

Administratorhandbuch für VMware Data Recovery

Data Recovery 1.1

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter <http://www.vmware.com/de/support/pubs>.

DE-000193-00

vmware[®]

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

<http://www.vmware.com/de/support/pubs/>

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2009 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter <http://www.vmware.com/go/patents-de> aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Über dieses Handbuch	5
1 Grundlegendes zu VMware Data Recovery	7
Sichern von virtuellen Maschinen	7
Volume Shadow Copy Service (VSS)	8
Vorteile des Deduplizierungsspeichers	10
2 Installieren von VMware Data Recovery	11
VMware Data Recovery - Systemanforderungen	11
Installieren des Client-Plug-Ins	14
Installieren der Backup-Appliance	14
Hinzufügen einer Festplatte zur Backup-Appliance	15
3 Verwenden von VMware Data Recovery	17
Einschalten der Backup-Appliance	17
Konfigurieren der Backup-Appliance	18
Verwenden des Assistenten für erste Schritte	18
Verwenden von Sicherungsaufgaben	19
Wiederherstellen von virtuellen Maschinen	22
Grundlegendes zu File Level Restore (Wiederherstellen auf Dateiebene)	25
Fehlerbehebung für VMware Data Recovery	28
Index	35

Über dieses Handbuch

Im *Administratorhandbuch für VMware Data Recovery* finden Sie Informationen zum Einrichten von Sicherungslösungen für kleine und mittlere Unternehmen.

Zielgruppe

Zielgruppe dieses Handbuchs sind alle Personen, die mithilfe von VMware Data Recovery Sicherungslösungen bereitstellen möchten. Die Informationen in diesem Handbuch sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der VM-Technologie und Datencenteroperationen vertraut sind.

Feedback zu diesem Dokument

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Falls Sie Anmerkungen haben, senden Sie diese bitte an: docfeedback@vmware.com.

Technischer Support und Schulungsressourcen

Ihnen stehen die folgenden Ressourcen für die technische Unterstützung zur Verfügung. Die aktuelle Version dieses Handbuchs sowie weitere Handbücher finden Sie auf folgender Webseite:

<http://www.vmware.com/de/support/pubs>.

Online- und Telefon-Support

Auf der folgenden Webseite können Sie über den Onlinesupport technische Unterstützung anfordern, Ihre Produkt- und Vertragsdaten abrufen und Produkte registrieren: <http://www.vmware.com/de/support>.

Kunden mit entsprechenden Support-Verträgen erhalten über den telefonischen Support schnelle Hilfe bei Problemen der Prioritätsstufe 1. Rufen Sie die folgende Webseite auf:

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

Support-Angebote

Informationen zum Support-Angebot von VMware und dazu, wie es Ihre geschäftlichen Anforderungen erfüllen kann, finden Sie unter

<http://www.vmware.com/de/support/services>.

VMware Professional Services

Die VMware Education Services-Kurse umfassen umfangreiche Praxisübungen, Fallbeispiele 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 optimale Vorgehensweise für die Implementierung verfügt VMware Consulting Services über Angebote, die Sie bei der Beurteilung, Planung, Erstellung und Verwaltung Ihrer virtuellen Umgebung unterstützen. Informationen zu Schulungen, Zertifizierungsprogrammen und Consulting-Diensten finden Sie auf der folgenden Webseite: <http://www.vmware.com/de/services>.

Grundlegendes zu VMware Data Recovery

1

VMware® Data Recovery erstellt Sicherungen virtueller Maschinen, ohne deren Betrieb bzw. ohne den Zugriff auf die Daten und Dienste, die sie anbieten, zu unterbrechen. Data Recovery verwaltet vorhandene Sicherungen und entfernt Sicherungen, wenn diese älteren Datums sind. Es unterstützt zudem die Deduplizierung zum Entfernen redundanter Daten.

Data Recovery basiert auf der VMware vStorage API für den Schutz von Daten. Es ist in VMware vCenter Server integriert, was die zentrale Zeitplanung von Sicherungsaufgaben ermöglicht. Die Integration mit vCenter Server ermöglicht außerdem selbst dann die Sicherung virtueller Maschinen, wenn diese unter Verwendung von VMware VMotion™ oder VMware Distributed Resource Scheduler (DRS) verschoben werden.

Data Recovery verwendet zum Verwalten und Wiederherstellen von Sicherungen eine Appliance einer virtuellen Maschine und ein Client-Plug-In. Die Backup-Appliance hat das „Open Virtualization Format“ (OVF). Für das Data Recovery-Plug-In wird der VMware vSphere Client benötigt.

Sicherungen können auf jeder virtuellen Festplatte gespeichert werden, die von VMware ESX™ unterstützt wird. Sie können Storage Area Networks (SAN, Network Attached Storage-Geräte (NAS-Geräte) oder auf Common Internet File System (CIFS) basierenden Speicher, wie z. B. SAMBA, verwenden. Alle gesicherten virtuellen Maschinen werden in einem Deduplizierungsspeicher gespeichert.

VMware Data Recovery unterstützt Volume Shadow Copy Service (VSS), der die Backup-Infrastruktur für bestimmte Windows-Betriebssysteme bereitstellt.

Dieses Kapitel behandelt die folgenden Themen:

- [„Sichern von virtuellen Maschinen“](#), auf Seite 7
- [„Volume Shadow Copy Service \(VSS\)“](#), auf Seite 8
- [„Vorteile des Deduplizierungsspeichers“](#), auf Seite 10

Sichern von virtuellen Maschinen

Bei der Sicherung erstellt Data Recovery einen Snapshot der stillgelegten virtuellen Maschine. Die Deduplizierung wird bei jedem Sicherungsvorgang automatisch durchgeführt.

Data Recovery kann gleichzeitig bis zu acht virtuelle Maschinen sichern. Um mehrere Sicherungen starten zu können, muss die CPU-Nutzung bei weniger als 90 Prozent liegen. Aufgrund von Arbeitsspeichereinschränkungen unterstützt Data Recovery gleichzeitig nicht mehr als zwei Sicherungsziele. Wenn mehr als zwei Sicherungsziele verwendet werden müssen, konfigurieren Sie diese so, dass sie zu unterschiedlichen Zeiten benutzt werden.

Für virtuelle Maschinen, die in vSphere 4.0 erstellt wurden, erstellt die Data Recovery-Appliance während der Sicherung einen Snapshot der stillgelegten virtuellen Maschine. Die Sicherungen wenden die Verfolgungsfunktionalität für geänderte Blöcke auf die ESX-Hosts an. Diese überprüft für jede zu sichernde virtuelle Festplatte die vorherige Sicherung. Anhand der Änderungsverfolgungsfunktionalität der ESX-Hosts werden die Änderungen seit der letzten Sicherung eingeholt. Der von Duplikaten bereinigte Speicher erstellt eine vollständige virtuelle Sicherung auf Basis des letzten Sicherungs-Images und übernimmt darin die Änderungen.

HINWEIS Diese Optimierungen gelten nicht für virtuelle Maschinen, die mit VMware-Produkten vor vSphere 4.0 erstellt wurden. Beispielsweise werden Änderungs-Token nicht für virtuelle Maschinen verwendet, die mit Virtual Infrastructure 3.5 oder früher erstellt wurden. Als Ergebnis dauert das Sichern virtueller Maschinen länger, die mit früheren VMware-Versionen erstellt wurden.

Wenn eine virtuelle Maschine doppelte Teile enthält, werden die doppelten Informationen nur einmal gespeichert. Die Deduplizierung kann für eine bedeutende Platzersparnis sorgen. Es gibt oft viele identische Betriebssystemdateien bei virtuellen Maschinen, die unter demselben Betriebssystem ausgeführt werden. Um die Deduplizierung zu maximieren, sichern Sie ähnliche virtuelle Maschinen in demselben Ziel. Die virtuellen Maschinen müssen nicht mit derselben Aufgabe gesichert werden.

Data Recovery stellt anhand der vSphere-Lizenzierungsinfrastruktur sicher, dass alle virtuellen Maschinen, die durch Data Recovery geschützt sind, über die entsprechende Lizenzierung verfügen. Eine gültige vSphere-Lizenzierung enthält Lizenzen für Essential Plus, Advanced, Enterprise oder Enterprise Plus.

Jede Backup-Appliance zu Data Recovery kann bis zu 100 virtuelle Maschinen schützen. Es ist möglich, Sicherungsaufgaben zu erstellen, die so konfiguriert sind, dass sie mehr als 100 virtuelle Maschinen schützen, aber die Backup-Appliance schützt nur 100 virtuelle Maschinen, was bedeutet, dass die zusätzlichen virtuellen Maschinen ignoriert werden. Durch die Installation zusätzlicher virtueller Maschinen ist es allerdings möglich, mehr als 100 virtuelle Maschinen zu schützen. Allerdings haben die einzelnen Backup-Appliances keinen Zugriff auf die Informationen zu den Sicherungsaufgaben der jeweils anderen Appliances. Dies kann zu unbeabsichtigten Konfigurationen führen. Beispielsweise können zwei Backup-Appliances zu Data Recovery so konfiguriert sein, dass sie einen Ordner mit 200 virtuellen Maschinen schützen, aber es ist sehr wahrscheinlich, dass einige dieser virtuellen Maschinen doppelt und andere gar nicht gesichert werden.

Volume Shadow Copy Service (VSS)

VMware Data Recovery verwendet den Volume Shadow Copy Service (VSS) von Microsoft Windows. Dieser liefert die Backup-Infrastruktur für bestimmte Windows-Betriebssysteme sowie einen Mechanismus zum Erstellen konsistenter Kopien von Daten, die auch als Schattenkopien bezeichnet werden, zu einem bestimmten Zeitpunkt.

VSS erstellt konsistente Schattenkopien, die auf Geschäftsanwendungen, Dateisystemdiensten, Sicherungsanwendungen, Lösungen für schnelle Wiederherstellungen und Speicherhardware abgestimmt sind. VSS-Unterstützung wird durch VMware Tools bereitgestellt, die im Gastbetriebssystem ausgeführt werden. VMware enthält einen VSS Requestor und einen VSS Snapshot Provider (VSP). Die Requester-Komponente befindet sich in einem unterstützten Gastbetriebssystem und reagiert auf Ereignisse einer externen Sicherungsanwendung. Der Requestor steuert außerdem den Fortschritt von Sicherungsvorgängen im Gastbetriebssystem und interagiert mit dem VSP. Der Requestor wird vom VMware Tools-Dienst instanziiert, wenn ein Sicherungsvorgang initialisiert wird. Der VSP wird als Windows-Dienst registriert und benachrichtigt Data Recovery über anbieterspezifische Ereignisse während einer VSS-Sicherung.

VSS wird auf virtuellen Maschinen mit den folgenden Gastbetriebssystemen unterstützt:

- Windows Server 2003, 32-Bit und 64-Bit
- Windows Vista, 32-Bit und 64-Bit
- Windows Server 2008, 32-Bit und 64-Bit

Data Recovery verwendet je nach Gastbetriebssystem, das Sie in Ihren virtuellen Maschinen ausführen, verschiedene Mechanismen zur Stilllegung.

Tabelle 1-1. Von Data Recovery verwendete Mechanismen zur Stilllegung

Gastbetriebssystem	Verwendeter Treiber und Stilllegungstyp
Windows XP 32-Bit	SYNC-Treiber
Windows 2000 32-Bit	Stilllegung mit Dateisystemkonsistenz
Windows 2003 32-Bit/64-Bit	VMware VSS-Komponente Stilllegung mit Anwendungskonsistenz
Windows Vista 32-Bit/64-Bit	VMware VSS-Komponente
Windows 2008 32-Bit/64-Bit	Stilllegung mit Dateisystemkonsistenz
Andere Gastbetriebssysteme	Stilllegung mit Dateisystemkonsistenz

In den meisten Fällen legt der von Data Recovery bereitgestellte Mechanismus zur Stilllegung Anwendungen ordnungsgemäß still. Wenn Ihre Umgebung Anwendungen oder Betriebssysteme umfasst, die nicht wie erwartet auf enthaltene Mechanismen zur Stilllegung reagieren, werden benutzerdefinierte Stilllegungsskripts von Data Recovery unterstützt. Stellen Sie die benutzerdefinierten Stilllegungsskripts in der geschützten virtuellen Maschine bereit und führen Sie sie aus.

Tabelle 1-2. Speicherort der benutzerdefinierten Stilllegungsskripts

Gastbetriebssystem	Skript	Speicherort des Skripts auf der virtuellen Maschine
Windows	Vor dem Einfrieren	C:\Programme\VMware\VMware Tools\backupScripts.d Sämtliche Skripts werden in aufsteigender alphabetischer Reihenfolge aufgerufen. Dabei ist „freeze“ das erste Argument.
	Nach dem Auftauen	C:\Programme\VMware\VMware Tools\backupScripts.d Sämtliche Skripts werden in absteigender alphabetischer Reihenfolge aufgerufen. Dabei ist „thaw“ oder „freeze-Fail“ das erste Argument.
Anderes	Vor dem Einfrieren	/usr/sbin/pre-freeze-script
	Nach dem Auftauen	/usr/sbin/post-thaw-script

Beim Ausführen der Skripts können Sie auch die SYNC-Treiber oder VSS-Komponenten in den virtuellen Maschinen verwenden, die sie unterstützen.

Da Data Recovery VSS verwendet, kann Data Recovery Snapshots erstellen und dabei die Anwendungskonsistenz sicherstellen. Dies bedeutet, dass Anwendungen wichtige Daten, die sich gerade im Arbeitsspeicher befinden, auf die Festplatte schreiben, wodurch sichergestellt wird, dass eine spätere Wiederherstellung dieser virtuellen Maschine die Anwendung in einem konsistenten Status wiederherstellen kann.

Weitere Informationen dazu, welche virtuellen Windows-Maschinen Volume Shadow Copy Service verwenden, finden Sie im „Sicherungshandbuch für virtuelle Maschinen“. Detaillierte Informationen über VSS finden Sie unter <http://technet.microsoft.com/en-us/library/cc785914.aspx>.

Vorteile des Deduplizierungsspeichers

Die von VMware Data Recovery verwendete Deduplizierungsspeichertechnologie wurde von VMware entwickelt und bietet eine nahtlose Integration. Die Deduplizierungstechnologie wertet Muster aus, die in Wiederherstellungspunkten gespeichert werden, und überprüft, ob identische Abschnitte bereits gespeichert wurden.

Da VMware das Speichern der Ergebnisse mehrerer Sicherungsaufgaben unterstützt, wodurch derselbe Deduplizierungsspeicher verwendet werden kann und die Deduplizierungsraten maximiert werden, sollten Sie sicherstellen, dass gleichartige virtuelle Maschinen an demselben Ziel gespeichert werden. Zwar kann das Sichern gleichartiger virtueller Maschinen in demselben Deduplizierungsspeicher zu einer größeren Ersparnis an Speicherplatz führen, allerdings müssen die gleichartigen virtuellen Maschinen nicht mit derselben Aufgabe gesichert werden. Die Deduplizierung wird für alle gespeicherten virtuellen Maschinen ausgewertet, selbst wenn einige zurzeit nicht gesichert sind.

Data Recovery ist für die Unterstützung von Deduplizierungsspeichern von bis zu einem Terabyte Größe und jede Backup-Appliance ist für den Einsatz von zwei Deduplizierungsspeichern ausgelegt. Bei Data Recovery gibt es kein Limit hinsichtlich der Größe oder der Anzahl der Deduplizierungsspeicher, wenn aber mehr als zwei Speicher verwendet werden oder die Größe eines Speichers ein Terabyte überschreitet, kann dies die Leistung beeinträchtigen.

Der Deduplizierungsspeicher führt mehrere Prozesse durch, einschließlich der Integritätsprüfung, Neukatalogisierung und Zurückgewinnung.

Integritätsprüfung

Dieser Vorgang dient dazu, die Datenintegrität im Deduplizierungsspeicher zu überprüfen und zu warten. Der Vorgang wird täglich automatisch ausgeführt, die vollständige Integritätsprüfung jedoch einmal pro Woche. Außerdem kann die Integritätsprüfung auch manuell ausgeführt werden. Normalerweise sind die Sicherungs- und Wiederherstellungsvorgänge vom Deduplizierungsspeicher aus zulässig, während die Integritätsprüfung läuft. Wenn ein Wiederherstellungspunkt manuell zum Löschen markiert ist, sind Sicherungen bei laufender Integritätsprüfung nicht zulässig. Allerdings sind Wiederherstellungsvorgänge erlaubt. Wenn im Deduplizierungsspeicher beschädigte Wiederherstellungspunkte gefunden werden, muss nach dem Markieren der beschädigten Wiederherstellungspunkte zum Löschen eine manuelle Integritätsprüfung durchgeführt werden. Während einer solchen manuellen Integritätsprüfung sind Sicherungen und Wiederherstellungen nicht zulässig.

Neukatalogisierung

Dieser Vorgang dient dazu, sicherzustellen, dass der Katalog mit Wiederherstellungspunkten mit dem Inhalt des Deduplizierungsspeichers synchronisiert wird. Dieser Vorgang wird automatisch ausgeführt, wenn eine Inkonsistenz zwischen dem Katalog und dem Deduplizierungsspeicher erkannt wird. Bei laufender Neukatalogisierung sind keine weiteren Vorgänge im Deduplizierungsspeicher zulässig.

Zurückgewinnung

Dieser Vorgang dient dazu, Speicherplatz im Deduplizierungsspeicher zurückzugewinnen. Dies kann eine Folge davon sein, dass die Data Recovery-Appliance die Aufbewahrungsrichtlinie umsetzt und abgelaufene Wiederherstellungspunkte löscht. Dieser Vorgang wird automatisch täglich ausgeführt, wenn eine Sicherungsaufgabe mehr Speicherplatz benötigt, als auf dem Deduplizierungsspeicher verfügbar ist. Bei laufendem Zurückgewinnungsvorgang sind Sicherungen in den Deduplizierungsspeicher nicht zulässig. Allerdings sind Wiederherstellungsvorgänge aus dem Deduplizierungsspeicher heraus erlaubt.

Installieren von VMware Data Recovery

2

VMware Data Recovery verwendet ein Plug-In zum vSphere-Client und eine Backup-Appliance, um Backups auf Zielen, z. B. Festplatten, zu speichern.

Bevor Sie Data Recovery benutzen können, müssen Sie den Installationsprozess abschließen. Stellen Sie zu Beginn sicher, dass in Ihrer Umgebung die Ressourcen vorhanden sind, die die Systemanforderungen von Data Recovery erfüllen.

Data Recovery besteht aus mehreren Komponenten, die auf verschiedenen Maschinen ausgeführt werden.

- Das Client-Plug-In ist auf einem Computer installiert, der zum Verwalten von Data Recovery dient.
- Die Backup-Appliance ist auf einem ESX-Host installiert.
- Der optionale File Level Restore-Client (FLR-Client) ist in einer virtuellen Windows-Maschine installiert. Weitere Informationen zu FLR finden Sie in „[Grundlegendes zu File Level Restore \(Wiederherstellen auf Dateiebene\)](#)“, auf Seite 25.

Dieses Kapitel behandelt die folgenden Themen:

- „[VMware Data Recovery - Systemanforderungen](#)“, auf Seite 11
- „[Installieren des Client-Plug-Ins](#)“, auf Seite 14
- „[Installieren der Backup-Appliance](#)“, auf Seite 14
- „[Hinzufügen einer Festplatte zur Backup-Appliance](#)“, auf Seite 15

VMware Data Recovery - Systemanforderungen

Stellen Sie vor dem Installieren von VMware Data Recovery sicher, dass in Ihrer Umgebung die System- und Speicheranforderungen erfüllt sind.

Für Data Recovery werden vCenter Server und der vSphere-Client benötigt. Data Recovery funktioniert nicht mit ähnlichen VMware-Produkten, z. B. VirtualCenter Server. Sie können den vSphere-Client von Ihrem vCenter Server herunterladen. Zu sichernde virtuelle Maschinen und die Backup-Appliance müssen auf ESX 4 oder später oder auf ESX 4i oder später ausgeführt werden. Verwenden Sie Data Recovery nicht mit vCenter Servern, die im verknüpften Modus ausgeführt werden.

Sie können Backups auf jeder virtuellen Festplatte speichern, die von ESX unterstützt wird. Sie können Technologien verwenden, wie z. B. SANs (Storage Area Network) und NAS-Geräte (Network Attached Storage). Data Recovery unterstützt auch CIFS-basierten (Common Internet File System) Speicher, wie z. B. SAMBA. CIFS wird zwar unterstützt, ist aber möglicherweise weniger leistungsfähig als VMDKs oder RDMS. Deshalb ist es nicht empfehlenswert, CIFS-Freigaben zu verwenden, für die Folgendes gilt:

- Sie befinden sich auf einem Server, der eine andere Rolle hat, wie z. B. CIFS-Freigaben auf einem vCenter Server.
- Sie sind mit einer virtuellen Maschine verbunden.
- Sie sind für mehrere Dienste oder Server freigegeben.

Weitere Informationen zum Einrichten einer vSphere 4.0-Umgebung einschließlich ESX, ESXi, vCenter Server und des vSphere-Clients finden Sie in der neuesten Dokumentation zu vSphere.

Größe des Deduplizierungsspeichers

Die Menge des benötigten Speichers variiert je nach der Menge an Festplattenspeicher, den die Deduplizierung durch die Ausführung von ähnlichen virtuellen Maschinen sparen kann. Data Recovery kann bis zu zwei Deduplizierungsspeichern für jede Backup-Appliance zugeordnet werden und jeder Deduplizierungsspeicher kann bis zu 1 TB groß sein. Data Recovery ist in der Lage, bis zu 100 virtuelle Maschinen zu schützen, obwohl diese Anzahl je nach Größe und Komplexität der virtuellen Maschinen durch den Festplattenspeicher eingeschränkt wird. Selbst bei Speicherplatzeinsparungen benötigt Data Recovery ein absolutes Minimum an 10 GB freiem Speicherplatz. Dieser Speicherplatz dient zum Indizieren und Verarbeiten von Wiederherstellungspunkten, d. h. selbst wenn die zu sichernden virtuellen Maschinen sehr klein sind, werden sie möglicherweise nicht gesichert, wenn weniger als 10 GB Festplattenspeicher verfügbar ist. Ein Minimum von 10 GB ist zwar akzeptabel, es ist aber äußerst empfehlenswert, mindestens 50 GB zur Nutzung zur Verfügung zu haben. Je verschiedenartiger die Gruppe der zu schützenden virtuellen Maschinen ist, um so mehr Speicherplatz wird für jede virtuelle Maschine benötigt. Die benötigte Menge an Speicherplatz wird auch durch die Häufigkeit von Backups, die Aufbewahrungsdauer der Backups und die Anzahl an zu sichernden virtuellen Maschinen bestimmt.

Stellen Sie anfänglich Speicherplatz bereit, der der Menge an verwendetem Festplattenspeicher aller geschützten virtuellen Maschinen entspricht. Wenn Sie beispielsweise 10 virtuelle Maschinen schützen, jede mit einer 20 GB großen virtuellen Festplatte, und diese virtuellen Festplatten durchschnittlich zu 50 % belegt sind, sollten Sie zumindest 100 GB an verfügbarem Speicher für den Deduplizierungsspeicher bereitstellen. Mit der Zeit erreicht die vom Deduplizierungsspeicher verwendete Speicherplatzmenge ein Gleichgewicht, da die aktualisierten Daten in etwa den älteren Wiederherstellungspunkten entsprechen, die von der Aufbewahrungsrichtlinie entfernt werden.

Formate des Deduplizierungsspeichers

Deduplizierungsspeicher können auf virtuellen Thin-Provisioning- oder Thick-Provisioning-Festplatten gespeichert werden. Die Verwendung von Thin-Provisioning kann zu geringerer Leistung führen, da in diesem Fall Speicherplatz bei Bedarf zugeteilt wird. Deshalb sind Thick-Provisioning-Festplatten besser geeignet, um potenzielle Leistungseinbußen zu verhindern, wie sie beim Vergrößern von Thin-Provisioning-Festplatten auftreten. Wenn der verfügbare Speicherplatz auf einer Thick-Provisioning-Festplatte erschöpft ist, können Sie die Festplatte mit dem vSphere-Client erweitern.

Deduplizierungsspeicher können in allen HCL-unterstützten Speicher- und CIFS-basierten Netzwerkfreigaben gespeichert werden. Zudem sind sie mit deduplizierungsfähigem Speicher kompatibel. Obwohl jedes beliebige unterstützte Format verwendet werden kann, werden virtuelle Festplatten (VMDKs) oder RDMS als Deduplizierungsspeicher empfohlen, da sie die am besten nachvollziehbare und konsistenteste Leistung bieten. CIFS-Freigaben werden ebenfalls unterstützt. Aber die Leistung dieser Freigaben variiert je nach Anbieter und sind schlichtweg eine weniger ideale Lösung. Zudem bieten virtuelle Festplatten und RDMS in vielen Fällen eine bessere Leistung als netzwerkbasierende Deduplizierungsspeicher. Deduplizierungsspeicher kön-

nen in RDM entweder mit virtueller oder physischer Kompatibilität gespeichert werden. Wenn Sie beabsichtigen, den Deduplizierungsspeicher auf Band zu speichern, indem Sie Snapshots erstellen, sollten Sie ein RDM mit virtueller Kompatibilität verwenden. Snapshots können mit RDM mit physischer Kompatibilität erstellt werden.

Obwohl CIFS verwendet werden kann, verwenden Sie keine CIFS-Freigaben, für die Folgendes gilt:

- Sie befinden sich auf einem Server, der eine andere Rolle hat. Verwenden Sie beispielsweise keine CIFS-Freigaben, die sich auf einem vCenter Server befinden.
- Sie sind mit einer virtuellen Maschine verbunden.
- Sie sind für mehrere Dienste oder Server freigegeben.

HINWEIS Striping führt zu einem Verlust an Speicherplatzeffizienz in den Deduplizierungsspeichern. Wenn virtuelle Maschinen in separaten Deduplizierungsspeichern geschützt werden, bietet dies bessere Ergebnisse als das Striping zum Kombinieren von Festplatten zum Erstellen eines großen Deduplizierungsspeichers.

Besondere Überlegungen zur Data Recovery-Kompatibilität

Sie sollten bestimmte Aspekte beachten, wenn Sie Data Recovery in Ihrer Umgebung einrichten. Data Recovery unterstützt Folgendes nicht:

- vCenter Server im verknüpften Modus.
- IPv6-Adressen. IPv4-Adressen werden für die Data Recovery-Appliance benötigt.
- NFS wird nur dann unterstützt, wenn die Freigabe von einem ESX Server bereitgestellt wird und der Data Recovery-Appliance die VMDK zugewiesen ist.
- Das Hinzufügen von Festplatten im laufenden Betrieb mit vSphere-Versionen, die für das Hinzufügen im laufenden Betrieb nicht lizenziert sind.
- Das Wiederherstellen von verknüpften Klonen. Data Recovery kann Linked Clones sichern. Diese werden als nicht verlinkte Clones wiederhergestellt.
- Das Sichern virtueller Maschinen, die durch die VMware-Fehlertoleranz geschützt werden.
- Das Sichern virtueller Maschinen, die das Festplattenformat von VMware Workstation verwenden.
- Das Sichern virtueller Maschinen mit aktiviertem Multipathing von Drittanbietern.
- Festplatten mit Raw Device Mapping (RDM) im physischen Kompatibilitätsmodus.

Data Recovery wurde getestet zur Verwendung mit:

- Einer Backup-Appliance für jede vCenter-Instanz.
- Jeder Backup-Appliance, die bis zu 100 virtuelle Maschinen schützen.
- VMDK- oder CIFS-basierendem Deduplizierungsspeicher mit bis zu 1 TB.
- Bis zu zwei Deduplizierungsspeichern pro Backup-Appliance.

Installieren des Client-Plug-Ins

Installieren Sie das Client-Plug-In auf einem Computer, der zum Verwalten von Data Recovery verwendet wird. Sie müssen den Client installieren, bevor Sie VMware Data Recovery verwalten können.

Voraussetzungen

Bevor Sie das Data Recovery-Plug-In installieren können, muss vCenter Server in Ihrer Umgebung ausgeführt werden und Sie müssen den vSphere-Client installieren, den Sie von einem vCenter Server herunterladen können. Das Data Recovery-Plug-In stellt über Port 22024 eine Verbindung zur Backup-Appliance her. Wenn sich zwischen dem Client und der Backup-Appliance eine Firewall befindet, muss Port 22024 offen sein, bevor Data Recovery mit dem vSphere-Client verwaltet werden kann.

Mit dem Client-Plug-In können nur Backup-Appliances derselben Version verwaltet werden. Stellen Sie sicher, dass Sie über die korrekte Version des Plug-Ins für die Appliance verfügen, die Sie verwalten.

Vorgehensweise

- 1 Legen Sie die Data Recovery-Installations-CD ein.
Das VMware Data Recovery-Installationsfenster wird angezeigt.
- 2 Klicken Sie auf **[Data Recovery Client-Plug-In]**.
- 3 Befolgen Sie die Anweisungen des Installationassistenten.
- 4 Starten Sie den vSphere-Client und melden Sie sich bei einem vCenter Server an.
- 5 Wählen Sie **[Plug-Ins]** > **[Plug-Ins verwalten]** und stellen Sie sicher, dass das Data Recovery-Plug-In aktiviert ist.

Sie können das Client-Plug-In nun zum Verwalten von Data Recovery verwenden. Falls Data Recovery nicht im vSphere-Client registriert ist, starten Sie den Client neu.

Weiter

Sie können nun mit der Aufgabe „[Installieren der Backup-Appliance](#)“, auf Seite 14 fortfahren.

Installieren der Backup-Appliance

Sie müssen die Backup-Appliance auf ESX 4.0 oder später oder auf ESXi 4.0 oder später installieren, damit Data Recovery die Sicherungsaufgaben abschließen kann. Die Backup-Appliance wird über den vSphere-Client bereitgestellt.

Voraussetzungen

vCenter Server und ein ESX 4.0- oder ESXi 4.0-Host müssen in Ihrer Umgebung ausgeführt werden, um die Backup-Appliance installieren zu können.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die Option **[Datei]** > **[OVF-Vorlage bereitstellen]**.
- 2 Wählen Sie **[Von Datei bereitstellen]** und navigieren Sie dann zu `vmwareDataRecovery_OVF10.ovf`, um die Datei auszuwählen.

Die OVF-Datei befindet sich auf der Data Recovery-CD im Verzeichnis `<Laufwerksbuchstabe>:\VMware-DataRecovery-ovf\`.

- 3 Lesen Sie die Informationen zur OVF-Datei.

- 4 Lesen Sie die Endbenutzer-Lizenzvereinbarung (EULA). Wenn Sie mit den Bedingungen einverstanden sind, wählen Sie die entsprechende Option.
Wenn Sie den Bedingungen nicht zustimmen, können Sie den Vorgang nicht fortsetzen.
- 5 Wählen Sie einen Speicherort für die Backup-Appliance in der vSphere-Bestandsliste aus.
Sie können die Backup-Appliance umbenennen.
- 6 Wählen Sie den Host oder Cluster aus, auf dem die Backup-Appliance bereitgestellt werden soll.
- 7 Wählen Sie einen Datenspeicher aus, in dem die Dateien der virtuellen Maschine gespeichert werden sollen.
- 8 Überprüfen Sie den Bildschirm „Zuweisung der IP-Adresse“.
Dieser Bildschirm enthält keine konfigurierbaren Optionen, aber Sie können der Backup-Appliance nach der Installation mit dem vSphere-Client eine statische IP zuweisen.
- 9 Wählen Sie eine Zeitzoneneinstellung.
- 10 Überprüfen Sie die Einstellungen für die Bereitstellung und klicken Sie auf **[Beenden]**.

Die Backup-Appliance wird nun in Ihrer Umgebung bereitgestellt.

Weiter

Sie können Sicherungen auf Netzwerkspeichern oder auf Festplatten speichern. Wenn Sie Sicherungen auf einer Festplatte speichern, können Sie nun die Aufgabe „[Hinzufügen einer Festplatte zur Backup-Appliance](#)“, auf Seite 15 durchführen. Anderenfalls können Sie mit [Kapitel 3](#), „[Verwenden von VMware Data Recovery](#)“, auf Seite 17 fortfahren.

Wenn während der Bereitstellung der Backup-Appliance Probleme auftreten, finden Sie unter http://www.vmware.com/de/support/developer/studio/studio20/va_user.pdf weitere Informationen zum Bereitstellen virtueller Appliances.

Hinzufügen einer Festplatte zur Backup-Appliance

Sie können Sicherungen auf einer Festplatte speichern, die zur Backup-Appliance hinzugefügt wurde. Festplatten bieten eine schnellere Sicherung verglichen mit anderen Zielen, wie z. B. CIFS-Freigaben.

Voraussetzungen

Wenn Sie eine Festplatte hinzufügen, muss die Backup-Appliance und das Data Recovery-Plug-In für den vSphere-Client bereits installiert sein.

Vorgehensweise

- 1 Starten Sie den vSphere-Client und melden Sie sich bei dem vCenter Server an, der die Backup-Appliance verwaltet.
- 2 Wählen Sie **[Bestandsliste]** > **[VMs und Vorlagen]**.
- 3 Klicken Sie in der Bestandsliste mit der rechten Maustaste auf die virtuelle Maschine, die als Backup-Appliance dient, und wählen Sie **[Einstellungen bearbeiten]**.
- 4 Klicken Sie auf der Registerkarte „Hardware“ auf **[Hinzufügen]**.
- 5 Wählen Sie **[Festplatte]**, und klicken Sie auf **[Weiter]**.

- 6 Wählen Sie einen Speichertyp.
 - Wählen Sie **[Neue virtuelle Festplatte erstellen]** , und klicken Sie auf **[Weiter]** .
 - Wählen Sie **[Vorhandene virtuelle Festplatte verwenden]** , um eine vorhandene Festplatte hinzuzufügen, wie z. B. beim Upgrade älterer Appliances, und klicken Sie auf **[Weiter]** .
 - Wählen Sie **[Zuordnungen für Raw-Geräte]** , um die Festplatte als RDM hinzuzufügen, und klicken Sie auf **[Weiter]** .
- 7 Geben Sie beim Erstellen einer neuen virtuellen Festplatte die Festplattengröße und andere Optionen an und klicken Sie auf **[Weiter]** .
- 8 Geben Sie beim Erstellen einer neuen virtuellen Festplatte die erweiterten Optionen an und klicken Sie auf **[Weiter]** .
- 9 Klicken Sie auf **[Beenden]** .

Die Festplatte wird nun zur Backup-Appliance hinzugefügt und kann als Ziel für Sicherungen verwendet werden. Wenn die Backup-Appliance eingeschaltet ist, wenn die Festplatte hinzugefügt wird, wird die Festplatte erst erkannt, wenn die Backup-Appliance neu gestartet wird. Sollte die Backup-Appliance also eingeschaltet sein, starten Sie sie neu, um das Hinzufügen der Festplatte vollständig abzuschließen.

Weiter

Hier erfahren Sie mehr über [Kapitel 3, „Verwenden von VMware Data Recovery“](#), auf Seite 17.

Verwenden von VMware Data Recovery

3

Verbinden Sie zum Verwenden von Data Recovery die Backup-Appliance mit vCenter Server und legen Sie Sicherungskonfigurationen fest.

Die allgemeinen Aufgaben beim Erstellen und Verwenden von Sicherungskonfigurationen umfassen:

- Einschalten der Backup-Appliance.
- Verbinden der Backup-Appliance mit vCenter Server.
- Konfigurieren von Data Recovery.
- Einrichten von Sicherungsaufgaben und der benötigten Ressourcen, z. B. das Hinzufügen von Netzwerkfreigaben oder das Formatieren von Volumes.

Dieses Kapitel behandelt die folgenden Themen:

- [„Einschalten der Backup-Appliance“](#), auf Seite 17
- [„Konfigurieren der Backup-Appliance“](#), auf Seite 18
- [„Verwenden des Assistenten für erste Schritte“](#), auf Seite 18
- [„Verwenden von Sicherungsaufgaben“](#), auf Seite 19
- [„Wiederherstellen von virtuellen Maschinen“](#), auf Seite 22
- [„Grundlegendes zu File Level Restore \(Wiederherstellen auf Dateiebene\)“](#), auf Seite 25
- [„Fehlerbehebung für VMware Data Recovery“](#), auf Seite 28

Einschalten der Backup-Appliance

Sie müssen zum Durchzuführen von Sicherungen die VM-Backup-Appliance einschalten.

Voraussetzungen

Sie müssen den folgenden Vorgang abgeschlossen haben, bevor Sie die Backup-Appliance einschalten: [„Installieren der Backup-Appliance“](#), auf Seite 14. Verwenden Sie vCenter Server, um sicherzustellen, dass die Zeitzeoneninformationen beim ersten Einschalten der Backup-Appliance korrekt sind. Nach dem ersten Einschalten der Backup-Appliance werden die Zeitzeoneninformationen festgelegt. Nachdem diese Informationen festgelegt wurden, kann die Backup-Appliance vom Host eingeschaltet werden, ohne dass die Zeitzone beeinträchtigt wird.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Bestandsliste] > [VMs und Vorlagen]** .
- 2 Klicken Sie mit der rechten Maustaste in der Bestandsliste auf die virtuelle Maschine, die als Backup-Appliance verwendet werden soll, und wählen Sie **[Einschalten]** .

- 3 Klicken Sie nach dem Einschalten der virtuellen Maschine mit der rechten Maustaste auf die Backup-Appliance-VM und wählen Sie **[Konsole öffnen]** .
Das Konsolenfenster für die Backup-Appliance erscheint.
- 4 Geben Sie den Benutzernamen und die Anmeldedaten für dieses System an.
Wenn Sie sich zum ersten Mal bei dieser Backup-Appliance anmelden, ist der Standardbenutzername „root“ und das Kennwort „vmw@re“.
- 5 Sofern das Standardkennwort des Stammkontos nicht geändert wurde, verwenden Sie den Befehl `passwd`, um das Kennwort des Stammkontos in ein stärkeres Kennwort Ihrer Wahl zu ändern.
- 6 Schließen Sie das Konsolenfenster.
Die Backup-Appliance bleibt eingeschaltet und ist bereit, die Sicherungsaufgaben durchzuführen.

Konfigurieren der Backup-Appliance

Sie können über die Webschnittstelle die Backup-Appliance neu starten oder Netzwerkeinstellungen vornehmen.

Voraussetzungen

Schalten Sie die Backup-Appliance zunächst ein, bevor Sie mit der Konfiguration beginnen.

Vorgehensweise

- 1 Geben Sie die URL der Backup-Appliance in einem Webbrowser ein.
Die URL der Backup-Appliance wird in der Appliance-Konsole angezeigt. Öffnen Sie die Appliance-Konsole im vSphere-Client.
- 2 Geben Sie den Benutzernamen und das Kennwort für das Administratorkonto ein.
- 3 Klicken Sie auf die Registerkarte „System“, um Informationen über die Appliance abzurufen oder klicken Sie auf **[Neu starten]** bzw. auf **[Herunterfahren]** .
- 4 Klicken Sie auf die Registerkarte **[Netzwerk]** und klicken Sie anschließend auf **[Status]** , um Informationen zu den aktuellen Netzwerkeinstellungen anzuzeigen.
- 5 Klicken Sie auf die Registerkarte **[Netzwerk]** und wählen Sie **[Adresse]** , um die Netzwerkeinstellungen zu konfigurieren. Sie können die Backup-Appliance so konfigurieren, dass sie ihre Adresse von DHCP erhält, oder IP-Einstellungen manuell festlegen.
- 6 Klicken Sie auf die Registerkarte **[Netzwerk]** und anschließend auf **[Proxy]** , um Proxy-Einstellungen festzulegen. Wenn Sie die Backup-Appliance für die Verwendung eines Proxy-Servers konfigurieren möchten, geben Sie den Namen oder die IP-Adresse und den Port für den Proxy-Server ein.

Die Backup-Appliance ist einsatzbereit.

HINWEIS Unter „Bestandsliste > Hosts und Cluster“ im vSphere-Client gibt der Status für VMware Tools der Data Recovery-Appliance an, dass sie „Nicht verwaltet“ sind. Es ist nicht nötig, die VMware Tools auf der Data Recovery-Appliance zu aktualisieren.

Verwenden des Assistenten für erste Schritte

Mit dem Assistenten für erste Schritte können Sie eine anfängliche Systemkonfiguration einrichten, die zum Starten der Sicherung virtueller Maschinen auf Wiederherstellungspunkte verwendet werden kann.

Voraussetzungen

Bevor Sie den Assistenten für erste Schritte verwenden, müssen Sie den unter [Backup-Appliance mit vCenter Server verbinden](#) beschriebenen Vorgang durchführen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home]** > **[Lösungen und Anwendungen]** > **[VMware Data Recovery]**.
- 2 Geben Sie auf der Seite „Anmeldedaten“ einen Benutzernamen und ein Kennwort ein und klicken Sie auf **[Weiter]**.
Data Recovery verwendet diese Informationen zum Herstellen einer Verbindung mit vCenter, um Sicherungen zu erstellen. Das angegebene Benutzerkonto muss über Administratorrechte verfügen.
- 3 Wählen Sie auf der Seite „Sicherungsziel“ aus der Auswahlliste ein Ziel für die Sicherung aus.
- 4 Wählen Sie auf der Seite „Sicherungsziel“ die Aufgaben aus, die Sie durchführen möchten.
 - Um den SCSI-Bus für neue SCSI-Geräte erneut zu prüfen, klicken Sie auf **[Aktualisieren]**.
 - Um eine virtuelle Festplatte zu formatieren, die zur Appliance hinzugefügt wurde, klicken Sie auf **[Format]**. Nach der Formatierung wird die Festplatte als `scsi:x:y` angezeigt. Verwenden Sie für Festplatten, die bereits Daten enthalten, **[Mounten]** an Stelle des Formatierens.
 - Klicken Sie zum Mounten einer Festplatte, die einen vorhandenen Deduplizierungsspeicher enthält, auf **[Mounten]**.
 - Klicken Sie zum Mounten der CIFS-Freigabe auf **[Netzwerkfreigabe hinzufügen]** und geben Sie die Anmeldedaten an. Diese Anmeldedaten werden in der Appliance gespeichert, d. h., das erneute Mounten wird automatisch ausgeführt, wenn die Appliance neu gestartet wird.
- 5 Klicken Sie auf **[Weiter]**.

Die anfängliche Systemkonfiguration ist nun abgeschlossen und der Assistent „Neue Sicherungsaufgabe erstellen“ wird standardmäßig geöffnet. Verwenden Sie, wie in „[Verwenden von Sicherungsaufgaben](#)“, auf Seite 19 beschrieben, den Assistenten „Neue Sicherungsaufgabe erstellen“, um eine Sicherungsaufgabe zu erstellen.

Verwenden von Sicherungsaufgaben

Mithilfe von Sicherungsaufgaben legen Sie fest, welche virtuellen Maschinen gesichert werden sowie wo und wie lange die Sicherungen gespeichert werden.

Virtuelle Maschinen

Geben Sie Erfassungen virtueller Maschinen an, z. B. alle virtuellen Maschinen in einem Datacenter, oder wählen Sie einzelne virtuelle Maschinen aus. Wenn Sie den gesamten Ressourcenpool, einen Host, ein Datacenter oder einen Ordner auswählen und neue virtuelle Maschinen zu einem dieser Container hinzufügen, sind diese in den nachfolgenden Sicherungen enthalten. Wenn Sie eine virtuelle Maschine auswählen, werden alle zur virtuellen Maschine hinzugefügten Festplatten gesichert. Falls Sie eine virtuelle Maschine vom ausgewählten Container in einen anderen Container verschieben, wird sie nicht mehr gesichert.

Ziel

Sie können Sicherungen auf Netzwerkfreigaben, in VMDKs oder auf RDMs speichern. Wenn Sie Sicherungen auf einer Netzwerkfreigabe speichern und die Netzwerkfreigabe, auf der Sie die Sicherung speichern möchten, nicht verfügbar ist, können Sie eine Netzwerkfreigabe hinzufügen. Weitere Informationen hierzu finden Sie unter „[Hinzufügen einer Netzwerkfreigabe](#)“, auf Seite 21. Sie müssen VMDKs und RDMs formatieren und partitionieren, um Sicherungen darauf speichern zu können. Sie können Ziele, bei denen dies noch nicht erfolgt ist, formatieren bzw. partitionieren. Weitere Informationen finden Sie unter „[Formatieren eines Volumens](#)“, auf Seite 21.

Sicherungsfenster

Standardmäßig werden Sicherungsaufgaben von Montag bis Freitag nachts und am Samstag und Sonntag zu jeder beliebigen Zeit ausgeführt. Data Recovery versucht, alle der Aufgabe zugewiesenen virtuellen Maschinen einmal täglich innerhalb des Sicherungsfensters zu sichern. Falls bei der Durchführung eines Sicherungsvorgangs der für das Sicherungsfenster festgelegte Zeitraum überschritten wird, wird die Sicherung gestoppt. Sie wird erneut gestartet, sobald sich das nächste Sicherungsfenster öffnet. Falls während des ersten angegebenen Fensters zu viele virtuelle Maschinen von Data Recovery gesichert werden müssen, werden einige dieser virtuellen Maschinen möglicherweise nicht gesichert. Letztendlich werden jedoch alle virtuellen Maschinen von Data Recovery gesichert und die nachfolgenden Sicherungen können in der Regel innerhalb eines Sicherungsfensters durchgeführt werden. Wenn einige Maschinen während eines Sicherungsfensters nicht gesichert werden können, erhalten diese Maschinen in nachfolgenden Sicherungsfenstern eine höhere Priorität. Dadurch wird sichergestellt, dass alle virtuellen Maschinen so oft gesichert werden, wie die Sicherungsfenster sowie die Ressourcen es zulassen und es wird verhindert, dass einige virtuelle Maschinen immer und andere niemals gesichert werden.

Aufbewahrungsrichtlinie

Von Data Recovery vorgenommene Sicherungen werden für einen variablen Zeitraum aufbewahrt. Sie können festlegen, ob Sie mehr oder weniger Sicherungen für einen längeren oder kürzeren Zeitraum aufbewahren möchten. Wenn eine größere Anzahl an Sicherungen aufbewahrt wird, wird mehr Festplattenplatz belegt, es stehen aber auch mehr Zeitpunkte für die Wiederherstellung virtueller Maschinen zur Verfügung. Mit zunehmendem Alter werden einige Sicherungen automatisch gelöscht, um Platz für neue Sicherungen zu schaffen. Sie können eine vordefinierte Aufbewahrungsrichtlinie auswählen oder eine eigene Richtlinie erstellen. Sicherungen werden einmal täglich innerhalb des Sicherungsfensters durchgeführt.

Bereit zum Abschließen

Überprüfen Sie die Einstellungen für die Sicherungsaufgabe. Diese Seite enthält folgende Informationen:

- Welche virtuellen Maschinen von dieser Aufgabe gesichert werden.
- Wo die Sicherungen für die angegebenen virtuellen Maschinen gespeichert werden.
- Der Zeitplan für das Sichern der virtuellen Maschinen.
- Die Anzahl der Sicherungen, die für die jeweiligen Zeiträume aufbewahrt werden. Beispielsweise die Anzahl der Sicherungen, die pro Monat aufbewahrt werden.

Verwenden des Assistenten für Sicherungsaufgaben

Mit dem Assistenten für Sicherungsaufgaben können Sie angeben, welche virtuellen Maschinen wann gesichert werden müssen.

Voraussetzungen

Bevor Sie den Assistenten für Sicherungsaufgaben verwenden, müssen Sie eine VMware Data Recovery-Konfiguration einrichten. Dies kann mit dem Assistenten für erste Schritte vorgenommen werden, wie unter [„Verwenden des Assistenten für erste Schritte“](#), auf Seite 18 beschrieben.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]** .
- 2 Klicken Sie auf **[Neue Sicherungsaufgabe...]** , um den Assistenten für Sicherungsaufgaben zu starten.
- 3 Wählen Sie auf der Seite „Virtuelle Maschinen“ einzelne virtuelle Maschinen oder Container aus, die zu sichernde virtuelle Maschinen enthalten, und klicken Sie auf **[Weiter]** .

- 4 Akzeptieren Sie auf der Seite „Sicherungsfenster“ die Standardzeiten oder geben Sie alternative Sicherungsfenster an und klicken Sie auf **[Weiter]** .
- 5 Akzeptieren Sie auf der Seite „Aufbewahrungsrichtlinie“ die standardmäßige Aufbewahrungsrichtlinie oder geben Sie eine alternative Aufbewahrungsrichtlinie an und klicken Sie auf **[Weiter]** .
- 6 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die zusammengefassten Informationen für die Sicherungsaufgabe und klicken Sie auf **[Weiter]** .

Hinzufügen einer Netzwerkfreigabe

Sie können eine Netzwerkfreigabe einrichten, die zum Speichern von Sicherungen verwendet wird.

Geben Sie Informationen über die Netzwerkfreigabe an, auf der VMware Data Recovery Datensicherungen speichern kann. Es handelt sich dabei normalerweise um die folgenden erforderlichen Informationen:

- URL - Geben Sie die IP-Adresse des Servers ein, der die Netzwerkfreigabe hostet.
- Benutzername - der Benutzername eines Kontos mit den erforderlichen Schreibberechtigungen für die Netzwerkfreigabe.
- Kennwort - Das Kennwort für das Benutzerkonto.

Informationen zum Hinzufügen einer Festplatte zur Backup-Appliance finden Sie unter [„Hinzufügen einer Festplatte zur Backup-Appliance“](#), auf Seite 15.

Formatieren eines Volumes

VMware Data Recovery kann Sicherungen auf Netzwerkvolumes, VMDKs und RDMs speichern. Netzwerkvolumes erfordern vielleicht keine Formatierung, VMDKs und RDMs müssen jedoch vor ihrer Verwendung formatiert werden.

Bei der Formatierung eines Volumes wird der Speicherplatz automatisch formatiert und partitioniert. Als Ergebnis werden die an diesem Speicherplatz gespeicherten Daten gelöscht. Formatieren Sie nach Bedarf das Volume, das Sie zum Speichern der Sicherung verwenden möchten.

In Übereinstimmung bringen

Sie können veranlassen, dass Data Recovery das Sicherungsfenster für ausgewählte Sicherungsaufgaben öffnet, bis alle anwendbaren virtuellen Maschinen gesichert sind. Sie können diese Funktion verwenden, um nach der Erstinstallation von Data Recovery einen anfänglichen Satz von Sicherungen zu erstellen oder zu erzwingen, dass alle Sicherungen von virtuellen Maschinen aktualisiert werden. Virtuelle Maschinen, die unabhängig vom Ausmaß der Änderungen seit der letzten Sicherung in den letzten 24 Stunden gesichert wurden, werden von der Option „In Übereinstimmung bringen“ nicht gesichert.

Voraussetzungen

Bevor Sie die Option „In Übereinstimmung bringen“ verwenden, müssen Sie Data Recovery bereits installiert und konfiguriert haben und über mindestens eine Sicherungsaufgabe verfügen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home]** > **[Lösungen und Anwendungen]** > **[VMware Data Recovery]** .
- 2 Klicken Sie auf die Registerkarte **[Sicherung]** , klicken Sie mit der rechten Maustaste auf eine Sicherungsaufgabe und klicken Sie dann auf **[In Übereinstimmung bringen]** .

Das Sicherungsfenster wird offen gehalten, damit Sicherungen auf jeder virtuellen Maschine, die in den letzten 24 Stunden nicht gesichert wurde, durchgeführt werden können. Das Sicherungsfenster kehrt zur vorher definierten Konfiguration zurück, wenn diese virtuellen Maschinen gesichert wurden.

Außerkräftsetzung von Sicherungsaufgaben

Einstellungen für Sicherungsaufgaben können außer Kraft gesetzt werden. Dabei werden Wiederherstellungspunkte entweder beibehalten, indem sie gesperrt werden, oder entfernt, indem sie zum Löschen markiert werden.

Voraussetzungen

Bevor Sie Wiederherstellungspunkte sperren oder zum Löschen markieren können, muss Data Recovery installiert und konfiguriert und es muss wenigstens ein Wiederherstellungspunkt vorhanden sein.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]** .
- 2 Klicken Sie auf die Registerkarte **[Wiederherstellen]** und wählen Sie einen oder mehrere Wiederherstellungspunkte aus.
 - a Um Wiederherstellungspunkte zum Löschen zu markieren, klicken Sie auf **[Zum Löschen markieren]** .
 - b Sollen Wiederherstellungspunkte auf unbegrenzte Zeit beibehalten werden, klicken Sie auf **[Sperren]** .

Zum Löschen markierte Wiederherstellungspunkte werden bei der nächsten Integritätsprüfung bzw. beim nächsten Rückgewinnungsvorgang gelöscht.

Wiederherstellen von virtuellen Maschinen

Mithilfe des Wiederherstellungsassistenten für virtuelle Maschinen können Sie die virtuellen Maschinen angeben, die wiederhergestellt werden sollen. Zudem können Sie die Art der Wiederherstellung angeben.

Mit Data Recovery können Sie testen, wie eine virtuelle Maschine wiederhergestellt würde, und den tatsächlichen Wiederherstellungsvorgang durchführen. Bei Probe-Wiederherstellungen werden virtuelle Maschinen aus Wiederherstellungspunkten erstellt. Aus Probe-Wiederherstellungen erstellte virtuelle Maschinen ersetzen keine aktuellen virtuellen Maschinen, vielmehr dienen sie dazu, sicherzustellen, dass Backups von virtuellen Maschinen erwartungsgemäß erstellt und erfolgreich wiederhergestellt werden können. Das tatsächliche Wiederherstellen einer virtuellen Maschinen versetzt sie in einem ausgewählten vorherigen Zustand.

Der Wiederherstellungsassistent bietet sowohl bei Wiederherstellungen als auch bei Proben Seiten, auf denen Sie die Quelle und das Ziel für das Wiederherstellen virtueller Maschinen konfigurieren können.

Quellenauswahl

Wählen Sie zum Festlegen der Quelle aus der Baumansicht der gesicherten vSphere-Objekte aus. Wählen Sie die wiederherzustellenden virtuellen Maschinen und virtuellen Festplatten aus. Anhand von Filtern können Sie nur den relevanten Teil der verfügbaren Auswahl anzeigen. Ähnlich wie beim Erstellen von Sicherungsaufgaben können Sie Sammlungen von virtuellen Maschinen angeben, wie z. B. alle virtuellen Maschinen in einem Datacenter, oder einzelne virtuelle Maschinen bzw. vmdk-Dateien zum Wiederherstellen auswählen. Wenn für eine einzelne virtuelle Maschine mehrere Wiederherstellungspunkte ausgewählt werden, stellt Data Recovery diese virtuelle Maschine anhand des zuletzt ausgewählten Wiederherstellungspunkts wieder her.

Zielauswahl

Diese Seite enthält eine Baumansicht des Speicherorts, an dem gesicherte vSphere-Objekte wiederhergestellt werden, und wie diese Objekte bei der Wiederherstellung konfiguriert werden. Falls es seit der letzten Sicherung Änderungen in Ihrer Bestandslistenhierarchie gegeben hat, werden die Pfade nicht mehr vorhandener Bestandslistenobjekte grau dargestellt. VM-Dateien, die an Speicherorten gesichert wurden, die nicht mehr vorhanden sind, müssen in gültige Speicherorte verschoben werden, damit der Wiederherstellungsvorgang durchgeführt werden kann. Sie können Optionen neu konfigurieren wie z. B.:

- Den Datenspeicher und den Knoten der virtuellen Festplatte, in dem die Dateien wiederhergestellt werden.
- Ob die Konfiguration wiederhergestellt wird. Wenn die Konfiguration nicht wiederhergestellt wird, wird möglicherweise die Konfiguration einiger anderer Optionen nicht unterstützt. Beispielsweise kann in diesem Fall möglicherweise konfiguriert werden, ob die virtuelle Maschine eingeschaltet wird, jedoch nicht, ob die Netzwerkkarte verbunden wird.
- Ob die Netzwerkkarte verbunden wird.
- Ob die virtuelle Maschine eingeschaltet wird.

Virtuelle Maschinen und VMDKs können entweder per Ziehen und Ablegen oder durch Auswählen neuer Ziele aus dem Popup-Baum verschoben werden. Klicken Sie zum Anzeigen weiterer Informationen über die vorhandene Bestandsliste auf den Link im oberen Teil der Seite.

Benennen Sie zum Klonen einer virtuellen Maschine die virtuelle Maschine, die Sie wiederherstellen, um.

Wenn die Standardanmeldeinformationen für das Backup keine Wiederherstellungsrechte aufweisen, können Sie alternative Anmeldedaten angeben.

Bereit zum Abschließen

Überprüfen Sie die Einstellungen für die Sicherungsaufgabe. Diese Seite enthält eine Baumstruktur dessen, was wiederhergestellt werden soll, sowie zusammenfassende Informationen. Die Baumstruktur enthält Informationen wie z. B.:

- Objektnamen.
- Wann der Wiederherstellungspunkt erstellt wurde.
- Welcher Datenspeicher als Ziel für wiederhergestellte virtuelle Maschinen oder virtuelle Festplatten verwendet wird.
- Informationen zum Knoten einer virtuellen Festplatte.
- Ob die Konfiguration wiederhergestellt wird.
- Ob die Netzwerkkarte verbunden wird.
- Ob die virtuelle Maschine eingeschaltet wird.

Die Zusammenfassung enthält die folgenden Informationen:

- Wie viele virtuelle Maschinen überschrieben werden.
- Wie viele virtuelle Maschinen erstellt werden.
- Wie viele virtuelle Festplatten überschrieben werden.

- Wie viele virtuelle Festplatten erstellt werden.
- Die Gesamtmenge an Daten, die wiederhergestellt wird.

HINWEIS Falls auf dem Zieldatenspeicher nicht genügend Speicherplatz zum Durchführen des Wiederherstellungsvorgangs zur Verfügung steht, wird eine Warnung angezeigt. Sie können andere Datenspeicher mit einer höheren Kapazität angeben oder in Kauf nehmen, dass Wiederherstellungen möglicherweise nicht wie erwartet abgeschlossen werden.

Erstellen einer Probe-Wiederherstellung

Führen Sie eine Probe-Wiederherstellung durch, um zu bestätigen, dass eine virtuelle Maschine erwartungsgemäß gesichert und dass ein erfolgreicher Wiederherstellungsvorgang durchgeführt wird.

Voraussetzungen

Bevor Sie eine Probe-Wiederherstellung durchführen können, müssen Sie VMware Data Recovery konfiguriert haben und über mindestens eine Sicherung verfügen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]**.
- 2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine, für die eine Sicherung verfügbar ist, und wählen Sie **[Probe-Wiederherstellung]**.

Der Wiederherstellungsassistent für virtuelle Maschinen wird mit der geöffneten Seite „Bereit zum Abschließen“ angezeigt.

- 3 Klicken Sie auf **[Wiederherstellen]**, um die Probe-Wiederherstellung durchzuführen, oder klicken Sie auf **[Zurück]**, um die Einstellungen zu ändern.

Eine Version der virtuellen Maschine wird in der Bestandsliste wiederhergestellt. Bei der virtuellen Maschine, die bei der Probe-Wiederherstellung erstellt wird, ist die Verbindung zu allen Netzwerkkarten getrennt. Dies verhindert, dass bei der Probe-Wiederherstellung eine virtuelle Maschine erstellt wird, die damit beginnt, Aufgaben zu erledigen, die für eine vorhandene, nicht wiederhergestellte virtuelle Maschine gedacht sind.

Weiter

Danach können Sie die virtuelle Maschine löschen, die beim Testen des Wiederherstellungsvorgangs erstellt wurde.

Wiederherstellen virtueller Maschinen von einer Sicherung

Das Wiederherstellen virtueller Maschinen auf den Stand einer vorherigen Sicherung geschieht anhand des Wiederherstellungsassistenten für virtuelle Maschinen.

Voraussetzungen

Bevor Sie virtuelle Maschinen wiederherstellen können, müssen Sie VMware Data Recovery konfigurieren und über mindestens eine Sicherung verfügen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]**.
- 2 Geben Sie den Namen der virtuellen Maschine oder die IP-Adresse der Backup-Appliance ein und klicken Sie auf **[Verbinden]**.

- 3 Wechseln Sie zur Registerkarte **[Wiederherstellen]** und klicken Sie auf den Link **[Wiederherstellen]**, um den Wiederherstellungsassistenten für virtuelle Maschinen zu starten.

Der Wiederherstellungsassistent für virtuelle Maschinen wird angezeigt.

- 4 Geben Sie auf der Quellauswahlseite eine Quelle an, von der die virtuellen Maschinen wiederhergestellt werden sollen, und klicken Sie auf **[Weiter]**.
- 5 Geben Sie auf der Zielauswahlseite an, wie wiederhergestellte Maschinen konfiguriert werden sollen, und klicken Sie auf **[Weiter]**.
- 6 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Konfiguration und klicken Sie auf **[Beenden]**.

Die virtuellen Maschinen werden wie im Assistenten angegeben wiederhergestellt.

Grundlegendes zu File Level Restore (Wiederherstellen auf Dateiebene)

Benutzer möchten möglicherweise eine Version einer einzelnen Datei wiederherstellen, die mithilfe von Data Recovery gesichert wurde. Möglicherweise wurde die Datei gelöscht oder es werden Informationen aus einer Vorgängerversion benötigt. In einem solchen Fall können Benutzer die vorherige Version der virtuellen Maschine, die die Datei enthielt, vollständig wiederherstellen, aber dies kann umständlich sein. Bei einem Rollback auf eine Vorgängerversion wird möglicherweise die vorhandene virtuelle Maschine überschrieben und auch dann, wenn die virtuelle Maschine an einem anderen Speicherort wiederhergestellt wird, verläuft der Vorgang nicht so schnell wie gewünscht.

File Level Restore (FLR) bietet dafür die Möglichkeit, auf einzelne Dateien innerhalb eines Wiederherstellungspunkts für virtuelle Windows-Maschinen zuzugreifen. Somit ist es möglich, Kopien von Dateien zu lesen oder diese innerhalb von Wiederherstellungspunkten an einem beliebigen Speicherort wiederherzustellen. Mit FLR können Sie beispielsweise zwei Kopien einer Datei erstellen, um die Versionen vergleichen zu können, oder FLR kann eine vorhandene Datei durch eine ältere, im Wiederherstellungspunkt enthaltene Version überschreiben, d. h. eine Vorgängerversion wiederherstellen.

Beachten Sie, dass die Verwendung von FLR zum Zugriff auf Dateien in Wiederherstellungspunkten nur eine Möglichkeit darstellt, deren Inhalte zu lesen. Mit FLR können Sie den Inhalt eines Wiederherstellungspunkts ändern. Obwohl FLR den Inhalt von Wiederherstellungspunkten nicht ändert, erwecken einige Anwendungen den Anschein, als ob Änderungen vorgenommen werden. So führt beispielsweise das Ziehen und Ablegen einer Datei von einem Wiederherstellungspunkt an eine andere Position dazu, dass die Datei möglicherweise aus der Liste entfernt wird. Diese Änderung gibt das eigentliche Ereignis nicht wieder. Um zu bestätigen, dass der Inhalt der Wiederherstellungspunkte nicht geändert wurde, aktualisieren Sie die Anzeige. Beachten Sie dabei, dass keine Dateien geändert wurden.

Wenn FLR aufgerufen wird, werden alle Dateien, die zum Durchführen des Wiederherstellungsvorgangs auf Dateiebene benötigt werden, aus der ausführbaren Datei extrahiert. Auf ähnlicher Weise werden beim Beenden der FLR-Sitzung nicht nur alle Verbindungen mit Wiederherstellungspunkten geschlossen, sondern alle extrahierten Dateien werden auch aus dem System entfernt.

Wenn FLR gestartet wird, wird eine Verbindung mit dem Data Recovery-Backup-Appliance hergestellt. FLR funktioniert in Verbindung mit dem Virtual Disk Development Kit (VDDK) in VMware, um auf Informationen über den Inhalt der Wiederherstellungspunkte zuzugreifen. Alle Wiederherstellungspunkte werden angezeigt, aber FLR kann nur Wiederherstellungspunkte für kompatible virtuelle Windows-Maschinen mounten.

Beim Mounten eines Wiederherstellungspunkts wird auf der lokalen Festplatte der virtuellen Maschine ein Knotenpunkt erstellt. Der Knotenpunkt ist ein Verzeichnis, das denselben Namen wie der Wiederherstellungspunkt hat. Er enthält ein Verzeichnis für jede gemountete Festplatte, die dem Wiederherstellungspunkt zugeordnet ist. Benutzer können die Inhalte der VMDK-Festplattendateien nach dem Wiederherstellungspunkt für die virtuelle Maschine durchsuchen. Die Dateien der Festplattendateien für den ausgewählten Wiederherstellungspunkt können dann an einen Speicherort nach Wahl kopiert werden.

Nachdem alle FLR-Vorgänge beendet wurden, können Sie einen einzelnen Wiederherstellungspunkt unmounten, indem Sie ihn auswählen und auf **[Unmounten]** klicken, oder Sie können alle Wiederherstellungspunkte unmounten, indem Sie auf **[Alle unmounten]** klicken.

Nach dem Beenden von FLR werden alle Dateien entfernt, die zum Aktivieren der FLR-Funktionalität extrahiert wurden. Beachten Sie, dass bereits extrahierte Dateien nicht entfernt werden, falls FLR unerwartet beendet wird. Die Anzahl und Größe der Dateien ist unerheblich, sodass das Aufräumen der verbliebenen Dateien nicht zwingend erforderlich ist, falls das Programm unerwartet beendet wird. Beim nächsten Verwenden des Programms werden alle verbliebenen Dateien verwendet: Sie werden nach Beenden der nächsten Sitzungen dann aus dem System entfernt.

Installieren von FLR

Sie können FLR auf einer virtuellen Maschine mit Windows XP oder höher installieren, indem Sie die Programmdatei von FLR auf eine virtuelle Maschine kopieren.

Vorgehensweise

- 1 Legen Sie die Data Recovery-Installations-CD ein.
Das VMware Data Recovery-Installationsfenster wird angezeigt.
- 2 Klicken Sie auf **[Medien durchsuchen]**.
- 3 Kopieren Sie die Programmdatei des FLR-Clients von der Installations-CD unter <Laufwerksbuchstabe>:/WinFLR/VMwareRestoreClient.exe auf die virtuelle Maschine, die den FLR-Client verwenden wird.

Der FLR-Client ist nun für die Verwendung auf der virtuellen Windows-Maschine bereit.

Wiederherstellen von Dateien mithilfe des FLR-Standardmodus

Verwenden Sie den File Level Restore-Client, um von Wiederherstellungspunkten aus auf einzelne Dateien zuzugreifen, anstatt komplette virtuelle Maschinen wiederherzustellen. Dieser Client ist zwar nicht für das ordnungsgemäße Funktionieren von Data Recovery erforderlich, er bietet aber Zugriff auf zusätzliche Funktionen.

Voraussetzungen

Der FLR-Client kann von Benutzern mit Administratorrechten auf virtuellen Maschinen mit Windows XP oder höher verwendet werden. Der FLR-Client benötigt das .NET 2.0 Framework. Damit FLR relevant wird, ist es nützlich, eine Backup-Appliance mit Wiederherstellungspunkten zu haben. FLR kann in eine Umgebung installiert werden, in der es weder eine Backup-Appliance noch Wiederherstellungspunkte gibt, aber ohne diese ist der Client nutzlos. Im Standardmodus können Dateien nur für die virtuelle Maschine wiederhergestellt werden, bei der Sie angemeldet sind. FLR funktioniert nicht mit Wiederherstellungspunkten für virtuelle Maschinen, die GUID-Partitionstabellen (GPT) verwenden.

Vorgehensweise

- 1 Starten Sie die virtuelle Windows-Maschine, in der Sie FLR verwenden werden.
- 2 Doppelklicken Sie auf die FLR-Programmdatei.
Das Fenster des VMware Data Recovery-Wiederherstellungs-Clients wird geöffnet.
- 3 Wählen Sie in der Dropdown-Liste **[IP-Adresse / Name]** eine Data Recovery-Appliance aus oder geben Sie den Namen bzw. die IP-Adresse der Appliance ein, mit der Sie eine Verbindung herstellen möchten, und klicken Sie auf **[Anmeldung]**.

FLR zeigt eine Liste aller verfügbaren Wiederherstellungspunkte für die aktuelle virtuelle Maschine an.

- 4 Wählen Sie einen Wiederherstellungspunkt aus und klicken Sie auf **[Mounten]** .
Der ausgewählte Wiederherstellungspunkt wird als Verzeichnis auf der lokalen Festplatte der verwendeten virtuellen Maschine gemountet. Die Inhalte des Wiederherstellungspunkts stehen nun zur Verfügung und können von der virtuellen Maschine aus durchsucht werden.
- 5 Sie können von der virtuellen Maschine aus jede gewünschte Datei durchsuchen und sie wiederherstellen.
- 6 Ist das Durchsuchen und Wiederherstellen von Dateien beendet, klicken Sie auf **[Alle unmounten]** und beenden Sie FLR.

Wiederherstellen von Dateien mithilfe des erweiterten FLR-Modus

Verwenden Sie FLR im erweiterten Modus, um von Wiederherstellungspunkten mehrerer virtueller Maschinen aus auf Dateien zuzugreifen.

Voraussetzungen

Der FLR-Client kann von Benutzern mit Administratorrechten auf virtuellen Maschinen mit Windows XP oder höher verwendet werden. Der FLR-Client benötigt das .NET 2.0 Framework. Damit FLR relevant wird, ist es nützlich, eine Backup-Appliance mit Wiederherstellungspunkten zu haben. FLR kann in eine Umgebung installiert werden, in der es weder eine Backup-Appliance noch Wiederherstellungspunkte gibt, aber ohne diese ist der Client nutzlos. Im erweiterten Modus können Dateien für alle gesicherten virtuellen Maschinen wiederhergestellt werden. Sie müssen zum Verwenden des erweiterten Modus Zugriff auf ein Konto mit Administratorberechtigungen in vCenter haben. FLR funktioniert nicht mit Wiederherstellungspunkten für virtuelle Maschinen, die GUID-Partitionstabellen (GPT) verwenden.

Vorgehensweise

- 1 Starten Sie die virtuelle Windows-Maschine, in der Sie FLR verwenden werden.
- 2 Doppelklicken Sie auf die FLR-Programmdatei.
Das Fenster des VMware Data Recovery-Wiederherstellungs-Clients wird geöffnet.
- 3 Markieren Sie das Kontrollkästchen **[Erweiterter Modus]** .
- 4 Stellen Sie Verbindungsinformationen zu FLR bereit.
 - a Wählen Sie unter „Data Recovery-Appliance“ in der Dropdown-Liste **[IP-Adresse/Name]** eine Data Recovery-Appliance aus oder geben Sie den Namen bzw. die IP-Adresse der Appliance ein, mit der eine Verbindung hergestellt werden soll.
 - b Wählen Sie unter „vCenter Server“ in der Dropdown-Liste **[IP-Adresse/Name]** eine Data Recovery-Appliance aus oder geben Sie den Namen bzw. die IP-Adresse der Appliance ein, mit der eine Verbindung hergestellt werden soll.
 - c Geben Sie im Feld **[Benutzername]** den Namen eines Benutzers mit Administratorrechten für vCenter ein.
 - d Geben Sie unter vCenter Server im Feld **[Kennwort]** das Kennwort für den zuvor angegebenen administrativen Benutzer ein.
 - e Klicken Sie auf **[Anmelden]** .

FLR zeigt eine Liste aller verfügbaren Wiederherstellungspunkte für alle gesicherten virtuellen Maschinen auf der Data Recovery-Appliance an, mit der Sie verbunden sind.
- 5 Wählen Sie einen Wiederherstellungspunkt aus und klicken Sie auf **[Mounten]** .
Der ausgewählte Wiederherstellungspunkt wird als Verzeichnis auf der lokalen Festplatte der verwendeten virtuellen Maschine gemountet. Die Inhalte des Wiederherstellungspunkts stehen nun zur Verfügung und können von der virtuellen Maschine aus durchsucht werden.

- 6 Sie können von der virtuellen Maschine aus jede gewünschte Datei durchsuchen und sie wiederherstellen.
- 7 Ist das Durchsuchen und Wiederherstellen von Dateien beendet, klicken Sie auf **[Alle unmounten]** und beenden Sie FLR.

Fehlerbehebung für VMware Data Recovery

Falls Sie Verbindungs- oder Konfigurationsprobleme mit Data Recovery haben, können Sie versuchen, die Fehler wie folgt zu beheben.

Problem	Mögliche Lösung
Es kann keine Verbindung zur Backup-VM hergestellt werden.	Prüfen Sie, ob die virtuelle Maschine in der Ansicht „Hosts und Cluster“ der Bestandsliste aufgeführt ist. Stellen Sie sicher, dass die IPv4-Adresse der Data Recovery-Appliance korrekt ist.
Data Recovery schlägt beim Erstellen von Sicherungen fehl mit dem Fehler <code>disk full error -1115</code> , aber die Festplatte ist nicht voll.	Data Recovery benötigt Festplattenspeicher zum Indizieren und Verarbeiten von Wiederherstellungspunkten. Dies bedeutet, dass Data Recovery in der Regel ausreichend freien Speicherplatz für die Sicherungen virtueller Maschinen plus 10 GB zusätzlich benötigt. Um beispielsweise einen Wiederherstellungspunkt für eine einzelne 10 GB große virtuelle Maschine zu erstellen, sollten 20 GB Speicherplatz zur Verfügung stehen. Fügen Sie zum Beheben dieses Problems zusätzliche Festplatten zur Backup-Appliance hinzu.
Die NFS-Freigabe funktioniert nicht wie erwartet.	NFS wird nur dann unterstützt, wenn die Freigabe von einem ESX Server bereitgestellt wird und der Appliance die VMDK zugewiesen ist. NFS-Freigaben können der Appliance nicht direkt zugeordnet werden.
Data Recovery ist ausgefallen. Ist der Systemzustand in Ordnung?	Weil der Status der Appliance im Deduplizierungsspeicher gespeichert ist, kann sie wiederhergestellt werden. Installieren Sie die Data Recovery-Appliance auf dem ESX-Host neu und konfigurieren Sie die Appliance so, dass sie auf den vorhandenen Deduplizierungsspeicher verweist.
Die Backup-Appliance ist mit vCenter Server verbunden und es gab einen Absturz.	Falls nach dem Anwenden von Änderungen der vSphere-Client abstürzt, starten Sie den vSphere-Client neu und stellen Sie die Verbindung zur Backup-Appliance wieder her.
Es wurde ein gültiger Netzwerkname eingegeben, aber Data Recovery stellt keine Verbindung her.	In einigen Fällen funktioniert die Namensauflösung nicht. Versuchen Sie, für das gewünschte Ziel die IP-Adresse zu verwenden.

Backup- und Wiederherstellungsvorgänge werden nicht wie erwartet durchgeführt.

Eine Integritätsprüfung hat möglicherweise ein Problem mit der Integrität des Deduplizierungsspeichers festgestellt.

Die Integrität von neuen Backups wird täglich, der gesamte Deduplizierungsspeicher wöchentlich überprüft. Falls während der Integritätsprüfung Probleme festgestellt werden, wird der Deduplizierungsspeicher gesperrt. Demzufolge können Sicherungs- und Wiederherstellungsvorgänge erst dann durchgeführt werden, wenn die von der Integritätsprüfung festgestellten Probleme behoben wurden. Wählen Sie zum Beheben dieses Problems auf der Registerkarte „Wiederherstellen“ die problematischen Wiederherstellungspunkte aus und klicken Sie auf „Zum Löschen markieren“. Diese Wiederherstellungspunkte werden während der nächsten Integritätsprüfung gelöscht. Anschließend wird die Sperre des Deduplizierungsspeichers aufgehoben.

Falls durch die Integritätsprüfung kein Problem festgestellt wurde, verursacht möglicherweise die Menge an Aufgaben das Problem. Data Recovery begrenzt die Anzahl der Aufgaben, die ausgeführt werden können, um zu verhindern, dass Systeme überladen werden und so deren Leistung beeinträchtigt wird. Einige dieser Beschränkungen sind:

- Es können maximal acht Sicherungsaufgaben gleichzeitig ausgeführt werden.
- Es können maximal acht Wiederherstellungsaufgaben gleichzeitig ausgeführt werden.
- Aufgaben können nur dann gestartet werden, wenn die CPU-Nutzung 90 Prozent oder weniger beträgt.
- Im Deduplizierungsspeicher muss für jede Aufgabe mindestens 5 GB an verfügbarem Speicherplatz zur Verfügung stehen.

Falls eine dieser Einschränkungen nicht eingehalten wird, werden keine neuen Aufgaben gestartet.

Die Backup-Appliance von Data Recovery wird nicht verwaltet.

Dies ist erwartetes Verhalten. Die Backup-Appliance wird nicht von vSphere Server oder anderen Diensten, wie z. B. Update Manager, verwaltet. Dies ist nicht erforderlich und es ist eventuell auch nicht möglich, die Backup-Appliance zu verwalten.

Falls Probleme auftreten, die nicht mithilfe dieser Fehlerbehebungshinweise behoben werden können, wenden Sie sich an den technischen Support von VMware. Erfassen Sie Ihre Data Recovery-Protokolldateien und versteckten Protokolle und führen Sie das entsprechende Skript zum Erfassen der Protokolle aus, bevor Sie sich an den technischen Support wenden. Weitere Informationen zum Ausführen des Skripts zur Protokollerfassung finden Sie unter <http://kb.vmware.com/kb/1012282>.

Sie können zudem die ausführlichen Data Recovery-Protokolle auf hilfreiche Informationen überprüfen.

Grundlegendes zu beschädigten Wiederherstellungspunkten

Wiederherstellungspunkte können durch ausgefallene Speichermedien und Lese-/Schreibfehler beschädigt werden. Wenn solche Beschädigungen auftreten, entfernen Sie die betroffenen Wiederherstellungspunkte.

Beschädigte Wiederherstellungspunkte werden während einer Integritätsprüfung identifiziert. Alle beschädigten Wiederherstellungspunkte sollten entfernt werden, da sie möglicherweise Data Recovery-Vorgänge, wie z. B. das Ausdünnen, blockieren. Durchsuchen Sie das Vorgangsprotokoll nach Einträgen, die sich auf beschädigte Wiederherstellungspunkte beziehen. Falls das Protokoll darauf hindeutet, dass es in Ihrer Umgebung beschädigte Wiederherstellungspunkte gibt, entfernen Sie diese, indem Sie sie in der Bestandsliste suchen oder nach allen beschädigten Wiederherstellungspunkten suchen. Nachdem die beschädigten Wiederherstellungspunkte zum Löschen markiert wurden, führen Sie eine weitere Integritätsprüfung durch, um den Vorgang abzuschließen.

Entfernen von beschädigten Wiederherstellungspunkten

Beschädigte Wiederherstellungspunkte, die während Integritätsprüfungen erkannt werden, sollten entfernt werden. Wiederherstellungspunkte können bei vorübergehenden Verbindungsfehlern als beschädigt identifiziert werden. Wenn vorübergehende Verbindungsfehler möglich sind, überprüfen Sie nach dem Wiederherstellen der Verbindungen, ob beschädigte Wiederherstellungspunkte behoben wurden.

Voraussetzungen

Bevor Sie beschädigte Wiederherstellungspunkte entfernen können, muss es Wiederherstellungspunkte in einer funktionierenden Data Recovery-Bereitstellung geben.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]** .
- 2 Klicken Sie auf die Registerkarte **[Berichte]** und doppelklicken Sie auf die fehlgeschlagene Integritätsprüfung.

Das Vorgangsprotokoll für das Ereignis wird in einem separaten Fenster geöffnet. Beachten Sie, welche Wiederherstellungspunkte die Störung ausgelöst haben.
- 3 Schließen Sie das Vorgangsprotokoll und klicken Sie auf die Registerkarte **[Wiederherstellen]** .
- 4 Wählen Sie in der Filter-Dropdown-Liste **[Beschädigte Wiederherstellungspunkte]** .

Die verfügbaren Wiederherstellungspunkte werden gefiltert und zeigen nur die virtuellen Maschinen mit beschädigten Wiederherstellungspunkten an. Es ist möglicherweise erforderlich, den Knoten einer virtuellen Maschine zu erweitern, um den beschädigten Wiederherstellungspunkt anzuzeigen.
- 5 Wählen Sie die beschädigten Wiederherstellungspunkte zum Entfernen aus und klicken Sie auf **[Zum Löschen markieren]** .
- 6 Starten Sie eine Integritätsprüfung.

Wenn eine Integritätsprüfung abgeschlossen wird, werden alle zum Löschen markierten Wiederherstellungspunkte entfernt.
- 7 Überprüfen Sie die Ergebnisse der Integritätsprüfung, um sicherzugehen, dass keine beschädigten Wiederherstellungspunkte mehr vorhanden sind.

Grundlegendes zur Datei „datarecovery.ini“

Die Einstellungen in der Datei „datarecovery.ini“ können geändert werden, um zu beeinflussen, wie die Backup-Appliance Aufgaben ausführt. Das Ändern der Datei „datarecovery.ini“ ist ein Verfahren für Fortgeschrittene, das in der Regel dazu dient, das Verhalten von Data Recovery zu ändern, um Probleme zu beheben.

Ändern des Backup-Appliance-Verhaltens mithilfe der Datei „datarecovery.ini“

Änderungen an den Einstellungen in der Datei „datarecovery.ini“ beeinflussen das Verhalten der Data Recovery-Backup-Appliance.

Um diese Aufgabe ausführen zu können, benötigen Sie Zugriff auf ein Konto mit administrativen Berechtigungen für die Backup-Appliance.

Voraussetzungen

Schalten Sie die Backup-Appliance ein, bevor Sie die folgenden Schritte durchführen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Backup-Appliance und wählen Sie **[Konsole öffnen]** .
- 2 Geben Sie den Benutzernamen und die Anmeldedaten für dieses System an.
Es ist empfehlenswert, den Standardbenutzernamen und das Standardkennwort im Anschluss an die Installation der Backup-Appliance zu ändern. Werden die Standardanmeldeinformationen nicht geändert, lautet der Benutzername „root“ und das Kennwort „vmw@re“.
- 3 Beenden Sie den datarecovery-Dienst mithilfe des Befehls `service datarecovery stop`.
- 4 Verwenden Sie einen beliebigen Editor und ändern Sie die Datei „datarecovery.ini“. Falls nicht vorhanden, erstellen Sie die Datei `datarecovery.ini` im Verzeichnis `/var/vmware/datarecovery`.
In diesem Fall muss die erste Zeile in der Datei [Options] lauten. In der Datei „datarecovery.ini“ wird die Groß-/Kleinschreibung beachtet.
- 5 Speichern Sie die Änderungen und schließen Sie die Datei „datarecovery.ini“.
- 6 Starten Sie den datarecovery-Dienst mithilfe des Befehls `service datarecovery start neu`.

datarecovery.ini - Referenz

Ändern Sie die Einstellungen der INI-Datei, um das Verhalten von Data Recovery zu beeinflussen.

Beim Inhalt der Datei „datarecovery.ini“ muss die Groß-/Kleinschreibung beachtet werden.

Tabelle 3-2. Einstellungen von „datarecovery.ini“

Option	Beschreibung	Beispiel	Bereich
MaxLogFiles	Legt die maximale Anzahl an Protokolldateien fest, die Data Recovery beibehält. Wenn das Maximum erreicht ist, ersetzt die nächste erstellte Protokolldatei die älteste vorhandene Protokolldatei.	MaxLogFiles=20	
DisableHotaddCopy	Deaktiviert bei einer Einstellung von 1 das SCSI-Hot-Add.	DisableHotaddCopy=1	0-1.
DisableNetworkCopy	Deaktiviert bei einer Einstellung von 1 die Netzwerkkopie.	DisableNetworkCopy=1	0-1.
SetVCBLogging	Die interne Protokollierungsebene für das VMware Consolidated Backup API.	SetVCBLogging=7	0-7. 7 ist die ausführlichste Protokollierungsebene.
SetRAPILogging	Die interne Protokollierungsebene für das Data Recovery API.	SetRAPILogging=7	0-7. 7 ist die ausführlichste Protokollierungsebene.
SetEngineLogging	Die interne Protokollierungsebene für die Backup-Appliance von Data Recovery.	SetEngineLogging=7	0-7. 7 ist die ausführlichste Protokollierungsebene.
SetDevicesLogging	Die interne Protokollierungsebene für den Duplizierungsvorgang.	SetDevicesLogging=7	0-7. 7 ist die ausführlichste Protokollierungsebene.

Tabelle 3-2. Einstellungen von „datarecovery.ini“ (Fortsetzung)

Option	Beschreibung	Beispiel	Bereich
SetAppLogging	Die interne Protokollierungsebene für die allgemeine Anwendungslogik.	SetAppLogging=7	0-7. 7 ist die ausführlichste Protokollierungsebene.
SetVolumesLogging	Die interne Protokollierungsebene für die Interaktionen zwischen virtuellen Maschinen und Volumes.	SetVolumesLogging=7	0-7. 7 ist die ausführlichste Protokollierungsebene.
SetBackupSetsLogging	Die interne Protokollierungsebene für Katalogvorgänge.	SetBackupSetsLogging=7	0-7. 7 ist die ausführlichste Protokollierungsebene.
IntegrityCheckInterval	Das Intervall in Tagen für Integritätsprüfungen.	IntegrityCheckInterval=7	0-7.
BackupRetryInterval	Die Anzahl an Minuten, die die Backup-Appliance wartet, bevor eine fehlgeschlagene Sicherung erneut durchgeführt wird.	BackupRetryInterval=20	
RetentionPolicyInterval	Die Anzahl an Tagen, bevor Speicherplatz im Deduplizierungsspeicher zurückgewonnen wird.	RetentionPolicyInterval=4	1-7.
DedupeCheckOnRecatalog	Schließt bei einer Einstellung von 1 nach einer Neukatalogisierung eine Integritätsprüfung ab.	DedupeCheckOnRecatalog=1	0-1.
EnableFileRestore	Deaktiviert bei einer Einstellung von 0 das File Level Restore. Diese Option wirkt sich nur auf Data Recovery Version 1.1 oder später aus. Diese Option wird ignoriert, wenn FLR im Administratormodus verwendet wird.	EnableFileRestore=1	0-1.
MaxBackupRestoreTasks	Die maximale Anzahl gleichzeitiger Sicherungen und Wiederherstellungen.	MaxBackupRestoreTasks=4	1-8.

Verwenden der Data Recovery-Protokolle

Data Recovery bietet eine Protokollierung, die unterschiedlich detailliert ausfallen kann und an unterschiedliche Bedingungen angepasst werden kann.

Die drei beachtenswerten Protokollierungstypen sind:

- Grundlegende Protokolle - Diese Protokolle enthalten die grundlegenden Informationen.
- Ausführliche Data Recovery-Protokolle - Diese Protokolle bieten ausführlichere Informationen.
- Client-Verbindungsprotokolle - Diese Protokolle können auch dann angezeigt werden, wenn Sie keine Verbindung zu einer Backup-Appliance herstellen können.

Es ist möglich, die Protokolle für eine einzelne Backup-Appliance anzuzeigen. Um alle Protokollierungsinformationen in einer Umgebung mit mehreren Appliances zu überprüfen, müssen Sie zu jeder Appliance eine Verbindung herzustellen und das Protokoll jeder Appliance prüfen.

Anzeigen der Data Recovery-Protokolle

Lesen Sie die Data Recovery-Protokolle, um Informationen über die Leistungsfähigkeit des Systems zu erhalten.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home]** > **[Lösungen und Anwendungen]** > **[VMware Data Recovery]**.
- 2 Geben Sie den Namen der virtuellen Maschine oder die IP-Adresse der Backup-Appliance ein und klicken Sie auf **[Verbinden]**.
- 3 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Protokoll]**.

Anzeigen der ausführlichen Data Recovery-Protokolle

Zeigen Sie die ausführlichen Data Recovery-Protokolle an, wenn Sie zusätzliche Informationen zu erkannten Problemen benötigen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home]** > **[Lösungen und Anwendungen]** > **[VMware Data Recovery]**.
- 2 Geben Sie den Namen der virtuellen Maschine oder die IP-Adresse der Backup-Appliance ein und klicken Sie auf **[Verbinden]**.
- 3 Klicken Sie auf die Registerkarte **[Konfiguration]**, halten Sie die Umschalttaste gedrückt und klicken Sie auf den Link **[Protokoll]**.

Die Schnittstelle des ausführlichen Protokolls wird angezeigt.

- 4 Klicken Sie je nach benötigten Informationen auf **[Client-Protokoll]**, **[Appliance-Betriebsprotokoll]** oder **[Appliance-Assert-Protokoll]**.
- 5 Halten Sie zum Ändern der Protokollierungsebene die Umschalttaste gedrückt und klicken Sie auf **[Protokoll aktualisieren]**.

Die Protokollierungsebenensteuerung wird angezeigt.

- 6 Klicken Sie auf den Auf- oder Abwärtspfeil für die **[Protokollierungsebene]**, um die Standardeinstellungen außer Kraft zu setzen.

Anzeigen der Client-Verbindungsprotokolle

Sie können den Inhalt der Client-Verbindungsprotokolle anzeigen, selbst wenn eine Verbindung zu einer Backup-Appliance nicht möglich ist. Die Informationen in diesen Protokollen können Ihnen dabei helfen, Konnektivitätsprobleme zu beheben.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **[Home]** > **[Lösungen und Anwendungen]** > **[VMware Data Recovery]** .
- 2 Geben Sie den Namen der virtuellen Maschine oder die IP-Adresse der Backup-Appliance ein und klicken Sie auf **[Verbinden]** .

Wenn die Verbindung erfolgreich verläuft, können Sie normale Protokolle anzeigen, wie in „[Anzeigen der Data Recovery-Protokolle](#)“, auf Seite 33 beschrieben. Wenn die Verbindung fehlschlägt, fahren Sie mit diesem Vorgang fort.

- 3 Drücken Sie die Tastatursequenz 'Strg-Alt-G-G'.
Die Client-Verbindungsprotokolle werden angezeigt.

Index

A

Assistent für erste Schritte, verwenden **18**
Assistent für Sicherungsaufgaben, verwenden **20**

B

Backup-Appliance
Einschalten **17**
Installieren **14**
konfigurieren **18**

C

Client, Installieren **14**

D

Dateien wiederherstellen, FLR **26**
Datenwiederherstellung
konfigurieren **17**
Skalierung **11**
Voraussetzungen **11**
Deduplizierung
optimale Vorgehensweisens **10**
Skalierung **10**

E

Einführung, Datenwiederherstellung **7**
erstellen, Sicherungsaufgabe **19**

F

Fehlerbehebung **28**
Firewalls **14**
FLR
Dateien wiederherstellen **26**
Grundlegendes zu **25**

G

Grundlegendes zu, FLR **25**

H

hinzufügen
Netzwerkfreigabe **21**
Speicher **15**

I

In Übereinstimmung bringen **21**
Installieren
Backup-Appliance **14**

Client **14**

Datenwiederherstellung **11**

Integritätsprüfung **10**

K

konfigurieren
Backup-Appliance **18**
Datenwiederherstellung **17**

L

Lizenzierung **7**

N

Netzwerkfreigabe, hinzufügen **21**
Neukatalogisierung **10**

P

Probe-Wiederherstellung **22, 24**

S

Sicherung
manuell **21**
Prozess **7**
Skalierung **7**
Sicherungsaufgabe
erstellen **19, 20**
Optionen **19**
Skalierung
Datenwiederherstellung **11**
Deduplizierung **10**
Sicherung **7**
Speicher, hinzufügen **15**

U

Unterstützter Speicher **7**

V

verwenden, Assistent für erste Schritte **18**
Virtuelle Maschinen, Wiederherstellen **22, 24**
Volume Shadow Copy Service, *Siehe auch* VSS
Volumes, Formatierung **21**
VSS
Grundlegendes zu **8**
Unterstützung **8**
Vorteile **8**

W

Wiederherstellen, Virtuelle Maschinen **22, 24**
Wiederherstellen auf Dateiebene, , *siehe* FLR

Z

Zurückgewinnung **10**