CA ARCserve® Backup for Windows

Agent for Virtual Machines Guide

r12.5

ca.

CA Product References

This documentation set references the following CA products:

- BrightStor® ARCserve® Backup for Laptops and Desktops
- BrightStor® CA-Dynam®/TLMS Tape Management
- BrightStor® CA-Vtape™ Virtual Tape System
- BrightStor® Enterprise Backup
- BrightStor® High Availability
- BrightStor® Storage Resource Manager
- CA Antivirus
- CA ARCserve® Backup Agent 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
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint
- 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 Disk to Disk to Tape 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 Dynam®/B Backup for z/VM
- CA VM:Tape for z/VM
- CA XOsoft™ Assured Recovery™
- CA XOsoft™
- 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 http://ca.com/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/support.

Documentation Changes

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

- Backup and Restore Limitations on Virtual Machines (see page 81)--Removed the following items from this topic because they are not pertinent:

  - There is no application level consistency support when backing up data using a backup proxy system.

    To protect application level data, you can create custom prescripts and postscripts that let you keep application level data in a consistent state. You can use the custom scripts as pre-freeze and post-thaw scripts. For more information about pre-freeze and post-thaw scripts, see the *VMware Virtual Machine Backup Guide*.

  - 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.

- How the Agent Protects Hyper-V Systems (see page 19)--Describes how the CA ARCserve Backup for Virtual Machines lets you protect Hyper-V systems.

- Deploy Agents to VMs Using Agent Deployment (see page 29)--Describes how to install and upgrade agents on local and remote VMs using Agent Deployment.

- Populate the Database Using ARCserve VMware Configuration Tool (see page 34)--Includes information about fields that were added to ARCserve VMware Configuration Tool in this release.

- Specify a Temporary VM Mount Location (see page 38)--Describes how to change the default mount location on the backup proxy system.

- Populate the Database Using the ca_vcbpopulatedb Command Line Utility (see page 39) and ca_vcbpopulatedb Usage (see page 41)--Includes information about syntax and arguments that were added this release.

- Populate the Database Using ARCserve Hyper-V Configuration Tool (see page 46)--Describes how to populate the CA ARCserve Backup database with information about the Hyper-V systems running in your virtual machine environment using a graphical user interface called ARCserve Hyper-V Configuration Tool.

- **Populate the Database Using the ca_msvmpopulatedb Command Line Utility** (see page 49)--Describes how to populate the CA ARCserve Backup database with information about the Hyper-V systems running in your virtual machine environment using a Windows Command Line based utility called ca_msvmpopulatedb.

- **How to Uninstall the Agent** (see page 51)--Updated the procedure that describes how to uninstall the CA ARCserve Backup Agent for Virtual Machines.

- **Best Practices for Installing and Configuring the Agent for Virtual Machines** (see page 53)--Describes best practices that you can use to install and configure the CA ARCserve Backup Agent for Virtual Machines.

- **How Global and Local Backup Modes Work** (see page 57)--Describes how to apply backup modes to maximize backup efficiency and restore flexibility.

- **Specify Backup Modes as a Global Backup Option** (see page 61) and **Specify Backup Modes as a Local Backup Option** (see page 63)--Describes backup modes, when to use them, and how to specify.

- **Recover Hyper-V Virtual Machines** (see page 78)--Added to the section Restoring Data and describes how to restore Hyper-V VMs.

- **Restore Data at File Level Granularity** (see page 71)--Added a topic that describes how to restore data from file mode backup data, raw (full VM) backup data, and mixed mode backup data.

- **How to Use Virtual Machine Log Files** (see page 82)--Describes how to use log files to analyze VM backup and restore operations.

- **Troubleshooting** (see page 87)--Added several topics that describe troubleshooting scenarios.

- **Configure VirtualCenter Server 2.5 Systems** (see page 108)--Updated procedure to include information about configuring http and https communication.

- **Protecting Hyper-V Systems Using the Hyper-V VSS Writer** (see page 111)--Describes how to protect VM data using the Hyper-V VSS Writer.

Contents

Index   **119**

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 Server and VMware VirtualCenter Server--**VMware provides you with a mechanism called VMware Consolidated Backup (VCB) that is integrated with VMware ESX Server and VMware VirtualCenter Server. VCB lets you protect Virtual Machine (VM) files and data. Using VCB 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.

- **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

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

■ You want to reduce resource restraints in the ESX Server system.

   Note: VMware ESX Server 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 ESX Server 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 Server system.

Note: The agent supports backing up and restoring VMs that are configured locally to the ESX 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 VCB snapshot of the VM and mounts or exports the VCB 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 57), 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 38).

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 24).

- 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 ESX Server 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.

- 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 ESX Server system. With local storage environments, the backup proxy system should be able to communicate with the ESX Server system via the LAN.

Note: The terms SAN/iSCSI are used to denote shared storage between Proxy and ESX Server 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 data store types of the VMs in your environment.

However, if the VMs reside on a SAN, and the backup proxy system is not attached to the same SAN, you must modify an .ini file labeled VMDatastoreTypes.ini that contains the data store types detected by CA ARCserve Backup when you populate the CA ARCserve Backup database. CA ARCserve Backup creates the VMDatastoreTypes.ini file in the Client Agent for Windows installation directory. By default, the CA ARCserve Backup Client Agent for Windows is installed in the following directory:

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

Note: For information about how to modify VMDatastoreTypes.ini to protect VMs that reside on a SAN, see Configure the Agent to Protect VMs that Reside on a SAN.

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 ESX Server 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 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

- 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 at 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 and Mirrored volumes--**CA ARCserve Backup lets you protect VM data that resides in spanned, striped, and mirrored volumes.

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

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

Example 1

– 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.

Example 2

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

Example 3

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

Example 4

– Your environment consists of one VM host system (VMware ESX Server 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 (1 host system + 2 VMs) licenses on the CA ARCserve Backup server.

Note: For more information about backup modes, see How Global and Local Backup Modes Work (see page 57).

Where to Install the Agent

The table the follows identifies the type of backup modes that you will perform and where you will need to install the agent.

For more information about backup modes, see How Global and Local Backup Modes Work (see page 57).

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

Note: All agent licenses must be registered on the CA ARCserve Backup primary server or stand-alone server.

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 57).

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	Using the Client Agent	Using VCB	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	Using the Client Agent	Using VCB	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.

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.

- 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.

Installation Considerations

The following section provides information about installation considerations for CA ARCserve Backup Agent for Virtual Machines.

- You must install the agent on the following locations:

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

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

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

    Note: For more information, see <u>How to License the Agent</u> (see page 23) and <u>Where to Install the Agent</u> (see page 24).

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 32).

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 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 ESX Server and VirtualCenter Server VMware systems. The agent does not require post-installation configuration to protect Hyper-V based systems.

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 Agents to VMs Using Virtual Machine Deployment.

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 and click OK.
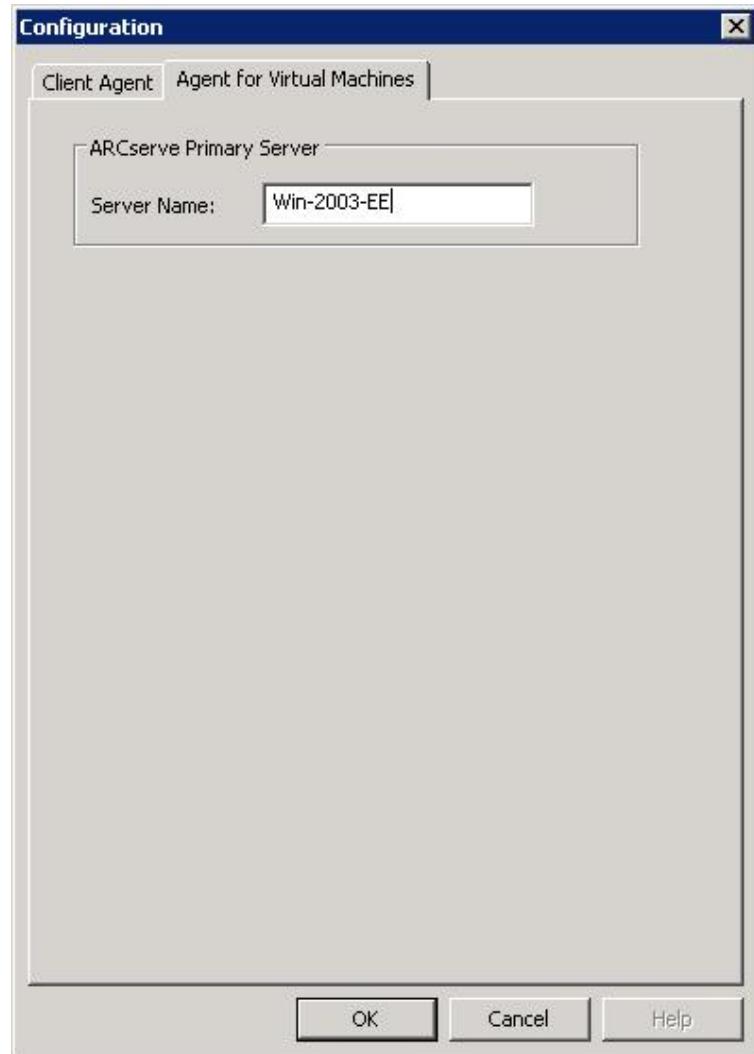
The name of the CA ARCserve Backup server is saved.

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

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 ESX Server. This tool integrates with a command-line utility called 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

- ESX Server or VirtualCenter 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 back up 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 to 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 ESX Server 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 ESX Server 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: VCBUI.exe is installed in one of 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
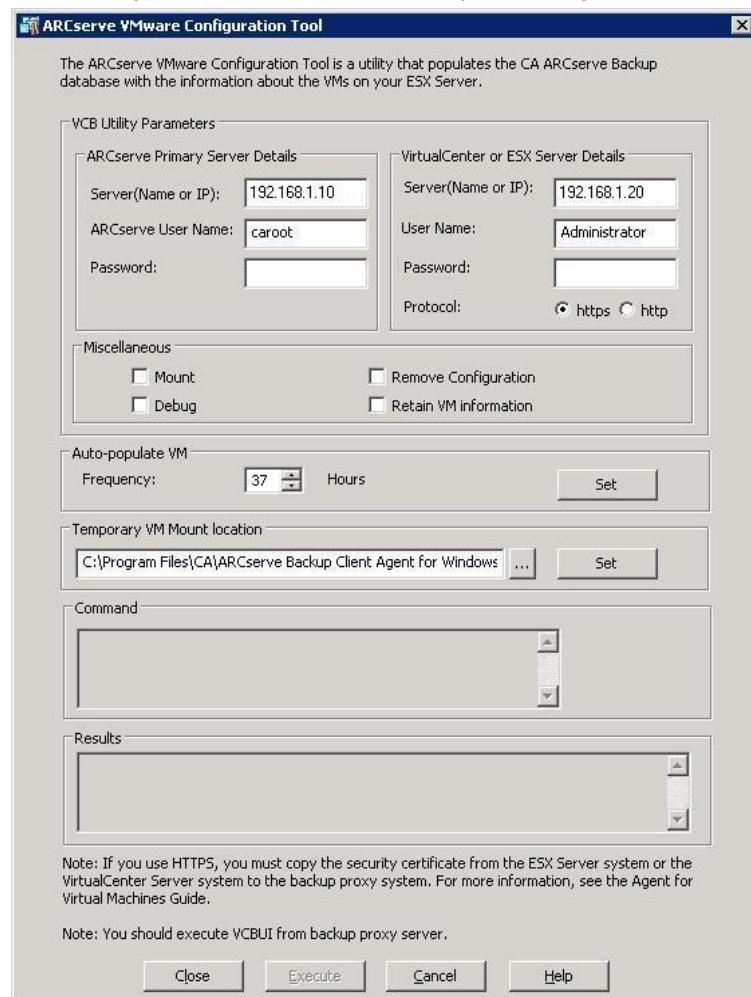
4. Complete the following fields:

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 system.

- **ARCserve User Name--**Lets you specify the user name, with CAROOT privileges, for the CA ARCserve Backup primary system.

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

VirtualCenter or ESX Server Details

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

- **Server (Name or IP)--**Lets you specify the name of the ESX Server system or the VirtualCenter Server system.

- **User Name--**Lets you specify the name of the ESX Server user or the VirtualCenter user with Administrator privileges.

- **Password--**Lets you specify the password for the ESX Server or the VirtualCenter Server User Name.

- **Protocol--**Lets you specify the communication protocol between the backup proxy system and the ESX Server system or the VirtualCenter 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 given ESX Server system or a VirtualCenter Server system under the given 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 utility 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.

Auto-populate the 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

Defines where ARCserve VMware Configuration Tool will temporarily mount (store) the backup information for the VMs while the tool is running.

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

`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 38).

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, and 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.

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: On non-Windows systems, 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. However, on Windows-based systems, you do not need to reserve additional disk space for the data in the temporary VM 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 the ca_vcbpopulatedb Command Line Utility

The ca_vcbpopulatedb utility is a data collection tool that lets you populate the CA ARCserve Backup database with information about the following:

- VCB backup proxy system names

- ESX Server or VirtualCenter 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 VMware systems. To accomplish this, you must execute the ca_vcbpopulatedb utility on the backup proxy system or any other Windows 2003 (x86 and X64) system where the CA ARCserve Backup Client Agent for Windows is installed.

Note: If you do not perform this task, you will not be able to browse the VMware VMs in your environment using the Backup Manager.

To populate the CA ARCserve Backup database using the ca_vcbpopulatedb Command Line utility

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

   Note: If the VMs are not in a running state, the ca_vcbpopulatedb utility 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 ESX Server systems.

2. Access the backup proxy system, open a command-line window, and run the ca_vcbpopulatedb utility.

   Important! You must execute this utility on the backup proxy system or any other Windows 2003 system where the Agent for Virtual Machines is installed.

   The ca_vcbpopulatedb utility is stored in the Client Agent for Windows 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

3. There are two methods that you can use to run the utility. Choose one of the following methods to run this utility:

   ■ Execute the command using the arguments described in the following syntax:

      ca_vcbpopulatedb -Primary <PrimaryServerName> -carootUser <ARCserve caroot User> -carootPass <ARCserve caroot password> [-vcb <VCBMachineName>] -esxServer <ESXServerName> -esxUser <ESXAdmin> -esxUserPass <ESXAdminPassword> [-proto <https/http>] [-vcbMountableVM] [-delProxydb] [-retainVMinDB] [-silent] [-debug] -insertvm <VMname> -deleteVM <VMname> [-stopAutoPopulate]

      Note: For information about the usage for this command, see ca_vcbpopulatedb Usage (see page 41).

   ■ Execute the command using the arguments described in the following syntax:

      Note: You must create a configuration file to use this syntax. For more information, see Create a ca_vcbpopulatedb Configuration File (see page 41).

      ca_vcbpopulatedb –config <config_file_name>

      <config_file_name>

      Specifies the name of the ca_vcbpopulatedb configuration file.

4. Execute the command.

   The ca_vcbpopulatedb utility populates the CA ARCserve Backup database with information about the VMs that are in a running state in your environment.

Create a ca_vcbpopulatedb Configuration File

You create a configuration file with details about the CA ARCserve Backup Primary server machine, the CA ARCserve Backup Primary user name, and so on. The ca_vcbpopulatedb utility uses the information specified in the configuration file to populate the CA ARCserve Backup database.

To create a ca_vcbpopulatedb configuration file

1. Open a text editing application such as Notepad. Save the configuration file with a .cfg file extension in the same directory as the ca_vcbpopulatedb utility.

2. Complete the arguments in the following syntax:

   ```
   ca_vcbpopulatedb -Primary <PrimaryServerName> -carootUser <ARCserve caroot User>
   -carootPass <ARCserve caroot password> [-vcb <VCBMachineName>] -esxServer
   <ESXServerName> -esxUser <ESXAdmin> -esxUserPass <ESXAdminPassword> [-proto
   <https/http>] [-vcbMountableVM] [-delProxydb] [-retainVMinDB] [-silent] [-debug]
   -insertvm <VMname> -deleteVM <VMname> [-stopAutoPopulate]
   ```

   Note: For information about the usage for this command, see ca_vcbpopulatedb Usage .

3. Close and save the configuration file.

ca_vcbpopulatedb Usage

The ca_vcbpopulatedb command contains arguments and options that are used to define actions to follow when populating VM information into the CA ARCserve Backup database.

The ca_vcbpopulatedb command includes the arguments and options that follow:

-Primary <PrimaryServerName>

   Indicates the name or IP address of the CA ARCserve Backup primary system.

-carootUser <ARCserve caroot User>

   Indicates the user name, with CAROOT privileges, for the CA ARCserve Backup primary system.

-carootPass <ARCserve caroot Password>

   Indicates the password for the User name.

(Optional) –vcb <VCBMachineName>

Indicates the name or IP address of the VCB backup proxy system.

Note: If you omit this argument, the utility assumes that the current machine name will be used as VCB machine name.

-esxserver <ESXServerName>

Indicates the name of the ESX Server system or the VirtualCenter Server system containing the VMs.

-esxUser <ESXAdmin>

Indicates the name of the ESX Server system user or the VirtualCenter Server system user with Administrator privileges.

-esxUserPass <ESXAdminPassword>

Indicates the password for the ESXAdmin user.

(Optional) -proto <https/http>

Indicates the communication protocol between the backup proxy system and the ESX Server system or the VirtualCenter Server system.

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

-VCBMountableVM

Gives you the following options:

If you execute the ca_vcbpopulatedb command-line utility with this switch, you must run the utility on a backup proxy system. Without this switch, you can execute the ca_vcbpopulatedb utility on the backup proxy system or any other Windows 2003 system where the CA ARCserve Backup Client Agent for Windows is installed.

If you specify this switch as a parameter, the utility populates the database with the names of the VMs that are running and mountable.

You should run the ca_vcbpopulatedb command-line utility with this switch when you have VMs in an ESX Server residing on multiple storage media, such as the local disk of an ESX Server, SAN LUN, NAS/NFS, or iSCSI storage device.

Note: If you run this utility with the VCBMountableVM switch, the utility would take longer to run because it performs a mount and unmount operation of each running VM.

-DelProxydb

Deletes all the VMs available in the database for the given ESX Server system or the VirtualCenter Server system under the given backup proxy system.

-retainVMinDB

Lets you retain data (backup information) for VMs that are not available when you execute this command.

By default, this utility captures information from VMs that are available when you execute this utility. 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.

-Silent

Prevents the utility from printing messages to the command line console.

-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`

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

-insertVM

Lets you add information about a specific VM that resides in the VM host system to the CA ARCserve Backup database.

Note: You cannot combine this argument with any other argument when you execute ca_vcbpopulateDB.

-deleteVM

Lets you delete information about a specific VM from the CA ARCserve Backup database.

Note: You cannot combine this argument with any other argument when you execute ca_vcbpopulateDB.

-stopAutoPopulate

Lets you disable the auto-populate process for the specified backup proxy system.

More information:

Examples (see page 45)

ca_vcbpopulatedb Utility Return Codes

The ca_vcbpopulatedb utility generates return codes are written to a log file named ca_vcbpopulatedb.log. The log is created in the Client Agent for Windows installation directory after the ca_vcbpopulatedb utility execution is finished.

The ca_vcbpopulatedb utility generates the following return codes:

0

Indicates that the operation was successful.

1

Indicates that an invalid argument was specified.

2

Indicates that a CA ARCserve Backup domain user authentication failure occurred.

3

Indicates that an ESX Server or a VirtualCenter Server user authentication error occurred.

4

Indicates that an ESX Server or a VirtualCenter Server connection failure occurred.

5

Indicates that a database operation failure occurred.

6

Indicates that an XML creation failure occurred.

7

Indicates that Microsoft .NET version 2.0 or later is not installed in your environment.

8

Indicates that more than one instance of ca_vcbpopulatedb is currently running.

9

Indicates that an unknown error has occurred.

Examples

The following are examples of syntax for the ca_vcbpopulatedb command:

- Use the following command populate the VM details of the ESX Server having a hostname "ESXServer1" into the ARCserve server "ARCserver1" database under VCB Proxy machine "VCBProxy1" using http protocol with the debug flag set:

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

- Use the following command to remove the all VM details of the ESX Server having a hostname "ESXServer1" from the ARCserve server "ARCserver1" database available under VCB Proxy machine "VCBProxy1" with the debug flag unset:

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

- Use the following command to populate the VM details of the ESX Server having a hostname "ESXServer1" into the ARCserve server "ARCserver1" database, only the VM mountable inside the VCB proxy machine "VCBProxy1" with the debug flag set:

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

- Use the following command to stop populating the CA ARCserve Backup database automatically.

  - The server name is Myvirtualserver and the server resides in a VirtualCenter Server system:

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

  - The server name is MyEsxserver and the server resides in an ESX Server system:

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

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 back up 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 to 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 will not populate the CA ARCserve Backup database with information about Hyper-V VMs that are in a powered off state when you execute the tool.

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

   Note: If the VMs are not in a running state, ARCserve Hyper-V Configuration Tool cannot detect the host name of the VM and collects the VM name in the Hyper-V system instead of the host name. In addition, CA ARCserve Backup can perform raw (full VM) backups of the VM, but will not be able to perform file level backups and restores.

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.
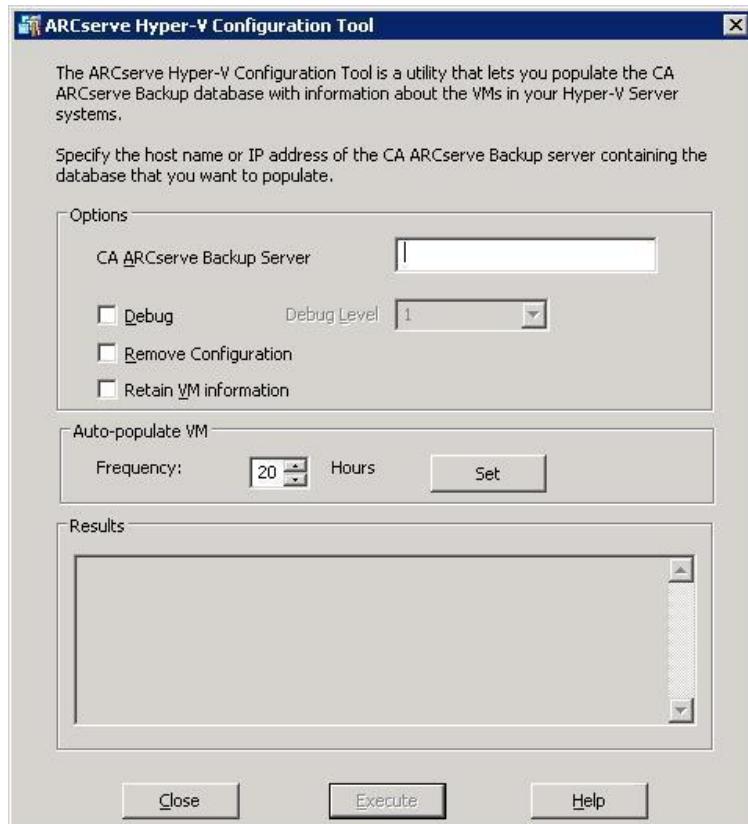
4. Complete the following fields:

   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, and populate the latest VM data into the CA ARCserve Backup database.

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.

Auto-populate the 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

5. Click Execute.

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

Populate the Database Using the ca_msvmpopulatedb Command Line Utility

The ca_msvmpopulatedb utility is a data collection tool that lets you populate the CA ARCserve Backup database with information about the VMs running in the Hyper-V host system.

After you install the agent, you must populate the CA ARCserve Backup database with the information about your Hyper-V systems. To accomplish this, you must execute the ca_msvmpopulatedb utility on the Hyper-V host system where the CA ARCserve Backup Client Agent for Windows is installed.

By default, ca_msvmpopulatedb is installed in the directory that follows on the Hyper-V host system:

```
c:\Program Files\CA\ARCserve Backup Client Agent for Windows
```

To populate the database using the ca_msvmpopulatedb command line utility

1. Ensure that the VMs in the Hyper-V host system are in a running state.

   Note: If the VMs are not in a running state, the ca_msvmpopulatedb utility 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 Hyper-V host systems.

2. Log in to the Hyper-V host system, open a command line window, and execute the ca_msvmpopulatedb utility using the syntax that follows:

   ```
   ca_msvmpopulatedb -primary <ARCservePrimaryServerName> [-Debug] <debuglevel>]
   [-retainVMinDB] [-DelVMinDB]
   ```

   Note: For more information about the usage for the ca_msvmpopulatedb command, see ca_msvmpopulatedb Usage (see page 49).

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

ca_msvmpopulatedb Usage

The ca_msvmpopulatedb command contains arguments and options that are used to define actions to follow when populating VM information into the CA ARCserve Backup database.

The ca_msvmpopulatedb command includes the arguments and options that follow:

-Primary

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 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.

-retainVMinDB

Lets you retain data (backup information) for VMs that are not available when you execute this command.

By default, this utility captures information from VMs that are available when you execute this utility. 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.

-DelVMinDB

Lets you delete the VMs available in the CA ARCserve Backup database for the specified Hyper-V server, and populate the latest VM data into the CA ARCserve Backup database.

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).

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
    ```

More information:

How to Uninstall the Agent

Use Add or Remove Programs in the Windows Control Panel to uninstall CA ARCserve Backup Agent for Virtual Machines.

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 VirtualCenter 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 ESX Server 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 ESX Server 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 ESX Server 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.

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. **VMware VCB Framework** ■ Ensure that VMware VCB Framework is installed on the system that will function as the backup proxy system.	**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 the Hyper-V host system.

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 34). ■ Deploy the Agent for Virtual Machines using Agent Deployment. For more information, see Deploy the Agent to VMs Using Agent Deployment (see page 29).	■ 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 46). ■ Deploy the Agent for Virtual Machines using Agent Deployment. For more information, see Deploy the Agent to VMs Using Agent Deployment (see page 29).
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 66).	

Chapter 3: Backing Up and Restoring Data

This section contains the following topics:

How to Browse 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 Server systems

- VMware VirtualCenter Server systems

- Microsoft Hyper-V 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 VCB Systems object can be expanded to display the names of the VMware VCB Systems, the backup proxy systems, the ESX Server or the VirtualCenter Server systems, and the VM volumes contained in the Windows operating system.
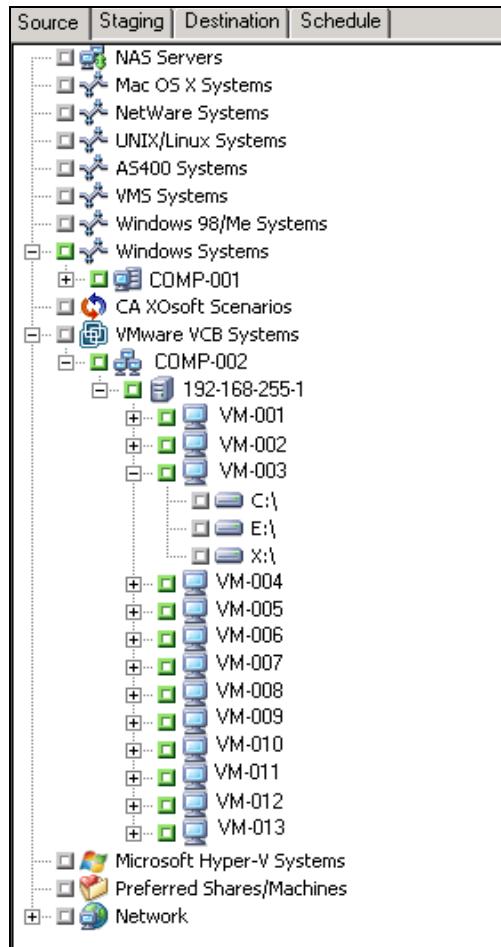
- When you submit a backup job, CA ARCserve Backup prompts you to provide the Username and password credentials for ESX Server system or the VirtualCenter Server system.

  CA ARCserve Backup validates the credentials at runtime.

- 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

How Global and Local Backup Modes Work

Backup modes define how CA ARCserve Backup backs up data stored on VMs. CA ARCserve Backup lets you process backup data using the backup modes that follow:

- **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.

- **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 .

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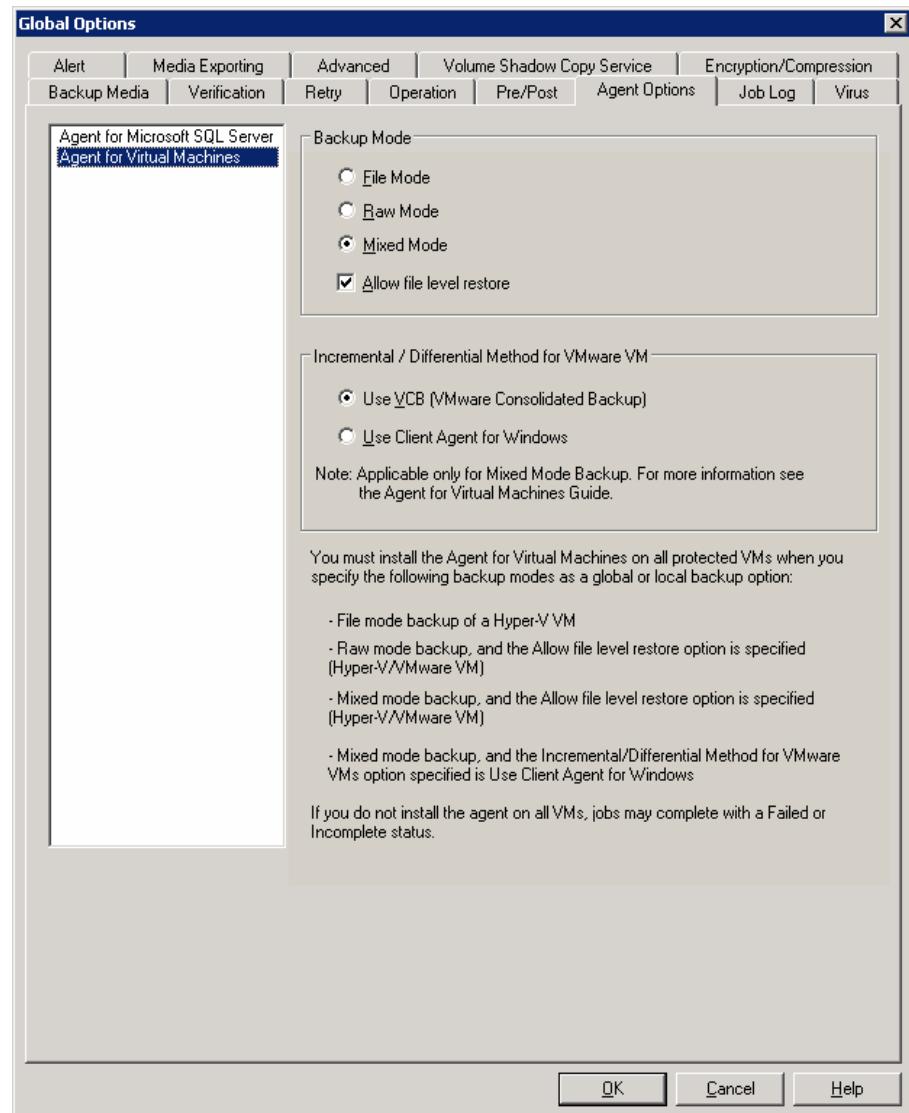
You can specify backup modes as either a global backup option or a local backup option.

- **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 Specify Backup Modes as a Global Backup Option (see page 61).

- **Local backup option--**Lets you apply a Backup Mode to individual VMware and Hyper-V VMs at the job level. For more information, see Specify Backup Modes as a Local Backup Option (see page 63).

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	CA ARCserve Backup processes the raw (full) VM backup data and the file mode backup data using VCB.	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 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 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 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 VCB 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

   Use File Mode when you need to 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

Use Raw mode when you need to 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

Use Allow file level restore when you need to 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 32).

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

■ Restore Raw Mode backups at file level granularity

■ Restore Mixed Mode backups at file level granularity

   Note: Allow file level restore can be used on 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.

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--**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 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 VCB 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 57).

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

    File Mode

    Use File Mode when you need to 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

    Use Raw mode when you need to 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

Use Allow file level restore when you need to 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 32).

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

■ Restore Raw Mode backups at file level granularity

■ Restore Mixed Mode backups at file level granularity

Note: Allow file level restore can be used on 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.

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 61).

Back Up Data

Use the steps that follow to submit backup jobs on local disk-based virtual machines (VMs) and SAN-based VMs. This topic applies to VMware VCB systems and Microsoft Hyper-V systems.

Note: For information about the limitations of backing up with VCB, see Backup and Restore Limitations on Virtual Machines (see page 81).

To back up data

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

    The Backup Manager source directory tree displays.

2. Expand the VMware VCB Systems object or the Microsoft Hyper-V Systems object.

    The backup proxy systems, ESX Server systems, VirtualCenter Server systems, VMs, and 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.

4. Specify a Backup Mode for the job.

    Note: For more information about backup modes, see Backup Modes (see page 57).

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 69).

    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 69). For more information about specifying filters, click the Help button on the Filter dialog.

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

   The Security and Agent Information dialog opens.

   You must provide ESX Server or VirtualCenter Server and backup proxy system credentials 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 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 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 ESX Server system or the VirtualCenter 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 Server backups under the following scenarios:

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

  The following message displays:

  Note: The target node <VCB Proxy System's Name/IP> is a VMware VCB Proxy System. PFC only verifies the status of Client Agent on the VMware VCB 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 VCB proxy system.

  The following message displays:

  Issues: Failed to connect to the client agent on <VCB Proxy System's Name/IP>. Ensure that the client agent on <VCB Proxy System's Name/IP> is running.
  Note: The target node <VCB Proxy System's Name/IP> is a VMware VCB Proxy System. PFC only verifies the status of Client Agent on the VMware VCB 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.

How to Browse Restore 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 will display.
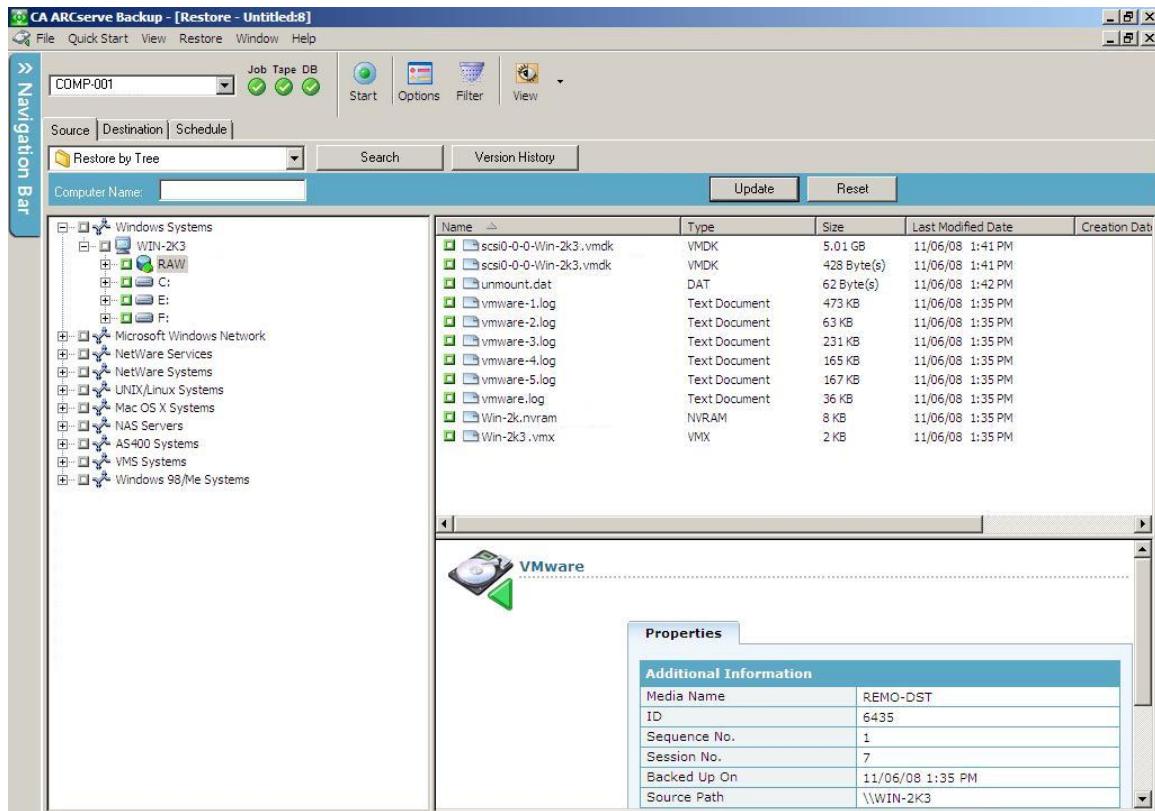
The session properties section of the Restore Manager window displays the following information about the VMware backup data:

VMware Proxy

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

VMware ESX Server

Indicates the name of the ESX Server or the VirtualCenter 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).

Restoring Data

When you back up a VM using CA ARCserve Backup on the backup proxy system, you can restore the following types of data:

■ File level backups

■ [Raw (full VM) level backups](see page 73)

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 57).

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 57).

■ 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.
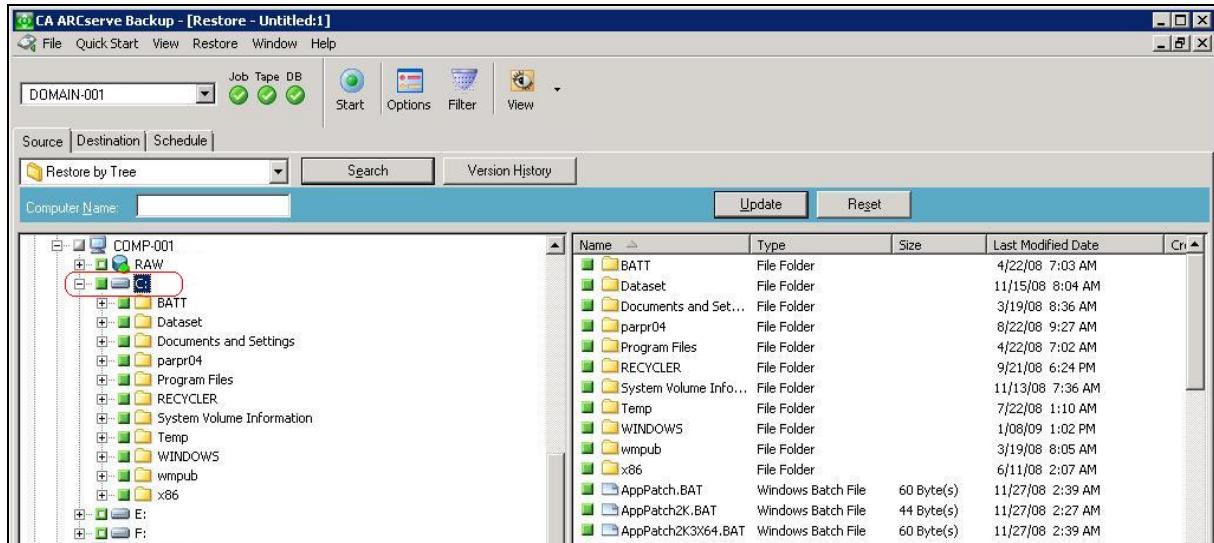
3. Click the Destination tab. Click the Restore files to their original locations check box to restore the files to their original location.

   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) 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.
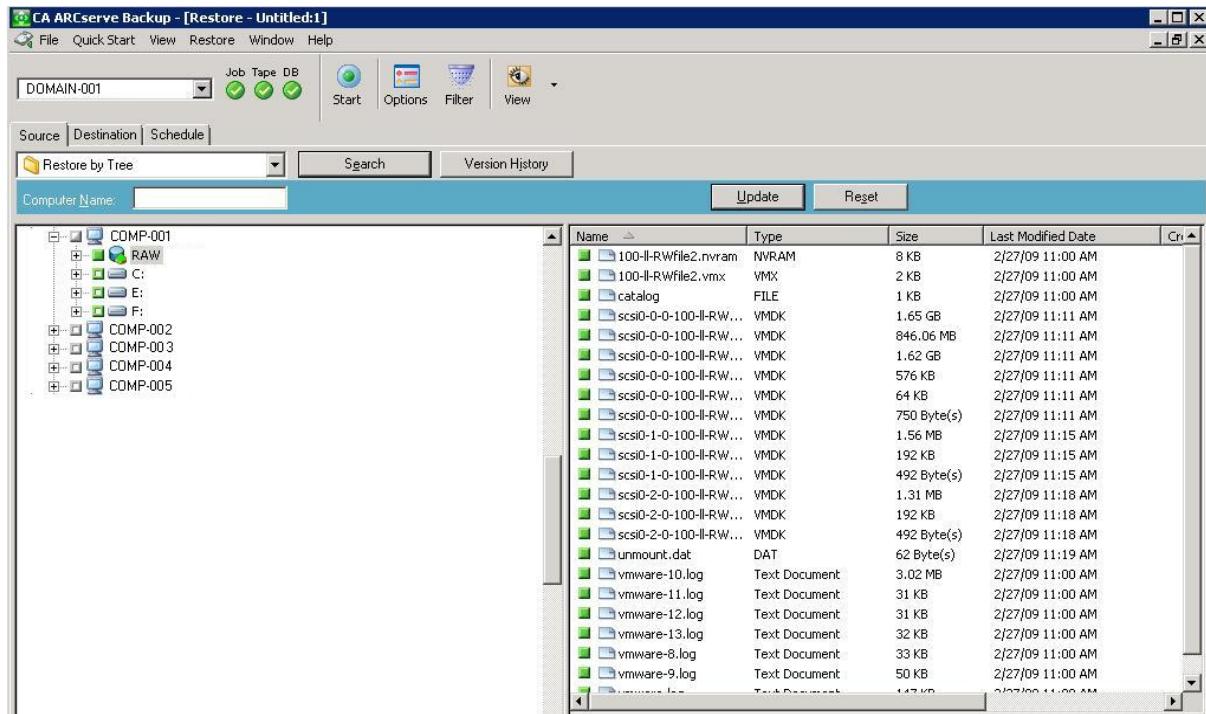
2. Click the Destination tab.

    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.

Recover VMware Virtual Machines

The process of recovering a VMware VM 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:

- 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 ESX Server 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:
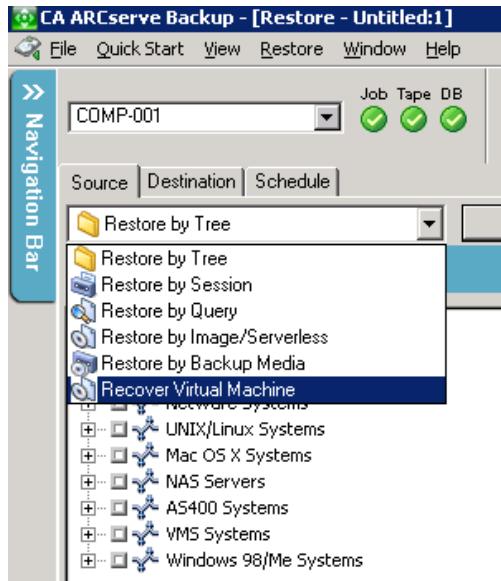
The Recover Virtual Machine window opens.

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 of 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 of 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.

   ESX Server Name

   Lets you specify the ESX Server and the security information required to recover the VM image.

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

   Data Store

   Lets you specify the Data Store associated with the ESX Server system.

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

6. Click OK.

    The options are applied.

7. Click Start on the toolbar 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

The process of recovering a Hyper-V VM 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 Restore Virtual Machine from the drop-down list as illustrated by the following screen:
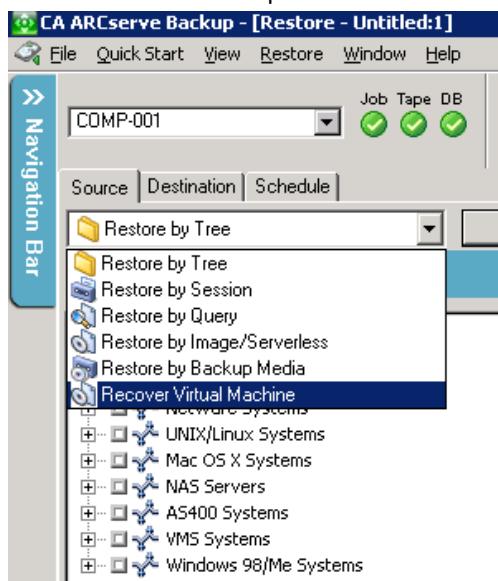
The Restore Virtual Machine window opens.

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 of 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 of 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.

   Accept the Host Name Backup displayed or click in the Host Name field and then click the ellipsis to search for the Hyper-V host system associated with this VM.

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 need to use the VM immediately after the recovery is complete.

6. Click OK.

    The options are applied.

7. Click Start on the toolbar 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*.

Backup and Restore Limitations on Virtual Machines

The limitations that follow affect VM backup and restore operations:

■   The VMs in the ESX Server must be in a running state when you run the ca_vcbpopulatedb utility.

    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 the ESX Server systems.

■   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 VMw 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.

How to Use Virtual Machine 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 34) and ARCserve Hyper-V Configuration Tool (see page 46).

How VM 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.

Appendix A: Troubleshooting

This section contains the following topics:

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 the 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 ESX server is down.

  Action 2: Take corrective action if the ESX server 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 Server or VirtualCenter 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 Server system credentials or VirtualCenter 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 ESX Server 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

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 ESX Server or VirtualCenter Server system to bypass the process of connecting with the backup proxy system.

To add ESX Server systems, VirtualCenter 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 ESX Server or VirtualCenter Server system. To add multiple ESX Server systems and VirtualCenter Server systems, separate the entries using semicolons (;).

   Click OK, as required, to close all open dialogs.

   The ESX Server systems and VirtualCenter Server systems are added to the exceptions list.

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 32).

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 VCB Systems object or the 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 VCB 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.

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 will fail on VMware VMs. The list that follows describes the reasons jobs will fail and the required corrective actions.

- **Reason 1:** The credentials specified for the ESX Server system are not correct:

  Action 1: Ensure that the credentials specified for the ESX Server 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 ESX Server system. Optionally, you can move the target datastore to a different ESX Server system.

- **Reason 3:** The ESX Server system is down or not reachable.

  Action 3: Ensure that the ESX Server 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 of x64 architecture on an ESX Server system of x86 architecture.

  Action 5: Ensure that the ESX Server 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`

Unable to Restore File Level Backup Data to a CA ARCserve Backup Server

Valid on Windows systems.

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:
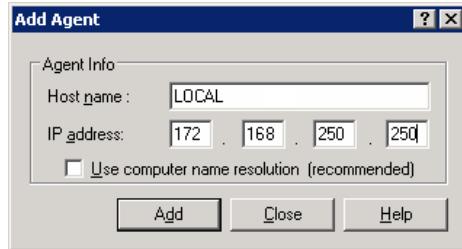
Click Add.

The CA ARCserve Backup server is added to the Windows Systems object, as illustrated by the following screen.
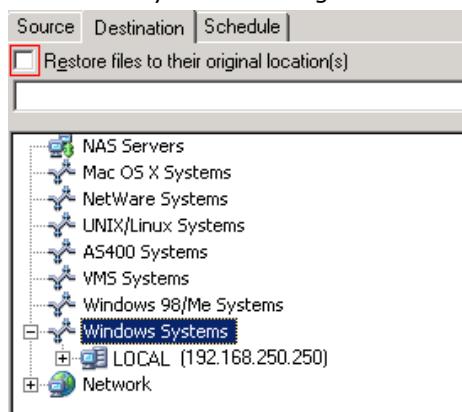
4. Click Close.

   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.

Appendix B: Configuring ESX Server Systems and VirtualCenter Server Systems

The sections that follow describe how to configure the communication protocol to set up backing up ESX Server systems and VirtualCenter Server systems using a backup proxy system.

This section contains the following topics:

Configure ESX Server 3.0.2 Systems

This topic describes how to configure the communication protocol on ESX Server 3.0.2 systems.

To configure ESX Server 3.0.2 systems

1. Install ESX Server. For more information about ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your ESX Servers through VMware VirtualCenter, you must install and configure VirtualCenter 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 ESX Server 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 an ESX Server 3.0.2 system, configure one of the following communication protocols:

https

To use https as the communication protocol between the ESX Server system and the backup proxy system, copy the self-generated SSL certificate from the ESX Server 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 ESX Server system or the VirtualCenter Server system.

You can find the SSL certificate (labeled rui.crt) from the following directory on the ESX Server 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 ESX Server 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 ESX Server system, you must configure the http protocol on the ESX Server 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 38).

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 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.

Configure ESX Server 3.5 Systems

This topic describes how to configure the communication protocol on ESX Server 3.5 systems.

To configure ESX Server 3.5 systems

1. Install ESX Server. For more information about ESX Server requirements, see the VMware ESX 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 ESX Server 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 38).

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 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.

Configure ESX Server 3i Systems

This topic describes how to configure the communication protocol on ESX Server 3i systems.

To configure ESX Server 3i systems

1. Install ESX Server. For more information about ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your ESX Servers through VMware VirtualCenter, you must install and configure VirtualCenter 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 ESX Server 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 38).

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 VirtualCenter Server 2.0.2 Systems

This topic describes how to configure the communication protocol on VirtualCenter Server 2.0.2 systems.

To configure VirtualCenter Server 2.0.2 systems

1. Install ESX Server. For more information about ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your ESX Servers through VMware VirtualCenter, you must install and configure VirtualCenter 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 ESX Server 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 VirtualCenter Server system, configure one of the following communication protocols:

https

To use https as the communication protocol between the VirtualCenter Server system and the backup proxy system, you must copy the self-generated SSL certificate from the VirtualCenter 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 VirtualCenter 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 VirtualCenter Server 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 VirtualCenter Server system, you must configure the http protocol on the VirtualCenter 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 VirtualCenter 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. 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 38).

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 CA ARCserve Backup 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.

Configure VirtualCenter Server 2.5 Systems

This topic describes how to configure the communication protocol on VirtualCenter Server 2.5 systems.

To configure VirtualCenter Server 2.5 systems

1. Install ESX Server. For more information about ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your ESX Servers through VMware VirtualCenter, you must install and configure VirtualCenter 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 ESX Server 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 VirtualCenter Server system, configure one of the following communication protocols:

   https

   To use https as the communication protocol between the VirtualCenter Server system and the backup proxy system, you must copy the self-generated SSL certificate from the VirtualCenter 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 VirtualCenter 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 VirtualCenter Server 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 VirtualCenter Server system, you must configure the http protocol on the VirtualCenter 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 VirtualCenter 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 38).

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.

Appendix C: Protecting Hyper-V Systems Using the Hyper-V VSS Writer

This section contains the following topics:

Overview of Protecting Hyper-V VMs Using the Hyper-V VSS Writer

CA ARCserve Backup lets you protect Hyper-V VMs using the ARCserve Volume Shadow Copy Service (VSS) agent. The agent is designed to protect Microsoft Hyper-V data with VSS Writers using Volume Shadow Copy Service technologies.

The sections that follow describe how to configure, back up, and restore Hyper-V VMs using the Hyper-V VSS writer. The processes described are applicable to CA ARCserve Backup for Windows r12 SP1 installations, and can be used protect Hyper-V systems in CA ARCserve Backup for Windows r12.5 installations.

Limitations and Considerations

- You cannot restore data at file level granularity from raw (full VM) backup data.

- You cannot perform mixed mode backups, which consist of raw (full VM) weekly backups and file mode daily backups.

- You can protect Hyper-V VMs that are in a powered off state when you execute ARCserve Hyper-V Configuration Tool.

Prerequisite Components

The prerequisite components for Hyper-V VSS Writer protection are identical to that of standard VSS Writer requirements. The applications that follow are required to deploy Hyper-V VSS technology in your CA ARCserve Backup environment:

- CA ARCserve Backup for Windows r12.5

- CA ARCserve Backup for Windows r12.5 Client Agent for Windows

  The CA ARCserve Backup Client Agent for Windows must be installed in partition zero (0) on the Hyper-V server machine. Partition zero (0) is reserved for the host operating system and its applications. All other partitions, for example, partition 1, 2, and so on, are reserved for child partitions or virtual machines (VMs).

- CA ARCserve Backup for Windows r12.5 Agent for Open Files

  You must register the license for the Agent for Open Files on the Hyper-V host system.

  Note: You may use the license key for the Agent for Open Files that was provided with the license key for the Agent for Virtual Machines.

Configure CA ARCserve Backup to Detect Hyper-V VMs

To perform backup and restore operations on machines using the Hyper-V VSS writer, you must configure CA ARCserve Backup to detect the Hyper-V server.

To configure CA ARCserve Backup to detect Hyper-V VMs

1. Based on the configuration in your backup environment, complete one of the following actions and then go to the next step.

   ■ If the CA ARCserve Backup server components are installed on the Hyper-V server system, add the local Hyper-V server into the Backup Manager.

   ■ If the CA ARCserve Backup server components are not installed in the Hyper-V server, add the remote Hyper-V server into the Backup Manager by completing the steps that follow:

   a. From the Source tree in the Backup Manager, right click the Windows Systems object and select Add Machine/Object from the pop-up menu.
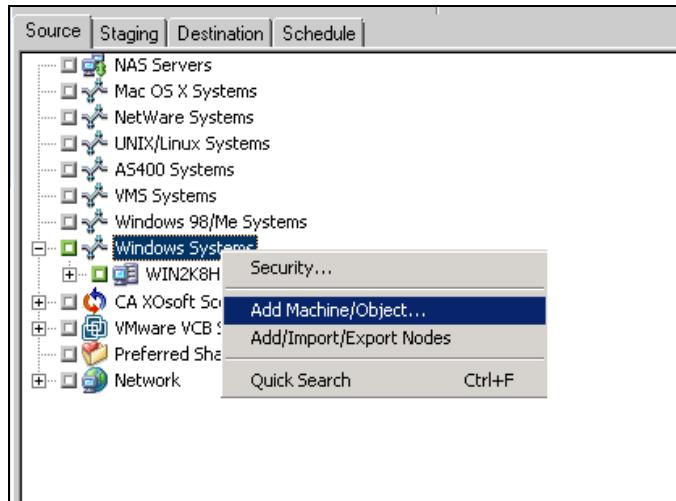
   The Add Agent dialog opens.

b. From the Add Agent dialog, specify the name of the Hyper-V server in the Host Name field or the IP address in the IP address field, and then click Add.
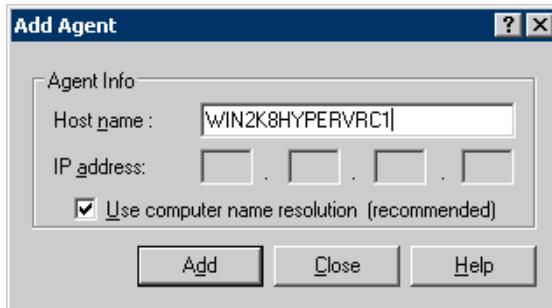
After you add the Hyper-V server system into the Backup Manager, expand the Hyper-V server to display the Microsoft Hyper-V VSS Writer as illustrated by the following screen.
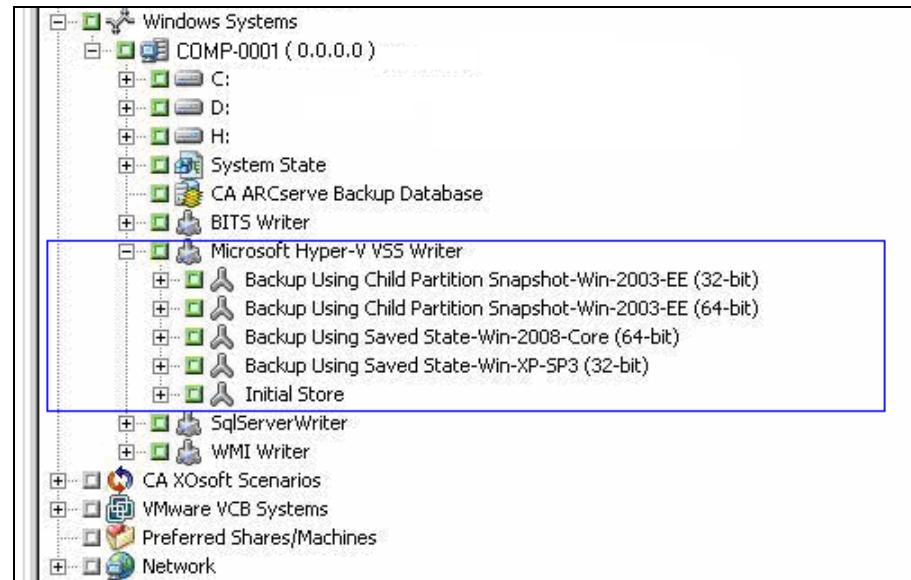
How Back Up Using Saved State Works

Back up Using Saved State is a backup operation that places VMs into a saved state before the backup is performed. This state lets you perform point-in-time backups of guest operating systems. It is a stateful, data inconsistent backup. Back up Using Saved State presents the following limitations on VM backups:

■ The virtual hard disk in the backup cannot be offline mounted to retrieve specific files.

■ The applications in the VM will not be aware that a backup, a restore, or both occurred when you restore the backed up data.

Note: For more information about these limitations, see the Microsoft website.

How Back Up Using Child Partition Snapshot Works

Back up Using Child Partition Snapshot is a backup operation that lets the VSS Writer take a snapshot of the data from the guest operating system in the VM. Backups of this type let you back up VMs that support VSS and have the Integration components installed and enabled. It is a stateless, data consistent backup.

Back up Using Child Partition Snapshot presents the following advantages on VM backups:

■ You can offline mount the virtual hard disk from this backup to retrieve specific files.

■ The VSS capable applications residing in the VM will detect that the backup or restore of the VM is taking place, and they will participate in that backup or restore process to ensure that the application data is consistent.

Note: For more information, see the Microsoft website.

Back Up Hyper-V VMs Using the Hyper-V VSS Writer

The Hyper-V VSS Writer lets you back up VMs that are in an online and offline state. These operations are transparent to CA ARCserve Backup.

Note: The Hyper-V VSS Writer supports only full backups.

The following steps describe how to back up Hyper-V VMs using the Hyper-V VSS Writer. For information about backing up data using the VSS Writer, see the *CA ARCserve Backup for Windows Microsoft Volume Shadow Copy Service Guide*.

To back up Hyper-V VMs using the Hyper-V VSS writer

1. Open the Backup Manager, select the Source tab, and select the Microsoft Hyper-V VSS Writer object.

   All Hyper-V settings and virtual machines are specified for backup. If you do not want to back up all of the VMs, expand the Microsoft Hyper-V VSS Writer object (to display all servers) and clear the check mark next to the server that you do not want to back up.

2. (Optional) Right-click the Microsoft Hyper-V VSS Writer object and select Writer Options from the pop-up menu.

3. Click the destination tab to specify the destination for backup.

4. Click the Start toolbar button to submit the job.

Restore Data to Its Original Location

This method lets you restore the Hyper-V configuration, the VMs configurations, and the backup data to its original location. The current Hyper-V configuration and VMs configuration and data will be restored to the state they were in when they were backed up.

Limitations and Considerations

- The Hyper-V servers can be in an online state or offline state during the restore operation.

- The Hyper-V VSS Writer ensures that the backup data is properly restored to its original location.

- You do not need to perform additional steps during the restore or after the restore is complete.

- The VM can be used as soon as the restore is complete.

Using CA ARCserve Backup to restore Hyper-V server data, you can recover data in the following scenarios:

- You can restore Hyper-V server backup data to its original location.

- You can restore VM backup data to its original location.

- You can recover a guest operating system in a VM to its original location.

Note: For information about using the VSS Writer, see the *CA ARCserve Backup for Windows Microsoft Volume Shadow Copy Service Guide*.

To restore data to its original location

1. Open the Restore Manager and do one of the following:

   ■ From the drop-down list, select the Restore by tree method, expand the Windows Systems object, browse to Microsoft Hyper-V VSS Writer, and specify one or more VMs that you want to restore.
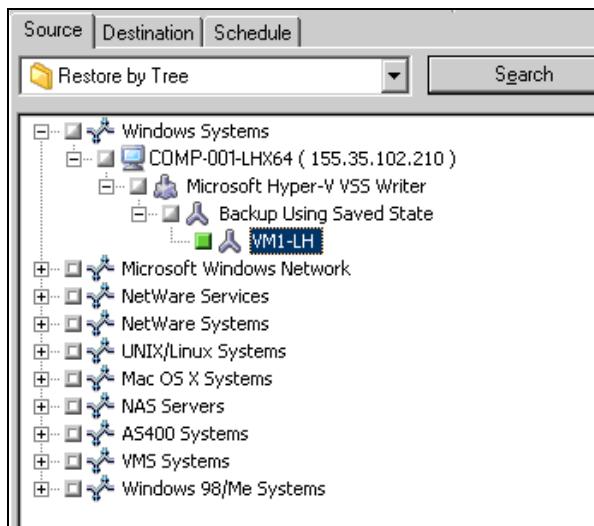
   ■ From the drop-down list, select Restore by session, browse to and specify a session to restore.

2. Click the Destination tab.

   Click the Restore files to their original location option.

3. Click the Start toolbar button to submit the job.

   After the restore is complete, the restored VMs will be in a Saved state. In other words, the online restore places the VMs in an offline state when the restore is complete. You must then start the VMs manually to bring them to an online state.

Index