

Virtual Machine Backup Guide

ESX Server 3.5, ESX Server 3i version 3.5

VirtualCenter 2.5

Virtual Machine Backup Guide

Revision: 20071129

You can find the most up-to-date technical documentation on our Web site at

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

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2007-2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, and 7,290,253; patents pending.

VMware, the VMware “boxes” logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book	7
1 Backing Up with VMware Infrastructure	11
Backup Concepts	12
What to Back Up	12
Virtual Machine Contents	13
Accessing and Managing Virtual Disk Files	14
Backup Components and Approaches	15
Using Traditional Backup Methods	16
Traditional Backup Considerations	16
Backing Up the ESX Server 3 Service Console	16
Backing Up Virtual Machines	17
Running the Backup Client in a Virtual Machine	17
Running the Backup Client in the ESX Server 3 Service Console	19
Running the Backup Server in a Virtual Machine	20
Treating Virtual Machines as Files on Shared Storage	21
Using VMware Consolidated Backup	22
2 VMware Consolidated Backup	23
VMware Consolidated Backup Overview	24
How VMware Consolidated Backup Works	24
VMware Consolidated Backup Usage Models	25
VMware Consolidated Backup Workflow	28
Types of Backups	29
Performing Image-Level Virtual Machine Backups	30
Performing File-Level Virtual Machine Backups	30
VMware Consolidated Backup Limitations	30
Consolidated Backup Software and Hardware Requirements	31
Setting Up VMware Consolidated Backup	32
Configuring VMware ESX Server and Virtual Machines to Back Up	32
Setting Up a VCB Proxy	33

	Configuring Windows on the VCB Proxy	34
	Configuring Networking on the VCB Proxy	35
	Configuring Third-Party Software on the VCB Proxy	35
	Installing VMware Consolidated Backup	36
	Installing a Backup Software Integration Module	36
	Configuring VMware Consolidated Backup	36
	Enabling SSL Certificate Verification	39
	Configuring SAN	41
	Using VMware Consolidated Backup	41
	Creating Backup Roles	42
	Grouping Virtual Machines	43
	Configuring Backup Jobs	43
	First-Time Backup	44
	Advanced Configurations	44
	Running Custom Quiescing Scripts	44
	Canceling a Backup Job	46
	Cleaning up After a Failed Backup Job	46
	Upgrading Consolidated Backup	47
3	Restoration and Disaster Recovery	49
	Restoring Virtual Machines Using VMware Consolidated Backup	50
	Using VMware Converter to Restore Virtual Machine Images	50
	Using the vcbRestore Utility to Restore Virtual Machines	51
	Centralized Restore	51
	Per-Group Restore	51
	Direct Restore to a Virtual Machine	52
	Data Recovery	52
4	Backup Scenarios and Troubleshooting	53
	Backup Usage Scenarios	54
	Typical Consolidated Backup Usage Scenario	54
	Troubleshooting	55
	Changing Backup Policies after ESX Server Upgrades	55
	Identifying VMFS Volumes in Backup GUI	55
A	Using Service Console to Back Up and Restore Virtual Machines	57
	General Configuration Settings for Consolidated Backup Utilities	58
	Configuration File Settings	58
	Backing Up Virtual Machines	60

Performing Backups	60
Identifying Virtual Machines	61
Identifying Virtual Machines by DNS Name or IP Address	61
Identifying Virtual Machines by BIOS UUID	62
Identifying Virtual Machines by MoRef	62
Displaying Virtual Machine Information	62
Specifying Backup Destinations	63
Backing Up to a Local Directory	63
Backing Up to a Remote Server	63
Archiving Virtual Machines	64
Restoring Virtual Machines	64
Restoring Virtual Machines to Original Locations	64
Restoring Virtual Machines to Alternative Locations	65
Copying a Catalog File	65
Editing a Catalog File	66
Restoring Virtual Machines Using an Alternate Catalog	67
Non-Interactive Use of the vcbRestore Utility	68
Restoring Virtual Machines from Archives	68
B Restoring Virtual Machines from ESX Server 2.5.x to ESX Server 3.x	69
Setting Configuration Parameters	70
Restoring ESX 2.5.x Server Virtual Machines	71
Index	73

About This Book

This manual, the *Virtual Machine Backup Guide*, provides information on different methods you can use to perform backup and restore tasks. It also describes how to set up and use VMware Consolidated Backup, a backup solution offered by VMware Infrastructure 3 and recommended to perform daily backups for virtual machines residing on a Fibre Channel or iSCSI SAN, or on a local store.

Virtual Machine Backup Guide covers both ESX Server 3.5 and ESX Server 3i version 3.5. For ease of discussion, this book uses the following product naming conventions:

- For topics specific to ESX Server 3.5, this book uses the term “ESX Server 3.”
- For topics specific to ESX Server 3i version 3.5, this book uses the term “ESX Server 3i.”
- For topics common to both products, this book uses the term “ESX Server.”
- When the identification of a specific release is important to a discussion, this book refers to the product by its full, versioned name.
- When a discussion applies to all versions of ESX Server for VMware Infrastructure 3, this book uses the term “ESX Server 3.x.”

Intended Audience

This manual is intended for anyone who wants to perform backup and restore tasks using VMware Infrastructure. The information in this manual is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to:

docfeedback@vmware.com

VMware Infrastructure Documentation

The VMware Infrastructure documentation consists of the combined VMware VirtualCenter and ESX Server documentation set.

Abbreviations Used in Figures

The figures in this manual use the abbreviations listed in [Table 1](#).

Table 1. Abbreviations

Abbreviation	Description
database	VirtualCenter database
datastore	Storage for the managed host
dsk#	Storage disk for the managed host
host <i>n</i>	VirtualCenter managed hosts
SAN	Storage area network type datastore shared between managed hosts
tplt	Template
user#	User with access permissions
VC	VirtualCenter
VM#	Virtual machines on a managed host

Technical Support and Education Resources

The following sections describe the technical support resources available to you. You can access the most current versions of this manual and other books by going to:

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

Online and Telephone Support

Use online support to submit technical support requests, view your product and contract information, and register your products. Go to

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

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

Find out how VMware support offerings can help meet your business needs. Go to <http://www.vmware.com/support/services>.

VMware Education Services

VMware courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. For more information about VMware Education Services, go to <http://mylearn1.vmware.com/mgreg/index.cfm>.

Backing Up with VMware Infrastructure

1

Backup, restoration, and disaster recovery are among the most critical processes of datacenter management. VMware® Infrastructure and VMware ESX Server provide many different solutions, each suitable for a specific environment, to perform backup and restore tasks.

This introduction describes which resources should be backed up on an ESX Server system and explains options available for that backup.

This chapter includes the following sections:

- [“Backup Concepts”](#) on page 12
- [“What to Back Up”](#) on page 12
- [“Backup Components and Approaches”](#) on page 15
- [“Using Traditional Backup Methods”](#) on page 16
- [“Using VMware Consolidated Backup”](#) on page 22

Backup Concepts

The following concepts are essential for your understanding of backup procedures:

- **Differential backup.** Backs up only those files that have changed since the last *full backup*.
- **File-level backup.** A type of backup that is defined at the level of files and folders.
- **Full backup.** Backs up all selected files.
- **Full virtual machine backup.** Backs up all files that comprise the entire virtual machine. These files include disk images, `.vmtx` files, and so on.
- **Image-level (volume-level) backup.** Backs up an entire storage volume.
- **Incremental backup.** Backs up only files that have changed since the last backup, whether it is a full or incremental backup.
- **Quiescing.** A process of bringing the on-disk data of a physical or virtual computer into a state suitable for backups. This process might include such operations such as flushing dirty buffers from the operating system's in-memory cache to disk, or other higher-level application-specific tasks.
- **VCB proxy.** In the context of VMware Consolidated Backup, VCB proxy is a physical or virtual machine running Microsoft Windows 2003, Consolidated Backup, and third-party backup software. Used to perform file-level and image-level virtual machine backups.

What to Back Up

Within the ESX Server environment, you need to back up the following major items:

- **Virtual machine contents.** The virtual machine data you back up can include virtual disks or Raw Device Mappings (RDMs), configuration files, and so on.

As with physical machines, you must back up virtual machine data periodically to prevent its potential damage and loss due to human or technical errors.

Generally, use the following backup schedule for your virtual machines:

- At the image level, perform backups periodically for Windows and nightly for Linux. For example, back up a boot disk image of a Windows virtual machine once a week.
- At the file level, perform backups once a day. For example, back up files on drives D, E, and so on every night.

For information on how to work with the files, see [“Accessing and Managing Virtual Disk Files”](#) on page 14.

- **Service Console** (ESX Server 3 only). The service console, a customized version of Linux, is the ESX Server 3 command-line management interface. It provides tools and a command prompt for more direct management of ESX Server 3. With the VI Client being the main interface to the ESX Server 3 host, use the service console to perform only advanced administration operations.

NOTE ESX Server 3i does not have a service console.

During its lifetime, the service console does not experience any major changes other than periodic upgrades. In case of a failure, you can recover the state of your service console by reinstalling ESX Server 3. If you decide to back up the service console, you do not need to back it up as frequently as the virtual machines and their data.

Virtual Machine Contents

To store virtual machines, ESX Server uses *VMware Virtual Machine File System (VMFS)*. VMFS is a high-performance file system on physical disks and LUNs capable of storing large files, such as the virtual disk images for ESX Server virtual machines and the memory images of suspended virtual machines.

For more information on VMFS, see *ESX Server 3 Server Configuration Guide* or *ESX Server 3i Configuration Guide*.

Since ESX Server 3.0, VMFS3 supports directories. Typically, a separate subdirectory is used for each virtual machine on VMFS. This directory contains all the files that comprise the virtual machine, such as `.vmdk` virtual disk files, virtual machine configuration `.vmx` files, log files, and so on.

NOTE All the information typically backed up in the enterprise infrastructure, including the operating system, applications, and data, is included in the virtual disks.

An alternative to a virtual disk is a raw device mapping (RDM) that connects your virtual machine to a raw SAN LUN. RDMs can exist in two modes, virtual compatibility and physical compatibility.

For more information on RDMs, see the *ESX Server 3 Server Configuration Guide* or *ESX Server 3i Configuration Guide*.

Accessing and Managing Virtual Disk Files

Typically, you use *VMware Infrastructure Client (VI Client)* to perform a variety of operations on your virtual machines.

Direct manipulation of your virtual disk files on VMFS is possible through service console (ESX Server 3) and command-line interface (ESX Server 3i), although using the VI Client is the preferred method.

From the service console or Remote Command-Line Interface (Remote CLI), you can view and manipulate files in the `/vmfs/volumes` directory in mounted VMFS volumes with ordinary file commands, such as `ls` and `cp`. The VMFS volume is primarily intended to store large files, such as disk images with the size of up to 2TB. You can use `ftp`, `scp`, and `cp` commands for copying files to and from a VMFS volume as long as the host file system supports these large files.

NOTE In Linux, importing a large disk from a Common Internet File System (CIFS) mount stalls the ESX Server host. If this happens, your host must be rebooted. Move large files from the service console to tape backup. To do this effectively, use supported programs with no known issues. As a workaround, use `smbclient` to copy the large file onto a local directory on the service console and import from there.

Additional file operations are enabled through the `vmkfstools` command. Use this command to perform the following:

- Creating, extending, and deleting disk images.
- Importing, exporting, and renaming disk images.
- Setting and querying properties of disk images.
- Creating and extending a VMFS file system.

For more information on the `vmkfstools` command, see the *ESX Server 3 Server Configuration Guide* or *ESX Server 3i Configuration Guide*.

Backup Components and Approaches

When you perform a backup, the following three components of backup software are involved in the process:

- **Backup Client (Backup Agent).** A program that scans virtual machine file systems and transfers data to be backed up to a backup server. During restore operations, the backup client writes the data into the file systems.
- **Backup Server.** A program that writes the data, pushed by the backup client, to a backup medium, such as a robotic tape library. During restore operation, the backup server reads the data from the backup medium and pushes it to the backup client.
- **Scheduler.** A program that allows you to schedule regular backup jobs and coordinate their execution. You can schedule backups at periodic intervals, or you can schedule individual files to be backed up immediately after they have been updated.

Each of the backup software components can be run in a virtual machine, on the service console (only with ESX Server 3), or on a VCB proxy running Microsoft Windows 2003. While the location of the scheduler is not important, the locations of the backup server and backup client are important.

Depending on where you want to run each component, choose one of the following approaches:

- **Traditional backup approach.** You deploy a backup client to every system that requires backup services. You can then regularly schedule automatic backups.

With this approach, several methodologies exist. Choose a method that better suits your needs and requirements.

See [“Using Traditional Backup Methods”](#) on page 16.

- **VMware Consolidated Backup.** If used with SAN storage, Consolidated Backup enables offloaded and impact-free backups for virtual machines running on ESX Server. This approach lets you use the virtual machine snapshot technology and SAN-based data transfer in conjunction with traditional file-based backup software. When running Consolidated Backup, you can back up virtual machine contents from a centralized Microsoft Windows 2003 backup proxy rather than directly from the ESX Server system. Utilizing a backup proxy reduces the load on ESX Server allowing it to run more virtual machines.

If you do not have SAN, you can use Consolidated Backup in the LAN mode. This mode lets you run Consolidated Backup on a physical machine connected to your

ESX Server system over regular TCP/IP network, or in one of the virtual machines on your ESX Server host.

See “[VMware Consolidated Backup](#)” on page 23.

Using Traditional Backup Methods

With the traditional backup methods, you deploy a backup agent on each host whose data needs to be protected. Regular backups are conducted automatically.

The backup agent scans the file system for changes during periods of low system utilization and sends the changed information across the network to a backup server that writes the data to a backup medium, such as a robotic tape library.

With the traditional methods, you can back up your virtual machines and, if you are using ESX Server 3, the service console.

Traditional Backup Considerations

When using traditional methods to back up your system, keep in mind the following:

- To be able to capture the data in its consistent state, perform backups at the times of the lowest activity on the network and when your computer resources are mostly idle. While performing backups, you might need to take critical applications off line.
- Make sure that network bandwidth between the server you are backing up and the backup server is sufficient.
- With a large number of servers, both physical and virtual, allocate enough resources to manage backup software on each host. Managing agents in every virtual machine is time consuming.

Backing Up the ESX Server 3 Service Console

Because the ESX Server 3 service console does not experience major changes during its lifetime and its state is easily recoverable in case of a failure, you might decide against backing it up. If you choose to back up the service console, you do not need to do it frequently.

Use the following methods when backing up service console:

- **File-Based.** Treat the service console as a physical machine with a deployed backup agent. To restore the service console, reinstall it, reinstall the agent, and then restore the files that you backed up. This approach makes sense if management agents that are hard to set up have been deployed in the service

console. Otherwise, this approach provides no advantage over not backing up the service console.

- **Image-Based.** Use third-party software to create a backup image that you can restore quickly. Use your boot CD or whatever the backup software created to restore the service console.

Backing Up Virtual Machines

Depending on your needs and available resources, you might choose one of the traditional methods for backing up your virtual machines. Traditional backup methods do not use Consolidated Backup.

Traditional backup methods offer the following options:

- Run backup clients from within a virtual machine performing file-level or image-level backups. As long as you are backing up over the network, no compatibility guide is needed. See [“Running the Backup Client in a Virtual Machine”](#) on page 17.
- Run backup clients from the ESX Server 3 service console, backing up virtual machines in their entirety as files residing in the VMFS file system. See [“Running the Backup Client in the ESX Server 3 Service Console”](#) on page 19.
- Back up virtual machine data by running a backup server within a virtual machine that is connected to a tape drive or other SCSI-based backup media attached to the physical system. See [“Running the Backup Server in a Virtual Machine”](#) on page 20.
- When virtual machine files reside on shared storage, use storage-based imaging on storage such as SAN, NAS, or iSCSI, or an independent backup server (a proxy backup server or NDMP) to back up virtual machine files. See [“Treating Virtual Machines as Files on Shared Storage”](#) on page 21.

NOTE Running the backup server in the ESX Server 3 service console is not supported.

Running the Backup Client in a Virtual Machine

Because a virtual machine is just a physical machine, you can back it up in the same manner as a physical machine, using backup software running inside a virtual machine.

Method 1 and Method 2 illustrate how you can install a backup agent within each virtual machine and back up data over the network to backup servers, deployed in other virtual machines or inside physical machines.

Method 1: Backup Server in a Virtual Machine

With this method, deploy your backup client in one virtual machine while the backup server is in another virtual machine. VMware recommends that you run both virtual machines on the same ESX Server system. In this case, data between the two virtual machines moves through the virtual Ethernet that connects these virtual machines, but does not have to be transferred over a physical Ethernet connection.

When you use Method 1, the backup agent performs quiescing of a virtual machine being backed up.

Method 1 is generally used for file-level backups of the data stored within the virtual machine's disk image.

Table 1-1. Backup Client in One Virtual Machine, Backup Server in Another Virtual Machine

Recommended:	When hardware for a VCB proxy or backup server isn't available
File-level restore:	Very easy
Full virtual machine restore:	No
Quiescing:	Excellent
Load on ESX Server:	Extremely high
LAN-free backup:	No
Manageability:	Very poor

Method 2: Backup Server in a Physical Machine

With Method 2, you deploy the backup client in a virtual machine while the backup server runs on a physical machine.

NOTE Instead of Method 2, consider using Consolidated Backup.

Use Method 2 for file-level backups of the data stored within the virtual machine's disk image.

Table 1-2. Backup Client in a Virtual Machine, Backup Server in a Physical Machine

Recommended:	VCB can be used instead
File-level restore:	Very Easy
Full virtual machine restore:	No
Quiescing:	Excellent
Load on ESX Server:	High
LAN-free backup:	No
Manageability:	Very poor

Running the Backup Client in the ESX Server 3 Service Console

Because an entire virtual machine is encapsulated in only a few files, you can treat virtual machines as files on an ESX Server 3 host and back up these files from the service console. As Method 3 and Method 4 illustrate, with this approach, you deploy your backup client in the service console and back up the files to backup servers, deployed in other virtual machines or inside physical machines.

When you run backup clients in the service console, do one of the following to perform a backup of your virtual machines:

- Power off your virtual machines.
- Use snapshots to backup running virtual machines.

Method 3: Backup Server in a Virtual Machine

With Method 3, you deploy the backup client in the ESX Server 3 service console while the backup server runs in the virtual machine.

NOTE Use Method 3 only when separate hardware for a VCB proxy or backup server is not available.

Method 3 is used to perform image-level backups or backups of entire virtual machines.

Table 1-3. Backup Client in a ESX Server 3 Service Console, Backup Client in a Virtual Machine

Recommended:	When hardware for a VCB proxy or backup server isn't available
File-level restore:	No
Full virtual machine restore:	Very easy
Quiescing:	Excellent
Load on ESX Server:	Extremely high
LAN-free backup:	No
Manageability:	Very poor

Method 4: Backup Server in a Physical Machine

With Method 4, you deploy the backup client in the ESX Server 3 service console while the backup server runs on a physical machine.

NOTE Instead of Method 4 consider using Consolidated Backup.

Method 4 is used to perform image-level backups.

Table 1-4. Backup Client in an ESX Server 3 Service Console, Backup Server in a Physical Machine

Recommended:	VCB can be used instead.
File-level restore:	No
Full virtual machine restore:	Very Easy
Quiescing:	Excellent
Load on ESX Server:	High
LAN-free backup:	No
Manageability/Scalability:	Very poor

Running the Backup Server in a Virtual Machine

You can back up virtual machine data by running a backup server within a virtual machine that is connected to a tape drive or other SCSI-based backup media attached to the physical system.

When using this method, keep in mind the following:

- VMware supports attaching SCSI drives to the ESX Server using Adaptec SCSI adapters. Using other adapters, such as LSI MPT-Fusion SCSI, is not supported.
- If you are using a tape drive library (versus using a stand-alone tape drive), the library must be multitarget, and not multi-LUN.
- Set the tape drive's virtual target ID in the virtual machine's configuration to be the same as the physical target ID.

For information on attaching a SCSI-based tape drive to your virtual machine, see *Basic System Administration*.

Treating Virtual Machines as Files on Shared Storage

When virtual machine files reside on shared storage, it is possible to use storage-based imaging on storage such as SAN, NAS, or iSCSI, or an independent backup server (a proxy backup server or NDMP) to back up virtual machine files without creating an additional load on the ESX Server host that runs the virtual machines.

SAN Backups

If your virtual disk files are stored on a SAN, use features supplied by your SAN vendor to create a copy of your production LUN containing all virtual disk files and then send these copies to your backup media. With this method, you do not have to use virtual machine snapshot functionality during the backup process because the SAN hardware provides the snapshot functionality.

When using SAN snapshots to back up your data, keep in mind the following:

- Some vendors support snapshots for both VMFS and RDMS. If both are supported, you can make either a snapshot of the whole virtual machine file system for a host, or make snapshots of individual virtual machines (one per disk).
- Some vendors support snapshots for a setup using RDMS only. If only RDMS are supported, you can make snapshots of individual virtual machines.

See your storage vendor's documentation for additional information. For more information on SAN, see the *Fibre Channel SAN Configuration Guide* or the *iSCSI SAN Configuration Guide*.

NFS Backups

If your virtual machines are stored on external network attached storage (NAS) systems using the NFS protocol, you can perform image-level backups of the virtual machines.

See your storage vendor documentation for additional information.

Using VMware Consolidated Backup

In a modern datacenter environment, performing traditional backups might cause problems, some of which are described in [“Traditional Backup Considerations”](#) on page 16. To avoid many of the problems, consider using VMware Consolidated Backup.

VMware Consolidated Backup addresses most of the problems you encounter when performing traditional backups. Consolidated Backup helps you to:

- Reduce the load on your ESX Server systems by moving the backup tasks to one or more dedicated backup proxies.

NOTE To take advantage of the Consolidated Backup offloading capabilities, you are required to use Fibre Channel or iSCSI SAN for your virtual machine data.

- Eliminate the need for a backup window by moving to a snapshot-based backup approach.
- Simplify backup administration by making optional the deployment of backup agents in each virtual machine you back up.
- Back up virtual machines regardless of their power state.

VMware Consolidated Backup

2

VMware Consolidated Backup is a backup solution offered by VMware Infrastructure 3. It is the recommended way to perform daily backups for virtual machines residing on a Fibre Channel or iSCSI SAN.

You can also use Consolidated Backup to backup virtual machines residing on ESX Server systems that do not have an access to shared storage.

This chapter includes the following information:

- [“VMware Consolidated Backup Overview”](#) on page 24
- [“Consolidated Backup Software and Hardware Requirements”](#) on page 31
- [“Setting Up VMware Consolidated Backup”](#) on page 32
- [“Using VMware Consolidated Backup”](#) on page 41
- [“Advanced Configurations”](#) on page 44
- [“Upgrading Consolidated Backup”](#) on page 47

VMware Consolidated Backup Overview

You use Consolidated Backup along with a third-party software to perform backups of virtual machine disks.

The following are the key features of Consolidated Backup:

- Most major backup applications integrate with Consolidated Backup providing you with a fast and efficient way of backing up data in virtual machines.
- Consolidated Backup eliminates a need for a backup agent in a virtual machine.
- Consolidated Backup can read virtual disk data directly from your SAN storage device using Fibre Channel or iSCSI, or use a network connection to an ESX Server host to access virtual disk data.
- When used to back up virtual machines residing on a storage device accessed over a network connection, Consolidated Backup can run in a virtual machine.
- When used with iSCSI, Consolidated Backup can run in a virtual machine.
- Consolidated Backup supports file-level full and incremental backups for virtual machines running Microsoft Windows operating system and image-level backups for virtual machines running any operating system.
- You can use Consolidated Backup with a single ESX Server host or with a VirtualCenter Management Server.

How VMware Consolidated Backup Works

Consolidated Backup consists of a set of utilities and scripts that work in conjunction with a third-party backup software. To ensure that Consolidated Backup works with the specific backup software, either VMware or your backup software vendor provide integration modules containing any required pre-backup and post-backup scripts.

The third-party software, integration module, and Consolidated Backup run on the VCB proxy, a physical or virtual machine that has Microsoft Windows operating system installed.

For specific versions of Microsoft Windows, see [“Configuring Windows on the VCB Proxy”](#) on page 34.

VMware Consolidated Backup Usage Models

To store and manage virtual disk files, ESX Server uses a variety of physical storage devices, including local disks, NAS storage, Fibre Channel SANs, or iSCSI SANs.

For more information on different types of storage, see *ESX Server 3 Configuration Guide* or *ESX Server 3i Configuration Guide*.

The type of storage device your ESX Server system has access to determines how you set up the VCB proxy and the transportation method Consolidated Backup uses to access virtual disk data.

VMware supports the following two modes of Consolidated Backup:

- SAN Mode (Fibre Channel and iSCSI)
- LAN Mode

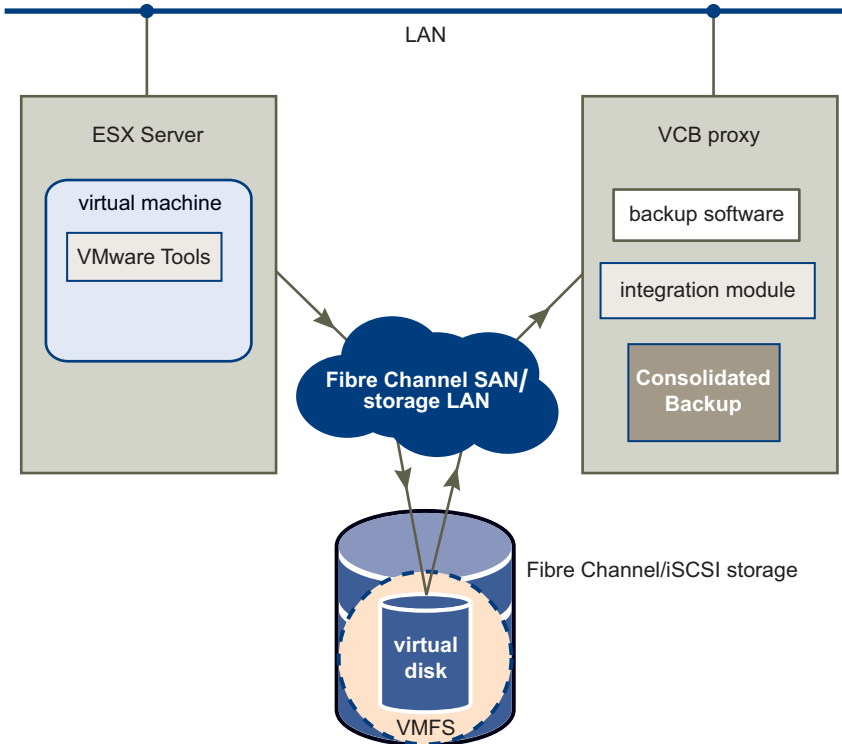
SAN Mode of Consolidated Backup

You select this mode when your ESX Server uses Fibre Channel SAN or iSCSI SAN to store its virtual machine disks.

In the SAN mode, Consolidated Backup reads virtual disk data directly from the shared Fibre Channel or iSCSI storage device, completely offloading backup processes from the ESX Server system to the VCB proxy.

Figure 2-1 illustrates how Consolidated Backup works in the SAN mode.

Figure 2-1. VMware Consolidated Backup in the SAN mode



LAN Mode of Consolidated Backup

You select this mode when your ESX Server does not have access to a SAN, but uses local storage devices or NAS to store its virtual machine disks.

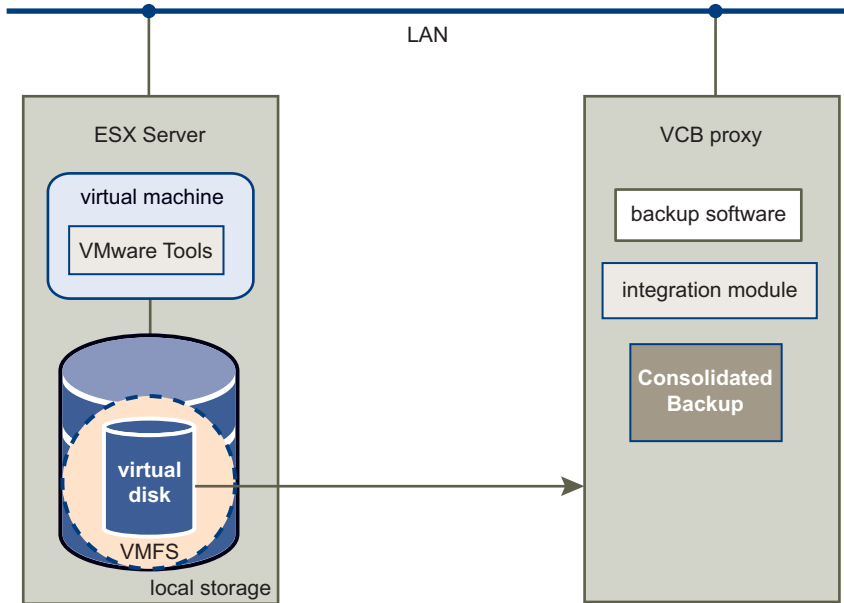
In this mode, Consolidated Backup uses an over-the-network protocol to access the virtual disk. The ESX Server host reads the data from the storage device and sends it across a network channel to the VCB proxy.

To be able to run Consolidated Backup in the LAN mode:

- You need to have ESX Server 3.5 or ESX Server 3i version 3.5.
- If you are using VirtualCenter, make sure to have version 2.5 installed.
- Your virtual disks cannot be larger than 1TB each.

Figure 2-2 illustrates how Consolidated Backup works in the LAN mode.

Figure 2-2. VMware Consolidated Backup in the LAN mode



Because the virtual disk data is transferred from the ESX Server host across the LAN, this mode does not provide the LAN-free capabilities of the SAN mode. However, running Consolidated Backup in the LAN mode offers you the following advantages:

- You are not required to store virtual disks on a SAN. You can use any storage device, including NAS, that ESX Server can access.
- You are not required to have a dedicated physical server for your VCB proxy. In addition to setting up a physical server as the VCB proxy, you have an option of configuring one of your virtual machines as the VCB proxy.

While this configuration does not completely off-load backup processes from the ESX Server host, it still has an advantage over using a backup agent in the service console or in the production virtual machine. You can use the advanced resource scheduling capabilities of VMware Infrastructure to prevent the virtual machine running your backups from impacting the performance of your production workloads. For example, you can put the virtual machine performing your backups and your production virtual machines in different resource pools. See the *Resource Management Guide*.

- If your ESX Server host and the VCB proxy are on a secure isolated network, you can use an unencrypted data transfer, which is faster and takes less resources of the ESX Server host and the proxy. When you need to protect sensitive information, you have an option of transferring virtual machine data in an encrypted form.

VMware Consolidated Backup Workflow

Before using Consolidated Backup, you need to configure and schedule a backup job for each virtual machine or a group of virtual machines.

At the scheduled time, the backup software starts the backup job on the VCB proxy. When the backup job is launched, the following steps take place:

- 1 The backup software calls the pre-backup script.

The pre-backup script performs these tasks:

- a (Optional) Runs your custom pre-freeze script in the virtual machine. The pre-freeze script prepares the critical software components in the virtual machine for backups. See [“Running Custom Quiescing Scripts”](#) on page 44.
 - b Quiesces NTFS and FAT file systems inside the virtual machine (only for virtual machines running 32-bit versions of Windows XP, Windows 2000, or Windows 2003). This ensures that no file system writes are pending at the time the snapshot is taken, allowing the creation of file-system consistent backups.
 - c Puts the virtual machine into snapshot mode, so that changes to its disks are stored for later writing. The virtual machine can continue to operate during this process.
 - d Unquiesces the NTFS and FAT file systems that were quiesced in [Step b](#).
 - e (Optional) Runs your custom post-thaw script in the virtual machine. The post-thaw script reverses any changes made by the pre-freeze script in [Step a](#).
 - f Makes the virtual machine snapshot available to the third-party software:
 - For image-level virtual machine backups, see [“Performing Image-Level Virtual Machine Backups”](#) on page 30.
 - For file-level backups of Microsoft Windows virtual machines, see [“Performing File-Level Virtual Machine Backups”](#) on page 30.
- 2 The backup software performs an ordinary backup of the virtual machine snapshot moving the data to a backup medium. The virtual machine can continue to operate during this process.

- 3 The backup software calls the post-backup script, which performs the following tasks:
 - a Unmounts the virtual machine snapshot from the backup proxy.
 - b Takes the virtual machine out of snapshot mode, committing to disk any changes made while the machine was in snapshot mode.

Types of Backups

Consolidated Backup supports image-level backups for virtual machines running any guest operating system and file-level backups for virtual machines running Microsoft Windows operating systems.

- **Image-level backup** allows backup clients to make a copy of all virtual disks and configuration files associated with a particular virtual machine. This type of backup is suitable for restoring an entire virtual machine in the event of a hardware failure or a system administrator error, such as the accidental deletion of the virtual machine.
- **File-level backup** allows backup clients to make copies of individual files contained within the virtual disks. File-level backups can be of the following types:
 - Full file backup — Backs up all files.
 - Differential backup — Backs up only files that have changed since the last full file backup.
 - Incremental backup — Backs up only files that have changed since the last backup, whether the last backup was full or incremental.

File-level backups allow files or directories to be restored individually. Use the file-level backups to prevent data loss due to user errors, such as accidental file deletion.

Performing Image-Level Virtual Machine Backups

An image-level virtual machine backup is operating-system neutral and can be performed regardless of the guest operating system.

When you run the image-level virtual machine backup, Consolidated Backup first creates a snapshot of your virtual machine. Then the following steps take place:

- 1 Consolidated Backup exports the virtual machine snapshot to a local directory on the VCB proxy. For example:

```
C:\mnt\mytestvm.foo.com-fullVM
```

- 2 The third-party backup software picks up the virtual machine disk images and configuration files and moves them to the backup medium.

Performing File-Level Virtual Machine Backups

For virtual machines running Windows, Consolidated Backup supports file-level backups.

When you run file-level backups, you first create a snapshot of your virtual machine. Then the following steps take place:

- 1 Consolidated Backup discovers volumes within virtual machine snapshots and mounts discovered volumes on the VCB proxy at predefined junction points.

Each junction point corresponds to a drive letter assigned to each volume in the virtual machine. For example:

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



CAUTION Because the VCB proxy can recognize only volumes that have drive letters assigned to them, make sure that each volume on a virtual disk has a drive letter.

- 2 The third-party backup software makes file-level backups from these volumes.

VMware Consolidated Backup Limitations

Under certain circumstances, you cannot use Consolidated Backup for backing up data in a virtual machine.

- Consolidated Backup in SAN mode cannot back up virtual machines with disk images stored on a storage device that the VCB proxy cannot access.
- Consolidated Backup cannot back up RDMS in physical compatibility mode.

- Consolidated Backup cannot perform file-level backups of virtual machines running operating systems other than Microsoft Windows.
- You cannot use Consolidated Backup to backup virtual machines in a cluster. These virtual machines share an SCSI controller and snapshot operations cannot be performed on them.

If you are unable to use Consolidated Backup, deploy a backup agent in the virtual machine and perform the backup from within the virtual machine. The backup agent is supplied by your third-party backup software vendor.

For details on installation of the backup agent, refer to the documentation provided with the integration module matching your backup software.

Consolidated Backup Software and Hardware Requirements

Whether you plan to use Consolidated Backup in the SAN or LAN mode, general requirements for Consolidated Backup include:

- A single ESX Server system and the VI Client, or multiple ESX Server systems and VirtualCenter to manage them.

NOTE To use Consolidated Backup in the LAN mode, make sure to upgrade your ESX Server to version 3.5 and your VirtualCenter to version 2.5.

- Backup hardware, such as a tape system.
- The following versions of Microsoft Windows operating system to install on your VCB proxy:
 - Microsoft Windows Server 2003 Service Pack 1 (32-bit or 64-bit)
 - Microsoft Windows Server 2003 R2 (32-bit or 64-bit)
 - Microsoft Windows Server 2003 Service Pack 1 (32-bit or 64-bit) ([SEE UPDATE](#))
- Backup software that supports Consolidated Backup. For a list of supporting third-party backup packages, see the *VMware Infrastructure 3 Backup Software Compatibility Guide*.

NOTE If you use Consolidated Backup in conjunction with a VMware supported third party software, make sure that the versions of Microsoft Windows and your backup software match. For example, if you run the 64-bit version of Microsoft Window, install the 64-bit version of the backup software.

- Network adapter (NIC).

To use Consolidated Backup in the SAN mode, additional requirements include:

- Fibre Channel or iSCSI SAN storage hosting virtual machines data you plan to back up.
- If you use Fibre Channel SAN, a dedicated physical system for a VCB proxy with a Fibre Channel host bus adapter (HBA) installed.

Setting Up VMware Consolidated Backup

Follow these steps to configure all the components that work with Consolidated Backup:

- 1 Configure your ESX Server or multiple servers. See [“Configuring VMware ESX Server and Virtual Machines to Back Up”](#) on page 32.
- 2 Set up your VCB proxy and install your backup software, Consolidated Backup, and corresponding integration module on the VCB proxy. See [“Setting Up a VCB Proxy”](#) on page 33.
- 3 If needed, enable SSL certificate verification. See [“Enabling SSL Certificate Verification”](#) on page 39.
- 4 If you use SAN, configure your SAN fabric. See [“Configuring SAN”](#) on page 41.

Configuring VMware ESX Server and Virtual Machines to Back Up

You should have an existing ESX Server host or multiple ESX Server hosts and VirtualCenter to manage them.

Using VI Client, configure storage for your ESX Server and create virtual machines. The following are requirements for Consolidated Backup to run successfully:

- Virtual machines you are planning to back up have their virtual disks on VMFS datastores created on local storage, or on iSCSI or FC SAN. Virtual machines can also use RDMS in virtual compatibility mode. Consolidated Backup does not support RDMS in physical compatibility mode.
- If you plan to use Consolidated Backup in the LAN mode, the size of your virtual disk files should not exceed 1TB.
- A latest version of VMware Tools is installed in each virtual machine you are planning to back up. Without VMware Tools, the snapshots that Consolidated

Backup creates for backups are crash-consistent only. That is, no file system synchronization is performed.

- For file-level backups, your virtual machines run Microsoft Windows NT 4.0, Windows 2000, Windows XP, Windows XP Professional, Windows 2003, Windows Vista, or Windows Server 2008 (“Longhorn Server”) operating systems.

Image-level virtual machine backups are supported for all guest operating systems.

For more information on configuring storage and RDMS, see the *ESX Server 3 Configuration Guide* or *ESX Server 3i Configuration Guide* at www.vmware.com.

For information on creating virtual machines and installing VMware Tools, see *Basic System Administration* at www.vmware.com.

Setting Up a VCB Proxy

The VCB proxy is a machine that runs Consolidated Backup, your third-party backup software, and an integration module for the backup software. Depending on the type of storage you use to store your virtual machine data, requirements for your VCB proxy differ:

- With FC SAN storage, you are required to have a dedicated physical server for your VCB proxy. See “[Consolidated Backup Software and Hardware Requirements](#)” on page 31 for additional hardware requirements for your VCB proxy.
- With iSCSI storage, and with any type of storage that supports NBD format including your ESX Server host’s local storage, you are not required to use a physical server. You have an option of configuring one of your virtual machines to work as the VCB proxy.

Whether your VCB proxy is a physical or a virtual machine, follow these steps to configure it.

To configure your VCB proxy

- 1 On the VCB proxy, install and configure Microsoft Windows. See “[Configuring Windows on the VCB Proxy](#)” on page 34.
- 2 Configure networking on the VCB proxy. See “[Configuring Networking on the VCB Proxy](#)” on page 35.
- 3 Install and configure the third-party backup software to be used with Consolidated Backup. See “[Configuring Third-Party Software on the VCB Proxy](#)” on page 35.

- 4 Install Consolidated Backup. See [“Installing VMware Consolidated Backup”](#) on page 36.
- 5 Install an integration module corresponding to your third-party backup software. See [“Installing a Backup Software Integration Module”](#) on page 36.
- 6 Configure Consolidated Backup. See [“Configuring VMware Consolidated Backup”](#) on page 36.

Configuring Windows on the VCB Proxy

On your VCB proxy, install a supported version of Microsoft Windows. See [“Consolidated Backup Software and Hardware Requirements”](#) on page 31.

All versions of Windows, except Windows 2003 Enterprise Edition and Windows 2003 Datacenter Edition, assign drive letters to each visible new technology file system (NTFS) and file allocation table (FAT) volumes. To be able to use Consolidated Backup, you need to clear any unused drive letter assignments.



CAUTION If you do not perform this configuration step, data corruption for virtual machines using RDM can occur.

To disable assignment of drive letters

- 1 Shut down the VCB proxy.
- 2 Disconnect the VCB proxy from the SAN or mask all the LUNs containing VMFS volumes or RDMs.
- 3 Boot the proxy and log in as administrator.
- 4 Open a command-line interface.
- 5 Run the Diskpart utility by typing:

```
diskpart
```

The Diskpart utility starts up and prints its own command prompt.
- 6 Disable automatic drive-letter assignment to newly seen volumes by typing at the Diskpart command prompt:

```
automount disable
```
- 7 Clean out entries of previously mounted volumes in the registry by typing at the Diskpart command prompt:

```
automount scrub
```

- 8 Exit the Diskpart utility by typing:

```
exit
```
- 9 Shut down Windows.
- 10 Reconnect the VCB proxy to the SAN, or unmask all previously masked LUNs containing either VMFS volumes or RDMS.
- 11 Boot the proxy.

Configuring Networking on the VCB Proxy

Your VCB proxy needs to establish a connection to VirtualCenter managing your ESX Server cluster or to a single ESX Server system if you do not have a cluster.

To configure networking for your VCB proxy, follow these guidelines:

- If there is a firewall between the VCB proxy and the VirtualCenter, the firewall must permit TCP/IP connections to VirtualCenter. By default, VirtualCenter expects incoming connections at TCP/IP port 443.
- Establish TCP/IP connections to port 902 for all ESX Server hosts that run virtual machines you plan to back up from the VCB proxy.

For more information on configuring Networking, see the *ESX Server 3 Configuration Guide* or *ESX Server 3i Configuration Guide*.

Configuring Third-Party Software on the VCB Proxy

The third-party backup software that you use in conjunction with Consolidated Backup runs on the VCB proxy.

After you install the backup software, you need to configure it, so it is able to use the Consolidated Backup scripts and utilities.

To configure your backup software, follow directions that your vendor provides.

For any specific requirements and instructions, consult the `README.html` file included in the integration module that corresponds to your backup software. You might be required to do the following for your backup software:

- Turn on the cross junctions (mount points) option for your backup software.
- Turn off the Windows archive bit and change journal functions if your third-party backup software performs incremental or differential backups. Both functions require the backup software to alter the file system being backed up, which is not possible in a snapshot-based backup.

- Windows archive bit. The archive bit is an attribute of a file that some backup products use to determine whether the file has changed since its previous backup and whether it should be backed up. Configure the backup client to use time stamps instead.
- Windows change journal cannot be used for incremental backups in snapshot-based backup scenarios.

After you install and configure your third-party backup software, you can verify it by running a backup and restoration job on a local directory on the VCB proxy.

Installing VMware Consolidated Backup

Install Consolidated Backup base package on the VCB proxy.

To install the basic Consolidated Backup

- 1 Log in to the VCB proxy using an account with administrator privileges.
- 2 Install the Consolidated Backup package by running `setup.exe` from your CD-ROM or electronic distribution.
- 3 During the installation, choose an installation directory for Consolidated Backup or accept the default one.

Installing a Backup Software Integration Module

On the VCB proxy, you must install a Consolidated Backup integration module that matches your third-party backup software. For each supported third-party backup software, either the backup software vendor or VMware provides an integration module.

Integration modules provided by VMware are distributed as ZIP files. Unpack the ZIP file into your VMware Consolidated Backup installation directory. This will create a subdirectory containing a `README.html` file that describes how to install the integration module. In addition, the `README.html` file provides any specific instructions you need to configure your backup software for Consolidated Backup.

Configuring VMware Consolidated Backup

Essential configuration for Consolidated Backup is stored in a configuration file called `config.js`. It is located in a subdirectory named `config` in the following default installation directory for Consolidated Backup:

```
C:\Program Files\VMware\VMware Consolidated Backup Framework
```

When configuring Consolidated Backup, make sure to specify all options in the `config.js` file that don't have any default values.

[Table 2-1](#) provides an overview of all the configuration settings in this file.

Table 2-1. Consolidated Backup Configuration Settings

Option	Default	Description
BACKUPROOT	C:\mnt	<p>Directory in which all the virtual machine backup jobs reside.</p> <p>For each backup job, a directory with a unique name derived from the backup type and the virtual machine name is created here.</p> <p>Make sure this directory exists before you try virtual machine backups.</p> <p>For image-level virtual machine backups, the volume containing this mount point must be large enough to hold the exported disk images of the largest virtual machine to be handled.</p>
HOST	(no default)	Host name of the VirtualCenter server or the ESX Server host used by the VCB proxy.
PORT	443	Port number to connect to the VirtualCenter or ESX Server host.
USERNAME	(no default)	User ID to be used for logging in to the VirtualCenter host or ESX Server host.
PASSWORD	(no default)	Password to be used for logging in to the VirtualCenter host or ESX Server host.
TRANSPORT_MODE	san	<p>Determines how VCB accesses virtual disk data. For information on the two modes of Consolidated Backup, see “VMware Consolidated Backup Usage Models” on page 25.</p> <p>The following options exist:</p> <ul style="list-style-type: none"> ■ san – Back up virtual disk files residing on a shared Fibre Channel or iSCSI storage device. ■ Use one of the following options to back up virtual disk files residing on a storage device accessed through the Network Block Device (NBD) protocol. Also, use one of these options to enable Consolidated Backup inside a virtual machine that serves as a VCB proxy. <ul style="list-style-type: none"> ■ nbd – Select if you do not need to encrypt virtual disk data. ■ nbdssl – Select to encrypt virtual disk data for over-the-network transfers. Also, you may want to enable SSL certificate verification. See “Enabling SSL Certificate Verification” on page 39.

Table 2-1. Consolidated Backup Configuration Settings (Continued)

Option	Default	Description
SNAPSHOT_POLICY	automatic	<p>Valid options:</p> <ul style="list-style-type: none"> ■ automatic: Consolidated Backup creates and deletes backup snapshots for virtual machines on demand. ■ manual: Consolidated Backup does not create or delete any snapshots but detects a backup snapshot named <code>_VCB_BACKUP_</code> and uses this snapshot for backup. This option is useful for creative scripting. ■ createonly: Consolidated Backup creates a backup snapshot when the pre-backup script is being run, but it does not remove the snapshot after backup. This option is used to run a verification job. Your verification script would be responsible for tearing down the mount. ■ deleteonly: Consolidated Backup detects that a backup snapshot named <code>_VCB_BACKUP_</code> exists and does not attempt to create one. However, the snapshot is deleted by the post-backup script. This option is useful for creative scripting.
VM_LOOKUP_METHOD	ipaddr	<p>Use one of the following options to specify how Consolidated Backup identifies virtual machines:</p> <ul style="list-style-type: none"> ■ ipaddr: Identifies virtual machines based on DNS name/IP address. ■ name: Identifies virtual machines based on names as shown in VirtualCenter. Use this option if you have multiple virtual machines with the same IP address, but with different names. Each virtual machine must have a unique name, otherwise a backup job fails.
PREEXISTING_MOUNTPOINT	fail	<p>Use one of the following options to specify whether a backup job should proceed or fail if Consolidated Backup discovers a preexisting mount point for a virtual machine:</p> <ul style="list-style-type: none"> ■ fail: Instructs Consolidated Backup to fail the backup job. ■ delete: Instructs Consolidated Backup to remove the preexisting mount point and backup snapshots associated with it. <p>If this operation is successful, the backup job proceeds. If this operation fails, the backup job fails.</p>

Table 2-1. Consolidated Backup Configuration Settings (Continued)

Option	Default	Description
PREEXISTING_VCB_SNAPSHOT	fail	<p>Use one of the following options to specify whether a backup job should proceed or fail if Consolidated Backup discovers a preexisting backup snapshot of a virtual machine:</p> <ul style="list-style-type: none"> ■ fail: Instructs Consolidated Backup to fail the backup job. ■ delete: Instructs Consolidated Backup to remove the preexisting backup snapshot. If this operation is successful, the backup job proceeds. If this operation fails, the backup job fails as well.
MAX_RETRIES	0	The number of times to retry an operation after it fails. Use this option if multiple backup jobs fail with resource busy errors.
BACKOFF_TIME	10 seconds	The time interval (in seconds) between retrials of a failed operation. This setting is valid only when MAX_RETRIES is larger than 0.

Enabling SSL Certificate Verification

When Consolidated Backup communicates with the VirtualCenter server or ESX Server host, it can transfer data over an encrypted SSL connection or use an unencrypted network channel.

Use unencrypted channel only if you create a trusted environment with fully isolated transmissions between your ESX Server host and VCB proxy. Disabling SSL can improve performance because you avoid the overhead required to perform encryption.

However, to secure the communication channel and prevent potential man-in-the-middle attacks, enable the SSL certificate verification in your Consolidated Backup environment. The SSL certificate verification is not enabled by default.

NOTE You can use the SSL certificate verification only with ESX Server 3.5 and ESX Server 3i version 3.5. Enabling the SSL certificate verification in a mixed environment, for example, when you run ESX Server 3.0.x and ESX Server 3.5, can cause backup operations to fail.

For the SSL certificate verification to succeed, the host name on the certificate must match the current fully-qualified domain name of the host that presents the certificate. If you use the default self-signed certificate, these names do not match and the certificate verification fails. To address this issue, add a certificate that is signed by a

recognized certificate authority. See the *Replacing VirtualCenter Server Certificates* white paper.

To enable SSL certificate verification on a VCB proxy

- 1 Using the Microsoft Registry Editor (`regedit.exe`), locate the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Consolidated Backup
- 2 Make sure that the DWORD entry with the following name is present. Otherwise, create a new one.
VerifySSLCertificates
- 3 To enable SSL certificate verification, set the value for this entry to 1.
- 4 Connect to your ESX Server host or VirtualCenter server through the VI Client, entering the names exactly as you specified in the `config.js` file, the Consolidated Backup configuration file.

If your ESX Server host or VirtualCenter server use the default self-signed certificate, you will receive a security alert asking you to verify the SSL thumbprint.

- 5 After verifying the thumbprint, click Yes to add the certificate to the Windows certificate store.

You can also enable the SSL certificate authentication for the ESX Server 3 command line utilities on the service console.

To enable SSL certificate verification on an ESX Server 3 service console

- 1 Obtain the thumbprint of the ESX Server host by entering the following command on the service console:

```
openssl x509 -noout -in /etc/vmware/ssl/rui.crt -fingerprint -sha1
```
- 2 Open the `/etc/vmware/backuptools.conf` file in an editor.
- 3 Set `HOST_THUMBPRINT` to the thumbprint of the ESX Server host.

The thumbprint is case-sensitive and you must enter it in the exact same way as displayed. The format of the thumbprint is `XX:XX:XX:XX:XX:...`, where `XX` are hexadecimal digits.

Configuring SAN

If you are using SAN to store your virtual machine data, configure the SAN fabric to which both the ESX Server and the VCB proxy are connected.

For Consolidated Backup, your SAN configuration must meet the following requirements:

- The VCB proxy has a read-write access to the SAN LUNs that contain either VMFS volumes (datastores) with virtual disks, or virtual compatibility RDMs you plan to back up. Do this by adding the VCB proxy to the same fabric zones where the ESX Server system belongs.
- The host mode (connection type) settings on the VCB proxy and on the ESX Server match. For example, if you have an IBM array and the host mode setting is LNXCL, set the same for the VCB proxy.

See documentation provided by your SAN storage array and switch vendors, as well as the *Fibre Channel SAN Configuration Guide* and *iSCSI SAN Configuration Guide*.

Using VMware Consolidated Backup

Because Consolidated Backup works in conjunction with a third-party software, details on how you use Consolidated Backup depend on the specific software. Refer to a `README.html` file that comes with your backup software integration module.

Follow these guidelines when using Consolidated Backup:

- If you are running a VirtualCenter version earlier than 2.5, create a backup role and assign backup privileges to this account. See [“Creating Backup Roles”](#) on page 42.
- If you have multiple virtual machines to back up, group these virtual machines and manage that group as a single entity in your backup software by configuring DNS aliases for the proxy. See [“Grouping Virtual Machines”](#) on page 43.

NOTE Consolidated Backup supports a maximum of 60 concurrently mounted virtual machines. For example, you can concurrently mount 60 virtual machines that have a C: drive, or 30 virtual machines that have a C: and a D: each.

- After you have associated a group of virtual machines with one host name, you can set up a backup job for each alias using the alias as the client name for the job. See [“Configuring Backup Jobs”](#) on page 43.
- When you perform a first backup for a particular virtual machine, power on this virtual machine. See [“First-Time Backup”](#) on page 44.

NOTE You cannot use Consolidated Backup to backup virtual machines in a cluster. These virtual machines share an SCSI controller and snapshot operations cannot be performed on them.

Creating Backup Roles

In VirtualCenter 2.5, use a predefined role called VMware Consolidated Backup User. If you are running an earlier version of VirtualCenter, create a new role with the backup privileges.

To create a VCB role

- 1 Log on to the VI Client as a user with Administrator privileges.
- 2 From the VI Client, click **Administration** in the navigation bar.
- 3 Click the **Roles** tab.
- 4 Click **Add Role**.
The Add Role dialog box appears.
- 5 Type a name for the new role, for example, VMware Consolidated Backup User.
- 6 Select the following privileges for the new role. Click the plus (+) signs to expand the lists, as needed.
 - VirtualMachine > Configuration > Disk Lease
 - VirtualMachine > State > Create Snapshot
 - VirtualMachine > State > Remove Snapshot
 - VirtualMachine > Provisioning > Allow Virtual Machine Download
 - Virtual Machine > Provisioning > Allow Read-only Disk Access
- 7 Click **OK** to complete the process.

After you create the backup role, associate a specific user with this role and specify the user name and password in the VCB configuration file. See [“Configuring VMware Consolidated Backup”](#) on page 36.

Grouping Virtual Machines

If you have multiple virtual machines to back up, assign the virtual machines to groups and set up different aliases for the groups, all pointing to the same IP address of the VCB proxy.

For example, you can create separate groups for virtual machines belonging to the Accounting, Engineering, and Marketing departments of your company, assign the following aliases, and manage each group as a single entity in your backup software:

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

Setting up different aliases lets you:

- Associate different permissions with each group of virtual machines. For example, Accounting, Engineering, and Marketing groups can each have their own set of permissions that might grant backup and restore privileges to different users.
- Easily move a group of virtual machines to a different proxy. For example, if your datacenter grows, you can add a new proxy and move jobs for the group by pointing the alias to the new proxy.

Configuring Backup Jobs

The rules that your backup software follows when backing up virtual machines are organized into backup jobs. Backup jobs describe the process of backing up virtual machine data and include choosing a name for the backup process to distinguish it from other jobs, selecting the files for backing up, choosing backup type, setting up the schedule, and so on.

Directions to configure backup jobs for your virtual machines are different for each software. Refer to the `README.html` file provided with the integration module for your third-party backup software.

When configuring backup jobs, follow these directions:

- Assign all jobs to the VCB proxy.
- Use aliases as the names for the jobs.
- Specify all jobs with one of the following directories:
 - file-level: `C:\mnt\mytestvm.foo.com\letters\D`
 - image-level: `C:\mnt\mytestvm.foo.com-fullVM`

- Schedule each job to run at specific time.
- If you run multiple backup jobs on the same VCB proxy at the same time, remember that backup products might have limitations on a number of jobs you can run in parallel.

NOTE You cannot perform a file-level backup simultaneously with an image-level backup for the same virtual machine.

First-Time Backup

When you perform a first backup for a virtual machine, the virtual machine has to be powered on, otherwise the backup fails.

NOTE You do not need to power on a virtual machine if your integration module is configured to use virtual machine display names instead of IP addresses or DNS names.

After you have completed the first backup of the virtual machine, Consolidated Backup can perform backups of the virtual machine regardless of its power state at backup time.

Advanced Configurations

You might need to perform advanced configurations when using Consolidated Backup. For example, you can run custom scripts to create a quiescent snapshot of your virtual machine. Also, you might need to run a post-backup command for your virtual machines to cancel backup jobs.

Running Custom Quiescing Scripts

When you use Consolidated Backup, your virtual machines are quiesced when you start the backup process.

You can also run custom pre-freeze and post-thaw quiescing scripts to create a quiescent snapshot of your virtual machine. For example, use the scripts to achieve application-consistent backups in Windows virtual machines. Deploy and run the custom quiescing scripts inside the protected virtual machine.

When running the scripts, you can use the SYNC driver, an optional feature that you can install when installing VMware Tools. If installed, the SYNC driver holds incoming I/O and flushes all dirty data to a disk, making file systems consistent.

Keep in mind the following:

- Creating quiesced snapshots using the SYNC driver requires waiting for I/O to drain in the guest operating system. This might affect time-sensitive applications, such as DBHammer.
- If you do not install the SYNC driver when installing VMware Tools, you can avoid the delay caused by the I/O draining. However, your snapshots will be crash-consistent only, unless you provide custom quiescing through pre-backup and post-backup scripts in the guest.

The SYNC driver is supported only on the 32-bit versions of Windows XP, Windows 2000, and Windows 2003. Because it is not supported on Windows NT 4.0 or Windows Vista guest operating systems, file system consistency is not guaranteed in virtual machines that run these guest operating systems.

When running the scripts, Consolidated Backup performs the following steps:

1 Runs the pre-freeze script within the virtual machine being backed up:

- For Windows:

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

- For all other operating systems:

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

If the pre-freeze script returns a nonzero exit code, the snapshot create operation fails.

2 (Optional) Engages the SYNC driver.

If this step fails, Consolidated Backup proceeds to [Step 5](#).

3 Creates a snapshot.

4 Disengages the SYNC driver.

Disengage the SYNC driver to allow I/O again. This step can fail if the snapshot creation in [Step 3](#) took too long and timed out.

5 Runs the post-thaw script within the virtual machine:

- For Windows:

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

- For all other operating systems:

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

If successful, the exit status of this script is 0.

Canceling a Backup Job

If a backup operation is canceled from your third-party software while the backup is in process, the virtual machine might not be unmounted from the backup proxy, and the snapshot might not be deleted. This is expected because the cleanup script was unable to run. To fix the problem, you must manually run the post-backup command for each virtual machine. As an alternative, run `vcbCleanup` as described in [“Cleaning up After a Failed Backup Job”](#) on page 46.

To run the post-backup command

- 1 Check the folders in the `C:\mnt` directory to determine the virtual machine host names.
- 2 For each virtual machine host name, run the following command from the `generic` subdirectory in the Consolidated Backup installation directory.

```
cscript /nologo post-command.wsf <VCB installation path ["C:\Program
Files\VMware\VMware Consolidated Backup Framework"]
<virtual_machine_hostname>>
```

Cleaning up After a Failed Backup Job

When you use Consolidated Backup with a VMware-provided integration module to perform file-level virtual machine backups, after completing the backup, a backup software calls the post-backup script to unmount the virtual machine snapshot from the backup proxy and take the virtual machine out of snapshot mode.

However, if a backup job fail, some backup applications never run the post-backup script. As a result, virtual machines can still remain mounted and in the snapshot mode at the end of the backup cycle.

To clean up snapshots and unmount virtual machines from the directory specified in `BACKUPROOT` of the `config.js` file, run `vcbCleanup` at the end of your backup cycle.



CAUTION Do not run `vcbCleanup` while backups are still in progress on the VCB proxy. This can cause currently running backups to fail.

You can run `vcbCleanup` interactively, without a command option. If you enter the `-y` option, the utility performs the cleanup without your interaction. This allows you to automate cleaning up after a backup cycle.

Upgrading Consolidated Backup

When you upgrade Consolidated Backup from its earlier versions, perform the following procedure on the VCB proxy.

To upgrade to VMware Consolidated Backup version 1.1

- 1 Upgrade to the latest Consolidated Backup version by running the VMware Consolidated Backup 1.1 installer.
- 2 Open Command Prompt and enter `net stop vmount2` to stop any running vmount services.
- 3 Run the Diskpart utility and issue the `automount scrub` command to remove registry settings for any previously mounted virtual machines.

For instructions on how to run Diskpart, see [“To disable assignment of drive letters”](#) on page 34.

- 4 Clean the `C:\Windows\Temp` directory to remove any accumulated temporary files.

Restoration and Disaster Recovery

3

This chapter describes how to restore your data or recover from a disaster. You need to find a balance between the number of agents that you want to use and the ease with which you can restore your data.

This chapter includes the following information:

- [“Restoring Virtual Machines Using VMware Consolidated Backup”](#) on page 50
- [“Data Recovery”](#) on page 52

Restoring Virtual Machines Using VMware Consolidated Backup

Consolidated Backup helps you perform an image-level restoration of entire virtual machines and file-level restoration of the data or files from inside a virtual disk.

For specific restoration instructions, consult the documentation that comes with the integration module for your backup software.

VMware supports the following restoration processes:

- Image-level restoration
 - Restore a VCB image of your virtual machine using VMware Converter. See [“Using VMware Converter to Restore Virtual Machine Images”](#) on page 50.
 - (ESX Server 3 only) Restore your virtual machine using the command-line `vcbRestore` utility. See [“Using the vcbRestore Utility to Restore Virtual Machines”](#) on page 51.
- File-level restoration
 - No backup software in the virtual machine. Restoration is done by the administrator on a backup proxy network share that is accessible by the protected virtual machine. See [“Centralized Restore”](#) on page 51
 - Backup software in dedicated virtual machines and data moved to target virtual machines. See [“Per-Group Restore”](#) on page 51.
 - Backup software deployed in every protected virtual machine. Restoration is done directly by the system administrator or the user. See [“Direct Restore to a Virtual Machine”](#) on page 52.

Using VMware Converter to Restore Virtual Machine Images

You can use VMware Converter version 3.0.1 and later to restore VCB images of virtual machines to running virtual machines. Using the VMware Converter, integrated into VirtualCenter, you can restore your virtual machine files to a different datastore, host, or Resource Pool directly through the VI Client.

For information on VMware Converter, see www.vmware.com/products/converter/.

Using the vcbRestore Utility to Restore Virtual Machines

The vcbRestore utility is a command-line utility that you use to restore data that has been backed up using image-based backup. vcbRestore runs on the ESX Server 3 service console.

For information on how to use this utility, see [“Using Service Console to Back Up and Restore Virtual Machines”](#) on page 57.

Centralized Restore

When performing a centralized restore, you have a group of virtual machines on ESX Server, a proxy, and a backup agent on the proxy in a dedicated virtual machine that you plan to use to restore your data. Use the backup software to get the data to the proxy that is running the agent. After the administrator restores the data to the central server, copy it back to the virtual machine using the Common Internet File System (CIFS) remote-access file-sharing protocol.

Advantages: The number of agents to maintain is minimal.

Disadvantages: Because data restoration is centralized, an administrator must be involved in file-level restoration.

Per-Group Restore

When performing a per-group restoration, one virtual machine has a backup agent for each group, such as accounting, engineering, and marketing. The group administrator restores workflows to a per-group restore host. Files are copied to a target virtual machine using CIFS file share.

Advantages:

- Restorations can be delegated.
- This type of restoration is a good compromise between the number of agents and ease of restoration.

Disadvantages: This process is not a complete self-service restoration.

Direct Restore to a Virtual Machine

Backup agents are deployed in every virtual machine. The user can use the agent to back up data to a tape and restore the same way. The backup agent in the virtual machine is used to restore the data.

Advantages: This process is a self-service restoration.

Disadvantages: Agents are required in each virtual machine.

Data Recovery

The following guidelines can help you recover your data:

- Make sure you have image-level virtual machine backups.
- Back up your VirtualCenter database.
- Make sure you have your license keys.
- Make sure you have enough servers to run all the virtual machines you plan to restore.

Enabling migration with VMotion or using DRS enhances your disaster recovery capabilities.

Backup Scenarios and Troubleshooting

4

This chapter describes real-world scenarios that can help you plan your backup strategies.

This chapter includes the following information:

- [“Backup Usage Scenarios”](#) on page 54
- [“Typical Consolidated Backup Usage Scenario”](#) on page 54
- [“Troubleshooting”](#) on page 55

Backup Usage Scenarios

The following are the most recommended use cases:

- **Datacenter**
 - At the file level, perform backups every night.
 - At the image level, perform backups periodically for Windows, and nightly for Linux. This is a disaster recovery scenario.
- **Agents in virtual machines.** Perform incremental backups for Linux.
- **Backup server in a virtual machine.** For branch offices, deploy agents in the virtual machine as well.

Typical Consolidated Backup Usage Scenario

This is an example of how you can use Consolidated Backup to protect data in virtual machines:

- 1 The system administrator configures backup schedules and policies in the third-party backup software.

For example, the system administrator might instruct the backup software to back up `D:\Data` on `vm37.company.com` daily at 3:05 a.m.
- 2 The backup software schedules this backup job.
- 3 When the backup software launches this job, it calls into Consolidated Backup by using a pre-backup script.

Consolidated Backup performs the following:
 - a Contacts a VirtualCenter instance or an ESX Server host, and sends a request to create a snapshot of the virtual machine to be backed up.
 - b Makes this snapshot available (mounted) on the backup proxy. This makes the data that needs to be backed up visible to the third-party backup software.
- 4 The third-party backup software performs the backup procedure of copying changed data to the backup media.

- 5 At the end of the backup job, the third-party backup software calls into Consolidated Backup, using a post-backup script.

Consolidated Backup does the following:

- a Detaches (unmounts) the snapshot from the backup proxy.
- b Requests VirtualCenter or the ESX Server host to remove the virtual machine snapshot.

Troubleshooting

This section guides you through issues you might encounter when performing backups.

This section covers the following topics:

- [“Changing Backup Policies after ESX Server Upgrades”](#) on page 55
- [“Identifying VMFS Volumes in Backup GUI”](#) on page 55

Changing Backup Policies after ESX Server Upgrades

If you upgraded your ESX Server 2.x to 3.x, you need to modify all VMFS volume paths that you configured in the backup software. A path format in ESX Server 3.x is different from the ESX Server 2.x format and follows this standard:

- VMFS volume
 - `/vmfs/volumes/<file_system_UUID>`
 - or
 - `/vmfs/volumes/<file_system_label>`
- VMFS file
 - `/vmfs/volumes/<file system label|file system UUID>/[dir]/myDisk.vmdk`

Identifying VMFS Volumes in Backup GUI

When you use a backup agent in the service console for file-level backups, you work with VMFS volumes.

In ESX Server 3.x, VMFS volumes are identified by unique identifiers. The name of the directory, under which each VMFS volume is mounted in `/vmfs/volumes`, corresponds to this unique identifier. The unique identifier is assigned to the volume during formatting, and you cannot change it.

VMFS volumes can have user-friendly labels. These labels appear as symbolic links in `/vmfs/volumes` and point to the corresponding directory. For example, for a VMFS volume with the unique identifier `43a0552e-ae6093b2-47a1-00145e0a7ec0` and the label `storage1`, the following entries are created under `/vmfs/volumes`:

- A directory named `43a0552e-ae6093b2-47a1-00145e0a7ec0`, under which the file system is mounted.
- A symbolic link named `storage1`, pointing to the directory `43a0552e-ae6093b2-47a1-00145e0a7ec0`.

Your backup software GUIs that allow you to select files for backups show only the directory (the unique ID) in their Browse Directory pane. If you know your VMFS volume only by its label, it might be difficult for you to find your VMFS volume in the GUI directory.

To identify a VMFS volume by its label

- 1 Browse the `/vmfs/volumes` directory in your backup software GUI.
The symbolic links pointing to the VMFS volume mount points show up in the file selection pane.
- 2 Use these entries to find the unique ID for the file system label you need.
- 3 Select the directory corresponding to this unique ID in the directory pane for browsing.

When performing file-based backups, the backup application uses paths referencing the unique identifier, so the backed-up files show up as the following:

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

When restoring files from the backup application, you might need to perform a reverse mapping to identify the correct VMFS volume label (in this example, `storage1`) corresponding to this unique identifier. To do this, back up the symbolic link itself while performing backups.

Using Service Console to Back Up and Restore Virtual Machines



This appendix describes how to back up and restore virtual machines using your ESX Server 3 service console. The appendix walks you through the process of configuring the Consolidated Backup command-line utilities and provides examples on how to use these utilities.

NOTE Because ESX Server 3i does not have a service console, information in this chapter is not applicable to ESX Server 3i. To perform image-level virtual machine backups on an ESX Server 3i host that does not have access to SAN, use Consolidated Backup in LAN mode and run it on a virtual machine.

This appendix includes the following sections:

- [“General Configuration Settings for Consolidated Backup Utilities”](#) on page 58
- [“Backing Up Virtual Machines”](#) on page 60
- [“Archiving Virtual Machines”](#) on page 64
- [“Restoring Virtual Machines”](#) on page 64

General Configuration Settings for Consolidated Backup Utilities

Before using service console Consolidated Backup utilities, edit the `/etc/vmware/backuptools.conf` configuration file to set the most common parameters for these tools.

Because this configuration file is parsed as a Bourne shell script, follow syntax conventions of the Bourne shell when editing the file:

- Use the `#` character to indicate a comment.
- Do not use spaces when entering variables. For example, `F00="bar"` should have no spaces around the equals sign.
- Use a backslash before entering any special characters, such as `$`. For example, `\$server`.

Administrators familiar with Bourne shell script programming can use all the standard Bourne shell mechanisms, such as command execution, for example ``foo``, or use environment variables.

Configuration File Settings

Use the `/etc/vmware/backuptools.conf` configuration file to set up the following options.

- **VCHOST**

Specifies the URL of the Virtual Center instance that manages the ESX Server 3 host being backed up or restored. VCHOST should point to the Virtual Center instance managing the host.

If you perform the backup or restore operations on a standalone host, you can use `localhost` as the host name.

NOTE You can use the `-h` command-line option for any Consolidated Backup command-line utility to override this setting.

- **USERNAME**

Specifies the user name to log in to the VirtualCenter instance defined by VCHOST. The user must have privileges to be able to register or create virtual machines.

NOTE You can use the `-u` command-line option for any Consolidated Backup command-line utility to override this setting.

- **PASSWORD**

Specifies the password corresponding to `USERNAME`. This option allows you to perform virtual machine backups in a non-interactive way.



CAUTION Because specifying a password in a configuration file can present a security risk, make sure that the Service Console is not used by anyone except an ESX Server 3 administrator.

NOTE You can use the `-p` command-line option for any Consolidated Backup command-line utility to override this setting.

- **VMNAMECACHE**

The most common way of identifying a virtual machine for backup purposes is by its DNS name or by its IP address. However, when you back up a virtual machine from a standalone ESX Server 3 host, the ESX Server 3 host can recognize the IP address only when the virtual machine is powered on and running VMware Tools.

To be able to perform backups of the virtual machine on the standalone ESX Server 3 host even when the virtual machine is powered off, you should maintain a cache file. The cache file records the IP address of the virtual machine each time the virtual machine is being backed up. This allows you to perform the future backups of this virtual machine regardless of its power state.

VMware recommends that you do not change the default setting.

NOTE You can use the `-c` command-line option for `vcbMounter` to override this setting. The `vcbRestore` command does not use this setting.

- **TEMPDIR**

If you are using the secure copy capabilities of the Consolidated Backup command-line utilities, you can use this option to specify a temporary holding space for your virtual machine data.

This holding space must have enough free storage to hold the largest of your virtual machines.

NOTE You cannot override this setting from the command line.

Backing Up Virtual Machines

You can use `vcbMOUNTER` to back up an entire virtual machine in the service console. The `vcbMOUNTER` utility creates a quiesced snapshot of the virtual machine and exports the snapshot into a set of files, which can be later used to restore the virtual machine. To back up the set of files, you can use any file-based third-party backup software.

Before backing up a virtual machine using `vcbMOUNTER`, determine the following:

- Which virtual machine to back up.

See [“Identifying Virtual Machines”](#) on page 61.

- Where to store the backup data.

Consolidated Backup service console supports different transport plug-ins to either back up the virtual machine to a local directory or back it up to a remote directory using `scp`. See [“Specifying Backup Destinations”](#) on page 63.

Performing Backups

After setting up configuration options as described in [“Configuration File Settings”](#) on page 58, enter the following command in the command line:

```
vcbMOUNTER -a <virtual_machine_identifier> -r <backup_destination> -m
<cos|nbd|nbdssl>,
```

where

- `<virtual_machine_identifier>` is a unique identifier of the virtual machine you’re backing up. See [“Identifying Virtual Machines”](#) on page 61.
- `<backup_destination>` specifies the location for backup data. See [“Specifying Backup Destinations”](#) on page 63.
- `<cos|nbd|nbdssl>` specifies the transportation mode for `vcbMOUNTER`:
 - `cos` — Use this option to back up virtual machines whose disks are accessible to the ESX Server host directly through `/vmfs/volumes`. Run the `vcbMOUNTER` utility in the service console of the ESX Server host where the virtual machines reside or on any ESX Server host which has access to the datastore where the virtual machine disks are stored.
 - `nbd` — Use this option to back up virtual machines over the network from a different ESX Server host than the host where you run the `vcbMOUNTER` utility. Select this option if you do not need to encrypt virtual disk data for over-the-network transfer.

- `nbdssl` — Use this option to back up virtual machines over the network from a different ESX Server host than the host where you run the `vcbMounter` utility. Select this option if you need to encrypt virtual disk data for-over-the-network transfer.

Follow these examples when backing up virtual machines:

- Backing up the virtual machine `vm37.company.com` to the local directory `/home/VMs/vm37`:

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

- Backing up the virtual machine `vm37.company.com` to the directory `/backups/VMs/vm37`. The directory is located on the remote server `backups.company.com` with the user ID `vmware`. The `backups.company.com` host is running a secure shell (ssh) server. Use the Consolidated Backup secure copy (scp) plug-in to transfer the virtual machine to `backups.company.com`.

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

- Backing up a virtual machine on a standalone ESX Server 3 host. To identify the virtual machine, use the virtual machine's name displayed in the VI Client. The virtual machine is backed up to the local directory `/home/VMs/vm37`.

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

NOTE The virtual machine name argument is case-sensitive.

Identifying Virtual Machines

You can use different standards to specify the virtual machine you want to back up.

Identifying Virtual Machines by DNS Name or IP Address

The most common way of identifying virtual machines is to use their DNS name or IP address. To identify the virtual machine, use the following specification:

```
ipaddr:<DNS name or IP address>
```

For example, to refer to the virtual machine `vm37.company.com` with the IP address `10.17.5.12`, use one of the following search specifiers:

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

Identifying Virtual Machines by BIOS UUID

You can identify a virtual machine by its universally unique identifier (UUID). Use the following search specifier:

```
uuid:<uuid>
```

For example:

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

Identifying Virtual Machines by MoRef

Internally, VirtualCenter and ESX Server 3 refer to objects by Managed Object References (MoRef). To identify a virtual machine by MoRef, follow these examples:

- `moref:vm-00027` – Use this format when accessing VirtualCenter Server.
- `moref:248` – Use this format when accessing the ESX Server 3 host.

Because MoRefs change every time the VirtualCenter server or the host instance that Consolidated Backup connects to restarts, you should not use MoRefs to identify virtual machines. However, when running a shell script to back virtual machines, you can use MoRefs to identify the virtual machines.

For example, you can write a script that uses `vcbVmName` with the `any:` search specifier to get a list of all virtual machines, and perform custom filtering to produce a list of only those virtual machines you want to back up. Virtual machines on this list can use MoRefs as their identifiers. Another part of your script can call `vcbMounter` on each of these MoRefs to perform the backup operations.

In a case like this, using MoRefs rather than other identifiers, such as UUID, causes less search overhead because the entire list of all virtual machines does not need to be parsed each time the identifier is used.

Displaying Virtual Machine Information

To search for a particular virtual machine and get information about it, use `vcbVmName`.

Follow these examples:

- `vcbVmName -s powerstate:on` – Lists all powered-on virtual machines.
- `vcbVmName -s any:` – Lists all known virtual machines.
- `vcbVmName -s ipaddr:vm37.company.com` – Displays information about the virtual machine with the specified address.

The following is the sample output you get after using `vcbVmName`:

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

Specifying Backup Destinations

You can back up a virtual machine to a local directory or to a remote server using `scp`.

Backing Up to a Local Directory

When backing up a virtual machine to a local directory, specify the path to the directory, for example, `/home/VMs/vm37`.

NOTE You do not need to create the destination subdirectory, such as `/home/VMs/vm37`, in advance because the backup operation will create it. However, the directory that lists your destination subdirectory, for example `/home/VMs`, must exist before you start a backup process.

Backing Up to a Remote Server

When you back up a virtual machine to a remote server, use a corresponding `scp` plug-in. Use the following syntax:

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

To perform the `scp` backup automatically, use RSA key-based authentication. In this case, `scp` will not prompt you for a password during backup.

For example, to back up a virtual machine to the directory `/backup/VMs/vm37` located on the remote server `backups.company.com` that uses the `vmware` user ID. Enter the following:

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

NOTE Prior to backup, make sure that the `/backups/VMs` directory exists on the remote server. However, you do not need to create the `/backups/VMs/vm37` directory because it is created during the backup operation.

Archiving Virtual Machines

Use `vcbSnapAll` to create an archive of groups of virtual machines in the service console. The `vcbSnapAll` utility has the same functionality as `vcbMounter`, but, in addition, can identify groups of virtual machines.

Use the following syntax:

```
vcbSnapAll -a <virtual_machine_identifier> -r <backup_destination>
           -m<cos|nbd|nbdssl>,
```

where `<virtual_machine_identifier>` specifies a group of virtual machines. Use one of the following search specifiers:

- `powerstate: on|off|suspended` – Finds all virtual machines with the specified power state.
- `any:` – Finds all virtual machines.
- `none:` – Does not find any virtual machines. You can use this option for testing.

You can also use one of the unique identifiers of the virtual machine. See [“Identifying Virtual Machines”](#) on page 61.

The backup destination directory must exist before you start the archiving process using `vcbSnapAll`. While running, the `vcbSnapAll` utility creates a subdirectory for each virtual machine that meets the search criteria inside the backup destination directory. You do not need to create the subdirectories in advance.

After you move the virtual machine backup data from the backup destination directory to a secondary storage, you can delete the directory contents.

Restoring Virtual Machines

You can restore a virtual machine to its original location or to another location of your choice.

Restoring Virtual Machines to Original Locations

If you set up all configuration options as described in [“Configuration File Settings”](#) on page 58, the following is the only command you need to pass to `vcbRestore` to restore a virtual machine:

```
vcbRestore -s <backup_directory>
```

See [“Specifying Backup Destinations”](#) on page 63.

Follow these examples when restoring your virtual machines:

- Restoring a virtual machine from a local backup directory named `/home/VMs/vm37`:


```
vcbRestore -s /home/VMs/vm37
```
- Restoring a virtual machine from the remote server `backup.company.com`, directory `/backups/VMs/vm37`, and user ID `vmware`:


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

Restoring Virtual Machines to Alternative Locations

To restore a virtual machine to a location other than its original location, or to a different ESX Server 3 host, use the virtual machine's `catalog` file. The `vcbMounter` utility creates this file for each virtual machine it backs up. The `catalog` file contains summary information about the virtual machine, such as its display name, its power state at the time of backup, and so on.

To restore a virtual machine to an alternative location

- 1 Make a copy of the virtual machine's catalog file.
See [“Copying a Catalog File”](#) on page 65.
- 2 In the copy of the catalog file, specify the new settings for datastores, folder path, and resource pool.
See [“Editing a Catalog File”](#) on page 66.
- 3 Restore the virtual machine using `vcbRestore`.
See [“Restoring Virtual Machines Using an Alternate Catalog”](#) on page 67

Copying a Catalog File

When restoring a virtual machine to a location other than the original, make a copy of the virtual machine's `catalog` file.

For example, make a copy of the `catalog` file of the `/home/VMs/vm37` virtual machine. Enter the following:

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

Editing a Catalog File

In the copy of the `catalog` file you made, change the following settings:

- **Datastore.** Identifies where to store all the files that comprise a virtual machine.
- **Folder path.** The virtual machine's folder path defines where the virtual machine will be placed in the VirtualCenter folder hierarchy.
- **Resource pool.** This host-specific configuration item determines the virtual machine's behavior with respect to DRS (Distributed Resource Scheduling). When you use multiple ESX Server 3 hosts managed by VirtualCenter, this item also specifies the host that will run the virtual machine.

NOTE If you change the name of the virtual machine in the catalog file, `vcbRestore` does not pick up the new name from the file, but instead uses the original virtual machine name specified in the `.vmx` file.

You can change the name of the virtual machine later using the VI Client.

Changing Datastore Paths

The datastore path in the `catalog` file identifies where to store all the files that comprise a virtual machine. Change datastore paths in the following entries:

- `disk.scsi*.diskname` – Names and locations of all disks associated with this virtual machine.
- `config.vmx` – Location for the virtual machine's main configuration file.
- `config.suspenddir` – Location for the memory snapshots taken when the virtual machine gets suspended.
- `config.logdir` – Location for the virtual machine's log files.

By default, all these entries use the same path, which points to the same directory on the same datastore. VMware recommends that you follow this standard when changing the path.

The datastore paths have the following syntax:

```
[<datastore_name>] <path_on_datastore>
```

You can obtain a list of valid datastore names from the datastore browser in your VI Client, or by looking at the file system labels of your VMFS volumes in the service console under `/vmfs/volumes`.

Changing Folder Paths

The virtual machine's folder path in the `catalog` file specifies the folder within the VirtualCenter folder hierarchy where the restored virtual machine will be placed.

To change the folder path for the virtual machine

- 1 Identify the folder that will store the virtual machine by running the following command in the service console:

```
vcbUtil -c vmfolders
```

Running this command assumes that you have set up appropriate configuration options as described in [“Configuration File Settings”](#) on page 58.

- 2 In the `catalog` file, set the folder path to one of the folder paths printed out by the `vcbUtil` command.

Changing Resource Pools

The resource pools entry in the `catalog` file determines the virtual machine's behavior with respect to DRS (Distributed Resource Scheduling). When you use multiple ESX Server 3 hosts managed by VirtualCenter, this item also specifies the host that will run the virtual machine.

To change the resource pool setting for the virtual machine

- 1 Identify the resource pool that the virtual machine will use by running the following command:

```
vcbUtil -c resourcepools
```

Running this command assumes that you have set up appropriate configuration options as described in [“Configuration File Settings”](#) on page 58.

- 2 In the `catalog` file, set the resource pool to one of the options provided by the `vcbUtil` command.

Restoring Virtual Machines Using an Alternate Catalog

After modifying the settings in the virtual machine's alternate catalog, use this file to restore the virtual machine.

To restore the virtual machine, use the `-a` entry to specify the alternate catalog.

For example, to restore a virtual machine backed up under `/home/VMs/vm37` by using the alternate catalog file `/tmp/catalog-vm37`, enter:

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

Non-Interactive Use of the vcbRestore Utility

By default, vcbRestore prompts you about what to do when the restore operation detects a file that already exists or a virtual machine already known to VirtualCenter.

If vcbRestore is used by a script in a non-interactive way, use the `-b` command-line entry to specify the default behavior. The following options are available:

- `prompt`
Prompts a user about what to do before overwriting files or configurations of virtual machines already known to VirtualCenter.
- `overwrite`
Overwrites any existing files and virtual machine configurations known to VirtualCenter during restore.
- `keep`
Preserves existing files and configurations of virtual machines known to VirtualCenter without replacing them.
- `abort`
Terminates the restore operation after detecting an existing file or a virtual machine configuration already known to VirtualCenter.

Restoring Virtual Machines from Archives

Use `vcbResAll` to restore all the virtual machines from the archive you created using `vcbSnapAll`. The `vcbResAll` utility supports all the functionality of `vcbRestore`.

Use the following syntax:

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

See [“Restoring Virtual Machines to Original Locations”](#) on page 64 and [“Restoring Virtual Machines to Alternative Locations”](#) on page 65.

Restoring Virtual Machines from ESX Server 2.5.x to ESX Server 3.x



This appendix describes how to restore virtual machines that were created and backed up on ESX Server 2.5.x, in ESX Server 3.x using the service console.

NOTE Because ESX Server 3i does not have a service console, information in this chapter is not applicable to ESX Server 3i.

This appendix includes the following sections:

- [“Setting Configuration Parameters”](#) on page 70
- [“Restoring ESX 2.5.x Server Virtual Machines”](#) on page 71

Setting Configuration Parameters

To restore virtual machines from ESX Server 2.5.x to ESX Server 3.x, set up configuration parameters in the `/etc/vmware/backuptools.conf` file.

To set up general parameters, follow recommendations in [“General Configuration Settings for Consolidated Backup Utilities”](#) on page 58.

In addition, define the following parameters.

- **DSPATH**

Specifies the path to a datastore where your restored virtual machine will reside. To avoid setting up this option individually for each virtual machine you restore, use the `%VMNAME%` entry. During the restore process, the base name of the virtual machine's `.vmx` configuration file substitutes this entry.

For example, to restore virtual machines to the `o1dvms` datastore using the base name of the virtual machine's `.vmx` file, enter the following:

```
DSPATH="[o1dvms] %VMNAME%"
```

This entry restores the virtual machine with the `myvm.vmx` file into `[o1dvms]/myvm`.

- **VMHOST**

Specifies the host for the virtual machine you restore. The virtual machine is powered on from this host.

- **RESOURCEPOOL**

Specifies the resource pool for the virtual machine you restore. See [“Changing Resource Pools”](#) on page 67.

NOTE Select a valid resource pool on the host you specified in `VMHOST`. Typically, the resource pool name contains the name of the corresponding ESX Server 3 host. You can also use the `%VMHOST%` entry, which will be replaced by the value you assigned to `VMHOST`.

- **FOLDERPATH**

Specifies the folder within the VirtualCenter hierarchy, in which the restored virtual machine will be placed. See [“Changing Folder Paths”](#) on page 67.

Restoring ESX 2.5.x Server Virtual Machines

After defining all necessary settings in the `/etc/vmware/backuptools.conf` file, you can restore virtual machines that were backed up on ESX Server 2.5.x.

The restore process is the same as for the ESX Server 3.x virtual machines.

See [“Restoring Virtual Machines”](#) on page 64.

Index

A

aliases **43**
archive bit **36**

B

backup clients
 about **15**
 in a virtual machine **17**
 in the service console **19**
backup jobs
 canceling **46**
 setting up **43**
backup policies, modifying **55**
backup schedulers **15**
backup servers **15**
backup utilities **58**
backups
 differential **12**
 file-level **30**
 from NFS **21**
 from SAN **21**
 image-level **30**
 incremental **12**
 overview **12**
 performing first **44**
 sample scenario **54**
 techniques **15**
 traditional **16**
backuptools.conf file **58**
BIOS UUID **62**

C

catalog files **65**
change journal **36**
CIFS **51**
Common Internet File System
 protocol **51**
configuration file
 backup utilities **58**
 Consolidated Backup **36**
Consolidated Backup
 and third-party backup software **24**
 configuration file **36**
 configuring SAN **41**
 configuring third-party software **35**
 configuring VCB proxy **33**
 considerations **22**
 customizing **44**
 features **24**
 file-level backups **30**
 image-level backups **30**
 installing **36**
 interoperability modules **36**
 limitations **30**
 overview **24**
 performing first backup **44**
 running **41**
 setting up backup jobs **43**
 turning off drive-letter
 assignment **34**
 utilities **58**

versus traditional backup
methods **22**
VMware Tools **32**

D

directory, /vmfs/volumes **14**
disaster recovery **52**
disk images, exporting **30**
DNS name **61**
drive letters **34**

E

ESX Server 2.5.x **69**
ESX Server, upgrading **55**

F

FAT **34**
files
 .vmdk **13**
 .vmx **13**

I

incremental backups
 archive bit **36**
interoperability modules
 about **24**
 installing **36**
IP address **61**

J

junction points
 about **30**
 turning on **35**

M

MoRef **62**

N

NFS storage and backups **21**
NTFS **34**

P

physical compatibility **14**

Q

quiescing
 about **12**
 customizing **44**

R

raw device mapping **14**
RDM
 physical compatibility **14**
 turning off drive-letter
 assignment **34**
 virtual compatibility **14**

README.html file **36**

restorations

 centralized **51**
 ESX Server 2.5.x virtual
 machines **69**
 file-based **50**
 per-group **51**
 self-service **52**
 vcbRestore utility **51**
 workflows **50**

S

SAN storage
 and backups **21**
 configuring for VCB **41**
schedulers **15**
SCSI disks **13**
service console **13**
 backing up **16**
 file-based backups **16**
 image-based backups **16**

T

- third-party software
 - configuring for VCB **35**
 - interoperability modules **24**
 - turning off archive bit **36**
 - turning off change journal **36**
 - working with Consolidated Backup **24**
- time stamps **36**
- traditional backup methods **17**
- troubleshooting
 - backup software GUI **55**
 - path formats **55**

U

- utilities
 - Consolidated Backup **58**
 - vcbMounter **60**
 - vcbRestore **51, 64**

V

- VCB proxy
 - about **12**
 - and networking **33**
 - installing Consolidated Backup **36**
 - junction points **30**
 - running Windows **34**
 - setting up **33**
 - turning off drive-letter assignment **34**
- VCB, see Consolidated Backup
- vcbMounter
 - destinations **63**
 - overview **60**
 - performing backups **60**
 - specifying virtual machines **61**

- vcbRestore **64**
 - catalog files **65**
 - default use **68**
 - restoring to alternative locations **65**
 - restoring to original locations **64**
- virtual compatibility **14**
- virtual disks
 - manipulating **14**
 - storing **13**
- virtual machines
 - aliases **43**
 - groups **43**
- VMFS **13**
- vmkfstools commands **14**
- VMware Tools **32**

W

- Windows archive bit **36**
- Windows change journal **36**
- workflow **24**

Updates for the Virtual Machine Backup Guide

Last Updated: February 21, 2008

This document provides updates to the ESX Server 3.5, ESX Server 3i version 3.5, and VirtualCenter 2.5 version of the *Virtual Machine Backup Guide*. Updated descriptions, procedures, and graphics are organized by page number so that you can easily locate the areas of the guide that have changes. If the change spans multiple sequential pages, this document provides the starting page number only.

The following is an update to the *Virtual Machine Backup Guide*:

[Updates for the Consolidated Backup Software and Hardware Requirements Section on Page 31](#)

Updates for the Consolidated Backup Software and Hardware Requirements Section on [Page 31](#)

In “[Consolidated Backup Software and Hardware Requirements](#)” on page 31, the third bullet under the versions of Microsoft Windows operating system to install on a VCB proxy incorrectly lists Microsoft Windows Server 2003 Service Pack 1 (32-bit or 64-bit). Instead, it should list the following:

- Microsoft Windows Server 2003 Service Pack 2 (32-bit or 64-bit)

