Administratorhandbuch für VMware Data Recovery

Data Recovery 1.2

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

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

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/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/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/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/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 Best Practices 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/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/ESXi™ 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

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

Für virtuelle Maschinen, die in vSphere 4.0 oder höher 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/ESXi-Hosts an. Diese überprüft für jede zu sichernde virtuelle Festplatte die vorherige Sicherung. Anhand der Änderungsverfolgungsfunktionalität der ESX/ESXi-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 für virtuelle Maschinen, die mit Hardwareversion 7 oder höher erstellt wurden, aber sie gelten nicht für virtuelle Maschinen, die mit älteren VMware-Produkten als vSphere 4.0 erstellt wurden. Beispielsweise wird die Verfolgungsfunktionalität für geänderte Blöcke nicht bei virtuellen Maschinen verwendet, die mit Virtual Infrastructure 3.5 oder früher erstellt wurden. Als Ergebnis dauert das Sichern virtueller Maschinen länger, die mit früheren Hardwareversionen 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 Essentials Plus, Advanced, Enterprise oder Enterprise Plus.

Jede Instanz von vCenter Server kann bis zu zehn Backup-Appliances von Data Recovery unterstützen und jede Backup-Appliance kann insgesamt 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 - Stilllegen

VMware Data Recovery verwendet das Stilllegen anhand des Volume Shadow Copy Service (VSS). 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 Requestor-Komponente befindet sich in einem unterstützten Gastbetriebssystem und reagiert auf Ereignisse einer externen Sicherungsanwendung. Der Requestor wird vom VMware Tools-Dienst instanziiert, wenn ein Sicherungsvorgang initialisiert wird. Der VSP ist als Windows-Dienst registriert und benachrichtigt den ESX/ESXi-Host, wenn die Anwendungen stillgelegt werden, damit er einen Snapshot der virtuellen Maschine erstellen kann.

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

Tabelle 1-1. Verwendeter Treibertyp und Stilllegungsmechanismen gemäß dem Gastbetriebssystem

Gastbetriebssystem	Verwendeter Treibertyp	Verwendeter Stilllegungstyp
Windows XP 32-Bit Windows 2000 32-Bit	SYNC-Treiber	Stilllegung mit Absturzkonsistenz
Windows 2003 32 Bit/64 Bit	VMware VSS-Komponente	Außerbetriebnahme mit Anwendungskonsistenz
Windows 2008 32-Bit/64-Bit Windows 2008 R2 Windows Vista 32-Bit/64-Bit Windows 7 32-Bit/64-Bit	VMware VSS-Komponente	Stilllegung mit Absturzkonsistenz
Andere Gastbetriebssysteme	Nicht anwendbar	Außerbetriebnahme mit Absturzkonsistenz

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.

Detaillierte Informationen über VSS finden Sie unter http://technet.microsoft.com/en-us/library/cc785914.aspx.

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

Tabelle 1-2. Speicherort der benutzerdefinierten Skripts für die Stilllegung

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, welche die entsprechende Unterstützung bieten.

Vorteile des Deduplizierungsspeichers

Die von VMware Data Recovery verwendete Deduplizierungsspeichertechnologie 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 auf den Einsatz von zwei Deduplizierungsspeichern beschränkt. Bei Data Recovery gibt es kein Limit hinsichtlich der Größe der Deduplizierungsspeicher, wenn aber die Größe eines Speichers ein Terabyte überschreitet, kann dies die Leistung beeinträchtigen. Obwohl Data Recovery der Größe des Deduplizierungsspeichers kein Limit auferlegt, schränken andere Faktoren die Größe des Deduplizierungsspeichers ein. Deduplizierungsspeicher werden durch folgende Limits eingeschränkt:

- 500 GB bei CIFS-Netzwerkfreigaben
- 1 TB bei VMDKs und RDMs

HINWEIS NFS wird nur dann als Format für den Deduplizierungsspeicher unterstützt, wenn die Freigabe von einem ESX/ESXi Server bereitgestellt wird und der Data Recovery-Appliance die VMDK zugewiesen ist.

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

Integritätsprüfung

Dieser Vorgang dient dazu, die Datenintegrität im Deduplizierungsspeicher zu überprüfen und zu warten. Integritätsprüfungen werden unter verschiedenen Bedingungen für den gesamten Deduplizierungsspeicher oder Teile davon ausgeführt. Data Recovery ist darauf ausgelegt, alle 24 Stunden eine inkrementelle Integritätsprüfung auszuführen. Bei inkrementellen Integritätsprüfungen wird die Integrität von Wiederherstellungspunkten überprüft, die seit der letzten vollständigen oder inkrementellen Integritätsprüfung zum Deduplizierungsspeicher hinzugefügt wurden. Außerdem ist Data Recovery darauf ausgelegt, einmal pro Woche eine Integritätsprüfung für alle Wiederherstellungspunkte auszuführen.

Data Recovery wurde in der Absicht entwickelt, zu verhindern, dass Integritätsprüfungen Computing-Ressourcen verbrauchen oder laufende Sicherungsvorgänge auf andere Art behindern. Wenn infolgedessen der geplante Zeitpunkt gekommen ist, eine inkrementelle oder vollständige Integritätsprüfung durchzuführen, überprüft Data Recovery, ob das Sicherungsfenster aktiv ist. Wenn das Sicherungsfenster nicht aktiv ist, beginnt die Integritätsprüfung. Wenn das Sicherungsfenster aktiv ist, überprüft Data Recovery, ob das Sicherungsfenster innerhalb der nächsten 24 Stunden inaktiv wird. Wenn das Sicherungsfenster während der nächsten 24 Stunden aktiv bleibt, wird die Integritätsprüfung begonnen. Wenn das Sicherungsfenster innerhalb der nächsten 24 Stunden beendet wird, verschiebt Data Recovery die Integritätsprüfung auf den Zeitpunkt, zu dem das Sicherungsfenster nicht mehr aktiv ist.

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 Dedupli-

zierungsspeicher 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.

Katalogaktualisierung

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 Katalogaktualisierung 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.

Der Zurückgewinnungsvorgang wird auf Basis derselben Logik gestartet oder verschoben, anhand der ermittelt wird, ob eine Integritätsprüfung abgeschlossen werden soll. Zurückgewinnungsvorgänge werden in der Regel einmal alle 24 Stunden ausgeführt, wenn keine Sicherungsfenster aktiv sind.

Zurückgewinnungsvorgänge werden auch ausgeführt, wenn ein Schreibvorgang auf den Deduplizierungsspeicher fehlschlägt, da solch ein Fehlschlag möglicherweise darauf hindeutet, dass der Speicher voll ist. In solch einem Fall kann die Ausführung eines Zurückgewinnungsvorgangs dazu führen, dass Speicherplatz im Deduplizierungsspeicher frei wird. Wenn folglich in den letzten 12 Stunden keine Zurückgewinnungsvorgänge ausgeführt wurden, wird sofort ein Zurückgewinnungsvorgang gestartet. Dieser Zurückgewinnungsvorgang wird unabhängig vom Status des Sicherungsfensters gestartet.

Beim Zurückgewinnungsvorgang wendet Data Recovery die Aufbewahrungsrichtlinie auf jede virtuelle Quellmaschine in einer Sicherungsaufgabe für das entsprechende Ziel an. Wenn sich mehrere Sicherungsaufgaben mit unterschiedlichen Aufbewahrungsrichtlinien auf dieselbe virtuelle Maschine beziehen, führt Data Recovery die Aufbewahrungsrichtlinien zusammen und behält genügend Sicherungen bei, um die Kriterien aller Sicherungsaufgaben zu erfüllen. Wenn eine virtuelle Quellmaschine in einer Sicherungsaufgabe definiert wurde, aber die virtuelle Maschine gelöscht oder nicht mehr in der Sicherungsaufgabe definiert ist, werden keine der Wiederherstellungspunkte dieser virtuellen Maschine entfernt.

Die Aufbewahrungsrichtlinie sorgt für die Aufbewahrung von Sicherungen, die eine Kombination von wöchentlichen, monatlichen, vierteljährlichen und jährlichen Sicherungen sein können. Diese Zeiträume werden wie folgt definiert:

Tabelle 1-3. Kriterien zum Festlegen unterschiedlicher Sicherungstypen

Sicherungstyp	Kriterien
Wöchentlich	Die erste Sicherung freitags nach 22:00 Uhr.
Monatlich	Die erste Sicherung nach 22:00 Uhr am letzten Tage eines Monats.

Tabelle 1-3. Kriterien zum Festlegen unterschiedlicher Sicherungstypen (Fortsetzung)

Sicherungstyp	Kriterien
Vierteljährlich	Die erste Sicherung nach 22:00 Uhr am letzten Tage eines Monats für März, Juni, September und Dezember.
Jährlich	Die erste Sicherung nach 22:00 Uhr am 31. Dezember.

HINWEIS Wenn durch Zurückgewinnungsvorgänge Speicherplatz in Dateien frei wird, werden diese Dateien nicht um den frei gewordenen Platz verkleinert. Demzufolge erhöht sich die Anzahl des freien Speicherplatzes im Deduplizierungsspeicher nicht, selbst wenn durch Zurückgewinnungsvorgänge Speicherplatz frei wird. Der frei gewordene Speicherplatz wird für nachfolgende Sicherungen reserviert.

Installieren von VMware Data Recovery 2

VMware Data Recovery verwendet ein Plug-In zum vSphere-Client und eine Backup-Appliance, um Backups auf 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/ESXi 4-Host installiert.
- Der optionale File Level Restore-Client (FLR-Client) ist in einer virtuellen Maschine installiert, die ein unterstütztes Gastbetriebssystem ausführt. Weitere Informationen zu FLR finden Sie in „Grundlegendes zu File Level Restore (Wiederherstellen auf Dateiebene)“, auf Seite 33.

Dieses Kapitel behandelt die folgenden Themen:

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.
- Die zu sichernden virtuellen Maschinen und die Backup-Appliance müssen auf ESX/ESXi 4 oder später ausgeführt werden. Der ESX/ESXi-Host, der die Backup-Appliance einstellt, muss von vCenter Server verwaltet werden.
- Wenn beim Verwenden von Data Recovery vCenter Server-Systeme im verknüpften Modus ausgeführt werden, melden Sie sich bei dem vCenter Server an, mit dem die Data Recovery-Appliance verknüpft ist.

Sie können Backups auf jeder virtuellen Festplatte speichern, die von ESX/ESXi 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.

Wenn Sie Festplatten zur Backup-Appliance hinzufügen, beachten Sie, über wie viele Festplatten die meisten zu sichernden virtuellen Maschinen verfügen. Jede Backup-Appliance kann 100 virtuelle Maschinen sichern. Maximal können acht virtuelle Maschinen gleichzeitig gesichert werden. Jede Festplatte auf jeder virtuellen Maschine kann im laufenden Betrieb hinzugefügt werden, damit die Sicherung durchgeführt wird. In der Standardkonfiguration hat die Backup-Appliance einen SCSI-Adapter #0 und eine SCSI-Festplatte #0, die mit dem SCSI-Adapter verbunden ist. Da der erste SCSI-Adapter über eine Systemfestplatte bei SCSI 0:0 verfügt, können nur 14 SCSI-Festplatten im laufenden Betrieb hinzugefügt werden. Nach abgeschlossener Sicherung einer virtuellen Maschine werden die Festplatten dieser virtuellen Maschine entfernt und nachfolgende Sicherungen können gestartet werden. Wenn in der Standardkonfiguration die Gesamtzahl der Festplatten der gesicherten virtuellen Maschinen 15 erreicht, werden die Festplatten über das Netzwerk gesichert anstatt durch das Hinzufügen im laufenden Betrieb. Wenn Sie virtuelle Maschinen mit einer höheren Anzahl an Festplatten verwenden, sollten Sie zusätzliche Festplatten zur Appliance hinzufügen. Wenn beispielsweise jede virtuelle Maschine in Ihrer Umgebung drei Festplatten hat, werden einige Festplatten der virtuellen Maschinen über das Netzwerk gesichert und die Leistung wird möglicherweise beeinträchtigt. Indem Sie eine Dummy-Festplatte mit 1 MB zu einem anderen SCSI-Busadapter hinzufügen, erhöht sich die Anzahl der insgesamt verfügbaren Positionen für SCSI-Busse zum Hinzufügen im laufenden Betrieb auf 30, d. h. dass alle acht virtuellen Maschinen des hier angeführten Beispiels durch das Hinzufügen im laufenden Betrieb gleichzeitig gesichert werden können. Zusätzliche Festplatten sollten bei Bedarf zu SCSI 1:0, SCSI 2:0 und SCSI 3:0 hinzugefügt werden. Eine virtuelle Maschine, wie z. B. die Backup-Appliance, kann über bis zu vier SCSI-Adapter verfügen, wodurch maximal 60 Positionen für SCSI-Busse zum Hinzufügen im laufenden Betrieb zur Verfügung stehen, was für die meisten Umgebungen ausreicht.

Weitere Informationen zum Einrichten einer vSphere 4.0-Umgebung oder höher 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. 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 ermpfehlenswert, 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-bereitgestellten oder Thick-Provisioned-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-Provisioned-Festplatten besser geeignet, um potenzielle Leistungseinbußen zu verhindern, wie sie beim Vergrößern von Thin-bereitgestellten-Festplatten auftreten. Wenn der verfügbare Speicherplatz auf einer Thick-Provisioned-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 Anbietern und sie sind schlichtweg keine ideale Lösung. Zudem bieten virtuelle Festplatten und RDMs in vielen Fällen eine bessere Leistung als netzwerkbasierende Deduplizierungsspeicher. Deduplizierungsspeicher können in RDM entweder mit virtueller oder physischer Kompatibilität gespeichert 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.

Beim Verwenden von Thin-bereitgestellten virtuellen Festplatten als Zielfestplatten für die Datenwiederherstellung gilt es, bestimmte Überlegungen anzustellen. vSphere friert automatisch jede virtuelle Maschine ein, wenn die Nutzung deren Thin-bereitgestellter Festplatte die Kapazität des VMFS-Datenspeichers überschreitet, auf dem sie sich befindet. Deshalb empfiehlt VMware, eine von zwei Strategien zu verwenden, um zu vermeiden, dass für die Zielfestplatte für Data Recovery kein Speicherplatz mehr zur Verfügung steht.

- Verwenden Sie Alarme, um darauf aufmerksam zu machen, dass der Speicherplatz auf einer Thin-bereitgestellten Festplatte gering ist und mehr Speicherplatz erforderlich ist.
- Verwenden Sie kleinere Thick-provisioned virtuelle Festplatten und erweitern Sie die Festplatte bei Bedarf.

Netzwerkanforderungen

Verschiedene Komponenten von Data Recovery kommunizieren untereinander über TCP. Stellen Sie demzufolge sicher, dass die entsprechenden Ports in Ihrer Umgebung geöffnet sind, um einen ordnungsgemäßen Betrieb zu gewährleisten.

- Die Backup-Appliance wird mit den vCenter Server-Webservices verbunden. Standardmäßig erfolgt diese Verbindung über die Ports 80 und 443.
- Über Port 22024 werden das Data Recovery-Client-Plug-In und der FLR-Client (File Level Restore) mit der Backup-Appliance verbunden.
- Über Port 902 verbindet sich die Backup-Appliance mit VMware ESX oder VMware ESXi.

ESX/ESXi Server, die unter Verwendung eines DNS-Namens zu vCenter hinzugefügt wurden, müssen über einen Namen verfügen, der aufgelöst werden kann. In einigen Fällen führt die Verwendung von DNS-Namen zu Problemen. Sollten Probleme beim Auflösen von DNS-Namen auftreten, sollten Sie stattdessen mithilfe von IP-Adressen ESX/ESXi Server hinzufügen.

Sicherheitsanforderungen für Anmeldedaten

Damit die Tätigkeiten von Data Recovery abgeschlossen werden können, müssen in diesem Kontext bestimmte Berechtigungen vorhanden sein. Stellen Sie sicher, dass den entsprechenden Benutzern die folgenden Berechtigungen erteilt werden.

Die Rolle, die die Backup-Appliance zum Ausführen von Sicherungen verwendet, muss für alle zu sichernden virtuellen Maschinen über die folgenden Berechtigungen verfügen:

- Virtuelle Maschine->Konfiguration->Festplattenänderungsverfolgung
- Virtuelle Maschine->Bereitstellung->Lesezugriff auf Festplatte zulassen
- Virtuelle Maschine->Bereitstellung->Download virtueller Maschinen zulassen
- Virtuelle Maschine->Status->Snapshot erstellen
- Virtuelle Maschine->Status->Snapshot entfernen

Der Benutzer muss für die Backup-Appliance über die folgenden Berechtigungen verfügen:

- Datenspeicher->Speicher zuteilen
- Virtuelle Maschine->Konfiguration->Neue Festplatte hinzufügen
- Virtuelle Maschine->Konfiguration->Ressourcen ändern
- Virtuelle Maschine->Konfiguration->Festplatte entfernen
- Virtuelle Maschine->Konfiguration->Einstellungen

Der Benutzer muss für alle vCenter Server-Systeme, für alle Hosts der zu sichernden virtuellen Maschinen und für den Host der Backup-Appliance über die folgenden Berechtigungen verfügen:

- Global->Lizenz

Besondere Überlegungen zur Data Recovery-Kompatibilität

Sie sollten bestimmte Aspekte beachten, wenn Sie Data Recovery in Ihrer Umgebung einrichten. Data Recovery wird unterstützt zur Verwendung mit:

- Zehn Backup-Appliances von Data Recovery für jede vCenter Server-Instanz.
- Jede Backup-Appliance schützt bis zu 100 virtuelle Maschinen.
- VMDK- oder RDM-basierende Deduplizierungsspeicher mit bis zu 1 TB oder CIFS-basierende Deduplizierungsspeicher mit bis zu 500 GB.
- CIFS-Freigaben mit Kennwörtern, die aus 64 Zeichen oder weniger bestehen. Kennwörter für CIFS-Freigaben müssen dem Standard „Latin 1“ (ISO 8859-1) entsprechen. Doppelbyte-Zeichen werden nicht unterstützt.
- Wenn zum Sichern des Deduplizierungsspeichers eine Drittanbieterlösung verwendet wird, dürfen diese Sicherungen nicht bei laufendem Data Recovery-Dienst ausgeführt werden. Sichern Sie den Deduplizierungsspeicher erst, wenn Sie die Backup-Appliance von Data Recovery ausgeschaltet oder den Data Recovery-Dienst mithilfe des Befehls `service datarecovery stop` gestoppt haben.
- Bis zu zwei Deduplizierungsspeichern pro Backup-Appliance.
- vCenter Server im verknüpften Modus. Damit diese Konfiguration wie erwartet funktioniert, müssen Sie sich bei dem vCenter Server anmelden, mit dem die Data Recovery-Appliance verknüpft ist.

Data Recovery unterstützt Folgendes nicht:

- IPv6-Adressen. IPv4-Adressen werden für die Data Recovery-Appliance benötigt.
- Das Hinzufügen von Festplatten im laufenden Betrieb mit vSphere-Versionen, die für das Hotplug nicht lizenziert sind.
- Das Wiederherstellen von verknüpften Klonen von VMware View. Data Recovery kann verknüpfte Klone von VMware View sichern, aber sie werden als nicht verknüpfte Klone 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, wobei gemeinsam genutzte SCSI-Busse in Gebrauch sind.
- Festplatten mit Raw Device Mapping (RDM) im physischen Kompatibilitätsmodus bei zu sichernden virtuellen Maschinen.
- Das Verwenden älterer Versionen des vSphere-Client-Plug-Ins oder älterer Versionen von FLR zusammen mit der aktuellen Version von Data Recovery.
- Mehrere Backup-Appliances auf einem einzelnen Host.
- Das Verwenden von Data Recovery zum Sichern von Backup-Appliances von Data Recovery. Obwohl nicht unterstützt, sollte dies kein Problem darstellen. Die Backup-Appliance ist ein statusfreies Gerät. Dies bedeutet, es besteht weniger die Notwendigkeit, es zu sichern, als dies bei anderen Arten von virtuellen Maschinen der Fall ist.

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 18 fortfahren.

Installieren der Backup-Appliance

Installieren Sie die Backup-Appliance auf ESX/ESXi 4.0 Update 2 oder höher, damit Data Recovery die Sicherungsaufgaben abschließen kann. Die Backup-Appliance wird über den vSphere-Client bereitgestellt.

Voraussetzungen

vCenter Server muss und ein ESX/ESXi 4.0 Update 2-Host sollte in Ihrer Umgebung ausgeführt werden, um die Backup-Appliance installieren zu können. Die Verbindung der Backup-Appliance mit ESX/ESXi erfolgt über Port 902. Wenn sich zwischen der Backup-Appliance und ESX/ESXi eine Firewall befindet, muss Port 902 offen sein. Die Backup-Appliance, das Client-Plug-In und FLR sollten alle dieselbe Version haben. Installieren Sie nicht mehrere Backup-Appliances auf einem einzelnen Host.

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 Wählen Sie einen Speicherort für die Backup-Appliance in der vSphere-Bestandsliste aus.

   Sie können die Backup-Appliance umbenennen.

5 Wählen Sie den Host oder Cluster aus, auf dem die Backup-Appliance bereitgestellt werden soll.

6 Wählen Sie einen Datenspeicher aus, in dem die Dateien der virtuellen Maschine gespeichert werden sollen.

   Wenn Sie einen Datenspeicher wählen, auf dem die Dateien für die Backup-Appliance gespeichert werden sollen, wählen Sie den Datenspeicher mit der größten VMFS-Blockgröße aus. Dies ist notwendig, um sicherzustellen, dass die Backup-Appliance virtuelle Maschinen von allen Datenspeichern sichern kann.

7 Wählen Sie ein Festplattenformat für die virtuelle Festplatte aus.

8 Wählen Sie unter „Eigenschaften“ eine Zeitzone für die Appliance aus.

9 Überprüfen Sie die Einstellungen für die Bereitstellung und klicken Sie auf **[Beenden]** .

Die Backup-Appliance wird nun in Ihrer Umgebung bereitgestellt.

Weiter

Sie können die IP-Adresseneinstellungen über die Backup-Appliance-Konsole nach der Installation ändern. Falls dies erforderlich ist, öffnen Sie das Konsolenfenster der Backup-Appliance über den vSphere-Client und nehmen Sie die gewünschten Änderungen an den IP-Adresseneinstellungen vor.

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 19 durchführen. Anderenfalls lesen Sie den Abschnitt Kapitel 3, „Verwenden von VMware Data Recovery“, auf Seite 21.

Die Backup-Appliance wird durch eine Anmerkung auf der virtuellen Maschine erkannt, die „VMware Data Recovery Module“ lautet. Ändern Sie diese Anmerkung nicht bzw. fügen Sie diese Anmerkung nicht anderen virtuellen Maschinen hinzu. Das manuelle Hinzufügen oder Entfernen dieser Anmerkung führt zu unerwünschten Ergebnissen.

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. Weitere Informationen zu Festplattenformaten, einschließlich der Verwendung von Thin-bereitgestellten Festplatten, finden Sie unter „Formate des Deduplizierungsspeichers“, auf Seite 15. Weitere Informationen dazu, wie sinnvoll es ist, SCSI-Festplatten hinzuzufügen, finden Sie unter „VMware Data Recovery - Systemanforderungen“, auf Seite 13.

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 hinzufügen, wie z. B. beim Upgrade einer älteren Appliance, 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]** .

Beim Erstellen einer virtuellen SCSI-Festplatte wird empfohlen, dass Sie den SCSI-Wert auf „SCSI 1:0“ festlegen.

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 beim Hinzufügen der Festplatte die Backup-Appliance eingeschaltet ist, wird die Festplatte möglicherweise nicht sofort erkannt. Entweder Sie warten, bis die Festplatte angezeigt wird, oder Sie starten die Backup-Appliance neu.

Weiter

Hier erfahren Sie mehr über Kapitel 3, „Verwenden von VMware Data Recovery“, auf Seite 21.

Erweitern einer Festplatte

Um mehr freien Speicherplatz zu erhalten, können Festplatten erweitert werden.

Voraussetzungen

Zum Erweitern einer Festplatte muss eine Festplatte mit freiem Speicherplatz verfügbar sein, damit die Erweiterung eingerichtet werden kann.

Vorgehensweise

1 Stellen Sie sicher, dass zurzeit keine Vorgänge auf der Festplatte ausgeführt werden.

2 Schließen Sie die Erweiterung der Festplatte im laufenden Betrieb ab.

Die Festplatte wird im laufenden Betrieb erweitert, es muss aber einige Minuten gewartet werden, bis das Betriebssystem die aktualisierte Festplattenkonfiguration erkennt.

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:

- Konfigurieren von Data Recovery.
- Einrichten von Sicherungsaufgaben und der benötigten Ressourcen, z. B. das Hinzufügen von Netzwerkfreigaben oder das Formatieren von Volumes.

Wenn beim Verwenden von Data Recovery vCenter Server-Systeme im verknüpften Modus ausgeführt werden, müssen Sie sich bei dem vCenter Server anmelden, mit dem die Data Recovery-Appliance verknüpft ist.

Dieses Kapitel behandelt die folgenden Themen:

Grundlegendes zur Data Recovery-Benutzerschnittstelle

Das vSphere-Client-Plug-In für Data Recovery bietet mehrere neue Benutzerschnittstellenelemente für die Konfiguration des Verhaltens von Data Recovery.

Die Benutzerschnittstelle von Data Recovery ist in mehrere Registerkarten unterteilt. Die Registerkarten mit den neuen Schnittstellenoptionen sind: die Registerkarten „Erste Schritte“, „Sicherung“ und „Wiederherstellen“.

Registerkarte „Erste Schritte“

Die Registerkarte „Erste Schritte“ enthält grundlegende Informationen zu Data Recovery sowie Funktionen zum Durchführen allgemeiner Konfigurationsaufgaben.

Tabelle 3-1. Registerkarte „Erste Schritte“

Symbol	Name	Beschreibung
	Aufgabe hinzufügen	Startet den Assistenten für Sicherungsaufgaben. Weitere Informationen finden Sie unter „Verwenden des Assistenten für Sicherungsaufgaben“, auf Seite 28.
	Virtuelle Maschine wiederherstellen	Startet den Assistenten für die Wiederherstellung einer virtuellen Maschine. Weitere Informationen finden Sie unter „Wiederherstellen virtueller Maschinen von einer Sicherung“, auf Seite 32.
	Berichte anzeigen	Wechselt von der aktuellen Ansicht in die Registerkarte „Berichte“, auf der Sie sich den Status der vorhandenen Aufgaben ansehen können.

Registerkarte „Sicherung“

Auf der Registerkarte „Sicherung“ finden Sie Informationen zu vorhandenen Sicherungsaufgaben sowie zu deren Status. Sie können zudem Sicherungsaufgaben erstellen, bearbeiten und löschen.

Tabelle 3-2. Registerkarte „Sicherung“

Symbol	Name	Beschreibung
	Aufgabe hinzufügen	Startet den Assistenten für Sicherungsaufgaben. Weitere Informationen finden Sie unter „Verwenden des Assistenten für Sicherungsaufgaben“, auf Seite 28.
	Aufgabe bearbeiten	Startet den Assistenten für Sicherungsaufgaben zum Bearbeiten einer vorhandenen Aufgabe.
	Aufgabe löschen	Löscht die ausgewählte Sicherungsaufgabe.

Registerkarte „Wiederherstellen“

Über die Registerkarte „Wiederherstellen“ können Sie vorhandene Wiederherstellungspunkte wiederherstellen, sperren oder zum Löschen markieren. Die Funktionen zum Sperren und Markieren schließen sich gegenseitig aus, sodass Sie nur eine der beiden Optionen auswählen können. Weitere Informationen zum Sperren und Markieren von Wiederherstellungspunkten finden Sie unter „Markieren von Wiederherstellungspunkten zum Entfernen oder Sperren“, auf Seite 30. Die Registerkarte „Wiederherstellen“ steht möglicherweise nicht zur Verfügung, wenn keine Wiederherstellungspunkte vorhanden sind.

Tabelle 3-3. Registerkarte „Wiederherstellen“

Symbol	Name	Beschreibung
	Virtuelle Maschine wiederherstellen	Startet den Assistenten für die Wiederherstellung virtueller Maschinen von einer Sicherung, mit dem Sie festlegen können, wie virtuelle Maschinen in den Zustand, der in den ausgewählten Wiederherstellungspunkten gespeichert ist, wiederhergestellt werden sollen. Weitere Informationen finden Sie unter „Wiederherstellen von virtuellen Maschinen“, auf Seite 30. Standardmäßig führt Data Recovery das Speichern und etwaige Löschen von ältereren Wiederherstellungspunkten gemäß der in der Sicherungsaufgabe angegebenen Aufbewahrungsrichtlinie durch. Von Data Recovery verwaltete Wiederherstellungspunkte werden durch folgende Symbole dargestellt: 
	Wiederherstellungspunkt sperren	Sie können die ausgewählten Wiederherstellungspunkte sperren oder die Sperrung aufheben. Gesperrte Wiederherstellungspunkte werden auf unbestimmte Zeit beibehalten, statt sie im Laufe der Zeit gemäß der Wiederherstellungsrichtlinie zu löschen.
	Wiederherstellungspunkt löschen	Sie können die ausgewählten Wiederherstellungspunkte zum Löschen markieren oder die Markierung aufheben. Wiederherstellungspunkte, die zum Löschen markiert sind, werden von Data Recovery entfernt. Zum Löschen markierte Wiederherstellungspunkte werden in der Regel nicht sofort gelöscht.

Einschalten der Backup-Appliance

Die Backup-Appliance der virtuellen Maschine muss eingeschaltet sein, um Sicherungen durchzuführen. Die Backup-Appliance wird in einigen Fällen automatisch eingeschaltet, aber Sie können die Backup-Appliance auch manuell einschalten, beispielsweise um das Kennwort zu ändern.

Voraussetzungen

Bevor Sie die Backup-Appliance einschalten, müssen Sie Folgendes durchführen:„Installieren des Client-Plug-Ins“, auf Seite 17 und „Installieren der Backup-Appliance“, auf Seite 18. Das Verwenden nicht übereinstimmender Versionen des Plug-Ins wird nicht unterstützt und kann zu Fehlern führen. Das Plug-In nimmt fälschlicherweise an, dass die Backup-Appliance nicht eingeschaltet ist.

Verwenden Sie vCenter Server, um sicherzustellen, dass die Zeitzoneninformationen beim ersten Einschalten der Backup-Appliance korrekt sind. Nach dem ersten Einschalten der Backup-Appliance werden die Zeitzoneninformationen 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.

Weiter

Wenn Sie die Backup-Appliance herunterfahren oder neu starten müssen, sollten Sie dies nicht tun, solange Sicherungen laufen. Bevor Sie die Appliance herunterfahen, halten Sie alle Sicherungen mithilfe des Data Recovery-Clients an, warten Sie, bis die Sicherungen angehalten wurden, und fahren Sie anschließend die Appliance herunter.

Konfigurieren der Backup-Appliance

Sie können über die Webschnittstelle die Backup-Appliance neu starten oder Netzwerkeinstellungen vornehmen. Falls die Backup-Appliance über vCenter Server bereitgestellt wurde, wird die Zeitzone der Backup-Appliance automatisch konfiguriert. Falls die Backup-Appliance über ESX/ESXi Server bereitgestellt wurde, müssen Sie die Zeitzone möglicherweise konfigurieren.

Voraussetzungen

Stellen Sie vor der Konfiguration der Backup-Appliance sicher, dass sie eingeschaltet und die aktuelle Version des Client-Plug-Ins installiert ist.

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 Clusters]** im vSphere-Client gibt der Status für VMware Tools der Data Recovery-Appliance an, dass sie nicht von vSphere verwaltet wird. Aktualisieren Sie die VMware Tools nicht auf der Data Recovery-Appliance. Wenn der Status „Nicht verwaltet“ lautet, bedeutet dies, dass die Appliance nicht von vSphere, sondern von Data Recovery verwaltet wird.

Backup-Appliance mit vCenter Server verbinden

Die Backup-Appliance von VMware Data Recovery muss mit dem vCenter Server verbunden sein, um automatische Aufgaben durchführen zu können, wie z. B. automatische Sicherungen und Zurückgewinnungsvorgänge. Schalten Sie die Backup-Appliance ein, bevor Sie sie verbinden.

Voraussetzungen

Wenn eine Backup-Appliance eingeschaltet wird, wird sie in der Regel automatisch mit einem vCenter Server verbunden, aber Sie müssen diesen Vorgang möglicherweise manuell abschließen. Um die Backup-Appliance zu verbinden, können Sie entweder den Namen der virtuellen Maschine oder die IP-Adresse verwenden. Zur Verwendung eines Namens benötigen Sie einen Namensauflösungsdienst und einen eindeutigen Namen für die Backup-Appliance. Wenn Ihre Umgebung über keinen Namensauflösungsdienst verfügt oder mehrere Backup-Appliances desselben Namens hat, schlägt die Verbindung möglicherweise fehl. Geben Sie in einem solchen Fall die IP-Adresse ein und versuchen Sie es erneut.

Vorgehensweise

1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]**.

2 Wählen Sie die Backup-Appliance aus der Bestandsliste im linken Bereich aus. Die Namen der Backup-Appliances werden fett dargestellt, um die Auswahl zu erleichtern. Sie können alternativ den Namen der virtuellen Maschine oder die IP-Adresse der Backup-Appliance eingeben. Klicken Sie auf **[Verbinden]**.

   - Falls dies das erste Mal ist, dass ein vSphere-Client eine Verbindung zur Backup-Appliance herstellt, wird der Assistent automatisch gestartet. Führen Sie den Assistenten vollständig aus, wie in „Verwenden des Assistenten für erste Schritte“, auf Seite 26 beschrieben.

3 Wählen Sie auf der Registerkarte **[Konfiguration]** die Option **[Backup-Appliance]** aus.

4 Klicken Sie auf den Link **[vCenter Server- oder ESX/ESXi-Host-Anmeldedaten festlegen]**.

5 Geben Sie den Benutzernamen und das Kennwort für vCenter ein und klicken Sie auf **[Übernehmen]**. Die Appliance speichert die zum Herstellen einer Verbindung mit vCenter Server erforderlichen Informationen, damit Sicherungs- und Wiederherstellungsvorgänge durchgeführt werden können.

Die Backup-Appliance ist jetzt mit dem vCenter Server verbunden und die Sicherungen können nun vorgenommen werden.

Weiter

Als Nächstes können Sie Sicherungsaufgaben erstellen, wie in „Verwenden des Assistenten für erste Schritte“, auf Seite 26 oder „Verwenden von Sicherungsaufgaben“, auf Seite 26 beschrieben.

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“, auf Seite 25 beschriebenen Vorgang durchführen. Der Assistent für erste Schritte wird nach dem erstmaligen Verbinden mit der Backup-Appliance automatisch gestartet, wobei Sie mit Schritt 4 beginnen.

Vorgehensweise

1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]** .

2 Falls dies nicht das erste Mal ist, dass ein Verbindung zur Backup-Appliance hergestellt wird, starten Sie den Assistenten für erste Schritte, indem Sie die Registerkarte **[Konfiguration]** auswählen und auf **[Assistent für Erste Schritte]** klicken.

3 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.

4 Wählen Sie auf der Seite „Sicherungsziel“ aus der Auswahlliste ein Ziel für die Sicherung aus.

5 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 formatierten Festplatte 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. Das Kennwort für CIFS-Freigaben ist auf maximal 64 Zeichen beschränkt und muss dem Standard „Latin 1“ (ISO 8859-1) entsprechen. Doppelbyte-Zeichen werden nicht unterstützt.

6 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 26 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.

Data Recovery verwendet das Sicherungsfenster zum Erstellen neuer Sicherungen und die Aufbewahrungsrichtlinie zum Entfernen bestimmter älterer Sicherungen. Weitere Informationen darüber, wie der Deduplizierungsspeicher Integritätsprüfungen verarbeitet und wie Zurückgewinnungsvorgänge diese Funktionalität unterstützen, finden Sie unter „Vorteile des Deduplizierungsspeichers“, auf Seite 10.

Virtuelle Maschinen

Geben Sie Erfassungen virtueller Maschinen an, z. B. alle virtuellen Maschinen in einem Datencenter, oder wählen Sie einzelne virtuelle Maschinen aus. Wenn Sie den gesamten Ressourcenpool, einen Host, ein Datencenter 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.

HINWEIS Das Verwenden von Data Recovery zum Sichern der Backup-Appliance von Data Recovery wird nicht unterstützt.

Ziel

Sie können Sicherungen in VMDKs, auf RDMs oder auf Netzwerkfreigaben 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 finden Sie unter „Hinzufügen einer Netzwerkfreigabe“, auf Seite 29. VMDKs und RDMs müssen zum Speichern von Sicherungen formatiert werden. Sie können Ziele formatieren, die noch nicht formatiert bzw. partitioniert wurden. Weitere Informationen finden Sie unter „Formatieren eines Volumes“, auf Seite 29.

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 Aufbewahrungsrichtline auswählen oder eine eigene Richtlinie erstellen. Weitere Informationen zum Bewerten unterschiedlicher Sicherungszeiträume finden Sie unter Tabelle 1-3.

Wenn der Deduplizierungsspeicher weniger als 80 % gefüllt ist, wird die Aufbewahrungsrichtlinie einmal pro Woche ausgeführt. Wenn der Deduplizierungsspeicher mehr als 80 % gefüllt ist, wird die Aufbewahrungsrichtlinie einmal pro Tag ausgeführt. Wenn der Deduplizierungsspeicher voll ist, wird die Aufbewahrungsrichtlinie sofort ausgeführt, sofern sie innerhalb der letzten 12 Stunden nicht ausgeführt wurde.

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 26 beschrieben.

Vorgehensweise

1 Wählen Sie im vSphere-Client **[Home] > [Lösungen und Anwendungen] > [VMware Data Recovery]** und klicken Sie auf **[Verbinden]** .

2 Klicken Sie auf die Registerkarte **[Sicherung]** und klicken Sie auf **[Neu]** , um den Assistenten für Sicherungsaufgaben zu starten.

3 Übernehmen Sie den Namen auf der Seite „Name“ oder geben Sie einen anderen Namen ein und klicken Sie anschließend auf **[Weiter]** .

4 Wählen Sie auf der Seite „Virtuelle Maschinen“ einzelne virtuelle Maschinen oder Container aus, die zu sichernde virtuelle Maschinen enthalten, und klicken Sie auf **[Weiter]** .

5 Geben Sie auf der Seite „Ziel“ ein Speicherziel ein und klicken Sie auf **[Weiter]** .

6 Akzeptieren Sie auf der Seite „Sicherungsfenster“ die Standardzeiten oder geben Sie alternative Sicherungsfenster an und klicken Sie auf **[Weiter]** .

7 Akzeptieren Sie auf der Seite „Aufbewahrungsrichtlinie“ die standardmäßige Aufbewahrungsrichtlinie oder geben Sie eine alternative Aufbewahrungsrichtlinie an und klicken Sie auf **[Weiter]** .

8 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. Beispiele für eine gültige URL sind `\\192.168.12.1\C$` oder `\\MyNetworkShare\MySharedDirectory`.
- Benutzername - der Benutzername eines Kontos mit den erforderlichen Schreibberechtigungen für die Netzwerkfreigabe.
- Kennwort - Das Kennwort für das Benutzerkonto. Bei älteren Versionen von VMware Data Recovery unterliegen möglicherweise die Kennwortlänge und die Verwendung von Nicht-ASCII-Zeichen Einschränkungen.

Informationen zum Hinzufügen einer Festplatte zur Backup-Appliance finden Sie unter „Hinzufügen einer Festplatte zur Backup-Appliance“, auf Seite 19.

Formatieren eines Volumes

VMware Data Recovery kann Sicherungen auf VMDKs, RDMs und Netzwerkvolumes 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.

Jetzt sichern

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 worden sind, werden durch die Funktion „Jetzt sichern“ nicht gesichert.

Voraussetzungen

Bevor Sie die Option „Jetzt sichern“ 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]** und klicken Sie auf **[Verbinden]** .

2 Klicken Sie auf die Registerkarte **[Sicherung]** , klicken Sie mit der rechten Maustaste auf eine Sicherungsaufgabe, klicken Sie auf **[Jetzt sichern]** und wählen Sie entweder **[Alle Quellen]** oder **[Veraltete Quellen]** .

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.

Markieren von Wiederherstellungspunkten zum Entfernen oder Sperren

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]** und klicken Sie auf **[Verbinden]** .

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. Um das sofortige Löschen der Wiederherstellungspunkte zu erzwingen, starten Sie eine Integritätsprüfung manuell.

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 und den Ort der Wiederherstellung angeben.

Quellauswahl

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 die Erfassungen virtueller Maschinen angeben, z. B. alle virtuellen Maschinen in einem Datencenter. Es ist möglich, virtuelle Maschinen und VMDK-Dateien an andere Speicherorte zu verschieben. 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 Wiederherstellungsaufgabe. 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.

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 Stellen Sie eine Verbindung mit der Backup-Appliance her.

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.

Erstellen einer Probe-Wiederherstellung von der letzten Sicherung

Bei der Probe-Wiederherstellung von der letzten Sicherung wird eine neue virtuelle Maschine von der letzten Sicherung der ausgewählten virtuellen Maschine erstellt. Führen Sie eine Probe-Wiederherstellung der letzten Sicherung durch, um zu bestätigen, dass eine virtuellen Maschine erwartungsgemäß gesichert und dass ein erfolgreicher Wiederherstellungsvorgang durchgeführt werden kann.

Voraussetzungen

Bevor Sie eine Probe-Wiederherstellung der letzten Sicherung 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 Stellen Sie eine Verbindung mit der Backup-Appliance her.

3 Klicken Sie mit der rechten Maustaste auf eine virtuellen Maschine, für die eine Sicherung verfügbar ist, und wählen Sie **[Probe-Wiederherstellung von letzter Sicherung]** .

Der Wiederherstellungsassistent für virtuelle Maschinen wird mit der geöffneten Seite „Quellen“ angezeigt. Die neueste Sicherung der VM, die in der Bestandslistenstruktur ausgewählt wurde, wird standardmäßig verwendet.

4 Überprüfen Sie auf der Seite „Quellen“ die vorgeschlagenen Einstellungen. Sie können die angegebenen Einstellungen bei Bedarf ändern. Klicken Sie auf **[Weiter]** .

Die Seite „Ziele“ wird angezeigt.

5 Überprüfen Sie auf der Seite „Ziele“ die vorgeschlagenen Einstellungen. Sie können die angegebenen Einstellungen bei Bedarf ändern. Klicken Sie auf **[Weiter]** .

Eine neue virtuelle Maschine mit dem Namenszusatz „Probe“ wird standardmäßig an demselben Speicherort wie die virtuelle Quellmaschine erstellt. Sie können auf dieser Seite die neue virtuelle Maschine umbenennen und den Speicherort ändern, an dem sie erstellt wird.

Die Seite „Bereit zum Abschließen“ wird angezeigt.

6 Klicken Sie auf **[Wiederherstellen]** , um die Probe-Wiederherstellung von der letzten Sicherung 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 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.

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 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.

Die Verwendung von FLR zum Zugriff auf Dateien in Wiederherstellungspunkten stellt nur eine Möglichkeit dar, deren Inhalte zu lesen. Verwenden Sie FLR nicht, um den Inhalt eines Wiederherstellungspunkts zu 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. Ebenso ist es möglich, die in Wiederherstellungspunkten enthaltenen Dateien zu öffnen und Änderungen daran vorzunehmen sowie sie anschließend zu speichern und zu schließen. Die im Deduplizierungsspeicher im Wiederherstellungspunkt abgelegten Daten bleiben jedoch unverändert. Demzufolge gehen alle an den Dateien im Wiederherstellungspunkt vermeintlich vorgenommenen Änderungen

verloren, sobald FLR beendet wird. Damit diese Änderungen gespeichert werden, müssen Sie entweder eine lokale Kopie der entsprechenden Datei außerhalb des Wiederherstellungspunkts erstellen und bearbeiten oder den Inhalt des Wiederherstellungspunkts bearbeiten, indem Sie die virtuelle Maschine starten und die Dateien in der virtuellen Maschine bearbeiten.

Wenn die Backup-Appliance andere Aufgaben erledigt, beispielsweise Sicherungs- oder Wiederherstellungsaufgaben ausführt, kann sich das Herstellen einer Verbindung mit FLR möglicherweise verzögern. Alle Wiederherstellungspunkte werden angezeigt, aber FLR kann nur Wiederherstellungspunkte für kompatible virtuelle Maschinen mounten. Einige Dateisysteme können möglicherweise von einer bestimmten virtuellen Maschine nicht gemountet werden. FLR verwendet zum Lesen des Inhalts von Wiederherstellungspunkten das Betriebssystem, auf dem es ausgeführt wird. Wenn das Betriebssystem der virtuellen Maschine, unter dem FLR ausgeführt wird, das Dateisystem des Wiederherstellungspunkts nicht lesen kann, ist der Zugriff auf diesen Wiederherstellungspunkt somit nicht möglich. Wenn beispielsweise eine Linux-Maschine nicht in der Lage ist, NTFS-Dateien zu lesen, schlägt der Versuch, auf einer virtuellen Maschine unter Linux den Inhalt des Wiederherstellungspunkts einer virtuellen Windows-Maschine mithilfe von FLR zu lesen, wahrscheinlich fehl.

Beim Mounten eines Wiederherstellungspunkts wird auf der lokalen Festplatte der virtuellen Maschine ein Root-Mount-Punkt erstellt. Der Mount-Punkt ist ein Verzeichnis, das denselben Namen wie das Datum der Wiederherstellungspunkte im langen Datumsformat 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.

Wenn die Wiederherstellungsvorgänge auf Dateiebene abgeschlossen sind, können Sie die Wiederherstellungspunkte unmounten. Um ein Unmounten einzelner Wiederherstellungspunkte in Windows durchzuführen, wählen Sie einen Wiederherstellungspunkt aus und klicken Sie auf **[Unmounten]** . Sie können auch ein Unmounten aller Wiederherstellungspunkte durchführen, indem Sie auf **[Alle unmounten]** klicken. Geben Sie zum Unmounten der Wiederherstellungspunkte unter Verwendung von FLR in Linux den Befehl `unmount` ein.

Nach dem Beenden von FLR werden alle Ressourcen entfernt, die zum Aktivieren der FLR-Funktionalität extrahiert wurden. Wenn Mount-Punkte weiterhin belegt sind und FLR vorhanden ist, müssen Sie möglicherweise eine manuelle Bereinigung dieser Ressourcen durchführen. Weitere Informationen zum manuellen Bereinigen belegter Ressourcen beim Unmounten finden Sie in den Versionshinweisen.

Der FLR-Client kann von Benutzern mit Administratorrechten auf virtuellen Windows- oder mit sudo-Berechtigungen auf virtuellen Linux-Maschinen verwendet werden. Auf virtuellen Windows-Maschinen benötigt der FLR-Client das .NET 2.0 Framework oder höher. Auf virtuellen Linux-Maschinen benötigt der FLR-Client die 32-Bit-Version von FUSE 2.5 oder höher. Beachten Sie, dass bei Linux die 32-Bit-Version erforderlich ist, und zwar unabhängig davon, ob die verwendete virtuelle Maschine eine 32-Bit- oder 64-Bit-Maschine ist. 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. Stellen Sie sicher, dass die FLR-Version mit der Backup-Appliance-Version übereinstimmt. Eine ältere FLR-Version schlägt möglicherweise fehl. FLR funktioniert nicht mit Wiederherstellungspunkten für virtuelle Maschinen, die GUID-Partitionstabellen (GPT) verwenden. FLR kann auf virtuellen Maschinen mit den folgenden Betriebssystemen installiert und ausgeführt werden:

- Virtuelle Linux-Maschinen (32- oder 64-Bit):
  - Red Hat Enterprise Linux (RHEL) 5.4/CentOS 5.4
  - Red Hat 4.8/CentOS 4.8
  - Ubuntu 8.04

- Ubuntu 8.10
- Ubuntu 9.04

- Virtuelle Windows-Maschinen:
  - Windows XP
  - Windows Vista
  - Windows 7
  - Windows Server 2003
  - Windows Server 2008

HINWEIS FLR wird von physischen Maschinen nicht unterstützt.

Verwenden von FLR in Windows

Verwenden Sie FLR auf einer virtuellen Windows-Maschine, indem Sie die ausführbare Datei von FLR auf diese 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 ausführbare Datei des FLR-Clients von der Installations-CD unter `<Laufwerksbuchstabe>:\WinFLR\VMwareRestoreClient.exe` auf die virtuelle Windows-Maschine, die den FLR-Client verwenden wird.

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

Wiederherstellen von Dateien mithilfe des FLR-Standardmodus in Windows

Verwenden Sie den FLR-Client in einer virtuellen Windows-Maschine, 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

Bevor Sie Dateien wiederherstellen, führen Sie die in „Verwenden von FLR in Windows“, auf Seite 35 beschriebenen Schritte aus. FLR stellt über Port 22024 eine Verbindung zur Backup-Appliance her. Wenn sich zwischen dem FLR-Client und ESX/ESXi eine Firewall befindet, muss Port 22024 offen sein, damit der Zugriff auf Wiederherstellungspunkte mithilfe von FLR möglich ist. Um mit Dateien auf anderen virtuellen Maschinen zu arbeiten, verwenden Sie den erweiterten Modus, wie in „Wiederherstellen von Dateien mithilfe des erweiterten FLR-Modus in Windows“, auf Seite 36 beschrieben.

Vorgehensweise

1 Starten Sie die virtuelle Maschine, in der Sie FLR verwenden werden.

2 Doppelklicken Sie auf die ausführbare FLR-Datei.

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 **[Anmelden]** .

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 in Windows

Verwenden Sie auf einer virtuellen Windows-Maschine FLR im erweiterten Modus, um von Wiederherstellungspunkten mehrerer virtueller Maschinen aus auf Dateien zuzugreifen.

Voraussetzungen

FLR stellt über Port 22024 eine Verbindung zur Backup-Appliance her. Wenn sich zwischen dem FLR-Client und ESX/ESXi eine Firewall befindet, muss Port 22024 offen sein, damit der Zugriff auf Wiederherstellungspunkte mithilfe von FLR möglich ist.

Vorgehensweise

1 Starten Sie die virtuelle Maschine, in der Sie FLR verwenden werden.

2 Doppelklicken Sie auf die ausführbare FLR-Datei.

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 Klicken Sie bei ausgewähltem gemountetem Wiederherstellungspunkt auf **[Durchsuchen]** , um eine Instanz von Windows Explorer am Speicherort der gemounteten Dateien zu öffnen.

7 Sie können von der virtuellen Maschine aus jede gewünschte Datei durchsuchen und sie wiederherstellen.

8 Ist das Durchsuchen und Wiederherstellen von Dateien beendet, klicken Sie auf **[Alle unmounten]** und beenden Sie FLR.

Verwenden von FLR in Linux

Verwenden Sie FLR auf einer virtuellen Linux-Maschine, indem Sie die ausführbare Datei von FLR auf diese virtuelle Maschine kopieren.

Voraussetzungen

Auf virtuellen Linux-Maschinen benötigt der FLR-Client die installierte 32-Bit-Version von FUSE 2.5 oder höher. Dies ist eine Anforderung für virtuelle Linux-Maschinen sowohl für 32-Bit als auch für 64-Bit. Auf Linux benötigt FLR „fuser“ und „LVM“. FLR verwendet „fuser“ bei Unmount-Versuchen, um zu ermitteln, ob Mounts belegt sind, und verwendet LVM zum Zugriff auf LVM-Volumes. Damit diese Dienstprogramme zur Verfügung stehen, müssen sie installiert und zur Systemumgebungsvariablen PATH hinzugefügt worden sein.

Vorgehensweise

1 Legen Sie die Data Recovery-Installations-CD ein.

2 Kopieren Sie das FLR-Client-Archiv `LinuxFLR/VMwareRestoreClient.tgz` auf der Installations-CD auf die virtuelle Maschine, die den FLR-Client verwenden soll.

3 Extrahieren Sie das Archiv mit dem Befehl `tar xzvf VMwareRestoreClient.tgz`.

4 Navigieren Sie zum Verzeichnis `VMwareRestoreClient` und rufen Sie FLR auf, indem Sie `./VdrFileRestore` ausführen.

   Stellen Sie sicher, dass Sie „VdrFileRestore“ und nicht „vdrFileRestore“ verwenden. Dies sind zwei unterschiedliche ausführbare Programme. VdrFileRestore ist ein Wrapper-Skript, das vdrFileRestore enthält, und bietet zusätzliche Vorteile, wie z. B. das Einrichten korrekter Bibliotheksabhängigkeiten und das Sicherstellen, dass die richtige FUSE-Installation verfügbar ist.

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

Wiederherstellen von Dateien mithilfe des FLR-Standardmodus in Linux

Verwenden Sie den FLR-Client in einer virtuellen Linux-Maschine, 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. Eine vollständige Liste der für VdrFileRestore zur Verfügung stehenden Befehlsoptionen finden Sie in der Readme-Datei, die sich in der Linux-FLR-tgz-Datei befindet.

Voraussetzungen

Bevor Sie die Dateien wiederherstellen, führen Sie die unter „Verwenden von FLR in Linux“, auf Seite 37 beschriebenen Schritte aus. FLR stellt über Port 22024 eine Verbindung zur Backup-Appliance her. Wenn sich zwischen dem FLR-Client und ESX/ESXi eine Firewall befindet, muss Port 22024 offen sein, damit der Zugriff auf Wiederherstellungspunkte mithilfe von FLR möglich ist. Um mit Dateien auf anderen virtuellen Maschinen zu arbeiten, verwenden Sie den erweiterten Modus, wie in „Wiederherstellen von Dateien mithilfe des erweiterten FLR-Modus in Linux“, auf Seite 38 beschrieben.

Vorgehensweise

1 Starten Sie die virtuelle Maschine, in der Sie FLR verwenden werden.

2 Führen Sie `VdrFileRestore` aus und geben Sie die IP-Adresse oder den Namen der Data Recovery-Appliance anhand der Syntax (`–a | ––appliance <ip | dns name>`) an. Ein Beispiel hierfür wäre der Befehl: **`./VdrFileRestore –a 10.0.1.124`**

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

3 Wählen Sie einen Wiederherstellungspunkt aus.

   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.

4 Sie können von der virtuellen Maschine aus jede gewünschte Datei durchsuchen und sie wiederherstellen.

5 Ist das Durchsuchen und Wiederherstellen von Dateien beendet, geben Sie den Befehl `unmount` ein und FLR wird beendet.

Wiederherstellen von Dateien mithilfe des erweiterten FLR-Modus in Linux

Verwenden Sie auf einer virtuellen Linux-Maschine FLR im erweiterten Modus, um von Wiederherstellungspunkten mehrerer virtueller Maschinen aus auf Dateien zuzugreifen. Eine vollständige Liste der für VdrFileRestore zur Verfügung stehenden Befehlsoptionen finden Sie in der Readme-Datei, die sich in der Linux-FLR-tgz-Datei befindet.

Voraussetzungen

FLR stellt über Port 22024 eine Verbindung zur Backup-Appliance her. Wenn sich zwischen dem FLR-Client und ESX/ESXi eine Firewall befindet, muss Port 22024 offen sein, damit der Zugriff auf Wiederherstellungspunkte mithilfe von FLR möglich ist.

Vorgehensweise

1 Starten Sie die virtuelle Maschine, in der Sie FLR verwenden werden.

2 Führen Sie VdrFileRestore aus. Sie müssen mindestens eine IP-Adresse bzw. einen Namen für die Data Recovery-Appliance angeben (`–a <ip | dns name>`), eine IP-Adresse / einen Namen von vCenter Server (`–s <ip | dns name>`), einen Benutzernamen eines Benutzers mit administrativen vCenter-Berechtigungen (`–u <Benutzer>`) und ein Kennwort für den zuvor angegebenen administrativen Benutzer (`–p | ––password <Kennwort>`). Ein Beispiel hierfür wäre der Befehl: **`./VdrFileRestore –a 10.0.1.124 –s 10.1.1.78 –u administrator –p mypw`**.

   FLR zeigt eine Liste aller verfügbaren Wiederherstellungspunkte für alle gesicherten virtuellen Maschinen auf der Data Recovery-Appliance an, mit der Sie verbunden sind.

3 Wählen Sie einen Wiederherstellungspunkt aus. 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.

4 Sie können von der virtuellen Maschine aus jede gewünschte Datei durchsuchen und sie wiederherstellen.

5 Ist das Durchsuchen und Wiederherstellen von Dateien beendet, geben Sie den Befehl `unmount` ein und FLR wird beendet.

Fehlerbehebung für VMware Data Recovery

Falls Sie Verbindungs- oder Konfigurationsprobleme mit Data Recovery haben, können Sie versuchen, die Fehler anhand der vorgeschlagenen Fehlerbehebungslösungen zu beheben.

Tabelle 3-4. Fehlerbehebung für VMware Data Recovery

Problem	Mögliche Lösung
Es kann keine Verbindung zur Backup-Appliance hergestellt werden.	Für dieses Problem gibt es mehrere mögliche Lösungen. Stellen Sie zunächst sicher, dass: ■ Die IPv4-Adresse der Data Recovery-Appliance korrekt eingegeben wurde. ■ Die Version des Client-Plug-Ins mit der Version der Backup-Appliance übereinstimmt. Die Verwendung älterer Client-Plug-Ins führt möglicherweise zu Fehlern, da sie fälschlicherweise annehmen, dass die Appliance nicht eingeschaltet ist. ■ Die virtuelle Sicherungsmaschine eingeschaltet ist. ■ Der ESX/ESXi Server, der die Backup-Appliance hostet, befindet sich im Netzwerk. Bei DNS-Namensauflösungen können Komplikationen auftreten. Diese Probleme werden möglicherweise dadurch gelöst, dass die sich aus DNS-Namensauflösungen ergebenden Probleme behoben werden oder indem der ESX/ESXi Server unter Verwendung der IP-Adresse hinzugefügt wird.
Data Recovery schlägt beim Erstellen von Sicherungen fehl mit dem Fehler `disk full error –1115`, 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/ESXi Server bereitgestellt wird und der Appliance die VMDK zugewiesen ist. NFS-Freigaben können der Appliance nicht direkt zugeordnet werden.
Data Recovery ist abgestürzt und der Status von Data Recovery ist unbekannt.	Weil der Status der Appliance im Deduplizierungsspeicher gespeichert ist, kann sie wiederhergestellt werden. Installieren Sie die Data Recovery-Appliance auf dem ESX/ESXi-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.

Tabelle 3-4. Fehlerbehebung für VMware Data Recovery (Fortsetzung)

Problem	Mögliche Lösung
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. ■ Die Prozessornutzung darf nicht über 90 % liegen, damit einzelne Sicherungen gestartet werden können, und nicht über 80 %, damit mehrere Sicherungen gestartet werden können. ■ Der Datenspeicher, auf dem sich virtuelle Maschinen befinden, muss über mindestens 10 GB Speicherplatz zur Indizierung und Verarbeitung von Wiederherstellungspunkten und über 5 GB verfügbaren Speicherplatz für jede zu sichernde virtuelle Maschine verfügen. Um beispielsweise acht virtuelle Maschinen gleichzeitig zu sichern, die sich auf einem Datenspeicher befinden, sollten 50 GB Speicherplatz verfügbar sein, wobei 10 GB zur Indizierung und Verarbeitung und 40 GB für die virtuellen Maschinen vorgesehen sind. Falls eine dieser Einschränkungen nicht eingehalten wird, werden keine neuen Aufgaben gestartet.
Der Tools-Status für die Backup-Appliance von Data Recovery wird als „Nicht verwaltet“ aufgelistet.	Dies ist erwartetes Verhalten. Die Backup-Appliance wird nicht von vCenter 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.

Tabelle 3-4. Fehlerbehebung für VMware Data Recovery (Fortsetzung)

Problem	Mögliche Lösung
Sicherungen schlagen mit Fehler -3960 fehl (virtuelle Maschine kann nicht stillgelegt werden)	Dies kann von veralteten VMware Tools verursacht werden. Stellen Sie sicher, dass die zu sichernde virtuelle Maschine über die korrekte Version von VMware Tools verfügt, die installiert und auf dem neuesten Stand sind. Wenn die korrekte Version der Tools nicht installiert ist, deinstallieren Sie die vorhandenen Versionen von VMware Tools und installieren Sie anschließend die korrekte Version von VMware Tools. Dadurch ist das Problem möglicherweise behoben. Falls die Sicherungen weiterhin fehlschlagen, versuchen Sie, manuell einen Snapshot der virtuellen Maschine zu erstellen, wobei die Option **[Snapshot des Arbeitsspeichers der virtuellen Maschine erstellen]** deaktiviert und die Option **[Gast-Dateisystem stilllegen]** aktiviert sein soll. Überprüfen Sie bei virtuellen Maschinen unter Windows 2003 und höher, ob VSS-Meldungen und programmierbezogene Meldungen im System- und Anwendungsereignisprotokoll festgehalten werden. Überprüfen Sie, ob ntbackup oder Windows Server Backup in der virtuellen Maschine verwendet werden kann, um Sicherungen unter Verwendung von VSS im Gast durchzuführen.
Nach dem Herstellen der Verbindung werden nicht alle Bestandslistenelemente sofort angezeigt.	Falls eine große Anzahl an Bestandslistenelementen vorhanden ist, werden einige der Elemente möglicherweise nicht sofort in der Data Recovery-Benutzerschnittstelle angezeigt. Dies kann passieren, wenn die Data Recovery-Appliance erst vor wenigen Minuten eingeschaltet wurde. Warten Sie in diesem Fall einige Minuten, damit alle Bestandslistenelemente abgerufen werden können, bevor Sie Sicherungsaufgaben erstellen oder ändern.
Sicherungsaufgaben werden nicht wie erwartet gestartet.	Wenn die Backup-Appliance während des Verarbeitens von Aufgaben heruntergefahren wurde, werden Aufgaben möglicherweise nicht wieder gestartet, wenn die Appliance neu gestartet wird. Um diese Situation zu vermeiden, halten Sie alle Sicherungen mithilfe des Data Recovery-Clients an, warten Sie, bis die Sicherungen angehalten wurden, und fahren Sie anschließend die Appliance herunter.

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 Protokollerstellung 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 Freigeben, 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 3-5. Einstellungen von „datarecovery.ini“

Option	Beschreibung	Beispiel	Bereich	Standard
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		20
DisableHotaddCopy	Deaktiviert bei einer Einstellung von 1 das SCSI Hot-Add.	DisableHotaddCopy=1	0-1.	0
DisableNetworkCopy	Deaktiviert bei einer Einstellung von 1 die Netzwerkkopie.	DisableNetworkCopy=1	0-1.	0
SetVCBLogging	Die interne Protokollierungsstufe für das VMware Consolidated Backup API.	SetVCBLogging=7	0-7. 7 ist die ausführlichste Protokollierungsstufe.	5
SetRAPILogging	Die interne Protokollierungsstufe für das Data Recovery API.	SetRAPILogging=7	0-7. 7 ist die ausführlichste Protokollierungsstufe.	5

Tabelle 3-5. Einstellungen von „datarecovery.ini“ (Fortsetzung)

Option	Beschreibung	Beispiel	Bereich	Standard
SetEngineLogging	Die interne Protokollierungsstufe für die Backup-Appliance von Data Recovery.	SetEngineLogging=7	0-7. 7 ist die ausführlichste Protokollierungsstufe.	5
SetDevicesLogging	Die interne Protokollierungsstufe für den Deduplizierungsvorgang.	SetDevicesLogging=7	0-7. 7 ist die ausführlichste Protokollierungsstufe.	5
SetAppLogging	Die interne Protokollierungsstufe für die allgemeine Anwendungslogik.	SetAppLogging=7	0-7. 7 ist die ausführlichste Protokollierungsstufe.	5
SetVolumesLogging	Die interne Protokollierungsstufe für die Interaktionen zwischen virtuellen Maschinen und Volumes.	SetVolumesLogging=7	0-7. 7 ist die ausführlichste Protokollierungsstufe.	5
SetBackupSetsLogging	Die interne Protokollierungsstufe für Katalogvorgänge.	SetBackupSetsLogging=7	0-7. 7 ist die ausführlichste Protokollierungsstufe.	5
IntegrityCheckInterval	Das Intervall in Tagen für Integritätsprüfungen.	IntegrityCheckInterval=7	0-7.	1
BackupRetryInterval	Die Anzahl an Minuten, die die Backup-Appliance wartet, bevor eine fehlgeschlagene Sicherung erneut durchgeführt wird.	BackupRetryInterval=20		30
RetentionPolicyInterval	Die Anzahl an Tagen, bevor Speicherplatz im Deduplizierungsspeicher zurückgewonnen wird.	RetentionPolicyInterval=4	1-7.	1
DedupeCheckOnRecatalog	Schließt bei einer Einstellung von 1 nach einer Katalogaktualisierung eine Integritätsprüfung ab.	DedupeCheckOnRecatalog=1	0-1.	0

Tabelle 3-5. Einstellungen von „datarecovery.ini“ (Fortsetzung)

Option	Beschreibung	Beispiel	Bereich	Standard
EnableFileRestore	Deaktiviert bei einer Einstellung von 1 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.	1
MaxBackupRestoreTasks	Die maximale Anzahl gleichzeitiger Sicherungen und Wiederherstellungen.	MaxBackupRestoreTasks=4	1-8.	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-Verbindungsprotokoll - 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 Protokollierungsstufe die Umschalttaste gedrückt und klicken Sie auf **[Protokoll aktualisieren]** .

Die Protokollierungsstufensteuerung wird angezeigt.

6 Klicken Sie auf den Auf- oder Abwärtspfeil für die **[Protokollierungsstufe]** , 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 Klicken Sie auf das Textfeld „IP-Adresse“.

3 Drücken Sie die Tastatursequenz 'Strg-Alt-G-G'.

Die Client-Verbindungsprotokolle werden angezeigt.

Index