

CA ARCserve® Backup für Windows

Agent für virtuelle Rechner – Handbuch

r12.5



Diese Dokumentation (die "Dokumentation") und das zugehörige Computerprogramm (die "Software") (nachfolgend zusammen als "Produkt" bezeichnet) dienen ausschließlich zu Informationszwecken des Endbenutzers und können jederzeit durch CA geändert oder zurückgenommen werden.

Dieses Produkt darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Die Informationen in diesem Produkt sind geistiges Eigentum von CA und durch die in den Vereinigten Staaten von Amerika geltenden Urheberrechte sowie internationale Verträge geschützt.

Ungeachtet der oben genannten Bestimmungen ist der Benutzer, der über eine Lizenz verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch auszudrucken sowie eine Kopie der Software zu Sicherungs- und Wiederherstellungszwecken im Notfall (Disaster Recovery) in angemessenem Umfang anzufertigen, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält. Der Zugriff auf diese Kopien ist berechtigten Beschäftigten, Beratern oder Vertretern des Benutzers vorbehalten, die an die Vertraulichkeitsbestimmungen der Software-Lizenz gebunden sind.

Das Recht zum Drucken von Kopien der Dokumentation und zum Erstellen einer Software-Kopie ist auf den Zeitraum der vollen Wirksamkeit der Produktlizenz beschränkt. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer schriftlich gegenüber CA, dass alle Kopien oder Teilkopien des Produkts an CA zurückgegeben oder vernichtet worden sind.

CA STELLT DIESES PRODUKT GEMÄSS GELTENDEM GESETZ UND SOFERN IN DER ANWENDBAREN LIZENZVEREINBARUNG NICHT ANDERS ANGEgeben IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN, OHNE SICH JEDOCH DARAUF ZU BESCHRÄNKEN, STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER DEM ENDBENUTZER ODER DRITTEM FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER VERWENDUNG DIESES PRODUKTS ENTSTEHEN; DAZU GEHÖREN, OHNE SICH JEDOCH DARAUF ZU BESCHRÄNKEN, ENTGANGENE GEWINNE, BETRIEBSUNTERBRECHUNG, VERLUST IDEELLER UNTERNEHMENSWERTE ODER DATENVERLUST, SELBST WENN CA ÜBER DIESEN VERLUST ODER SCHADEN INFORMIERT WURDE.

Die Verwendung dieses Produkts und aller in der Dokumentation aufgeführten Produkte unterliegt der geltenden Lizenzvereinbarung des Endbenutzers.

Dieses Produkt wurde von CA hergestellt.

Für das bereitgestellte Produkt gelten "Eingeschränkte Rechte". Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absatz 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227.7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Folgebestimmungen.

Alle Marken, Markennamen, Dienstleistungsmarken und Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Unternehmen.

Copyright © 2009 CA. Alle Rechte vorbehalten.

CA-Produktreferenzen

Diese Dokumentation bezieht sich auf die folgenden CA-Produkte:

- BrightStor® ARCserve® Backup for Laptops & Desktops
- BrightStor® CA-Dynam®/TLMS Tape Management
- BrightStor® CA-Vtape™ Virtual Tape System
- BrightStor® Enterprise Backup
- BrightStor® High Availability
- BrightStor® Storage Resource Manager
- CA Antivirus
- CA ARCserve® Backup Agent für Advantage™ Ingres®
- CA ARCserve® Backup Agent für Novell Open Enterprise Server für Linux
- CA ARCserve® Backup Agent for Open Files für NetWare
- CA ARCserve® Backup Agent for Open Files für Windows
- CA ARCserve® Backup Client Agent für FreeBSD
- CA ARCserve® Backup Client Agent für Linux
- CA ARCserve® Backup Client Agent für Mainframe Linux
- CA ARCserve® Backup Client Agent für NetWare
- CA ARCserve® Backup Client Agent für UNIX
- CA ARCserve® Backup Client Agent für Windows
- CA ARCserve® Backup Enterprise Option für AS/400
- CA ARCserve® Backup Enterprise Option für Open VMS
- CA ARCserve® Backup für Microsoft Windows Essential Business Server
- CA ARCserve® Backup für Windows
- CA ARCserve® Backup für Windows Agent für IBM Informix
- CA ARCserve® Backup für Windows Agent für Lotus Domino
- CA ARCserve® Backup für Windows Agent für Microsoft Exchange
- CA ARCserve® Backup für Windows Agent für Microsoft SharePoint
- CA ARCserve® Backup für Windows Agent für Microsoft SQL Server
- CA ARCserve® Backup für Windows Agent für Oracle
- CA ARCserve® Backup für Windows Agent für Sybase
- CA ARCserve® Backup für Windows Agent für virtuelle Rechner

- CA ARCserve® Backup für Windows Disaster Recovery Option
- CA ARCserve® Backup für Windows Disk to Disk to Tape Option
- CA ARCserve® Backup für Windows Enterprise Module
- CA ARCserve® Backup für Windows Enterprise Option für IBM 3494
- CA ARCserve® Backup für Windows Enterprise Option für SAP R/3 für Oracle
- CA ARCserve® Backup für Windows Enterprise Option für StorageTek ACSLS
- CA ARCserve® Backup für Windows Image Option
- CA ARCserve® Backup für Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup für Windows NDMP NAS Option
- CA ARCserve® Backup für Windows Serverless Backup Option
- CA ARCserve® Backup für Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup für Windows Tape Library Option
- CA Dynam®/B Backup für z/VM
- CA VM: Band für z/VM
- CA XOsoft™ Assured Recovery™
- CA XOsoft™
- CA 1® Bandverwaltung
- Common Services™
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM:Operator®

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter <http://www.ca.com/worldwide>. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Änderungen in der Dokumentation

Seit der letzten Version dieser Dokumentation wurden folgende Aktualisierungen der Dokumentation vorgenommen:

- [So schützt der Agent Hyper-V-Systeme](#) (siehe Seite 17): Hier wird beschrieben, wie Sie mit CA ARCserve Backup für virtuelle Rechner Hyper-V-Systeme schützen können.
- [Bereitstellen von Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung](#) (siehe Seite 30): Hier wird beschrieben, wie Sie Agenten unter Verwendung der Agent-Bereitstellung auf lokalen und Remote-VMs installieren und aktualisieren.
- [Aufnehmen der Datenbank mit Hilfe des ARCserve VMware-Konfigurationstools](#) (siehe Seite 36): Beinhaltet Informationen zu Feldern, die dem ARCserve VMware-Konfigurationstool in dieser Version hinzugefügt wurden.
- [Festlegen eines temporären VM-Ladeorts](#) (siehe Seite 40): Hier wird beschrieben, wie Sie den Standard-Ladeort auf dem Sicherungs-Proxy-System ändern.
- [Einpflegen von Informationen in die Datenbank mit dem Befehlszeilenhilfsprogramm "ca_vcbpopulatedb"](#) (siehe Seite 41) und [ca_vcbpopulatedb – Verwendung](#) (siehe Seite 44): Enthält Informationen zur Syntax und zu Argumenten, die in dieser Version hinzugefügt wurden.
- [Aufnehmen der Datenbank mit Hilfe des ARCserve Hyper-V-Konfigurationstools](#) (siehe Seite 49): Hier wird beschrieben, wie Sie mit Hilfe einer grafischen Benutzeroberfläche, dem ARCserve Hyper-V-Konfigurationstool, Informationen zu Hyper-V-Systemen, die in Ihrer virtuellen Rechner-Umgebung ausgeführt werden, in die CA ARCserve Backup-Datenbank aufnehmen können.
- [Aufnehmen der Datenbank mit Hilfe des Befehlszeilenhilfsprogramms "ca_msmpopulatedb"](#) (siehe Seite 52): Hier wird beschrieben, wie Sie mit Hilfe eines auf der Windows-Befehlszeile basierenden Hilfsprogramms mit dem Namen "ca_msmpopulatedb" Informationen zu den Hyper-V-Systemen, die in Ihrer virtuellen Rechner-Umgebung ausgeführt werden, in die CA ARCserve Backup-Datenbank aufnehmen können.

- [Deinstallieren des Agenten](#) (siehe Seite 55): Aktualisierung der Vorgehensweise zur Deinstallation des CA ARCserve Backup Agenten für virtuelle Rechner.
 - [Empfehlungen für die Installation und Konfiguration des Agenten für virtuelle Rechner](#) (siehe Seite 57): Bietet Empfehlungen für die beste Vorgehensweise in Bezug auf die Installation und Konfiguration des CA ARCserve Backup Agenten für virtuelle Rechner.
 - [Funktionsweise globaler und lokaler Sicherungsmodi](#) (siehe Seite 61): Hier wird die Anwendung von Sicherungsmodi zur Maximierung von Sicherungseffizienz und Wiederherstellungsflexibilität beschrieben.
 - [Angeben von Sicherungsmodi als globale Sicherungsoption](#) (siehe Seite 65) und [Angeben von Sicherungsmodi als lokale Sicherungsoption](#) (siehe Seite 68): Hier werden Sicherungsmodi beschrieben sowie wann diese verwendet und wie sie angegeben werden sollen.
 - [Wiederherstellen virtueller Hyper-V-Rechner](#) (siehe Seite 87): Wurde zum Abschnitt "Wiederherstellen von Daten" hinzugefügt und beschreibt die Wiederherstellung von virtuellen Hyper-V-Rechnern.
 - [Wiederherstellen von Daten auf Dateiebenengranularität](#) (siehe Seite 78): Wurde der Beschreibung der Wiederherstellung von Daten mit Sicherungsdaten im Dateimodus, Raw-(vollständigen VM-)Sicherungsdaten und Sicherungsdaten im gemischten Modus hinzugefügt.
 - [Verwenden von Protokolldateien virtueller Rechner:](#) (siehe Seite 92) Beschreibt die Verwendung von Protokolldateien zur Analyse von VM-Sicherungs- und Wiederherstellungsvorgängen.
 - [Fehlerbehebung](#) (siehe Seite 97): Zusätzliche Themen mit Szenarien zur Fehlerbehebung.
 - [Konfigurieren von VirtualCenter Server 2.5-Systemen](#) (siehe Seite 118): Aktualisierte Vorgehensweise mit Informationen zur Konfiguration der HTTP- und HTTPS-Kommunikation.
 - [Schützen von Hyper-V-Systemen unter Verwendung des Hyper-V-VSS-Autors:](#) (siehe Seite 121) Beschreibt den Schutz von VM-Daten mit dem Hyper-V-VSS-Autor.
-

Inhalt

Kapitel 1: Einführung	11
Einführung.....	11
Schutzfunktion des Agenten für VMware-Systeme	12
Einsatz von VCB durch CA ARCserve Backup zum Schutz Ihrer VMware-Umgebung.....	13
So schützt der Agent VMs in einem lokalen Speicher und einem SAN.....	15
VCB-Einschränkungen.....	16
Schutz von Hyper-V-Systemen durch den Agenten	17
Einsatz von Hyper-V durch CA ARCserve Backup zum Schutz Ihrer Umgebung	18
Unterstützte CA ARCserve Backup-Funktionen	19
Kapitel 2: Installieren und Konfigurieren des Agenten	21
Lizenzierung des Agenten	21
Installationsorte für den Agenten.....	22
Sicherungsmodus und Installationsmatrix.....	23
Voraussetzungen für die Installation	28
Installationshinweise.....	29
Installieren und Konfigurieren des Agenten.....	29
Bereitstellen des Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung	30
Aufgaben nach der Installation	33
Geben Sie den Namen des CA ARCserve Backup-Servers an.....	34
Einpflegen von Informationen in die Datenbank mit Hilfe des ARCserve-Konfigurationstools für VMware	36
Festlegen eines temporären VM-Ladeorts.....	40
Einpflegen von Informationen in die Datenbank mit Hilfe des Befehlszeilenhilfsprogramms "ca_vcbsuppopulatedb"	41
Einpflegen von Informationen in die Datenbank mit Hilfe des ARCserve Hyper-V-Konfigurationstools	49
Einpflegen von Informationen in die Datenbank mit Hilfe des Befehlszeilenhilfsprogramms "ca_msmpopulatedb"	52
Hinzufügen oder Entfernen bestimmter VM-Daten zu/aus der CA ARCserve Backup-Datenbank	54
So deinstallieren Sie den Agenten:.....	55
So verwenden Sie den Transportmodus "hotadd" von VMware:.....	55
Beenden von Vorgängen bei abgelaufenen SSL-Zertifikaten	56
Best Practices für die Installation und Konfiguration des Agenten für virtuelle Rechner	57

Kapitel 3: Sichern und Wiederherstellen von Daten	59
Durchsuchen von Sicherungs-Volumes	59
Funktionsweise des globalen und lokalen Sicherungsmodus	61
Festlegen von Sicherungsmodi als globale Sicherungsoption.....	65
Festlegen von Sicherungsmodi als lokale Sicherungsoption	68
Verarbeitung von Zuwachs- und Änderungssicherungen virtueller VMware-Rechner durch den Agenten.....	71
Sichern von Daten	71
Funktionsweise der Agent-Unterstützung für das Hilfsprogramm Pre-Flight Check	74
Filtern von VM-Sicherungsdaten.....	75
Durchsuchen von Wiederherstellungssitzungen	76
Wiederherstellen von Daten	78
Daten auf Dateiebenengranularität wiederherstellen	78
Wiederherstellen von Sicherungsdaten auf Raw-Ebene (vollständige VM)	81
Wiederherstellen virtueller VMware-Rechner.....	83
Wiederherstellen virtueller Hyper-V-Rechner	87
Einschränkungen beim Sichern und Wiederherstellen auf virtuellen Rechnern.....	91
Verwenden von Protokolldateien virtueller Rechner	92
Auswirkungen von VM-Namen auf Jobs	94
Anhang A: Fehlerbehebung	97
VM konnte nicht geladen werden	97
VM konnte nicht entladen werden.....	99
Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"	100
Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"	101
Sicherungsjobs schlagen anscheinend fehl	103
VMs erscheinen nicht in der Verzeichnisstruktur des Sicherungs-Managers	103
Die Größe von Sicherungssitzungen übersteigt den auf virtuellen Rechnern belegten Speicherplatz	104
Fehler bei der Wiederherstellung von virtuellen Rechnern auf virtuellen VMware-Rechnern	105
Sicherungsdaten auf Dateiebene können nicht auf einem CA ARCserve Backup-Server wiederhergestellt werden	106
Anhang B: Konfigurieren von ESX Server-Systemen und VirtualCenter Server-Systemen	109
Konfigurieren von ESX Server 3.0.2-Systemen.....	109
Konfigurieren von ESX Server 3.5-Systemen.....	112
Konfigurieren von ESX Server 3i-Systemen.....	113
Konfigurieren von VirtualCenter Server 2.0.2-Systemen.....	115

Konfigurieren von VirtualCenter Server 2.5-Systemen.....	118
--	-----

Anhang C: Schützen von Hyper-V-Systemen unter Verwendung des Hyper-V-VSS-Autors	121
--	------------

Übersicht zum Schützen von Hyper-V-VMs unter Verwendung des Hyper-V-VSS-Autors	121
Erforderliche Komponenten.....	122
Konfigurieren von CA ARCserve Backup zur Ermittlung von Hyper-V-VMs	123
Sichern mit Hilfe des Status "Gespeichert"	125
Sichern mit Hilfe untergeordneter Partitions-Snapshots	125
Sichern von Hyper-V-VMs mit Hilfe des Hyper-V-VSS-Autors.....	125
Wiederherstellen von Daten an ihrem ursprünglichen Speicherort.....	126

Index	129
--------------	------------

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

[Einführung](#) (siehe Seite 11)

[Schutzfunktion des Agenten für VMware-Systeme](#) (siehe Seite 12)

[VCB-Einschränkungen](#) (siehe Seite 16)

[Schutz von Hyper-V-Systemen durch den Agenten](#) (siehe Seite 17)

[Unterstützte CA ARCserve Backup-Funktionen](#) (siehe Seite 19)

Einführung

CA ARCserve Backup ist eine umfassende Sicherungslösung für Anwendungen, Datenbanken, verteilte Server und Dateisysteme. Sie bietet Sicherungs- und Wiederherstellungsfunktionen für Datenbanken, unternehmenswichtige Anwendungen und Netzwerk-Clients.

CA ARCserve Backup enthält verschiedene Agenten, unter anderem den CA ARCserve Backup Agent für virtuelle Rechner. Mit dem Agenten können Sie virtuelle Rechner (VMs, Virtual Machines) schützen, auf denen folgende Systeme ausgeführt werden:

- **VMware ESX Server und VMware VirtualCenter Server:** VMware verfügt über einen Mechanismus, der als VMware Consolidated Backup (VCB) bezeichnet wird und in VMware ESX Server und VMware VirtualCenter Server integriert ist. Mit VCB können Sie Virtual Machine (VM)-Dateien und -Daten schützen. Mit VCB können Sie VM-Sicherungsaktivitäten auf ein dafür vorgesehenes Sicherungs-Proxysystem übertragen und anschließend die virtuellen Rechner mit den Sicherungs- und Wiederherstellungsfunktionen von CA ARCserve Backup schützen.
- **Microsoft Hyper-V:** Microsoft Hyper-V ist eine im Betriebssystem Windows Server 2008 enthaltene Komponente. Hyper-V ist eine Technologie, die auf Hypervisor basiert und es Ihnen ermöglicht, mehrere Betriebssysteme unabhängig von Windows Server 2008 auszuführen. Mit CA ARCserve Backup können Sie Daten auf den Gastbetriebssystemen und auf dem Betriebssystem Windows Server 2008 sichern und wiederherstellen.

Schutzfunktion des Agenten für VMware-Systeme

Der Agent ermöglicht Ihnen die Datensicherung und funktioniert unter den folgenden Umständen besonders gut:

- Sie möchten die Einschränkung von Ressourcen im ESX-Server-System reduzieren.
Hinweis: VMware ESX Server ist eine Anwendung zur Verwaltung von System-, Speicher- und Netzwerkressourcen in mehreren VM-Umgebungen.
- Ihre Umgebung besteht aus VMs, die sich in verschiedenen Datenspeichern befinden.
- Sie möchten Daten auf Datei- oder Raw-Ebene (vollständige VM) wiederherstellen.

Mit VCB können Sie folgende Aufgaben ausführen:

- Einen Snapshot eines virtuellen Rechners erstellen und die Sicherungsdaten in ein oder mehrere Sicherungs-Proxysysteme laden oder exportieren und die Ladung vom ESX-Server-System entfernen.
- Sicherungen auf Dateiebene und Wiederherstellungen einer VM durchführen, auf der ein von VMware unterstütztes Windows-basiertes Betriebssystem ausgeführt wird.
- Sicherungen auf Raw-Ebene (vollständige VM) und Wiederherstellungen einer VM mit einem beliebigen von VMware unterstützten Betriebssystem durchführen.
- LAN (Local Area Network)-freie Sicherungen durchführen, sofern sich die VMs in einem SAN befinden.
- Eine VM unabhängig von ihrem Status sichern.
- Verwaltungsaufwand durch zentrale Sicherungsverwaltung auf Sicherungs-Proxysystemen reduzieren. Sie müssen keine Agenten auf den VMs verwenden.

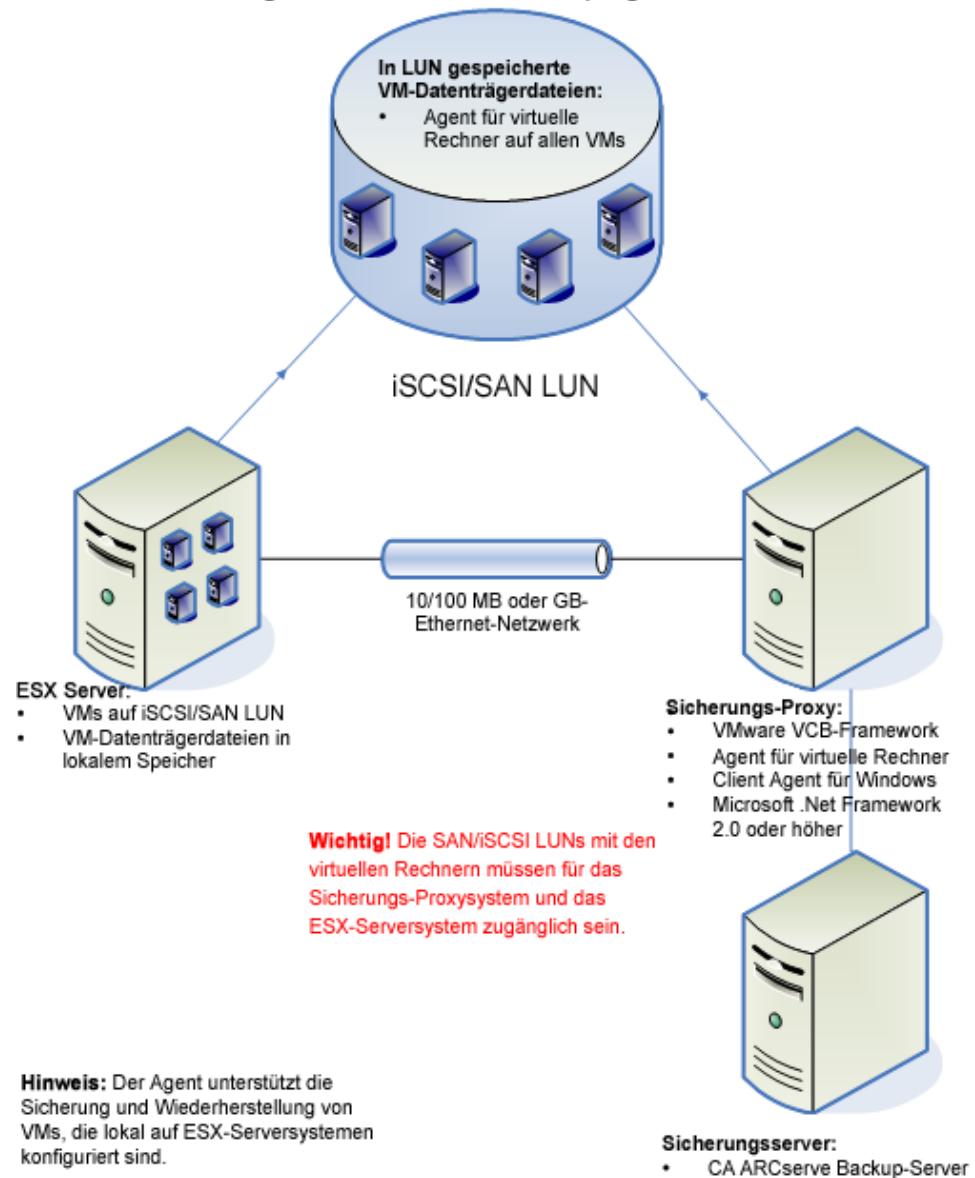
Hinweis: Diese Funktion erfordert die Installation des Agenten für virtuelle Rechner auf dem Sicherungs-Proxysystem.

Einsatz von VCB durch CA ARCserve Backup zum Schutz Ihrer VMware-Umgebung

Mit diesem Agenten können Sie VM-Sicherungen auf Raw-Ebene (vollständige VM), VM-Sicherungen auf Dateiebene und VM-Sicherungen im gemischten Modus unter Verwendung eines Sicherungs-Proxysystems durchführen.

Die folgende Abbildung veranschaulicht die Netzwerkarchitektur zur Sicherung von VMware-Images oder -Dateien mit Hilfe eines Sicherungs-Proxysystems:

Sichern von VMware-Umgebungen über ein externes Sicherungs-Proxysystem unter Verwendung von CA ARCserve Backup Agent für virtuelle Rechner



1. Der CA ARCserve Backup-Primärserver oder -Mitgliedsserver kommuniziert mit dem Agenten für virtuelle Rechner, der während der Ausführung des Sicherungsjobs auf dem Sicherungs-Proxysystem ausgeführt wird. Der Agent erstellt dann einen VCB-Snapshot des virtuellen Rechners und lädt oder exportiert diesen standardmäßig in das Installationsverzeichnis des Client Agent für Windows auf dem Sicherungs-Proxysystem.
2. Falls beim Sicherungsmodus die Option "[Wiederherstellung im Dateimodus erlauben](#) (siehe Seite 61)" angegeben ist, erstellt CA ARCserve Backup Katalogdateien für die Volumes auf dem virtuellen Rechner.
3. Anschließend werden der virtuelle Rechner und die Kataloge auf den Zieldatenträgern gesichert.

Hinweis: Informationen zum Ändern des Standardbereitstellungspfades finden Sie unter [Angeben eines temporären VM-Ladeortes](#) (siehe Seite 40).

Wenn Sie diese Architektur in Ihrer Umgebung verwenden, berücksichtigen Sie Folgendes:

- Der Agent muss auf dem Primär- bzw. Standalone-Server von CA ARCserve Backup lizenziert sein.
 - Der Agent muss auf allen virtuellen Rechnern installiert sein, auf denen Sie Wiederherstellungen auf Dateiebene für das Gastbetriebssystem durchführen möchten.
- Hinweis:** Weitere Informationen finden Sie unter "[Installationsorte für den Agenten](#)" (siehe Seite 22).
- Auf dem Sicherungs-Proxysystem muss Microsoft .NET Framework Version 2.0 oder höher ausgeführt werden.
 - Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem freigegeben sein und dieselbe LUN-Nummer aufweisen.

Hinweis: Die obige Einschränkung gilt nur für die VCB-Versionen 1.0, 1.0.1 und 1.0.2. Bei VCB ab Version 1.0.3 ist keine einheitliche LUN-Nummer erforderlich.

Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware VCB-Dokumentation.

- Die Sicherung auf Raw-Ebene (vollständige VM) erstellt eine Kopie der gesamten Festplatte und aller Konfigurationsdateien, die zu einer bestimmten VM gehören. Damit wird Ihnen die Wiederherstellung der gesamten VM ermöglicht.

Die Sicherung auf Raw-Ebene kann zur Wiederherstellung von VMs im Falle eines Systemausfalls oder totalen Verlusts der ursprünglichen virtuellen Rechner verwendet werden.

- Mit Hilfe der Sicherung auf Dateiebene können Sie eine Kopie einzelner Dateien auf der Festplatte einer VM erstellen. Dies kann alle Dateien umfassen.

Sie können diese Methode in Situationen verwenden, in denen beschädigte oder versehentlich gelöschte Dateien wiederhergestellt werden.
 - Bei Sicherungen im gemischten Modus können Sie GFS- und Rotationssicherungsjobs durchführen, die wöchentliche vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen im Dateimodus in einem einzigen Sicherungsjob umfassen.

Sie können mit dieser Methode Daten mit der Effizienz des Raw-Modus sichern (vollständige VM) und mit Dateiebenengranularität wiederherstellen.
 - Wenn Sie einen Sicherungsjob übergeben, können Sie eine Sicherung auf Raw-Ebene (vollständige VM) oder Dateiebene der VM durchführen. Sie müssen den Primär- oder Mitgliedsserver angeben, auf dem der Job ausgeführt wird.
- Wichtig!** Zur Durchführung von VM-Sicherungen auf Dateiebene muss ein von VMware unterstütztes Windows-Betriebssystem auf der VM installiert sein.

So schützt der Agent VMs in einem lokalen Speicher und einem SAN

Mit dem CA ARCserve Backup Agent für virtuelle Rechner können Sie VMware-basierte Daten schützen, die sich an einem lokalen Speicherort oder in einem Storage Area Network (SAN) befinden. Für alle Datenspeichertypen müssen VMs über das Sicherungs-Proxysystem zugänglich sein.

Die folgende Liste beschreibt die Umgebungskonfiguration, die für jeden Datenspeichertyp erforderlich ist:

- **SAN-, iSCSI-Datenspeicher:** Das Sicherungs-Proxysystem muss über dieselbe SAN- bzw. iSCSI-Infrastruktur mit dem Laufwerk des VMs verbunden sein.
- **Datenspeicher des lokalen Speichers:** Die VMs müssen sich auf Laufwerken befinden, die direkt mit dem ESX Server-System verbunden sind. In Umgebungen mit lokalem Speicher sollte das Sicherungs-Proxysystem über das LAN mit dem ESX Server-System kommunizieren können.

Hinweis: Die Begriffe SAN und iSCSI weisen auf einen gemeinsamen Speicher zwischen Proxy- und ESX-Server-System hin. Der Begriff SAN gilt auch für iSCSI-Umgebungen, in denen Festplatten mittels iSCSI-Infrastruktur freigegeben werden.

Wenn Sie den Agenten mit VI 2.5 implementieren und mit Hilfe des Befehlszeilenhilfsprogramms ca_vcbsubsystem oder des ARCserve VMware-Konfigurationstools Informationen in die CA ARCserve Backup-Datenbank einpflegen, kann CA ARCserve Backup den Agenten so konfigurieren, dass er die Datenspeichertypen der VMs in Ihrem Netzwerk erkennt.

Wenn sich das VM jedoch auf einem SAN befindet und das Sicherungs- Proxysystem nicht mit diesem SAN verbunden ist, müssen Sie die INI-Datei "VMDatastoreTypes.ini", die von CA ARCserve Backup erkannten Datenspeichertypen enthält, beim Einpflegen von Informationen in die CA ARCserve Backup-Datenbank bearbeiten. CA ARCserve Backup erstellt die Datei "VMDatastoreTypes.ini" im Installationsverzeichnis des Client Agent für Windows. Der CA ARCserve Backup Client Agent für Windows ist standardmäßig in folgendem Verzeichnis installiert:

C:\Programme\CA\ARCserve Backup Client Agent for windows

Hinweis: Weitere Informationen darüber, wie die Datei "VMDatastoreTypes.ini" zum Schutz der VMs in einem SAN bearbeitet werden muss, finden Sie unter "Konfigurieren des Agenten zum Schutz von VMs in einem SAN".

VCB-Einschränkungen

Wenn Sie VCB in Ihrer Umgebung verwenden, sollten Sie die folgenden Einschränkungen bedenken:

- Sie können keine VMs mit virtuellen Festplatten sichern, bei denen es sich um kompatible Raw Device Maps (RDM) mit der Eigenschaft "Unabhängig (Persistent/Nicht persistent)" handelt.
- Sie müssen allen Volumes einer VM, die Sie sichern möchten, einen Laufwerksbuchstaben zuweisen und über die Funktion zum Durchsuchen des Ladeverzeichnisses verfügen. Wird dem Volume kein Laufwerksbuchstabe zugeordnet, verhindert VCB, dass Sie das geladene Volume im Ladeverzeichnis suchen können. Dies führt dazu, dass CA ARCserve Backup die Sicherung nicht abschließen kann und den Job als unvollständig ausweist.
- Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem freigegeben sein und dieselbe LUN-Nummer aufweisen.

Hinweis: Die obige Einschränkung gilt nur für die VCB-Versionen 1.0, 1.0.1 und 1.0.2. Bei VCB ab Version 1.0.3 ist keine einheitliche LUN-Nummer erforderlich.

Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware VCB-Dokumentation.

- Um eine einzelne Datei oder ein einzelnes Verzeichnis zu sichern, muss ein von VMware unterstütztes Windows-basiertes Betriebssystem auf der VM laufen.
- VCB unterstützt Ladungen mit bis zu 60 gleichzeitigen VM-Volumes.

Beispiele: Laden von gleichzeitigen VMware Volumes

- 60 VMs mit einem C:\ Laufwerk
- 30 VMs mit zwei VM-Volumes: einem C:\ Laufwerk und einem D:\ Laufwerk
- VCB unterstützt die Verwendung nicht englischer Multibyte-Zeichen nicht. Pfade und Registrierungszeichenfolgen mit nicht englischen Multibyte-Zeichen werden möglicherweise nicht richtig angezeigt.

Hinweis: Informationen zur Installation und zum Setup von VCB sowie zu den Einschränkungen bei der Verwendung von VCB finden Sie im Handbuch "VMware Virtual Machine Backup Guide" auf der Website von VMware.

Schutz von Hyper-V-Systemen durch den Agenten

Der Agent ermöglicht Ihnen das Sichern von Daten und funktioniert am besten, wenn Sie Daten auf Dateiebene, Raw-Ebene (vollständige VM) oder auf gemischter Ebene wiederherstellen möchten.

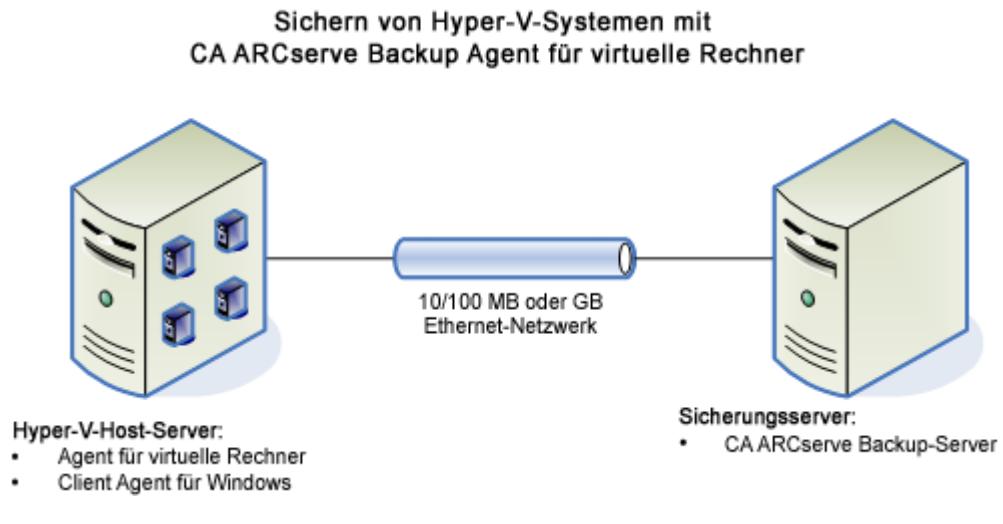
Mit Microsoft Hyper-V können Sie folgende Verwaltungsaufgaben durchführen:

- Auf Dateiebene Sicherungen und Wiederherstellungen von VMs durchführen, auf denen ein beliebiges von Hyper-V unterstütztes Windows-basiertes Betriebssystem ausgeführt wird.
- Sicherungen und Wiederherstellungen auf Raw-Ebene einer VM (vollständige VM) durchführen, auf der ein beliebiges von Hyper-V unterstütztes Betriebssystem ausgeführt wird.
- Eine VM unabhängig von ihrem Status sichern.
- Verwaltungsaufwand durch zentrale Sicherungsverwaltung auf Hyper-V-Hostsystemen reduzieren.

Einsatz von Hyper-V durch CA ARCserve Backup zum Schutz Ihrer Umgebung

Mit diesem Agenten können Sie VM-Sicherungen auf Raw-Ebene (vollständige VM), VM-Sicherungen auf Dateiebene und VM-Sicherungen im gemischten Modus durchführen.

Die folgende Abbildung veranschaulicht die Netzwerkarchitektur zur Sicherung von VM-Images oder -Dateien.



Wenn Sie diese Architektur in Ihrer Umgebung verwenden, berücksichtigen Sie Folgendes:

- Der Agent muss auf dem Primär- bzw. Standaloneserver von CA ARCserve Backup lizenziert sein.
- Der Agent muss auf allen virtuellen Rechnern installiert sein, auf denen Sie Wiederherstellungen auf Dateiebene für das Gastbetriebssystem durchführen möchten.

Hinweis: Weitere Informationen finden Sie unter "[Installationsorte für den Agenten](#)" (siehe Seite 22).

- Die Sicherung auf Raw-Ebene (vollständige VM) erstellt eine Kopie der gesamten Festplatte und aller Konfigurationsdateien, die zu einer bestimmten VM gehören. Damit wird Ihnen die Wiederherstellung der gesamten VM ermöglicht.

Die Sicherung auf Raw-Ebene kann zur Wiederherstellung von VMs im Falle eines Systemausfalls oder totalen Verlusts der ursprünglichen virtuellen Rechner verwendet werden.

- Mit Hilfe der Sicherung auf Dateiebene können Sie eine Kopie einzelner Dateien auf der Festplatte einer VM erstellen. Dies kann alle Dateien umfassen.
Sie können diese Methode in Situationen verwenden, in denen beschädigte oder versehentlich gelöschte Dateien wiederhergestellt werden.
 - Wenn Sie einen Sicherungsjob übergeben, können Sie eine Sicherung auf Raw-Ebene (vollständige VM) oder Dateiebene der VM durchführen. Sie müssen den Primär- oder Mitgliedsserver angeben, auf dem der Job ausgeführt wird.
- Wichtig!** Zur Durchführung von VM-Sicherungen auf Dateiebene muss ein von Hyper-V unterstütztes Windows-Betriebssystem auf der VM installiert sein.

Unterstützte CA ARCserve Backup-Funktionen

Der Agent unterstützt folgende CA ARCserve Backup-Funktionen:

- **Multistreaming:** Mit CA ARCserve Backup können Sie Jobs mit Hilfe von Multistreaming auf VM-Ebene übergeben.
- **Staging:** Mit CA ARCserve Backup können Sie VM-Sicherungsjobs an Disk-Staging- und Band-Staging-Geräte übergeben.
Sie können Daten auf Dateiebenengranularität direkt vom Staging-Gerät und von einem endgültigen Zieldatenträger, wie zum Beispiel einem Banddatenträger, wiederherstellen.
- **Deduplizierung:** Mit CA ARCserve Backup können Sie Speicherplatz sparen, indem Sie Blöcke redundanter Sicherungsdaten löschen.
- **Multiplexing:** Mit CA ARCserve Backup können Sie Jobs mit Hilfe von Multiplexing übergeben.
- **GFS- und Rotationssicherungen:** Mit CA ARCserve Backup können Sie GFS- und Rotationssicherungsjobs übergeben.
- **Ergänzungsjobs:**
 - **Raw-(vollständige VM-)Sicherungen:** CA ARCserve Backup startet den fehlgeschlagenen Job auf VM-Ebene neu.
 - **Zuwachs- und Änderungssicherungen:** CA ARCserve Backup startet fehlgeschlagene Jobs auf Volume-Ebene neu.
- **Komprimierung:** Mit CA ARCserve Backup können Sie VM-Sicherungsdaten auf dem Agent-System oder dem CA ARCserve Backup-Server komprimieren.
- **Verschlüsselung:** Mit CA ARCserve Backup können Sie VM-Sicherungsdaten auf dem Agent-System oder dem CA ARCserve Backup-Server verschlüsseln.

- **CRC-Prüfung:** Dadurch dass die CRC-Prüfung auf VM-Sicherungsdaten unterstützt wird, haben Sie mit CA ARCserve Backup die Möglichkeit, die Datenintegrität zu überprüfen.
- **Übergreifende und gespiegelte Volumes sowie Volumes mit Stripes:** Mit CA ARCserve Backup können Sie VM-Daten schützen, die sich auf übergreifenden und gespiegelten Volumes und Volumes mit Stripes befinden.

Hinweis: Weitere Informationen zu den oben beschriebenen Funktionen finden Sie in der Online-Hilfe oder im *Administrationshandbuch*.

Kapitel 2: Installieren und Konfigurieren des Agenten

Dieses Kapitel enthält folgende Themen:

- [Lizenzierung des Agenten](#) (siehe Seite 21)
- [Installationsorte für den Agenten](#) (siehe Seite 22)
- [Sicherungsmodus und Installationsmatrix](#) (siehe Seite 23)
- [Voraussetzungen für die Installation](#) (siehe Seite 28)
- [Installationshinweise](#) (siehe Seite 29)
- [Installieren und Konfigurieren des Agenten](#) (siehe Seite 29)
- [Aufgaben nach der Installation](#) (siehe Seite 33)
- [Best Practices für die Installation und Konfiguration des Agenten für virtuelle Rechner](#) (siehe Seite 57)

Lizenzierung des Agenten

Der CA ARCserve Backup Agent für virtuelle Rechner verwendet eine anzahlbasierte Lizenzierungsmethode. Sie müssen für jeden virtuellen Rechner und jedes Hostsystem, das mit CA ARCserve Backup geschützt wird, einen CA ARCserve Backup Agent für virtuelle Rechner lizenziieren. Die Lizenzen für den Agenten müssen auf dem CA ARCserve Backup-Primärserver oder dem Standalone-Server registriert werden.

Beispiele: Lizenzierung des Agenten

Beispiel 1

- Ihre Umgebung besteht aus einem Hyper-V-Host mit drei Gastbetriebssystemen. Sie müssen vier Lizenzen (1 Hostsystem plus 3 VMs) auf dem CA ARCserve Backup-Server lizenziieren.

Beispiel 2

- Ihre Umgebung besteht aus einem ESX-Serversystem mit drei Gastbetriebssystemen. Sie müssen vier Lizenzen (1 Sicherungs-Proxy-System plus 3 VMs) auf dem CA ARCserve Backup-Server lizenziieren.

Beispiel 3

- Ihre Umgebung besteht aus zwei Hyper-V-Hostsystemen. Jedes Hyper-V-Hostsystem besteht aus drei Gastbetriebssystemen. Sie müssen acht Lizenzen (1 Hostsystem plus 3 VMs, 1 Hostsystem plus 3 VMs) auf dem CA ARCserve Backup-Server registrieren.

Beispiel 4

- Ihre Umgebung besteht aus einem VM-Hostsystem (VMware-ESX-Server oder Hyper-V-Server) mit zwei VMs. Sie benötigen nur Raw-Sicherungen (vollständige VM) und arbeiten ohne die Option "Wiederherstellung im Dateimodus erlauben". In diesem Szenario wird der Agent nur auf dem Hostsystem installiert. Auf dem CA ARCserve Backup-Server muss jedoch eine Lizenz für jeden virtuellen Rechner registriert werden. Daher müssen Sie drei Lizenzen (1 Hostsystem plus 2 VMs) auf dem CA ARCserve Backup-Server registrieren.

Hinweis: Weitere Informationen zu den Sicherungsmodi finden Sie unter "[Funktionsweise des globalen und lokalen Sicherungsmodus](#) (siehe Seite 61)".

Installationsorte für den Agenten

In der folgenden Tabelle finden Sie eine Übersicht über die möglichen Sicherungsmodi und den entsprechenden Installationsort des Agenten.

Weitere Informationen zu den Sicherungsmodi finden Sie unter "[Funktionsweise des globalen und lokalen Sicherungsmodus](#) (siehe Seite 61)".

Ausgewählter Sicherungsmodus	Hyper-V-Hostsystem	VMware-Sicherungsproxysystem	VMware-VM	Hyper-V-VM
Dateimodus	Benötigt	Benötigt	Nicht benötigt	Benötigt
Raw-Modus (vollständige VM) ohne Auswahl der Option "Wiederherstellung im Dateimodus erlauben"	Benötigt	Benötigt	Nicht benötigt	Nicht benötigt
Raw-Modus (vollständige VM) mit Auswahl der Option "Wiederherstellung im Dateimodus erlauben"	Benötigt	Benötigt	Benötigt	Benötigt
Gemischter Modus ohne Auswahl der Option "Wiederherstellung im Dateimodus erlauben"	Benötigt	Benötigt	Nicht benötigt	Benötigt

Ausgewählter Sicherungsmodus	Hyper-V-Hostsystem	VMware-Sicherungs- Proxysystem	VMware-VM	Hyper-V-VM
Gemischter Modus mit Auswahl der Option "Wiederherstellung im Dateimodus erlauben"	Benötigt	Benötigt	Benötigt	Benötigt

Hinweis: Alle Agent-Lizenzen müssen auf dem CA ARCserve Backup-Primär- bzw. Standalone-Server registriert werden.

Sicherungsmodus und Installationsmatrix

Der Sicherungsmodus, der zum Sichern von VM-Daten verwendet werden kann, ist abhängig vom Installationsort des Agenten für virtuelle Rechner. In der folgenden Tabelle finden Sie eine Übersicht über die möglichen Sicherungsmodi mit dem jeweiligen Installationsort des Agenten.

Weitere Informationen zu den Sicherungsmodi finden Sie unter ["Funktionsweise des globalen und lokalen Sicherungsmodus \(siehe Seite 61\)".](#)

VMware-Systeme

Schlüssel:

- Beim Sicherungsmodus **Raw #** handelt es sich um eine Raw-(vollständige VM-)Sicherung mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Beim Sicherungsmodus **Mixed#** handelt es sich um eine Sicherung im gemischten Modus mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Der Begriff **Agent** bezieht sich auf den Agenten für virtuelle Rechner.
- **Client Agent** bezieht sich auf Client Agent für Windows.

Wichtig! Client Agent für Windows ist für den Agenten für virtuelle Rechner erforderlich.

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwend en von VCB	Verwenden des Client Agent	Verwen den von VCB	Verwenden des Client Agent

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwend en von VCB	Verwenden des Client Agent	Verwen den von VCB	Verwenden des Client Agent
Muss der Agent auf dem virtuellen Rechner/Gast -BS installiert werden?	Nein	Nein	Ja	Nein	Ja	Ja	Ja
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, ohne dass der Agent auf dem virtuellen Rechner/Gast -BS installiert ist?	Ja	Ja	Nein	Ja	Nein	Siehe Hinweis 1.	Nein

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwend en von VCB	Verwenden des Client Agent	Verwen den von VCB	Verwenden des Client Agent
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Können Wiederherstellungen anhand von Sitzungen erfolgen, die in diesem Sicherungsmodus und mit dem auf dem virtuellen Rechner/Gast-BS installierten Agenten durchgeführt wurden?	Nein	Ja	Ja	Siehe Hinweis 2.	Ja	Ja	Ja
Lassen sich virtuelle Rechner mit Hilfe von Daten wiederherstellen, die in diesem Sicherungsmodus und mit	Nein	Nein	Nein	Nein	Nein	Nein	Nein

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwend en von VCB	Verwenden des Client Agent	Verwen den von VCB	Verwenden des Client Agent
dem auf dem virtuellen Rechner/Gast -BS installierten Agenten durchgeführt wurden (siehe Hinweis 3)?							

Hinweis 1: Sicherungen im Raw-Modus und mit aktiverter Option "Wiederherstellung im Dateimodus erlauben" haben am Ende den Status "Abgeschlossen". Zuwachs- und Änderungssicherungen werden erfolgreich beendet.

Hinweis 2: Das Tool "VMware Converter" muss auf dem virtuellen Rechner installiert werden, damit CA ARCserve Backup virtuelle Rechner wiederherstellen kann. VMware Virtual Consolidated Backup (VCB) ist nicht erforderlich, um VM-Daten wiederherzustellen oder um Vorgänge zur Wiederherstellung der VM durchzuführen.

Hinweis 3: CA ARCserve Backup führt mit Hilfe des Mware Converter-Tools Vorgänge zur Wiederherstellung der VM durch, wobei das Tool auf dem Sicherungs-Proxy-System installiert ist. Sie müssen nicht den Agenten für virtuelle Rechner oder den Client Agent für Windows auf der VM installieren, um Vorgänge zur Wiederherstellung der VM durchzuführen.

Hyper-V-Systeme

Schlüssel:

- Beim **Raw**-Sicherungsmodus handelt es sich um eine Sicherung im Raw-Modus (gesamte VM) mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Beim **gemischten** Sicherungsmodus handelt es sich um eine Sicherung im gemischten Modus mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Der Begriff **Agent** bezieht sich auf den Agenten für virtuelle Rechner.
- Der Ausdruck **Client Agent** bezieht sich auf den Client Agent für Windows.

Wichtig! Der Client Agent für Windows ist eine für den Agenten für virtuelle Rechner erforderliche Komponente.

Frage	Raw	Datei	Raw #	Gemischt	Gemischt #
Muss der Agent auf dem virtuellen Rechner/Gast-BS installiert werden?	Nein	Ja	Ja	Ja	Ja
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, ohne dass der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Ja	Nein	Nein	Nein	Nein
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Ja	Ja	Ja	Ja	Ja
Können Sitzungen wiederhergestellt werden, die in diesem Sicherungsmodus gesichert wurden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Nein	Ja	Ja	Siehe Hinweis 1.	Ja
Können VMs von Daten wiederhergestellt werden, die in diesem Modus gesichert wurden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist (siehe Hinweis 2)?	Nein	Nein	Nein	Nein	Nein

Hinweis 1: Ja, Sie können Sitzungen wiederherstellen, die im gemischten Modus gesichert wurden. Dies gilt jedoch nur für Zuwachs- und Änderungssicherungen. Sie können Sitzungen, die im gemischten Modus gesichert wurden, jedoch nicht aus der ersten vollständigen Sitzungssicherung wiederherstellen.

Hinweis 2: Sie müssen den Agenten für virtuelle Rechner oder den Client Agent für Windows nicht auf den Hyper-V-VMs installieren. CA ARCserve Backup verwaltet die Wiederherstellung von Hyper-V-VMs, wenn Sie den Agenten für virtuelle Rechner auf dem Hyper-V-Hostsystem installieren.

Voraussetzungen für die Installation

Vor der Installation des Agenten müssen Sie zunächst folgende vorbereitende Aufgaben ausführen:

- Stellen Sie sicher, dass das System die für die Installation des Agenten erforderlichen Mindestvoraussetzungen erfüllt.
Eine Liste der Voraussetzungen finden Sie in der Readme.
- Stellen Sie sicher, dass Sie über ein Administratorprofil oder ein Profil mit Rechten für die Softwareinstallation verfügen.
- Stellen Sie sicher, dass Sie den Benutzernamen und das Kennwort des Systems kennen, auf dem Sie den Agenten installieren.
- Stellen Sie bei VMware-Umgebungen sicher, dass Microsoft .NET Framework Version 2 oder höher auf dem Sicherungs-Proxysystem installiert ist und ausgeführt wird.
- Stellen Sie bei VMware-Umgebungen sicher, dass das VMware VCB-Framework auf dem Sicherungs-Proxysystem installiert ist.

Installationshinweise

Der folgende Abschnitt bietet Informationen zu besonderen Aspekten bei der Installation des CA ARCserve Backup Agenten für virtuelle Rechner.

- Sie müssen den Agenten an folgenden Speicherorten installieren:
 - VMware-Umgebungen: auf dem Sicherungs-Proxysystem und auf den VMs, die Sie schützen möchten.
 - Hyper-V-Umgebungen: auf dem Hyper-V-Hostsystem und auf den VMs, die Sie schützen möchten.
- Für jede VM, die Sie mit CA ARCserve Backup schützen, müssen Sie eine Lizenz registrieren. Alle Lizenzen müssen auf dem Primär- und Standalone-Server registriert werden.
- Für den Agenten ist der CA ARCserve Backup Client Agent für Windows erforderlich. Sie müssen den Client Agent für Windows an allen Speicherorten installieren, an denen Sie den Agenten für virtuelle Rechner installiert haben.

Hinweis: Weitere Informationen finden Sie unter "[Lizenzierung des Agenten](#)" (siehe Seite 21) und unter "[Installationsorte für den Agenten](#)" (siehe Seite 22).

Installieren und Konfigurieren des Agenten

Es gibt zwei Methoden, wie Sie den Agenten installieren können:

- Installieren Sie den Agenten bei der Installation von CA ARCserve Backup. Der Agent kann entsprechend den Standardvorgehensweisen für die Installation von Systemkomponenten, Agenten und Optionen von CA ARCserve Backup installiert werden.
- Installieren Sie den Agenten nach der Installation von CA ARCserve Backup. Mit der Agent-Bereitstellung können Sie den Agenten jederzeit nach der Installation von CA ARCserve Backup installieren.

Hinweis: Weitere Informationen zum Installieren von Agenten mit Hilfe der Agent-Bereitstellung finden Sie im *Administrationshandbuch*.

Um den Agenten zu installieren und zu konfigurieren, müssen Sie zunächst folgende Aufgaben ausführen:

1. Befolgen Sie die Anweisungen zur Installation von CA ARCserve Backup im "*Implementierungshandbuch*".
2. Installieren Sie die für den Agenten erforderliche Anzahl von Lizenzen auf dem Primärserver oder dem Standalone-Server.
3. Führen Sie die Konfigurationsaufgaben wie unter [Aufgaben nach der Installation](#) (siehe Seite 33) beschrieben aus.

Bereitstellen des Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung

Mit der CA ARCserve Backup Agent-Bereitstellung können Sie CA ARCserve Backup-Agenten auf lokalen VMs oder Remote-VMs installieren und aktualisieren. Bei der Methode zur Bereitstellung virtueller Rechner können Sie die Agenten angeben, die Sie auf lokalen VMs oder Remote-VMs installieren oder aktualisieren möchten. Durch diese Methode wird sichergestellt, dass alle in Ihrer CA ARCserve Backup-Umgebung auf VMs ausgeführten Agenten die gleiche Versionsnummer aufweisen wie der CA ARCserve Backup-Server.

Beachten Sie folgende Einschränkungen:

- Um einen Agenten auf einer VM zu installieren oder zu aktualisieren, muss die VM ausgeführt werden.
- Die Agent-Bereitstellung installiert oder aktualisiert Agenten auf allen VMs innerhalb des ESX-Serversystems und des Hyper-V-Hostsystems.

So stellen Sie mittels der VM-Bereitstellung CA ARCserve Backup-Agenten auf VMs bereit:

1. Öffnen Sie die CA ARCserve Backup-Managerkonsole.

Wählen Sie im Schnellstartmenü die Option "Verwaltung", und klicken Sie auf "Agent-Bereitstellung".
Die CA ARCserve Backup-Agent-Bereitstellung wird gestartet und das Dialogfeld "Anmeldeserver" geöffnet.
2. Füllen Sie die erforderlichen Felder in diesem Dialogfeld aus, und klicken Sie auf "Weiter".

Das Dialogfeld "Methoden" wird geöffnet.
3. Wählen Sie im Dialogfeld "Methoden" die Option "Bereitstellung virtueller Rechner" aus, und klicken Sie auf "Weiter".

Das Dialogfeld "Komponenten" wird geöffnet.
4. Wählen Sie im Dialogfeld "Komponenten" die Agenten aus, die Sie auf allen Remote-Hosts installieren möchten, und klicken Sie auf "Weiter".

Das Dialogfeld "Hostinformationen" wird angezeigt.

5. Geben Sie auf eine der folgenden Arten die Namen der Remote-Hosts an, auf denen sich die VMs befinden:

- Klicken Sie auf "Importieren", um eine Liste mit Remote-Hosts aus einer Textdatei zu importieren.

Hinweis: Die Hostnamen müssen durch einen Zeilenumbruch voneinander abgetrennt werden. Sie können mehrere Textdateien importieren, die Gesamtanzahl der Remote-Hosts darf jedoch maximal 1000 betragen.

Sobald die Hostnamen in der Spalte "Host" angezeigt werden, fahren Sie mit dem folgenden Schritt fort.

- Klicken Sie auf "Aktualisieren", um die vorhandenen VMs aus der CA ARCserve Backup-Datenbank zu importieren.

Sobald die Hostnamen in der Spalte "Host" angezeigt werden, fahren Sie mit dem folgenden Schritt fort.

- Geben Sie den Namen des Remote-Hosts im Feld "Hostname" an, und klicken Sie auf "Hinzufügen".

Hinweis: Wiederholen Sie diesen Schritt, bis alle erforderlichen Hostnamen in der Spalte "Host" angezeigt werden.

Sobald die Hostnamen in der Spalte "Host" angezeigt werden, fahren Sie mit dem folgenden Schritt fort.

Hinweis: Sie können bis zu 1000 Remote-Hosts angeben. Wenn Sie Agenten auf mehr als 1000 Remote-Hosts bereitstellen möchten, können Sie die Agent-Bereitstellung neu starten und diese Aufgabe wiederholen, oder Sie können die Agent-Bereitstellung von einem alternativen CA ARCserve Backup-Primärserver oder -Standalone-Server ausführen.

6. Geben Sie wie folgt den Benutzernamen und das Kennwort für die Remote-Hosts an:

a. Klicken Sie in das Feld "Benutzername" (neben dem Hostnamen), und geben Sie den Benutzernamen in folgendem Format an:

<Domäne>\<Benutzername>

b. Klicken Sie in das Feld "Kennwort", und geben Sie das entsprechende Kennwort ein.

c. Wiederholen Sie diesen Schritt, bis Sie den Benutzernamen und das Kennwort für alle Remote-Hosts angegeben haben.

Falls Benutzername und Kennwort für alle Remote-Hosts identisch sind, geben Sie optional den Benutzernamen im Feld "Benutzer" ein (<Domäne>\<Benutzername>) und das Kennwort im Feld "Kennwort", stellen Sie sicher, dass alle Kontrollkästchen aktiviert sind, und klicken Sie dann auf "Anmeldeinformationen anwenden".

Der Benutzername und das Kennwort werden für alle Remote-Hosts in der Liste übernommen.

Hinweis: Um einen Host von der Liste "Hosts und Anmeldeinformationen" zu entfernen, aktivieren Sie das Kontrollkästchen neben dem Host, den Sie entfernen möchten, und klicken Sie auf "Entfernen".

Klicken Sie auf Weiter, um fortzufahren.

Die Agent-Bereitstellung überprüft den für alle festgelegten Hosts angegebenen Hostnamen, den Benutzernamen und das Kennwort. Wenn die Agent-Bereitstellung keinen Authentifizierungsfehler ermittelt, wird das Statusfeld auf "Ausstehend" gesetzt. Wenn die Agent-Bereitstellung einen Authentifizierungsfehler ermittelt, wird das Statusfeld auf "Fehlgeschlagen" gesetzt. Sie können dann auf "Fehlgeschlagen" klicken, um die Gründe für den Fehler zu ermitteln. Sie müssen alle gemeldeten Fehler korrigieren, um fortzufahren.

Klicken Sie auf Weiter.

7. Wenn das Statusfeld aller Hosts "Ausstehend" oder "Bestätigt" anzeigt, klicken Sie auf "Weiter".

Das Dialogfeld "Setup-Zusammenfassung" wird geöffnet.

8. Überprüfen Sie im Dialogfeld "Setup-Zusammenfassung" die angegebenen Komponenten und Hostnamen.

Klicken Sie auf Weiter.

Das Dialogfeld "Installationsstatus" wird geöffnet.

9. Klicken Sie im Dialogfeld "Installationsstatus" auf "Installieren".

Die Agent-Bereitstellung installiert oder aktualisiert die CA ARCserve Backup-Agenten auf den angegebenen Hosts.

Nach Abschluss aller Installationen und Aktualisierungen wird das Dialogfeld "Installationsbericht" geöffnet.

10. Wählen Sie eine der folgenden Vorgehensweisen:

- Wenn bei einigen Remote-Hosts ein Neustart erforderlich ist, klicken Sie auf "Weiter".

Das Dialogfenster "Neu starten" wird geöffnet. In ihm sind die Remote-Hosts angegeben, die einen Neustart erfordern.

Klicken Sie auf "Neu starten".

Fahren Sie mit dem nächsten Schritt fort.

- Wenn bei keinem der Remote-Hosts ein Neustart erforderlich ist, klicken Sie auf "Fertig stellen", um die Aufgabe abzuschließen.

11. Aktivieren Sie im Dialogfeld "Neu starten" das Kontrollkästchen neben dem Remote-Host, den Sie jetzt neu starten möchten.

Optional können Sie das Kontrollkästchen "Alles markieren" aktivieren, um alle Remote-Hosts jetzt zu starten.

Klicken Sie auf "Neu starten".

Die Agent-Bereitstellung führt nun einen Neustart für alle Remote-Hosts aus.

Hinweis: Wenn Sie eine Liste der Remote-Hosts erstellen möchten, für die ein Neustart erforderlich ist, klicken Sie auf "Bericht über Neustart exportieren".

12. Wenn das Statusfeld aller Remote-Hosts "Abgeschlossen" anzeigt, klicken Sie auf "Fertig stellen".

Die CA ARCserve Backup-Agenten sind nun auf den VMs bereitgestellt.

Aufgaben nach der Installation

In den folgenden Abschnitten werden die Aufgaben beschrieben, die Sie nach der Installation durchführen müssen, um verschiedene Versionen von ESX Server- und VirtualCenter Server-VMware-Systemen zu schützen. Zum Schutz von Hyper-V-basierten Systemen ist nach der Installation des Agenten keine weitere Konfiguration erforderlich.

Geben Sie den Namen des CA ARCserve Backup-Servers an.

Um Wiederherstellungen auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben.

Diese Aufgabe entfällt, wenn Sie den CA ARCserve Backup Agenten für virtuelle Rechner mit Hilfe des Agent-Bereitstellungstools auf Ihren virtuellen Rechnern installiert haben. Weitere Informationen finden Sie unter Bereitstellen von Agenten für virtuelle Rechner unter Verwendung der VM-Bereitstellung.

Hinweis: Die folgenden Schritte gelten für VMware- und Hyper-V-VMs.

So geben Sie den Namen des CA ARCserve Backup-Servers an:

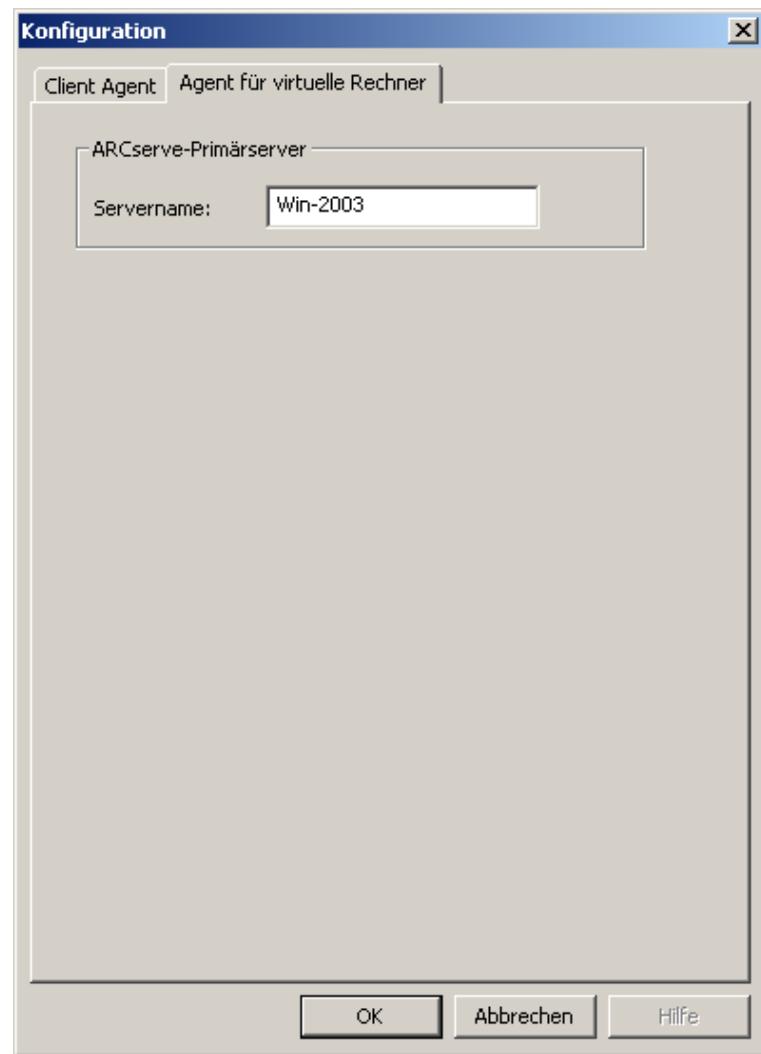
1. Melden Sie sich bei der VM an, und öffnen Sie den Bereich für die Backup Agent-Verwaltung.

Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent - Verwaltung".
Das Dialogfeld "Backup Agent - Verwaltung" wird geöffnet.
2. Wählen Sie in der Dropdown-Liste die Option "CA ARCserve Backup Client Agent", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".

Das Dialogfeld "Konfiguration" wird geöffnet.

3. Klicken Sie auf die Registerkarte "Agent für virtuelle Rechner".

Geben Sie im Feld "Servername" den Hostnamen oder die IP-Adresse des CA ARCserve Backup-Servers ein, der diese VM schützt, und klicken Sie auf "OK".



Der Name des CA ARCserve Backup-Servers wird gespeichert.

Hinweis: Wiederholen Sie diese Schritte nach Bedarf auf allen VMs in Ihrer CA ARCserve Backup-Umgebung.

Einpfliegen von Informationen in die Datenbank mit Hilfe des ARCserve-Konfigurationstools für VMware

Das ARCserve VMware-Konfigurationstool ist ein Hilfsprogramm zum Sammeln von Daten, das Informationen zu den VMs auf Ihrem ESX-Server in die CA ARCserve Backup-Datenbank einpflegt. In dieses Tool ist ein Befehlszeilendienstprogramm mit dem Namen "ca_vcbpopulatedb" integriert, das im Hintergrund ausgeführt wird und Informationen zu den VMs in die ARCserve-Datenbank einpflegt. Das Konfigurationstool sammelt folgende Informationen:

- VCB-Sicherungs-Proxynamen
- ESX-Server- oder VirtualCenter-Servernamen
- VM-Hostnamen
- Namen der Volumes auf den VMs in Windows-Systemen

Nach der Installation des Agenten müssen Sie die CA ARCserve Backup-Datenbank mit Informationen zu Ihren VM-Systemen füllen. Hierfür müssen Sie das ARCserve-Konfigurationstool für VMware auf dem Sicherungs-Proxysystem ausführen.

Nachdem Sie das ARCserve VMware-Konfigurationstool ausgeführt und einen Sicherungsjob für die Daten auf den virtuellen Rechnern übergeben haben, wird die CA ARCserve Backup-Datenbank automatisch mit den Informationen über die virtuellen Rechner gefüllt, die bei der Ausführung des Konfigurationstools angegeben wurden. Mit der Option zur automatischen Aufnahme können Sie sicherstellen, dass der Sicherungs-Manager richtig durchsucht wird und die aktuellen Daten auf den virtuellen Rechnern gesichert werden. CA ARCserve Backup füllt die Datenbank standardmäßig automatisch in 24-Stunden-Abständen nach Abschluss der Sicherung mit aktualisierten Daten.

So pflegen Sie mit Hilfe des ARCserve VMware-Konfigurationstools Informationen in die Datenbank ein:

1. Stellen Sie sicher, dass die VMs im ESX-Server-System ausgeführt werden.
Hinweis: Wenn die VMs nicht ausgeführt werden, pflegt das ARCserve-Konfigurationstool für VMware keine Daten in die CA ARCserve Backup-Datenbank ein, und Sie können die VMs in den ESX-Server-Systemen nicht richtig durchsuchen und sichern.
2. Melden Sie sich beim Sicherungs-Proxysystem an, und öffnen Sie den Bereich für die Backup Agent-Verwaltung.
Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent – Verwaltung".
Das Dialogfeld "Backup Agent – Verwaltung" wird geöffnet.

3. Wählen Sie in der Dropdown-Liste die Option "CA ARCserve Backup Agent für virtuelle Rechner", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".

Das ARCserve-Konfigurationstool für VMware wird geöffnet.

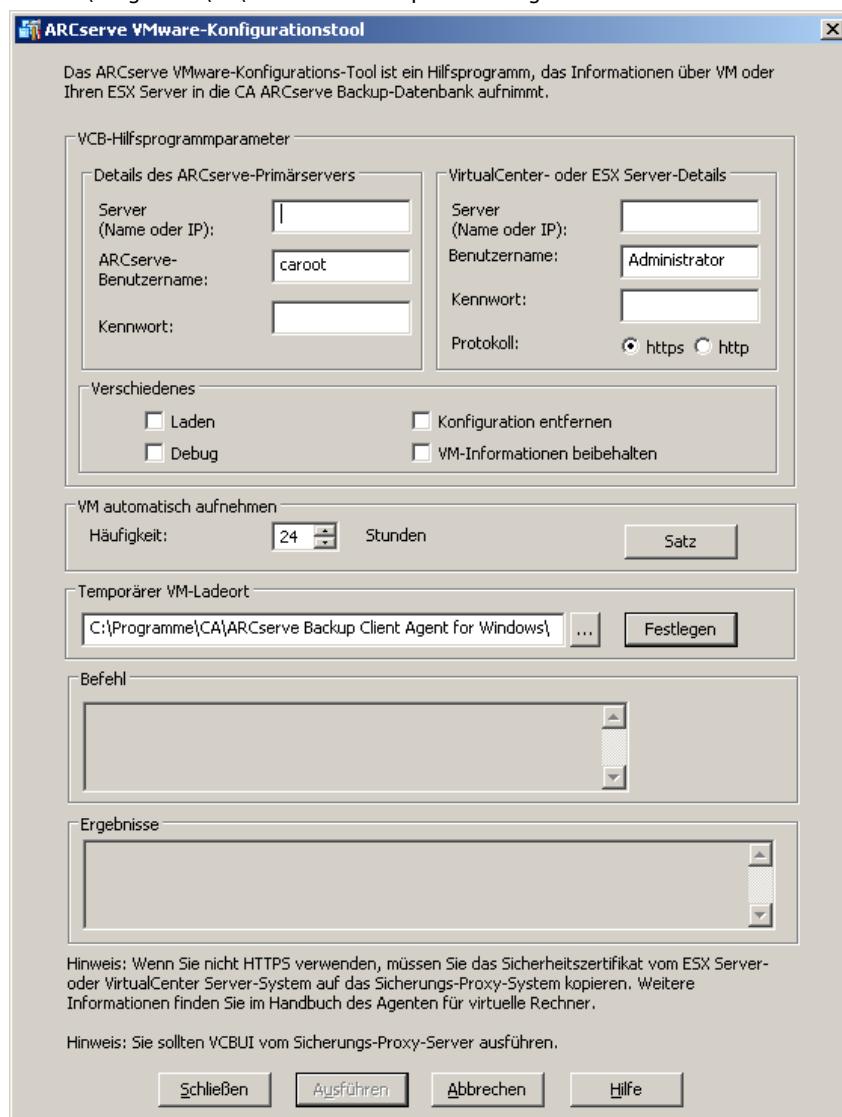
Hinweis: Die Datei "VCBUI.exe" wird in eines der folgenden Verzeichnisse auf dem Sicherungs-Proxysystem installiert:

- X86-Systeme

C:\Programme\CA\ARCserve Backup Client Agent für windows\x86

- X64-Systeme

C:\Programme\CA\ARCserve Backup Client Agent for windows



4. Füllen Sie die folgenden Felder aus:

Informationen zum ARCserve-Primärserver

Folgende Optionen gelten für den CA ARCserve Backup-Primärserver oder - Standalone-Server:

- **Server (Name oder IP):** Hier können Sie den Namen oder die IP-Adresse des CA ARCserve Backup-Primärsystems angeben.
- **ARCserve-Benutzername:** Hier können Sie den Benutzernamen mit (CAROOT-Rechten) für das CA ARCserve Backup-Primärsystem angeben.
- **Kennwort:** Hier können Sie das Kennwort für den CA ARCserve Backup-Benutzernamen eingeben.

Informationen zum VirtualCenter- oder ESX-Server

Folgende Optionen gelten für die virtuelle VMware-Infrastruktur in Ihrer Umgebung:

- **Server (Name oder IP):** Hier können Sie den Namen des ESX-Server- oder VirtualCenter-Server-Systems angeben.
- **Benutzername:** Hier können Sie den Namen des ESX-Server- oder VirtualCenter-Benutzers (mit Administratorrechten) angeben.
- **Kennwort:** Hier können Sie das Kennwort für den ESX-Server- oder VirtualCenter-Server-Benutzernamen eingeben.
- **Protokoll:** Hier können Sie das Protokoll für die Kommunikation zwischen dem Sicherungs-Proxysystem und dem ESX-Server-System oder VirtualCenter-Server-System angeben.

Hinweis: Falls Sie dieses Argument auslassen, verwendet das Tool https als Kommunikationsprotokoll.

Verschiedenes

Legen Sie die folgenden verschiedenen Optionen nach Bedarf fest, um Informationen in die CA ARCserve Backup-Datenbank einzupflegen:

- **Laden:** Wenn die Option "Laden" aktiviert ist, pflegt das Konfigurationstool die Namen der VMs, die geladen werden können, in die Datenbank ein.
- **Hinweis:** Wenn Sie das Konfigurationstool ausführen und die Option "Laden" nicht aktiviert ist, dauert das Ausführen des Hilfsprogramms länger, da für jede ausgeführte VM ein Lade- und ein Entladevorgang ausgeführt wird.
- **Konfiguration entfernen:** Mit dieser Option können Sie die VMs in der Datenbank für das angegebene ESX-Server-System oder VirtualCenter-Server-System unter dem angegebenen Sicherungs- Proxysystem löschen.
- **Debug:** Mit dieser Option können Sie ein detailliertes Debug-Protokoll schreiben. Das Protokoll wird im Client Agent für Windows- Installationsverzeichnis erstellt. Dieses Verzeichnis lautet standardmäßig wie folgt:

```
C:\Programme\CA\ARCserve Backup Client Agent für Windows\LOG
```

Hinweis: Der Name der Protokolldatei lautet "ca_vcbpopulatedb.log".
- **VM-Informationen beibehalten:** Ermöglicht Ihnen, Daten (Sicherungsinformationen) für virtuelle Rechner, die nicht verfügbar sind, wenn Sie dieses Tool ausführen, beizubehalten.
- Standardmäßig erfasst dieses Hilfsprogramm Informationen von virtuellen Rechnern, die verfügbar sind, wenn Sie dieses Tool ausführen. Wenn eine VM nicht verfügbar ist (zum Beispiel weil sie heruntergefahren oder aus der Umgebung gelöscht wurde), löscht CA ARCserve Backup die mit dieser VM verbundenen Daten aus der CA ARCserve Backup-Datenbank. Wenn diese Option aktiviert wurde, erfasst CA ARCserve Backup Informationen zu virtuellen Rechnern, die verfügbar sind, und behält die Sicherungsinformationen von virtuellen Rechnern, die nicht verfügbar sind, bei.

VM automatisch aufnehmen

Hiermit können Sie festlegen, wie oft die CA ARCserve Backup- Datenbank automatisch mit Informationen zu den virtuellen Rechnern gefüllt wird.

Standardeinstellung: 24 Stunden

Bereich: 1 bis 99 Stunden

Temporärer VM-Ladeort

Legt fest, wo das ARCserve VMware-Konfigurationstool während dessen Ausführung die Sicherungsinformationen für die VMs vorübergehend lädt (speichert).

Standardmäßig speichert CA ARCserve Backup die temporären Sicherungsinformationen an folgendem Speicherort:

C:\Programme\CA\ARCserve Backup Client Agent for windows

Hinweis: Sie müssen auf "Festlegen" klicken, um den Speicherort zu übernehmen.

Es kann beispielsweise nötig sein, den temporären Ladeort zu verschieben, da nicht genügend freier Speicherplatz vorhanden ist, um die Sicherung auf das Volume zu laden. Weitere Informationen finden Sie unter [Angaben eines temporären VM-Ladeortes](#) (siehe Seite 40).

5. Klicken Sie auf "Ausführen".

Hinweis: Sie können erst dann auf "Ausführen" klicken, wenn alle erforderlichen Felder vollständig ausgefüllt sind.

Das ARCserve VMware-Konfigurationstool befüllt die CA ARCserve Backup-Datenbank mit Daten. Die Ergebnisse der Ausführung werden im ARCserve VMware-Konfigurationstool im Feld "Ergebnis" angezeigt. Zum Anzeigen detaillierter Protokollinformationen öffnen Sie die Protokolldatei mit dem Namen "ca_vcbsystem.log", die sich im Installationsverzeichnis des Client Agent für Windows auf dem Sicherungs-Proxysystem befindet.

Festlegen eines temporären VM-Ladeorts

Um Informationen zu den virtuellen Rechnern in Ihrer VMware-Sicherungsumgebung in die CA ARCserve Backup-Datenbank aufzunehmen, benötigt CA ARCserve Backup einen Speicherort, um die Sicherungsinformationen temporär zu speichern, während das ARCserve VMware-Konfigurationstool ausgeführt wird.

Standardmäßig speichert CA ARCserve Backup die temporären Sicherungsinformationen an dem Speicherort, der auf das Sicherungs-Proxy-System folgt:

C:\Programme\CA\ARCserve Backup Client Agent for windows

Hinweis: Bei Systemen ohne Windows reservieren Sie mindestens so viel Speicher wie auf dem Laufwerk verwendet wird bzw. wie maximal zulässig ist, um die am temporären Speicherort der VM abgelegten Daten speichern zu können. Bei Systemen mit Windows ist dies nicht erforderlich.

Führen Sie folgende Schritte aus, um einen anderen Speicherort für den temporären VM-Ladeort auf dem Sicherungs-Proxy-System festzulegen.

Beachten Sie Folgendes:

- Der temporäre VM-Ladeort muss sich auf dem Sicherungs-Proxy-System befinden.
- Die Verwendung zugeordneter Laufwerke auf dem Sicherungs-Proxy-System für den temporären VM-Ladeort wird von CA ARCserve Backup nicht unterstützt.

So legen Sie einen temporären VM-Ladeort fest:

1. Melden Sie sich beim Sicherungs-Proxy-System an, und öffnen Sie den Bereich für die Backup Agent-Verwaltung.
Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent – Verwaltung".
Das Dialogfeld "Backup Agent-Verwaltung" wird geöffnet.
2. Wählen Sie in der Dropdown-Liste die Option "CA ARCserve Backup Agent für virtuelle Rechner", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".
Das ARCserve-Konfigurationstool für VMware wird geöffnet.
3. Geben Sie im Feld "Temporärer VM-Ladeort" den Pfad zu dem Standort an, an dem Sie die Daten laden möchten.
4. Klicken Sie auf <cs id="559">Festlegen</cs>.
Der temporäre VM-Ladeort ist eingestellt.
5. Klicken Sie auf "Schließen".
Das ARCserve VMware-Konfigurationstool wird beendet.

Einpflegen von Informationen in die Datenbank mit Hilfe des Befehlszeilenhilfsprogramms "ca_vcbpopulatedb"

Das Hilfsprogramm "ca_vcbpopulatedb" ist ein Tool zur Datenerfassung, das es Ihnen ermöglicht, folgende Informationen in die CA ARCserve Backup-Datenbank aufzunehmen:

- Namen der VCB-Sicherungs-Proxy-Systeme
- ESX-Server- oder VirtualCenter-Servernamen
- VM-Hostnamen
- Namen der Volumes auf den VMs in Windows-Systemen

Nach der Installation des Agenten müssen Sie die CA ARCserve Backup-Datenbank mit Informationen zu Ihren VMware-Systemen füllen. Hierzu müssen Sie das Hilfsprogramm "ca_vcbpopulatedb" auf dem Sicherungs-Proxysystem oder einem anderen Windows 2003 (X86 und X64)-System ausführen, auf dem der CA ARCserve Backup Client Agent für Windows installiert ist.

Hinweis: Wenn Sie diese Aufgabe nicht ausführen, können Sie die VMware-VMs in Ihrer Umgebung nicht mit Hilfe des Sicherungs-Managers durchsuchen.

So pflegen Sie mit Hilfe des Befehlszeilenhilfsprogramms "ca_vcbpopulatedb" Informationen in die CA ARCserve Backup-Datenbank ein:

1. Stellen Sie sicher, dass die VMs im ESX-Server-System ausgeführt werden.

Hinweis: Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm "ca_vcbpopulatedb" nicht die korrekten Daten in die CA ARCserve Backup-Datenbank ein, und Sie können die VMs in den ESX-Server-Systemen nicht richtig durchsuchen und sichern.

2. Rufen Sie das Sicherungs-Proxysystem auf, öffnen Sie ein Befehlszeilenfenster, und führen Sie das Hilfsprogramm "ca_vcbpopulatedb" aus.

Wichtig! Sie müssen dieses Hilfsprogramm auf dem Sicherungs-Proxysystem oder einem anderen Windows 2003-System ausführen, auf dem der Agent für virtuelle Rechner installiert ist.

Das Hilfsprogramm "ca_vcbpopulatedb" ist im Verzeichnis von Client Agent für Windows gespeichert. Der Client Agent für Windows ist standardmäßig in einem der folgenden Verzeichnissen installiert:

- X86-Systeme
C:\Programme\CA\ARCserve Backup Client Agent for windows
- X64-Systeme
C:\Programme\CA\ARCserve Backup Client Agent für windows\x86

3. Es gibt zwei Methoden, wie Sie das Hilfsprogramm ausführen können:
Führen Sie das Hilfsprogramm mit einer der folgenden Methoden aus:

- Führen Sie den Befehl mit den in der folgenden Syntax beschriebenen Argumenten aus:

```
ca_vcbpopulatedb -Primary <Primärservername> -carootUser <ARCserve-
caroot-Benutzer> -carootPass <ARCserve-caroot-Kennwort> [-vcb <VCB-
Rechnername>] -esxServer <ESX-Servername> -esxUser <ESX-Admin> -
esxUserPass <ESX-Admin-Kennwort> [-proto <https/http>] [-vcbMountablevM]
[-delProxydb] [-retainvMinDB] [-silent] [-debug] -insertvM <VM-Name> -
deletevM <VM-Name> [-stopAutoPopulate]
```

Hinweis: Informationen zur Verwendung dieses Befehls finden Sie unter [ca_vcbpopulatedb – Verwendung](#) (siehe Seite 44).

- Führen Sie den Befehl mit den in der folgenden Syntax beschriebenen Argumenten aus:

Hinweis: Sie müssen eine Konfigurationsdatei erstellen, um diese Syntax zu verwenden. Weitere Informationen finden Sie unter ["Erstellen einer 'ca_vcbpopulatedb'-Konfigurationsdatei](#) (siehe Seite 43)".

ca_vcbpopulatedb -config <Name der Konfigurationsdatei>

<Name der Konfigurationsdatei>

Der Name der Konfigurationsdatei für "ca_vcbpopulatedb".

4. Führen Sie den Befehl aus.

Das Hilfsprogramm "ca_vcbpopulatedb" pflegt Informationen zu den VMs, die derzeit in Ihrer Umgebung ausgeführt werden, in die CA ARCserve Backup-Datenbank ein.

Erstellen einer ca_vcbpopulatedb-Konfigurationsdatei

Sie erstellen eine Konfigurationsdatei mit Einzelheiten über den CA ARCserve Backup-Primärserverrechner, den CA ARCserve Backup-Primärbenutzernamen usw. Das Hilfsprogramm "ca_vcbpopulatedb" verwendet die in der Konfigurationsdatei angegebenen Informationen zur Aufnahme in der CA ARCserve Backup-Datenbank.

So erstellen Sie eine ca_vcbpopulatedb-Konfigurationsdatei:

1. Öffnen Sie eine Texteditoranwendung wie beispielsweise Notepad. Speichern Sie die Konfigurationsdatei mit der Dateierweiterung ".cfg" in demselben Verzeichnis wie das Hilfsprogramm "ca_vcbpopulatedb".

2. Ergänzen Sie die Argumente in der folgenden Syntax:

```
ca_vcbpopulatedb -Primary <Primärservername> -carootUser <ARCserve-caroot-Benutzer> -carootPass <ARCserve-caroot-Kennwort> [-vcb <VCB-Rechnername>] -esxServer <ESX-Servername> -esxUser <ESX-Admin> -esxUserPass <ESX-Admin-Kennwort> [-proto <https/http>] [-vcbMountableVM] [-delProxydb] [-retainVMDB] [-silent] [-debug] -insertVM <VM-Name> -deleteVM <VM-Name> [-stopAutoPopulate]
```

Hinweis: Informationen zur Verwendung dieses Befehls finden Sie unter [ca_vcbpopulatedb – Verwendung](#) (siehe Seite 44).

3. Schließen und sichern Sie die Konfigurationsdatei.

ca_vcbpopulatedb – Verwendung

Der Befehl "ca_vcbpopulatedb" beinhaltet Argumente und Optionen zur Definition von Aktionen, die beim Füllen der CA ARCserve Backup-Datenbank mit Informationen über virtuelle Rechner (VM) zu befolgen sind.

Der Befehl "ca_vcbpopulatedb" umfasst folgende Argumente und Optionen:

-Primary <Primärservername>

Gibt Namen oder IP-Adresse des CA ARCserve Backup-Primärsystems an.

-carootUser <ARCserve caroot-Benutzer>

Gibt den Benutzernamen (mit CAROOT-Rechten) für das CA ARCserve Backup-Primärsystem an.

-carootPass <ARCserve caroot-Kennwort>

Gibt das Kennwort für den Benutzernamen an.

(Optional) -vcb <VCB-Rechnername>

Gibt den Namen oder die IP-Adresse des VCB-Sicherungs-Proxysystems an.

Hinweis: Wenn Sie dieses Argument weglassen, setzt das Hilfsprogramm voraus, dass der aktuelle Rechnername als VCB-Rechnername verwendet wird.

-esxserver <ESX-Servername>

Gibt den Namen des ESX Server-Systems oder des VirtualCenter Server-Systems an, das die VMs enthält.

-esxUser <ESX-Administrator>

Gibt den Benutzernamen für das ESX-Server-System oder das VirtualCenter-Server-System (mit Administratorrechten) an.

-esxUserPass <ESX-Administratorkennwort>

Gibt das Kennwort für den ESXAdmin-Benutzer an.

(Optional) -proto <https/http>

Gibt das Protokoll für die Kommunikation zwischen dem Sicherungs-Proxysystem und dem ESX-Server-System oder dem VirtualCenter-Server-System an.

Hinweis: Falls Sie dieses Argument auslassen, verwendet das Hilfsprogramm https als Kommunikationsprotokoll.

-VCBMountableVM

Folgende Optionen stehen zur Verfügung:

Wenn Sie das Befehlszeilenhilfsprogramm "ca_vcbsystem" mit diesem Schalter ausführen, müssen Sie das Hilfsprogramm auf einem Sicherungs-Proxysystem ausführen. Ohne diesen Schalter müssen Sie das Hilfsprogramm "ca_vcbsystem" auf dem Sicherungs-Proxysystem oder einem anderen Windows 2003-System ausführen, auf dem der CA ARCserve Backup Client Agent für Windows installiert ist.

Wenn Sie diesen Schalter als Parameter angeben, fügt das Hilfsprogramm der Datenbank die Namen der VMs hinzu, die ausgeführt werden und geladen werden können.

Sie sollten das Befehlszeilenhilfsprogramm "ca_vcbsystem" mit diesem Schalter ausführen, wenn Sie VMs in einem ESX-Server auf mehreren Speicherdatenträgern haben, wie beispielsweise auf der lokalen Festplatte eines ESX-Servers, einem SAN-LUN-, NAS/NFS- oder iSCSI-Speichergerät.

Hinweis: Wenn Sie dieses Hilfsprogramm mit dem Schalter "VCBMountableVM" ausführen, dauert das Ausführen lange, da für jede ausgeführte VM ein Lade- und Entladevorgang ausgeführt wird.

-DelProxydb

Löscht alle VMs in der Datenbank für das angegebene ESX-Server-System oder das VirtualCenter-Server-System unter dem angegebenen Sicherungs-Proxysystem.

-retainVMinDB

Hiermit können Sie Daten (Sicherungsinformationen) zu VMs aufbewahren, die während der Ausführung dieses Befehls nicht verfügbar sind.

Standardmäßig erfasst dieses Hilfsprogramm Informationen von virtuellen Rechnern, die verfügbar sind, wenn Sie dieses Hilfsprogramm ausführen. Wenn eine VM nicht verfügbar ist (zum Beispiel weil sie heruntergefahren oder aus der Umgebung gelöscht wurde), löscht CA ARCserve Backup die mit dieser VM verbundenen Daten aus der CA ARCserve Backup-Datenbank. Wenn diese Option aktiviert wurde, erfasst CA ARCserve Backup Informationen zu virtuellen Rechnern, die verfügbar sind, und behält die Sicherungsinformationen von virtuellen Rechnern, die nicht verfügbar sind, bei.

-Silent

Verhindert, dass das Hilfsprogramm Meldungen an die Befehlszeilenkonsole sendet.

-Debug

Mit dieser Option können Sie ein detailliertes Debug-Protokoll schreiben. Das Protokoll wird im Client Agent für Windows-Installationsverzeichnis erstellt. Dieses Verzeichnis lautet standardmäßig wie folgt:

C:\Programme\CA\ARCserve Backup Client Agent for windows

Hinweis: Der Name der Protokolldatei lautet "ca_vcbpopulatedb.log".

-insertVM

Mit dieser Option können Sie Informationen zu einer bestimmten VM, die sich auf dem VM-Hostsystem befindet, zur CA ARCserve Backup-Datenbank hinzufügen.

Hinweis: Dieses Argument können Sie mit keinem anderen Argument kombinieren, wenn Sie "ca_vcbpopulateDB" ausführen.

-deleteVM

Mit dieser Option können Sie Informationen zu einer bestimmten VM aus der CA ARCserve Backup-Datenbank löschen.

Hinweis: Dieses Argument können Sie mit keinem anderen Argument kombinieren, wenn Sie "ca_vcbpopulateDB" ausführen.

-stopAutoPopulate

Hiermit können Sie die automatische Aufnahme für das angegebene Sicherungs-Proxy-System deaktivieren.

Weitere Informationen:

[Beispiele](#) (siehe Seite 48)

Rückgabecodes des Hilfsprogramms "ca_vcbpopulatedb"

Das Hilfsprogramm "ca_vcbpopulatedb" generiert Rückgabecodes in einer Protokolldatei namens "ca_vcbpopulatedb.log". Das Protokoll wird nach dem Ausführen des Hilfsprogramms "ca_vcbpopulatedb" im Client Agent für Windows-Installationsverzeichnis erstellt.

Das Hilfsprogramm "ca_vcbpopulatedb" generiert die folgenden Rückgabecodes:

0

Gibt an, dass der Vorgang erfolgreich war.

1

Gibt an, dass ein ungültiges Argument angegeben wurde.

2

Gibt an, dass die Authentifizierung des CA ARCserve Backup-Domänenbenutzers fehlgeschlagen ist.

3

Gibt an, dass bei der Authentifizierung des ESX-Server- oder VirtualCenter-Server-Benutzers ein Fehler aufgetreten ist.

4

Gibt an, dass die ESX-Serververbindung oder die VirtualCenter-Serververbindung fehlgeschlagen ist.

5

Gibt an, dass ein Datenbankvorgang fehlgeschlagen ist.

6

Gibt an, dass eine XML-Erstellung fehlgeschlagen ist.

7

Gibt an, dass Microsoft .NET Version 2.0 oder höher nicht in Ihrer Umgebung installiert ist.

8

Gibt an, dass derzeit mehr als eine Instanz von "ca_vcbpopulatedb" ausgeführt wird.

9

Gibt an, dass ein unbekannter Fehler aufgetreten ist.

Beispiele

Nachfolgend finden Sie Syntaxbeispiele für den Befehl "ca_vcbpopulatedb":

- Mit Hilfe des folgenden Befehls übernehmen Sie die VM-Details des ESX-Servers mit dem Hostnamen "ESXServer1" in die Datenbank auf dem ARCserve-Server "ARCserver1" (unter dem VCB-Proxyrechner "VCBProxy1"), wobei Sie das HTTP-Protokoll mit gesetztem Debug-Flag verwenden:

```
ca_vcbpopulatedb.exe -Primary ARCserver1 -carootUser caroot -carootPass ca123  
-vcb VCBProxy1 -esxServer ESXServer1 -esxUser root -esxUserPass rootpasswd -  
proto http -debug
```

- Mit Hilfe des folgenden Befehls entfernen Sie alle VM-Details des ESX-Servers mit dem Hostnamen "ESXServer1" aus der Datenbank auf dem ARCserve-Server "ARCserver1" unter dem VCB-Proxyrechner "VCBProxy1" mit entferntem Debug-Flag:

```
ca_vcbpopulatedb.exe -Primary ARCserver1 -carootUser caroot -carootPass ca123  
-vcb VCBProxy1 -esxServer ESXServer1 -esxUser root -esxUserPass rootpasswd -  
delProxydb
```

- Mit Hilfe des folgenden Befehls übernehmen Sie die VM-Details des ESX-Servers mit dem Hostnamen "ESXServer1" in die Datenbank auf dem ARCserve-Server "ARCserver1", wobei nur die VM im VCB-Proxyrechner "VCBProxy1" mit gesetztem Debug-Flag geladen werden kann:

```
ca_vcbpopulatedb.exe -Primary ARCserver1 -carootUser caroot -carootPass ca123  
-vcb VCBProxy1 -esxServer ESXServer1 -esxUser root -esxUserPass rootpasswd -  
vcbMountableVM -debug
```

- Verwenden Sie den folgenden Befehl, um das automatische Einpflegen von Informationen in dieCA ARCserve Backup-Datenbank zu beenden:

- Der Server heißt "Myvirtualserver" und befindet sich in einem VirtualCenter-Serversystem:

```
ca_vcbpopulatedb.exe -stopAutoPopulate Myvirtualserver
```

- Der Server heißt "My Esxserver" und befindet sich in einem SWX-Serversystem:

```
ca_vcbpopulatedb.exe -stopAutoPopulate MyEsxserver
```

Einpflegen von Informationen in die Datenbank mit Hilfe des ARCserve Hyper-V-Konfigurationstools

Das ARCserve Hyper-V-Konfigurationstool ist ein Hilfsprogramm zum Sammeln von Daten, das Informationen zu den VMs im Hyper-V-Hostsystem in die CA ARCserve Backup-Datenbank einpflegt.

Nach der Installation des Agenten müssen Sie die CA ARCserve Backup-Datenbank mit Informationen zu Ihren VM-Systemen füllen. Hierfür müssen Sie das ARCserve Hyper-V-Konfigurationstool auf dem Hyper-V-Hostsystem ausführen.

Nachdem Sie das ARCserve Hyper-V-Konfigurationstool ausgeführt und einen Sicherungsjob für die Daten auf den virtuellen Rechnern übergeben haben, wird die CA ARCserve Backup-Datenbank automatisch mit den Informationen über die virtuellen Rechner gefüllt, die bei der Ausführung des Konfigurationstools angegeben wurden. Mit der Option zur automatischen Aufnahme können Sie sicherstellen, dass der Sicherungs-Manager richtig durchsucht wird und die aktuellen Daten auf den virtuellen Rechnern gesichert werden. CA ARCserve Backup füllt die Datenbank standardmäßig automatisch in 24-Stunden-Abständen nach Abschluss der Sicherung mit aktualisierten Daten.

Beachten Sie beim ARCserve Hyper-V-Konfigurationstool folgende Einschränkungen:

- Informationen zu virtuellen Hyper-V-Rechnern, die zum Zeitpunkt der Ausführung dieses Tools heruntergefahren waren, werden vom ARCserve Hyper-V-Konfigurationstool nicht in die CA ARCserve Backup-Datenbank aufgenommen.
- Das ARCserve Hyper-V-Konfigurationstool befüllt die CA ARCserve Backup-Datenbank mit den Hostnamen der ermittelten VMs. Falls das ARCserve Hyper-V-Konfigurationstool den Hostnamen einer VM nicht ermitteln kann, ersetzt CA ARCserve Backup den Hostnamen der VM mit dem VM-Namen der VM in der CA ARCserve Backup-Datenbank.
- CA ARCserve Backup unterstützt nur Hostnamen und VM-Namen, die maximal 15 Zeichen umfassen. Wenn die ermittelten Hostnamen oder VM-Namen länger als 15 Zeichen sind, werden sie in der CA ARCserve Backup-Datenbank auf 15 Zeichen gekürzt.
- Das ARCserve Hyper-V-Konfigurationstool unterstützt nicht die Verwendung von JIS2004-Unicode-Zeichen für Hostnamen und VM-Namen. Wenn das Tool JIS2004-Unicode-Zeichen in den Namen erkennt, erfasst CA ARCserve Backup dieses Ereignis im Feld "Ergebnis" im ARCserve Hyper-V-Konfigurationstool, und die Informationen zu den VMs werden nicht in die CA ARCserve Backup-Datenbank aufgenommen.

So pflegen Sie mit Hilfe des ARCserve Hyper-V-Konfigurationstools Informationen in die Datenbank ein:

1. Stellen Sie sicher, dass die VMs in Ihren Hyper-V-Serversystemen ausgeführt werden.

Hinweis: Falls die VMs momentan nicht ausgeführt werden, kann das ARCserve Hyper-V-Konfigurationstool den Hostnamen der VM nicht erkennen und sammelt im Hyper-V-System den VM-Namen anstelle des Hostnamen. Außerdem kann CA ARCserve Backup VM-Sicherungen im Raw-Modus (vollständige VM) erstellen, es kann jedoch keine Sicherungen und Wiederherstellungen auf Dateiebene durchführen.

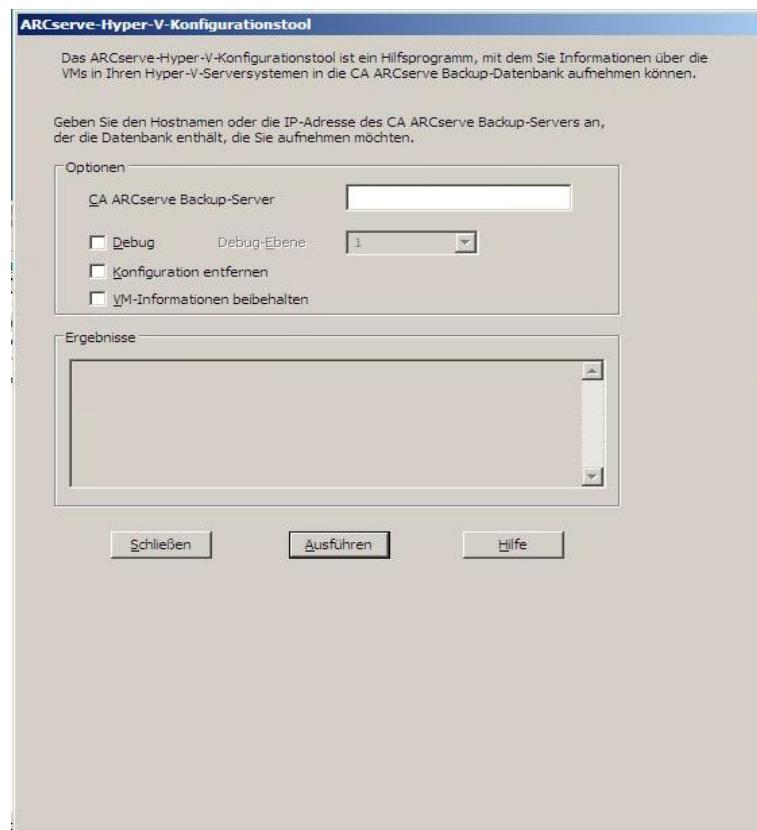
2. Melden Sie sich beim Hyper-V-Hostsystem an, und öffnen Sie die Backup Agent-Verwaltung.

Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent - Verwaltung".

Das Dialogfeld "Backup Agent - Verwaltung" wird geöffnet.

3. Wählen Sie in der Dropdown-Liste die Option "CA ARCserve Backup Agent für virtuelle Rechner", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".

Das ARCserve Hyper-V-Konfigurationstool wird geöffnet.



4. Füllen Sie die folgenden Felder aus:

CA ARCserve Backup-Server

Hier können Sie den Hostnamen oder die IP-Adresse des CA ARCserve Backup-Servers angeben, der die zu befüllende Datenbank enthält.

Debug

Mit dieser Option können Sie ein detailliertes Debug-Protokoll schreiben. Das Protokoll wird im Client Agent für Windows-Installationsverzeichnis erstellt. Dieses Verzeichnis lautet standardmäßig wie folgt:

C:\Programme\CA\ARCserve Backup Client Agent für windows\Log

Hinweis: Der Name der Protokolldatei lautet "ca_msmpopulatedb".

Debug-Ebene

Hier geben Sie die gewünschte Detailgenauigkeit für das Debug-Protokoll an ("ca_msmpopulatedb.log").

Standard: 2

Bereich: 1 bis 6.

Hinweis: Eine höhere Debug-Ebene bedeutet, dass detailliertere Informationen im Debug-Protokoll angegeben werden.

Konfiguration entfernen

Mit Hilfe dieser Option können Sie die für den festgelegten Hyper-V-Server in der CA ARCserve Backup-Datenbank verfügbaren virtuellen Rechner löschen und die neuesten VM-Daten in die CA ARCserve Backup-Datenbank aufnehmen.

VM-Informationen beibehalten

Hiermit können Sie Daten (Sicherungsinformationen) zu VMs aufbewahren, die während der Ausführung dieses Tools nicht verfügbar sind.

Standardmäßig erfasst dieses Tool Informationen von virtuellen Rechnern, die verfügbar sind, wenn Sie dieses Tool ausführen. Wenn eine VM nicht verfügbar ist (zum Beispiel weil sie heruntergefahren oder aus der Umgebung gelöscht wurde), löscht CA ARCserve Backup die mit dieser VM verbundenen Daten aus der CA ARCserve Backup-Datenbank. Wenn diese Option aktiviert wurde, erfasst CA ARCserve Backup Informationen zu virtuellen Rechnern, die verfügbar sind, und behält die Sicherungsinformationen von virtuellen Rechnern, die nicht verfügbar sind, bei.

VM automatisch aufnehmen

Hiermit können Sie festlegen, wie oft die CA ARCserve Backup-Datenbank automatisch mit Informationen zu den virtuellen Rechnern gefüllt wird.

Standardeinstellung: 24 Stunden

Bereich: 1 bis 99 Stunden

5. Klicken Sie auf "Ausführen".

Die CA ARCserve Backup-Datenbank wird mit Informationen über die VMs gefüllt, die im Hyper-V-Hostsystem ausgeführt werden.

Einpflegen von Informationen in die Datenbank mit Hilfe des Befehlszeilenhilfsprogramms "ca_msmpopulatedb"

Das Hilfsprogramm "ca_msmpopulatedb" ist ein Tool zum Sammeln von Daten, das Informationen zu den VMs im Hyper-V-Hostsystem in die CA ARCserve Backup-Datenbank einpflegt.

Nach der Installation des Agenten müssen Sie die CA ARCserve Backup-Datenbank mit Informationen zu Ihren Hyper-V-Systemen füllen. Dazu müssen Sie das Hilfsprogramm "ca_msmpopulatedb" auf dem Hyper-V-Hostsystem ausführen, auf dem der CA ARCserve Backup Client Agent für Windows installiert ist.

Standardmäßig ist "ca_msmpopulatedb" in folgendem Verzeichnis auf dem Hyper-V-Hostsystem installiert:

C:\Programme\CA\ARCserve Backup Client Agent für Windows

So pflegen Sie mit Hilfe des Befehlszeilenhilfsprogramms "ca_msmpopulatedb" Informationen in die Datenbank ein:

1. Stellen Sie sicher, dass die VMs im Hyper-V-Hostsystem ausgeführt werden.

Hinweis: Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm "ca_msmpopulatedb" keine Daten in die CA ARCserve Backup-Datenbank ein, und Sie können die VMs in den Hyper-V-Hostsystemen nicht richtig durchsuchen und sichern.

2. Melden Sie sich beim Hyper-V-Hostsystem an, öffnen Sie ein Befehlszeilenfenster und führen Sie das Hilfsprogramm "ca_msmpopulatedb" mit folgender Syntax aus:

```
ca_msmpopulatedb -primary <ARCserve-Primärservername> [-Debug] <debuglevel>]
[-retainVMinDB] [-DelVMinDB]
```

Hinweis: Weitere Informationen zur Verwendung des Befehls "ca_msmpopulatedb" finden Sie unter [Verwendung von ca_msmpopulatedb](#) (siehe Seite 53).

Die CA ARCserve Backup-Datenbank wird mit Informationen über die VMs gefüllt, die im Hyper-V-Hostsystem ausgeführt werden.

Verwendung von ca_msmpopulatedb

Der Befehl "ca_msmpopulatedb" beinhaltet Argumente und Optionen zur Definition von Aktionen, die beim Aufnehmen von Informationen zu virtuellen Rechnern (VMs) in die CA ARCserve Backup-Datenbank zu befolgen sind.

Der Befehl "ca_msmpopulatedb" umfasst folgende Argumente und Optionen:

-Primary

Hier können Sie den Hostnamen oder die IP-Adresse des CA ARCserve Backup-Servers angeben, der die zu befüllende Datenbank enthält.

-Debug

Hier geben Sie die gewünschte Detailgenauigkeit für das Debug-Protokoll an ("ca_msmpopulatedb.log").

Standard: 2

Bereich: 1 bis 6

Hinweis: Eine höhere Debug-Ebene bedeutet, dass detailliertere Informationen im Debug-Protokoll angegeben werden.

-retainVMinDB

Hiermit können Sie Daten (Sicherungsinformationen) zu VMs aufbewahren, die während der Ausführung dieses Befehls nicht verfügbar sind.

Standardmäßig erfasst dieses Hilfsprogramm Informationen von virtuellen Rechnern, die verfügbar sind, wenn Sie dieses Hilfsprogramm ausführen. Wenn eine VM nicht verfügbar ist (zum Beispiel weil sie heruntergefahren oder aus der Umgebung gelöscht wurde), löscht CA ARCserve Backup die mit dieser VM verbundenen Daten aus der CA ARCserve Backup-Datenbank. Wenn diese Option aktiviert wurde, erfasst CA ARCserve Backup Informationen zu virtuellen Rechnern, die verfügbar sind, und behält die Sicherungsinformationen von virtuellen Rechnern, die nicht verfügbar sind, bei.

-DelVMinDB

Mit Hilfe dieser Option können Sie die für den festgelegten Hyper-V-Server in der CA ARCserve Backup-Datenbank verfügbaren virtuellen Rechner löschen und die neuesten VM-Daten in die CA ARCserve Backup-Datenbank aufnehmen.

Hinzufügen oder Entfernen bestimmter VM-Daten zu/aus der CA ARCserve Backup-Datenbank

CA ARCserve Backup bietet Befehlszeilenargumente, mit denen Sie bestimmte VM-Daten zur CA ARCserve Backup-Datenbank hinzufügen oder daraus entfernen können. Sie können die Argumente verwenden, wenn Sie den Namen des bestimmten virtuellen Rechners kennen, den Sie zur CA ARCserve Backup-Datenbank hinzufügen oder daraus entfernen möchten. Dies sind die Befehlszeilenargumente:

`-insertvm <vmname>`
`-deletevm <vmname>`

Hinweis: Sie können "-insertVM" und "-deleteVM" mit dem VMware-Befehlszeilenhilfsprogramm (ca_vcpopulateDB) und dem Hyper-V-Befehlszeilenhilfsprogramm (ca_msmpopulateDB) verwenden.

So fügen Sie VM-Daten zur CA ARCserve Backup-Datenbank hinzu oder entfernen Sie daraus:

1. Rufen Sie die Windows-Eingabeaufforderung auf.
Ändern Sie das Verzeichnis auf das Verzeichnis, unter dem der Client Agent für Windows installiert ist.
2. Führen Sie unter Verwendung der folgenden Syntax "ca_vcpopulateDB" (VMware-VMs) oder "ca_msmpopulateDB" (Hyper-V-VMs) aus:

-insertvm <vmname>

Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine VMware-VM mit Hostnamen VM-001 in die CA ARCserve Backup-Datenbank einzufügen:

```
ca_vcpopulatedb.exe -Primary ARCServe1 -carootUser caroot -carootPass ca  
-esxServer ESXServer1 -esxUser root -esxUserPass rootpass -insertVM VM-  
001 -debug
```

Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine Hyper-V-VM mit Hostnamen VM-001 in die CA ARCserve Backup-Datenbank einzufügen:

```
ca_msmpopulatedb.exe -Primary ARCServe1 -insertVM VM-001 -debug 1
```

-deletevm <vmname>

Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine VMware-VM mit Hostnamen VM-001 aus der CA ARCserve Backup-Datenbank zu löschen:

```
ca_vcbsubjectdb.exe -Primary ARCServe1 -carootUser caroot -carootPass ca  
-esxServer ESXServer1 -esxUser root -esxUserPass rootpass -deleteVM VM-  
001 -debug
```

Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine Hyper-V-VM mit Hostnamen VM-001 aus der CA ARCserve Backup-Datenbank zu löschen:

```
ca_msmpopulatedb.exe -Primary ARCServe1 -deleteVM VM-001 -debug 1
```

Weitere Informationen:

[ca_vcbsubjectdb – Verwendung](#) (siehe Seite 44)

[Verwendung von ca_msmpopulatedb](#) (siehe Seite 53)

So deinstallieren Sie den Agenten:

Verwenden Sie die Option "Software" in der Windows-Systemsteuerung, um den CA ARCserve Backup Agenten für virtuelle Rechner zu deinstallieren.

So verwenden Sie den Transportmodus "hotadd" von VMware:

Der Transportmodus "hotadd" von VMware ist eine Option in VMware Consolidated Backup r1.5, die verwendet werden kann, wenn VCB auf einer VM installiert ist.

Hinweis: Weitere Informationen zur Verwendung des Transportmodus "hotadd" finden Sie im Handbuch *Virtual Machine Backup Guide* unter www.vmware.com.

Beachten Sie folgende Punkte, wenn Sie den Transportmodus "hotadd" von VMware in Ihrer Umgebung verwenden.

- Auf dem Sicherungs-Proxy-System muss ESX Server 3.5, ESX Server 3i ab Version 3.5 oder VirtualCenter Server ab Version 2.5 installiert sein.
- Das Sicherungs-Proxysystem muss auf einer VM konfiguriert sein.
- Die VCB-Helper-VM muss ohne die Verwendung virtueller Festplatten erstellt werden.
- Falls Sie nur auf lokale Speichergeräte sichern, muss auf allen ESX-Serversystemen eine VCB-Proxy-VM konfiguriert sein.
- Sie müssen DWORD UseHotadd in dem Registrierungsschlüssel erstellen, der auf das Sicherungs-Proxysystem folgt.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe Backup\ClientAgent\Parameters

DWORD: UseHotadd

Wert: 1

Beenden von Vorgängen bei abgelaufenen SSL-Zertifikaten

Sicherungs-Proxy-Systeme können so konfiguriert werden, dass bei der Kommunikation mit ESX-Serversystemen gültige SSL-Zertifikate bezogen werden. Standardmäßig setzt der Agent VM-basierte Vorgänge (wie etwa die automatische Aufnahme, Sicherungen und Wiederherstellungen) auch bei ungültigen oder abgelaufenen SSL-Zertifikaten fort. Hiermit soll ein kontinuierlicher Schutz der virtuellen Rechner in Ihrer Umgebung gewährleistet werden.

Falls diese Vorgehensweise nicht den Erfordernissen Ihrer Organisation entspricht, können Sie selbst festlegen, was geschehen soll, wenn der Agent auf dem ESX-System auf ungültige oder abgelaufene SSL-Zertifikate trifft.

So beenden Sie Vorgänge bei abgelaufenen SSL-Zertifikaten:

1. Öffnen Sie den Registrierungs-Editor, und rufen Sie den folgenden Registrierungsschlüssel auf:
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA Arcserve Backup\ClientAgent\Parameters
2. Erstellen Sie den Registrierungsschlüsselwert "SSLCertificateVerify" mit dem Typ DWORD.
Legen Sie als Wert für den Schlüssel "SSLCertificateVerify" "1" fest.
3. Schließen Sie den Registrierungs-Editor.

Best Practices für die Installation und Konfiguration des Agenten für virtuelle Rechner

Folgende Best Practices sind für die Installation des CA ARCserve Backup Agenten für virtuelle Rechner zu empfehlen:

Task	VMware-Systeme	Hyper-V-Systeme
Erforderliche Komponenten	<p>CA ARCserve Backup</p> <ul style="list-style-type: none"> ■ Installieren Sie die CA ARCserve Backup-Serverkomponenten auf dem System, das als Primärserver oder Standalone-Server dienen soll. <p>Agent für virtuelle Rechner</p> <ul style="list-style-type: none"> ■ Installieren Sie den Agenten auf dem System, das als Sicherungs-Proxysystem dienen soll. Die Best Practice ist, den Sicherungsserver als Sicherungs-Proxysystem zu verwenden. Sollte diese Konfiguration jedoch Ihrer Einschätzung nach Leistungseinbußen für den Server bedeuten, installieren Sie den Agenten auf einem Remote-System, und nutzen Sie ihn als Sicherungs-Proxy-System. <p>VMware VCB-Framework</p> <ul style="list-style-type: none"> ■ Stellen Sie sicher, dass das VMware VCB-Framework auf dem Sicherungs-Proxysystem installiert ist. 	<p>CA ARCserve Backup</p> <ul style="list-style-type: none"> ■ Installieren Sie die CA ARCserve Backup-Serverkomponenten auf dem System, das als Primärserver oder Standalone-Server dienen soll. <p>Agent für virtuelle Rechner</p> <ul style="list-style-type: none"> ■ Installieren Sie den Agenten auf dem Hyper-V-Hostsystem.

Für das Konfigurieren des CA ARCserve Backup Agenten für virtuelle Rechner und zum Sichern von Daten empfehlen sich folgende Best Practices:

Task	VMware-Systeme	Hyper-V-Systeme
Konfiguration	<ul style="list-style-type: none"> ■ Füllen Sie mit dem ARCserve VMware-Konfigurationstool auf dem Sicherungs-Proxysystem die CA ARCserve Backup-Datenbank mit Daten. Weitere Informationen finden Sie unter Einpfliegen von Informationen in die Datenbank mit Hilfe des ARCserve VMware-Konfigurationstools (siehe Seite 36). ■ Stellen Sie den Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung bereit. Weitere Informationen finden Sie unter Bereitstellen des Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung (siehe Seite 30). 	<ul style="list-style-type: none"> ■ Befüllen Sie mit dem ARCserve Hyper-V-Konfigurationstool auf dem Hyper-V-Host die CA ARCserve Backup-Datenbank mit Daten. Weitere Informationen finden Sie unter Einpfliegen von Informationen in die Datenbank mit Hilfe des ARCserve Hyper-V-Konfigurationstools (siehe Seite 49). ■ Stellen Sie den Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung bereit. Weitere Informationen finden Sie unter Bereitstellen des Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung (siehe Seite 30).
Sicherungsmodus	<p>Akzeptieren Sie den Standard-Sicherungsmodus, der folgende festgelegte Optionen umfasst:</p> <ul style="list-style-type: none"> ■ Sicherung im gemischten Modus ■ Wiederherstellung auf Dateiebene aktivieren 	
Sicherungsoptionen – Multistreaming	<p>Für eine effiziente Durchführung von Sicherungsjobs sollten Sie die Multistreaming-Option verwenden und maximal vier VMs für einen Sicherungsjob angeben. Informationen über Multistreaming finden Sie im <i>Administrationshandbuch</i>.</p>	
Sichern von Daten	<p>Folgen Sie den unter Sichern von Daten (siehe Seite 71) beschriebenen Schritten.</p>	

Kapitel 3: Sichern und Wiederherstellen von Daten

Dieses Kapitel enthält folgende Themen:

- [Durchsuchen von Sicherungs-Volumes](#) (siehe Seite 59)
- [Funktionsweise des globalen und lokalen Sicherungsmodus](#) (siehe Seite 61)
- [Sichern von Daten](#) (siehe Seite 71)
- [Durchsuchen von Wiederherstellungssitzungen](#) (siehe Seite 76)
- [Wiederherstellen von Daten](#) (siehe Seite 78)
- [Einschränkungen beim Sichern und Wiederherstellen auf virtuellen Rechnern](#) (siehe Seite 91)
- [Verwenden von Protokolldateien virtueller Rechner](#) (siehe Seite 92)
- [Auswirkungen von VM-Namen auf Jobs](#) (siehe Seite 94)

Durchsuchen von Sicherungs-Volumes

Im Sicherungs-Manager können Sie innerhalb einer Verzeichnisstruktur Informationen zu folgenden VM-Objekten durchsuchen und anzeigen:

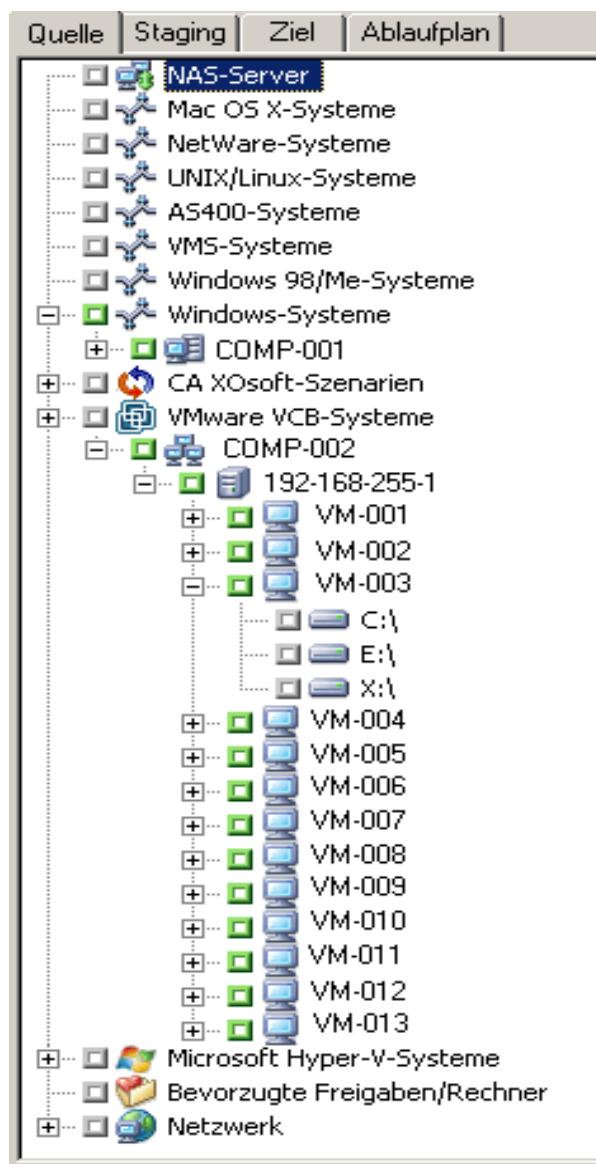
- Sicherungs-Proxysysteme
- VMware ESX Server-Systeme
- VMware VirtualCenter Server-Systeme
- Microsoft Hyper-V-Systeme

Damit Sie VMware-VMs und Hyper-V-VMs durchsuchen können, müssen Sie das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool ausführen. Diese Tools füllen die CA ARCserve Backup-Datenbank mit Informationen zu den in den VMs enthaltenen Daten, sodass Sie die VMs im Sicherungs-Manager durchsuchen können.

Beachten Sie folgende Einschränkungen:

- Sie können die Volumes der VMware-VMs durchsuchen, wenn die VM ein VMware-unterstütztes, Windows-basiertes Betriebssystem ausführt.
- Sie können die Volumes in den Hyper-V-VMs durchsuchen, wenn Sie den Agent für virtuelle Rechner auf den Hyper-V-VMs installieren. Bei dieser Konfiguration ist es nicht erforderlich, das ARCserve Hyper-V-Konfigurationstool auszuführen, um die Volumes der Hyper-V-VMs zu durchsuchen.

Wenn im Sicherungs-Manager die Registerkarte "Quelle" ausgewählt ist, kann das Objekt "VMware VCB-Systeme" eingeblendet werden, sodass die Namen der VMware VCB-Systeme, der Sicherungs-Proxysysteme, der ESX-Server-Systeme oder der VirtualCenter-Serversysteme sowie die im Windows-Betriebssystem enthaltenen VM-Volumes angezeigt werden.



- Wenn Sie einen Sicherungsjob übergeben, werden Sie von CA ARCserve Backup dazu aufgefordert, die Benutzernamen- und Kennwortinformationen für das ESX-Server- oder VirtualCenter-Server-System anzugeben.
CA ARCserve Backup überprüft die Anmeldeinformationen während der Laufzeit.

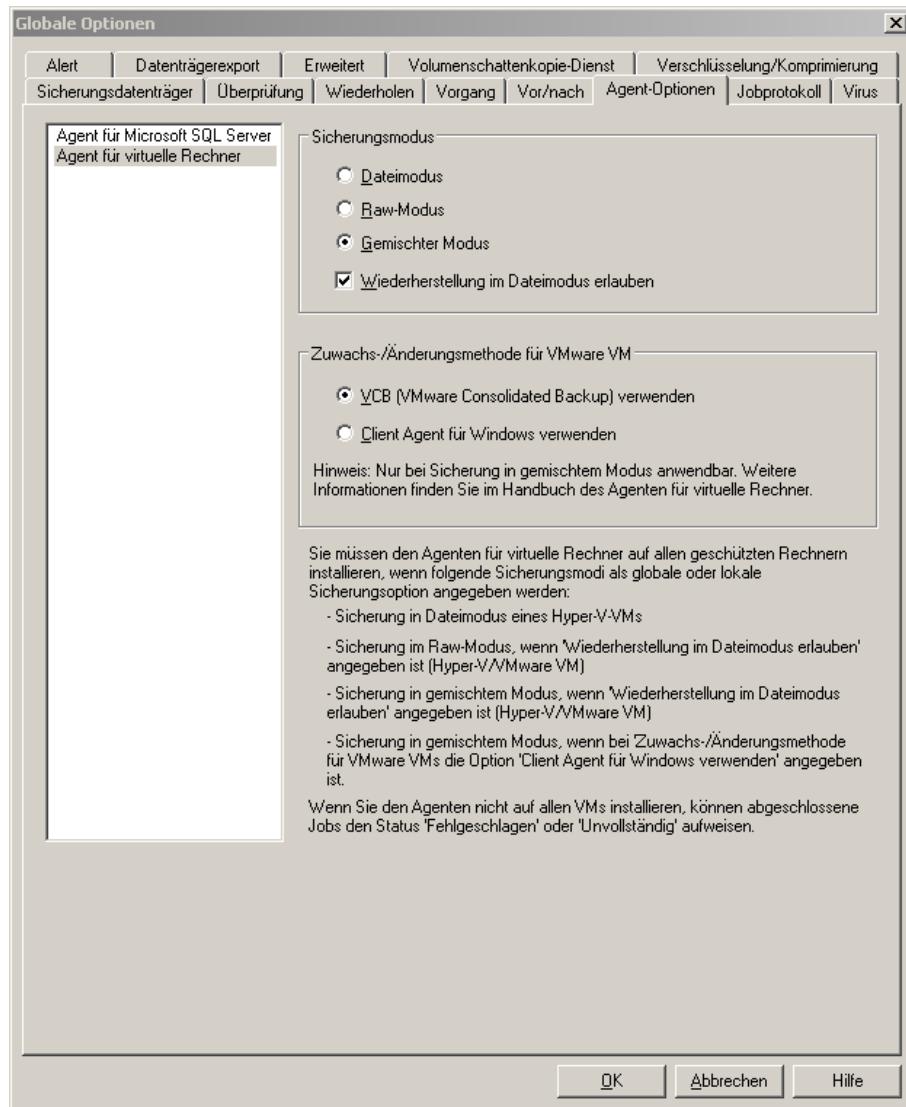
- Auf VM-Ebene können Sie im Raw-Modus (vollständige VM) oder im Dateimodus durchsuchen.
Um eine VM auf Dateiebene zu durchsuchen, muss ein VMware-unterstütztes Windows-Betriebssystem auf der VM installiert sein.
- Durchsuchungsmodi:
 - Windows VMs: Dateimodus und Raw-Modus (vollständige VM).
 - VMs, die von anderen Systemen als Windows unterstützt werden: Nur Raw-Modus (vollständige VM).

Funktionsweise des globalen und lokalen Sicherungsmodus

Die Sicherungsmodi bestimmen, wie CA ARCserve Backup auf VMs gespeicherte Daten sichert. In CA ARCserve Backup können Sie Sicherungsdaten mit folgenden Sicherungsmodi verarbeiten:

- **Dateimodus:** Damit können Sie auf VMs gespeicherte einzelne Dateien oder Verzeichnisse sichern. Bei Sicherungen im Dateimodus können Sie VM-Sicherungsdaten mit Dateiebenengranularität wiederherstellen.
- **Raw-Modus (vollständige VM):** Hiermit können Sie ein vollständiges Image der auf einer VM befindlichen Daten sichern. Im Raw-Modus (vollständige VM) können Sie Daten sichern, die für Disaster Recovery-Vorgänge verwendet werden können.
- **Gemischter Modus:** Ermöglicht das Durchführen vollständiger Datensicherungen im Raw-Modus (vollständige VM) sowie von Zuwachs- und Änderungssicherungen im Dateimodus. Mit Sicherungen im gemischten Modus können Sie geplante Sicherungen und GFS-Rotationssicherungen durchführen. Außerdem bieten Sicherungen im gemischten Modus den Vorteil, dass sie wöchentliche, vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen mit Dateiebenengranularität durchführen können.
Hinweis: Die Standardeinstellung bilden Sicherungen im gemischten Modus.
- **Wiederherstellung im Dateimodus erlauben:** Mit dieser Option können Sie Raw-(vollständige VM-)Sicherungen und Sicherungen im gemischten Modus auf Dateiebenengranularität wiederherstellen.
Hinweis: Um Wiederherstellungen auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben. Weitere Informationen finden Sie unter [Angeben des CA ARCserve Backup-Servernamens](#) (siehe Seite 34).

Im folgenden Dialogfeld werden die VM-Sicherungsmodi dargestellt, die Sie im Dialogfeld "Globale Optionen" festlegen können.



Sie können Sicherungsmodi entweder als globale Sicherungsoption oder als lokale Sicherungsoption festlegen.

- **Globale Sicherungsoption:** Damit werden Sicherungsmodi global auf alle Sicherungsjobs angewendet, die sich auf VMs in VMware- und Hyper-V-Systemen in Ihrer Umgebung beziehen. Weitere Informationen finden Sie im Abschnitt zum [Festlegen von Sicherungsmodi als globale Sicherungsoption](#) (siehe Seite 65).

- **Lokale Sicherungsoption:** Damit können Sie auf Jobebene einen Sicherungsmodus auf einzelne VMware- und Hyper-V-VMs anwenden. Weitere Informationen finden Sie unter [Festlegen von Sicherungsmodi als lokale Sicherungsoption](#) (siehe Seite 68).

Hinweis: Wenn Sie Sicherungsmodi auf globaler und lokaler Ebene festlegen, führt CA ARCserve Backup den Sicherungsjob immer mit den lokalen Sicherungsoptionen aus, die für die betreffende VM festgelegt wurden.

In der folgenden Tabelle wird das Verhalten der Sicherungsmodi beschrieben:

Ausgewählter Sicherungsmodus	Ausgewählte globale Änderungs-/Zuwachsmethode	Ergebnis unter VMware-Systemen	Ergebnis unter Hyper-V-Systemen
Gemischt (als globale oder lokale Option ausgewählt)	<ul style="list-style-type: none"> ■ VCB verwenden 	CA ARCserve Backup verarbeitet die im Raw-Modus (vollständige VM) und die im Dateimodus erstellten Sicherungsdaten unter Verwendung von VCB.	CA ARCserve Backup verarbeitet die wöchentlichen vollständigen Sicherungen im Raw-Modus unter Verwendung des VSS-Hyper-V Writers und die aufeinander folgenden täglichen Zuwachs- und Änderungssicherungen im Dateimodus unter Verwendung des Agenten für virtuelle Rechner, der auf der VM ausgeführt wird.

Hinweis: Die globale Option zur Verwendung von VCB wirkt sich nicht auf Sicherungen auf Hyper-V-Systemen aus.

Ausgewählter Sicherungsmodus	Ausgewählte globale Änderungs-/Zuwachsmethode	Ergebnis unter VMware-Systemen	Ergebnis unter Hyper-V-Systemen
Gemischt (als globale oder lokale Option ausgewählt)	<ul style="list-style-type: none"> ■ Client Agent verwenden <p>Hinweis: Der Agent für virtuelle Rechner muss auf der VM installiert sein und ausgeführt werden.</p>	<p>CA ARCserve Backup verarbeitet die wöchentlichen vollständigen Sicherungen im Raw-Modus unter Verwendung von VCB und die aufeinander folgenden täglichen Zuwachs- und Änderungssicherungen im Dateimodus unter Verwendung des Client Agent für Windows, der auf der VM ausgeführt wird.</p>	<p>CA ARCserve Backup verarbeitet die wöchentlichen vollständigen Sicherungen im Raw-Modus (vollständige VM) unter Verwendung des VSS-Hyper-V Writers und die aufeinander folgenden täglichen Zuwachs- und Änderungssicherungen im Dateimodus unter Verwendung des Agenten für virtuelle Rechner, der auf den VMs ausgeführt wird.</p> <p>Hinweis: Die globale Option zur Verwendung von VCB wirkt sich nicht auf Sicherungen auf Hyper-V-Systemen aus.</p>

Beispiele: So wenden Sie Sicherungsoptionen an

Um Daten im Raw-Modus (vollständige VM) sichern zu können und mit Dateiebenengranularität wiederherstellen zu können, empfiehlt es sich als Best Practice, die Standardoptionen für den Sicherungsmodus zu übernehmen und global auf alle Ihre Sicherungen anzuwenden. Um eine einzelne VM zu schützen, etwa eine VM, auf der ein unterstütztes Nicht-Windows-Betriebssystem ausgeführt wird, können Sie die Sicherungsoptionen entweder für die einzelne VM festlegen; oder Sie können sie als lokale Sicherungsoption festlegen und dann die global für alle Sicherungen ausgewählten Optionen beibehalten.

Ihre Sicherungsumgebung besteht aus zahlreichen Servern, auf denen VMs installiert sind. Die meisten Ihrer Sicherungen sind Rotationssicherung für VMs. Die übrigen Server erfordern vollständige Sicherungen im dateibasierten Modus. Um den Konfigurationsprozess zu vereinfachen, können Sie die Sicherung im gemischten Modus global auf alle Sicherungen anwenden und dann den Sicherungsmodus auf Dateiebene lokal auf alle Server anwenden, auf denen Sie Sicherungen auf Dateiebene ausführen möchten.

Festlegen von Sicherungsmodi als globale Sicherungsoption

Globale Optionen betreffen alle VM-Sicherungen auf Jobebene in Ihrer Umgebung. Legen Sie mit den folgenden Schritten Sicherungsmodi fest, die für alle VM-Sicherungsjobs gelten.

So legen Sie Sicherungsmodi als globale Sicherungsoption fest:

1. Öffnen Sie den Sicherungs-Manager, und klicken Sie auf die Registerkarte "Quelle".
Die Quellverzeichnisstruktur wird angezeigt.
2. Erweitern Sie das Objekt "VMware VCB-Systeme" oder das Objekt "Microsoft Hyper-V-Systeme", und navigieren Sie zu der zu sichernden VM.
Klicken Sie in der Symbolleiste auf "Optionen".
Das Dialogfeld "Optionen" wird geöffnet.
3. Klicken Sie auf die Registerkarte "Agent-Optionen" und dann auf "Agent für virtuelle Rechner".
4. Geben Sie einen Sicherungsmodus an, indem Sie auf eine der folgenden Optionen klicken:

Dateimodus

Verwenden Sie den "Dateimodus", wenn Sie einzelne Dateien und Verzeichnisse sichern möchten. Mit Sicherungen im Dateimodus können Sie folgende Aufgaben ausführen:

- In einer VM enthaltene Dateien und Verzeichnisse auf Dateiebenengranularität sichern
- Vollständige Sicherungen, Zuwachs- und Änderungssicherungen durchführen
- Daten auf Dateiebenengranularität wiederherstellen
- Mehrere Daten-Streams mit Hilfe der Multistreaming-Option gleichzeitig bearbeiten
- Daten mit Hilfe der Filteroption filtern

Hinweis: Die erforderliche Laufzeit für die Sicherung einer vollständigen VM auf Dateiebene ist länger als die erforderliche Laufzeit für die Sicherung desselben Volumes auf Raw-Ebene (vollständige VM).

Raw-Modus

Verwenden Sie den Raw-Modus, wenn Sie gesamte Systeme zum Zweck der Disaster Recovery sichern müssen. Mit Sicherungen im Raw-Modus können Sie folgende Aufgaben ausführen:

- Ausschließlich Durchführen vollständiger Sicherungen von vollständigen VM-Images

- Mehrere Daten-Streams mit Hilfe der Multistreaming-Option gleichzeitig bearbeiten

Hinweis: Im Raw-Modus können Daten nicht auf Dateiebenengranularität wiederhergestellt oder Raw-Daten (vollständige VM) gefiltert werden. Bei Sicherungen im Raw-Modus (vollständige VM) angewendete Filter werden während der Laufzeit ignoriert.

Gemischter Modus

Die Standardsicherungsmethode ist der gemischte Modus. Im gemischten Modus können Sie folgende Aufgaben ausführen:

- GFS- und Rotationssicherungsjobs durchführen, die wöchentliche vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen im Dateimodus in einem einzigen Sicherungsjob umfassen

Hinweis: Rotations- und GFS-Rotationsjobs haben den Vorteil, dass Sie Sicherungsdaten enthalten, die Ihnen den täglichen Schutz (Sicherungen auf Dateiebene) und den Disaster Recovery-Schutz (vollständige VM-Sicherungen im Raw-Modus) in einem einzigen Sicherungsjob bieten.

Wiederherstellung auf Dateiebene aktivieren

Verwenden Sie die Option "Wiederherstellung auf Dateiebene aktivieren", wenn Sie Daten mit der Effizienz des Raw-Modus sichern möchten und Daten mit Dateiebenengranularität wiederherstellen möchten.

Um Wiederherstellungen auf Dateiebenengranularität von Raw- (vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben. Weitere Informationen finden Sie unter [Angeben des CA ARCserve Backup-Servernamens](#) (siehe Seite 34).

Mit der Option zum Aktivieren der Wiederherstellung auf Dateiebene können Sie folgende Aufgaben ausführen:

- Wiederherstellen von im Raw-Modus erstellten Sicherungen mit Dateiebenengranularität

- Wiederherstellen von im gemischten Modus erstellten Sicherungen mit Dateiebenengranularität

Hinweis: Die Option "Wiederherstellung auf Dateiebene aktivieren" kann für alle Sicherungstypen verwendet werden, einschließlich benutzerdefinierte Sicherungen, Rotationssicherungen und GFS-Rotationen, die aus vollständigen Sicherungen, Zuwachssicherungen und Änderungssicherungen bestehen. Die vollständigen Sicherungen werden im Raw-Modus erstellt (vollständige VM), und die Zuwachs- und Änderungssicherungen werden im Sicherungsmodus auf Dateiebene erstellt. Wenn Sie die Aktivierung der Wiederherstellung auf Dateiebene nicht festlegen, stellt CA ARCserve Backup nur die Zuwachs- und Änderungssicherungen wieder her. Die im Raw-Modus erstellte vollständige Sicherung wird bei der Wiederherstellung nicht mit einbezogen.

Zuwachs-/Änderungsmethode für VMware VM

Hiermit können Sie die Kommunikationsmethode angeben, die CA ARCserve Backup zur Übertragung von Daten der Zuwachs- und Änderungssicherung zwischen VMware-VMs und dem Sicherungs-Proxy-System verwendet.

- **VCB verwenden**--Diese Option legt fest, dass CA ARCserve Backup VMware Virtual Consolidated Backup verwendet, um Daten der Zuwachs- bzw. Änderungssicherung an das Sicherungs-Proxy-System zu übermitteln. Sie sollten diese Option aktivieren, um die Belastung Ihres Netzwerks zu reduzieren.

Hinweis: Die Option "VCB verwenden" ist standardmäßig aktiviert.

- **Client Agent für Windows verwenden:** Sorgt dafür, dass CA ARCserve Backup zur Ausführung der Sicherung Client Agent für Windows verwendet. Mit dieser Option führt CA ARCserve Backup eine Dateisystemsicherung durch, bei der das Sicherungs-Proxy-System nicht für den Abschluss der Sicherung erforderlich ist.

Klicken Sie auf "OK".

Der Sicherungsmodus wird auf alle Ihre VM-Sicherungen angewendet.

5. Klicken Sie auf "OK", um das Dialogfeld "Optionen" zu schließen.

Festlegen von Sicherungsmodi als lokale Sicherungsoption

Lokale Optionen wirken sich auf einzelne VM-Sicherungen auf der Jobebene aus. Legen Sie mit den folgenden Schritten Sicherungsmodi fest, die für einzelne Sicherungsjobs gelten.

So legen Sie Sicherungsmodi als lokale Sicherungsoption fest:

1. Öffnen Sie den Sicherungs-Manager, und klicken Sie auf die Registerkarte "Quelle".
Die Quellverzeichnisstruktur wird angezeigt.
2. Erweitern Sie das Objekt "VMware VCB-Systeme" oder das Objekt "Microsoft Hyper-V-Systeme", und navigieren Sie zu der zu sichernden VM.
Klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie im Kontextmenü "Lokale Optionen" aus.
Das Dialogfeld "Sicherungsmodus" wird geöffnet.
3. Klicken Sie auf "Globale Optionen außer Kraft setzen". Weitere Informationen finden Sie unter [Sicherungsmodi](#) (siehe Seite 61).
Geben Sie einen Sicherungsmodus an, indem Sie auf eine der folgenden Optionen klicken:

Dateimodus

Verwenden Sie den "Dateimodus", wenn Sie einzelne Dateien und Verzeichnisse sichern möchten. Mit Sicherungen im Dateimodus können Sie folgende Aufgaben ausführen:

- In einer VM enthaltene Dateien und Verzeichnisse auf Dateiebenengranularität sichern
- Vollständige Sicherungen, Zuwachs- und Änderungssicherungen durchführen
- Daten auf Dateiebenengranularität wiederherstellen
- Mehrere Daten-Streams mit Hilfe der Multistreaming-Option gleichzeitig bearbeiten
- Daten mit Hilfe der Filteroption filtern

Hinweis: Die erforderliche Laufzeit für die Sicherung einer vollständigen VM auf Dateiebene ist länger als die erforderliche Laufzeit für die Sicherung desselben Volumes auf Raw-Ebene (vollständige VM).

Raw-Modus

Verwenden Sie den Raw-Modus, wenn Sie gesamte Systeme zum Zweck der Disaster Recovery sichern müssen. Mit Sicherungen im Raw-Modus können Sie folgende Aufgaben ausführen:

- Ausschließlich Durchführen vollständiger Sicherungen von vollständigen VM-Images
- Mehrere Daten-Streams mit Hilfe der Multistreaming-Option gleichzeitig bearbeiten

Hinweis: Im Raw-Modus können Daten nicht auf Dateiebenengranularität wiederhergestellt oder Raw-Daten (vollständige VM) gefiltert werden. Bei Sicherungen im Raw-Modus (vollständige VM) angewendete Filter werden während der Laufzeit ignoriert.

Gemischter Modus

Die Standardsicherungsmethode ist der gemischte Modus. Im gemischten Modus können Sie folgende Aufgaben ausführen:

- GFS- und Rotationssicherungsjobs durchführen, die wöchentliche vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen im Dateimodus in einem einzigen Sicherungsjob umfassen

Hinweis: Rotations- und GFS-Rotationsjobs haben den Vorteil, dass Sie Sicherungsdaten enthalten, die Ihnen den täglichen Schutz (Sicherungen auf Dateiebene) und den Disaster Recovery-Schutz (vollständige VM-Sicherungen im Raw-Modus) in einem einzigen Sicherungsjob bieten.

Wiederherstellung auf Dateiebene aktivieren

Verwenden Sie die Option "Wiederherstellung auf Dateiebene aktivieren", wenn Sie Daten mit der Effizienz des Raw-Modus sichern möchten und Daten mit Dateiebenengranularität wiederherstellen möchten.

Um Wiederherstellungen auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben. Weitere Informationen finden Sie unter [Angeben des CA ARCserve Backup-Servernamens](#) (siehe Seite 34).

Mit der Option zum Aktivieren der Wiederherstellung auf Dateiebene können Sie folgende Aufgaben ausführen:

- Wiederherstellen von im Raw-Modus erstellten Sicherungen mit Dateiebenengranularität
- Wiederherstellen von im gemischten Modus erstellten Sicherungen mit Dateiebenengranularität

Hinweis: Die Option "Wiederherstellung auf Dateiebene aktivieren" kann für alle Sicherungstypen verwendet werden, einschließlich benutzerdefinierte Sicherungen, Rotationssicherungen und GFS-Rotationen, die aus vollständigen Sicherungen, Zuwachssicherungen und Änderungssicherungen bestehen. Die vollständigen Sicherungen werden im Raw-Modus erstellt (vollständige VM), und die Zuwachs- und Änderungssicherungen werden im Sicherungsmodus auf Dateiebene erstellt. Wenn Sie die Aktivierung der Wiederherstellung auf Dateiebene nicht festlegen, stellt CA ARCserve Backup nur die Zuwachs- und Änderungssicherungen wieder her. Die im Raw-Modus erstellte vollständige Sicherung wird bei der Wiederherstellung nicht mit einbezogen.

Klicken Sie auf "OK".

Das Dialogfeld "Sicherungsmodus" wird geschlossen, und der Sicherungsmodus wird angewendet.

Verarbeitung von Zuwachs- und Änderungssicherungen virtueller VMware-Rechner durch den Agenten

Der Agent verwendet folgende Dateieigenschaften als Datei-Auswahlkriterien für Zuwachs- und Änderungssicherungen:

- **Erstellungs- oder Änderungsdatum der Datei:** Sicherungen der VCB-Kommunikation

Der Agent kommuniziert über VCB mit dem virtuellen Rechner. Der Agent ermittelt und filtert Daten basierend auf dem Erstellungs- oder Änderungszeitpunkt der Dateien. Mit Hilfe dieser Kommunikationsmethode sichert der Agent unabhängig von Datei-Attributen alle Dateien mit Erstellungs- oder Änderungszeitpunkten, die sich zeitlich vor der letzten vollständigen Sicherung oder -Zuwachssicherung befinden.

- **Archivbit:** Client Agent für Windows-Kommunikationssicherungen

Der Agent kommuniziert über den Client Agent für Windows mit dem virtuellen Rechner. Der Agent ermittelt und filtert Dateien basierend auf dem Archivbit. Wenn der Agent Systemstatusdateien und Dateien mit dem Status "FilesNotToBackup" ermittelt, schließt er diese von der Zuwachs- oder Änderungssicherung aus.

Hinweis: Weitere Informationen zur Sicherungsoption "VCB verwenden" und den Kommunikationssicherungen "Client Agent für Windows verwenden" finden Sie unter [Festlegen von Sicherungsmodi als globale Sicherungsoption](#) (siehe Seite 65).

Sichern von Daten

Gehen Sie wie im Folgenden beschrieben vor, um Sicherungsjobs auf lokalen, plattenbasierten virtuellen Rechnern (VMs) und SAN-basierten VMs zu übergeben. Dieses Thema gilt für VMware VCB- und Microsoft Hyper-V-Systeme.

Hinweis: Weitere Informationen zu den Einschränkungen bei Sicherungen mit VCB finden Sie unter ["Einschränkungen beim Sichern und Wiederherstellen mit VCB"](#) (siehe Seite 91).

So sichern Sie Daten:

1. Wählen Sie im "Sicherungs-Manager" die Registerkarte "Quelle" aus.
Die Quellverzeichnisstruktur des Sicherungs-Managers wird angezeigt.
2. Erweitern Sie das Objekt "VMware VCB- Systeme" bzw. das Objekt "Microsoft Hyper-V-Systeme".
Die Sicherungs-Proxysysteme, ESX-Server- und VirtualCenter-Server-Systeme, virtuellen Rechner und Hyper-V-Systeme in Ihrer Umgebung werden angezeigt.

3. Aktivieren Sie das Kontrollkästchen neben den Objekten, die gesichert werden sollen. Sie können Volumes, einen kompletten Knoten oder eine Kombination davon als Quelle auswählen.

4. Legen Sie einen Sicherungsmodus für den Job fest.

Hinweis: Weitere Informationen zu Sicherungsmodi finden Sie unter "[Sicherungsmodi](#) (siehe Seite 61)".

5. Um VM-Sicherungsdaten zu filtern, klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie im Kontextmenü "Filter" aus.

Hinweis: Weitere Informationen zu Filtern finden Sie unter "[Filtern von VM-Sicherungsdaten](#) (siehe Seite 75)".

Wichtig! Wenn der "Sicherungsmodus" auf "Raw-Modus" festgelegt ist und Sie Filter angeben, filtert CA ARCserve Backup keine VM-Sicherungsdaten.

6. Um anzugeben, wo Sie den Sicherungsjob speichern möchten, klicken Sie auf die Registerkarte "Ziel" oder die Registerkarte "Staging".

Hinweis: Weitere Informationen zur Zielfestlegung oder zum Staging bei der Datensicherung finden Sie im "*Administrationshandbuch*" oder in der Online-Hilfe.

Zur Verwendung von Multistreaming bei der Übermittlung von Sicherungsdaten aktivieren Sie das Kontrollkästchen "Multi-Stream".

7. Um die Planungsoptionen für den Job anzugeben, klicken Sie auf die Registerkarte "Ablaufplan".

Hinweis: Weitere Informationen zu den Planungsoptionen für Jobs finden Sie im "*Administrationshandbuch*" oder in der Online-Hilfe.

8. Um globale Filter anzugeben, klicken Sie in der Symbolleiste auf "Filter".

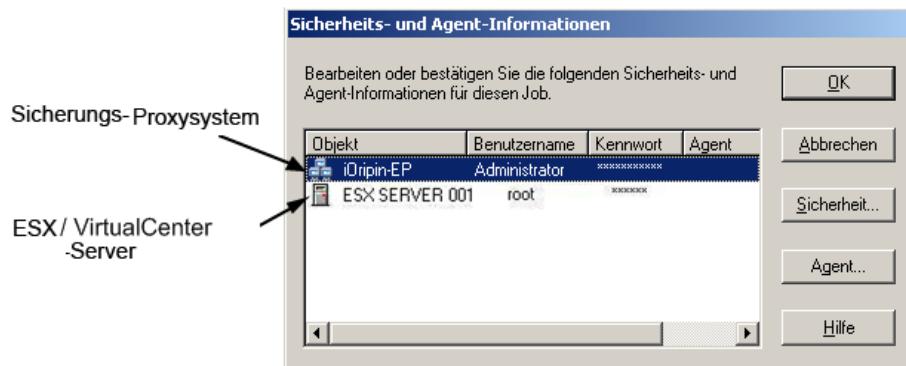
Das Dialogfeld "Filter" wird geöffnet.

Hinweis: Weitere Informationen zum Filtern von VM-Daten finden Sie unter "[Filtern von VM-Sicherungsdaten](#) (siehe Seite 75)". Wenn Sie weitere Informationen zum Angeben von Filtern benötigen, klicken Sie im Dialogfeld "Filter" auf die Schaltfläche "Hilfe".

9. Klicken Sie in der Symbolleiste auf "Starten", um den Job zu übergeben.

Das Dialogfeld "Sicherheits- und Agent-Informationen" wird geöffnet.

Zum Übergeben des Jobs müssen Sie die Anmeldeinformationen für den ESX- oder VirtualCenter-Server und das Sicherungs-Proxysystem angeben, wie in der folgenden Abbildung dargestellt:



10. Wählen Sie den zu sichernden Server aus, und klicken Sie im Dialogfeld "Sicherheits- und Agent-Informationen" auf die Schaltfläche "Sicherheit".

Das Dialogfeld "Sicherheit" wird geöffnet.

11. Geben Sie Ihre Anmeldeinformationen in den Feldern "Benutzername" und "Kennwort" ein, und klicken Sie auf "OK".

Hinweis: CA ARCserve Backup unterstützt keine Systemanmeldungen mit Kennwörtern, die mehr als 23 Zeichen umfassen. Wenn das Kennwort für das System, bei dem Sie sich anmelden möchten, mehr als 23 Zeichen umfasst, müssen Sie das Kennwort auf dem Agenten-System ändern, so dass es 23 Zeichen oder weniger umfasst, damit Sie sich beim Agenten-System anmelden können.

CA ARCserve Backup wendet Ihre Anmeldeinformationen an, und das Dialogfeld "Job in Warteschlange stellen" wird geöffnet.

12. Nehmen Sie die Eingaben in den Feldern im Dialogfeld "Job in Warteschlange stellen" vor, und klicken Sie auf "OK".

Hinweis: Klicken Sie im Dialogfeld "Job wird in die Warteschlange gestellt" auf die Schaltfläche "Hilfe", um weitere Informationen zum Übergeben von Jobs anzuzeigen.

CA ARCserve Backup übergibt den Job. Weitere Informationen zum Anzeigen des Jobstatus und anderer jobbezogener Aufgaben finden Sie im *Administrationshandbuch* oder in der Online-Hilfe.

Funktionsweise der Agent-Unterstützung für das Hilfsprogramm Pre-Flight Check

Mit dem Hilfsprogramm Pre-Flight Check (PFC) können Sie wichtige Überprüfungen auf dem CA ARCserve Backup-Server und den zugehörigen Agenten ausführen, so dass Sie die möglichen Ursachen für das Fehlschlagen von Sicherungsjobs erkennen können.

Bei Sicherungen von virtuellen Rechnern überprüft das PFC-Hilfsprogramm den Status des Client Agent für Windows, der auf dem Sicherungs-Proxysystem bzw. dem Hyper-V-Hostsystem ausgeführt wird. PFC überprüft nicht den Status der VMs, die Sie für die Sicherung auf dem ESX Server- oder VirtualCenter-Server-System angegeben haben.

Hinweis: Weitere Informationen zur Verwendung des PFC-Hilfsprogramms finden Sie im "Administrationshandbuch".

Mit dem PFC-Hilfsprogramm werden folgende Überprüfungen für VMware ESX-Server-Sicherungen in folgenden Szenarien durchgeführt:

- Mit dem Agenten wird ein Sicherungsjob übergeben. Der Client Agent für Windows wird auf dem VCB-Proxysystem ausgeführt.

Die folgende Meldung wird angezeigt:

Hinweis: Der Zielknoten <Name/IP des VCB-Proxysystems> ist ein VMware VCB-Proxysystem. PFC überprüft nur den Status des Client Agent auf dem VMware VCB-Proxyserver. Der Status der virtuellen Rechner (VMs), die Sie auf dem VMware ESX-Server zur Sicherung ausgewählt haben, wird nicht überprüft.

- Mit dem Agenten wird ein Sicherungsjob übergeben. Der Client Agent für Windows wird auf dem VCB-Proxysystem nicht ausgeführt.

Die folgende Meldung wird angezeigt:

Probleme: Verbindung zum Client Agent auf <Name/IP des VCB-Proxysystems> konnte nicht hergestellt werden. Stellen Sie sicher, dass der Client Agent auf <Name/IP des VCB-Proxysystems> ausgeführt wird.

Hinweis: Der Zielknoten <Name/IP des VCB-Proxysystems> ist ein VMware VCB-Proxysystem. PFC überprüft nur den Status des Client Agent auf dem VMware VCB-Proxyserver. Der Status der virtuellen Rechner (VMs), die Sie auf dem VMware ESX-Server zur Sicherung ausgewählt haben, wird nicht überprüft.

Filtern von VM-Sicherungsdaten

In CA ARCserve Backup können Sie Daten filtern, wenn Sie eine Sicherung im Dateimodus oder eine Rotationsicherung im gemischten Modus durchführen, die Zuwachssicherungen und/oder Änderungssicherungen umfasst. Mit dieser Funktion können Sie folgende Aufgaben ausführen:

- Sicherung der Daten auf den virtuellen Rechnern basierend auf beispielsweise Dateimuster, Datumsbereich, Änderungsdatum oder Dateigröße
- Sicherung von ausgewählten Dateien, Ordnern oder beidem in einem ausgewählten Volume
- Anwendung von globalen oder lokalen Filterkriterien auf Ihre Sicherungsjobs

Hinweis: Ein *globaler* Filter wendet Filter auf all Ihre Sicherungsjobs an, während ein *lokaler* Filter lediglich Filter auf die ausgewählte VM anwendet.

So filtern Sie VM-Sicherungsdaten:

1. Öffnen Sie den Sicherungs-Manager, und suchen Sie nach der VM, die Sie filtern möchten.
2. Führen Sie eine der folgenden Aktionen aus:
 - Zur Anwendung von globalen Filtern bei Ihrer Sicherung klicken Sie in der Symbolleiste des Sicherungs-Managers auf die Schaltfläche "Filter".
 - Zur Anwendung von lokalen Filtern bei Ihrer Sicherung klicken Sie mit der rechten Maustaste auf das VM-Objekt, und wählen Sie im Kontextmenü "Filter" aus.

Das Dialogfeld "Filter" wird geöffnet.

3. Geben Sie die Filter an, die zum Abschließen des Sicherungsjobs erforderlich sind.

Hinweis: Informationen zur Datenfilterung erhalten Sie, wenn Sie im Dialogfeld "Filter" auf "Hilfe" klicken.

Durchsuchen von Wiederherstellungssitzungen

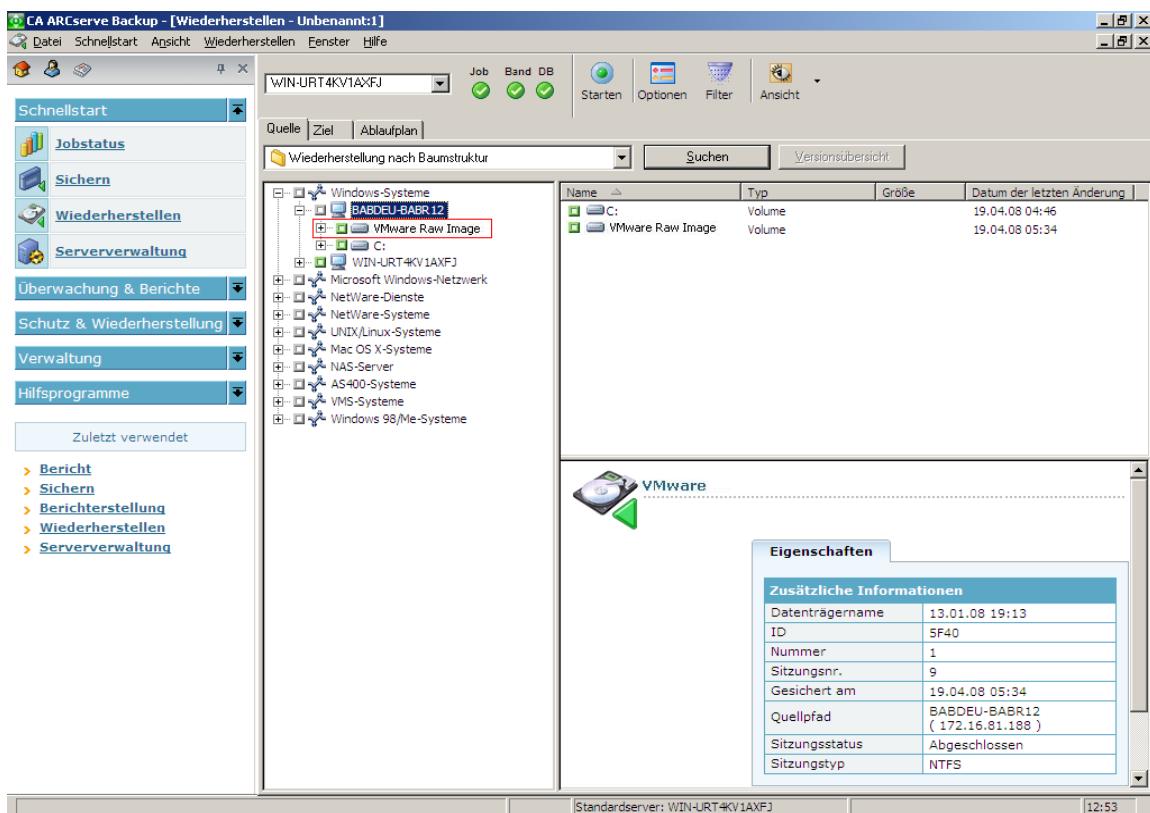
Sie verwenden zur Wiederherstellung von Daten, die sich in einer VM befinden, denselben Prozess wie bei der Wiederherstellung von einem beliebigen anderen physischen Server.

Hinweis: Weitere Informationen zum Wiederherstellen von Daten finden Sie im *"Administrationshandbuch"* oder in der Online-Hilfe.

Allerdings weist die Wiederherstellung von Daten von einer VM folgende Einschränkungen auf:

- Sie können Sicherungen auf Dateiebene (Dateimodus) an deren ursprünglichen Speicherort oder einem anderen Speicherort wiederherstellen.
- Hinweis:** Um Dateien an ihrem ursprünglichen Speicherort auf einer VM wiederherzustellen, muss der Client Agent für Windows auf der VM installiert sein.
- Sie können Sicherungen auf Raw-Ebene (vollständige VM) nur an einem anderen Speicherort wiederherstellen.

Wenn Sie im Wiederherstellungs-Manager auf der Registerkarte "Quelle" die Option "Wiederherstellung nach Baumstruktur" ausgewählt haben, werden die Raw-Modus (vollständige VM) durchgeführten VM-Sicherungen als VMware-Raw-Image angezeigt. Wenn Sie Sicherungen im Dateimodus durchführen, werden die entsprechenden Volumes in der VM angezeigt.



Im Eigenschaftsbereich der Sitzung im Fenster "Wiederherstellungs-Manager" werden die folgenden Informationen über die VMware-Sicherungsdaten angezeigt:

VMware-Proxy

Gibt den Namen des Sicherungs-Proxysystems an, das für die Sicherung dieser VM verwendet wurde.

VMware ESX Server

Gibt den Namen des ESX-Server- oder VirtualCenter-Server-Systems an, auf dem die VM bei Übergabe des Sicherungsjobs ausgeführt wurde.

Hostname

Gibt den Hostnamen der VM des Sicherungsjobs an.

Sitzungsmethode

Gibt die Sicherungsmethode an, die zur Sicherung der VM verwendet wurde (z. B. "Raw" und "Datei").

Wiederherstellen von Daten

Wenn Sie mit Hilfe von CA ARCserve Backup eine VM auf dem Sicherungs- Proxysystem sichern, können Sie die folgenden Datentypen wiederherstellen:

- Sicherungen auf Dateiebene
- [Sicherungen auf Raw-Ebene \(vollständige VM\)](#) (siehe Seite 81)

Daten auf Dateiebenengranularität wiederherstellen

Dieses Thema beschreibt, wie Daten wiederhergestellt werden, die in folgenden Sicherungsmodi gesichert wurden:

- Dateimodus
- Raw-Modus mit aktiverter Option "Wiederherstellung auf Dateiebene aktivieren"
- Gemischter Modus mit aktiverter Option "Wiederherstellung auf Dateiebene aktivieren"

Hinweis: Weitere Informationen finden Sie unter [Sicherungsmodi](#) (siehe Seite 61).

Anhand dieser Schritte können Sie Wiederherstellungsvorgänge auf lokalen, festplattenbasierten virtuellen Rechnern (VMs) und SAN-basierten VMs durchführen. Sie stellen Daten, die auf einer VM gesichert wurden, auf Dateiebene wieder her, wenn eine Datei beschädigt oder versehentlich gelöscht wurde, um ein System nach einem Ausfall wiederherzustellen oder um ein System zu klonen. Sie verwenden zur Wiederherstellung von Sicherungen auf Dateiebene denselben Prozess wie bei der Wiederherstellung von einer beliebigen Windows-basierten Client Agent-Datei.

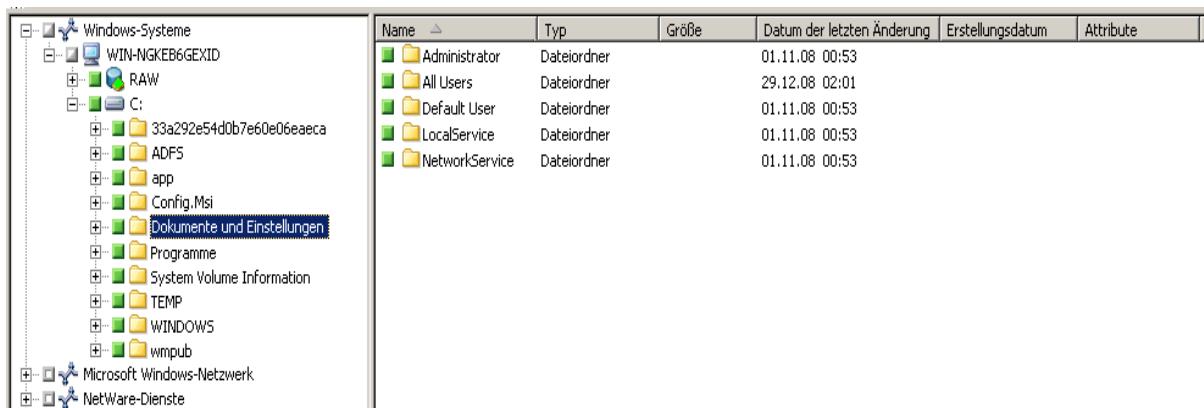
Hinweis: Weitere Informationen zum Wiederherstellen von Daten finden Sie im *Administrationshandbuch*.

Beim Wiederherstellen von Sicherungsdaten auf Dateiebene ist Folgendes zu beachten:

- Sie können Daten nur dann durchsuchen und auf Verzeichnis- und Dateiebenengranularität wiederherstellen, wenn die Daten im Dateimodus, im Raw-Modus (vollständige VM) mit aktivierter Option "Wiederherstellung im Dateimodus erlauben" oder im gemischten Modus mit aktivierter Option "Wiederherstellung im Dateimodus erlauben" gesichert wurden.
- Hinweis:** Weitere Informationen finden Sie unter [Sicherungsmodi](#) (siehe Seite 61).
- Die aktuelle Version des Client Agent für Windows muss auf dem Zielsystem installiert sein, damit Daten wiederhergestellt werden können, die mit Hilfe des Agenten für virtuelle Rechner gesichert wurden.
 - Wenn Sie Daten auf Dateiebenengranularität wiederherstellen und die Option "Dateien am ursprünglichen Speicherort wiederherstellen" aktivieren, werden Windows-Systemdateien von CA ARCserve Backup absichtlich ausgelassen. Windows-Systemdateien sind normalerweise in den folgenden Verzeichnissen gespeichert:
 - C:\WINNT (Windows 2000)
 - C:\WINDOWS\SYSTEM
 - C:\WINDOWS\SYSTEM32

So stellen Sie Daten auf Dateiebenengranularität wieder her

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie aus der Dropdown-Liste die Option "Wiederherstellung nach Baumstruktur".
2. Erweitern Sie das Objekt "Windows-Systeme", und navigieren Sie zu den Daten, die wiederhergestellt werden sollen.



The screenshot shows the 'Windows-Systeme' tree structure on the left. Under 'C:', the 'Dokumente und Einstellungen' folder is selected. On the right, a detailed list of files and folders is shown in a table:

Name	Typ	Größe	Datum der letzten Änderung	Erstellungsdatum	Attribute
Administrator	Dateiordner		01.11.08 00:53		
All Users	Dateiordner		29.12.08 02:01		
Default User	Dateiordner		01.11.08 00:53		
LocalService	Dateiordner		01.11.08 00:53		
NetworkService	Dateiordner		01.11.08 00:53		

3. Klicken Sie auf die Registerkarte "Ziel". Aktivieren Sie das Kontrollkästchen "Dateien am ursprünglichen Speicherort wiederherstellen", um die Dateien an dem ursprünglichen Speicherort wiederherzustellen.

Wenn Sie Dateien am ursprünglichen Speicherort wiederherstellen möchten, muss der Client Agent für Windows auf der VM installiert sein. Ist der Client Agent für Windows auf der VM nicht installiert, können Sie Daten an einem beliebigen Speicherort wiederherstellen und dann die Daten manuell auf die VM mit Hilfe einer Netzwerk-Dateisystemfreigabe kopieren.

Hinweis: Wenn Sie Daten auf Dateiebenengranularität wiederherstellen und die Option "Dateien am ursprünglichen Speicherort wiederherstellen" aktivieren, werden Windows-Systemdateien von CA ARCserve Backup ausgelassen.

Wichtig! Um VMware-basierte Sicherungssitzungen an einem alternativen Speicherort wiederherzustellen, muss der Client Agent für Windows auf dem alternativen System laufen, und das alternative System muss unter dem Objekt "Windows-Systeme" angezeigt werden. Wenn Sie versuchen, Daten auf einem System wiederherzustellen, das nicht unter dem Objekt "Windows-Systeme" angezeigt wird, schlägt der Wiederherstellungsjob fehl. Um Daten an einem alternativen Speicherort auf einem lokalen System wiederherzustellen, auf dem ein Windows-X86-Betriebssystem ausgeführt wird, fügen Sie im Wiederherstellungs-Manager auf der Registerkarte "Ziel" das System mit einem fiktiven Hostnamen und der echten IP-Adresse unter dem Objekt "Windows-Systeme" hinzu. Dann können Sie das Ziel als das lokale System angeben und den Wiederherstellungsjob übergeben.

Falls die Sicherungsdaten von einer Sicherung im Raw-Modus (vollständige VM) erstellt wurden, unterstützt CA ARCserve Backup die Option "Dateien am ursprünglichen Speicherort wiederherstellen" nicht.

4. Klicken Sie auf die Registerkarte "Ablaufplan", und wählen Sie aus der Dropdown-Liste eine "Wiederholungsmethode" aus.
5. Klicken Sie auf der Symbolleiste auf die Schaltfläche "Übergeben", um den Wiederherstellungsjob zu übergeben.

Das Dialogfeld "Sicherheits- und Agent-Informationen" wird geöffnet. Um den Job zu übergeben, müssen Sie für das System, auf dem die Daten wiederhergestellt werden, Ihre Anmeldeinformationen angeben.

6. Geben Sie Ihre Anmeldeinformationen in den Feldern "Benutzername" und "Kennwort" ein, und klicken Sie auf "OK".
- CA ARCserve Backup wendet Ihre Anmeldeinformationen an, und das Dialogfeld "Job in Warteschlange stellen" wird geöffnet.

7. Nehmen Sie die Eingaben in den Feldern im Dialogfeld "Job in Warteschlange stellen" vor, und klicken Sie auf "OK".

Der Job wird übergeben.

Hinweis: Klicken Sie im Dialogfeld "Job wird in die Warteschlange gestellt" auf die Schaltfläche "Hilfe", um weitere Informationen zum Übergeben von Jobs anzuzeigen. Weitere Informationen über die Anzeige des Jobstatus und andere jobbezogene Aufgaben finden Sie im *Administrationshandbuch* oder in der Online-Hilfe.

Wiederherstellen von Sicherungsdaten auf Raw-Ebene (vollständige VM)

Führen Sie mit den folgenden Schritten Wiederherstellungsvorgänge auf lokalen, festplattenbasierten virtuellen Rechnern (VMs) und SAN-basierten VMs durch. Eine Wiederherstellung von Raw-Daten (vollständige VM) wird im Rahmen der Disaster Recovery erforderlich oder wenn ein System geklont werden soll. Sie verwenden zur Wiederherstellung von Sicherungen auf Dateiebene denselben Prozess wie bei der Wiederherstellung von einer beliebigen Windows-basierten Client Agent-Datei.

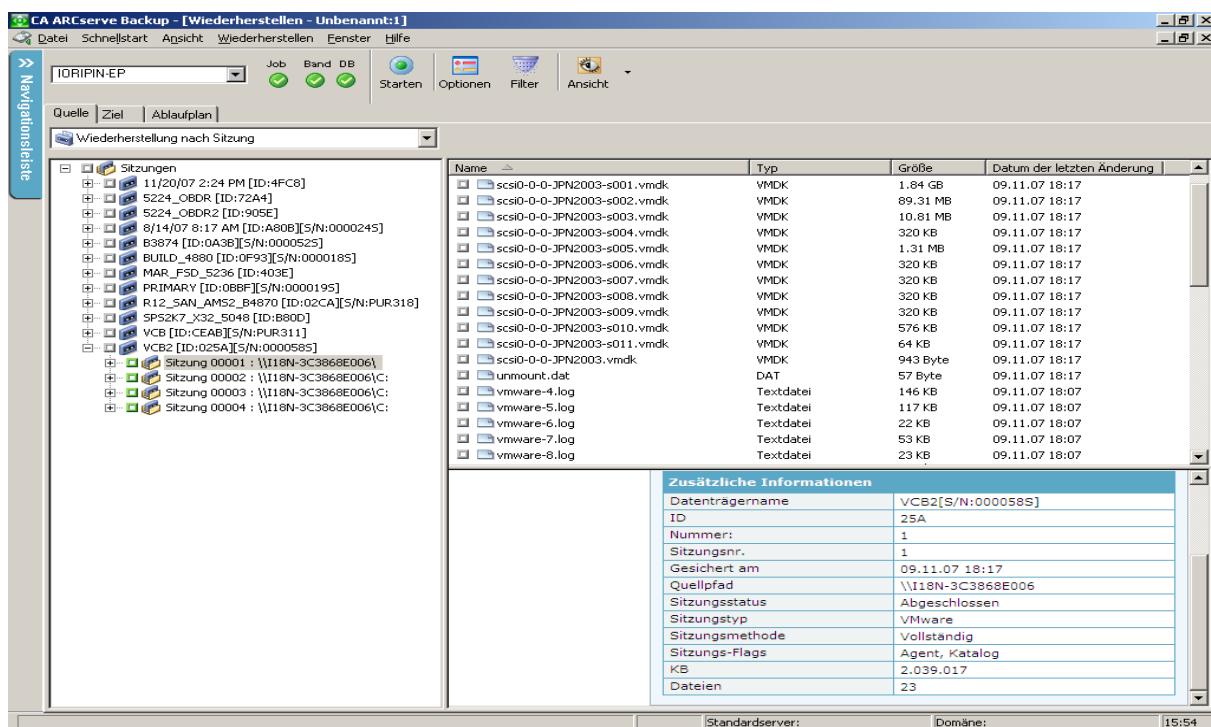
Hinweis: Weitere Informationen zum Wiederherstellen von Daten finden Sie im *Administrationshandbuch*.

Beim Wiederherstellen von Sicherungsdaten auf Raw-Ebene ist Folgendes zu beachten:

- Die aktuelle Version des Client Agent für Windows muss auf dem Zielsystem installiert sein, damit Daten wiederhergestellt werden können, die mit Hilfe des Agenten für virtuelle Rechner gesichert wurden.
- Daten, die im Raw-Modus (vollständige VM) oder gemischten Modus bei deaktivierter Option "Wiederherstellung im Dateimodus erlauben" gesichert wurden, können nicht auf Verzeichnis- oder Dateiebene durchsucht und wiederhergestellt werden.

Wiederherstellen von Sicherungsdaten auf Raw-Ebene (vollständige VM)

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie aus der Dropdown-Liste die Option "Wiederherstellung nach Baumstruktur".
- Erweitern Sie das Objekt "Windows-Systeme", und navigieren Sie zu dem VMware-System oder Hyper-V-System, das wiederhergestellt werden soll.
- Erweitern Sie das gewünschte System, und wählen Sie die Daten aus, die Sie wiederherstellen möchten.



2. Klicken Sie auf die Registerkarte "Ziel".
- Geben Sie den Speicherort für die Wiederherstellung der Daten an.
3. Klicken Sie auf die Registerkarte "Ablaufplan", und wählen Sie aus der Dropdown-Liste eine "Wiederholungsmethode" aus.
4. Klicken Sie auf der Symbolleiste auf die Schaltfläche "Übergeben", um den Wiederherstellungsjob zu übergeben.

Das Dialogfeld "Sicherheits- und Agent-Informationen" wird geöffnet. Um den Job zu übergeben, müssen Sie für das System, auf dem die Daten wiederhergestellt werden, Ihre Anmeldeinformationen angeben.

5. Geben Sie Ihre Anmeldeinformationen in den Feldern "Benutzername" und "Kennwort" ein, und klicken Sie auf "OK".

CA ARCserve Backup wendet Ihre Anmeldeinformationen an, und das Dialogfeld "Job in Warteschlange stellen" wird geöffnet.

6. Nehmen Sie die Eingaben in den Feldern im Dialogfeld "Job in Warteschlange stellen" vor, und klicken Sie auf "OK".

Der Job wird übergeben.

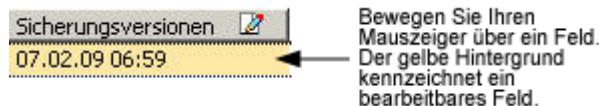
Hinweis: Klicken Sie im Dialogfeld "Job wird in die Warteschlange gestellt" auf die Schaltfläche "Hilfe", um weitere Informationen zum Übergeben von Jobs anzuzeigen. Weitere Informationen über die Anzeige des Jobstatus und andere jobbezogene Aufgaben finden Sie im *Administrationshandbuch* oder in der Online-Hilfe.

Wiederherstellen virtueller VMware-Rechner

Beim Wiederherstellen von VMware-VMs können Sie die gesamte VM sowie ihre Daten wiederherstellen. Mit diesem Vorgang können Sie Desaster Recovery für eine VM durchführen oder eine VM klonen.

Durchsuchen des Fensters "VM wiederherstellen"

Mit Hilfe des Fensters "VM wiederherstellen" können Sie verschiedene Felder durchsuchen, auswählen und ändern. Wenn Sie den Mauszeiger über ein bearbeitbares Feld führen, färbt sich der Hintergrund des Feldes gelb, so wie im Folgenden dargestellt:



Um ein bearbeitbares Feld zu ändern, wählen Sie das Zielfeld, und klicken Sie dann auf die Auslassungspunkte, um das Feld wie im Folgenden dargestellt zu durchsuchen:



Überlegungen

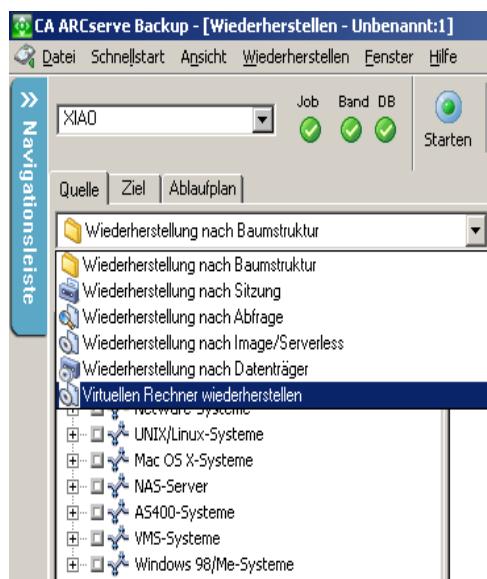
Beachten Sie Folgendes:

- CA ARCserve Backup stellt die Sicherungsdaten des virtuellen Rechners auf dem Sicherungs-Proxy-System an einem temporären Ladeort wieder her und stellt die Daten anschließend im ESX Server-System wieder her.
- Auf dem Sicherungs-Proxy-System muss VMware Converter in der Version 3.0.2 oder später installiert sein. CA ARCserve Backup verwendet die Tools von VMware Converter, um VCB-Images virtueller Rechner wiederherzustellen.

Hinweis: Informationen zum VMware Converter finden Sie unter www.vmware.com/de/products/converter.

So stellen Sie virtuelle VMware-Rechner wieder her:

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie in der Dropdown-Liste die Option "Virtuellen Rechner wiederherstellen" aus.



Das Fenster "Virtuellen Rechner wiederherstellen" wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus, um nach einer VMware-VM zu suchen, und fahren Sie dann mit dem nächsten Schritt fort.

- Um nach einer bestimmten VM zu suchen, geben Sie im Feld für den Namen des virtuellen Rechners den Namen der VM an, und klicken Sie auf "Abfragen".

Der gesuchte VM-Name wird in der Liste der VMs angezeigt.

- Um nach allen VMs zu suchen, wählen Sie im Feld für den Namen des virtuellen Rechners die Option << ALLE >> aus, und klicken Sie auf "Abfragen".

Alle VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

- Um nach einem unvollständigen VM-Namen zu suchen, ersetzen Sie die unbekannten Zeichen durch einen Stern (*), und klicken Sie auf "Abfragen".

Die VMs, die den Suchkriterien entsprechen, werden in der Liste der VMs angezeigt.

Beispiel: Wenn Sie den Wert 100-* eingeben, werden die Namen aller VMs zurückgegeben, die mit 100- beginnen, z. B. 100-1, 100-01, and 100-001.

- Klicken Sie im Feld "Nach virtuellem Rechner suchen" auf "VMware".

Alle VMware-VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

3. Füllen Sie in der VM-Liste folgende Felder aus.

Name des virtuellen Rechners (DNS-Name)

Aktivieren Sie das Kontrollkästchen neben "Name des virtuellen Rechners", um die wiederherzustellenden VMs anzugeben.

Hinweis: Wenn Sie mehr als eine VM angeben, verarbeitet CA ARCserve Backup die Wiederherstellungsvorgänge sequenziell.

Sicherungsversionen

Mit dieser Option können Sie eine Sicherungsversion angeben.

Akzeptieren Sie die angezeigte Sicherungsversion, oder klicken Sie in das Feld "Sicherungsversionen" und dann auf die Auslassungspunkte, um nach mehreren Versionen der Sicherungsdaten zu suchen.

Proxy-Rechner

Hier können Sie das Sicherungs-Proxy-System und die Sicherheitsinformationen angeben, die für die Wiederherstellung des VM-Images erforderlich sind.

Akzeptieren Sie den angezeigten Proxy-Rechner, oder klicken Sie in das Feld "Proxy-Rechner" und dann auf die Auslassungspunkte, um nach einem anderen Sicherungs-Proxy-System zu suchen und dieses auszuwählen.

Pfad

Hier können Sie den Pfad zum Laden des VM-Images angeben.

Akzeptieren Sie den angezeigten Pfad, oder klicken Sie in das Feld "Pfad", um einen alternativen Pfad für das temporäre VM-Ladeverzeichnis anzugeben.

ESX Server-Name

Hier können Sie den ESX Server und die Sicherheitsinformationen angeben, die für die Wiederherstellung des VM-Images erforderlich sind.

Akzeptieren Sie den angezeigten ESX Server-Namen, oder klicken Sie in das Feld "ESX Server-Name" und dann auf die Auslassungspunkte, um einen alternativen ESX Server zu suchen und festzulegen.

Datenspeicher

Hier können Sie den Datenspeicher angeben, der mit dem ESX-Serversystem verbunden ist.

Akzeptieren Sie den angezeigten, mit dem ESX-Serversystem verbundenen Datenspeicher-Namen, oder klicken Sie in das Feld "Datenspeicher", um den Datenspeicher des Ziel-ESX-Serversystems festzulegen.

Hinweis: Beim Datenspeicher ist die Groß- und Kleinschreibung zu beachten.

4. Klicken Sie in der Symbolleiste auf "Optionen".

Das Dialogfeld "Globale Optionen" wird geöffnet.

5. Klicken Sie auf die Registerkarte "Vorgang", und legen Sie folgende Optionen fest:

Hinweis: Die folgenden Optionen werden nicht auf der Registerkarte "Vorgang" angezeigt, es sei denn, die Methode "Virtuellen Rechner wiederherstellen" wurde festgelegt.

VMware- oder Hyper-V-VM nach der Wiederherstellung einschalten

Mit dieser Option können Sie die VM einschalten, wenn die Wiederherstellung abgeschlossen ist.

Standardwert: Aktiviert.

Beispiel: Legen Sie diese Option fest, wenn Sie den VM unmittelbar nach Abschluss der Wiederherstellung verwenden müssen.

VMware-VM überschreiben, falls vorhanden

Mit dieser Option können Sie die VM falls vorhanden überschreiben.

Standardwert: Aktiviert.

Wenn Sie eine VMware-VM wiederherstellen, ermittelt CA ARCserve Backup die virtuellen Rechner, die sich auf dem Hostsystem befinden. Falls der virtuelle Rechner auf dem Hostsystem vorhanden ist, können Sie ihn mit dieser Option unter Verwendung der bestehenden UUID des virtuellen Rechners überschreiben.

6. Klicken Sie auf "OK".
Die Optionen werden übernommen.
7. Klicken Sie auf der Symbolleiste auf die Schaltfläche "Starten", um den Wiederherstellungsjob zu übergeben.
Das Dialogfeld "Job in Warteschlange stellen" wird angezeigt.
8. Wählen Sie im Dialogfeld "Job in Warteschlange stellen" die Option "Jetzt ausführen" aus, um den Job sofort zu starten, oder wählen Sie "Ausführen am" aus, und geben Sie ein Datum und eine Uhrzeit für den Job an.
Geben Sie eine Beschreibung für den Job ein, und klicken Sie auf "OK".
Der Job wird übergeben.

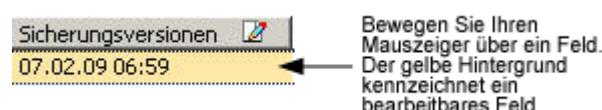
Hinweis: Weitere Informationen zum Übergeben von Jobs finden Sie im *Administrationshandbuch*.

Wiederherstellen virtueller Hyper-V-Rechner

Beim Wiederherstellen von Hyper-V-VMs können Sie die gesamte VM sowie ihre Daten wiederherstellen. Mit diesem Vorgang können Sie Disaster Recovery für eine VM durchführen oder eine VM klonen.

Durchsuchen des Fensters "VM wiederherstellen"

Mit Hilfe des Fensters "VM wiederherstellen" können Sie verschiedene Felder durchsuchen, auswählen und ändern. Wenn Sie den Mauszeiger über ein bearbeitbares Feld führen, färbt sich der Hintergrund des Feldes gelb, so wie im Folgenden dargestellt:



Um ein bearbeitbares Feld zu ändern, wählen Sie das Zielfeld, und klicken Sie dann auf die Auslassungspunkte, um das Feld wie im Folgenden dargestellt zu durchsuchen:



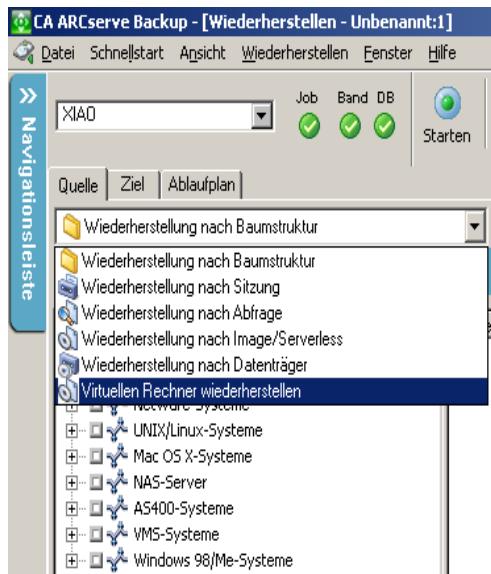
Überlegungen

Beachten Sie Folgendes:

- Die Ziel-VM sollte ausgeschaltet werden und vom System gelöscht oder umbenannt werden. Wenn die VM nicht heruntergefahren und gelöscht oder umbenannt wird, werden die Daten auf der Ziel-VM während des Wiederherstellungsvorgangs überschrieben.

So stellen Sie virtuelle Hyper-V-Rechner wieder her:

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie wie unten gezeigt in der Dropdown-Liste die Option "Virtuellen Rechner wiederherstellen" aus:



Das Fenster "Virtuellen Rechner wiederherstellen" wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus, um nach einem Hyper-V-VM zu suchen, und fahren Sie dann mit dem nächsten Schritt fort.

- Um nach einer bestimmten VM zu suchen, geben Sie im Feld für den Namen des virtuellen Rechners den Namen der VM an, und klicken Sie auf "Abfragen".

Der gesuchte VM-Name wird in der Liste der VMs angezeigt.

- Um nach allen VMs zu suchen, wählen Sie im Feld für den Namen des virtuellen Rechners die Option << ALLE >> aus, und klicken Sie auf "Abfragen".

Alle VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

- Um nach einem unvollständigen VM-Namen zu suchen, ersetzen Sie die unbekannten Zeichen durch einen Stern (*), und klicken Sie auf "Abfragen".

Die VMs, die den Suchkriterien entsprechen, werden in der Liste der VMs angezeigt.

Beispiel: Wenn Sie den Wert 100-* eingeben, werden die Namen aller VMs zurückgegeben, die mit 100- beginnen, z. B. 100-1, 100-01, and 100-001.

- Klicken Sie im Feld "Nach virtuellem Rechner suchen" auf "Hyper-V".

Alle Hyper-V-VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

3. Füllen Sie in der VM-Liste folgende Felder aus.

Name des virtuellen Rechners (DNS-Name)

Aktivieren Sie das Kontrollkästchen neben "Name des virtuellen Rechners", um die wiederherzustellenden VMs anzugeben.

Hinweis: Wenn Sie mehr als eine VM angeben, verarbeitet CA ARCserve Backup die Wiederherstellungsvorgänge sequenziell.

Sicherungsversionen

Mit dieser Option können Sie eine Sicherungsversion angeben.

Akzeptieren Sie die angezeigte Sicherungsversion, oder klicken Sie in das Feld "Sicherungsversionen" und dann auf die Auslassungspunkte, um nach mehreren Versionen der Sicherungsdaten zu suchen.

Hostname

Hier können Sie das Hyper-V-Hostsystem und die Sicherheitsinformationen angeben, die für die Wiederherstellung des VM-Images erforderlich sind.

Akzeptieren Sie den angezeigten Hostnamen für die Sicherung, oder klicken Sie in das Feld "Hostname" und dann auf die Auslassungspunkte, um nach dem Hyper-V-Hostsystem zu suchen, das mit dieser VM verbunden ist.

4. Klicken Sie in der Symbolleiste auf "Optionen".
Das Dialogfeld "Globale Optionen" wird geöffnet.
5. Klicken Sie auf die Registerkarte "Vorgang", und legen Sie folgende Optionen fest:

Hinweis: Die folgenden Optionen werden nicht auf der Registerkarte "Vorgang" angezeigt, es sei denn, die Methode "Virtuellen Rechner wiederherstellen" wurde festgelegt.

VMware- oder Hyper-V-VM nach der Wiederherstellung einschalten

Mit dieser Option können Sie die VM einschalten, wenn die Wiederherstellung abgeschlossen ist.

Standardwert: Aktiviert.

Beispiel: Legen Sie diese Option fest, wenn Sie den VM unmittelbar nach Abschluss der Wiederherstellung verwenden müssen.

6. Klicken Sie auf "OK".
Die Optionen werden übernommen.
7. Klicken Sie auf der Symbolleiste auf die Schaltfläche "Starten", um den Wiederherstellungsjob zu übergeben.
Das Dialogfeld "Job in Warteschlange stellen" wird angezeigt.
8. Wählen Sie im Dialogfeld "Job in Warteschlange stellen" die Option "Jetzt ausführen" aus, um den Job sofort zu starten, oder wählen Sie "Ausführen am" aus, und geben Sie ein Datum und eine Uhrzeit für den Job an.
Geben Sie eine Beschreibung für den Job ein, und klicken Sie auf "OK".
Der Job wird übergeben.

Hinweis: Weitere Informationen zum Übergeben von Jobs finden Sie im *Administrationshandbuch*.

Einschränkungen beim Sichern und Wiederherstellen auf virtuellen Rechnern

Die folgenden Einschränkungen gelten für die Sicherung und Wiederherstellung auf virtuellen Rechnern:

- Die VMs im ESX-Server müssen ausgeführt werden, während Sie das Hilfsprogramm "ca_vcbpopulatedb" ausführen.
Die virtuellen Rechner müssen ausgeführt werden, damit die CA ARCserve Backup-Datenbank mit dem ARCserve VMware-Konfigurationstool (ca_vcbpopulatedb.exe) und dem ARCserve Hyper-V -Konfigurationstool (ca_msmpopulatedb.exe) gefüllt werden kann und damit die virtuellen Rechner in ESX-Server-Systemen richtig durchsucht werden können.
- Sie müssen das ARCserve VMware-Konfigurationstool (ca_vcbpopulatedb.exe) und das ARCserve Hyper-V-Konfigurationstool (ca_msmpopulatedb.exe) ausführen, nachdem Sie Volumes auf einem virtuellen Rechner bzw. einen virtuellen Rechner in einem Hostsystem hinzugefügt, entfernt oder geändert haben.
Ein Versäumnis dessen kann zu inkorrekt VM-Volume-Daten in der CA ARCserve Backup-Datenbank führen, und während der Laufzeit kommt es dann zu fehlgeschlagenen Sicherungsjobs.
- In CA ARCserve Backup kann die Befehlszeile nicht für Sicherungen und Wiederherstellungen auf virtuellen Rechnern verwendet werden. Z. B. ca_backup und ca_restore.
Sie müssen für alle VM-basierten Sicherungen und Wiederherstellungen den Sicherungs-Manager und den Wiederherstellungs-Manager verwenden.
- Sie können die Wiederherstellung nach Datenträger nicht zur Wiederherstellung von Sicherungsdaten auf Dateiebene und Raw-Ebene (vollständige VM) verwenden.
- Bei der Datensicherung mit Hilfe eines Sicherungs-Proxysystems gibt es keine Konsistenzunterstützung auf Anwendungsebene.
Um Daten auf Anwendungsebene zu schützen, können Sie benutzerdefinierte pre- und post-Skripts erstellen, mit deren Hilfe Sie Daten auf Anwendungsebene konsistent halten können. Sie können die benutzerdefinierten Skripts als pre-freeze- und post-thaw-Skripts verwenden. Weitere Informationen zu pre-freeze- und post-thaw-Skripts finden Sie im Handbuch "VMware Virtual Machine Backup Guide".
- Das Hilfsprogramm "Vergleichen" unterstützt keine Vergleiche von VM-Sicherungssitzungen.
Wenn Sie versuchen, VM-Sitzungen zu vergleichen, führt CA ARCserve Backup anstelle des Vergleichs einen Suchvorgang aus.

- Der Agent bietet keine Unterstützung für die folgenden globalen Sicherungsoptionen:
 - Dateien nach Sicherungsjob löschen
 - Wiederholungsverfahren bei Zugriff auf geöffnete Dateien
- **Hinweis:** Weitere Informationen zu globalen Sicherungsoptionen finden Sie im "Administrationshandbuch".
- Aufgrund der Einschränkungen bei den technischen und logischen Zuordnungen von Volumes in der CA ARCserve Backup-Datenbank unterstützt das Hilfsprogramm "Einfügen" kein sequenzielles Einfügen.
Falls Sie Daten zu VM-Sitzungen in die CA ARCserve Backup-Datenbank einfügen möchten, können Sie die Katalogdaten einfügen.
- Vom Agent unterstützte VM-Bereitstellungspfade dürfen ausschließlich englische Zeichen enthalten. Wenn der Pfad nicht englische Zeichen enthält, werden diese unlesbar angezeigt.

Verwenden von Protokolldateien virtueller Rechner

CA ARCserve Backup beinhaltet Protokolldateien, die Ihnen Einzelheiten zu Sicherungsvorgängen liefern, die mit Hilfe des Agenten für virtuelle Rechner ausgeführt wurden. CA ARCserve Backup speichert die Protokolldateien auf dem Sicherungs-Proxy-System und dem Hyper-V-Hostsystem an folgendem Speicherort:

C:\Programme\CA\ARCserve Backup Client Agent für Windows\Log

Folgende Protokolldateien gelten für Sicherungen von VMware-VMs:

ca_vcbpopulatedb.log

Zeigt Meldungen zu Sicherungsjobs von VMware-VMs an.

Die Meldungen beginnen mit der Job-ID und der Sitzungsnummer, durch die Sie Jobs unterscheiden können, die gleichzeitig ausgeführt werden.

- **Maximale Protokollgröße:** Standardmäßig beschränkt der Agent die Größe von "ca_vcbpopulatedb.log" auf 250 KB. Um die Grenze zu ändern (zu erhöhen oder zu verringern), erstellen Sie folgende Registrierung:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters\VMMaxLogSize

Wertdaten: Legen Sie die maximale Protokollgröße fest, die Sie benötigen.

mount_jnl.log

Zeigt Informationen zu Lade- und Entladevorgängen an.

Die Protokolldatei enthält die für jeden Lade- und Entladevorgang angegebenen Parameter.

ca_vcbmounteroutput_xxx.log

Zeigt Informationen zu fehlgeschlagenen Lade- und Entladevorgängen an.

- **Maximale Protokollanzahl:** Standardmäßig speichert CA ARCServe Backup maximal 1 000 Protokolldateien. Sie können eine andere Anzahl an Protokolldateien festlegen, indem Sie die Wertdaten in folgendem Registrierungsschlüssel ändern:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe Backup\ClientAgent\Parameters\VMMaxLogFiles

Hinweis: Wenn die Anzahl der "ca_vcbmounteroutput_xxx.log"-Protokolle den maximalen Wert erreicht, überschreibt CA ARCServe Backup "ca_vcbmounteroutput_000.log" beim nächsten Ladevorgang und löscht "ca_vcbmounteroutput_001.log".

- **Maximale Protokollgröße:** Standardmäßig beschränkt der Agent die Größe der Datei "ca_vcbmounteroutput_xxx.log" auf 250 KB. Um die Grenze zu ändern (zu erhöhen oder zu verringern), erstellen Sie folgende Registrierung:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe Backup\ClientAgent\Parameters\VMMaxMountLogSize

Wertdaten: Legen Sie die maximale Protokollgröße fest, die Sie benötigen.

Die folgende Protokolldatei gilt für Sicherungen von Hyper-V-VMs:

Hyper.log

Zeigt Meldungen zu Sicherungen und Wiederherstellungen von Hyper-V-VMs an.

Die Meldungen beginnen mit der Job-ID und der Sitzungsnummer, durch die Sie Jobs unterscheiden können, die gleichzeitig ausgeführt werden.

Die folgende Protokolldatei gilt für Sicherungen von VMware- und Hyper-V-VMs:

vmdbupd.log

Enthält Informationen zur automatischen Aufnahme.

Die Protokolldatei enthält die angegebenen Parameter und den Status aller automatischen Ausführungen des [ARCServe VMware-Konfigurationstools](#) (siehe Seite 36) und des [ARCServe Hyper-V-Konfigurationstools](#) (siehe Seite 49).

Auswirkungen von VM-Namen auf Jobs

CA ARCserve Backup unterscheidet virtuelle Rechner anhand ihrer VM-Namen (DNS-Namen) in Verbindung mit ihren Hostnamen oder dem Namen des Sicherungs-Proxy-Systems. CA ARCserve Backup füllt die CA ARCserve Backup-Datenbank mit diesen Informationen, wenn Sie das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool ausführen.

Mit Hilfe des ARCserve VMware-Konfigurationstools und des ARCserve Hyper-V-Konfigurationstools können Sie Informationen zu den virtuellen Rechnern in der CA ARCserve Backup-Datenbank beibehalten oder entfernen, indem Sie die Option "VM-Informationen beibehalten" entweder aktivieren oder deaktivieren. Mit Hilfe dieses Designs können Sie Informationen zu den ausgeschalteten virtuellen Rechnern beibehalten, wenn Sie die oben genannten Tools ausführen.

Das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool greifen auf den VM-Namen zurück, um den Status eines virtuellen Rechners zu bestimmen (Beispiel: der VM ist ausgeschaltet). Wenn das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool nicht in der Lage sind, einen virtuellen Rechner anhand seines VM-Namens zu finden, suchen die Tools virtuelle Rechner anhand von deren Hostnamen oder anhand des Namens des Sicherungs-Proxy-Systems.

Beispiel: Auswirkungen von VM-Namen auf Jobs

Stellen Sie sich folgende VM-Umgebung vor:

- Sie erstellen eine Umgebung, die aus einem virtuellen Rechner besteht.
- Der Hostname dieses VM lautet VM1.
- Der VM-Name ist "VM_eins".

Folgende Ereignisse finden statt:

1. Sie führen das ARCserve VMware-Konfigurationstool oder das ARCserve Hyper-V-Konfigurationstool aus.
CA ARCserve Backup füllt die CA ARCserve Backup-Datenbank mit den Informationen zu den Daten, die auf VM1 vorhanden sind.
 2. Sie übergeben einen geplanten Sicherungsjob von VM1.
CA ARCserve Backup führt den Job aus und dieser wird erfolgreich abgeschlossen.
 3. Sie benennen VM1 in VM2 um, Sie ändern jedoch nicht den VM-Namen.
 4. Sie führen das ARCserve VMware-Konfigurationstool oder das ARCserve Hyper-V-Konfigurationstool aus und aktivieren die Option "VM-Informationen beibehalten".
CA ARCserve Backup füllt die Datenbank mit Informationen zu den Daten, die auf VM2 vorhanden sind.
- Hinweis:** Bei den Sicherungsdaten zu VM2 handelt es sich um die Daten, die sich auf VM_eins befinden.
5. Sie übergeben einen geplanten Sicherungsjob von VM2 und schalten diesen anschließend aus.
 6. CA ARCserve Backup führt beide Jobs aus. Dabei kommen folgende Ergebnisse zustande:
 - Die Sicherung von VM1 wird erfolgreich abgeschlossen. Die Sicherungsdaten bestehen aus den Daten, die sich auf VM2 befinden.
 - Die Sicherung von VM2 wird erfolgreich abgeschlossen. Die Sicherungsdaten bestehen aus den Daten, die sich auf VM2 befinden.

Beobachtungen:

- In diesem Beispiel hat der Benutzer den Hostnamen des VM geändert, jedoch nicht den VM-Namen.
- CA ARCserve Backup ist nicht in der Lage, einen virtuellen Rechner anhand seines Hostnamens zu finden (zum Beispiel VM1 und VM2), wenn der virtuelle Rechner ausgeschaltet ist. In diesem Szenario sucht CA ARCserve Backup nach dem VM-Namen (zum Beispiel VM_eins), der dem Hostnamen entspricht.
- Wenn beide virtuellen Rechner ausgeschaltet sind, haben sie in der CA ARCserve Backup-Datenbank dieselbe Identität. Infolgedessen sichert CA ARCserve Backup während der Ausführung des VM1-Jobs den falschen virtuellen Rechner.

Anhang A: Fehlerbehebung

Dieses Kapitel enthält folgende Themen:

[VM konnte nicht geladen werden](#) (siehe Seite 97)
[VM konnte nicht entladen werden](#) (siehe Seite 99)
[Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"](#) (siehe Seite 100)
[Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"](#) (siehe Seite 101)
[Sicherungsjobs schlagen anscheinend fehl.](#) (siehe Seite 103)
[VMs erscheinen nicht in der Verzeichnisstruktur des Sicherungs-Managers](#) (siehe Seite 103)
[Die Größe von Sicherungssitzungen übersteigt den auf virtuellen Rechnern belegten Speicherplatz](#) (siehe Seite 104)
[Fehler bei der Wiederherstellung von virtuellen Rechnern auf virtuellen VMware-Rechnern](#) (siehe Seite 105)
[Sicherungsdaten auf Dateiebene können nicht auf einem CA ARCserve Backup-Server wiederhergestellt werden](#) (siehe Seite 106)

VM konnte nicht geladen werden

Gültig auf Windows-Plattformen.

Symptom:

Ein Raw-Ladevorgang (vollständige VM) oder ein VM-Ladevorgang auf Dateiebene ist fehlgeschlagen.

Lösungen:

Um einen Raw-Ladevorgang (vollständige VM) oder einen VM-Ladevorgang auf Dateiebene auszuführen, erstellt VCB zuerst einen Snapshot der VM und exportiert dann die Dateien zum Sicherungs-Proxysystem. Es gibt mehrere mögliche Ursachen für dieses Problem sowie mehrere Maßnahmen zur Fehlerbehebung.

- **Ursache 1:** Es ist zu wenig freier Speicherplatz auf dem Datenträgervolume des Sicherungs-Proxy-Systems verfügbar.
Maßnahme 1: Geben Sie Speicherplatz auf dem Datenträger frei, oder verwenden Sie als Bereitstellungspfad ein anderes Volume mit ausreichend Speicherplatz.
- **Ursache 2:** Der ESX-Server wurde heruntergefahren.
Maßnahme 2: Fahren Sie den ESX-Server mit dem virtuellen Rechner wieder hoch.

- **Ursache 3:** Der virtuelle Rechner kann vorübergehend nicht geladen werden.

Maßnahme 3: Führen Sie das Hilfsprogramm "vcbMounter" für den virtuellen Rechner auf dem Sicherungs-Proxy-System aus, falls der virtuelle Rechner vorübergehend nicht geladen werden kann.

Das Hilfsprogramm kann über die Befehlszeile ausgeführt werden, indem Sie zum Installationsverzeichnis von VMware VCB-Framework navigieren. Zum Anzeigen der Syntax für das Hilfsprogramm geben Sie in der Befehlszeile Folgendes ein:

```
vcbMounter -help
```

Wenn das Hilfsprogramm "vcbMounter" die angegebene VM nicht laden kann, kann der Fehler beim VMware VCB-Framework liegen. Starten Sie das Sicherungs-Proxysystem neu, und übergeben Sie den VM-Sicherungsjob erneut.

- **Ursache 4:** Die Sicherungsquelle umfasst virtuelle Rechner, für die ein unabhängiger (persistent/nicht persistent) Datenträgermodus angegeben wurde.

Maßnahme 4: Löschen oder entfernen Sie die Datenträgermoduseinstellung "Unabhängig" für alle virtuellen Laufwerke, die mit dem virtuellen Rechner verknüpft sind.

- **Ursache 5:** Der Job wurde mit falschen Anmeldeinformationen für den VMware-ESX-Server- bzw. den VirtualCenter-Server-Benutzer übergeben. Die Anmeldeinformationen wurden im Dialogfeld "Sicherheits- und Agent-Informationen" angegeben.

Maßnahme 5: Übergeben Sie den VM-Sicherungsjob noch einmal mit gültigen Anmeldeinformationen. Sie müssen im Dialogfeld "Sicherheits- und Agent-Informationen" gültige Anmeldeinformationen für das VMware ESX-Server- oder VirtualCenter-Server-System und das Sicherungs-Proxysystem angeben.

- **Ursache 6:** Ein virtueller Rechner ist nicht mehr in der VMware-Umgebung verfügbar.

Maßnahme 6: Führen Sie das ARCserve-Konfigurationstool für VMware oder das Hilfsprogramm "ca_vcbpopulatedb" aus, um die CA ARCserve Backup-Datenbank mit aktuellen Informationen zur VMware-Umgebung zu füllen.

VM konnte nicht entladen werden

Gültig auf Windows-Plattformen.

Symptom:

Nach einer erfolgreichen Ladung schlägt eine Entladung auf einer VM fehl.

Lösung:

Eine Entladung kann unter den folgenden Bedingungen fehlschlagen:

- Der Bereitstellungspfad ist inkorrekt.
- Es wurde ein falscher Bereitstellungsmodus angegeben, zum Beispiel "Datei" oder "Raw" (vollständige VM).
- Einige der Katalogdateien wurden eventuell im Bereitstellungspunkt gelöscht.
- Der VCB-Bereitstellungs-Snapshot wurde vom Benutzer gelöscht, oder es wurde versucht, ihn zu löschen.
- Die VM wurde während der Sicherung mit Hilfe von VMotion auf ein anderes ESX-Server-System verschoben.
- VMware Converter ist nicht auf dem Sicherungs-Proxysystem installiert.

Um dieses Problem zu beheben, müssen Sie den VCB-Bereitstellungs-Snapshot der VM mit Hilfe des VI Client manuell löschen. Schlägt der Löschvorgang fehl, starten Sie die VM neu, und löschen Sie den VCB-Bereitstellungs-Snapshot für die VM.

Um Protokollinformationen zu Ladungen und Entladungen anzuzeigen, sehen Sie die Datei "mount_jnl.log" ein, die im Protokollordner im Client Agent-Installationsverzeichnis gespeichert ist.

Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"

Gültig auf Windows-Plattformen.

Symptom:

Beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb" tritt ein Fehler auf. Im ARCserve-Konfigurationstool für VMware wird im Feld "Ergebnisse" folgende Fehlermeldung angezeigt.

.NET version >=2 nicht gefunden. ca_vcbpopulatedb wird beendet.

Hinweis: Diese Meldung wird in der Eingabeaufforderung angezeigt, wenn Sie das Hilfsprogramm "ca_vcbpopulatedb" über die Windows-Eingabeaufforderung ausführen.

Lösung:

Dieser Fehler tritt auf, wenn Microsoft .NET Framework, Version 2.0 oder höher, auf dem Sicherungs-Proxysystem nicht erkannt wird.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass Microsoft .NET Framework Version 2.0 oder höher auf dem Sicherungs-Proxysystem installiert ist und ausgeführt wird.
2. Öffnen Sie eine .NET-Eingabeaufforderung, und wechseln Sie in das Installationsverzeichnis des Client Agent für Windows. Der Client Agent für Windows ist standardmäßig in einem der folgenden Verzeichnissen installiert:
 - X86-Systeme
C:\Programme\CA\ARCserve Backup Client Agent for windows
 - X64-Systeme
C:\Programme\CA\ARCserve Backup Client Agent für windows\x86

Führen Sie den folgenden Befehl aus:

```
regasm vcb_com.dll
```

(Optional) Wenn Sie die .NET-Eingabeaufforderung nicht finden, führen Sie die folgenden Schritte aus:

- a. Öffnen Sie eine Windows-Befehlszeile, und wechseln Sie in das folgende Verzeichnis:

C:\WINDOWS\Microsoft.NET\Framework

- b. Wenn Sie in dieses Verzeichnis gewechselt sind, wechseln Sie in das Verzeichnis mit einer höheren Versionsnummer als Microsoft .NET Framework Version 2.0. Beispiel:

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727

- c. Führen Sie den folgenden Befehl aus:

```
regasm <Installationsverzeichnis des Client Agent für  
windows>\vcb_com.dll
```

Nachdem die Ausführung erfolgreich abgeschlossen wurde, wird in der .NET- oder Windows-Eingabeaufforderung folgende Ausgabe angezeigt:

```
Microsoft (R) .NET Framework Assembly Registration utility 2.0.50727.42  
Copyright (C) Microsoft Corporation 1998-2004. Alle Rechte vorbehalten.
```

Types registered successfully.

Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"

Gültig auf Windows-Plattformen.

Symptom:

Beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb" tritt ein Fehler auf. Im ARCserve-Konfigurationstool für VMware wird im Feld "Ergebnisse" folgende Fehlermeldung angezeigt.

```
Err_code: -100 Make_Connection: Exception Raised - System.Net.WebException: The  
request failed with HTTP status 407: Proxy Authentication Required. Browse:  
Exception raised - Error in Make_Connection.
```

Lösung:

Der obige Fehler tritt auf, weil das ARCserve VMware-Konfigurationstool und das Hilfsprogramm "ca_vcbpopulatedb" dem Sicherungs-Proxy-System zur Laufzeit keine Anmeldeinformationen bereitstellen können. Um Abhilfe zu schaffen, müssen Sie die Einstellungen so konfigurieren, dass das ESX-Serversystem bzw. das VirtualCenter-Serversystem die Verbindung mit dem Sicherungs-Proxy-System umgehen darf.

Gehen Sie wie folgt vor, um ESX- und/oder VirtualCenter-Serversysteme zur Ausnahmenliste hinzuzufügen:

1. Öffnen Sie "Internet Explorer".
Klicken Sie im Menü "Extras" auf "Internetoptionen".
Das Dialogfeld "Internetoptionen" wird geöffnet.
2. Klicken Sie auf die Registerkarte "Verbindungen".
Die Verbindungsoptionen werden angezeigt.
3. Klicken Sie auf "LAN-Einstellungen".
Das Dialogfeld "LAN-Einstellungen" wird geöffnet.
4. Aktivieren Sie im Abschnitt "Proxyserver" die Option "Proxyserver für LAN verwenden".
Klicken Sie auf "Erweitert".
Das Dialogfeld "Proxyeinstellungen" wird geöffnet.
5. Fügen Sie im Feld "Ausnahmen" die gewünschten ESX- bzw. VirtualCenter-Serversysteme hinzu. Falls Sie mehrere ESX- und VirtualCenter-Serversysteme hinzufügen, trennen Sie die Einträge mit einem Semikolon (;) voneinander.
Klicken Sie auf "OK", um alle geöffneten Dialogfelder zu schließen.
Die ESX- und VirtualCenter-Serversysteme werden zur Ausnahmenliste hinzugefügt.

Sicherungsjobs schlagen anscheinend fehl.

Gilt für Hyper-V- und VMware-Systeme.

Symptom:

Sie übermitteln eine Sicherung von VMware- oder Hyper-V-VMs. Folgende Optionen wurden für die Sicherung festgelegt:

- Raw-Modus oder gemischter Modus
- Wiederherstellung auf Dateiebene aktivieren

Der Job wird mit dem Status "Unvollständig" beendet, und im Aktivitätsprotokoll wird die Fehlermeldung AW0550 angezeigt.

Lösung:

Das oben beschriebene Verhalten tritt auf, da der Name des CA ARCserve Backup-Servers, der die VM schützt, nicht angegeben wurde oder der angegebene Name nicht korrekt ist.

Stellen Sie zur Behebung dieses Fehlers sicher, dass der Name des CA ARCserve Backup-Servers, der die VM schützt, korrekt angegeben ist.

Weitere Informationen finden Sie unter [Angeben des CA ARCserve Backup-Servernamens](#) (siehe Seite 34).

VMs erscheinen nicht in der Verzeichnisstruktur des Sicherungs-Managers

Gilt für Hyper-V- und VMware-Systeme.

Symptom:

Sie führen das ARCserve VMware-Konfigurationstool oder das ARCserve Hyper-V-Konfigurationstool aus. Nachdem Sie den Sicherungs-Manager geöffnet haben, werden einige VMs nicht unter dem Objekt "VMware VCB-Systeme" oder dem Objekt "Microsoft Hyper-V Systeme" angezeigt.

Lösung:

Das oben beschriebene Verhalten ist normal. Obwohl die zuvor genannten Tools Sicherungsinformationen zu VMs erfassen, die zum Zeitpunkt der Ausführung der Tools ausgeschaltet sind, werden die mit den ausgeschalteten VMs verbundenen Informationen nicht unter dem Objekt "VMware VCB-Systeme" oder dem Objekt "Microsoft Hyper-V-Systeme" angezeigt. Um dieses Problem beheben zu können, müssen Sie die VMs einschalten und dann das entsprechende Tool ausführen.

Die Größe von Sicherungssitzungen übersteigt den auf virtuellen Rechnern belegten Speicherplatz

Gültig auf Windows-Plattformen.

Symptom:

Die Größe von Sicherungssitzungen übersteigt den auf virtuellen Rechnern belegten Speicherplatz.

Lösung:

Dies ist das normale Verhalten, wenn Sie einen Sicherungsjob im Raw-Modus mit aktiverter Option "Wiederherstellung im Dateimodus erlauben" übergeben. Sehen Sie sich das folgende Beispiel an:

Daten	Größe der Sicherungssitzung mit "Wiederherstellung im Dateimodus erlauben"	Größe der Sicherungssitzung ohne "Wiederherstellung im Dateimodus erlauben"
Virtueller Datenträger: 20 GB	20 GB	4 GB
Belegter Speicher: 4 GB		
Freier Speicherplatz: 16 GB		

Bei aktiverter Option "Wiederherstellung im Dateimodus erlauben" sichert CA ARCserve Backup den belegten und den freien Speicherplatz auf dem virtuellen Rechner. Daher entspricht die Größe der Sicherungssitzung der Größe des virtuellen Rechners.

Ohne die Option "Wiederherstellung im Dateimodus erlauben" sichert CA ARCserve Backup nur den belegten Speicherplatz auf dem virtuellen Rechner. Daher ist die Sicherungssitzung etwas größer als der Umfang des belegten Speicherplatzes auf dem virtuellen Rechner. (CA ARCserve Backup reserviert zusätzlichen Platz für Metadaten.)

Fehler bei der Wiederherstellung von virtuellen Rechnern auf virtuellen VMware-Rechnern

Gültig auf Windows-Plattformen.

Symptom:

Wenn Sie Jobs zur Wiederherstellung virtueller Rechner auf VMware-basierten virtuellen Rechnern übergeben, tritt der Fehler AE0564 auf.

Lösungen:

Es gibt verschiedene Gründe für Fehler bei der Wiederherstellung virtueller Rechner auf virtuellen VMware-Rechnern. In der folgenden Liste finden Sie mögliche Fehlerursachen sowie die erforderlichen Maßnahmen.

- **Ursache 1:** Die für das ESX-Serversystem angegebenen Anmeldeinformationen sind falsch.
Maßnahme 1: Stellen Sie sicher, dass die für das ESX-Serversystem angegebenen Anmeldeinformationen richtig sind.
- **Ursache 2:** Der Zieldatenspeicher verfügt nicht über ausreichend freien Speicherplatz.
Maßnahme 2: Stellen Sie sicher, dass im Zieldatenspeicher auf dem ESX-Serversystem ausreichend freier Speicherplatz verfügbar ist. Sie können den Zieldatenspeicher ggf. auch in ein anderes ESX-Serversystem verschieben.
- **Ursache 3:** Das ESX-Serversystem ist heruntergefahren oder nicht erreichbar.
Maßnahme 3: Stellen Sie sicher, dass das ESX-Serversystem mit dem Sicherungs-Proxy-System kommunizieren kann.
- **Ursache 4:** VMware unterstützt das auf dem virtuellen Rechner ausgeführte Gastbetriebssystem nicht.
Maßnahme 4: Stellen Sie sicher, dass der VMware Converter das auf dem virtuellen Rechner ausgeführte Gastbetriebssystem unterstützt. Weitere Informationen finden Sie auf der VMware-Support-Website.

- **Ursache 5:** Sie haben versucht, ein Gastbetriebssystem mit einer x64-Architektur auf einem ESX-Serversystem mit einer x86-Architektur wiederherzustellen.

Maßnahme 5: Stellen Sie sicher, dass das ESX-Serversystem über eine x64-Architektur verfügt.

Hinweis: Sie können zum Wiederherstellen des virtuellen Rechners die VMDK-Dateien verwenden. Den Pfad zu den VMDK-Dateien finden Sie in der Datei "CA_VCBpopulateDB.log" auf dem Sicherungs-Proxysystem. Die Datei "CA_VCBpopulateDB.log" befindet sich in folgendem Verzeichnis:

<<Installationsverzeichnis des Client-Agent>>\Log

Sicherungsdaten auf Dateiebene können nicht auf einem CA ARCserve Backup-Server wiederhergestellt werden

Gültig auf Windows-Systemen.

Symptom:

In CA ARCserve Backup gibt es keinen Mechanismus, mit dem Sicherungsdaten auf Dateiebene auf einem CA ARCserve Backup-Server wiederhergestellt werden können.

Lösung:

Damit Sicherungsdaten auf Dateiebene an einem anderen Standort wiederhergestellt werden können, muss der CA ARCserve Backup Client Agent für Windows auf dem Zielcomputer installiert sein. Der CA ARCserve Backup Client Agent für Windows ist standardmäßig auf dem CA ARCserve Backup-Server installiert. Damit Sicherungsdaten auf Dateiebene auf dem CA ARCserve Backup-Server wiederhergestellt werden können, müssen Sie den CA ARCserve Backup-Server im Wiederherstellungs-Manager auf der Registerkarte "Ziel" zum Objekt "Windows-Systeme" hinzufügen. Fügen Sie den CA ARCserve Backup-Server unter Verwendung seiner IP-Adresse und eines fiktiven Hostnamens zum Objekt "Windows-Systeme" hinzu.

Nachdem Sie den CA ARCserve Backup-Server zum Objekt "Windows-Systeme" hinzugefügt haben, können Sie den Server durchsuchen und den Standort für die Wiederherstellung der Dateien angeben.

Gehen Sie wie folgt vor, um den CA ARCserve Backup-Server zum Objekt "Windows-Systeme" hinzuzufügen:

1. Öffnen Sie den Wiederherstellungs-Manager, und klicken Sie auf die Registerkarte "Ziel".

Deaktivieren Sie die Option "Dateien am ursprünglichen Speicherort wiederherstellen".

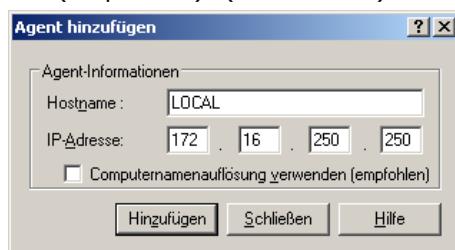
Die Verzeichnisstruktur des Agenten wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf das Objekt "Windows-Systeme", und wählen Sie im Kontextmenü die Option "Rechner/Objekt hinzufügen" aus (siehe folgende Abbildung).

Das Dialogfeld "Agent hinzufügen" wird geöffnet.

3. Füllen Sie die folgenden Felder aus:

- **Hostname:** Ermöglicht die Angabe des Hostnamens für den CA ARCserve Backup-Server.
Hinweis: Sie müssen einen fiktiven Hostnamen verwenden. Beispiel: LOKAL
- **IP-Adresse:** Ermöglicht die Registrierung des CA ARCserve Backup-Servers über die IP-Adresse. Zum Angeben der IP-Adresse deaktivieren Sie die Option "Computernamenauflösung verwenden (empfohlen)" (siehe unten):



Klicken Sie auf "Hinzufügen".

Der CA ARCserve Backup-Server wird wie unten gezeigt zum Objekt "Windows-Systeme" hinzufügt.



4. Klicken Sie auf "Schließen".

Das Dialogfeld "Agent hinzufügen" wird geschlossen.

Sie können den CA ARCserve Backup-Server jetzt durchsuchen und den Standort für die Wiederherstellung der Sicherungsdaten auf Dateiebene angeben.

Anhang B: Konfigurieren von ESX Server-Systemen und VirtualCenter Server-Systemen

In den folgenden Abschnitten wird beschrieben, wie das Kommunikationsprotokoll konfiguriert werden muss, damit ESX Server- und VirtualCenter Server-Systeme über ein Sicherungs-Proxy-System gesichert werden.

Dieses Kapitel enthält folgende Themen:

[Konfigurieren von ESX Server 3.0.2-Systemen](#) (siehe Seite 109)

[Konfigurieren von ESX Server 3.5-Systemen](#) (siehe Seite 112)

[Konfigurieren von ESX Server 3i-Systemen](#) (siehe Seite 113)

[Konfigurieren von VirtualCenter Server 2.0.2-Systemen](#) (siehe Seite 115)

[Konfigurieren von VirtualCenter Server 2.5-Systemen](#) (siehe Seite 118)

Konfigurieren von ESX Server 3.0.2-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf ESX Server 3.0.2-Systemen konfiguriert werden muss.

So konfigurieren Sie ESX Server 3.0.2-Systeme:

1. Installieren Sie ESX-Server. Weitere Informationen zu den ESX-Server-Voraussetzungen finden Sie im Handbuch "VMware ESX Server Installation Guide" auf der Website von VMware.

Hinweis: Zum Verwalten des ESX-Servers mit Hilfe von VMware VirtualCenter müssen Sie den VirtualCenter-Server als Teil der Virtual Infrastructure-Installation installieren und konfigurieren.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

- Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
- Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem freigegeben sein und dieselbe LUN-Nummer aufweisen.

Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Wenn Sie die Sicherung von VMs über ein VCB-Sicherungs-Proxy unter Verwendung eines ESX Server 3.0.2-Systems einrichten möchten, konfigurieren Sie eines der folgenden Kommunikationsprotokolle:

HTTPS

Wenn Sie HTTPS als Kommunikationsprotokoll zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem verwenden möchten, müssen Sie das selbst generierte SLL-Zertifikat vom ESX-Server-System auf das Sicherungs-Proxysystem kopieren und dann auf dem Sicherungs-Proxysystem installieren.

Hinweis: HTTPS ist das Kommunikationsprotokoll, das standardmäßig vom ARCserve-Konfigurationstool für VMware und dem Hilfsprogramm "ca_vcbpopulatedb" verwendet wird. HTTPS ermöglicht die Kommunikation von CA ARCserve Backup mit dem VCB-Sicherungs-Proxy und dem ESX-Server-System oder dem VirtualCenter-Server-System.

Sie können über das folgende Verzeichnis auf dem ESX-Server-System auf das SSL-Zertifikat (mit der Bezeichnung "rui.crt") zugreifen:

/etc/vmware/ssl/rui.crt

Zur Installation des SSL-Zertifikats klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontextmenü "Installieren" aus.

Hinweis: Der im SSL-Zertifikat zugewiesene Hostname muss dem Namen des ESX-Server-Systems entsprechen, der beim Ausführen des Befehlszeilenhilfsprogramms "ca_vcbpopulatedb" festgelegt wird. Wenn der Name nicht identisch ist oder der Hostname im SSL-Zertifikat fehlt, wird die folgende Meldung angezeigt: "Ungültiges Server-Zertifikat. Der Zertifikatsname CN stimmt nicht mit dem übergebenen Wert überein". Wählen Sie "Ja", um fortzufahren.

HTTP

Um HTTP als Kommunikationsprotokoll zwischen dem Sicherungs-
Proxysystem und dem ESX-Server-System zu verwenden, müssen Sie das
HTTP-Protokoll auf dem ESX-Server-System in der Datei "config.xml" unter
"/etc/vmware/hostd/config.xml" wie folgt konfigurieren:

- a. Suchen Sie das <proxy Database>-Tag im <http>-Tag.
- b. Fügen Sie den folgenden Text dem <proxy Database>-Tag hinzu:

```
<server id="1">
<namespace> /sdk </namespace>
<host> localhost </host>
<port> 8085 </port>
</server>
```

- c. Entfernen Sie den folgenden Text:

```
<redirect id="2"> /sdk </redirect>
```

- d. Starten Sie den VMware Infrastructure SDK Management Service mit
Hilfe des folgenden Befehls neu:

```
# service mgmt-vmware restart
```

Hinweis: Weitere Informationen finden Sie in der Virtual Infrastructure
SDK-Dokumentation auf der VMware-Website.

4. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs-
Proxysystem.
5. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort
an. Weitere Informationen finden Sie unter [Angeben eines temporären VM-
Ladeortes](#) (siehe Seite 40).
6. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um
Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-
Datenbank einzupflegen.
Optional können Sie mit Hilfe des Befehlszeilendienstprogramms
"ca_vcpopulate" Informationen in die ARCserve-Datenbank einpflegen.

Wichtig! Die VMs im ESX-Server-System müssen ausgeführt werden,
während Sie dieses Hilfsprogramm ausführen. Wenn die VMs nicht
ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den
VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen
über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es
müssen die neuesten VMware-Tools installiert sein.

Konfigurieren von ESX Server 3.5-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf ESX Server 3.5-Systemen konfiguriert werden muss.

So konfigurieren Sie ESX Server 3.5-Systeme:

1. Installieren Sie ESX-Server. Weitere Informationen zu den ESX-Server-Voraussetzungen finden Sie im Handbuch "VMware ESX Server Installation Guide" auf der Website von VMware.
2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:
 - Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
 - Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem freigegeben sein und dieselbe LUN-Nummer aufweisen.

Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Melden Sie sich als Root-Benutzer bei der Service-Konsole an, und wechseln Sie zu folgendem Verzeichnis:

/etc/vmware/hostd

4. Öffnen Sie die Datei "proxy.xml" mit einem Texteditor.

Navigieren Sie zur Liste der Endpunkte in der Datei (gekennzeichnet durch das Tag <EndpointList>). Diese enthalten die Einstellungen für den Webdienst, der das SDK unterstützt. Die verschachtelten Tags können folgendermaßen angezeigt werden:

```
<e id="1">
<_type>vim.ProxyService.NamedPipesServiceSpec</_type>
<accessMode>httpswithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-sdk</pipeName>
<serverNamespace>/sdk</serverNamespace>
</e>
```

Ändern Sie den Zugriffsmodus (accessMode) in "httpAndHttps".

Speichern Sie Ihre Einstellungen, und schließen Sie die Datei.

5. Starten Sie den vmware-hostd-Prozess mit Hilfe des folgenden Befehls neu:
`service mgmt-vmware restart`
6. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs- Proxysystem.
7. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter [Angeben eines temporären VM-Ladeortes](#) (siehe Seite 40).
8. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup- Datenbank einzupflegen.
Optional können Sie mit Hilfe des Befehlszeilendienstprogramms "ca_vcbpopulatedb" Informationen in die ARCserve-Datenbank einflegen.
Wichtig! Die VMs im ESX-Server-System müssen ausgeführt werden, während Sie dieses Hilfsprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Konfigurieren von ESX Server 3i-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf ESX Server 3i-Systemen konfiguriert werden muss.

So konfigurieren Sie ESX Server 3i-Systeme:

1. Installieren Sie ESX-Server. Weitere Informationen zu den ESX-Server- Voraussetzungen finden Sie im Handbuch "VMware ESX Server Installation Guide" auf der Website von VMware.

Hinweis: Zum Verwalten des ESX-Servers mit Hilfe von VMware VirtualCenter müssen Sie den VirtualCenter-Server als Teil der Virtual Infrastructure-Installation installieren und konfigurieren.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

- Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
- Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem freigegeben sein und dieselbe LUN-Nummer aufweisen.

Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Installieren Sie die Remote-Befehlszeilenschnittstelle (RCLI), die von VMware auf jedem Windows- oder Linux-System bereitgestellt wird.
4. Rufen Sie mit Hilfe des RCLI-Befehls "vifs" eine Kopie der Datei "proxy.xml" zum Bearbeiten ab. Die Syntax für diesen Befehl ist wie folgt:

```
vifs --server hostname --username username --get /host/proxy.xml proxy.xml
```

5. Öffnen Sie die Datei "proxy.xml" mit einem Texteditor.

Navigieren Sie zur Liste der Endpunkte in der Datei (gekennzeichnet durch das Tag <EndpointList>). Diese enthalten die Einstellungen für den Webdienst, der das SDK unterstützt. Die verschachtelten Tags können folgendermaßen angezeigt werden:

```
<e id="1">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-sdk</pipeName>
<serverNamespace>/sdk</serverNamespace>
</e>
```

Ändern Sie den Zugriffsmodus (accessMode) in "httpAndHttps".

Speichern Sie Ihre Änderungen, und schließen Sie die Datei.

6. Kopieren Sie die Datei "proxy.xml" mit Hilfe des Befehls "vifs" wieder auf den ESX Server. Die Syntax für diesen Befehl ist wie folgt:

```
vifs --server hostname --username username --put proxy.xml /host/proxy.xml
```

7. Übernehmen Sie die Einstellungen mit Hilfe des Vorgangs zum Neustart von Management-Agenten über die lokale Konsole.

Hinweis: Standardmäßig wird auf ESX Server 3i das Kommunikationsprotokoll "httpsWithRedirect" verwendet.

8. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs-
Proxysystem.
- 9.
10. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort
an. Weitere Informationen finden Sie unter [Angeben eines temporären VM-
Ladeortes](#) (siehe Seite 40).
11. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um
Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-
Datenbank einzupflegen.
Optional können Sie mit Hilfe des Befehlszeilendienstprogramms
"ca_vcbsuppliedb" Informationen in die ARCserve-Datenbank einpflegen.
Wichtig! Die VMs im ESX-Server-System müssen ausgeführt werden,
während Sie dieses Hilfsprogramm ausführen. Wenn die VMs nicht
ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den
VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen
über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es
müssen die neuesten VMware-Tools installiert sein.

Informationen zur Verwendung des Befehls "vifs" finden Sie im *ESX Server 3i Configuration Guide* unter "Performing File System Operations with vifs".

Informationen zum Konfigurieren der ESX Server 3i-Sicherheit und zum
Verwenden des Vorgangs zum Neustart von Managementagenten finden Sie im
ESX Server 3i Configuration Guide.

Konfigurieren von VirtualCenter Server 2.0.2-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf
VirtualCenter Server 2.0.2-Systemen konfiguriert werden muss.

So konfigurieren Sie VirtualCenter Server 2.0.2-Systeme:

1. Installieren Sie ESX-Server. Weitere Informationen zu den ESX-Server-
Voraussetzungen finden Sie im Handbuch "VMware ESX Server Installation
Guide" auf der Website von VMware.

Hinweis: Zum Verwalten des ESX-Servers mit Hilfe von VMware
VirtualCenter müssen Sie den VirtualCenter-Server als Teil der Virtual
Infrastructure-Installation installieren und konfigurieren.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

- Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
- Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem freigegeben sein und dieselbe LUN-Nummer aufweisen.

Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Wenn Sie die Sicherung von VMs über einen VCB-Sicherungs-Proxy und ein VirtualCenter-Server-System einrichten möchten, konfigurieren Sie eines der folgenden Kommunikationsprotokolle:

HTTPS

Wenn Sie HTTPS als Kommunikationsprotokoll zwischen dem VirtualCenter-Server-System und dem Sicherungs-Proxysystem verwenden möchten, müssen Sie das selbst generierte SSL-Zertifikat vom VirtualCenter-Server-System auf das Sicherungs-Proxysystem kopieren und dann auf dem Sicherungs-Proxysystem installieren.

Hinweis: HTTPS ist das Kommunikationsprotokoll, das standardmäßig vom ARCserve VMware-Konfigurationstool und dem Hilfsprogramm "ca_vcbsigneddb" verwendet wird. Die HTTPS-Kommunikation ermöglicht CA ARCserve Backup die Kommunikation mit dem VCB-Sicherungs-Proxy-System und dem ESX Server-System oder dem VirtualCenter Server-System.

Sie können über das folgende Verzeichnis auf dem ESX-Server-System auf das SSL-Zertifikat (mit der Bezeichnung RUI.CRT) zugreifen :

C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware virtualCenter\SSL\rui.crt

Zur Installation des SSL-Zertifikats klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontextmenü "Installieren" aus.

Hinweis: Der im SSL-Zertifikat zugewiesene Hostname muss mit dem Namen des VirtualCenter-Server-Systems übereinstimmen, der beim Ausführen des Befehlszeilenhilfsprogramms "ca_vcbsigneddb" angegeben wurde. Wenn der Name nicht identisch ist oder der Hostname im SSL-Zertifikat fehlt, wird die folgende Meldung angezeigt: "Ungültiges Server-Zertifikat. Der Zertifikatsname CN stimmt nicht mit dem übergebenen Wert überein". Wählen Sie "Ja", um fortzufahren.

HTTP

Wenn Sie HTTP als Kommunikationsprotokoll zwischen dem Sicherungs- Proxysystem und dem VirtualCenter-Server-System verwenden möchten, müssen Sie das HTTP-Protokoll auf dem VirtualCenter-Server-System wie folgt in der Datei "vpxd.cfg" konfigurieren. Die Datei finden Sie unter:

C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware virtualCenter\SSL\vpxd.cfg.

- a. Suchen Sie das <proxy Database>-Tag im <http>-Tag.
- b. Fügen Sie den folgenden Text dem <proxy Database>-Tag hinzu:

```
<server id="1">
<namespace> /sdk </namespace>
<host> localhost </host>
<port> -2 </port>
</server>
```

- c. Entfernen Sie den folgenden Text:

```
<redirect id="1"> /sdk </redirect>
```

- d. Starten Sie den VMware VirtualCenter Server-Dienst neu:

Dies kann über die Systemsteuerung für Dienste erfolgen.

Hinweis: Weitere Informationen finden Sie im Handbuch "VMware VCB Backup Guide" auf der Website von VMware.

4. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs- Proxysystem.
5. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter [Angeben eines temporären VM-Ladeortes](#) (siehe Seite 40).
6. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup- Datenbank einzupflegen.

Optional können Sie mit Hilfe des Befehlszeilenhilfsprogramms "ca_vcbpopulatedb" Informationen in die ARCserve-Datenbank aufnehmen.

Wichtig! Die VMs im ESX-Server-System müssen ausgeführt werden, während Sie dieses Hilfsprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Konfigurieren von VirtualCenter Server 2.5-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf VirtualCenter Server 2.5-Systemen konfiguriert werden muss.

So konfigurieren Sie VirtualCenter Server 2.5-Systeme:

1. Installieren Sie ESX-Server. Weitere Informationen zu den ESX-Server-Voraussetzungen finden Sie im Handbuch "VMware ESX Server Installation Guide" auf der Website von VMware.

Hinweis: Zum Verwalten des ESX-Servers mit Hilfe von VMware VirtualCenter müssen Sie den VirtualCenter-Server als Teil der Virtual Infrastructure-Installation installieren und konfigurieren.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

- Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
- Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem ESX-Server-System und dem Sicherungs-Proxysystem freigegeben sein und dieselbe LUN-Nummer aufweisen.

Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Wenn Sie die Sicherung von VMs über einen VCB-Sicherungs-Proxy und ein VirtualCenter-Server-System einrichten möchten, konfigurieren Sie eines der folgenden Kommunikationsprotokolle:

HTTPS

Wenn Sie HTTPS als Kommunikationsprotokoll zwischen dem VirtualCenter-Server-System und dem Sicherungs-Proxysystem verwenden möchten, müssen Sie das selbst generierte SLL-Zertifikat vom VirtualCenter-Server-System auf das Sicherungs-Proxysystem kopieren und dann auf dem Sicherungs-Proxysystem installieren.

Hinweis: HTTPS ist das Kommunikationsprotokoll, das standardmäßig vom ARCserve VMware-Konfigurationstool und dem Hilfsprogramm "ca_vcbpopulatedb" verwendet wird. Die HTTPS-Kommunikation ermöglicht CA ARCserve Backup die Kommunikation mit dem VCB-Sicherungs-Proxy-System und dem ESX Server-System oder dem VirtualCenter Server-System.

Sie können über das folgende Verzeichnis auf dem ESX-Server-System auf das SSL-Zertifikat (mit der Bezeichnung RUI.CRT) zugreifen :

C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware virtualCenter\SSL\rui.crt

Zur Installation des SSL-Zertifikats klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontextmenü "Installieren" aus.

Hinweis: Der im SSL-Zertifikat zugewiesene Hostname muss mit dem Namen des VirtualCenter-Server-Systems übereinstimmen, der beim Ausführen des Befehlszeilenhilfsprogramms "ca_vcbpopulatedb" angegeben wurde. Wenn der Name nicht identisch ist oder der Hostname im SSL-Zertifikat fehlt, wird die folgende Meldung angezeigt: "Ungültiges Server-Zertifikat. Der Zertifikatsname CN stimmt nicht mit dem übergebenen Wert überein". Wählen Sie "Ja", um fortfahren.

HTTP

Wenn Sie HTTP als Kommunikationsprotokoll zwischen dem Sicherungs-Proxy-System und dem VirtualCenter Server-System verwenden möchten, müssen Sie das HTTP-Protokoll auf dem VirtualCenter Server-System in der folgenden Datei konfigurieren:

C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware virtualCenter\proxy.xml";

- a. Öffnen Sie die Datei "proxy.xml" mit einem Texteditor.
- b. Navigieren Sie zur Liste der Endpunkte in der Datei (gekennzeichnet durch das Tag <EndpointList>). Diese enthalten die Einstellungen für den Webdienst, der das SDK unterstützt. Die verschachtelten Tags können folgendermaßen angezeigt werden:

```
<e id="1">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<serverNamespace>/sdk</serverNamespace>
<accessMode>httpsWithRedirect</accessMode>
<port> 8085 </port>
</e>
```

- c. Ändern Sie den Zugriffsmodus (accessMode) in "httpAndHttps".
4. Starten Sie den VirtualCenter-Dienst über die Befehlszeile oder die Systemsteuerungsoption für Windows-Dienste neu.
5. Installieren Sie den CA ARCserve Backup Client Agent für Windows auf dem Sicherungs-Proxysystem.

6. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter [Angeben eines temporären VM-Ladeortes](#) (siehe Seite 40).
7. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-Datenbank einzupflegen.
Optional können Sie mit Hilfe des Befehlszeilendienstprogramms "ca_vcbpopulatedb" Informationen in die ARCserve-Datenbank einpflegen.

Wichtig! Die VMs im ESX-Server-System müssen ausgeführt werden, während Sie dieses Hilfsprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Weitere Informationen finden Sie im *Developer's Setup Guide für VMware Infrastructure SDK 2.5* auf der Website von VMware.

Anhang C: Schützen von Hyper-V-Systemen unter Verwendung des Hyper-V-VSS-Autors

Dieses Kapitel enthält folgende Themen:

- [Übersicht zum Schützen von Hyper-V-VMs unter Verwendung des Hyper-V-VSS-Autors](#) (siehe Seite 121)
- [Erforderliche Komponenten](#) (siehe Seite 122)
- [Konfigurieren von CA ARCserve Backup zur Ermittlung von Hyper-V-VMs](#) (siehe Seite 123)
- [Sichern mit Hilfe des Status "Gespeichert"](#) (siehe Seite 125)
- [Sichern mit Hilfe untergeordneter Partitions-Snapshots](#) (siehe Seite 125)
- [Sichern von Hyper-V-VMs mit Hilfe des Hyper-V-VSS-Autors](#) (siehe Seite 125)
- [Wiederherstellen von Daten an ihrem ursprünglichen Speicherort](#) (siehe Seite 126)

Übersicht zum Schützen von Hyper-V-VMs unter Verwendung des Hyper-V-VSS-Autors

Mit CA ARCserve Backup können Sie Hyper-V-VMs mit Hilfe des Agenten des ARCserve Volumenschattenkopie-Dienstes (VSS) schützen. Der Agent wurde zum Schutz von Microsoft Hyper-V-Daten durch VSS-Autoren unter Verwendung der Technologien des Volumenschattenkopie-Dienstes entwickelt.

In den folgenden Abschnitten wird beschrieben, wie Sie Hyper-V-VMs mit Hilfe des Hyper-V-VSS-Autors konfigurieren, sichern und wiederherstellen. Die beschriebenen Vorgänge sind anwendbar auf Installationen von CA ARCserve Backup für Windows r12 SP1 und können verwendet werden, um Hyper-V-Systeme in Installationen von CA ARCserve Backup für Windows r12.5 zu schützen.

Einschränkungen und Überlegungen

- Sie können Daten nicht auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungsdaten wiederherstellen.
- Sie können keine Sicherungen im gemischten Modus durchführen, die aus wöchentlich erstellten Raw-(vollständigen VM-)Sicherungen und täglichen Sicherungen im Dateimodus bestehen.
- Sie können ausgeschaltete Hyper-V-VMs schützen, wenn Sie das ARCserve Hyper-V-Konfigurationstool ausführen.

Erforderliche Komponenten

Die erforderlichen Komponenten für den Schutz von Hyper-V-Daten mit Hilfe des VSS-Autors sind identisch mit den Standardanforderungen des VSS-Autors. Folgende Anwendungen sind für die Bereitstellung der Hyper-V-VSS-Technologie in Ihrer Umgebung erforderlich:

- CA ARCserve Backup für Windows r12.5
 - CA ARCserve Backup für Windows r12.5 Client Agent für Windows
- Der CA ARCserve Backup Client Agent für Windows muss auf der Partition Null (0) auf dem Hyper-V-Serverrechner installiert sein. Die Partition Null (0) ist für das Betriebssystem des Hosts und die zugehörigen Anwendungen reserviert. Alle anderen Partitionen, zum Beispiel 1, 2 und so weiter, sind für untergeordnete Partitionen oder virtuelle Rechner (virtual machines, kurz VMs) reserviert.

- CA ARCserve Backup für Windows r12.5 Agent for Open Files
- Sie müssen die Lizenz für den Agent for Open Files auf dem Hyper-V-Hostsystem registrieren.

Hinweis: Sie können den Lizenzschlüssel für den Agent for Open Files verwenden, der mit dem Lizenzschlüssel für den Agent für virtuelle Rechner bereitgestellt wurde.

Konfigurieren von CA ARCserve Backup zur Ermittlung von Hyper-V-VMs

Um Sicherungs- und Wiederherstellungsvorgänge mit dem Hyper-V-VSS-Autor auf Rechnern durchführen zu können, müssen Sie CA ARCserve Backup so konfigurieren, dass es den Hyper-V-Server ermittelt.

So konfigurieren Sie CA ARCserve Backup zur Ermittlung von Hyper-V-VMs:

1. Führen Sie je nach Konfiguration Ihrer Sicherungsumgebung eine der folgenden Aktionen durch, und fahren Sie dann mit dem nächsten Schritt fort.
 - Wenn die CA ARCserve Backup-Serverkomponenten auf dem Hyper-V-Serversystem installiert sind, fügen Sie den lokalen Hyper-V-Server zum Sicherungs-Manager hinzu.
 - Wenn die CA ARCserve Backup-Serverkomponenten nicht auf dem Hyper-V-Server installiert sind, fügen Sie den Remote-Hyper-V-Server zum Sicherungs-Manager hinzu, indem Sie die folgenden Schritte durchführen:
 - a. Klicken Sie in der Quellbaumstruktur des Sicherungs-Managers mit der rechten Maustaste auf das Objekt "Windows-Systeme", und wählen Sie im Kontextmenü die Option "Rechner/Objekt hinzufügen" aus.

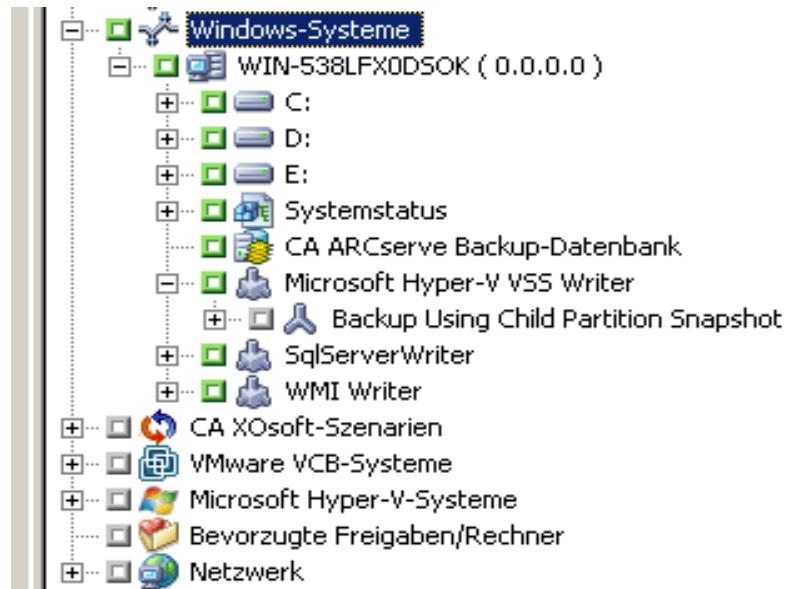


Das Dialogfeld "Agent hinzufügen" wird geöffnet.

- b. Geben Sie im Dialogfeld "Agent hinzufügen" den Namen des Hyper-V-Servers in das Feld "Hostname" oder die IP-Adresse in das Feld "IP-Adresse" ein, und klicken Sie dann auf "Hinzufügen".



Wenn Sie den Namen des Hyper-V-Serversystems zum Sicherungs-Manager hinzugefügt haben, erweitern Sie den Hyper-V-Server, so dass der Microsoft Hyper-V-VSS-Autor so wie im folgenden Bildschirm angezeigt wird.



Sichern mit Hilfe des Status "Gespeichert"

Beim Sichern mit Hilfe des Status "Gespeichert" werden VMs vor dem Sichern in den Status "Gespeichert" gesetzt. Dies erlaubt die Sicherung von Gastbetriebssystemen zu einem bestimmten Zeitpunkt. Es handelt sich dabei um eine statusbehaftete, dateninkonsistente Sicherung. Im Zusammenhang mit VM-Sicherungen gelten hierbei folgende Einschränkungen:

- Die virtuelle Festplatte der Sicherung kann nicht offline geladen werden, um bestimmte Dateien abzurufen.
- Beim Wiederherstellen der gesicherten Daten wird in den Anwendungen auf der VM nicht erkannt, dass es sich um eine Sicherung, Wiederherstellung oder beides handelt.

Hinweis: Weitere Informationen zu diesen Einschränkungen finden Sie auf der Website von Microsoft.

Sichern mit Hilfe untergeordneter Partitions-Snapshots

Beim Sichern mit Hilfe untergeordneter Partitions-Snapshots erstellt der VSS Writer einen Snapshot der Daten des Gastbetriebssystems auf der VM. Mit diesem Verfahren können Sie VMs sichern, auf denen VSS unterstützt wird und die Integrationskomponenten installiert und aktiviert sind. Es handelt sich dabei um eine statusbehaftete, datenkonsistente Sicherung.

Das Sichern mit Hilfe untergeordneter Partitions-Snapshots bietet folgende Vorteile:

- Die virtuelle Festplatte der Sicherung kann offline geladen werden, um bestimmte Dateien abzurufen.
- In den auf der VM installierten VSS-fähigen Anwendungen wird erkannt, dass eine Sicherung oder Wiederherstellung der VM stattfindet. Die Anwendungen sind an der Sicherung oder Wiederherstellung beteiligt, um zu gewährleisten, dass die Anwendungsdaten konsistent bleiben.

Hinweis: Weitere Informationen finden Sie auf der Microsoft-Website.

Sichern von Hyper-V-VMs mit Hilfe des Hyper-V-VSS-Autors

Mit dem Hyper-V-VSS-Autor können Sie VMs sichern, die online oder offline sind. Diese Vorgänge sind für CA ARCserve Backup transparent.

Hinweis: Der Hyper-V-VSS-Autor unterstützt nur vollständige Sicherungen.

In den folgenden Schritten wird beschrieben, wie Sie Hyper-V-VMs mit Hilfe des Hyper-V-VSS-Autors sichern. Informationen zum Sichern von Daten mit Hilfe des VSS-Autors finden Sie im *Benutzerhandbuch von CA ARCserve Backup für Windows Microsoft Volumenschattenkopie-Dienst*.

So sichern Sie Hyper-V-VMs mit Hilfe des Hyper-V-VSS-Autors:

1. Öffnen Sie den Sicherungs-Manager, wählen Sie die Registerkarte "Quelle", und wählen Sie dann das Objekt "Microsoft Hyper-V-VSS-Autor" aus.
Alle Hyper-V-Einstellungen und virtuellen Rechner werden für die Sicherung festgelegt. Wenn Sie nicht alle VMs sichern möchten, erweitern Sie das Objekt "Microsoft Hyper-V-VSS-Autor", (so dass alle Server angezeigt werden) und deaktivieren Sie das Kontrollkästchen neben dem Server, den Sie nicht sichern möchten.
2. (Optional) Klicken Sie mit der rechten Maustaste auf das Objekt "Microsoft Hyper-V-VSS-Autor", und wählen Sie aus dem Kontextmenü die "Writer-Optionen".
3. Klicken Sie auf die Zielregisterkarte, um ein Ziel für die Sicherung festzulegen.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche "Starten", um den Job zu übergeben.

Wiederherstellen von Daten an ihrem ursprünglichen Speicherort

Mit dieser Methode können Sie die Hyper-V-Konfiguration, die Konfigurationen der VMs und die Sicherungsdaten an ihrem ursprünglichen Speicherort wiederherstellen. Die aktuelle Hyper-V-Konfiguration und die Konfigurationen und Daten der VMs werden wieder in den Zustand zurückversetzt, in dem sie sich befanden, als sie gesichert wurden.

Einschränkungen und Überlegungen

- Während des Wiederherstellungsvorgangs können die Hyper-V-Servers entweder online oder offline sein.
- Durch den Hyper-V-VSS-Autor wird sichergestellt, dass die Sicherungsdaten an ihrem ursprünglichen Speicherort ordnungsgemäß wiederhergestellt werden.
- Es ist nicht erforderlich, dass Sie während oder nach Abschluss der Wiederherstellung zusätzliche Schritte durchführen.
- Sobald die Wiederherstellung abgeschlossen ist, kann die VM verwendet werden.

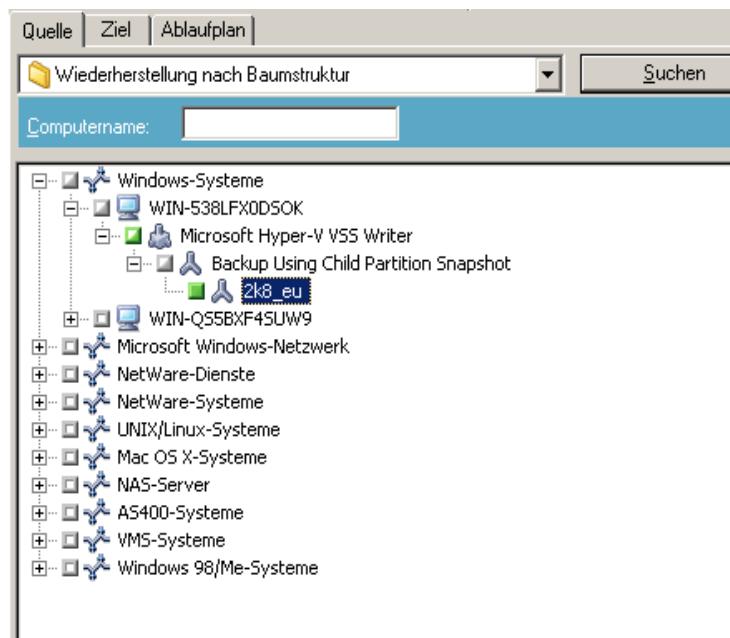
Wenn Sie CA ARCserve Backup verwenden, um Hyper-V-Serverdaten wiederherzustellen, können Sie Daten in den folgenden Szenarien wiederherstellen:

- Sie können Sicherungsdaten von Hyper-V-Servern an ihrem ursprünglichen Speicherort wiederherstellen.
- Sie können VM-Sicherungsdaten an ihrem ursprünglichen Speicherort wiederherstellen.
- Sie können ein Gastbetriebssystem in einer VM an seinem ursprünglichen Speicherort wiederherstellen.

Hinweis: Informationen zur Verwendung des VSS-Autors finden Sie im *Benutzerhandbuch von CA ARCserve Backup für Windows Microsoft Volumenschattenkopie-Dienst*.

So stellen Sie Daten an ihrem ursprünglichen Speicherort wieder her:

1. Öffnen Sie den Wiederherstellungs-Manager, und führen Sie einen der folgenden Schritte durch:
 - Wählen Sie im Kontextmenü die Methode "Wiederherstellung nach Baumstruktur", erweitern Sie das Objekt "Windows-Systeme", navigieren Sie zum Microsoft Hyper-V-VSS-Autor, und geben Sie eine oder mehrere VMs zur Wiederherstellung an.



- Wählen Sie im Kontextmenü "Wiederherstellung nach Sitzung", wählen Sie dann eine Sitzung aus und geben sie diese zur Wiederherstellung an.

2. Klicken Sie auf die Registerkarte "Ziel".

Klicken Sie auf die Option "Dateien am ursprünglichen Speicherort wiederherstellen".

3. Klicken Sie in der Symbolleiste auf die Schaltfläche "Starten", um den Job zu übergeben.

Wenn die Wiederherstellung abgeschlossen ist, werden die wiederhergestellten VMs als "Gespeichert" ausgewiesen. Mit anderen Worten, die Online-Wiederherstellung versetzt die VMs in einen Offline-Status, wenn die Wiederherstellung abgeschlossen ist. Sie müssen die VMs anschließend manuell starten, um sie in einen Online-Status zu versetzen.

Index

A

Agent

- Deinstallieren - 55
- Installieren - 29
- Lizenzierung - 21
- Pre-Flight Check-Hilfsprogramm - 74
- ARCserve Hyper-V-Konfigurationstool - 49
- ARCserve VMware-Konfigurationstool - 36
- ARCserve-Servername, angeben - 34

C

- ca_msmpopulatedb, Hilfsprogramm - 52
- ca_vcipopulatedb-Hilfsprogramm
 - Argumente - 41
 - Rückgabecodes - 47

D

- Durchsuchen
 - Sicherungs-Volumes - 59
 - Wiederherstellungssitzungen - 76

E

- Einpflegen von Informationen in die ARCserve-Datenbank
 - Verwenden der Befehlszeile - 41, 52
 - Verwenden des ARCserve Hyper-V-Konfigurationstools - 49
 - Verwenden des ARCserve-Konfigurationstools für VMware - 36
- Einschränkungen - 91
- Empfehlungen - 57
- Erstellen einer Konfigurationsdatei - 43

F

- Filtern von Sicherungsdaten - 75

I

- Installieren
 - Standard - 29

K

- Konfigurieren des Agenten - 29
- Kontaktinformationen, Technischer Support - 5

- Kunden-Support, Kontaktieren - 5

L

- Lizenzierung - 21

P

- Pre-Flight Check-Hilfsprogramm - 74

R

- Rückgabecodes - 47

S

- Sichern von Daten - 71
- Sichern von VMs - 13
- Sicherungsmodi
 - Dateimodus - 61
 - Gemischter Modus - 12, 17, 61, 65, 68, 75
 - Raw-Modus - 61
 - Sicherungsmodi, Infos zu - 61
- Support, kontaktieren - 5

T

- Technischer Support, kontaktieren - 5

V

- VCB-Einschränkungen - 16
- Verwalten von Virtual Machines - 12
 - Hyper-V-Systeme - 17
 - VMware-Systeme - 12
- Verwenden des Sicherungs-Proxysystems - 109
- Voraussetzungen für die Installation - 28