen“ auf Seite 12
- „Systemanforderungen“ auf Seite 13
- „Konfiguration vor der Installation“ auf Seite 14
- „Bereitstellen der OVF-Vorlage“ auf Seite 15
- „Installation und Konfiguration von vSphere Data Protection“ auf Seite 16
- „Konfiguration nach der Installation“ auf Seite 17

Dimensionierung von vSphere Data Protection

Über die vSphere Data Protection-Dimensionierung lässt sich anhand der folgenden Faktoren die vSphere Data Protection 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 2-1. Beispielhafte Empfehlungen für die vSphere Data Protection-Dimensionierung

Anzahl VMs	Daten-speicher pro Client	Auf-bewahrungs-frist: täglich	Auf-bewahrungs-frist: wöchentlich	Auf-bewahrungs-frist: monatlich	Auf-bewahrungs-frist: jährlich	Empfehlung
25	20 GB	30	0	0	0	1 VDP mit 0,5 TB
25	20 GB	30	4	12	7	1 VDP mit 2 TB
25	40 GB	30	4	12	7	2 VDPs mit 2 TB
50	20 GB	30	0	0	0	1 VDP mit 1 TB
50	20 GB	30	4	12	7	2 VDPs mit 2 TB
50	40 GB	30	4	12	7	3 VDPs mit 2 TB
100	20 GB	30	0	0	0	1 VDP mit 2 TB
100	20 GB	30	4	12	7	3 VDPs mit 2 TB
100	40 GB	30	4	12	7	6 VDPs mit 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 Appliance bereitgestellt wurde, ist die Größe des Datenspeichers nicht mehr veränderbar.

Softwareanforderungen

Für vSphere Data Protection 5.1 ist folgende Software erforderlich:

- VMware vCenter Server
  - vCenter Server Linux oder Windows: Version 5.1
  - vSphere Web Client wird von Microsoft Internet Explorer 7 und 8 (es gibt derzeit bekannte Probleme in Bezug auf die vSphere Web Client-Ausführung in IE 8) oder Mozilla Firefox ab Version 3.6 unterstützt.
  - Webbrowser müssen über Adobe Flash Player ab Version 11.3 verfügen, um auf die Funktionen von vSphere Web Client oder vSphere Data Protection zuzugreifen.

- VMware ESX/ESXi (die folgenden Versionen werden unterstützt):
  - 4.0, 4.0i, 4.1i, 5.0i, 5.1
- Appliance-Version:
  - vSphere Data Protection: 5.1

Systemanforderungen

Die vSphere Data Protection Appliance ist in Form von drei Optionen erhältlich:

- VDP mit 0,5 TB
- VDP mit 1 TB
- VDP mit 2 TB

WICHTIGER HINWEIS Sobald eine vSphere Data Protection Appliance bereitgestellt wurde, ist die Größe nicht mehr veränderbar.

Die Systemanforderungen für die jeweiligen vSphere Data Protection-Option sind in der folgenden Tabelle angegeben.

	VDP mit 0,5 TB	VDP mit 1 TB	VDP mit 2 TB
Dedizierte Prozessoren für vSphere Data Protection	vSphere Data Protection stehen immer mindestens vier 2-GHz-Prozessoren zur Verfügung.	vSphere Data Protection stehen immer mindestens vier 2-GHz-Prozessoren zur Verfügung.	vSphere Data Protection stehen immer mindestens vier 2-GHz-Prozessoren zur Verfügung.
Dedizierter physischer Speicher für vSphere Data Protection	4 GB	4 GB	4 GB
Festplattenspeicher	850 GB	1.600 GB	3.100 GB
Netzwerkverbindung	1-GbE-Verbindung	1-GbE-Verbindung	1-GbE-Verbindung

Spezifikationen von vSphere Data Protection

vSphere Data Protection unterstützt die folgenden Spezifikationen:

- Jede vSphere Data Protection Appliance unterstützt das Backup von bis zu 100 virtuellen Maschinen.
- Jede vCenter Server-Installation kann bis zu 10 vSphere Data Protection Appliances unterstützen.
- Es besteht Unterstützung für 0,5 TB, 1 TB oder 2 TB Deduplizierungsspeicher.

Konfiguration vor der Installation

Vor der vSphere Data Protection-Installation müssen DNS und NTP konfiguriert werden.

DNS-Konfiguration

Bevor vSphere Data Protection bereitgestellt wird, muss dem DNS-Server für die Appliance-IP-Adresse und den vollständig qualifizierten Domain-Namen ein Eintrag hinzugefügt werden. Dieser DNS-Server muss Forward und Reverse Lookup unterstützen.

WICHTIGER HINWEIS Ein nicht ordnungsgemäß eingerichteter DNS kann zahlreiche Laufzeit- oder Konfigurationsprobleme nach sich ziehen.

So können Sie eine ordnungsgemäße DNS-Konfiguration bestätigen:

1 Öffnen Sie eine Eingabeaufforderung, und geben Sie den folgenden Befehl ein:

nslookup <*VDP_IP_Adresse*> <*DNS_IP_Adresse*>

Der nslookup-Befehl gibt den vollständig qualifizierten Domain-Namen der vSphere Data Protection Appliance zurück.

2 Geben Sie den folgenden Befehl ein:

nslookup <*vollständig_qualifizierter_Domain_Name_von_VDP*> <*DNS_IP_Adresse*>

Der nslookup-Befehl gibt die IP-Adresse der vSphere Data Protection Appliance zurück.

3 Wenn der nslookup-Befehl die richtigen Informationen zurückgegeben hat, schließen Sie die Eingabeaufforderung. Falls nicht, korrigieren Sie die DNS-Konfiguration vor der vSphere Data Protection-Installation.

Konfiguration von NTP

vSphere Data Protection nutzt NTP (Network Time Protocol). Vor der vSphere Data Protection-Installation muss NTP auf dem vCenter Server-Rechner und dem ESXi-Host, auf dem vSphere Data Protection installiert werden soll, konfiguriert werden.

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

Konfiguration des Benutzerkontos

Bevor das vCenter-Benutzerkonto oder der SSO-Admin-Benutzer mit vSphere Data Protection verwendet werden kann, sollten diese Benutzer explizit als Administrator auf dem vCenter-Stammknoten hinzugefügt werden. Anhand der folgenden Schritte wird der vSphere Data Protection- oder SSO-Admin-Benutzer mit vSphere Client konfiguriert.

1 Melden Sie sich bei vSphere Web Client an, und wählen Sie **vCenter** > **Hosts und Cluster** aus.

2 Klicken Sie im linken Bereich auf „vCenter Server“.

3 Klicken Sie auf die Registerkarte **Managen** und anschließend auf die Unterregisterkarte **Berechtigungen**.

4 Klicken Sie auf das Symbol **Berechtigung hinzufügen**.

5 Klicken Sie auf **Hinzufügen**.

6 Wählen Sie in der Domain-Dropdown-Liste „Domain“, „Server“ oder „SYSTEM-DOMAIN“ aus.

7 Wählen Sie den Benutzer aus, der vSphere Data Protection verwalten oder als SSO-Admin fungieren wird, und klicken Sie auf **Hinzufügen**.

8 Klicken Sie auf **OK**.

9 Wählen Sie über die Dropdown-Liste „Zugewiesene Rolle“ die Option „Administrator“ aus.

10 Vergewissern Sie sich, dass das Kontrollkästchen „Auf untergeordnete Objekte übertragen“ aktiviert ist.

11 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 vSphere Data Protection-Backup-Benutzer, der die Benutzeroberfläche von VDP-configure nutzt, zu einem Domain-Konto gehört, sollte der Benutzername in VDP-configure im Format „SYSTEM-DOMAIN\admin“ verwendet werden. Wenn der Benutzername im Format „admin@SYSTEM-DOMAIN“ eingegeben wird, werden Aufgaben im Zusammenhang mit einem Backup-Job möglicherweise nicht in den Aufgaben mit dem Status „Zuletzt ausgeführt“ angezeigt.

Bereitstellen der OVF-Vorlage

Voraussetzungen

- Die vSphere Data Protection Appliance wird auf einem Host mit ESXi 4.0, 4.1, 5.0 oder 5.1 installiert.
- vCenter 5.1 ist erforderlich. Melden Sie sich bei vCenter über vSphere Web Client an, um die OVF-Vorlage bereitzustellen.
- Die vSphere Data Protection Appliance stellt über den Port 902 eine Verbindung zu ESXi her. Ist eine Firewall zwischen Appliance und ESXi vorhanden, muss der Port 902 offen sein.
- Das VMware Client Integration Plug-In 5.1.0 muss in Ihrem Browser installiert sein.

Verfahren

1 Melden Sie sich bei vSphere Web Client an, und wählen Sie **vCenter > Rechenzentren** aus.

2 Klicken Sie auf der Registerkarte „Objekte“ auf **Aktionen > OVF-Vorlage bereitstellen.**

3 Wählen Sie die Quelle aus, auf der sich die vSphere Data Protection Appliance befindet.

4 Standardmäßig ist das Dialogfeld zur Auswahl der Quelle auf OVF-Pakete eingestellt. Ändern Sie die Einstellung auf **OVA-Pakete**.

5 Wählen Sie die Appliance aus, und klicken Sie auf **Öffnen**.

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

7 Überprüfen Sie die Vorlagendetails, und klicken Sie auf **Weiter**.

8 Lesen Sie auf dem Bildschirm „EULAs akzeptieren“ die Lizenzvereinbarung, klicken Sie auf **Akzeptieren** und dann auf **Weiter**.

9 Geben Sie auf dem Bildschirm zum Auswählen von Namen und Ordner den Namen für die Appliance ein, und klicken Sie auf einen Ordner oder ein Rechenzentrum für die Appliance-Bereitstellung. Klicken Sie anschließend auf **Weiter**.

10 Wählen Sie den Host für die Appliance aus, und klicken Sie auf **Weiter**.

11 Wählen Sie das Format des virtuellen Laufwerks (zusätzliche Informationen unter „Auswirkung durch die Auswahl von Thin- oder Thick-Provisioning-Festplatten“ auf Seite 44) und das Verzeichnis für den Speicher der Appliance aus. Klicken Sie auf **Weiter**.

12 Wählen Sie das Zielnetzwerk für die Appliance aus, und klicken Sie auf **Weiter**.

13 Geben Sie in der Vorlage „Anpassen“ Werte für **Standard-Gateway**, **DNS**, **Netzwerk 1 IP-Adresse** und **Netzwerk 1 Netzmaske** an. Vergewissern Sie sich, dass die IP-Adressen korrekt sind. Wenn in diesem Dialogfeld falsche IP-Adressen angegeben werden, ist es erforderlich, die .ova-Datei neu bereitzustellen. Klicken Sie auf **Weiter**.

HINWEIS Die vSphere Data Protection Appliance unterstützt nicht DHCP. Die Appliance erfordert eine statische IP-Adresse.

14 Vergewissern Sie sich im Bildschirm „Bereit zur Fertigstellung“, dass sämtliche Bereitstellungsoptionen korrekt sind, und klicken Sie auf **Fertig stellen**.

vCenter stellt die vSphere Data Protection Appliance bereit. Überwachen Sie **Letzte Aufgaben**, um den Abschluss der Bereitstellung bestimmen zu können.

Installation und Konfiguration von vSphere Data Protection

Voraussetzungen

Die .ovf-Vorlage von vSphere Data Protection (siehe „Bereitstellen der OVF-Vorlage“ auf Seite 15) muss erfolgreich bereitgestellt worden sein, und Sie müssen bei vCenter Server über vSphere Web Client angemeldet sein.

Verfahren

1 Wählen Sie **vCenter-Startseite > vCenter > VMs und Vorlagen**. Blenden Sie die vCenter-Struktur ein, und wählen Sie die vSphere Data Protection Appliance aus. Klicken Sie mit der rechten Maustaste auf die Appliance, und wählen Sie **Einschalten** aus.

2 Klicken Sie mit der rechten Maustaste auf die Appliance, und wählen Sie **Konsole öffnen** aus.

3 Nach dem Laden der Installationsdateien wird der Begrüßungsbildschirm für das vSphere Data Protection-Menü angezeigt. Öffnen Sie einen Webbrowser, und geben Sie Folgendes ein:

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

4 Geben Sie über den VMware-Anmeldebildschirm Folgendes ein:

a Benutzer: **root**

b Passwort: **changeme**

c Klicken Sie auf **Anmelden**.

5 Der Begrüßungsbildschirm wird angezeigt. Klicken Sie auf **Weiter**.

6 Das Dialogfeld „Netzwerkeinstellungen“ wird angezeigt. Geben Sie Werte in den folgenden Feldern ein, bzw. bestätigen Sie diese:

a Statische IPv4-Adresse

b Netzmaske

c Gateway

d Primärer DNS

e Sekundärer DNS

f Hostname

g Domain

7 Klicken Sie auf **Weiter**.

8 Das Dialogfeld „Zeitzone“ wird angezeigt. Wählen Sie die entsprechende Zeitzone aus, und klicken Sie auf **Weiter**.

9 Das Dialogfeld „vSphere Data Protection-Anmeldedaten“ wird angezeigt. Geben Sie für die vSphere Data Protection-Anmeldedaten das Appliance-Passwort ein. Dieses wird als universelles Konfigurationspasswort verwendet. Geben Sie ein Passwort ein, das folgende Kriterien erfüllt:

- neun Zeichen
- mindestens ein Großbuchstabe
- mindestens ein Kleinbuchstabe
- mindestens eine Ziffer
- keine Sonderzeichen

10 Klicken Sie auf **Weiter**.

11 Das Dialogfeld „vCenter-Registrierung“ wird angezeigt. Geben Sie Folgendes an:

a vCenter-Benutzername (Wenn der Benutzer zu einem Domain-Konto gehört, sollte der Name im Format „SYSTEM-DOMAIN\admin“ eingegeben werden.)

b vCenter-Passwort

c vCenter-Hostname (IP-Adresse oder vollständig qualifizierter Domain-Name)

d vCenter-Port

e SSO-Hostname (IP-Adresse oder vollständig qualifizierter Domain-Name)

f SSO-Port

12 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.

Wird die Meldung „Angegebener Benutzer ist entweder kein dedizierter VDP-Benutzer oder verfügt nicht über ausreichende vCenter-Privilegien zum Verwalten von VDP. Bitte aktualisieren Sie Ihre Benutzerrolle und versuchen Sie es erneut“ angezeigt, finden Sie unter „Konfiguration des Benutzerkontos“ auf Seite 14 Anweisungen zum Aktualisieren der Benutzerrolle.

13 Klicken Sie auf **OK**.

14 Klicken Sie auf **Weiter**.

15 Die Seite „Bereit zur Fertigstellung“ wird angezeigt. Klicken Sie auf **Fertig stellen**.

16 Durch eine Meldung wird über den Abschluss der Konfiguration informiert. Klicken Sie auf **OK**.

Die Konfiguration der vSphere Data Protection Appliance ist nun abgeschlossen, Sie müssen jedoch zu vSphere Web Client zurückkehren und die Appliance neu starten. Klicken Sie in vSphere Web Client mit der rechten Maustaste auf die Appliance, und wählen Sie **Gastbetriebssystem neu starten** aus. Klicken Sie im Meldungsfenster „Neustart bestätigen“ auf **Ja**. Der Neustart kann bis zu 30 Minuten dauern.

Konfiguration nach der Installation

Während der Installation von vSphere Data Protection wird das Konfigurationsdienstprogramm beim erstmaligen Ausführen im „Installationsmodus“ ausgeführt. Mit diesem Modus können Sie die anfänglichen Netzwerkeinstellungen, die Zeitzone, das Appliance-Passwort und die vCenter-Anmeldedaten eingeben. Nach der Erstinstallation wird das Dienstprogramm VDP-configure im „Wartungsmodus“ ausgeführt und zeigt eine andere Benutzeroberfläche an.

Zum Zugreifen auf VDP-Configure öffnen Sie einen Webbrowser und geben Folgendes ein:

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

Die Wartungsschnittstelle wird für Folgendes verwendet:

- Anzeigen des Status – Hiermit können Sie die Services anzeigen, die derzeit auf der Appliance ausgeführt (oder beendet) werden.
- Starten und Stoppen von Services – Hiermit können Sie ausgewählte Services auf der Appliance starten oder beenden.
- Sammeln von Protokollen – Hiermit können Sie aktuelle Protokolle von der Appliance herunterladen.
- Anzeigen oder Ändern der vSphere Data Protection-Konfiguration – Hiermit können Sie Netzwerkeinstellungen anzeigen oder ändern, die vCenter-Registrierung konfigurieren oder Systemeinstellungen (Zeitzonenangaben und vSphere Data Protection-Anmeldedaten) anzeigen bzw. bearbeiten.
- Rollback einer Appliance – Hiermit können Sie Ihre Appliance in einem früheren bekannten und gültigen Status wiederherstellen. (Weitere Informationen finden Sie unter „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38.)
- Upgrade – Hiermit können Sie ein Upgrade der ISO-Images auf Ihrer vSphere Data Protection Appliance durchführen.

Registerkarte „Status“

Die Registerkarte „Status“ wird verwendet, um vSphere Data Protection-Services anzuzeigen (und zu stoppen oder zu starten).

Managen von Statusoptionen

Im linken Bildschirmbereich der Registerkarte „Status“ wird der Status der Hauptservices der vSphere Data Protection Appliance angezeigt. Der Status der folgenden Services wird angezeigt:

Tabelle 2-2. Beschreibung der auf der vSphere Data Protection Appliance ausgeführten Services

Service	Beschreibung
Kernservices	Hierbei handelt es sich um die Services, die die Backup Engine der Appliance beinhalten. Wenn diese Services deaktiviert sind, werden keine Backup-Jobs ausgeführt, weder geplant noch „nach Bedarf“. Außerdem können keine Wiederherstellungsaktivitäten initiiert werden.
Managementservices	Managementservices sollten nur auf Anweisungen des technischen Support gestoppt werden.
Dateisystemservices	Hierbei handelt es sich um die Services, durch die sich Backups für Recovery-Vorgänge auf Dateiebene mounten lassen.
Services für die Wiederherstellung auf Dateiebene	Hierbei handelt es sich um die Services, die das Management von Recovery-Vorgängen auf Dateiebene 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 während der ersten 24-48 Stunden des vSphere Data Protection Appliance-Betriebs deaktiviert. So steht zusätzliche Zeit zum Abschließen der ersten Backups zur Verfügung.
Backup-Planer	Beim Backup-Planer handelt es sich um den Service, der geplante Backup-Jobs initiiert. Wird der Planer gestoppt, werden keine geplanten Backups ausgeführt; Backups „nach Bedarf“ können jedoch nach wie vor initiiert werden.

Folgende Statuswerte sind für diese Services möglich:

- Wird gestartet
- Start fehlgeschlagen
- Läuft

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

Starten und Stoppen von Services

Auf dem Bildschirm „Status“ können Sie gestoppte Services 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 Support gestoppt werden.

Wenn Ihnen auffällt, dass ein Service gestoppt wurde, können Sie versuchen, ihn neu zu starten. Klicken Sie hierzu auf **Starten**. In manchen Fällen sind jedoch zusätzliche Troubleshooting-Schritte erforderlich, damit der Service ordnungsgemäß funktioniert.

Sammeln von Protokolldateien

Das Protokolldateibündel soll den Versand von Protokollen Ihrer vSphere Data Protection Appliance an Support-Mitarbeiter vereinfachen. Sie können sämtliche Protokolle von den vSphere Data Protection-Services als „Protokollbündel“ herunterladen, indem Sie auf **Protokolle sammeln** klicken. Daraufhin wird ein Dialogfeld „Speichern unter“ angezeigt, über das Sie das Protokollbündel auf das Dateisystem des Rechners herunterladen können, auf dem Ihr Webbrowser ausgeführt wird. Das Protokollbündel trägt den Namen LogBundle.zip.

Registerkarte „Konfiguration“

Die Registerkarte „Konfiguration“ wird verwendet, um die vSphere Data Protection-Konfiguration anzuzeigen und zu bearbeiten.

Folgende vSphere Data Protection-Konfigurationswerte lassen sich u. a. anzeigen oder bearbeiten:

- Netzwerkeinstellungen
  - IP-Adresse
  - Netzmaske
  - Gateway
  - Primärer DNS
  - Sekundärer DNS
  - Hostname
  - Domain
- vCenter-Registrierung
  - vCenter-Benutzername
  - vCenter-Passwort
  - vCenter-Hostname
  - vCenter-Port
  - SSO-Hostname
  - SSO-Port

- Systemeinstellungen
  - Zeitzone
  - VDP-Anmeldedaten (VDP-Passwort ändern)

Registerkarte „Rollback“

Über die Registerkarte „Rollback“ ist es möglich, ein Rollback auf einen bekannten Kontrollpunkt durchzuführen, falls vSphere Data Protection-Daten beschädigt werden.

HINWEIS Die Verwendung der Rollback-Funktion wird unter „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38 beschrieben.

Registerkarte „Upgrade“

Die Registerkarte „Upgrade“ wird verwendet, um ISO-Images auf der vSphere Data Protection Appliance zu aktualisieren.

HINWEIS Die Durchführung von Upgrades wird unter „Verwenden von VDP Configure“ auf Seite 20 beschrieben.

Verwenden von VDP Configure

VDP Configure dient den nach der Installation durchzuführenden Konfigurationsschritten.

Voraussetzungen

Die vSphere Data Protection Appliance muss installiert sowie konfiguriert sein, und Sie müssen mit dem vSphere Data Protection-Administratorkonto angemeldet sein.

Verfahren

1 Öffnen Sie einen Webbrowser, und geben Sie Folgendes ein:

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

2 Geben Sie über den VMware-Anmeldebildschirm Folgendes ein:

a Benutzer: **root**

b Passwort: ***VDP-Passwort***

c Klicken Sie auf **Anmelden**.

3 (Optional) Zum Anzeigen der vSphere Data Protection-Services klicken Sie auf die Registerkarte **Status**. Zum Stoppen oder Starten der vSphere Data Protection-Services klicken Sie auf die jeweilige Schaltfläche „Stoppen“ oder „Starten“.

4 (Optional, falls vom VMware-Support gefordert) Zum Erstellen von Support-Protokolldateien klicken Sie auf die Registerkarte **Status** und dann auf die Schaltfläche **Protokolle sammeln**. Speichern Sie die Protokollbündeldatei, und befolgen Sie die Anweisungen des VMware-Support zum Einsenden der Datei.

5 (Optional) Zum Anzeigen oder Bearbeiten der vSphere Data Protection-Konfiguration klicken Sie auf die Registerkarte **Status**.

- Netzwerkeinstellungen: Zeigen Sie die Konfiguration an, oder bearbeiten Sie diese. Wenn Sie Änderungen an der Konfiguration vornehmen, klicken Sie auf die Schaltfläche **Speichern**.
- vCenter-Registrierung: Die Einstellungen können geändert werden. Zum Bearbeiten der Einstellungen klicken Sie auf das Sperrsymbol. Wenn Sie Änderungen an den Einstellungen für die vCenter-Registrierung vornehmen, gehen die aktuellen Backup-Jobeinstellungen verloren, und Sie müssen die Backup-Jobs neu konfigurieren. Klicken Sie nach Abschluss der Änderungen auf die Schaltfläche **Speichern**.
- Systemeinstellungen: Die Zeitzone kann angezeigt oder bearbeitet werden. Wenn Sie die Zeitzone ändern, klicken Sie auf die Schaltfläche **Speichern**. Das vSphere Data Protection-Passwort lässt sich durch Klicken auf die Schaltfläche **VDP-Passwort ändern** wechseln.

Aktualisieren der vSphere Data Protection Appliance

Der Upgradeprozess umfasst die folgenden allgemeinen Schritte:

1 Erstellen eines Snapshot der vSphere Data Protection Appliance

2 Installieren des Upgrades

3 Entfernen von Snapshots

HINWEIS Wenn Sie sich nach dem Upgrade der Appliance zum ersten Mal bei vSphere Web Client anmelden, wird vSphere Data Protection in vSphere Web Client nicht als Option angezeigt. Sie müssen sich bei vSphere Web Client ab- und erneut anmelden. Bei nachfolgenden Anmeldevorgängen wird vSphere Data Protection dann als Option angezeigt.

Voraussetzungen

Um ein Softwareupgrade durchführen zu können, muss ein ISO-Upgrade-Image heruntergeladen und müssen alle vSphere Data Protection-Services ausgeführt werden.

Erstellen eines Snapshot der vSphere Data Protection Appliance

Während der Installation werden die von der vSphere Data Protection Appliance verwendeten virtuellen Festplatten auf den Status „Unabhängig – Dauerhaft“ gesetzt. Um einen Snapshot zu erstellen, ist es jedoch erforderlich, die Festplatten vorübergehend in den Status „Abhängig“ wechseln zu lassen.

So erstellen Sie einen Snapshot der vSphere Data Protection Appliance:

1 Melden Sie sich über vSphere Web Client bei vCenter Server als Benutzer an, der zum Bearbeiten von Hardwareeinstellungen und zum Erstellen von Snapshots berechtigt ist.

2 Klicken Sie auf **Hosts und Cluster**.

3 Klicken Sie in der Struktur auf der linken Seite auf die Erweiterungspfeile, bis die vSphere Data Protection Appliance angezeigt wird.

4 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Gastbetriebssystem herunterfahren** aus.

5 Klicken Sie auf **Ja**. Warten Sie, bis die vSphere Data Protection Appliance heruntergefahren wurde. Dieser Vorgang kann einige Minuten dauern.

6 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Einstellungen bearbeiten** aus.

7 Klicken Sie nun, beginnend mit Festplatte 2, auf den Erweiterungspfeil.

8 Klicken Sie in der Zeile „Festplattenmodus“ der Tabelle „Virtuelle Hardware“ auf **Abhängig**.

9 Fahren Sie mit Festplatte 3 fort, und wiederholen Sie Schritt 8, bis alle verbleibenden Festplatten in den Modus „Abhängig“ versetzt wurden.

10 Klicken Sie auf **OK**.

11 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Alle vCenter-Aktionen > Snapshot > Snapshot erstellen** aus.

12 Geben Sie einen Namen für den Snapshot ein. Geben Sie eine optionale Beschreibung ein. Klicken Sie auf **OK**.

13 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Einschalten** aus.

Installieren des Upgrades

1 Melden Sie sich bei vCenter Server mit vSphere Web Client als Administrator an.

2 Klicken Sie auf **Hosts und Cluster**.

3 Klicken Sie in der Struktur auf der linken Seite auf die Erweiterungspfeile, bis die vSphere Data Protection Appliance angezeigt wird.

4 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Einstellungen bearbeiten** aus.

5 Blenden Sie über die Registerkarte „Virtuelle Hardware“ das CD-/DVD-Laufwerk ein. Wählen Sie aus dem Dropdown-Menü die Option **Datenspeicher-ISO-Datei** aus.

6 Navigieren Sie von der Dateiauswahl zum ISO-Image, und wählen Sie dieses aus. Klicken Sie auf **OK**.

7 Aktivieren Sie rechts neben der Datenspeicher-ISO-Datei das Kontrollkästchen **Verbunden**. Klicken Sie auf **OK**. Abhängig von der Größe der ISO-Datei kann der Mount-Vorgang bis zu fünf Minuten dauern.

8 Öffnen Sie einen Webbrowser, und geben Sie Folgendes ein:

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

9 Geben Sie über den VMware-Anmeldebildschirm Folgendes ein:

a Benutzer: **root**

b Passwort: ***VDP-Passwort***

c Klicken Sie auf **Anmelden**.

10 Klicken Sie auf die Registerkarte **Upgrade**. Vergewissern Sie sich, dass das ISO-Image verfügbar ist und der Status „Bereit“ lautet. Falls nicht, ist der Ladevorgang für das ISO-Image möglicherweise noch nicht abgeschlossen.

HINWEIS Wird das ISO-Image nicht angezeigt, melden Sie sich bei VDP-Configure ab und wieder an.

11 Klicken Sie auf **VDP aktualisieren**. Das Upgrade beginnt mit der Installation. Der Installationsabschnitt des Upgrades kann lange dauern, aber Sie werden anhand einer Statusleiste über den Fortschritt der Installation auf dem Laufenden gehalten.

12 Nach erfolgreicher Upgradeinstallation klicken Sie auf **OK**. Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Gastbetriebssystem herunterfahren** aus.

Entfernen von Snapshots

Es wird ausdrücklich empfohlen, Snapshots nach erfolgreich abgeschlossenem Upgrade zu entfernen.

So entfernen Sie einen Snapshot:

1 Melden Sie sich über vSphere Web Client bei vCenter Server als Benutzer an, der zum Bearbeiten von Hardwareeinstellungen und zum Entfernen von Snapshots berechtigt ist.

2 Klicken Sie auf **Hosts und Cluster**.

3 Klicken Sie in der Struktur auf der linken Seite auf die Erweiterungspfeile, bis die vSphere Data Protection Appliance angezeigt wird.

4 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Alle vCenter-Aktionen > Snapshot > Snapshot-Manager** aus.

5 Klicken Sie auf den für die vSphere Data Protection Appliance erstellten Snapshot.

6 Klicken Sie auf **Löschen** und dann auf **Ja**.

7 Klicken Sie auf **Schließen**.

8 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Einstellungen bearbeiten** aus.

9 Klicken Sie nun, beginnend mit Festplatte 2, auf den Erweiterungspfeil.

10 Klicken Sie in der Zeile „Festplattenmodus“ der Tabelle „Virtuelle Hardware“ auf **Unabhängig – Dauerhaft**.

11 Fahren Sie mit Festplatte 3 fort, und wiederholen Sie Schritt 10, bis alle verbleibenden Festplatten in den Modus „Unabhängig – Dauerhaft“ versetzt wurden.

12 Unmounten Sie das ISO-Image. Blenden Sie über die Registerkarte „Virtuelle Hardware“ das CD-/DVD-Laufwerk ein. Wählen Sie aus dem Dropdown-Menü die Option „Client-Device“ aus. Klicken Sie auf **OK**.

13 Klicken Sie auf **OK**.

14 Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Einschalten** aus.

15 Klicken Sie nach Abschluss des Neustarts mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Einstellungen bearbeiten** aus.

Der Upgradeprozess für die vSphere Data Protection Appliance ist abgeschlossen.

Verwenden von vSphere Data Protection

3

Nach der Installation und Konfiguration von vSphere Data Protection (VDP) kann das Programm über vSphere Web Client für vSphere Data Protection gemanagt werden.

In diesem Kapitel werden folgende Themen behandelt:

- „Wissenswertes über die vSphere Data Protection-Benutzeroberfläche“ auf Seite 26
- „Zugreifen auf vSphere Data Protection“ auf Seite 29
- „Wechseln zwischen vSphere Data Protection Appliances“ auf Seite 29
- „Erstellen von Backup-Jobs“ auf Seite 29
- „Wiederherstellen virtueller Maschinen“ auf Seite 31
- „Anzeigen von Berichten“ auf Seite 33
- „Managen der Konfiguration“ auf Seite 34
- „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38
- „Verwenden der Recovery auf Dateiebene“ auf Seite 39
- „Verfahren zum Herunterfahren und Starten von vSphere Data Protection“ auf Seite 42

Wissenswertes über die vSphere Data Protection-Benutzeroberfläche

vSphere Web Client für vSphere Data Protection bietet eine Reihe neuer Benutzeroberflächenelemente, die zur Konfiguration und zum Management von vSphere Data Protection verwendet werden können.

Die Benutzeroberfläche von vSphere Data Protection besteht aus fünf Registerkarten:

- **Erste Schritte** – Enthält eine Übersicht über die Funktionen von vSphere Data Protection sowie Quicklinks zum Assistenten „Backup-Job erstellen“ und zum Assistenten „Wiederherstellen“.
- **Backup** – Enthält eine Liste der geplanten Backup-Jobs sowie Details zu jedem Backup-Job. Außerdem können über diese Seite Backup-Jobs erstellt und bearbeitet werden. Darüber hinaus bietet diese Seite die Möglichkeit, einen Backup-Job unmittelbar auszuführen.
- **Wiederherstellen** – Enthält eine Liste erfolgreicher Backups, die wiederhergestellt werden können.
- **Berichte** – Enthält Backup-Statusberichte zu den virtuellen Maschinen in vCenter.
- **Konfiguration** – Zeigt Informationen zur Konfiguration von vSphere Data Protection an und ermöglicht Ihnen die Bearbeitung mancher dieser Einstellungen.

All diese Registerkarten werden in den folgenden Abschnitten beschrieben.

Registerkarte „Erste Schritte“

Die Registerkarte „Erste Schritte“ bietet einführende Informationen über vSphere Data Protection sowie eine Möglichkeit zum Starten allgemeiner Konfigurationsaufgaben.

Tabelle 3-1. Registerkarte „Erste Schritte“

Symbol	Name	Beschreibung
	Backup-Job erstellen	Startet den Backup-Job-Assistenten. Weitere Informationen finden Sie unter „Verwenden des Backup-Job-Assistenten“ auf Seite 30.
	VM wiederherstellen	Startet den Assistenten zum Wiederherstellen einer virtuellen Maschine. Weitere Informationen finden Sie unter „Wiederherstellen virtueller Maschinen aus Backups“ auf Seite 32.
	Übersicht anzeigen	Wechselt von der aktuellen Ansicht auf die Registerkarte „Berichte“. So kann der Status vorhandener Jobs überprüft werden. Weitere Informationen finden Sie unter „Anzeigen von Berichten“ auf Seite 33.

Registerkarte „Backup“

Auf der Registerkarte „Backup“ werden Informationen über vorhandene Backup-Jobs und ihren Status angezeigt. Darüber hinaus bietet sie eine Möglichkeit, Ad-hoc-Backup-Jobs zu erstellen, zu bearbeiten, zu löschen, zu aktivieren bzw. deaktivieren und auszuführen.

Tabelle 3-2. Symbole der Registerkarte „Backup“

Symbol	Name	Beschreibung
	Neu	Startet den Backup-Job-Assistenten. Weitere Informationen finden Sie unter „Verwenden des Backup-Job-Assistenten“ auf Seite 30.
	Bearbeiten	Startet den Backup-Job-Assistenten zur Bearbeitung eines vorhandenen Jobs.
	Löschen	Löscht den ausgewählten Backup-Job.
	Aktivieren/Deaktivieren	Konfiguriert den Backup-Job als „Aktiviert“ oder „Deaktiviert“.
	Jetzt sichern	Startet ein Ad-hoc-Backup.

Auf der Registerkarte „Backup“ wird eine Liste der erstellten Backup-Jobs angezeigt. Die Backup-Jobs sind in einer Tabelle aufgeführt, die die folgenden Informationen enthält:

Tabelle 3-3. Spaltenbeschreibungen der Registerkarte „Backup“

Spalte	Beschreibung
Name	Name des Backup-Jobs
Status	„Aktiviert“ oder „Deaktiviert“. Deaktivierte Backup-Jobs werden nicht ausgeführt.
Letzte Startzeit	Der letzte Zeitpunkt, zu dem der Job gestartet wurde.
Dauer	Die Dauer des Jobs bei der letztmaligen Ausführung.
Nächste Ausführungszeit	Der Zeitpunkt, zu dem der Job für eine weitere Ausführung geplant ist.
Erfolgsanzahl	Die Anzahl virtueller Maschinen, die bei der letzten Ausführung des Backup-Jobs erfolgreich gesichert wurden.
Fehleranzahl	Die Anzahl virtueller Maschinen, die bei der letzten Ausführung des Backup-Jobs nicht erfolgreich gesichert wurden.

Registerkarte „Wiederherstellen“

Auf der Registerkarte „Wiederherstellen“ wird eine Liste der in der vSphere Data Protection Appliance gesicherten virtuellen Maschinen angezeigt. Sie können durch die Liste der Backups navigieren und bestimmte Backups auswählen und wiederherstellen. Nach einer gewissen Zeit können die auf der Registerkarte „Wiederherstellen“ angezeigten Informationen veralten. Um die neuesten Informationen zu Backups anzuzeigen, die für eine Wiederherstellung bereitstehen, klicken Sie auf **Aktualisieren**.

Auf der Registerkarte „Wiederherstellen“ werden die folgenden Symbole verwendet.

Tabelle 3-4. Symbole der Registerkarte „Wiederherstellen“

Symbol	Name	Beschreibung
	Wiederherstellen	Startet den Assistenten bzw. das Dialogfeld zum Wiederherstellen virtueller Maschinen aus Backups. Hierüber kann konfiguriert werden, wie virtuelle Maschinen in den in den Wiederherstellungspunkten gespeicherten Status zurückversetzt werden. Weitere Informationen finden Sie unter „Wiederherstellen virtueller Maschinen aus Backups“ auf Seite 32. Standardmäßig managt vSphere Data Protection die Speicherung und letztendliche Löschung älterer Wiederherstellungspunkte gemäß der im Backup-Job angegebenen Aufbewahrungs-Policy.
	Sperren/Entsperren	„Sperren“ ändert den Ablaufpunkt eines Backup-Jobs zu „kein Enddatum“.
	Löschen	Legt fest, dass die ausgewählten Wiederherstellungspunkte gelöscht werden.
	Gesamte Auswahl löschen	Löscht die gesamte Auswahl auf der Registerkarte „Wiederherstellen“.

Registerkarte „Berichte“

Die Registerkarte „Berichte“ liefert eine Übersicht über die Informationen zur vSphere Data Protection Appliance sowie über die virtuellen Maschinen im virtuellen Center.

Registerkarte „Konfiguration“

Über die Registerkarte „Konfiguration“ können Sie Wartungsaufgaben für die vSphere Data Protection Appliance managen.

Die folgenden drei Aufgaben können auf dieser Registerkarte ausgeführt werden:

- Anzeigen oder Bearbeiten des Backup-Zeitfensters (siehe „Konfiguration des Backup-Zeitfensters“ auf Seite 34)
- Ausführen einer Integritätsprüfung (siehe „Manuelles Ausführen einer Integritätsprüfung“ auf Seite 37)
- Konfigurieren von E-Mails (siehe „Konfigurieren der E-Mail-Benachrichtigung“ auf Seite 37)

Zugreifen auf vSphere Data Protection

Auf vSphere Data Protection wird über vSphere Web Client zugegriffen.

HINWEIS vSphere Data Protection wird ausschließlich durch vSphere Web Client gemanagt. vSphere Client bietet keine Unterstützung für das Management von vSphere Data Protection.

Voraussetzungen

Bevor vSphere Data Protection verwendet werden kann, müssen Sie die vSphere Data Protection Appliance, wie unter „Installieren und Konfigurieren von vSphere Data Protection“ auf Seite 11 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 vCenter-Benutzernamen und ein vCenter-Passwort ein, und klicken Sie auf **Anmelden**.

vSphere Data Protection nutzt diese Informationen, um für Backups eine vCenter-Verbindung herzustellen. Das angegebene Benutzerkonto muss also über Administratorrechte verfügen.

3 Wählen Sie in vSphere Web Client die Option **vSphere Data Protection** aus.

4 Wählen Sie auf der Seite „Willkommen bei vSphere Data Protection“ die vSphere Data Protection Appliance aus, und klicken Sie auf **Verbinden**.

Wechseln zwischen vSphere Data Protection Appliances

Jede vCenter Server-Installation unterstützt bis zu 10 vSphere Data Protection Appliances. Sie können zwischen Appliances wechseln, indem Sie aus der Dropdown-Liste rechts neben der Bezeichnung „Appliance wechseln“ eine Appliance wählen.

HINWEIS Die vSphere Data Protection Appliances in der Dropdown-Liste sind alphabetisch sortiert, und das erste Element in der Liste, das auf dem Bildschirm angezeigt wird, stimmt möglicherweise nicht mit der aktuellen Appliance überein. Bei dem auf dem vSphere Data Protection-Bildschirm links angezeigten Appliance-Namen handelt es sich um die aktuelle Appliance, und der Appliance-Name in der Dropdown-Liste ist die erste Appliance in der Liste der verfügbaren Appliances.

Erstellen von Backup-Jobs

Sie können Backup-Jobs erstellen, in denen festgelegt ist, welche virtuellen Maschinen gesichert werden, wie oft Backups stattfinden und wie lange die Aufbewahrungsfrist zum Speichern der Backups ist. vSphere Data Protection nutzt das Backup-Zeitfenster, um neue Backups und die Aufbewahrungs-Policy zu erstellen bzw. um bestimmte ältere Backups zu entfernen.

Virtuelle Maschinen

Sie können Sammlungen virtueller Maschinen angeben, z. B. alle virtuelle Maschinen in einem Rechenzentrum, oder einzelne virtuelle Maschinen auswählen. Bei Auswahl eines kompletten Ressourcenpools, Hosts, Rechenzentrums oder Ordners sind alle neuen virtuellen Maschinen in diesem Container Teil nachfolgender Backups. Bei Auswahl einer virtuellen Maschine wird jede der virtuellen Maschine hinzugefügte Festplatte in das Backup aufgenommen. Wenn eine virtuelle Maschine aus dem ausgewählten Container in einen anderen nicht ausgewählten Container verschoben wird, ist die virtuelle Maschine nicht länger Teil des Backup.

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.

HINWEIS Die Verwendung von vSphere Data Protection zum Backup der vSphere Data Protection Appliance wird nicht unterstützt.

Planung

Anhand der Backup-Planung wird festgelegt, wie oft Ihre Auswahl gesichert wird. Die Backups werden so nah wie möglich am Startzeitpunkt des Backup-Zeitfensters ausgeführt. Sie können Backups so planen, dass sie täglich, wöchentlich oder an einem bestimmten Tag im Monat ausgeführt werden.

Aufbewahrungs-Policy

Mithilfe von Backup-Aufbewahrungs-Policies kann festgelegt werden, wie lange ein Backup im System aufbewahrt wird.

Eine Aufbewahrungs-Policy wird jedem Backup während des Backup-Vorgangs zugewiesen. Wenn die Aufbewahrungsfrist für ein Backup abläuft, wird das Backup gelöscht.

Tabelle 3-5 enthält eine Beschreibung der Aufbewahrungs-Policies für Backups.

Tabelle 3-5. Einstellungen für Aufbewahrungs-Policies

Aufbewahrungseinstellung	Beschreibung
Immer	Bewahrt Backups auf unbestimmte Zeit auf. Diese Einstellung ist nützlich, wenn dafür gesorgt werden soll, dass alle dieser Aufbewahrungs-Policy zugewiesenen Backups während des gesamten Lebenszyklus des Systems aufbewahrt werden.
Für (Aufbewahrungsfrist)	Definiert eine fixe Aufbewahrungsfrist in Tagen, Wochen, Monaten oder Jahren für die Zeit nach dem Backup. Beispielsweise können Sie festlegen, dass Backups nach 6 Monaten ablaufen.
Bis (Enddatum)	Weist ein Kalenderdatum als Ablaufdatum zu. Beispielsweise können Sie als Ablaufdatum für Backups den 31. Dezember 2013 angeben.
Für (diese Planung)	Definiert eine fixe Aufbewahrungsfrist, und zwar basierend auf der Angabe zur täglichen, wöchentlichen, monatlichen und jährlichen Aufbewahrung. Beispielsweise können Sie festlegen, dass Backups täglich für 30 Tage, wöchentlich für 52 Wochen, monatlich für 12 Monate und jährlich für 2 Jahre aufbewahrt werden.

Bereit zur Fertigstellung

Überprüfen Sie die Einstellungen für den Backup-Job. Auf dieser Seite sind die folgenden Informationen enthalten:

- Name des Backup-Jobs
- die von diesem Job gesicherten virtuellen Maschinen
- die Planung für das Backup virtueller Maschinen
- die für das Backup ausgewählte Aufbewahrungs-Policy

Verwenden des Backup-Job-Assistenten

Verwenden Sie den Backup-Job-Assistenten, um die zu sichernden virtuellen Maschinen und den Zeitpunkt für das Backup anzugeben.

Verfahren

1 Wählen Sie in vSphere Web Client die Option **vSphere Data Protection** aus.

2 Wählen Sie auf der Seite „Willkommen bei vSphere Data Protection“ die vSphere Data Protection Appliance aus, und klicken Sie auf **Verbinden**.

3 Klicken Sie auf die Registerkarte **Backup** und dann auf **Neu**, um den Backup-Job-Assistenten zu starten.

4 Wählen Sie auf der Seite „Virtuelle Maschinen“ einzelne zu sichernde virtuelle Maschinen oder Container mit virtuellen Maschinen aus, und klicken Sie auf **Weiter**.

5 Wählen Sie auf der Seite „Planung“ die Backup-Planung für den Job aus, und klicken Sie auf **Weiter**.

6 Nehmen Sie auf der Seite „Aufbewahrungs-Policy“ die standardmäßige Aufbewahrungs-Policy an, oder legen Sie eine alternative Aufbewahrungs-Policy fest. Klicken Sie dann auf **Weiter**.

7 Geben Sie auf der Seite „Name“ einen Backup-Jobnamen ein, und klicken Sie auf **Weiter**.

8 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung“ die Zusammenfassung zum Backup-Job, und klicken Sie auf **Fertig stellen**.

9 In einem Informationsdialogfeld wird die erfolgreiche Erstellung des Backup-Jobs bestätigt. Klicken Sie auf **OK**.

Jetzt sichern

Nach der Erstellung eines Backup-Jobs können Sie über das Symbol „Jetzt sichern“ einen Backup-Job manuell initiieren.

Voraussetzungen

Vor der Verwendung der Option „Jetzt sichern“ müssen Sie vSphere Data Protection installieren und konfigurieren, und Sie sollten über mindestens einen Backup-Job verfügen.

Verfahren

1 Wählen Sie in vSphere Web Client die Option **vSphere Data Protection** aus.

2 Wählen Sie auf der Seite „Willkommen bei vSphere Data Protection“ die vSphere Data Protection Appliance aus, und klicken Sie auf **Verbinden**.

3 Klicken Sie auf die Registerkarte **Backup**, und wählen Sie einen Backup-Job aus. Klicken Sie auf **Jetzt sichern**, und wählen Sie entweder „Alle Quellen sichern“ oder „Nur veraltete Quellen sichern“ aus.

- Die Option „Alle Quellen sichern“ legt fest, dass alle Jobs gesichert werden sollen.
- Die Option „Nur veraltete Quellen sichern“ legt fest, dass nur die Backup-Jobs gesichert werden, bei denen der letzte Backup-Versuch fehlgeschlagen ist.

Wiederherstellen virtueller Maschinen

Sie können mithilfe des Assistenten zum Wiederherstellen virtueller Maschinen festlegen, welche virtuellen Maschinen wiederhergestellt sowie wie und wohin diese wiederhergestellt werden.

ACHTUNG Wenn die virtuelle Maschine, auf die Sie wiederherstellen, einen Snapshot enthält, schlägt die Wiederherstellung fehl. Entfernen Sie vor dem Beginn des Wiederherstellungsprozesses etwaige Snapshots von der virtuellen Maschine.

Backup auswählen

Mit der Option „Backup auswählen“ werden die wiederherzustellenden virtuellen Maschinen angegeben. Die Erstellung von Wiederherstellungen ähnelt der von Backup-Jobs. Sie können einen Container virtueller Maschinen oder bestimmte virtuelle Maschinen festlegen. Es ist möglich, virtuelle Maschinen an alternativen Speicherorten wiederherzustellen.

Wiederherstellungsoptionen festlegen

Mit der Option „Wiederherstellungsoptionen festlegen“ wird angegeben, wo das Backup wiederhergestellt werden soll.

Sie können Folgendes festlegen:

- ob das Backup am ursprünglichen Speicherort wiederhergestellt wird
- ob das Backup an einem alternativen Speicherort wiederhergestellt wird
  - Neuer Name
  - Ziel
  - Datenspeicher

Zum Klonen einer virtuellen Maschine benennen Sie sie während der Wiederherstellung um.

Bereit zur Fertigstellung

Überprüfen Sie die Einstellungen für den Wiederherstellungsjob. Die Zusammenfassung enthält Informationen zur Anzahl der wiederhergestellten virtuellen Maschinen und zur Anzahl der erstellten virtuellen Maschinen.

Wiederherstellen virtueller Maschinen aus Backups

Versetzen Sie virtuelle Maschinen mit dem Assistenten zum Wiederherstellen virtueller Maschinen in einen früheren Backup-Status zurück.

Voraussetzungen

Bevor virtuelle Maschinen wiederhergestellt werden können, müssen Sie vSphere Data Protection konfigurieren. Außerdem ist mindestens ein Backup erforderlich, aus dem wiederhergestellt werden kann.

Verfahren

1 Wählen Sie in vSphere Web Client die Option **vSphere Data Protection** aus.

2 Wählen Sie auf der Seite „Willkommen bei vSphere Data Protection“ die vSphere Data Protection Appliance aus, und klicken Sie auf **Verbinden**.

3 Klicken Sie auf der Registerkarte **Wiederherstellen** auf die gleichnamige Schaltfläche.

4 Der Assistent zum Wiederherstellen virtueller Maschinen wird angezeigt.

5 Geben Sie auf der Seite „Backup auswählen“ eine Quelle an, aus der virtuelle Maschinen wiederhergestellt werden sollen, und klicken Sie auf **Weiter**.

6 Wenn die virtuelle Maschine über mehr als einen Backup-Punkt verfügt, heben Sie die Auswahl all der Punkte auf, die nicht wiederhergestellt werden. Es sollte nur ein Backup-Punkt ausgewählt werden.

7 Vergewissern Sie sich auf der Seite „Wiederherstellungsoptionen festlegen“, dass Client- und Backup-Wiederherstellungspunkt korrekt sind. Wählen Sie „Am ursprünglichen Speicherort wiederherstellen“ aus. Zum Wiederherstellen an einem alternativen Speicherort deaktivieren Sie das Kontrollkästchen „Am ursprünglichen Speicherort wiederherstellen“, und geben Sie ein alternatives Ziel und einen alternativen Datenspeicher an. Klicken Sie auf **Weiter**.

8 Überprüfen Sie auf der Seite „Bereit zur Fertigstellung“ die Konfiguration, und klicken Sie auf **Fertig stellen**.

Die virtuellen Maschinen werden wie im Assistenten angegeben wiederhergestellt.

Anzeigen des Fortschritts von Wiederherstellungsjobs

Nach der Initiierung eines Wiederherstellungsjobs kann der aktuelle Wiederherstellungsprozess über das Fenster „Letzte Aufgaben“ angezeigt werden.

Sperren von Backup-Jobs

Das Sperrsymbol dient zum Ändern des Ablaufpunkts eines Backup-Job zu „kein Enddatum“. Hierdurch wird vermieden, dass ein Backup-Job nach Erreichen des Ablaufdatums manuell abläuft und automatisch gelöscht wird. Die Sperroption verhindert nicht das Löschen eines Backup-Jobs. Ein gesperrter Job kann nach wie vor von einem Administrator gelöscht werden. Zum Sperren eines Backup-Jobs wählen Sie den oder die Backup-Job(s) auf der Registerkarte „Wiederherstellen“ aus und klicken auf das Sperrsymbol. Gesperrte Backup-Jobs werden links vom Backup-Jobnamen mit einem gelben Schloss angezeigt.

Anzeigen von Berichten

Auf der Registerkarte „Berichte“ wird der aktuelle Status für Folgendes angezeigt:

- Appliance-Status
- Genutzte Kapazität
- Status der Integritätsprüfung
- Aktuelle erfolgreiche Backups
- Aktuelle fehlgeschlagene Backups

Filtern auf der Registerkarte „Berichte“

Standardmäßig werden auf der Registerkarte „Berichte“ alle mit vCenter Server verbundenen virtuellen Maschinen angezeigt. Die Option „Filter“ auf der Registerkarte „Berichte“ filtert anhand folgender Kriterien:

- Alle anzeigen
- Virtuelle Maschine
  - Name
  - Status
  - Letztes erfolgreiches Backup
- Letzter Backup-Job
  - Name
  - Status
  - Datum

Managen der Konfiguration

Die Registerkarte „Konfiguration“ wird verwendet, um Konfigurationsinformationen anzuzeigen und zu ändern. Die folgenden Themen werden in diesem Abschnitt behandelt:

- „Anzeigen und Bearbeiten von Backup-Appliance-Details“ auf Seite 34
- „Konfiguration des Backup-Zeitfensters“ auf Seite 34
- „Ändern der Einstellungen für das Wartungsfenster“ auf Seite 36
- „Manuelles Ausführen einer Integritätsprüfung“ auf Seite 37
- „Konfigurieren der E-Mail-Benachrichtigung“ auf Seite 37

Über die Registerkarte „Konfiguration“ können Backup-Appliance-Details, eine Speicherübersicht und die Konfiguration des Backup-Zeitfensters angezeigt werden.

Anzeigen und Bearbeiten von Backup-Appliance-Details

Zu den Backup-Appliance-Details gehören folgende Informationen:

- IP-Adresse
- VDP-Appliance-Version
- Status
- vCenter Server
- Aktueller Benutzer
- Ortszeit
- Zeitzone
- Freier Speicherplatz
- Deduplizierte Größe
- Nicht deduplizierte Größe

HINWEIS Die Speicherkapazität wird in GiB (statt in GB) angezeigt, was 1024 MB entspricht.

Konfiguration des Backup-Zeitfensters

Jeder 24 Stunden umfassende Tag ist in drei Betriebszeitfenster (Backup-Zeitfenster, Ausfallzeitfenster und Wartungsfenster) unterteilt, während denen Systemaktivitäten durchgeführt werden können.

Backup-Zeitfenster

Das Backup-Zeitfenster ist der Teil jedes Tages, der zur Ausführung von normal geplanten Backups reserviert ist.

- Betriebliche Auswirkungen – Standardmäßig werden während des Backup-Zeitfensters keine Wartungsvorgänge durchgeführt.
- Standardeinstellungen – Das standardmäßige Backup-Zeitfenster beginnt um 20 Uhr lokale Serverzeit und läuft 12 Stunden ununterbrochen bis um 8 Uhr am folgenden Morgen.
- Anpassung – Sie können Startzeit und Dauer des Backup-Zeitfensters an bestimmte Standortanforderungen anpassen.

vSphere Data Protection versucht, jede virtuelle Maschine eines Jobs einmal am Tag während des zugehörigen Backup-Zeitfensters zu sichern. Backups starten zu Beginn des Backup-Zeitfensters, und es können bis zu acht Backup-Jobs gleichzeitig ausgeführt werden.

HINWEIS Wenn mehrere vSphere Data Protection Appliances dieselben virtuellen Maschinen sichern, sollten die Backup-Zeitfenster angepasst werden, damit sich die Backup-Jobs auf den verschiedenen Appliances nicht überschneiden. Wenn sich Backup-Jobs überschneiden, treten Backup-Fehler auf.

Ausfallzeitfenster

Das Ausfallzeitfenster ist der Teil jedes Tages, der zur Ausführung von Serverwartungsaktivitäten reserviert ist, für die z. B. zur Sammlung veralteter Daten unbeschränkter Zugriff auf den Server erforderlich ist. Bei der Sammlung veralteter Daten werden die verwaisten Datensegmente gelöscht, die nicht länger innerhalb von im System gespeicherten Backups referenziert werden.

- Betriebliche Auswirkungen – Während des Ausfallzeitfensters sind weder Backup- noch Administrationsvorgänge zulässig. Wiederherstellungen sind möglich.
- Standardeinstellungen – Das standardmäßige Ausfallzeitfenster beginnt um 8 Uhr lokale Serverzeit und läuft 3 Stunden ununterbrochen bis um 11 Uhr desselben Morgens.
- Anpassung – Sie können Startzeit und Dauer des Ausfallzeitfensters an bestimmte Standortanforderungen anpassen.

Alle Änderungen in Bezug auf die Dauer des Ausfallzeitfensters wirken sich auch auf die Dauer des Wartungsfensters aus. Wenn z. B. die Dauer des Ausfallzeitfensters von 3 auf 2 Stunden geändert wird, verlängert sich hierdurch das Wartungsfenster um eine Stunde, da es eine Stunde früher beginnt. Das Backup-Zeitfenster ist hiervon nicht betroffen.

Wartungsfenster

Das Wartungsfenster ist der Teil jedes Tages, der zur Ausführung routinemäßiger Wartungsaktivitäten am Server wie Validierung der Integritätsprüfungen reserviert ist.

- Betriebliche Auswirkungen – Kurzzeitig sind ggf. weder Backup- noch Administrationsvorgänge zulässig.

  Obwohl Backups während des Wartungsfensters initiiert werden können, beeinflusst dies sowohl Backup- als auch Wartungsvorgänge. Beschränken Sie daher während des Wartungsfensters Backup- oder Administrationsvorgänge auf ein Minimum. Wiederherstellungen können allerdings durchgeführt werden.

  Integritätsprüfung und Backups dürfen sich zwar überschneiden, dies kann jedoch zu I/O-Ressourcenkonflikten führen, sodass die Vorgänge jeweils länger dauern und womöglich fehlschlagen.
- Standardeinstellungen – Das standardmäßige Wartungsfenster beginnt um 11 Uhr lokale Serverzeit und läuft 9 Stunden ununterbrochen bis um 20 Uhr desselben Abends.
- Anpassung – Auch wenn das Wartungsfenster nicht direkt anpassbar ist, werden Startzeit und Dauer vom Backup- und Ausfallzeitfenster abgeleitet.

Das Wartungsfenster beginnt direkt nach dem Ausfallzeitfenster und endet erst zur Startzeit des Backup-Zeitfensters.

Integritätsprüfung

Dieser Vorgang wird durchgeführt, um die Datenintegrität im Deduplizierungsspeicher zu verifizieren und zu bewahren. vSphere Data Protection ist auf den Abschluss einer inkrementellen oder vollständigen Integritätsprüfung während des Wartungsfensters ausgelegt. Bei inkrementellen Integritätsprüfungen wird die Integrität der Kontrollpunkte überprüft, die dem Deduplizierungsspeicher seit der letzten vollständigen oder inkrementellen Integritätsprüfung hinzugefügt wurden. vSphere Data Protection ist außerdem so konzipiert, dass einmal am Tag alle Kontrollpunkte einer Integritätsprüfung unterzogen werden. Weitere Informationen finden Sie unter „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38.

Das Wartungsfenster sollte verwendet werden, um Situationen zu vermeiden, in denen Integritätsprüfungen möglicherweise Rechenressourcen belegen oder laufende Backup-Vorgänge anderweitig stören. Daher sind das Wartungsfenster und das Backup-Zeitfenster so definiert, dass keine Überschneidungen vorliegen. Der Wartungsprozess wird gestoppt, wenn er nicht innerhalb des definierten Zeitfensters abgeschlossen wird.

Selbst wenn der Wartungsprozess gestoppt wird, ist das Ziel nicht von anderen Vorgängen wie Backup und Wiederherstellung ausgeschlossen. Beim nächsten Öffnen des Zielwartungsfensters wird der Vorgang an der Stelle, an der er unterbrochen wurde, fortgesetzt. Weitere Informationen zum Konfigurieren des Wartungsfensters finden Sie unter „Ändern der Einstellungen für das Wartungsfenster“ auf Seite 36.

Ferner ist ein manueller Start der Integritätsprüfung möglich. Wird die Integritätsprüfung manuell gestartet, wird das gesamte Ziel einer vollständigen Integritätsprüfung unterzogen, und das Wartungsfenster wird nicht verwendet. Normalerweise sind während der Integritätsprüfung Backup- und Wiederherstellungsvorgänge vom Deduplizierungsspeicher zulässig. Wenn ein Wiederherstellungspunkt manuell zum Löschen markiert wird, sind Backups während der Integritätsprüfung nicht zulässig, Wiederherstellungsvorgänge jedoch schon. Sollten während der Integritätsprüfung beschädigte Wiederherstellungspunkte im Deduplizierungsspeicher gefunden werden, ist es zum Löschen erforderlich, dass nach der Markierung der beschädigten Wiederherstellungspunkte eine manuelle Integritätsprüfung durchgeführt wird. Während dieser manuell ausgeführten Integritätsprüfung sind weder Backups noch Wiederherstellungen zulässig. Weitere Informationen zum manuellen Starten von Integritätsprüfungen finden Sie unter „Manuelles Ausführen einer Integritätsprüfung“ auf Seite 37.

vSphere Data Protection speichert Informationen zum Fortschritt von Integritätsprüfungen. Wenn die vSphere Data Protection Appliance eine Integritätsprüfung stoppt, lässt sich der Prozess daher wieder an der Stelle neu starten, an der er unterbrochen wurde. So wird dafür gesorgt, dass die im Rahmen einer Integritätsprüfung abgeschlossene Arbeit nicht verloren geht. Die Appliance stoppt Integritätsprüfungen nach Ablauf der innerhalb des Wartungsfensters zur Verfügung stehenden Zeit. Durch die Nachverfolgung des Fortschritts wird erreicht, dass Integritätsprüfungen am Ende auch abgeschlossen werden. Bei durch Eingreifen des Benutzers manuell gestoppten Integritätsprüfungen werden keine Informationen zum Fortschritt gespeichert, sodass nach einem Stopp die Integritätsprüfung wieder von vorne beginnt.

Ändern der Einstellungen für das Wartungsfenster

Die Einstellungen für das Wartungsfenster werden über die Registerkarte „Konfiguration“ geändert.

Voraussetzungen

Bevor Sie die Einstellungen für das Wartungsfenster ändern können, müssen Sie vSphere Data Protection installieren und konfigurieren.

Verfahren

1 Wählen Sie in vSphere Web Client die Option **vSphere Data Protection** aus.

2 Wählen Sie auf der Seite „Willkommen bei vSphere Data Protection“ Ihre vSphere Data Protection Appliance aus, und klicken Sie auf **Verbinden**.

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

4 Klicken Sie unter „Konfiguration des Backup-Zeitfensters“ auf **Bearbeiten**.

5 Legen Sie Werte für „Backup-Startzeit“, „Backup-Dauer“ und „Ausfalldauer“ fest, und klicken Sie auf **Speichern**.

Manuelles Ausführen einer Integritätsprüfung

Integritätsprüfungen können manuell über die Registerkarte „Konfiguration“ ausgeführt werden.

Voraussetzungen

Vor der Ausführung einer Integritätsprüfung müssen Sie vSphere Data Protection konfigurieren.

Verfahren

1 Wählen Sie in vSphere Web Client die Option **vSphere Data Protection** aus.

2 Wählen Sie auf der Seite „Willkommen bei vSphere Data Protection“ Ihre vSphere Data Protection Appliance aus, und klicken Sie auf **Verbinden**.

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

4 Klicken Sie im Bildschirmabschnitt „Konfiguration des Backup-Zeitfensters“ auf das Symbol „Einstellungen“ (oben rechts auf der Registerkarte „Konfiguration“) und dann auf **Integritätsprüfung ausführen**.

5 Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Ja**.

Konfigurieren der E-Mail-Benachrichtigung

Wenn keine E-Mail-Benachrichtigung aktiviert ist, enthalten gesendete E-Mails folgende Informationen:

- VDP-Appliance-Status
- Zusammenfassung Backup-Jobs
- Zusammenfassung virtuelle Maschinen

Voraussetzungen

Damit E-Mail-Berichte konfiguriert werden können, muss zunächst ein E-Mail-Konto vorhanden sein.

Verfahren

1 Wählen Sie in vSphere Web Client die Option **vSphere Data Protection** aus.

2 Wählen Sie auf der Seite „Willkommen bei vSphere Data Protection“ Ihre vSphere Data Protection Appliance aus, und klicken Sie auf **Verbinden**.

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

4 Klicken Sie auf die Schaltfläche **E-Mail**.

5 Klicken Sie unten rechts auf dem Bildschirm auf die Schaltfläche **Bearbeiten**.

6 Geben Sie Folgendes an:

   a Wählen Sie **E-Mail-Berichte aktivieren** aus.

   b Legen Sie den **Postausgangsserver** fest.

   c (Optional) Wählen Sie **Mein Server erfordert eine Anmeldung** aus. Ist diese Option aktiviert, geben Sie den zugehörigen **Benutzernamen** und das zugehörige **Passwort** an.

   d Legen Sie die **Absenderadresse** fest.

   e Legen Sie die **Empfängeradresse(n)** fest.

   f Wählen Sie den/die **Sendetag(e)** aus.

   g Wählen Sie das **Berichtsgebietsschema** aus.

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

Verwenden von Kontrollpunkten und Rollback

Bei einem Kontrollpunkt handelt es sich um ein systemweites, ausdrücklich zur Disaster-Recovery-Unterstützung erstelltes Backup. Kontrollpunkte werden während des Wartungsfensters einmal am Tag geplant und erstellt, wie unter „Wartungsfenster“ auf Seite 35 beschrieben. vSphere Data Protection speichert zwei Kontrollpunkte (einen validierten und einen nicht validierten Kontrollpunkt). Ein Rollback ist der Prozess, bei dem die vSphere Data Protection Appliance mithilfe der in einem validierten Kontrollpunkt gespeicherten Daten in einem bekannten fehlerfreien Zustand wiederhergestellt wird. Standardmäßig sind die Wartungsservices nach der Bereitstellung einer Appliance 24-48 Stunden deaktiviert. Dies ermöglicht ein längeres Backup-Zeitfenster und damit Unterstützung bei den ersten Backups.

Im Falle eines unerwarteten Herunterfahren-Vorgangs führt die Appliance beim Neustart ein Rollback auf den letzten validierten Kontrollpunkt durch. Hierbei handelt es sich um erwartetes Verhalten, mit dem eine Beschädigung der Appliance verhindert werden soll.

Bei der Bereitstellung der Appliance wird ein Ad-hoc-Kontrollpunkt erstellt. Dieser Kontrollpunkt umfasst die Appliance-Einstellungen der Installation. Wenn eine Appliance während der ersten 24-48 Stunden der Bereitstellung unerwartet heruntergefahren wird, wird für die Appliance ein Rollback auf den Ad-hoc-Kontrollpunkt durchgeführt. Alle zwischen der Erstellung des Ad-hoc-Kontrollpunkts und dem unerwarteten Herunterfahren-Vorgang erstellten Backup-Jobs oder Backups gehen verloren. Wenn während dieses Zeitfensters ein Kontrollpunkt erstellt werden soll, führen Sie manuell eine Integritätsprüfung aus. Zusätzliche Informationen finden Sie unter „Manuelles Ausführen einer Integritätsprüfung“ auf Seite 37.

HINWEIS Bei Anwendung eines Rollback gehen alle nach dem ausgewählten Kontrollpunkt durchgeführten Backups verloren.

Voraussetzungen

Bevor ein Rollback durchgeführt werden kann, müssen Sie vSphere Data Protection installieren und konfigurieren. Außerdem müssen Kontrollpunkte erstellt und validiert worden sein.

ACHTUNG Es wird ausdrücklich empfohlen, ein Rollback ausschließlich auf den zuletzt validierten Kontrollpunkt durchzuführen.

Verfahren

1 Öffnen Sie einen Webbrowser, und geben Sie Folgendes ein:

http://<*IP_Adresse_der _VDP_Appliance*>:8543/vdp-configure/

2 Geben Sie über den VMware-Anmeldebildschirm Folgendes ein:

a Benutzer: **root**

b Passwort: ***VDP-Passwort***

c Klicken Sie auf **Anmelden**.

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

4 Klicken Sie auf **Entsperren, um VDP-Rollback zu aktivieren**.

5 Ein Warndialogfeld warnt davor, dass alle nach dem ausgewählten Kontrollpunkt durchgeführten Backups verloren gehen. Wenn dies akzeptabel ist, geben Sie das Passwort für die vSphere Data Protection Appliance ein, und klicken Sie auf **OK**.

6 Wählen Sie einen validierten Kontrollpunkt (valid=true) aus, und klicken Sie auf **VDP-Rollback auf ausgewählten Kontrollpunkt durchführen**.

Verwenden der Recovery auf Dateiebene

vSphere Data Protection erstellt Backups gesamter virtueller Maschinen. Diese Backups lassen sich mithilfe von vSphere Web Client für vSphere Data Protection komplett wiederherstellen. Wenn jedoch nur bestimmte Dateien von diesen virtuellen Maschinen wiederhergestellt werden sollen, dann verwenden Sie den Wiederherstellungsclient von vSphere Data Protection.

Der Wiederherstellungsclient ermöglicht es, bestimmte VM-Backups als Dateisysteme zu mounten und anschließend das Dateisystem nach den wiederherzustellenden Dateien zu „durchsuchen“.

Der Wiederherstellungsclient verfügt über zwei Betriebsmodi:

- Standard – Sie können nur die Backups mounten, die von dem Rechner, an dem Sie angemeldet sind, erstellt werden, und alle von Ihnen wiederhergestellten Dateien werden auf diesem Client wiederhergestellt.

  Wenn Sie sich z. B. im Standardmodus von einem Windows-Host namens „WS44“ beim Wiederherstellungsclient angemeldet haben, können Sie die Backups von „WS44“ mounten und durchsuchen.

- Erweitert – Sie können alle in vSphere Data Protection vorhandenen Backups mounten und durchsuchen.

Gleichzeitig können höchstens acht Backups gemountet sein.

HINWEIS Zum Wiederherstellen von Dateien mithilfe der Recovery auf Dateiebene muss auf der virtuellen Maschine, die Sie mit dem Wiederherstellungsclient verbinden, VMware Tools installiert sein. Eine virtuelle Maschine mit VMware Tools-Installation kann den Wiederherstellungsclient einsetzen, um Dateien aus Backups von Rechnern ohne VMware Tools-Installation wiederherzustellen. Virtuelle Maschinen ohne VMware Tools können gesicherte Dateien mithilfe des Wiederherstellungsclients hingegen nicht erfolgreich wiederherstellen.

HINWEIS Der Wiederherstellungsclient unterstützt nicht die Verwendung von VMware vSphere vMotion oder VMware vSphere Storage vMotion.

Unterstützte Konfigurationen bei der Recovery auf Dateiebene:

Die Recovery auf Dateiebene kann für Backups der folgenden Dateisysteme durchgeführt werden:

- NTFS (primäre Partition mit MBR)
- Ext2 (primäre Partition mit MBR)
- Ext3 (primäre Partition mit MBR)
- LVM mit ext2 (primäre Partition mit MBR und eigenständiges [ohne MBR] LVM mit ext2)
- LVM mit ext3 (primäre Partition mit MBR und eigenständiges [ohne MBR] LVM mit ext3)

Einschränkungen der Recovery auf Dateiebene

Bei einer Recovery auf Dateiebene werden die folgenden Konfigurationen virtueller Laufwerke nicht unterstützt:

- unformatierte Festplatten
- dynamische Festplatten (Windows)/Multi-Laufwerkspartitionen (aus 2 oder mehr virtuellen Laufwerken bestehende Partitionen)
- GUID Partition Table- (GPT-)Festplatten
- ext4-Dateisysteme
- FAT16-Dateisysteme
- FAT32-Dateisysteme
- erweiterte Partitionen

- verschlüsselte Partitionen
- komprimierte Partitionen

Die folgenden Einschränkungen gelten im Zusammenhang mit der Recovery auf Dateiebene:

- Symbolische Links können weder wiederhergestellt noch angezeigt werden.
- 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.

Die folgenden Einschränkungen gelten für von Logical Volume Manager gemanagte logische Volumes:

- Ein physisches Volume (.vmdk) muss genau einem logischen Volume zugeordnet sein.
- Es werden ausschließlich ext2- und ext3-Formatierungen unterstützt.

Anmeldeoptionen

Es gibt zwei Möglichkeiten, um sich beim Wiederherstellungsclient von vSphere Data Protection anzumelden:

Der Service für die Recovery auf Dateiebene ist nur für die virtuellen Maschinen verfügbar, deren Backups von vSphere Data Protection gemanagt werden. Dies bedeutet, dass Sie entweder über die vCenter-Konsole oder eine andere Remote-Verbindung bei einer der von vSphere Data Protection gesicherten virtuellen Maschinen angemeldet sein müssen, um sich beim Wiederherstellungsclient anmelden zu können.

Standardanmeldung

Bei der Standardanmeldung müssen Sie zunächst über eine mit vSphere Data Protection gesicherte virtuelle Maschine eine Verbindung zum Wiederherstellungsclient herstellen. Melden Sie sich beim Wiederherstellungsclient mit den lokalen Administrator-Anmeldedaten der virtuellen Maschine an, bei der Sie angemeldet sind. Der Wiederherstellungsclient zeigt nur Backups für die virtuelle Maschine an, bei der Sie angemeldet sind, und alle Wiederherstellungsdateien werden auf der virtuellen Maschine wiederhergestellt, bei der Sie angemeldet sind.

Erweiterte Anmeldung

Bei der erweiterten Anmeldung müssen Sie zunächst über eine mit vSphere Data Protection gesicherte virtuelle Maschine eine Verbindung zum Wiederherstellungsclient herstellen. Melden Sie sich beim Wiederherstellungsclient mit den lokalen Administrator-Anmeldedaten der virtuellen Maschine, bei der Sie angemeldet sind, sowie mit den Administrator-Anmeldedaten für vCenter Server an. Nachdem eine Verbindung zum Wiederherstellungsclient hergestellt wurde, ist es möglich, Dateien von einer beliebigen mit vSphere Data Protection gesicherten virtuellen Maschine aus zu mounten, zu durchsuchen und wiederherzustellen. Alle Wiederherstellungsdateien werden auf der virtuellen Maschine wiederhergestellt, bei der Sie derzeit angemeldet sind.

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

Vor einem vSphere Data Protection-Backup muss auf der virtuellen Maschine VMware Tools installiert werden. (Auf der VMware-Website ist eine Liste der Betriebssysteme mit VMware Tools-Unterstützung verfügbar.)

Die folgenden Laufwerkstypen werden vom Wiederherstellungsclient unterstützt:

- Windows (Basislaufwerk, nicht erweitert): NTFS
- Linux (Basislaufwerk, nicht erweitert): LVM, Ext2, Ext3

Verfahren

1 Greifen Sie auf den mit vSphere Data Protection gesicherten lokalen Host mit Remote Desktop oder vSphere Web Client zu.

2 Greifen Sie über folgenden Link auf den Wiederherstellungsclient für vSphere Data Protection zu:

https://<*IP_Adresse_der _VDP_Appliance*>:8543/flr

3 Geben Sie auf der Seite „Anmeldedaten“ unter „Lokale Anmeldedaten“ den **Benutzernamen** und das **Passwort** für den lokalen Host an, und klicken Sie auf **Anmelden**.

4 Das Dialogfeld „Gemountete Backups managen“ wird angezeigt. Darin werden alle Wiederherstellungspunkte zum Client, auf den Sie zugreifen, aufgelistet. Wählen Sie den Mount-Punkt aus, der wiederhergestellt wird, und klicken Sie auf **Mounten**.

5 Nach Abschluss des Mount-Vorgangs wird das Laufwerksymbol als grünes Netzlaufwerk angezeigt.

6 Klicken Sie auf **Schließen**.

7 Navigieren Sie im Fenster „Gemountete Backups“ zu den wiederherzustellenden Ordnern und Dateien, und wählen Sie diese aus.

8 Klicken Sie auf **Ausgewählte Dateien wiederherstellen ...**.

9 Navigieren Sie im Dialogfeld „Ziel auswählen“ zum Laufwerk und Zielordner für die Recovery, und wählen Sie diese aus.

10 Klicken Sie auf **Wiederherstellen**.

11 Das Bestätigungsdialogfeld „Wiederherstellung initiieren?“ wird angezeigt. Klicken Sie auf **Ja**.

12 Ein Dialogfeld zur erfolgreichen Wiederherstellung wird angezeigt. Klicken Sie auf **OK**.

13 Klicken Sie auf die Registerkarte **Wiederherstellungen überwachen**, um den Wiederherstellungsstatus anzuzeigen.

14 Vergewissern Sie sich, dass als Jobstatus „Abgeschlossen“ angegeben ist.

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 Dateiebene auf eine virtuelle Maschine eines vCenter Server-Rechners mit Wiederherstellungspunkten zuzugreifen.

Voraussetzungen

Vor dem Backup muss auf der virtuellen Maschine VMware Tools installiert werden. (Auf der VMware-Website ist eine Liste der Betriebssysteme mit VMware Tools-Unterstützung verfügbar.)

Die folgenden Laufwerkstypen werden vom Wiederherstellungsclient unterstützt:

- Windows (Basislaufwerk, nicht erweitert): NTFS
- Linux (Basislaufwerk, nicht erweitert): LVM, Ext2, Ext3

Verfahren

1 Greifen Sie mit Remote Desktop oder vSphere Web Client auf eine virtuelle Maschine zu.

2 Greifen Sie über folgenden Link auf den Wiederherstellungsclient für vSphere Data Protection zu:

https://<*IP_Adresse_der _VDP_Appliance*>:8543/flr

3 Geben Sie auf der Seite „Anmeldedaten“ unter „Lokale Anmeldedaten“ den **Benutzernamen** und das **Passwort** für den lokalen Host an. Geben Sie unter „vCenter-Anmeldedaten“ den **Benutzernamen** und das **Passwort** des vCenter-Administrators an, und klicken Sie auf **Anmelden**.

4 Das Dialogfeld „Gemountete Backups managen“ wird angezeigt. Darin werden alle Wiederherstellungspunkte zum Client, auf den Sie zugreifen, aufgelistet. Wählen Sie den Mount-Punkt aus, der wiederhergestellt wird, und klicken Sie auf **Mounten**.

5 Nach Abschluss des Mount-Vorgangs wird das Laufwerksymbol als grünes Netzlaufwerk angezeigt.

6 Klicken Sie auf **Schließen**.

7 Navigieren Sie im Fenster „Gemountete Backups“ zu der virtuellen Maschine, den Ordnern und Dateien für die Recovery, und wählen Sie diese aus.

8 Klicken Sie auf **Ausgewählte Dateien wiederherstellen ...**.

9 Navigieren Sie im Dialogfeld „Ziel auswählen“ zum Laufwerk und Zielordner für die Recovery, und wählen Sie diese aus.

10 Klicken Sie auf **Wiederherstellen**.

11 Das Bestätigungsdialogfeld „Wiederherstellung initiieren?“ wird angezeigt. Klicken Sie auf **Ja**.

12 Ein Dialogfeld zur erfolgreichen Wiederherstellung wird angezeigt. Klicken Sie auf **OK**.

Sie können feststellen, ob die Wiederherstellung abgeschlossen wurde, indem Sie auf die Registerkarte **Wiederherstellungen überwachen** klicken und den Wiederherstellungsstatus anzeigen.

Verfahren zum Herunterfahren und Starten von vSphere Data Protection

Wenn Sie die vSphere Data Protection Appliance herunterfahren müssen, verwenden Sie hierzu die Aktion **Gastbetriebssystem herunterfahren**. Bei dieser Aktion wird die Appliance automatisch ordnungsgemäß heruntergefahren. Wenn die Appliance ohne die Aktion „Gastbetriebssystem herunterfahren“ heruntergefahren wird, sind Beschädigungen möglich. Nach dem Herunterfahren einer Appliance lässt sich diese durch die Aktion **Einschalten** 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 Backup-Jobs 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 „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38.

WICHTIGER HINWEIS Die vSphere Data Protection Appliance ist auf einen Betrieb an sieben Tagen die Woche rund um die Uhr ausgelegt, um so Wartungsvorgänge zu unterstützen und für Wiederherstellungsvorgänge verfügbar zu sein. Sie sollte nicht heruntergefahren werden, es sei denn, es besteht hierfür ein bestimmter Grund.

Kapazitätsmanagement mit vSphere Data Protection

4

In diesem Kapitel liegt der Schwerpunkt auf dem Kapazitätsmanagement mit vSphere Data Protection. Dabei werden die folgenden Themen behandelt:

- „Auswirkung durch die Auswahl von Thin- oder Thick-Provisioning-Festplatten“ auf Seite 44
- „Auswirkung der Speicherkapazität auf die erste vSphere Data Protection-Bereitstellung“ auf Seite 45
- „Überwachen der vSphere Data Protection-Kapazität“ auf Seite 45
- „Kapazitätsschwellwerte von vSphere Data Protection“ auf Seite 45
- „Kapazitätsmanagement“ auf Seite 45

Auswirkung durch die Auswahl von Thin- oder Thick-Provisioning-Festplatten

Mit der Auswahl von Partitionen mit Thin- oder Thick-Provisioning-Festplatten für den vSphere Data Protection-Datenspeicher sind Vorteile und Nachteile verbunden.

Thin Provisioning nutzt Virtualisierungstechnologie, die es ermöglicht, mehr Festplattenressourcen als möglicherweise physisch verfügbar darzustellen. Dies kann verwendet werden, wenn ein Administrator aktiv den Festplattenspeicher überwacht und beim Wachstum der Thin-Provisioning-Festplatten zusätzlichen physischen Laufwerkspeicher zuweisen kann. Ohne Management und bei vSphere Data Protection-Datenspeicher, der sich auf einer Thin-Provisioning-Festplatte befindet, die keinen Speicherplatz zuweisen kann, schlägt die vSphere Data Protection Appliance fehl. In einem solchen Fall können Sie ein Rollback auf einen validierten Kontrollpunkt durchführen (zusätzliche Informationen unter „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38). Alle nach dem Kontrollpunkt auftretenden Backups gehen verloren.

Beim Thick Provisioning wird während der Festplattenerstellung sämtlicher erforderlicher Speicher zugewiesen. Best Practice für den vSphere Data Protection-Datenspeicher ist das Erstellen einer Thin-Provisioning-Festplatte, wenn die vSphere Data Protection Appliance bereitgestellt wird (dies sorgt für eine schnelle Bereitstellung). Nach der Bereitstellung wird die Festplatte dann von Thin Provisioning zu Thick Provisioning konvertiert.

Das folgende Verfahren kommt bei einer Konvertierung von Thin zu Thick Provisioning zum Einsatz. Es setzt voraus, dass die vSphere Data Protection Appliance heruntergefahren wird, was u. U. mehrere Stunden dauert.

Voraussetzungen

Die vSphere Data Protection Appliance muss mit Thin Provisioning installiert werden. Es muss ausreichend Festplattenspeicher vorhanden sein, um die Festplatte auf Thick Provisioning zu erweitern.

Verfahren

1. Klicken Sie in vSphere Client mit der rechten Maustaste auf die vSphere Data Protection Appliance, und wählen Sie **Gastbetriebssystem herunterfahren** aus.
2. Markieren Sie die Appliance, und wählen Sie die Registerkarte **Zusammenfassung** aus. Klicken Sie im Abschnitt **Speicher** auf den Datenspeicher, und wählen Sie **Datenspeicher durchsuchen ...** aus.
3. Wählen Sie im Bildschirm „Datenspeicher-Browser“ Ihre Appliance aus, und blenden Sie den damit verbundenen Datenspeicher ein.
4. Klicken Sie auf eine .vmdk-Datei, und wählen Sie **Erweitern** aus.
5. Wiederholen Sie diesen Schritt für alle .vmdk-Dateien.
   - Für VDP mit 0,5 TB gibt es 3 .vmdk-Dateien.
   - Für VDP mit 1 TB gibt es 7 .vmdk-Dateien.
   - Für VDP mit 2 TB gibt es 13 .vmdk-Dateien.

Auswirkung der Speicherkapazität auf die erste vSphere Data Protection-Bereitstellung

Beim Bereitstellen einer neuen vSphere Data Protection Appliance wird die Appliance normalerweise in den ersten Wochen schnell aufgefüllt. Dies ist darauf zurückzuführen, dass fast jeder gesicherte Client einmalig vorkommende Daten umfasst. Die vSphere Data Protection-Deduplizierung lässt sich am besten 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. Im Anschluss an die ersten Backups und bei Überschreitung der maximalen Aufbewahrungsfristen kann überlegt und gemessen werden, ob das System täglich genauso viele neue Daten speichern kann, wie es während der Wartungsfenster freigibt.

Dies wird als Erreichen einer stabilen Kapazitätsauslastung bezeichnet. Eine stabile Kapazität sollte idealerweise bei 80 % liegen.

Überwachen der vSphere Data Protection-Kapazität

Die vSphere Data Protection-Kapazität sollte proaktiv überwacht werden. Die vSphere Data Protection-Kapazität kann auf der vSphere Data Protection-Registerkarte „Berichte“ über den Eintrag „Genutzte Kapazität“ angezeigt werden.

Kapazitätsschwellwerte von vSphere Data Protection

In der folgenden Tabelle wird das vSphere Data Protection-Verhalten in Bezug auf wichtige Kapazitätsschwellwerte beschrieben:

Tabelle 4-1. Kapazitätsschwellwerte von vSphere Data Protection

Schwellwert	Wert	Verhalten
Kapazitätswarnung	80 %	vSphere Data Protection gibt ein Warnereignis aus.
Grenzwert für Integritätsprüfung	95 %	Der Abschluss vorhandener Backups wird zugelassen, neue Backup-Vorgänge werden jedoch unterbrochen. vSphere Data Protection gibt Warnereignisse aus.
Serverbeschränkung durch Schreibschutz	100 %	vSphere Data Protection wechselt in den schreibgeschützten Modus; es sind keine neuen Daten erlaubt.

Kapazitätsmanagement

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

- Fügen Sie keine neuen virtuellen Maschinen als Backup-Clients hinzu.
- Löschen Sie nicht benötigte Backup-Jobs.
- Führen Sie eine Neubewertung der Aufbewahrungs-Policies durch, um festzustellen, ob Aufbewahrungs-Policies entschärft werden können.
- Erwägen Sie die Aufnahme zusätzlicher vSphere Data Protection Appliances, und verteilen Sie Backup-Jobs gleichmäßig auf mehrere Appliances.

vSphere Data Protection-Troubleshooting

5

In diesem Kapitel werden folgende Troubleshooting-Themen behandelt:

- „Installation der vSphere Data Protection Appliance“ auf Seite 48
- „vSphere Data Protection-Backups“ auf Seite 48
- „vSphere Data Protection-Wiederherstellungen“ auf Seite 49
- „Recovery auf Dateiebene“ auf Seite 50
- „vSphere Data Protection-Reporting“ auf Seite 50

Installation der vSphere Data Protection Appliance

Gehen Sie bei Problemen im Zusammenhang mit der Installation der vSphere Data Protection Appliance wie folgt vor:

- Vergewissern Sie sich, dass sämtliche Software die minimalen Softwareanforderungen erfüllt (siehe „Softwareanforderungen“ auf Seite 12).
- Vergewissern Sie sich, dass sämtliche Hardware die minimalen Hardwareanforderungen erfüllt (siehe „Systemanforderungen“ auf Seite 13).
- Vergewissern Sie sich, dass die DNS-Konfiguration für die vSphere Data Protection Appliance ordnungsgemäß durchgeführt wurde. (siehe „Konfiguration vor der Installation“ auf Seite 14).

vSphere Data Protection-Backups

In Verbindung mit vSphere Data Protection-Backups bestehen folgende bekannte Probleme.

„Backup-Jobdaten werden geladen“

Diese Meldung kann über längere Zeit (bis zu fünf Minuten) angezeigt werden, wenn eine große Anzahl virtueller Maschinen (~100 virtuelle Maschinen) für einen einzigen Backup-Job ausgewählt wird. Dieses Problem kann auch bei Aktionen zum Sperren/Entsperren, Aktualisieren oder Löschen für große Jobs auftreten. 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 Backup-Jobs {Backup-Jobname} nicht der VDP-Appliance hinzugefügt werden.“

Dieser Fehler kann auftreten, wenn ein doppelter Clientname im vApp-Container bzw. auf dem ESX-/ESXi-Host vorhanden ist. In diesem Fall wird nur ein Backup-Job 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 Maschine(n) während der Bearbeitung eines Backup-Jobs nicht möglich ist. Dies ist ein bekanntes Problem.

Das Backup virtueller Windows 2008 R2-Maschinen kann fehlgeschlagen, wenn „disk.EnableUUID“ mit „true“ konfiguriert ist.

Windows 2008 R2-Backups können fehlschlagen, wenn auf der virtuellen Maschine der Parameter *disk.EnableUUID* mit *true* konfiguriert ist. Um dieses Problem zu beheben, können Sie den vmx-Konfigurationsparameter *disk.EnableUUID* aktualisieren und manuell auf *false* setzen.

So konfigurieren Sie *disk.EnableUUID* mithilfe von vSphere Web Client mit dem Wert *false*:

1. Fahren Sie die virtuelle Maschine herunter, indem Sie mit der rechten Maustaste auf die virtuelle Maschine klicken und die Option **Gastbetriebssystem herunterfahren** wählen.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, und wählen Sie **Einstellungen bearbeiten** aus.
3. Klicken Sie auf **VM-Optionen**.
4. Blenden Sie den Abschnitt **Erweitert** ein, und klicken Sie auf **Konfiguration bearbeiten**.
5. Navigieren Sie zu dem Namen *disk.EnableUUId*, und setzten Sie den Wert auf *false*.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **OK**.

8 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, und wählen Sie **Einschalten** aus.

Nach dem Update des Konfigurationsparameters sollten Backups der virtuellen Windows 2008 R2-Maschinen erfolgreich durchgeführt werden können.

Backup schlägt fehl, wenn vSphere Data Protection nicht über ausreichend vSphere Data Protection-Datenspeicherkapazität verfügt.

Geplante Backups schlagen bei zu 92 % abgeschlossenem Vorgang fehl, wenn die vSphere Data Protection-Datenspeicherkapazität nicht ausreicht. Wenn der vSphere Data Protection-Datenspeicher mit Thin Provisioning konfiguriert ist und die maximale Kapazität nicht erreicht wurde, fügen Sie zusätzliche Speicherressourcen hinzu. Wenn der vSphere Data Protection-Datenspeicher mit Thick Provisioning konfiguriert ist und die maximale Kapazität erreicht hat, finden Sie unter „Kapazitätsmanagement mit vSphere Data Protection“ auf Seite 43 weitere Informationen.

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. vSphere Data Protection unterstützt nicht das Backup von virtuellen Maschinen mit aktivierter VMware Fault Tolerance.

Wenn virtuelle Maschinen in oder aus verschiedenen Clustergruppen verschoben werden, gehen damit verknüpfte Backup-Quellen 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 Backup-Jobs, die Container schützen, oder erstellen Sie diese neu.

Nach einem unerwarteten Herunterfahren-Vorgang gehen aktuelle Backup-Jobs und Backups verloren.

Bei jedem unerwarteten Herunterfahren nutzt die vSphere Data Protection Appliance ein Rollback auf den zuletzt validierten Kontrollpunkt. Hierbei handelt es sich um erwartetes Verhalten. Zusätzliche Informationen finden Sie unter „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38.

vSphere Data Protection-Wiederherstellungen

In Verbindung mit vSphere Data Protection-Wiederherstellungen bestehen folgende bekannte Probleme.

Registerkarte „Wiederherstellen“ mit der Meldung „Backups werden geladen“ und langem Ladevorgang

Das Laden der Backups auf der Registerkarte „Wiederherstellen“ dauert normalerweise zwei Sekunden pro VM-Backup. Hierbei handelt es sich um erwartetes Verhalten.

Wiederherstellung am ursprünglichen Speicherort schlägt fehl, wenn VM über verknüpfte Snapshots verfügt.

Wenn eine virtuelle Maschine über verknüpfte Snapshots verfügt, schlägt die Wiederherstellung am ursprünglichen Speicherort möglicherweise fehl. Hierbei handelt es sich um erwartetes Verhalten. vSphere Data Protection Support unterstützt nicht die Wiederherstellung von virtuellen Maschinen, die über Snapshots zum ursprünglichen Standort verfügen. Stellen Sie die virtuelle Maschine an einem alternativen Standort wieder her, oder löschen Sie die Snapshots vor der Wiederherstellung zum ursprünglichen Standort.

Recovery auf Dateiebene

In Bezug auf die Recovery auf Dateiebene bestehen im Zusammenhang mit dem vSphere Data Protection-Wiederherstellungsclient folgende bekannte Probleme.

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
- FAT32
- erweiterte Partitionen
- dynamische Festplatten
- GPT-Festplatten
- Ext4 fs
- verschlüsselte Partitionen
- komprimierte Partitionen

Führen Sie eine Wiederherstellung auf Dateiebene durch, und kopieren Sie die erforderlichen Dateien manuell.

Symbolische Links werden im Wiederherstellungsclient nicht angezeigt.

Der Wiederherstellungsclient unterstützt nicht die Anzeige symbolischer Links.

vSphere Data Protection-Reporting

In Verbindung mit vSphere Data Protection-Reporting bestehen folgende bekannte Probleme.

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.

Von vSphere Data Protection verwendete Ports

6

vSphere Data Protection verwendet die in der folgenden Tabelle aufgeführten Ports.

Tabelle 6-1. Von vSphere Data Protection verwendete Ports

Port	Protokoll(e)	Verbundener Service
22	TCP	ssh
80	TCP	http
111	TCP	rpcbind
443	TCP	https
700	TCP	Loginmgr tool
5555	TCP	Postgres
5558	TCP	Postgres
7778	TCP	VDP RMI
7779	TCP	VDP RMI
8509	TCP	Tomcat AJP Connector
8543	TCP	Redirect for Tomcat
8580	TCP	VDP Downloader
9443	TCP	VDP Web Services
25000	TCP/UDP	VDP Internal Communications
26000	TCP/UDP	VDP Internal Communication
27000	TCP	VDP Client Server Communications
28001	TCP	VDP Internal Proxy
28002	TCP	VDP Internal Proxy
28003	TCP	VDP Internal Proxy
28004	TCP	VDP Internal Proxy
28005	TCP	VDP Internal Proxy
28006	TCP	VDP Internal Proxy
28007	TCP	VDP Internal Proxy
28008	TCP	VDP Internal Proxy
28009	TCP	VDP Internal Proxy
29000	TCP	VDP internal client secure communications
34250	TCP	ssl/soap gSoap (localhost)
53	UDP	DNS

Tabelle 6-1. Von vSphere Data Protection verwendete Ports

Port	Protokoll(e)	Verbundener Service
111	UDP	RPC
941	UDP	RPC

Disaster Recovery von vSphere Data Protection 7

vSphere Data Protection verfügt über robuste Speicher- und Managementfunktionen für Backups. Bei einem Ausfall sollte als erste Maßnahme ein Rollback auf einen bekannten validierten Kontrollpunkt durchgeführt werden (siehe „Verwenden von Kontrollpunkten und Rollback“ auf Seite 38). Zur Wiederherstellung nach einem vSphere Data Protection Appliance-Ausfall werden anhand des folgenden Verfahrens Backups der Appliance und aller verknüpften vSphere Data Protection Backups für die Disaster Recovery erstellt.

Im Folgenden finden Sie Richtlinien für die Disaster Recovery von vSphere Data Protection:

1 Vergewissern Sie sich vor dem Herunterfahren der vSphere Data Protection Appliance, dass keine Backup- oder Wartungsaufgaben durchgeführt werden. Planen Sie abhängig von der verwendeten Backup-Methode und der Backup-Dauer Ihren vSphere Data Protection-Backup-Vorgang so, dass er zu einer Zeit ohne geplante Aufgaben stattfindet. Wenn Ihr Backup-Zeitfenster beispielsweise acht Stunden umfasst und Backups bereits nach einer Stunde abgeschlossen sind, stehen Ihnen vor der Durchführung geplanter Wartungsaufgaben zusätzlich sieben Stunden zur Verfügung. Dies ist ein idealer Zeitpunkt, um die Appliance herunterzufahren und zu sichern. Zusätzliche Informationen finden Sie unter „Konfiguration des Backup-Zeitfensters“ auf Seite 34.

2 Navigieren Sie in vSphere Client zur Appliance. Führen Sie die Option „Gastbetriebssystem herunterfahren“ auf der virtuellen Maschine aus. Verwenden Sie nicht „Ausschalten“. Eine Aufgabe „Ausschalten“ ist mit dem Ziehen eines Steckers am physischen Server gleichbedeutend und kann zu einem nicht ordnungsgemäßen Herunterfahren-Vorgang führen. Weitere Informationen finden Sie unter „Verfahren zum Herunterfahren und Starten von vSphere Data Protection“ auf Seite 42.

3 Sobald Sie bestätigt haben, dass die Appliance heruntergefahren wurde, fahren Sie mit der von Ihnen bevorzugten Data-Protection-Methode fort.

4 Überprüfen Sie, ob vSphere Data Protection vollständig gesichert wurde, und vergewissern Sie sich, dass keine Backup-/Snapshot-/Kopierjobs gegen vSphere Data Protection durchgeführt werden.

5 Führen Sie über vSphere Client die Option „Einschalten“ für die Appliance aus.

Index

A

Appliance Snapshot erstellen **21**
Aufbewahrungs-Policy **30**
Ausfallzeitfenster **35**

B

Backup, Registerkarte **27**
Backup-Job-Assistent **30**
Backup-Jobs **29**
Backup-Planung **30**
Backups auf Image-Ebene **8**
Backup-Zeitfenster **34**
Berichte, Registerkarte **33**

C

Changed Block Tracking (CBT) **8**

D

Datensegment fester Länge **9**
Datensegment variabler Länge **9**
Datenspeicher **8**
Deduplizierungsspeicher **9**
DNS-Konfiguration **14**

E

E-Mail-Benachrichtigung **37**

F

Filter, Option **33**

I

Integritätsprüfungen **35**

J

Jetzt sichern **31**

K

Konfiguration, Registerkarte **34**
Kontrollpunkt **38**

O

OVF-Vorlagendatei **15**

P

Plattformprodukt-Support **8**

R

Recovery auf Dateiebene **9**, **39**
Recovery auf Dateiebene, erweiterte Anmeldung **40**
Recovery auf Dateiebene, Standardanmeldung **40**
Registerkarte „Erste Schritte“ **26**
Rollback **38**
Rückkehr zu einem Snapshot **23**

S

Snapshot
- entfernen **23**
- erstellen **21**
- Rückkehr zu **23**

Sperrung eines Backup-Jobs **33**
stabile Kapazität **45**
Systemanforderungen **13**

T

technischer Support, Ressourcen **5**

U

Unternehmensdaten **9**

V

vCenter-Registrierung **19**
VDP-configure, Dienstprogramm **17**
Virtual Machine Disk (VMDK) **8**
VMware vStorage APIs for Data Protection (VADP) **8**
vSphere Data Protection Appliance **10**
vSphere Data Protection Appliance, Definition **8**
vSphere Data Protection Appliance, Details **34**
vSphere Data Protection Appliance, Herunterfahren und Starten **42**
vSphere Data Protection, Architektur **10**
vSphere Data Protection, Dimensionierung **12**
vSphere Data Protection, Disaster Recovery **53**
vSphere Data Protection, Installation **16**
vSphere Data Protection, Konfiguration **19**
vSphere Data Protection, Passwort **20**
vSphere Data Protection, Speicherkapazität **45**
vSphere Data Protection, Spezifikationen **13**
vSphere Data Protection, Thick-Provisioning-Festplatten **44**
vSphere Data Protection, Thin-Provisioning-Festplatten **44**
vSphere Data Protection., Systemeinstellungen **20**

W

Wartungsfenster **35**
Wiederherstellungsassistent **31**
Wiederherstellungsclient **39**