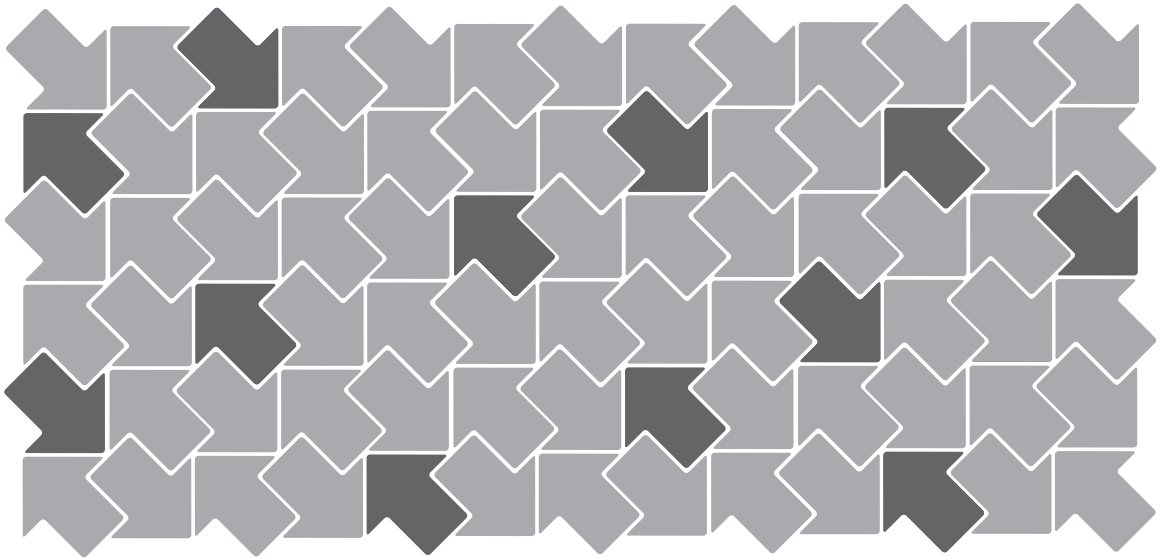


Virtual Machine Backup Guide

ESX Server 3.0.1 and VirtualCenter 2.0.1



Virtual Machine Backup Guide

Revision: 20060925

Item: VI-ENG-Q206-216

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

© 2006 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, 6,961,941, 6,961,806 and 6,944,699; 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.

3145 Porter Drive
Palo Alto, CA 94304
www.vmware.com

Contents

Preface 7

1 Introduction 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
 - Backup Approaches 15
- Using Traditional Backup Methods 16
 - Traditional Backup Considerations 16
 - Backing Up the Service Console 16
 - Backing Up Virtual Machines 17
 - Backup Client in a Virtual Machine 18
 - Backup Client in the Service Console 19
 - SAN Backups 20
 - NFS Backups 21
- Using VMware Consolidated Backup 21
 - VMware Consolidated Backup Advantages 21

2 VMware Consolidated Backup 23

- VMware Consolidated Backup Overview 24
- VMware Consolidated Backup Usage Models 24
- Consolidated Backup Software and Hardware Requirements 25
- How VMware Consolidated Backup Works 25
 - Before you Begin 26
 - VMware Consolidated Backup Workflow 26
 - Creating Snapshots 28
 - Performing Image-Level Virtual Machine Backups 29
 - Performing File-Level Virtual Machine Backups 29
 - Considerations When Creating Snapshots 30
- VMware Consolidated Backup Limitations 30

Setting Up VMware Consolidated Backup	31
Configuring VMware ESX Server	31
Configuring SAN	31
Configuring Third-Party Software	32
Client Settings for File-Level Incremental and Differential Backups	32
Configuring VCB Proxy	33
Hardware Requirements	33
Prerequisites	33
Configuring Windows on the VCB Proxy	34
Disabling Automatic Drive-Letter Assignment	34
Installing VMware Consolidated Backup	35
Configuring VMware Consolidated Backup	35
Installing a Backup Software Integration Module	37
Configuring Virtual Machines for Consolidated Backup	37
Using VMware Consolidated Backup	37
Grouping Virtual Machines	38
Configuring Backup Jobs	38
First-Time Backup	39
Advanced Configurations	39
Running Custom Quiescing Scripts	40
Canceling a Backup Job	41
3 Restoration and Disaster Recovery	43
Restoring Your Files Using VMware Consolidated Backup	44
Centralized Restore	44
Per-Group Restore	44
Self-Service Restore	45
Restoring Files Using the vcbRestore Utility	45
Data Recovery	45
4 Backup Scenarios and Troubleshooting	47
Backup Usage Scenarios	48
Typical Consolidated Backup Usage Scenario	48
Troubleshooting	49
Configuring Identical SAN LUN IDs	49
Disabling Multipathing	49
Changing Backup Policies after ESX Server Upgrades	51
Identifying VMFS Volumes in Backup GUI	51

A	Using Service Console to Back Up and Restore Virtual Machines	53
	General Configuration Settings for Consolidated Backup Utilities	54
	Configuration File Settings	54
	Backing Up Virtual Machines	56
	Performing Backups	56
	Identifying Virtual Machines	57
	Identifying Virtual Machines by DNS Name or IP Address	57
	Identifying Virtual Machines by BIOS UUID	57
	Identifying Virtual Machines by MoRef	58
	Identifying Groups of Virtual Machines	58
	Specifying Backup Destinations	59
	Backing Up to a Local Directory	59
	Backing Up to a Remote Server	59
	Restoring Virtual Machines	60
	Restoring Virtual Machines to Original Locations	60
	Restoring Virtual Machines to Alternative Locations	60
	Copying a Catalog File	61
	Editing a Catalog File	61
	Restoring Virtual Machines Using an Alternate Catalog	63
	Non-Interactive Use of the vcbRestore Utility	63
B	Restoring Virtual Machines from ESX Server 2.5.x to ESX Server 3.x	65
	Setting Configuration Parameters	66
	Restoring ESX 2.5.x Server Virtual Machines	67
	Index	69

Preface

This preface describes the contents of the *Virtual Machine Backup Guide* and provides pointers to VMware® technical and educational resources.

This preface contains the following topics:

- [“About This Book”](#) on page 8
- [“Technical Support and Education Resources”](#) on page 10

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 new backup solution offered by VMware Infrastructure 3 and recommended to perform daily backups for virtual machines residing on a SAN.

Revision History

This manual is revised with each release of the product or when necessary. A revised version can contain minor or major changes. [Table P-1](#) provides you with the revision history of this manual.

Table P-1. Revision History

Revision	Description
20060615	ESX Server 3.0 and VirtualCenter 2.0 version of the VMware Infrastructure 3 <i>Virtual Machine Backup Guide</i> . This is the first edition of this manual.
20060925	ESX Server 3.0.1 and VirtualCenter 2.0.1 version of the VMware Infrastructure 3 <i>Virtual Machine Backup Guide</i> . This edition contains minor changes.

Intended Audience

The information presented in this manual is written for experienced Windows or Linux system administrators and who are familiar with virtual machine technology datacenter operations.

Document Feedback

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

docfeedback@vmware.com

VMware Infrastructure Documentation

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

You can access the most current versions of this manual and other books by going to:

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

Conventions

[Table P-2](#) illustrates the typographic conventions used in this manual.

Table P-2. Conventions Used in This Manual

Style	Elements
Blue (online only)	Cross-references and email addresses
Blue boldface (online only)	Links
Black boldface	User interface elements such as button names and menu items
Monospace	Commands, filenames, directories, and paths
Monospace bold	User input
<i>Italic</i>	Document titles, glossary terms, and occasional emphasis
< Name >	Variable and parameter names

Abbreviations Used in Graphics

The graphics in this manual use the abbreviations listed in [Table P-3](#).

Table P-3. Abbreviations

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

Technical Support and Education Resources

The following sections describe the technical support resources available to you.

Self-Service Support

Use the VMware Technology Network (VMTN) for self-help tools and technical information:

- Product information – <http://www.vmware.com/products/>
- Technology information – <http://www.vmware.com/vcommunity/technology>
- Documentation – <http://www.vmware.com/support/pubs>
- VMTN Knowledge Base – <http://www.vmware.com/support/kb>
- Discussion forums – <http://www.vmware.com/community>
- User groups – <http://www.vmware.com/vcommunity/usergroups.html>

For more information about the VMware Technology Network, go to <http://www.vmtn.net>.

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/mgrreg/index.cfm>.

Introduction

Backup, restoration, and disaster recovery are among the most critical processes of datacenter management. VMware® ESX Server and VMware Infrastructure 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 21

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, `.vmx` files, and so on.
- **Image-level (volume-level) backup** – Backs up an entire storage volume.
- **Incremental backup** – Backs up only those 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 machine running Microsoft Windows 2003, Consolidated Backup, and third-party backup software. Used to perform LAN-free 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, virtual machine data needs to be backed up periodically to prevent its corruption 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 more information on virtual machine files, see [“Virtual Machine Contents”](#) on page 13.

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

- **ESX Server service console** – The service console, a customized version of Linux, is the ESX Server command-line management interface. It provides the ESX Server management tools and a command prompt for more direct management of ESX Server. It also keeps track of all the virtual machines on the server and their configurations.

NOTE In earlier releases, the service console was the main interface to the ESX Server host. With ESX Server 3 and later, the VI Client has priority, although you still might use the service console to perform some advanced administration operations.

During its lifetime, the service console doesn’t experience any major changes other than periodic upgrades. In case of a failure, you can easily recover the state of your service console by reinstalling ESX Server. Therefore, although you might consider backing up the service console, it doesn’t need to be backed up as frequently as the virtual machines and their data.

Virtual Machine Contents

To store virtual machines, ESX Server uses *VMware File System (VMFS)*. VMFS is a simple, high-performance file system on physical SCSI disks and partitions 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 *Server Configuration Guide*.

NOTE If you upgraded your ESX Server software 2.x to 3.x, modify all VMFS volume paths that you configured in the software you use for backup. See [“Changing Backup Policies after ESX Server Upgrades”](#) on page 51.

In ESX Server 3.x, VMFS supports directories. Typically, there is one directory 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 normally 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. RDM can exist in two modes, virtual compatibility and physical compatibility.

For more information on RDM, see *Server Configuration Guide*.

Accessing and Managing Virtual Disk Files

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

Direct manipulation of your virtual disk files on VMFS is possible through ESX Server service console and VMware SDKs, although using the VI Client is the preferred method.

From the service console, you can view and manipulate files in the `/vmfs/volumes` directory in mounted VMFS volumes with ordinary file commands, such as `ls` and `cp`. Although mounted VMFS volumes might appear similar to any other file system, such as ext3, VMFS 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 hangs the ESX Server. It must then be rebooted. If Consolidated Backup is not used, 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. This command supports the creation of a VMFS on a SCSI disk and is used for 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 *Server Configuration Guide*.

Backup Components and Approaches

When you perform a backup, the following three components of backup software are generally 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 automatic backup jobs and coordinate their execution. Backups can be scheduled at periodic intervals, or individual files can be automatically backed up immediately after they have been updated.

Depending on where you run each of the components, you can choose different approaches. For more information, see [“Backup Approaches.”](#)

Backup Approaches

Each of the backup software components can be run in a virtual machine, on the service console, or on a VCB proxy running Microsoft Windows 2003. While the location of the scheduler isn't 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 perform automatic backups.

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

For more information, see [“Using Traditional Backup Methods”](#) on page 16.

- **VMware Consolidated Backup.** Enables offloaded and impact-free backup 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.

For more information on Consolidated Backup, see [“VMware Consolidated Backup”](#) on page 23.

For more information on the snapshot technology that Consolidated Backup uses, see [“Creating Snapshots”](#) on page 28.

Using Traditional Backup Methods

With the traditional backup methods, you deploy a backup agent on each host whose data needs to be secured. Backups are then conducted regularly in an automated way.

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.

Using traditional methods, you can back up your service console and virtual machines. For more information, see:

- [“Traditional Backup Considerations”](#) on page 16
- [“Backing Up the Service Console”](#) on page 16
- [“Backing Up Virtual Machines”](#) on page 17

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. Remember that managing agents in every virtual machine is very time consuming.

Backing Up the Service Console

Because the service console doesn't experience any 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 don't 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.

[Table 1-1](#) compares available traditional methods.

Table 1-1. Recommended Traditional Backup Methods (No Consolidated Backup)

		Backup Server	
		Virtual Machine	Physical Machine
Backup Client	Virtual Machine	Method 1	Method 2
	Service Console	Method 3	Method 4

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

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.
- Run backup clients from the ESX Server Service Console, backing up virtual machines in their entirety as .dsk and .vmdk files residing in the ESX Server host VMFS file system.
- 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.

For more details on traditional backup methods, see:

- [“Backup Client in a Virtual Machine”](#) on page 18
- [“Backup Client in the Service Console”](#) on page 19
- [“SAN Backups”](#) on page 20
- [“NFS Backups”](#) on page 21

Backup Client in a Virtual Machine

Method 1 and Method 2 assume that you deploy your backup client in a virtual machine.

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. Both virtual machines run on the same ESX Server system. Data between the two virtual machines moves through the virtual Ethernet that connects these virtual machines.

NOTE Use Method 1 only when separate hardware for a VCB proxy or backup server isn’t available.

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 1-2. 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
Backup Impact:	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 1-3. 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
Backup Impact:	No
Manageability:	Very poor

Backup Client in the Service Console

Method 3 and Method 4 assume that you deploy your backup client in the service console.

Method 3: Backup Server in a Virtual Machine

With Method 3, you deploy the backup client in the 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 isn't available.

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

Table 1-4. Backup cleating in a 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
Backup Impact:	No
Manageability:	Very poor

Method 4: Backup Server in a Physical Machine

With Method 4, you deploy the backup client in the 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 1-5. Backup client in a 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
Backup Impact:	No
Manageability/Scalability:	Very poor

SAN Backups

If your virtual disk files are stored on a SAN, you can use features supplied by your SAN vendor to create a copy of your production LUN, containing all virtual disks. 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 snapshot guarantees consistency.

If you decide to use SAN snapshots to back up your data, consider the following points:

- 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 snapshots for the individual virtual machines (one per disk).
- Some vendors support snapshots only for a setup using RDM. If only RDM is 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 *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's documentation for additional information.

Using VMware Consolidated Backup

In a modern datacenter environment, it has become increasingly difficult to apply the traditional approach to your backup processes. Using it might cause a number of 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 Advantages

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.
- Avoid congesting and overloading the data center network infrastructure by enabling LAN-free backup.
- 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 that are powered off.

VMware Consolidated Backup

2

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

This chapter includes the following information:

- [“VMware Consolidated Backup Overview”](#) on page 24
- [“Consolidated Backup Software and Hardware Requirements”](#) on page 25
- [“How VMware Consolidated Backup Works”](#) on page 25
- [“VMware Consolidated Backup Limitations”](#) on page 30
- [“Setting Up VMware Consolidated Backup”](#) on page 31
- [“Using VMware Consolidated Backup”](#) on page 37
- [“Advanced Configurations”](#) on page 39

VMware Consolidated Backup Overview

VMware Consolidated Backup helps you perform backups from a dedicated physical host (VCB backup proxy) using the VMware snapshot technique and an industry-standard backup software. Consolidated Backup integrates with most major backup applications providing you with a fast and efficient way of backing up data in virtual machines.

You can use Consolidated Backup with a single ESX Server host or with a VirtualCenter Management Server.

Consolidated Backup offers the following features:

- Offloads backup processes to a dedicated physical host (VCB proxy).
- Eliminates the need for a backup window by using VMware virtual machine snapshot technology.
- Doesn't require backup agents in virtual machines.
- Works with industry-leading backup applications allowing you to take advantage of their advanced scheduling and backup management features.
- Doesn't restrict the use of Fibre Channel tapes.
- Supports file-level backups for virtual machines running Microsoft Windows guest operating system.
- Supports image-level backups for virtual machines running any guest operating system.

VMware Consolidated Backup Usage Models

Consolidated Backup supports both virtual machine image-level backup and file-level backup (for virtual machines running Microsoft Windows operating systems).

- **Image-level backup.** Makes a copy of all the disk and configuration files associated with a particular virtual machine, allowing the restoration of the entire virtual machine. This type of backup is suitable for restoring virtual machines in the event of a hardware failure or a system administrator error, such as the accidental deletion of the virtual machine.
- **File-level backup.** Makes a copy of individual files contained on the disks within a virtual machine. This can include all files (a full file backup), or selected files, such as those which changed since a previous backup (differential or incremental file backups). File-level backups allow files or directories to be restored individually. Use the file-level backups to prevent data loss due to errors, for example, accidental file deletion.

Consolidated Backup Software and Hardware Requirements

([SEE UPDATE](#)) Requirements for VMware Consolidated Backup include:

- One or more VCB proxy systems running Microsoft Windows 2003 SP1. The VCB proxy needs to be connected to the VirtualCenter Server managing your ESX Server cluster, or to a single ESX Server system if you are not using VirtualCenter and have only one ESX Server system. To connect to Fibre Channel (FC) SAN, the VCB proxy needs a FC host bus adapter (HBA).
- Backup software that Consolidated Backup supports. For a list of supported third-party backup packages, see the *VMware Infrastructure 3 Backup Software Compatibility Guide*.
- Backup hardware, such as a tape system.
- One or more ESX Server 3.x systems.
- Fibre Channel SAN storage hosting VMFS or RDMs. The VCB proxy needs to have access to SAN LUNs.

NOTE Currently, Consolidated Backup is not supported for iSCSI or NAS/NFS.

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 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 machine that has Microsoft Windows 2003 installed.

See the following sections for more information:

- [“Before you Begin”](#) on page 26
- [“VMware Consolidated Backup Workflow”](#) on page 26
- [“Creating Snapshots”](#) on page 28

Before you Begin

To run Consolidated Backup, make sure that the following initial requirements are met:

- Configure you VCB proxy. For more information, see [“Configuring VCB Proxy”](#) on page 33.
- Install your backup software, Consolidated Backup, and corresponding integration module on the VCB proxy.
- For file-level backups, make sure your virtual machines run Windows guest operating systems. Image-level virtual machine backups are supported for all guest operating systems.
- (Optional) Install the latest version of VMware Tools in each virtual machine you plan to backup. Without this, some features of Consolidated Backup are not available.
- Create backup administrator accounts on the VCB proxy with read access to the data. Because SAN LUNs containing VMFS volumes are accessible by the proxy, to protect the VMFS volumes from accidental deletion, restrict access to the proxy to trained personnel only.

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 automatically 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 Quiesces NTFS and FAT file systems inside the virtual machine (only for Microsoft Windows virtual machines). This ensures that no file system writes are pending at the time the snapshot is taken, allowing the creation of file-system consistent backups.
- b 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. See [“Creating Snapshots”](#) on page 28.

- c Takes the virtual machine snapshot and makes it available to the third-party software:
 - For image-level virtual machine backups, exports the virtual machine snapshot to the VCB proxy. See [“Performing Image-Level Virtual Machine Backups”](#) on page 29.
 - For file-level backups of Microsoft Windows virtual machines, mounts the virtual machine snapshot from the SAN to a local directory on the VCB proxy. See [“Performing File-Level Virtual Machine Backups”](#) on page 29.
- 2 The backup software performs an ordinary backup of the virtual machine snapshot. The virtual machine can continue to operate during this process.
 - For all virtual machines, the backup client backs up the contents of the virtual machine as a virtual disk image.
 - For virtual machines running Microsoft Windows operating systems, the backup client can also back up the contents of the virtual machines as a set of files and directories.
- 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.

Figure 2-1 illustrates how different components of Consolidated Backup work together interacting with a third-party backup software.

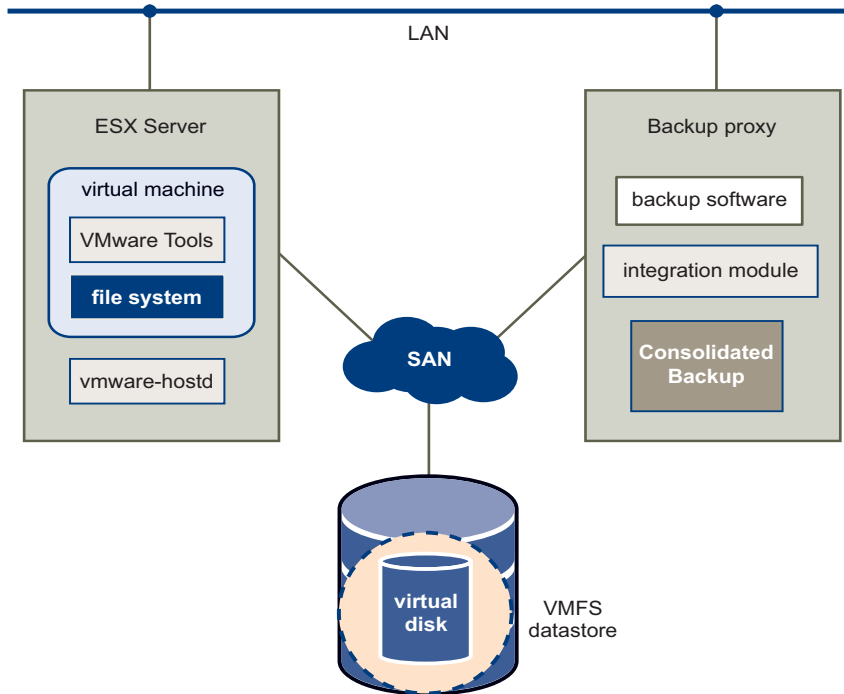


Figure 2-1. VMware Consolidated Backup

Creating Snapshots

(SEE UPDATE) When you use Consolidated Backup, a pre-backup script creates a snapshot of a virtual machine while the virtual machine is powered-on and continues to write to its virtual disk. Because no writes are pending, the snapshot captures the entire state of the virtual machine at the time you take the snapshot. This includes the state of the virtual machine's memory, disks, and settings.

NOTE File-system-consistent snapshots can be created only for virtual machines that run Windows guest operating systems and have VMware Tools installed.

To achieve even higher levels of data consistency, configure pre-freeze and post-thaw scripts in both Windows and Linux virtual machines. See [“Running Custom Quiescing Scripts”](#) on page 40 for more information.

After the snapshot of the virtual machine has been created, it becomes available to the third-party software.

For more details, see the following sections:

- [“Performing File-Level Virtual Machine Backups”](#) on page 29
- [“Performing Image-Level Virtual Machine Backups”](#) on page 29
- [“Considerations When Creating Snapshots”](#) on page 30

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, you first create 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 proxy can recognize only volumes that have drive letters assigned to them, make sure that each virtual disk volume has a drive letter.

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

Considerations When Creating Snapshots

When creating snapshots, consider the following:

- Taking a snapshot of a virtual machine freezes it for a short period of time, usually less than a second.
- Creating a memory snapshot through the UI can leave a virtual machine frozen for a few seconds. This might affect time-sensitive applications, such as DBHammer.
- 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, it results in snapshots being only crash-consistent, unless you provide custom quiescing through pre-backup and post-backup scripts in the guest.
- When snapshots are mounted on the VCB proxy, the virtual machine disks appear to be writable. However, any changes are cached on the proxy as “transient writes” and are discarded once the disk is unmounted.

VMware Consolidated Backup Limitations

Under certain circumstances, Consolidated Backup cannot be used for backing up data in a virtual machine. You cannot use Consolidated Backup to do any of the following:

- Back up virtual machines with disk images stored on a storage device that the VCB proxy cannot access.
- Back up virtual machines with virtual disks that are RDMs in physical compatibility mode.
- Back up virtual machines that do not have an IP address or a domain name server DNS name associated with them.
- Perform a file-level backup of virtual machines running operating systems other than Microsoft Windows NT 4.0, Windows 2000, Windows XP, Windows XP Professional, or Windows 2003.
- Back up virtual machines that reside on NAS/NFS or iSCSI storage devices.

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 should be 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.

Setting Up VMware Consolidated Backup

To be able to use Consolidated Backup, configure the following components:

- VMware ESX Server (version 3.0 or higher) or multiple servers. See [“Configuring VMware ESX Server”](#) on page 31.
- SAN fabric. See [“Configuring SAN”](#) on page 31.
- Third-party software. See [“Configuring Third-Party Software”](#) on page 32.
- Backup proxy (VCB proxy). See [“Configuring VCB Proxy”](#) on page 33.
- Windows on the VCB proxy. See [“Configuring Windows on the VCB Proxy”](#) on page 34.
- A new version of VMware Tools corresponding to your ESX Server in each protected virtual machine. [“Configuring Virtual Machines for Consolidated Backup”](#) on page 37.

Configuring VMware ESX Server

You should have an existing installation of an ESX Server and the Virtual Infrastructure (VI) Client, or multiple hosts and VirtualCenter to manage the hosts.

Set up your ESX Server to use VMware File System (VMFS) or virtual compatibility raw device mappings (RDMs). Consolidated Backup doesn't support RDMs in physical compatibility mode.

For more information, see *Server Configuration Guide* on the VMware Web site at www.vmware.com.

Configuring SAN

After setting up your ESX Server, configure the SAN fabric to which both the ESX Server and the VCB proxy are connected.

The VCB proxy must have access to storage LUNs managed by ESX Server systems. This is accomplished by adding the VCB proxy to the same fabric zones that ESX Server systems belong.

For more information, see documentation provided by your SAN storage array and switch vendors, as well as the *SAN Configuration Guide*.

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

- The VCB proxy must have access to either:
 - All the SAN arrays containing VMFS volumes (datastores) with virtual disks on them.
 - or
 - All the SAN arrays containing virtual compatibility RDMs that are supposed to be backed up using Consolidated Backup.
- For every LUN containing VMFS or RDM data, the LUN ID on the VCB proxy must match the LUN ID as seen by the ESX Server.

-
- NOTE**
- There is no support for EMC AX100 managed with NaviExpress. Use full NaviSphere.
 - IBM ESS should be explicitly configured to have the consistency of LUN ID presentation.
-

Configuring Third-Party Software

You must configure the third-party backup software that you use in conjunction with Consolidated Backup. This involves enabling the use of the Consolidated Backup pre-scripts and post-scripts for your backup software. You might have to turn on the cross junctions (mount points) option for your backup software.

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

For any specific instructions, consult documentation included in the integration module that corresponds to your backup software. For information on integration modules, see [“Installing a Backup Software Integration Module”](#) on page 37.

Client Settings for File-Level Incremental and Differential Backups

When configuring third-party backup software to perform incremental or differential backups, make sure that the backup client running on the VCB proxy ignores the following functions. 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 or shouldn't be backed up. Configure the backup client to use time stamps instead.
- Windows change journal for incremental backups.

If your backup software requires that the Windows archive bit and change journal functions are turned off, the `README.html` file included in the integration module provides directions to turn off these functions.

Configuring VCB Proxy

You need to configure a VCB backup proxy, a physical machine that runs Consolidated Backup and your third-party backup software.

See these sections for more information:

- [“Hardware Requirements”](#) on page 33
- [“Prerequisites”](#) on page 33

Hardware Requirements

The VCB proxy must be able to run Microsoft Windows 2003. In addition, the proxy requires the following hardware components:

- Network adapter (NIC)
- Fibre Channel host bus adapter (HBA)

Prerequisites

To be able to install Consolidated Backup on the VCB proxy, make sure that the following requirements are met:

- The proxy is running Microsoft Windows 2003. Consolidated Backup doesn't support any other versions of Windows on the proxy.
- Networking on the backup proxy is configured so that the proxy can establish a connection to VirtualCenter.

If there is a firewall between the backup proxy and the VirtualCenter, the firewall must permit TCP/IP connections to VirtualCenter. By default, VirtualCenter expects incoming connections at TCP/IP port 902.

For information on configuring Networking, see *Server Configuration Guide*.

- The third-party backup software to be used with Consolidated Backup is installed and correctly configured.

Verify the configuration of the third-party backup software at this time by running a backup and restoration job on a local directory on the VCB proxy.

For more information, see [“Configuring Third-Party Software”](#) on page 32.

Configuring Windows on the VCB Proxy

After setting up the VCB proxy, you need to configure Windows that runs on the proxy. Configuring Windows involves the following:

- [“Disabling Automatic Drive-Letter Assignment”](#) on page 34
- [“Installing VMware Consolidated Backup”](#) on page 35
- [“Configuring VMware Consolidated Backup”](#) on page 35
- [“Installing a Backup Software Integration Module”](#) on page 37

Disabling Automatic Drive-Letter Assignment

All versions of Windows, except Windows 2003 Enterprise Edition and Windows 2003 Datacenter Edition, automatically assign drive letters to each visible new technology file system (NTFS) and file allocation table (FAT) volume.

For Consolidated Backup, change this default behavior so that volumes are not automatically mounted on the proxy.



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

To prevent Windows from automatically assigning drive letters to RDM

- 1 Shut down the Windows proxy.
- 2 Disconnect the Windows proxy from the SAN or mask all the LUNs containing VMFS volumes or RDM for virtual machines.
- 3 Boot the proxy and log into an account with administrator privileges.
- 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 Windows proxy to the SAN, or unmask all previously masked LUNs containing either VMFS volumes or RDM.
- 11 Boot the proxy.

Installing VMware Consolidated Backup

You are now ready to install Consolidated Backup base package on the VCB proxy.

To install the basic Consolidated Backup

- 1 Log into 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.

You now have Consolidated Backup installed on your VCB proxy.

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` within the installation directory for Consolidated Backup.

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 attempting any 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/port of the VirtualCenter server or the ESX Server peer used by the VCB proxy.
PORT	902	Port number to connect to on the VirtualCenter or ESX Server peer.
USERNAME	(no default)	User ID to be used for logging into the VirtualCenter host or ESX Server peer.
PASSWORD	(no default)	Password to be used for logging into the VirtualCenter host or ESX Server peer.
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. This is the default used most of the time. ■ manual: Consolidated Backup does not create or delete any snapshots but assumes that a backup snapshot named <code>_VCB_BACKUP_</code> already exists and uses this snapshot for backup purposes. 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 if you need to run a verification job. Your verification script would then be responsible for tearing down the mount. ■ deleteonly: Consolidated Backup assumes that a backup snapshot named <code>_VCB_BACKUP_</code> already 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.

Installing a Backup Software Integration Module

Finally, 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. This module is a ZIP file containing all the required pre-backup and post-backup scripts.

The ZIP file contains a `README.html` file that describes how to install the integration module on the respective third-party backup software. In addition, the `README.html` file provides any specific instructions you need to configure your backup software for Consolidated Backup.

For more information on configuring your backup software, see [“Configuring Third-Party Software”](#) on page 32.

Configuring Virtual Machines for Consolidated Backup

In general, no particular configuration is required within the virtual machine to support Consolidated Backup.

However, you must install a new version of VMware Tools corresponding to ESX Server in each protected virtual machine. Without installing VMware Tools, the snapshots that Consolidated Backup creates for backup will be crash-consistent only. That is, no file system synchronization will be performed.

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. For more information, refer to a `README.html` file that comes with your backup software integration module.

Follow these general guidelines when using Consolidated Backup:

- 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 38.

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 38.
- When you perform a first backup for a particular virtual machine, power on this virtual machine. See [“First-Time Backup”](#) on page 39.

Before using Consolidated Backup, check the following:

- Your VCB proxy doesn’t run any third-party multipathing software nor has multiple paths to a SAN LUN showing up. See [“Disabling Multipathing”](#) on page 49 for more information.
- Each SAN LUN containing VMFS or RDM data is presented to the VCB proxy and ESX Server system with the same LUN ID. See [“Configuring Identical SAN LUN IDs”](#) on page 49.

Grouping Virtual Machines

If you have multiple virtual machines to back up, group these virtual machines and set up different aliases for these 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 entire 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 on how to configure backup jobs for your virtual machines are different for each individual software. For details, refer to the `README.html` file provided with the integration module for your third-party backup software.

When configuring backup jobs, follow these general 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 plan to 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.



CAUTION When running backup jobs, keep in mind the following:

- Running two backup jobs on the same VCB proxy, one that performs an image-level backup for one virtual machine and another that performs a file-level backup for another virtual machine, can trigger a failure of one of these operations. If this happens, restart the failed operation.
 - 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 particular virtual machine, the virtual machine has to be powered on, or the backup fails on ESX Server.

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 some 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.

For more information, see:

- [“Running Custom Quiescing Scripts”](#) on page 40
- [“Canceling a Backup Job”](#) on page 41

Running Custom Quiescing Scripts

When you use Consolidated Backup, your virtual machines are automatically 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, thus making file systems consistent.

The SYNC driver is not supported on the following operating systems:

- 64-bit guest operating systems
- Any operating system other than Windows

To run custom quiescing scripts

Running the scripts involves the following steps.

Step 1 Running a pre-freeze script

Consolidated Backup runs the following 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.

Step 2 Engaging the SYNC driver (optional)

Engage the SYNC driver to hold incoming I/O and flush all dirty data to a disk. This helps to make the file systems consistent.

If this step fails, proceed to step 5.

Step 3 Creating a snapshot

An actual quiescent snapshot of your virtual machine is created. If this step takes too long and times out, the snapshot create operation fails and the snapshot is deleted. Proceed to step 5.

Step 4 Disengaging 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.

Step 5 Running post-thaw script

Consolidated Backup runs the following 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 should be 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 to be 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.

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.

Run this 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>
```

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 Your Files Using VMware Consolidated Backup”](#) on page 44
- [“Restoring Files Using the vcbRestore Utility”](#) on page 45
- [“Data Recovery”](#) on page 45

Restoring Your Files Using VMware Consolidated Backup

Consolidated Backup helps you perform a file-level restore of the data backed up from your virtual machines.

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

In general, three restoration workflows are supported:

- No backup software in 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 44
- Backup software in dedicated virtual machines and data moved to target virtual machines. See [“Per-Group Restore”](#) on page 44.
- Backup software deployed in every protected virtual machine. Restoration is done directly by the system administrator or the user. See [“Self-Service Restore”](#) on page 45.

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 are planning to use to restore your data. In this case, 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.

Pros: The number of agents to maintain is minimal.

Cons: 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.

Pros:

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

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

Self-Service Restore

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.

Pros: This process is a self-service restoration.

Cons: Agents are required in each virtual machine.

Restoring Files Using the vcbRestore Utility

The `vcbRestore` utility is a command-line utility that you use to restore data that has been backed up using image-based backup.

For information on how to use this utility, see [“Using Service Console to Back Up and Restore Virtual Machines”](#) on page 53.

Data Recovery

The following guidelines can help you in recovering 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 greatly 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 48
- [“Typical Consolidated Backup Usage Scenario”](#) on page 48
- [“Troubleshooting”](#) on page 49

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 automatically.
- 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 peer, and requests it 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 its ESX Server peer 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:

- [“Configuring Identical SAN LUN IDs”](#) on page 49
- [“Disabling Multipathing”](#) on page 49
- [“Changing Backup Policies after ESX Server Upgrades”](#) on page 51
- [“Identifying VMFS Volumes in Backup GUI”](#) on page 51

Configuring Identical SAN LUN IDs

When configuring SAN for Consolidated Backup, make sure that for every LUN containing VMFS or RDM data, the LUN ID on the VCB proxy matches the LUN ID seen by the ESX Server system.

Because instructions on how to configure identical SAN LUN IDs are vendor-specific, you should consult your storage array documentation for more information.

Disabling Multipathing

Consolidated Backup doesn’t support multipathing. As a result, you can’t have any third-party multipathing software installed on your VCB proxy or any multiple paths to a SAN LUN showing up on the VCB proxy.

If you have multipathing software, such as EMC PowerPath, or if you have inactive paths that have not been disabled on the VCB proxy, Consolidated Backup may fail:

- Image-level backups will fail with the following error message:
Error: Failed to export the disk: The device is not ready.
- File-level backups for Windows virtual machines will fail to mount the file systems in the virtual machine's disk images.

To be able to run Consolidated Backup, uninstall multipathing software and deactivate all inactive paths on the VCB proxy.

To disable inactive paths on the VCB proxy

- 1 Log on to your VCB proxy as a user with administrative privileges.
- 2 Click Start. Right-click **My Computer** in the Start menu and select **Manage**.

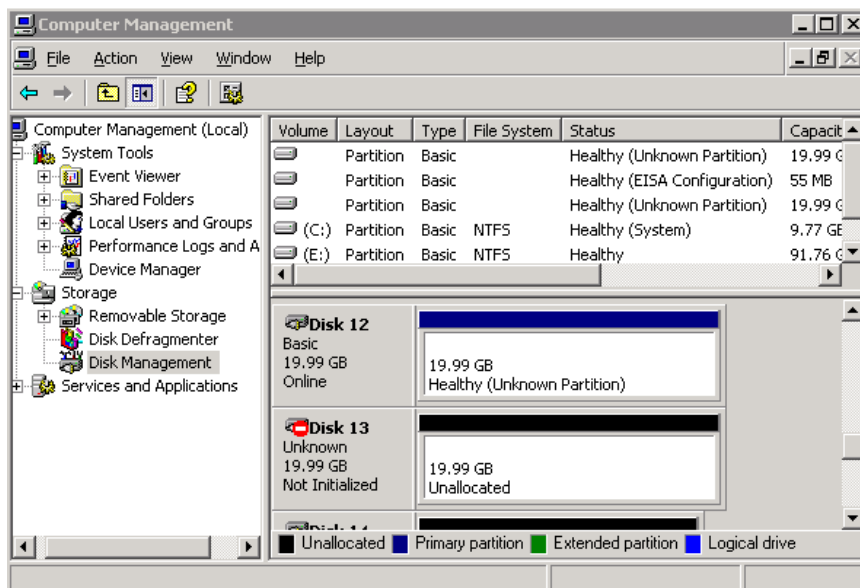
The Computer Management window opens.

- 3 In the Computer Management window, select **Storage > Disk Management**.

If the Initialize and Convert Disk Wizard opens, close it.

The lower right portion of the Computer Management window displays a list of all disks visible to the system.

Inactive paths to disks are indicated by a No Entry icon placed over the disk. The following example shows Disk 13 as an inactive path:



- 4 To disable an inactive path, right-click its icon and select **Properties** from the context menu.

The Disk Drive Properties dialog box opens.

- 5 On the **General** tab, change the value for Device usage to **Do not use this device (disable)**.

This removes the disk from the list of devices presented by Disk Management.

- 6 Repeat [Step 4](#) and [Step 5](#) for all inactive paths.

If you need to activate a path again, or if you have accidentally disabled the wrong path, you can re-enable the devices.

To activate paths on the VCB proxy

- 1 Log on to your VCB proxy as a user with administrative privileges.
- 2 Click Start. Right-click **My Computer** in the Start menu and select **Manage**.
The Computer Management window opens.
- 3 In the Computer Management window, select **System Tools > Device Manager**.
- 4 Click **Disk drives**.
A list of all disks and paths available to your system opens.
- 5 Right-click a disk symbol of the disk you want to activate.
The Device Properties dialog box opens.
- 6 Set the Device usage value to **Use this device (enable)**.

Changing Backup Policies after ESX Server Upgrades

If you have upgraded your ESX Server software 2.x to 3.x, you need to modify all VMFS volume paths that you configured in the backup software. A path format that ESX Server 3.x uses 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

In ESX 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 automatically during formatting, and you cannot change it.

VMFS volumes can have user-friendly labels. These labels show up 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 the 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.

This appendix includes the following sections:

- [“General Configuration Settings for Consolidated Backup Utilities”](#) on page 54
- [“Backing Up Virtual Machines”](#) on page 56
- [“Restoring Virtual Machines”](#) on page 60

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 general 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 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 into 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.



WARNING 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 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 host, the ESX Server 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 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.
For information on identifying virtual machines, see [“Identifying Virtual Machines”](#) on page 57.
- 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. For more information, see [“Specifying Backup Destinations”](#) on page 59.

Performing Backups

After setting up configuration options as described in [“Configuration File Settings”](#) on page 54, enter the following command in the command line:

```
vcbMounter -a <virtual_machine_identifier> -r <backup_destination> ,
```

where

- `<virtual_machine_identifier>` is a unique identifier of the virtual machine you’re backing up. For more information, see [“Identifying Virtual Machines”](#) on page 57.
- `<backup_destination>` specifies the location for backup data. For more information, see [“Specifying Backup Destinations”](#) on page 59.

NOTE When backing up a group of virtual machines, use the `vcbSnapAll` command instead of `vcbMounter`. For information on how to identify the group you want to back up, see [“Identifying Groups of Virtual Machines”](#) on page 58.

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. You can use Consolidated Backup's 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 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 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 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 first, and then performs 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 doesn't need to be parsed each time the identifier is used.

Identifying Groups of Virtual Machines

When you need to back up a group of virtual machines, you use the `vcbSnapAll` command instead of `vcbMounter`. Identify a specific group by using 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:` – Doesn't find any virtual machines. You can use this option for testing.

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, you can specify the path to the directory or use the file transport plug-in descriptor.

For example, to back up a virtual machine to the local directory `/home/VMs/vm37`, use one of the following specifiers:

- `/home/VMs/vm37`
- `file://home/VMs/vm37`

NOTE You don't 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 backing up a virtual machine to a remote server, you can use a corresponding `scp` plug-in. Use the following syntax:

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

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

For example, you need 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 already exists on the remote server. However, you do not need to create the `/backups/VMs/vm37` directory because it will be created during the backup operation.

Restoring Virtual Machines

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

See the following sections:

- [“Restoring Virtual Machines to Original Locations”](#) on page 60
- [“Restoring Virtual Machines to Alternative Locations”](#) on page 60

Restoring Virtual Machines to Original Locations

If you set up all configuration options as described in [“Configuration File Settings”](#) on page 54, the following is the only command you need to pass to `vcbRestore` to restore a virtual machine:

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

For information on how to specify a backup directory, see [“Specifying Backup Destinations”](#) on page 59.

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 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 61.

- 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 61.

- 3 Restore the virtual machine using `vcbRestore`.

See [“Restoring Virtual Machines Using an Alternate Catalog”](#) on page 63

Copying a Catalog File

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

For example, you need to 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 Servers 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` doesn't 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. It is highly recommended 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 VirtualCenter 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 54.

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

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 Servers 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 54.

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

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 ESX Server 2.5.x to ESX Server 3.x



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

This appendix includes the following sections:

- [“Setting Configuration Parameters”](#) on page 66
- [“Restoring ESX 2.5.x Server Virtual Machines”](#) on page 67

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 54.

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 `oldvms` datastore using the base name of the virtual machine's `.vmx` file, enter the following:

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

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

VMHOST

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

RESOURCEPOOL

Specifies the resource pool for the virtual machine you restore. For more information on this parameter, see [“Changing Resource Pools”](#) on page 62.

NOTE Make sure to 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 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. For more information on this parameter, see [“Changing Folder Paths”](#) on page 62.

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.

For more information, see [“Restoring Virtual Machines”](#) on page 60.

Index

A

- aliases **38**
- archive bit **32**

B

- backup clients
 - about **15**
 - in a virtual machine **18**
 - in the service console **19**
- backup jobs
 - canceling **41**
 - setting up **38**
- backup policies, modifying **51**
- backup schedulers **15**
- backup servers **15**
- backup utilities **54**
- backups
 - differential **12**
 - file-level **29**
 - from NFS **21**
 - from SAN **20**
 - image-level **29**
 - incremental **12**
 - overview **12**
 - performing first **39**
 - sample scenario **48**
 - techniques **15**
 - traditional **16**
- backuptools.conf file **54**
- BIOS UUID **57**

C

- catalog files **61**
- change journal **32**
- CIFS **44**
- Common Internet File System protocol **44**
- configuration file
 - backup utilities **54**
 - Consolidated Backup **35**
- Consolidated Backup
 - and snapshots **28**
 - and third-party backup software **26**
 - configuration file **35**
 - configuring SAN **31**
 - configuring third-party software **32**
 - configuring VCB proxy **33**
 - considerations **21**
 - customizing **39**
 - features **24**
 - file-level backups **29**
 - image-level backups **29**
 - installing **35**
 - interoperability modules **37**
 - limitations **30**
 - overview **25**
 - performing first backup **39**
 - prerequisites **26**
 - running **37**
 - setting up backup jobs **38**
 - turning off drive-letter assignment **34**

- utilities **54**
- versus traditional backup methods **21**
- VMware Tools **37**

D

- directory, /vmfs/volumes **14**
- disaster recovery **45**
- disk images, exporting **29**
- DNS name **57**
- drive letters **34**

E

- ESX Server 2.5.x **65**
- ESX Server, upgrading **51**

F

- file allocation table **34**
- files
 - .vmdk **13**
 - .vmx **13**

I

- incremental backups
 - archive bit **32**
- interoperability modules
 - about **25**
 - installing **37**
- IP address **57**

J

- junction points
 - about **29**
 - turning on **32**

K

- knowledge base
 - accessing **10**

M

- MoRef **58**

N

- new technology file system **34**
- NFS storage and backups **21**

P

- physical compatibility **14**

Q

- quiescing
 - about **12**
 - customizing **40**

R

- raw device mapping **14**
- RDM
 - physical compatibility **14**
 - turning off drive-letter assignment **34**
 - virtual compatibility **14**
- README.html file **37**
- restorations
 - centralized **44**
 - ESX Server 2.5.x virtual machines **65**
 - file-based **44**
 - per-group **44**
 - self-service **45**
 - vcbRestore utility **45**
 - workflows **44**

S

- SAN storage
 - and backups **20**
 - configuring for VCB **31**
- schedulers **15**

- SCSI disks **13**
- service console **13**
 - backing up **16**
 - file-based backups **17**
 - image-based backups **17**
- snapshots
 - about **28**
 - and DBHammer **30**
- SYNC driver **30**

T

- third-party software
 - configuring for VCB **32**
 - interoperability modules **25**
 - turning off archive bit **32**
 - turning off change journal **32**
 - working with Consolidated Backup **26**
- time stamps **32**
- traditional backup methods **17**
- troubleshooting
 - backup software GUI **51**
 - path formats **51**

U

- user groups
 - accessing **10**
- utilities
 - Consolidated Backup **54**
 - vcbMounter **56**
 - vcbRestore **45, 60**

V

- VCB proxy **26**
 - about **12**
 - and networking **33**
 - hardware **33**
 - installing Consolidated Backup **35**

- junction points **29**
- requirements **33**
- running Windows **34**
- setting up **33**
- turning off drive-letter assignment **34**

VCB, see Consolidated Backup

- vcbMounter
 - destinations **59**
 - overview **56**
 - performing backups **56**
 - specifying virtual machines **57**

- vcbRestore **60**
 - catalog files **61**
 - default use **63**
 - restoring to alternative locations **60**
 - restoring to original locations **60**

virtual compatibility **14**

- virtual disks
 - manipulating **14**
 - storing **13**

- virtual machines
 - aliases **38**
 - groups **38**

VMFS **13**

vmkfstools commands **14**

VMware community forums

- accessing **10**

VMware Tools **37**

W

Windows archive bit **32**

Windows change journal **32**

workflow **26**

Updates for the Virtual Machine Backup Guide

Last Updated: November 21, 2007

This document provides you with updates to ESX Server 3.0.1 and VirtualCenter 2.0.1 version of the *Virtual Machine Backup Guide*. Updated descriptions are organized by page number so 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 a list of *Virtual Machine Backup Guide* page updates in this document:

- [“Updates for the Software and Hardware Requirements on Page 25”](#)
- [“Updates for the Creating Snapshots Discussion on Page 28”](#)

Updates for the Software and Hardware Requirements on Page 25

The Consolidated Backup Software and Hardware Requirements section on this page should mention that the VCB proxy supports only 32-bit versions of Microsoft Windows. Microsoft Windows 64-bit is not supported.

Updates for the Creating Snapshots Discussion on Page 28

The note on this page suggests that file-system-consistent snapshots can be created for virtual machines that run any Windows guest operating system. However, you should be aware that Windows NT4 guest operating system does not guarantee the file system consistency.

