Arcserve® Backup for Windows

Agent for Virtual Machines Guide

r17.5

arcserve®

Arcserve Product References

This document references the following Arcserve products:

- Arcserve® Backup
- Arcserve® Unified Data Protection
- Arcserve® Unified Data Protection Agent for Windows
- Arcserve® Unified Data Protection Agent for Linux
- Arcserve® Replication and High Availability

Contact Arcserve

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

https://www.arcserve.com/support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.

You can access other helpful resources appropriate for your Arcserve product.

Contents

Appendix A: Troubleshooting 117

Appendix B: Configuring VMware ESX Host Systems and vCenter Server Systems 147

Chapter 1: Introducing the Agent

This section contains the following topics:

Introduction

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 Arcserve Backup offers is the Arcserve Backup Agent for Virtual Machines. The agent lets you protect virtual machines running the following systems:

- **VMware ESX/ESXi Server and VMware vCenter Server--**VMware provides you with a mechanism called Virtual Disk Development Kit (VDDK) that integrates with VMware ESX/ESXi Server and VMware vCenter Server. VDDK lets you protect Virtual Machine (VM) files and data. With VDDK you offload virtual machine backup activity to a dedicated backup proxy system, and then use the backup and restore functionalities provided by Arcserve Backup to protect the VMs.
- **VMware vSphere--**VMware vSphere is a virtualization tool kit that lets you integrate the latest versions of VMware vCenter Server and VMware VDDK with Arcserve Backup.
- **Microsoft Hyper-V--**Microsoft Hyper-V is a component that is included with Windows Server 2008 x64 or later operating systems. Hyper-V is hypervisor-based technology that lets you run multiple operating systems independently within the Windows Server system. Arcserve Backup lets you back up and restore data contained within the guest operating systems and Windows Server operating systems.

How the Agent Protects VMware Systems

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

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

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

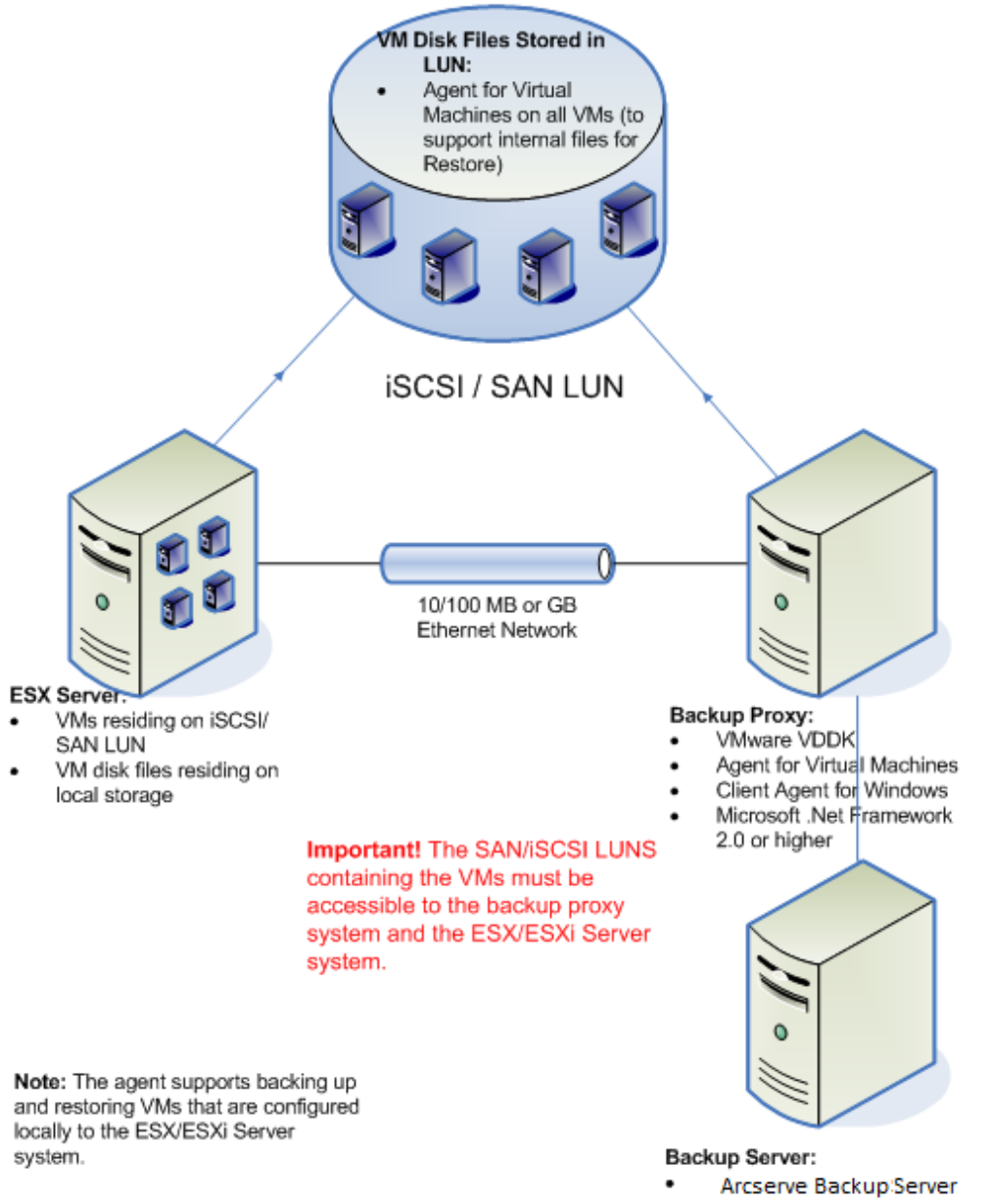
- Your environment consists of VMs residing on different types of data stores.
- You want to restore data at the file level or raw (full VM) level.

How the Agent Protects VMware Environments

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 Using the Agent with a Backup Proxy System



1. The Arcserve Backup primary or member server communicates with the Agent for Virtual Machines that is running on the backup proxy system while the backup job is running. The agent then takes a snapshot of the VM and mounts or exports the snapshot to the backup proxy system, by default, into the Client Agent for Windows installation directory.
2. If the backup mode specifies Allow File Level Restore, Arcserve Backup creates catalog files representing the volumes on the VM.
3. 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.

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

- The agent must be licensed on the Arcserve Backup primary or stand-alone server.
- When you perform raw (full VM) backups on VMware Windows VMs, the agent is not required to be installed on the VMs to provide file level restore. File level restore is automatically provided from raw backups. However, the agent is required to be installed when performing a restore. For more information, see Where to Install the Agent.

  Note: To take advantage of this feature, it is required to upgrade the server and the Agent for Virtual Machines with the Arcserve Backup r17 release.
- Microsoft .NET Framework Version 2.0 or higher must be running on the backup proxy system.
- When the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host and the backup proxy system and have the same LUN number assigned. The LUN in the backup proxy system should not be signed.
- 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.

  Note: With the latest Arcserve Backup release, the agent for virtual machines is no longer required to be installed on the VM. Therefore, when you run incremental backup jobs through the mixed mode backup method, the only option available to run an incremental backup job is through VDDK on the proxy server.

- 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 Virtual Machines that Reside on Local Storage and SANs

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

- **SAN, iSCSI Data Stores--**The backup proxy system must be attached to the same disk where the VM resides and must be attached using the same SAN, iSCSI infrastructure.
- **Local Storage Data Stores--**The VMs must reside on disks that are attached directly to the VMware ESX Host system. With local storage environments, the backup proxy system should be able to communicate with the VMware ESX Host system via the LAN.

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

How the Agent Protects VMware vSphere Systems Using VDDK

Arcserve Backup lets you protect VMware vSphere systems using VDDK.

This section contains the following topics:

VMware VDDK Included on the Installation Media

Arcserve Backup installs VMware Virtual Disk Development Kit (VDDK) 6.0.1 on all systems where you install the agent. You do not need to download and install VDDK on your backup proxy systems.

Introduction to Integrating with VMware vSphere

Arcserve Backup Agent for Virtual Machines integrates with the latest version of VMware Virtual Infrastructure named vSphere. This capability lets you protect virtual machines (VMs) that reside in vSphere environments (for example, the VMs reside in ESX Server 4.0 systems and vCenter Server 4.0 systems). The agent facilitates protecting virtual machines using VMware Virtual Disk Development Kit (VDDK).

VDDK lets you access VM disks remotely on ESX Server systems without exporting the disks to the backup proxy system. This approach can be used with only the following VMware platforms:

- ESX Server 6.0, 5.5, and 5.1
- vCenter 6.0, 5.5, and 5.1 systems

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

The advantages of using VDDK are as follows:

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

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

- VDDK minimizes the dependency on VMware tools. VDDK provides more control and improved reporting for VM backup and recovery operations.

You can use the following approaches to protect your virtual machine environment:

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

How vSphere Integrates with Previous Releases of the Agent

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

- Back up file level data and raw (full VM) data using Arcserve Backup r16, and r16.5 with VMware VDDK in an environment that is running older version of ESX Server or VirtualCenter Server.
- Restore raw (full VM) data, file level data, and recover VMs using data that was backed up with Arcserve Backup r16 or Arcserve Backup r16.5 using VDDK.

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

How the Agent Protects Hyper-V Systems

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

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

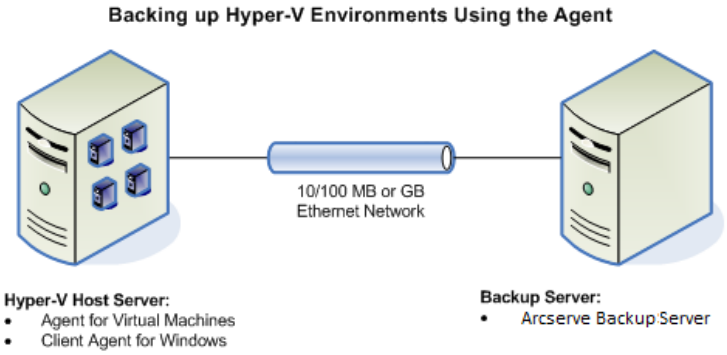
- Perform file level backups and restores of a VM running any Hyper-V supported Windows-based operating system.
- Perform raw (full VM) level backups and restores of a VM running any Hyper-V supported operating system.
- Back up VMs, regardless of their power state.

  Note: The agent lets you back up VMs while they are in a powered off state. However, the VMs should be powered on when populating the Arcserve database.
- Reduce administration overhead by centralizing backup management on Hyper-V host systems.

How the Agent Protects Hyper-V Environments

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.



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

- The agent must be licensed on the 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.
- 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 Functionalities

The agent supports the following functionalities:

- **Multistreaming--**Arcserve Backup lets you submit jobs using multistreaming at the VM level.
- **Staging--**Arcserve Backup lets you submit VM backup jobs to disk staging and tape staging devices.

  You can restore data at file level granularity directly from the staging device and from final destination media, such as tape media.
- **Deduplication--**Arcserve Backup lets you save disk space by eliminating blocks of redundant backup data.

- **Multiplexing**--Arcserve Backup lets you submit jobs using multiplexing.
- **GFS and rotation backups**--Arcserve Backup lets you submit GFS and rotation backup jobs.
- **Makeup Jobs:**
  - **Raw (full VM) backups**--Arcserve Backup restarts failed jobs at the VM level.
  - **Incremental and differential backups**--Arcserve Backup restarts failed jobs at the volume level.
- **Compression**--Arcserve Backup lets you compress VM backup data on the agent system or the Arcserve Backup server.
- **Encryption**--Arcserve Backup lets you encrypt VM backup data on the agent system or the Arcserve Backup server.
- **CRC verification**--Arcserve Backup lets you verify data integrity by supporting CRC verification on VM backup data.
- **Spanned, Striped, Mirrored, and RAID-5 volumes**--Arcserve Backup lets you protect VM data that resides in spanned, striped, mirrored, and RAID-5 volumes.
- **Raw Device Mapping (RDM)**--Arcserve Backup lets you back up data on volumes that contain Raw Device Mapping (RDM) configured in virtual compatibility mode. Arcserve Backup supports this capability on VDDK-based backups.

  When you restore data using the Recover Virtual Machine method, RDMs that are configured in virtual compatibility mode will be restored as normal virtual disks.
- **Hyper-V Dynamic Memory**--Windows Server 2008 R2 SP1 and Windows Server 2012 support the capability to adjust the amount of memory available to Hyper-V virtual machines dynamically as workloads on the virtual machines change. To support this capability, Arcserve Backup lets you recover virtual machines that were backed up with Hyper-V dynamic memory specified to the amount of memory that was originally allocated to the virtual machines.

How the Agent Analyzes Data that Resides on Virtual Machines

Virtual machines (VMs) running VMware vSphere and Microsoft Hyper-V can identify the used blocks of data on virtual disks. This capability lets Arcserve Backup decrease the overall backup time for jobs. The overall backup time decreases because Arcserve Backup backs up only the used blocks of data, not the entire disk.

Arcserve Backup uses the block analysis approach when backing up data that resides on Hyper-V VMs, and on VMware VMs that have VMware vSphere Web Services SDK and VMware VDDK running in the environment. In addition, change block tracking must be enabled on the VMware VMs. For more information about change block tracking, see the VMware website.

Note: On VMware VMs, you must specify a backup approach. For more information, see Specify a Backup Approach.

When backups of VMs run, Arcserve Backup backs up only the active blocks relating to the full backup phase of Raw (full VM) backups (with and without the Allow file level restore option specified), and Mixed mode backups with the Allow file level restore option specified.

Be aware of the following behavior:

- On Hyper-V VMs, Arcserve Backup does not use the active block analysis approach to backups when the agent cannot create disk bitmaps of the VM. The agent cannot create disk bitmaps when the parent virtual hard disk (VHD or VHDX) is a fixed disk and not a dynamic expanding disk. If the agent detects this condition, Arcserve Backup reverts to previous backup behavior, which is to analyze each block of data contained within the backup.

Backup and Restore Limitations on Virtual Machines

The limitations that follow affect VM backup and restore operations:

- **Backing up data through pass-through disks--**Pass-through disks are physical disks or LUNs that are attached to virtual machines. Pass-through disks do not support some of the functionality of virtual disks, such as virtual machine snapshots. With pass-through disks, you can expect the agent to behave as follows:
  - When backing up data, the agent skips the pass-through disks that are attached to the virtual machine.
  - When restoring the data, the agent cannot recover the data that was skipped during the backup.
- **Running state of the virtual machines--**The VMs in the VMware ESX Host must be in a running state when you populate the Arcserve Backup database.

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

- **When to run the configuration tools--**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 Arcserve Backup database, and failed backup jobs will occur at runtime.

- **Command Line support--**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.

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

- **Compare utility--**The Compare Utility does not support comparing VM backup sessions.

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

- **Merge utility--**Due to limitations in the physical and logical mapping of the volumes in the Arcserve Backup database, the Merge Utility does not support performing a sequential merge.

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

- **Global backup options not supported--**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*.

- **Mount path character limitations--**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.

- **Version of Hyper-V**--The agent cannot recover Hyper-V virtual machines to an older version of Hyper-V. The version of Hyper-V that is running on the restore destination must be equal to or later than the version of Hyper-V that was backed up.

Chapter 2: Installing and Configuring the Agent

This section contains the following topics:

How to License the Agent

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

Examples: How to License the Agent

The following list describes typical installation scenarios:

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

- Your environment consists of two Hyper-V host systems. Each Hyper-V host system contains three guest operating systems. You must register eight licenses (1 host system + 3 VMs, 1 host system + 3 VMs) on the Arcserve Backup server.
- Your environment consists of one 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 Arcserve Backup server. Therefore, you must register three licenses (1 host system + 2 VMs) on the Arcserve Backup server.

  Note: Upgrading to the Arcserve Backup r17 release does not require you to install the agent on the VM for VMware ESX host systems when performing a raw (full VM) backup with the file level restore option enabled.

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

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.

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 VDDK	Using the Client Agent	Using VDDK	Using the Client Agent

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

Note: 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.

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. Arcserve Backup manages the recovery of Hyper-V VMs when you install the Agent for Virtual Machines on the Hyper-V Host system.

Best Practices for Installing and Configuring the Agent for Virtual Machines

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

Task	VMware Systems	Hyper-V Systems

Task	VMware Systems	Hyper-V Systems
Required components	**Arcserve Backup** Install the Arcserve Backup Server components on the system that is designated to function as a primary server or a stand-alone server. **Agent for Virtual Machines** Install the agent on the system that is designated to 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 can impose performance issues on the server, install the agent on a remote system and allow it to function as the backup proxy system. **Be aware of the following considerations:** When you have to back up virtual machines that reside on ReFS volumes, the backup proxy system should reside on a server that is running Windows Server 2012 or 2012 R2. This is specific to file mode backups. You can register the agent license on the Arcserve Backup server. The r17 release of the agent installs VDDK 6.0.1. If you want to use the version of VDDK that the agent installs, you do not need to install VDDK. When you perform raw (full VM) backups on VMware Windows VMs, the agent is not required to be installed on the VMs to provide file level restore. File level restore is automatically provided from raw backups. However, the agent is required to be installed when performing a restore. For more information, see Where to Install the Agent. **Note:** To take advantage of this feature, it is required to upgrade the server and the Agent for Virtual Machines to the Arcserve Backup r17 release.	**Arcserve Backup** Install the Arcserve Backup Server components on the system that is designated to function as a primary server or a stand-alone server. **Agent for Virtual Machines** Install the agent on the Hyper-V host system. **Note:** You must register the agent license on the Arcserve Backup server.

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

Task	VMware Systems	Hyper-V Systems
Configuration	Populate the 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 53) Deploy the Agent for Virtual Machines using Agent Deployment. For more information, see Deploy the Agent to VMs Using Agent Deployment (see page 32).	Populate the 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 58) Deploy the Agent for Virtual Machines using Agent Deployment. For more information, see Deploy the Agent to VMs Using Agent Deployment (see page 32).
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 should 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 65).	

Where to Install the Agent

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

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

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

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

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

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

Be aware of the following considerations:

- You must register one license for each VM that you are protecting with Arcserve Backup. All licenses must be registered on the primary server or stand-alone server.
- You can register an agent license for each virtual machine, hypervisor (host), or per-socket. The type of license that you can use in an environment depends on the number of virtual machines that are protected or the number of sockets per host.
- For Raw (full VM) backups, the agent is not required to be installed on the VMware virtual machines to provide file level restore. File level restore is automatically provided from raw backups. However, the agent is required to be installed when performing a restore. For more information, see Where to Install the Agent.

  Note: This feature is available when you upgrade to the Arcserve Backup r17 release.
- In r16.5, you can run incremental backup jobs for Mixed mode backups through VMware VDDK on the proxy server or through the agent that is installed on the virtual machine. When you upgrade to the Arcserve Backup r17 release; the agent is no longer required to be installed on the virtual machine; therefore the only option available to run an incremental backup job for Mixed mode backups is through VMware VDDK on the proxy server.

Installation Prerequisites

The agent requires the following prerequisite components.

- For VMware environments, verify that Microsoft .NET Framework Version 2 or higher is installed and running on the backup proxy system.
- This release of Arcserve Backup Agent for Virtual Machines.

Before installing the agent, complete the following prerequisite tasks:

- Verify that your system meets the minimum requirements needed to install the agent.

  For a list of requirements, see the Readme file.
- Verify that you have an Administrator profile or a profile with the rights to install software.
- Verify that you know the user name and password of the system where you are installing the agent.

Note: Windows 32-bit proxy is not supported for Agent for Virtual Machine backups.

Supported Configurations to Integrate with VMware vSphere

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

- Windows Server 2008 x64
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 r2

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 Arcserve Backup. The agent follows the standard installation procedure for Arcserve Backup system components, agents, and options.
- Install the agent after you install Arcserve Backup. Using Agent Deployment you can install the agent at any time after you install 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 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 35).

Deploy the Agent to VMs Using Agent Deployment

Arcserve Backup Agent Deployment lets you install and upgrade 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 Arcserve Backup environment are the same release number as the Arcserve Backup server.

Be aware of the considerations that follow:

- To install or upgrade an agent on a VM, the VM must be powered on.
- Agent Deployment installs or upgrades agents on all VMs that reside in the ESX/ESXi Server system and the Hyper-V host system.

To deploy Arcserve Backup agents to VMs using Virtual Machine deployment

1. Open the Arcserve Backup Manager Console.

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

   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 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 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 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 Arcserve Backup agents are deployed on the VMs.

Post Installation Tasks

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

This section contains the following topics:

VMware vSphere Integration Post Installation Tasks

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

1. Populate the Arcserve Backup database.
2. Specify a backup approach.
3. Modify the default VDDK communication port (see page 37).
4. (Optional) Configure concurrent read operations using VDDK (see page 38).
5. (Optional) Define the permissions for vCenter roles.

Populate the Arcserve Backup Database

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

For more information, see Populate the Database Using Arcserve VMware Configuration Tool.

Specify a Backup Approach

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

VMware vSphere Web Services SDK and VMware VDDK--Lets you protect the following implementations:

- ESX Server 3.5 and above when managed by vCenter Server 4.0 and above
- VMware Virtual Center 2.5 and above up to vCenter Server 5.1 managing ESX Server 3.5 and above up to ESX Server 5.1.

VMware vSphere Web Services SDK and VMware VDDK Approach

When using the VMware vSphere Web Services SDK and VMware VDDK approach, consider the following:

- With this approach specified, Arcserve Backup uses VDDK to process raw (full VM) backups and raw (full VM) backups with the Allow file level restore option specified when VDDK is installed on the backup proxy system. However, by default, the agent always uses VDDK for all backups and all versions of ESX Server.
- Arcserve Backup backs up only the active blocks relating to the full backup phase of raw (full VM) backups (with and without the allow file level restore option specified), and mixed mode backups with the allow file level restore option specified.

  If the virtual disks are provisioned as Lazy zeroed thick or thin disks, the agent creates backup sessions that are approximately the same size as the used disk space on the VM.

  Arcserve Backup does not support the active block analysis approach on virtual machines that contain virtual raw device mapping (RDM) disks. However, if Arcserve Backup detects virtual RDM disks, you can submit full backups of the virtual RDM disks and recover the disks as normal thick disks.

  Note: Although active block backup jobs complete successfully, one of the following messages can appear in the Activity Log after the jobs run:

  - AW0720:Failed to create the disk bitmap for the disk, "Full disk including unused blocks will be backed up".
  - AW0589:Failed to enable changed block tracking for the virtual machine, "Full disk including unused blocks will be backed up".

  To correct the condition that generated messages AW0720 and AW0589, reset changed block tracking. For more information, see Failed to Create Disk Bitmap Errors Occur During Backups.

Be aware of the following limitations:

- Due to a VMware limitation, the agent does not support backing up raw device mapping (RDM) in physical compatible mode.
- The first time you back up virtual machines using this approach (active block backup), verify there are no snapshots on the virtual machines. For all subsequent backups, there can be one or more snapshots on the VMs.
- Arcserve Backup performs active block backups on virtual machines running on VMware hardware version 7 or later and the following VMware platforms:
  - ESX Server 4.0 or later
  - vCenter Server 4.0 or later

- Backups store the snapshot in the mount directory specified using Arcserve VMware Configuration Tool.
- Arcserve Backup uses VDDK to recover data when the VM data is backed up using VDDK.

  Note: VMware converter is not required to restore virtual machine data that was backed up using VDDK.
- The backup process creates a file named vmconfig.dat in binary format that contains the VM configuration details.

  Note: You should not attempt to modify vmconfig.dat.
- The backup process does not create or update catalog files.
- The mount point directory does not display files for the mounted volume. This behavior occurs because VDDK does not mount volumes to a directory or map volumes to a drive letter.
- The backup process creates disk files with a zero file size in the mount directory for raw (full VM) backups and raw (full VM) backups with the Allow file level restore option specified.

  Note: You should not attempt to modify the disk files.

Modify the Default VDDK Communication Port

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

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

To modify the default VDDK communication port

1. From the Windows Start menu, click Run.

   The Run dialog opens.

2. In the Open field, type regedit.

   Windows Registry Editor opens.

3. Browse to the key that follows:

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

   The values for the key appear.

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

   The Edit DWORD Value dialog opens.

   Note: The default value of VDDKPort is 902.

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

   The key is modified.

5. Close Registry Editor.

Configure the Number of Concurrent Read Operations Using VDDK

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

Path

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

Key name

VmdkReaderCount

Default value

4 (Back up data using VDDK)

Max value

8

Define the Permissions for vCenter Roles

When you configure vCenter to manage virtual machines, under most circumstances you set up users or groups with vCenter administrator privileges. This approach helps to ensure that the vCenter accounts have unrestricted access to vCenter functionality and tasks. Optionally, you can create vCenter users and groups that can be used to facilitate only backup operations or only backup and restore operations.

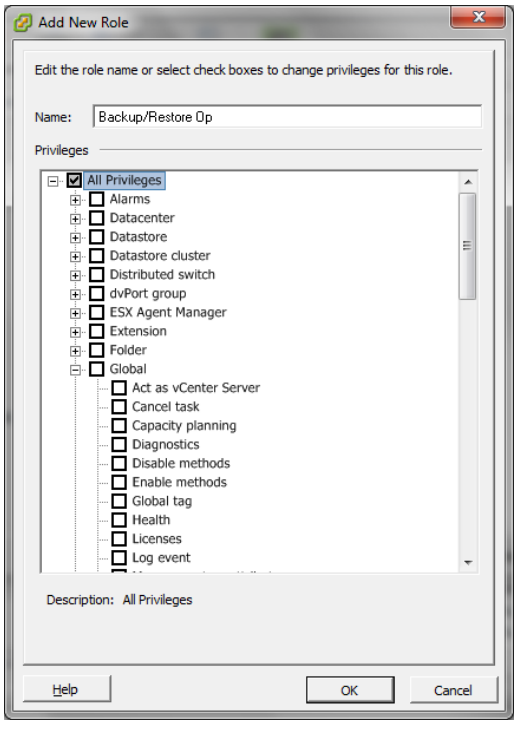
When using vCenter nonadministrative accounts to facilitate backup and restore operations, you create vCenter roles, assign privileges to the roles, and then apply the role to individual users or groups.

Note: As a best practice, VMware recommends that you allow nonadministrative vCenter user accounts to be members of the Windows local administrator group.

Important! The following steps assume that you are familiar with how to configure vCenter users, groups, roles, and permissions. Consult the vCenter documentation as needed.

Follow these steps:

1. Log in to vCenter using the VI Client.
2. Open the Add New Roles dialog and specify a name for the role.



3. Expand All privileges.

4. **(Optional)** To allow the role to **facilitate only backup operations**, specify the following privileges:

   Important! To allow the role to facilitate backup and restore operations, continue to the next step.

   - Expand Virtual machine and Configuration, and specify the following privileges:
     - Disk change tracking
     - Disk Lease
     - Add existing disk
     - Add new disk
     - Add or remove device
     - Change resource
     - Remove Disk
     - Settings
   - Expand Virtual machine and Provisioning, and specify the following privileges:
     - Allow read-only disk access
     - Allow virtual machine download
   - Expand Virtual machine and specify the following privileges:
     - **vSphere 4:** Expand State and specify Create Snapshot and Remove snapshot.
     - **vSphere 5:** Expand Snapshot management, expand State and then specify Create Snapshot and Remove snapshot.
   - Expand Global and specify the following privileges:
     - Disable methods
     - Enable methods
     - Licenses

   Go to Step 6.

5. To allow the role to **facilitate backup and restore operations**, specify the following privileges:
   - Expand Datastore and specify the following privileges:
     - Allocate space
     - Browse datastore
     - Low level file operations

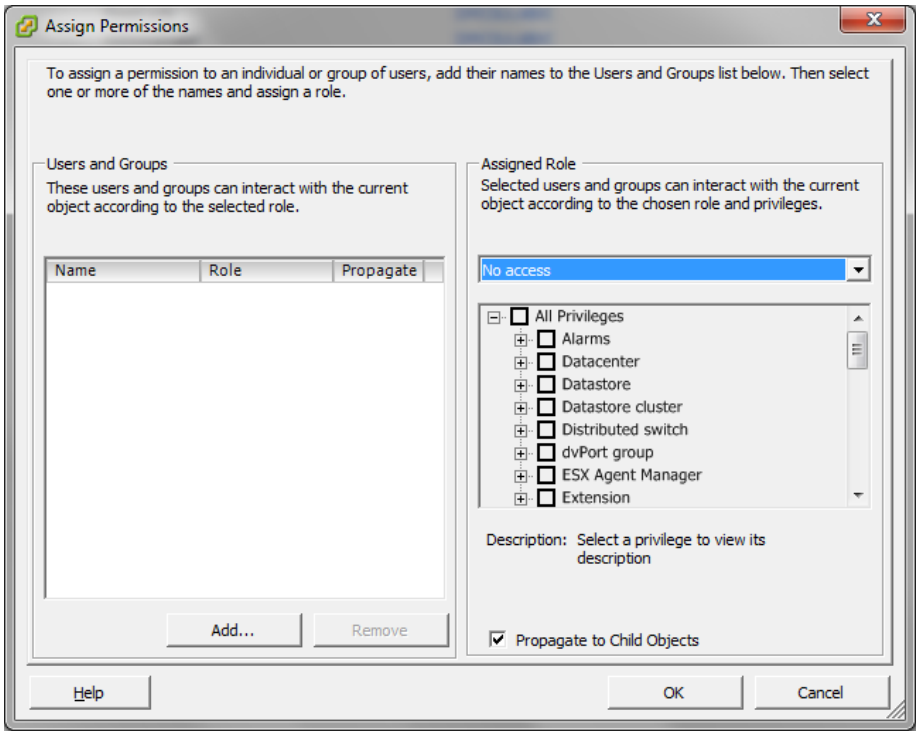
- Expand Global and specify the following privileges:
  - Disable methods
  - Enable methods
  - Licenses
- Expand Host, expand Local Operations, and then specify Reconfigure virtual machine.

  Note: This privilege is only required when you need to perform backup and restore operations using the Hotadd transport mode.
- Expand Network and specify Assign Network.
- Expand Resource and click Assign Virtual Machine to resource pool.
- Expand Virtual machine and Configuration, and specify the following privileges:
  - Add existing disk
  - Add new disk
  - Add or Remove device
  - Advanced
  - Change CPU count
  - Change resource
  - Disk change tracking
  - Disk Lease
  - Host USB device
  - Memory
  - Modify device setting
  - Raw device
  - Reload from path
  - Remove disk
  - Rename
  - Reset guest information
  - Settings
  - Swapfile placement
  - Upgrade virtual hardware

- Expand Virtual machine and Guest Operations, and specify the following privileges:
  - Guest Operation Modifications
  - Guest Operation Program Execution
  - Guest Operation Queries (vSphere 5)
- Expand Virtual Machine and Interaction, and specify the following privileges:
  - Power off
  - Power on
- Expand Virtual machine and Inventory, and specify the following privileges:
  - Create new
  - Register
  - Remove
  - Unregister
- Expand Virtual machine and Provisioning, and specify the following privileges:
  - Allow disk access
  - Allow read-only disk access
  - Allow virtual machine download
- Expand Virtual Machine and specify the following privileges:
  - **vSphere 4:** Expand State and specify Create snapshot, Remove snapshot, and Revert to snapshot.
  - **vSphere 5:** Expand Snapshot management, expand State, and then specify Create snapshot, Remove snapshot, and Revert to snapshot.
  - **vSphere 6**: Expand Snapshot management, expand State, and then specify Create snapshot, Remove snapshot, and Revert to snapshot.

6. Click OK to create the role.

7. Open the Assign Permissions dialog, to assign the newly created role to users, groups, or both.



8. From the Users and Groups list, select the custom user that you want to use for backups and restores.

   From the Assigned Role drop-down list, specify that role that you want to apply to the users or groups.

   Click OK to apply the role to the users or groups.

The permissions are now defined for vCenter roles.

Add or Remove Specific VM Data from the Arcserve Backup Database

Arcserve Backup provides you with command line arguments that let you add and remove specific VM data from the 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 Arcserve Backup database. The command line arguments are as follows:

-insertVM <vmname>
-deleteVM <vmname>

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

To add or remove VM data from the 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 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 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 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 Arcserve Backup database:

   ca_msvmpopulatedb.exe –Primary Arcserve1 –deleteVM VM-001 –debug 1

How to Use the VMware hotadd Transport Mode

The VMware hotadd Transport Mode is a mechanism that lets you transport data in a manner that is more efficient than the LAN transport mode. To use VMware hotadd Transport Mode in your environment, consider the following:

- The agent supports the VMware hotadd transport mode using VDDK on virtual machines that are running the following applications:
  - ESX Server 3.5 or later
  - vCenter Server 2.5 or later
- The backup proxy system must be configured on a virtual machine.

  The ESX Server system where the backup proxy virtual machine resides requires access to the data store of the virtual machine that you are backing up or recovering.

To configure the agent to back up and restore data using the hotadd transport mode with VDDK, complete the following tasks:

1. Install Arcserve Backup Client Agent for Windows and Arcserve Backup Agent for Virtual Machines inside the virtual machine.
2. Populate the Arcserve Backup database with information about the virtual machine using Arcserve VMware Configuration Tool.

Note: To configure the agent to use the hotadd transport mode on VDDK backup proxy systems, you do not need to add, remove, or modify registry keys.

Terminate Operations when the Agent Detects Expired SSL Certificates

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

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

To terminate operations when the agent detects expired SSL Certificates

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

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

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

   Set the key value of SSLCertificateVerify to 1.

3. Close Registry Editor.

Specify Custom HTTP/HTTPS Communication Ports

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

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

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

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

To specify custom HTTP/HTTPs communication ports

1. Log in to the backup proxy system.
2. Open Windows Registry Editor.
3. Create the following registry key:

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

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

   The Edit DWORD Value dialog opens.

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

   Click OK.

   The port number is applied.

5. Create the following resgistry key:

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

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

   The Edit DWORD Value dialog opens.

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

   Click OK.

   The port number is applied.

Configure the Agent to Retain MAC Addresses After Recovering VMs

The process of recovering virtual machines using the Recover VM recovery method may not let you retain the MAC addresses of the virtual machines (if a MAC address was defined) after the recovery process is complete. Arcserve Backup behaves in this manner in backup environments that use the VMware VDDK backup approach.

Note: The vSphere client application lets you verify whether the MAC address were retained after recovering virtual machines.

To configure the agent to retain MAC addresses after recovering VMs

1. Log in to the computer where the agent is installed and open Windows Registry Editor.
2. Browse to the following:

   HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve Backup\Client Agent\Parameters

3. Create the following key:

   Key Name:

   RetainMACForVDDK

   Specify one of the following values for the key:

   - **1**--Retain the MAC address
   - **0**--Do not retain the MAC address

4. Save the key and close Windows Registry Editor.

Configure the Agent to Retain Disk Resource Allocation After Recovering VMs

The process of recovering virtual machines using the Recover VM recovery method may not let you retain the disk resource allocation of the virtual machines. You can retain the disk resource allocation after recovering virtual machines only if you use the VMware VDDK backup approach in your backup environment.

To configure the agent to retain disk resource allocation after recovering VMs

1. Log in to the computer where the agent is installed and open Windows Registry Editor.
2. Browse to the following registry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve Backup\Client Agent\Parameters
3. Create the following key:

   Key Name:

   RetainDiskResourceForVDDK

   Specify one of the following DWORD values for the key:

   - **1--**Retain the disk resource allocation
   - **0--**Do not retain the disk resource allocation
4. Save the key and close Windows Registry Editor.

Enable Debugging for VDDK Jobs

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

To enable debugging for VDDK jobs

1. Log in to the backup proxy system.

   Open Windows Registry Editor.

   Open the following registry key:

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

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

   The Edit DWORD Value dialog opens.
2. In the Value field, specify 1.

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

Uninstall the Agent

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

To uninstall the agent

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

   Locate and select Arcserve Backup.

   Click Uninstall.

   The Arcserve Backup Remove Application, Components dialog opens.

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

   Click Next.

   The Arcserve Backup Remove Application, Messages dialog opens.

3. Click Next.

   The Arcserve Backup Remove Application, Remove dialog opens.

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

   The agent is uninstalled.

Chapter 3: Populating the Arcserve Backup Database

This section contains the following topics:

Specify the Name of the Arcserve Backup Server

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

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

Follow these steps:

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

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

   The Backup Agent Admin opens.

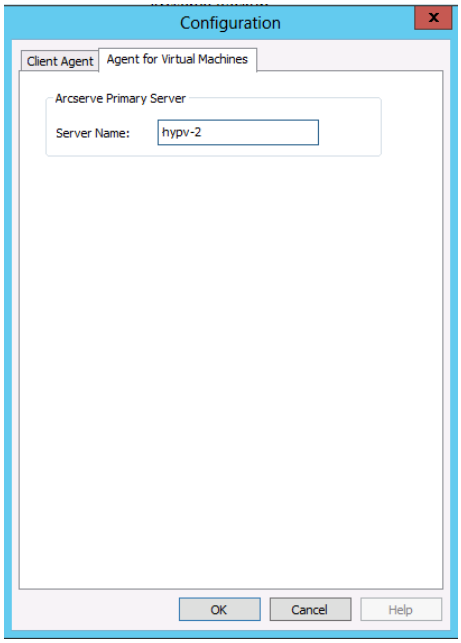
2. From the drop-down list, select Arcserve Backup Client Agent and click Configuration on the toolbar.

   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 Arcserve Backup server that will protect this VM.



   Click OK.

The name of the Arcserve Backup server is saved.

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

Specify a Temporary VM Mount Location

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

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

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

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

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

Be aware of the following:

- The Temporary VM Mount Location must reside on the backup proxy system.
- 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, Arcserve, Arcserve Backup, and click Backup Agent Admin.

   The Backup Agent Admin dialog opens.

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

   The Arcserve VMware Configuration Tool opens.

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

4. Click Set.

   The Temporary VM Mount Location is set.

5. Click Close.

   The Arcserve VMware Configuration Tool closes.

Populate the Database Using Arcserve VMware Configuration Tool

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

After you install the agent, you must populate the 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.

Note: Windows 32-bit proxy is not supported for Agent for Virtual Machine backups.

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

The configuration tool collects the following information:

- Names of the backup proxy systems
- VMware ESX Host names or VMware vCenter Server names
- VM Host names
- Volume names contained within the VMs on Windows systems

Be aware of the following behavior:

By default, the configuration tool populates the Arcserve database with information about all of the the virtual machines in your backup environment. However, when the configuration tool cannot identify the host name of virtual machines, the Arcserve Managers display UNKNOWNVM as the host name of the virtual machine. When you do not want to display UNKNOWNVM in the Managers, you can configure the tool to skip over unidentifiable virtual machines. To skip over the unidentifiable virtual machines, create a keyword named SkipPopulateUnknownVMs in the following registry key and define the value of the keyword as 1.

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

Follow these steps:

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

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

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

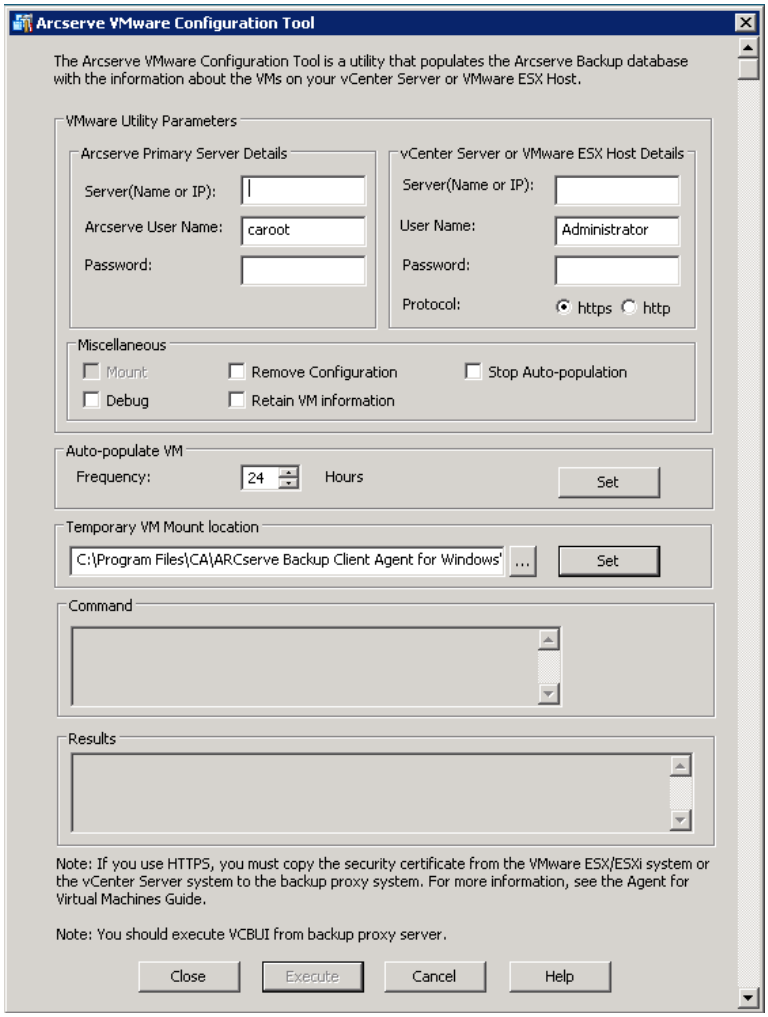
   To open the Backup Agent Admin, click Start, Programs, Arcserve, Arcserve Backup, and click Backup Agent Admin to open the Backup Agent Admin.

3. From the drop-down list, select Arcserve Backup Agent for Virtual Machines and click Configuration on the toolbar to open the Arcserve VMware Configuration Tool dialog.

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

- x64 systems

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



4. Complete the following fields on the Arcserve VMware Configuration Tool dialog:

   Arcserve Primary Server Details

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

   - **Server (Name or IP)--**Lets you specify the name or IP address of the Arcserve Backup primary server.
   - **Arcserve User Name--**Lets you specify the user name, with caroot privileges, for the Arcserve Backup primary server.
   - **Password--**Lets you specify the password for the Arcserve Backup User Name.

   vCenter Server or VMware ESX Host Details

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

   - **Server (Name or IP)--**Lets you specify the name of the VMware ESX Host system or the vCenter Server system.
   - **User Name--**Lets you specify the name of the VMware ESX Host user or the vCenter user with Administrator privileges.
   - **Password--**Lets you specify the password for the VMware ESX Host User Name or the vCenter Server User Name.
   - **Protocol--**Lets you specify the communication protocol between the backup proxy system and the VMware ESX Host system or the vCenter Server system.

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

   Miscellaneous

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

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

     Note: If you run the configuration tool with the Mount option enabled, the utility takes longer to run because it performs a mount and unmount operation of each running VM.
   - **Remove Configuration--**Lets you delete the VMs available in the database for the specified VMware ESX Host system or vCenter Server system for a specified backup proxy system.
   - **Debug--**Lets you write a detailed debug log. The log will be created in the Client Agent for Windows installation directory. By default, this directory is as follows:

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

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

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

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

  Consider the following best practices:

  - You should specify the Retain VM Information option in environments where the VMs will be in a powered off state when the populate operation executes. This approach helps ensure that Arcserve Backup backs up the VMs the next time the backup job runs.
  - You should not specify the Retain VM Information option in environments where the VMs migrate from one ESX Server or vCenter Server system to another to support load balancing operations. This approach helps ensure that backups of ESX Server and vCenter Server systems do not fail.

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

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

  - The Arcserve Backup database was populated with information about the ESX Server or vCenter Server systems, and you want to stop the Arcserve Backup database auto-population process.
  - An ESX Server or vCenter Server system was disabled. After the system was returned to service, the Arcserve Backup database was populated with information about the ESX Server or vCenter Server system. You now want to stop the Arcserve Backup database auto-population process.
  - A new ESX Server or vCenter Server system was installed in your backup environment. The Arcserve Backup database was populated with information about the ESX Server or vCenter Server system. You now want to stop the Arcserve Backup database auto-population process.

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

Auto-populate VM

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

Default: 24 hours

Range: 1 to 99 hours

Temporary VM Mount Location

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

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

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

Note: You must click Set to apply the location.

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

5. Click Execute.

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

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

Populate the Database Using Arcserve Hyper-V Configuration Tool

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

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

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

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

- Arcserve Hyper-V Configuration Tool populates the Arcserve Backup database with information about Hyper-V VMs that are in a powered on state when you execute the tool. The tool cannot populate the database with Hyper-V VM data when the VMs are in a powered off state.
- Arcserve Hyper-V Configuration Tool populates the 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, Arcserve Backup substitutes the host name of the VM with the VM name of the VM in the Arcserve Backup database.
- 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 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, 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 Arcserve Backup database.

To populate the database using Arcserve Hyper-V Configuration Tool

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

   Note: Arcserve Hyper-V Configuration Tool will not populate the Arcserve Backup database with information about Hyper-V VMs that are not in running state.

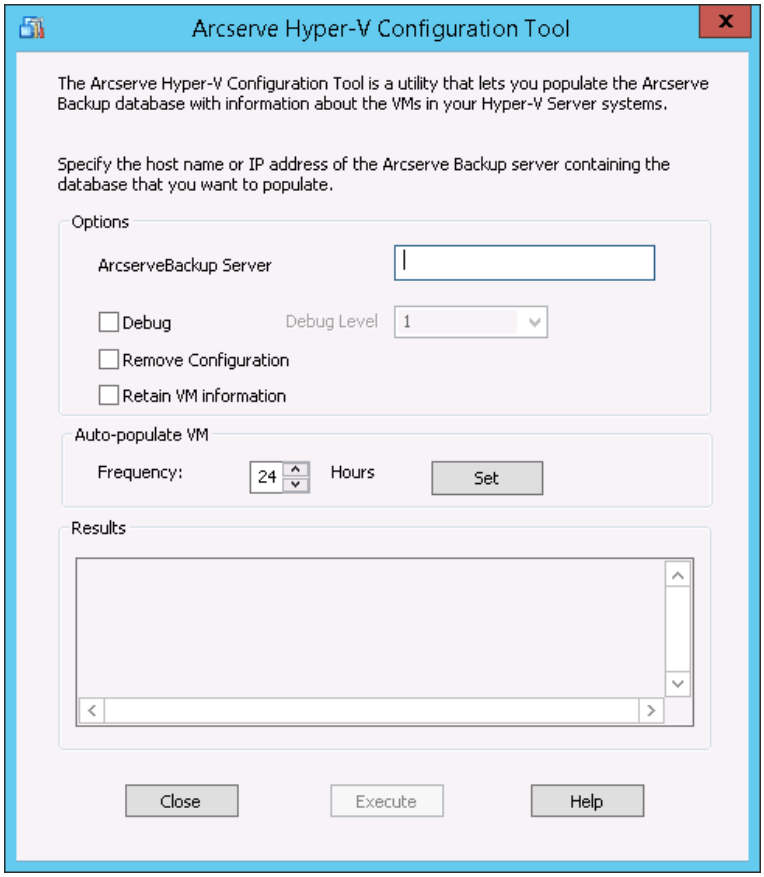
2. Log in to the Hyper-V host system and open the Backup Agent Admin.

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

   Backup Agent Admin opens.

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

   Arcserve Hyper-V Configuration Tool dialog opens.



4. Complete the following fields on the Arcserve Hyper-V Configuration Tool dialog:

   Options

   - **Arcserve Backup Server--**Lets you specify the host name or IP address of the 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 Arcserve Backup database for the specified Hyper-V server.
   - **Retain VM Information--**Lets you retain data (backup information) for VMs that are not available when you execute this tool.

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

     Consider the following best practices:

     - You should specify the Retain VM Information option in environments where the VMs will be in a powered off state when the populate operation executes. This approach helps ensure that Arcserve Backup backs up the VMs the next time the backup job runs.
     - You should not specify the Retain VM Information option in environments where the VMs migrate from one Hyper-V server to another to support load balancing operations. This approach helps ensure that backups Hyper-V servers do not fail.

Auto-populate the VM

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

  Default: 24 hours

  Range: 1 to 99 hours

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

5. Click Execute.

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

Populating the Arcserve Backup Database Using Command Line Utilities

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

- **ca_vcbpopulatedb--**Lets you populate the Arcserve Backup database with information about the VMware VMs in your backup environment.
- **ca_msvmpopulatedb--**Lets you populate the Arcserve Backup database with information about the Hyper-V VMs in your backup environment.

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

How Virtual Machine Names Affect Jobs

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. Arcserve Backup populates the 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 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.

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

2. You submit a scheduled backup job of VM1.

   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.

   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. 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.
- 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, 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 Arcserve Backup database. As a result, When the VM1 job runs, Arcserve Backup does not back up the correct VM.

Chapter 4: Backing Up Data

This section contains the following topics:

How to Browse Virtual Machine Backup Volumes

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

- Backup proxy systems
- VMware ESX/ESXi Server systems
- VMware vCenter Server systems
- Microsoft Hyper-V host systems

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

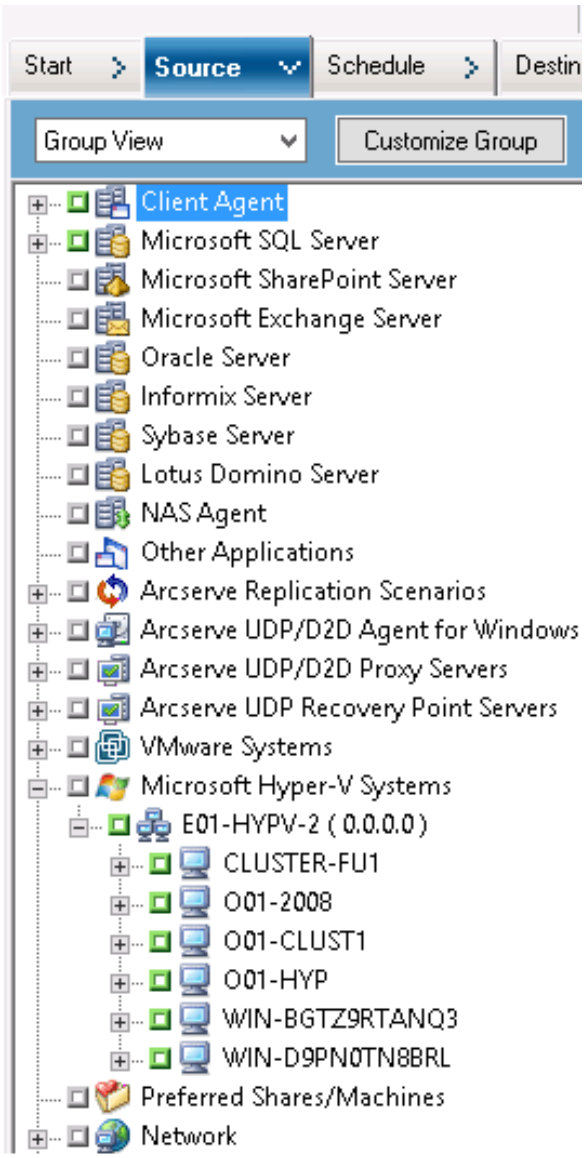
Be aware of the limitations that follow:

- You can browse the volumes in the VMware VMs when the VM is running a VMware-supported Windows-based operating system.
- You can browse the volumes in the Hyper-V VMs when you install the Agent for Virtual Machine in the Hyper-V VMs. With this configuration, you do not need to execute Arcserve Hyper-V Configuration Tool to browse the volumes in the Hyper-V VMs.
- From the Backup Manager window with the Source tab selected, the VMware Systems object can be expanded to display the names of the VMware Systems, the backup proxy systems, the ESX Server system or the vCenter Server system, and the VM volumes contained in the Windows operating system.
  At the VM level, you can browse in raw mode (full VM) or file mode.

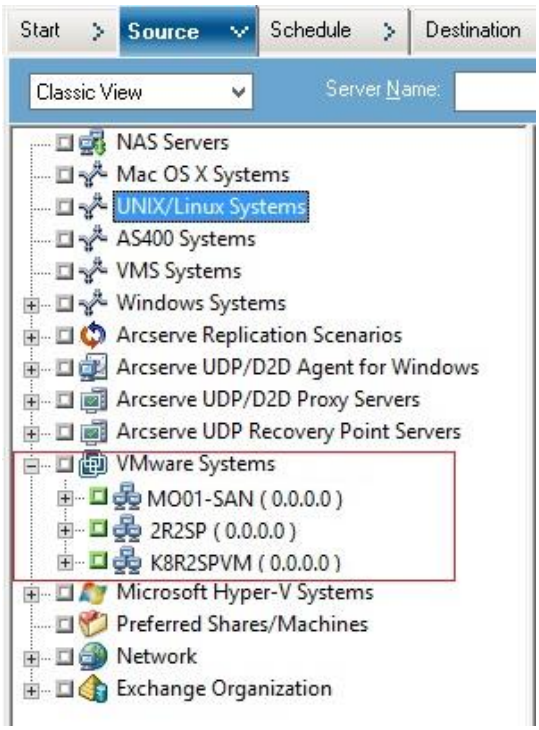
  To browse a VM at the file level, a VMware supported Windows operating system must be installed on the VM.

- The browsing modes are as follows:
  - Windows VMs--file mode and raw mode (full VM)
  - Non-Windows VMs--raw mode (full VM) only

The following screen illustrates browsing Hyper-V VMs:



The following screen illustrates browsing VMware VMs:



- When you submit a backup job, Arcserve Backup prompts you to provide the User name and password credentials for ESX Server system, the vCenter Server system, or the Hyper-V host system.

  Arcserve Backup validates the credentials at runtime.

Using Global and Local Backup Options

This section contains the following topics:

How Global and Local Backup Options Work

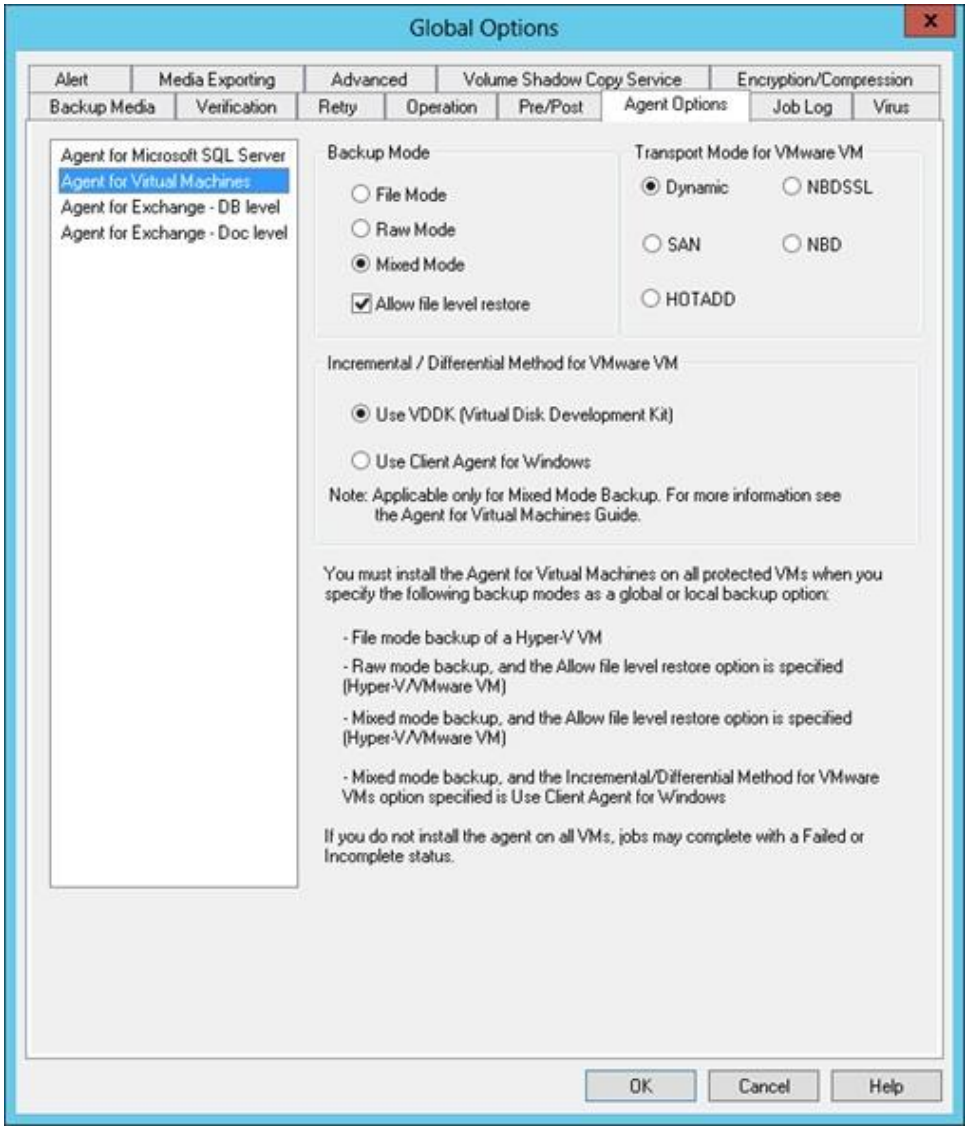
Backup options let you define how Arcserve Backup backs up data stored on VMs. Arcserve Backup lets you process backup data using the following backup options:

- **File mode--**Lets you back up data that resides on a VM as individual files and directories. File mode backup lets you restore VM backup data at file level granularity. By default, the agent always uses VDDK for all backups and all versions of ESX Server.
- **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 Arcserve Backup server on your VMs. For more information, see Specify the Name of the Arcserve Backup Server.

The following dialog 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 71).
- **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 74).

Note: When you specify backup modes at the global level and at the local level, 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 VDDK	Arcserve Backup processes the raw (full) VM backup data and the file mode backup data (incremental and differential backups) using VDDK. With mixed mode backups, by default, the agent processes raw (full) mode backups and file mode backups using VDDK.	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 VDDK global option does not affect backups on Hyper-V systems.

Examples: How to Apply Backup Options

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

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

Specify Backup Modes as a Global Backup Option

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

To specify backup modes as a global backup option

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

   The Source directory tree appears.

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

   Click Options on the Toolbar.

   The Options dialog opens.

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

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

   Backup Mode Options

   Lets you determine the backup method used for the backup.

   - **File Mode--**Lets you protect individual files and directories. File mode backup lets you perform the tasks that follow:
     - Back up files and directories at file level granularity contained in VM.
     - Perform full, incremental, and differential backups.
     - Restore data at file level granularity.
     - Process multiple streams of data simultaneously using the Multistreaming option.
     - Filter data using the Filter option.

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

- **Raw Mode--**Lets you protect entire systems for disaster recovery. Raw mode backup lets you perform the tasks that follow:
  - Perform full backups of full VM images only.
  - Process multiple streams of data simultaneously using the multistreaming option.

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

- **Mixed Mode--**Mixed mode is the default backup mode. Mixed mode lets you perform the tasks that follow:
  - Perform GFS and rotation backup jobs that consist of weekly full backups in full VM (raw) mode and daily incremental and differential backups in file mode in a single backup job.

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

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

  Allow file level restore lets you perform the tasks that follow:
  - Restore data at file level granularity from Raw Mode (full VM) backups.
  - Restore data at file level granularity from Mixed Mode backups.

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

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

Transport Mode for VMware VM Options

Lets you determine the transport method used for backup for VMware virtual machines.

- **Dynamic**--(*default*) This option lets VMware Virtual Disk Development Kit (VDDK) select the available transport mode.
- **SAN**--(Storage Area Network) This option lets you transfer backup data from proxy systems connected to the SAN to storage devices using Fibre Channel communication.
- **HOTADD**--This option lets you back up virtual machines configured with SCSI disks.
- **NBDSSL**--(Network Block Device Secure Sockets Layer) This option lets you use the Network File Copy (NFC) protocol to communicate. NBDSSL transfers encrypted data using TCP/IP communication networks.
- **NBD**--(Network Block Device, also referred to as LAN transport mode) This option lets you use the Network File Copy (NFC) protocol to communicate. Various VDDK and VCB operations use one connection for each virtual disk that it accesses on each ESX/ESXi Server host when using NBD.

Note: If the specified transport mode is not available, the transport mode defaults back to the Dynamic option.

Incremental / Differential Method for VMware VM

Lets you specify the communication method that Arcserve Backup will use to transfer incremental and differential backup data on VMware VMs to the backup proxy system.

- **Use VDDK--**Lets Arcserve Backup use VMware Virtual Disk Development Kit 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 VDDK is the default setting.

- **Use Client Agent for Windows--**Lets Arcserve Backup use Client Agent for Windows to execute the backup. With this option specified, 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.

Follow these steps:

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

   The Source directory tree appears.

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

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

   The Backup Mode dialog opens.

3. Click Override Global Backup Options. For more information see How Global and Local Backup Options Work.

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

   - **File Mode--**Lets you protect individual files and directories. File mode backup lets you perform the tasks that follow:
     - Back up files and directories at file level granularity contained in VM.
     - Perform full, incremental, and differential backups.
     - Restore data at file level granularity.
     - Process multiple streams of data simultaneously using the Multistreaming option.
     - Filter data using the Filter option.

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

   - **Raw Mode--**Lets you protect entire systems for disaster recovery. Raw mode backup lets you perform the tasks that follow:
     - Perform full backups of full VM images only.
     - Process multiple streams of data simultaneously using the multistreaming option.

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

- **Mixed Mode--**Mixed mode is the default backup mode. Mixed mode lets you perform the tasks that follow:
  - Perform GFS and rotation backup jobs that consist of weekly full backups in full VM (raw) mode and daily incremental and differential backups in file mode in a single backup job.

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

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

  Allow file level restore lets you perform the tasks that follow:
  - Restore data at file level granularity from Raw Mode (full VM) backups.
  - Restore data at file level granularity from Mixed Mode backups.

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

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

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

- **Dynamic**--(*default*) This option lets VMware Virtual Disk Development Kit (VDDK) select the available transport mode.
- **SAN**--(Storage Area Network) This option lets you transfer backup data from proxy systems connected to the SAN to storage devices using Fibre Channel communication.
- **HOTADD**--This option lets you back up virtual machines configured with SCSI disks.
- **NBDSSL**--(Network Block Device Secure Sockets Layer) This option lets you use the Network File Copy (NFC) protocol to communicate. NBDSSL transfers encrypted data using TCP/IP communication networks.
- **NBD**--(Network Block Device, also referred to as LAN transport mode) This option lets you use the Network File Copy (NFC) protocol to communicate. Various VDDK and VCB operations use one connection for each virtual disk that it accesses on each ESX/ESXi Server host when using NBD.

Note: If the specified transport mode is not available, the transport mode defaults back to the Dynamic option.

Click OK.

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

How the Agent Processes Incremental and Differential Backups on VMware Virtual Machines

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

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

  The agent communicates with the VM using VDDK. 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.

Back Up Data Residing on VMware Virtual Machines

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

Follow these steps:

1. Open the Backup Manager and select the Source tab to open the Backup Manager source directory tree.
2. Expand the VMware Systems object to display the backup proxy systems, VMware ESX Host systems, vCenter Server systems, and VMs in your environment.
3. Click the check box next to the objects that you want to back up. You can select volumes, an entire node, or any combination thereof as the source.

   Note: For information about browsing volumes, see How to Browse Virtual Machine Backup Volumes.
4. Specify a Backup Mode for the job.

   Note: For more information about backup modes, see How Global and Local Backup Options Work.
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 82).

   Important! If the Backup Mode specified is Raw Mode and you specify filters, 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*.

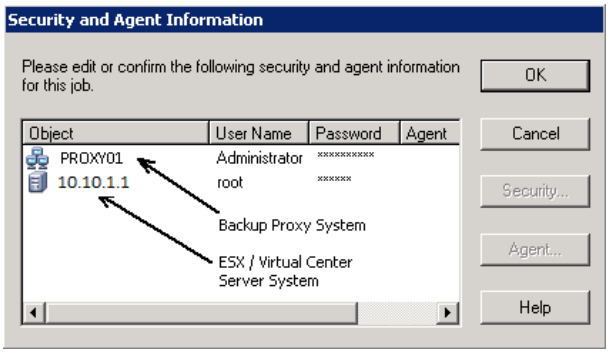
   To use multistreaming to transmit backup data, click the Multi Stream check box.
7. To specify the scheduling options for the job, click the Schedule tab.

   Note: For more information about job scheduling options, see the *Administration Guide*.
8. To specify global filters, click Filter on the toolbar to open the Filter dialog.

   Note: For more information about filtering VM data, see Filter VM Backup Data (see page 82). For more information about specifying filters, click the Help button on the Filter dialog.

9. Click Submit on the toolbar to submit the job to open the Security and Agent Information dialog.

   You must provide credentials for the VMware ESX Host system or the vCenter Server system and the backup proxy system to submit the job.



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

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

    Note: 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.

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

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

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

    Arcserve Backup submits the job. For more information about viewing job status and other job-related tasks, see the *Administration Guide*.

How the Agent Names Mount Points

Arcserve Backup uses the following different naming conventions for mount points:

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

  _ARCSERVE_BACKUP__J<JobID>_S<SessionID>_date_time

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

Back Up Data Residing on Hyper-V Virtual Machines

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

Be aware of the following behavior:

- When backing up data, the agent skips the pass-through disks that are attached to the virtual machine.
- When restoring the data, the agent cannot recover the data that was skipped during the backup.

Note: For information about the limitations of backing up data, see Backup and Restore Limitations on Virtual Machines.

To back up data residing on Hyper-V VMs

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

   The Backup Manager source directory tree displays.

2. Expand the Microsoft Hyper-V Systems object.

   The Hyper-V systems in your environment appear.

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

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

4. Specify a Backup Mode for the job.

   Note: For more information about backup modes, see How Global and Local Backup Options Work.

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 82).

   Important! If the Backup Mode specified is Raw Mode and you specify filters, 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.*

   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*.

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

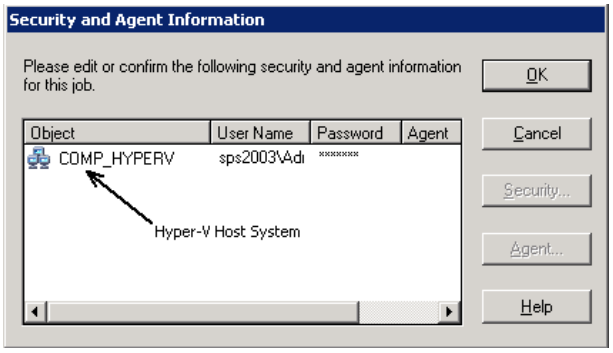
   The Filter dialog opens.

   Note: For more information about filtering VM data, see Filter VM Backup Data (see page 82). For more information about specifying filters, click the Help button on the Filter dialog.

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

   The Security and Agent Information dialog opens.

   You must provide credentials for the Hyper-V host system to submit the job.



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: 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.

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

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

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

    Arcserve Backup submits the job. For more information about viewing job status and other job-related tasks, see the *Administration Guide*.

Miscellaneous Tasks

This section contains the following topics:

How the Agent Supports the Preflight Check Utility

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

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

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

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

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

  The following message displays:

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

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

  The following message displays:

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

Filter VM Backup Data

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

- Back up only the data on the VMs based on, for example, file pattern, date range, date modified, file size, and so on.
- Selectively back up files, folders, or both in a selected volume.
- Apply filtering criteria globally or locally to your backup jobs.

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

To filter VM backup data

1. Open the Backup Manager window and browse to the VM that you want to filter.
2. Do one of the following actions:
   - To apply global filters to the backup operation, click the Filter toolbar button on the Backup Manager window.
   - To apply local filters to the backup operation, right-click the VM object and select Filter from the pop-up menu

   The Filter dialog opens.
3. Specify the filters required to complete the backup job.

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

Agent Log Files

Arcserve Backup includes log files that provide you with details about backup operations executed using the Agent for Virtual Machines. 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:

recovervm.log

Lets you view information about Recover VM recovery operations.

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, 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, 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 53)and Arcserve Hyper-V Configuration Tool (see page 58).

How the Agent Protects Volumes Mounted from Virtual Hard Disks

This section contains the following topics:

Overview of Virtual Hard Disks

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

Arcserve Backup protects the volumes mounted in VHDs or VHDXs.

Limitations of Protecting Volumes Mounted from Virtual Hard Disks

Consider the following limitations when backing up VHD and VHDX volumes:

- Arcserve Backup lets you restore individual VHD files (using the Restore by Session or Restore by Tree restore methods) and mount those VHD files that were backed up using the Raw (full VM) backup mode **only** when the Allow file level restore option **was not specified**. To recover and mount VHD files that were backed up using the Raw (full VM) backup mode **and** the Allow file level restore option **was specified**, use the Recover VM restore method. After the virtual machine is recovered, you can mount the VHD files of the recovered virtual machine.
- Arcserve Backup does not support using VSS to back up nested VHD or VHDX volumes that contain more than one level of data.

  Consider the following example:

  - Disk 0 contains drive C:\.
  - Drive C:\ contains mounted volume drive V:\.
  - Drive V:\ contains mounted volume drive W:\.

  Arcserve Backup cannot detect the .vhd or .vhdx file that resides in drive V:\.

  Note: To protect data files that reside in drive W:\, submit the backup using the Client Agent for Windows in conjunction with the Agent for Open Files.
- Arcserve Backup creates separate backup sessions for mounted volumes that contain VHD or VHDX files.

  Note: This behavior applies to backups that were submitted using the Client Agent for Windows in conjunction with the Agent for Open Files.

  Consider the following example:

  - A server contains physical disk (C:\) that contains VHDs or VHDXs D:\ and E:\. VHD or VHDX files (D.vhd or D.vhdx and E.vhd or E.vhdx) that reside in C:\ are mounted as drive D:\, and drive E:\. Drive D:\ is mounted to C:\MountD, and drive E:\ is mounted to C:\MountE.
  - When you back up C:\MountD and specify the Traverse Directory Junctions and Volume Mount Points option, Arcserve Backup creates separate backup sessions for drive D:\ and C:\MountD.
  - When you back up C:\MountE and specify the Traverse Directory Junctions and Volume Mount Points option and the Backup Mount Points as Part of the volume that they are mounted on option, Arcserve Backup creates separate backup sessions for drive E:\ and C:\MountE.

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

    - Traverse Directory Junctions and Volume Mount Points
    - Backup Mount Points as Part of the volume that they are mounted on

How the Agent Protects Cluster Shared Volumes

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

With the agent, you can protect CSVs residing in Hyper-V configured systems using Microsoft Volume Shadow Copy Service (VSS) technology. VSS is a component contained within Windows operating systems that lets you create point-in-time snapshots of data called shadow copies. For more information, see the *Administration Guide*, the *Microsoft Volume Shadow Copy Service Guide*, or both, which you can access from the Arcserve Backup Bookshelf.

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

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

How to Protect Virtual Machines that Reside on Cluster Shared Volumes

To back up the data that resides in the virtual machines, complete the following tasks:

1. Install the agent on the Hyper-V node.
2. Run Arcserve Hyper-V Configuration Tool on the Hyper-V clustered nodes to add the nodes to the Backup Manager.

   Note: For more information, see Populate the Database Using Arcserve Hyper-V Configuration Tool (see page 58).
3. Use the Backup Manager to select the virtual machines and submit the backups.

   Note: The process of backing up virtual machines is identical to that of backing up files, folders, directories, and so on.

To back up data that resides in the virtual machines on clustered shared volumes, with support for live migration, complete the following tasks:

1. Install the agent on the Hyper-V node.
2. Run Arcserve Hyper-V Configuration Tool on each of the Hyper-V clustered nodes to add the virtual machines running in the cluster to the Backup Manager.

   Note: For more information, see Populate the Database Using Arcserve Hyper-V Configuration Tool (see page 58).
3. Select all of the cluster nodes containing the virtual machines that you want to protect. (This step lets you back up all of the virtual machines that are contained within the nodes.)

   Note: When Live Migration operations for virtual machines occur, the agent backs up the virtual machine using the new host that is hosting the virtual machine.

Chapter 5: Restoring Data

This section contains the following topics:

Restore VMware Virtual Machine Data

This section contains the following topics:

How to Browse VMware Sessions

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

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

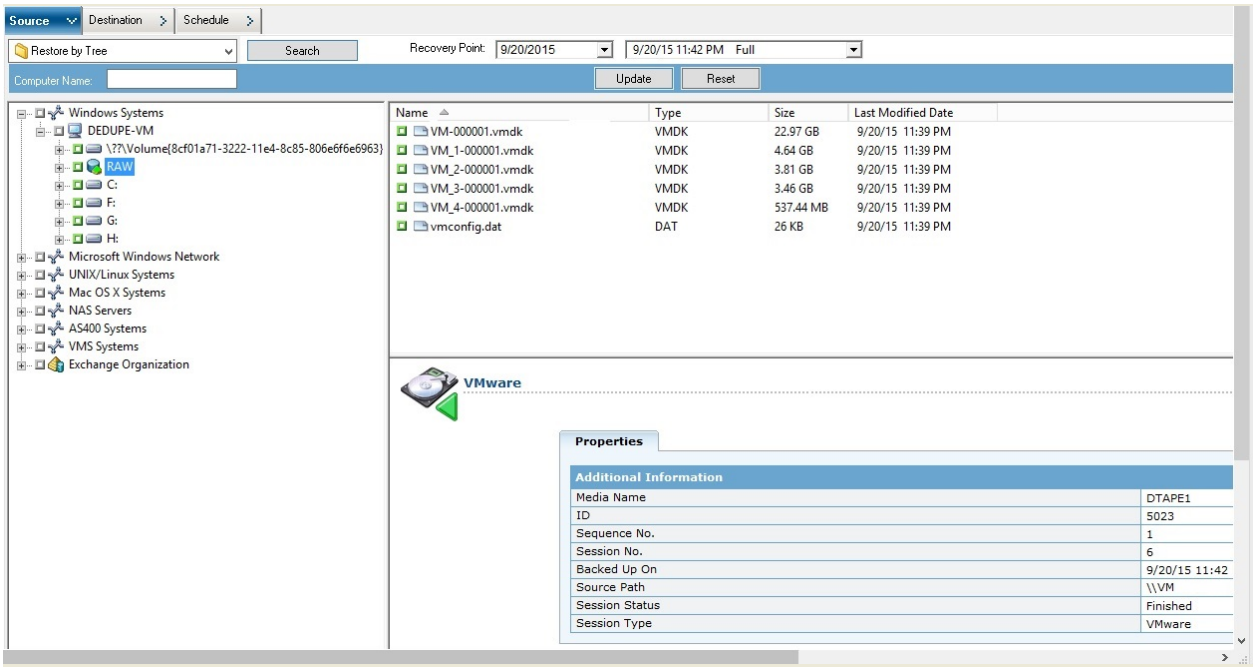
However, restoring data from a VM presents the following limitations:

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

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

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

When you select the Restore by Tree option on the Source tab in the Restore Manager, the VM backups performed in raw (full VM) mode display as VMware Raw Image. When you perform file mode backups, the corresponding volumes in the VM display.



The session properties section of the Restore Manager window displays the following information about the VMware backup data:

- **VMware Proxy--**Indicates the name of the backup proxy system that was used to back up this VM.
- **VMware vCenter Server/VMware ESX Host--**Indicates the name of the VMware ESX Host system or the vCenter Server system from which the VM was running when the backup job was submitted.
- **Host Name--**Indicates the host name of the VM involved with the backup job.
- **Session Method--**Indicates the type of backup method that was used to back up the VM (for example, Raw and File).

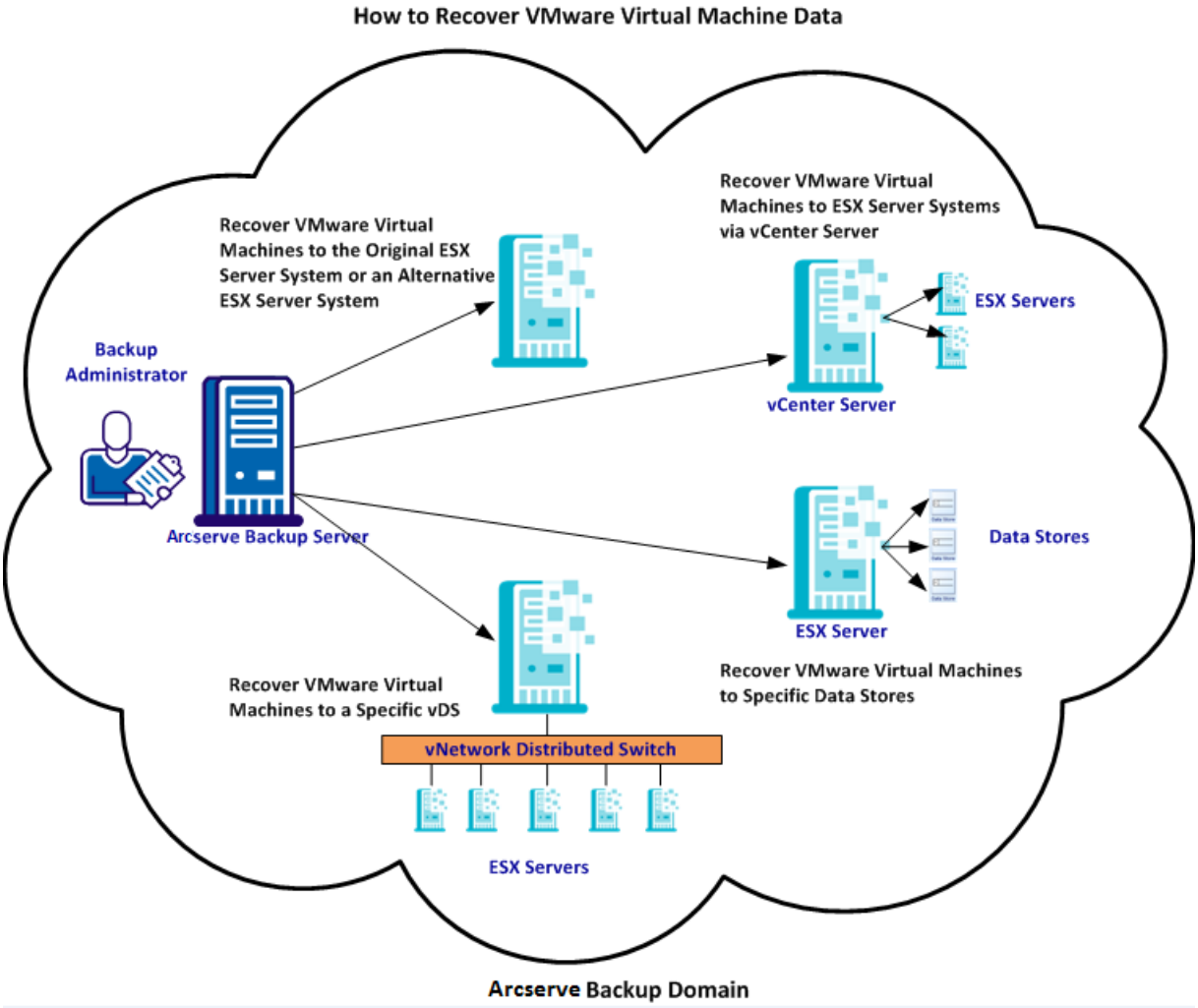
Limitations of Recovering Data

The following considerations apply to VDDK backups:

- VMware Converter cannot be used to recover backup data.
- ESX Server 3.5 and ESX Server 4.0 can be used to recover VM data that was backed up using ESX Server 3.5.
- ESX Server 3.5 cannot be used to recover VM data that was backed up using ESX Server 4.0.
- The recovery process does not require free disk space on the backup proxy system.

How to Recover VMware Virtual Machine Data

The agent lets you recover VMware virtual machine data using the methods described in the following illustration:



The following table describes the methods that you can use to recover VMware virtual machine data:

Method	When to Use
Recover VMware Virtual Machines to the Original ESX Server System or an Alternative ESX Server System	Use this method to recover virtual machines to the original or an alternative ESX Server system.

Method	When to Use
Recover VMware Virtual Machines to ESX Servers via vCenter Server Systems	Use this method to recover virtual machines that are connected to an ESX Server system using vCenter Server to facilitate the recovery operation.
Recover VMware Virtual Machines to Specific Data Stores	Use this method to recover the VMDK files to multiple data stores that exist on the destination ESX Server system.
Recover VMware Virtual Machines to a Specific vDS	Use this method to recover virtual machines that are connected to source machines through vNetwork Distributed Switches (vDS).

Recover VMware Virtual Machines to the Original ESX Server System or an Alternative ESX Server System

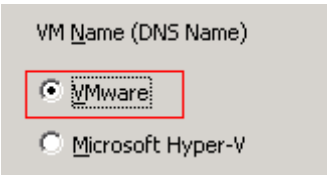
The agent lets you recover VMware virtual machines to the original ESX Server system or an alternative ESX Server system. The recovery process lets you restore the entire virtual machine and its data. Using this process, you can recover virtual machines from a disaster and can clone virtual machines.

With this recovery method, you recover virtual machines to the original ESX Server or vCenter Server from which the backup was taken. This method also lets you recover virtual machine VDDK files to multiple data stores that were not present in the source data.

Follow these steps:

1. Open the Restore Manager, click the Source tab, and select Recover Virtual Machine from the drop-down list to open the Recover Virtual Machine screen.

2. Click the VMware option on the Recover Virtual Machine screen as illustrated by the following screen:



The Transport Mode for VMware VM dialog appears.

Select one of the following transport methods to use for backup:

- **Dynamic**--(*default*) This option lets VMware Virtual Disk Development Kit (VDDK) select the available transport mode.
- **SAN**--(Storage Area Network) This option lets you transfer backup data from proxy systems connected to the SAN to storage devices using Fibre Channel communication.
- **HOTADD**--This option lets you back up virtual machines configured with SCSI disks.
- **NBDSSL**--(Network Block Device Secure Sockets Layer) This option lets you use the Network File Copy (NFC) protocol to communicate. NBDSSL transfers encrypted data using TCP/IP communication networks.
- **NBD**--(Network Block Device, also referred to as LAN transport mode) This option lets you use the Network File Copy (NFC) protocol to communicate. Various VDDK operations use one connection for each virtual disk that it accesses on each ESX/ESXi Server host when using NBD.

Note: If the specified transport mode is not available, the transport mode defaults back to the Dynamic option.

3. To search for virtual machines, use one of the following search methods and continue to the next step:

- **Search for a specific virtual machine**
- **Search all virtual machines**

  Note: Select << ANY >> in the VM Name (DNS Name) field and click Query.

- **Search using wildcard characters**

  Note: Replace the unknown characters of the virtual machine name with an asterisk in the VM Name (DNS Name) field, and click Query. For example, using 100-* returns the names of all virtual machines that start with 100-, such as 100-1, 100-01, and 100-001.

4. In the VM Name (DNS Name) column, click the check box next to the virtual machines that you want to recover. Then, specify the values that you require for each virtual machine that you selected in the following columns:
   - **Backup Versions--**Click the ellipsis to search for multiple versions of the backup data.
   - **Proxy Machine--**Click the ellipsis to search for and specify a backup proxy system.
   - **Path--**You can accept the displayed path or click in the Path field to specify an alternate path for the temporary VM mount directory.
   - **VM Destination--**Click in the VM Destination field and then click the ellipsis to open the Destination dialog.
5. From the vCenter/ESX drop-down list on the Destination dialog, select the ESX Server system where you want to recover the virtual machines.

   Specify the User Name and Password that is required to log in to the ESX Server system and click Connect.

   The agent enumerates the data stores on the specified ESX Server system. From here, you can specify one virtual machine data store as the destination. Additionally, you can specify a data store for each virtual machine.

   Note: If you want to recover virtual machine data to specific data stores, follow the steps described in Recover VMware Virtual Machines to Specific Data Stores.
6. Click OK to apply the destination.

   Note: Repeat Steps 4, 5, and 6 for each virtual machine that you are recovering in this job.
7. Click the Schedule tab and specify the schedule that you require for the job.

   Note: For more information about scheduling jobs, see the *Administration Guide*.
8. Click Options on the toolbar to open the Global Options dialog.

9. Click the Operation tab and specify the following options:

   Power on VMware or Hyper-V VM after restore

   Default value: Enabled.

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

   Overwrite VMware VM, if it exists

   When you restore VMware virtual machines, the agent detects the virtual machines that reside in the host system. If the virtual machine exists in the host system, this option lets you overwrite the virtual machine using the existing UUID and host name of the virtual machine.

   Default value: Enabled.

   Note: For troubleshooting information, see The Agent Does Not Delete Existing VMs after a Recover VM Job Completes (see page 118).

10. Click OK to apply the options.
11. Click Submit to submit the restore job.
12. Complete the required fields on the Submit Job dialog and then click OK.

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

Recover VMware Virtual Machines to ESX Servers via vCenter Server Systems

The recovery process lets you use vCenter Server to recover VMware virtual machines to ESX Server systems via vCenter Server systems. Using vCenter Server systems to facilitate recovery operations of this type lets you do the following:

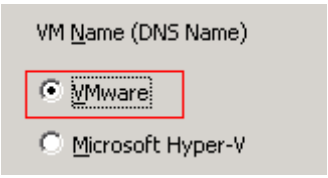
- Simplify the process of managing ESX Server recoveries. You can manage all recovery operations using one vCenter Server system.
- Eliminate the need to provide ESX Server login credentials for the disks that you are recovering.
- Reduce the workload on ESX Server systems.

Use this method to move entire virtual machines and their data to alternative ESX Server or vCenter Servers systems or when you want to clone virtual machines.

Follow these steps:

1. Open the Restore Manager, click the Source tab, and select Recover Virtual Machine from the drop-down list to open the Recover Virtual Machine screen.

2. Click the VMware option on the Recover Virtual Machine screen as illustrated by the following:



The Transport Mode for VMware VM dialog appears.

Select one of the following transport methods to use for backup:

- **Dynamic**--(*default*) This option lets VMware Virtual Disk Development Kit (VDDK) select the available transport mode.
- **SAN**--(Storage Area Network) This option lets you transfer backup data from proxy systems connected to the SAN to storage devices using Fibre Channel communication.
- **HOTADD**--This option lets you back up virtual machines configured with SCSI disks.
- **NBDSSL**--(Network Block Device Secure Sockets Layer) This option lets you use the Network File Copy (NFC) protocol to communicate. NBDSSL transfers encrypted data using TCP/IP communication networks.
- **NBD**--(Network Block Device, also referred to as LAN transport mode) This option lets you use the Network File Copy (NFC) protocol to communicate. Various VDDK operations use one connection for each virtual disk that it accesses on each ESX/ESXi Server host when using NBD.

Note: If the specified transport mode is not available, the transport mode defaults back to the Dynamic option.

3. To search for virtual machines, use one of the following search methods and continue to the next step:

- **Search for a specific virtual machine**
- **Search all virtual machines**

  Note: Select << ANY >> in the VM Name (DNS Name) field and click Query.

- **Search using wildcard characters**

  Note: Replace the unknown characters of the virtual machine name with an asterisk in the VM Name (DNS Name) field, and click Query. For example, using 100-* returns the names of all virtual machines that start with 100-, such as 100-1, 100-01, and 100-001.

4. In the VM Name (DNS Name) column, click the check box next to the virtual machines that you want to recover. Then, specify the values that you require for each virtual machine that you selected in the following columns:

   - **Backup Versions--**Click the ellipsis to search for multiple versions of the backup data.
   - **Proxy Machine--**Click the ellipsis to search for and specify a backup proxy system.
   - **Path--**You can accept the displayed path or click in the Path field to specify an alternate path for the temporary VM mount directory.

     VM Destination--Click in the VM Destination field and then click the ellipsis to open the Destination dialog.

     Click in the VM Destination field and then click the ellipsis to open the Destination dialog.

5. From the vCenter/ESX drop-down list on the Destination dialog, select the vCenter Server system where you want to recover the virtual machines.

   Specify the User Name and Password that is required to log in to the vCenter Server or ESX Server system. Then do the following:

   a. Click Connect.

      The agent enumerates all of the ESX Server systems that are associated with the vCenter Server system that you specified in the drop-down list.

   b. From the ESX Server drop-down list, specify the ESX Server system where you want to recover the virtual machines.

      When you specify an ESX Server system, the agent enumerates the data stores on the specified ESX Server system. Then you can specify the data store that you want to use as the destination for the recovery.

   Note: If you want to recover virtual machine data to specific data stores, follow the steps described in Recover VMware Virtual Machines to Specific Data Stores.

6. Click OK.

   The Destination dialog closes and the agent populates the VM Destination field with the location to recover the data.

   Note: Repeat Steps 4, 5 and 6 for each virtual machine that you want to recover in this job.

7. Click the Schedule tab and specify the schedule that you require for the job.

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

8. Click Options on the toolbar to open the Global Options dialog.

9. Click the Operation tab and specify the following:

   Power on VMware or Hyper-V VM after restore

   Default value: Enabled.

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

   Overwrite VMware VM, if it exists

   When you restore a VMware virtual machine, the agent detects the virtual machines that reside in the host system. If the virtual machine exists in the host system, this option lets you overwrite the virtual machine using the existing UUID and host name for the virtual machine.

   Default value: Enabled.

   Note: For troubleshooting information, see The Agent Does Not Delete Existing VMs after a Recover VM Job Completes (see page 118).

10. Click OK to apply the options.
11. Click Submit to submit the restore job.
12. Complete the required fields on the Submit Job dialog and then click OK.

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

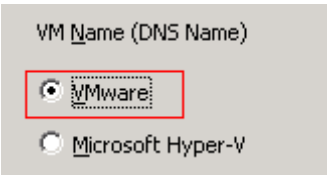
Recover VMware Virtual Machines to Specific Data Stores

The agent lets you recover the virtual machines to any data store that resides on the destination vCenter Server or ESX Server system. For example, a single data store does not contain sufficient free disk space to recover all of the VMDK files. The recovery process lets you specify an alternative data store that contains sufficient free disk space to recover all of the VMDK files.

Follow these steps:

1. Open the Restore Manager, click the Source tab, and select Recover Virtual Machine from the drop-down list to open the Recover Virtual Machine screen.

2. Click the VMware option on the Recover Virtual Machine screen as illustrated by the following screen:



The Transport Mode for VMware VM dialog appears.

Select one of the following transport methods to use for backup:

- **Dynamic**--(*default*) This option lets VMware Virtual Disk Development Kit (VDDK) select the available transport mode.
- **SAN**--(Storage Area Network) This option lets you transfer backup data from proxy systems connected to the SAN to storage devices using Fibre Channel communication.
- **HOTADD**--This option lets you back up virtual machines configured with SCSI disks.
- **NBDSSL**--(Network Block Device Secure Sockets Layer) This option lets you use the Network File Copy (NFC) protocol to communicate. NBDSSL transfers encrypted data using TCP/IP communication networks.
- **NBD**--(Network Block Device, also referred to as LAN transport mode) This option lets you use the Network File Copy (NFC) protocol to communicate. Various VDDK operations use one connection for each virtual disk that it accesses on each ESX/ESXi Server host when using NBD.

Note: If the specified transport mode is not available, the transport mode defaults back to the Dynamic option.

3. To search for virtual machines, use one of the following search methods and continue to the next step:

- **Search for a specific virtual machine**
- **Search all virtual machines**

  Note: Select << ANY >> in the VM Name (DNS Name) field and click Query.

- **Search using wildcard characters**

  Note: Replace the unknown characters of the virtual machine name with an asterisk in the VM Name (DNS Name) field, and click Query. For example, using 100-* returns the names of all virtual machines that start with 100-, such as 100-1, 100-01, and 100-001.

4. In the VM Name (DNS Name) column, click the check box next to the virtual machines that you want to recover. Then, specify the values that you require for each virtual machine that you selected in the following columns:

   - **Backup Versions--**Click the ellipsis to search for multiple versions of the backup data.
   - **Proxy Machine--**Click the ellipsis to search for and specify a backup proxy system.
   - **Path--**You can accept the displayed path or click in the Path field to specify an alternate path for the temporary VM mount directory.
   - **VM Destination--**Click in the VM Destination field and then click the ellipsis to open the Destination dialog.

5. From the vCenter/ESX drop-down list on the Destination dialog, select the ESX Server system or vCenter Server system where you want to recover the virtual machines.

   Specify the User Name and Password that is required to log in to the vCenter Server or ESX Server system and click Connect.

   The agent connects to the specified system based on the following scenarios:

   - When you specify vCenter Server systems in the vCenter/ESX drop-down list, the agent connects to the specified vCenter Server system and enumerates the available ESX Server systems in the ESX Server drop-down list. You can then specify the required ESX Server system and select a destination data store from the VM Data Store drop-down list.
   - When you specify ESX Server systems in the vCenter/ESX drop-down list, the agent connects to the specified ESX Server system and enumerates the available data stores for the specified ESX Server system. You can then specify the required destination data store from the VM Data Store drop-down list. In this scenario, you cannot click the ESX Server drop-down list to specify a different ESX Server system.

6. Complete the following fields on the Destination dialog:

   ESX Server

   Specify the host name or IP address of the ESX Server system where you want to recover the virtual machines.

   Note: When the system specified in the vCenter/ESX drop-down list is an ESX Server system, you cannot click the ESX Server drop-down list.

   VM Data Store

   Specify the name of the data store where you want to recover the virtual machine configuration files.

7. For each VMDK file listed in the Disk Data Store table, specify the data store where you want to store the VMDK file. To do this, click in the VMDK Data store drop-down list and click the required data store.

   Click OK.

   The Destination dialog closes and the agent populates the VM Destination field with the location to recover the data.

   Note: Repeat Steps 4 through 7 for each virtual machine that you are recovering in this job.

8. Click the Schedule tab and specify the schedule that you require for the job.

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

9. Click Options on the toolbar to open the Global Options dialog.

10. Click the Operation tab and specify the following options:

    Power on VMware or Hyper-V VM after restore

    Default value: Enabled.

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

    Overwrite VMware VM, if it exists

    When you restore VMware virtual machines, the agent detects the virtual machines that reside in the host system. If the virtual machine exists in the host system, this option lets you overwrite the virtual machine using the existing UUID and host name for the virtual machine.

    Default value: Enabled.

    Note: For troubleshooting information, see The Agent Does Not Delete Existing VMs after a Recover VM Job Completes (see page 118).

11. Click OK to apply the options.

12. Click Submit to submit the restore job.

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

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

After the job completes, the agent recovers the VMDK files to the data stores specified on the Destination dialog.

Recover VMware Virtual Machines to a Specific vDS

The recovery process lets you recover virtual machines that are connected to source machines to vNetwork Distributed Switches (vDS). Using the Recover VM screen, you can browse vDS network device information. For example, you can browse vDS switch names and vDS port group keys.

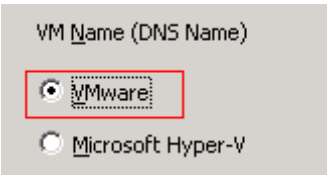
The agent always restores source virtual machines residing on non-vDS networks to ESX Server systems or vCenter Server systems as non-vDS networks. The agent behaves in this manner regardless of whether the vDS check box is selected on the Recover VM screen.

Note: When vDS is not configured on the destination ESX Server or vCenter Server system, the agent performs the recovery operation as a traditional, virtual network recovery.

Follow these steps:

1. Open the Restore Manager, click the Source tab, and select Recover Virtual Machine from the drop-down list to open the Recover Virtual Machine screen.

2. Click the VMware option on the Recover Virtual Machine screen as illustrated by the following screen:



The Transport Mode for VMware VM dialog appears.

Select one of the following transport methods to use for backup:

- **Dynamic**--(*default*) This option lets VMware Virtual Disk Development Kit (VDDK) select the available transport mode.
- **SAN**--(Storage Area Network) This option lets you transfer backup data from proxy systems connected to the SAN to storage devices using Fibre Channel communication.
- **HOTADD**--This option lets you back up virtual machines configured with SCSI disks.
- **NBDSSL**--(Network Block Device Secure Sockets Layer) This option lets you use the Network File Copy (NFC) protocol to communicate. NBDSSL transfers encrypted data using TCP/IP communication networks.
- **NBD**--(Network Block Device, also referred to as LAN transport mode) This option lets you use the Network File Copy (NFC) protocol to communicate. Various VDDK operations use one connection for each virtual disk that it accesses on each ESX/ESXi Server host when using NBD.

Note: If the specified transport mode is not available, the transport mode defaults back to the Dynamic option.

3. To search for virtual machines, use one of the following search methods and continue to the next step:

- **Search for a specific virtual machine**
- **Search all virtual machines**

  Note: Select << ANY >> in the VM Name (DNS Name) field and click Query.

- **Search using wildcard characters**

  Note: Replace the unknown characters of the virtual machine name with an asterisk in the VM Name (DNS Name) field, and click Query. For example, using 100-* returns the names of all virtual machines that start with 100-, such as 100-1, 100-01, and 100-001.

4. In the VM Name (DNS Name) column, click the check box next to the virtual machines that you want to recover. Then, specify the values that you require for each virtual machine that you selected in the following columns:

   - **Backup Versions--**Click the ellipsis to search for multiple versions of the backup data.
   - **Proxy Machine--**Click the ellipsis to search for and specify a backup proxy system.
   - **Path--**You can accept the displayed path or click in the Path field to specify an alternate path for the temporary VM mount directory.
   - **VM Destination--**Click in the VM Destination field and then click the ellipsis to open the Destination dialog.

5. From the vCenter/ESX drop-down list on the Destination dialog, select vCenter Server system where you want to recover the virtual machines.

   Specify the User Name and Password that is required to log in to the vCenter Server and click Connect.

   The agent enumerates all the ESX server systems associated with the vCenter Server system that you specified in the drop-down list.

6. From the ESX Server drop-down list, specify the ESX Server system where you want to recover the virtual machines.

   Note: If you want to recover virtual machine data to specific data stores, follow the steps described in Recover VMware Virtual Machines to Specific Data Stores.

   To specify a vDS switch, do the following:

   a. Check vDS Switch to enumerate the vDS switch.

   b. From the vDS switch drop-down list, select one vDS switch to enumerate the vDS port group.

   c. From the vDS port group, select a port group.

   Click OK.

   The Destination dialog closes and the agent populates the VM Destination field with the location to recover the data.

   Note: Repeat Steps 4, 5, and 6 for each virtual machine that you want to recover in this job.

7. Click the Schedule tab and specify the schedule that you require for the job.

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

8. Click Options on the toolbar to open the Global Options dialog.

   Click the Operation tab and specify the following:

   Power on VMware or Hyper-V VM after restore

   Default value: Enabled.

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

   Overwrite VMware VM, if it exists

   When you restore a VMware VM, the agent detects the virtual machines that reside in the host system. If the virtual machine exists in the host system, this option lets you overwrite the virtual machine using the existing UUID and host name for the virtual machine.

   Default value: Enabled.

   Note: For troubleshooting information, see The Agent Does Not Delete Existing VMs after a Recover VM Job Completes (see page 118).

   Click OK to apply the options.

9. Click Submit to submit the restore job.

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

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

Restore Hyper-V Virtual Machine Data

This section contains the following topics:

How to Browse Hyper-V Sessions

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

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

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

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

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

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

Recover Hyper-V Virtual Machines

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

Browsing the Recover VM Window

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

To modify an editable field, select the target field and then click the ellipsis to browse the field.

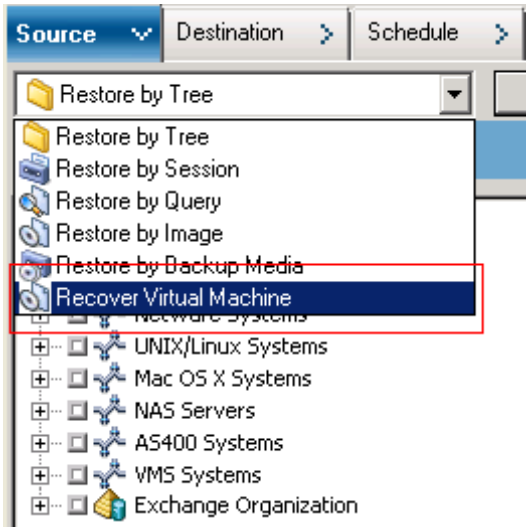
Considerations

Be aware of the following considerations:

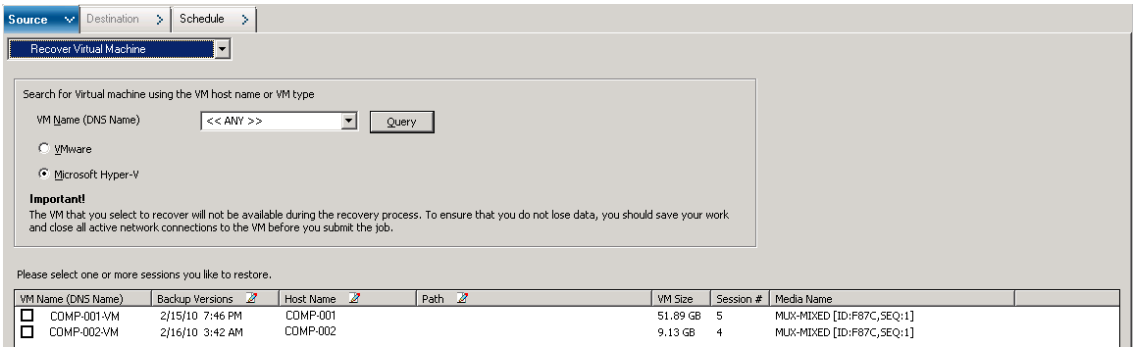
- The target VM should be powered off and deleted from the system or renamed. If the VM is not powered off and deleted or renamed, the restore process overwrites the data on the target VM.

To recover Hyper-V virtual machines

1. Open the Restore Manager, click the Source tab, and select Recover Virtual Machine from the drop-down list.



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 the VMs in your environment display in the VM list.

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

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

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

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

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

3. Complete the following fields in the VM list.

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

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

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

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

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

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

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

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

4. Click Options on the toolbar.

   The Global Options dialog opens.

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

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

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

     Default value: Enabled.

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

6. Click OK.

   The options are applied.

7. Click Submit to submit the restore job.

   The Submit Job dialog opens.

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

   Enter a description for your job and click OK.

   The job is submitted.

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

Recover Hyper-V Virtual Machines to Alternate Locations

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

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

These capabilities let you do the following:

- Recover virtual machines (VMs) to the same or a different Windows Server Hyper-V system.
- Create directories (with and without drive letters) on the target VMs during the recovery process, if the directories do not exist.

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

- Recover Hyper-V VMs to an alternate location where Hyper-V server is a Windows Server Hyper-V system.
- Specify paths to an alternate location on the target Windows Server Hyper-V system.

Be aware of the following behavior:

- If you specify an alternate path, Arcserve Backup takes the entire path from backup set, with the exception of the root drive or volume name, and adds it to the specified path.
- If you try to recover the VM at a different server, where there is a mismatch in the server network settings, the VM does not power-on. Modify the VM settings to the available Network Adapter settings on the server for VM to power-on.

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 How Global and Local Backup Options Work.

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*.

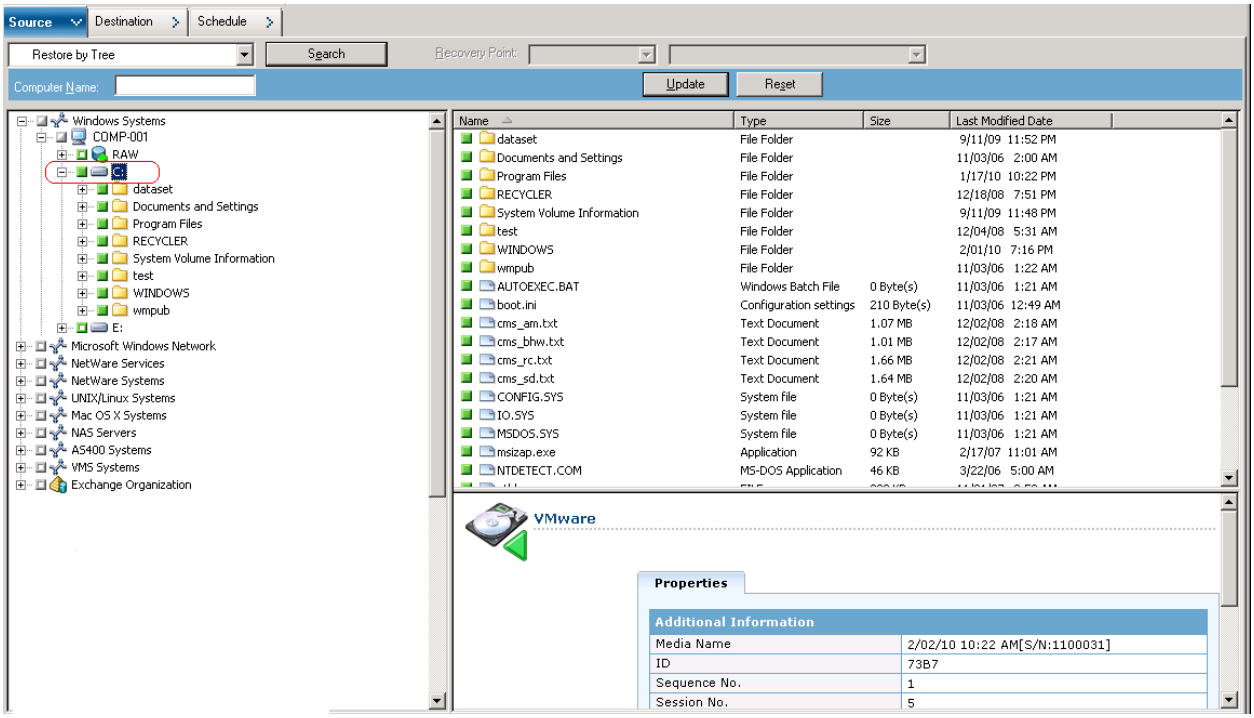
When you restore file level backup data, consider the following:

- 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 How Global and Local Backup Options Work.
- 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, Arcserve Backup intentionally omits Windows system files. Windows system files are usually stored in the directories that follow:
  - 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, Arcserve Backup omits Windows system files.

   If the backup data was created from a raw (full-VM) backup, 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.

   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*.

Restore Raw (Full VM) Level Backup Data

Use the steps that follow to perform restore operations on local disk-based virtual machines (VMs) and SAN-based VMs. You would restore raw (full VM) data when you need to recover a system from a disaster or clone a system. You use the same process to restore file level backup data as that of restoring any Windows-based client agent file.

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

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

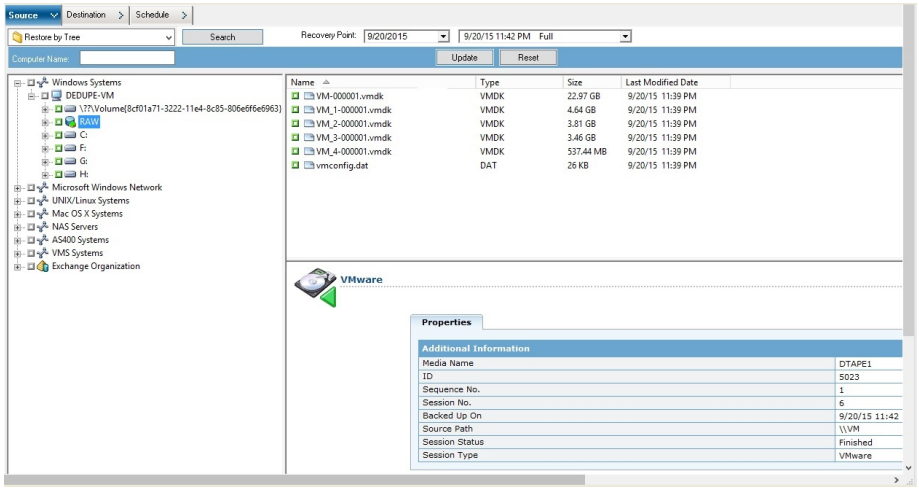
- The current version of the Client Agent for Windows must be installed on the destination system to restore data that was backed up using the Agent for Virtual Machines.
- You cannot browse and restore data at directory and file level granularity from data that was backed up using raw (full VM) or Mixed mode without specifying the Allow file level restore option.

To 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.

   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.*

Appendix A: Troubleshooting

This section contains the following topics:

Backup and Recovery Operations

The following topics describe how to troubleshoot backup and recovery operations on systems running VMware vSphere.

The Auto-Populate VM Process Does Not Start On Schedule

Valid on all Windows operating systems supported by Arcserve Backup.

Symptom

The auto-populate VM process does not start on schedule. The frequency of the auto-populate process was changed recently.

Solution

After you change the frequency of the auto-populate process, the process will start the next calendar day.

Example: Change the Frequency of the Auto-populate VM Process

You change the frequency of the auto-populate VM process to one hour at 11:00 AM on April 5. Although you expect the process to start at 12:00 PM on April 5, it does not start. The auto-populate VM process will start at 12:00 AM on April 6 and execute at one hour intervals.

Optionally, you can run the auto-populate process manually to update the Arcserve database using the ca_vcbpopulatedb command line utility. For information about the ca_vcbpopulatedb command line utility, see the Command Line Reference Guide.

The Agent Does Not Delete Existing VMs after a Recover VM Job Completes

Valid on all supported Windows operating systems.

Symptom

Arcserve Backup may not delete the existing VM on the target ESX Server system in the following scenario:

- You submit a Recover VM job.
- You specified the Overwrite VM global restore option.
- Arcserve Backup successfully recovers the VM to the backup proxy system (ESX Server system).

Solution

This is expected behavior.

The agent combines the UUID and host name of a VM to create a unique identifier for the VM. Arcserve Backup uses the identifier to distinguish backup and restore operations for the particular VM. However, VMware vSphere no longer uses the UUID as a mechanism to identify VMs. When you submit a job to recover the VM and specify the Overwrite VM option, Arcserve Backup does not delete the original VM if it cannot detect a VM with the same UUID and host name as that of the original VM. As a result, Arcserve Backup creates a new VM rather than overwrite the existing VM. The approach helps ensure that Arcserve Backup does not delete VM in error. Arcserve Backup also behaves in this manner in the following scenarios:

- The UUID or host name of the VM was changed.
- The VM was powered off or down (the agent cannot retrieve the host name of the VM).

Backup Jobs Fail with Snapshot Creation Errors

Valid on Windows platforms.

When you submit backups of VMware based virtual machines, the following symptoms occur:

Symptom 1

Backup jobs fail and the following message appears in the ca_vcbpopulatedb.log file:

Failed to take snapshot. ESX/vCenter report error. A general system error occurred. Protocol error from VMX.

Solution 1

This error is a VMware issue. To correct this problem, uninstall and then reinstall VMware Tools inside the guest operating system and then resubmit the job.

Symptom 2

Backup jobs fail and the following message appears in the ca_vcbpopulatedb.log file:

Could not take snapshot of the virtual machine. ESX Server/vCenter Server reported the following error: Cannot create a quiesced snapshot because the create snapshot operation exceeded the time limit for holding off I/O in the frozen virtual machine..

Solution 2

This error occurs when VSS encounters errors when creating snapshots. VSS can encounter errors under the following conditions:

A VSS writer is in an unstable state.

To determine the source and correct this behavior, perform the following remedial actions:

1. Run the command "vssadmin list writers" from the command line on the guest operating system on the virtual machine.
2. Verify that all VSS writers are in a healthy state.
3. For writers that are in the following states, contact Microsoft or the vendor of the writer for information about how to fix the errors.

   state=Stable
   Last Error=No Error

   Note: Restarting writers usually solves the problem.

VSS encountered errors when creating snapshots.

To determine the source and correct this behavior, perform the following remedial actions:

1. Review the Windows event log in the guest operating system. Check for errors that are related to the VSS components about the time the backup started.
2. When VSS reports errors due to insufficient disk space, free disk space on the volume that is associated with the error.
3. When VSS or the Windows Volsnap driver generates time-out errors, the applications running inside the virtual machine are in a highly active state. The highly active state prevents VSS from creating consistent snapshots. To remedy this condition, schedule backups at times when the applications perform fewer input and output operations to the volume.
4. When the Windows Event Log indicates that the VolSnap driver encountered errors, see the article Volume Snapshot Driver Integrity at the Microsoft Technet Library for information about how to correct VolSnap driver errors.

Jobs Incorrectly Report Snapshots are Not Deleted

Valid on Windows platforms.

Symptom

When you back up and restore virtual machines running on ESX Server, the operation deletes the snapshots for the guest virtual machine successfully, however, the jobs fail and the Activity Log reports that the snapshots were not deleted. The following is an example of the message that appears in the Activity Log:

AW0585 RMDMISLARCRW009 01/06/2013 11:03:38 AM 54
Failed to delete Virtual Machine Snapshot for the VM on ESX/VC server.

Solution

This behavior occurs due to the length of time that was required to delete the snapshots. By default, the agent reports timeout error messages when there is a period of inactivity for the job for 10 or more minutes. Because of the length time that was required to delete the snapshots, the agent interpreted the delay (deleting the snapshots) as a failed operation and returned message AW0585 in the Activity Log.

Use one of the following solutions to modify this behavior:

- **Increase the timeout value:** By default, the agent waits 10 minutes before reporting a timeout error. To increase the timeout value, open the following Registry key:

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

  Change the value data of the DWORD VimTimeout to a value of 10 through 20 (inclusive).

  Note: You may need to create the DWORD VimTimeout.

  Resubmit the job.

- **Perform disk consolidation on the guest virtual machine:** Use the VMware VI Client to consolidate the disks and then resubmit the job.

  Note: You can use this solution only on vSphere 5.0 (ESX Server) environments.

Backups of VMs in a Cluster-Aware Environment Fail

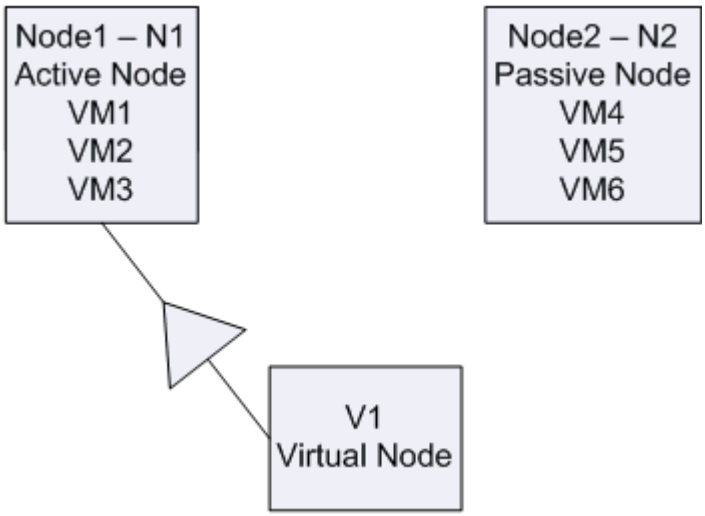
Valid on Windows Hyper-V systems.

Symptom

Backups of VMs in a cluster-aware environment fail.

Solution

The following diagram illustrates VMs installed in a cluster-aware environment:



In an ideal scenario, virtual cluster node V1 directs network traffic to the active node (N1). When failover occurs, virtual cluster node V1 directs the network traffic to the passive node (N2), and all of the VMs in the active node (N1) move to the passive node (N2).

If Arcserve Backup backs up the active node (N1) after failover occurs, the backup will fail because Arcserve Backup cannot locate the VMs in the active node (N1).

To remedy this problem, do the following:

- Submit backups by specifying the entire Hyper-V node, which includes the active node and the passive node, rather than the individual VMs that are configured in the Hyper-V node.
- Ensure that Arcserve Backup executes the auto-population process before Arcserve Backup backs up the clustered nodes.

Note: Arcserve Backup does not support backing up VMs that are configured with virtual node names. For example, If you submit a backup Job using the virtual node V1 as the backup proxy system, Arcserve Backup will back up data using the active node (N1 or N2), as the backup proxy system.

VDDK Backup Jobs Fail

Valid on Windows operating systems.

Symptom

Backup jobs fail when you use VDDK to back up VMware VMs. This problem is evident by the following symptoms:

- Error E8535 appears in the Arcserve Backup Activity Log.
- The following error message appears in the VMDKIO.log file:

  System libeay32.dll library is older than our library (90709F < 9070AF)
  SSLLoadSharedLibrary: Failed to load library libeay32.dll:126

Solution

VMware VDDK installs library files named libeay32.dll and ssleay32.dll in the default VDDK installation directory. The problem occurs when other applications install different versions of the same libraries in the Windows\system32 directories. With multiple instances of the same libraries, the Agent for Virtual Machines may to try to load incorrect versions of these libraries when the backup executes. As a result, the above message appears in the VMDKIO.log file, and backup jobs involving VDDK may fail.

To remedy this problem, do the following:

1. Browse to the VDDK installation directory on the backup proxy system.

   x64 Systems (default):

   C:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit

2. Locate the files named libeay32.dll and ssleay32.dll in the following directory:

   x64 Systems:

   C:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\vddk64\bin

3. Copy libeay32.dll and ssleay32.dll from the above directory to the Universal Agent installation directory on the backup proxy system. By default, the Universal Agent is installed in the following directory:

   C:\Program Files\CA\SharedComponents\ARCserve Backup\UniAgent

Recover VM Jobs Fail on VMware VMs

Valid on Windows platforms.

Symptom

When you submit Recover VM jobs on VMware based VMs, the jobs fail with error AE0564.

Solutions:

There are several reasons why Recover VM jobs on VMware VMs can fail. The following list describes the reasons jobs can fail and the required corrective actions.

- **Symptom 1:** The credentials specified for the VMware ESX Host system are not correct:

  Solution 1: Verify that the credentials specified for the VMware ESX Host system are correct.

- **Symptom 2:** There is insufficient free disk space in the target datastore.

  Solution 2: Verify that there is sufficient free disk space in the target datastore on the VMware ESX Host system. Optionally, you can move the target datastore to a different VMware ESX Host system.

- **Symptom 3:** The VMware ESX Host system is down or not reachable.

  Solution 3: Verify that the VMware ESX Host system can communicate with the backup proxy system.

Recover VM Operations Fail with Unknown Errors

Valid on Windows operating systems.

Symptom

Recover VM jobs fail. You can submit the Recover VM job, however, the following message appears in the Activity Log:

Failed to recover virtual disks.

In addition, VDDK reports the following error message:

Unknown Error.

Solution 1:

To correct this problem, consider the following solutions:

- Recover VM jobs can fail when there is not enough free disk space on the original datastore. VDDK returns the message because the VDDK API (currently) does not support the capability to detect the amount of free disk space on the original datastore. (The datastore is the location where you specified to recover the virtual machine.) To correct this problem, free the amount of disk space on the original datastore that is required to complete the operation and then resubmit the job.
- Network disturbance and high network traffic can cause Recover VM jobs to fail. To correct this problem, verify that the proxy server and the ESX Server system or the vCenter Server system can communicate with each other though the network, then resubmit the job.
- Multiple concurrent connections consisting of backup or recover VM jobs to the ESX Server system or the vCenter Server system, which includes vSphere SDK connections through the VMware vSphere Client, can cause the jobs to fail. To correct this problem, close all unnecessary connections and then resubmit the job. For information about the maximum quantity of concurrent connections that are allowed, see Cannot Open VMDK File.
- Examine the Tasks and Events sections of the VMware vSphere Client log to discover internal errors for the specific virtual machine. Correct the internal errors and then resubmit the job.

  Example: Another application or operation is using the VMDK file. To correct this problem, release the file and resubmit the job.

Solution 2:

This problem can occur under the following conditions:

- VDDK did not process a snapshot properly.
- VDDK did not delete a snapshot manually or internal to the virtual machine.

To correct this problem, resubmit the job. If the job fails again, delete the recovered virtual machine and resubmit the job.

Cannot Power on VMs When Restoring Data

Valid on Windows platforms.

Symptom

Arcserve Backup may not be able to power on VMs after restores are complete. This behavior occurs only when all the following conditions are present:

- The VM is configured with Windows Server 2008 R2 or Windows 7 as a guest operating system on VMware ESX Server 4.0. The default SCSI controller is specified for the VM (for example, LSI Logic SAS).
- Arcserve Backup for Windows Agent for Virtual Machines is installed on the backup proxy system.
- The guest operating system contained in the VM that you recovered is Windows Server 2008 R2 or Windows 7.
- You submitted the backup using the Agent for Virtual Machines and the VMware vSphere Web Services SDK and VMware VDDK approach.
- You submitted the restore with the Power on after restore option specified.

Solution

To remedy this problem, do the following:

1. Let Arcserve Backup complete the restore operation.
2. Access the VMware ESX Host system through the VI client where the VM is recovered.
3. Select the VM that was recovered.
4. Right-click the VM and select Edit Settings from the pop-up menu.
5. Change the controller type from BusLogic Parallel to LSI Logic SAS.
6. Power on the VM.

Cannot Power on Hyper-V VMs When Restoring Data to an Alternate Location

Valid on Windows Server 2008 systems.

Symptom 1:

When restoring Hyper-V VMs to an alternate location, Arcserve Backup may not be able to power on the target VM. This behavior occurs if the friendly name of the network switch is not the same as that of the original backup.

Solution 1:

There are several approaches that you can use to remedy this problem.

- The best practice is to ensure that the friendly name of the destination VM (alternate location) is the same as the source location before you submit the restore.
- An alternate solution is to edit the VM's settings after the restore is complete, and then configure the appropriate network switch before you power on the VM.

Symptom 2:

When restoring Hyper-V VMs to an alternate location, Arcserve Backup may not be able to power on the target VM. This behavior occurs if the CD/DVD name is not the same as that of the original backup.

Solution 2:

There are several approaches that you can use to remedy this problem.

- The best practice is to ensure that the CD/DVD name of the destination VM (alternate location) is the same as the source location before you submit the restore.
- An alternate solution is to edit the VM's settings after the restore is complete, and then configure the appropriate CD/DVD name before you power on the VM.

Symptom 3:

You cannot power on Hyper-V VMs manually in the following scenario:

- The Hyper-V VM was restored to an alternate location.
- The Power on VMware or Hyper-V VM after restore option was not specified.

  Note: The Power on VMware or Hyper-V VM after restore option is a global restore option that appears on the Operations tab on the Options dialog.

Solution 3:

To remedy this problem, do the following:

1. After the restore is complete, open the Hyper-V Manager and specify the Remove Saved State option.
2. Power on the Hyper-V VM.

Backup and Recover VM Operations Fail Using NBD Transport Mode

Valid on all Windows platforms running on backup proxy systems.

Symptom

Backup and recover VM operations fail.

The following errors appear in the VDDK error logs:

Failed to open NBD extent

NBD_ERR_GENERIC

NFC connection errors relating to NFC operations appear in the error logs. For example:

NfcFssrvrRecv

NfcFssrvr_DiskOpen

NfcNetTcpWriteNfcNet_Send

NfcSendMessage

Note: Debugging must be enabled to view the above error logs. For more information, see Enable Debugging for VDDK Jobs (see page 48).

Solution

Network Block Device (NBD) transport mode, also referred to as LAN transport mode, uses the Network File Copy (NFC) protocol to communicate. Various VDDK operations use one connection for each virtual disk that it accesses on each ESX Server and ESXi Server host when using NBD. Furthermore, connections cannot be shared across disks. The VI Client and periodic communication between the host systems, the vpxd, the ESX Server, and ESXi Server systems account for the number of concurrent connections.

The following table describes the maximum number NFC connections:

Host Platform	Connecting to	Limits to
vSphere 4	an ESX host	9 connections directly and 27 connections through vCenter server
vSphere 4	an ESXi host	11 connections directly and 23 connections through vCenter Server
vSphere 5 and 6	an ESXi host	Limited by a transfer buffer for all NFC connections enforced by the host: the sum of all NFC connection buffers to an ESXi host cannot exceed 32MB. 52 connections through vCenter server, including the above per-host limit.

Be aware if the following:

- The Maximum Connections values represent host limits.
- The Maximum Connections values do not represent process limits.
- The Maximum Connections values do not apply to SAN and hotadd connections.
- The error messages described under Symptoms occur when the number of NFC connections to the host systems exceed the maximum number of connections described in the above table. When failures occur, the number of connections to the ESX Server or ESXi Server increase, which causes the communication sessions to the host systems to exceed the number of maximum connections.
- If the NFC client does not shut down properly, ESX Server and ESXi Server allow the communication sessions to remain open for an additional ten minutes. This behavior can increase the number of open connections.

Best Practices:

The solution to this problem is to use the following best practices to help ensure that backup and recovery operations do not fail when using NBD transport protocol:

- Ensure that open connections to ESX Server systems and ESXi Server systems are closed properly.
- Use the following best practices when submitting backup and restore jobs:
  - If you suspect that you will need a high number of connections to the host systems, you should populate the VMs in your Arcserve Backup environment using VMware vCenter Server.
  - When backing up data using the VDDK approach, you should optimize the number of streams specified for multistreaming backups and optimize the number of concurrent read operations of the VM disks. This approach helps to minimize the number of communication sessions to the host system. You can estimate the number of connections using the following calculations:
    - **Mixed Mode backups and Raw (full VM) backups (with or without the Allow file level restore option specified) using VDDK--**The number of connections equals the lesser of the number of streams in a multistreaming job or the number of VMs specified in a multistreaming job, multiplied times the value of vmdkReaderCount.

      Note: For backups of VMs that use VDDK, Arcserve Backup backs up one disk at a time, and there are multiple connections to each disk as indicated by the value of vmdkReaderCount.

      Example: A job consists of 4 VMs. VM1 contains 5 disks. VM2, VM3, and VM4 contain 4 disks each. There are 3 streams specified for the job.

      The number of connections equals 3 (the number of streams is less than number of VMs) multiplied times 4 (the value of vmdkReaderCount).

      The number of connections required is 12.

      Note: By default, VDDK backups use a vmdkReaderCount value of 4. For information about how to change the value of VDDK vmdkReaderCount, see Configure the Number of Concurrent Read Operations Using VDDK (see page 38).

    - **Raw (full VM) backups (with or without the Allow file level restore option specified) and File mode backups using VDDK--**The number of connections equals the total number of disks for all VMs backed up concurrently, limited by the number of streams specified for a multiplexing job.

      Example: A job consists of 4 VMs. VM1 contains 5 disks. VM2, VM3, and VM4 contain 4 disks each. There are 3 streams specified for the job.

      the number of connections equals 5 (VM1) plus 4 (VM2) plus 5 (VM3).

      The number of connections required is 14. Arcserve Backup will back up VM4 when the backup pertaining to VM1, VM2, or VM3 is complete.

Unable to Recover Hyper-V VMs to an Alternate Location

Valid on Windows Server 2008 systems.

Symptom

You are attempting to recover a Hyper-V VM to an alternate location using the Recover Virtual Machine restore method. The Recover Virtual Machine view (in the Restore Manager) does not display information about the backup data (for example, the host name, the backup version, and the path of the backup). This problem presents itself only under the following conditions:

- Windows Server 2008 is the operating system running on the Hyper-V server.
- You made a recent, unsuccessful attempt to recover the Arcserve Backup database.

  Note: The database information, such as the host name, the backup version, and so on, appears in the Recover Virtual Machine view only when you recovered the Arcserve Backup database successfully.
- The Hyper-V backup data resides on media, such as a tape library, file system device, or deduplication device, and the information about the backup data cannot be retrieved from the Arcserve Backup database.

Solution

Arcserve Backup lets you recover Hyper-V VMs to an alternate location. You can then specify the missing information (the host name, backup version, path, and so on) in the Restore Manager window. However, Windows Server 2008 does not support recovering Hyper-V VMs to an alternate location. As a result, the job will fail.

Note: Windows Server 2008 R2 supports recovering Hyper-V VMs to an alternate location.

To remedy this problem, do the following:

1. Use the Restore by Session restore method and recover the Hyper-V VM to any location on any Hyper-V server in your Arcserve Backup VM environment.
2. Use the Hyper-V Manager to create the VMs using the recovered VHD or VHDX files.

The Agent Deletes Snapshots After Recovering VMs

Valid on Windows Hyper-V systems.

Symptom

After you recover a VM with data that was backed up using the raw (full VM) backup mode with the allow file level restore option specified, the recovery process deletes the snapshot.

Solution

The symptom described above is expected behavior. To preserve snapshots after recovering VMs, you must specify the raw (full VM) backup mode, but do not specify the allow file level restore option.

Virtual Machines Do Not Start After Recover VM Operations Complete

Valid on Windows platforms.

Symptom

Virtual machines may not start properly after Recover VM operations complete. In addition, you may encounter the Stop Error screen (blue screen) when you try to start the virtual machine. The problem occurs only when you back up virtual machines that reside on ESX Server version 4.0 (and older versions) using VCB and a previous release of the agent, and recover the virtual machines to alternative servers running ESX Server version 4.1 (and later versions) using VDDK.

Solution

This behavior occurs because the agent cannot define the SCSI controller type from data that was backed up using VCB from a previous release of the agent. The solution to this problem is to change the SCSI controller type manually after the recovery operation completes, and then restart the virtual machine.

To change the SCSI controller type, do the following:

1. Open the VMware vSphere Client and select the virtual machine that you recovered.
2. Right-click the virtual machine and click Edit Settings on the pop-up menu.

   The Virtual Machine Properties dialog opens.
3. Do one of the following:
   - When the source virtual machine is available in the ESX Server system, verify that the SCSI controller type that was used for the backup is same as the SCSI Controller Type that appears on the Virtual Machine properties for the recovered virtual machine. If the SCSI Controller Type is the same, no changes are required.
   - When the source virtual machine is not available in the ESX Server system, for any reason, change the SCSI Controller Type from LSI Logic Parallel to LSI Logic SAS.

     You can now restart the recovered virtual machine successfully.

License Errors Occur When Backing Up and Recovering VMs

Valid on Windows.

Symptom

Backup jobs and recover VM jobs fail. The following error messages appear in the Arcserve Backup Activity Log:

- **Backup jobs--**Failed to backup the virtual machine.
- **Recover VM jobs--**Failed to recover the virtual machine.

In addition, the following message appears in the backup and restore log files on the backup proxy system:

```
VMDKInit : OpenVMDKFileA failed Error: Host is not licensed for this feature
```

Note: The backup and restore log files are stored in the following directory on the backup proxy system:

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

Solution

Various files and directories can be created and modified when you install the Client Agent for Windows and VMware VDDK on computers that function as backup proxy systems. In this scenario, the following temporary directory is created on the backup proxy system:

C:\Documents and Settings\Administrator\Local Settings\Temp\vmware-Administrator

When you submit jobs, the files within this directory can prevent backup jobs and restore jobs from completing successfully. To remedy this problem, delete the temporary directory referenced above and then resubmit the job.

Important! This is a unique scenario. You should delete the temporary directory only when jobs fail and the license message appears in the backup and restore log files.

The Agent Does Not Generate Internal Sessions

Valid on Windows Hyper-V systems.

Symptom

When backing up data through pass through storage devices, the agent does not generate internal backup sessions.

Solution

This is expected behavior under the following conditions:

- The backup was submitted through a pass through storage device.
- The backup mode was one of the following:
  - Mixed mode with the Allow file level restore option specified.
  - Raw (full VM) mode with the Allow file level restore option specified.

Note: For more information about backup modes, see How Global and Local Backup Options Work.

Virtual hard disk (VHD or VHDX) files are files that are stored on Hyper-V systems that define the configuration of the volumes that reside on Hyper-V systems. Under most scenarios, Hyper-V virtual machines access storage based on the configurations that are defined in the VHD or VHDX files. Optionally, the VMs can be figured to access storage using pass through storage devices. Pass through storage devices are not defined in VHD or VHDX files; they are mapped directly to the Hyper-V servers. The devices can be physical disks that reside on Hyper-V servers or SAN (storage area network) LUNs (logical unit number) that are mapped to the Hyper-V servers.

The agent generates internal sessions the following types of VM backup jobs run:

- Mixed mode with the Allow file level restore option specified.
- Raw (full VM) mode with the Allow file level restore option specified.

However, when jobs of these types run, the agent does not access the VHD or VHDX files, which prevents the agent from generating internal sessions.

The Agent Does Not Recover Snapshots

Valid on VMware and Windows hypervisors.

Symptom

When you recover VMs from backup sessions, the recovery process does not restore the individual snapshots that were created on the source VM.

Solution

This is expected behavior for the following backup modes:

- Mixed mode with the Allow file level restore option specified
- Raw (full VM) mode with the Allow file level restore option specified

Note: For more information about backup modes, see How Global and Local Backup Options Work.

With the mixed and raw (full VM) modes, Arcserve Backup consolidates the individual backup sessions into a session that represents the most current state of the VM. As a result, Arcserve Backup does not retain the individual snapshots.

If you must recover the individual snapshots, specify the Raw (full VM) backup mode but do not specify the Allow file level restore option. With this approach, Arcserve Backup lets you recover the individual snapshots from the latest full backup of the VM.

Throughput Decreases on SAN Backups

Valid on Windows operating systems.

Symptom

When you use VDDK to back up virtual machine data in SAN transport mode, the throughput decreases while the job is in progress.

Solution

If you use VDDK to back up virtual machine data in SAN transport mode and the throughput decreases while the job is in progress, do the following:

1. Delete or rename the following directory on the backup proxy system:

   C:\Documents and Settings\Administrator\Local Settings\Temp\vmware-<<username>>

   Example:

   C:\Documents and Settings\Administrator\Local Settings\Temp\vmware-Administrator\vmware-administrator

2. Resubmit the job.

Error Message Appears When Backing Up Virtual Machines that Reside on the Same CSV

Valid on Windows Hyper-V systems.

Symptom

When you back up multiple virtual machines that reside on the same cluster shared volume concurrently, Windows warning ID 1584 appears in Windows Event Viewer. Windows warning ID 1584 is as follows:

A backup application initiated a VSS snapshot on Cluster Shared Volume Volume1 (Cluster Disk 8) without properly preparing the volume for snapshot. This snapshot may be invalid and the backup may not be usable for restore operations. Please contact your backup application vendor to verify compatibility with Cluster Shared Volumes.

Solution

Microsoft confirms that the message is a false alarm. You can ignore the message.

Recover VM Jobs Fail When Using Custom HTTPS Ports for vCenter Server/ESX Server Systems

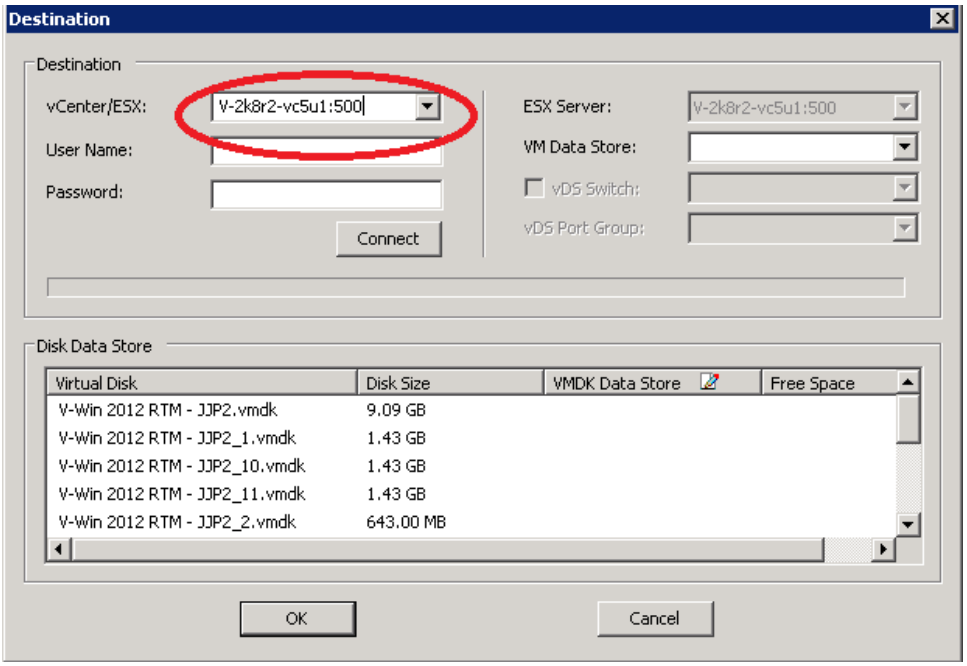
Valid on Windows operating systems.

Symptom

When you try to recover virtual machines associated with vCenter Server or ESX Server systems that communicate using a custom https port, you can submit the Recover VM job successfully, however, the recovery operation fails.

Solution

When you submit a Recover VM job but do not provide the host name or IP address and the custom port on the Recover VM screen, the Restore Manager lets you submit the job successfully. The Restore Manager behaves in this manner because it can enumerate the ESX Server system using the http port when the https communication fails or using the https port when the http communication fails. The job inevitably fails because VDDK cannot revert back to the default communication port during the recovery operation. To prevent this behavior from occurring, provide the custom port on the Recover VM screen before you submit the job as illustrated by the following screen:



Using Different Versions of VDDK for VMware Backups

Valid on Windows operating systems.

Symptom

Arcserve Backup is packaged with the default binaries for VDDK 6.0.1. When you install a different version of VDDK, change the VDDK installed location in the registry manually. Otherwise, the VMware backups are going to use VDDK 6.0.1 instead of the version that you installed.

Solution

To remedy this problem, perform the following steps:

1. Open the registry.
2. Navigate to the following location:

   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters
3. Specify VDDKDirectory as the Value Name.
4. Change the "ValueData" field to the location where the latest VDDK version is installed.

The location in the registry is updated.

Back Up VM in a Hyper-V Server Fails

Valid on all Windows operating systems.

Symptom

When performing an online backup for a Volume Shadow Copy Service (VSS), the VSS requires the mounting of snapshot VHDs to revert them back to their proper state. If automount is disabled, VSS cannot mount the snapshot VHDs as required.

To determine if automount is enabled, run DISKPART.EXE from a command prompt and then run the following command without quotes at the DISKPART prompt: "automount".

Backing up the virtual machine fails when the following error message appears in the Activity Log:

AE0603 RMDMISLARCRW009 11/05/2012 05:37:09 PM 2171 1 Failed to create VSS shadow copy for the VM on the Hyper-V host machine.

Solution

Run DISKPART.EXE from a command prompt and then run the following command without quotes at the DISKPART prompt:

"automount enable"

Ensure the “Microsoft Hyper-V VSS Writer” state is Stable and resubmit the job.

http://support.microsoft.com/kb/2004712

Mount Operation Problems

This section contains the following topics:

Directories Do Not Appear Under the Mount Point When Completing File Level Backups

Valid on all Windows systems functioning as backup proxy systems.

Symptom

File and folder directories do not appear under the mount point when performing file level backups using VDDK.

Solution

VMware VDDK cannot map file and folder directories to a mount directory on a volume or drive letter. However, VDDK maps the mounted volume to a symbolic link device path using the signature that follows:

\.\vstor2-mntapi10-F0751CFD007E00000000000001000000\.

The above signature is a low-level device path that you can view in the Windows Object namespace. However, the namespace is not mapped to a volume drive letter on a mounted volume on the backup proxy system.

Arcserve Backup Cannot Mount Volumes that Use GUID Partitions

Valid on all Windows systems functioning as backup proxy systems.

Symptom

Arcserve Backup cannot mount volumes that use Globally Unique Identifier (GUID) based partitioning.

Solution

This is expected behavior. VMware VDDK does not support mounting volumes that use GUID-based partitioning.

Volume Mount Points Cannot be Traversed

Valid on all Windows systems functioning as backup proxy systems.

Symptom

Arcserve Backup cannot traverse volume mount points after the agent mounts a file mode backup using VDDK.

Solution

This is expected behavior. VMware VDDK does not support the capability to traverse volume mount points related to file level backups.

Virtual Machine Mount Operations Fail

Valid on Windows platforms.

Symptom

A raw (full VM) mount operation or a file level VM mount operation failed.

Solutions:

There are several reasons this problem can occur and actions you can take to remedy this problem.

- **Reason 1:** There is not enough free disk space in the disk volume on the backup proxy system.

  Action 1: Clean up the disk or change the mount path to a different volume that has enough space.

- **Reason 2:** The VMware ESX Host system is down.

  Action 2: Take corrective action if the VMware ESX Host system on which the VM resides is down.

- **Reason 3:** The backup source included VMs with an Independent (Persistent/Nonpersistent) disk mode specified.

  Action 3: Clear or Remove the Independent disk mode setting for all virtual disks associated with the VM.

- **Reason 4:** The job was submitted with incorrect VMware ESX Host or vCenter Server user credentials. The credentials were specified on the Security and Agent Information dialog.

  Action 4: Resubmit the VM backup job with valid credentials. You must provide valid VMware ESX Host system credentials or vCenter Server system credentials, and backup proxy system credentials on the Security and Agent Information dialog.

- **Reason 5:** A VM is no longer available in the VMware environment.

  Action 5: Run the Arcserve VMware Configuration Tool or ca_vcbpopulatedb utility to populate the Arcserve Backup database with updated information about your VMware environment.

Cannot Open VMDK File

Valid on Windows platforms.

Symptom

Multiple concurrent backup jobs fail in NBD (or LAN) transport mode. The following message appears in the Activity Log:

Cannot open VMDK File

Solution

This is a VMware connection limitation. The following Network File Copy (NFC) protocol limits apply:

Host Platform	Connecting to	Limits to
vSphere 4	an ESX host	9 connections directly and 27 connections through vCenter server
vSphere 4	an ESXi host	11 connections directly and 23 connections through vCenter Server
vSphere 5 and 6	an ESXi host	Limited by a transfer buffer for all NFC connections enforced by the host: the sum of all NFC connection buffers to an ESXi host cannot exceed 32MB. 52 connections through vCenter server, including the above per-host limit.

Connections cannot be shared across disks. The maximum limits do not apply to SAN or hotadd connections. If the NFC client fails to shut down properly, connections can remain open for ten minutes.

Arcserve Configuration Tool Problems

This section contains the following topics:

ca_vcbpopulatedb Utility Fails with .NET version >= Not Found

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 the following directory:
   - 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.

ca_vcbpopulatedb Utility Fails with Err_code: -100 Make_Connection

Valid on Windows platforms.

Symptom

The Arcserve VMware Configuration Tool or the ca_vcbpopulatedb utility fails. The error message that follows appears in the Results field on the Arcserve VMware Configuration Tool:

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

Solution

The above-described error occurs because Arcserve VMware Configuration Tool and ca_vcbpopulatedb Utility cannot provide credentials to the backup proxy system at runtime. To remedy this behavior you must allow the VMware ESX Host system or vCenter Server system to bypass the process of connecting with the backup proxy system.

To add VMware ESX Host systems, vCenter Server systems, or both to the exceptions list, do the following:

1. Open Internet Explorer.

   From the Tools menu, click Internet Options.

   The Internet Options dialog opens.

2. Click the Connections tab.

   The Connections options appear.

3. Click LAN Settings.

   The Local Area Network (LAN) Settings dialog opens.

4. In the Proxy server section, click Use a proxy server for your LAN.

   Click Advanced.

   The Proxy Settings dialog opens.

5. In the Exceptions field, add your VMware ESX Host system or vCenter Server system. To add multiple VMware ESX Host systems vCenter Server systems, separate the entries using semicolons (;).

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

   The VMware ESX Host systems and vCenter Server systems are added to the exceptions list.

Miscellaneous Problems

This section contains the following topics:

VMs Do Not Appear in the Backup Manager Directory Tree (see page 145)

VMs Do Not Appear in the Backup Manager Directory Tree

Valid on Hyper-V and VMware systems.

Symptom

You execute Arcserve VMware Configuration Tool or Arcserve Hyper-V Configuration Tool. After you open the Backup Manager, some VMs do not appear under the VMware Systems object or the Microsoft Hyper-V Systems object.

Solution

The symptom described above is expected behavior. Although the aforementioned tools capture backup information about VMs that are in a powered off state when you execute tools, the information relating to powered off VMs will not appear under the VMware Systems object or the Microsoft Hyper-V Systems object. To remedy this condition, you must power on the VMs and then execute the appropriate tool.

Appendix B: Configuring VMware ESX Host Systems and vCenter Server Systems

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

This section contains the following topics:

Configure VMware ESX Server 3.0.2 Systems

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

To configure VMware ESX Server 3.0.2 systems

1. Install VMware ESX 3.0.2 Server. For more information about VMware ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your VMware ESX Host systems using VMware vCenter Server, you must install and configure VMware vCenter Server as part of Virtual Infrastructure installation.

2. Install VDDK 5.0 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.
   - When the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

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

3. To set up backing up VMs through a Backup Proxy using a VMware ESX Server 3.0.2 system, configure one of the following communication protocols:

   https

   To use https as the communication protocol between the VMware ESX Host system and the backup proxy system, copy the self-generated SSL certificate from the VMware ESX Host system to the backup proxy system, and then install the certificate on the backup proxy system.

   You can find the SSL certificate (labeled rui.crt) from the following directory on the VMware ESX Host system:

   ```
   /etc/vmware/ssl/rui.crt
   ```

   To install the SSL certificate, right-click the object and select Install from the pop-up menu.

   http

   To use http as the communication protocol between the backup proxy system and the VMware ESX Host system, you must configure the http protocol on the VMware ESX Host system as follows in the config.xml file located at /etc/vmware/hostd/config.xml:

   a. Locate the <proxy Database> tag within the <http> tag.

   b. Add the following text with the <proxy Database> tag:

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

   c. Remove the following text:

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

   d. Restart the VMware Infrastructure SDK Management Service by executing the following command:

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

   Note: For more information, see the Virtual Infrastructure SDK documentation on the VMware website.

4. Install the Agent for Virtual Machines on the backup proxy system.

5. On the backup proxy system, specify temporary VM mount location. For more information, see Specify a Temporary VM Mount Location.

6. Execute the Arcserve VMware Configuration Tool to populate the Arcserve Backup database with information about your VMware environment.

   Important! The VMs in the VMware ESX Host system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the Arcserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

Configure VMware ESX Server 3.5 Systems

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

To configure VMware ESX Server 3.5 systems

1. Install VMware ESX Server 3.5. For more information about VMware ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your VMware ESX Host systems using VMware vCenter Server, you must install and configure VMware vCenter Server as part of Virtual Infrastructure installation.

2. Install VDDK 5.0 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.
   - When the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

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

   Note: To ensure VDDK 5.0 is installed correctly, it is required to manually change the registry key to point to the location where VDDK 5.0 was installed. See Using Different Versions of VDDK for VMware Backups for details.

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.

8. Execute the Arcserve VMware Configuration Tool to populate the Arcserve Backup database with information about your VMware environment.

   Important! The VMs in the VMware ESX Host system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the Arcserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

Configure VMware ESX Server 3i Systems

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

To configure ESX Server 3i systems

1. Install VMware ESX Server 3i. For more information about VMware ESX Server requirements, see the VMware ESX Server Installation guide on the VMware website.

   Note: To manage your VMware ESX Host systems through VMware vCenter Server, you must install and configure VMware vCenter Server as part of Virtual Infrastructure installation.

2. Install VDDK 5.0 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.
   - When the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

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

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.

10. Execute the Arcserve VMware Configuration Tool to populate the Arcserve Backup database with information about your VMware environment.

    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 Arcserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

For information about using vifs, see "Performing File System Operations with vifs" in the *ESX Server 3i Configuration Guide*.

For information about configuring ESX Server 3i security and using the Restart Management Agents operation, see the *ESX Server 3i Configuration Guide*.

Configure VMware vCenter Server 2.0.2 Systems

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

To configure VMware vCenter Server 2.0.2 systems

1. Install VMware VCenter Server. For more information about VMware vCenter Server requirements, see the VMware vCenter Server Installation guide on the VMware website.
2. Install VDDK 5.0 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.
   - When the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

     The LUN in the backup proxy system should not be signed.
3. To set up backing up VMs through a Backup Proxy and a VMware vCenter Server system, configure one of the following communication protocols:

   https

   To use https as the communication protocol between the VMware vCenter Server system and the backup proxy system, you must copy the self-generated SSL certificate from the VMware vCenter Server system to the backup proxy system, and then install the certificate on the backup proxy system.

You can access the SSL certificate (labeled rui.crt) from the following directory on the Vmware vCenter Server system:

C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\rui.crt

To install the SSL certificate, right-click the object and select Install from the pop-up menu.

http

To use http as the communication protocol between the backup proxy system and the VMware vCenter Server system, you must configure the http protocol on the VMware vCenter Server system as follows in the vpxd.cfg file located at

"C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\vpxd.cfg";

a. Locate the <proxy Database> tag within the <http> tag.

b. Add the following text with the <proxy Database> tag:

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

c. Remove the following text:

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

d. Restart the VMware vCenter Server service:

This can be done by from the Services Control Panel.

4. Restart the VMware vCenter Server service from the command line or from the Windows Services control panel.

5. Install the Agent for Virtual Machines on the backup proxy system.

6. On the backup proxy system, specify temporary VM mount location. For more information, see Specify a Temporary VM Mount Location.

7. Execute the Arcserve VMware Configuration Tool to populate the Arcserve Backup database with information about your VMware environment.

Important! The VMs in the Vmware vCenter Server system must be in a running state when you execute this utility. If the VMs are not in a running state, this utility will not populate the Arcserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

Configure VMware vCenter Server 2.5 Systems

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

To configure VMware vCenter Server 2.5 systems

1. Install VMware vCenter Server. For more information about VMware vCenter Server requirements, see the VMware vCenter Installation guide on the VMware website.
2. Install VDDK 5.0 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.
   - When the VM resides on a SAN LUN, the LUN must be shared between the VMware ESX Host system and the backup proxy system and have the same LUN number assigned.

     The LUN in the backup proxy system should not be signed.
3. To set up backing up VMs through a Backup Proxy and VMware vCenter Server system, configure one of the following communication protocols:

   https

   To use https as the communication protocol between the vCenter Server system and the backup proxy system, you must copy the self-generated SSL certificate from the vCenter Server system to the backup proxy system, and then install the certificate on the backup proxy system.

   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.

http

To use http as the communication protocol between the backup proxy system and the vCenter Server system, you must configure the http protocol on the vCenter Server system in the file that follows:

"C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\proxy.xml";

a. Open the file labeled proxy.xml using a text-editing application.

b. Navigate to the list of end points in the file (identified by the <EndpointList> tag) that contain the settings for the Web service supporting the SDK. The nested tags may appear as follows:

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

c. Change the accessMode to httpAndHttps.

4. Restart the VMware vCenter Server service from the command line or from the Windows Services control panel.

5. Install the 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.

7. Execute the Arcserve VMware Configuration Tool to populate the Arcserve Backup database with information about your VMware environment.

   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 Arcserve Backup database with information about the VMs. All the VMs must have a host name and IP address assigned and the latest VMware tools installed.

For more information, see the *Developer's Setup Guide for VMware Infrastructure SDK 2.5* on the VMware web site.

Configure HTTP Communication Protocol on vCenter Server Systems

By default, the backup proxy system and the vCenter Server systems communicate using HTTPS protocol. To specify an alternative protocol, you can configure the backup proxy system and the ESX/ESXi Server system to communicate using HTTP protocol.

Note: In addition to vCenter Server 4.0 systems, the following steps apply to vCenter Server 4.1 and vCenter Server 5.0/5.1 systems.

To configure HTTP communication protocol on vCenter Server systems

1. Log in to the vCenter Server system.

   Open the file that follows using a text editor:

   C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\proxy.xml";

   Find the list of endpoints that contain the settings for the web service supported by the SDK.

   Note: You can identify endpoints by the <EndpointList> tag.

   The nested tags appear as follows:

   ```
   <e id="5">
   <_type>vim.ProxyService.LocalServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <port>8085</port>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

2. Change the accessMode to the following:

   httpAndHttps

   Close and save proxy.xml.

3. Restart the vCenter Service from the command line or from the Windows Services control panel.

Configure HTTP Communication Protocol on ESX Server 4.0 Systems

By default, the backup proxy system and the ESX Server systems communicate using HTTPS protocol. To specify an alternative protocol, you can configure the backup proxy system and the ESX Server system to communicate using HTTP protocol.

Note: In addition to ESX Server 4.0 systems, the following steps apply to ESX Server 4.1 and ESX Server 5.0 and 5.1 systems.

To configure HTTP communication protocol on ESX Server 4.0 systems

1. Log in to the service console on the ESX Server system as the root user and change to the directory that follows:

   /etc/vmware/hostd

   Open proxy.xml using a text editor.

   Find the list of endpoints that contain the settings for the web service supported by the SDK.

   Note: You can identify endpoints by the <EndpointList> tag.

   The nested tags may appear as follows:

   ```
   <e id="5">
   <_type>vim.ProxyService.LocalServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <port>8307</port>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

2. Change the accessMode to the following:

   httpAndHttps

   Close and save proxy.xml.

3. Restart the vmware-hostd process using the command that follows:

   service mgmt-vmware restart

Configure HTTP Communication Protocol on vCenter Server 5.1 Systems

By default, the backup proxy system and the vCenter Server systems communicate using HTTPS protocol. To specify an alternative protocol, you can configure the backup proxy system and the ESX Server system to communicate using HTTP protocol.

Follow these steps:

1. Log in to the vCenter Server system and open the following file using a text editor:

   C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\proxy.xml";

2. Find the list of endpoints that contain the settings for the web service supported by the SDK.

   Note: You can identify endpoints by the <EndpointList> tag.

   The nested tags appear as follows:

   ```
   <e id="5">
   <_type>vim.ProxyService.LocalServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <port>8085</port>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

3. Change the accessMode to the following:

   httpAndHttps

4. Save and Close proxy.xml.

5. Restart the vCenter Service from the command line or from the Windows Services control panel.

Configure HTTP Communication Protocol on ESXi Server 5.1 Systems

By default, the backup proxy system and the ESX Server systems communicate using HTTPS protocol. To specify an alternative protocol, you configure the backup proxy system and the ESX Server system to communicate using HTTP protocol.

Follow these steps:

1. Log in to the service console on the ESXi 5.1 Server system as the root user

2. Change the directory to /etc/vmware/rhttpproxy

   Example: cd /etc/vmware/rhttpproxy

3. Open endpoints.conf using a text editor.
4. Find the tag for SDK.

   Note: The tag should appear as follows:

   /sdk local 8307 redirect allow

5. Change the redirect (accessMode) to allow (accessMode). The changes appear as follows:

   /sdk local 8307 allow allow

6. Save and Close endpoints.conf.
7. Restart the VMware Management Services. For information about restarting the management services, see Restarting the Management agents on an ESXi or ESX host on the VMware website.

Glossary

temporary mount location

The temporary mount location is a directory on a backup proxy system where Arcserve Backup temporarily stores VMware VM backup information while the Arcserve VMware Configuration Tool is running.

By default, Arcserve Backup stores the backup information in the following directory on the backup proxy system:

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

Optionally, you can change the location using the Backup Agent Admin.

VMware Virtual Disk Development Kit

VMware Virtual Disk Development Kit (VDDK) is a mechanism that lets you integrate Arcserve Backup VMware ESX/ESXi Server and VMware vCenter Server. VDDK lets you protect virtual machine files and data.

VMware vSphere

VMware vSphere is a virtualization tool kit that lets you integrate Arcserve Backup with the latest versions of VMware vCenter Server and VMware VDDK.

Index