CA ARCserve® Backup for Windows

Agent for Virtual Machines Guide
r15

CA Product References

This document references the following CA products:

- BrightStor® Enterprise Backup
- CA Antivirus
- CA ARCserve® Assured Recovery™
- CA ARCserve® Backup Agent for Advantage™ Ingres®
- CA ARCserve® Backup Agent for Novell Open Enterprise Server for Linux
- CA ARCserve® Backup Agent for Open Files on NetWare
- CA ARCserve® Backup Agent for Open Files on Windows
- CA ARCserve® Backup Client Agent for FreeBSD
- CA ARCserve® Backup Client Agent for Linux
- CA ARCserve® Backup Client Agent for Mainframe Linux
- CA ARCserve® Backup Client Agent for NetWare
- CA ARCserve® Backup Client Agent for UNIX
- CA ARCserve® Backup Client Agent for Windows
- CA ARCserve® Backup Enterprise Option for AS/400
- CA ARCserve® Backup Enterprise Option for Open VMS
- CA ARCserve® Backup for Microsoft Windows Essential Business Server
- CA ARCserve® Backup for Windows
- CA ARCserve® Backup for Windows Agent for IBM Informix
- CA ARCserve® Backup for Windows Agent for Lotus Domino
- CA ARCserve® Backup for Windows Agent for Microsoft Exchange Server
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint Server
- CA ARCserve® Backup for Windows Agent for Microsoft SQL Server
- CA ARCserve® Backup for Windows Agent for Oracle
- CA ARCserve® Backup for Windows Agent for Sybase
- CA ARCserve® Backup for Windows Agent for Virtual Machines
- CA ARCserve® Backup for Windows Disaster Recovery Option
- CA ARCserve® Backup for Windows Enterprise Module

- CA ARCserve® Backup for Windows Enterprise Option for IBM 3494
- CA ARCserve® Backup for Windows Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Windows Enterprise Option for StorageTek ACSLS
- CA ARCserve® Backup for Windows Image Option
- CA ARCserve® Backup for Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup for Windows NDMP NAS Option
- CA ARCserve® Backup for Windows Serverless Backup Option
- CA ARCserve® Backup for Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup for Windows Tape Library Option
- CA ARCserve® Backup Patch Manager
- CA ARCserve® Backup UNIX and Linux Data Mover
- CA ARCserve® D2D
- CA ARCserve® High Availability
- CA ARCserve® Replication
- CA VM:Tape for z/VM
- CA 1® Tape Management
- Common Services™
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM:Operator®

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At CA ARCserve Backup Support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- New chapter--Populating the CA ARCserve Backup Database.

- Removed appendix--Protecting Hyper-V Systems Using the Hyper-V VSS Writer. For more information, see the *Administration Guide*.

- Removed content--ca_vcbpopulatedb Command Line Utility, syntax, usage, and examples. For more information, see the *Command Line Reference Guide.*

- Removed content--ca_msvmpopulatedb Command Line Utility, syntax, usage, and examples. For more information, see the *Command Line Reference Guide*.

Contents

Chapter 4: Backing Up Data   67

Chapter 5: Restoring Data   91

Index   **145**

Chapter 1: Introducing the Agent

This section contains the following topics:

Introduction

CA ARCserve Backup is a comprehensive storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, business-critical applications, and network clients.

Among the agents CA ARCserve Backup offers is the CA ARCserve Backup Agent for Virtual Machines. The agent lets you protect virtual machines (VMs) running the following systems:

- **VMware ESX/ESXi Server and VMware vCenter Server--**VMware provides you with mechanisms called VMware Consolidated Backup (VCB) and Virtual Disk Development Kit (VDDK) that integrate with VMware ESX/ESXi Server and VMware vCenter Server. VCB and VDDK let you protect Virtual Machine (VM) files and data. Using VCB or VDDK you can offload VM backup activity to a dedicated backup proxy system, and then use the backup and restore functionalities provided by CA ARCserve Backup to protect the VMs.

- **VMware vSphere--**VMware vSphere is a virtualization toolkit that lets you integrate the latest versions of VMware vCenter Server, VMware VCB, and VMware VDDK with CA ARCserve Backup.

- **Microsoft Hyper-V--**Microsoft Hyper-V is a component that is included with Windows Server 2008 operating systems. Hyper-V is hypervisor-based technology that lets you run multiple operating systems independently within the Windows Server 2008 system. CA ARCserve Backup lets you back up and restore data contained within the guest operating systems and Windows Server 2008 operating systems.

How the Agent Protects VMware Systems Using VCB

The agent lets you back up data and works best under the following circumstances:

- You want to reduce resource restraints in the VMware ESX Host system.

  Note: VMware ESX/ESXi is an application that manages system, storage, and network resources in multiple VM environments.

- Your environment consists of VMs residing on different types of data stores.

- You need to restore data at the file level or raw (full VM) level.

VCB lets you perform the following administrative tasks:

- Take a snapshot of a VM and mount or export the backup data to one or more backup proxy systems and remove the load from the VMware ESX Host system.

- Perform file level backups and restores of a VM running any VMware-supported Windows-based operating system.

- Perform raw (full VM) level backups and restores of a VM running any VMware-supported operating system.

- Perform LAN-free (Local Area Network) backups, if the VMs reside on a SAN.

- Back up a VM, regardless of its power state.

- Reduce administration overhead by centralizing backup management on backup proxy systems. You do not need to deploy agents on the VMs.

  Note: This capability requires you to install the Agent for Virtual Machines on the backup proxy system.

How CA ARCserve Backup Leverages VCB to Protect Your VMware Environment

The agent lets you perform raw VM (full VM), file level VM backups, and mixed-mode VM backups using a backup proxy system.

The following diagram illustrates the network architecture for backing up VMware images or files using a backup proxy system:

Backing up VMware Environments Via an External Backup Proxy System Using CA ARCserve Backup Agent for Virtual Machines

VM Disk Files Stored in LUN:
- Agent for Virtual Machines on all VMs

iSCSI / SAN LUN

10/100 MB or GB Ethernet Network

ESX Server:
- VMs residing on iSCSI/ SAN LUN
- VM disk files residing on local storage

Backup Proxy:
- VMware VCB Framework
- Agent for Virtual Machines
- Client Agent for Windows
- Microsoft .Net Framework 2.0 or higher

Important! The SAN/iSCSI LUNS containing the VMs must be accessible to the backup proxy system and the ESX/ESXi Server system.

Note: The agent supports backing up and restoring VMs that are configured locally to the ESX/ESXi Server system.

Backup Server:
- CA ARCserve Backup Server

1. The CA ARCserve Backup primary or member server communicates with the Agent for Virtual Machines that is running on the backup proxy system while the backup job is running. The agent then takes a snapshot of the VM and mounts or exports the snapshot to the backup proxy system, by default, into the Client Agent for Windows installation directory.

2. If the backup mode specifies Allow File Level Restore (see page 70), CA ARCserve Backup creates catalog files representing the volumes on the VM.

3. CA ARCserve Backup then backs up the VM and the catalogs to the target backup media.

Note: For information about changing the default mount path, see Specify a Temporary VM Mount Location (see page 52).

When you deploy this architecture in your environment, consider the following:

■ The agent must be licensed on the CA ARCserve Backup primary or stand-alone server.

■ The agent must be installed on all VMs where you want to perform file level restores to the guest operating system.

   Note: For more information, see Where to Install the Agent (see page 26).

■ Microsoft .NET Framework Version 2.0 or higher must be running on the backup proxy system.

■ If the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host and the backup proxy system and have the same LUN number assigned.

   Note: The above limitation only applies to VCB versions 1.0, 1.0.1, and 1.0.2. VCB versions 1.0.3 and later do not require a consistent LUN number.

   The LUN in the backup proxy system should not be signed.

   Note: To obtain the latest information about this configuration, see the VMware VCB documentation.

■ The raw (full VM) level backup method makes a copy of the entire disk and the configuration files associated with a specific VM, letting you restore the entire VM.

   The raw level backup can be used to recover VMs in the event a disaster occurs or there is total loss of the original VM.

■ The file level backup method lets you make a copy of individual files contained on the disk in a VM, which can include all files.

   You can use this method for situations that involve restoring files that were corrupted or accidentally deleted.

- The mixed mode backup method lets you perform GFS and rotation backup jobs that consist of weekly full backups in full VM (raw) mode and daily incremental and differential backups in file mode in a single backup job.

  You can use this method to back up data at raw (full VM) efficiency and restore data at file level granularity.

- When you submit a backup job, you can perform a raw (full VM) level or file level backup of the VM. You must specify the primary or member server where the job will execute.

  Important! To perform file level backups of a VM, a VMware-supported Windows operating system must be installed on the VM.

How the Agent Protects VMs that Reside on Local Storage and a SAN

The CA ARCserve Backup Agent for Virtual Machines lets you protect VMware-based data that resides on local storage and on a storage area network (SAN). For all data store types, the VMs must be accessible from the backup proxy system.

The list that follows describes the environment configuration requirements for each of the data store types:

- **SAN, iSCSI Data Stores--**The backup proxy system must be attached to the same disk where the VM resides and must be attached using the same SAN, iSCSI infrastructure.

- **Local Storage Data Stores--**The VMs must reside on disks that are attached directly to the VMware ESX Host system. With local storage environments, the backup proxy system should be able to communicate with the VMware ESX Host system via the LAN.

Note: The terms SAN/iSCSI are used to denote shared storage between Proxy and VMware ESX Host systems. Wherever SAN is mentioned is also applicable to iSCSI environments where Disks are shared using iSCSI infrastructure.

When you implement the agent with VI 2.5, the process of populating the CA ARCserve Backup database using the ca_vcbpopulatedb Command Line Utility or the ARCserve VMware Configuration Tool lets CA ARCserve Backup configure the agent to detect the types of VM data stores in your environment.

However, if the VMs reside on a SAN and the backup proxy system is not attached to the same SAN, CA ARCserve Backup will try to back up the VMs using the information about the VMs contained in the following file located on the backup proxy system:

C:\Program Files\CA\ARCserve Backup Client Agent for Windows\VMDatastoreTypes.ini

If CA ARCserve Backup cannot secure the required information about the VMs from the VMDatastoreTypes.ini file, CA ARCserve Backup then proceeds with the backup using Network Block Device (NBD) communication.

VCB Limitations

When you use VCB in your environment, consider the following limitations:

- You cannot back up VMs with virtual disks that are physically compatible Raw Device Maps (RDM), Independent - persistent and Independent non-persistent disks.

- You must assign a drive letter to all volumes in a VM that you want to back up and have the capability to browse in the mount directory. If a drive letter is not assigned to the volume, VCB prevents you from browsing the mounted volume in the mount directory. As a result, CA ARCserve Backup cannot complete the backup and statuses the job as incomplete.

- If the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

  Note: The above limitation only applies to VCB versions 1.0, 1.0.1, and 1.0.2. VCB versions 1.0.3 and later do not require a consistent LUN number.

  The LUN in the backup proxy system should not be signed.

  Note: To obtain the latest information about this configuration, see the VMware VCB documentation.

- To back up an individual file or directory, a VMware-supported Windows-based operating system must be running on the VM.

- VCB supports mounting up to 60 concurrent VM volumes.

Examples: Mounting Concurrent VMware Volumes

- 60 VMs with one C:\ drive

- 30 VMs with two VM volumes: one C:\ drive and one D:\ drive

■ VCB does not support the use of non-English, multibyte characters. Paths and registry strings that consist of non-English, multibyte characters may not display properly.

Note: For information about how to install VCB, set up VCB, and the limitations of using VCB, see the VMware Virtual Machine Backup Guide on the VMware website.

How the Agent Protect VMware vSphere Systems Using VDDK

CA ARCserve Backup lets you protect VMware vSphere systems using VDDK.

This section contains the following topics:

Introduction to Integrating with VMware vSphere

CA ARCserve Backup Agent for Virtual Machines integrates with the latest version of VMware Virtual Infrastructure named vSphere. This capability lets you protect virtual machines (VMs) that reside in vSphere environments (for example, the VMs reside in ESX Server 4.0 systems and vCenter Server 4.0 systems). The agent facilitates protecting VMs using VMware Virtual Consolidated Backup Framework (VCB) 1.5 Update 1 or later, and VMware Virtual Disk Development Kit (VDDK) 1.1 or later.

VDDK lets you access VM disks remotely on ESX Server systems without exporting the disks to the backup proxy system. Integrating with VDDK provides you with an alternative approach to using VCB Framework to back up VMs. This approach can be used only on ESX Server 4.0 systems, ESX Server 3.5 systems, vCenter 4.0 systems, and VirtualCenter Server 2.5 systems.

VMware Virtual Disk Development Kit is a collection of APIs and management tools that let you create, manage, and access virtual storage systems. VMware VDDK is supported on x86 and x64 versions of Windows and Linux operating systems.

The primary advantages of using VDDK are as follows:

- VDDK eliminates the requirement to store VM snapshots on the backup proxy system. Using VDDK, CA ARCserve Backup can transfer data for all raw (full VM) backups directly from the ESX Server datastores to the backup media.

   Note: CA ARCserve Backup stores the sectors corresponding to disk and filesystem metadata on the backup proxy system when processing raw (full VM) backups with the Allow file level restore option specified.

- VDDK minimizes the dependency on VMware tools. Using VDDK, CA ARCserve Backup does not require that VMware Virtual Consolidated Backup (VCB) be installed on the backup proxy systems. In addition, VMware Converter is not required to recover VMs. VDDK provides more control and improved reporting for VM backup and recovery operations.

Note: The latest version of ESX Server is VMware vSphere 4.0 Update 1. The latest version of VMware vCenter Server is VMware vCenter Server 4.0 Update 1.

There are two approaches that you can use to protect your VM environment:

- Through the ESX Server or ESXi Server host system--A single host can manage only the VMs contained within the host system. This approach uses VCB Framework and VDDK to perform backup and restore operations.

- Through the vCenter Server system--A vCenter Server system can manage VMs that are distributed over many ESX Server and ESXi Server host systems. This approach uses VCB Framework and VDDK to perform backup and restore operations.

How to Use the Agent with VMware vSphere

Using VMware vSphere may affect the manner in which you plan your backup infrastructure.

Without VMware vSphere, CA ARCserve Backup integrates with VMware Virtual Infrastructure (version 2.0 and 2.5) using VMware VCB Framework tools to back up VM data. With VCB Framework you must designate a Windows server to function as a backup proxy system. The backup proxy system requires a large amount of free disk space to stage the snapshot images of the VMs that you are backing up.

To recover a full VM (for example, to recover a VM from a disaster), VMware Converter must be installed on the backup proxy system. VMware provides a variety of converter tools. However, CA ARCserve Backup supports using only stand-alone versions of the converter tools.

Note: CA ARCserve Backup cannot recover VMs using enterprise versions of VMware Converter.

Integrating with VMware vSphere lets you perform the following operations:

■ Back up VMs on all currently supported versions of VMware ESX Server and VMware VirtualCenter Server using VMware VCB Framework.

■ Back up VMs that reside on ESX Server 4.0 systems or other hosts that are managed by vCenter Server 4.0 using VDDK.

■ Back up VMs that reside on ESX Server 4.0 systems or other hosts that are managed by vCenter 4.0 using VCB Framework 1.5 Update 1.

■ Back up and recover VMs that reside on ESX Server version 3.5 and version 4.0 systems, VirtualCenter Server version 2.5 and version 4.0 systems, or both, using a new approach. The new approach lets you use a combination of the APIs provided by VMware vSphere Web Service SDK and VMware VDDK, and is recommended by VMware.

Examples: How to Use the Agent with VMware vSphere

■ Decreased hardware requirements--A backup proxy system is not required to facilitate backing up and recovering VMs. You can back up and recover VMs from the primary server or a member server without incurring additional overhead on the CA ARCserve Backup server.

■ Eliminates the Temporary Mount location--To back up VMs in a VMware backup environment using VCB tools, a mount location with a large amount of free disk space is required on the backup proxy system. The amount of free disk space on the backup proxy system must be as large as the total size of all VMs that you can back up concurrently using multistreaming when performing raw (full VM) backups with the Allow file level restore option specified. The new approach lets CA ARCserve Backup eliminate the need to store the VM backups on the backup proxy system. As a result, the agent lets you free valuable system resources and disk space on the backup proxy system.

■ Decreased software dependency--You do not need to install VCB and VMware Converter on the backup proxy system. This requirement frees valuable system resources and disk space on the backup proxy system. Using the agent with VMware vSphere requires less software to manage your VM backups and restores. If you use the new approach with VMware vSphere Web Services SDK and VDDK, you must install only VDDK on the backup proxy system to perform backup and recovery operations. This requirement improves VM reporting and simplifies the process of managing your VMs because there are fewer components that can fail.

How vSphere Integrates with Previous Releases of the Agent

In addition to the protection provided by this release of the agent, you can perform the operations that follow:

- Back up file level data and raw (full VM) data using CA ARCserve Backup r12.5 with VMware VDDK in an environment that is running older version of ESX Server or VirtualCenter Server.

- Restore raw (full VM) data, file level data, and recover VMs using data that was backed up with CA ARCserve Backup r12, CA ARCserve Backup r12 SP1, or CA ARCserve Backup r12.5 using VDDK.

Note: For information about that tasks that you can perform using vSphere, see Tasks You Can Perform Using vSphere.

How the Agent Protects Hyper-V Systems

The agent lets you back up data and it works best when you need to restore data at the file level, raw (full VM) level, or mixed level.

Microsoft Hyper-V lets you perform the following administrative tasks:

- Perform file level backups and restores of a VM running any Hyper-V supported Windows-based operating system.

- Perform raw (full VM) level backups and restores of a VM running any Hyper-V supported operating system.

- Back up a VM, regardless of its power state.

- Reduce administration overhead by centralizing backup management on Hyper-V host systems.

How CA ARCserve Backup Leverages Hyper-V to Protect Your Environment

The agent lets you perform raw VM (full VM), file level VM backups, and mixed-mode VM backups.

The following diagram illustrates the network architecture for backing up VM images or files.
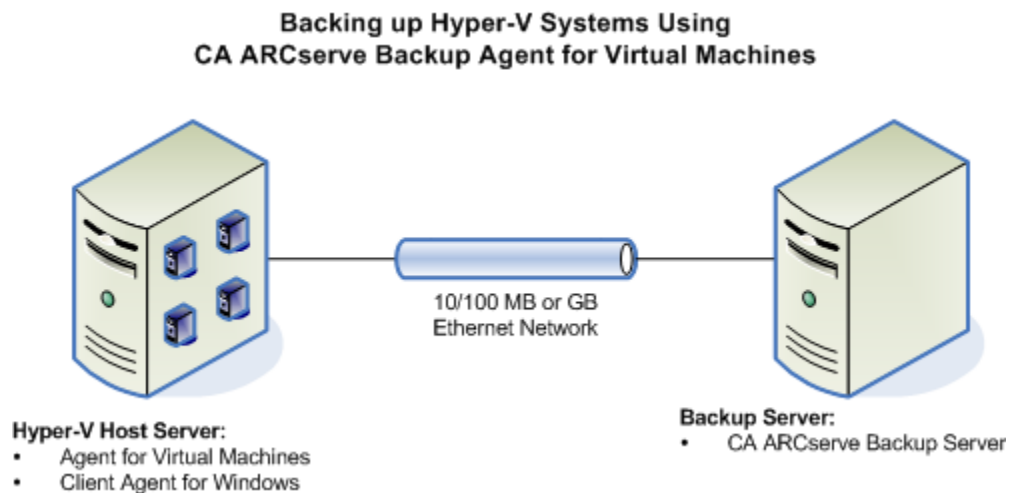
**Backing up Hyper-V Systems Using
CA ARCserve Backup Agent for Virtual Machines**

10/100 MB or GB
Ethernet Network

Hyper-V Host Server:
- Agent for Virtual Machines
- Client Agent for Windows

Backup Server:
- CA ARCserve Backup Server

When you deploy this architecture in your environment, consider the following:

- The agent must be licensed on the CA ARCserve Backup primary or stand-alone server.

- The agent must be installed on all VMs where you want to perform file level restores to the guest operating system.

  Note: For more information, see Where to Install the Agent (see page 26).

- The raw (full VM) level backup method makes a copy of the entire disk and configuration files associated with a specific VM, letting you restore the entire VM.

  The raw level backup can be used to recover VMs in the event a disaster occurs or there is total loss of the original VM.

- The file level backup method lets you make a copy of individual files contained on the disk in a VM, which can include all files.

  You can use this method for situations that involve restoring files that were corrupted or accidentally deleted.

- When you submit a backup job, you can perform a raw (full VM) level or file level backup of the VM. You must specify the primary or member server where the job will execute.

  Important! To perform file level backups of a VM, a Hyper-V supported Windows operating system must be installed on the VM.

Supported CA ARCserve Backup Functionalities

The agent supports the CA ARCserve Backup functionalities that follow:

- Multi-streaming--CA ARCserve Backup lets you submit jobs using multi-streaming at the VM level.

- Staging--CA ARCserve Backup lets you submit VM backup jobs to disk staging and tape staging devices.

    You can restore data at file level granularity directly from the staging device and from final destination media, such as tape media.

- Deduplication--CA ARCserve Backup lets save disk space by eliminating blocks of redundant backup data.

- Multiplexing--CA ARCserve Backup lets you submit jobs using multiplexing.

- GFS and rotation backups--CA ARCserve Backup lets you submit GFS and rotation backup jobs.

- Makeup Jobs:

    - Raw (full VM) backups--CA ARCserve Backup restarts failed jobs at the VM level.

    - Incremental and differential backups--CA ARCserve Backup restarts failed jobs at the volume level.

- Compression--CA ARCserve Backup lets you compress VM backup data on the agent system or the CA ARCserve Backup server.

- Encryption--CA ARCserve Backup lets you encrypt VM backup data on the agent system or the CA ARCserve Backup server.

- CRC verification--CA ARCserve Backup lets you check for data integrity by supporting CRC verification on VM backup data.

- Spanned, Striped, Mirrored, and RAID-5 volumes--CA ARCserve Backup lets you protect VM data that resides in spanned, striped, mirrored, and RAID-5 volumes.

Note: For more information about the above-described functionalities, see the online help or the *Administration Guide*.

Backup and Restore Limitations on Virtual Machines

The limitations that follow affect VM backup and restore operations:

■ The VMs in the VMware ESX Host must be in a running state when you populate the CA ARCserve Backup database.

If the VMs are not in a running state, ARCserve VMware Configuration Tool (ca_vcbpopulatedb.exe) and ARCserve Hyper-V Configuration Tool (ca_msvmpopulatedb.exe) cannot populate the CA ARCserve Backup database with accurate data, and you cannot accurately browse the VMs in VMware ESX Host systems.

■ You must run ARCserve VMware Configuration Tool (ca_vcbpopulatedb.exe) and ARCserve Hyper-V Configuration Tool (ca_msvmpopulatedb.exe) after you add, remove, or change volumes in a VM or a VM in the host system.

Failure to do so can result in inaccurate VM volume data in the CA ARCserve Backup database, and failed backup jobs will occur at runtime.

■ CA ARCserve Backup does not provide command line support for VM backup and restore operations. For example, ca_backup and ca_restore.

You must use the Backup Manager and Restore Manager to perform all VM based backups and restores.

■ You cannot use the Restore by Media method to restore file level and raw (full VM) level backup data.

■ The Compare Utility does not support comparing VM backup sessions.

When you try to perform a Compare operation on VM sessions, CA ARCserve Backup performs a Scan operation instead of a Compare operation.

■ The agent does not support the following global backup options:

– Delete files after backup job

– Open file retry

Note: For more information about global backup options, see the *Administration Guide*.

■ Due to limitations in the physical and logical mapping of the volumes in the CA ARCserve Backup database, the Merge Utility does not support performing a sequential merge.

If you need to merge data about VM sessions into the CA ARCserve Backup database, you can merge the catalog data.

■ The agent does not support specifying a VM Mount Path that contains non-English language-based characters. Garbled characters will appear when the path contains non-English language-based characters.

Chapter 2: Installing and Configuring the Agent

This section contains the following topics:

How to License the Agent

The CA ARCserve Backup Agent for Virtual Machines uses a count-based licensing method. You must register one CA ARCserve Backup Agent for Virtual Machines license for each host system and VM that you are protecting using CA ARCserve Backup. You must register the licenses for the agent on the CA ARCserve Backup primary server or stand-alone server.

Examples: How to License the Agent

The following list describes typical installation scenarios:

- Your environment consists of one Hyper-V host with three guest operating systems. You must register four licenses (1 host system + 3 VMs) on the CA ARCserve Backup server.

- Your environment consists of one VMware ESX Host system with three guest operating systems. You must register four licenses (1 backup proxy system + 3 VMs) on the CA ARCserve Backup server.

■ Your environment consists of two Hyper-V host systems. Each Hyper-V host system contains three guest operating systems. You must register eight licenses (1 host system + 3 VMs, 1 host system + 3 VMs) on the CA ARCserve Backup server.

■ Your environment consists of one VM host system (VMware ESX Host or Hyper-V Server) with two VMs. You require only raw (full VM) backups and will not specify the Allow file level restore option. In this scenario, you must install the agent only on the host system. However, one license for each VM must be registered on the CA ARCserve Backup server. Therefore, you must register three licenses (1 host system + 2 VMs) on the CA ARCserve Backup server.

Note: For more information about backup modes, see How Global and Local Backup Modes Work (see page 70).

Where to Install the Agent

As a general best practice, you must install the agent on the following locations:

■ VMware environments--on the backup proxy systems and in the VMs that you want to protect.

■ Hyper-V environments--on the Hyper-V host systems and in the VMs that you want to protect.

However, the backup mode that you require for your backups determines where you must install the agent.

Note: For more information about backup modes, see How Global and Local Backup Modes Work (see page 70).

The following table identifies the type of backup modes that you require and where you must install the agent.

Backup Mode Specified	Hyper-V Host System	VMware Backup Proxy System	Hyper-V VM	VMware VM
File mode	Required	Required	Required	Not required
Raw (full VM) mode and Allow file level restore *is not* specified	Required	Required	Not required	Not required
Raw (full VM) mode and Allow file level restore *is* specified	Required	Required	Required	Required

Backup Mode Specified	Hyper-V Host System	VMware Backup Proxy System	Hyper-V VM	VMware VM
Mixed mode and Allow file level restore *is not* specified	Required	Required	Required	Not required
Mixed mode and Allow file level restore *is* specified	Required	Required	Required	Required

Be aware of the following considerations:

- You must register one license for each VM that you are protecting with CA ARCserve Backup. All licenses must be registered on the primary server or stand-alone server.

- The agent requires the CA ARCserve Backup Client Agent for Windows. You must install the Client Agent for Windows in all locations where you installed the Agent for Virtual Machines.

Backup Mode and Installation Matrix

The backup mode that you can use to protect VM data is dependent upon the location of where you install the Agent for Virtual Machines. The tables that follow describe the backup modes that you can use and the location where you must install the agent.

For more information about backup modes, see How Global and Local Backup Modes Work (see page 70).

VMware Systems

Key:

- **Raw #** backup mode is a Raw (full VM) mode backup and the Allow file level restore option is specified.

- **Mixed #** backup mode is a Mixed mode backup and the Allow file level restore option is specified.

- The term **agent** refers to the Agent for Virtual Machines.

- The phrase **Client Agent** refers to the Client Agent for Windows.

  Important! The Client Agent for Windows is a prerequisite component for the Agent for Virtual Machines.

Question	Raw	File	Raw #	Mixed as a Global Option		Mixed # as a Global Option	
				Using VCB/VDDK	Using the Client Agent	Using VCB/VDDK	Using the Client Agent
Do I need to install the agent on the VM/guest OS?	No	No	Yes	No	Yes	Yes	Yes
Can I perform backups using this backup mode without installing the agent on the VM/Guest OS?	Yes	Yes	No	Yes	No	See **Note 1**.	No

Question	Raw	File	Raw #	Mixed as a Global Option		Mixed # as a Global Option	
				Using VCB/VDDK	Using the Client Agent	Using VCB/VDDK	Using the Client Agent
Can I perform backups using this backup mode with the agent installed on the VM/Guest OS?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Can I perform restores from sessions that were backed up using this backup mode with the agent installed on the VM/Guest OS?	No	Yes	Yes	See **Note 2**.	Yes	Yes	Yes
Can I recover VMs from data that was backed up using this mode with the agent installed on the VM/Guest OS (see **Note 3**)?	No	No	No	No	No	No	No

Note 1: A Raw mode backup with the Allow file level restore option specified finishes with a status of Complete. Incremental and differential backups will complete successfully.

Note 2: The VMware Converter tool must be installed on the VM to allow CA ARCserve Backup to execute Recover VM operations. VMware Virtual Consolidated Backup (VCB) is not required to restore VM data and to perform Recover VM operations.

Note 3: CA ARCserve Backup executes Recover VM operations using the VMware Converter tool, where the tool is installed on the backup proxy system. You do not need to install the Agent for Virtual Machines or the Client Agent for Windows on the VM to perform Recover VM operations.

Hyper-V Systems

Key:

- **Raw #** backup mode is a Raw (full VM) mode backup and the Allow file level restore option is specified.

- **Mixed #** backup mode is a Mixed mode backup and the Allow file level restore option is specified.

- The term **agent** refers to the Agent for Virtual Machines.

- The phrase **Client Agent** refers to the Client Agent for Windows.

  Important! The Client Agent for Windows is a prerequisite component for the Agent for Virtual Machines.

Question	Raw	File	Raw #	Mixed	Mixed #
Do I need to install the agent on the VM/guest OS?	No	Yes	Yes	Yes	Yes
Can I perform backups using this backup mode without installing the agent on the VM/Guest OS?	Yes	No	No	No	No
Can I perform backups using this backup mode with the agent installed on the VM/Guest OS?	Yes	Yes	Yes	Yes	Yes
Can I perform restores from sessions that were backed up using this backup mode with the agent installed on the VM/Guest OS?	No	Yes	Yes	See **Note 1**.	Yes
Can I recover VMs from data that was backed up using this mode with the agent installed on the VM/Guest OS (see **Note 2**)?	No	No	No	No	No

Note 1: Yes, you can perform restores from sessions that were backed up using Mixed mode from only incremental and differential backup sessions. You cannot perform restores from sessions that were backed up using Mixed mode from the first full backup session.

Note 2: You do not need to install the Agent for Virtual Machines or the Client Agent for Windows on the Hyper-V VMs. CA ARCserve Backup manages the recovery of Hyper-V VMs when you install the Agent for Virtual Machines on the Hyper-V Host system.

Best Practices for Installing and Configuring the Agent for Virtual Machines

Consider using the best practices that follow to install the CA ARCserve Backup Agent for Virtual Machines.

Task	VMware Systems	Hyper-V Systems
Required components	**CA ARCserve Backup** Install the CA ARCserve Backup Server components on the system designated to function as a primary server or a stand-alone server. **Agent for Virtual Machines** Install the agent on the system that will function as the backup proxy system. The best practice is to allow the backup server to function as the backup proxy system. However, if you feel that this configuration will impose performance issues on the server, install the agent on a remote system and allow it to function as the backup proxy system. **Note:** You must register the agent license on the CA ARCserve Backup server. **VMware VCB Framework/VDDK** Ensure that VMware VCB Framework or VDDK is installed on the system that will function as the backup proxy system. **Note:** As a best practice, you should install VCB Framework and VDDK on the backup proxy system. This configuration lets you perform full VM backups and restores using VDDK, and file mode backups using VCB Framework.	**CA ARCserve Backup** Install the CA ARCserve Backup Server components on the system designated to function as a primary server or a stand-alone server. **Agent for Virtual Machines** Install the agent on the Hyper-V host system. **Note:** You must register the agent license on the CA ARCserve Backup server.

Consider using the best practices that follow to configure the CA ARCserve Backup Agent for Virtual Machines and to back up data.

Task	VMware Systems	Hyper-V Systems
Configuration	Populate the CA ARCserve Backup database using ARCserve VMware Configuration Tool on the backup proxy system. For more information, see Populate the Database Using ARCserve VMware Configuration Tool (see page 54).	Populate the CA ARCserve Backup database using ARCserve Hyper-V Configuration Tool on the Hyper-V host system. For more information, see Populate the Database Using ARCserve Hyper-V Configuration Tool (see page 59).
	Deploy the Agent for Virtual Machines using Agent Deployment. For more information, see Deploy the Agent to VMs Using Agent Deployment (see page 34).	Deploy the Agent for Virtual Machines using Agent Deployment. For more information, see Deploy the Agent to VMs Using Agent Deployment (see page 34).
Backup mode	Accept the default backup mode, which includes the following options specified: ■ Mixed mode backup ■ Allow file level restore	
Backup options--Multistreaming	To ensure that backup jobs complete efficiently, you should use the Multistreaming option and specify a maximum of four VMs in a backup job. For information about Multistreaming, see the *Administration Guide.*	
Backing up data	Follow the procedure described in Back Up Data (see page 67).	

Installation Prerequisites

Before installing the agent, you must complete the prerequisite tasks that follow:

■ Ensure that your system meets the minimum requirements needed to install the agent.

   For a list of requirements, see the readme file.

■ Ensure that you have an Administrator profile or a profile with the rights to install software.

■ Ensure that you know the user name and password of the system where you are installing the agent.

Prerequisite Components

The agent requires the following prerequisite components.

■ For VMware environments, ensure that Microsoft .NET Framework Version 2 or higher is installed and running on the backup proxy system.

■ For VMware environments, ensure that VMware VCB Framework is installed on the backup proxy system.

■ To integrate with VMware vSphere, the components listed below must be installed on the backup proxy systems:

– This release of CA ARCserve Backup Agent for Virtual Machines.

– VMware Virtual Disk Development Kit (VDDK) 1.1 or later, VMware VCB Framework 1.5 Update 1, or both.

Note: As a best practice, you should always install the latest version of VMware VDDK and VMware VCB. The latest version of VMware VDDK is 1.1.1.

Supported Configurations to Integrate with VMware vSphere

You can integrate the agent with VMware vSphere on the following operating systems when VMware VCB Framework is installed on the backup proxy system:

■ Windows Server 2003 x64

■ Windows Server 2003 x86

■ Windows Server 2008 x64

■ Windows Server 2008 x86

You can integrate the agent with VMware vSphere on the following operating systems when VMware VDDK is installed on the backup proxy system:

■ Windows Server 2003 x64

■ Windows Server 2003 x86

How to Install and Configure the Agent

There are two methods that you can use to install the agent:

- Install the agent while you are installing CA ARCserve Backup. The agent follows the standard installation procedure for CA ARCserve Backup system components, agents, and options.

- Install the agent after you install CA ARCserve Backup. Using Agent Deployment you can install the agent at any time after you install CA ARCserve Backup.

  Note: For more information about using Agent Deployment to install agents, see the *Administration Guide*.

To install and configure the agent, ensure that you complete the following tasks:

1. Follow the procedures about installing CA ARCserve Backup in the *Implementation Guide*.

2. Install the required number of licenses for the agent on the primary or stand-alone server.

3. Complete the configuration tasks described in Post Installation Tasks (see page 37).

Deploy the Agent to VMs Using Agent Deployment

CA ARCserve Backup Agent Deployment lets you install and upgrade CA ARCserve Backup agents on local or remote VMs. The virtual machine deployment method lets you specify the agents that you want to install and upgrade on local or remote VMs. This method helps to ensure that all agents running on the VMs in your CA ARCserve Backup environment are the same release number as the CA ARCserve Backup server.

Be aware of the considerations that follow:

- To install or upgrade an agent on a VM, the VM must be powered on.

- Agent Deployment installs or upgrades agents on all VMs that reside in the ESX/ESXi Server system and the Hyper-V host system.

To deploy CA ARCserve Backup agents to VMs using Virtual Machine deployment

1. Open the CA ARCserve Backup Manager Console.

   From the Quick Start Menu, select Administration and click Agent Deployment.

   CA ARCserve Backup Agent Deployment starts and the Login Server dialog opens.

2. Complete the required fields on the Login Server dialog and click Next.

   The Methods dialogs opens.

3. From the Methods dialog, select Virtual Machine deployment and click Next.

   The Components dialog opens.

4. From the Components dialog, select the agents that you want to install on all remote hosts and click Next.

   The Host Information dialog opens.

5. Specify the names of remote hosts that contain the VMs by doing one of the following:

   ■ Click Import to import a list of remote hosts from a text file.

      Note: The host names must be separated the new line delimiter. You can import multiple text files, however, the total number of remote hosts must be less than or equal to 1000.

      After the host names appear in the Host column, continue to the next step.

   ■ Click Refresh to import the existing VMs from the CA ARCserve Backup database.

      After the host names appear in the Host column, continue to the next step.

   ■ Specify the remote host name in the Host Name field and click Add.

      Note: Repeat this step as necessary until all required host names appear in the Host column.

      After the host names appear in the Host column, continue to the next step.

   Note: You can specify up to 1000 remote hosts. To deploy agents to more than 1000 remote hosts, you can restart Agent Deployment and repeat this task, or, run Agent Deployment from an alternate CA ARCserve Backup primary server or stand-alone server.

6. Specify the user name and password for the remote hosts by doing the following:

   a. Click the UserName field (next to the host name) and specify the user name using the following format:

      <domain>\<user name>

   b. Click the Password field and specify the corresponding password.

   c. Repeat this step as required until you specify the user name and password for all remote hosts.

   Optionally, if the user name and password are the same for all remote hosts, specify the user name in the User field (<domain>\<user name>), specify the password in the Password field, ensure that all the check boxes are checked, and then click Apply Credentials.

   The user name and the password are applied to all remote hosts in the list.

   Note: To remove a host from the Host and Credentials list, click the check box next to the host that you want to remove and click Remove.

   Click Next to continue.

   Agent Deployment validates the host name, user name, and password specified for all specified hosts. If Agent Deployment does not detect an authentication error, pending appears in the Status field. If Agent Deployment detects an authentication error, Failed appears in the Status field. Click Failed to discover the reason for the error. You must correct all Failed messages continue.

   Click Next.

7. After the Status field for all hosts displays Pending or Verified, click Next.

   The Setup Summary dialog opens.

8. From the Setup Summary dialog, verify the components and the host names specified.

   Click Next.

   The Installation Status dialog opens.

9. From the Installation Status dialog, click Install.

   Agent Deployment installs or upgrades the CA ARCserve Backup agents on the specified hosts.

   After all installations and upgrades are complete, the Installation Report dialog opens.

10. Do one of the following:

    ■ If there are remote hosts that require a restart, click Next.

       The Restart dialog opens to identify the remote hosts that require a restart.

       Click Restart.

       Continue to the next step.

    ■ If there are no remote hosts that require a restart, click Finish to complete this task.

11. From the Restart dialog, click the check box next to the remote host that you want to restart now.

    Optionally, you can click the All check box to restart all remote hosts now.

    Click Restart.

    Agent Deployment restarts all remote hosts now.

    Note: If you want to create a list of remote hosts that require a restart, click Export Restart Report.

12. After the Status field for all remote hosts displays complete, click Finish.

The CA ARCserve Backup agents are deployed on the VMs.

Post Installation Tasks

The sections that follow describe post installation tasks that you must perform to protect various versions of VMware ESX/ESXi and vCenter Server systems. The agent does not require post-installation configuration to protect Hyper-V based systems.

VMware vSphere Integration Post Installation Tasks

To integrate with VMware vSphere, complete the following tasks, as required, for your VM infrastructure:

1. Populate the CA ARCserve Backup database (see page 38).

2. Specify a backup approach (see page 38).

3. Allow the mount points to remain on the backup proxy system (see page 41).

4. Modify the default VDDK communication port (see page 42).

5. Specify a logging level for vcbmounter (see page 43).

Populate the CA ARCserve Backup Database

ARCserve VMware Configuration Tool is a data collection utility that lets you populate the CA ARCserve Backup database with the information about the VMs in your environment.

For more information, see Populate the Database Using ARCserve VMware Configuration Tool (see page 54).

Specify a Backup Approach

The agent lets you specify one of the following approaches to protect VM backup data:

■ VCB Framework--Lets you protect VMs on all ESX Server systems supported by the version of VCB Framework that is installed on the backup proxy system.

Note: VMware ESX Server 4.0 and VMware vCenter Server 4.0 are supported with only VCB Framework 1.5, Update 1 and later releases.

■ VMware vSphere Web Services SDK and VMware VDDK--Lets you protect the implementations that follow using the agent.

– ESX Server 3.5 and above up to ESX Server 4.0

– VMware Virtual Center 2.5 and above up to vCenter Server 4.0 managing ESX Server 3.5 and above up to ESX Server 4.0

Important! After you install the agent, by default, CA ARCserve Backup processes backups using VDDK if VDDK is installed. However, you can specify to use the VCB approach for backups by modifying the registry keys described in this topic.

When using the **VDDK approach**, be aware of the following expected behavior:

- CA ARCserve Backup uses VDDK to process raw (full VM) backups and raw (full VM) backups with the Allow file level restore option specified when VDDK and VCB Framework are installed on the backup proxy system that is protecting the VMs. However, CA ARCserve Backup always uses VCB Framework to perform file mode backups if VCB Framework and VDDK or only VCB Framework is installed on the backup proxy system.

- CA ARCserve Backup tries to use VCB Framework to execute backups when VCB Framework is installed on the backup proxy system and VDDK is not installed on the backup proxy system.

- Backups fail when VDDK and VCB Framework are not installed on the backup proxy system.

- Backups store the snapshot in the mount directory specified using ARCserve VMware Configuration Tool.

- CA ARCserve Backup uses VDDK to recover data when the VM data is backed up using VDDK.

  Note: VMware converter cannot be used to restore data when you used VDDK to back up the VM.

- The backup process creates a file named vmconfig.dat in binary format that contains the VM configuration details.

  Note: You should not attempt to modify vmconfig.dat.

- The backup process does not create or update catalog files.

- The backup process creates disk files with a zero file size in the mount directory for raw (full VM) backups and raw (full VM) backups with the Allow file level restore option specified.

  Important! You should not attempt to modify the disk files.

When using the **VCB Framework approach**, be aware of the expected behavior that follows:

- CA ARCserve Backup uses VCB to perform backup operations when VCB and VDDK are installed on the backup proxy system.

- CA ARCserve Backup attempts using VDDK for backup operations when VCB is not installed on the backup proxy system.

Note: CA ARCserve Backup attempts the above-described failover actions when the backup operation starts. After CA ARCserve Backup detects the applications corresponding with the approach specified, CA ARCserve Backup does not attempt to fail over to the alternate approach only if a failure occurs during the backup operation.

When executing file level backups using the VCB approach or the VDDK approach, be aware of the expected behavior that follows:

- The backup process does not create or update catalog files.

- The backup process creates a child disk in the mount point directory.

The mount point directory does not display files for the mounted volume. This behavior occurs because VDDK does not mount volumes to a directory or map volumes to a drive letter.

To specify a backup approach

1. Open Windows Registry Editor

   Modify the following registry keys, as required, using the values specified.

   - **Key Name--**useVCBFor35

     Lets you specify the VMware application to use for backup operations on ESX Server 3.5 systems when VCB Framework and VDDK are installed on the backup proxy system.

     Path

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

     Type

     REG_DWORD

     Default Value

     0 (Back up data using VDDK)

     Note: To protect VMs using VCB Framework when ESX Server 3.5 is installed on the backup proxy system, set this value to 1.

- ■ **Key Name--**useVCBFor40

  Lets you specify the VMware application to use for backup operations on ESX Server 4.0 systems when VCB Framework and VDDK are installed on the backup proxy system.

  Path

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

  Type

  REG_DWORD

  Default Value

  0 (Back up data using VDDK)

  Note: To protect VMs using VCB Framework when ESX Server 4.0 is installed on the backup proxy system, set this value to 1.

2. Close Windows Registry Editor.

Important! To protect VM data using the VDDK approach, VMware VDDK must be installed in the backup proxy system. Similarly, to protect VM data using the VCB approach, VMware VCB Framework must be installed on the backup proxy system.

Allow the Mount Points to Remain on the Backup Proxy System

By default, CA ARCserve Backup deletes the mount point directory on the backup proxy system after a successful backup of the VMs is complete. If the backup fails and the mount point is not deleted from the backup proxy system, CA ARCserve Backup deletes the mount point directory the next time the backup job executes. This approach helps ensure that the agent minimizes the amount disk space required to execute VM backups.

Optionally, you can allow the mount point to remain on the backup proxy system if all of the conditions that follow apply in your VM backup environment:

- ■ You are backing up data using deduplication.

- ■ The deduplication devices function as data stores that reside on the backup proxy system.

- ■ Freeing disk space on the backup proxy system is not a requirement.

This approach lets you decrease the amount of time required to recover VM data.

When mount points remain on the backup proxy system, CA ARCserve Backup names the mount points using the following conventions:

■ Successful Backups--CA ARCserve Backup renames the mount point directory to the following:

<vmname>_J<JobID>_S<SessionID>_date_time

Note: CA ARCserve Backup renames the mount point directory when the backup completes.

■ Unsuccessful and Incomplete Backups--The next time a backup job executes for the VM with the same backup proxy system, CA ARCserve Backup renames the mount point directory to the following:

<vmname>_J<JobID>_S<SessionID>_err_date_time

To allow the mount points to remain on the backup proxy system

1. From the Windows Start menu, click Run.

   The Run dialog opens.

2. In the Open field, type regedit.

   Windows Registry Editor opens.

3. Browse to the key that follows:

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

   The values for the key appear.

4. From the Edit menu, select New and click DWORD Value.

   Name the DWORD retainVCBMountDir.

   Right-click retainVCBMountDir and click Modify on the pop-up menu.

   The Edit DWORD Value dialog opens.

5. In the Value data field, type 1 and click OK.

   The key is created.

6. Close Registry Editor.

Modify the Default VDDK Communication Port

By default, VDDK communicates using port 902. You can modify the port when you require VDDK to communicate using a secured port or a specific port that is required by your organization.

The steps that follow describe how to modify the default VDDK communication port.

To modify the default VDDK communication port

1. From the Windows Start menu, click Run.

    The Run dialog opens.

2. In the Open field, type regedit.

    Windows Registry Editor opens.

3. Browse to the key that follows:

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

    The values for the key appear.

4. Right-click VDDKPort and click Modify on the pop-up menu.

    The Edit DWORD Value dialog opens.

    Note: The default value of VDDKPort is 902.

    In the Value data field, specify a communication port and click OK.

    The key is modified.

5. Close Registry Editor.

Specify a Logging Level for VCBMounter

Using the log file labeled vcbmounteroutput_xxx.log you can view the details about mount operations that relate to VM backups. Optionally, CA ARCserve Backup lets you specify the amount of detail that you would like described in the log file.

To specify a logging level for VCBMounter

1. From the Windows Start menu, click Run.

    The Run dialog opens.

2. In the Open field, type regedit.

    Windows Registry Editor opens.

3. Browse to the key that follows:

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

    The values for the key appear.

4. From the Edit menu, select New and click DWORD Value.

    Name the DWORD VcbMountLogLevel.

    Right-click VcbMountLogLevel and click Modify on the pop-up menu.

    The Edit DWORD Value dialog opens.

5. In the Value data field, specify a logging level of 1 through 6.

   Note: A higher logging level value specifies more detailed information will be included in the log.

   Click OK.

   The key is created and the logging level is applied.

6. Close Registry Editor.

Configure the Number of Concurrent Read Operations Using VDDK

CA ARCserve Backup lets you increase and decrease the number of concurrent reads from VM virtual disks when executing backups using VDDK. The capability to increase and decrease the number of concurrent reads helps minimize the overall backup window. You increase and decrease the number of concurrent reads based on the number of VMs that you are backing up as part of the same job or multiple jobs that are running from a backup proxy system. To specify the number of concurrent reads, create or modify (if already present in the Registry) the following key:

Path

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

Key name

VmdkReaderCount

Default value

4 (Back up data using VDDK)

Max value

8

Add or Remove Specific VM Data from the CA ARCserve Backup Database

CA ARCserve Backup provides you with command line arguments that let you add and remove specific VM data from the CA ARCserve Backup database. The arguments can be used when you know the name of the specific VM that you want to add to or remove from the CA ARCserve Backup database. The command line arguments are as follows:

-insertVM <vmname>
-deleteVM <vmname>

Note: You can use -insertVM and -deleteVM with the VMware command line utility (ca_vcbpopulateDB) and the Hyper-V command line utility (ca_msvmpopulateDB). For more information about these utilities, see the *Command Line Reference Guide*.

To add or remove VM data from the CA ARCserve Backup database

1. Open the Windows command prompt.

   Change the directory to directory where the Client Agent for Windows is installed.

2. Execute ca_vcbpopulateDB (VMware VMs) or ca_msvmpopulateDB (Hyper-V VMs) using the syntax that follows:

   -insertVM <vmname>

   The example that follows describes the syntax required to insert a VMware VM with hostname VM-001 into the CA ARCserve Backup database:

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

   The example that follows describes the syntax required to insert a Hyper-V VM with hostname VM-001 into the CA ARCserve Backup database:

   ca_msvmpopulatedb.exe –Primary ARCServe1 –insertVM VM-001 –debug 1

   -deleteVM <vmname>

   The example that follows describes the syntax required to delete a VMware VM with hostname VM-001 from the CA ARCserve Backup database:

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

   The example that follows describes the syntax required to delete a Hyper-V VM with hostname VM-001 from the CA ARCserve Backup database:

   ca_msvmpopulatedb.exe –Primary ARCServe1 –deleteVM VM-001 –debug 1

How to Use the VMware hotadd Transport Mode

The VMware hotadd Transport Mode is a VMware Consolidated Backup r1.5 option that can be used when VCB is installed in a VM.

Note: For more information about using the hotadd Transport Mode, see the *Virtual Machine Backup Guide* at www.vmware.com.

To use VMware hotadd Transport Mode in your environment, consider the following:

- ESX Server 3.5, ESX Server 3i version 3.5 or later, or vCenter Server 2.5 or later must be installed on the backup proxy system.

- The backup proxy system must be configured on a VM.

- The VCB helper VM must be created without using virtual hard disks.

- A VCB proxy VM must be configured on all VMware ESX Host systems if you are backing up only to local storage devices.

- You must create the DWORD UseHotadd in the registry key that follows on the backup proxy system:

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

  DWORD: UseHotadd

  Value: 1

Terminate Operations when the Agent Detects Expired SSL Certificates

Backup proxy systems can be configured to obtain valid SSL Certificates when communicating with VMware ESX Host systems. By default, the agent continues processing VM-based operations (for example, auto-populate, back up, and recovery operations) when it detects bad or expired SSL Certificates. This behavior is designed to allow uninterrupted protection of the VMs in your environment.

If this behavior does not fulfill the needs of your organization, you can modify how the agent behaves when it detects bad and expired SSL Certificates on the VMware ESX Host system.

To terminate operations when the agent detects expired SSL Certificates

1. Open Registry Editor and access the registry key that follows:

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

2. Create a registry key value SSLCertificateVerify of type DWORD.

   Set the key value of SSLCertificateVerify to 1.

3. Close Registry Editor.

Specify Custom HTTP/HTTPS Communication Ports

VMware vCenter Server Virtual Infrastructure (VI) SDK uses HTTP port 80 and HTTPS port 443 for Web Services communication. These particular ports may conflict with the communication ports used by Microsoft Internet Information Services (IIS). To avoid port conflicts, VMware vCenter Server and VMware ESX Server let you specify custom VI SDK Web Service ports. However, if you modify the VI SDK Web Service ports, CA ARCserve Backup may not be able to mount the VM data to the backup proxy system, and backups may fail.

To remedy this problem, CA ARCserve Backup lets you create a set of custom HTTP and HTTPS communication ports that will allow CA ARCserve Backup to mount the VM data to the backup proxy system.

Note: For information about how to configure VI SDK Web Services ports on VMware vCenter Server and VMware ESX Server systems, see the VMware documentation.

The remedy that follows is a global change that affects ESX Server Systems and vCenter Server systems that you back up using a particular backup proxy system. Therefore, the best practice is to identify a dedicated backup proxy system that will be used to mount data for VMware vCenter Server systems that contain a VI SDK customized port.

To specify custom HTTP/HTTPs communication ports

1. Log in to the backup proxy system.

2. Open Windows Registry Editor.

3. Create the following registry key:

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

   Right-click VIHTTPPort and click Modify on the pop-up menu.

   The Edit DWORD Value dialog opens.

4. In the Value data field, specify the customized HTTP communication port number that was configured with VMware vCenter Server.

    Click OK.

    The port number is applied.

5. Create the following resgistry key:

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

    Right-click VIHTTPSPort and click Modify on the pop-up menu.

    The Edit DWORD Value dialog opens.

6. In the Value data field, specify the customized HTTPS communication port number that was configured with VMware vCenter Server.

    Click OK.

    The port number is applied.

Enable Debugging for VDDK Jobs

CA ARCserve Backup lets you enable debugging logs for VDDK backups. Debug logs can be used to troubleshoot backup and recovery operation failures.

To enable debugging for VDDK jobs

1. Log in to the backup proxy system.

    Open Windows Registry Editor.

    Open the following registry key:

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

    Right-click Debug and click Modify on the pop-up menu.

    The Edit DWORD Value dialog opens.

2. In the Value field, specify 1.

    CA ARCserve Backup generates a log file on the backup proxy system in the ARCserve Backup Client Agent for Windows\Log directory named VMDKIOXXXX.log.

Uninstall the Agent

As a best practice, you can use Add or Remove Programs in Windows Control Panel to uninstall the agent. The CA ARCserve Backup uninstallation routine lets you uninstall the agent and any combination of CA ARCserve Backup components.

To uninstall the agent

1. Open Windows Control Panel and double-click the Add or Remove Programs icon.

   Locate and select CA ARCserve Backup.

   Click Uninstall.

   The CA ARCserve Backup Remove Application, Components dialog opens.

2. Place a check mark next to CA ARCserve Backup Agent for Virtual Machines.

   Click Next.

   The CA ARCserve Backup Remove Application, Messages dialog opens.

3. Click Next.

   The CA ARCserve Backup Remove Application, Remove dialog opens.

4. Place a check mark next to Click this check box to confirm that you want to remove the specified components from your computer and click Remove.

   The agent is uninstalled.

Chapter 3: Populating the CA ARCserve Backup Database

This section contains the following topics:

Specify the Name of the CA ARCserve Backup Server

To perform granular file level restores from raw (full VM) backups, you must specify the name of the CA ARCserve Backup server on your VMs.

This task is not required if you installed the CA ARCserve Backup Agent for Virtual Machines on your VMs using the Agent Deployment tool. For more information, see Deploy the Agent to VMs Using Virtual Machine Deployment (see page 34).

Note: The steps that follow apply to VMware VMs and Hyper-V VMs.

To specify the name of the CA ARCserve Backup server

1. Log in to the VM and open the Backup Agent Admin.

   To open the Backup Agent Admin, click Start, Programs, CA, ARCserve Backup, and click Backup Agent Admin.

   The Backup Agent Admin opens.

2. From the drop-down list, select CA ARCserve Backup Client Agent and click Configuration on the toolbar.

   The Configuration dialog opens.

3. Click the Agent for Virtual Machines tab.

In the Server Name field, specify the Host Name or IP address of the CA ARCserve Backup server that will protect this VM.
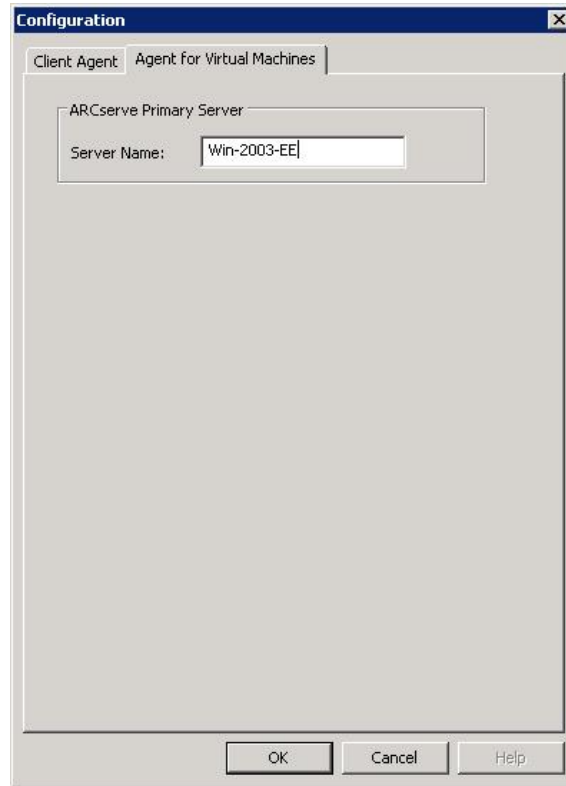
Click OK.

The name of the CA ARCserve Backup server is saved.

Note: Repeat these steps, as necessary, on all VMs in your CA ARCserve Backup environment.

Specify a Temporary VM Mount Location

To populate the CA ARCserve Backup database with information about the VMs in your VMware backup environment, CA ARCserve Backup requires a location to temporarily store the backup information while the ARCserve VMware Configuration Tool is running.

By default, CA ARCserve Backup stores the temporary backup information in the location that follows on the backup proxy system:

C:\Program Files\CA\ARCserve Backup Client Agent for Windows

Note: To perform raw (full VM) mode backups and raw (full VM) with allow file level restore backups, you must reserve at least the amount of disk space used on the drive or up to the maximum size of the drive to accommodate the data stored in the temporary VM mount location. To perform file level backups, the amount of free disk space is independent of the size of the VM. File mode backups require a minimal amount of free disk space in the temporary mount location.

Use the steps the follow to specify a different location for the Temporary VM Mount Location on the backup proxy system.

Be aware of the following:

■ The Temporary VM Mount Location must reside on the backup proxy system.

■ CA ARCserve Backup does not support using mapped drives on the backup proxy system for the Temporary VM Mount Location.

To specify a Temporary VM Mount Location

1. Log in to the backup proxy system and open the Backup Agent Admin.

   To open the Backup Agent Admin, click Start, Programs, CA, ARCserve Backup, and click Backup Agent Admin.

   The Backup Agent Admin dialog opens.

2. From the drop-down list, select CA ARCserve Backup Agent for Virtual Machines and click Configuration on the toolbar.

   The ARCserve VMware Configuration Tool opens.

3. In the Temporary VM Mount Location field, specify the path to the location where you want to mount the data.

4. Click Set.

   The Temporary VM Mount Location is set.

5. Click Close.

   The ARCserve VMware Configuration Tool closes.

Populate the Database Using ARCserve VMware Configuration Tool

ARCserve VMware Configuration Tool is a data collection utility that lets you populate the CA ARCserve Backup database with the information about the VMs on your VMware ESX Host systems. This tool integrates with a command-line utility named ca_vcbpopulatedb, which runs in the background, to populate the ARCserve database with information about the VMs. The configuration tool collects the information that follows:

- VCB backup proxy names

- VMware ESX Host names or VMware vCenter Server names

- VM Host names

- Volume names contained within the VMs on Windows systems

After you install the agent, you must populate the CA ARCserve Backup database with the information about your VM systems. To accomplish this, you must execute the ARCserve VMware Configuration Tool on the backup proxy system.

After you execute ARCserve VMware Configuration Tool, and submit a successful backup job of the data that resides in the VMs, CA ARCserve Backup automatically populates the CA ARCserve Backup database using the information about the VM that was specified when you executed the configuration tool. The Auto-populate option helps ensure that you can accurately browse the Backup Manager and back up the most current data in your VMs. By default, CA ARCserve Backup automatically populates the database with updated information in 24-hour intervals after the backup job is complete.

To populate the database using ARCserve VMware Configuration Tool

1. Ensure that the VMs in the VMware ESX Host systems are in a running state.

   Note: If the VMs are not in a running state, the ARCserve VMware Configuration Tool will not populate the CA ARCserve Backup database with data, and you will not be able to accurately browse and back up the VMs in the VMware ESX Host systems.

2. Log in to the backup proxy system and open the Backup Agent Admin.

   To open the Backup Agent Admin, click Start, Programs, CA, ARCserve Backup, and click Backup Agent Admin.

   The Backup Agent Admin opens.

3. From the drop-down list, select CA ARCserve Backup Agent for Virtual Machines and click Configuration on the toolbar.

The ARCserve VMware Configuration Tool opens.

Note: (Optional) You can open VCBUI.exe from the following directories on the backup proxy system:

- x86 systems

   C:\Program Files\CA\ARCserve Backup Client Agent for Windows\x86

- X64 systems

   C:\Program Files\CA\ARCserve Backup Client Agent for Windows

4. Complete the following fields:

    ARCserve Primary Server Details

    The following options apply to the CA ARCserve Backup primary or stand-alone server:

    ■   **Server (Name or IP)--**Lets you specify the name or IP address of the CA ARCserve Backup primary server.

    ■   **ARCserve User Name--**Lets you specify the user name, with caroot privileges, for the CA ARCserve Backup primary server.

    ■   **Password--**Lets you specify the password for the CA ARCserve Backup User Name.

    vCenter Server or VMware ESX Host Details

    The following options apply to the VMware Virtual Infrastructure in your environment:

    ■   **Server (Name or IP)--**Lets you specify the name of the VMware ESX Host system or the vCenter Server system.

    ■   **User Name--**Lets you specify the name of the VMware ESX Host user or the vCenter user with Administrator privileges.

    ■   **Password--**Lets you specify the password for the VMware ESX Host User Name or the vCenter Server User Name.

    ■   **Protocol--**Lets you specify the communication protocol between the backup proxy system and the VMware ESX Host system or the vCenter Server system.

    Note: If you omit this argument, the tool assumes that https is to be used as the communication protocol.

Miscellaneous

Specify the following Miscellaneous options, as required, to populate the CA ARCserve Backup database:

■   **Mount--**With the Mount option enabled, the configuration tool populates the database with the names of the VMs that are mountable.

   Note: If you run the configuration tool with the Mount option enabled, the utility takes longer to run because it performs a mount and unmount operation of each running VM.

■   **Remove Configuration--**Lets you delete the VMs available in the database for the specified VMware ESX Host system or vCenter Server system for a specified backup proxy system.

■   **Debug--**Lets you write a detailed debug log. The log will be created in the Client Agent for Windows installation directory. By default, this directory is as follows:

   C:\Program Files\CA\ARCserve Backup Client Agent for Windows\LOG

   Note: The name of the log file is ca_vcbpopulatedb.log.

■   **Retain VM Information--**Lets you retain data (backup information) for VMs that are not available when you execute this tool.

   By default, this tool captures information from VMs that are available when you execute this tool. If a VM is not available (for example, the VM is powered off or deleted from the environment), CA ARCserve Backup deletes the data relating to the VM from the CA ARCserve Backup database. With this option enabled, CA ARCserve Backup captures information from VMs that are available, and retains the backup information from VMs that are not available.

   Consider the following best practices:

   –   You should specify the Retain VM Information option in environments where the VMs will be in a powered off state when the populate operation executes. This approach helps ensure that CA ARCserve Backup backs up the VMs the next time the backup job runs.

   –   You should not specify the Retain VM Information option in environments where the VMs migrate from one ESX Server or vCenter Server system to another to support load balancing operations. This approach helps ensure that backups of ESX Server and vCenter Server systems do not fail.

■   **Stop Auto-population--**Lets CA ARCserve Backup stop automatically populating the VM-related information automatically for the ESX Server or vCenter Server system.

   As a best practice, you should use this option under the following scenarios:

- The CA ARCserve Backup database was populated with information about the ESX Server or vCenter Server systems, and you want to stop the CA ARCserve Backup database auto-population process.

- An ESX Server or vCenter Server system was disabled. After the system was returned to service, the CA ARCserve Backup database was populated with information about the ESX Server or vCenter Server system. You now want to stop the CA ARCserve Backup database auto-population process.

- A new ESX Server or vCenter Server system was installed in your backup environment. The CA ARCserve Backup database was populated with information about the ESX Server or vCenter Server system. You now want to stop the CA ARCserve Backup database auto-population process.

With the Stop Auto-population option enabled, the auto-population process does not execute the next time CA ARCserve Backup is scheduled to populate the CA ARCserve Backup database. The auto-population process populates the database with updated information in 24-hour intervals (default) after the backup job is complete, or based on the frequency that you specified for the Auto-populate VM option.

Auto-populate VM

Lets you specify how frequently CA ARCserve Backup will automatically populate the CA ARCserve Backup database with VM-related information.

Default: 24 hours

Range: 1 to 99 hours

Temporary VM Mount Location

Lets you define where ARCserve VMware Configuration Tool temporarily mounts (stores) the backup information for the VMs while the tool is running.

By default, CA ARCserve Backup mounts the temporary backup information in the following location:

C:\Program Files\CA\ARCserve Backup Client Agent for Windows

Note: You must click Set to apply the location.

For example, you may need to move the Temporary Mount Path because there is an insufficient amount of free disk space to mount the backup on the volume. For more information, see Specify a Temporary VM Mount Location (see page 52).

5. Click Execute.

   Note: You cannot click Execute unless all required fields are complete.

   The ARCserve VMware Configuration Tool populates the CA ARCserve Backup database. The results of the execution display in the Results field on the ARCserve VMware Configuration Tool. To view detailed log information, open the log file labeled ca_vcbpopulatedb.log located in the Client Agent for Windows installation directory on the backup proxy system.

Populate the Database Using ARCserve Hyper-V Configuration Tool

ARCserve Hyper-V Configuration Tool is a data collection utility lets you populate the CA ARCserve Backup database with the information about the VMs in the Hyper-V host system.

After you install the agent, you must populate the CA ARCserve Backup database with the information about your VM systems. To accomplish this, you must execute the ARCserve Hyper-V Configuration Tool on the Hyper-V host system.

After you execute ARCserve Hyper-V Configuration Tool, and submit a successful backup of the data that resides in the VMs, CA ARCserve Backup automatically populates the CA ARCserve Backup database using the information about the VM that was specified when you executed the configuration tool. The Auto-populate option helps ensure that you can accurately browse the Backup Manager and back up the most current data in your VMs. By default, CA ARCserve Backup automatically populates the database with updated information in 24-hour intervals after the backup job is complete.

With ARCserve Hyper-V Configuration Tool, consider the limitations that follow:

- ARCserve Hyper-V Configuration Tool populates the CA ARCserve Backup database with information about Hyper-V VMs that are in a powered on state when you execute the tool. The tool cannot populate the database with Hyper-V VM data when the VMs are in a powered off state.

- ARCserve Hyper-V Configuration Tool populates the CA ARCserve Backup database with the host names of the detected VMs. However, if ARCserve Hyper-V Configuration Tool does not detect the host name of a VM, CA ARCserve Backup substitutes the host name of the VM with the VM name of the VM in the CA ARCserve Backup database.

- CA ARCserve Backup does not support using host names and VM names that exceed 15 characters. If the detected host names or VM names exceed 15 characters, the names will be truncated to 15 characters in the CA ARCserve Backup database.

- ARCserve Hyper-V Configuration Tool does not support the use of JIS2004 Unicode characters for host names and VM names. If the tool detects JIS2004 Unicode characters in theses names, CA ARCserve Backup records the event in the Results field on the ARCserve Hyper-V Configuration Tool and the information about the VMs will not be populated into the CA ARCserve Backup database.

To populate the database using ARCserve Hyper-V Configuration Tool

1. Verify that the VMs in your Hyper-V Server systems are in a running state.

    Note: ARCserve Hyper-V Configuration Tool will not populate the CA ARCserve Backup database with information about Hyper-V VMs that are not in running state.
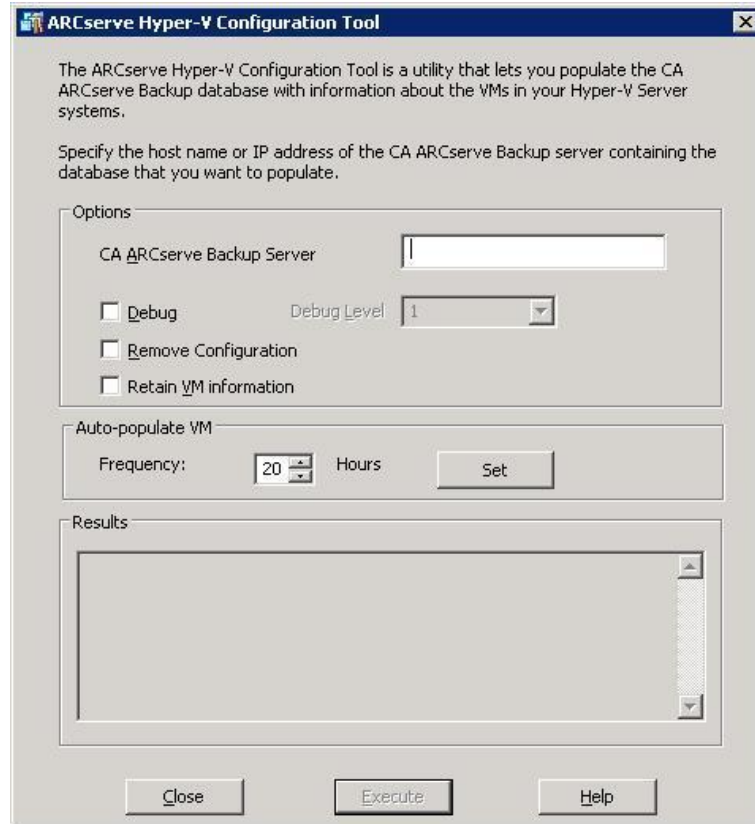
2. Log in to the Hyper-V host system and open the Backup Agent Admin.

    To open the Backup Agent Admin, click Start, Programs, CA, ARCserve Backup, and click Backup Agent Admin.

    Backup Agent Admin opens.

3. From the drop-down list, select CA ARCserve Backup Agent for Virtual Machines and click Configuration on the toolbar.

ARCserve Hyper-V Configuration Tool opens.

4. Complete the following fields:

    Options

    ■   **CA ARCserve Backup Server--**Lets you specify the host name or IP address of the CA ARCserve Backup server containing the database that you want to populate.

    ■   **Debug--**Lets you write a detailed debug log. The log will be created in the Client Agent for Windows installation directory. By default, this directory is as follows:

    C:\Program Files\CA\ARCserve Backup Client Agent for Windows\Log

    Note: The name of the log file is ca_msvmpopulatedb.log.

    ■   **Debug Level--**Lets you specify the level of details that you require in the debug log (ca_msvmpopulatedb.log).

    Default: 2

    Range: 1 to 6.

    Note: A higher Debug Level means that more detailed information will be provided in the Debug log.

    ■   **Remove Configuration--**Lets you delete the VMs available in the CA ARCserve Backup database for the specified Hyper-V server.

    ■   **Retain VM Information--**Lets you retain data (backup information) for VMs that are not available when you execute this tool.

    By default, this tool captures information from VMs that are available when you execute this tool. If a VM is not available (for example, the VM is powered off or deleted from the environment), CA ARCserve Backup deletes the data relating to the VM from the CA ARCserve Backup database. With this option enabled, CA ARCserve Backup captures information from VMs that are available, and retains the backup information from VMs that are not available.

    Consider the following best practices:

    –   You should specify the Retain VM Information option in environments where the VMs will be in a powered off state when the populate operation executes. This approach helps ensure that CA ARCserve Backup backs up the VMs the next time the backup job runs.

    –   You should not specify the Retain VM Information option in environments where the VMs migrate from one Hyper-V server to another to support load balancing operations. This approach helps ensure that backups Hyper-V servers do not fail.

Auto-populate the VM

■ **Frequency--**Lets you specify how frequently CA ARCserve Backup will automatically populate the CA ARCserve Backup database with VM-related information.

Default: 24 hours

Range: 1 to 99 hours

Note: You must click Set to apply the Frequency value.

5. Click Execute.

The CA ARCserve Backup database is populated with information about the VMs that are running in the Hyper-V host system.

Populating the CA ARCserve Backup Database Using Command Line Utilities

CA ARCserve Backup lets you populate the CA ARCserve Backup database using the following command line utilities:

■ **ca_vcbpopulatedb--**Lets you populate the CA ARCserve Backup database with information about the VMware VMs in your backup environment.

■ **ca_msvmpopulatedb--**Lets you populate the CA ARCserve Backup database with information about the Hyper-V VMs in your backup environment.

Note: For more information about the syntax, arguments, and examples for the above-described utilities, see the *Command Line Reference Guide*.

How Virtual Machine Names Affect Jobs

CA ARCserve Backup distinguishes VMs based on their VM name (DNS name) in conjunction with their host name or the name of the backup proxy system. CA ARCserve Backup populates the CA ARCserve Backup database with this information when you execute ARCserve VMware Configuration Tool and ARCserve Hyper-V Configuration Tool.

ARCserve VMware Configuration Tool and ARCserve Hyper-V Configuration Tool let you retain or remove information about the VMs in the CA ARCserve Backup database by enabling and disabling the Retain VM Information option. This design lets you retain information about the VMs that are in a powered off state when you execute the above tools.

ARCserve VMware Configuration Tool and ARCserve Hyper-V Configuration Tool rely upon the VM name to determine the state of a VM (for example, the VM is powered off). If ARCserve VMware Configuration Tool and ARCserve Hyper-V Configuration Tool cannot locate a VM by its VM name, the tools search for VMs by their host name or the name of the backup proxy system.

Example: How VM Names Affect Jobs

Consider the following VM environment:

- You create an environment that consists of one VM.

- The host name of the VM is VM1.

- The VM name is VM_one.

The events that follow occur:

1. You execute ARCserve VMware Configuration Tool or ARCserve Hyper-V Configuration Tool.

   CA ARCserve Backup populates the CA ARCserve Backup database with the information about the data contained within VM1.

2. You submit a scheduled backup job of VM1.

   CA ARCserve Backup runs the job and it completes successfully.

3. You rename VM1 to VM2, but you do not change the VM name.

4. You execute ARCserve VMware Configuration Tool or ARCserve Hyper-V Configuration Tool and enable the Retain VM Information option.

   CA ARCserve Backup populates the database with information about the data contained within VM2.

   Note: The backup data relating to VM2 is the data that is contained within VM_one.

5. You submit a scheduled backup job of VM2, and then power off VM2.

6. CA ARCserve Backup runs both jobs and the results that follow can be observed:

   - The backup of VM1 completes successfully. The backup data consists of the data contained within VM2.

   - The backup of VM2 completes successfully. The backup date consists of the data contained within VM2.

Observations:

- In this example, the user changed the host name of the VM and did not change the VM name.

- CA ARCserve Backup cannot discover a VM using its host name (for example, VM1 and VM2) when the VM is in a powered off state. In this scenario, CA ARCserve Backup searches for the VM name (for example, VM_one) that corresponds with the host name.

- When both VMs are powered off, they maintain the same identity in the CA ARCserve Backup database. As a result, When the VM1 job runs, CA ARCserve Backup does not back up the correct VM.

Chapter 4: Backing Up Data

This section contains the following topics:

How to Browse Virtual Machine Backup Volumes

The Backup Manager lets you browse and view information about the VM objects that follow in a directory tree structure:

- Backup proxy systems

- VMware ESX/ESXi Server systems

- VMware vCenter Server systems

- Microsoft Hyper-V host systems

To have the capability to browse VMware and Hyper-V VMs, you must execute ARCserve VMware Configuration Tool and ARCserve Hyper-V Configuration Tool. The aforementioned tools populate the CA ARCserve Backup database with information about the data contained in the VMs, which allows you to browse the VMs in the Backup Manager.

Be aware of the limitations that follow:

- You can browse the volumes in the VMware VMs when the VM is running a VMware-supported Windows-based operating system.

- You can browse the volumes in the Hyper-V VMs when you install the Agent for Virtual Machine in the Hyper-V VMs. With this configuration, you do not need to execute ARCserve Hyper-V Configuration Tool to browse the volumes in the Hyper-V VMs.

■ From the Backup Manager window with the Source tab selected, the VMware Systems object can be expanded to display the names of the VMware Systems, the backup proxy systems, the ESX Server system or the vCenter Server system, and the VM volumes contained in the Windows operating system.
At the VM level, you can browse in raw mode (full VM) or file mode.

To browse a VM at the file level, a VMware supported Windows operating system must be installed on the VM.

■ The browsing modes are as follows:

– Windows VMs--file mode and raw mode (full VM)

– Non-Windows VMs--raw mode (full VM) only

The following screen illustrates browsing Hyper-V VMs:
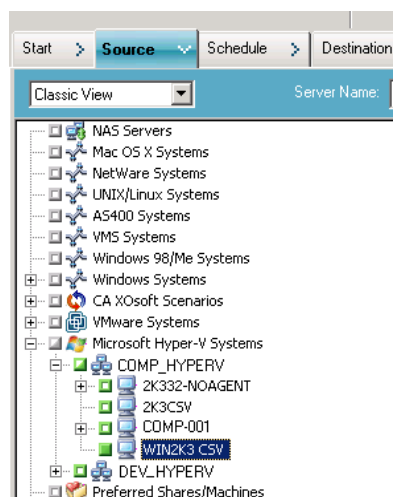
The following screen illustrates browsing VMware VMs:
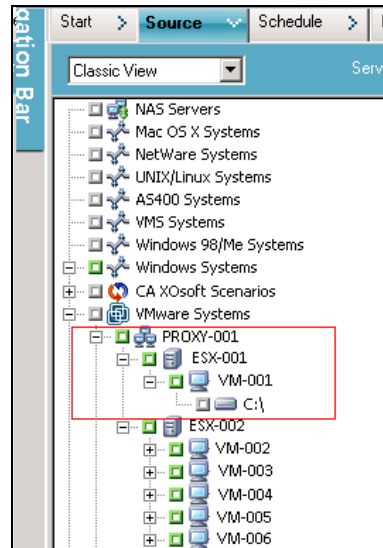
- When you submit a backup job, CA ARCserve Backup prompts you to provide the User name and password credentials for ESX Server system, the vCenter Server system, or the Hyper-V host system.

  CA ARCserve Backup validates the credentials at runtime.

Backup Approaches

Before you submit a backup job, you must specify the approach that you want to use for your backups. You can specify either VCB of VDDK. As a best practice, you should use the VDDK approach.

Note: For more information about the advantages of using the VDDK approach, see Introduction to Integrating with VMware vSphere (see page 17).

For information about the VDDK approach, the VCB approach, and how to specify a backup approach, see Specify a Backup Approach (see page 38).

Using Global and Local Backup Options

This section contains the following topics:

How Global and Local Backup Options Work

Backup options lets you define how CA ARCserve Backup backs up data stored on VMs. CA ARCserve Backup lets you process backup data using the following backup options:

- **File mode--**Lets you back up data that resides on a VM as individual files and directories. File mode backup lets you restore VM backup data at file level granularity.

  By default, CA ARCserve Backup uses VCB Framework to perform file level backups when VCB Framework and VDDK are installed on the backup proxy system. However, if only VDDK is installed on the backup proxy system, CA ARCserve Backup uses VDDK to perform file level backups of VM data. This behavior occurs because VMware VDDK does not support the capability to traverse volume mount points related to file level backups.

- **Raw (full VM) mode--**Lets you back up a full image of data that resides on a VM. Raw (full VM) mode lets you back up data that can be used for disaster recovery operations.

- **Mixed mode--**Lets you perform full backups of data in raw (full VM) mode and incremental and differential backups in file mode. Mixed mode backup lets you perform scheduled backups and GFS rotation backups. In addition, Mixed mode backups are advantageous in that you can perform weekly, full backups at raw (full VM) efficiency and daily, incremental and differential backups at file level granularity.

  Note: Mixed mode backup is the default backup mode.

- **Allow file level restore--**Lets you restore raw (full VM) mode backups and mixed mode backups at file level granularity.

  Note: To perform granular file level restores from raw (full VM) backups, you must specify the name of the CA ARCserve Backup server on your VMs. For more information, see Specify the Name of the CA ARCserve Backup Server (see page 51).

The dialog that follows illustrates the VM backup modes that you can specify from the Global Options dialog.
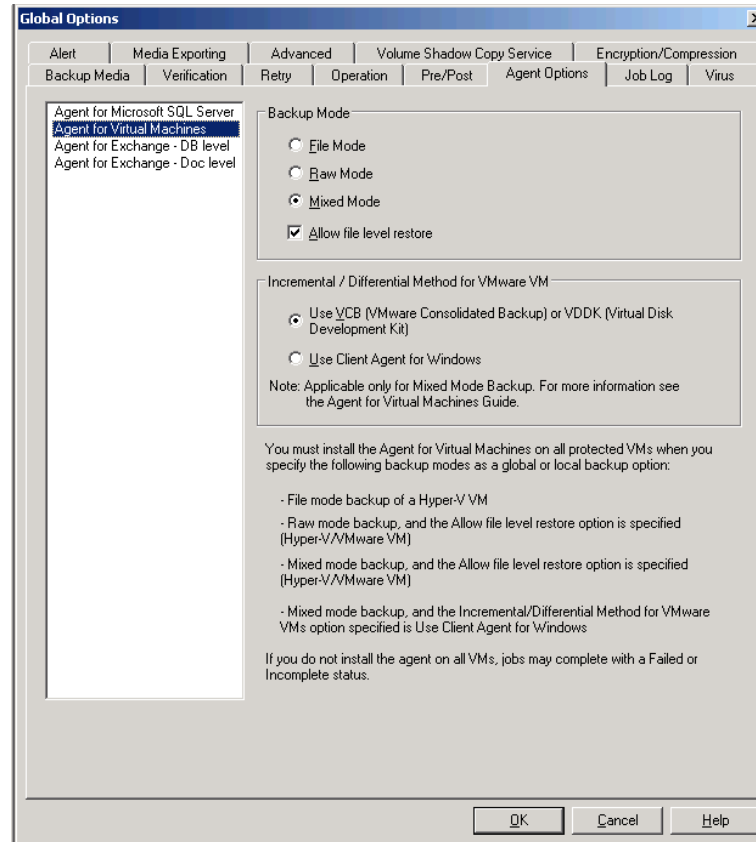
You can specify backup modes as either a global backup option or a local backup option.

■ **Global backup option--**Lets you apply Backup Modes globally to all backup jobs that relate to all VMs in VMware and Hyper-V systems in your environment. For more information, see .

■ **Local backup option--**Lets you apply a Backup Mode to individual VMware and Hyper-V VMs at the job level. For more information, see .

Note: When you specify backup modes at the global level and at the local level, CA ARCserve Backup always executes the backup job using the local backup options specified for the individual VM.

The table that follows describes how backup modes behave:

Backup Mode Specified	Global Incremental/Differential Method Specified	Outcome on VMware Systems	Outcome on Hyper-V Systems
Mixed (specified as a global or local option)	■ Use VCB or VDDK	CA ARCserve Backup processes the raw (full) VM backup data and the file mode backup data (incremental and differential backups) using VCB or VDDK. **Note:** With mixed mode backups, CA ARCserve Backup processes the raw (full) mode backup using the specified mode: VCB or VDDK. However, CA ARCserve Backup will always process file mode backups using VCB when VCB and VDDK are installed on the backup proxy system.	CA ARCserve Backup processes the weekly, full backups in raw mode using the VSS Hyper-V writer and the subsequent daily, incremental and differential backups in file mode via the Agent for Virtual Machines that is running on the VM **Note:** The Use VCB/VDDK global option does not affect backups on Hyper-V systems.
Mixed (specified as a global or local option)	■ Use Client Agent **Note:** The Agent for Virtual Machines must be installed and running on the VM.	CA ARCserve Backup processes the weekly, full backups in raw mode using VCB/VDDK and the subsequent daily, incremental and differential backups in file mode via the Client Agent for Windows that is running on the VM.	CA ARCserve Backup processes the weekly, full backups in raw (full VM) mode using the VSS Hyper-V writer and the subsequent daily, incremental and differential backups in file mode using the Agent for Virtual Machines that is running on the VMs. **Note:** The Use VCB/VDDK global option does not affect backups on Hyper-V systems.

Examples: How to Apply Backup Options

To have the capability to back up data with raw (full VM) efficiency and to restore data at file level granularity, the best practice is accept the default backup mode options and apply them globally to all of your backups. To protect a single VM, such as a VM that is running a supported non-Windows operating system, you can specify the backup options for the individual VM, or, as a local backup option and retain then options specified globally for all backups.

Your backup environment consists of many servers with VMs installed. Most of your backups consist of VMs that require a rotation backup. The remaining servers require full backups in file level mode. To simplify the process of configuration, you can apply the mixed mode backup mode globally to all backups and then apply the file level backup mode locally to all servers where you want to perform file level backups.

Specify Backup Modes as a Global Backup Option

Global options affect all VM backups in your environment at the job level. Use the steps that follow specify backup modes that will apply to all VM backup jobs.

To specify backup modes as a global backup option

1. Open the Backup Manager window and click the Source tab.

   The Source directory tree appears.

2. Expand the VMware Systems object or the Microsoft Hyper-V Systems object and browse to the VM that you want to back up.

   Click Options on the Toolbar.

   The Options dialog opens.

3. Click the Agent Options tab and then click Agent for Virtual Machines.

4. Specify a backup mode by clicking one of the options that follow:

   ■ **File Mode--**Lets you protect individual files and directories. File mode backup lets you perform the tasks that follow:

     – Back up files and directories at file level granularity contained in VM.

     – Perform full, incremental, and differential backups.

     – Restore data at file level granularity.

     – Process multiple streams of data simultaneously using the Multistreaming option.

     – Filter data using the Filter option.

     Note: The elapsed time required to perform a file level backup of a full VM is greater than the elapsed time required to perform a raw (full VM) level backup of the same volume.

■ **Raw Mode--**Lets you protect entire systems for disaster recovery. Raw mode backup lets you perform the tasks that follow:

– Perform full backups of full VM images only.

– Process multiple streams of data simultaneously using the multistreaming option.

Note: Raw mode does not let you restore data at file level granularity or filter raw (full VM) data. Filters applied to raw mode (full VM) backups are ignored at runtime.

■ **Mixed Mode--**Mixed mode is the default backup mode. Mixed mode lets you perform the tasks that follow:

– Perform GFS and rotation backup jobs that consist of weekly full backups in full VM (raw) mode and daily incremental and differential backups in file mode in a single backup job.

Note: Rotation and GFS rotation jobs are advantageous in that they contain backup data that provides you with daily protection (file level backups) and disaster recovery protection (raw, full VM backups) in a single backup job.

■ **Allow file level restore--**Lets you back up data using Raw Mode efficiency and restore data with File level granularity. To perform granular file level restores from raw (full VM) backups, you must specify the name of the CA ARCserve Backup server on your VMs. For more information, see Specify the Name of the CA ARCserve Backup Server (see page 51).

Allow file level restore lets you perform the tasks that follow:

– Restore data at file level granularity from Raw Mode (full VM) backups.

– Restore data at file level granularity from Mixed Mode backups.

With the Allow file level restore option, CA ARCserve Backup demonstrates the following behavior:

■ You can use the Allow file level restore option with all types of backups, including custom backups, rotation backups, and GFS rotations that consist of full, incremental, and differential backups. The full backups are captured in raw (full VM) mode and the incremental and differential backups are captured in file level backup mode. If you do not specify Allow file level restore, CA ARCserve Backup restores only the incremental and differential backups. The full backup, which is captured in Raw mode, is not packaged with the restore.

■ CA ARCserve Backup cannot restore data at file level granularity when performing raw mode backups and mixed mode backups of data that resides on dynamic disks connected to Windows 2000 Server systems.

■ **Incremental / Differential Method for VMware VM--**Lets you specify the communication method that CA ARCserve Backup will use to transfer incremental and differential backup data on VMware VMs to the backup proxy system.

– **Use VCB/VDDK--**Lets CA ARCserve Backup use VMware Virtual Consolidated Backup communication to transfer incremental and differential backup data to the backup proxy system. You should specify this option when you want to reduce the load on your network.

Note: Use VCB/VDDK is the default setting.

– **Use Client Agent for Windows--**Lets CA ARCserve Backup use Client Agent for Windows to execute the backup. With this option specified, CA ARCserve Backup performs a filesystem backup and does not require the backup proxy system to complete the backup.

Click OK.

The backup mode is applied to all of your VM backups.

5. Click OK to close the Options dialog.

Specify Backup Modes as a Local Backup Option

Local options affect individual VM backups at the job level. Use the steps that follow to specify backup modes that apply to individual backup jobs.

To specify backup modes as a local backup option

1. Open the Backup Manager window and click the Source tab.

The Source directory tree appears.

2. Expand the VMware Systems object or the Microsoft Hyper-V Systems object and browse to the VM that you want to back up.

Right-click the VM and select Local Options from the pop-up menu.

The Backup Mode dialog opens.

3. Click Override Global Backup Options. For more information see Backup Modes (see page 70).

Specify a backup mode by clicking one of the options that follow:

■ **File Mode--**Lets you protect individual files and directories. File mode backup lets you perform the tasks that follow:

  – Back up files and directories at file level granularity contained in VM.

  – Perform full, incremental, and differential backups.

  – Restore data at file level granularity.

  – Process multiple streams of data simultaneously using the Multistreaming option.

  – Filter data using the Filter option.

  Note: The elapsed time required to perform a file level backup of a full VM is greater than the elapsed time required to perform a raw (full VM) level backup of the same volume.

■ **Raw Mode--**Lets you protect entire systems for disaster recovery. Raw mode backup lets you perform the tasks that follow:

  – Perform full backups of full VM images only.

  – Process multiple streams of data simultaneously using the multistreaming option.

  Note: Raw mode does not let you restore data at file level granularity or filter raw (full VM) data. Filters applied to raw mode (full VM) backups are ignored at runtime.

■ **Mixed Mode--**Mixed mode is the default backup mode. Mixed mode lets you perform the tasks that follow:

  – Perform GFS and rotation backup jobs that consist of weekly full backups in full VM (raw) mode and daily incremental and differential backups in file mode in a single backup job.

  Note: Rotation and GFS rotation jobs are advantageous in that they contain backup data that provides you with daily protection (file level backups) and disaster recovery protection (raw, full VM backups) in a single backup job.

■ **Allow file level restore--**Lets you back up data using Raw Mode efficiency and restore data with File level granularity. To perform granular file level restores from raw (full VM) backups, you must specify the name of the CA ARCserve Backup server on your VMs. For more information, see Specify the Name of the CA ARCserve Backup Server (see page 51).

Allow file level restore lets you perform the tasks that follow:

– Restore data at file level granularity from Raw Mode (full VM) backups.

– Restore data at file level granularity from Mixed Mode backups.

With the Allow file level restore option, CA ARCserve Backup demonstrates the following behavior:

■ You can use the Allow file level restore option with all types of backups, including custom backups, rotation backups, and GFS rotations that consist of full, incremental, and differential backups. The full backups are captured in raw (full VM) mode and the incremental and differential backups are captured in file level backup mode. If you do not specify Allow file level restore, CA ARCserve Backup restores only the incremental and differential backups. The full backup, which is captured in Raw mode, is not packaged with the restore.

■ CA ARCserve Backup cannot restore data at file level granularity when performing raw mode backups and mixed mode backups of data that resides on dynamic disks connected to Windows 2000 Server systems.

Click OK.

The Backup Mode dialog closes and the backup mode is applied.

How the Agent Processes Incremental and Differential Backups on VMware VMs

The agent uses the following file properties as the file selection criteria for incremental and differential backups:

- **File creation or modification date--**VCB communication backups.

  The agent communicates with the VM using VCB. The agent detects and filters data based on file creation time or modify time. Using this communication method, the agent backs up all files with a creation time or modified that is later than the last full or incremental backup time, regardless of the file attributes.

- **Archive bit--**Client Agent for Windows communication backups.

  The agent communicates with the VM using the Client Agent for Windows. The agent detects and filters file based on the archive bit. If the agent detects system state files and files statused "FilesNotToBackup," the agent excludes the detected files from the incremental or differential backup.

Note: For more information about the Use VCB backup option and the Use Client Agent for Windows communication backups, see Specify Backup Modes as a Global Backup Option (see page 73).

Back Up Data Residing on VMware Virtual Machines

CA ARCserve Backup lets you back up data that resides in VMware VMs. Use the following steps to submit backup jobs on local disk-based virtual machines (VMs) and SAN-based VMs.

Note: For information about the limitations of backing up with VCB, see Backup and Restore Limitations on Virtual Machines (see page 23).

To back up data residing on VMware VMs

1. Open the Backup Manager and select the Source tab.

    The Backup Manager source directory tree displays.

2. Expand the VMware Systems object.

    The backup proxy systems, VMware ESX Host systems, vCenter Server systems, and VMs in your environment appear.

3. Click the check box next to the objects that you want to back up. You can select volumes, an entire node, or any combination thereof as the source.

    Note: For information about browsing volumes, see How to Browse Virtual Machine Backup Volumes (see page 67).

4. Specify a Backup Mode for the job.

   Note: For more information about backup modes, see Backup Modes (see page 70).

5. To filter VM backup data, right-click the VM and select Filter from the pop-up menu.

   Note: For more information about filters, see Filter VM Backup Data (see page 84).

   Important! If the Backup Mode specified is Raw Mode and you specify filters, CA ARCserve Backup does not filter the VM backup data.

6. To specify where you want to store the backup job, click the Destination tab or the Staging tab.

   Note: For more information about specifying a destination or using staging to back up data, see the *Administration Guide* or the online help.

   To use multistreaming to transmit backup data, click the Multi Stream check box.

7. To specify the scheduling options for the job, click the Schedule tab.

   Note: For more information about job scheduling options, see the *Administration Guide* or the online help.

8. To specify global filters, click Filter on the toolbar.

   The Filter dialog opens.

   Note: For more information about filtering VM data, see Filter VM Backup Data (see page 84). For more information about specifying filters, click the Help button on the Filter dialog.

9. Click Submit on the toolbar to submit the job.

   The Security and Agent Information dialog opens.

   You must provide credentials the VMware ESX Host system or the vCenter Server system and the backup proxy system to submit the job, as shown in the following illustration:

10. Select the respective server and click the Security button on the Security and Agent Information dialog.

    The Security dialog opens.

11. Enter your login credentials in the User name and Password fields and click OK.

    Note: CA ARCserve Backup does not support logging in to systems with passwords that are greater than 23 characters. If the password on the system you are attempting to log in to is greater than 23 characters, you must modify the password on the agent system such that it is 23 characters or less, and then you can log in to the agent system.

    CA ARCserve Backup applies your security credentials and the Submit Job dialog opens.

12. Complete the required fields on the Submit Job dialog and click OK.

    Note: For more information about Submitting Jobs, click Help on the Submit Job dialog.

    CA ARCserve Backup submits the job. For more information about viewing job status and other job-related tasks, see the *Administration Guide* or the online help.

How the Agent Names Mount Points

CA ARCserve Backup uses a different naming convention for mount points for each type of VM backup.

For VCB Framework backups, CA ARCserve Backup uses the following naming convention:

- CA ARCserve Backup creates a mount point directory (snapshot) on the backup proxy system when it executes a VCB backup. CA ARCserve Backup names the snapshot using the convention that follows:

    VCB-BACKUP

- After the backup is complete, CA ARCserve Backup deletes the VM snapshot from the ESX Server system. If the backup does not complete successfully, the snapshot remains on the backup proxy system until the next backup job starts and deletes the snapshot. Subsequent backups will fail when CA ARCserve Backup cannot delete the snapshot from the backup proxy system.

For VDDK backups, CA ARCserve Backup uses the following naming convention:

- CA ARCserve Backup creates a mount point directory (snapshot) on the backup proxy system when it executes a VDDK backup. CA ARCserve Backup names the snapshot using the convention that follows:

  _ARCServe_Backup__ J<JobID>_S<SessionID>_date_time

- After the backup is complete, CA ARCserve Backup deletes the snapshot from the backup proxy system. If the backup does not complete successfully, the snapshot remains on the backup proxy system until you delete it from the ESX Server system. Subsequent backups are not affected by snapshots that remain on the backup proxy system.

Back Up Data Residing on Hyper-V Virtual Machines

Use the steps that follow to submit backup jobs on local disk-based virtual machines (VMs) and SAN-based VMs.

Note: For information about the limitations of backing up with VCB, see Backup and Restore Limitations on Virtual Machines (see page 23).

To back up data residing on Hyper-V VMs

1. Open the Backup Manager and select the Source tab.

    The Backup Manager source directory tree displays.

2. Expand the Microsoft Hyper-V Systems object.

    The Hyper-V systems in your environment appear.

3. Click the check box next to the objects that you want to back up. You can select volumes, an entire node, or any combination thereof as the source.

    Note: For information about browsing volumes, see How to Browse Virtual Machine Backup Volumes (see page 67).

4. Specify a Backup Mode for the job.

    Note: For more information about backup modes, see Backup Modes (see page 70).

5. To filter VM backup data, right-click the VM and select Filter from the pop-up menu.

    Note: For more information about filters, see Filter VM Backup Data (see page 84).

    Important! If the Backup Mode specified is Raw Mode and you specify filters, CA ARCserve Backup does not filter the VM backup data.

6. To specify where you want to store the backup job, click the Destination tab or the Staging tab.

   Note: For more information about specifying a destination or using staging to back up data, see the *Administration Guide* or the online help.

   To use multistreaming to transmit backup data, click the Multi Stream check box.

7. To specify the scheduling options for the job, click the Schedule tab.

   Note: For more information about job scheduling options, see the *Administration Guide* or the online help.

8. To specify global filters, click Filter on the toolbar.

   The Filter dialog opens.

   Note: For more information about filtering VM data, see Filter VM Backup Data (see page 84). For more information about specifying filters, click the Help button on the Filter dialog.

9. Click Submit on the toolbar to submit the job.

   The Security and Agent Information dialog opens.

   You must provide credentials the Hyper-V host system to submit the job, as shown in the following dialog:

10. Select the respective server and click the Security button on the Security and Agent Information dialog.

    The Security dialog opens.

11. Enter your login credentials in the User name and Password fields and click OK.

    Note: CA ARCserve Backup does not support logging in to systems with passwords that are greater than 23 characters. If the password on the system you are attempting to log in to is greater than 23 characters, you must modify the password on the agent system such that it is 23 characters or less, and then you can log in to the agent system.

    CA ARCserve Backup applies your security credentials and the Submit Job dialog opens.

12. Complete the required fields on the Submit Job dialog and click OK.

    Note: For more information about Submitting Jobs, click Help on the Submit Job dialog.

    CA ARCserve Backup submits the job. For more information about viewing job status and other job-related tasks, see the *Administration Guide* or the online help.

Miscellaneous Tasks

This section contains the following topics:

How the Agent Supports the Preflight Check Utility

The preflight check (PFC) utility lets you run vital checks on the CA ARCserve Backup server and agents to detect conditions that may cause backup jobs to fail.

For virtual machines backups, the PFC utility checks the status of the Client Agent for Windows that is running on the backup proxy system or the Hyper-V host system. The PFC does not check the status of the VMs that you specified for the backup on the VMware ESX Host system or the vCenter Server system.

Note: For more information about using the PFC utility, see the *Administration Guide*.

The PFC utility performs the following checks on VMware ESX Host backups under the following scenarios:

■ A backup job is submitted using the agent. The Client Agent for Windows is running on the backup proxy system.

The following message displays:

Note: The target node <Proxy System's Name/IP> is a VMware Proxy System. PFC only verifies the status of Client Agent on the VMware Proxy Server. It will not check the status of Virtual Machines which you have selected for backup on the VMware ESX Server.

■ A backup job is submitted using the agent. The Client Agent for Windows is not running on the backup proxy system.

The following message displays:

Issues: Failed to connect to the client agent on <Proxy System's Name/IP>. Ensure that the client agent on <Proxy System's Name/IP> is running.
Note: The target node <Proxy System's Name/IP> is a VMware Proxy System. PFC only verifies the status of Client Agent on the VMware Proxy Server. It will not check the status of Virtual Machines which you have selected for backup on the VMware ESX Server.

Filter VM Backup Data

CA ARCserve Backup lets you filter data when you are performing a file mode backup or a rotation, mixed mode backup that consists of incremental backups, differential backups, or both. This capability lets you perform the following tasks:

■ Back up only the data on the VMs based on, for example, file pattern, date range, date modified, file size, and so on.

■ Selectively back up files, folders, or both in a selected volume.

■ Apply filtering criteria globally or locally to your backup jobs.

Note: A *global* filter applies filters to all of your backup jobs while a *local* filter applies filters only to the selected VM.

To filter VM backup data

1. Open the Backup Manager window and browse to the VM that you want to filter.

2. Do one of the following actions:

   ■ To apply global filters to the backup operation, click the Filter toolbar button on the Backup Manager window.

   ■ To apply local filters to the backup operation, right-click the VM object and select Filter from the pop-up menu

   The Filter dialog opens.

3. Specify the filters required to complete the backup job.

   Note: For more information about filtering data, click Help on the Filter dialog.

Agent Log Files

CA ARCserve Backup includes log files that provide you with details about backup operations executed using the Agent for Virtual Machines. CA ARCserve Backup stores the log files on the backup proxy system and the Hyper-V host system in the location that follows:

C:\Program Files\CA\ARCserve Backup Client Agent for Windows\Log

The log files that follow apply to VMware VM backups:

ca_vcbpopulatedb.log

Lets you view messages about VMware VM backup jobs.

The messages are prefixed by the Job ID number and the Session number, which lets you distinguish jobs that are running simultaneously.

   ■ **Maximum log size--**By default, the agent limits the size of ca_vcbpopulatedb.log to 250 kb. To change the limit (increase or decrease the limit), create the registry that follows:

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

   Value data: Specify the maximum log size that you require.

mount_jnl.log

Lets you view information about mount and unmount operations.

The log file contains the parameters specified for each mount and unmount operation.

ca_vcbmounteroutput_xxx.log

Lets you view information about mount and unmount operations that fail.

- **Maximum log count**--By default, CA ARCserve Backup saves a maximum of 1000 log files. You can specify a different number of log files by modifying the Value data in the registry key that follows:

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

  Note: When the number of ca_vcbmounteroutput_xxx.log logs reaches the maximum value, CA ARCserve Backup overwrites ca_vcbmounteroutput_000.log on the next mount operation and deletes ca_vcbmounteroutput_001.log.

- **Maximum mount log size--**By default, the agent limits the size of ca_vcbmounteroutput_xxx.log to 250 kb. To change the limit (increase or decrease the limit), create the registry that follows:

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

  Value data: Specify the maximum log size that you require.

The log file that follows applies to Hyper-V VM backups:

Hyper.log

Lets you view messages about Hyper-V VM backups and restores.

The messages are prefixed by the Job ID number and the Session number, which lets you distinguish jobs that are running simultaneously.

The log file that follows applies to VMware and Hyper-V VM backups:

vmdbupd.log

Lets you view information about auto-populate executions.

The log file contains the parameters specified and the status of all automatic executions of ARCserve VMware Configuration Tool (see page 54) and ARCserve Hyper-V Configuration Tool (see page 59).

How the Agent Protects Volumes Mounted from Virtual Hard Disks

This section contains the following topics:

Overview of Virtual Hard Disks

A virtual hard disk (VHD) is an image format that contains the contents of a disk and virtual operating systems and their associated applications in a single file using virtualization methodologies. Thus, you can use VHD files (.vhd), which reside in container volumes, to run operating systems natively from VHDs. Container volumes can include a collection of operating system files, data files, drivers, and so on that let the operating system mounted in the VHD function independently of the VHD where it resides.

CA ARCserve Backup protects the volumes mounted in VHDs.

Limitations of Protecting Volumes Mounted from Virtual Hard Disks

Consider the following limitations when backing up VHDs:

- CA ARCserve Backup cannot recover data at file level granularity when you back up VHD volumes mounted inside the VM.

  Be aware of the following considerations:

  - This limitation applies only when using the raw (full VM) backup mode with the Allow file level restore option specified.

  - This limitation does not apply to backups executed using the Client Agent for Windows. CA ARCserve Backup cannot recover data at file level granularity using only the Client Agent for Windows.

- CA ARCserve Backup does not support using VSS to back up nested VHD volumes that contain more than one level of data.

  Consider the following example:

  - Disk 0 contains drive C:\.

  - Drive C:\ contains mounted volume drive V:\.

  - Drive V:\ contains mounted volume drive W:\.

  CA ARCserve Backup cannot detect the .vhd file that resides in drive V:\.

  To protect data files that reside in drive W:\, you must submit the backup using Client Agent for Windows with CA ARCserve Backup Agent for Open Files.

■ CA ARCserve Backup creates separate backup sessions for mounted volumes that contain VHDs.

Consider the following example:

– A server contains physical disk (C:\) that contains VHDs D:\ and E:\. VHD files (D.vhd and E.vhd) that reside in C:\ are mounted as drive D:\, and drive E:\. Drive D:\ is mounted to C:\MountD, and drive E:\ is mounted to C:\MountE.

– If you back up C:\MountD and specify the Traverse Directory Junctions and Volume Mount Points option, CA ARCserve Backup creates separate backup sessions for drive D:\ and C:\MountD.

– If you back up C:\MountE and specify the Traverse Directory Junctions and Volume Mount Points option and the Backup Mount Points as Part of the volume that they are mounted on option, CA ARCserve Backup creates separate backup sessions for drive E:\ and C:\MountE.

Note: The following options are located on the Backup Manager, Global Options, Advanced dialog:

■ Traverse Directory Junctions and Volume Mount Points

■ Backup Mount Points as Part of the volume that they are mounted on

How the Agent Protects Cluster Shared Volumes

This section contains the following topics:

Overview of Cluster Shared Volumes

CA ARCserve Backup lets you protect VMs located on CSVs using CA ARCserve Backup Agent for Virtual Machines.

A cluster shared volume (CSV) is a Windows Server 2008 R2 feature that lets you cluster multiple Hyper-V virtual machines (VMs) distributed across several cluster nodes. The clustered Hyper-V VMs can access all files mounted in the CSVs simultaneously.

Although you can store files of any type in CSVs, Microsoft recommends that you create only VMs in CSVs. As a best practice, we suggest that you support this recommendation, and that you back up the data that resides in the VMs using the Agent for Virtual Machines.

CA ARCserve Backup lets you protect CSVs residing in Hyper-V configured systems using Microsoft Volume Shadow Copy Service technology. Microsoft Volume Shadow Copy Service is a component that is included with CA ARCserve Backup Agent for Open Files. For more information, see the *Administration Guide*.

Limitations of Protecting Cluster Shared Volumes

Consider the following limitations when backing up CSVs:

- The nodes sharing the CSVs must be able to access the shared volumes. The shared volumes are located in the following directory:

  <system drive>\ClusterStorage

- Backups of nodes sharing CSVs cannot run concurrently. This approach ensures that the node that you are backing up has full control of input and output operations to the shared storage while the backup is in progress. For example, node A and node B are sharing CSV 1. You submit jobs to back up node A and node B. The backup of node B must start after the backup of node A completes.

- When submitting backups consisting of VMs that reside on CSVs in Hyper-V systems, you must specify the Windows domain account for the Hyper-V systems in the Backup Manager Source tree. In addition, the Windows domain account must have backup operator and cluster administrator privileges on the Hyper-V system. This approach helps to ensure that backups of VMs that reside on CSVs in Hyper-V systems complete successfully. If you do not provide valid domain credentials for the Hyper-V systems, backup jobs will fail and generate the following message:

  AE0603   Failed to create VSS shadow copy for the VM on the Hyper-V host machine.

Chapter 5: Restoring Data

This section contains the following topics:

Restore VMware Virtual Machine Data

This section contains the following topics:

How to Browse VMware Sessions

You use the same process to restore data contained in a VM as that of restoring from any other physical server.

Note: For more information about restoring data, see the *Administration Guide* or the online help.

However, restoring data from a VM presents the following limitations:

- You can restore file level backups (File Mode) to their original location or an alternate location.

  Note: To restore files to their original location on a VM, the Client Agent for Windows must be installed on the VM.

- You can restore raw (full VM) level backups to an alternate location only.

When you select the Restore by Tree option on the Source tab in the Restore Manager, the VM backups performed in raw (full VM) mode display as VMware Raw Image. When you perform file mode backups, the corresponding volumes in the VM display.
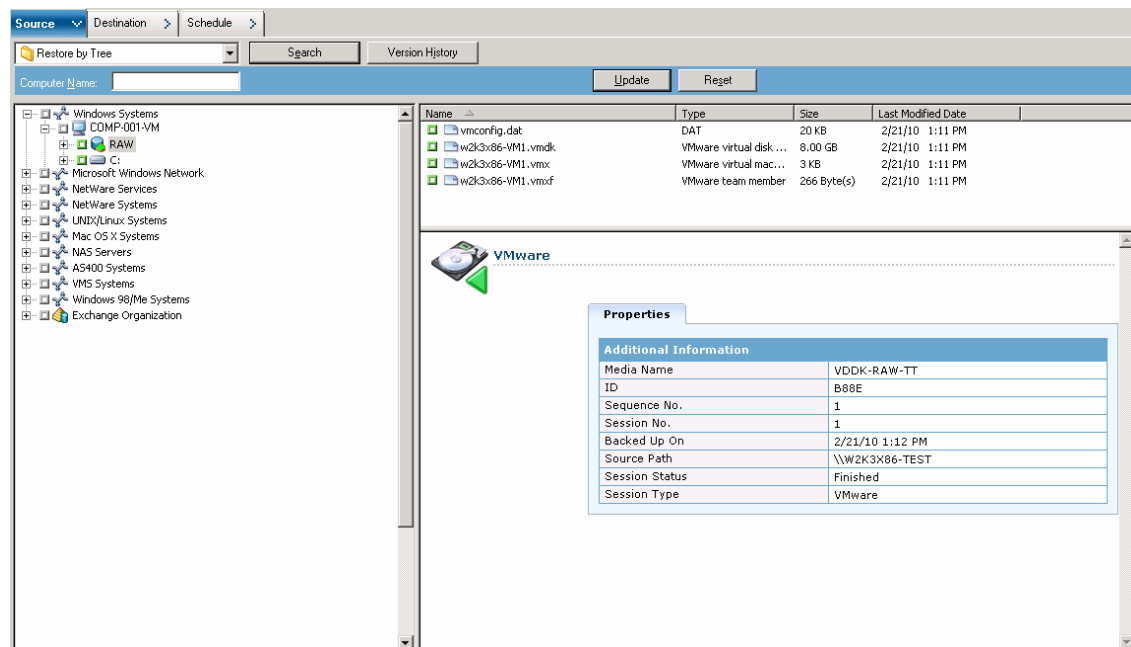
The session properties section of the Restore Manager window displays the following information about the VMware backup data:

- **VMware Proxy--**Indicates the name of the backup proxy system that was used to back up this VM.

- **VMware vCenter Server/VMware ESX Host--**Indicates the name of the VMware ESX Host system or the vCenter Server system from which the VM was running when the backup job was submitted.

- **Host Name--**Indicates the host name of the VM involved with the backup job.

- **Session Method--**Indicates the type of backup method that was used to back up the VM (for example, Raw and File).

How You Can Recover VMs Using vSphere

The method the agent uses to recover VMs is dependent upon the approach that you used to back up the VMs.

Note: For more information about backup approaches, see Specify a Backup Approach (see page 38).

For VCB Framework backups, review the following considerations:

- VMware Converter (stand-alone) or VDDK can be used to recover VCB backup data.

- If VDDK and VMware Converter (stand-alone) are installed on the backup proxy system, VMware Converter is used to recover the VM, if backup was executed using VCB Framework.

- If VDDK is installed on the backup proxy system and VMware Converter is not installed on the backup proxy system, VDDK is used to recover the VM.

- You can recover VM backup data using VDDK with ESX Server 3.0.x and ESX Server 3.5 if the backup was executed using CA ARCserve Backup r12 SP1 and CA ARCserve Backup r12.5.

For VDDK backups, review the following considerations:

- VDDK backup data must be recovered using VDDK. VMware Converter cannot be used to recover VDDK backups.

- ESX Server 3.5 and ESX Server 4.0 can be used to recover VM data that was backed up using ESX Server 3.5.

- ESX Server 3.5 cannot be used to recover VM data that was backed up using ESX Server 4.0.

- When recovering VDDK backup data using VDDK, the recovery process does not require free disk space on the backup proxy system.

- When recovering VCB backup data using VDDK, the recovery process restores the data to the backup proxy system, VDDK reads the backup data, and then VDDK restores the data to the ESX Server system.

Restore VMware Virtual Machines

The process of recovering VMware VMs lets you recreate the entire VM and restore its data. Using this process you can recover a VM from a disaster and clone a VM.

Browsing the Recover VM Window

The Recover VM window lets you browse, select, and modify various fields. When you rest your mouse pointer over an editable field, the background color of the field appears yellow, as illustrated by the following:

Roll your mouse pointer over a field. The yellow background denotes an editable field.

To modify an editable field, select the target field and then click the ellipsis to browse the field as illustrated by the following:

Click the ellipsis to browse.

Considerations

Be aware of the following considerations:

- CA ARCserve Backup restores the VM's backup data to the backup proxy system in a temporary mount location, and then restores the data to the VMware ESX Host system.

- VMware Converter version 3.0.2 and later must be installed on the backup proxy system. CA ARCserve Backup uses the VMware Converter tools to restore VCB images of VMs.

  Note: For information about VMware Converter, see http://www.vmware.com/products/converter.

To recover VMware virtual machines

1. Open the Restore Manager, click the Source tab, and select Recover Virtual Machine from the drop-down list as illustrated by the following screen:
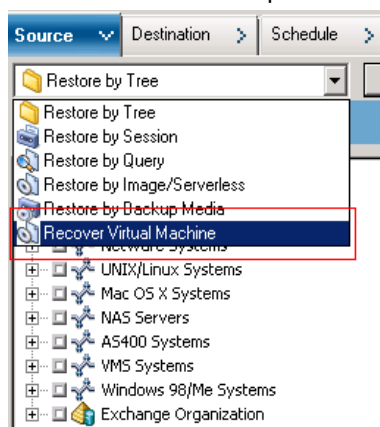
The Recover Virtual Machine window opens.

2. To search for a VMware VM, perform one of the following actions and then go to the next step.

    ■   To search for a specific VM, specify the name of the VM in the Virtual Machine Name field, and click Query.

        The Virtual Machine Name specified displays in the VM list.

    ■   To search for all VMs, select << ANY >> in the Virtual Machine Name field and click Query.

        All the VMs in your environment display in the VM list.

    ■   To search using a partial Virtual Machine Name, replace the unknown characters with an asterisk, and click Query.

        The Virtual Machines equaling the search criteria display in the VM list.

        Example: Using 100-* returns the names of all VMs that start with 100-, such as 100-1, 100-01, and 100-001.

    ■   In the Search for virtual machine box, click VMware.

        All the VMware VMs in your environment display in the VM list.

3. Complete the following fields in the VM list.

    ■   **VM Name (DNS Name)--**Check the check box next to VM Name to specify the VMs that you want to recover.

        Note: CA ARCserve Backup processes the restore operations sequentially when you specify more than one VM.

    ■   **Backup Versions--**Lets you specify a Backup Version.

        You can accept the Backup Version displayed or click in the Backup Versions field and then click the ellipsis to search for multiple versions of the backup data.

    ■   **Proxy Machine--**Lets you specify the backup proxy system and the security information required to recover the VM image.

        You can accept the Proxy Machine displayed or click in the Proxy Machine field and then click the ellipsis to search for and specify a different backup proxy system.

    ■   **Path--**Lets you specify the path to mount the VM image.

        You can accept the Path displayed or click in the Path field to specify an alternate path for the temporary VM mount directory.

    ■   **VMware ESX Host Name--**Lets you specify the ESX Server and the security information required to recover the VM image.

        You can accept the VMware ESX Host Name displayed or click in the VMware ESX Host Name field and then click the ellipsis to search for and specify a different VMware ESX Host system.

- **Data Store--**Lets you specify the Data Store associated with the VMware ESX Host system.

    You can accept the Data Store name displayed associated with the VMware ESX Host system or click in the Data Store field to specify the Data Store of the target VMware ESX Host system.

    Note: Data Store is a case-sensitive value.

4. Click Options on the toolbar.

    The Global Options dialog opens.

5. Click the Operation tab and specify the options that follow:

    Note: The options that follow do not appear on the Operation tab unless the Recover Virtual Machine method is specified.

    - **Power on VMware or Hyper-V VM after restore--**Lets you power on the VM after the recovery is complete.

        Default value: Enabled.

        Example: Specify this option when you must use the VM immediately after the recovery is complete.

    - **Overwrite VMware VM, if it exists--**Lets you overwrite the VM, if the VM exists.

        Default value: Enabled.

        When you restore a VMware VM, CA ARCserve Backup detects the VMs that reside in the host system. If the VM exists in the host system, this option lets you overwrite the VM using the existing VM UUID and host name.

        Note: For troubleshooting information, see The Agent Does Not Delete Existing VMs after a Recover VM Job Completes (see page 108).

6. Click OK.

    The options are applied.

7. Click Submit to submit the restore job.

    The Submit Job dialog opens.

8. On the Submit Job dialog, select Run Now to run the job immediately, or select Run On and select a future date and time when you want the job to run.

    Enter a description for your job and click OK.

    The job is submitted.

    Note: For more information about submitting jobs, see the *Administration Guide*.

Restore Hyper-V Virtual Machine Data

This section contains the following topics:

How to Browse Hyper-V Sessions

You use the same process to restore data contained in a VM as that of restoring from any other physical server.

Note: For more information about restoring data, see the *Administration Guide* or the online help.

However, restoring data from a VM presents the following limitations:

- You can restore file level backups (File Mode) to their original location or an alternate location.

  Note: To restore files to their original location on a VM, the Client Agent for Windows must be installed on the VM.

- You can restore raw (full VM) level backups to an alternate location only.

Recover Hyper-V Virtual Machines

The process of recovering Hyper-V VMs lets you recreate the entire VM and restore its data. Using this process you can recover a VM from a disaster and clone a VM.

Browsing the Recover VM Window

The Recover VM window lets you browse, select, and modify various fields. When you rest your mouse pointer over an editable field, the background color of the field appears yellow, as illustrated by the following:

To modify an editable field, select the target field and then click the ellipsis to browse the field as illustrated by the following:

Considerations

Be aware of the following considerations:

- The target VM should be powered off and deleted from the system or renamed. If the VM is not powered off and deleted or renamed, the restore process overwrites the data on the target VM.

To recover Hyper-V virtual machines

1. Open the Restore Manager, click the Source tab, and select Recover Virtual Machine from the drop-down list as illustrated by the following screen:
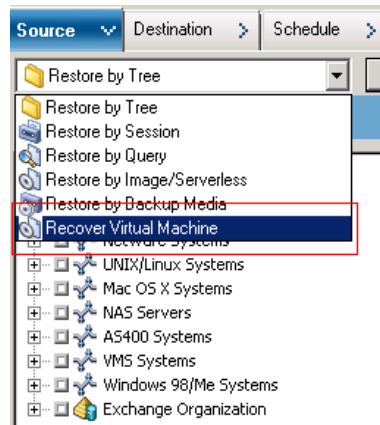
The Restore Virtual Machine window opens as illustrated by the following screen:
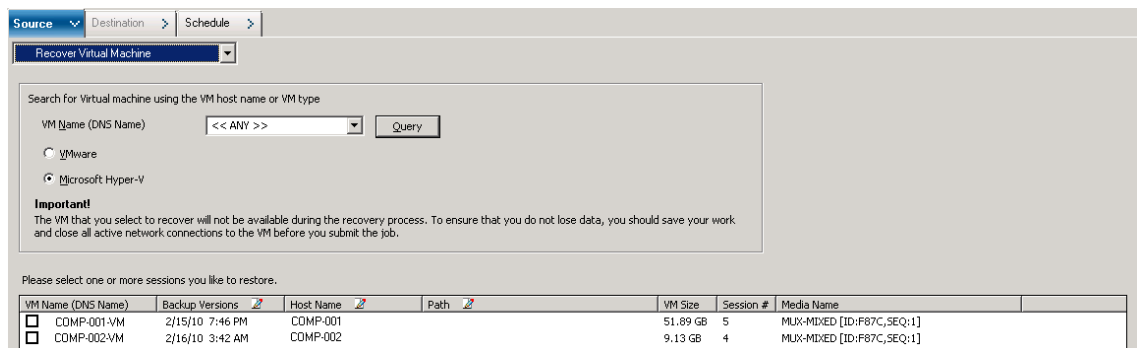
2. To search for a Hyper-V VM, perform one of the following actions and then go to the next step.

   ■ To search for a specific VM, specify the name of the VM in the Virtual Machine Name field, and click Query.

     The Virtual Machine Name specified displays in the VM list.

   ■ To search for all VMs, select << ANY >> in the Virtual Machine Name field and click Query.

     All the VMs in your environment display in the VM list.

   ■ To search using a partial Virtual Machine Name, replace the unknown characters with an asterisk, and click Query.

     The Virtual Machines equaling the search criteria display in the VM list.

     Example: Using 100-* returns the names of all VMs that start with 100-, such as 100-1, 100-01, and 100-001.

   ■ In the Search for virtual machine box, click Hyper-V.

     All the Hyper-V VMs in your environment display in the VM list.

3. Complete the following fields in the VM list.

   ■ **VM Name (DNS Name)--**Check the check box next to VM Name to specify the VMs that you want to recover.

     Note: CA ARCserve Backup processes the restore operations sequentially when you specify more than one VM.

   ■ **Backup Versions--**Lets you specify a Backup Version.

     You can accept the Backup Version displayed or click in the Backup Versions field and then click the ellipsis to search for multiple versions of the backup data.

   ■ **Host Name--**Lets you specify the host Hyper-V system and the security information required to recover the VM image.

     If you want to recover the Hyper-V system to a different Hyper-V host, you must specify the directory where you want to recover the VM image.

   ■ **Path--**Lets you specify the path where you want to recover the VM image.

     Note: If the Path field is blank, CA ARCserve Backup recovers the VM image to its original location.

4. Click Options on the toolbar.

   The Global Options dialog opens.

5. Click the Operation tab and specify the option that follows:

   Note: The option that follows does not appear on the Operation tab unless the Recover Virtual Machine method is specified.

   ■ **Power on VMware or Hyper-V VM after restore--**Lets you power on the VM after the recovery is complete.

   Default value: Enabled.

   Example: Specify this option when you must use the VM immediately after the recovery is complete.

6. Click OK.

   The options are applied.

7. Click Submit to submit the restore job.

   The Submit Job dialog opens.

8. On the Submit Job dialog, select Run Now to run the job immediately, or select Run On and select a future date and time when you want the job to run.

   Enter a description for your job and click OK.

   The job is submitted.

   Note: For more information about submitting jobs, see the *Administration Guide*.

Recover Hyper-V Virtual Machines to Alternate Locations

CA ARCserve Backup lets you recover Hyper-V backup data to an alternate location and protect VMs that reside on unnamed volumes.

Note: An unnamed volume is a volume that does not have an assigned drive letter.

These capabilities let you do the following:

- Recover virtual machines (VMs) to the same or a different Windows Server 2008 Hyper-V system.

- Create directories (with and without drive letters) on the target VMs during the recovery process, if the directories do not exist.

The Recover VM screen in the Restore Manager contains controls that let you perform the following tasks:

- Recover Hyper-V VMs to an alternate location where Hyper-V server is a Windows Server 2008 R2 Hyper-V system.

- Specify paths to an alternate location on the target Windows Server 2008 R2 Hyper-V system.

Be aware of the following behavior:

- If you specify an alternate path, CA ARCserve Backup takes the entire path from backup set, with the exception of the root drive or volume name, and adds it to the specified path.

Restore Data at File Level Granularity

This topic describes how to restore data that was backed up using the backup modes that follow:

- File mode

- Raw mode with the Allow file level restore option specified

- Mixed mode with the Allow file level restore option specified

    Note: For more information, see Backup Modes (see page 70).

You can use these steps to perform restore operations on local disk-based virtual machines (VMs) and SAN-based VMs. You would restore file level data that was backed up on a VM when a file is corrupt or deleted in error, to recover a system from a disaster, or to clone a system. You use the same process to restore file level backup data as that of restoring any Windows-based client agent file.

Note: For more information about restoring data, see the *Administration Guide*.

When you restore file level backup data, consider the following:

■ You can browse and restore data at directory and file granularity only if the data was backed up using the file level mode, the raw (full VM) backup mode with the Allow file level restore option specified, or the Mixed backup mode with the Allow file level restore option specified.

Note: For more information, see Backup Modes (see page 70).

■ The current version of the Client Agent for Windows must be installed on the destination system to restore data that was backed up using the Agent for Virtual Machines.

■ When you restore data at file level granularity and specify Restore files to their original location, CA ARCserve Backup intentionally omits Windows system files. Windows system files are usually stored in the directories that follow:

– C:\WINNT (Windows 2000)

– C:\WINDOWS\SYSTEM

– C:\WINDOWS\SYSTEM32

To restore data at file level granularity data

1. Open the Restore Manager, click the Source tab, and select Restore by Tree from the drop-down list.

2. Expand the Windows Systems object and browse to the data that you want to restore.
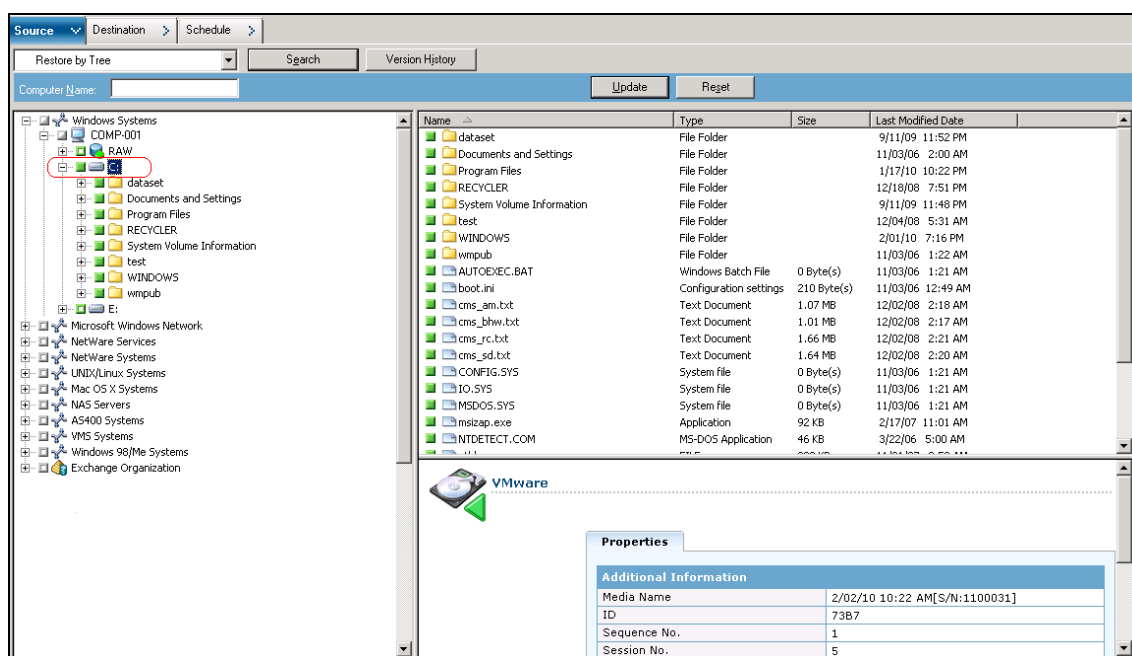
3. Click the Destination tab. Click the Restore files to their original locations check box to restore the files to their original location.

    To restore files to their original location, the Client Agent for Windows must be installed on the VM. If the Client Agent for Windows is not installed on the VM, you can restore the data to any location and then copy the data manually to the VM using a network filesystem share.

    Note: When you restore data at file level granularity and specify Restore files to their original location, CA ARCserve Backup omits Windows system files.

    Important! To restore VMware-based backup sessions to an alternate location, the Client Agent for Windows must be running on the alternate system and the alternate system must appear under Windows Systems object. If you attempt to restore data to system that does not appear under the Windows Systems object, the restore job will fail. To restore data to an alternate location on a local system that is running a Windows x86 operating system, add the system with a fictitious host name and its real IP address under the Windows Systems object on the Restore Manager, Destination tab. Then you can specify the destination as the local system and submit the restore job.

    If the backup data was created from a raw (full-VM) backup, CA ARCserve Backup does not support the Restore files to their original location option.

4. Click the Schedule tab and specify a schedule from the Repeat Method drop-down.

5. Click Submit on the toolbar to submit the restore job.

    The Security and Agent Information dialog opens. To submit the job, you must provide login credentials for the system where you are restoring data.

6. Specify your login credentials in the User name and Password fields and click OK.

    CA ARCserve Backup applies your security credentials and the Submit Job dialog opens.

7. Complete the fields on the Submit Job dialog and click OK.

    The job is submitted.

    Note: For more information about Submitting Jobs, click Help on the Submit Job dialog. For more information about viewing job status and other job-related tasks, see the *Administration Guide* or the online help.

Restore Raw (Full VM) Level Backup Data

Use the steps that follow to perform restore operations on local disk-based virtual machines (VMs) and SAN-based VMs. You would restore raw (full VM) data when you need to recover a system from a disaster or clone a system. You use the same process to restore file level backup data as that of restoring any Windows-based client agent file.

Note: For more information about restoring data, see the *Administration Guide*.

When you restore raw level backup data, consider the following:

■ The current version of the Client Agent for Windows must be installed on the destination system to restore data that was backed up using the Agent for Virtual Machines.

■ You cannot browse and restore data at directory and file level granularity from data that was backed up using raw (full VM) or Mixed mode without specifying the Allow file level restore option.

Restore raw (full VM) level backup data

1. Open the Restore Manager, click the Source tab, and select Restore by Tree from the drop-down list.

    Expand the Windows Systems object and browse to the VMware system or the Hyper-V system that you want to restore.

    Expand the system that you want to restore, and select the data that you want to restore.
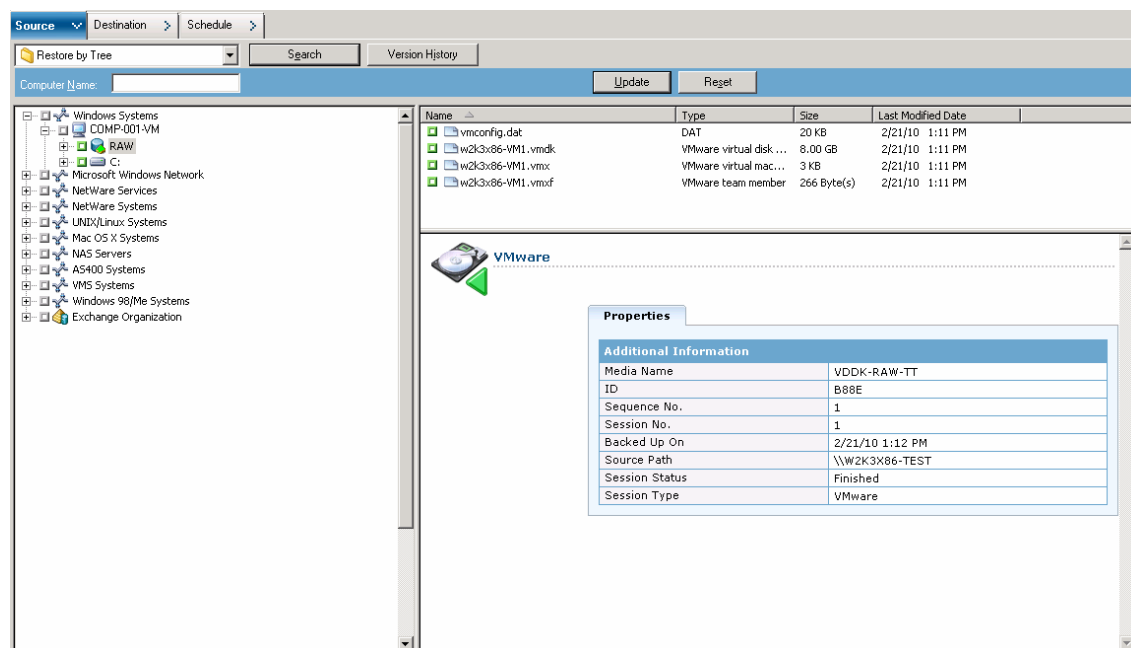
2. Click the Destination tab.

   Specify the location to restore the data.

3. Click the Schedule tab and specify a schedule from the Repeat Method drop-down.

4. Click Submit on the toolbar to submit the restore job.

   The Security and Agent Information dialog opens. To submit the job, you must provide login credentials for the system where you are restoring data.

5. Specify your login credentials in the User name and Password fields and click OK.

   CA ARCserve Backup applies your security credentials and the Submit Job dialog opens.

6. Complete the fields on the Submit Job dialog and click OK.

   The job is submitted.

   Note: For more information about Submitting Jobs, click Help on the Submit Job dialog. For more information about viewing job status and other job-related tasks, see the *Administration Guide* or the online help.

Appendix A: Troubleshooting

This section contains the following topics:

Backup and Recovery Operations

The following topics describe how to troubleshoot backup and recovery operations on systems running VMware vSphere.

The Auto-Populate VM Process Does Not Start On Schedule

Valid on all Windows operating systems supported by CA ARCserve Backup.

Symptom:

The auto-populate VM process does not start on schedule. The frequency of the auto-populate process was changed recently.

Solution:

After you change the frequency of the auto-populate process, the process will start the next calendar day.

Example: Change the Frequency of the Auto-populate VM Process

You change the frequency of the auto-populate VM process to one hour at 11:00 AM on April 5. Although you expect the process to start at 12:00 PM on April 5, it does not start. The auto-populate VM process will start at 12:00 AM on April 6 and execute at one hour intervals.

Agent for Virtual Machines Log Files Do Not Appear on the Backup Proxy System

Valid on all Windows systems functioning as backup proxy systems.

Symptom:

The log files MntJrnl.log and vcbmounter_outputxxxx.log do not appear in the Client Agent log directory on the backup proxy system.

Solution:

This behavior occurs when backing up VM data using VDDK. VDDK does not use the VMware component named vcbmounter to process VCB backups. As such, the backup operation does not generate the mount operation log files MntJrnl.log and vcbmounter_outputxxxx.log.

The vcbmounter Process Does Not Stop After a Backup Job is Canceled

Valid on all Windows systems functioning as backup proxy systems.

Symptom:

The vcbmounter process does not stop running on the backup proxy system after you cancel a VCB Framework backup job.

Solution:

Although backup jobs using VMware VCB Framework can be canceled, the mount and export operations associated with VCB Framework backups do not stop. This behavior occurs because VCB Framework does not provide an option to cancel vcbmounter mount and export operations.

The Agent Does Not Delete Existing VMs after a Recover VM Job Completes

Valid on all supported Windows operating systems.

Symptom:

CA ARCserve Backup may not delete the existing VM on the target ESX Server system in the following scenario:

- You submit a Recover VM job.

- You specified the Overwrite VM global restore option.

- CA ARCserve Backup successfully recovers the VM to the backup proxy system (ESX Server system).

Solution:

This is expected behavior.

The agent combines the UUID and host name of a VM to create a unique identifier for the VM. CA ARCserve Backup uses the identifier to distinguish backup and restore operations for the particular VM. However, VMware vSphere no longer uses the UUID as a mechanism to identify VMs. When you submit a job to recover the VM and specify the Overwrite VM option, CA ARCserve Backup does not delete the original VM if it cannot detect a VM with the same UUID and host name as that of the original VM. As a result, CA ARCserve Backup creates a new VM rather than overwrite the existing VM. The approach helps ensure that CA ARCserve Backup does not delete VM in error. CA ARCserve Backup also behaves in this manner in the following scenarios:

■ The UUID or host name of the VM was changed.

■ The VM was powered off or down (the agent cannot retrieve the host name of the VM).

Backup Jobs Appear to Fail

Valid on Hyper-V and VMware systems.

Symptom:

You submit a backup of VMware or Hyper-V VMs. The options specified for the backup are as follows:

■ Raw mode or Mixed mode

■ Allow file level restore

The job finishes with an Incomplete status and error message AW0550 appears in the Activity Log.

Solution:

The above-described behavior occurs because the name of the CA ARCserve Backup server that is protecting the VM was not specified or the name of the CA ARCserve Backup specified is not correct.

To remedy this behavior, ensure that the name of the CA ARCserve Backup server protecting the VM is properly specified.

For more information, see Specify the Name of the CA ARCserve Backup Server (see page 51).

The Sizes of Backup Sessions are Greater than the Amount of Used Disk Space on VMs

Valid on Windows platforms.

Symptom:

The sizes of backup sessions are greater than the amount of used disk space on VMs.

Solution:

This is expected behavior when you submit a raw mode backup job with the Allow File Level Restore option specified. Consider the example that follows:

Data	Size of Backup Session With Allow File Level Restore	Size of Backup Session Without File Level Restore
Virtual disk: 20 GB **Used space:** 4 GB **Free disk space:** 16 GB	20 GB	4 GB

With the Allow File Level Restore option specified, CA ARCserve Backup backs up the used space and the free disk space that resides on the VM. As a result, the size of the backup session is equal to the size of the VM.

Without the Allow File Level Restore option specified, CA ARCserve Backup backs up only the used disk space that resides on the VM. As a result, the size of the backup session is slightly greater than the amount of used disk space on the VM. (CA ARCserve Backup reserves extra MBs for metadata.)

Recover VM Jobs Fail on VMware VMs

Valid on Windows platforms.

Symptom:

When you submit Recover VM jobs on VMware based VMs, the jobs fail with error AE0564.

Solutions:

There are several reasons why Recover VM jobs on VMware VMs will fail. The following list describes the reasons jobs will fail and the required corrective actions.

- **Reason 1:** The credentials specified for the VMware ESX Host system are not correct:

  Action 1: Ensure that the credentials specified for the VMware ESX Host system are correct.

- **Reason 2:** There is insufficient free disk space in the target datastore.

  Action 2: Ensure that there is sufficient free disk space in the target datastore on the VMware ESX Host system. Optionally, you can move the target datastore to a different VMware ESX Host system.

- **Reason 3:** The VMware ESX Host system is down or not reachable.

  Action 3: Ensure that the VMware ESX Host system can communicate with the backup proxy system.

- **Reason 4:** VMware does support the guest operating system that is running in the VM.

  Action 4: Ensure that VMware Converter supports the guest operating system that is running in the VM. For more information, see the VMware support website.

- **Reason 5:** You attempted to recover a guest operating system with x64 architecture on a VMware ESX Host system with x86 architecture.

  Action 5: Ensure that the VMware ESX Host system is x64 architecture.

  Note: You can use the VMDK files to recover the VM. The path to the VMDK files can be found in CA_VCBpopulateDB.log that is stored on the on the backup proxy system. CA_VCBpopulateDB.log is stored in the directory that follows:

  <<Client Agent Installation Directory>>\Log

- **Reason 6:** VDDK is not installed on the backup proxy system and VMware Converter Enterprise is installed on the backup proxy system.

  The agent does not support using enterprise versions of VMware Converter. For recover VMs jobs to complete successfully, stand-alone versions of VMware Converter must be installed on the backup proxy system.

- **Action 6:** Uninstall VMware Converter Enterprise from the backup proxy system. Install a stand-alone version of VMware Converter on the backup proxy system.

Unable to Restore File Level Backup Data to a CA ARCserve Backup Server

Valid on Windows platforms.

Symptom:

CA ARCserve Backup does not have a mechanism that lets you restore file level backup data to a CA ARCserve Backup server.

Solution:

To restore backup data at file level granularity to an alternate location, the CA ARCserve Backup Client Agent for Windows must be installed on the destination computer. By default, the CA ARCserve Backup Client Agent for Windows is installed on the CA ARCserve Backup server. To restore backup data at file level granularity to the CA ARCserve Backup server, you must add the CA ARCserve Backup server to the Windows Systems object on the Restore Manager, Destination tab. To add the CA ARCserve Backup server to the Windows Systems object, you must add the server using its IP address with a fictitious host name.

After the CA ARCserve Backup server is added to the Windows System object, you can browse the server and specify the location to restore the files.

To add the CA ARCserve Backup server to the Windows Systems object, do the following:

1. Open the Restore Manager and click the Destination tab.

   Clear the check mark from Restore files to their original locations(s).

   The agent directory tree appears.

2. Right-click the Windows System object and select Add Machine/Object from the pop-up menu.

   The Add Agent Dialog opens.

3. Complete the following fields:

   ■ **Host Name--**Lets you specify the host name of the CA ARCserve Backup server.

     Note: You must specify a fictitious host name. For example, LOCAL.

   ■ **IP Address--**Lets you register the CA ARCserve Backup server using the IP address. To specify the IP address, clear the check mark from Use computer name resolution (recommended), as illustrated by the following dialog:
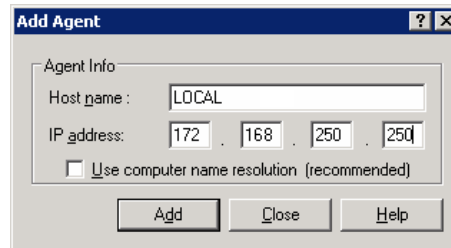
   Click Add.

   The CA ARCserve Backup server is added to the Windows Systems object, as illustrated by the following screen.
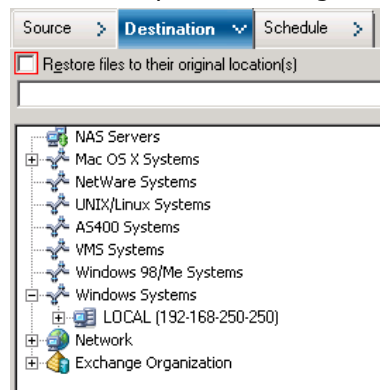
4. Click Close.

   The Add Agent dialog closes.

You can now browse the CA ARCserve Backup server and specify the location where to restore backup data with file level granularity.

Cannot Power on VMs When Restoring Data

Valid on Windows platforms.

Symptom:

CA ARCserve Backup may not be able to power on VMs after restores are complete. This behavior occurs only when all the following conditions are present:

- The VM is configured with Windows Server 2008 R2 or Windows 7 as a guest operating system on VMware ESX Server 4.0. The default SCSI controller is specified for the VM (for example, LSI Logic SAS).

- CA ARCserve Backup for Windows Agent for Virtual Machines is installed on the backup proxy system.

- The guest operating system contained in the VM that you recovered is Windows Server 2008 R2 or Windows 7.

- You submitted the backup using the Agent for Virtual Machines and the VMware vSphere Web Services SDK and VMware VDDK approach.

- You submitted the restore with the Power on after restore option specified.

Solution:

To remedy this problem, do the following:

1. Let CA ARCserve Backup complete the restore operation.

2. Access the VMware ESX Host system through the VI client where the VM is recovered.

3. Select the VM that was recovered.

4. Right-click the VM and select Edit Settings from the pop-up menu.

5. Change the controller type from BusLogic Parallel to LSI Logic SAS.

6. Power on the VM.

Cannot Power on Hyper-V VM When Restoring Data to an Alternate Location

Valid on Windows Server 2008 systems.

Symptom 1

When restoring Hyper-V VMs to an alternate location, CA ARCserve Backup may not be able to power on the target VM. This behavior occurs if the friendly name of the network switch is not the same as that of the original backup.

Solution 1

There are several approaches that you can use to remedy this problem.

- The best practice is to ensure that the friendly name of the destination VM (alternate location) is the same as the source location before you submit the restore.

- An alternate solution is to edit the VM's settings after the restore is complete, and then configure the appropriate network switch before you power on the VM.

Symptom 2

When restoring Hyper-V VMs to an alternate location, CA ARCserve Backup may not be able to power on the target VM. This behavior occurs if the CD/DVD name is not the same as that of the original backup.

Solution 2

There are several approaches that you can use to remedy this problem.

- The best practice is to ensure that the CD/DVD name of the destination VM (alternate location) is the same as the source location before you submit the restore.

- An alternate solution is to edit the VM's settings after the restore is complete, and then configure the appropriate CD/DVD name before you power on the VM.

Symptom 3

You cannot power on Hyper-V VMs manually in the following scenario:

- The Hyper-V VM was restored to an alternate location.

- The Power on VMware or Hyper-V VM after restore option was not specified.

  Note: The Power on VMware or Hyper-V VM after restore option is a global restore option that appears on the Operations tab on the Options dialog.

Solution 3

To remedy this problem, do the following:

1. After the restore is complete, open the Hyper-V Manager and specify the Remove Saved State option.

2. Power on the Hyper-V VM.

Backup and Recover VM Operations Fail Using NBD Transport Mode

Valid on all Windows platforms running on backup proxy systems.

Symptom:

Backup and recover VM operations using VCB or VDDK fail.

The following errors appear in the VCB and VDDK error logs:

Failed to open NBD extent

NBD_ERR_GENERIC

NFC connection errors relating to NFC operations appear in the error logs. For example:

NfcFssrvrRecv

NfcFssrvr_DiskOpen

NfcNetTcpWriteNfcNet_Send

NfcSendMessage

Note: Debugging must be enabled to view the above error logs. For more information, see Enable Debugging for VDDK Jobs (see page 48).

Solution:

Network Block Device (NBD) transport mode, also referred to as LAN transport mode, uses the Network File Copy (NFC) protocol to communicate. Various VDDK and VCB operations use one connection for each virtual disk that it accesses on each ESX Server and ESXi Server host when using NBD. Furthermore, connections cannot be shared across disks. The VI Client and periodic communication between the host systems, the vpxd, the ESX Server, and ESXi Server systems account for the number of concurrent connections.

The following table describes the maximum number NFC connections:

Host Platform	Connection Type	Maximum Connections
ESX Server 4	Direct	9
ESX Server 4	Through vCenter Server	27
ESXi Server 4	Direct	11
ESXi Server 4	Though vCenter Server	23

Be aware if the following:

- The Maximum Connections values represent host limits.

- The Maximum Connections values do not represent process limits.

- The Maximum Connections values do not apply to SAN and hotadd connections.

- The error messages described under Symptoms occur when the number of NFC connections to the host systems exceed the maximum number of connections described in the above table. When failures occur, the number of connections to the ESX Server or ESXi Server increase, which causes the communication sessions to the host systems to exceed the number of maximum connections.

- If the NFC client does not shut down properly, ESX Server and ESXi Server allow the communication sessions to remain open for an additional ten minutes. This behavior can increase the number of open connections.

Best Practices:

The solution to this problem is to use the following best practices to help ensure that backup and recovery operations do not fail when using NBD transport protocol:

- Ensure that open connections to ESX Server systems and ESXi Server systems are closed properly.

- Use the following best practices when submitting backup and restore jobs:

    – If you suspect that you will need a high number of connections to the host systems, you should populate the VMs in your CA ARCserve Backup environment using VMware vCenter Server.

    – When backing up data using the VDDK approach, you should optimize the number of streams specified for multistreaming backups and optimize the number of concurrent read operations of the VM disks. This approach helps to minimize the number of communication sessions to the host system. You can estimate the number of connections using the following calculations:

        - **Mixed Mode backups and Raw (full VM) backups (with or without the Allow file level restore option specified) using VDDK--**The number of connections equals the lesser of the number of streams in a multistreaming job or the number of VMs specified in a multistreaming job, multiplied times the value of vmdkReaderCount.

            Note: For backups of VMs that use VDDK, CA ARCserve Backup backs up one disk at a time, and there are multiple connections to each disk as indicated by the value of vmdkReaderCount.

            Example: A job consists of 4 VMs. VM1 contains 5 disks. VM2, VM3, and VM4 contain 4 disks each. There are 3 streams specified for the job.

            The number of connections equals 3 (the number of streams is less than number of VMs) multiplied times 4 (the value of vmdkReaderCount).

            The number of connections required is 12.

            Note: By default, VDDK backups use a vmdkReaderCount value of 4. For information about how to change the value of VDDK vmdkReaderCount, see Configure the Number of Concurrent Read Operations Using VDDK (see page 44).

- **Raw (full VM) backups (with or without the Allow file level restore option specified), File mode backups using VCB, and File mode backups using VDDK--**The number of connections equals the total number of disks for all VMs backed up concurrently, limited by the number of streams specified for a multiplexing job.

  Example: A job consists of 4 VMs. VM1 contains 5 disks. VM2, VM3, and VM4 contain 4 disks each. There are 3 streams specified for the job.

  the number of connections equals 5 (VM1) plus 4 (VM2) plus 5 (VM3).

  The number of connections required is 14. CA ARCserve Backup will back up VM4 when the backup pertaining to VM1, VM2, or VM3 is complete.

Unable to Recover Hyper-V VMs to an Alternate Location

Valid on Windows Server 2008 systems.

Symptom:

You are attempting to recover a Hyper-V VM to an alternate location using the Recover Virtual Machine restore method. The Recover Virtual Machine view (in the Restore Manager) does not display information about the backup data (for example, the host name, the backup version, and the path of the backup). This problem presents itself only under the following conditions:

- Windows Server 2008 is the operating system running on the Hyper-V server.

- You made a recent, unsuccessful attempt to recover the CA ARCserve Backup database.

  Note: The database information, such as the host name, the backup version, and so on, appears in the Recover Virtual Machine view only when you recovered the CA ARCserve Backup database successfully.

- The Hyper-V backup data resides on media, such as a tape library, file system device, or deduplication device, and the information about the backup data cannot be retrieved from the CA ARCserve Backup database.

Solution:

CA ARCserve Backup lets you recover Hyper-V VMs to an alternate location. You can then specify the missing information (the host name, backup version, path, and so on) in the Restore Manager window. However, Windows Server 2008 does not support recovering Hyper-V VMs to an alternate location. As a result, the job will fail.

Note: Windows Server 2008 R2 supports recovering Hyper-V VMs to an alternate location.

To remedy this problem, do the following:

1. Use the Restore by Session restore method and recover the Hyper-V VM to any location on any Hyper-V server in your CA ARCserve Backup VM environment.
2. Use the Hyper-V Manager to create the VMs using the recovered VHD files.
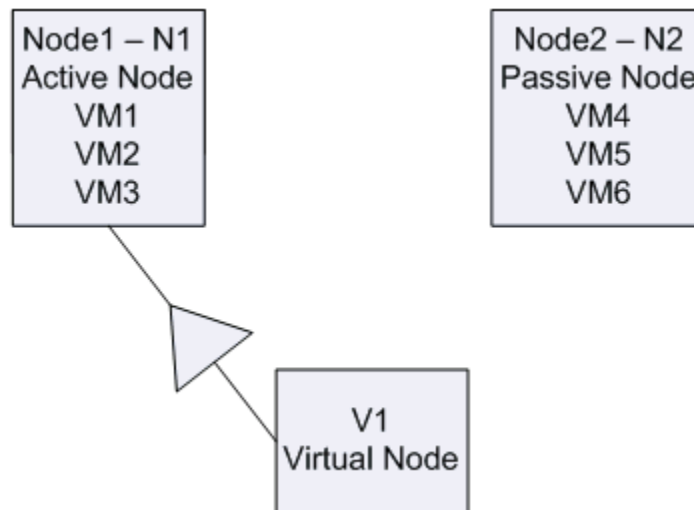
Backups of VMs in a Cluster-Aware Environment Fail

Valid on Windows Hyper-V systems.

Symptom:

Backups of VMs in a cluster-aware environment fail.

Solution:

The following diagram illustrates VMs installed in a cluster-aware environment:

In an ideal scenario, virtual cluster node V1 directs network traffic to the active node (N1). When failover occurs, virtual cluster node V1 directs the network traffic to the passive node (N2), and all of the VMs in the active node (N1) move to the passive node (N2).

If CA ARCserve Backup backs up the active node (N1) after failover occurs, the backup will fail because CA ARCserve Backup cannot locate the VMs in the active node (N1).

To remedy this problem, do the following:

- Submit backups by specifying the entire Hyper-V node, which includes the active node and the passive node, rather than the individual VMs that are configured in the Hyper-V node.

- Ensure that CA ARCserve Backup executes the auto-population process before CA ARCserve Backup backs up the clustered nodes.

Note: CA ARCserve Backup does not support backing up VMs that are configured with virtual node names. For example, If you submit a backup Job using the virtual node V1 as the backup proxy system, CA ARCserve Backup will back up data using the active node (N1 or N2), as the backup proxy system.

The Agent Backs Up Variable Size VHDs as Fixed Size VHDs

Valid on Windows Hyper-V systems.

Symptom:

You back up VMs configured with Virtual Hard Disks (VHDs) that are set up using a variable size. The agent backs up the VHDs using the maximum data size allowed for the VHDs, which is a fixed value. You can observe the following behavior:

- The amount of disk space required to store the VHD backup data is about the same size as the maximum data size allowed for the VHDs.
- The recovery process converts the VHD maximum data size value from a variable value to a fixed value after the recovery is complete.

Solution:

This is expected behavior. The agent allocates the maximum data size value to store the backup of the VHDs. To recover VHDs to their last backup state, you must manually configure the VHD maximum data size value to a variable value after the recovery is complete.

Note: This limitation does not affect VMs with VHDs that were backed up using raw mode. You can recover the VHD as a variable size VHD only if the VM was backed up using the raw backup mode.

The Agent Deletes Snapshots After Recovering VMs

Valid on Windows Hyper-V systems.

Symptom:

After you recover a VM with data that was backed up using the raw (full VM) backup mode with the allow file level restore option specified, the recovery process deletes the snapshot.

Solution:

The symptom described above is expected behavior. To preserve snapshots after recovering VMs, you must specify the raw (full VM) backup mode, but do not specify the allow file level restore option.

VDDK Backup Jobs Fail

Valid on Windows operating systems.

Symptom:

Backup jobs fail when you use VDDK to back up VMware VMs. This problem is evident by the following symptoms:

- Error E8535 appears in the CA ARCserve Backup Activity Log.

- The following error message appears in the VMDKIO.log file:

    System libeay32.dll library is older than our library (90709F < 9070AF)
    SSLLoadSharedLibrary: Failed to load library libeay32.dll:126

Solution:

VMware VDDK installs library files named libeay32.dll and ssleay32.dll in the default VDDK installation directory. The problem occurs when other applications install different versions of the same libraries in the Windows\system32 directories. With multiple instances of the same libraries, the Agent for Virtual Machines may to try to load incorrect versions of these libraries when the backup executes. As a result, the above message appears in the VMDKIO.log file, and backup jobs involving VDDK may fail.

To remedy this problem, do the following:

1. Browse to the VDDK installation directory on the backup proxy system.

    x86 Systems (default):

    C:\Program Files\VMware\VMware Virtual Disk Development Kit

    x64 Systems (default):

    C:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit

2. Locate the files named libeay32.dll and ssleay32.dll in the following directory:

    x86 Systems:

    C:\Program Files\VMware\VMware Virtual Disk Development Kit\bin

    x64 Systems:

    C:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\vddk64\bin

3. Copy libeay32.dll and ssleay32.dll from the above directory to the Universal Agent installation directory on the backup proxy system. By default, the Universal Agent is installed in the following directory:

    C:\Program Files\CA\SharedComponents\ARCserve Backup\UniAgent

Mount Operation Problems

This section contains the following topics:

Directories Do Not Appear Under the Mount Point When Completing File Level Backups

Valid on all Windows systems functioning as backup proxy systems.

Symptom:

File and folder directories do not appear under the mount point when performing file level backups using VDDK.

Solution:

VMware VDDK cannot map file and folder directories to a mount directory on a volume or drive letter. However, VDDK maps the mounted volume to a symbolic link device path using the signature that follows:

\\vstor2-mntapi10-F0751CFD007E000000000000001000000\.

The above signature is a low-level device path that you can view in the Windows Object namespace. However, the namespace is not mapped to a volume drive letter on a mounted volume on the backup proxy system.

CA ARCserve Backup Cannot Mount Volumes that Use GUID Partitions

Valid on all Windows systems functioning as backup proxy systems.

Symptom:

CA ARCserve Backup cannot mount volumes that use Globally Unique Identifier (GUID) based partitioning.

Solution:

This is expected behavior. VMware VDDK does not support mounting volumes that use GUID-based partitioning.

Volume Mount Points Cannot be Traversed

Valid on all Windows systems functioning as backup proxy systems.

Symptom:

CA ARCserve Backup cannot traverse volume mount points after the agent mounts a file mode backup using VDDK.

Solution:

To traverse volume mount points on the backup proxy system, CA ARCserve Backup must use VMware VCB Framework to perform file level backups. VMware VDDK does not support the capability to traverse volume mount points related to file level backups.

By default, CA ARCserve Backup uses VCB Framework to perform file level backups when VCB Framework and VDDK are installed on the backup proxy system. However, if only VDDK is installed on the backup proxy system, CA ARCserve Backup uses VDDK to perform file level backups of VM data.

VM Mount Operation Fails

Valid on Windows platforms.

Symptom:

A raw (full VM) mount operation or a file level VM mount operation failed.

Solutions:

To perform a raw (full VM) mount operation or a file level VM mount operation, VCB first takes a snapshot of a VM and then exports the files to the backup proxy system. There are several reasons this problem can occur and actions you can take to remedy this problem.

- **Reason 1:** There is not enough free disk space in the disk volume on the backup proxy system.

  Action 1: Clean up the disk or change the mount path to a different volume that has enough space.

- **Reason 2:** The VMware ESX Host system is down.

  Action 2: Take corrective action if the VMware ESX Host system on which the VM resides is down.

- **Reason 3:** VM has become temporarily unmountable.

  Action 3: Run vcbMounter utility for the VM on the backup proxy system, if the VM has become temporarily unmountable.

  You can run the utility using the command-line by navigating to the directory where VMware VCB framework is installed. To view the syntax for the utility, type the following in the command line:

  vcbMounter -help

  If the vcbMounter utility fails to mount the specified VM, then the problem could be with the VMware VCB framework. Restart the backup proxy system and resubmit the VM backup job.

- **Reason 4:** The backup source included VMs with an Independent (Persistent/Nonpersistent) disk mode specified.

  Action 4: Clear or Remove the Independent disk mode setting for all virtual disks associated with the VM.

- **Reason 5:** The job was submitted with incorrect VMware ESX Host or vCenter Server user credentials. The credentials were specified on the Security and Agent Information dialog.

  Action 5: Resubmit the VM backup job with valid credentials. You must provide valid VMware ESX Host system credentials or vCenter Server system credentials, and backup proxy system credentials on the Security and Agent Information dialog.

- **Reason 6:** A VM is no longer available in the VMware environment.

  Action 6: Run the ARCserve VMware Configuration Tool or ca_vcbpopulatedb utility to populate the CA ARCserve Backup database with updated information about your VMware environment.

VM Unmount Operation Fails

Valid on Windows platforms.

Symptom:

On a VM, an unmount operation fails after a successful mount operation.

Solution:

An unmount operation can fail under the following conditions:

- The mount path is not correct.

- An incorrect mount mode was specified, for example, File or Raw (Full VM).

- Some of the catalog files may have been deleted in the mount point.

- The user deleted or tried to delete the VCB mount snapshot.

- The VM is moved to a different VMware ESX Host system during the backup operation using VMotion.

- VMware Converter is not installed on the backup proxy system.

To fix this problem, you must manually delete the VCB mount snapshot of the VM using the VI Client. If the delete operation fails, restart the VM and delete the VCB mount snapshot for the VM.

To view log information for mount and unmount operations, view the file labeled Mount_jnl.log, which is stored in the Log folder under the Client Agent installation directory

Configuration Tool Problems

This section contains the following topics:

ARCserve VMware Configuration Tool or ca_vcbpopulatedb Utility Fails

Valid on Windows platforms.

Symptom:

The ARCserve VMware Configuration Tool or the ca_vcbpopulatedb utility fails. The following error message appears in the Results field on the ARCserve VMware Configuration Tool.

.NET version >= not found. Exiting ca_vcbpopulatedb.

Note: This message appears in the Command Prompt window when you execute the ca_vcbpopullatedb utility using the Windows Command Prompt.

Solution:

This error occurs when Microsoft .NET Framework, Version 2.0 or higher, is not detected on the backup proxy system.

To remedy this problem, complete the following steps:

1. Ensure that Microsoft .NET Framework, Version 2.0 or higher, is installed and running on the backup proxy system.

2. Open a .NET Command Prompt and change to the Client Agent for Windows installation directory. By default, the Client Agent for Windows is installed in one of the following directories:

   ■ x86 systems

     C:\Program Files\CA\ARCserve Backup Client Agent for Windows

   ■ X64 systems

     C:\Program Files\CA\ARCserve Backup Client Agent for Windows\x86

   Execute the following command:

   regasm vcb_com.dll

(Optional) If you cannot locate the .NET Command Prompt, complete the following steps:

a. Open a Windows Command Line and change to the following directory:

    C:\WINDOWS\Microsoft.NET\Framework

b. After you change to this directory, change to the directory that is greater than Microsoft .NET Framework Version 2.0. For example:

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

c. Execute the following command:

    regasm <Client Agent for Windows installation directory>\Vcb_com.dll

After the execution is complete and successful, the following output appears in the .NET Command Prompt or the Windows Command Prompt:

Microsoft (R) .NET Framework Assembly Registration Utility 2.0.50727.42
Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.

Types registered successfully.

ARCserve VMware Configuration Tool or ca_vcbpopulatedb Utility Fails

Valid on Windows platforms.

Symptom:

The ARCserve VMware Configuration Tool or the ca_vcbpopulatedb utility fails. The error message that follows appears in the Results field on the ARCserve VMware Configuration Tool:

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.

Solution:

The above-described error occurs because ARCserve VMware Configuration Tool and ca_vcbpopulatedb Utility cannot provide credentials to the backup proxy system at runtime. To remedy this behavior you must allow the VMware ESX Host system or vCenter Server system to bypass the process of connecting with the backup proxy system.

To add VMware ESX Host systems, vCenter Server systems, or both to the exceptions list, do the following:

1. Open Internet Explorer.

    From the Tools menu, click Internet Options.

    The Internet Options dialog opens.

2. Click the Connections tab.

    The Connections options appear.

3. Click LAN Settings.

    The Local Area Network (LAN) Settings dialog opens.

4. In the Proxy server section, click Use a proxy server for your LAN.

    Click Advanced.

    The Proxy Settings dialog opens.

5. In the Exceptions field, add your VMware ESX Host system or vCenter Server system. To add multiple VMware ESX Host systems vCenter Server systems, separate the entries using semicolons (;).

    Click OK, as required, to close all open dialogs.

    The VMware ESX Host systems and vCenter Server systems are added to the exceptions list.

Miscellaneous Problems

This section contains the following topics:

VMs Do Not Appear in the Backup Manager Directory Tree

Valid on Hyper-V and VMware systems.

Symptom:

You execute ARCserve VMware Configuration Tool or ARCserve Hyper-V Configuration Tool. After you open the Backup Manager, some VMs do not appear under the VMware Systems object or the Microsoft Hyper-V Systems object.

Solution:

The symptom described above is expected behavior. Although the aforementioned tools capture backup information about VMs that are in a powered off state when you execute tools, the information relating to powered off VMs will not appear under the VMware Systems object or the Microsoft Hyper-V Systems object. To remedy this condition, you must power on the VMs and then execute the appropriate tool.

Appendix B: Configuring VMware ESX Host Systems and vCenter Server Systems

The sections that follow describe how to configure the communication protocol to set up backing up VMware ESX Host systems and vCenter Server systems using a backup proxy system.

This section contains the following topics:

Configure VMware ESX Server 3.0.2 Systems

This topic describes how to configure the communication protocol on VMware ESX Server 3.0.2 systems.

To configure VMware ESX Server 3.0.2 systems

1. Install VMware ESX 3.0.2 Server. For more information about VMware ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

    Note: To manage your VMware ESX Host systems using VMware vCenter Server, you must install and configure VMware vCenter Server as part of Virtual Infrastructure installation.

2. Install VCB on the backup proxy system with the following environmental conditions:

   ■ Windows 2003 Server (x86 or X64) must be the operating system running on the backup proxy system.

   ■ If the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

   Note: The requirement to have the same LUN number assigned to the ESX Server system and the backup proxy system only applies to VCB versions 1.0, 1.0.1, and 1.0.2. VCB versions 1.0.3 and later do not require the same LUN number.

   The LUN in the backup proxy system should not be signed.

   Note: To obtain the latest information about this configuration, see the VMware VCB documentation.

3. To set up backing up VMs through a VCB Backup Proxy using a VMware ESX Server 3.0.2 system, configure one of the following communication protocols:

   https

   To use https as the communication protocol between the VMware ESX Host system and the backup proxy system, copy the self-generated SSL certificate from the VMware ESX Host system to the backup proxy system, and then install the certificate on the backup proxy system.

   Note: https the default communication protocol used by the ARCserve VMware Configuration Tool and the ca_vcbpopulatedb utility. https lets CA ARCserve Backup communication between VCB Backup Proxy and the VMware ESX Host system or the vCenter Server system.

   You can find the SSL certificate (labeled rui.crt) from the following directory on the VMware ESX Host system:

   /etc/vmware/ssl/rui.crt

   To install the SSL certificate, right-click the object and select Install from the pop-up menu.

   Note: The host name assigned in the SSL certificate must match the name of the VMware ESX Host system specified when running the ca_vcbpopulatedb command line utility. If the name does not match or if the host name is missing in the SSL certificate then the following message appears "Bad Server Certificate, The certificate CN name does not match the passed value". You must select Yes to continue.

http

To use http as the communication protocol between the backup proxy system and the VMware ESX Host system, you must configure the http protocol on the VMware ESX Host system as follows in the config.xml file located at /etc/vmware/hostd/config.xml:

a. Locate the <proxy Database> tag within the <http> tag.

b. Add the following text with the <proxy Database> tag:

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

c. Remove the following text:

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

d. Restart the VMware Infrastructure SDK Management Service by executing the following command:

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

Note: For more information, see the Virtual Infrastructure SDK documentation on the VMware website.

4. Install the Agent for Virtual Machines on the backup proxy system.

5. On the backup proxy system, specify temporary VM mount location. For more information, see Specify a Temporary VM Mount Location (see page 52).

6. Execute the ARCserve VMware Configuration Tool to populate the CA ARCserve Backup database with information about your VMware environment.

   Optionally, you can populate the ARCserve database using the ca_vcbpopulatedb command line utility.

   Important! The VMs in the VMware ESX Host system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the CA ARCserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

Configure VMware ESX Server 3.5 Systems

This topic describes how to configure the communication protocol on VMware ESX Server 3.5 systems.

To configure VMware ESX Server 3.5 systems

1. Install VMware ESX Server 3.5. For more information about VMware ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

    Note: To manage your VMware ESX Host systems using VMware vCenter Server, you must install and configure VMware vCenter Server as part of Virtual Infrastructure installation.

2. Install VCB on the backup proxy system with the following environmental conditions:

    ■   Windows 2003 Server (x86 or X64) must be the operating system running on the backup proxy system.

    ■   If the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

        Note: The requirement to have the same LUN number assigned to the ESX Server system and the backup proxy system only applies to VCB versions 1.0, 1.0.1, and 1.0.2. VCB versions 1.0.3 and later do not require the same LUN number.

        The LUN in the backup proxy system should not be signed.

        Note: To obtain the latest information about this configuration, see the VMware VCB documentation.

3. Log in to the service console as the root user and change to the following directory:

    /etc/vmware/hostd

4. Open the file labeled proxy.xml using a text-editing application.

    Navigate to the list of end points in the file (identified by the <EndpointList> tag) that contain the settings for the Web service supporting the SDK. The nested tags may appear as follows:

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

    Change the accessMode to httpAndHttps.

    Save your settings and close the file.

5. Restart the vmware-hostd process using the following command:

   service mgmt-vmware restart

6. Install the Agent for Virtual Machines on the backup proxy system.

7. On the backup proxy system, specify temporary VM mount location. For more information, see Specify a Temporary VM Mount Location (see page 52).

8. Execute the ARCserve VMware Configuration Tool to populate the CA ARCserve Backup database with information about your VMware environment.

   Optionally, you can populate the ARCserve database using the ca_vcbpopulatedb command line utility.

   Important! The VMs in the VMware ESX Host system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the CA ARCserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

Configure VMware ESX Server 3i Systems

This topic describes how to configure the communication protocol on VMware ESX Server 3i systems.

To configure ESX Server 3i systems

1. Install VMware ESX Server 3i. For more information about VMware ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your VMware ESX Host systems through VMware vCenter Server, you must install and configure VMware vCenter Server as part of Virtual Infrastructure installation.

2. Install VCB on the backup proxy system with the following environmental conditions:

- ■ Windows 2003 Server (x86 or X64) must be the operating system running on the backup proxy system.

- ■ If the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

  Note: The requirement to have the same LUN number assigned to the ESX Server system and the backup proxy system only applies to VCB versions 1.0, 1.0.1, and 1.0.2. VCB versions 1.0.3 and later do not require the same LUN number.

  The LUN in the backup proxy system should not be signed.

  Note: To obtain the latest information about this configuration, see the VMware VCB documentation.

3. Install the Remote Command-Line Interface (RCLI), which is provided by VMware, on any Windows or Linux system.

4. Use the vifs command, which is available with RCLI, to get a copy of the proxy.xml file for editing. The syntax for this command is as follows:

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

5. Open the file labeled proxy.xml with a text editing application.

   Navigate to the list of end points in the file (identified by the <EndpointList> tag) that contain the settings for the Web service supporting the SDK. The nested tags may appear as follows:

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

   Change the accessMode to httpAndHttps.

   Save your changes and close the file.

6. Use the vifs command to copy the proxy.xml file back to the ESX Server. The syntax for this command is as follows:

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

7. Use the Restart Management Agents operation through the local console to apply the settings.

   Note: The default Communication Protocol on ESX Server 3i is httpsWithRedirect.

8. Install the Agent for Virtual Machines on the backup proxy system.

9. On the backup proxy system, specify temporary VM mount location. For more information, see Specify a Temporary VM Mount Location (see page 52).

10. Execute the ARCserve VMware Configuration Tool to populate the CA ARCserve Backup database with information about your VMware environment.

   Optionally, you can populate the ARCserve database using the ca_vcbpopulatedb command line utility.

   Important! The VMs in the ESX Server system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the CA ARCserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

For information about using vifs, see "Performing File System Operations with vifs" in the *ESX Server 3i Configuration Guide*.

For information about configuring ESX Server 3i security and using the Restart Management Agents operation, see the *ESX Server 3i Configuration Guide*.

Configure VMware vCenter Server 2.0.2 Systems

This topic describes how to configure the communication protocol on VMware vCenter Server 2.0.2 systems.

To configure VMware vCenter Server 2.0.2 systems

1. Install VMware VCenter Server. For more information about VMware vCenter Server requirements, see the VMware vCenter Server Installation guide on the VMware website.

2. Install VCB on the backup proxy system with the following environmental conditions:

■ Windows 2003 Server (x86 or X64) must be the operating system running on the backup proxy system.

■ If the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

Note: The requirement to have the same LUN number assigned to the ESX Server system and the backup proxy system only applies to VCB versions 1.0, 1.0.1, and 1.0.2. VCB versions 1.0.3 and later do not require the same LUN number.

The LUN in the backup proxy system should not be signed.

Note: To obtain the latest information about this configuration, see the VMware VCB documentation.

3. To set up backing up VMs through a VCB Backup Proxy and a VMware vCenter Server system, configure one of the following communication protocols:

https

To use https as the communication protocol between the VMware vCenter Server system and the backup proxy system, you must copy the self-generated SSL certificate from the VMware vCenter Server system to the backup proxy system, and then install the certificate on the backup proxy system.

Note: https is the default communication protocol used by the ARCserve VMware Configuration Tool and the ca_vcbpopulatedb utility. https communication lets CA ARCserve Backup communicate with the VCB backup proxy system and the VMware vCenter Server system.

You can access the SSL certificate (labeled rui.crt) from the following directory on the Vmware vCenter Server system:

C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\rui.crt

To install the SSL certificate, right-click the object and select Install from the pop-up menu.

Note: The host name assigned in the SSL certificate must match the name of the VMware vCenter Server system specified when running ARCserve VMware Configuration Tool (ca_vcbpopulatedb utility). If the name does not match or if the host name is missing in the SSL certificate then the following message appears "Bad Server Certificate, The certificate CN name does not match the passed value". You must select Yes to continue.

http

To use http as the communication protocol between the backup proxy system and the VMware vCenter Server system, you must configure the http protocol on the VMware vCenter Server system as follows in the vpxd.cfg file located at

"C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\vpxd.cfg";

a. Locate the <proxy Database> tag within the <http> tag.

b. Add the following text with the <proxy Database> tag:

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

c. Remove the following text:

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

d. Restart the VMware vCenter Server service:

This can be done by from the Services Control Panel.

Note: For more information, see the VMware VCB Backup guide on the VMware website.

4. Restart the VMware vCenter Server service from the command line or from the Windows Services control panel.

5. Install the Agent for Virtual Machines on the backup proxy system.

6. On the backup proxy system, specify temporary VM mount location. For more information, see Specify a Temporary VM Mount Location (see page 52).

7. Execute the ARCserve VMware Configuration Tool to populate the CA ARCserve Backup database with information about your VMware environment.

Optionally, you can populate the CA ARCserve Backup database using the ca_vcbpopulatedb command line utility.

Important! The VMs in the Vmware vCenter Server system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the CA ARCserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

Configure VMware vCenter Server 2.5 Systems

This topic describes how to configure the communication protocol on vCenter Server 2.5 systems.

To configure VMware vCenter Server 2.5 systems

1. Install VMware vCenter Server. For more information about VMware vCenter Server requirements, see the VMware vCenter Installation guide on the VMware website.

2. Install VCB on the backup proxy system with the following environmental conditions:

    ■   Windows 2003 Server (x86 or X64) must be the operating system running on the backup proxy system.

    ■   If the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

        Note: The requirement to have the same LUN number assigned to the ESX Server system and the backup proxy system only applies to VCB versions 1.0, 1.0.1, and 1.0.2. VCB versions 1.0.3 and later do not require the same LUN number.

        The LUN in the backup proxy system should not be signed.

        Note: To obtain the latest information about this configuration, see the VMware VCB documentation.

3. To set up backing up VMs through a VCB Backup Proxy and VMware vCenter Server system, configure one of the following communication protocols:

    https

    To use https as the communication protocol between the vCenter Server system and the backup proxy system, you must copy the self-generated SSL certificate from the vCenter Server system to the backup proxy system, and then install the certificate on the backup proxy system.

    Note: https is the default communication protocol used by the ARCserve VMware Configuration Tool and the ca_vcbpopulatedb utility. https communication lets CA ARCserve Backup communicate with the VCB backup proxy system and the ESX Server system or the vCenter Server system.

You can access the SSL certificate (labeled rui.crt) from the following directory on the ESX Server system:

C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\rui.crt

To install the SSL certificate, right-click the object and select Install from the pop-up menu.

Note: The host name assigned in the SSL certificate must match the name of the vCenter Server system specified when running ARCserve VMware Configuration Tool (ca_vcbpopulatedb utility). If the name does not match or if the host name is missing in the SSL certificate then the following message appears "Bad Server Certificate, The certificate CN name does not match the passed value". You must select Yes to continue.

http

To use http as the communication protocol between the backup proxy system and the vCenter Server system, you must configure the http protocol on the vCenter Server system in the file that follows:

"C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\proxy.xml";

a. Open the file labeled proxy.xml using a text-editing application.

b. Navigate to the list of end points in the file (identified by the <EndpointList> tag) that contain the settings for the Web service supporting the SDK. The nested tags may appear as follows:

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

c. Change the accessMode to httpAndHttps.

4. Restart the VMware vCenter Server service from the command line or from the Windows Services control panel.

5. Install the CA ARCserve Backup Client Agent for Windows on the backup proxy system.

6. On the backup proxy system, specify temporary VM mount location. For more information, see Specify a Temporary VM Mount Location (see page 52).

7. Execute the ARCserve VMware Configuration Tool to populate the CA ARCserve Backup database with information about your VMware environment.

   Optionally, you can populate the ARCserve database using the ca_vcbpopulatedb command line utility.

   Important! The VMs in the ESX Server system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the CA ARCserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

   For more information, see the *Developer's Setup Guide for VMware Infrastructure SDK 2.5* on the VMware web site.

Configure HTTP Communication Protocol on vCenter Server 4.0 Systems

By default, the backup proxy system and the vCenter Server systems communicate using HTTPS protocol. To specify an alternative protocol, you can configure the backup proxy system and the ESX Server system to communicate using HTTP protocol.

To configure HTTP communication protocol on vCenter Server 4.0 systems

1. Log in to the vCenter Server system.

   Open the file that follows using a text editor:

   C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\proxy.xml";

   Find the list of endpoints that contain the settings for the web service supported by the SDK.

   Note: You can identify endpoints by the <EndpointList> tag.

   The nested tags appear as follows:

   ```
   <e id="5">
   <_type>vim.ProxyService.LocalServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <port>8085</port>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

2. Change the accessMode to the following:

   httpAndHttps

   Close and save proxy.xml.

3. Restart the vCenter Service from the command line or from the Windows Services control panel.

Configure HTTP Communication Protocol on ESX Server 4.0 Systems

By default, the backup proxy system and the ESX Server systems communicate using HTTPS protocol. To specify an alternative protocol, you can configure the backup proxy system and the ESX Server system to communicate using HTTP protocol.

To configure HTTP communication protocol on ESX Server 4.0 systems

1. Log in to the service console on the ESX Server system as the root user and change to the directory that follows:

   /etc/vmware/hostd

   Open proxy.xml using a text editor.

   Find the list of endpoints that contain the settings for the web service supported by the SDK.

   Note: You can identify endpoints by the <EndpointList> tag.

   The nested tags may appear as follows:

   <e id="5">

   <_type>vim.ProxyService.LocalServiceSpec</_type>

   <accessMode>httpsWithRedirect</accessMode>

   <port>8307</port>

   <serverNamespace>/sdk</serverNamespace>

   </e>

2. Change the accessMode to the following:

   httpAndHttps

   Close and save proxy.xml.

3. Restart the vmware-hostd process using the command that follows:

   service mgmt-vmware restart

Index

troubleshooting • 107

U

uninstall the agent • 49
unnamed volumes, recovering • 101
using backup proxy system • 131

V

VCB limitations • 16
virtual hard disks
    backup limitations • 87
    overview • 87

W

where to install the agent • 26