

# Sicherungshandbuch für virtuelle Maschinen

ESX Server 3.5, ESX Server 3i, Version 3.5  
VirtualCenter 2.5



Sicherungshandbuch für virtuelle Maschinen

Überarbeitung: 20080430

Artikelnummer: VI-DEU-Q208-505

Die neueste technische Dokumentation finden Sie auf unserer Website unter:

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

Auf der VMware-Website finden Sie auch die neuesten Produktaktualisierungen.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese bitte an:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

© 2008 VMware, Inc. Alle Rechte vorbehalten. Geschützt durch mindestens eines der US-Patente Nr. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102 und 7,290,253. Weitere Patente sind angemeldet.

VMware, das VMware-Logo und -Design, Virtual SMP und VMotion sind eingetragene Marken oder Marken der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Inhalt

Über dieses Handbuch	7
<b>1 Sichern mit VMware Infrastructure</b>	<b>11</b>
Sicherungskonzepte	12
Welche Daten sollten gesichert werden?	12
Inhalte virtueller Maschinen	13
Zugreifen auf und Verwalten von Dateien virtueller Festplatten	14
Sicherungskomponenten und -verfahren	15
Verwendung herkömmlicher Sicherungsmethoden	16
Überlegungen zur herkömmlichen Sicherung	16
Sichern der ESX Server 3-Servicekonsole	17
Sichern von virtuellen Maschinen	17
Ausführen des Sicherungsclients auf einer virtuellen Maschine	18
Ausführen des Sicherungsclients über die ESX Server 3-Servicekonsole	20
Ausführen des Sicherungsservers auf einer virtuellen Maschine	22
Behandeln virtueller Maschinen als Dateien auf gemeinsam genutztem Speicher	22
Verwenden von VMware Consolidated Backup	23
<b>2 VMware Consolidated Backup</b>	<b>25</b>
Übersicht über VMware Consolidated Backup	26
Funktionsweise von VMware Consolidated Backup	26
Modelle zur Nutzung von VMware Consolidated Backup	27
Ablauf von VMware Consolidated Backup	30
Sicherungstypen	31
Sichern virtueller Maschinen auf Image-Ebene	32
Sichern virtueller Maschinen auf Dateiebene	32
Einschränkungen bei VMware Consolidated Backup	33
Software- und Hardwareanforderungen von Consolidated Backup	33
Einrichten von VMware Consolidated Backup	34
Konfigurieren von VMware ESX Server und virtuellen Maschinen zum Sichern	35

- Einrichten eines VCB-Proxys 35
  - Konfigurieren von Windows auf dem VCB-Proxy 36
  - Konfigurieren der Vernetzung auf dem VCB-Proxy 37
  - Konfigurieren der Drittanbieter-Software auf dem VCB-Proxy 38
  - Installieren von VMware Consolidated Backup 39
  - Installieren eines Integrationsmoduls für die Sicherungssoftware 39
  - Konfigurieren von VMware Consolidated Backup 39
  - Aktivieren der Verifizierung des SSL-Zertifikats 43
  - Konfigurieren von SAN 45
- Verwenden von VMware Consolidated Backup 46
  - Erstellen von Sicherungsrollen 46
  - Gruppieren virtueller Maschinen 47
  - Konfigurieren von Sicherungsaufträgen 48
  - Erstmalige Sicherung 49
- Erweiterte Konfigurationen 49
  - Ausführen benutzerdefinierter Skripts zum außer Betrieb nehmen 49
  - Abbrechen eines Sicherungsauftrags 51
  - Bereinigung nach misslungenem Sicherungsauftrag 51
- Aktualisieren von Consolidated Backup 52
- 3 Wiederherstellung und Rettung von Daten 53**
  - Wiederherstellen virtueller Maschinen mittels VMware Consolidated Backup 54
    - Verwenden von VMware Converter zum Wiederherstellen von Images virtueller Maschinen 55
    - Verwenden des Dienstprogramms vcbRestore zum Wiederherstellen virtueller Maschinen 55
    - Zentrales Wiederherstellen von Daten 55
    - Wiederherstellen von Daten in Gruppen 56
    - Direktes Wiederherstellen auf eine virtuelle Maschine 56
  - Datenwiederherstellung 56
- 4 Sicherungsszenarien und Fehlerbehebung 57**
  - Szenarien zur Sicherungsanwendung 58
  - Typisches Anwendungsszenario für Consolidated Backup 58
  - Fehlerbehebung 59
    - Ändern der Sicherungsrichtlinien nach ESX Server-Upgrades 59
    - Identifizieren von VMFS-Volumes in GUI der Sicherungssoftware 59

<b>A</b>	<b>Sichern und Wiederherstellen von virtuellen Maschinen mithilfe der Servicekonsole</b>	<b>61</b>
	Allgemeine Konfigurationseinstellungen für Consolidated Backup-Dienstprogramme	62
	Einstellungen der Konfigurationsdatei	62
	Sichern von virtuellen Maschinen	64
	Durchführen von Sicherungen	64
	Auswählen von virtuellen Maschinen	66
	Auswählen von virtuellen Maschinen mithilfe des DNS-Namens oder der IP-Adresse	66
	Auswählen von virtuellen Maschinen mithilfe des BIOS-UUIDs	66
	Auswählen von virtuellen Maschinen mithilfe von Managed Object References (MoRefs)	67
	Anzeigen von Informationen über virtuelle Maschinen	67
	Festlegen von Sicherungszielen	68
	Sichern in einem lokalen Verzeichnis	68
	Sichern auf einem Remoteserver	68
	Archivieren virtueller Maschinen	69
	Wiederherstellen von virtuellen Maschinen	69
	Wiederherstellen von virtuellen Maschinen am ursprünglichen Speicherort	70
	Wiederherstellen von virtuellen Maschinen an einem alternativen Speicherort	70
	Kopieren einer „catalog“-Datei	71
	Bearbeiten einer „catalog“-Datei	71
	Wiederherstellen von virtuellen Maschinen mithilfe einer alternativen „catalog“-Datei	73
	Nicht interaktiver Einsatz des Dienstprogramms vcbRestore	73
	Wiederherstellen virtueller Maschinen aus Archiven	74
<b>B</b>	<b>Wiederherstellen von virtuellen Maschinen der Version ESX Server 2.5.x unter ESX Server 3.x</b>	<b>75</b>
	Einstellen der Konfigurationsparameter	76
	Wiederherstellen von virtuellen Maschinen, die unter ESX Server 2.5.x gesichert wurden	77

Index	79
-------	----



# Über dieses Handbuch

---

Dieses Handbuch, das *Sicherungshandbuch für virtuelle Maschinen*, enthält Informationen zu verschiedenen Methoden, die Sie zur Durchführung von Sicherungs- und Wiederherstellungsaufgaben verwenden können. Es beschreibt außerdem die Einrichtung und Verwendung von VMware Consolidated Backup, einer empfohlenen Sicherungslösung von VMware Infrastructure 3 zur Durchführung täglicher Sicherungen für virtuelle Maschinen, die sich auf einem Fibre-Channel- oder iSCSI-SAN bzw. einem lokalen Speicher befinden.

Das *Sicherungshandbuch für virtuelle Maschinen* deckt sowohl ESX Server 3.5 als auch ESX Server 3i, Version 3.5, ab. Zur Vereinfachung der Erläuterung werden in diesem Buch die folgenden Produktbenennungskonventionen befolgt:

- Für Themen, die für ESX Server 3.5 spezifisch sind, wird in diesem Buch der Begriff „ESX Server 3“ verwendet.
- Für Themen, die für ESX Server 3i, Version 3.5, spezifisch sind, wird in diesem Buch der Begriff „ESX Server 3i“ verwendet.
- Für Themen, die für beide Produkte gelten, wird in diesem Buch der Begriff „ESX Server“ verwendet.
- Wenn die Bestimmung einer bestimmten Version für die Erläuterung wichtig ist, wird in diesem Buch für das jeweilige Produkt der vollständige Name samt Version angegeben.
- Wenn sich die Erläuterung auf alle Versionen von ESX Server für VMware Infrastructure 3 bezieht, wird in diesem Buch der Begriff „ESX Server 3.x“ verwendet.

## Zielgruppe

Zielgruppe dieses Handbuchs sind alle Personen, die Sicherungs- und Wiederherstellungsaufgaben mithilfe von VMware Infrastructure durchführen möchten. Die Informationen in diesem Handbuch sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit dem Betrieb virtueller Maschinen im Datacenter vertraut sind.

## Feedback zu diesem Dokument

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Bitte senden Sie Ihre Kommentare und Vorschläge an:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

## Dokumentation zu VMware Infrastructure

Die Dokumentation zu VMware Infrastructure umfasst die kombinierte Dokumentation zu VMware VirtualCenter und ESX Server.

## In Abbildungen verwendete Abkürzungen

In den Abbildungen, die in diesem Handbuch enthalten sind, werden die in [Tabelle 1](#) aufgeführten Abkürzungen verwendet.

**Tabelle 1.** Abkürzungen

<b>Abkürzung</b>	<b>Beschreibung</b>
Datenbank	VirtualCenter-Datenbank
Datenspeicher	Speicher für den verwalteten Host
Festplatte#	Speicherfestplatte für den verwalteten Host
Host $n$	Verwaltete VirtualCenter-Hosts
SAN	Storage Area Network-Datenspeicher (SAN), der von den verwalteten Hosts gemeinsam genutzt wird
Vrlg	Vorlage
Benutzer#	Benutzer mit Zugriffsberechtigungen
VC	VirtualCenter
VM#	Virtuelle Maschinen auf einem verwalteten Host

## Technischer Support und Schulungsressourcen

In den folgenden Abschnitten werden die verfügbaren technischen Supportressourcen beschrieben. Unter der folgenden Adresse haben Sie Zugang zu den neuesten Versionen dieses Handbuchs und anderen Büchern:

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

### Online- und Telefonsupport

Im Online-Support können Sie technische Unterstützung anfordern, Ihre Produkt- und Vertragsdaten abrufen und Produkte registrieren. Weitere Informationen finden Sie unter <http://www.vmware.com/support>.

Kunden mit entsprechenden Support-Verträgen erhalten über den telefonischen Support schnelle Hilfe bei Problemen der Prioritätsstufe 1. Weitere Informationen finden Sie unter [http://www.vmware.com/support/phone\\_support.html](http://www.vmware.com/support/phone_support.html).

### Support-Angebote

VMware stellt ein umfangreiches Support-Angebot bereit, um Ihre geschäftlichen Anforderungen zu erfüllen. Weitere Informationen finden Sie unter <http://www.vmware.com/support/services>.

### VMware Education Services

Die VMware-Kurse umfassen umfangreiche praktische Übungen, Fallbeispiele und Kursmaterialien, die zur Verwendung als Referenztools bei der praktischen Arbeit vorgesehen sind. Weitere Informationen zu den VMware Education Services finden Sie unter <http://mylearn1.vmware.com/mgrreg/index.cfm>.



# Sichern mit VMware Infrastructure

---

# 1

Sichern und Wiederherstellen von Daten sowie Notfallwiederherstellung sind einige der wichtigsten Vorgänge bei der Verwaltung von Datacentern. VMware® Infrastructure und VMware ESX Server bieten eine breite Palette von Lösungen für das Sichern und Wiederherstellen von Daten in spezifischen Umgebungen.

In dieser Einführung wird beschrieben, welche Ressourcen auf einem ESX Server-System gesichert werden sollten, und welche Optionen für die Sicherung zur Verfügung stehen.

Dieses Kapitel enthält die folgenden Abschnitte:

- [„Sicherungskonzepte“](#) auf Seite 12
- [„Welche Daten sollten gesichert werden?“](#) auf Seite 12
- [„Sicherungskomponenten und -verfahren“](#) auf Seite 15
- [„Verwendung herkömmlicher Sicherungsmethoden“](#) auf Seite 16
- [„Verwenden von VMware Consolidated Backup“](#) auf Seite 23

## Sicherungskonzepte

Die folgenden Konzepte sind wichtig für das Verständnis von Sicherungsvorgängen:

- **Differenzsicherung.** Sicherung der Dateien, die sich seit der letzten *kompletten Sicherung* geändert haben.
- **Sicherung auf Dateiebene.** Eine Sicherung auf der Ebene der Dateien und Ordner.
- **Komplette Sicherung.** Sichert alle ausgewählten Dateien.
- **Sicherung der ganzen virtuellen Maschine.** Sichert alle Dateien der ganzen virtuellen Maschine. Dazu gehören auch Festplatten-Images, `.vmtx`-Dateien usw.
- **Sicherung auf Image-Ebene (Volume-Ebene).** Sichert ein komplettes Speicher-Volume.
- **Inkrementelle Sicherung.** Sichert nur Dateien, die seit der letzten – kompletten oder inkrementellen – Sicherung geändert wurden.
- **Außer Betrieb nehmen.** Der Vorgang, mit dem die Daten auf einem physischen oder virtuellen Computer in einen Zustand versetzt werden, in dem sie gesichert werden können. Dieser Vorgang kann verschiedene Aktionen umfassen, zum Beispiel das Auslagern nicht bereinigter Puffer aus dem Betriebssystemcache auf eine Festplatte oder andere spezifische Aufgaben für Anwendungen auf höherer Ebene.
- **VCB-Proxy.** Im Kontext von VMware Consolidated Backup ist der VCB-Proxy eine physische oder virtuelle Maschine, auf der Microsoft Windows 2003, Consolidated Backup und Drittanbieter-Sicherungssoftware ausgeführt werden. Wird zur Sicherung virtueller Maschinen auf Datei- und Image-Ebene verwendet.

## Welche Daten sollten gesichert werden?

Die folgenden Hauptelemente einer ESX Server-Umgebung sollten gesichert werden:

- **Inhalte virtueller Maschinen.** Zu den Daten virtueller Maschinen, die gesichert werden sollten, zählen virtuelle Festplatten, Raw-Gerätezuordnungen (Raw Device Mappings, RDMs), Konfigurationsdateien usw.

Wie bei physischen Maschinen müssen Sie Daten virtueller Maschinen regelmäßig sichern, um potenzielle Schäden und Verluste aufgrund menschlicher oder technischer Fehler zu verhindern.

Im Allgemeinen sollten Sie folgenden Sicherungsplan für Ihre virtuellen Maschinen einhalten:

- Führen Sie auf Image-Ebene für Windows regelmäßige und für Linux jede Nacht Sicherungen durch. Sichern Sie z. B. unter Windows einmal wöchentlich ein Startlaufwerk-Image einer virtuellen Maschine.
- Führen Sie auf Dateiebene tägliche Sicherungen durch. Sichern Sie z. B. jede Nacht Dateien auf den Laufwerken D, E usw.

Informationen zur Arbeit mit den Dateien finden Sie unter „[Zugreifen auf und Verwalten von Dateien virtueller Festplatten](#)“ auf Seite 14.

- **Servicekonsole** (nur ESX Server 3). Die Servicekonsole, eine benutzerdefinierte Version von Linux, ist die Schnittstelle zur Befehlszeilenverwaltung von ESX Server 3. Sie bietet Tools und eine Eingabeaufforderung zur direkteren Verwaltung von ESX Server 3. Während der VI-Client die Hauptschnittstelle für den ESX Server 3-Host ist, verwenden Sie die Servicekonsole nur zur Durchführung erweiterter Verwaltungsvorgänge.

---

**HINWEIS** In ESX Server 3i ist keine Servicekonsole vorhanden.

---

Die einzige bedeutende Veränderung, die die Servicekonsole während ihrer gesamten Nutzungsdauer erfährt, sind regelmäßige Upgrades. Falls ein Fehler auftritt, können Sie den Status Ihrer Servicekonsole durch Neuinstallation von ESX Server 3 wiederherstellen. Sollten Sie sich für eine Sicherung der Servicekonsole entscheiden, müssen Sie sie nicht so häufig sichern wie die virtuellen Maschinen und deren Daten.

## Inhalte virtueller Maschinen

Zum Speichern virtueller Maschinen verwendet ESX Server das *VMware Virtual Machine File System (VMFS)*. VMFS ist ein Hochleistungs-Dateisystem auf physischen Festplatten und LUNs, die große Dateien speichern können, wie etwa die Images virtueller Festplatten für virtuelle Maschinen von ESX Server sowie die Arbeitsspeicher-Images angehaltener virtueller Maschinen.

Weitere Informationen zu VMFS finden Sie im *Handbuch zur Serverkonfiguration für ESX Server 3* oder *Handbuch zur Serverkonfiguration für ESX Server 3i*.

Seit ESX Server 3.0 unterstützt VMFS3 Verzeichnisse. In der Regel wird für jede virtuelle Maschine im VMFS ein separates Unterverzeichnis verwendet. Jedes dieser Verzeichnisse enthält alle Dateien der jeweiligen virtuellen Maschine, also zum Beispiel .vmdk-Dateien der virtuellen Festplatte, .vmx-Konfigurationsdateien der virtuellen Maschine, Protokolldateien usw.

---

**HINWEIS** Die virtuellen Festplatten enthalten alle Informationen, die normalerweise in der Unternehmensinfrastruktur gesichert werden, einschließlich Betriebssystem, Anwendungen und Daten.

---

Eine Alternative zur virtuellen Festplatte ist eine Raw-Gerätezuordnung (Raw Device Mapping, RDM), die Ihre virtuelle Maschine mit einer Raw-SAN-LUN verbindet. Bei RDMs werden zwei Modi unterschieden, die virtuelle und die physische Kompatibilität.

Weitere Informationen zu RDMs finden Sie im *Handbuch zur Serverkonfiguration für ESX Server 3* oder *Handbuch zur Serverkonfiguration für ESX Server 3i*.

## Zugreifen auf und Verwalten von Dateien virtueller Festplatten

In der Regel wird zur Durchführung zahlreicher Vorgänge auf virtuellen Maschinen ein *VMware Infrastructure-Client (VI-Client)* eingesetzt.

Eine direkte Bearbeitung von Dateien virtueller Festplatten im VMFS kann mithilfe der Servicekonsole (ESX Server 3) und der Befehlszeilenschnittstelle (ESX Server 3i) erfolgen, obwohl der Einsatz eines VI-Clients bevorzugt wird.

Mithilfe der Servicekonsole oder Remotebefehlszeilenschnittstelle (Remote-CLI) können Dateien im Verzeichnis `/vmfs/volumes` auf gemounteten VMFS-Volumes mit herkömmlichen Dateibefehlen, z. B. `ls` und `cp`, angezeigt und bearbeitet werden. Das VMFS-Volume dient primär zum Speichern großer Dateien wie etwa Festplatten-Images mit einer Größe bis zu 2 TB. Zum Kopieren von Dateien auf ein und von einem VMFS-Volume können FTP-, SCP- und CP-Befehle verwendet werden, vorausgesetzt, das Hostdateisystem unterstützt diese großen Dateien.

---

**HINWEIS** Unter Linux führt das Importieren von großen Festplatten aus einer Common Internet File System (CIFS)-Installation zum Absturz des ESX Server-Hosts. In diesem Fall muss der Host neu gestartet werden. Verschieben Sie große Dateien von der Servicekonsole auf die Bandsicherung. Damit dieser Vorgang problemlos verläuft, sollten ausschließlich unterstützte Programme eingesetzt werden, die nachweislich fehlerfrei ausgeführt werden. Um dieses Problem zu umgehen, kann eine große Datei zunächst mithilfe von `smbclient` in ein lokales Verzeichnis auf der Servicekonsole kopiert und anschließend von dort aus importiert werden.

---

Mithilfe des Befehls `vmfstools` werden weitere Dateivorgänge aktiviert. Verwenden Sie diesen Befehl für folgende Vorgänge:

- Erstellen, Erweitern und Löschen von Festplatten-Images
- Importieren, Exportieren und Umbenennen von Festplatten-Images

- Einstellen und Abfragen von Eigenschaften von Festplatten-Images
- Erstellen und Erweitern eines VMFS-Dateisystems

Weitere Informationen zum Befehl `vmkfstools` finden Sie im *Handbuch zur Serverkonfiguration für ESX Server 3* oder *Handbuch zur Serverkonfiguration für ESX Server 3i*.

## Sicherungskomponenten und -verfahren

An einer Sicherung sind in der Regel die folgenden drei Komponenten der Sicherungssoftware beteiligt:

- **Sicherungsclient (Sicherungs-Agent).** Ein Programm, das die Dateisysteme virtueller Maschinen durchsucht und Daten, die gesichert werden sollen, auf einen Sicherungsserver weiterleitet. Bei der Wiederherstellung schreibt der Sicherungsclient die Daten in die Dateisysteme.
- **Sicherungsserver.** Ein Programm, das die von einem Sicherungsclient weitergeleiteten Daten auf ein Sicherungsmedium (zum Beispiel eine Bandbibliothek) schreibt. Bei der Wiederherstellung liest der Sicherungsserver die Daten vom Sicherungsmedium und leitet sie an den Sicherungsclient weiter.
- **Planungsprogramm.** Ein Programm, mit dem regelmäßige Sicherungsaufgaben geplant und ihre Ausführung koordiniert werden können. Sicherungen können in regelmäßigen Abständen ausgeführt werden, oder einzelne Dateien können automatisch gesichert werden, sobald sie aktualisiert worden sind.

Jede einzelne Komponente der Sicherungssoftware kann auf einer virtuellen Maschine, in der Servicekonsole (nur mit ESX Server 3) oder auf einem VCB-Proxy mit Microsoft Windows 2003 ausgeführt werden. Dabei ist der Speicherort des Planungsprogramms unerheblich, der Speicherort des Sicherungsservers und Sicherungsclients jedoch wichtig.

Wählen Sie abhängig von dem Ort, an dem die einzelnen Komponenten ausgeführt werden, eines der folgenden Verfahren:

- **Das herkömmliche Sicherungsverfahren.** Bei diesem Verfahren wird auf jedem System, für das Sicherungsdienste ausgeführt werden sollen, ein Sicherungsclient bereitgestellt. Sie können dann regelmäßig automatische Sicherungen nach Plan durchführen.

Bei diesem Verfahren gibt es mehrere Ausführungsmöglichkeiten. Wählen Sie eine Methode, die Ihren Anforderungen am besten entspricht.

Siehe „[Verwendung herkömmlicher Sicherungsmethoden](#)“ auf Seite 16.

- **VMware Consolidated Backup.** Bei Verwendung mit einem SAN-Speicher ermöglicht Consolidated Backup ausgelagerte und problemlose Sicherungen von virtuellen Maschinen unter ESX Server. Dieses Verfahren nutzt die Snapshot-Technologie für virtuelle Maschinen und die SAN-basierte Datenübertragung in Verbindung mit herkömmlicher dateibasierter Sicherungssoftware. Beim Ausführen von Consolidated Backup können die Inhalte virtueller Maschinen von einem zentralen Sicherungs-Proxy-Server unter Microsoft Windows 2003 anstatt direkt vom ESX Server-System gesichert werden. Durch den Einsatz eines Sicherungs-Proxy-Servers wird die Auslastung des Servers, auf dem ESX Server ausgeführt wird, verringert, sodass eine größere Anzahl virtueller Maschinen ausgeführt werden kann.

Wenn Sie nicht über einen SAN-Speicher verfügen, können Sie Consolidated Backup im LAN-Modus verwenden. In diesem Modus können Sie Consolidated Backup auf einer physischen Maschine ausführen, die über ein reguläres TCP/IP-Netzwerk mit Ihrem ESX Server-System verbunden ist, oder auf einer der virtuellen Maschinen Ihres ESX Server-Hosts.

Siehe „[VMware Consolidated Backup](#)“ auf Seite 25.

## Verwendung herkömmlicher Sicherungsmethoden

Bei den herkömmlichen Sicherungsmethoden wird auf jedem Host, dessen Daten gesichert werden sollen, ein Sicherungs-Agent bereitgestellt. Regelmäßige Sicherungen werden automatisch durchgeführt.

In Zeiten geringer Systemnutzung durchsucht der Sicherungs-Agent das Dateisystem nach Änderungen und überträgt die geänderten Daten über das Netzwerk auf einen Sicherungsserver, der die Daten auf ein Sicherungsmedium (zum Beispiel eine Bandbibliothek) schreibt.

Mit den herkömmlichen Methoden können Sie Ihre virtuellen Maschinen sichern und, wenn Sie ESX Server 3 verwenden, auch die Servicekonsole.

## Überlegungen zur herkömmlichen Sicherung

Beim Einsatz herkömmlicher Methoden zum Sichern von Systemen sollte Folgendes bedacht werden:

- Um die Daten in einem möglichst konsistenten Zustand erfassen zu können, sollten Sicherungen zu einem Zeitpunkt erfolgen, an dem Aktivität im Netzwerk und Auslastung der Computerressourcen am geringsten sind. Während des Durchführens einer Sicherung müssen kritische Anwendungen unter Umständen deaktiviert werden.

- Achten Sie vor dem Durchführen einer Sicherung auf ausreichende Netzwerkbandbreite zwischen dem Server, dessen Daten gesichert werden sollen, und dem Sicherungsserver.
- Teilen Sie bei einer großen Anzahl an (physischen und virtuellen) Servern ausreichend Ressourcen für die Verwaltung der Sicherungssoftware auf den einzelnen Hosts zu. Die Verwaltung von Agenten in jeder virtuellen Maschine ist zeitraubend.

## Sichern der ESX Server 3-Servicekonsole

Da die ESX Server 3-Servicekonsole während ihrer Nutzungsdauer nur minimal verändert wird und nach einem Ausfall leicht wiederhergestellt werden kann, ist eine Sicherung der Servicekonsole unter Umständen nicht erforderlich. Falls die Servicekonsole trotzdem gesichert werden soll, ist dies nicht häufig erforderlich.

Verwenden Sie eine der folgenden Methoden, um die Servicekonsole zu sichern:

- **Dateibasiert.** Behandeln Sie die Servicekonsole als physische Maschine mit bereitgestelltem Sicherungs-Agenten. Zum Wiederherstellen der Servicekonsole installieren Sie zunächst die Servicekonsole sowie den Agenten neu und stellen anschließend die gesicherten Dateien wieder her. Dieser Ansatz ist sinnvoll, wenn schwer einzurichtende Verwaltungs-Agenten in der Servicekonsole bereitgestellt wurden. Andernfalls bietet dieser Ansatz keinen Vorteil gegenüber dem Verzicht auf Sicherung der Servicekonsole.
- **Image-basiert.** Verwenden Sie Software eines Drittanbieters, um ein Sicherungs-Image zu erstellen, das schnell wiederhergestellt werden kann. Verwenden Sie die Start-CD bzw. das von der Sicherungssoftware erstellte Medium, um die Servicekonsole wiederherzustellen.

## Sichern von virtuellen Maschinen

Je nach Ihren speziellen Anforderungen und verfügbaren Ressourcen können Sie eine der herkömmlichen Methoden zum Sichern von virtuellen Maschinen verwenden. Die herkömmlichen Sicherungsmethoden verwenden Consolidated Backup nicht.

Die herkömmlichen Sicherungsmethoden bieten folgende Optionen:

- Sie können Sicherungsclients auf virtuellen Maschinen ausführen, um Sicherungen auf Datei- oder Image-Ebene durchzuführen. Wenn die Sicherung über das Netzwerk erfolgt, ist kein Kompatibilitätshandbuch erforderlich. Siehe [„Ausführen des Sicherungsclients auf einer virtuellen Maschine“](#) auf Seite 18.

- Führen Sie Sicherungsclients über die ESX Server 3-Servicekonsole aus, wobei ganze virtuelle Maschinen als im VMFS-Dateisystem abgelegte Dateien gesichert werden. Siehe „[Ausführen des Sicherungsclients über die ESX Server 3-Servicekonsole](#)“ auf Seite 20.
- Sie können Daten virtueller Maschinen sichern, indem Sie auf einer virtuellen Maschine einen Sicherungsserver ausführen, der mit einem Bandlaufwerk oder einem anderen SCSI-basierten, an das physische System angeschlossenen Sicherungsmedium verbunden ist. Siehe „[Ausführen des Sicherungservers auf einer virtuellen Maschine](#)“ auf Seite 22.
- Wenn die Dateien virtueller Maschinen auf gemeinsam genutztem Speicher abgelegt sind, verwenden Sie bei Speichern wie SAN, NAS oder iSCSI speicherbasiertes Imaging oder einen unabhängigen Sicherungsserver (einen Proxy-Sicherungsserver oder NDMP) zur Sicherung der Dateien virtueller Maschinen. Siehe „[Behandeln virtueller Maschinen als Dateien auf gemeinsam genutztem Speicher](#)“ auf Seite 22.

---

**HINWEIS** Die Ausführung des Sicherungservers in der ESX Server 3-Servicekonsole wird nicht unterstützt.

---

## **Ausführen des Sicherungsclients auf einer virtuellen Maschine**

Da eine virtuelle Maschine im Prinzip eine physische Maschine ist, können Sie sie wie eine physische Maschine sichern, indem Sie Sicherungssoftware auf einer virtuellen Maschine ausführen.

Methode 1 und Methode 2 zeigen, wie Sie einen Sicherungs-Agenten in jeder virtuellen Maschine installieren und Daten über das Netzwerk auf Sicherungsservern sichern können, die auf anderen virtuellen Maschinen oder innerhalb physischer Maschinen bereitgestellt werden.

### **Methode 1: Sicherungsserver auf einer virtuellen Maschine**

Mit dieser Methode stellen Sie Ihren Sicherungsclient auf einer virtuellen Maschine bereit, während der Sicherungsserver sich auf einer anderen virtuellen Maschine befindet. VMware empfiehlt Ihnen, beide virtuellen Maschinen auf demselben ESX Server-System auszuführen. In diesem Fall werden Daten über das virtuelle Ethernet, das diese Maschinen verbindet, zwischen den beiden virtuellen Maschinen übertragen, jedoch nicht über eine physische Ethernet-Verbindung.

Bei Methode 1 nimmt der Sicherungs-Agent eine virtuelle Maschine, die gesichert wird, außer Betrieb.

Methode 1 wird in der Regel für Sicherungen der Daten, die im Festplatten-Image der virtuellen Maschine gespeichert sind, auf Dateiebene verwendet.

**Tabelle 1-1.** Sicherungsclient auf einer virtuellen Maschine, Sicherungsserver auf einer anderen virtuellen Maschine

<b>Empfohlen:</b>	Wenn keine Hardware für einen VCB-Proxy- oder Sicherungsserver verfügbar ist
<b>Wiederherstellen auf Dateiebene:</b>	Sehr leicht
<b>Wiederherstellen der ganzen virtuellen Maschine:</b>	Nein
<b>Außer Betrieb nehmen:</b>	Hervorragend
<b>Belastung von ESX Server:</b>	Sehr hoch
<b>Sicherung ohne LAN-Anbindung:</b>	Nein
<b>Verwaltungsfreundlichkeit:</b>	Sehr schlecht

### **Methode 2: Sicherungsserver auf einer physischen Maschine**

Bei Methode 2 stellen Sie den Sicherungsclient auf einer virtuellen Maschine bereit, während der Sicherungsserver auf einer physischen Maschine ausgeführt wird.

---

**HINWEIS** Anstelle von Methode 2 sollten Sie Consolidated Backup einsetzen.

---

Verwenden Sie Methode 2, um Daten, die im Festplatten-Image der virtuellen Maschine gespeichert sind, auf Dateiebene zu sichern.

**Tabelle 1-2.** Sicherungsclient auf einer virtuellen Maschine, Sicherungsserver auf einer physischen Maschine

<b>Empfohlen:</b>	Stattdessen kann VCB verwendet werden
<b>Wiederherstellen auf Dateiebene:</b>	Sehr leicht
<b>Wiederherstellen der ganzen virtuellen Maschine:</b>	Nein
<b>Außer Betrieb nehmen:</b>	Hervorragend
<b>Belastung von ESX Server:</b>	Hoch
<b>Sicherung ohne LAN-Anbindung:</b>	Nein
<b>Verwaltungsfreundlichkeit:</b>	Sehr schlecht

### Ausführen des Sicherungsclients über die ESX Server 3-Servicekonsole

Da eine ganze virtuelle Maschine in nur wenigen Dateien gekapselt ist, können Sie virtuelle Maschinen auf einem ESX Server 3-Host als Dateien behandeln und diese Dateien über die Servicekonsole sichern. Wie Methode 3 und Methode 4 zeigen, können Sie mit diesem Verfahren Ihren Sicherungsclient auf der Servicekonsole bereitstellen und die Dateien auf Sicherungsservern sichern, die auf anderen virtuellen oder physischen Maschinen bereitgestellt werden.

Wenn Sie Sicherungsclients auf der Servicekonsole ausführen, sichern Sie mit einem der folgenden Schritte Ihre virtuellen Maschinen:

- Schalten Sie Ihre virtuellen Maschinen aus.
- Sichern Sie ausgeführte virtuelle Maschinen mithilfe von Snapshots.

### Methode 3: Sicherungsserver auf einer virtuellen Maschine

Mit Methode 3 stellen Sie den Sicherungsclient auf der ESX Server 3-Servicekonsole bereit, während der Sicherungsserver auf der virtuellen Maschine ausgeführt wird.

---

**HINWEIS** Verwenden Sie Methode 3 nur, wenn keine separate Hardware für einen VCB-Proxy- oder Sicherungsserver verfügbar ist.

---

Methode 3 wird für Sicherungen auf Image-Ebene oder Sicherungen ganzer virtueller Maschinen verwendet.

**Tabelle 1-3.** Sicherungsclient auf einer ESX Server 3-Servicekonsole, Sicherungsclient auf einer virtuellen Maschine

<b>Empfohlen:</b>	Wenn keine Hardware für einen VCB-Proxy- oder Sicherungsserver verfügbar ist
<b>Wiederherstellen auf Dateiebene:</b>	Nein
<b>Wiederherstellen der ganzen virtuellen Maschine:</b>	Sehr leicht
<b>Außer Betrieb nehmen:</b>	Hervorragend
<b>Belastung von ESX Server:</b>	Sehr hoch
<b>Sicherung ohne LAN-Anbindung:</b>	Nein
<b>Verwaltungsfreundlichkeit:</b>	Sehr schlecht

**Methode 4: Sicherungsserver auf einer physischen Maschine**

Mit Methode 4 stellen Sie den Sicherungsclient auf der ESX Server 3-Servicekonsole bereit, während der Sicherungsserver auf einer physischen Maschine ausgeführt wird.

**HINWEIS** Anstelle von Methode 4 sollten Sie Consolidated Backup einsetzen.

Methode 4 wird für Sicherungen auf Image-Ebene verwendet.

**Tabelle 1-4.** Sicherungsclient auf einer ESX Server 3-Servicekonsole, Sicherungsserver auf einer physischen Maschine

<b>Empfohlen:</b>	Stattdessen kann VCB verwendet werden
<b>Wiederherstellen auf Dateiebene:</b>	Nein
<b>Wiederherstellen der ganzen virtuellen Maschine:</b>	Sehr leicht
<b>Außer Betrieb nehmen:</b>	Hervorragend
<b>Belastung von ESX Server:</b>	Hoch
<b>Sicherung ohne LAN-Anbindung:</b>	Nein
<b>Verwaltungsfreundlichkeit/ Skalierbarkeit:</b>	Sehr schlecht

## Ausführen des Sicherungsservers auf einer virtuellen Maschine

Sie können Daten virtueller Maschinen sichern, indem Sie auf einer virtuellen Maschine einen Sicherungsserver ausführen. Dazu muss eine Verbindung zu einem Bandlaufwerk oder anderen SCSI-basierten Sicherungsmedium bestehen, das an das physische System angeschlossen ist.

Bei Verwendung dieser Methode sollten folgende Punkte bedacht werden:

- VMware unterstützt den Anschluss von SCSI-Laufwerken an den ESX Server mithilfe von Adaptec-SCSI-Adaptern. Die Verwendung anderer Adapter, z. B. LSI MPT-Fusion-SCSI, wird nicht unterstützt.
- Wenn Sie eine Bandbibliothek verwenden (anstatt eines eigenständigen Bandlaufwerks), muss die Bibliothek ein Mehrfachziel und keine Mehrfach-LUN sein.
- Legen Sie in der Konfiguration der virtuellen Maschine die physische Ziel-ID der Bandbibliothek auch als virtuelle Ziel-ID fest.

Weitere Informationen zum Anschluss eines SCSI-basierten Bandlaufwerks an Ihre virtuelle Maschine finden Sie unter *Grundlagen der Systemverwaltung*.

## Behandeln virtueller Maschinen als Dateien auf gemeinsam genutztem Speicher

Wenn die Dateien virtueller Maschinen auf gemeinsam genutztem Speicher abgelegt sind, können Sie bei Speichern wie SAN, NAS oder iSCSI speicherbasiertes Imaging oder einen unabhängigen Sicherungsserver (einen Proxy-Sicherungsserver oder NDMP) zur Sicherung der Dateien virtueller Maschinen verwenden, ohne den ESX Server-Host, auf dem die virtuellen Maschinen ausgeführt werden, zusätzlich zu belasten.

### SAN-Sicherungen

Wenn Ihre virtuellen Festplattendateien in einem SAN gespeichert sind, verwenden Sie die von Ihrem SAN-Anbieter bereitgestellten Funktionen, um eine Kopie der Produktions-LUN zu erstellen, die alle virtuellen Festplattendateien enthält, und senden Sie diese Kopien dann an Ihre Sicherungsmedien. Bei dieser Methode müssen Sie die Snapshot-Funktionalität der virtuellen Maschine nicht während des Sicherungsprozesses nutzen, weil die SAN-Hardware die Snapshot-Funktionalität bietet.

Beim Einsatz von SAN-Snapshots zum Sichern der Daten sollte Folgendes bedacht werden:

- Einige Anbieter unterstützen Snapshots sowohl für VMFS als auch für RDMS. Werden beide unterstützt, können Sie entweder einen Snapshot des gesamten Dateisystems der virtuellen Maschine für einen Host oder Snapshots einzelner virtueller Maschinen (eine pro Festplatte) erstellen.
- Einige Anbieter unterstützen Snapshots nur für Einrichtungen mit RDMS. Werden nur RDMS unterstützt, können Sie Snapshots einzelner virtueller Maschinen erstellen.

Weitere Informationen finden Sie in der Dokumentation Ihres Speicheranbieters. Weitere Informationen zu SAN finden Sie im *SAN-Konfigurationshandbuch (für Fiber-Channel)* und im *SAN-Konfigurationshandbuch (für iSCSI)*.

### NFS-Sicherungen

Sind Ihre virtuellen Maschinen auf externen Netzwerk-Speichersystemen (NAS) unter Verwendung des NFS-Protokolls gespeichert, können Sie Sicherungen der virtuellen Maschinen auf Image-Ebene durchführen.

Weitere Informationen finden Sie in der Dokumentation Ihres Speicheranbieters.

## Verwenden von VMware Consolidated Backup

In einer modernen Datencenterumgebung kann die Durchführung herkömmlicher Sicherungen zu Problemen führen, von denen einige in „[Überlegungen zur herkömmlichen Sicherung](#)“ auf Seite 16 beschrieben werden. Viele dieser Probleme lassen sich durch den Einsatz von VMware Consolidated Backup vermeiden.

VMware Consolidated Backup löst die meisten der Probleme, die bei herkömmlichen Sicherungsverfahren auftreten können. Mithilfe von Consolidated Backup erreichen Sie Folgendes:

- Verringern der Last von ESX Server-Systemen, indem Sicherungsaufgaben auf einen oder mehrere dedizierte Backup-Proxys ausgelagert werden.

---

**HINWEIS** Um die Auslagerungsfunktionen von Consolidated Backup zu nutzen, müssen Sie ein Fibre-Channel- oder iSCSI-SAN für die Daten virtueller Maschinen verwenden.

---

- Eliminieren von Sicherungsfenstern, indem Sie zu einem Snapshot-basierten Sicherungsverfahren wechseln.
- Vereinfachen der Sicherungsverwaltung, indem Sie die Bereitstellung von Sicherungs-Agenten für die gesicherten VMs als optional festlegen.
- Sicherung virtueller Maschinen unabhängig von ihrem Betriebszustand.

# VMware Consolidated Backup

---

# 2

VMware Consolidated Backup ist eine Sicherungslösung von VMware Infrastructure 3 und wird zur Durchführung täglicher Sicherungen für die virtuellen Maschinen in einem Fibre-Channel- oder iSCSI-SAN empfohlen.

Sie können Consolidated Backup auch zur Sicherung virtueller Maschinen in ESX Server-Systemen verwenden, die keinen Zugriff auf gemeinsam genutzten Speicher haben.

Dieses Kapitel enthält die folgenden Informationen:

- [„Übersicht über VMware Consolidated Backup“](#) auf Seite 26
- [„Software- und Hardwareanforderungen von Consolidated Backup“](#) auf Seite 33
- [„Einrichten von VMware Consolidated Backup“](#) auf Seite 34
- [„Verwenden von VMware Consolidated Backup“](#) auf Seite 46
- [„Erweiterte Konfigurationen“](#) auf Seite 49
- [„Aktualisieren von Consolidated Backup“](#) auf Seite 52

## Übersicht über VMware Consolidated Backup

Sie setzen Consolidated Backup zusammen mit Drittanbietersoftware zur Sicherung der Festplatten virtueller Maschinen ein.

Die wesentlichen Funktionen von Consolidated Backup sind:

- Die meisten wichtigen Sicherungsanwendungen können in Consolidated Backup integriert werden, sodass Sie schnell und effizient Daten auf virtuellen Maschinen sichern können.
- Mit Consolidated Backup ist kein Sicherungs-Agent auf einer virtuellen Maschine erforderlich.
- Consolidated Backup kann Daten virtueller Festplatten mittels Fibre-Channel oder iSCSI direkt von einem SAN-Speichergerät lesen bzw. mittels einer Netzwerkverbindung zu einem ESX Server-Host auf Daten virtueller Festplatten zugreifen.
- Bei Sicherung virtueller Maschinen, die sich auf einem Speichergerät befinden, auf das über eine Netzwerkverbindung zugegriffen wird, kann Consolidated Backup auf einer virtuellen Maschine ausgeführt werden.
- Bei Verwendung mit iSCSI kann Consolidated Backup auf einer virtuellen Maschine ausgeführt werden.
- Für virtuelle Maschinen, auf denen Microsoft Windows ausgeführt wird, unterstützt Consolidated Backup komplette und inkrementelle Sicherungen auf Dateiebene, und für virtuelle Maschinen mit anderen Betriebssystemen Sicherungen auf Image-Ebene.
- Consolidated Backup kann entweder in Verbindung mit einem einzelnen ESX Server-Host oder mit einem VirtualCenter Management Server eingesetzt werden.

## Funktionsweise von VMware Consolidated Backup

Consolidated Backup besteht aus einer Gruppe von Dienstprogrammen und Skripten, die in Verbindung mit einer Drittanbieter-Sicherungssoftware eingesetzt werden. Um sicherzustellen, dass Consolidated Backup mit der spezifischen Sicherungssoftware einsetzbar ist, bieten entweder VMware oder der Anbieter Ihrer Sicherungssoftware Integrationsmodule an, die ggf. entsprechende Sicherungsvorbereitungs- bzw. Sicherungsnachbereitungsskripts enthalten.

Drittanbietersoftware, Integrationsmodul und Consolidated Backup werden auf dem VCB-Proxy ausgeführt, einer physischen oder virtuellen Maschine, auf der Microsoft Windows installiert ist.

Informationen zu den spezifischen Versionen von Microsoft Windows finden Sie unter [„Konfigurieren von Windows auf dem VCB-Proxy“](#) auf Seite 36.

## **Modelle zur Nutzung von VMware Consolidated Backup**

Zum Speichern und Verwalten der Dateien virtueller Festplatten setzt ESX Server verschiedene physische Speichergeräte inklusive lokaler Festplatten, NAS-Speicher, Fibre-Channel-SANs oder iSCSI-SANs ein.

Weitere Informationen zu unterschiedlichen Speichertypen finden Sie im *Handbuch zur Serverkonfiguration für ESX Server 3* oder *Handbuch zur Serverkonfiguration für ESX Server 3i*.

Die Einrichtung des VCB-Proxys sowie die von Consolidated Backup für den Zugriff auf Daten virtueller Festplatten verwendete Übertragungsmethode hängen davon ab, auf welchen Speichertyp Ihr ESX Server-System Zugriff hat.

VMware unterstützt die beiden folgenden Modi von Consolidated Backup:

- SAN-Modus (Fibre-Channel und iSCSI)
- LAN-Modus

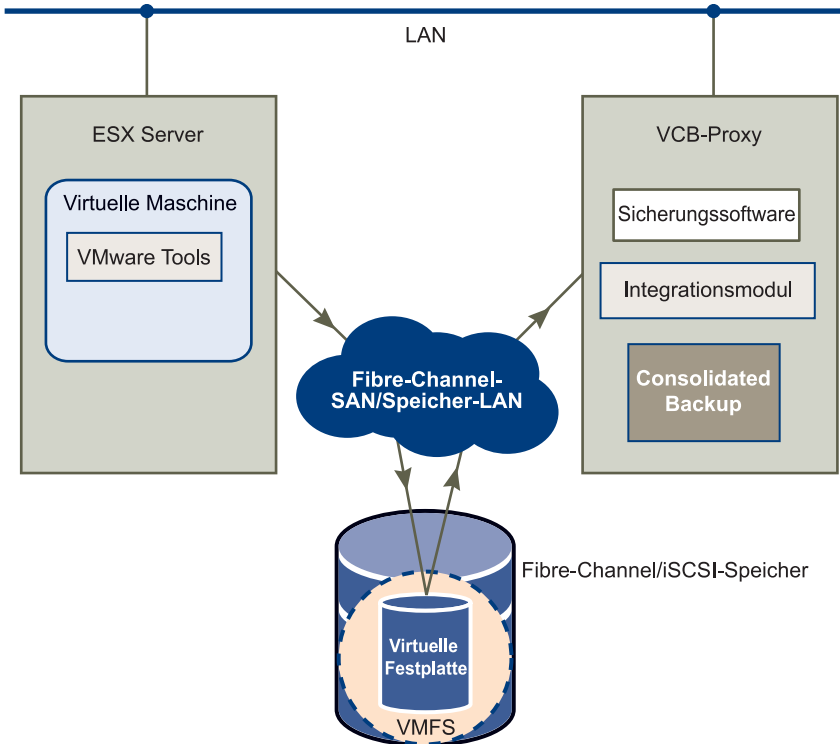
### **SAN-Modus von Consolidated Backup**

Sie wählen diesen Modus, wenn Ihr ESX Server Fibre-Channel-SAN oder iSCSI-SAN zum Speichern der Festplatten virtueller Maschinen verwendet.

Im SAN-Modus liest Consolidated Backup Daten virtueller Festplatten direkt von dem gemeinsam genutzten Fibre-Channel- oder iSCSI-Speichergerät, wobei Sicherungsvorgänge vollständig vom ESX Server-System auf den VCB-Proxy ausgelagert werden.

Abbildung 2-1 zeigt, wie Consolidated Backup im SAN-Modus funktioniert.

**Abbildung 2-1.** VMware Consolidated Backup im SAN-Modus



### LAN-Modus von Consolidated Backup

Sie wählen diesen Modus, wenn Ihr ESX Server keinen SAN-Zugriff hat, jedoch lokale Speichergeräte oder NAS zum Speichern der Festplatten virtueller Maschinen verwendet.

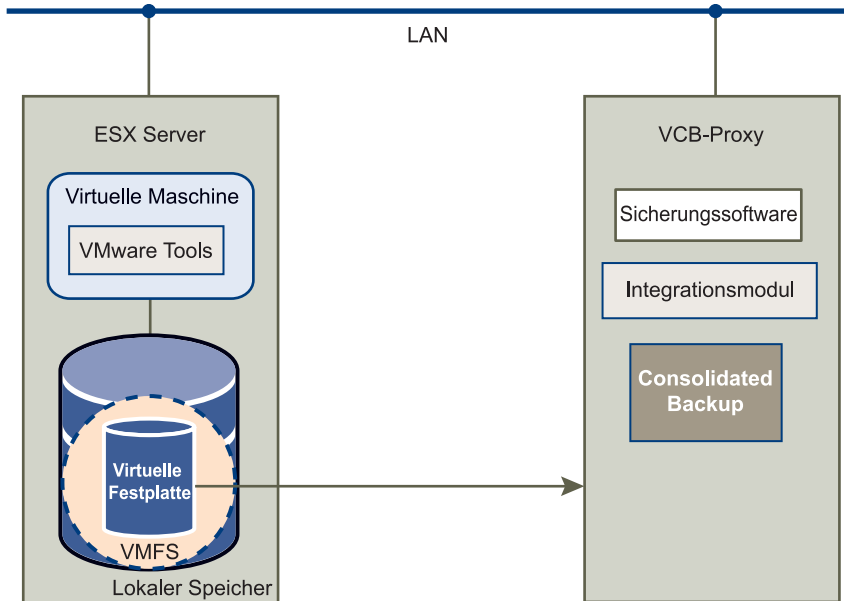
In diesem Modus verwendet Consolidated Backup ein Protokoll für den Netzwerkzugriff auf die virtuelle Festplatte. Der ESX Server-Host liest die Daten vom Speichergerät und sendet sie über einen Netzwerkanal an den VCB-Proxy.

So können Sie Consolidated Backup im LAN-Modus ausführen:

- Sie benötigen ESX Server 3.5 oder ESX Server 3i Version 3.5.
- Wenn Sie VirtualCenter verwenden, muss Version 2.5 installiert sein.
- Ihre virtuellen Festplatten dürfen jeweils nicht größer sein als 1 TB.

Abbildung 2-2 zeigt, wie Consolidated Backup im LAN-Modus funktioniert.

**Abbildung 2-2.** VMware Consolidated Backup im LAN-Modus



Da die Daten virtueller Festplatten vom ESX Server-Host über das LAN übertragen werden, stehen die LAN-unabhängigen Funktionen des SAN-Modus in diesem Modus nicht zur Verfügung. Die Ausführung von Consolidated Backup im LAN-Modus bietet Ihnen folgende Vorteile:

- Sie müssen keine virtuellen Festplatten in einem SAN speichern. Sie können jedes Speichergerät inklusive NAS nutzen, auf das ESX Server zugreifen kann.
- Sie benötigen keinen dedizierten physischen Server für Ihren VCB-Proxy. Außer der Einrichtung eines physischen Servers als VCB-Proxy können Sie optional eine Ihrer virtuellen Maschinen als VCB-Proxy konfigurieren.

Bei dieser Konfiguration werden die Sicherungsvorgänge zwar nicht vollständig vom ESX Server-Host ausgelagert, doch bietet sie gegenüber der Verwendung eines Sicherungs-Agenten auf der Servicekonsole oder der virtuellen Produktionsmaschine einen Vorteil. Sie können mittels der erweiterten Funktionen zur Ressourcenplanung von VMware Infrastructure verhindern, dass die virtuelle Maschine, die Ihre Sicherungen ausführt, die Produktionsleistung beeinträchtigt. Sie können z. B. die virtuelle Maschine, die Ihre Sicherungen ausführt, und Ihre virtuellen Produktionsmaschinen in verschiedenen Ressourcenpools einsetzen. Weitere Informationen finden Sie im *Handbuch zur Ressourcenverwaltung*.

- Wenn Ihr ESX Server-Host und der VCB-Proxy sich in einem sicheren isolierten Netzwerk befinden, können Sie die Daten unverschlüsselt übertragen. Dies ist schneller und belastet die Ressourcen von ESX Server-Host und Proxy weniger. Wenn Sie vertrauliche Daten schützen müssen, können Sie Daten virtueller Maschinen optional in verschlüsselter Form übertragen.

## Ablauf von VMware Consolidated Backup

Vor der Nutzung von Consolidated Backup müssen Sie für jede einzelne virtuelle Maschine oder Gruppe virtueller Maschinen einen Sicherungsauftrag konfigurieren.

Zum geplanten Zeitpunkt startet die Sicherungssoftware den Sicherungsauftrag auf dem VCB-Proxy. Nach dem Start des Sicherungsauftrags werden folgende Schritte ausgeführt:

- 1 Die Sicherungssoftware ruft das Sicherungsvorbereitungsskript auf.  
Das Sicherungsvorbereitungsskript führt folgende Aufgaben aus:
  - a (Optional) Ihr benutzerdefiniertes Skript zum Erfassen des Zustands vor dem Einfrieren wird auf der virtuellen Maschine ausgeführt. Das Skript zum Erfassen des Zustands vor dem Einfrieren bereitet die entscheidenden Softwarekomponenten auf der virtuellen Maschine auf Sicherungen vor. Siehe „[Ausführen benutzerdefinierter Skripts zum außer Betrieb nehmen](#)“ auf Seite 49.
  - b NTFS- und FAT-Dateisysteme der virtuellen Maschine werden außer Betrieb genommen (gilt nur für virtuelle Maschinen, auf denen 32-Bit-Versionen von Windows XP, Windows 2000 oder Windows 2003 ausgeführt werden). Dies gewährleistet, dass bei Erstellen des Snapshots keine Schreibvorgänge des Dateisystems ausstehen, sodass mit dem Dateisystem übereinstimmende Sicherungen erstellt werden können.
  - c Die virtuelle Maschine wird in den Snapshot-Modus gesetzt, sodass Änderungen ihrer Festplatten für spätere Schreibvorgänge gespeichert werden. Während dieses Vorgangs kann die virtuelle Maschine ihren Betrieb fortsetzen.
  - d Die in [Schritt b](#) außer Betrieb genommenen NTFS- und FAT-Dateisysteme werden wieder in Betrieb genommen.
  - e (Optional) Ihr benutzerdefiniertes Skript zum Erfassen des Zustands nach dem Auftauen wird auf der virtuellen Maschine ausgeführt. Das Skript zum Erfassen des Zustands nach dem Auftauen widerruft Änderungen, die das Skript zum Erfassen des Zustands vor dem Einfrieren in [Schritt a](#) vorgenommen hat.

- f Der Snapshot der virtuellen Maschine wird der Drittanbietersoftware zur Verfügung gestellt:
  - Zur Sicherung virtueller Maschinen auf Image-Ebene siehe „[Sichern virtueller Maschinen auf Image-Ebene](#)“ auf Seite 32.
  - Zur Sicherung virtueller Microsoft Windows-Maschinen auf Dateiebene siehe „[Sichern virtueller Maschinen auf Dateiebene](#)“ auf Seite 32.
- 2 Die Sicherungssoftware führt eine gewöhnliche Sicherung des Snapshots der virtuellen Maschine aus, wobei die Daten auf ein Sicherungsmedium verschoben werden. Während dieses Vorgangs kann die virtuelle Maschine ihren Betrieb fortsetzen.
- 3 Die Sicherungssoftware ruft das Sicherungsnachbereitungsskript auf, das folgende Aufgaben ausführt:
  - a Unmounten des Snapshots der virtuellen Maschine vom Sicherungs-Proxy.
  - b Die virtuelle Maschine wird aus dem Snapshot-Modus herausgenommen, wobei alle Änderungen, die vorgenommen wurden, während die Maschine sich im Snapshot-Modus befand, auf die Festplatte geschrieben werden.

## Sicherungstypen

Für virtuelle Maschinen, auf denen Gastbetriebssysteme ausgeführt werden, unterstützt Consolidated Backup Sicherungen auf Image-Ebene, und für virtuelle Maschinen mit Microsoft Windows-Betriebssystemen Sicherungen auf Dateiebene.

- **Sicherung auf Image-Ebene** ermöglicht Sicherungsclients das Erstellen einer Kopie aller mit einer bestimmten virtuellen Maschine verknüpften virtuellen Festplatten und Konfigurationsdateien. Dieser Sicherungstyp eignet sich zur Wiederherstellung ganzer virtueller Maschinen nach einem Hardwareausfall oder einem Fehler des Systemadministrators (z. B. dem versehentlichen Löschen einer ganzen virtuellen Maschine).
- **Sicherung auf Dateiebene** ermöglicht Sicherungsclients das Erstellen von Kopien einzelner, auf den virtuellen Festplatten enthaltener Dateien. Bei Sicherungen auf Dateiebene werden folgende Typen unterschieden:
  - **Komplette Dateisicherung** – Sichert alle Dateien.
  - **Differenzsicherung** – Sichert nur Dateien, die seit der letzten kompletten Dateisicherung geändert wurden.
  - **Inkrementelle Sicherung** – Sichert nur Dateien, die seit der letzten – kompletten oder inkrementellen – Sicherung geändert wurden.

Sicherungen auf Dateiebene ermöglichen die individuelle Wiederherstellung von Dateien oder Verzeichnissen. Mithilfe von Sicherungen auf Dateiebene können Sie Datenverluste aufgrund von Benutzerfehlern, wie etwa versehentlicher Dateilöschung, verhindern.

## Sichern virtueller Maschinen auf Image-Ebene

Eine Sicherung virtueller Maschinen auf Image-Ebene kann unabhängig vom jeweiligen Betriebssystem und Gastbetriebssystem durchgeführt werden.

Wenn Sie die Sicherung virtueller Maschinen auf Image-Ebene durchführen, erstellt Consolidated Backup zuerst einen Snapshot der virtuellen Maschine. Dann werden folgende Schritte ausgeführt:

- 1 Consolidated Backup exportiert den Snapshot der virtuellen Maschine in ein lokales Verzeichnis des VCB-Proxys. Beispiel:  
`C:\mnt\mytestvm.foo.com-fullVM`
- 2 Die Sicherungssoftware des Drittanbieters verschiebt die Festplatten-Images und Konfigurationsdateien der virtuellen Maschine auf das Sicherungsmedium.

## Sichern virtueller Maschinen auf Dateiebene

Für virtuelle Maschinen unter Windows unterstützt Consolidated Backup Sicherungen auf Dateiebene.

Bei Sicherungen auf Dateiebene erstellen Sie zuerst einen Snapshot der virtuellen Maschine. Dann werden folgende Schritte ausgeführt:

- 1 Consolidated Backup erkennt Volumes in Snapshots virtueller Maschinen und mountet erkannte Volumes auf dem VCB-Proxy an vordefinierten Knotenpunkten.

Jeder Knotenpunkt entspricht einem Laufwerksbuchstaben, der einem Volume der virtuellen Maschine zugewiesen ist. Beispiel:

`C:\mnt\mytestvm.foo.com\letters\D`



**VORSICHT** Da der VCB-Proxy nur Volumes mit zugewiesenen Laufwerksbuchstaben erkennen kann, stellen Sie sicher, dass jedem Volume einer virtuellen Festplatte ein Laufwerksbuchstabe zugewiesen wurde.

---

- 2 Die Drittanbieter-Sicherungssoftware erstellt von diesen Volumes Sicherungen auf Dateiebene.

## Einschränkungen bei VMware Consolidated Backup

Unter bestimmten Umständen können Sie Consolidated Backup nicht zur Sicherung von Daten auf einer virtuellen Maschine einsetzen.

- Consolidated Backup kann virtuelle Maschinen mit Festplatten-Images, die auf einem Speichergerät gespeichert sind, auf das der VCB-Proxy nicht zugreifen kann, im SAN-Modus nicht sichern.
- Consolidated Backup kann RDMS nicht im physischen Kompatibilitätsmodus sichern.
- Consolidated Backup kann virtuelle Maschinen, auf denen ein anderes Betriebssystem als Microsoft Windows ausgeführt wird, nicht auf Dateiebene sichern.
- Sie können Consolidated Backup nicht zum Sichern virtueller Maschinen in einem Cluster verwenden. Diese virtuellen Maschinen nutzen gemeinsam einen SCSI-Controller, sodass keine Snapshots von ihnen erstellt werden können.

Wenn die Verwendung von Consolidated Backup nicht möglich ist, setzen Sie auf der virtuellen Maschine einen Sicherungs-Agenten ein, und führen Sie die Sicherung von der virtuellen Maschine aus durch. Der Sicherungs-Agent wird vom Drittanbieter der Sicherungssoftware bereitgestellt.

Einzelheiten zur Installation des Sicherungs-Agenten finden Sie in der Dokumentation des zur Sicherungssoftware passenden Integrationsmoduls.

## Software- und Hardwareanforderungen von Consolidated Backup

Je nachdem, ob Sie Consolidated Backup im SAN- oder LAN-Modus einsetzen möchten, gelten für Consolidated Backup folgende allgemeine Anforderungen:

- Sie benötigen ein einzelnes ESX-Server-System und den VI-Client oder mehrere ESX-Server-Systeme und VirtualCenter zu ihrer Verwaltung.

---

**HINWEIS** Um Consolidated Backup im LAN-Modus einzusetzen, aktualisieren Sie unbedingt ESX Server auf Version 3.5 und VirtualCenter auf Version 2.5.

---

- Sie benötigen Sicherungshardware, z. B. ein Bandsystem.
- Sie benötigen folgende Versionen von Microsoft Windows zur Installation auf Ihrem VCB-Proxy:
  - Microsoft Windows Server 2003 Service Pack 1 (32-Bit oder 64-Bit)
  - Microsoft Windows Server 2003 R2 (32-Bit oder 64-Bit)

- Microsoft Windows Server 2003 Service Pack 1 (32-Bit oder 64-Bit)
- Sie benötigen Sicherungssoftware, die Consolidated Backup unterstützt. Eine Liste unterstützender Sicherungspakete von Drittanbietern finden Sie im *Kompatibilitätshandbuch für VMware Infrastructure 3-Sicherungssoftware*.

---

**HINWEIS** Wenn Sie Consolidated Backup in Verbindung mit einer von VMware unterstützten Drittanbietersoftware verwenden, stellen Sie sicher, dass die Versionen von Microsoft Windows und der Sicherungssoftware übereinstimmen. Führen Sie z. B. die 64-Bit-Version von Microsoft Windows aus, dann installieren Sie die 64-Bit-Version der Sicherungssoftware.

---

- Sie benötigen einen Netzwerkkadpter (NIC).

Zu den zusätzlichen Anforderungen für den Einsatz von Consolidated Backup im SAN-Modus zählen:

- Ein Fibre-Channel- oder iSCSI-SAN-Speicher, auf dem sich die Daten virtueller Maschinen befinden, die Sie sichern möchten.
- Bei Verwendung von Fibre-Channel-SAN muss ein dediziertes physisches System für einen VCB-Proxy mit einem Fibre-Channel-Hostbusadapter (HBA) installiert sein.

## Einrichten von VMware Consolidated Backup

Konfigurieren Sie alle mit Consolidated Backup eingesetzten Komponenten in folgenden Schritten:

- 1 Konfigurieren Sie den ESX Server bzw. mehrere Server. Siehe „[Konfigurieren von VMware ESX Server und virtuellen Maschinen zum Sichern](#)“ auf Seite 35.
- 2 Richten Sie den VCB-Proxy ein, und installieren Sie die Sicherungssoftware, Consolidated Backup sowie entsprechende Integrationsmodule auf dem VCB-Proxy. Siehe „[Einrichten eines VCB-Proxys](#)“ auf Seite 35.
- 3 Aktivieren Sie ggf. die Verifizierung des SSL-Zertifikats. Siehe „[Aktivieren der Verifizierung des SSL-Zertifikats](#)“ auf Seite 43.
- 4 Konfigurieren Sie bei Verwendung von SAN Ihr SAN-Fabric. Siehe „[Konfigurieren von SAN](#)“ auf Seite 45.

## Konfigurieren von VMware ESX Server und virtuellen Maschinen zum Sichern

Sie benötigen mindestens einen ESX Server-Host und VirtualCenter zur Verwaltung.

Konfigurieren Sie mit dem VI-Client den Speicher für den ESX Server, und erstellen Sie virtuelle Maschinen. Folgende Anforderungen müssen zur erfolgreichen Ausführung von Consolidated Backup erfüllt sein:

- Die virtuellen Festplatten virtueller Maschinen, die Sie sichern möchten, müssen sich in VMFS-Datenspeichern befinden, die in lokalem Speicher erstellt sind, bzw. in iSCSI- oder FC-SANs. Im virtuellen Kompatibilitätsmodus können virtuelle Maschinen auch RDMs nutzen. Consolidated Backup unterstützt RDMs im physischen Kompatibilitätsmodus nicht.
- Falls Sie Consolidated Backup im LAN-Modus verwenden möchten, darf die Größe der Dateien Ihrer virtuellen Festplatte 1 TB nicht überschreiten.
- Eine aktuelle Version der VMware Tools ist auf jeder virtuellen Maschine installiert, die Sie sichern möchten. Ohne die VMware Tools sind die von Consolidated Backup für Sicherungen erstellten Snapshots nur nach einem Systemabsturz konsistent. Es wird also keine Synchronisierung des Dateisystems durchgeführt.
- Für Sicherungen auf Dateiebene wird auf Ihren virtuellen Maschinen Microsoft Windows NT 4.0, Windows 2000, Windows XP, Windows XP Professional, Windows 2003, Windows Vista oder Windows Server 2008 („Longhorn Server“) ausgeführt.

Sicherungen virtueller Maschinen auf Image-Ebene werden für alle Gastbetriebssysteme unterstützt.

Weitere Informationen zur Konfiguration von Speicher und RDMs finden Sie im *Handbuch zur Serverkonfiguration für ESX Server 3* oder *Handbuch zur Serverkonfiguration für ESX Server 3i* unter [www.vmware.com](http://www.vmware.com).

Informationen zum Erstellen virtueller Maschinen und Installieren der VMware Tools finden Sie in *Grundlagen der Systemverwaltung* unter [www.vmware.com](http://www.vmware.com).

## Einrichten eines VCB-Proxys

Der VCB-Proxy ist eine Maschine, auf der Consolidated Backup, Ihre Drittanbieter-Sicherungssoftware sowie ein Integrationsmodul für die Sicherungssoftware ausgeführt werden. Die Anforderungen für Ihren VCB-Proxy hängen von dem Speichertyp ab, den Sie zum Speichern der Daten Ihrer virtuellen Maschine verwenden:

- Mit FC-SAN-Speicher benötigen Sie einen dedizierten physischen Server für Ihren VCB-Proxy. Zusätzliche Hardwareanforderungen für Ihren VCB-Proxy finden Sie unter [„Software- und Hardwareanforderungen von Consolidated Backup“](#) auf Seite 33.
- Mit iSCSI-Speicher sowie jedem Speichertyp, der das NBD-Format unterstützt – inklusive des lokalen Speichers des ESX Server-Hosts – müssen Sie keinen physischen Server verwenden. Optional können Sie eine der virtuellen Maschinen für den Einsatz als VCB-Proxy konfigurieren.

Der VCB-Proxy wird in den nachstehenden Schritten konfiguriert, wobei es keine Rolle spielt, ob es sich um eine physische oder virtuelle Maschine handelt.

### **So konfigurieren Sie Ihren VCB-Proxy**

- 1 Installieren und konfigurieren Sie Microsoft Windows auf dem VCB-Proxy. Siehe [„Konfigurieren von Windows auf dem VCB-Proxy“](#) auf Seite 36.
- 2 Konfigurieren Sie die Vernetzung auf dem VCB-Proxy. Siehe [„Konfigurieren der Vernetzung auf dem VCB-Proxy“](#) auf Seite 37.
- 3 Installieren und konfigurieren Sie die mit Consolidated Backup zu verwendende Drittanbieter-Sicherungssoftware. Siehe [„Konfigurieren der Drittanbieter-Software auf dem VCB-Proxy“](#) auf Seite 38.
- 4 Installieren Sie Consolidated Backup. Siehe [„Installieren von VMware Consolidated Backup“](#) auf Seite 39.
- 5 Installieren Sie ein Integrationsmodul, das Ihrer Drittanbieter-Sicherungssoftware entspricht. Siehe [„Installieren eines Integrationsmoduls für die Sicherungssoftware“](#) auf Seite 39.
- 6 Konfigurieren Sie Consolidated Backup. Siehe [„Konfigurieren von VMware Consolidated Backup“](#) auf Seite 39.

### **Konfigurieren von Windows auf dem VCB-Proxy**

Installieren Sie auf Ihrem VCB-Proxy eine unterstützte Version von Microsoft Windows. Siehe [„Software- und Hardwareanforderungen von Consolidated Backup“](#) auf Seite 33.

Alle Windows-Versionen mit Ausnahme von Windows 2003 Enterprise Edition und Windows 2003 Datacenter Edition weisen jedem sichtbaren NTFS-Volumen (New Technology File System) und FAT-Volumen (File Allocation Table) einen Laufwerksbuchstaben zu. Um Consolidated Backup verwenden zu können, müssen Sie alle nicht verwendeten Zuweisungen von Laufwerksbuchstaben löschen.



**VORSICHT** Wenn Sie diesen Konfigurationsschritt nicht durchführen, können bei virtuellen Maschinen, die RDM einsetzen, Datenverluste auftreten.

### **So deaktivieren Sie Zuweisungen von Laufwerksbuchstaben**

- 1 Fahren Sie den VCB-Proxy herunter.
- 2 Trennen Sie die Verbindung zwischen VCB-Proxy und SAN, oder maskieren Sie alle LUNs, die VMFS-Volumes oder RDMs enthalten.
- 3 Starten Sie den Proxy, und melden Sie sich als Administrator an.
- 4 Öffnen Sie eine Befehlszeilenschnittstelle.
- 5 Führen Sie das Dienstprogramm Diskpart aus, indem Sie Folgendes eingeben:  
`diskpart`  
Das Dienstprogramm Diskpart startet und zeigt eine eigene Eingabeaufforderung an.
- 6 Deaktivieren Sie die automatische Zuweisung von Laufwerksbuchstaben für neu sichtbare Volumes, indem Sie an der Eingabeaufforderung des Dienstprogramms Diskpart Folgendes eingeben:  
`automount disable`
- 7 Entfernen Sie die Einträge zuvor gemounteter Volumes aus der Registrierung, indem Sie an der Eingabeaufforderung des Dienstprogramms Diskpart Folgendes eingeben:  
`automount scrub`
- 8 Beenden Sie das Dienstprogramm Diskpart, indem Sie Folgendes eingeben:  
`exit`
- 9 Fahren Sie Windows herunter.
- 10 Stellen Sie die Verbindung zwischen VCB-Proxy und SAN wieder her bzw. entfernen Sie die Maskierung der LUNs, die VMFS-Volumes oder RDMs enthalten.
- 11 Starten Sie den Proxy.

### **Konfigurieren der Vernetzung auf dem VCB-Proxy**

Der VCB-Proxy muss eine Verbindung zu dem VirtualCenter herstellen, das Ihren ESX Server-Cluster verwaltet, bzw. zu einem einzelnen ESX Server-System, falls Sie nicht über einen Cluster verfügen.

Um die Vernetzung für Ihren VCB-Proxy zu konfigurieren, beachten Sie folgende Richtlinien:

- Eine ggf. zwischen VCB-Proxy und VirtualCenter befindliche Firewall muss TCP/IP-Verbindungen mit VirtualCenter zulassen. Standardmäßig erwartet VirtualCenter eingehende Verbindungen am TCP/IP-Port 443.
- Richten Sie TCP/IP-Verbindungen mit Port 902 für alle ESX Server-Hosts ein, auf denen virtuelle Maschinen ausgeführt werden, die Sie vom VCB-Proxy aus sichern möchten.

Weitere Informationen zur Konfiguration der Vernetzung finden Sie im *Handbuch zur Serverkonfiguration für ESX Server 3* oder *Handbuch zur Serverkonfiguration für ESX Server 3i*.

### **Konfigurieren der Drittanbieter-Software auf dem VCB-Proxy**

Die in Verbindung mit Consolidated Backup eingesetzte Drittanbieter-Sicherungssoftware wird auf dem VCB-Proxy ausgeführt.

Nach der Installation müssen Sie die Sicherungssoftware so konfigurieren, dass sie die Skripts und Dienstprogramme von Consolidated Backup nutzen kann.

Beachten Sie bei der Konfiguration der Sicherungssoftware die Anweisungen des Anbieters.

Spezifische Anforderungen und Anweisungen finden Sie in der Datei `README.html`, die zum Integrationsmodul Ihrer Sicherungssoftware gehört. Ggf. müssen Sie an der Sicherungssoftware folgende Einstellungen vornehmen:

- Aktivieren der Option für Mount-Punkte für die Sicherungssoftware.
- Deaktivieren des Windows-Archivbits und Ändern der Journalfunktionen, falls die Drittanbieter-Sicherungssoftware inkrementelle oder Differenzsicherungen durchführt. Beide Funktionen erfordern, dass die Sicherungssoftware das gesicherte Dateisystem ändert. Dies ist jedoch bei einer Sicherung auf Snapshot-Basis nicht möglich.
  - Windows-Archivbit. Das Archivbit ist ein Dateiattribut, anhand dessen manche Sicherungsprodukte bestimmen, ob die Datei seit der vorherigen Sicherung geändert wurde und gesichert werden sollte. Konfigurieren Sie den Sicherungsclient so, dass er stattdessen Zeitstempel verwendet.
  - Das Windows-Änderungsjournal kann nicht für inkrementelle Sicherungen in Sicherungsszenarien auf Snapshot-Basis verwendet werden.

Nach Installation und Konfiguration können Sie die Drittanbieter-Sicherungssoftware überprüfen, indem Sie in einem lokalen Verzeichnis des VCB-Proxys einen Sicherungs- und Wiederherstellungsauftrag ausführen.

## Installieren von VMware Consolidated Backup

Installieren Sie das Basispaket von Consolidated Backup auf dem VCB-Proxy.

### So installieren Sie das Basispaket von Consolidated Backup

- 1 Melden Sie sich mit einem Konto mit Administratorberechtigungen am VCB-Proxy an.
- 2 Installieren Sie Consolidated Backup, indem Sie die Datei `setup.exe` von der CD-ROM oder vom Speicherort der elektronischen Verteilung aus ausführen.
- 3 Wählen Sie während der Installation ein Installationsverzeichnis für Consolidated Backup aus, oder übernehmen Sie das angezeigte Standardinstallationsverzeichnis.

### Installieren eines Integrationsmoduls für die Sicherungssoftware

Auf dem VCB-Proxy müssen Sie ein Integrationsmodul für Consolidated Backup installieren, das zur Software des Drittanbieters passt. Für jede unterstützte Sicherungssoftware eines Drittanbieters stellt entweder der Anbieter der Sicherungssoftware oder VMware ein Integrationsmodul zur Verfügung.

Von VMware bereitgestellte Integrationsmodule werden als ZIP-Dateien verteilt. Extrahieren Sie die ZIP-Datei in Ihr VMware Consolidated Backup-Installationsverzeichnis. Damit wird ein Unterverzeichnis erstellt, das eine `README.html`-Datei mit einer Beschreibung der Installation des Integrationsmoduls enthält. Außerdem bietet die `README.html`-Datei spezifische Anweisungen, die Sie zur Konfiguration der Sicherungssoftware für Consolidated Backup benötigen.

### Konfigurieren von VMware Consolidated Backup

Die wichtigsten Konfigurationseinstellungen für Consolidated Backup sind in der Konfigurationsdatei `config.js` gespeichert. Sie befindet sich im Unterverzeichnis `config` des folgenden Standardinstallationsverzeichnisses für Consolidated Backup:

```
C:\Programme\VMware\VMware Consolidated Backup Framework
```

Achten Sie bei der Konfiguration von Consolidated Backup darauf, alle Optionen in der Datei `config.js` anzugeben, denen keine Standardwerte zugeordnet sind.

[Tabelle 2-1](#) gibt einen Überblick über die in dieser Datei enthaltenen Konfigurationseinstellungen.

**Tabelle 2-1.** Konfigurationseinstellungen für Consolidated Backup

<b>Option</b>	<b>Standard</b>	<b>Beschreibung</b>
BACKUPROOT	C:\mnt	<p>Verzeichnis, in dem alle Sicherungsaufträge für die virtuelle Maschine gespeichert werden.</p> <p>Für jeden Sicherungsauftrag wird hier ein Verzeichnis mit einem eindeutigen Namen erstellt, der sich aus dem Sicherungstyp und dem Namen der virtuellen Maschine ergibt.</p> <p>Überprüfen Sie, ob dieses Verzeichnis vorhanden ist, bevor Sie versuchen, Sicherungen für virtuelle Maschinen durchzuführen.</p> <p>Für Sicherungen virtueller Maschinen auf Image-Ebene muss das Volume, das diesen Mount-Punkt enthält, groß genug sein, um die exportierten Festplatten-Images der größten virtuellen Maschine aufnehmen zu können.</p>
HOST	(keine Standard-einstellung)	Hostname des vom VCB-Proxy verwendeten VirtualCenter Servers oder ESX Server-Hosts.
PORT	443	Nummer des Ports zur Verbindung mit VirtualCenter- oder ESX Server-Host.
USERNAME	(keine Standard-einstellung)	Benutzer-ID, die zur Anmeldung am VirtualCenter- oder ESX Server-Host verwendet werden soll.
PASSWORD	(keine Standard-einstellung)	Kennwort, das zur Anmeldung am VirtualCenter- oder ESX Server-Host verwendet werden soll.

**Tabelle 2-1.** Konfigurationseinstellungen für Consolidated Backup (Fortsetzung)

Option	Standard	Beschreibung
TRANSPORT_MODE	san	<p>Bestimmt den VCB-Zugriff auf Daten virtueller Festplatten. Informationen zu den beiden Modi von Consolidated Backup finden Sie unter <a href="#">„Modelle zur Nutzung von VMware Consolidated Backup“</a> auf Seite 27.</p> <p>Folgende Optionen sind verfügbar:</p> <ul style="list-style-type: none"> <li>■ <b>san</b> – Sichern der Dateien virtueller Festplatten, die auf einem gemeinsam genutzten Fibre-Channel- oder iSCSI-Speichergerät gespeichert sind.</li> <li>■ Sichern Sie mithilfe einer der folgenden Optionen Dateien virtueller Festplatten, die auf einem Speichergerät gespeichert sind, auf das über das NBD-Protokoll (Network Block Device) zugegriffen wird. Aktivieren Sie auch mithilfe einer dieser Optionen Consolidated Backup auf einer virtuellen Maschine, die als VCB-Proxy dient. <ul style="list-style-type: none"> <li>■ <b>nbd</b> – Wählen Sie diese Option, wenn Sie Daten virtueller Festplatten nicht verschlüsseln müssen.</li> <li>■ <b>nbdssl</b> – Wählen Sie diese Option, um Daten virtueller Festplatten für Netzwerkübertragungen zu verschlüsseln. Sie können auch die Verifizierung des SSL-Zertifikats aktivieren. Siehe <a href="#">„Aktivieren der Verifizierung des SSL-Zertifikats“</a> auf Seite 43.</li> </ul> </li> </ul>

**Tabelle 2-1.** Konfigurationseinstellungen für Consolidated Backup (Fortsetzung)

Option	Standard	Beschreibung
SNAPSHOT_POLICY	automatic	<p>Gültige Optionen:</p> <ul style="list-style-type: none"> <li>■ <b>automatic:</b> Consolidated Backup erstellt und löscht nach Bedarf Sicherungs-Snapshots für virtuelle Maschinen.</li> <li>■ <b>manual:</b> Consolidated Backup erstellt und löscht keine Snapshots, erkennt jedoch einen Sicherungs-Snapshot namens <code>_VCB_BACKUP_</code> und verwendet ihn zur Sicherung. Diese Option ist nützlich für die kreative Skripterstellung.</li> <li>■ <b>createonly:</b> Consolidated Backup erstellt beim Ausführen des Sicherungsvorbereitungsskripts einen Sicherungs-Snapshot, entfernt den Snapshot nach der Sicherung jedoch nicht. Verwenden Sie diese Option, wenn Sie einen Überprüfungsauftrag ausführen müssen. Das Entfernen der Installation wird dann vom Überprüfungsskript übernommen.</li> <li>■ <b>deleteonly:</b> Consolidated Backup erkennt, dass bereits ein Sicherungs-Snapshot namens <code>_VCB_BACKUP_</code> vorhanden ist, und versucht daher nicht, einen Snapshot zu erstellen. Der Snapshot wird jedoch vom Sicherungsnachbereitungsskript gelöscht. Diese Option ist nützlich für die kreative Skripterstellung.</li> </ul>
VM_LOOKUP_METHOD	ipaddr	<p>Legen Sie mithilfe einer der folgenden Optionen fest, wie Consolidated Backup virtuelle Maschinen identifiziert:</p> <ul style="list-style-type: none"> <li>■ <b>ipaddr:</b> Virtuelle Maschinen werden anhand von DNS-Name und IP-Adresse identifiziert.</li> <li>■ <b>name:</b> Virtuelle Maschinen werden gemäß Anzeige in VirtualCenter anhand von Namen identifiziert. Verwenden Sie diese Option bei mehreren virtuellen Maschinen mit derselben IP-Adresse, aber verschiedenen Namen. Jede virtuelle Maschine muss einen eindeutigen Namen haben, sonst misslingt ein Sicherungsauftrag.</li> </ul>

**Tabelle 2-1.** Konfigurationseinstellungen für Consolidated Backup (Fortsetzung)

Option	Standard	Beschreibung
PREEXISTING_MOUNTPOINT	fail	<p>Geben Sie mithilfe einer der folgenden Optionen an, ob ein Sicherungsauftrag fortgesetzt oder abgebrochen werden soll, wenn Consolidated Backup erkennt, dass bereits ein Mount-Punkt für eine virtuelle Maschine vorhanden ist:</p> <ul style="list-style-type: none"> <li>■ <b>fail</b>: Weist Consolidated Backup an, den Sicherungsauftrag abubrechen.</li> <li>■ <b>delete</b>: Weist Consolidated Backup an, den bereits vorhandenen Mount-Punkt und damit verknüpfte Sicherungs-Snapshots zu entfernen.</li> </ul> <p>Wenn dies gelingt, wird der Sicherungsauftrag fortgesetzt. Bei Scheitern wird der Sicherungsauftrag abgebrochen.</p>
PREEXISTING_VCB_SNAPSHOT	fail	<p>Geben Sie mithilfe einer der folgenden Optionen an, ob ein Sicherungsauftrag fortgesetzt oder abgebrochen werden soll, wenn Consolidated Backup erkennt, dass bereits ein Sicherungs-Snapshot für eine virtuelle Maschine vorhanden ist:</p> <ul style="list-style-type: none"> <li>■ <b>fail</b>: Weist Consolidated Backup an, den Sicherungsauftrag abubrechen.</li> <li>■ <b>delete</b>: Weist Consolidated Backup an, den bereits vorhandenen Sicherungs-Snapshot zu entfernen.</li> </ul> <p>Wenn dies gelingt, wird der Sicherungsauftrag fortgesetzt. Bei Scheitern wird der Sicherungsauftrag abgebrochen.</p>
MAX_RETRIES	0	Anzahl erneuter Versuche nach Scheitern eines Vorgangs. Verwenden Sie diese Option, wenn mehrere Sicherungsaufträge mit einer Fehlermeldung abgebrochen werden, nach der die Ressource belegt ist.
BACKOFF_TIME	10 Sekunden	Das Zeitintervall (in Sekunden) zwischen erneuten Versuchen bei gescheitertem Vorgang. Diese Einstellung gilt nur, wenn MAX_RETRIES größer als 0 ist.

## Aktivieren der Verifizierung des SSL-Zertifikats

Wenn Consolidated Backup mit dem VirtualCenter Server oder ESX Server-Host kommuniziert, können Daten über eine verschlüsselte SSL-Verbindung oder einen unverschlüsselten Netzwerkanal übertragen werden.

Verwenden Sie den unverschlüsselten Netzwerkkanal nur, wenn Sie eine vertrauenswürdige Umgebung mit vollständig isolierten Übertragungen zwischen ESX Server-Host und VCB-Proxy erstellen. Die Deaktivierung von SSL kann die Leistung verbessern, da der für die Verschlüsselung notwendige Verarbeitungsaufwand nicht anfällt.

Um jedoch den Kommunikationskanal zu sichern und potenzielle Man-in-the-Middle-Angriffe zu verhindern, aktivieren Sie die Verifizierung des SSL-Zertifikats in Ihrer Consolidated Backup-Umgebung. Die Verifizierung des SSL-Zertifikats ist nicht standardmäßig aktiviert.

---

**HINWEIS** Sie können die Verifizierung des SSL-Zertifikats nur mit ESX Server 3.5 und ESX Server 3i Version 3.5 verwenden. Das Aktivieren der Verifizierung des SSL-Zertifikats in einer gemischten Umgebung, wenn Sie z. B. ESX Server 3.0.x und ESX Server 3.5 ausführen, kann zur Folge haben, dass Sicherungsvorgänge misslingen.

---

Damit die Verifizierung des SSL-Zertifikats gelingt, muss der Hostname auf dem Zertifikat mit dem aktuellen vollqualifizierten Domännennamen des Hosts übereinstimmen, auf dem das Zertifikat verfügbar ist. Bei Verwendung des standardmäßigen selbst signierten Zertifikats stimmen diese Namen nicht überein, und die Verifizierung des Zertifikats misslingt. Um dieses Problem zu beheben, fügen Sie ein von einer anerkannten Zertifizierungsstelle signiertes Zertifikat hinzu. Nähere Informationen finden Sie im Whitepaper *Replacing VirtualCenter Server Certificates*.

### **So aktivieren Sie die Verifizierung des SSL-Zertifikats auf einem VCB-Proxy**

- 1 Rufen Sie im Microsoft Registrierungs-Editor (`regedit.exe`) folgenden Schlüssel auf:  
`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Consolidated Backup`
- 2 Achten Sie darauf, dass der DWORD-Eintrag mit dem folgenden Namen vorhanden ist. Erstellen Sie andernfalls einen neuen.  
`VerifySSLCertificates`
- 3 Um die Verifizierung des SSL-Zertifikats zu aktivieren, setzen Sie den Wert für diesen Eintrag auf 1.
- 4 Stellen Sie über den VI-Client eine Verbindung mit dem ESX Server-Host oder VirtualCenter Server her, wobei Sie die Namen genauso eingeben wie in der Datei `config.js`, der Konfigurationsdatei von Consolidated Backup, angegeben.

Falls ESX Server-Host oder VirtualCenter Server das standardmäßige selbst signierte Zertifikat verwenden, erhalten Sie eine Sicherheitswarnung, die Sie zur Überprüfung des SSL-Fingerabdrucks auffordert.

- 5 Klicken Sie nach Überprüfung des Fingerabdrucks auf Ja (Yes), um das Zertifikat zum Windows-Zertifikatspeicher hinzuzufügen.

Sie können auch die SSL-Zertifikatsauthentifizierung für die Befehlszeilendienstprogramme von ESX Server 3 auf der Servicekonsole aktivieren.

### **So aktivieren Sie die Verifizierung des SSL-Zertifikats auf einer ESX Server 3-Servicekonsole**

- 1 Durch Eingabe des folgenden Befehls an der Servicekonsole erhalten Sie den Fingerabdruck des ESX Server-Hosts:
 

```
openssl x509 -noout -in /etc/vmware/ssl/rui.crt -fingerprint -sha1
```
- 2 Öffnen Sie die Datei `/etc/vmware/backuptools.conf` in einem Editor.
- 3 Legen Sie für `HOST_THUMBPRINT` den Fingerabdruck des ESX Server-Hosts fest. Bei dem Fingerabdruck wird Groß-/Kleinschreibung unterschieden, und Sie müssen ihn genau wie angezeigt eingeben. Das Format des Fingerabdrucks ist `XX:XX:XX:XX:XX:...`, wobei `XX` für Hexadezimalziffern steht.

## **Konfigurieren von SAN**

Wenn Sie SAN zum Speichern der Daten Ihrer virtuellen Maschine verwenden, konfigurieren Sie das SAN-Fabric, mit dem sowohl ESX Server als auch VCB-Proxy verbunden sind.

Um Consolidated Backup nutzen zu können, muss die SAN-Konfiguration den folgenden Anforderungen entsprechen:

- Der VCB-Proxy verfügt über Lese- und Schreibzugriff auf SAN-LUNs, die entweder VMFS-Volumes (Datenspeicher) mit virtuellen Festplatten oder virtuell kompatible RDMs enthalten, die Sie sichern möchten. Fügen Sie hierzu den VCB-Proxy denselben Fabric-Zonen hinzu, zu denen das ESX Server-System gehört.
- Die Einstellungen des Hostmodus (Verbindungstyp) auf VCB-Proxy und ESX Server stimmen überein. Wenn Sie z. B. ein IBM-Array haben und die Einstellung des Hostmodus `LNXCL` lautet, wählen Sie dieselbe Einstellung für den VCB-Proxy.

Weitere Informationen finden Sie in der Dokumentation Ihres SAN-Speicher-Array- und Switch-Anbieters sowie im *SAN-Konfigurationshandbuch (für Fiber-Channel)* und *SAN-Konfigurationshandbuch (für iSCSI)*.

## Verwenden von VMware Consolidated Backup

Da Consolidated Backup in Verbindung mit einer Drittanbietersoftware einsetzbar ist, hängt der Einsatz von Consolidated Backup im Detail von der spezifischen Software ab. Ziehen Sie die `README.html`-Datei zum Integrationsmodul der Sicherungssoftware zu Rate.

Beachten Sie folgende Richtlinien bei der Verwendung von Consolidated Backup:

- Wenn Sie von VirtualCenter eine frühere Version als 2.5 ausführen, erstellen Sie eine Sicherungsrolle, und weisen Sie diesem Konto Sicherungsberechtigungen zu. Siehe „[Erstellen von Sicherungsrollen](#)“ auf Seite 46.
- Wenn mehrere virtuelle Maschinen gesichert werden sollen, sollten diese virtuellen Maschinen in einer Gruppe zusammengefasst und diese Gruppe anschließend durch Konfigurieren von DNS-Aliasen für den Proxy in der Sicherungssoftware als einzelne Instanz verwaltet werden. Siehe „[Gruppieren virtueller Maschinen](#)“ auf Seite 47.

---

**HINWEIS** Consolidated Backup unterstützt maximal 60 gleichzeitig gemountete virtuelle Maschinen. Sie können z. B. gleichzeitig 60 virtuelle Maschinen mit einem C:- bzw. 30 virtuelle Maschinen mit jeweils einem C:- und D:-Laufwerk mounten.

- Nach dem Verknüpfen eines Hostnamens mit einer Gruppe virtueller Maschinen können Sie für jeden Alias einen Sicherungsauftrag einrichten, indem Sie den Alias als Clientnamen für den Job verwenden. Siehe „[Konfigurieren von Sicherungsaufträgen](#)“ auf Seite 48.
- Wenn Sie die erste Sicherung für eine bestimmte virtuelle Maschine durchführen, schalten Sie diese virtuelle Maschine ein. Siehe „[Erstmalige Sicherung](#)“ auf Seite 49.

---

**HINWEIS** Sie können Consolidated Backup nicht zum Sichern virtueller Maschinen in einem Cluster verwenden. Diese virtuellen Maschinen nutzen gemeinsam einen SCSI-Controller, sodass keine Snapshots von ihnen erstellt werden können.

---

## Erstellen von Sicherungsrollen

Verwenden Sie in VirtualCenter 2.5 eine vordefinierte Rolle mit der Bezeichnung „VMware Consolidated Backup-Benutzer“. Wenn Sie eine frühere Version von VirtualCenter verwenden, erstellen Sie eine neue Rolle mit den Sicherungsberechtigungen.

## So erstellen Sie eine VCB-Rolle

- 1 Melden Sie sich am VI-Client als Benutzer mit Administratorberechtigungen an.
- 2 Klicken Sie im VI-Client in der Navigationsleiste auf **Verwaltung (Administration)**.
- 3 Klicken Sie auf die Registerkarte **Rollen (Roles)**.
- 4 Klicken Sie auf **Rolle hinzufügen (Add Role)**.  
Das Dialogfeld **Rolle hinzufügen (Add Role)** wird angezeigt.
- 5 Geben Sie einen Namen für die neue Rolle ein, z. B. „VMware Consolidated Backup-Benutzer“.
- 6 Legen Sie die folgenden Berechtigungen für die neue Rolle fest. Klicken Sie ggf. auf die Pluszeichen (+), um die Listen zu erweitern.
  - Virtuelle Maschine > Konfiguration (Configuration) > Festplatten-Lease (Disk Lease)
  - Virtuelle Maschine > Status (State) > Snapshot erstellen (Create Snapshot)
  - Virtuelle Maschine > Status (State) > Snapshot entfernen (Remove Snapshot)
  - Virtuelle Maschine > Bereitstellung (Provisioning) > VM-Download zulassen (Allow Virtual Machine Download)
  - Virtuelle Maschine > Bereitstellung (Provisioning) > Lesezugriff auf Festplatte zulassen (Allow Read-only Disk Access)
- 7 Klicken Sie auf **OK**, um den Vorgang abzuschließen.

Verknüpfen Sie nach Erstellen der Sicherungsrolle einen bestimmten Benutzer mit dieser Rolle und geben Sie Benutzernamen und Kennwort in der VCB-Konfigurationsdatei an. Siehe „[Konfigurieren von VMware Consolidated Backup](#)“ auf Seite 39.

## Gruppieren virtueller Maschinen

Wenn Sie mehrere virtuelle Maschinen sichern müssen, weisen Sie die virtuellen Maschinen Gruppen zu, und legen Sie verschiedene Aliasse für die Gruppen fest, die alle auf dieselbe IP-Adresse des VCB-Proxys weisen.

Sie können z. B. separate Gruppen für virtuelle Maschinen erstellen, die zu den Abteilungen Accounting, Engineering und Marketing Ihres Unternehmens gehören, die folgenden Aliasse zuweisen und jede Gruppe als einzelne Instanz in Ihrer Sicherungssoftware verwalten:

- vcb-accounting.company.com
- vcb-engineering.company.com

- `vcb-marketing.company.com`

Das Einrichten verschiedener Aliasse bietet Ihnen folgende Möglichkeiten:

- Verknüpfen verschiedener Berechtigungen mit jeder Gruppe virtueller Maschinen. Die Gruppen Accounting, Engineering und Marketing können z. B. jeweils über einen eigenen Satz von Berechtigungen verfügen, die unterschiedlichen Benutzern Rechte zum Sichern und Wiederherstellen gewähren.
- Müheloses Verschieben einer Gruppe virtueller Maschinen auf einen anderen Proxy. Wenn z. B. Ihr Datacenter wächst, können Sie einen neuen Proxy hinzufügen und Aufträge für die Gruppe verschieben, indem Sie den Alias auf den neuen Proxy weisen lassen.

## Konfigurieren von Sicherungsaufträgen

Die Regeln, nach denen Ihre Sicherungssoftware virtuelle Maschinen sichert, sind in Sicherungsaufträgen organisiert. Sicherungsaufträge beschreiben das Sichern der Daten virtueller Maschinen und umfassen die Auswahl eines Namens für den Sicherungsvorgang zur Unterscheidung von anderen Aufträgen sowie der zu sichernden Dateien und des Sicherungstyps, die Einrichtung des Plans usw.

Die Richtlinien zur Konfiguration von Aufträgen zur Sicherung virtueller Maschinen hängen von der jeweiligen Software ab. Weitere Informationen finden Sie in der `README.html`-Datei zum Integrationsmodul Ihrer Drittanbieter-Sicherungssoftware.

Beachten Sie bei der Konfiguration von Sicherungsaufträgen folgende Richtlinien:

- Weisen Sie alle Aufträge dem VCB-Proxy zu.
- Verwenden Sie Aliasse als Namen für die Aufträge.
- Definieren Sie alle Aufträge durch eines der folgenden Verzeichnisse:
  - Dateiebene: `C:\mnt\mytestvm.foo.com\letters\D`
  - Image-Ebene: `C:\mnt\mytestvm.foo.com-fullVM`
- Planen Sie für jeden Auftrag einen bestimmten Ausführungszeitpunkt.
- Wenn Sie gleichzeitig mehrere Sicherungsaufträge auf demselben VCB-Proxy ausführen, beachten Sie, dass die Anzahl der parallel ausführbaren Aufträge bei einzelnen Sicherungsprodukten beschränkt sein kann.

---

**HINWEIS** Sie können auf einer virtuellen Maschine nicht gleichzeitig eine Sicherung auf Dateiebene und eine Sicherung auf Image-Ebene durchführen.

---

## Erstmalige Sicherung

Vor dem Durchführen der ersten Sicherung für eine bestimmte virtuelle Maschine muss die virtuelle Maschine eingeschaltet sein, da die Sicherung andernfalls nicht gelingt.

---

**HINWEIS** Sie müssen eine virtuelle Maschine nicht einschalten, wenn das Integrationsmodul so konfiguriert ist, dass die Anzeigenamen der virtuellen Maschine anstelle von IP-Adressen oder DNS-Namen verwendet werden.

---

Nach der ersten Sicherung einer virtuellen Maschine kann Consolidated Backup jederzeit Sicherungen der virtuellen Maschine durchführen, unabhängig von ihrem Betriebszustand zum Zeitpunkt der Sicherung.

## Erweiterte Konfigurationen

Sie müssen zur Nutzung von Consolidated Backup ggf. erweiterte Konfigurationen vornehmen. Sie können z. B. benutzerdefinierte Skripts zum Erstellen eines Snapshots einer virtuellen Maschine ausführen. Unter Umständen kann es auch erforderlich sein, einen Sicherungsnachbereitungsbefehl zu verwenden, um Sicherungsaufträge für virtuelle Maschinen abubrechen.

## Ausführen benutzerdefinierter Skripts zum außer Betrieb nehmen

Bei der Arbeit mit Consolidated Backup werden virtuelle Maschinen außer Betrieb genommen, sobald Sie eine Sicherung starten.

Zum Erstellen eines Snapshots einer virtuellen Maschine können auch benutzerdefinierte Skripts zum Erfassen des Zustands vor dem Einfrieren und nach dem Auftauen ausgeführt werden. Sie können mithilfe von Skripts z. B. erreichen, dass Sicherungen in virtuellen Windows-Maschinen anwendungskonsistent sind. Stellen Sie die Skripts zur benutzerdefinierten Außerbetriebnahme auf der geschützten virtuellen Maschine bereit, und führen Sie sie dort aus.

Bei der Ausführung von Skripts können Sie den SYNC-Treiber verwenden, eine optionale, mit den VMware Tools installierbare Funktion. Der installierte SYNC-Treiber hält alle E/A-Vorgänge fest, lagert alle „unsauberen“ Daten auf eine Festplatte aus und sorgt so für konsistente Dateisysteme.

Beachten Sie Folgendes:

- Beim Erstellen von Snapshots mithilfe des SYNC-Treibers muss zunächst auf das Leeren der E/A-Vorgänge im Gastbetriebssystem gewartet werden. Dies kann negative Auswirkungen auf zeitkritische Anwendungen wie etwa DBHammer haben.

- Diese Verzögerung durch die E/A-Entleerung können Sie vermeiden, wenn Sie bei der Installation der VMware Tools auf die Installation des SYNC-Treibers verzichten. Die Snapshots sind jedoch nur dann absturzkonsistent, wenn Sie auf dem Gastsystem durch Sicherungsvorbereitungs- und Sicherungsnachbereitungsskripts für eine benutzerdefinierte Außerbetriebnahme sorgen.

Der SYNC-Treiber wird nur von den 32-Bit-Versionen von Windows XP, Windows 2000 und Windows 2003 unterstützt. Da er nicht auf Windows NT 4.0- oder Windows Vista-Gastbetriebssystemen unterstützt wird, ist die Konsistenz des Dateisystems in virtuellen Maschinen, auf denen diese Gastbetriebssysteme ausgeführt werden, nicht gewährleistet.

Bei der Ausführung von Skripten führt Consolidated Backup folgende Schritte aus:

- 1 Das Skript zur Erfassung des Zustands vor dem Einfrieren wird auf der zu sichernden virtuellen Maschine ausgeführt:

- Für Windows:

`C:\Windows\pre-freeze-script.bat`

- Für alle anderen Betriebssysteme:

`/usr/sbin/pre-freeze-script`

Wenn das Skript zur Erfassung des Zustands vor dem Einfrieren einen Exit-Code zurückgibt, der nicht null ist, wird der Snapshot nicht erstellt.

- 2 (Optional) Der SYNC-Treiber wird aktiviert.

Misslingt dieser Schritt, fährt Consolidated Backup mit [Schritt 5](#) fort.

- 3 Ein Snapshot wird erstellt.

- 4 Der SYNC-Treiber wird deaktiviert.

Deaktivieren Sie den SYNC-Treiber, um wieder E/A-Vorgänge zuzulassen. Dieser Schritt kann misslingen, wenn die Erstellung des Snapshots in [Schritt 3](#) zu lange gedauert und zu einer Zeitüberschreitung geführt hat.

- 5 Das Skript zum Erfassen des Zustands nach dem Auftauen wird auf der virtuellen Maschine ausgeführt:

- Für Windows:

`C:\Windows\post-thaw-script.bat`

- Für alle anderen Betriebssysteme:

`/usr/sbin/post-thaw-script`

Bei erfolgreichem Verlauf hat dieses Skript den Exitstatus 0.

## Abbrechen eines Sicherungsauftrags

Wenn ein ausgeführter Sicherungsvorgang von der Drittanbietersoftware abgebrochen wird, kann es vorkommen, dass die virtuelle Maschine auf dem Sicherungs-Proxy nicht unmountet und der Snapshot daher nicht gelöscht wird. Der Grund dafür ist, dass das Bereinigungsskript nicht ausgeführt werden konnte. Beheben Sie dieses Problem, indem Sie den Sicherungsnachbereitungsbefehl für jede virtuelle Maschine manuell ausführen: Alternativ können Sie `vcbCleanup` wie in „[Bereinigung nach misslungenem Sicherungsauftrag](#)“ auf Seite 51 beschrieben ausführen.

### So führen Sie den Sicherungsnachbereitungsbefehl aus

- 1 Überprüfen Sie die Ordner im Verzeichnis `C:\mnt`, um die Hostnamen der virtuellen Maschinen zu bestimmen.
- 2 Führen Sie für jeden Hostnamen einer virtuellen Maschine vom Unterverzeichnis `generic` des Installationsverzeichnisses von Consolidated Backup folgenden Befehl aus:

```
cscript /nologo post-command.wsf <VCB-Installationspfad
["C:\Programme\VMware\VMware Consolidated Backup Framework"]
<VM-Hostname>>
```

## Bereinigung nach misslungenem Sicherungsauftrag

Wenn Sie Consolidated Backup mit einem von VMware bereitgestellten Integrationsmodul zur Sicherung virtueller Maschinen auf Dateiebene verwenden, ruft nach Abschluss der Sicherung eine Sicherungssoftware das Sicherungsnachbereitungsskript auf, um den Snapshot der virtuellen Maschine vom Sicherungs-Proxy zu unmounten und die virtuelle Maschine aus dem Snapshot-Modus herauszunehmen.

Wenn ein Sicherungsauftrag jedoch misslingt, führen manche Sicherungsanwendungen kein Sicherungsnachbereitungsskript aus. Daraus kann resultieren, dass virtuelle Maschinen am Ende des Sicherungszyklus immer noch gemountet sind und im Snapshot-Modus bleiben.

Rufen Sie am Ende des Sicherungszyklus zum Bereinigen von Snapshots und Unmounten virtueller Maschinen in dem in der Datei `config.js` unter `BACKUPROOT` angegebenen Verzeichnis `vcbCleanup` auf.



**VORSICHT** Führen Sie `vcbCleanup` nicht aus, während Sicherungen auf dem VCB-Proxy ausgeführt werden. Dies kann zum Misslingen aktuell ausgeführter Sicherungen führen.

---

Sie können `vcbCleanup` ohne Befehlszeilenoption interaktiv ausführen. Wenn Sie die Option `-y` eingeben, führt das Dienstprogramm die Bereinigung ohne Interaktion durch. So können Sie die Bereinigung nach einem Sicherungszyklus automatisieren.

## Aktualisieren von Consolidated Backup

Wenn Sie frühere Versionen von Consolidated Backup aktualisieren, führen Sie die unten beschriebenen Schritte auf dem VCB-Proxy aus.

### So aktualisieren Sie auf VMware Consolidated Backup Version 1.1

- 1 Aktualisieren Sie durch Ausführung des Installationsprogramms von VMware Consolidated Backup 1.1 auf die aktuelle Version von Consolidated Backup.
- 2 Rufen Sie die Eingabeaufforderung auf, und geben Sie `net stop vmount2` ein, um ggf. ausgeführte `vmount`-Dienste anzuhalten.
- 3 Führen Sie das Dienstprogramm `Diskpart` aus, und entfernen Sie mithilfe des Befehls `automount scrub` die Registrierungseinstellungen für vorher gemountete virtuelle Maschinen.

Anweisungen zur Ausführung von `Diskpart` finden Sie unter „[So deaktivieren Sie Zuweisungen von Laufwerkbuchstaben](#)“ auf Seite 37.

- 4 Bereinigen Sie das Verzeichnis `C:\Windows\Temp`, um temporäre Dateien zu entfernen, die sich ggf. angesammelt haben.

# Wiederherstellung und Rettung von Daten

---

# 3

In diesem Kapitel wird beschrieben, wie Sie Daten wiederherstellen und retten können. Bedenken Sie, dass die Wiederherstellung von Daten umso schwieriger ist, je höher die Anzahl der Agenten ist, die Sie einsetzen.

Dieses Kapitel enthält die folgenden Informationen:

- [„Wiederherstellen virtueller Maschinen mittels VMware Consolidated Backup“](#) auf Seite 54
- [„Datenwiederherstellung“](#) auf Seite 56

## Wiederherstellen virtueller Maschinen mittels VMware Consolidated Backup

Consolidated Backup unterstützt Sie bei der Wiederherstellung einer ganzen virtuellen Maschine auf Image-Ebene und der Daten oder Dateien einer virtuellen Festplatte auf Dateiebene.

Spezifische Anweisungen zur Wiederherstellung finden Sie in der Dokumentation, die mit dem Integrationsmodul für Ihre Sicherungssoftware geliefert wird.

VMware unterstützt folgende Wiederherstellungsvorgänge:

- Wiederherstellung auf Image-Ebene
  - Stellen Sie ein VCB-Image Ihrer virtuellen Maschine mittels VMware Converter wieder her. Siehe [„Verwenden von VMware Converter zum Wiederherstellen von Images virtueller Maschinen“](#) auf Seite 55.
  - (nur ESX Server 3) Stellen Sie Ihre virtuelle Maschine mittels des Befehlszeilendienstprogramms vcbRestore wieder her. Siehe [„Verwenden des Dienstprogramms vcbRestore zum Wiederherstellen virtueller Maschinen“](#) auf Seite 55.
- Wiederherstellung auf Dateiebene
  - Auf der virtuellen Maschine ist keine Sicherungssoftware installiert. Die Wiederherstellung der Daten wird vom Administrator auf einem öffentlichen Netzwerkbereich eines Sicherungs-Proxys durchgeführt, auf den die geschützte virtuelle Maschine zugreifen kann. Siehe [„Zentrales Wiederherstellen von Daten“](#) auf Seite 55.
  - Auf dedizierten virtuellen Maschinen ist Sicherungssoftware installiert, und Daten werden auf virtuelle Zielmaschinen verschoben. Siehe [„Wiederherstellen von Daten in Gruppen“](#) auf Seite 56.
  - Auf jeder geschützten virtuellen Maschine ist Sicherungssoftware installiert. Die Wiederherstellung der Daten wird direkt vom Administrator oder Benutzer durchgeführt. Siehe [„Direktes Wiederherstellen auf eine virtuelle Maschine“](#) auf Seite 56.

## Verwenden von VMware Converter zum Wiederherstellen von Images virtueller Maschinen

Sie können VMware Converter ab Version 3.0.1 zum Wiederherstellen von VCB-Images virtueller Maschinen auf virtuellen Maschinen verwenden, die gerade ausgeführt werden. Mithilfe des in VirtualCenter integrierten VMware Converter können Sie die Dateien Ihrer virtuellen Maschine direkt über den VI-Client auf einem anderen Datenspeicher, Host oder Ressourcenpool wiederherstellen.

Informationen über den VMware Converter finden Sie unter [www.vmware.com/products/converter/](http://www.vmware.com/products/converter/).

## Verwenden des Dienstprogramms vcbRestore zum Wiederherstellen virtueller Maschinen

Das Dienstprogramm vcbRestore ist ein Befehlszeilendienstprogramm, das Sie zum Wiederherstellen von Daten verwenden, die mit einer image-basierten Sicherung gesichert wurden. vcbRestore wird auf der ESX Server 3-Servicekonsole ausgeführt.

Informationen zur Verwendung dieses Dienstprogramms finden Sie unter „[Sichern und Wiederherstellen von virtuellen Maschinen mithilfe der Servicekonsole](#)“ auf Seite 61.

## Zentrales Wiederherstellen von Daten

Zum zentralen Wiederherstellen von Daten benötigen Sie eine Gruppe virtueller Maschinen auf dem ESX Server, einen Proxy und einen Sicherungs-Agenten auf einer dedizierten virtuellen Maschine des Proxys, die für die Wiederherstellung der Daten verwendet werden soll. Die Daten werden mithilfe der Sicherungssoftware auf den Proxy übertragen, auf dem der Agent ausgeführt wird. Nachdem der Administrator die Daten auf dem Zentralserver wiederhergestellt hat, können Sie die Daten mithilfe des Protokolls des Common Internet File System (CIFS) für die gemeinsame Nutzung von Dateien und Remotezugriff auf die virtuelle Maschine zurückkopieren.

Vorteile: Die Anzahl der beizubehaltenden Agenten ist minimal.

Nachteile: Aufgrund der zentralen Datenwiederherstellung muss ein Administrator in die Wiederherstellung auf Dateiebene einbezogen werden.

## Wiederherstellen von Daten in Gruppen

Beim Wiederherstellen von Daten in Gruppen verfügt eine virtuelle Maschine über einen Sicherungs-Agenten für jede Gruppe (Buchhaltung, Technik, Marketing). Für jede Gruppe stellt der Gruppenadministrator die Abläufe auf einem Host zur Wiederherstellung von Daten wieder her. Die Dateien werden mithilfe der CIFS-Dateifreigabe auf eine virtuelle Zielmaschine kopiert.

Vorteile:

- Die Wiederherstellung von Daten kann delegiert werden.
- Dieses Verfahren ist ein guter Kompromiss zwischen der Anzahl der Agenten und dem Aufwand, der für die Wiederherstellung von Daten betrieben werden muss.

Nachteile: Die Wiederherstellung der Daten kann nicht vollständig im Self-Service erfolgen.

## Direktes Wiederherstellen auf eine virtuelle Maschine

Auf jeder virtuellen Maschine befinden sich Sicherungs-Agenten. Mithilfe dieser Agenten kann der Benutzer Daten auf Bandlaufwerken sichern und wiederherstellen. Zur Wiederherstellung der Daten wird der Sicherungs-Agent der virtuellen Maschine verwendet.

Vorteile: Es handelt sich um eine Self-Service-Wiederherstellung.

Nachteile: Auf jeder virtuellen Maschine müssen Agenten installiert sein.

## Datenwiederherstellung

Die folgenden Richtlinien können Ihnen bei der Wiederherstellung von Daten helfen:

- Achten Sie darauf, dass Sie über Sicherungen virtueller Maschinen auf Image-Ebene verfügen.
- Sichern Sie Ihre VirtualCenter-Datenbank.
- Stellen Sie sicher, dass Sie über alle erforderlichen Lizenzschlüssel verfügen.
- Stellen Sie sicher, dass Sie über eine ausreichende Anzahl an Servern zur Ausführung aller virtuellen Maschinen verfügen, die Sie wiederherstellen möchten.

Durch Aktivieren der Migration mit VMotion oder den Einsatz von DRS können Sie Ihre Möglichkeiten zur Notfallwiederherstellung erheblich erweitern.

# Sicherungsszenarien und Fehlerbehebung

---

# 4

In diesem Kapitel werden reale Szenarien beschrieben, die Sie bei der Planung Ihrer Sicherungsstrategien unterstützen sollen.

Dieses Kapitel enthält die folgenden Informationen:

- [„Szenarien zur Sicherungsanwendung“](#) auf Seite 58
- [„Typisches Anwendungsszenario für Consolidated Backup“](#) auf Seite 58
- [„Fehlerbehebung“](#) auf Seite 59

## Szenarien zur Sicherungsanwendung

Die folgenden Nutzungen werden am häufigsten empfohlen:

- **Datencenter**
  - Führen Sie auf Dateiebene jede Nacht Sicherungen durch.
  - Führen Sie auf Image-Ebene für Windows regelmäßige und für Linux jede Nacht Sicherungen durch. Dies ist ein Notfallwiederherstellungs-Szenario.
- **Agenten auf virtuellen Maschinen.** Führen Sie inkrementelle Sicherungen für Linux durch.
- **Sicherungsserver auf einer virtuellen Maschine.** Setzen Sie für Niederlassungen ebenfalls Agenten auf virtuellen Maschinen ein.

## Typisches Anwendungsszenario für Consolidated Backup

Dies ist ein Beispiel für den Einsatz von Consolidated Backup zum Schutz von Daten auf virtuellen Maschinen:

- 1 Der Systemadministrator konfiguriert Sicherungspläne und -richtlinien in der Drittanbieter-Sicherungssoftware.

Der Systemadministrator kann z. B. die Sicherungssoftware anweisen, täglich um 3:05 Uhr `D:\Data` auf `vm37.company.com` zu sichern.

- 2 Die Sicherungssoftware plant diesen Sicherungsauftrag.
- 3 Wenn die Sicherungssoftware diesen Auftrag startet, ruft sie mithilfe eines Sicherungsvorbereitungsskripts Consolidated Backup auf.

Consolidated Backup führt folgende Schritte durch:

- a Herstellen des Kontakts zu einer VirtualCenter-Instanz oder einem ESX Server-Host und Senden einer Anforderung zum Erstellen eines Snapshots der zu sichernden virtuellen Maschine.
  - b Bereitstellen (Mounten) dieses Snapshots auf dem Sicherungs-Proxy. So werden die zu sichernden Daten für die Drittanbieter-Sicherungssoftware sichtbar.
- 4 Die Drittanbieter-Sicherungssoftware führt den Sicherungsvorgang des Kopierens geänderter Daten auf das Sicherungsmedium durch.

- 5 Am Ende des Sicherungsauftrags ruft die Drittanbieter-Sicherungssoftware mithilfe eines Sicherungsnachbereitungsskripts Consolidated Backup auf.  
Consolidated Backup führt folgende Schritte durch:
  - a Trennen (Unmounten) des Snapshots vom Sicherungs-Proxy.
  - b Senden einer Anforderung an VirtualCenter oder ESX Server-Host, den Snapshot der virtuellen Maschine zu entfernen.

## Fehlerbehebung

In diesem Abschnitt werden Sie über Probleme informiert, die beim Durchführen von Sicherungen auftreten können.

In diesem Abschnitt werden folgende Themen behandelt:

- „Ändern der Sicherungsrichtlinien nach ESX Server-Upgrades“ auf Seite 59
- „Identifizieren von VMFS-Volumes in GUI der Sicherungssoftware“ auf Seite 59

### Ändern der Sicherungsrichtlinien nach ESX Server-Upgrades

Wenn Sie ESX Server 2.x auf 3.x aktualisiert haben, müssen Sie alle VMFS-Volume-Pfade ändern, die Sie in der Sicherungssoftware konfiguriert haben. Ein Pfadformat in ESX Server 3.x unterscheidet sich vom ESX Server 2.x-Format und entspricht diesem Standard:

- VMFS-Volume  
`/vmfs/volumes/<Dateisystem-UUID>`  
 oder  
`/vmfs/volumes/<Dateisystembezeichnung>`
- VMFS-Datei  
`/vmfs/volumes/<Dateisystembezeichnung|Dateisystem-UUID>/[dir]/myDisk.vmdk`

### Identifizieren von VMFS-Volumes in GUI der Sicherungssoftware

Wenn Sie einen Sicherungs-Agenten in der Servicekonsole für Sicherungen auf Dateiebene verwenden, arbeiten Sie mit VMFS-Volumes.

Unter ESX Server 3.x werden VMFS-Volumes anhand eindeutiger Bezeichner identifiziert. Die Namen der Verzeichnisse, in denen die einzelnen VMFS-Volumes unter `/vmfs/volumes` gemountet werden, entsprechen diesen eindeutigen

Bezeichnen. Die eindeutigen Bezeichner werden den Volumes während der Formatierung automatisch zugewiesen. Sie können sie nicht ändern.

VMFS-Volumes können benutzerfreundliche Bezeichnungen aufweisen. Diese Bezeichnungen werden unter `/vmfs/volumes` als symbolische Links angezeigt, die auf das jeweilige Verzeichnis zeigen. Für ein VMFS-Volume mit dem eindeutigen Bezeichner `43a0552e-ae6093b2-47a1-00145e0a7ec0` und der Bezeichnung `storage1` werden z. B. unter `/vmfs/volumes` folgende Einträge erstellt:

- Ein Verzeichnis namens `43a0552e-ae6093b2-47a1-00145e0a7ec0`, in dem das Dateisystem gemountet wird.
- Ein symbolischer Link namens `storage1`, der auf das Verzeichnis `43a0552e-ae6093b2-47a1-00145e0a7ec0` zeigt.

Grafische Benutzeroberflächen (GUIs) von Sicherungssoftware, die eine Auswahl zu sichernder Dateien ermöglichen, zeigen im entsprechenden Fenster zum Durchsuchen von Verzeichnissen nur das Verzeichnis (die eindeutige ID) an. Wenn Sie nur die Bezeichnung des VMFS-Volumes kennen, könnte es für Sie schwierig sein, das VMFS-Volume im GUI-Verzeichnis zu finden.

### **So identifizieren Sie ein VMFS-Volume anhand seiner Bezeichnung**

- 1 Durchsuchen Sie in der Benutzeroberfläche der Sicherungssoftware das Verzeichnis `/vmfs/volumes`.

Die symbolischen Links, die auf die VMFS-Volume-Mount-Punkte zeigen, werden im Fenster zur Auswahl von Dateien angezeigt.

- 2 Mithilfe dieser Einträge können Sie die eindeutige ID der gewünschten Dateisystembezeichnung finden.
- 3 Wählen Sie im Verzeichnisfenster das Verzeichnis aus, das dieser eindeutigen ID entspricht, um es zu durchsuchen.

Beim Durchführen dateibasierter Sicherungen verwendet die Sicherungsanwendung Pfade, die auf den eindeutigen Bezeichner verweisen, sodass die gesicherten Dateien wie folgt angezeigt werden:

```
/vmfs/volumes/43a0552e-ae6093b2-47a1-00145e0a7ec0/vm01/vm01.vmdk
```

Beim Wiederherstellen von Dateien mithilfe der Sicherungsanwendung müssen Sie unter Umständen eine umgekehrte Zuordnung vornehmen, um die VMFS-Volume-Bezeichnung (in diesem Beispiel `storage1`) zu finden, die diesem eindeutigen Bezeichner entspricht. Sichern Sie hierzu die symbolische Verknüpfung selbst, während Sie Sicherungen durchführen.

# Sichern und Wiederherstellen von virtuellen Maschinen mithilfe der Servicekonsole

---



In diesem Anhang wird beschrieben, wie die Daten virtueller Maschinen mithilfe der ESX Server 3-Servicekonsole gesichert und wiederhergestellt werden. Sie werden in diesem Anhang Schritt für Schritt durch den Vorgang des Konfigurierens der Consolidated Backup-Befehlszeilendienstprogramme geführt. Außerdem enthält dieser Anhang Beispiele für die Verwendung dieser Dienstprogramme.

---

**HINWEIS** Da ESX Server 3i nicht über eine Servicekonsole verfügt, sind die Informationen in diesem Kapitel nicht auf ESX Server 3i anwendbar. Um auf Imageebene Sicherungen virtueller Maschinen auf einem ESX Server 3i-Host durchzuführen, der nicht über SAN-Zugriff verfügt, verwenden Sie Consolidated Backup im LAN-Modus, und führen Sie das Programm auf einer virtuellen Maschine aus.

---

Dieser Anhang enthält die folgenden Abschnitte:

- „Allgemeine Konfigurationseinstellungen für Consolidated Backup-Dienstprogramme“ auf Seite 62
- „Sichern von virtuellen Maschinen“ auf Seite 64
- „Archivieren virtueller Maschinen“ auf Seite 69
- „Wiederherstellen von virtuellen Maschinen“ auf Seite 69

## Allgemeine Konfigurationseinstellungen für Consolidated Backup-Dienstprogramme

Bearbeiten Sie vor dem Verwenden der Consolidated Backup-Dienstprogramme der Servicekonsole die Konfigurationsdatei `/etc/vmware/backuptools.conf`, um die am häufigsten verwendeten Parameter dieser Tools einzustellen.

Da die Konfigurationsdatei als Bourne-Shell-Skript analysiert wird, sollten Sie beim Bearbeiten der Datei die Konventionen für die Syntax der Bourne-Shell beachten:

- Verwenden Sie das Zeichen `#`, um einen Kommentar zu kennzeichnen.
- Verwenden Sie bei der Eingabe von Variablen keine Leerzeichen. Beispiel: Bei `F00="bar"` darf vor und hinter dem Gleichheitszeichen kein Leerzeichen stehen.
- Setzen Sie vor Sonderzeichen (zum Beispiel `$`) einen umgekehrten Schrägstrich (Backslash). Zum Beispiel: `\$server`.

Administratoren, die Erfahrung mit der Programmierung von Bourne-Shell-Skripten haben, können alle standardmäßigen Bourne-Shell-Mechanismen wie die Befehlsausführung (zum Beispiel `'foo'`) oder Umgebungsvariablen einsetzen.

## Einstellungen der Konfigurationsdatei

Richten Sie mithilfe der Konfigurationsdatei `/etc/vmware/backuptools.conf` die folgenden Optionen ein:

- **VCHOST**

Gibt den URL der VirtualCenter-Instanz an, die den ESX Server 3-Host verwaltet, dessen Daten gesichert oder wiederhergestellt werden. VCHOST sollte auf die VirtualCenter-Instanz zeigen, die den Host verwaltet.

Wenn Sie die Sicherung oder das Wiederherstellen von Daten auf einem eigenständigen Host durchführen, können Sie als Hostnamen `localhost` verwenden.

---

**HINWEIS** Um diese Einstellung zu überschreiben, können Sie für jedes Consolidated Backup-Befehlszeilendienstprogramm die Befehlszeilenoption `-h` verwenden.

---

- **USERNAME**

Gibt den Benutzernamen für die Anmeldung bei der durch VCHOST definierten Instanz von VirtualCenter an. Der Benutzer muss über die Rechte zum Registrieren oder Erstellen von virtuellen Maschinen verfügen.

---

**HINWEIS** Um diese Einstellung zu überschreiben, können Sie für jedes Consolidated Backup-Befehlszeilendienstprogramm die Befehlszeilenoption `-u` verwenden.

---

■ **PASSWORD**

Gibt das jeweilige Kennwort für den entsprechenden USERNAME an. Mithilfe dieser Option können Sie auf nicht interaktive Weise Sicherungen virtueller Maschinen durchführen.



**VORSICHT** Da die Angabe eines Kennworts in einer Konfigurationsdatei ein Sicherheitsrisiko darstellen kann, sollten Sie unbedingt sicherstellen, dass die Servicekonsole ausschließlich von ESX Server 3-Administratoren verwendet wird.

---

---

**HINWEIS** Um diese Einstellung zu überschreiben, können Sie für jedes Consolidated Backup-Befehlszeilendienstprogramm die Befehlszeilenoption `-p` verwenden.

---

■ **VMNAMECACHE**

Üblicherweise wird eine virtuelle Maschine für Backups anhand ihres DNS-Namens oder ihrer IP-Adresse ausgewählt. Bei der Sicherung einer virtuellen Maschine auf einem eigenständigen ESX Server 3-Host kann der ESX Server 3-Host die IP-Adresse jedoch nur dann erkennen, wenn die virtuelle Maschine eingeschaltet ist und auf ihr die VMware Tools ausgeführt werden.

Um auch bei einer ausgeschalteten virtuellen Maschine auf einem eigenständigen ESX Server 3-Host Sicherungen dieser virtuellen Maschine durchführen zu können, sollten Sie eine Cachedatei vorhalten. In dieser Cachedatei wird bei jeder Sicherung der virtuellen Maschine deren IP-Adresse aufgezeichnet. Auf diese Weise können auch in Zukunft Sicherungen dieser virtuellen Maschine unabhängig von ihrem Betriebszustand durchgeführt werden.

VMware empfiehlt Ihnen, diese Voreinstellung nicht zu ändern.

---

**HINWEIS** Mit der Befehlszeilenoption `-c` für `vcbMounter` können Sie diese Einstellung überschreiben. Der Befehl `vcbRestore` verwendet diese Einstellung nicht.

---

- **TEMPDIR**

Wenn Sie die Funktionen zum sicheren Kopieren der Consolidated Backup-Befehlszeilendienstprogramme verwenden, können Sie mithilfe dieser Option einen temporären Speicherort für die Daten einer virtuellen Maschine festlegen.

Dieser Speicherort muss über ausreichend freien Speicherplatz verfügen, um auch die Daten der größten virtuellen Maschine aufnehmen zu können.

---

**HINWEIS** Sie können diese Einstellung nicht von der Befehlszeile aus überschreiben.

---

## Sichern von virtuellen Maschinen

Mithilfe von `vcbMounter` können Sie ganze virtuelle Maschinen in der Servicekonsole sichern. Das Dienstprogramm `vcbMounter` erstellt einen eingefrorenen Snapshot der virtuellen Maschine und exportiert den Snapshot in eine Gruppe von Dateien, die später zum Wiederherstellen der virtuellen Maschine verwendet werden kann. Zum Sichern dieser Gruppe von Dateien können Sie jede dateibasierte Sicherungssoftware eines Drittanbieters verwenden.

Legen Sie vor der Sicherung einer virtuellen Maschine mithilfe von `vcbMounter` Folgendes fest:

- Welche virtuelle Maschine gesichert werden soll.  
Siehe „[Auswählen von virtuellen Maschinen](#)“ auf Seite 66.
- Wo die Sicherungsdaten gespeichert werden sollen.

Die Consolidated Backup-Servicekonsole unterstützt verschiedene Transport-Plug-Ins für das Sichern der Daten von virtuellen Maschinen in einem lokalen Verzeichnis oder mithilfe von `scp` in einem Remoteverzeichnis. Siehe „[Festlegen von Sicherungszielen](#)“ auf Seite 68.

## Durchführen von Sicherungen

Geben Sie nach dem Einstellen von Konfigurationsoptionen gemäß der Beschreibung unter „[Einstellungen der Konfigurationsdatei](#)“ auf Seite 62 in der Befehlszeile den folgenden Befehl ein:

```
vcbMounter -a <virtual_machine_identifizier> -r <backup_destination> -m  
<cos|nbd|nbdssl> ,
```

wobei

- `<virtual_machine_identifizier>` ein eindeutiger Bezeichner der virtuellen Maschine ist, die Sie sichern. Siehe „[Auswählen von virtuellen Maschinen](#)“ auf Seite 66.
- `<backup_destination>` den Speicherort der Sicherungsdaten angibt. Siehe „[Festlegen von Sicherungszielen](#)“ auf Seite 68.
- `<cos|nbd|nbdssl>` legt den Transportmodus für `vcbMounter` fest:
  - `cos` – Verwenden Sie diese Option zum Sichern virtueller Maschinen, auf deren Festplatten der ESX Server-Host direkt über `/vmfs/volumes` zugreifen kann. Führen Sie das Dienstprogramm `vcbMounter` in der Servicekonsole des ESX Server-Hosts aus, auf dem sich die virtuellen Maschinen befinden, oder auf einem beliebigen ESX Server-Host, der auf den Datenspeicher zugreifen kann, auf dem die Festplatten der virtuellen Maschine gespeichert sind.
  - `nbd` – Verwenden Sie diese Option zum Sichern virtueller Maschinen über das Netzwerk von einem anderen ESX Server-Host aus als dem, auf dem Sie das Dienstprogramm `vcbMounter` ausführen. Wählen Sie diese Option, falls Sie keine Daten der virtuellen Festplatte für die Übertragung über das Netzwerk verschlüsseln müssen.
  - `nbdssl` – Verwenden Sie diese Option zum Sichern virtueller Maschinen über das Netzwerk von einem anderen ESX Server-Host aus als dem, auf dem Sie das Dienstprogramm `vcbMounter` ausführen. Wählen Sie diese Option, falls Sie Daten der virtuellen Festplatte für die Übertragung über das Netzwerk verschlüsseln müssen.

Gehen Sie wie in diesen Beispielen beschrieben vor, um virtuelle Maschinen zu sichern:

- Sichern der virtuellen Maschine `vm37.company.com` im lokalen Verzeichnis `/home/VMs/vm37`:

```
vcbMounter -a ipaddr:vm37.company.com -r /home/VMs/vm37
```

- Sichern der virtuellen Maschine `vm37.company.com` im Verzeichnis `/backups/VMs/vm37`. Das Verzeichnis befindet sich auf dem Remoteserver `backups.company.com` mit der Benutzer-ID `vmware`. Der Host `backups.company.com` führt einen Secure-Shell-Server (`ssh`) aus. Mithilfe des Consolidated Backup-Plug-Ins zum sicheren Kopieren (`scp`) können Sie die virtuelle Maschine auf `backups.company.com` übertragen.

```
vcbMounter -a ipaddr:vm37.company.com -r  
scp://vmware@backups.company.com:/backups/VMs/vm37
```

- Sichern einer virtuellen Maschine auf einem eigenständigen ESX Server 3-Host. Verwenden Sie zum Auswählen der virtuellen Maschine den im VI-Client angezeigten Namen der virtuellen Maschine. Die virtuelle Maschine wird im lokalen Verzeichnis `/home/VMs/vm37` gesichert.

```
vcbMounter -a name:"Virtual Machine 37" -r /home/VMs/vm37
```

---

**HINWEIS** Beim Argument des Namens der virtuellen Maschine auf Groß-/Kleinschreibung achten.

---

## Auswählen von virtuellen Maschinen

Sie können verschiedene Standards verwenden, um die virtuelle Maschine anzugeben, die Sie sichern möchten.

### Auswählen von virtuellen Maschinen mithilfe des DNS-Namens oder der IP-Adresse

Üblicherweise wird eine virtuelle Maschine anhand ihres DNS-Namens oder ihrer IP-Adresse ausgewählt. Verwenden Sie zum Auswählen einer virtuellen Maschine die folgende Spezifikation:

```
ipaddr:<DNS-Name oder IP-Adresse>
```

Zur Auswahl der virtuellen Maschine `vm37.company.com` mit der IP-Adresse `10.17.5.12` kann z. B. eine der folgenden Spezifikationen für die Suche verwendet werden:

- `ipaddr:vm37.company.com`
- `ipaddr:10.17.5.12`

### Auswählen von virtuellen Maschinen mithilfe des BIOS-UUIDs

Eine virtuelle Maschine kann auch anhand ihres universellen, eindeutigen Bezeichners (Universally Unique Identifier, UUID) ausgewählt werden. Verwenden Sie für die Suche folgende Spezifikation:

```
uuid:<uuid>
```

Beispiel:

```
uuid:564d78a1-8c1c-59b4-fa02-be14138797be
```

## Auswählen von virtuellen Maschinen mithilfe von Managed Object References (MoRefs)

Intern verweisen VirtualCenter und ESX Server 3 mithilfe von Managed Object References (MoRefs) auf Objekte. Gehen Sie zum Auswählen einer virtuellen Maschine mittels MoRefs wie in den folgenden Beispielen vor:

- `moref:vm-00027` – Verwenden Sie dieses Format beim Zugriff auf den VirtualCenter Server.
- `moref:248` – Verwenden Sie dieses Format beim Zugriff auf den ESX Server 3-Host.

Da sich MoRefs jedes Mal ändern, wenn der VirtualCenter Server oder die Hostinstanz, zu dem oder der Consolidated Backup eine Verbindung herstellt, neu gestartet wird, sollten Sie zum Auswählen von virtuellen Maschinen keine MoRefs einsetzen. Beim Ausführen eines Shell-Skripts zum Sichern von virtuellen Maschinen können Sie jedoch MoRefs einsetzen, um virtuelle Maschinen auszuwählen.

Sie können zum Beispiel ein Skript schreiben, das `vcbVmName` mit der Suchspezifikation `any`: verwendet, um eine Liste aller virtuellen Maschinen zu erhalten, und mithilfe benutzerdefinierter Filterung eine Liste erzeugen, die nur die virtuellen Maschinen enthält, die Sie sichern möchten. Die virtuellen Maschinen in dieser Liste können als Bezeichner MoRefs verwenden. In einem weiteren Teil des Skripts könnten Sie festlegen, dass für jede dieser MoRefs `vcbMounter` aufgerufen wird, um die Sicherungsvorgänge durchzuführen.

In solchen Fällen ist es sinnvoll, statt anderer Bezeichner (zum Beispiel UUID) MoRefs zu verwenden, da der Suchaufwand geringer ist, weil nicht bei jeder Verwendung des Bezeichners die gesamte Liste aller virtuellen Maschinen analysiert werden muss.

## Anzeigen von Informationen über virtuelle Maschinen

Verwenden Sie `vcbVmName`, um nach einer bestimmten virtuellen Maschine zu suchen und Informationen über diese Maschine anzuzeigen.

Gehen Sie wie in diesen Beispielen vor:

- `vcbVmName -s powerstate:on` – Zum Auflisten aller eingeschalteten virtuellen Maschinen.
- `vcbVmName -s any`: – Zum Auflisten aller bekannten virtuellen Maschinen.
- `vcbVmName -s ipaddr:vm37.company.com` – Zum Anzeigen von Informationen über die virtuelle Maschine mit der angegebenen Adresse.

Nach der Eingabe von `vcbVmName` wird zum Beispiel Folgendes angezeigt:

```
bash #vcbVmName -s name:vm37.company.com Found VM:
moref:192
name:Virtual Machine 37
uuid:564d78a1-8c1c-59b4-fa02-be14138797be
ipaddr:10.17.5.31
```

## Festlegen von Sicherungszielen

Sie können eine virtuelle Maschine entweder in einem lokalen Verzeichnis oder mithilfe von `scp` auf einem Remoteserver sichern.

### Sichern in einem lokalen Verzeichnis

Geben Sie beim Sichern einer virtuellen Maschine in einem lokalen Verzeichnis den Pfad zu dem Verzeichnis an, z. B. `/home/VMs/vm37`.

---

**HINWEIS** Sie müssen vorab kein Zielunterverzeichnis (z. B. `/home/VMs/vm37`) erstellen, weil es automatisch durch den Sicherungsvorgang angelegt wird. Das Verzeichnis, in dem das Zielunterverzeichnis aufgeführt ist, also z. B. `/home/VMs`, muss jedoch bereits vorhanden sein, bevor Sie den Sicherungsvorgang starten.

---

### Sichern auf einem Remoteserver

Zum Sichern einer virtuellen Maschine auf einem Remoteserver können Sie ein entsprechendes `scp`-Plug-In mit folgender Syntax verwenden.

```
scp://<user>@<host>:<path>
```

Verwenden Sie zum Durchführen einer automatischen `scp`-Sicherung die schlüsselbasierte RSA-Authentifizierung. In diesem Fall wird `scp` Sie während der Sicherung nicht zur Eingabe eines Kennworts auffordern.

Wenn Sie z. B. eine virtuelle Maschine im Verzeichnis `/backup/VMs/vm37` sichern möchten, das sich auf dem Remoteserver `backups.company.com` mit der Benutzer-ID `vmware` befindet, geben Sie Folgendes ein:

```
scp://vmware@backups.company.com:/backups/VMs/vm37
```

---

**HINWEIS** Überprüfen Sie vor dem Start der Sicherung, dass sich auf dem Remoteserver bereits das Verzeichnis `/backups/VMs` befindet. Das Verzeichnis `/backups/VMs/vm37` müssen Sie jedoch nicht erstellen, da es während des Sicherungsvorgangs automatisch erstellt wird.

---

## Archivieren virtueller Maschinen

Erstellen Sie mit `vcSnapAll` ein Archiv von Gruppen virtueller Maschinen in der Servicekonsole. Das Dienstprogramm `vcSnapAll` hat dieselbe Funktionalität wie `vcMounter`, kann jedoch zusätzlich Gruppen virtueller Maschinen identifizieren.

Verwenden Sie folgende Syntax:

```
vcSnapAll -a <virtual_machine_identifizier> -r <backup_destination>  
          -m<cos|nbd|nbdssl> ,
```

wobei `<virtual_machine_identifizier>` eine Gruppe virtueller Maschinen bestimmt. Verwenden Sie eine der folgenden Spezifikationen:

- `powerstate: on|off|suspended` – Zur Suche aller virtuellen Maschinen mit dem angegebenen Betriebszustand.
- `any` : – Zur Suche aller virtuellen Maschinen.
- `none` : – Nicht zur Suche virtueller Maschinen. Diese Option wird ausschließlich zum Testen verwendet.

Sie können auch einen der eindeutigen Bezeichner der virtuellen Maschine verwenden. Siehe „[Auswählen von virtuellen Maschinen](#)“ auf Seite 66.

Das Sicherungszielverzeichnis muss vor Starten des Archivierungsvorgangs mittels `vcSnapAll` vorhanden sein. Während der Ausführung erstellt das Dienstprogramm `vcSnapAll` für jede virtuelle Maschine, die die Suchkriterien erfüllt, innerhalb des Sicherungszielverzeichnisses ein Unterverzeichnis. Sie müssen die Unterverzeichnisse nicht vorab erstellen.

Nachdem Sie die Sicherungsdaten der virtuellen Maschine vom Sicherungszielverzeichnis in einen sekundären Speicher verschoben haben, können Sie die Inhalte des Verzeichnisses löschen.

## Wiederherstellen von virtuellen Maschinen

Sie können eine virtuelle Maschine an ihrem ursprünglichen oder einem anderen Speicherort wiederherstellen.

## Wiederherstellen von virtuellen Maschinen am ursprünglichen Speicherort

Wenn Sie alle Konfigurationsoptionen wie unter „[Einstellungen der Konfigurationsdatei](#)“ auf Seite 62 beschrieben eingerichtet haben, müssen Sie zur Wiederherstellung einer virtuellen Maschine nur noch den folgenden Befehl an `vcbRestore` weiterleiten:

```
vcbRestore -s <Sicherungsverzeichnis>
```

Siehe „[Festlegen von Sicherungszielen](#)“ auf Seite 68.

Gehen Sie wie in diesen Beispielen beschrieben vor, um virtuelle Maschinen wiederherzustellen:

- Wiederherstellen einer virtuellen Maschine aus einem lokalen Verzeichnis namens `/home/VMs/vm37`:

```
vcbRestore -s /home/VMs/vm37
```

- Wiederherstellen einer virtuellen Maschine vom Remoteserver `backup.company.com`, Verzeichnis `/backups/VMs/vm37`, Benutzer-ID `vmware`:

```
vcbRestore -s scp://vmware@backup.company.com:/backups/VMs/vm37
```

## Wiederherstellen von virtuellen Maschinen an einem alternativen Speicherort

Um eine virtuelle Maschine an einem anderen als dem ursprünglichen Speicherort oder auf einem anderen ESX Server 3-Host wiederherzustellen, verwenden Sie dazu die `catalog`-Datei der virtuellen Maschine. Das Dienstprogramm `vcbMounter` erstellt diese Datei für jede virtuelle Maschine, die es sichert. Die `catalog`-Datei enthält zusammengefasste Informationen über die virtuelle Maschine, zum Beispiel ihren Anzeigenamen, den Betriebszustand zum Zeitpunkt der Sicherung usw.

### So stellen Sie eine virtuelle Maschine an einem alternativen Speicherort wieder her

- 1 Kopieren Sie die `catalog`-Datei der virtuellen Maschine.  
Siehe „[Kopieren einer „catalog“-Datei](#)“ auf Seite 71.
- 2 Geben Sie in der Kopie der `catalog`-Datei die neuen Einstellungen für Datenspeicher, Ordnerpfad und Ressourcenpool an.  
Siehe „[Bearbeiten einer „catalog“-Datei](#)“ auf Seite 71.

3 Stellen Sie die virtuelle Maschine mithilfe von `vcbRestore` wieder her.

Siehe „[Wiederherstellen von virtuellen Maschinen mithilfe einer alternativen „catalog“-Datei](#)“ auf Seite 73.

### Kopieren einer „catalog“-Datei

Wenn Sie eine virtuelle Maschine an einem anderen als dem ursprünglichen Speicherort wiederherstellen möchten, müssen Sie zunächst eine Kopie der `catalog`-Datei der virtuellen Maschine erstellen.

Erstellen Sie z. B. eine Kopie der `catalog`-Datei der virtuellen Maschine `/home/VMs/vm37`. Geben Sie Folgendes ein:

```
cp /home/VMs/vm37/catalog /tmp/catalog-vm37
```

### Bearbeiten einer „catalog“-Datei

Ändern Sie in der Kopie der `catalog`-Datei, die Sie erstellt haben, folgende Einstellungen:

- **Datenspeicher.** Hier wird angegeben, wo alle Dateien, aus denen eine virtuelle Maschine besteht, gespeichert werden sollen.
- **Ordnerpfad.** Der Ordnerpfad einer virtuellen Maschine gibt an, wo die virtuelle Maschine in der Ordnerhierarchie von VirtualCenter platziert werden soll.
- **Ressourcenpool.** Dieses hostspezifische Konfigurationselement bestimmt das Verhalten der virtuellen Maschine hinsichtlich des DRS (Distributed Resource Scheduling). Wenn Sie mehrere von VirtualCenter verwaltete ESX Server 3-Hosts einsetzen, gibt dieses Element ebenfalls den Host an, auf dem die virtuelle Maschine ausgeführt wird.

---

**HINWEIS** Wenn Sie in der `catalog`-Datei den Namen der virtuellen Maschine ändern, verwendet `vcbRestore` nicht den neuen Namen aus dieser Datei, sondern den ursprünglichen, in der `.vmx`-Datei angegebenen Namen der virtuellen Maschine.

Sie können den Namen der virtuellen Maschine auch später mithilfe des VI-Clients ändern.

---

## Ändern von Datenspeicherpfaden

Der Datenspeicherpfad in der `catalog`-Datei gibt an, wo alle Dateien, aus denen eine virtuelle Maschine besteht, gespeichert werden sollen. Datenspeicherpfade können Sie in den folgenden Einträgen ändern:

- `disk.scsi*.diskname` – Die Namen und Speicherorte aller Festplatten, die dieser virtuellen Maschine zugeordnet sind.
- `config.vmx` – Der Speicherort der wichtigsten Konfigurationsdatei der virtuellen Maschine.
- `config.suspenddir` – Der Speicherort der Arbeitsspeicher-Snapshots, die vor dem Anhalten der virtuellen Maschine erstellt wurden.
- `config.logdir` – Der Speicherort der Protokolldateien der virtuellen Maschine.

Standardmäßig verwenden alle Einträge denselben Pfad, der auf dasselbe Verzeichnis in demselben Datenspeicher zeigt. VMware empfiehlt Ihnen, beim Ändern des Pfads diese Standardvorgabe zu berücksichtigen.

Die Syntax der Datenspeicherpfade lautet folgendermaßen:

```
[<Datenspeichename>] <Pfad_in_Datenspeicher>
```

Eine Liste gültiger Datenspeichernamen erhalten Sie, wenn Sie den Datenspeicherbrowser des VI-Clients aufrufen, oder über die Dateisystemkennzeichnungen der VMFS-Volumes in der Servicekonsole unter `/vmfs/volumes`.

## Ändern von Ordnerpfaden

Der Ordnerpfad der virtuellen Maschine in der `catalog`-Datei gibt an, in welchem Ordner innerhalb der Ordnerhierarchie von VirtualCenter die wiederhergestellte virtuelle Maschine gespeichert werden soll.

### So ändern Sie den Ordnerpfad für die virtuelle Maschine

- 1 Suchen Sie nach dem Ordner, in dem die virtuelle Maschine gespeichert werden soll, indem Sie in der Servicekonsole den folgenden Befehl eingeben:

```
vcbUtil -c vmfolders
```

Voraussetzung für das Ausführen des Befehls ist, dass Sie die Konfigurationsoptionen gemäß der Beschreibung unter „[Einstellungen der Konfigurationsdatei](#)“ auf Seite 62 eingerichtet haben.

- 2 Legen Sie in der `catalog`-Datei als Ordnerpfad einen der Ordnerpfade fest, die nach der Eingabe des Befehls `vcbUtil` ausgegeben werden.

## Ändern von Ressourcenpools

Durch Eingabe des Ressourcenpools in der `catalog`-Datei legen Sie das Verhalten der virtuellen Maschine hinsichtlich des DRS (Distributed Resource Scheduling) fest. Wenn Sie mehrere von VirtualCenter verwaltete ESX Server 3-Hosts einsetzen, gibt dieses Element ebenfalls den Host an, auf dem die virtuelle Maschine ausgeführt wird.

### So ändern Sie die Ressourcenpooleinstellung für die virtuelle Maschine

- 1 Suchen Sie nach dem Ressourcenpool, den die virtuelle Maschine verwendet, indem Sie den folgenden Befehl eingeben:

```
vcbUtil -c resourcepools
```

Voraussetzung für das Ausführen des Befehls ist, dass Sie die Konfigurationsoptionen gemäß der Beschreibung unter „[Einstellungen der Konfigurationsdatei](#)“ auf Seite 62 eingerichtet haben.

- 2 Stellen Sie in der `catalog`-Datei eine der Optionen für den Ressourcenpool ein, die nach der Eingabe des Befehls `vcbUtil` ausgegeben werden.

## Wiederherstellen von virtuellen Maschinen mithilfe einer alternativen „catalog“-Datei

Nach dem Ändern der Einstellungen in der alternativen `catalog`-Datei der virtuellen Maschine können Sie diese Datei verwenden, um die virtuelle Maschine wiederherzustellen.

Verwenden Sie zum Wiederherstellen der virtuellen Maschine den Eintrag `-a`, um die alternative `catalog`-Datei anzugeben.

Geben Sie zum Beispiel Folgendes ein, um mithilfe der alternativen `catalog`-Datei eine virtuelle Maschine wiederherzustellen, die unter `/home/VMs/vm37` gesichert wurde:

```
vcbRestore -s /home/VMs/vm37 -a /tmp/catalog-vm37
```

## Nicht interaktiver Einsatz des Dienstprogramms vcbRestore

Standardmäßig werden Sie von `vcbRestore` aufgefordert, anzugeben, wie Sie weiter vorgehen möchten, wenn während des Wiederherstellungsvorgangs festgestellt wird, dass eine Datei oder eine virtuelle Maschine bereits in VirtualCenter vorhanden ist.

Wenn `vcbRestore` nicht interaktiv von einem Skript verwendet wird, können Sie über den Eintrag `-b` in der Befehlszeile das Standardverhalten festlegen. Die folgenden Optionen stehen zur Verfügung:

- **prompt**

Der Benutzer wird aufgefordert, anzugeben, wie weiter vorgegangen werden soll, bevor Dateien oder Konfigurationen von virtuellen Maschinen, die bereits in VirtualCenter vorhanden sind, überschrieben werden.

- **overwrite**

Dateien oder Konfigurationen von virtuellen Maschinen, die bereits in VirtualCenter vorhanden sind, werden bei der Wiederherstellung überschrieben.

- **keep**

Dateien oder Konfigurationen von virtuellen Maschinen, die bereits in VirtualCenter vorhanden sind, werden bei der Wiederherstellung beibehalten.

- **abort**

Wenn festgestellt wird, dass eine Datei oder eine Konfiguration einer virtuellen Maschine bereits in VirtualCenter vorhanden ist, wird der Wiederherstellungsvorgang abgebrochen.

## Wiederherstellen virtueller Maschinen aus Archiven

Verwenden Sie `vcbResAll`, um alle virtuellen Maschinen aus dem mit `vcbSnapAll` erstellten Archiv wiederherzustellen. Das Dienstprogramm `vcbResAll` unterstützt die gesamte Funktionalität von `vcbRestore`.

Verwenden Sie folgende Syntax:

```
vcbResAll -s <sourceDir> [-a <Katalog>]
```

Siehe „[Wiederherstellen von virtuellen Maschinen am ursprünglichen Speicherort](#)“ auf Seite 70 und „[Wiederherstellen von virtuellen Maschinen an einem alternativen Speicherort](#)“ auf Seite 70.

# Wiederherstellen von virtuellen Maschinen der Version ESX Server 2.5.x unter ESX Server 3.x

---

# B

In diesem Anhang wird beschrieben, wie virtuelle Maschinen, die unter ESX Server 2.5.x erstellt und gesichert wurden, mithilfe der Servicekonsole unter ESX Server 3 wiederhergestellt werden.

---

**HINWEIS** Da ESX Server 3i nicht über eine Servicekonsole verfügt, sind die Informationen in diesem Kapitel nicht auf ESX Server 3i anwendbar.

---

Dieser Anhang enthält die folgenden Abschnitte:

- [„Einstellen der Konfigurationsparameter“](#) auf Seite 76
- [„Wiederherstellen von virtuellen Maschinen, die unter ESX Server 2.5.x gesichert wurden“](#) auf Seite 77

## Einstellen der Konfigurationsparameter

Um virtuelle Maschinen, die unter ESX Server 2.5.x erstellt und gesichert wurden, unter ESX Server 3.x wiederherzustellen, müssen Sie zunächst in der Datei `/etc/vmware/backuptools.conf` die entsprechenden Konfigurationsparameter einstellen.

Gehen Sie zum Einstellen der allgemeinen Parameter gemäß den Empfehlungen unter [„Allgemeine Konfigurationseinstellungen für Consolidated Backup-Dienstprogramme“](#) auf Seite 62 vor.

Stellen Sie zusätzlich die folgenden speziellen Parameter ein:

### ■ DSPATH

Gibt den Pfad zu einem Datenspeicher an, in dem die wiederhergestellte virtuelle Maschine gespeichert wird. Um diese Option nicht für jede virtuelle Maschine, die wiederhergestellt werden soll, einzeln einstellen zu müssen, können Sie den Eintrag `%VMNAME%` verwenden. Während des Wiederherstellungsvorgangs wird dieser Eintrag dann automatisch durch den Basisnamen der `.vmx`-Konfigurationsdatei der virtuellen Maschine ersetzt.

Geben Sie zum Beispiel Folgendes ein, um anhand des Basisnamens ihrer `vmx`-Datei virtuelle Maschinen im Datenspeicher `oldvms` wiederherzustellen:

```
DSPATH="[oldvms] %VMNAME%"
```

Mithilfe dieses Eintrags wird die virtuelle Maschine mit der Datei `myvm.vmx` unter `[oldvms]/myvm` wiederhergestellt.

### ■ VMHOST

Gibt den Host für die virtuelle Maschine an, die wiederhergestellt werden soll. Über diesen Host wird die virtuelle Maschine eingeschaltet.

### ■ RESOURCEPOOL

Gibt den Ressourcenpool für die virtuelle Maschine an, die wiederhergestellt werden soll. Siehe [„Ändern von Ressourcenpools“](#) auf Seite 73.

---

**HINWEIS** Wählen Sie einen gültigen Ressourcenpool auf dem in `VMHOST` angegebenen Host an. In der Regel enthält der Name des Ressourcenpools den Namen des entsprechenden ESX Server 3-Hosts. Sie können auch den Eintrag `%VMHOST%` verwenden, der dann durch den Wert ersetzt wird, den Sie `VMHOST` zugewiesen haben.

---

- FOLDERPATH

Gibt den Ordner innerhalb der VirtualCenter-Hierarchie an, in dem die wiederhergestellte virtuelle Maschine gespeichert wird. Siehe „[Ändern von Ordnerpfaden](#)“ auf Seite 72.

## Wiederherstellen von virtuellen Maschinen, die unter ESX Server 2.5.x gesichert wurden

Nach dem Festlegen aller erforderlichen Einstellungen in der Datei `/etc/vmware/backuptools.conf` können Sie virtuelle Maschinen wiederherstellen, die unter ESX Server 2.5.x gesichert wurden.

Der Wiederherstellungsvorgang ist identisch mit dem Vorgang für virtuelle Maschinen, die unter ESX Server 3.x gesichert wurden.

Siehe „[Wiederherstellen von virtuellen Maschinen](#)“ auf Seite 69.



# Index

## Symbole

„catalog“-Dateien **71**

## A

Ablauf **26**

Aliasse **47**

Änderungsjournal **38**

Archivbit **38**

Außer Betrieb nehmen

    Anpassen **49**

    grundlegende Informationen **12**

## B

BIOS-UUID **66**

## C

CIFS **55**

Common Internet File

    System-Protokoll **55**

Consolidated Backup

    Anpassen **49**

    Ausführen von **46**

    Deaktivieren der Laufwerkbuch-  
    stabenzuweisung **36**

    Dienstprogramme **62**

    Einrichten von

        Sicherungsaufträgen **48**

    Einschränkungen **33**

    erstmalige Sicherung  
    durchführen **49**

    Funktionen **26**

    Installieren von **39**

    Interoperabilitätsmodule **39**

Konfigurationsdatei **39**

Konfigurieren der

    Drittanbietersoftware **38**

Konfigurieren von SAN **45**

Konfigurieren von VCB-Proxy **35**

Sicherungen auf Dateiebene **32**

Sicherungen auf Image-Ebene **32**

Überlegungen **23**

Übersicht **26**

und Drittanbieter-

    Sicherungssoftware **26**

verglichen mit herkömmlichen

    Sicherungsmethoden **23**

VMware Tools **35**

## D

Datei backuptools.conf **62**

Dateien

    .vmdk **13**

    .vmx **13**

Dienstprogramme

    Consolidated Backup **62**

    vcbMounter **64**

    vcbRestore **55, 69**

DNS-Name **66**

Drittanbietersoftware

    Deaktivieren des

        Änderungsjournals **38**

    Deaktivieren des Archivbits **38**

    Funktionsweise mit Consolidated  
    Backup **26**

    Interoperabilitätsmodule **26**

    Konfigurieren für VCB **38**

## **E**

- ESX Server 2.5.x **75**
- ESX Server, Aktualisieren von **59**

## **F**

- FAT **36**
- Fehlerbehebung
  - GUI der Sicherungssoftware **59**
  - Pfadformate **59**
- Festplatten-Images, Exportieren von **32**

## **H**

- Herkömmliche Sicherungsmethoden **17**

## **I**

- Inkrementelle Sicherungen
  - Archivbit **38**
- Interoperabilitätsmodule
  - grundlegende Informationen **26**
  - Installieren der **39**
- IP-Adresse **66**

## **K**

- Knotenpunkte
  - Deaktivieren **38**
  - grundlegende Informationen **32**
- Konfigurationsdatei
  - Consolidated Backup **39**
  - Sicherungsdienstprogramme **62**

## **L**

- Laufwerkbuchstaben **36**

## **M**

- MoRefs **67**

## **N**

- NFS-Speicher und -Sicherungen **23**
- Notfallwiederherstellung **56**

- NTFS **36**

## **P**

- Physische Kompatibilität **14**
- Planungsprogramme **15**

## **R**

- Raw-Gerätezuordnung **14**
- RDM
  - Deaktivieren der Laufwerkbuchstabenzuweisung **36**
  - physische Kompatibilität **14**
  - virtuelle Kompatibilität **14**
- README.html-Datei **39**

## **S**

- SAN-Speicher
  - Konfigurieren für VCB **45**
  - und Sicherungen **22**
- SCSI-Festplatten **13**
- Servicekonsole **13**
  - dateibasierte Sicherungen **17**
  - image-basierte Sicherungen **17**
  - Sichern **17**
- Sicherungen
  - Beispielszenario **58**
  - Dateiebene **32**
  - Differenz **12**
  - erstmalige **49**
  - herkömmlich **16**
  - Image-Ebene **32**
  - inkrementell **12**
  - Methoden **15**
  - über ein SAN **22**
  - Übersicht **12**
  - von NFS **23**
- Sicherungsaufträge
  - Abbrechen **51**
  - Einrichten **48**

Sicherungsclients  
  auf einer virtuellen Maschine **18**  
  grundlegende Informationen **15**  
  in der Servicekonsole **20**  
Sicherungsdienstprogramme **62**  
Sicherungsplanungsprogramm **15**  
Sicherungsrichtlinien, Ändern der **59**  
Sicherungsserver **15**

## V

VCB. Siehe „Consolidated Backup“  
vcbMounter  
  Angeben von virtuellen  
  Maschinen **66**  
  Durchführen von Sicherungen **64**  
  Übersicht **64**  
  Ziele **68**  
VCB-Proxy  
  Ausführen von Windows **36**  
  Deaktivieren der Laufwerksbuch-  
  stabenzuweisung **36**  
  Einrichten von **35**  
  grundlegende Informationen **12**  
  Installieren von Consolidated  
  Backup **39**  
  Knotenpunkte **32**  
  und Vernetzung **36**  
vcbRestore **69**  
  „catalog“-Dateien **71**  
  Standardverwendung **73**  
  Wiederherstellen am ursprünglichen  
  Speicherort **70**  
  Wiederherstellen an alternativem  
  Speicherort **70**  
Verzeichnis, /vmfs/volumes **14**  
Virtuelle Festplatten  
  Bearbeiten **14**  
  Speichern **13**  
Virtuelle Kompatibilität **14**

Virtuelle Maschinen  
  Aliasse **47**  
virtuelle Maschinen  
  Gruppen **47**  
VMFS **13**  
vmkfstools (Befehl) **14**  
VMware Tools **35**

## W

Wiederherstellungen  
  Abläufe **54**  
  dateibasiert **54**  
  in Gruppen **56**  
  Self-Service **56**  
  vcbRestore, Dienstprogramm **55**  
  Virtuelle ESX Server 2.5.x-  
  Maschinen **75**  
  zentral **55**  
Windows-Änderungsjournal **38**  
Windows-Archivbit **38**

## Z

Zeitstempel **38**

