



**EMC® AVAMAR®**  
**FOR VMWARE GUIDE**  
**5.0**

**P/N 300-010-712**  
**REV A01**

**EMC CORPORATION**  
*CORPORATE HEADQUARTERS:*  
HOPKINTON, MA 01748-9103  
1-508-435-1000  
[www.EMC.com](http://www.EMC.com)

## Copyright and Trademark Notices

This document contains information proprietary to EMC Corporation. Due to continuing product development, product specifications and capabilities are subject to change without notice. You may not disclose or use any proprietary information or reproduce or transmit any part of this document in any form or by any means, electronic or mechanical, for any purpose, without written permission from EMC Corporation.

EMC Corporation has made every effort to keep the information in this document current and accurate as of the date of publication or revision. However, EMC Corporation does not guarantee or imply that this document is error free or accurate with regard to any particular specification. In no event will EMC Corporation be liable for direct, indirect, incidental, or consequential damages resulting from any defect in the documentation, even if advised of the possibility of such damages. No EMC Corporation agent or employee is authorized to make any modification, extension, or addition to the above statements.

EMC Corporation may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

The Avamar Agent for Microsoft Windows incorporates Open Transaction Manager (OTM), a product of Columbia Data Products, Inc. (CDP). CDP assumes no liability for any claim that may arise regarding this incorporation. In addition, EMC Corporation disclaims all warranties, both express and implied, arising from the use of Open Transaction Manager. Copyright 1999-2002 Columbia Data Products, Inc. Altamonte Springs. All rights reserved.

Avamar is a registered trademark of EMC Corporation in the US and/or other countries.

All other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All information presented here is subject to change and intended for general information.

Copyright 2002-2010 EMC Corporation. All rights reserved.

Printed in the USA.

# TABLE OF CONTENTS

---

- Foreword .....6**
  - Scope and Intended Audience ..... 6
  - Product Information ..... 6
  - Your Comments ..... 7
  - Typeface Conventions ..... 7
  - Notes, Tips, and Warnings ..... 8
  
- Introduction .....9**
  - Choosing a Data Protection Method ..... 10
    - ESX Server Version ..... 10
    - Ease of Implementation ..... 11
    - Efficiency ..... 12
    - Backup and Restore ..... 13
    - Required VMware Knowledge ..... 14
    - Important Differences Between Filesystem and Image Backups ..... 15
  - Additional Resources ..... 16
  
- Guest Backup and Restore .....17**
  - Capabilities and Limitations ..... 18
  - Installation and Configuration ..... 19
  - On-Demand Backups ..... 20
  - Directory (Folder) and File Restores ..... 20
  - Full System Restores Using Guest Backups ..... 21
  
- Avamar VMware Image Backup and Restore .....22**
  - Requirements ..... 23
  - Capabilities and Limitations ..... 23
  - Information Roadmap ..... 28
  
- Avamar VMware Image Backup and Restore Configuration and Setup 29**
  - Configuring the vCenter Environment ..... 29
    - Task 1: Download and Install vSphere Client Software ..... 30
    - Task 2: Create Dedicated vCenter User Account ..... 30
    - Task 3: Deploy One or More Avamar Image Backup Proxies ..... 31
  - Configuring vCenter-to-Avamar Authentication ..... 44
    - Option 1: Installing an Authentication Certificate on the Avamar MCS ..... 44
    - Option 2: Turning Off Certificate Authentication  
for All vCenter-to-Avamar MCS Communications ..... 46

Configuring the Avamar Environment . . . . .	47
Task 1: Download and Install Avamar Administrator Software . . . . .	48
Task 2: Add vCenter Client . . . . .	49
Task 3: Add Avamar VMware Image Proxy Client . . . . .	51
Task 4: Add Virtual Machine Clients . . . . .	51
Protecting Virtual Machines with Both Guest and Avamar VMware Image Backup . . . . .	52
<b>Using Avamar VMware Image Backup and Restore . . . . .</b>	<b>53</b>
Basic Client Administration . . . . .	54
How VMware Clients Appear in Avamar Administrator . . . . .	54
Adding and Activating a VMware Image Proxy Client . . . . .	55
Adding Virtual Machine Clients . . . . .	56
Editing Existing VMware Clients . . . . .	61
Viewing Protected Virtual Machines . . . . .	62
Viewing Replicated Virtual Machine Name . . . . .	63
VMware vCenter Connection Monitor . . . . .	64
Backup and Restore . . . . .	65
Performing an On-Demand VMware Image Backup . . . . .	65
Monitoring Backup and Restore Activities . . . . .	67
Backup Validation . . . . .	67
Viewing Backup Statistics . . . . .	67
Image Restore Overview . . . . .	68
Restoring to the Original Virtual Machine . . . . .	69
Restoring to a Different (Existing) Virtual Machine . . . . .	70
Restoring to a New Virtual Machine . . . . .	72
Groups and Policy Management . . . . .	75
Groups and Group Behavior . . . . .	75
Editing the Default Virtual Machine Group and Other vCenter Groups . . . . .	77
VMware Image Dataset . . . . .	79
Troubleshooting . . . . .	80
<b>Optional Windows File-Level Restore . . . . .</b>	<b>81</b>
Capabilities and Limitations . . . . .	81
Configuration and Setup . . . . .	83
Task 1: Configure and Set Up Avamar File System (AvFS) . . . . .	83
Task 2: Modify mcserver.xml Preferences . . . . .	84
Task 3: Prepare and Deploy Windows File-Level Restore Proxy . . . . .	85
Restoring Folders or Files from a VMware Image Backup . . . . .	91
<b>Protecting the vCenter Management Infrastructure . . . . .</b>	<b>94</b>
Backing Up the vCenter Management Infrastructure . . . . .	95
Task 1: Implement Guest Backups or VMware Image Backups . . . . .	95
Task 2: Define Custom Dataset for vCenter Backups . . . . .	96
Task 3: Add a Backup Client for vCenter Database Hosts . . . . .	97
Recovering vCenter Management Infrastructure Using Avamar Backups . . . . .	98
<b>Best Practices . . . . .</b>	<b>99</b>
<b>Appendix A — Avamar VCB Integration . . . . .</b>	<b>100</b>
Requirements . . . . .	101
Capabilities and Limitations . . . . .	102

---

Installation and Configuration. . . . .	103
Install Avamar Windows Client on Proxy Server . . . . .	103
Install AVIM on Proxy Server . . . . .	103
Create Custom Avamar Dataset . . . . .	104
Performing VCB Backups. . . . .	107
Restoring a Virtual Machine from VCB Backups . . . . .	107
Restoring a Virtual Machine from a Full VCB Backup . . . . .	107
Restoring a Virtual Machine from a File-Level Backup . . . . .	108
Restoring with the VMware vCenter Converter Standalone tool . . . . .	108
<b>Appendix B — ESX Server Backup and Restore . . . . .</b>	<b>109</b>
Capabilities and Limitations . . . . .	110
Installing and Configuring ESX Server Backup and Restore . . . . .	111
Install the Avamar Linux Client on the ESX Server . . . . .	111
Configure ESX Server Firewall . . . . .	111
Performing an ESX Server Backup . . . . .	112
Create Virtual Machine Snapshots . . . . .	112
Back Up Virtual Machine Snapshots to the Avamar Server. . . . .	113
Remove Temporary Snapshot Files . . . . .	113
Performing a Restore Using ESX Server Backups . . . . .	114
<b>Appendix C — vSphere Data Ports . . . . .</b>	<b>115</b>
<b>Index . . . . .</b>	<b>116</b>

# FOREWORD

---

## Scope and Intended Audience

**Scope.** This publication describes various methods and strategies for protecting VMware virtual machines.

**Intended Audience.** The information in this publication is intended for use by system administrators familiar with:

- Basic Avamar system administration principles and procedures found in the *Avamar System Administration Guide*
- Other Avamar client software information (primarily installation and configuration procedures) found in various Avamar client guides

---

**NOTE:** A comprehensive discussion of certain basic Avamar system administration concepts and principles, such as clients, datasets, schedules, retention policies, groups and group policy, is beyond the scope of this publication. Refer to your *Avamar System Administration Guide* for additional information.

---

## Product Information

For current documentation, release notes, software updates, information about EMC products, licensing and service, go to the EMC Powerlink website at <http://Powerlink.EMC.com>.

## Your Comments

Your suggestions will help us continue to improve the accuracy, organization and overall quality of our publications. You may email your comments to:

BSGDocumentation@emc.com

Please include the following information:

- Product name and version
- Document name, part number, and revision (for example, A01)
- Page numbers
- Other details that will help us address the documentation issue

## Typeface Conventions

The following table provides examples of standard typeface styles used in this publication to convey various kinds of information.

EXAMPLE	DESCRIPTION
Click <b>OK</b> . or Select <b>File &gt; Close</b> .	Bold text denotes actual buttons, commands, menus and options that initiate action. Sequential commands are separated by a greater-than (>) character. For example, the second example instructs you to select the <b>Close</b> command from the <b>File</b> menu.
Type: <b>cd /tmp</b>	Bold fixed-width text denotes shell commands that must be entered exactly as they appear.
--logfile=FILE	All caps text often denotes a placeholder (token) for an actual value that must be supplied by the user. In this example, FILE would be an actual filename.
Installation Complete.	Regular (not bold) fixed-width text denotes command shell messages, code and file contents.

## Notes, Tips, and Warnings

The following kinds of notes, tips, and warnings appear in this publication:

---

**IMPORTANT:** This is a warning. Warnings always contain information that if not heeded could result in unpredictable system behavior or loss of data.

---

---

**TIP:** This is a tip. Tips present optional information intended to improve your productivity or otherwise enhance your experience with the product. Tips never contain information that will cause a failure if ignored.

---

---

**NOTE:** This is a general note. Notes contain ancillary information intended to clarify a topic or procedure. Notes never contain information that will cause a failure if ignored.

---

# INTRODUCTION

---

EMC® Avamar® currently offers four different methods for protecting virtual machines residing in various VMware environments:

**Guest Backup and Restore.** Guest backup and restore is simply installing Avamar client software in a virtual machine just as if it were a physical machine, then registering and activating that client with an Avamar server. Refer to *Guest Backup and Restore* (page 17) for additional information.

**VMware Image Backup and Restore.** Avamar VMware image backup and restore is built on the VMware vStorage API for Data Protection (VADP). It is fully integrated with VMware vCenter Server to provide easy detection of virtual machine clients within the vCenter and enable efficient centralized management of backup jobs. Refer to *Avamar VMware Image Backup and Restore* (page 22) for additional information.

---

**IMPORTANT:** In addition to protecting individual virtual machines with either guest backup or Avamar VMware image backup and restore, you should also protect your vCenter management infrastructure. Refer to *Protecting the vCenter Management Infrastructure* (page 94) for additional information.

---

**Integration with VMware Consolidated Backup (VCB).** Avamar provides a script-based integration with VMware Consolidated Backup (VCB) running on ESX 3.x servers. Refer to *Appendix A — Avamar VCB Integration* (page 100) for additional information.

**ESX Server Backup and Restore.** Although this method of data protection is officially discouraged by VMware, it is possible to install Avamar client software inside the ESX server maintenance console in order to take image backups of the entire ESX server. Refer to *Appendix B — ESX Server Backup and Restore* (page 109) for additional information.

## Choosing a Data Protection Method

This topic explores the various advantages and considerations associated with each data protection method in each of the following contexts:

- *ESX Server Version* (page 10)
- *Ease of Implementation* (page 11)
- *Efficiency* (page 12)
- *Backup and Restore* (page 13)
- *Required VMware Knowledge* (page 14)

---

**IMPORTANT:** Due to significant limitations, Avamar VMware Consolidated Backup (VCB) integration and ESX Server backup and restore should only be considered under very special circumstances in which either guest backup or Avamar VMware image backup and restore has been deemed inappropriate. For this reason, documentation for these methods is presented in appendices.

---

### ESX Server Version

If you will be using a method other than guest backup to protect virtual machine data, your specific ESX server version will be an important consideration in determining which data protection method will best suit your particular needs.

METHOD	ESX SERVER VERSION		
	4.0.X	3.X	2.5.3
Guest Backup and Restore	YES	YES	YES
Avamar VMware Image Backup and Restore	YES	NO	NO
Avamar VMware Consolidated Backup (VCB) Integration	NO	YES	NO
ESX Server Backup and Restore	NO	YES	YES

---

**NOTE:** Guest backup is not directly dependent on ESX server version, but instead is dependent on whether or not a specific type and version virtual machine is supported by Avamar client software. Nonetheless, guest backup was included in the previous table to emphasize that it is a viable data protection method for most VMware environments.

---

## Ease of Implementation

METHOD	ADVANTAGES/CONSIDERATIONS
Guest Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Supports any virtual machine running an operating system for which Avamar client software is available</li> <li>• Supports applications such as DB2, Exchange, Oracle and SQL Server databases</li> <li>• Easily fits into most existing backup schemes; day-to-day backup procedures do not change</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Avamar client software must be individually installed and managed inside each virtual machine</li> </ul>
Avamar VMware Image Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Avamar client software is not individually installed and managed inside each virtual machine</li> <li>• Can leverage vCenter to discover virtual machines and add them to the Avamar server in batches</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Requires moderate amount of initial setup and configuration</li> </ul>
Avamar VMware Consolidated Backup (VCB) Integration	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Supports ESX 3.x servers</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Requires high degree of initial setup and configuration</li> <li>• Requires advanced scripting and VMware knowledge including working knowledge of Console Operating System (COS) shell commands and ability to log into COS as root</li> </ul>
ESX Server Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Supports ESX 3.5, 3.0.x, 2.5.3 servers</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Requires high degree of initial setup and configuration</li> <li>• Requires advanced scripting and VMware knowledge including working knowledge of Console Operating System (COS) shell commands and ability to log into COS as root</li> <li>• Cross-version restores not supported (that is, you can only restore an ESX server backup to exactly the same version ESX server)</li> <li>• Uses substantial amount of CPU, RAM and disk resources inside the COS, which is only minimally provisioned</li> </ul> <p><b>IMPORTANT:</b> VMware officially discourages this data protection method.</p>

## Efficiency

METHOD	DESCRIPTION
Guest Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Offers highest level of data deduplication efficiency</li> <li>• Does not consume ESX server CPU, RAM and disk resources</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Backups consume guest virtual machine CPU, RAM and disk resources</li> </ul>
Avamar VMware Image Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Moderate deduplication efficiency</li> <li>• Backups do not consume guest virtual machine CPU, RAM and disk resources</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Backups consume ESX server CPU, RAM and disk resources</li> <li>• If changed block tracking is not enabled, each virtual machine image must be fully processed for each backup, likely resulting in unacceptably long backup windows and excessive back-end storage read/write activity</li> </ul>
Avamar VMware Consolidated Backup (VCB) Integration	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Supports ESX 3.x servers</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Low data deduplication efficiency</li> <li>• Each image to be backed up must be copied completely to a proxy server, increasing backup time and time that source client is in snapshot mode</li> </ul>
ESX Server Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>• Supports ESX 3.5, 3.0.x, 2.5.3 servers</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>• Low data deduplication efficiency</li> </ul>

## Backup and Restore

METHOD	DESCRIPTION
Guest Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>Virtual machines are gracefully quiesced prior to each backup, resulting in a more dependable backup</li> <li>Backups are highly optimized (temp files, swap files and so forth not included)</li> <li>Backups are highly customizable (supports full range of include and exclude features)</li> <li>Database backups support transaction log truncation and other advanced features</li> <li>Unused filesystem space is not backed up</li> <li>Individual file and directory (folder) restores supported</li> <li>Backup and restore jobs can execute pre- and post-processing scripts</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>Virtual machines must have a network connection to Avamar server</li> <li>Virtual machines must be running for backups to occur</li> </ul>
Avamar VMware Image Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>Image backups are supported for all virtual machines</li> <li>Individual file and directory (folder) restores supported for Windows virtual machines</li> <li>Virtual machines need not have a network connection to Avamar server</li> <li>Virtual machines need not be running for backups to occur</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>Backups are a "crash-consistent" snapshot of the full virtual machine image, which might or might not reliably support a full system restore without data loss</li> <li>Individual file and directory (folder) restores only supported on Windows virtual machine (requires deployment of additional Windows proxy client)</li> <li>Unused filesystem space is backed up</li> <li>Backups not optimized (temp files, swap files and so forth are included)</li> <li>Backups not customizable (full image must be backed up)</li> </ul>
Avamar VMware Consolidated Backup (VCB) Integration	<p>Advantages:</p> <ul style="list-style-type: none"> <li>Supports ESX 3.x servers</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>Individual file and directory (folder) restores not supported</li> <li>Unused filesystem space is backed up</li> </ul>
ESX Server Backup and Restore	<p>Advantages:</p> <ul style="list-style-type: none"> <li>Supports ESX 3.5, 3.0.x, 2.5.3 servers</li> </ul> <p>Considerations:</p> <ul style="list-style-type: none"> <li>Individual file and directory (folder) restores not supported</li> <li>Unused filesystem space is backed up</li> </ul>

---

**TIP:** A virtual machine can be protected by both guest backup and image backup. For example, a daily guest backup to frequently protect selective files and a less frequent or on-demand full image backup protects the full machine. This scheme accommodates scenarios with limited backup windows.

---

## Required VMware Knowledge

METHOD	ADVANTAGES/CONSIDERATIONS
Guest Backup and Restore	No advanced scripting or VMware knowledge required.
Avamar VMware Image Backup and Restore	Moderate VMware knowledge required. Integrators should have working knowledge of actual vCenter topology in use at that customer site (that is, which ESX servers host each datastore and which datastores store each virtual machine's data) and ability to log into vCenter with administrator privileges.
Avamar VMware Consolidated Backup (VCB) Integration	Advanced scripting and VMware knowledge required. Integrators should have working knowledge of COS shell commands and ability to log into COS as root.
ESX Server Backup and Restore	Advanced scripting and VMware knowledge required. Integrators should have working knowledge of COS shell commands and ability to log into COS as root.

## Important Differences Between Filesystem and Image Backups

Filesystem and image backup exhibit fundamentally different behavior with regard to deduplication:

- A filesystem backup only backs up bytes that are actually contained within files
- An image backup will back up all bytes on a virtual disk whether these bytes are part of a file or not

### Physical Disk New Bytes Calculation

First, consider a 100 GB physical disk with 30 GB of files and none of the files have ever been backed up to the Avamar server. In this case, the percentage of new bytes added to the server in the first backup is:

$$30 \text{ GB divided by } 30 \text{ GB} = 100\%$$

### Virtual Disk New Bytes Calculation

Next, consider a 100 GB virtual machine disk with 30 GB of files in which none of the files have ever been backed up to the Avamar server. In this case, the percentage of new bytes added to the server in the first backup is:

$$30 \text{ GB divided by } 100 \text{ GB} = 30\%$$

Avamar filesystem plugins also offer the ability to exclude certain file types from backups. This exclusion mechanism is not available for VMware image backups.

Creating a file causes bytes on the virtual disk to be written to. This space will be included in all subsequent image backups. This is true even if the file is deleted before a backup occurs.

This behavior with regard to image backups and deleted files is an inherent characteristic of the process and there is no workaround available other than to switch to file based backup if this is a concern. This can be viewed as a desirable feature because features such as undeleting a file from the Windows Recycle bin will work even if the virtual machine is restored from a backup.

Also be aware that with some filesystems and applications, modifying a file might result in an entirely new file being written to the disk along with the old version, which is still present on the disk but not visible in the filesystem. Programs such as Mac OS X Time Machine and various shadow copy utilities behave in this manner.

Therefore, a virtual machine with a small percentage change (from a virtualized filesystem perspective) might actually have many changed bytes due to any of the following reasons:

- Swap files, which tend to change drastically even if they occupy the same location in the virtual machine.
- OS and application log files, which tend to change drastically as part of normal operation.
- Deleted and modified file areas of the disk that hold the filesystem directory.

Be aware that some filesystems maintain a last accessed timestamp for every file and that just reading a file can result in a modification within the file directory metadata.

- Fragmentation effects - a specific file might not occupy contiguous space on the underlying disk. Therefore, a modification to the file might result in changes to "chunks" scattered about the disk.

## Additional Resources

A comprehensive discussion of VMware technology is beyond the scope of this publication. Refer to the following VMware documentation for additional information:

- *Introduction to VMware vSphere*
- *Getting Started with ESX*
- *ESX and vCenter Server Installation Guide*
- *Basic System Administration*
- *vSphere Web Access Administrator's Guide*
- *ESX Configuration Guide*
- *Resource Management Guide*

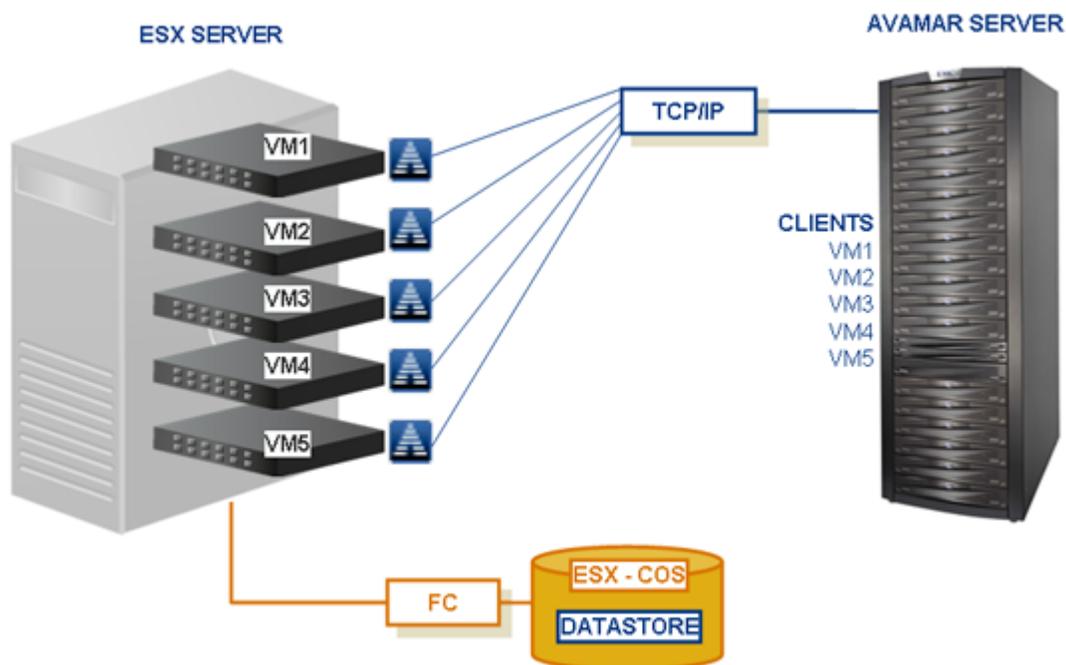
## GUEST BACKUP AND RESTORE

---

This chapter discusses using VMware guest backup and restore to protect virtual machine data.

Guest backup and restore is simply installing Avamar client software in a virtual machine just as if it were a physical machine, then registering and activating that client with an Avamar server.

The following illustration shows a typical guest backup and restore implementation in which an Avamar client agent is installed inside each VMware virtual machine.



## Capabilities and Limitations

This topic discusses the capabilities and limitations of guest backup and restore.

**Capabilities.** Guest protection offers the following capabilities:

- Supports any virtual machine running an operating system for which Avamar client software is available.
- Supports applications such as DB2, Exchange, Oracle and SQL Server databases.
- Easily fits into most existing backup schemes; day-to-day backup procedures do not change.
- Offers highest level of data deduplication efficiency.
- Does not consume ESX server CPU, RAM and disk resources.
- Virtual machine filesystems and databases are gracefully quiesced prior to each backup, resulting in a more dependable backup.
- Backups are highly optimized (temp files, swap files and so forth not included).
- Backups are highly customizable (supports full range of include and exclude features).
- Database backups support transaction log truncation and other advanced features.
- Unused filesystem space is not backed up.
- Individual file and directory (folder) restores supported.
- Backup and restore jobs can execute pre- and post-processing scripts.
- No advanced scripting or VMware knowledge required.

**Limitations.** Consider the following limitations before implementing guest backup and restore:

- Avamar client software must be individually installed and managed inside each virtual machine.
- Backups consume guest virtual machine CPU, RAM and disk resources.
- Virtual machines must have a network connection to Avamar server.
- Virtual machines must be running for backups to occur.
- Full system recovery comprises two distinct tasks:
  - First, you must load a known good operating system image inside the virtual machine.
  - Then, you can restore customer data from the guest backups stored on the Avamar server.

## Installation and Configuration

Guest backup and restore is implemented by installing Avamar client software in a virtual machine just as if it were a physical machine, then registering and activating that client with an Avamar server. No special configuration is required.

Refer to one of the following Avamar client guides for specific instructions about installing that Avamar client software in your virtual machines:

CLIENT	APPLICABLE CLIENT GUIDE
DB2 databases hosted on IBM AIX and Microsoft Windows	<i>Avamar DB2 Client User Guide</i>
FreeBSD filesystems	<i>Avamar Backup Clients User Guide</i>
HP-UX filesystems	<i>Avamar Backup Clients User Guide</i>
IBM AIX filesystems	<i>Avamar Backup Clients User Guide</i>
Lotus Domino databases	<i>Avamar Lotus Domino Client User Guide</i>
Mac OS X filesystems	<i>Avamar Backup Clients User Guide</i>
Microsoft Exchange databases	<i>Avamar Exchange Client User Guide</i>
Microsoft Office SharePoint implementations	<i>Avamar SharePoint Client User Guide</i>
Microsoft SQL Server databases	<i>Avamar SQL Server Client User Guide</i>
Microsoft Windows filesystems	<i>Avamar Backup Clients User Guide</i>
Novell NetWare filesystems	<i>Avamar Backup Clients User Guide</i>
Oracle Databases hosted on IBM AIX, Redhat and SUSE Linux, Sun Solaris and Microsoft Windows	<i>Avamar Oracle Client User Guide</i>
Redhat Linux filesystems	<i>Avamar Backup Clients User Guide</i>
SCO Open Server and UnixWare filesystems	<i>Avamar Backup Clients User Guide</i>
Sun Solaris filesystems	<i>Avamar Backup Clients User Guide</i>
SUSE Linux filesystems	<i>Avamar Backup Clients User Guide</i>

## On-Demand Backups

On-demand backups can be performed in the following manner:

- |   |  |
|---|--|
| Client-Initiated On-Demand Backups                    | <p>You can initiate an on-demand backup directly from the client virtual machine using:</p> <ul style="list-style-type: none"><li>• Avamar tray application on Windows platforms</li><li>• Avamar application icon on Mac OSX platforms</li><li>• Oracle RMAN commands and scripts (Oracle databases only)</li><li>• <b>avtar</b> commands on all other platforms</li></ul> <p>Refer to the correct Avamar client guide for specific instructions about initiating on-demand backups from that client.</p> |
| On-Demand Backups Initiated With Avamar Administrator | <p>Refer to your <i>Avamar System Administration Guide</i> for detailed information about initiating on-demand backups using Avamar Administrator.</p>   |

## Directory (Folder) and File Restores

Directory (folder) and file restores (that is, anything other than full system restores) can be performed in the following manner:

- |  |   |
|--|---|
| Client-Initiated Web Services Restores       | <p>Windows and Mac OSX client virtual machines can restore selected directories (folders) and files using the Avamar Web Services feature.</p> <p>Refer to your <i>Avamar Backup Clients User Guide</i> for additional information.</p> |
| Client-Initiated Command Line Restores       | <p>Client virtual machines other than Windows and Mac OSX must initiate restores and get status using <b>avtar</b> commands.</p> <p>Refer to your <i>Avamar Backup Clients User Guide</i> for additional information.</p>               |
| Restores Initiated With Avamar Administrator | <p>Directory (folder) and file restores can also be initiated with the Avamar Administrator graphical management console.</p> <p>Refer to your <i>Avamar System Administration Guide</i> for additional information.</p>                |

## Full System Restores Using Guest Backups

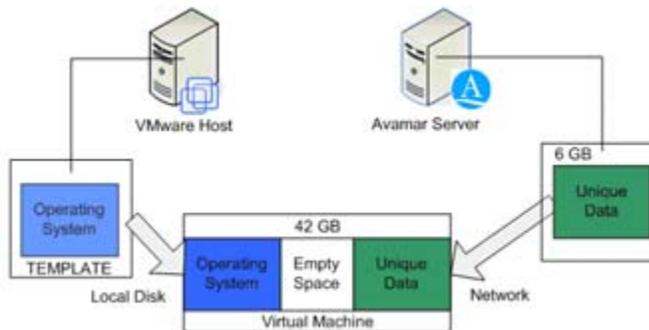
A typical full filesystem restore is performed by first deploying a “bootstrap” virtual machine from a virtual machine template that has a preinstalled Avamar backup agent.

Template deployment of a virtual machine is often faster than a full-image restore. Deploying from a template also typically results in a restored virtual machine that better complies with organizational standards such as security patches, network settings, antivirus signatures, and so forth. Optionally, a template might include fully-patched pre-installed applications, reducing recovery to data files only.

Performing a full system restore using guest backups comprises two tasks:

- *Task 1: Install the Operating System and Avamar Client Software* (page 21)
- *Task 2: Restore Unique Data from Guest Backups on the Avamar Server* (page 21)

The following illustration shows this two-step procedure:



### Task 1: Install the Operating System and Avamar Client Software

In order to perform a full system restore using guest backups, you must first ensure that the virtual machine has a functional operating system image loaded and that the correct Avamar client software is also installed. You can then register and activate the virtual machine with the Avamar server so that you can restore any unique data from a guest backup.

Once the operating system and Avamar client software is installed, activate the client with the Avamar server. Avamar Windows clients register and activate with the Avamar server by way of the Avamar system tray applet. Other Avamar clients register and activate with the Avamar server by running the **avregister** script. You can also activate an Avamar client using Avamar Administrator.

### Task 2: Restore Unique Data from Guest Backups on the Avamar Server

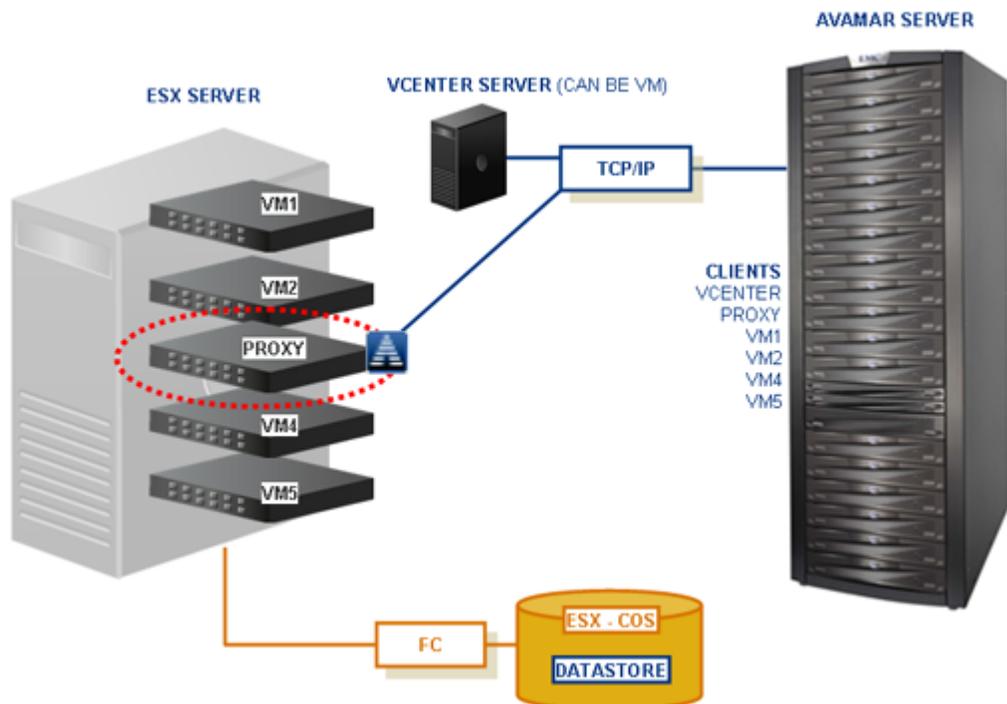
Use the correct restore procedure for your platform to restore any unique data back to the virtual machine.

# AVAMAR VMWARE IMAGE BACKUP AND RESTORE

This chapter introduces and discusses the Avamar VMware image backup and restore feature.

**IMPORTANT:** The Avamar VMware image backup and restore requires ESX Server 4.0 or later; it does not support previous versions of ESX servers. For ESX Server 3.x or earlier environments, refer to *Choosing a Data Protection Method* (page 10) for additional information.

The Avamar VMware image backup and restore is built on the VMware vStorage API for Data Protection (VADP). It is fully integrated with VMware vCenter Server to provide easy detection of virtual machine clients within the vCenter and enable efficient centralized management of backup jobs.



## Requirements

The Avamar VMware image backup and restore feature requires:

- ESX Server version 4.0
- Fiber channel SAN storage hosting VMFS or RDMS
- VMware proxy client machine running Red Hat Linux operating system
- VMware proxy client machine is connected to the vCenter
- Proxy client has access to SAN storage LUNs managed by the ESX Server
- Proxy client must be able to connect by way of TCP/IP ports 443 and 902 to the Service Console interface on the ESX server that hosts the target virtual machines
- Proxy client virtual machine is running
- VMware Tools is installed on proxy client virtual machine
- VMware vCenter installed and running

## Capabilities and Limitations

This topic discusses the capabilities and limitations of Avamar VMware image backup and restore.

**Capabilities.** Avamar VMware image backup and restore offers the following capabilities:

- Avamar client software is not individually installed and managed inside each virtual machine.

---

**NOTE:** It is permissible for Avamar client software to be installed inside a virtual machine (for example, to also support guest backup of that virtual machine), but it is not required for Avamar VMware image backup and restore.

---

- Virtual machines need not have a network connection to Avamar server.
- Virtual machines need not be running for backups to occur.
- Can leverage vCenter to discover virtual machines and add them to the Avamar server in batches.
- Performs global data deduplication across all machines, physical and virtual.

Downstream of the data deduplication engine, only new, unique, variable-length data segments are transmitted across the virtual/physical network infrastructure during backups, from the Avamar proxy virtual machine appliance to the Avamar server.

- Backups do not consume guest virtual machine CPU, RAM and disk resources.
- Image backups supported for all virtual machines.
- Backup content can be restored to the original virtual machine, a new virtual machine, or a pre-existing alternate virtual machine with a configuration similar to the original.

- Backups for selected virtual machines, once stored on the Avamar server, can easily be replicated to additional Avamar servers.
- Virtual machine templates can be backed up.
- Deployment of one or more Avamar proxy virtual machine appliances is required. These appliances consume CPU cycles and memory in small predictable quantities from the ESX host running the appliance.
- Avamar proxy clients do not need to be backed up and backup of proxy clients is not supported. These proxy clients virtual machines are readily redeployed from template if needed.
- Individual folder or file restores are supported for Windows virtual machines that have been backed up using Avamar VMware image backup. This feature requires additional configuration and setup. Refer to *Optional Windows File-Level Restore* (page 81) for additional information.
- Avamar automatically detects when a virtual machine configured for image backup is moved to a new vCenter folder or vmfs datastore and reconfigures the management environment appropriately.

---

**IMPORTANT:** This relocation tracking feature does not apply to virtual machine templates.

---

- Multiple Avamar servers can be deployed to protect a single vCenter.  
This might be desirable for scalability (extremely large vCenters) or as a means to constrain physical backup-related network traffic to local area networks rather than WAN connectivity. If multiple Avamar servers are deployed to protect a single vCenter, the Avamar server configurations should never split a VMware datacenter between multiple Avamar servers. Given one VMware datacenter, exactly one Avamar server will be managing all deployed proxy virtual machine appliances and managing backup for all protected virtual machines.
- A virtual machine can be protected by both guest backup and image backup.  
For example, a daily guest backup to frequently protect selective files and an infrequent or on-demand full image backup protects the full machine. This scheme accommodates scenarios with limited backup windows.  
However, if you decide to use both methods simultaneously on one or more virtual machines, a small amount of additional configuration is required. Refer to *Protecting Virtual Machines with Both Guest and Avamar VMware Image Backup* (page 52) for additional information.
- You can deploy more than one backup proxy.  
The Avamar system automatically distributes workload to the deployed proxies. Multiple proxy capability is desirable for various reasons:
  - Backup workload can be distributed across multiple ESX hosts.
  - Proxies can be positioned at multiple points of SAN LUN connectivity to ensure that SAN transport is always used during backups and restores.
  - A high level of concurrent operations is possible in the backup window.
  - Redundancy leads to higher availability.

**Limitations.** Consider the following limitations before implementing Avamar VMware image backup and restore:

- Requires moderate amount of initial setup and configuration.
- Requires moderate amount of VMware knowledge.
- Integrators should have working knowledge of actual vCenter topology in use at that customer site (that is, which ESX servers host each datastore and which datastores store each virtual machine's data) and ability to log into vCenter with administrator privileges.
- Avamar image backup is dependent on reliable DNS service and time synchronization. Network routing and firewall settings must be properly configured to allow access to the network hosts providing these services.
- SSL certificate installation across the vCenter, ESX host nodes, and Avamar proxy virtual machine appliances is highly desirable. However, SSL certificate authentication can be turned off at the Avamar server.
- Backups consume ESX server CPU, RAM and disk resources.
- Backups are a "crash-consistent" snapshot of the full virtual machine image, which might or might not reliably support a full system restore without data loss.
- Efficiency considerations:
  - Backups are not customizable (full image must be backed up).
  - Backups are not highly optimized (temp files, swap files and so forth are included).
  - Unused filesystem space is backed up.
  - An image backup of a disk includes 100 percent of disk content.

Unlike guest filesystem backup, there is no mechanism to filter captured content such as swap files, hibernation files, browser caches, or even invisible content such as deleted files that have not been overwritten.

Backing up such content unnecessarily consumes bandwidth and storage because deduplication efficiency can be severely reduced.

Retention policies such as time limits on retained email might also be impacted.

This scenario might be mitigated by moving swap files, cache files, and other such content to a separate disk, then excluding that disk from backups.

- Image proxy limitations:
  - An image proxy will only perform one backup at a time. Parallel processing can only be achieved by having more than one proxy in an environment.
  - A proxy can back up either Windows or Linux virtual machines but not both. The type of virtual machine each proxy can back up is set during initial configuration and deployment.
- Avamar VMware image backup of a virtual machine containing an IDE virtual hard disk is not supported primarily because it cannot be backed up using SAN connectivity.

IDE virtual disks are generally discouraged on virtual machines hosted by ESX for performance reasons. Furthermore, IDE virtual disks were not supported on earlier versions of ESX. Therefore this limitation should rarely cause difficulties.

- The image backup process requires temporary creation of a VMware virtual machine snapshot.

If the virtual machine is running at the time of backup, this snapshot can impact disk I/O and consume space on the VMware vmfs datastore. Snapshot creation and deletion can take a long time if the virtual machine runs a heavy disk I/O workload during backup. This requirement also limits the types of virtual disks that are supported to the following:

- Flat (version 1 and 2)
  - Raw Device Mapped (RDM) in virtual mode only (version 1 and 2)
  - Sparse (version 1 and 2)
- If changed block tracking is not enabled, each virtual machine image must be fully processed for each backup, likely resulting in unacceptably long backup windows and excessive back-end storage read/write activity.

Changed block tracking identifies unused space on a virtual disk during the initial backup of the virtual machine and blocks that have not changed since the previous backup. Avamar data deduplication performs a similar function. However, using this feature provides valuable I/O reduction earlier in the backup process. Changed block tracking dramatically improves performance if SAN connectivity is not available. Changed block tracking is only available with the following types of virtual machines that use the following specific types of virtual disk formats:

- Virtual machine versions 7 and later

---

**IMPORTANT:** The earlier version 4 is commonly used on ESX 3.X hosts and in virtual machines deployed from templates that support both ESX 3.x and 4.0 hosts. The version of a virtual machine does not change when the underlying ESX host is upgraded. Many commercial appliances are in version 4 form to allow deployment on ESX 3.x hosts.

---

---

**NOTE:** vCenter version 4 provides the ability to upgrade version 4 virtual machine hardware from to version 7 virtual machine hardware. This upgrade is irreversible and makes the virtual machine incompatible with earlier versions of VMware software products. Refer to vCenter online help for additional information.

---

- Virtual disks in flat version 1 format
- Virtual disks in sparse version 1 format
- Virtual disks that cannot be included in a snapshot

After this feature is enabled, the virtual machine must be powered off and then on to activate it.

- The image backup process always attempts to use the highest-performing available connection between the storage virtual disk vmfs and the Avamar source deduplication engine that runs on the Avamar proxy virtual machine appliance.

For example, assume a virtual disk (type SCSI) hosted by a SAN LUN connected to a Fibre Channel and an ESX host running the Avamar proxy virtual machine appliance connected by Fibre Channel to the same SAN LUN. In this case, the high-speed Fibre Channel is used. If instead no Avamar proxy virtual machine appliance has connectivity to high-performance SAN, the proxy uses regular network connectivity which can lead to bandwidth problems and slow or even failed backups. When SAN connectivity is not available, guest backup is likely preferred to image backup.

- If a virtual machine template is relocated, any scheduled backups of that template will fail. The template can be re-added as a backup client at the new location, but at that point, it is effectively a new backup entity, and any historical backups are not linked to the backup entity at the new location.
- Individual file and directory (folder) restores are only supported on Windows virtual machine.

This optional Windows file-level restore feature requires a special proxy client and other additional configuration and setup. Refer to *Optional Windows File-Level Restore* (page 81) for additional information.

- Restoring a virtual machine to a datacenter that is different from the one that hosted the virtual machine at the time of backup requires a compatible Avamar proxy client within the new target datacenter. If no compatible proxy is deployed on an ESX host within the target datacenter, the restore attempt will fail.
- If an Avamar Virtual Edition (AVE) appliance is deployed within a vCenter, never attempt to conduct a virtual machine image backup or restore of the AVE virtual machine. This is not supported.
- If you will also be using VMware Consolidated Backup (VCB) in Hot-Add mode, you need to create a shadow virtual machine for VCB to use internally. The shadow virtual machine has the same name as your virtual VCB proxy with the (VCB-HELPER) suffix added. Refer to your VMware *Virtual Machine Backup Guide* for additional information.

## Information Roadmap

Subsequent chapters in this publication cover various aspects of installing and using Avamar VMware image backup and restore as follows:

CHAPTER	SYNOPSIS
<i>Avamar VMware Image Backup and Restore Configuration and Setup</i> (page 29)	<p>This chapter covers essential configuration and setup procedures for both vCenter and Avamar environments. These procedures must be performed before Avamar VMware image backup and restore can be used to protect virtual machine data.</p> <p>Key topics include:</p> <ul style="list-style-type: none"> <li>• <i>Configuring the vCenter Environment</i> (page 29)</li> <li>• <i>Configuring vCenter-to-Avamar Authentication</i> (page 44)</li> <li>• <i>Configuring the Avamar Environment</i> (page 47)</li> <li>• <i>Protecting Virtual Machines with Both Guest and Avamar VMware Image Backup</i> (page 52)</li> </ul>
<i>Using Avamar VMware Image Backup and Restore</i> (page 53)	<p>This chapter covers using Avamar VMware image backup and restore to protect virtual machine data after the feature has been configured and set up.</p> <p>Key topics include:</p> <ul style="list-style-type: none"> <li>• <i>Basic Client Administration</i> (page 54)</li> <li>• <i>Backup and Restore</i> (page 65)</li> <li>• <i>Groups and Policy Management</i> (page 75)</li> <li>• <i>Troubleshooting</i> (page 80)</li> </ul>
<i>Optional Windows File-Level Restore</i> (page 81)	<p>This chapter covers the optional Windows file-level restore feature.</p> <p>Key topics include:</p> <ul style="list-style-type: none"> <li>• <i>Capabilities and Limitations</i> (page 81)</li> <li>• <i>Configuration and Setup</i> (page 83)</li> <li>• <i>Restoring Folders or Files from a VMware Image Backup</i> (page 91)</li> </ul>

---

**IMPORTANT:** In addition to protecting individual virtual machines, you should also protect your vCenter management infrastructure. Refer to *Protecting the vCenter Management Infrastructure* (page 94) for additional information.

---

# AVAMAR VMWARE IMAGE BACKUP AND RESTORE CONFIGURATION AND SETUP

---

This chapter covers essential configuration and setup procedures for both vCenter and Avamar environments that must be performed before Avamar VMware image backup and restore can be used to protect virtual machine data.

## Configuring the vCenter Environment

In order to successfully implement Avamar VMware image backup and restore, you first must configure vCenter-to-Avamar Management Console Server (MCS) authentication and deploy the Avamar image backup proxy appliance within vCenter. These tasks are performed using the vSphere client application.

**Task List.** Basic configuration and setup comprises the following tasks, which should be performed in the following order:

- *Task 1: Download and Install vSphere Client Software* (page 30)
- *Task 2: Create Dedicated vCenter User Account* (page 30)
- *Task 3: Deploy One or More Avamar Image Backup Proxies* (page 31)

## Task 1: Download and Install vSphere Client Software

vSphere client software is required in order to perform certain management tasks on the vCenter server.

If you have not already done so, download and install vSphere client software by performing the following:

1. From a Windows computer, point your web browser at the vSphere server by typing the following URL:

**HTTPS://VSPHERE**

Where VSPHERE is your actual vSphere server network hostname as defined in DNS or IP address.

---

**NOTE:** This URL must be a secure (HTTPS) web address.

---

The vSphere Welcome page appears.

2. Click **Download vSphere Client**.

Your browser might prompt you to either open the file "in-place" (on the server) or save it to your local computer. Either method will work. However, if you save the file to your local computer, you must open (double-click) that installation file to continue with this procedure.

3. Either open the installation file in place (on the server) or double-click the downloaded installation file.

The installation wizard appears.

4. Follow the on-screen instructions.
5. When prompted, click **Finish** to complete the installation procedure.

The installation wizard closes.

## Task 2: Create Dedicated vCenter User Account

EMC strongly recommends that you set up a separate vCenter user account that is strictly dedicated for use with Avamar. Use of a generic user account such as "Administrator" might hamper future troubleshooting efforts because it might not be clear which "Administrator" actions are actually interfacing or communicating with the Avamar server. Using a separate vCenter user account ensures maximum clarity should it become necessary to examine vCenter logs.

## Task 3: Deploy One or More Avamar Image Backup Proxies

Deploy each Avamar image backup proxy client as follows:

Download  
Appliance  
Template File

1. Download the Avamar image backup proxy appliance template file by performing the following:

- (a) From your Windows computer, point your web browser at the Avamar server by typing the following URL:

**http://AVAMARSERVER**

Where AVAMARSERVER is your actual Avamar server network hostname as defined in DNS or IP address.

You are automatically redirected to the Avamar secure web server.

Depending on your browser security settings, a security alert dialog box might appear.

- (b) If a security alert dialog box appears, click **Yes** or **OK** to allow redirection to the Avamar secure web server.

The Secure Log On page appears.

- (c) Page down until the **Documents and Downloads** hyperlink is visible.

- (d) Click **Documents and Downloads**.

The Documents and Downloads page appears.

- (e) Page down until the VMware 4.0 section is visible.

- (f) Click the **EMC Avamar VMware Image Backup Appliance** hyperlink.

The Downloads for EMC Avamar VMware Image Backup Appliance page appears.

- (g) Click the AvamarVmImageProxy-linux-VERSION.ova hyperlink.

Where VERSION is the specific version Avamar VMware Image Backup Appliance software you are installing.

The File Download dialog box appears.

- (h) Click **Save** to save AvamarVmImageProxy-linux-VERSION.ova to a convenient location on your computer (for example, your desktop or C:\Temp).

**Add Appliance in vCenter Server**

2. Add the Avamar image backup proxy appliance in the vCenter server as follows:

- (a) From your Windows computer, launch the vSphere client application.  
 The VMware vSphere Client login dialog box appears.

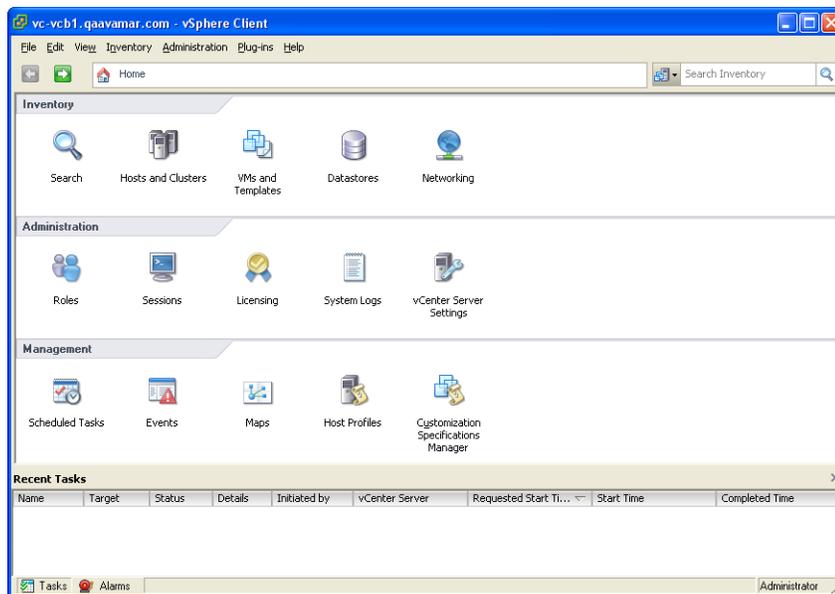


(b) Log into the vCenter server by typing the following:

FIELD	DESCRIPTION
IP address / Name	vCenter server IP address or network hostname as defined in DNS.
User name	User account name.
Password	Password for this user name.

(c) Click **Login**.

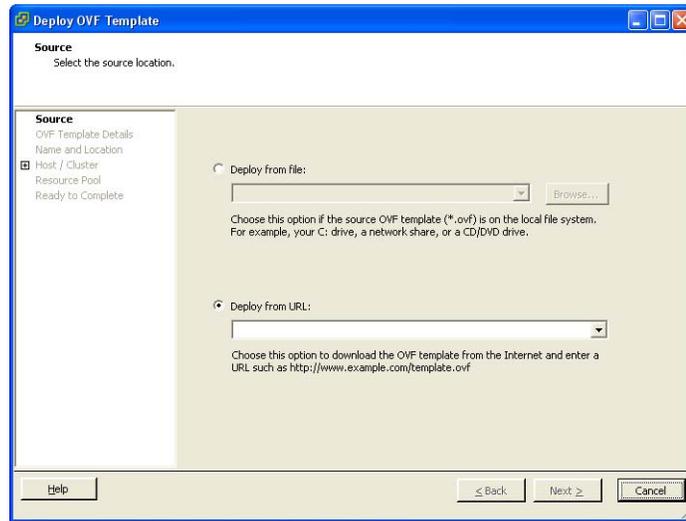
The VMware vSphere Client login dialog box closes. The vSphere Client window appears.



(d) Switch to Hosts and Clusters view by clicking **View > Inventory > Hosts and Clusters**.

- (e) Select **File > Deploy OVF Template...**

The Deploy OVF Template wizard appears.



- (f) Select **Deploy from file** and click **Browse...**

The Open dialog box appears.

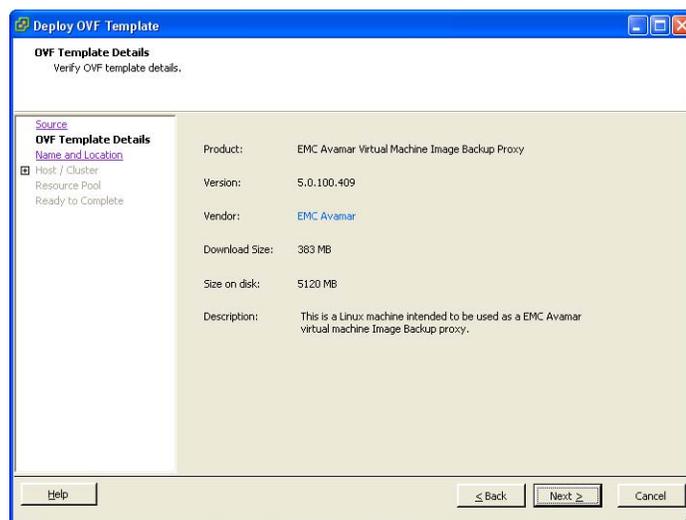
- (g) Select Ova files (\*.ova) from the Files of Type list.

- (h) Browse to the AvamarVmImageProxy-linux-VERSION.ova file you previously saved to your Windows computer, select it and click **Open**.

The Open dialog box closes. The full path to the AvamarVmImageProxy-linux-VERSION.ova file appears in the Deploy from file field.

- (i) Click **Next**.

The next Deploy OVF Template wizard screen appears.



Naming Your  
Image Backup  
Proxy

(j) Click **Next**.

The next Deploy OVF Template wizard screen appears.

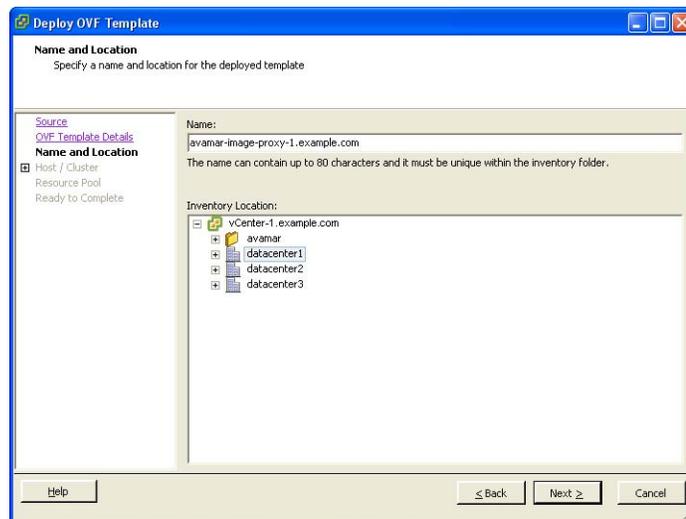
A proxy can potentially have three different names:

- The name of the virtual machine on which the proxy runs. This is also the name managed and visible within vCenter.
- The DNS name assigned to the proxy virtual machine.
- The Avamar client name after the proxy registers and activates with server.

In order to avoid confusion and potential problems, EMC strongly recommends that you consistently use the same name for each image backup proxy and that name be a fully-qualified hostname.

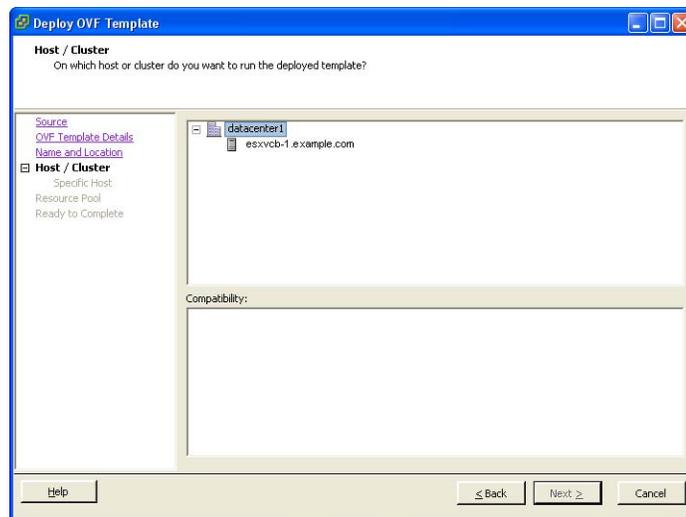
(k) Type a fully-qualified hostname in the Name field.

(l) Select a datacenter and folder location for this proxy in the Inventory tree.



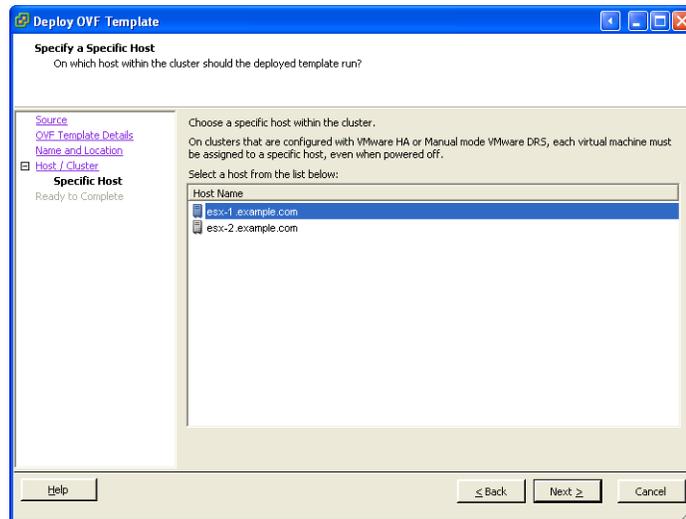
(m) Click **Next**.

The next Deploy OVF Template wizard screen appears.



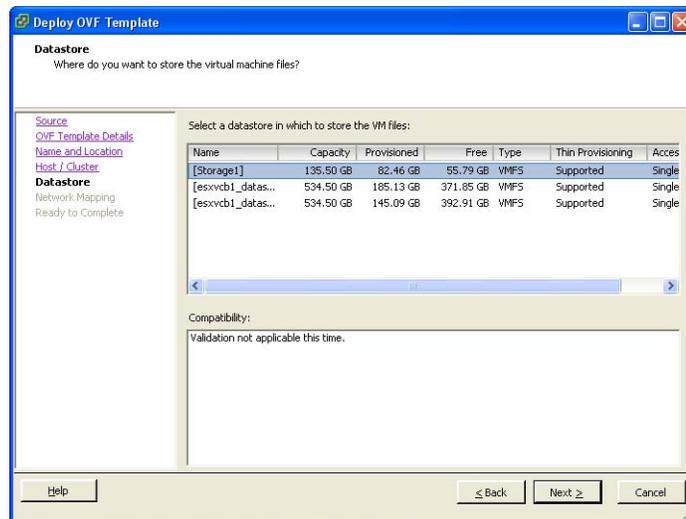
(n) Select an ESX server or cluster in the tree and click **Next**.

If you selected a cluster, the next Deploy OVF Template wizard screen appears.



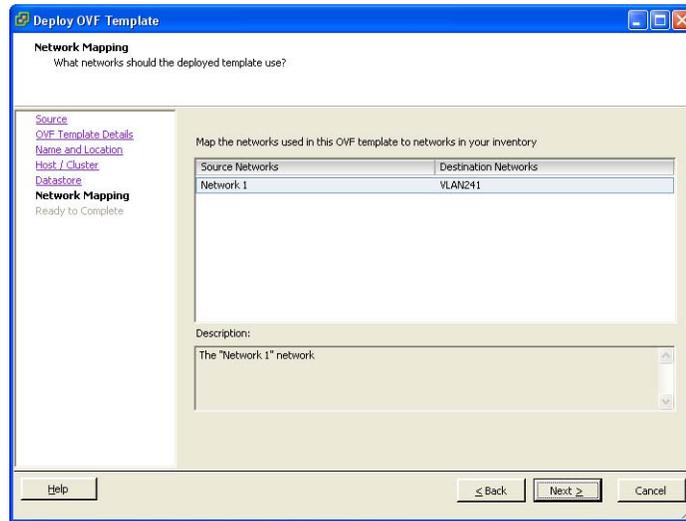
(o) Select an ESX server and click **Next**.

A validation check will be performed. If successful, the next Deploy OVF Template wizard screen appears.



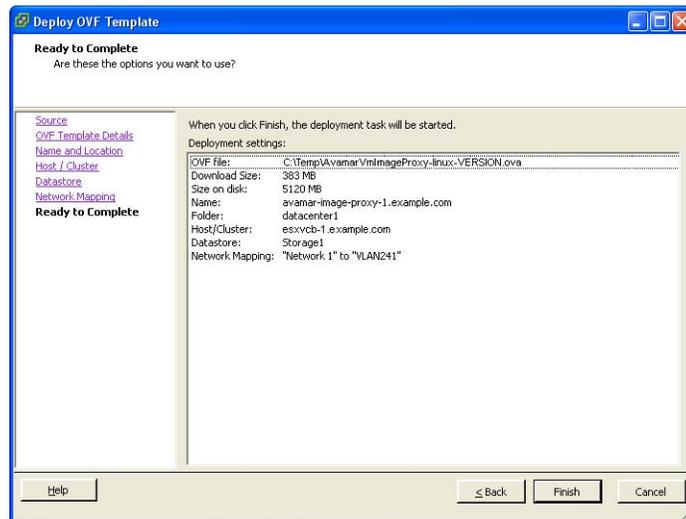
- (p) Select a datastore and click **Next**.

The next Deploy OVF Template wizard screen appears.



- (q) Select a destination network from drop-down list and click **Next**.

The final Deploy OVF Template wizard screen appears.



- (r) Click **Finish**.

The Deploy OVF Template wizard closes.

It might take several minutes for the deployment operation to complete.

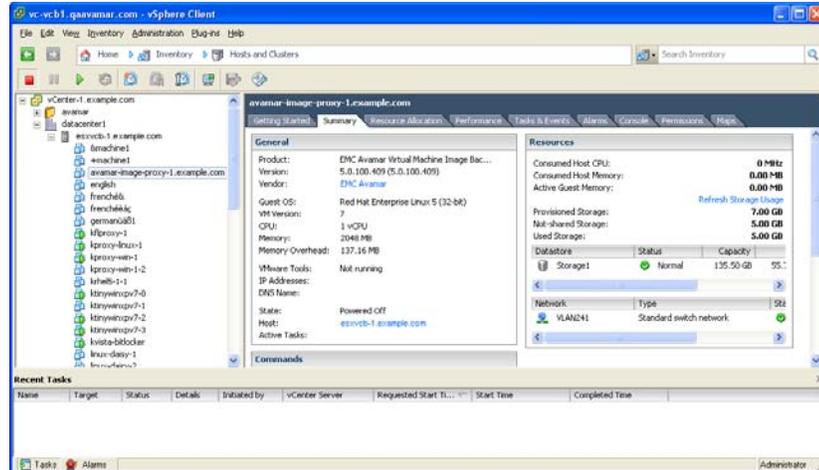
- (s) Wait for the deployment operation to complete.

A confirmation message appears.

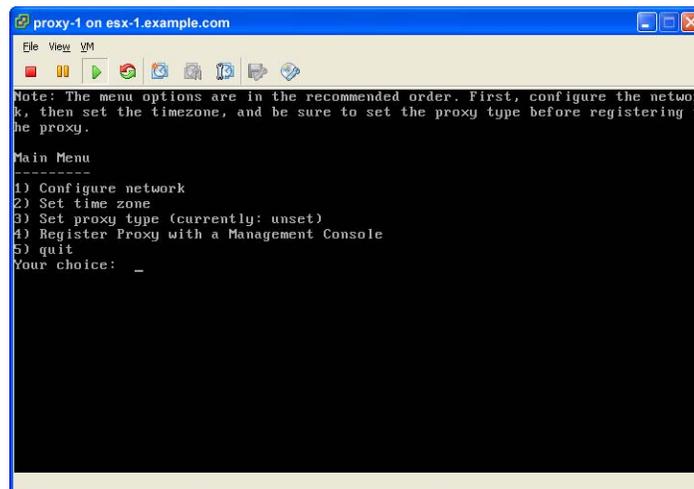
- (t) Click **Close** to dismiss the confirmation message.

Configure Appliance Network Settings in vCenter Server

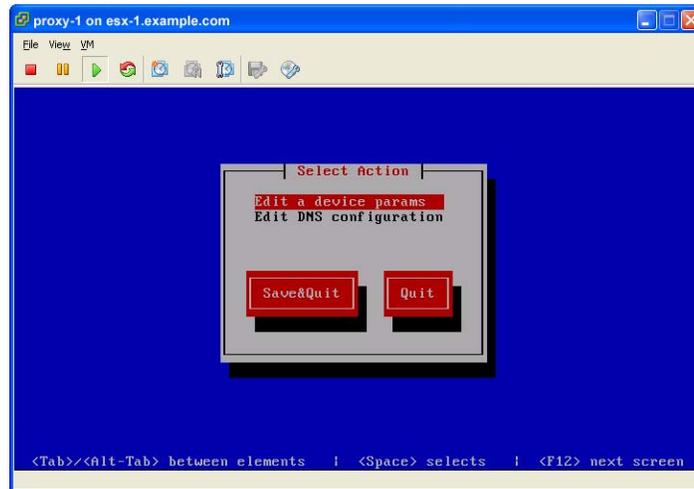
3. Configure Appliance Network Settings in vCenter Server as follows:
  - (a) Switch to the vSphere Client window.
  - (b) Locate and select the Avamar image backup proxy that was previously added in step 2.



- (c) Power on the new proxy virtual machine by right-clicking the Avamar image backup proxy and selecting **Power > Power On**.
  - (d) Open a console to the Avamar image backup proxy by right-clicking it and selecting **Open Console**.  
The Console window appears.
  - (e) Wait for the Main Menu to appear.

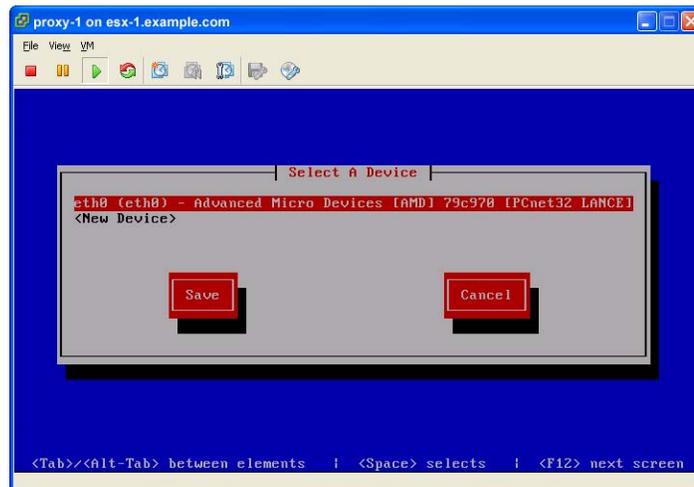


- (f) Configure network settings by typing 1.  
The Select Action screen appears.

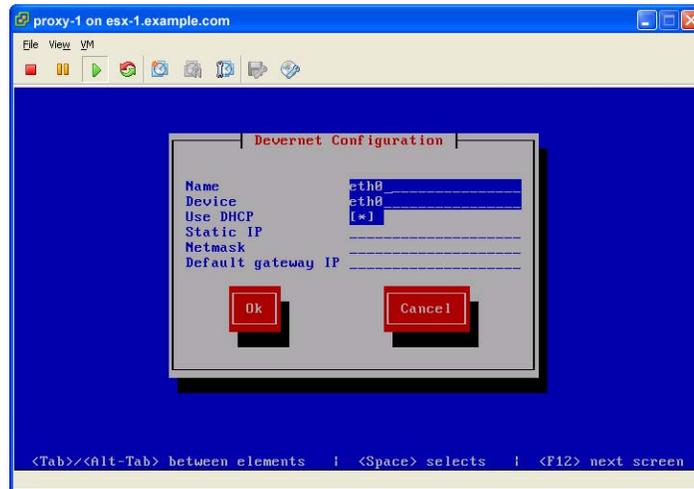


- (g) Use **Tab** or arrow keys to select **Edit a device params** and press **ENTER**.

The Select a Device screen appears.



- (h) Use **Tab** or arrow keys to select the eth0 device and press **ENTER**.  
 The Devernet Configuration screen appears.




---

**IMPORTANT:** The proxy must have connectivity to both the Avamar server and the vCenter server. Exact settings are highly dependent on the network configuration at your site.

If necessary, consult your Network Administrator for assistance.

---

- (i) Use **Tab** or arrow keys to select each parameter, then type the following:

PARAMETER	SETTING/DESCRIPTION
Name	Leave set to eth0.
Device	Leave set to eth0.
Use DHCP	If you want to use DHCP to assign an IP address, leave the asterisk. If you want to assign a static IP address, remove the asterisk.
Static IP	If not using DHCP, enter a valid routable IP address on your network.
Netmask	Set to 255.255.255.0.
Default gateway IP	Enter the default gateway IP address for your network.

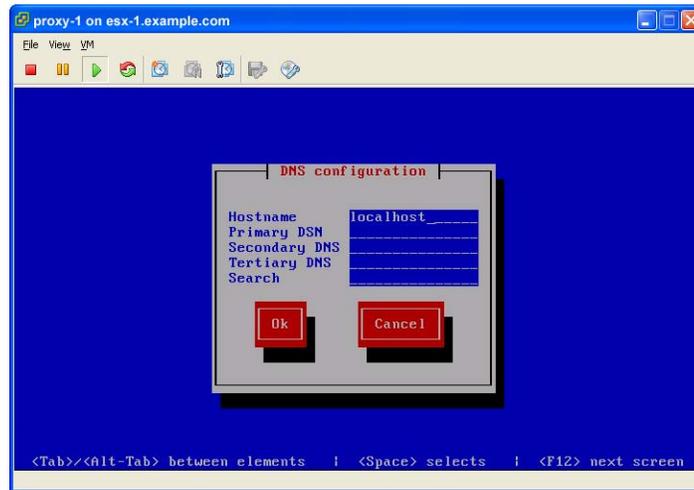
- (j) When complete, use **Tab** or arrow keys to select **OK** and press **ENTER**.  
 The Devernet Configuration screen closes and you are returned to the Select a Device screen.

- (k) Use **Tab** or arrow keys to select **Save** and press **ENTER**.

The Select a Device closes and you are returned to the Select Action screen.

- (l) Use **Tab** or arrow keys to select **Edit DNS configuration** and press **ENTER**.

The DNS Configuration screen appears.



- (m) Use **Tab** or arrow keys to select each of the following parameters, then use the following settings:

PARAMETER	SETTING/DESCRIPTION
Hostname	Type the hostname you defined when initially deploying the Avamar image backup proxy.
Primary DNS	Type the hostname or IP address of primary DNS lookup server. <b>NOTE:</b> Some versions of the Avamar image backup proxy incorrectly label this parameter as Primary DSN.
Secondary DNS	Type the hostname or IP address of optional secondary DNS lookup server.
Tertiary DNS	Type the hostname or IP address of optional tertiary DNS lookup server.
Search	Type the preferred domain for resolving DNS IP requests.

- (n) When complete, use **Tab** or arrow keys to select **OK** and press **ENTER**.

The DNS Configuration screen closes and you are returned to the Select Action screen.

- (o) Use **Tab** or arrow keys to select **Save&Quit** and press **ENTER**.

Network connections are now tested.

(p) Do one of the following:

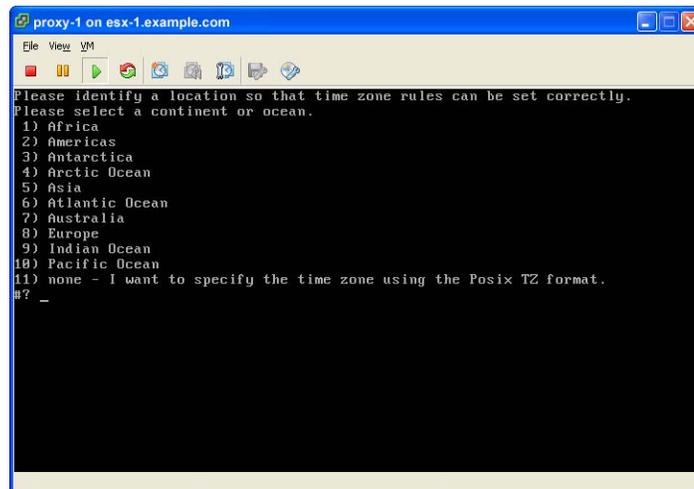
IF	DO THIS
All network connection tests pass.	Skip this step and go directly to step q.
Any network connection tests fail.	Resolve those issues before proceeding further. If necessary, contact EMC Technical Support for assistance.

(q) Press **y**.

The Console window Main Menu appears.

(r) Configure time zone settings by typing **2**.

The first time zone configuration screen appears. This screen allows you to select your continent.




---

**TIP:** If you know your POSIX time zone code, you can type **11** and enter it directly.

---

(s) Type the numeric code that corresponds to your continent and press **ENTER** (for example, type **2** and press **ENTER** for the Americas).

The next time zone configuration screen appears. This screen allows you to select your country.

(t) Type the numeric code that corresponds to your country and press **ENTER**.

The next time zone configuration screen appears. This screen allows you to select your time zone within your country.

(u) Type the numeric code that corresponds to your time zone and press **ENTER**.

The last time zone configuration screen appears. This screen allows you to confirm and accept your selections.

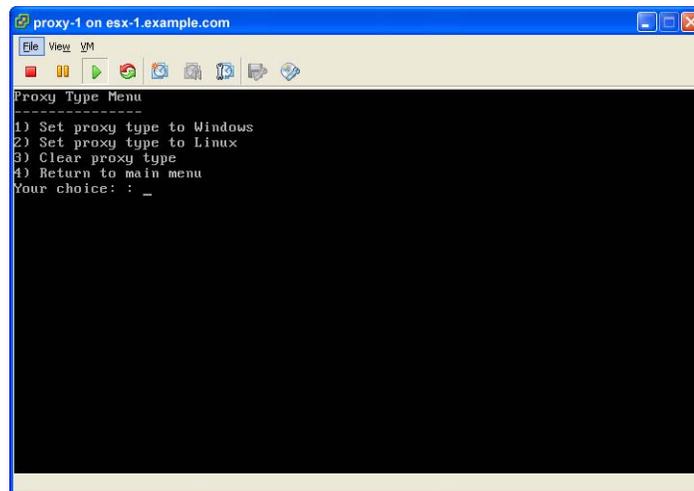
- (v) Type **1** and press **ENTER**.

**NOTE:** When you first configure the time zone, **Local time** and **Universal time** are both displayed. Because the underlying operating system has not been started, the values of those two parameters are typically reversed. This is expected behavior. After the proxy completes its first boot, the time zone values will be correct.

The Console window Main Menu appears.

- (w) Configure proxy backup type by typing **3**.

The Proxy Type Menu appears.



- (x) Type the numeric code that corresponds to the operating system that is running on the virtual machines you will be backing up and press **ENTER**.

Choices are **1** (Windows) or **2** (Linux that is non-Windows operating systems).

- (y) When complete, type **4** and press **ENTER** to return to the Main Menu.

The Console window Main Menu appears.

- (z) Register the Avamar image backup proxy with an Avamar server by typing **4**.

The following appears in the console window:

```
Enter the Administrator server address (DNS text name or numeric IP address,
DNS name preferred):
```

- (aa) Type the actual network hostname as defined in DNS of the Avamar server from which you want to initiate and manage backups and restores and press **ENTER**.

The following appears in the console window:

```
Enter the Avamar server domain [clients]:
```

The default domain is "clients." However, your Avamar system administrator may have defined other domains and subdomains. Consult your Avamar system administrator for the specific domain you should use when registering this client.

---

**IMPORTANT:** If typing a subdomain (for example, clients/MyClients), do not include a slash (/) as the first character. Including a slash as the first character will cause an error and prevent you from registering this client.

---

- (ab) Press **ENTER** to accept the default domain (clients).

The client registration process begins.

- (ac) After all parameters have been set, quit the configuration menu typing **5**.

The Avamar image backup proxy finishes booting and starts the remainder of its services.

**Changing Avamar Image Backup Proxy Settings.** Should you ever need to change any settings made in the previous procedure, you must perform the following from within vCenter:

1. Reboot this virtual machine by right-clicking the virtual machine and selecting **Guest > Send Ctrl + Alt + del**.
2. Before the boot process completes, open a console window by right-clicking the virtual machine and selecting **Open Console**.
3. Change the settings using the console window Main Menu.
4. After all parameters have been set, quit the configuration menu typing **5** and pressing **ENTER**.

The Avamar image backup proxy automatically reboots.

## Configuring vCenter-to-Avamar Authentication

Avamar VMware Image Backup will not work unless one of the following conditions is met:

- A valid authentication certificate is present on the Avamar MCS (page 44).
- Certificate authentication for all MCS-to-vCenter communications is turned off (page 46).

### Option 1: Installing an Authentication Certificate on the Avamar MCS

Avamar VMware Image Backup will not work unless a valid authentication certificate is present on the MCS. For security reasons, Avamar intentionally does not provide one. You must either obtain your own authentication certificate, or use the default certificate provided with vCenter, then install either one using this procedure.

This procedure assumes that you are installing the default certificate provided with vCenter.

The procedure uses the java **keytool** command, a utility that manages certificate keys. The **keytool** command is located in the Java bin directory (/usr/java/jreVERSION/bin), where VERSION is the specific Java Runtime Environment (JRE) version currently installed on the MCS. If this directory is not in your path, you can either add it to the path, or specify the complete path when using **keytool**.

User=root

1. Open a command shell.
2. Do one of the following:

IF	DO THIS
Administering a single-node Avamar server.	Log into the server as root. When prompted for a password, type the root password and press <b>ENTER</b> .
Administering a multi-node Avamar server.	Log into the utility node as root. When prompted for a password, type the root password and press <b>ENTER</b> .

Copy Certificate File to Server

3. Copy rui.crt from the vCenter machine to utility node /tmp.

The default certificate provided with vCenter is:

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

4. Create a temporary version of the MCS keystore by copying the live keystore (that is, /usr/local/avamar/lib/rmi\_ssl\_keystore) to /tmp by typing:

```
cp /usr/local/avamar/lib/rmi_ssl_keystore /tmp/
```

Stop MCS

5. Stop the MCS by typing:

```
dpnctl stop mcs
```

6. Add the default vCenter certificate to the temporary MCS keystore file by typing the following on a single command line:

```
$JAVA_HOME/bin/keytool -import -file rui.crt -alias ALIAS  
-keystore rmi_ssl_keystore
```

Where ALIAS is a user-defined name for this certificate, which can often be the file name.

7. When prompted for a password, enter the root password.

The following appears in the command shell:

```
Trust this certificate?
```

8. Enter **yes** and press **ENTER**.

9. Back up the live MCS keystore (that is, /usr/local/avamar/lib/rmi\_ssl\_keystore) by typing:

```
cd /usr/local/avamar/lib  
cp rmi_ssl_keystore rmi_ssl_keystore.DATE
```

Where DATE is today's date.

10. Copy the temporary MCS keystore (that is, /tmp/lib/rmi\_ssl\_keystore) to its original (live) location by typing:

```
cp /tmp/rmi_ssl_keystore /usr/local/avamar/lib/
```

Restart MCS

11. Restart the MCS by typing:

```
dpnctl start mcs
```

## Option 2: Turning Off Certificate Authentication for All vCenter-to-Avamar MCS Communications

1. Open a command shell.

User=admin

2. Do one of the following:

IF	DO THIS
Administering a single-node Avamar server.	Log into the server as user admin. When prompted for a password, type the admin password and press <b>ENTER</b> .
Administering a multi-node Avamar server.	Log into the utility node as user admin. When prompted for a password, type the admin password and press <b>ENTER</b> .

Stop MCS

3. Stop the MCS by typing:

```
dpnctl stop mcs
```

4. Open /usr/local/avamar/var/mc/server\_data/prefs/mcserver.xml in a Unix text editor.

5. Locate the ignore\_vc\_cert preference.

6. Change the ignore\_vc\_cert preference setting to true.

For example:

```
<entry key="ignore_vc_cert" value="true" />
```

7. Save your changes.

Restart MCS

8. Restart the MCS by typing:

```
dpnctl start mcs
```

## Configuring the Avamar Environment

After you have successfully completed *Configuring the vCenter Environment* (page 29), you must add the required clients to the Avamar server before you can begin protecting virtual machine data. These tasks are performed using the Avamar Administrator graphical management console.

Avamar VMware image backup and restore is implemented by adding three separate types of clients in Avamar Administrator:

CLIENT	DESCRIPTION
vCenter Server	Automatically added to the Default Group. vCenter clients are not initially activated as normal Avamar clients are. However, if you will be protecting the vCenter management infrastructure (which is highly recommended), you will eventually register and activate the vCenter Server in the normal manner. It is just not required that you do so as part of preparation for protecting virtual machine data. Refer to <i>Protecting the vCenter Management Infrastructure</i> (page 94) for additional information.
VMware Image Proxy	The VMware image proxy client performs the actual backups and restores of virtual machine clients. Image proxy clients are allowed in any part of Avamar Administrator account management tree except the vCenter domain or subdomains. This client is activated like normal Avamar clients.
Virtual Machines	Multiple virtual machine clients can be created. Allowed in the VirtualMachines domain of the vCenter domain or any subdomain. Because the actual backups and restores are performed on the image proxy client, virtual machine clients do not need to be activated as normal Avamar clients do.

---

**NOTE:** Neither the ESX Server nor datastore objects are represented as clients in Avamar Administrator.

---

**Task List.** Configuring the Avamar environment to protect virtual machine data comprises the following tasks:

- *Task 1: Download and Install Avamar Administrator Software* (page 48)
- *Task 2: Add vCenter Client* (page 49)
- *Task 3: Add Avamar VMware Image Proxy Client* (page 51)
- *Task 4: Add Virtual Machine Clients* (page 51)

## Task 1: Download and Install Avamar Administrator Software

Avamar Administrator graphical management console software is required in order to perform certain management tasks on the Avamar server.

If you have not already done so, download and install Avamar Administrator software by performing the following:

1. From a Windows computer, point your web browser at the Avamar server by typing the following URL:

**http://AVAMARSERVER**

Where AVAMARSERVER is your actual Avamar server network hostname as defined in DNS or IP address.

You will be automatically redirected to the Avamar secure web server.

Depending on your browser security settings, a security alert dialog box might appear.

2. If a security alert dialog box appears, click **Yes** or **OK** to allow redirection to the Avamar secure web server.

The Secure Log On page appears.

3. Page down until the **Documents and Downloads** hyperlink is visible.

4. Click **Documents and Downloads**.

The Downloads and Documentation page appears.

5. Page down until the Windows for x86 (32 bit) section is visible.

6. Click the **Microsoft Windows XP, 2003, Vista, 2008** hyperlink.

The Downloads for Microsoft Windows XP, 2003, Vista, 2008 page appears.

7. Click the **AvamarConsoleMultiple** install package.

Your browser might prompt you to either open the file "in-place" (on the server) or save it to your local computer. Either method will work. However, if you save the file to your local computer, you must open (double-click) that installation file to continue with this procedure.

8. Either open the installation file in place (on the server) or double-click the downloaded installation file.

The installation wizard appears.

9. Follow the on-screen instructions.

10. When prompted, click **Finish** to complete the installation procedure.

The installation wizard closes.

## Task 2: Add vCenter Client

---

**IMPORTANT:** Prior to adding a vCenter client, EMC strongly recommends that you set up a separate vCenter user account that is strictly dedicated for use with Avamar. Use of a generic user account such as "Administrator" might hamper future troubleshooting efforts because it might not be clear which "Administrator" actions are actually interfacing or communicating with the Avamar server. Use of a separate vCenter user account ensures maximum clarity should it be necessary to examine vCenter logs.

---

---

**IMPORTANT:** The vCenter must exist and be operational before this type of client can be added. Avamar Administrator attempts to make a connection with the vCenter.

---

---

**IMPORTANT:** If the vCenter client is already registered as a normal client (for example, to support guest level backup), adding that same vCenter client again will fail because the system will not allow you to register the same client twice. If this occurs, you must retire the existing client instance in Avamar Administrator, add the vCenter client (using the following procedure), then re-invite the vCenter client as a normal client to support guest level backup from the vCenter domain.

---

Adding a vCenter client in Avamar Administrator automatically accomplishes all of the following:

- The vCenter client is added to the Default Group.  
However, this client is not activated as normal Avamar clients are. Therefore, no backups are performed for it on behalf of the Default Group.
- A default vCenter domain is created with the same name as the vCenter's fully qualified hostname.
- A subdomain called VirtualMachines is created.
- A group called Default Virtual Machine Group is created.

This group that performs scheduled backups for the target virtual machines. This group cannot be deleted without first deleting the virtual center domain.

To add a vCenter client:

1. Start Avamar Administrator.
2. Select **Navigation > Administration** or click the **Administration** launcher button.

The Administration window appears.

3. Click the Account Management tab.
4. In the tree, select the top-level (root) domain.





5. Select **Actions > Account Management > New Client...** or click the toolbar button (shown left).

The New Client dialog box appears.

6. For Client Type, select VMware vCenter.

**IMPORTANT:** Only one VMware vCenter client is permitted for each Avamar MCS.

7. Type the following vCenter connection information:

FIELD	DESCRIPTION
New Client Name or IP	Fully-qualified name or IP address of the vCenter.
Port	vCenter web services listener port. Default setting is port 443.
User Name	vCenter user account name you previously created (page 30).
Password	Password for the the vCenter user account you previously created (page 30).
Verify Password	Type the password again.

8. If desired, also type the following optional information:

FIELD	DESCRIPTION
Contact	Optional contact name.
Phone	Optional contact telephone number.
Email	Optional contact email address.
Location	Optional contact location.

9. Click **OK**.

The New Client dialog box closes.

### Task 3: Add Avamar VMware Image Proxy Client

The next configuration and setup task is to add the Avamar VMware image proxy client you previously deployed as a client using Avamar Administrator. Refer to *Adding and Activating a VMware Image Proxy Client* (page 55) for detailed information.

### Task 4: Add Virtual Machine Clients

The final configuration and setup task is to add one or more virtual machine clients that will be protected by backing up to the VMware image proxy client, which was added in the previous task. Refer to *Adding Virtual Machine Clients* (page 56) for detailed information.

## Protecting Virtual Machines with Both Guest and Avamar VMware Image Backup

A virtual machine can be protected by both guest backup and image backup. For example, a daily guest backup to frequently protect selective files and an infrequent or on-demand full image backup protects the full machine. This scheme accommodates scenarios with limited backup windows.

However, if you decide to use both methods simultaneously on one or more virtual machines, a small amount of additional configuration is required.

User=admin

1. Open a command shell.
2. Do one of the following:

IF	DO THIS
Administering a single-node server.	Log into the server as user admin. When prompted for a password, type the admin password and press <b>ENTER</b> .
Administering a multi-node server.	Log into the utility node as user admin. When prompted for a password, type the admin password and press <b>ENTER</b> . Load the admin OpenSSH key by typing: <b>ssh-agent bash</b> <b>ssh-add ~admin/.ssh/admin_key</b> You are prompted to type a passphrase. Type the admin user account passphrase and press <b>ENTER</b> .

3. Stop the MCS by typing:  
**dpnctl stop mcs**
4. Open /usr/local/avamar/var/mc/server\_data/prefs/mcserver.xml in a Unix text editor.
5. Locate the allow\_duplicate\_client\_names preference.
6. Ensure that this preference is set true.
7. Save your changes.
8. Restart the MCS by typing:  
**dpnctl start mcs**

# USING AVAMAR VMWARE IMAGE BACKUP AND RESTORE

---

This chapter covers using Avamar VMware image backup and restore to protect virtual machine data.

Before proceeding further, ensure that this feature has been configured and set up according to the instructions found in *Avamar VMware Image Backup and Restore Configuration and Setup* (page 29).

---

**NOTE:** Although this publication makes every attempt to present complete and relevant information for every topic, a comprehensive discussion of certain basic system administration concepts and principles is beyond the scope of this publication. Refer to your *Avamar System Administration Guide* for additional information.

---

## Basic Client Administration

This topic describes how to add and manage VMware image proxy and virtual machine clients.

### How VMware Clients Appear in Avamar Administrator

In order to differentiate between the various types of clients in a typical vCenter environment, Avamar Administrator uses the following icons to communicate client type and state:

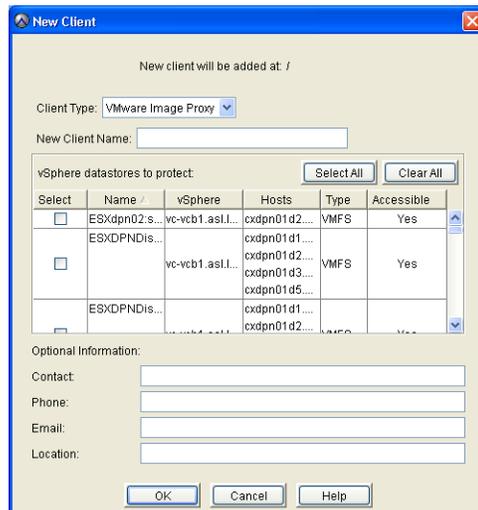
CLIENT TYPE	ICON/DESCRIPTION
vCenter Server	 vCenter server (activated). <b>NOTE:</b> This is the same icon used to show nonvirtual machine clients.  Replicated vCenter server (this icon only visible in REPLICATE domain).  Unactivated vCenter server. <b>NOTE:</b> Unless you are also protecting the vCenter server with guest backup (which is highly recommended), vCenter servers are not typically activated as normal Avamar clients. Therefore, in some circumstances, this is the normal state for a vCenter server.
VMware Image Proxy	 VMware image proxy client (activated and enabled).  Disabled VMware image proxy client.  Replicated VMware image proxy client (this icon only visible in REPLICATE domain).  Unactivated VMware image proxy client.
Virtual Machines	 Virtual machine client (enabled).  Disabled virtual machine client.  Replicated Virtual machine client (this icon only visible in REPLICATE domain).

## Adding and Activating a VMware Image Proxy Client

Adding a VMware image proxy client automatically adds it to the Default Proxy Group.

To add a VMware image proxy:

1. Start Avamar Administrator.
2. Select **Navigation > Administration** or click the **Administration** launcher button.  
The Administration window appears.
3. Click the Account Management tab.
4. Select any desired node except the vCenter subdomain and **Actions > Account Management > New Client...** or click the toolbar button (shown left).  
The New Client dialog box appears.
5. For Client Type, select VMware Image Proxy.



6. For New Client Name, type the fully qualified hostname or IP address of the proxy client.
7. Select all vCenter datastores that host virtual machines you want to protect with this proxy client.
8. If desired, also type the following optional information:

FIELD	DESCRIPTION
Contact	Contact name.
Phone	Contact telephone number.
Email	Contact email address.
Location	Contact location.

9. Click **OK**.

The New Client dialog box closes and a Client added confirmation message appears.

10. Click **OK**.

The Client added confirmation message closes.

Before you can begin backing virtual machine clients to this proxy client, you must activate it.

#### Activate Client

11. In the tree, select the VMware image proxy client you just added.

12. Select **Actions > Account Management > Invite Client...**

The following status message appears: Client has been sent invitation to activate with the server.

13. Click **OK**.

## Adding Virtual Machine Clients

Adding this client to vCenter domain or a lower subdomain automatically adds the client to the Default Virtual Machine Group.

You can add either a single virtual machine client (page 56) or multiple virtual machine clients (page 59).

### Adding a Single Virtual Machine Client

To add a single virtual machine client:

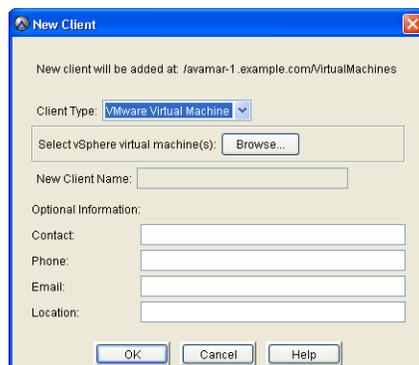
1. Start Avamar Administrator.
2. Select **Navigation > Administration** or click the **Administration** launcher button.

The Administration window appears.

3. Click the Account Management tab.
4. In the tree, select the vCenter domain or a lower subdomain.
5. Select **Actions > Account Management > New Client...** or click the toolbar button (shown left).

The New Client dialog box appears.

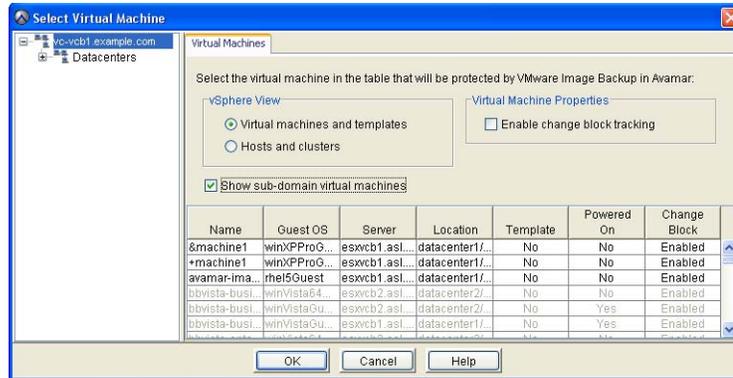
6. For Client Type, select VMware Virtual Machine.



7. Click **Browse**.

The Select Virtual Machine dialog box appears.

The left panel tree shows directories containing virtual machines. The right panel displays details about the virtual machines in each directory.



8. Expand the tree until you can view the desired virtual machine node.

The Virtual Machines tab at right displays all available virtual machines administered by vCenter.

Virtual machines for which a client already exists in Avamar are disabled.

Virtual machines considered proxy clients also cannot be selected because they are prohibited from backing themselves up with VMware Image Plugin.

For each virtual machine, the following information is shown:

- Name            Virtual machine name.
- Guest OS        Virtual machine operating system.
- Server           ESX Server or cluster hostname.
- Location        Folder location.
- Template        Whether or not the virtual machine is a template.
- Powered On     Whether or not the virtual machine is currently powered on.
- Change Block    Whether or not changed block tracking is turned on for this virtual machine.

The options at the top of the Select Virtual Machine dialog box perform the following functions:

OPTION	DESCRIPTION
vSphere View - <b>Virtual machines and template views</b>	The view is representative of vCenter's virtual machines and template views.
vSphere View - <b>Hosts and clusters view</b>	The view is representative of vCenter's hosts and clusters view.
<b>Show sub-domain virtual machines</b>	Displays all virtual machines in the vCenter.  If a virtual machine is already being protected with guest backup (page 17), it is shown as disabled in this view.
Virtual Machine Properties - <b>Enable change block tracking</b>	If selected, the changed block tracking is enabled.  <b>IMPORTANT:</b> If changed block tracking is not enabled, the virtual machine image must be fully processed for each backup, likely resulting in unacceptably long backup windows and excessive back-end storage read/write activity.  This feature is enabled by default. EMC strongly recommends that you leave this feature enabled for all virtual machines you will be protecting with Avamar VMware image backup.

9. Select the desired virtual machine.
10. To enable changed block tracking for this client, select **Enable change block tracking**.

---

**NOTE:** Turning on changed block tracking will not take effect until a stun-unstun cycle occurs on the virtual machine. A stun-unstun cycle is defined by VMware as any of the following actions: power on, resume after suspend, migrate, snapshot create, delete or revert.

---

11. Click **OK**.

New Client Name is automatically populated in the New Client dialog box with the fully-qualified name of the selected virtual machine.

12. If desired, also type the following optional information:

FIELD	DESCRIPTION
Contact	Contact name.
Phone	Contact telephone number.
Email	Contact email address.
Location	Contact location.

13. Click **OK**.

The New Client dialog box closes and a Client added confirmation message appears.

14. Click **OK**.

The Client added confirmation message closes.

### Adding Multiple Virtual Machine Clients

To add multiple virtual machine clients in a single operation:

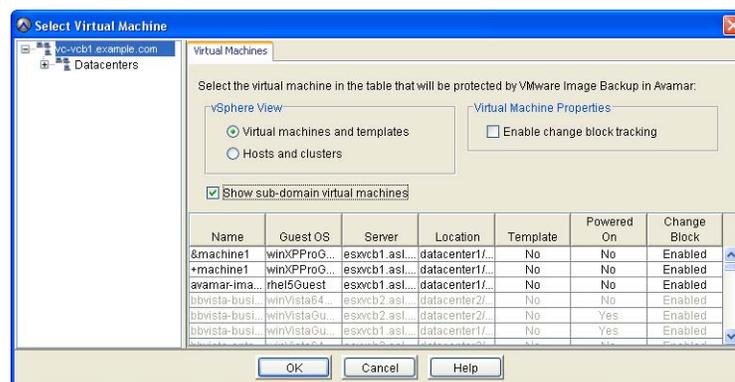
1. Start Avamar Administrator.
2. Select **Navigation > Administration** or click the **Administration** launcher button.



The Administration window appears.

3. Click the Account Management tab.
4. In the tree, select the location (that is, the vCenter domain or a lower subdomain) to which you want to add the new clients.
5. Select **Actions > Account Management > Import Multiple Clients...**

The Select Virtual Machine dialog box appears.



6. Expand the tree until you can view the desired virtual machine nodes.

The Virtual Machines tab at right displays all available virtual machines administered by vCenter.

Virtual machines for which a client already exists in Avamar are disabled.

Virtual machines considered proxy clients also cannot be selected because they are prohibited from backing themselves up with VMware Image Plugin.

For each virtual machine, the following information is shown:

Name	Virtual machine name.
Guest OS	Virtual machine operating system.
Server	ESX Server or cluster hostname.
Location	Folder location.
Template	Whether or not the virtual machine is a template.
Powered On	Whether or not the virtual machine is currently powered on.
Change Block	Whether or not changed block tracking is turned on for this virtual machine.

The options at the top of the Select Virtual Machine dialog box perform the following functions:

OPTION	DESCRIPTION
vSphere View - <b>Virtual machines and template views</b>	The view is representative of vCenter's virtual machines and template views.
vSphere View - <b>Hosts and clusters view</b>	The view is representative of vCenter's hosts and clusters view.
<b>Show sub-domain virtual machines</b>	Displays all virtual machines in the vCenter.  If a virtual machine is already being protected with guest backup (page 17), it is shown as disabled in this view.
Virtual Machine Properties - <b>Enable change block tracking</b>	If selected, the changed block tracking is enabled.  <b>IMPORTANT:</b> If changed block tracking is not enabled, the virtual machine image must be fully processed for each backup, likely resulting in unacceptably long backup windows and excessive back-end storage read/write activity.  This feature is enabled by default. EMC strongly recommends that you leave this feature enabled for all virtual machines you will be protecting with Avamar VMware image backup.

7. Select the desired virtual machines.

8. To enable changed block tracking for one or more clients, select **Enable change block tracking**.

---

**NOTE:** Turning on changed block tracking will not take effect until a stun-unstun cycle occurs on the virtual machine. A stun-unstun cycle is defined by VMware as any of the following actions: power on, resume after suspend, migrate, snapshot create, delete or revert.

---

9. Click **OK**.
10. Confirm the number of virtual machines selected.
11. Click **OK**.

The Progress... and Adding Virtual Machine Clients... dialog boxes appear.

12. Wait for the Progress... dialog box to close.
13. Switch to Adding Virtual Machine Clients... dialog box.

---

**TIP:** Click **Save As** to save the displayed results in a text file.

---

14. Click **Close**.

The Adding Virtual Machine Clients... dialog box closes.

## Editing Existing VMware Clients

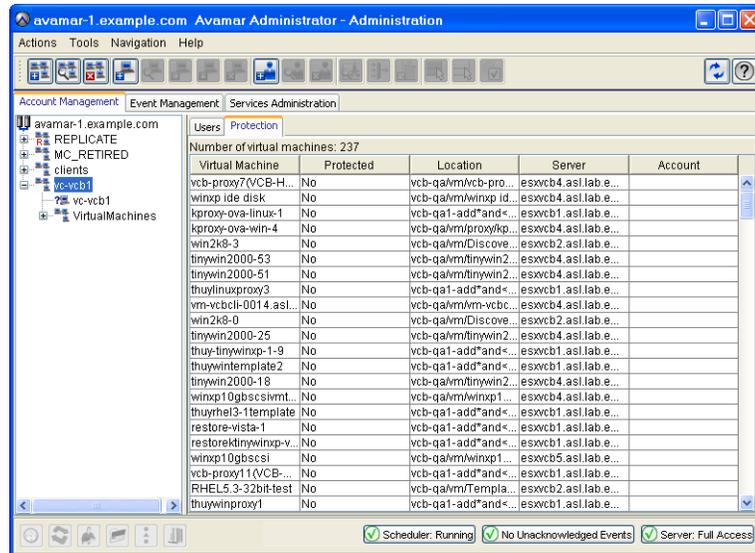
Editing VMware clients is similar to editing other Avamar clients. The primary difference is that when editing a client from the Policy window, each Edit Client dialog box includes a VMware tab that contains client properties relating to vCenter, image proxy or virtual machine clients. This tab is not shown for nonvirtual clients.

Contents of the VMware tab differs according to the type of client:

- On the Edit Client (vCenter) dialog box, editable credentials are shown.
- On the Edit Client (Image Proxy) dialog box, a list of all known datastores is shown.
- On the Edit Client (VirtualMachine) dialog box, datastores on which that virtual machine resides on are shown.

## Viewing Protected Virtual Machines

After you have created vCenter, virtual machine and proxy clients, the Administration window Account Management Protection tab displays the following when the vCenter domain is selected:



All the virtual machines in the vCenter, including those that are currently not protected with the VMware image proxy or guest backup, are listed on the Protection tab.

Virtual machines protected by guest have Avamar client software installed and are running backup agents in the guest operating system.

Virtual machines protected by image backup are backed up using the Avamar VMware Image Backup feature.

Those protected by both are protected by using both methods.

This tab serves as a single placeholder for viewing the backup protection state of all virtual machines. No action can be taken on this panel; it is for informational purposes only.

## Viewing Replicated Virtual Machine Name

The View Information feature is used to view the virtual machine name of any virtual machine in the REPLICATE domain.

This feature is disabled anywhere other than in the REPLICATE domain.

If you try to view information for a nonvirtual machine client, `No Information` appears.

1. Start Avamar Administrator.
2. Select **Navigation > Administration** or click the **Administration** launcher button.



The Administration window appears.

3. Click the Account Management tab.
4. In the tree, browse to the REPLICATE domain and select the client for which you want to view the virtual machine name.
5. Select **Actions > Account Management > View Information**.

A dialog box appears, which shows the virtual machine name.

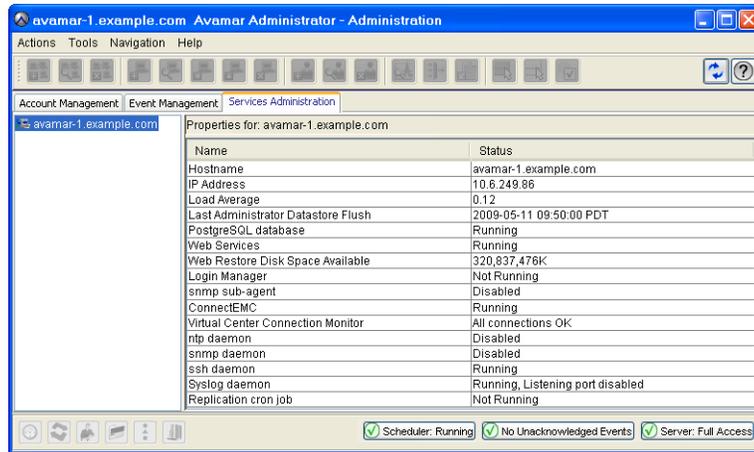
If you selected a nonvirtual machine client in step 5, a dialog box appears, which shows `No Information`.

6. Click **OK**.

The dialog box closes.

## VMware vCenter Connection Monitor

Avamar Administrator maintains a pool of connections to the vCenter. As with other essential services, the Administration window Services Administration tab provides continuous status for the vCenter connection.



To open the VMware vCenter Connection Monitor dialog box, double-click the VMware vCenter Connection Monitor.



Valid connection states are Unknown, Down, Idle and Active.

As with other essential services, connections to the vCenter can be stopped, started and restarted. Stop the connections for vCenter upgrades and start them when the upgrade has completed. If vCenter is shutdown, connections become invalid and must be reestablished. In such a case, windows such as the New Client dialog box display no vCenter structure or virtual machines.

## Backup and Restore

This topic describes how to perform on-demand VMware image backups, monitor backup and restore activities, and perform full image or file-level restores.

### Performing an On-Demand VMware Image Backup

All VMware Image Backups must be initiated from Avamar Administrator. It is not possible to initiate backups from the targeted virtual machine or image proxy client machine.

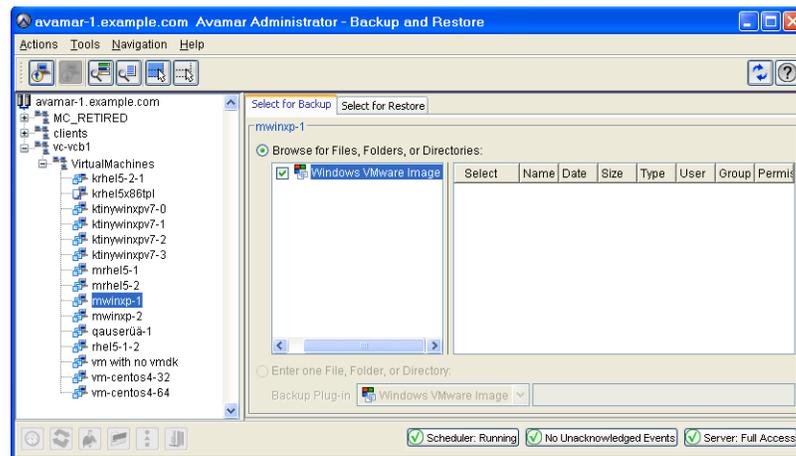
Performing a VMware Image Backup is substantially the same as performing any other on-demand Avamar backup.

1. Start Avamar Administrator.
2. Select **Navigation > Backup and Restore** or click the **Backup & Restore** launcher button.



The Backup and Restore window appears.

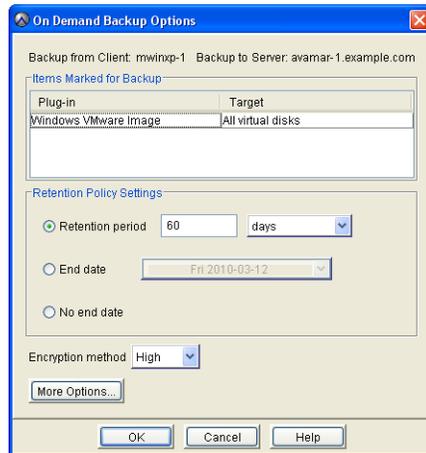
3. Click the Select for Backup tab.
4. Select a virtual machine client in the clients tree.
5. Select the top (root) folder.





6. Select **Actions > Backup Now...** or click the toolbar button (shown left).

The On Demand Backup Options dialog box appears.



7. Review your backup settings.

Clicking **Cancel** returns you to the Backup and Restore window where you can modify your backup selections.

Set Retention Policy

8. If you want to change your backup retention setting, select or type the following:

FIELD/OPTION	DESCRIPTION
Retention period	To delete this backup from the Avamar server after a specific number of days, weeks, months or years, select this option and type the number of days, weeks, months or years.
End date	To delete this backup from the Avamar server on a specific calendar date, select this option and browse to that date on the calendar.
No end date	To keep this backup for as long as this client remains active in the Avamar server, select this option.

9. Select the encryption method you want to use for client/server data transfer during this backup.

Choices are:

High      Strongest available encryption setting for that specific client platform.

Medium    Medium strength encryption.

None      No encryption.

**NOTE:** The exact encryption technology and bit strength used for any given client/server connection is dependent on a number of factors, including the client platform and Avamar server version. Refer to your *Avamar Product Security Guide* for additional information.

10. Click **OK**.

The On Demand Backup Options dialog box closes and the following status message appears: Backup initiated.

11. Click **OK**.

## Monitoring Backup and Restore Activities

For VMware Image backups and restores, the Activity Window Proxy column shows the name of the proxy client performing the backup or restore on behalf of the virtual machine. It shows N/A for all other activities.

## Backup Validation

Validation is not available for VMware image backups.

## Viewing Backup Statistics

If you attempt to view statistics for a virtual machine backup, a message appears stating that file statistics are not gathered for virtual machines.

## Image Restore Overview

All VMware image restores must be initiated from the Avamar Administrator. It is not possible to initiate restores from the virtual machine or proxy client machine.

All Virtual Disks  
and Browse Virtual  
Disks Toolbar  
Buttons

If your Avamar environment is configured to support both VMware image restore and optional Windows file-level restore feature (page 81), the Avamar Administrator Backup and Restore window Restore tab displays two buttons above the Select for Restore contents pane, which are not shown if a normal (non-VMware Image) backup is selected:



Clicking the All Virtual Disks button (left) initiates an image restore, which restores an entire image — all virtual disks and all information residing on those disks. This is the selection you will make for all restore procedures in this chapter.



Clicking the Browse Virtual Disks button (right) initiates a file level restore, which selectively restores a set of folders or files from an image backup. Refer to *Restoring Folders or Files from a VMware Image Backup* (page 91) for additional information.

Additionally, when performing a VMware image restore, the Restore Options dialog box is different from the normal (non-VMware Image) Restore Options dialog box. The primary differences are that virtual machine information is shown and three choices for restore destinations are offered:

- Original virtual machine
- Different (existing) virtual machine
- New virtual machine

Once the destination selection is made, each procedure varies slightly from that point forward.

Destination target virtual machines must be powered off in order for the restore to be successful.

If restoring from a template backup, the Restore to original virtual machine destination is disabled.

## Restoring to the Original Virtual Machine

1. Ensure that the target virtual machine is powered off.
2. Start Avamar Administrator.
3. Select **Navigation > Backup and Restore** or click the **Backup & Restore** launcher button.



The Backup and Restore window appears.

4. Click the Select for Restore tab.
5. Select a client in the clients tree.
6. Locate and select a backup from which you want to restore.
7. Do one of the following:



IF	DO THIS
Your Avamar environment is configured to support both VMware image restore and optional Windows file-level restore feature (page 81)	Click the All Virtual Disks button (shown left) directly above the contents pane.
Your Avamar environment is configured to only support VMware image restore.	Skip this step and go directly to step 8.

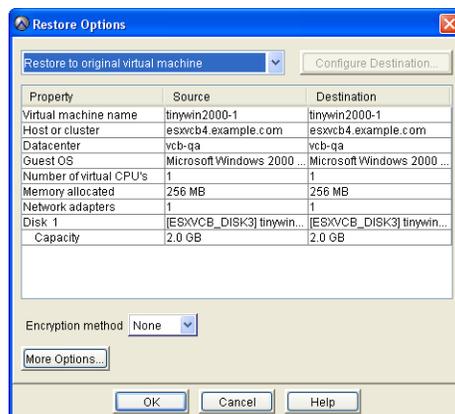
8. In the contents pane, select the All virtual disks folder checkbox.
9. Select **Actions > Restore Now...** or click the toolbar button (shown left).



The Restore Options dialog box appears.

**NOTE:** When restoring an image backup to the original virtual machine, the **Configure Destination...** option is disabled.

10. Select Restore to original virtual machine as the restore destination.



11. Click **OK**.

The Restore Options dialog box closes and the following warning message appears:

Hardware compatibility issues between source and target destinations may result in a non-operational restored virtual machine.

This warning is alerting you to the following possible serious ramifications of restoring a backup to the original virtual machine if that virtual machine configuration has changed since the backup was taken. Under these circumstances, the restored virtual machine might not boot.

If the original virtual machine no longer exists, the following message appears:

Virtual machine is no longer addressable through vCenter. Do you want to re-create the virtual machine with this backup?

If the original virtual machine no longer exists and you do not recreate it, the restore operation will fail.

12. Click **OK**.

The previous message dialog box closes and the following message appears: Restore initiated.

13. Click **OK**.

## Restoring to a Different (Existing) Virtual Machine

1. Ensure that the target virtual machine is powered off.
2. Start Avamar Administrator.
3. Select **Navigation > Backup and Restore** or click the **Backup & Restore** launcher button.



The Backup and Restore window appears.

4. Click the Select for Restore tab.
5. Select a client in the clients tree.
6. Locate and select a backup from which you want to restore.
7. Do one of the following:



IF	DO THIS
Your Avamar environment is configured to support both VMware image restore and optional Windows file-level restore feature (page 81)	Click the All Virtual Disks button (shown left) directly above the contents pane.
Your Avamar environment is configured to only support VMware image restore.	Skip this step and go directly to step 8.

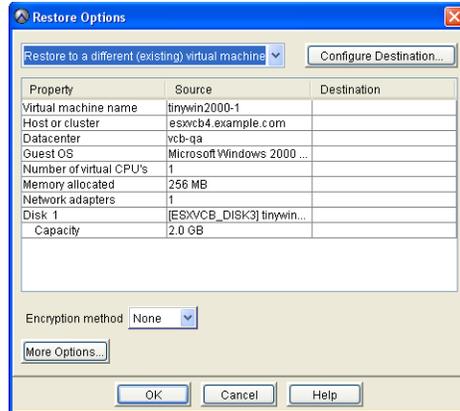
8. In the contents pane, select the All virtual disks folder checkbox.



9. Select **Actions > Restore Now...** or click the toolbar button (shown left).

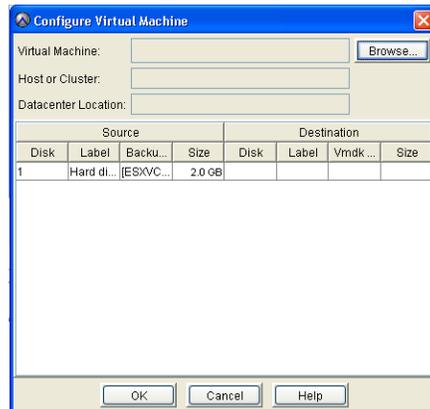
The Restore Options dialog box appears.

10. Select Restore to a different (existing) virtual machine as the restore destination.



11. Click **Configure Destination...**

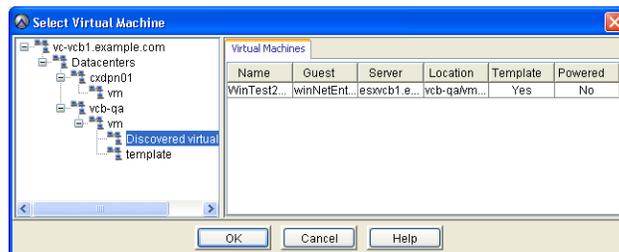
The Configure Virtual Machine dialog box appears.



Select Destination  
Virtual Machine

12. Click **Browse** to open

The Select Virtual Machine dialog box appears.



**NOTE:** Only virtual machines that are powered off can be selected from the list; all others are disabled. You are also prevented from selecting the original virtual machine.

13. Select the virtual machine you want to restore to and click **OK**.

The Select Virtual Machine dialog box closes.

14. Switch to Configure Virtual Machine dialog box and click **OK**.

The Configure Virtual Machine dialog box closes.

15. Switch to Restore Options dialog box and click **OK**.

The Restore Options dialog box closes and the following warning message appears:

Hardware compatibility issues between source and target destinations may result in a non-operational restored virtual machine.

This message is alerting you to the following possible serious ramifications of restoring a backup to the original virtual machine if that virtual machine configuration has changed since the backup was taken. Under these circumstances, the restored virtual machine might not boot.

## Restoring to a New Virtual Machine

1. Ensure that the target virtual machine is powered off.
2. Start Avamar Administrator.
3. Select **Navigation > Backup and Restore** or click the **Backup & Restore** launcher button.



The Backup and Restore window appears.

4. Click the Select for Restore tab.
5. Select a client in the clients tree.
6. Locate and select a backup from which you want to restore.
7. Do one of the following:



IF	DO THIS
Your Avamar environment is configured to support both VMware image restore and optional Windows file-level restore feature (page 81)	Click the All Virtual Disks button (shown left) directly above the contents pane.
Your Avamar environment is configured to only support VMware image restore.	Skip this step and go directly to step 8.

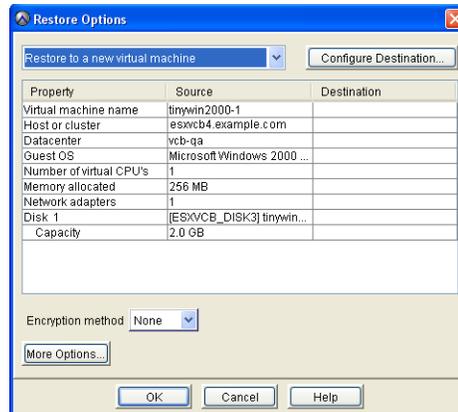
8. In the contents pane, select the All virtual disks folder checkbox.



9. Select **Actions > Restore Now...** or click the toolbar button (shown left).

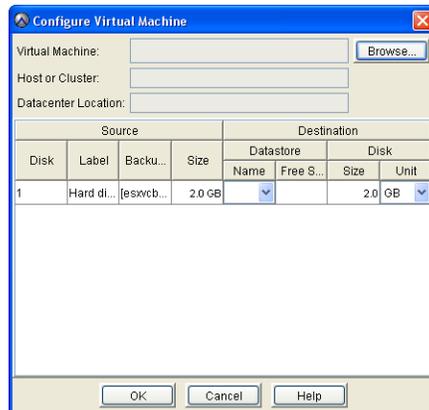
The Restore Options dialog box appears.

10. Select Restore to a new virtual machine as the restore destination.



11. Click **Configure Destination...**

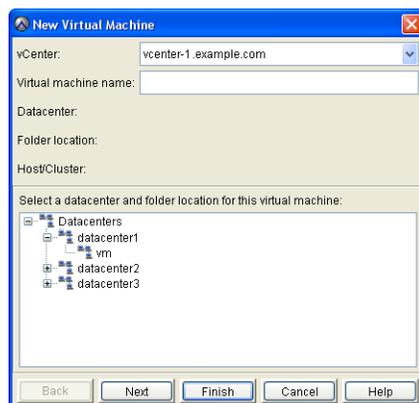
The Configure Virtual Machine dialog box appears.



Name the New  
 Virtual Machine  
 and Select a  
 Location

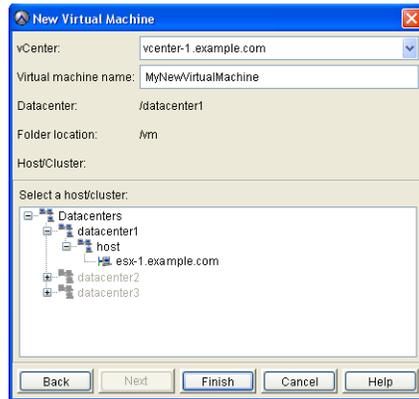
12. Click **Browse** to open

The New Virtual Machine wizard appears.



13. Type a name for the new virtual machine in the Virtual Machine Name field.
14. In the tree, select a datacenter and folder location for this new virtual machine.
15. Click **Next**.

The next New Virtual Machine wizard screen appears.



16. Select the vCenter ESX Server that will host the new virtual machine.
17. Click **Finish**.

The New Virtual Machine wizard screen closes.

18. Switch to Configure Virtual Machine dialog box and click **OK**.

The Configure Virtual Machine dialog box closes.

19. Switch to Restore Options dialog box and click **OK**.

The Restore Options dialog box closes.

## Groups and Policy Management

This topic discusses how to use Avamar groups and policy management features (datasets, retention policies, schedules, and so forth) to manage the VMware Image backup and restore feature.

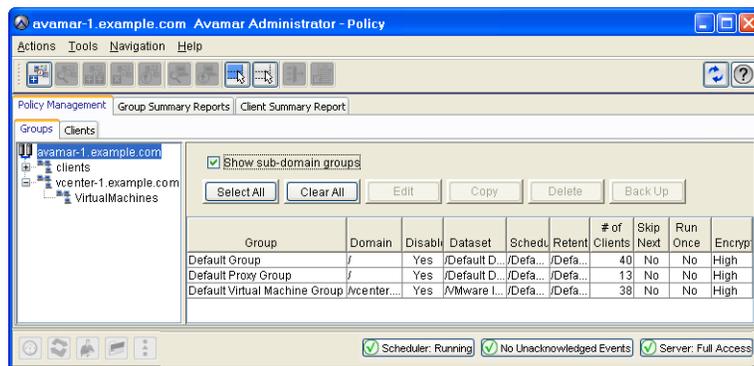
### Groups and Group Behavior

This topic discusses special groups and important behavioral differences related to the Avamar VMware Image Backup and Restore feature.

**Default Proxy Group.** By default, the Default Proxy Group is where VMware image proxy clients reside. This group cannot be deleted. Enabling the Default Proxy Group does not conflict with scheduled backups performed by other plugins configured on the proxy client.

**Default Virtual Machine Group.** By default, the Default Virtual Machine Group is where new virtual machine clients are automatically added when they are registered. This group cannot be manually deleted but is automatically deleted if the vCenter Domain is deleted.

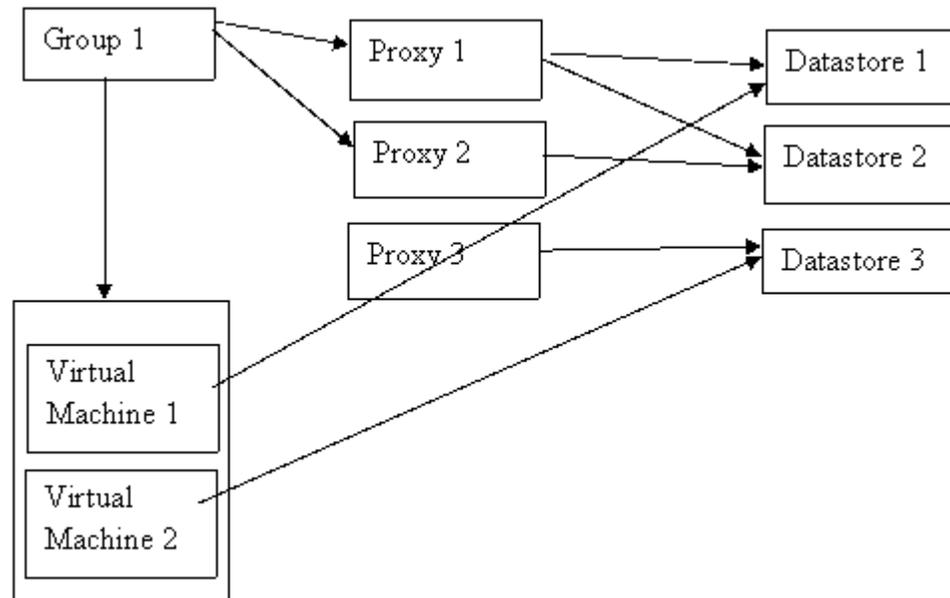
The following Policy window screenshot shows a Policy Management pane Groups tab listing, which includes the three default Avamar groups: the Default Group, Default Proxy Group and Default Virtual Machine Group.



**vCenter Groups.** Any group created under the vCenter domain is considered a "vCenter" group. This group behaves like any other group except that it contains provisions for specifying which VMware image proxy clients are assigned to perform backups on behalf of its group members.

### Virtual Machine and Proxy Client Relationships within vCenter

**Groups.** Consider the following (greatly simplified) example configuration:



Virtual machines VM-1, VM-2 and VM-3 store their data in Datastore-1, Datastore-2 and Datastore-3, respectively.

Within Avamar Administrator, proxies have been assigned to protect vCenter datastores as follows:

- Proxy-1 has been assigned to Datastore-1 and Datastore-2
- Proxy-2 has been assigned to Datastore-2
- Proxy-3 has been assigned to Datastore-3

All of these datastore assignments are made at the client level in the Client Properties dialog box.

A vCenter is group is created, to which virtual machine clients VM-1, VM-2 and VM-3 are added.

In order to protect these Virtual machines, proxy clients must also be added to the vCenter group as follows:

- Proxy-1, by way of its assignment to both Datastore-1 and Datastore-2, can protect both VM-1 and VM-2 virtual machine clients.
- Proxy-2, because it is only assigned to Datastore-2, is optional as long as Proxy-1 exists in the vCenter group.
- Proxy-3, because it is only assigned to Datastore-3 is mandatory in order to protect VM-3.

---

**IMPORTANT:** It is absolutely critical that every virtual machine client in your vCenter groups has a corresponding proxy client in that vCenter group that can access the required vCenter datastore. Otherwise, when a backup is initiated and a proxy cannot be located to perform the backup, the backup will fail with an Activity monitor status of "no proxy."

---

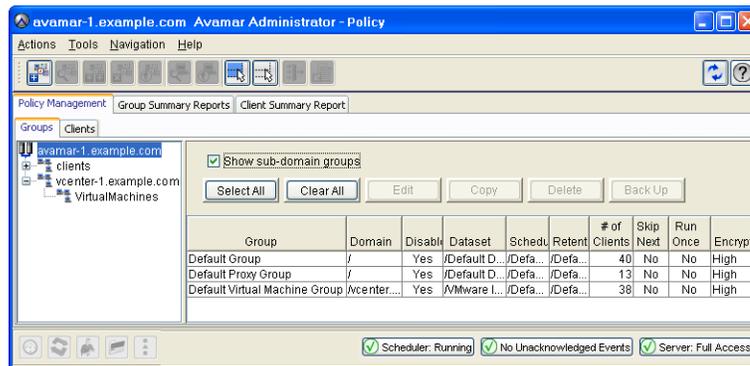
## Editing the Default Virtual Machine Group and Other vCenter Groups

The Default Virtual Machine Group and Other vCenter groups contain special settings that are unique to this context. This topic explains those special settings.

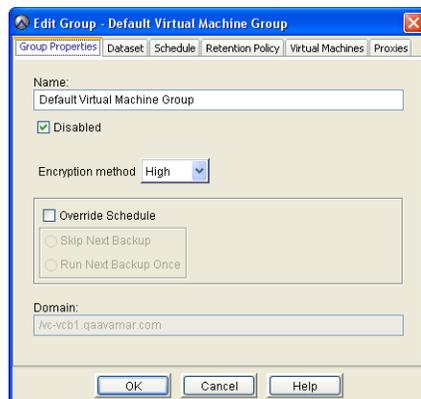
1. Start Avamar Administrator.
2. Select **Navigation > Policy** or click the **Policy** launcher button.

The Policy window appears.

3. Click the Policy Management tab.
4. Click the Groups tab.



5. Select the Default Virtual Machine Group.
6. Select **Actions > Group > Edit Group...**, right mouse button **Edit Group...**, click **Edit** or click the toolbar button (shown left).
7. The Edit Group Default Virtual Machine Group dialog box appears.



The following additions and changes are unique to editing the Default Virtual Machine Group and other vCenter groups:

- The Clients tab is renamed Virtual Machines.
- The Proxies tab presents a list of known VMware Image Proxies that can be assigned to this group.

To assign a image proxy client to this group, select the checkbox next to that image proxy client.

The Proxies tab is hidden for for non-vCenter groups.

- Clicking the Virtual Machines tab **Add** button shows a list of known virtual machine clients that are not yet members of the Default Virtual Machine Group.

If a virtual machine is not yet known (that is, it has not been registered with the Avamar server) or if it is already a member of the Default Virtual Machine Group, it is not shown in this list.

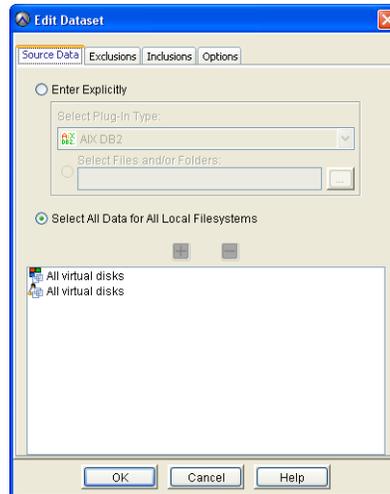
vCenter virtual machines do not show up in this list unless they have been registered as Avamar clients.

8. Edit the information you want to change.
9. Click **OK**.

The Edit Group Default Virtual Machine Group dialog box closes.

## VMware Image Dataset

The VMware Image Dataset is the default dataset that is assigned to the Default Virtual Machine Group (page 75), and other vCenter groups (page 75) when they are first added.



The VMware Image Dataset is in many respects simpler than most other datasets:

- The only source data plugins shown are Linux and Windows virtual disks; both are selected by default.
- The **Select Files and/or Folders** option, as well as the Exclusions and Inclusions tabs are disabled.
- Changed block tracking is enabled by default using an embedded `utilize_changed_block_list=true` plugin option statement.

---

**TIP:** When creating other datasets for use with the Avamar VMware image backup feature, you should copy this dataset so that you can use these recommended settings as the basis for other datasets. Refer to your *Avamar System Administration Guide* for additional information about copying datasets.

---

## Troubleshooting

This topic describes how to resolve common issues that might arise with Avamar VMware image backup and restore.

### Problems Adding vCenter Server as Avamar Client

If you encounter problems adding a vCenter server as an Avamar client (page 49), first ensure that your vCenter hostname, username and password are correct.

Also ensure that data port 443 is open between the Avamar server and vCenter system.

If that does not resolve the problem, try turning off certificate authentication for all vCenter-to-Avamar MCS communications (page 46).

### Backup Does Not Start

If a backup activity fails to start, ensure that an Avamar Image Backup Proxy has been properly deployed (page 31), and that the datastore for the source virtual machine has been selected on a running proxy server.

If that does not resolve the problem, the account used to connect to vCenter might not have sufficient privileges. To verify account privileges, log into the vSphere client with that username and password. Ensure that you can access datastores on that client. If you cannot, that account does not have the required privileges.

# OPTIONAL WINDOWS FILE-LEVEL RESTORE

---

Windows file-level restore is an optional feature that uses the Avamar VMware File-Level Restore plugin to selectively restore folders and files from a VMware image backup to a running virtual machine.

## Capabilities and Limitations

This topic discusses the capabilities and limitations of the Windows file-level restore feature.

**Capabilities.** The Windows file-level restore feature offers the following capabilities:

- Restore a selected folders or files without restoring the entire image backup.
- You can browse existing VMware image backups to select which folders or files to restore.
- You can browse running virtual machine filesystems to select an existing folder as the restore destination.
- You can restore to an existing folder or a new folder on a running virtual machine.
- You can monitor file-level restore activities using Avamar Administrator.
- Restore resources are off-loaded to a proxy client.
- Multiple restores can be queued from one or more Avamar Administrator user interfaces.
- Multiple browses can be performed from one or more Avamar Administrator user interfaces.
- Restore activities are reported through Avamar logs.

**Limitations.** Consider the following limitations before implementing the Windows file-level restore feature:

- File-level restore is supported only on properly configured Windows proxy clients; non-Windows systems are not supported.
- VMware Tools must be installed on the target virtual machine.
- The target virtual machine must be powered on.
- Queued restores are always processed serially.
- Cancellation of an in-progress restore might inhibit all file-level restore browse operations from all Avamar Administrator instances for approximately five minutes.
- The destination target must be a running Windows virtual machine.
- ACLs are not preserved.
- Hidden and system attributes are not preserved.
- Hidden, system, and other files with read-only attributes cannot be overwritten.
- When restoring very large files, single-file copy operations that take longer than 60 minutes will fail, causing that entire restore operation to be terminated.
- Restoring encrypted files is not supported. Restoring an encrypted file will result in a `file not found` error during the restore. The final restore activity status will be failed because an error occurred during the restore. If both encrypted and unencrypted files are selected in the same restore operation, the unencrypted files will be properly restored even though the encrypted files will not be restored.
- Compressed files will be restored uncompressed.
- Occasionally, VMware Tools on the target virtual machine might cause files to be in an unstable state. If this occurs, restart the VMware Tools Service on the target virtual machine.
- File-level restore does not send progress reports to the Avamar Administrator. So, no progress updates appear in the activity monitor for active restores.
- Explicit folder and files excludes are not supported. If restoring a folder, you must restore its entire contents.
- Restore mode is always overwrite. If this not desirable, restore to an empty folder to avoid overwriting existing folders and files.
- Direct restores to physical machines is not supported. To restore files to a physical machine, they must first be restored to a virtual machine, then copied to the physical machine.
- When upgrading the Windows proxy client, any existing Avamar software must be uninstalled prior to installing a new version. In some cases, you must reboot the system after uninstalling.

## Configuration and Setup

This topic describes how to configure and set up the file-level restore feature.

**Additional Required Software.** The file-level restore feature requires that you manually install the following additional Microsoft and VMware software on the proxy server:

- Microsoft .Net Framework v2.0
- VMware VIX API Version 1.7.0-186713

**How AvFS Works with VMware File Level Restore.** The Avamar VMware Windows file-level restore feature is implemented using a Windows proxy client virtual machine. The Avamar and VMware software running on the Windows proxy requires a CIFS share which is exported by the Avamar server. This CIFS share provides a remote hierarchical filesystem view of the backups stored on the Avamar server. VMware Image Backups are accessed by way of the CIFS share in order to browse and restore their contents.

The CIFS share exported by the Avamar server requires AvFS to be installed and configured as described in previously in this publication.

Access to the CIFS share requires a Samba username and password. The Samba credentials are chosen and created on an Avamar server as described previously in this publication. An Avamar MCS is configured with the Samba credentials as described in the *Avamar VMware Guide*.

During restore operations, the Avamar MCS server passes the Samba credentials to the Windows proxy client to perform the file level browses and restores.

**Task List.** Properly configuring and setting up the Windows file-level restore feature comprises the following tasks:

- *Task 1: Configure and Set Up Avamar File System (AvFS)* (page 83)
- *Task 2: Modify mcserver.xml Preferences* (page 84)
- *Task 3: Prepare and Deploy Windows File-Level Restore Proxy* (page 85)

### Task 1: Configure and Set Up Avamar File System (AvFS)

You must also install, configure and enable an Avamar File System (AvFS) according to the instructions found in EMC publication *300-009-660 Avamar File System (AvFS) Technical Note*.

You must also configure AvFS for use with Samba and apply the additional Samba security strengthening measures. Those instructions are also found in EMC publication *300-009-660 Avamar File System (AvFS) Technical Note*.

## Task 2: Modify mcserver.xml Preferences

After successfully configuring Avamar File System (AvFS), you must modify the Avamar server mcserver.xml preferences file as follows:

1. Open a command shell.
2. Do one of the following:

User=admin

IF	DO THIS
Administering a single-node Avamar server.	Log into the server as user admin. When prompted for a password, type the admin password and press <b>ENTER</b> .
Administering a multi-node Avamar server.	Log into the utility node as user admin. When prompted for a password, type the admin password and press <b>ENTER</b> .

Stop MCS

3. Stop the MCS by typing:

```
dpnctl stop mcs
```

4. Modify mcserver.xml preference settings as follows:

PARAMETER	DESCRIPTION
samba_addr	The Avamar server network hostname as defined in DNS or IP address.
samba_account	Samba user account name.
samba_password	Samba user account password.

- (a) Open `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` in a Unix text editor.
- (b) Locate the `samba_addr` preference.
- (c) Change the `samba_addr` preference setting to the actual Avamar server network hostname as defined in DNS or IP address.
- (d) Locate the `samba_account` preference.
- (e) Change the `samba_account` preference setting to a valid samba user account.
- (f) Locate the `samba_password` preference.
- (g) Change the `samba_password` preference setting to the actual password for the samba user account.
- (h) Save your changes.

Restart MCS

5. Restart the MCS by typing:

```
dpnctl start mcs
```

## Task 3: Prepare and Deploy Windows File-Level Restore Proxy

---

**IMPORTANT:** Windows proxies can only be used to implement file-level restore of Windows virtual machine image backups. They cannot at this time be used to implement Avamar VMware image backup and restore.

---

---

**IMPORTANT:** File-level restore must be installed on a clean virtual machine proxy running Windows Server 2003 Standard Edition SP2 operating system. Note that Windows Server 2003 Standard Edition SP2 is not Windows Server 2003 R2 Standard Edition SP2. The latter has significantly tighter security that prevents file-level restore from functioning.

---

---

**IMPORTANT:** Do not make the proxy a member of a domain. You might not be able to restore files if the ACLs do not have proper permissions.

---

### Create Virtual Machine

1. Create a clean Windows Server 2003 Standard Edition SP2 or later virtual machine with the following characteristics:
  - 1 CPU
  - 1 GB RAM
  - 8 GB hard disk space

2. Power on and log into the virtual machine.

The login user account must have Administrator privileges.

3. Install and configure VMware Tools as follows:

- (a) Install VMware Tools on this virtual machine.
- (b) Wait for installation to complete.
- (c) Double-click the VMware Tools tray icon.

The VMware Tools Properties dialog box appears.

- (d) Click the Options tab.

- (e) Set the **Time synchronization between the virtual machine and the host operating system** option and click **OK**.

The VMware Tools Properties dialog box closes.

4. Install Microsoft .NET Framework v2.0 as follows:

- (a) Log onto [www.microsoft.com/downloads](http://www.microsoft.com/downloads) and search for Microsoft .NET Framework Version 2.0 Redistributable Package (x86).
- (b) Download the software package to a convenient location on the virtual machine (for example, the desktop or C:\Temp).
- (c) Open a DOS prompt.

### Install and Configure VMware Tools

### Install Microsoft .NET Framework v2.0

- (d) Change directory to the folder in step b.
- (e) Type:  
**dotnetfx.exe.**
- (f) Wait for installation to complete.
- (g) Verify .NET Framework installation by checking for existence of the following folder:  
WINDIR\Microsoft.NET\Framework\v2.0.50727

Install VMware VIX  
API Version 1.7.0-  
186713

- 5. Install VMware VIX API Version 1.7.0-186713 as follows:
  - (a) Go to [www.vmware.com/support/developer/vix-api](http://www.vmware.com/support/developer/vix-api).
  - (b) Download VMware Vix API v1.7 to the virtual machine.
  - (c) Run (double-click) VMware-vix-1.7.0-186713.exe to install VMware Vix API v1.7.
  - (d) Accept all default parameters during installation.

Download Avamar  
Image Plugin ISO  
to datastore ESX  
host

- 6. Download the Avamar Image Plugin ISO to the virtual machine as follows:
  - (a) From your computer, point your web browser at the Avamar server by typing the following URL:  
**http://AVAMARSERVER**  
Where AVAMARSERVER is your actual Avamar server network hostname as defined in DNS or IP address.  
You will be automatically redirected to the Avamar secure web server.  
Depending on your browser security settings, a security alert dialog box might appear.
    - (b) If a security alert dialog box appears, click **Yes** or **OK** to allow redirection to the Avamar secure web server.  
The Secure Log On page appears.
    - (c) Page down until the **Documents and Downloads** hyperlink is visible.
    - (d) Click **Documents and Downloads**.  
The Downloads and Documentation page appears.  
Page down until the Windows for x86 (32 bit) section is visible.
    - (e) Click the **Microsoft Windows XP, 2003, Vista, 2008** hyperlink.  
The Downloads for Microsoft Windows XP, 2003, Vista, 2008 page appears.
    - (f) Click the AvamarVmImage-windows-x86-VERSION.iso hyperlink.  
Where VERSION is the specific version Avamar Image Plugin ISO you are installing.  
The File Download dialog box appears.
    - (g) Click **Save** to save AvamarVmImage-windows-x86-VERSION.iso to a convenient location on your computer (for example, your desktop or C:\Temp).

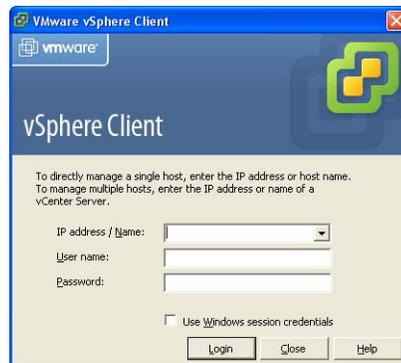
Install Avamar Image Plugin ISO on Virtual Machine.

7. Install AvamarVmImage-windows-x86-VERSION.iso on the virtual machine as follows:

(a) Do one of the following:

IF	DO THIS
You are upgrading existing EMC Avamar VM Image Backup Win32 software on this virtual machine.	Log into the Windows file-level restore proxy virtual machine. Use <b>Control Panel &gt; Add or Remove Programs</b> to remove the existing EMC Avamar VM Image Backup Win32 software.
You are installing EMC Avamar VM Image Backup Win32 software for the first time on this virtual machine.	Skip this step. Proceed directly to step (b).

(b) From your Windows computer, launch the vSphere client application. The VMware vSphere Client login dialog box appears.



(c) Log into the vCenter server by typing the following:

FIELD	DESCRIPTION
IP address / Name	vCenter server IP address or network hostname as defined in DNS.
User name	User account name.
Password	Password for this username.

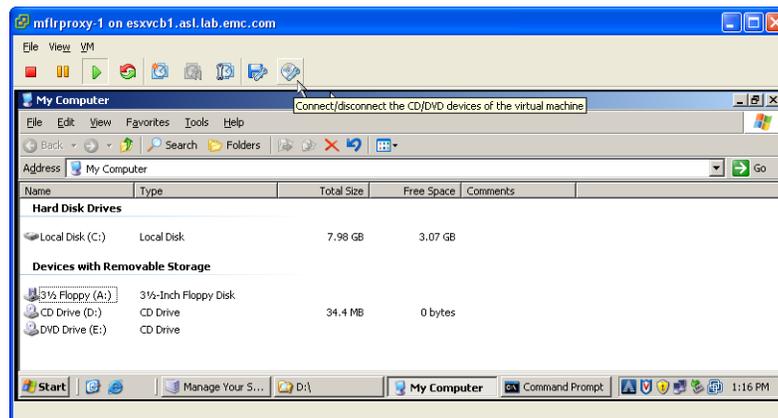
(d) Click **Login**.

The VMware vSphere Client login dialog box closes. The vSphere Client window appears.

(e) Switch to Hosts and Clusters view by clicking **View > Inventory > Hosts and Clusters**.

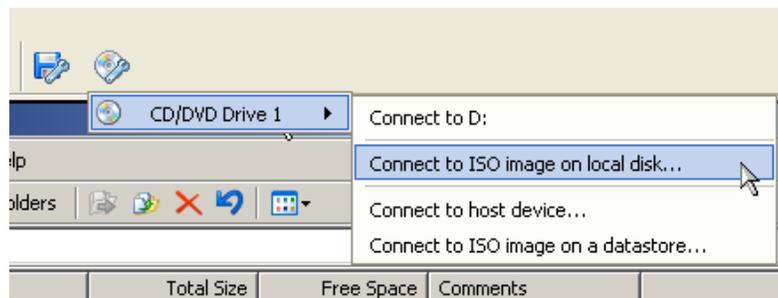
Mount ISO File and Install the Software

- (f) Locate and select the Windows proxy virtual machine client in vSphere.
- (g) Right-click the virtual machine and select **Open Console**.  
 The Console window appears.
- (h) Log into the virtual machine as Administrator.
- (i) Open My Computer.  
 Under Devices with Removable Storage, a CD Drive with by a drive letter in parentheses is present.
- (j) Click the Connect/disconnect CD/DVD devices toolbar icon (shown left and in following screenshot).



A menu appears.

- (k) Select **CD/DVD Drive 1**.  
 A sub-menu appears.
- (l) In the sub-menu, click **Connect to ISO image on local disk...**



The Open dialog box appears.

- (m) Ensure that ISO Image files (\*.iso) is the Files of type selection.
- (n) Browse to and select the AvamarVmlImage-windows-x86-VERSION.iso file that was previously downloaded in step 6.
- (o) Click **Open**.  
 The Open dialog box closes.
- (p) Switch to Windows Explorer My Computer.

- (q) Wait until the CD Drive shown in Devices with Removable Storage shows a total size used that is approximately the same size as the AvamarVmImage-windows-x86-VERSION.iso file.

This indicates that the ISO image successfully mounted.

Once the ISO image has successfully mounted, the installation process should automatically start. The EMC Avamar VM Image Backup Win32 Setup Wizard appears.

- (r) Do one of the following:

IF	DO THIS
The installation process automatically starts.	Skip this step. Proceed directly to setp (s).
The installation process does not automatically start.	Right-click the Vm Image backup Install file, and select <b>AutoPlay</b> . If <b>AutoPlay</b> is not available, select <b>Open</b> , then double-click <b>Setup.exe</b> to start the setup wizard.

If the the installation process does not automatically start, right-click the Vm Image backup Install file, and select **AutoPlay**. If **AutoPlay** is not available, select **Open**, then double-click **Setup.exe** to start the setup wizard.

- (s) Follow the on-screen instructions.
- (t) Click **Install** to initiate the installation.  
 Wait for the installation to complete.
- (u) Click **Finish** to exit the setup wizard.  
 The EMC Avamar Client icon appears in the Windows system tray.
- (v) Click the Connect/disconnect CD/DVD devices toolbar icon (shown left).  
 A menu appears.
- (w) Select **CD/DVD Drive 1**.  
 A sub-menu appears.
- (x) Click **Disconnect from C:\Temp\AvamarVmImage-windows-x86-VERSION.iso...**  
 A Disconnect Device warning appears.
- (y) Click **Yes**.  
 The Disconnect Device dialog box closes.
- (z) Switch to Windows Explorer My Computer.  
 The CD Drive shown Devices with Removable Storage shows 0 bytes total size.



Register and  
 Activate Proxy  
 Client with Avamar  
 Server



8. Register and activate proxy client with Avamar server as follows:

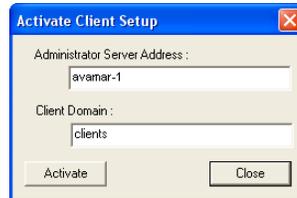
(a) Switch to Windows file-level restore proxy virtual machine.

(b) Right-click the Avamar system tray icon (shown left).

A menu appears.

(c) Select **Activate**.

The Activate Client Setup dialog box appears.



(d) Type the following:

FIELD	DESCRIPTION
Administrator Server Address	Administrator server network hostname as defined in DNS.
Client Domain	Avamar domain where you want this client to reside. The default domain is "clients." However, your Avamar system administrator may have defined other domains and subdomains. Consult your Avamar system administrator for the specific domain you should use when registering this client. <b>IMPORTANT:</b> If typing a subdomain (for example, clients/MyClients), do not include a slash (/) as the first character. Including a slash as the first character will cause an error and prevent you from registering this client.

(e) Click **OK**.

The Activate Client Setup dialog box closes.

9. Configure the proxy's DNS entries to resolve hostnames for the Avamar server, vCenter, ESX hosts, and all virtual machines that will be using it.

---

**IMPORTANT:** EMC recommends installing an antivirus program on the proxy.

---

## Restoring Folders or Files from a VMware Image Backup

The Windows file-level restore feature uses existing VMware image backups. However, except for the type of backup used for the restore, the procedure is substantially the same as restoring selected folders or files from a normal (non-VMware Image) backup.

### All Virtual Disks and Browse Virtual Disks Icons

In order to support both full image restores (page 68) and Windows file-level restores, once an existing image backup is selected, the system displays two icons above the Select for Restore contents pane, which are not shown if a normal (non-VMware Image) backup is selected:

-  Clicking the All Virtual Disks icon (left) initiates an image restore, which restores an entire image — all virtual disks and all information residing on those disks. Refer to *Image Restore Overview* (page 68) for additional information.
-  Clicking the Browse Virtual Disks icon (right) initiates a file level restore, which selectively restores a set of folders or files from an image backup. This is the selection you will make for all restore procedures in this chapter.

If restoring files to a different location (redirected restore), you are limited to restoring to an existing virtual machine that is known to the system. You cannot create a new virtual machine as part of the restore operation (as you can with image backups), nor can you restore folders or files directly to physical machines. In order to restore files to a physical machine, they must first be restored to a virtual machine, then copied to the physical machine.

To selectively restore folders and files from an existing VMware image backup:

1. Start Avamar Administrator.
2. Select **Navigation > Backup and Restore** or click the **Backup & Restore** launcher button.  
The Backup and Restore window appears.
3. Click the Select for Restore tab.
4. Select a client in the clients tree.
5. Locate and select a backup from which you want to restore.
6. Click the Browse Virtual Disks icon (shown left) directly above the contents pane.
7. Select one or more folders or files you want to restore.



---

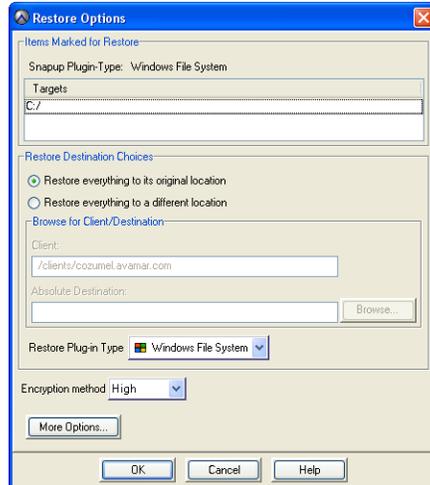
**TIP:** Select **Actions > Preview List...** to view a summary of all folders and files you have just selected for an on-demand restore.

---



Select **Actions > Restore Now...** or click the toolbar icon shown immediately to the left.

The Restore Options dialog box appears.



8. Review your restore settings.

Clicking **Cancel** returns you to the Backup and Restore window where you can modify your restore selections.

Restore destination choices allows you to specify which client and top-level (root) folder will receive the restored files.

9. If you want to change your restore destination choices, select or type the following:

FIELD/OPTION	DESCRIPTION
Restore everything to its original location	<p><b>Restore everything to its original location</b> is the default destination — all files are restored to original client in the original top-level (root) folder.</p>
Restore everything to a different location	<p><b>Restore everything to a different location</b> allows you to specify another client or another folder on the same client.</p> <p><b>IMPORTANT:</b> When restoring files to a different location (redirected restore), you are limited to restoring to an existing virtual machine that is known to the system. You cannot restore folders or files to nonvirtual machine clients</p> <p><b>IMPORTANT:</b> When redirecting a restore to a new location (a target folder other than the original folder that was backed up), restoring a single folder only restores the contents of the folder. The original parent folder is not restored as part of this operation. However, if you restore two or more folders to a new location, then the original parent folders do get restored along with the contents of those folders.</p>

FIELD/OPTION	DESCRIPTION
Browse for Client/ Destination	Click <b>Browse</b> to locate a client or folder for the restore. <b>TIP:</b> You can also type this destination path (client\folder) directly in the Absolute Destination field.
Restore Plug-in Type	Specifies which client plugin will be used to perform this restore. The default selection is the same plugin used to take the original backup.
Encryption Method	Encryption method used for client/server data transfer. Choices are:  High      Strongest available encryption setting for that specific client platform.  Medium    Medium strength encryption.  None      No encryption.  <b>NOTE:</b> The exact encryption technology and bit strength used for any given client-server connection is dependent on a number of factors, including the client platform and Avamar server version. Refer to your <i>Avamar Product Security Guide</i> for additional information.

---

**TIP:** If you want to include plugin options with this restore, click **More Options...**, then select or clear the desired options and type values where applicable.

Refer to your *Avamar System Administration Guide* for additional information about plugin options.

---

10. Click **OK**.

The Restore Options dialog box closes. The following status message appears: Restore initiated.

11. Click **OK**.

# PROTECTING THE vCENTER MANAGEMENT INFRASTRUCTURE

---

Previous chapters covered various aspects of protecting VMware virtual machine data using Avamar VMware image backup and restore. This chapter covers how to protect the actual vCenter management infrastructure (not the virtual machines within that environment).

Avamar provides support for backing up the following vCenter management infrastructure components:

- License files
- SSL certificates
- Audit logs
- Windows guest customization (sysprep) files
- Database-hosted configuration settings
- UpdateManager database
- Site Recovery Manager (SRM) database

The vCenter runs on a 32- or 64-bit Windows host and employs a database server which can run on a different host. Some optional vSphere components require additional databases that can be hosted on the same host as vCenter or on different database server hosts.

The basic methodology for protecting vCenter management infrastructure is to implement either guest backup (page 17) or VMware image backup (page 22) on each virtual host using a custom dataset that only backs up important vCenter management infrastructure components.

Recovering vCenter management infrastructure using Avamar backups is a two-step process in which you first create a restore target virtual machine with a fresh operating system image, then restore the vCenter management infrastructure components from the latest Avamar backup.

One advantage to protecting your vCenter management infrastructure with Avamar is that you can also use the Avamar backup to facilitate vCenter upgrades (for example, upgrading the vCenter host from a 32-bit to a 64-bit Windows virtual machine).

## Backing Up the vCenter Management Infrastructure

As previously mentioned, the basic methodology for protecting vCenter management infrastructure is to implement either guest backup (page 17) or VMware image backup (page 22) on each virtual host using a custom dataset that only backs up important vCenter management infrastructure components.

You should then add the vCenter Avamar clients to a group and schedule these backups at regular intervals.

A comprehensive discussion of groups, group policy, datasets, schedules and retention policies is beyond the scope of this publication. Refer to your *Avamar System Administration Guide* for additional information.

**Task List.** Protecting the vCenter management infrastructure comprises the following tasks, which should be performed in the following order:

- *Task 1: Implement Guest Backups or VMware Image Backups* (page 95)
- *Task 2: Define Custom Dataset for vCenter Backups* (page 96)
- *Task 3: Add a Backup Client for vCenter Database Hosts* (page 97)

### Task 1: Implement Guest Backups or VMware Image Backups

For each vCenter, you must implement the following in order to protect the vCenter management infrastructure:

Install and register Avamar Windows Client software on the vCenter host as described in the *Avamar Backup Clients User Guide*.

Install and register the correct Avamar database software on each database host as described in various database-specific documentation such as the *Avamar SQL Server Client User Guide*.

If the vCenter host is a virtual machine rather than a physical machine, consider protecting it using VMware image backup (page 22).

## Task 2: Define Custom Dataset for vCenter Backups

For best results, you should define a custom dataset strictly for use in backing up the following important vCenter management infrastructure components:

COMPONENT	DEFAULT LOCATION
License files	Exact location varies by VMware and Windows version, but typically one of the following folders: C:\Program Files(x86)\VMware\Infrastructure\VirtualCenter Server\licenses\site C:\Program Files\VMware\VMware License Server\Licenses
SSL certificates	Exact location varies by Windows version, but typically one of the following folders: C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL C:\ProgramData\VMWare\VMware VirtualCenter\SSL
Audit logs	Exact location varies by Windows version, but typically one of the following folders: C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\Logs C:\ProgramData\VMWare\VMware VirtualCenter\Logs
Windows guest customization (sysprep) files	Exact location varies by Windows version, but typically one of the following folders: C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\sysprep C:\ProgramData\VMWare\VMware VirtualCenter\sysprep

This will not only shorten backup and restore times, but will also allow you to use Avamar backups to facilitate vCenter upgrades (for example, upgrading the vCenter host from a 32-bit to a 64-bit Windows virtual machine).

1. Start Avamar Administrator.
2. Select **Tools > Manage Datasets...**  
 The Manage All Datasets window appears.
3. Click **New**.  
 The New Dataset dialog box appears.
4. Type a name for this new dataset (for example, vCenter).

---

**IMPORTANT:** Do not use any of the following characters in your dataset name: ~!@\$%^&(){}[]|,` ;#\/:\*?<>'"&.

---

5. Click the Source Data tab.

The Source Data tab is where you define a list of source data plugins that contribute data to this dataset.

6. Select **Enter Explicitly** and select the Windows File System plugin from the Select Plug-In Type drop-down list.
7. In the list of backup targets at the bottom of the dialog box, successively delete every entry except for the Windows File System plugin by selecting an entry and clicking -.
8. Add each important vCenter management infrastructure component to the dataset as follows:

---

**NOTE:** Refer to the previous table (page 96) for default locations of each important vCenter management infrastructure component.

---

- (a) Select Select Files and/or Folders and click ...

The Select Files And/Or Folders dialog box appears.

- (b) Browse to the correct license file folder and select it.

- (c) Click **OK**.

The Select Files And/Or Folders dialog box closes. The license file folder appears in the list of backup targets at the bottom of the New Dataset dialog box.

- (d) Repeat steps a thru c for the remaining important vCenter management infrastructure components (that is, the SSL certificates, audit logs and windows guest customization (sysprep) files).

9. Click **OK**.

The New Dataset dialog box closes.

### Task 3: Add a Backup Client for vCenter Database Hosts

The location of the database used by vCenter, UpdateManage, SRM, and so forth can be determined by running the Windows Data Sources (ODBC) administrative tool.

Install Avamar database backup agents on the database hosts as described in the database-specific documentation, such as the *Avamar SQL Server Client User Guide*.

Configure a scheduled backup to protect the databases.

You should truncate vCenter database transaction logs after each backup. This can be done by selecting the SQL Server plugin **Truncate database log** option. Truncating database transaction logs ensures that logs will not grow too large and consume excessive amounts of space on the Avamar server.

## Recovering vCenter Management Infrastructure Using Avamar Backups

Recovering vCenter management infrastructure using Avamar backups is a two-step process in which you first create a restore target virtual machine with a fresh operating system image, then restore the vCenter management infrastructure components from the latest Avamar backup. Refer to your *Avamar System Administration Guide* for additional information.

# BEST PRACTICES

---

**ESX Servers Should Use Fully-Qualified Hostnames.** When adding new ESX servers to your vCenter environments, you should adhere to the VMware recommended practice of naming your ESX servers with fully-qualified hostnames (not an IP address or simple hostname). Using anything other than a fully-qualified hostname can result in network connection failures due to incorrect SSL certificate handling.

**Group Guest Backups Should Be Throttled.** When performing scheduled guest backups of several virtual machines that reside on the same ESX server, you should add throttling parameters to the Avamar dataset. The reason for doing this is that Avamar will try to initiate as many backups as possible, subject to certain load restrictions on the Avamar MCS. However, if multiple guest backups are attempted on virtual machines that reside on the same ESX server, this can spike CPU usage, which will have an adverse effect on overall ESX server performance.

To prevent this from occurring, edit the dataset as follows:

1. Start Avamar Administrator.
2. Select **Tools > Manage Datasets...**  
The Manage All Datasets window appears.
3. Select a dataset from the list and click **Edit**.  
The Edit Dataset dialog box appears.
4. Click the Options tab.
5. Click **Show Advanced Options**.
6. Type a non-zero in the Network usage throttle (Mbps) field.  
Begin with a low value such as 20. Then monitor your next backup session to verify that this has resolved any ESX server CPU usage issues.
7. Click **OK**.  
The Edit Dataset dialog box closes.

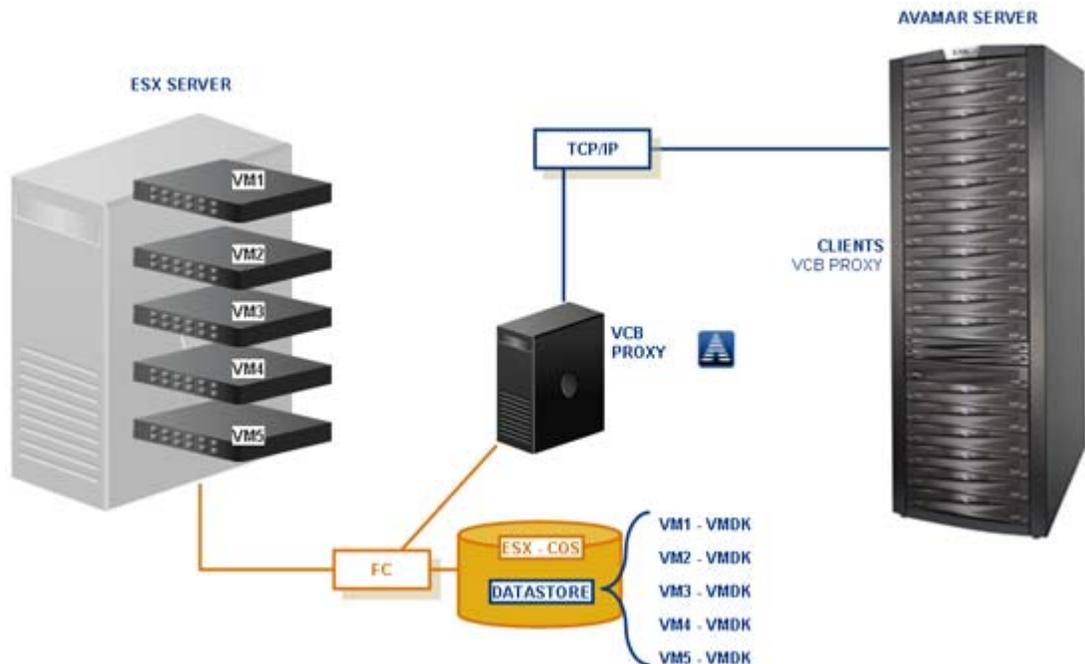
## APPENDIX A — AVAMAR VCB INTEGRATION

This appendix discusses using the Avamar script-based integration with VMware Consolidated Backup (VCB) to protect virtual machine data.

**IMPORTANT:** VMware Consolidated Backup (VCB) does not support ESX Server 4.0. For ESX Server 4.0 environments, see *Avamar VMware Image Backup and Restore* (page 22).

The information in this chapter assumes that VCB has been installed and configured prior to installation and configuration of the Avamar software. Refer to your *Virtual Machine Backup Guide* for additional information about setting up VCB.

Avamar integration with VMware Consolidated Backup (VCB) is achieved through the use of scripts that back up running virtual machines, then mount those virtual machines on a Microsoft Windows 2003 proxy server.



**Avamar-VCB Interoperability Module (AVIM).** These scripts, referred to as the Avamar-VCB Interoperability Module (AVIM), enable full image-level backup of all virtual machine types running on VMware ESX Server version 3.x. They also enable file-level backup of virtual machines running any version of Microsoft Windows that is supported by ESX Server version 3.x.

**How AVIM Works.** AVIM leverages VCB scripts that backup, mount and unmount running virtual machines. To accomplish this, those scripts are called before and after a backup process. Script code assumes the following (otherwise modification to the script is required):

VCB installed in the default location:

C:\program files\VMware\VMware Consolidated Backup\

- Generic scripts located in the generic directory
- VCB backup root directory exists

**SAN Storage Required.** Data must be stored on a VMFS (Virtual Machine Filesystem) in a SAN array. Backup is supported for virtual disks backed by VMFS files or by raw device mappings in logical compatibility mode. Backing up raw devices in physical compatibility mode is not supported.

## Requirements

In order to implement an Avamar VCB integration, you must satisfy the following requirements:

- ESX version 3.0.1 or later
- Fibre Channel SAN storage hosting VMFS or RDMS
- VCB proxy server system running Microsoft Windows Server 2003 Standard Edition SP2
- VCB proxy server connected to the VirtualCenter for VMware Server (or to a single ESX Server system if VirtualCenter is not used)
- Fibre Channel Host Bus Adapter (HBA) on the VCB proxy server
- Proxy access to SAN storage LUNs managed by the ESX Server (done by adding the proxy to the same fabric zones as the ESX Server)
- Virtual machine running
- VMware Tools installed on virtual machine
- Virtual machine network connectivity and FQDN
- Avamar Windows 2003 client installed and configured on the VCB proxy server
- AVIM scripts are installed on the VCB proxy server

## Capabilities and Limitations

This topic discusses the capabilities and limitations of the Avamar VCB integration.

**Capabilities.** Avamar VCB integration offers the following capabilities:

- Supports ESX 3.x servers
- Backup resources are off-loaded to the VCB proxy server
- Supports full-image backups of running virtual machines
- Supports file-level backups of some Windows virtual machines

**Limitations.** Consider the following limitations before implementing Avamar VCB integration:

- Requires high degree of initial setup and configuration
- Requires advanced scripting and VMware knowledge required (working knowledge of COS shell commands and ability to log into COS as root)
- Low data deduplication efficiency
- Individual file and directory (folder) restores not supported
- Unused filesystem space is backed up
- Restores are a multistep process
- iSCSI or NAS/NFS not supported
- VCB can only backup a virtual machine with a disk image stored on a device that the proxy can access
- VCB cannot backup virtual disks that are RDM in physical compatibility mode
- VCB can only backup a virtual machine that has an IP address or DNS name associated with it
- VCB can only perform a file-level backup of a virtual machine running Microsoft Windows NT 4.0, Windows 2000, Windows XP, Windows XP Professional or Windows 2003
- All backups and restores must be initiated using the Avamar Administrator graphical management console; it is not possible to initiate backups and restores directly from the virtual machine

## Installation and Configuration

Installing and configuring an Avamar VCB integration comprises the following tasks:

- *Install Avamar Windows Client on Proxy Server* (page 103)
- *Install AVIM on Proxy Server* (page 103)
- *Create Custom Avamar Dataset* (page 104)

### Install Avamar Windows Client on Proxy Server

Download, install and activate the Avamar Windows Client on according the instructions found in your *Avamar Backup Clients User Guide*.

### Install AVIM on Proxy Server

1. Obtain the AVIM script package from the EMC Powerlink website (powerlink.emc.com).
2. Save the AVIM zip file to a convenient location on your computer or VCB proxy server.
3. Extract the AVIM zip file to the \etc\scripts directory in the Avamar Windows Client install directory.
4. The default Avamar Windows Client install directory is C:\Program Files\avs.

The AVIM zip file contains the following scripts:

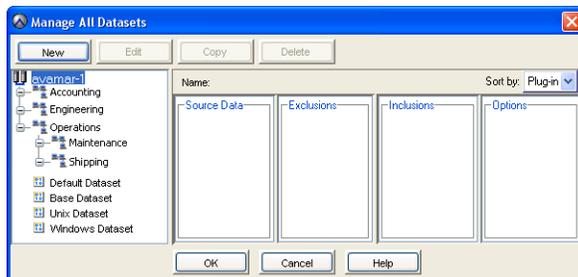
FILE	DESCRIPTION
<code>pre_avamar-fullVM.bat</code>	VMDK (full image-level) mount script.
<code>post_avamar-fullVM.bat</code>	VMDK cleanup script.
<code>pre_avamar-file.bat</code>	File-level mount script.
<code>post_avamar-file.bat</code>	File-level cleanup script.

## Create Custom Avamar Dataset

In order to perform VCB backups to the Avamar server, you must define a separate custom Avamar dataset for each virtual machine. Additionally, the same dataset cannot be used to perform both full VMDK and file-level backups. If you need to perform both backup types, you must create two separate datasets.

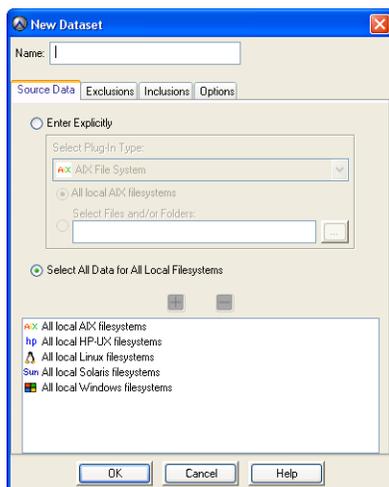
1. Start Avamar Administrator.
2. Select **Tools > Manage Datasets...**

The Manage All Datasets window appears.



3. Click **New**.

The New Dataset dialog box appears.



4. Type a name for this new dataset.

"VCB-fullVM" is used as an example dataset name for the remainder of this procedure.

**IMPORTANT:** Do not use any of the following characters in your dataset name: ~!@\$%^&(){}[]|,` ;#\/: \*?<>'"&.

5. Click the Source Data tab.

The Source Data tab is where you define a list of source data plugins that contribute data to this dataset.

6. Type or select the following:

- (a) Select **Enter Explicitly**.
- (b) Select Windows File System plugin type from the drop-down list.
- (c) Select **Select Files and/or Folders**.
- (d) Click the browse button (...).

The Select Files And/Or Folders dialog box appears.

(e) Browse to the VCB backup root directory configured in the config.js file.

The default VCB backup root directory is c:/mnt.

(f) Select the checkbox next to the VCB backup root directory and click **OK**.

The Select Files And/Or Folders dialog box closes.



7. Switch to New Dataset dialog box and click the **Options** tab.

The Options tab is where you set various plugin options.

8. Add the following three required plugin options to this dataset as follows:

ATTRIBUTE	ATTRIBUTE VALUE
run-at-start	pre_avamar-fullVM.bat VM-NAME -or- pre_avamar-file.bat VM-NAME
run-at-end	post_avamar-fullVM.bat VM-NAME -or- post_avamar-file.bat VM-NAME
cacheprefix	VM-NAME

Where VM-NAME is your actual virtual machine name.

**IMPORTANT:** You cannot mix VMDK and file-level backup scripts in the same dataset.

Use fullVM.bat scripts for VMDK backup. Use file.bat scripts for file-level backup.

(a) Click **More**.

The dialog box expands to include Enter Attribute and Attribute Value fields.

Select Windows File System plugin type from the drop-down list.

(b) Type **run-at-start** in the Enter Attribute field.

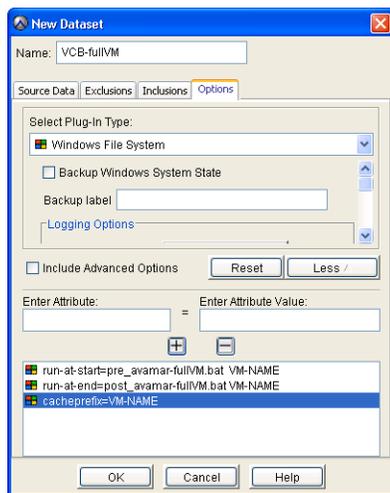
(c) Do one of the following:

IF	DO THIS
Creating this dataset for VMDK backups.	Type <b>pre_avamar-fullVM.bat VM-NAME</b> in the Attribute Value field.
Creating this dataset for file-level backups.	Type <b>pre_avamar-file.bat VM-NAME</b> in the Attribute Value field.

Where VM-NAME is your actual virtual machine name.

(d) Click the add button (+).

(e) Repeat steps b thru d for the remaining two plugin options.



(f) Click **OK**.

The New Dataset dialog box closes.

## Performing VCB Backups

All VCB backups must be initiated from Avamar Administrator. It is not possible to initiate backups from the virtual client because the Avamar Windows Client software is installed on the proxy server.

**On-Demand Backups.** When performing on-demand VCB backups, you must ensure that the custom dataset you created during *Installation and Configuration* (page 103) is the one you use to perform the backup. Otherwise, your backup will fail.

**Scheduled Backups.** Because each virtual machine must have its own dataset, in order to schedule VCB backups, you must create an Avamar group for each virtual machine and assign the correct dataset to that group.

## Restoring a Virtual Machine from VCB Backups

All VCB restores must be initiated from the Avamar Administrator graphical management console. It is not possible to initiate restores from the virtual client because the Avamar Windows Client software is only installed on the proxy server. Refer to your *Avamar System Administration Guide* for additional information.

The exact procedure differs according to whether or not full virtual machine or file-level backups were used.

### Restoring a Virtual Machine from a Full VCB Backup

1. Restore the virtual machine image to the ESX Server.
  - (a) Restore directly to the ESX Server.

---

**IMPORTANT:** This requires that Avamar client software installed on the ESX Server.

---

- (b) Restore to the VCB proxy.
  - (c) Manually copy the virtual machine to the ESX Server.
2. Run the `vcbRestore` command with correct options.

For example:

```
vcbRestore -h ESXSERVER -u USERNAME -p PASSWORD  
-s /vmfs/volumes/path/to/restored/files  
-a /vmfs/volumes/store/path/to/restored/files/catalog
```

## Restoring a Virtual Machine from a File-Level Backup

1. Select files to restore by doing one of the following:
  - (a) Restore the VCB proxy.
  - (b) Perform a redirected restore to another server with an Avamar client

---

**IMPORTANT:** A virtual machine client can restore files backed up by other clients (proxies) only when the user and the virtual machine have the proper permissions.

---

**VCB File-Level Restore Options.** The *Virtual Machine Backup Guide* lists the following options for performing a file-level restore for data backed up from virtual machines using VCB:

- Centralized restore
- Per-group restore
- Per-virtual machine restore

In centralized restore, the backup administrator manually performs the restore procedure, which can be implemented in one of two ways:

Exposing the target directory of the virtual machine as a CIFS share to the backup proxy and using Avamar on the VCB proxy to restore the desired file to this network share.

Copying the files to a shared network drive that both the backup proxy and the virtual machine can access and then copying the restored files from the virtual machine.

In per-group and per-virtual machine restores, the Avamar client software must be installed on some or all virtual machines. When restoring data for a virtual machine, note that respective backups are associated with the VCB proxy and not the virtual machine's DNS name.

## Restoring with the VMware vCenter Converter Standalone tool

An alternate method of performing restores in the VCB environment is using the VMware vCenter: Converter Standalone tool. This tool is particularly useful in the ESXi environment, which does not include support for the COS.

Download the VMware Converter and associated user's manual from the download site on <http://www.vmware.com/download/converter>. The tool must be installed on the proxy server. Make sure you download a version that is compatible with the VCB framework you already have on the proxy machine.

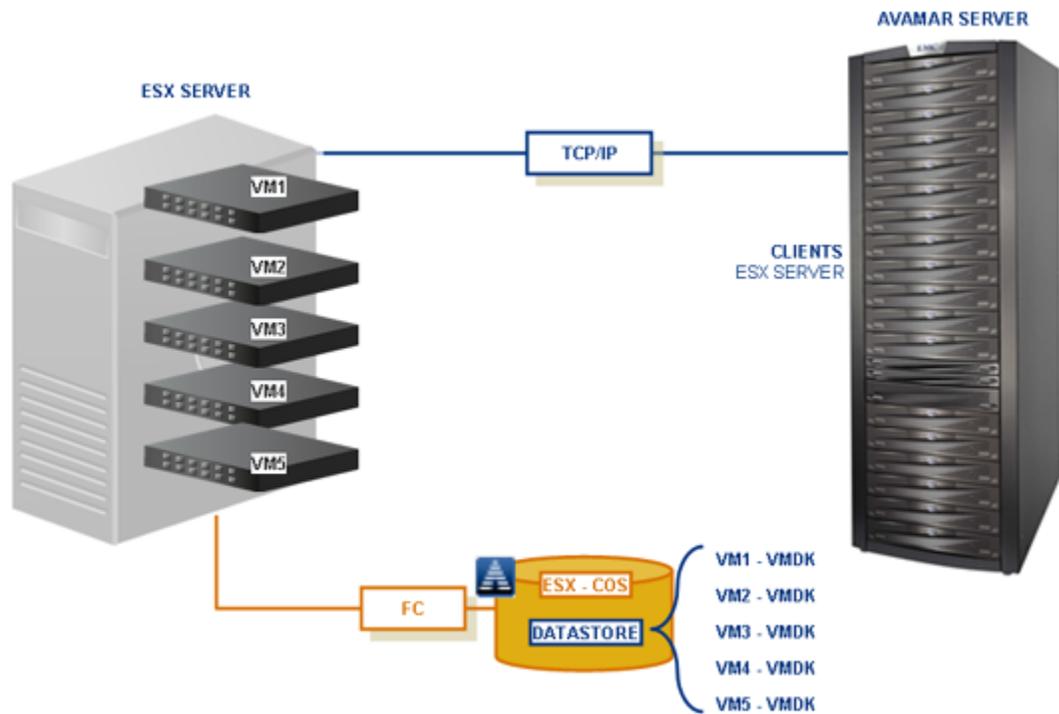
For restores in VCB environments, you must first restore the file or image to the VCB proxy server. After that is completed, use the VMware Converter tool to restore the file or image from the proxy server to the ESX server.

To run the VMware Converter, select **File > New > Import**. The VMware Converter Wizard provides additional information that guides you through the restore process.

# APPENDIX B — ESX SERVER BACKUP AND RESTORE

**IMPORTANT:** VMware officially discourages this data protection method. Refer to *Choosing a Data Protection Method* (page 10) for additional information.

ESX Server backup installs Avamar Linux Client software inside the maintenance Console Operating System (COS). Due to the limited resources of the COS, this method requires advanced configuration to ensure that backups do not impact critical resources needed by running virtual machines.



**Supported ESX Versions.** This procedure is approved for use any of the following ESX versions:

- ESX 2.5.3
- ESX 3.0.x
- ESX 3.5

**How ESX Server Backup Works.** There are two methods for backing up virtual machines from the console:

1. Use `vcbMount` to create a snapshot of a running virtual machine for backup.
2. Suspend or power down a virtual machine and then back it up directly.

## Capabilities and Limitations

**Capabilities.** ESX Server backup implementations offer the following capabilities:

- Virtual machine image-level backups without VMware Image Backup or VCB
- No proxy or SAN required

**Limitations.** If considering an ESX Server backup implementation, you should aware of the following:

- No file-level backup
- Two-step restore
- Requires high degree of initial setup and configuration
- Requires advanced scripting and VMware knowledge required (working knowledge of COS shell commands and ability to log into COS as root)
- Cross-version restores not supported (that is, you can only restore an ESX server backup to exactly the same version ESX server)
- Uses substantial amount of CPU, RAM and disk resources inside the COS, which is only minimally provisioned

If suspending or powering down a virtual machine and backing it up directly:

- Virtual machine must be powered down or suspended before backup begins
- Virtual disk images are not compressed (empty space is processed)

# Installing and Configuring ESX Server Backup and Restore

In order to implement ESX Server backup and restores, you must perform the following tasks:

- *Install the Avamar Linux Client on the ESX Server* (page 111)
- *Configure ESX Server Firewall* (page 111)

## Install the Avamar Linux Client on the ESX Server

- User=root
1. Log into the COS as root.
  2. Download, install and activate the Avamar Linux Client according to the instructions found in your *Avamar Backup Clients User Guide*.

## Configure ESX Server Firewall

You must configure the ESX Server firewall to allow communication with the Avamar server on data ports 7778, 27000, 28001, 28002 and 29000.

- User=root
1. Ensure that you are still logged into the COS as root.
  2. Open the required ports by typing the following:  

```
esxcfg-firewall -o 7778,tcp,in,Avamar
esxcfg-firewall -o 7778,tcp,out,Avamar
esxcfg-firewall -o 27000,tcp,in,Avamar
esxcfg-firewall -o 27000,tcp,out,Avamar
esxcfg-firewall -o 28001,tcp,in,Avamar
esxcfg-firewall -o 28001,tcp,out,Avamar
esxcfg-firewall -o 28002,tcp,in,Avamar
esxcfg-firewall -o 28002,tcp,out,Avamar
esxcfg-firewall -o 29000,tcp,in,Avamar
esxcfg-firewall -o 29000,tcp,out,Avamar
```
  3. Verify all ports have been opened successfully by typing:

```
esxcfg-firewall -q
```

The following information might appear in your command shell:

```
Chain INPUT (policy ACCEPT 318K packets, 39M bytes)
  pkts bytes target prot opt in out source destination
Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 596K packets, 708M bytes)
  pkts bytes target prot opt in out source destination
Neither incoming nor outgoing blocked by default
Enabled services: CIMSLP CIMHttpsServer sshClient vpxHeartbeats AAMClient
LicenseClient sshServer CIMHttpServer
Opened ports:
Avamar: port 7778 tcp.in tcp.out
Avamar: port 27000 tcp.in tcp.out
Avamar: port 28002 tcp.in tcp.out
Avamar: port 28001 tcp.in tcp.out
Avamar: port 29000 tcp.in tcp.out
```

## Performing an ESX Server Backup

Backing up an ESX Server to an Avamar server comprises two tasks:

- *Create Virtual Machine Snapshots* (page 112)
- *Back Up Virtual Machine Snapshots to the Avamar Server* (page 113)
- *Remove Temporary Snapshot Files* (page 113)

### Create Virtual Machine Snapshots

You cannot directly back up a running virtual machine. Instead, you must first use the VMware **vcbMounter** command to take a static snapshot of each running virtual machine. Once these snapshots have been taken, you can use the Avamar Linux Client software to back the snapshots up to the Avamar server.

#### Practical vcbMounter Examples

This topic provides practical examples of the VMware **vcbMounter** command. Fully documenting the VMware **vcbMounter** command is beyond the scope of this publication. Refer to your VMware documentation for comprehensive **vcbMounter** command documentation.

The following example shows how to take a full snapshot of virtual machine MyVM.example.com, which resides on ESX/VC host MyESX.example.com, then save that snapshot across a SAN as d:\backups\MyVM-Files:

```
vcbMounter -h MyESX.example.com -u USER -p PASSWORD  
-a ipaddr:MyVM.example.com -r d:\backups\MyVM-Files -t fullvm  
-m san
```

Where USER and PASSWORD are actual VMware user account and password with the required privileges to perform this action, respectively.

---

**IMPORTANT:** Space limitations cause the previous command to continue (wrap) to more than one line. Your commands must be entered on a single command line (no line feeds or returns allowed).

---

Full virtual machine backups export an entire virtual machine to a set of files in a directory. Backing up this fileset provides the basis for restoring an entire virtual machine at a future date and time.

The following example performs the same operation as the previous example except it also performs a file-level mount and assumes the virtual machine's disk files are located on a datastore that is a NAS share mounted on the proxy as described in the datastores.lst datastore catalog:

```
vcbMounter -h MyESX.example.com -u USER -p PASSWORD  
-a ipaddr:MyVM.example.com -r d:\backup\MyVM-Files -t file  
-m nas -C datastores.lst
```

File-level mounts provide access to the data in a virtual machine disk images.

The following example performs an automatic un-mount of the export created in the previous example.

```
vcbMounter -h MyESX.example.com -u USER -p PASSWORD  
-U d:\backups\MyVM-Files
```

## Procedure

User=root

1. Log into the COS as root.
2. Back up a running virtual machine by typing:

```
vcbMounter -h VIRTUALCENTER -u USER -p PASSWORD  

-a name:_NAME -r /vmfs/volumes/BACKUPLOCATION  

-t fullvm -m cos
```

Where VIRTUALCENTER, USER, PASSWORD and /vmfs/volumes/BACKUPLOCATION are your actual ESX Server hostname, VMware user account, VMware password and location for the temporary snapshot files, respectively.

The following information might appear in your command shell:

```
[2007-06-11 10:42:50.593 'App' 3076464768 info] Current working directory:  

/vmfs/volumes/464118c4-6da711e1-3dac-001422210ad5  

[2007-06-11 10:42:50.630 'BaseLibs' 11271088 warning] [Vmdb_Unset] Unsetting  

unknown path: /vmomi/  

Copying "[storage1] longnamevm1.example.com/longnamevm1.example.com.vmx":  

 0%=====50%=====100%  

*****  

Copying "[storage1] longnamevm1.example.com/longnamevm1.example.com.nvram":  

 0%=====50%=====100%  

*****  

Copying "[storage1] longnamevm1.example.com/VMware.log":  

 0%=====50%=====100%  

*****  

Converting "/vmfs/volumes/store3/Mount-Long/  

scsi0-0-0-longnamevm1.example.com.vmdk" (compact file):  

 0%=====50%=====100%  

*****
```

## Back Up Virtual Machine Snapshots to the Avamar Server

Once the virtual machine snapshots have been created (page 112), you can use the Avamar Linux Client to back the snapshots up to the Avamar server just as you would any other Linux filesystem directory.

---

**IMPORTANT:** When creating an Avamar dataset that will be used to backup virtual machine snapshots, always explicitly exclude the /vmfs/devices directory.

---

## Remove Temporary Snapshot Files

Once you have successfully backed up the VMware snapshot files to the Avamar server, you should delete the snapshot files in order to free up disk space on the ESX Server.

User=root

1. Ensure that you are still logged into the COS as root.
2. Remove the temporary snapshot files from the backup location.  
/vmfs/volumes/BACKUPLOCATION was used as an example back up location in previous tasks.

## Performing a Restore Using ESX Server Backups

In order to restore virtual machines, you must first restore the entire snapshot files set stored on the Avamar server to a temporary location, then use the VMware **vcbRestore** command to restore that snapshot files set to the virtual machine to the ESX Server.

Fully documenting the VMware **vcbRestore** command is beyond the scope of this publication. Refer to your VMware documentation for comprehensive **vcbRestore** documentation.

1. Restore the virtual machine snapshot files from the Avamar server to a location on the ESX Server.

User=root

2. Log into the COS as root.
3. Restore a virtual machine to the ESX Server by typing:

```
vcbRestore -h VIRTUALCENTER -u USER -p PASSWORD  
-s /vmfs/volumes/storage/LOCATION_OF_VM -m cos
```

Where VIRTUALCENTER, USER, PASSWORD and **/vmfs/volumes/storage/LOCATION\_OF\_VM** are your actual ESX Server hostname, VMware user account, VMware password and location of the temporary snapshot files, respectively.

The following information might appear in your command shell:

```
[2007-08-23 13:06:26.296 'App' 3076464768 info] Current working directory:/root  
[2007-08-23 13:06:26.323 'BaseLibs' 6593456 warning] [Vmdb_Unset] Unsetting  
unknown path: /vmomi/  
Converting "/vmfs/volumes/storage1/winvm1/winvm1.vmdk" (VMFS (flat)):  
  
0%=====50%=====100%  
  
*****
```

4. When the virtual machine has been successfully restored, remove the temporary snapshot files from the backup location.



# INDEX

---

## Symbols

.iso files 86, 87, 88, 89  
.log files 113  
.ova files 31, 33

## A

activation  
  client with Avamar server 56  
  image proxy client with Avamar server 55  
  proxy client, with Avamar server 90  
Activity monitor 76, 82  
adding  
  backup client for vCenter database hosts 97  
  image proxy appliance in vCenter 32  
  image proxy client 51, 55  
  vCenter client 49  
  virtual machine clients 51, 56, 59  
admin user account 46, 52, 84  
All Virtual Disks toolbar button 68, 91  
appliance, VMware 23, 24, 26, 27, 29, 31, 32, 37  
  downloading template file 31  
  files 31, 33  
authentication certificate 44  
Avamar Administrator  
  Activity monitor 76, 82  
  All Virtual Disks toolbar button 68, 91  
  Browse Virtual Disks toolbar button 68, 91  
  client icons 54  
  Default Group 47, 49, 75  
  Default Proxy Group 55, 75  
  Default Virtual Machine Group 49, 56, 75, 77, 78, 79  
  encryption setting, client socket 67, 93  
  installing 48  
  naming  
    image backup proxy 34  
    new virtual machine client 73

  REPLICATE domain 54, 63  
  Restore Options dialog box 68, 69, 70, 71, 72, 73, 74, 91, 93  
  vCenter Connection Monitor 64  
  vCenter groups 75, 76, 77, 78, 79  
  virtual machine and proxy client relationships 76  
Avamar File System (AvFS) 83  
Avamar image plugin ISO 86, 87  
Avamar server 44, 46, 52, 84, 111, 113, 114  
  MCS 29, 44, 45, 46, 50, 52, 80, 83, 84, 99  
  multi-node 44, 46, 52, 84  
  read-only state 82  
  single-node 44, 52, 84  
  utility node 44, 46, 52, 84  
Avamar VCB integration 9  
  capabilities 102  
  configuring 103  
  file-level restores using 108  
  installing 103  
  limitations 102  
  requirements 101  
Avamar Virtual Edition (AVE) 27  
Avamar-VCB Interoperability Module (AVIM) 101, 103  
avtar program 20

## B

backing up  
  vCenter management infrastructure 95  
  virtual machine snapshots to Avamar server 113  
backups  
  errors 80  
  monitoring 67  
  on-demand guest 20  
  on-demand VCB 107

scheduled VCB 107  
 statistics 67  
 validation 67  
 Browse Virtual Disks toolbar button 68, 91

## C

cacheprefix 105  
 capabilities  
   Avamar VCB integration 102  
   ESX server backup and restore 110  
   guest backup 18  
   VMware image backup 23  
   Windows file-level restore 81  
 certificate, authentication 44  
 changed block tracking 12, 26, 57, 58, 60, 61, 79  
 changing  
   *See Also* modifying  
   Default Virtual Machine Group 77  
   existing VMware clients 61  
   image proxy client settings 43  
 CIFS filesystems 83, 108  
 client  
   activation with Avamar server 56  
   image proxy 12, 13, 23, 24, 25, 26, 27, 29, 31, 32, 34, 37, 39, 40, 42, 43, 47, 51, 54, 55, 56, 57, 60, 61, 62, 65, 67, 68, 75, 76, 78, 80, 81, 82, 83, 85, 87, 88, 90, 100, 101, 102, 103, 107, 108, 110, 112  
   plugin 57, 60, 79, 81, 86, 87, 93, 97, 105, 106  
   registration with Avamar server 43  
   vCenter 49, 50  
   virtual machine 54, 56, 65, 76, 88, 108  
   Windows file-level restore proxy 85  
 client-initiated  
   command line restores 20  
   on-demand backups 20  
   web services restores 20  
 config.js file 105  
 configuring  
   appliance network settings in vCenter 37  
   Avamar environment 47  
   Avamar File System (AvFS) 83  
   Avamar VCB integration 103  
   ESX server backup and restore 111  
   ESX server firewall 111  
   guest backup 19  
   vCenter environment 29  
   vCenter-to-Avamar authentication 44  
   Windows file-level restore 83  
 Console Operating System (COS), ESX server 11, 14, 102, 108, 109, 110, 111, 113, 114  
 creating  
   *See Also* adding  
   Avamar dataset, for VCB backups 104  
   virtual machine snapshots 112

## D

data deduplication 12, 15, 18, 23, 25, 26, 102  
 data port 50, 80, 111, 115  
 datasets 79, 94, 95, 96, 97, 99, 104, 105, 106, 107, 113  
 datastore, VMware 14, 24, 25, 26, 36, 47, 76, 80, 86, 112  
 default gateway 39  
 Default Group 47, 49, 75  
 Default Proxy Group 55, 75  
 Default Virtual Machine Group 49, 56, 75, 77, 78, 79  
 DHCP 39  
 DNS 25, 30, 31, 32, 34, 40, 42, 43, 48, 84, 86, 87, 90, 102, 108  
 dpnctl program 44, 45, 46, 52, 84

## E

EMC Powerlink website 103  
 encryption setting, client socket 67, 93  
 errors  
   “Backup Does Not Start” 80  
   adding vCenter server as Avamar client 80  
 ESX server 9, 10, 11, 12, 13, 14, 18, 22, 23, 24, 25, 26, 27, 35, 47, 57, 60, 74, 86, 90, 99, 100, 101, 102, 107, 108, 109, 110, 111, 112, 113, 114  
   backup and restore 9, 10, 11, 12, 13, 14, 109, 110, 111, 112, 113  
   COS 11, 14, 102, 108, 109, 110, 111, 113, 114  
   fully-qualified hostnames, importance of 99  
   restores using ESX server backups 114  
   VCB restore user account 107  
   version 10

## F

fibre channel 27, 101  
 files  
   .iso 86, 87, 88, 89  
   .log 113  
   .ova 31, 33  
   config.js 105  
   log 11, 13, 14, 15, 18, 25, 31, 32, 44, 46, 48, 52, 80, 84, 85, 86, 87, 88, 97, 102, 110, 111, 113, 114  
   mcsrvr.xml 46, 52, 79, 84  
 firewalls 25, 111  
 flat virtual disks 26

## G

groups  
   Default Group 47, 49, 75  
   Default Proxy Group 55, 75  
   Default Virtual Machine Group 49, 56, 75, 77, 78, 79

guest backups 9, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 23, 24, 27, 52, 54, 58, 60, 62, 94, 95, 99  
 capabilities 18  
 configuring 19  
 full system restores 21  
 installing 19  
 limitations 18

**I**

IDE virtual disks 25  
 image backup 9, 10, 11, 12, 13, 14, 15, 22, 23, 24, 25, 26, 27, 28, 29, 31, 32, 34, 37, 40, 42, 43, 44, 47, 52, 53, 58, 60, 62, 65, 68, 69, 75, 79, 80, 81, 85, 87, 89, 91, 94, 95, 110  
 image proxy client 12, 13, 23, 24, 25, 26, 27, 29, 31, 32, 34, 37, 39, 40, 42, 43, 47, 51, 54, 55, 56, 57, 60, 61, 62, 65, 67, 68, 75, 76, 78, 80, 81, 82, 83, 85, 87, 88, 90, 100, 101, 102, 103, 107, 108, 110, 112  
 image restore 21, 68, 91  
 installing  
   authentication certificate on MCS 44  
   Avamar Administrator 48  
   Avamar Linux Client on the ESX Server 111  
   Avamar VCB integration 103  
   Avamar windows client on proxy server 103  
   AVIM on proxy server 103  
   ESX server backup and restore 111  
   guest backup 19  
   guest backup Avamar client software 21  
   guest backup operating system 21  
   Microsoft .NET Framework 85  
   VIX API 86  
   vSphere client 30  
 IP address 30, 31, 32, 39, 40, 42, 48, 50, 55, 84, 86, 87, 99, 102  
   static 39  
 iSCSI 102  
 ISO images 86, 87, 88, 89

**J**

Java  
   keytool program 44, 45  
   runtime environment 44

**K**

keytool program 44, 45

**L**

limitations  
   Avamar VCB integration 102  
   ESX server backup and restore 110  
   guest backup 18  
   image backup 25  
   Windows file-level restore 82

log files 11, 13, 14, 15, 18, 25, 31, 32, 44, 46, 48, 52, 80, 84, 85, 86, 87, 88, 97, 102, 110, 111, 113, 114  
 LUNs 24, 27

**M**

management console  
   *See* Avamar Administrator  
 Management Console Server (MCS), Avamar 29, 44, 45, 46, 50, 52, 80, 83, 84, 99  
   restarting 45, 46, 84  
   stopping 44, 46, 84  
   turning off certificate authentication 46  
 mcserver.xml file 46, 52, 84  
 Microsoft .NET Framework 83, 85  
 modifying  
   Default Virtual Machine Group 77  
   existing VMware clients 61  
   image proxy client settings 43  
 multi-node Avamar server 44, 46, 52, 84

**N**

NAS storage 102, 112  
 netmask 39  
 networks/networking  
   CIFS 83, 108  
   default gateway 39  
   DHCP 39  
   DNS 25, 30, 31, 32, 34, 40, 42, 43, 48, 84, 86, 87, 90, 102, 108  
   fibre channel 27, 101  
   firewalls 25, 111  
   IP address 30, 31, 32, 39, 40, 42, 48, 50, 55, 84, 86, 87, 99, 102  
   iSCSI 102  
   netmask 39  
   NFS 102  
   Samba 83, 84  
   SCSI 27  
   SSL 25, 44, 45, 94, 96, 97, 99  
   static IP address 39  
   WAN 24  
 new bytes calculation  
   physical disk 15  
   virtual disk 15  
 NFS filesystems 102

**O**

on-demand  
   guest backup 20  
   VCB backup 107  
   VMware image backup 65

**P**

physical disk new bytes calculation 15

plugins, Avamar client 57, 60, 79, 81, 86, 87, 93, 97, 105, 106

port, data 50, 80, 111, 115

post\_avamar-file.bat program 103, 105  
*See Also* Avamar-VCB Interoperability Module (AVIM)

post\_avamar-fullVM.bat program 103, 105  
*See Also* Avamar-VCB Interoperability Module (AVIM)

Powerlink website 103

pre\_avamar-file.bat program 103, 105, 106  
*See Also* Avamar-VCB Interoperability Module (AVIM)

pre\_avamar-fullVM.bat program 103, 105, 106  
*See Also* Avamar-VCB Interoperability Module (AVIM)

programs  
 AVIM 101, 103  
 avtar 20  
 dpnctl 44, 45, 46, 52, 84  
 keytool 44, 45  
 post\_avamar-file.bat 103, 105  
 post\_avamar-fullVM.bat 103, 105  
 pre\_avamar-file.bat 103, 105, 106  
 pre\_avamar-fullVM.bat 103, 105, 106  
 vcbMounter 112  
 vcbRestore 107, 114

**R**

RDM virtual disks 26, 102

read-only server state 82

recovering vCenter management infrastructure using Avamar backups 98

registration  
 client, with Avamar server 43  
 proxy client, with Avamar server 90

REPLICATE domain 54, 63

requirements  
 Avamar VCB integration 101  
 VMware image backup 23  
 VMware knowledge 14  
 Windows file-level restore virtual machine 85

restarting  
 MCS 45, 46, 84

restore  
 file-level 68, 91

Restore Options dialog box 68, 69, 70, 71, 72, 73, 74, 91, 93

restores  
 command line 20  
 file-level 68, 91  
 monitoring 67

restoring  
 all virtual disks 68, 69, 70, 72, 91  
 folders or files from image backup 91

from guest backups 20

full system, from guest backups 21

unique data from guest backups 21

using web services 20

VCB environment with VMware vCenter Converter Standalone tool 108

virtual machine  
 from a full VCB backup 107  
 from file-level backup 108  
 to a different (existing) virtual machine 70  
 to a new virtual machine 72  
 to the original virtual machine 69

retention policies 25, 46, 66, 75, 95

root user account 44, 111, 113, 114

**S**

Samba  
 user account 83

Samba filesystems 83, 84

SAN storage 23, 24, 25, 26, 27, 101, 110, 112

schedules 95, 107

SCSI interfaces 27

security 21, 31, 44, 48, 83, 85, 86  
 authentication certificate 44  
 SSL 25, 44, 45, 94, 96, 97, 99

single-node Avamar server 44, 52, 84

sparse virtual disks 26

SSL 25, 44, 45, 94, 96, 97, 99

static IP address 39

stopping  
 MCS 44, 46, 84

storage  
 LUNs 24, 27  
 NAS 102, 112  
 SAN 23, 24, 25, 26, 27, 101, 110, 112

**T**

task list  
 Avamar configuration and setup for image backup and restore 47  
 vCenter configuration and setup for image backup and restore 29  
 for vCenter management infrastructure backup using Avamar 95  
 Windows file-level restore configuration and setup 83

templates  
 virtual machine 21, 24, 27, 31, 33, 34, 35, 36, 57, 58, 60, 68

**U**

user accounts 30  
 Avamar server admin 46, 52, 84

Avamar server root 44, 111, 113, 114  
 ESX server VCB restore 107  
 Samba 83  
 vCenter login 32, 50, 80, 87  
 utility node 44, 46, 52, 84  
 utilize\_changed\_block\_list setting 79

## V

VCB-HELPER 27  
 vcbMounter program 112  
 vcbRestore program 107, 114  
 vCenter 9, 11, 14, 22, 23, 24, 25, 26, 27, 28, 29, 30, 32, 34, 37, 39, 43, 44, 45, 46, 47, 49, 50, 54, 55, 56, 57, 58, 59, 60, 61, 62, 64, 70, 74, 75, 76, 77, 78, 79, 80, 87, 90, 94, 95, 96, 97, 98, 99, 108  
   configuring for image backup and restore 29  
 Connection Monitor 64  
 Converter Standalone tool 108  
 groups, in Avamar Administrator 75, 76, 77, 78, 79  
 login 30  
 login user account 32, 50, 80, 87  
 management infrastructure backup using Avamar 95  
 server 9, 22, 30, 32, 37, 39, 47, 54, 80, 87  
 virtual disks  
   flat 26  
   IDE 25  
   new bytes calculation 15  
   RDM 26, 102  
 virtual machine  
   Avamar client 54, 56, 65, 76, 88, 108  
   naming as Avamar client 73  
   relationship with proxy clients in Avamar Administrator 76  
   template 21, 24, 27, 31, 33, 34, 35, 36, 57, 58, 60, 68  
   viewing protected in Avamar Administrator 62  
   viewing replicated client name in Avamar Administrator 63  
 virtual machines 71  
 VIX API 83, 86  
 VMware  
   appliance 23, 24, 26, 27, 29, 31, 32, 37  
   appliance files 31, 33  
   datastore 14, 24, 25, 26, 36, 47, 76, 80, 86, 112  
   image backups 9, 10, 11, 12, 13, 14, 15, 22, 23, 24, 25, 26, 27, 28, 29, 31, 32, 34, 37, 40, 42, 43, 44, 47, 52, 53, 58, 60, 62, 65, 68, 69, 75, 79, 80, 81, 85, 87, 89, 91, 94, 95, 110  
   knowledge, required 14  
   VADP 9, 22  
   VCB-HELPER 27  
   vCenter Converter Standalone tool 108

VIX API 83, 86  
 VMware Consolidated Backup (VCB) 9, 10, 11, 12, 13, 14, 27, 100, 101, 102, 103, 104, 105, 107, 108, 110  
 VMware Image Dataset 79  
 VMware Tools 23, 82, 85, 101  
 VMware vStorage API for Data Protection (VADP) 9, 22  
 vSphere 29, 30, 32, 37, 58, 60, 80, 87, 88, 94, 115  
   client 29, 30, 32, 37, 80, 87

## W

WAN 24  
 Windows file-level restore 27, 28, 81, 82, 83, 85, 87, 90, 91  
   capabilities 81  
   configuration and setup 83  
   configuring 83  
   installing proxy client ISO file 88  
   proxy client 85  
   virtual machine requirements 85  
 Windows file-level restores  
   limitations 82