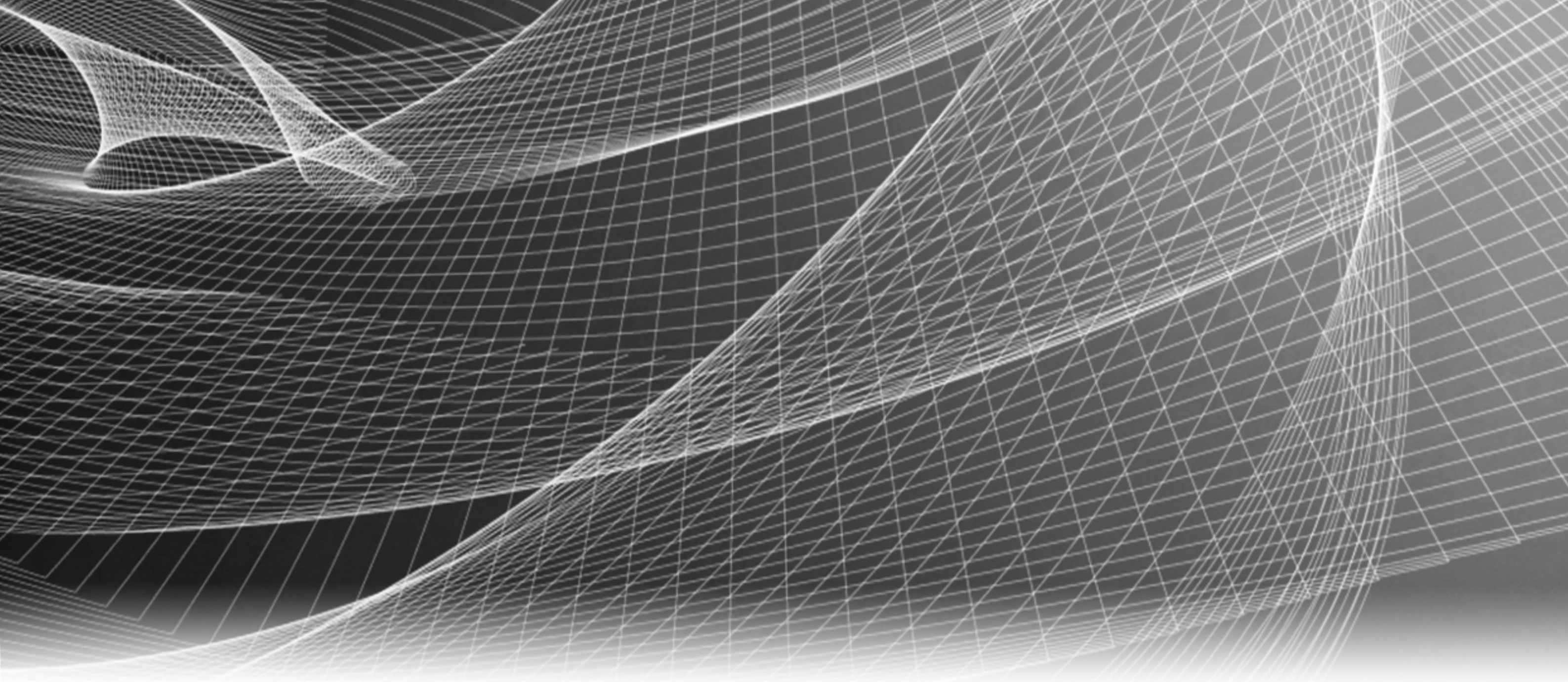


EMC® Avamar® 7.0 for VMware

User Guide

P/N 300-015-230
REV 07

Published January, 2015

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the technical documentation and advisories section on the EMC online support website.

CONTENTS

Preface

Chapter 1 Introduction

Chapter 2 Configuration and Setup

Chapter 3 Administration

Appendix B Plug-in Options

Index

TABLES

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

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

Audience

The information in this publication is intended for system administrators familiar with:

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

A comprehensive discussion of 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. The *EMC Avamar Administration Guide* provides details.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history (page 1 of 2)

Revision	Date	Description
07	January 15, 2015	• Added "(Optional) Configuring proxy certificate authentication" on page 40 • Revised "(Optional) Performing proxy performance optimization" on page 42
06	August 12, 2014	• Revised "Clients and containers" on page 50 • Revised "Limitations" on page 70 • Revised "Limitations" on page 77
05	July 17, 2014	• Revised "Performing optional proxy plug-in configuration" on page 44 with new socket and core recommendations. • Revised "File-level restore limitations" on page 78 to explain that progress bytes are not shown in the Activity Monitor. • Revised "Listen ports" on page 104.

Table 1 Revision history (page 2 of 2)

Revision	Date	Description
04	May 2, 2014	• Revised "Changed block tracking" on page 20 to clarify which specific virtual machine actions will enable CBT. • Revised "Creating a dedicated vCenter user account" on page 29 to include vCenter 5.5 and 5.5U1 permissions. • Revised "Adding clients and containers" on page 52 to clarify which specific virtual machine actions will enable CBT. • Added "vApp backups fail if any subvirtual machine fails to backup" on page 70. • Added "Changed block tracking does not take effect" on page 95 to provide assistance when virtual machines are not stunned after enabling CBT.
03	November 8, 2013	• Revised "Minimum required vCenter user account privileges" on page 29 by adding vApp › Import and DeviceConnection and Host › Configuration › Storage partition configuration privileges. • Added "Performing optional proxy plug-in configuration" on page 44. • Revised "Plug-in Options" on page 105 because some plug-in option labels changed.
02	August 31, 2013	• Revised "(Optional) Performing proxy performance optimization" on page 42. • Revised "File-level restore limitations" on page 78 to support LVM.
01	July 10, 2013	First release of Avamar 7.0.

Related documentation

The following EMC publications provide additional information:

- *EMC Avamar Compatibility and Interoperability Matrix*
- *EMC Avamar Release Notes*
- *EMC Avamar Administration Guide*
- *EMC Avamar Operational Best Practices*
- *EMC Avamar Product Security Guide*
- *EMC Avamar Backup Clients User Guide*
- *EMC Avamar for Exchange Guide*
- *EMC Avamar for IBM DB2 User Guide*
- *EMC Avamar for Lotus Domino User Guide*
- *EMC Avamar for Microsoft SharePoint Guide*
- *EMC Avamar for Oracle User Guide*
- *EMC Avamar for SQL Server User Guide*

Conventions used in this document

EMC uses the following conventions for special notices:

NOTICE

NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

IMPORTANT

An important notice contains information essential to software or hardware operation.

Typographical conventions

EMC uses the following type style conventions in this document:

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: • System output, such as an error message or script • System code • Pathnames, filenames, prompts, and syntax • Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

The Avamar support page provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may enable you to resolve a product issue before you contact EMC Customer Support.

To access the Avamar support page:

1. Go to https://support.EMC.com/products.
2. Type a product name in the **Find a Product** box.
3. Select the product from the list that appears.
4. Click the arrow next to the **Find a Product** box.
5. (Optional) Add the product to the **My Products** list by clicking **Add to my products** in the top right corner of the **Support by Product** page.

Documentation

The Avamar product documentation provides a comprehensive set of feature overview, operational task, and technical reference information. Review the following documents in addition to product administration and user guides:

- Release notes provide an overview of new features and known limitations for a release.
- Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.
- White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

The EMC Knowledgebase contains applicable solutions that you can search for either by solution number (for example, esgxxxxxx) or by keyword.

To search the EMC Knowledgebase:

1. Click the **Search** link at the top of the page.
2. Type either the solution number or keywords in the search box.
3. (Optional) Limit the search to specific products by typing a product name in the **Scope by product** box and then selecting the product from the list that appears.
4. Select **Knowledgebase** from the **Scope by resource** list.
5. (Optional) Specify advanced options by clicking **Advanced options** and specifying values in the available fields.
6. Click the search button.

Online communities

Visit EMC Community Network at https://community.EMC.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners and certified professionals for all EMC products.

Live chat

To engage EMC Customer Support by using live interactive chat, click Join Live Chat on the Service Center panel of the Avamar support page.

Service Requests

For in-depth help from EMC Customer Support, submit a service request by clicking Create Service Requests on the Service Center panel of the Avamar support page.

Note: To open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

To review an open service request, click the Service Center link on the Service Center panel, and then click View and manage service requests.

Facilitating support

EMC recommends that you enable ConnectEMC and Email Home on all Avamar systems:

- ConnectEMC automatically generates service requests for high priority events.
- Email Home emails configuration, capacity, and general system information to EMC Customer Support.

Your comments

Your suggestions help us to continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

BSGDocumentation@emc.com

Please include the following information:

- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Other details that will help us address the documentation issue

CHAPTER 1
Introduction

This chapter discusses the following:

Avamar for VMware image backup and restore

The following topics introduce and describe Avamar for VMware image backup and restore.

Overview

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

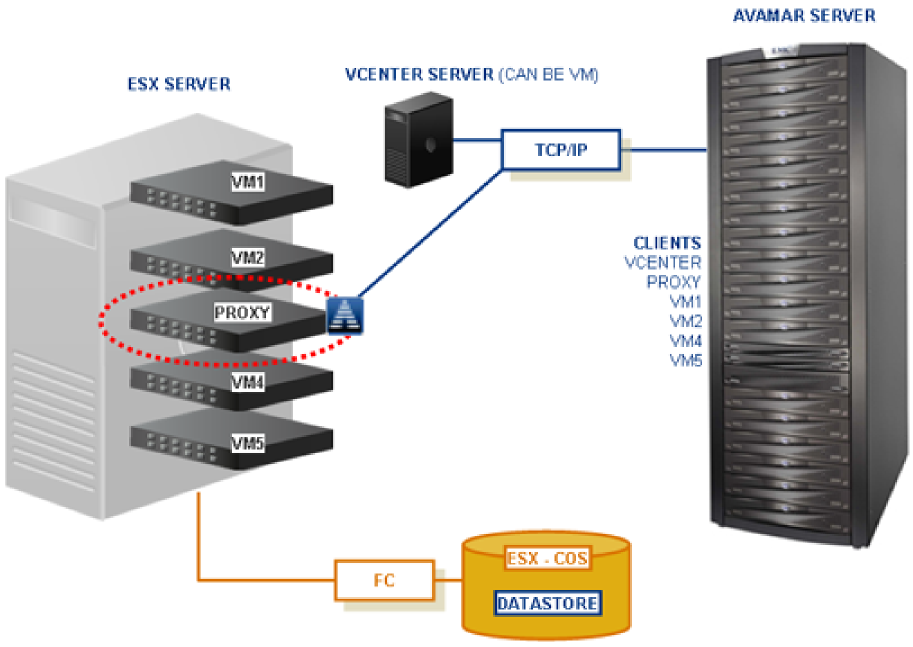


Figure 1 Avamar for VMware image backup and restore diagram

Backups and restores require the use of proxy virtual machine clients. Each proxy virtual machine client provides all of the following capabilities:

- Backup of Microsoft Windows and Linux virtual machines (entire images or specific drives)
- Restore of Microsoft Windows and Linux virtual machines (entire images or specific drives)
- Selective restore of individual folders and files to Microsoft Windows and Linux virtual machines

Proxies run Avamar software inside a Linux virtual machine, and are deployed using an appliance template (.ova) file.

Supported configurations

- The following storage architectures are fully supported:
  - Fiber channel SAN storage hosting VMFS or RDMS
  - iSCSI SAN storage
  - NFS
- 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)

Guest backup and restore

Guest backup and restore is another way to protect virtual machine data. It 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.

NOTICE

When registering virtual machine clients protected by guest backup, do not register them to a vCenter domain. Doing so will prevent you from locating or managing that virtual machine in Avamar Administrator. Instead register any virtual machine clients protected by guest backup to some other domain or subdomain (for example, /clients).

The following Avamar client guides provide details about installing Avamar client software in virtual machines:

Table 2 Avamar client guides (page 1 of 2)

Client	Publication
IBM AIX file systems	*EMC Avamar Backup Clients User Guide*
Linux file systems: • CentOS • Debian • Red Hat • SUSE • Ubuntu	*EMC Avamar Backup Clients User Guide*
Novell NetWare file systems	*EMC Avamar Backup Clients User Guide*

Table 2 Avamar client guides (page 2 of 2)

Client	Publication
UNIX file systems: • FreeBSD • HP-UX • SCO Open Server and UnixWare • Sun Solaris	*EMC Avamar Backup Clients User Guide*
IBM DB2 databases hosted on IBM AIX, Red Hat and SUSE Linux, and Microsoft Windows	*EMC Avamar for IBM DB2 User Guide*
Lotus Domino databases	*EMC Avamar for Lotus Domino User Guide*
Mac OS X file systems	*EMC Avamar Backup Clients User Guide*
Microsoft Exchange databases	*EMC Avamar for Exchange Guide*
Microsoft Office SharePoint implementations	*EMC Avamar for Microsoft SharePoint Guide*
Microsoft SQL Server databases	*EMC Avamar for SQL Server User Guide*
Microsoft Windows file systems	*EMC Avamar Backup Clients User Guide*
Oracle databases hosted on IBM AIX, Red Hat, and SUSE Linux, Sun Solaris, and Microsoft Windows	*EMC Avamar for Oracle User Guide*

Choosing a data protection method

This topic explores the various advantages and considerations associated with image backup and restore versus guest backup and restore.

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

Types of virtual machines

Guest backup is generally the preferred strategy for protecting application servers such as Microsoft Exchange, Microsoft Office SharePoint, Microsoft SQL Server, and Oracle. The reason that guest backup is particularly suited for this is that the Avamar agent gracefully quiesces applications prior to backup, ensuring a true “application consistent” backup.

Guest backup and restore is also the only way to back up virtual machines, such as desktops and laptops, that are not hosted within a vCenter.

Avamar for VMware image backup and restore is generally the preferred strategy for protecting any nonapplication intensive virtual machines that are hosted within a vCenter. Avamar's integration with vCenter enables multiple virtual machines to be protected with the least amount of effort.

Ease of implementation

Guest backup and restore:

- 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
- Avamar client software must be individually installed, and managed inside each virtual machine

Avamar for VMware image backup and restore:

- Can leverage vCenter to discover virtual machines, and add them to the Avamar server in batches
- Requires moderate amount of initial setup and configuration

Efficiency

Guest backup and restore:

- Offers highest level of data deduplication efficiency
- Backups do not consume ESX Server CPU, RAM, and disk resources
- Backups consume small amounts of guest virtual machine CPU, RAM, and disk resources when backups are occurring

Avamar for VMware Image backup and restore:

- Moderate deduplication efficiency
- Backups do not consume guest virtual machine CPU, RAM, and disk resources
- Backups consume ESX Server CPU, RAM, and disk resources when backups are occurring

Backup and restore

Guest backup and restore:

- Applications are gracefully quiesced before each backup, ensuring a true “application consistent” 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 file system space is not backed up
- Individual folder and file restores are supported
- Backup and restore jobs can execute pre- and postprocessing scripts
- Virtual machines must have a network connection to Avamar server
- Virtual machines must be running for backups to occur

Avamar for VMware Image backup and restore:

- Image backups are supported for all machines that are currently supported by VMware
- Individual folder and file restores supported for both Windows and Linux virtual machines

- Virtual machines need not have a network connection to Avamar server
- Virtual machines need not be running for backups to occur
- Unused file system space is backed up
- Backups not optimized (temp files, swap files, and so forth are included)
- Backups can comprise an entire virtual machine image (all drives) or selected drives (vmdk files)

Required VMware knowledge

Guest backup and restore requires no advanced scripting or VMware knowledge.

Avamar for VMware Image backup and restore requires moderate 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 the ability to log in to vCenter with administrator privileges.

Changed block tracking

Changed block tracking is a VMware feature that tracks which specific file system blocks on a virtual machine have changed between backups.

Changed block tracking identifies unused space on a virtual disk during the initial backup of the virtual machine, and also empty space that has 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.

If changed block tracking is not enabled, each virtual machine file system image must be fully processed for each backup, possibly resulting in unacceptably long backup windows, and excessive back-end storage read/write activity.

Changed block tracking can also reduce the time required to restore (“roll back”) a virtual machine to a recent backup image by automatically eliminating unnecessary writes during the restore process.

Changed block tracking is only available with the following types of virtual machines that use the following specific types of virtual disk formats:

- Virtual machines versions 7 and later

  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 exist in version 4 to allow deployment on ESX 3.x hosts.

  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 details.

- Disks cannot be physical compatibility RDM
- The same disk cannot be mounted by multiple virtual machines

- Virtual machines must be in a configuration that supports snapshots

Enabling changed block tracking will not take effect until any of the following actions occur on the virtual machine: reboot, power on, resume after suspend, or migrate.

Virtual Machine Quiescing

Avamar for VMware image backup and restore does not provide any additional virtual machine quiescing capabilities other than those provided by VMware Data Recovery (VDR).

Prior to performing a backup, three levels of virtual machine quiescing are possible:

- Crash-consistent quiescing
- File system-consistent quiescing
- Application-consistent quiescing

Crash-consistent quiescing is the least desirable level of quiescing because the virtual disk image being backed up is consistent with what would occur by interrupting power to a physical computer. File system writes might or might not be in progress when power is interrupted. Because of that, there is always a chance of some data loss.

File system-consistent quiescing is more desirable because the virtual machine is allowed to complete any file system writes before the disk is backed up. This level of quiescing is only available on Windows virtual machines capable of providing Windows Volume Snapshot Service (VSS) services, and that are running VMware Tools.

Application-consistent quiescing is the most desirable level of quiescing because, in addition to the advantages provided by file system-consistent quiescing, applications are notified that a backup has occurred so that they can clear their transaction logs.

Application-consistent quiescing is only available on Windows 2008 32-bit/64-bit, and Windows 2008 R2 virtual machines that are running VMware Tools. Additionally, for application-consistent quiescing to be available, the following conditions must be met:

- The UUID attribute must be enabled. This is enabled by default on virtual machines created on ESX 4.1 hosts.
- The virtual machine must use only SCSI disks. For example, application-consistent quiescing is not supported for virtual machines with IDE disks.
- The virtual machine cannot use dynamic disks.

A complete discussion of virtual machine quiescing and VDR is beyond the scope of this publication. Refer to your *VMware Data Recovery Administration Guide* for details including specific platform capabilities and limitations.

Additional VMware resources

A comprehensive discussion of VMware technology is beyond the scope of this publication. The following VMware documentation provides additional details:

- *Introduction to VMware vSphere*
- *Getting Started with ESX*

- *vSphere Basic System Administration*
- *vSphere Resource Management Guide*
- *vSphere Web Access Administrator's Guide*
- *ESX and vCenter Server Installation Guide*
- *ESX Configuration Guide*
- *VMware Data Recovery Administration Guide*

CHAPTER 2
Configuration and Setup

This chapter provides essential configuration and setup procedures, for both vCenter and Avamar environments, that must be performed before Avamar for VMware image backup and restore can be used to protect virtual machine data. Topics in this chapter include:

Task road map

Successfully configuring Avamar for VMware image backup and restore comprises the following tasks, which must be performed in this specific order:

- "Enabling support for multiple vCenters" on page 24 (only required if Avamar server was upgraded from a previous version)
- "Downloading and installing vSphere Client software (optional)" on page 25
- "Downloading and installing Avamar Administrator software" on page 26
- For each vCenter, perform the following tasks:
  - "Configuring vCenter-to-Avamar authentication" on page 26, by performing one of the following tasks:
    - "Installing an authentication certificate on the Avamar MCS" on page 27
    - "Turning off certificate authentication for all vCenter-to-Avamar MCS communications" on page 28
  - "Creating a dedicated vCenter user account" on page 29
  - "Adding a vCenter client in Avamar Administrator" on page 31
- "Deploying proxies" on page 32, by performing all of the following tasks:
  - "Adding DNS Entries" on page 33
  - "Downloading the proxy appliance template file" on page 33
  - "Deploying a proxy appliance in vCenter" on page 33, by performing one of the following tasks:
    - "Deploying a proxy appliance in vCenter using the vSphere Web Client" on page 35
    - "Deploying a proxy appliance in vCenter using the vSphere Client" on page 34
  - "Registering and activating a proxy with Avamar server" on page 38
  - "Configuring proxy settings in Avamar Administrator" on page 39

Enabling support for multiple vCenters

Avamar for VMware image backup and restore supports protecting up to 5 vCenters from a single Avamar server. Beginning with Avamar 6.0, support for multiple vCenters is enabled by default during new Avamar server software installations. However, if your Avamar server was upgraded from the previous version, you might need to perform the following manual configuration in order to enable support for multiple vCenters.

To enable support for multiple vCenters, perform the following:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server, log in to the utility node as admin.

2. Change directories by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

3. Open mcserver.xml in a UNIX text editor.
4. Find the com.avamar.mc.vmware.max_number_of_vcenters node, as shown below:

   ```
   <root type="system">
      <node name="com">
          <node name="avamar">
              <node name="mc">
                  <node name="vmware">
                      <entry key="max_number_of_vcenters" value="1" />
   ```

   Note: Substantial portions of mcserver.xml have been omitted for clarity.

5. Change the max_number_of_vcenters entry to 5.
6. Save your changes.
7. Restart the MCS by typing:

   ```
   dpnctl stop mcs
   dpnctl start mcs
   ```

8. Close the command shell.

Downloading and installing vSphere Client software (optional)

This task is only required if you will be using the vSphere Client running on a Windows computer, rather than the vSphere Web Client, which supports multiple computing platforms.

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

1. Open a web browser and type the following URL:

   ```
   https://VSPHERE
   ```

   where VSPHERE is the vSphere server network hostname or IP address.

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

   The vSphere Welcome page appears.

2. Click **Download vSphere Client**.
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.

Downloading and installing Avamar Administrator software

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

1. Open a web browser and type the following URL:

   ```
   http://AVAMARSERVER
   ```

   where AVAMARSERVER is the Avamar server network hostname or IP address.

   The EMC Avamar Web Restore web page appears.

2. Click **Downloads**.
3. Click + next to the **Windows for x86 (32 bit)** folder.
4. Click + next to the **Microsoft Windows XP, Vista, 7, 8, Microsoft Windows Server 2003** folder.
5. Locate the Java Runtime Environment (JRE) install package (it is typically the last entry in the folder).
6. If the JRE on the client computer is older than the JRE hosted on the Avamar server, download and install the newer JRE from the Avamar server as follows:

   a. Click the **jre-**VERSION**-windows-i586-p** install package.

      where VERSION is the JRE version.

   b. Open the installation file, or download the file, and then open it from the saved location.

   c. Follow the onscreen instructions to complete the JRE installation.

7. Click the **AvamarConsoleMultiple-windows-x86-**VERSION**.exe** install package.

   where VERSION is the Avamar Administrator software version.

   Avamar Administrator is only available as a 32-bit application. However, it will also run on 64-bit windows computers.

8. Open the installation file, or download the installation file, and then open it from the saved location.
9. Follow the onscreen instructions to complete the Avamar Administrator software installation.

Configuring vCenter-to-Avamar authentication

Avamar VMware Image Backup will not work unless:

- A valid authentication certificate is present on the Avamar Management Console Server (MCS).
- Certificate authentication for all MCS-to-vCenter communications is turned off.

NOTICE

You must perform this task for each vCenter you intend to protect.

Installing an authentication certificate on the Avamar MCS

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 folder (/usr/java/jreVERSION/bin), where VERSION is the specific Java Runtime Environment (JRE) version currently installed on the MCS. If this folder is not in your path, you can either add it to the path, or specify the complete path when using **keytool**.

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server, log in to the utility node as admin.
2. Stop the MCS by typing:
   ```
   dpnctl stop mcs
   ```
3. Switch user to root by typing:
   ```
   su -
   ```
4. Copy rui.crt from the vCenter machine to /tmp on the utility node or single-node server.

   The default certificate provided with vCenter is:
   - Windows 2008: C:\ProgramData\VMware\VMware VirtualCenter\SSL\rui.crt
   - Other Windows versions: C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\rui.crt
   - Linux: /etc/vmware-vpx/ssl/rui.crt
5. Create a temporary version of the MCS keystore by copying the live keystore to /tmp by typing:
   ```
   cp /usr/local/avamar/lib/rmi_ssl_keystore /tmp/
   ```
6. Add the default vCenter certificate to the temporary MCS keystore file by typing:
   ```
   cd /tmp
   $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, type the keystore password.

   The following appears in the command shell:
   ```
   Trust this certificate?
   ```
8. Type **yes**, and press **Enter**.

9. Back up the live MCS 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 to the live location by typing:

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

11. Exit the root subshell, and restart the MCS by typing:

    ```
    exit
    dpnctl start mcs
    ```

Turning off certificate authentication for all vCenter-to-Avamar MCS communications

If you do not want to Install an authentication certificate on the Avamar MCS, as described in "Installing an authentication certificate on the Avamar MCS" on page 27, turn off certificate authentication for all vCenter-to-Avamar MCS communications by performing the following:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server, log in to the utility node as admin.
2. Stop the MCS by typing:

   ```
   dpnctl stop mcs
   ```

3. Open /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml in a UNIX text editor.
4. Locate the ignore_vc_cert preference.
5. Change the ignore_vc_cert preference setting to true.

   For example:

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

6. Save your changes.
7. Restart the MCS by typing:

   ```
   dpnctl start mcs
   ```

Creating a 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 actions are actually interfacing, or communicating with the Avamar server. Using a separate vCenter user account ensures maximum clarity if it becomes necessary to examine vCenter logs.

NOTICE

The user account must be added to the top (root) level in each vCenter you intend to protect.

This vCenter user account must have the following minimum privileges:

Table 3 Minimum required vCenter user account privileges (page 1 of 3)

	vCenter 5.5U1	vCenter 5.5/5.1	vCenter 5.0
Alarms	• Create alarm	• Create alarm	• Create alarm
Datastore	• Allocate space • Browse datastore • Configure datastore • Low level file operations • Move datastore • Remove datastore • Remove file • Rename datastore	• Allocate space • Browse datastore • Low level file operations • Move datastore • Remove datastore • Remove file • Rename datastore	• Allocate space • Browse datastore • Low level file operations • Move datastore • Remove datastore • Remove file • Rename datastore
Extension	• Register extension • Unregister extension • Update extension	• Register extension • Unregister extension • Update extension	
Folder	• Create folder	• Create folder	• Create folder
Global	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Settings	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Settings	• Cancel task • Disable methods • Enable methods • License method • Log event • Manage custom attributes • Settings
Host		• Configuration › Storage partition configuration	• Configuration › Storage partition configuration
Network	• Assign network • Configure	• Assign network • Configure	• Assign network • Configure
Resource	• Assign virtual machine to resource pool	• Assign virtual machine to resource pool	• Assign virtual machine to resource pool
Sessions	• Validate session	• Validate session	• Validate session
Tasks	• Create task • Update task	• Create task • Update task	• Create task • Update task

Table 3 Minimum required vCenter user account privileges (page 2 of 3)

	vCenter 5.5U1	vCenter 5.5/5.1	vCenter 5.0
vApp	• Export • Import • vApp application configuration	• Export • Import • vApp application configuration	• Export • Import • vApp application configuration
Virtual machine			
Configuration	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device setting s • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device setting s • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device setting s • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual hardware
Guest Operations	• Guest Operation Modifications • Guest Operation Program Execution • Guest Operation Queries	• Guest Operation Modifications • Guest Operation Program Execution • Guest Operation Queries	• Guest Operation Modifications • Guest Operation Program Execution • Guest Operation Queries
Interaction	• Console interaction • DeviceConnection • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install	• Console interaction • DeviceConnection • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install	• Acquire guest control ticket • Console interaction • DeviceConnection • Power off • Power on • Reset • VMware Tools install
Inventory	• Create new • Register • Remove • Unregister	• Create new • Register • Remove • Unregister	• Create new • Register • Remove • Unregister

Table 3 Minimum required vCenter user account privileges (page 3 of 3)

	vCenter 5.5U1	vCenter 5.5/5.1	vCenter 5.0
Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Mark as Template
Snapshot Management	• Create snapshot • Remove Snapshot • Revert to snapshot	• Create snapshot • Remove Snapshot • Revert to snapshot	
State			• Create snapshot • Remove Snapshot • Revert to snapshot

Adding a vCenter client in Avamar Administrator

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.

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 Server.

NOTICE

You must perform this task for each vCenter you intend to protect.

Adding a vCenter client in Avamar Administrator automatically:

- Adds the vCenter client 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.

- Creates a default vCenter Server with the same name as the vCenter's fully qualified hostname.
- Creates a VirtualMachines subdomain within that vCenter Server.
- Creates a Default Virtual Machine Group.

  This group 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. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Select the **Account Management** tab.

3. In the tree, select the top-level (root) domain, and select **Actions › Account Management › New Client(s)...**

   The New Client dialog box appears.

4. For **Client Type**, select **VMware vCenter**.

5. Complete the following settings:

Table 4 New vCenter client settings

Setting	Description
New Client Name or IP	Fully-qualified DNS 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.
Password	Password for the vCenter user account you previously created.
Verify Password	Type the password again.
Contact	Optional contact name.
Phone	Optional contact telephone number.
Email	Optional contact email address.
Location	Optional contact location.

6. Click **OK**.

   The New Client dialog box closes.

Deploying proxies

Backups and restores require deployment of proxy virtual machines. Once deployed, each proxy virtual machine client provides all of the following capabilities:

- Backup of Microsoft Windows and Linux virtual machines (entire images or specific drives)
- Restore of Microsoft Windows and Linux virtual machines (entire images or specific drives)
- Selective restore of individual folders and files to Microsoft Windows and Linux virtual machines

Proxies run Avamar software inside a Linux virtual machine, and are deployed using an appliance template (.ova) file.

Proxies are allowed in any part of Avamar Administrator account management tree except the vCenter Server domain or subdomains.

Although it is possible to restore across datacenters (that is, use a proxy deployed in one datacenter to restore files to a virtual machine in another datacenter), restores will take noticeably longer than if the proxy and the target virtual machine are both located in the same datacenter. Therefore, for best performance, deploy at least one proxy on each datacenter you are protecting.

For best results, always register and activate proxies from the client during deployment (as described in "Registering and activating a proxy with Avamar server" on page 38). Using the alternative method of inviting the proxy to register with the Avamar server from Avamar Administrator is known to have unpredictable results.

Adding DNS Entries

During "Deploying a proxy appliance in vCenter" on page 33, you will be asked to assign a unique IP address to each proxy. vCenter performs a reverse DNS lookup of that IP address to ensure that it is resolvable to a hostname. For best results, configure all required DNS entries for proxies you plan to deploy before proceeding with the remainder of this procedure.

Downloading the proxy appliance template file

NOTICE

If adding more than one proxy, you only need to perform this task once.

Download the proxy appliance template file by performing the following:

1. Open a web browser and type the following URL:

   ```
   http://AVAMARSERVER
   ```

   where AVAMARSERVER is the Avamar server network hostname or IP address.

   The EMC Avamar Web Restore web page appears.

2. Click **Downloads**.
3. Click **+** next to the **VMware vSphere** folder.
4. Click **+** next to the **EMC Avamar VMware Image Backup/FLR Appliance** folder.
5. Click the **AvamarCombinedProxy-linux-sles11_64-**VERSION**.ova** link.

   where VERSION is the specific version Avamar software available for download.

6. Save **AvamarCombinedProxy-linux-sles11_64-**VERSION**.ova** to a temporary folder, such as C:\Temp, or the desktop.

Deploying a proxy appliance in vCenter

When deploying a proxy appliance in vCenter, two vSphere Client applications are available. Use the correct vSphere Client for your specific vCenter environment.

- If you are deploying a proxy in a vCenter running on a Windows virtual machine, you can use either the vSphere Client running on a Windows computer, or the vSphere Web Client.
- If you are deploying a proxy in a vCenter running on a Linux virtual machine, you must use the vSphere Web Client.

Deploying a proxy appliance in vCenter using the vSphere Client

To deploy a proxy appliance in vCenter using the vSphere Client running on a Windows computer:

1. Launch the vSphere Client and log in to the vCenter Server.

   The vSphere Client window appears.

2. Select **File › Deploy OVF Template**.

   The Deploy OVF Template wizard appears.

3. In the **Source** screen, complete the following:

   a. Click **Browse**.

      The Open dialog box appears.

   b. Select **Ova files (*.ova)** from the **Files of Type** list.

   c. Browse to the appliance template file that was previously downloaded in "Downloading the proxy appliance template file" on page 33.

   d. Select the appliance template file and click **Open**.

      The Open dialog box closes.

      The full path to the appliance template file appears in the **Deploy from file** field.

   e. Click **Next**.

4. In the **OVF Template Details** screen, ensure that the information is correct, and then **Next**.

5. In the **Name and Location** screen, complete the following:

   a. Type a unique fully-qualified hostname in the **Name** field.

      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.

      NOTICE

      In order to avoid confusion and potential problems, EMC strongly recommends that you consistently use the same fully-qualified hostname for this proxy in all contexts.

   b. Select a datacenter and folder location for this proxy in the Inventory tree.

   c. Click **Next**.

6. In the **Host / Cluster** screen, complete the following:

   a. Select an ESX Server or cluster.

   b. Click **Next**.

   If you selected a cluster, the Specific Host screen appears.

7. In the **Specific Host** screen, complete the following:

    a. Select a specific ESX Server from the **Host Name** list.

    b. Click **Next**.

8. In the **Storage** screen, complete the following:

    a. Select a storage location for this proxy.

    b. Click **Next**.

9. In the **Disk Format** screen, click **Next**.

10. In the **Network Mapping** screen, complete the following:

    a. Select a destination network from list.

    b. Click **Next**.

11. In the **Networking Properties** screen, complete the following:

    NOTICE

    Proxy network settings are difficult to change once they proxy is registered and activated with the Avamar server. Therefore, ensure that the settings you enter in the Networking Properties screen are correct.

    a. Enter the default gateway IP address for your network in the Default Gateway field.

    b. If not using DHCP, enter one or more Domain Name Server (DNS) IP addresses in the DNS field. Separate multiple entries with commas.

    c. If not using DHCP, enter a valid IP address on your network in the Network IP Address field.

    d. Type the correct network mask in the Network Netmask field.

    e. Click **Next**.

12. In the **Ready To Complete** screen, ensure that the information is correct.

13. Click **Finish**.

    The Deploy OVF Template wizard closes.

14. Wait for the deployment operation to complete.

    This might take several minutes.

    A confirmation message appears.

15. Click **Close** to dismiss the confirmation message.

Deploying a proxy appliance in vCenter using the vSphere Web Client

To deploy a proxy appliance in vCenter using the vSphere Web Client:

1. Connect to the vCenter Server by opening a web browser, and then typing the following URL:

    ```
    http://vCenterServer:9443/
    ```

    where vCenterServer is the vCenter Server network hostname or IP address.

The vSphere Web Client web page appears.

2. Download and install the Client Integration Plug-in:

   Note: These steps only need to be performed the first time you connect to this vCenter Server using the vSphere Web Client. You can skip these steps on subsequent vSphere Web Client sessions.

   a. Click the Download Client Integration Plug-in link at the bottom of the vSphere Web Client web page.

   b. Run the installation program.

   c. Close your web browser.

   d. Complete the remaining on-screen installation instructions.

   e. After the installation completes, reconnect to the vCenter Server by repeating step 1.

3. Log in to the vCenter Server by typing your **User name** and **Password**, and then clicking **Login**.

4. Select **Home** › **vCenter** › **Hosts and Clusters**.

5. Select **Actions** › **Deploy OVF Template**.

6. Allow plug-in access control.

   The Deploy OVF Template wizard appears.

7. In the **Source** screen, complete the following:

   a. Select **Local file** and then click **Browse**.

      The Open dialog box appears.

   b. Select **Ova files (*.ova)** from the **Files of Type** list.

   c. Browse to the appliance template file that was previously downloaded in "Downloading the proxy appliance template file" on page 33.

   d. Select the appliance template file and click **Open**.

      The Open dialog box closes.

      The full path to the appliance template file appears in the **Deploy from file** field.

   e. Click **Next**.

8. In the **OVF Template Details** screen, ensure that the information is correct, and then **Next**.

9. In the **Select name and folder** screen, complete the following:

   a. Type a unique fully-qualified hostname in the **Name** field.

      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.

NOTICE

In order to avoid confusion and potential problems, EMC strongly recommends that you consistently use the same fully-qualified hostname for this proxy in all contexts.

b. Select a datacenter and folder location for this proxy in the tree.

c. Click **Next**.

10. In the **Select a resource** screen, complete the following:

a. Select an ESX Server host, cluster, vApp or resource pool in which to run this proxy.

b. Click **Next**.

11. In the **Select storage** screen, select a storage location for this proxy, and then click **Next**.

12. In the **Setup networks** screen, complete the following:

a. Select a **Destination** network from list.

b. Select an **IP protocol** from the list.

c. Click **Next**.

13. In the **Customize template** screen, complete the following:

NOTICE

Proxy network settings are difficult to change once they proxy is registered and activated with the Avamar server. Therefore, ensure that the settings you enter in the Networking Properties screen are correct.

a. Enter the default gateway IP address for your network in the **Default Gateway** field.

b. If not using DHCP, enter one or more DNS IP addresses in the **DNS** field. Separate multiple entries with commas.

c. If not using DHCP, enter a valid IP address on your network in the **Isolated Network IP Address** field.

d. Type the correct network mask in the **Isolated Network Netmask** field.

e. Click **Next**.

14. In the **Ready To Complete** screen, ensure that the information is correct.

15. Click **Finish**.

The Deploy OVF Template wizard closes.

16. Wait for the deployment operation to complete.

This might take several minutes.

Registering and activating a proxy with Avamar server

NOTICE

For best results, always register and activate proxies as described in this task. Using the alternative method of inviting the proxy from Avamar Administrator is known to have unpredictable results.

1. From either the vSphere Client or vSphere Web Client, locate and select a Avamar image backup proxy that was previously deployed in "Deploying a proxy appliance in vCenter" on page 33.
2. Power on the new proxy virtual machine by right-clicking the proxy and selecting **Power › Power On**.
3. Open a console to the proxy by right-clicking it and selecting **Open Console**.

   The Console window appears.
4. Wait for the Main Menu to appear.
5. Register the proxy with an Avamar server by typing **1**.

   The following appears in the console window:

   ```
   Enter the Administrator server address (DNS text name, or numeric IP
   address, DNS name preferred):
   ```
6. Type the actual network hostname as defined in DNS of the Avamar server from which you want to initiate, and manage backups and restores.
7. 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.

   Note: 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.
8. Press **Enter** to accept the default domain (clients).

   In order to implement file-level restore, this proxy requires the Avamar server root password.

   The following appears in the console window:

   ```
   Has the Avamar server software root password changed since last
   running this utility? [no]
   ```

9. Do one of the following:

   - If the Avamar server software root password has not changed since you last ran this utility, press **Enter** and go directly to step 11.

   - If the Avamar server software root password has changed since you last ran this utility, type **y** and press **Enter**, then go to step 10.

   The following appears in the console window:

   ```
   Enter the Avamar server software root password:
   ```

10. Enter the Avamar server software root password and press **Enter**.

11. Wait for the Main Menu to appear.

12. Type **2** and press **Enter** to quit.

Configuring proxy settings in Avamar Administrator

Each deployed proxy appliance provides 8 image backup and restore, and 8 file-level restore plug-ins. Each of these plug-ins functions as a separate logical proxy that can be independently assigned to different groups.

In order to differentiate between these logical proxies, proxy names in Avamar Administrator have "proxy-1" through "proxy-8" appended to the hostname you defined in "Deploying a proxy appliance in vCenter" on page 33.

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Select the **Account Management** tab.

3. In the tree, select a proxy and select **Actions › Account Management › Client Edit...**

   The Edit Client dialog box appears.

4. Select the **Datastores** tab, then select all vCenter datastores that host virtual machines you want to protect with this proxy.

5. Select the **Groups** tab, then assign this proxy to one, or more existing groups by selecting the **Select** checkbox next to each group.

6. (Optional) complete the following optional contact information:

   a. Enter an optional contact name in the **Contact** field.

   b. Enter an optional contact telephone number in the **Phone** field.

   c. Enter an optional contact email address in the **Email** field.

   d. Enter an optional contact location in the **Location** field.

7. Click **OK**.

   The Edit Client dialog box closes.

(Optional) Configuring proxy certificate authentication

By default, Avamar proxies do not validate SSL certificates when connecting to the vCenter Server. This can leave the vCenter Server vulnerable to a man-in-the-middle exploitation, which might result in unauthorized access to the vCenter Server. Configuring each Avamar proxy to use SSL certificate authentication when connecting to the vCenter Server corrects this vulnerability.

Before you begin

Ensure that a Certificate Authority (CA) signed SSL certificate is installed on the vCenter Server.

Detailed instructions for generating and installing a CA signed SSL certificate and installing it on the vCenter Server are found in the VMware Knowledge Base.

This procedure supports both standalone certificates and chained permission files. For the remainder of this procedure, *certificate-file* can be either a standalone certificate (*.crt) or chained permission (*.pem) file. Use the correct *certificate-file* for your site.

Procedure

1. Open a command shell and log in to the proxy as root.
2. Copy the vCenter Server certificate file to /usr/local/avamarclient/bin on the proxy.
3. Set the proper operating system permissions on the certificate by typing:

   ```
   chmod 600 /usr/local/avamarclient/bin/certificate-file
   ```

   where *certificate-file* is a standalone certificate (*.crt) or chained permission (*.pem) file.
4. Use OpenSSL to obtain the fingerprint of the SSL certificate of the vCenter Server by typing:

   ```
   openssl x509 -in certificate-file -fingerprint | grep Finger
   ```

   The command returns the SHA1 fingerprint of the SSL certificate of the vCenter Server.

   The format of the returned value is:

   ```
   SHA1 Fingerprint=
   C7:35:19:95:9C:3F:56:1D:73:35:52:41:F3:02:46:A3:B9:46:4F:D9
   ```

   where C7:35:19:95:9C:3F:56:1D:73:35:52:41:F3:02:46:A3:B9:46:4F:D9 represents the fingerprint.
5. Open /usr/local/avamarclient/var/avvcbimageAll.cmd in a UNIX text editor.
6. Append the following entry to the end of the file:

   ```
   --ssl_server_authentication_file=/usr/local/avamarclient/bin/certif
   icate-file
   ```

   where *certificate-file* is a standalone certificate (*.crt) or chained permission (*.pem) file.

7. Append the following entry to the end of the file:

   ```
   --ssl_server_cert_thumbprint="fingerprint"
   ```

   where *fingerprint* is the fingerprint of the SSL certificate of the vCenter Server that was obtained by using OpenSSL.

   For example, when the fingerprint value is:

   ```
   C7:35:19:95:9C:3F:56:1D:73:35:52:41:F3:02:46:A3:B9:46:4F:D9
   ```

   the appended entry is:

   ```
   --ssl_server_cert_thumbprint="C7:35:19:95:9C:3F:56:1D:
   73:35:52:41:F3:02:46:A3:B9:46:4F:D9"
   ```

8. Save the changes and close /usr/local/avamarclient/var/avvcbimageAll.cmd.
9. Open /usr/local/avamarclient/var/avvmwfileAll.cmdin a UNIX text editor.
10. Append the following entry to the end of the file:

    ```
    --ssl_server_authentication_file=/usr/local/avamarclient/bin/certif
    icate-file
    ```

    where *certificate-file* is a standalone certificate (*.crt) or chained permission (*.pem) file.

11. Save the changes and close /usr/local/avamarclient/var/avvmwfileAll.cmd.
12. Open /etc/vmware/config in a UNIX text editor.
13. Append the following entries to the end of the file:

    ```
    vix.enableSslCertificateCheck = "true"
    vix.sslCertificateFile =
    "/usr/local/avamarclient/bin/certificate-file"
    ```

    where *certificate-file* is a standalone certificate (*.crt) or chained permission (*.pem) file.

14. Open /usr/local/avamarclient/var/vddkconfig.ini in a UNIX text editor.
15. Find the vixDiskLib.linuxSSL.verifyCertificates=0 entry.
16. Change the value of the vixDiskLib.linuxSSL.verifyCertificates=0 entry to 1.

    ```
    vixDiskLib.linuxSSL.verifyCertificates=1
    ```

17. Save the changes and close /usr/local/avamarclient/var/vddkconfig.ini.
18. Ensure that there are no running backup or restore jobs on this proxy.
19. Restart the **avagent** and **vmwareflr** services by typing:

    ```
    service avagent restart
    service vmwareflr restart
    ```

After you finish

Repeat this procedure for each Avamar proxy.

(Optional) Performing proxy performance optimization

By default, Avamar proxies are configured with four virtual CPU sockets and one core per socket. However, changing the proxy configuration to four virtual CPU sockets and two cores per socket will achieve better backup and restore performance.

Upgrading Avamar proxy software

Perform the following procedure when a newer version of the Avamar proxy software is available for download from the Avamar server.

NOTICE

This procedure cannot be used to upgrade an Avamar 6.0 proxy. Instead, use the upgrade procedure in the *EMC Avamar 6.0 for VMware Guide*.

1. On the computer where the software will be installed, open a web browser and type the following URL:

   `http://AVAMARSERVER`

   where AVAMARSERVER is the Avamar server network hostname or IP address.

   The EMC Avamar Web Restore web page appears.
2. Click **Downloads**.
3. Click **+** next to the **VMware vSphere** folder.
4. Click **+** next to the **EMC Avamar VMware Image Backup/FLR Appliance** folder.
5. Click the **AvamarCombinedProxy-linux-x86-**VERSION**.iso** link.

   where VERSION is the specific version Avamar software available for download.
6. Save **AvamarCombinedProxy-linux-x86-**VERSION**.iso** to a temporary folder, such as C:\Temp, or the desktop.
7. Launch the vSphere Client, and log in to the vCenter Server.

   The vSphere Client window appears.
8. Locate and select the ESX Server that hosts the proxy you want to update.
9. Select the **Summary** tab.
10. In the **Resources** pane, select a datastore in the **Datastore** list.

    This datastore is where you will upload the ISO file.

    Note: If you are performing multiple upgrades, you should select a datastore that is accessible to the greatest number of proxies.
11. Right click the datastore and select **Browse Datastore**.

    The Datastore Browser window appears.
12. In the Folder tree, select a folder.

    This folder is where you will upload the ISO file.

13. Click **Upload files to this datastore**, then select **Upload file**.

    The Upload Items dialog box appears.

14. Browse to the ISO file that you downloaded in step 6.
15. Select the ISO file and click **Open**.

    The Upload Items dialog box closes.

16. If an Upload/Download Operation Warning appears, click **Yes** to dismiss the warning and continue with the upload.
17. Wait for the upload to complete.
18. Switch to vSphere Client window VMs and Templates view by clicking **View › Inventory › VMs and Templates**.
19. In the left pane, locate and select the proxy you want to upgrade.
20. Right click **Edit Settings**.

    The Virtual Machine Properties dialog box appears.

21. In the **Hardware** list, select **CD/DVD Drive 1**.
22. Set the following options:
    a. In **Device Status**, select **Connected**.
    b. In **Device Status**, select **Connect at power on**.
    c. In **Device Type**, select **Datastore ISO File**.
23. Click **Browse**.

    The Browse Datastores dialog box appears.

24. Locate and select the ISO file you uploaded in steps 8–17.
25. Click **Open**.

    The Browse Datastores dialog box closes.

26. Switch to **Virtual Machine Properties** dialog box and click **OK**.

    The Virtual Machine Properties dialog box closes.

    The ISO file is mounted on the proxy.

    The proxy automatically waits until no backups are running, then updates itself. Because the polling interval is set to 30 minutes, it make take up to 30 minutes after the last backup completes for the upgrade to begin.

    NOTICE

    When you reboot the proxy VM, it updates its software. Backups that are running during the reboot fail. You should only reboot when you are absolutely certain the proxy is not being used for backups.

27. Switch to vSphere Client window VMs and Templates view by clicking **View › Inventory › VMs and Templates**.
28. In the left pane, locate and select the proxy you just upgraded.

29. Right click **Edit Settings**.

    The Virtual Machine Properties dialog box appears.

30. In the **Hardware** list, select **CD/DVD Drive 1**.

31. In **Device Status**, clear the **Connected** option.

32. Click **OK**.

    The Virtual Machine Properties dialog box closes.

33. Repeat steps 18–32 to upgrade additional proxies.

Performing optional proxy plug-in configuration

By default, each 7.0 proxy provides eight plug-in instances, each of which appears as a separate logical proxy instance in Avamar Administrator. This topic provides instructions for changing this setting.

1. From the **vSphere Client** window, locate and select a Avamar image backup proxy.

2. Ensure that the proxy is powered on.

3. Open a console to the proxy by right-clicking it and selecting **Open Console**.

   The Console window appears.

4. Wait for the Main Menu to appear.

5. Type **2** and press **Enter** to quit the default script session.

   The login screen appears.

6. Log in as root.

7. Run the initproxyappliance.sh shell script in expert mode by typing:

   ```
   cd /usr/local/avamarclient/etc
   ./initproxyappliance.sh start --expert
   ```

8. Wait for the Main Menu to appear.

9. Type **1** and press **Enter**.

10. Press **Enter** to accept the previous settings until the following prompt appears:

    ```
    Number of proxy clients (1 to 8) [8]: 8
    ```

11. Type the number of logical proxy clients and press **Enter**.

12. Continue pressing **Enter** to accept the previous settings until the Main Menu appears.

13. Type **2** and press **Enter** to quit.

Re-registering a proxy with a different Avamar server

Should it become necessary to re-register an existing proxy virtual machine with a different Avamar server, perform the following:

1. Launch the vSphere Client and log in to the vCenter Server.

   The vSphere Client window appears.

2. Locate the Avamar proxy.

3. Right-click **Power › Shut Down Guest.**

   The following message appears:

```
Shut down the guest operating system of virtual machine?
```

4. Click **Yes** to dismiss the message.

5. Right-click **Power › Power Off.**

   The following message appears:

```
Ensure that you have shut down your guest operating system before
powering off.
Power off the selected virtual machine?
```

6. Click **Yes** to dismiss the message.

7. Right-click **Power › Open Console.**

   A console window appears:

8. In the vSphere Client window, right-click **Power › Power On.**

9. Monitor the console window until the following message appears:

```
Please press a key now if you want to re-register this proxy with
Avamar Administrator. Continuing in 10 seconds...
```

10. Click inside the console windown and press **Enter.**

    The following message appears:

```
=== Client Registration and Activation ===
This script will register and activate the client with the
Administrator server.
Enter the Administrator server address (DNS text name or numeric IP
address, DNS name preferred):
```

11. Type the network hostname (as defined in DNS) of the Avamar Administrator server and press **Enter.**

    The following appears in the command shell:

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

The default domain is “clients.” However, the Avamar system administrator might have defined other domains and subdomains. Consult the Avamar system administrator for the specific domain to use when registering this client.

NOTICE

If typing a subdomain (for example, clients/MyClients), do not include a slash (/) as the first character. Including a slash as the first character causes an error and prevents you from registering this client.

12. Press **Enter** to accept the default domain (clients).

Changing the proxy operating system root password

To change the proxy operating system root password:

1. Open a command shell and log in to the proxy as root.
2. Type:

   ```
   passwd
   ```

   The following appears in the command shell:

   ```
   Current Password:
   ```

3. Type the current proxy operating system root password and press **Enter**.

   The following appears in the command shell:

   ```
   New Password:
   ```

4. Type the new proxy operating system root password and press **Enter**.

   The following appears in the command shell:

   ```
   Confirm New Password:
   ```

5. Type the same password entered in step 4 and press **Enter**.

Protecting virtual machines with both guest and image backup

You can protect a virtual machine using 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, complete the following configuration steps:

1. Open a command shell, and log in:
   - If logging into a single-node server, log in to the server as admin.
   - If logging into a multi-node server, log in to the utility node as admin.
2. Stop the MCS by typing:

   ```
   dpnctl stop mcs
   ```

3. Open /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml in a UNIX text editor.
4. Locate the **allow_duplicate_client_names** preference.
5. Change the **allow_duplicate_client_names** preference setting to true.

   For example:

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

6. Save your changes.

7. Restart the MCS by typing:

```
dpnctl start mcs
```

CHAPTER 3
Administration

This chapter provides instructions for administering an operational Avamar for VMware image backup and restore environment. Topics in this chapter include:

Clients and containers

Image backup can be used manage and protect any of the following VMware entities in a vCenter:

- Virtual machines
- vApps
- Virtual machine folders (that is, any folder residing below the datacenter level)
- Resource pools

In Avamar Administrator, virtual machines and vApps are managed as clients; folders and resource pools are managed as containers.

Containers provide the capability of managing multiple virtual machines, vApps, virtual machine folders, and resource pools as a single logical object.

Dynamic versus static containers

When containers are added to Avamar Administrator, you define them to be either dynamic or static.

Dynamic containers—include all contents of the vCenter container, but also continuously monitor the container entity in vCenter, so that if changes occur (for example, virtual machines or folders are added or deleted), those changes will automatically be reflected in Avamar Administrator.

Static containers—only include what is in the vCenter container at the time it is added to Avamar. If subsequent changes occur in vCenter, they will not be reflected in Avamar Administrator.

Dynamic container behavior

When adding a dynamic container, only one level of subcontainers is added to Avamar Administrator. Virtual machines residing in subcontainers or vApps must be manually added to Avamar Administrator in order for those virtual machines to be protected by image backup.

If a virtual machine client is deleted from a container in vCenter, and that container was being protected as a dynamic container in Avamar Administrator, that virtual machine client will continue to exist in Avamar as part of that dynamic container. However, the icon changes change color from blue to gray. This enables past backups to be used for future restores. However, no new backups will occur because the virtual machine client no longer exists in vCenter.

If you need to delete or retire one or more virtual machine clients from an Avamar dynamic container, you must first change that container to a static container. An alternative method is to move those virtual machine clients to another container in vCenter.

How independent and container protection interact

When a virtual machine is protected independently and as a container member, retiring or deleting that virtual machine are some special conditions. Consider the following example nested container structure and scenario:

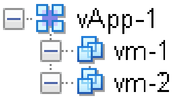


Figure 2 Example independent and container protection

First, vm-1 is added to Avamar as a virtual machine client; it is said to be independently protected. Next, the vApp-1 container is added to Avamar; vm-1 is also protected as a member of the vApp-1 container. At this point, Avamar recognizes that the same virtual machine exists in two contexts:

- Independently protected as standalone virtual machine client vm-1
- Protected as a member of vApp-1 container

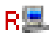
However, if container the vApp-1 container is retired or deleted, vm-1 will continue to exist in Avamar as a standalone virtual machine client because it was explicitly added that way before it was protected as a member of the vApp-1 container. The standalone context supercedes the container member context. Therefore, if you need to retire or delete vm-1, you cannot simply delete or retire vApp-1 container. You must also retire or delete the standalone instance as well. Otherwise, vm-1 will continue to be protected by scheduled backups.

Icons and what they mean

In order to differentiate between the various types of entities, Avamar Administrator uses the following icons to communicate entity type and state:

- vCenter Server:

  Activated. This is the same icon used to show nonvirtual machine clients.

   Replicated. This icon is only visible in REPLICATE domain.

  Unactivated.

  Note: Unless you are also protecting the vCenter Server with guest backup, vCenter Servers are not activated as normal Avamar clients. Therefore, can be the normal state for a vCenter Server.

- Virtual machine clients:

  Powered off.

  Powered on.

  Template.

- Proxies:

  Activated and enabled.

  Disabled.

  Replicated. This icon is only visible in REPLICATE domain.

  Unactivated

- Other entities:

  vCenter folder

  vApp

  Resource pool

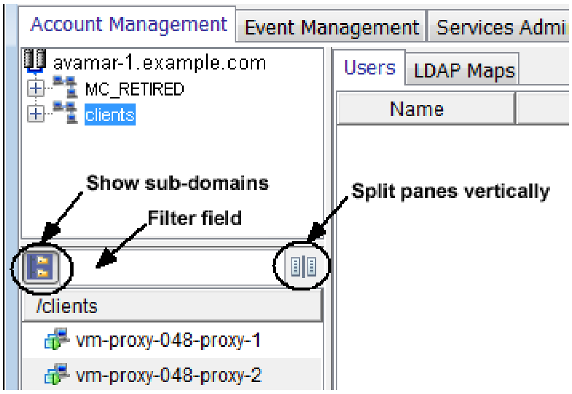
Adding clients and containers

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Select the **Account Management** tab.

   The left side of the Account Management tab shows two panes and several controls used to facilitate easily locating one or more virtual machine or vApp clients:

   - The upper pane shows the Avamar server domain structure.
   - The lower pane shows contents of any domain selected in the upper pane.
   - Clicking the ▣ button shows all virtual machine or vApp clients in subfolders.
   - Typing one or more characters filter field only shows clients that contain those characters.
   - Clicking the ▥ button splits the two panes vertically.

3. In the upper tree, select a vCenter domain or subdomain.

4. Select **Actions › Account Management › New Client(s)**.

   The Select VMware Entity dialog box appears.

   - **The VMs & Templates tab is** representative of the vCenter Virtual Machines and Template view.

- **The Hosts & Clusters tab is** representative of the vCenter **Hosts and Clusters view.**

  Note: Resource pools are not visible in the **VMs & Templates tab. They are** only visible in the **Hosts & Clusters tab.**

- VMware entities that already exist as Avamar clients are grayed out.
- Proxy virtual machines cannot be selected.
- For each VMware entity, the following information is shown in the right properties pane:
  - Name—Entity name.
  - Location—Folder location.
- The following information is shown in the right properties pane for virtual machines:
  - Guest OS—Virtual machine operating system.
  - Server—ESX Server or cluster hostname where the virtual machine resides.
  - Template—Whether or not the virtual machine is a template.
  - Powered On—Whether or not the virtual machine is currently powered on.
  - Changed Block—Whether or not changed block tracking is turned on.

5. In the tree, browse to a folder that contains a VMware entity.

   Contents of the folder are listed in the right properties pane.

6. (Optional) To view all entities within the selected folder, select **Show sub-entities**.
7. Select a folder, resource pool, virtual machine or vApp in the right properties pane.
8. If you selected a container in step 7, select either **Dynamic or Static Virtual Machine Container Inclusion.** “Dynamic versus static containers” on page 50 provides details.
9. To enable changed block tracking, select **Enable changed block tracking**.

   If changed block tracking is not enabled, each virtual machine image must be fully processed for each backup, which might result in unacceptably long backup windows, or excessive back-end storage read/write activity.

   Note: Enabling changed block tracking will not take effect until any of the following actions occur on the virtual machine: reboot, power on, resume after suspend, or migrate.

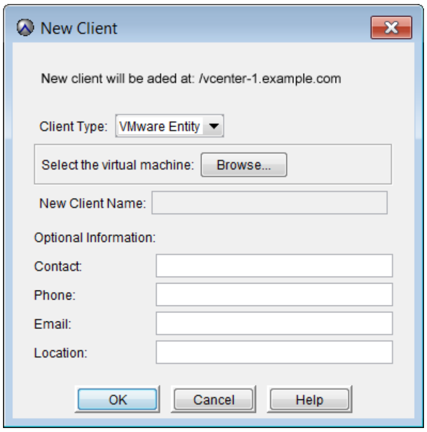
   ---

10. Click **OK**.

    The Select VMware Entity dialog box closes.

11. Do one of the following:

    - If you selected multiple entities in step 7, proceed directly to step 13.
    - If you selected a single entity in step 7, the New Client dialog box appears and is populated with information.



New Client

New client will be added at: /vcenter-1.example.com

Client Type: VMware Entity

Note: VMware Entity is the only available **Client Type** selection.

12. (Optional) Type the following contact information:

    - **Contact** name.
    - Contact telephone (**Phone**) number.
    - Contact **Email** address.
    - Contact **Location**.

13. Click **OK**.

    A Client added confirmation message appears.

14. Click **OK**.

    The Client added confirmation message closes.

15. If you enabled changed block tracking:

    a. In the vSphere Client or vSphere Web Client, locate a virtual machine for which you have enabled changed block tracking.

    b. Perform any of the following actions for each virtual machine: reboot, power on, resume after suspend, or migrate.

    c. Repeat steps a—b for each affected virtual machine.

Editing clients and containers

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Select the **Policy Management** tab, and click the **Clients** tab.

3. Select a virtual machine, proxy, or container.

   The Edit Client dialog box appears.

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

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

   - When editing a vCenter Server, editable credentials are shown.
   - When editing a proxy, two tabs are shown:
     - The **Datstores** tab is used to select all vCenter datastores that host virtual machines you want to protect with this image proxy.
     - The **Groups** tab is used to assign an image proxy to one or more existing groups.

       "Editing proxy datastore and group settings" on page 64 provides details.
   - When editing a virtual machine client, datastores on which that virtual machine resides are shown.
   - When editing a VMware container, the **Properties** tab shows a **Dynamic** option, which is used to enable or disable dynamic inclusion for that container.

Renaming a vCenter client

If an existing vCenter client's DNS name changes, the Avamar server will lose its connection to that vCenter. This will prevent any interaction with that vCenter, including scheduled backups, from occurring. If this occurs, you must manually rename that vCenter client in Avamar Administrator.

NOTICE

This is the only method by which you should ever rename a vCenter client. In Avamar Administrator, the vCenter client name must always be the fully qualified DNS name or a valid IP address.

To rename an existing vCenter client:

1. Ensure that vCenter-to-Avamar authentication is working as described in "Configuring vCenter-to-Avamar authentication" on page 26.

2. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

3. Select the **Account Management** tab.
4. In the tree, select the vCenter client.
5. Select **Actions › Account Management › Edit Client.**

   The Edit Client dialog box appears.
6. In the **New Client Name or IP** field, type the new fully qualified DNS name.
7. Click **OK.**

   The Edit Client dialog box closes.
8. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter.**
9. Restart the MCS by typing:

   ```
   dpnctl stop mcs
   dpnctl start mcs
   ```

10. Reboot Avamar proxies as follows:

    a. Launch the vSphere Client and log in to the vCenter Server.

       The vSphere Client window appears.

    b. Locate an Avamar proxy.

    c. Right-click **Power › Shut Down Guest.**

       The following message appears:

       ```
       Shut down the guest operating system of virtual machine?
       ```

    d. Click **Yes** to dismiss the message.

    e. Right-click **Power › Power Off.**

       The following message appears:

       ```
       Ensure that you have shut down your guest operating system before
       powering off.
       Power off the selected virtual machine?
       ```

    f. Click **Yes** to dismiss the message.

    g. Right-click **Power › Power On.**

    h. Repeat steps c–g for each Avamar proxy.

Viewing protected virtual machines

To view protected virtual machines:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Select the **Account Management** tab.
3. Select the **Protection** tab.

You can view the backup protection state for all virtual machines from the Protection tab. You cannot take any actions on this tab.

All the virtual machines in the vCenter 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.

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, the following message appears: No Information.

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Select the **Account Management** tab.
3. In the tree, browse to the REPLICATE domain and select a client.
4. Select **Actions › Account Management › View Information.**

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

5. Click **OK.**

   The dialog box closes.

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 Active and Idle.

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. If this occurs, windows such as the New Client dialog box do not display vCenter structure or virtual machines.

Manually synchronizing Avamar Administrator with a vCenter

Although Avamar Administrator automatically synchronizes with any vCenter it monitors at regular intervals, you can also perform a manual synchronization at any time.

To manually synchronize Avamar Administrator with a vCenter:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Select the **Account Management** tab.

3. In the tree, select a vCenter.

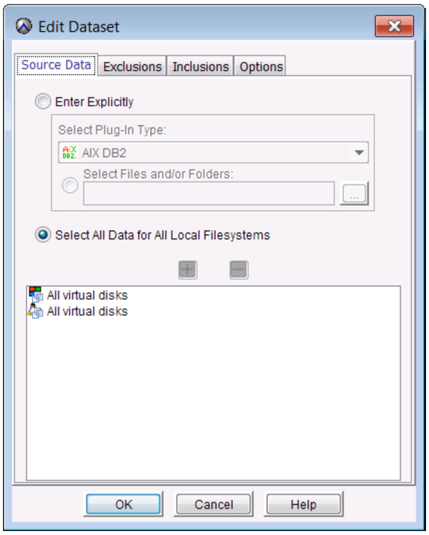
4. Select **Actions** › **Account Management** › **Sync. with vCenter.**

   A confirmation message appears.

5. Click **Yes.**

VMware Image Dataset

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



○ Enter Explicitly

Select Plug-In Type: AIX DB2

○ Select Files and/or Folders:

● Select All Data for All Local Filesystems

All virtual disks
All virtual disks

For the VMware Image Dataset:

- The only source data plug-ins shown are Linux and Windows virtual disks. Both are selected by default.
- The **Select Files and/or Folders** option, and the Exclusions and Inclusions tabs are disabled.

- Changed block tracking is enabled by default using an embedded **utilize_changed_block_list=true** plug-in option statement.

Note: When creating other datasets for use with the Avamar VMware image backup feature, copy this dataset so that you can reuse these recommended settings as the basis for other datasets. The *EMC Avamar Administration Guide* provides details about adding and copying datasets.

Groups

This topic discusses groups and important behavioral differences related to Avamar for VMware image backup and restore.

Default Proxy Group

The Default Proxy Group is where proxies reside. This group cannot be deleted.

Default Virtual Machine Group

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.

vCenter groups

Any group created under a vCenter Server automatically becomes a “vCenter” group. This group behaves similar to nonvCenter groups except that it also provides to ability to specify which proxies are assigned to perform backups on behalf of its group members.

Virtual machine and proxy relationships within vCenter groups

Consider the following simplified example configuration:

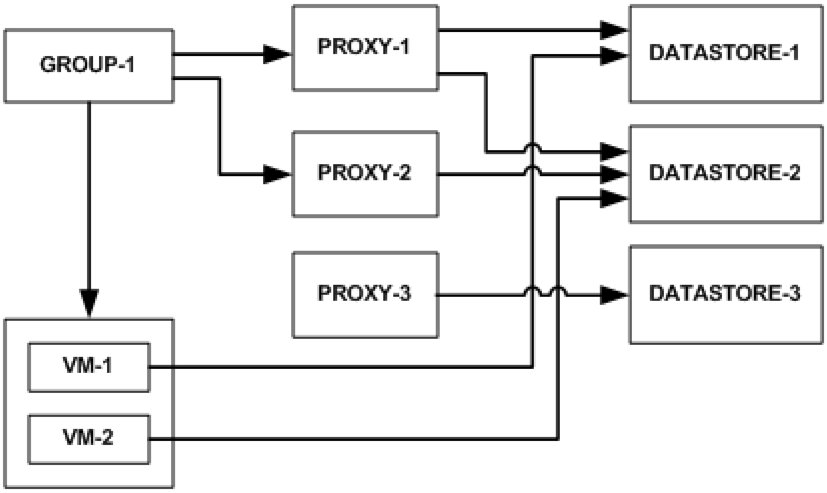


Figure 3 Virtual machine and proxy relationships within vCenter groups

Virtual machines VM-1 and VM-2 store their data in DATASTORE-1 and DATASTORE-2, 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

Datastore assignments are made at the proxy level in the Edit Client dialog box.

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

In order to protect these Virtual machines, proxies 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, cannot protect either VM-1 or VM-2.

NOTICE

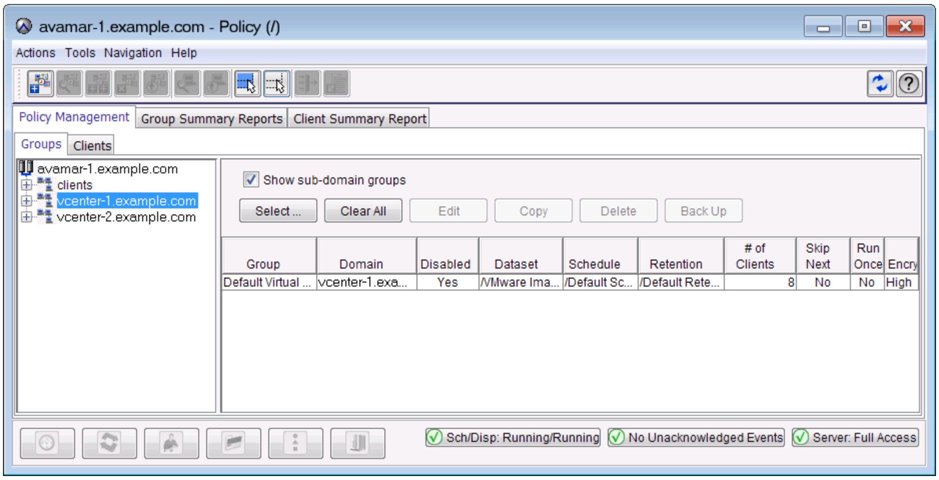
Every vCenter group must include enough proxies to support all the datastores assigned to every client. Otherwise, when a backup is initiated and a proxy cannot be located to perform the backup, the backup will fail with an Activity monitor status of “no proxy.”

Adding a vCenter group

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Select the **Policy Management** tab.
3. Select the **Groups** tab.
4. In the tree, select a vCenter Server.

The data table lists the Default Virtual Machine Group, as well as any other vCenter groups that have been added.

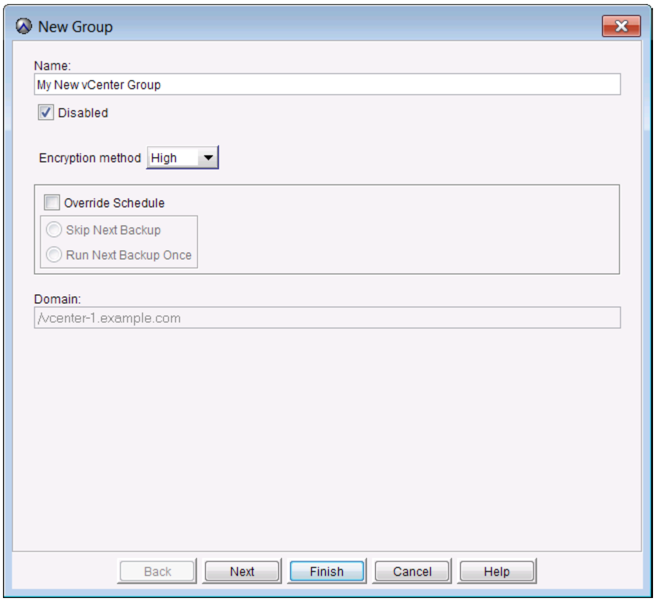


☑ Show sub-domain groups

Group	Domain	Disabled	Dataset	Schedule	Retention	# of Clients	Skip Next	Run Once	Encry
Default Virtual ...	vcenter-1.exa...	Yes	/VMware Ima...	/Default Sc...	/Default Rete...	8	No	No	High

5. Select **Actions › New Group.**

   The New Group dialog box appears.



Name: My New vCenter Group

☑ Disabled

Encryption method: High

□ Override Schedule

○ Skip Next Backup

○ Run Next Backup Once

Domain: /vcenter-1.example.com

6. Complete the following settings:

   a. Type a name for the group in the **Name** field.

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

   b. Select or clear the Disabled option.

      This option is selected by default. Clear this option to immediately enable regularly scheduled group backups.

   c. Select one of the following encryption methods for client/server data transfers:

      – **High**—Strongest available encryption setting.

- **Medium**—Medium strength encryption.
- **None**—No encryption.

Note: The exact encryption technology and bit strength used for any particular client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

d. Select or clear the Override Schedule option.

This option is cleared by default. Select this option to override the assigned schedule for the group and either

You can also skip the next scheduled backup entirely (**Skip Next Backup**) or perform the next scheduled backup one time only (**Run Next Backup Once**).

e. The vCenter Server name appears in the Domain field.

This field is read-only.

The remaining wizard screens are used to select a dataset, schedule, and retention policy, build a client list, and assign proxies for this vCenter group.

7. Click **Next**.

The next New Group wizard screen appears.

8. Select a dataset from the **Select An Existing Dataset** list.

NOTICE

You cannot edit dataset properties from this screen. Detailed dataset properties are shown so that you can review them before you make a selection. The *EMC Avamar Administration Guide* provides details about editing datasets.

9. Click **Next**.

The next New Group wizard screen appears.

10. Select a schedule from the **Select An Existing Schedule** list.

NOTICE

You cannot edit schedules from this screen. Detailed schedule properties are shown so that you can review them before you make a selection. The *EMC Avamar Administration Guide* provides details about editing schedules.

11. Click **Next**.

The next New Group wizard screen appears.

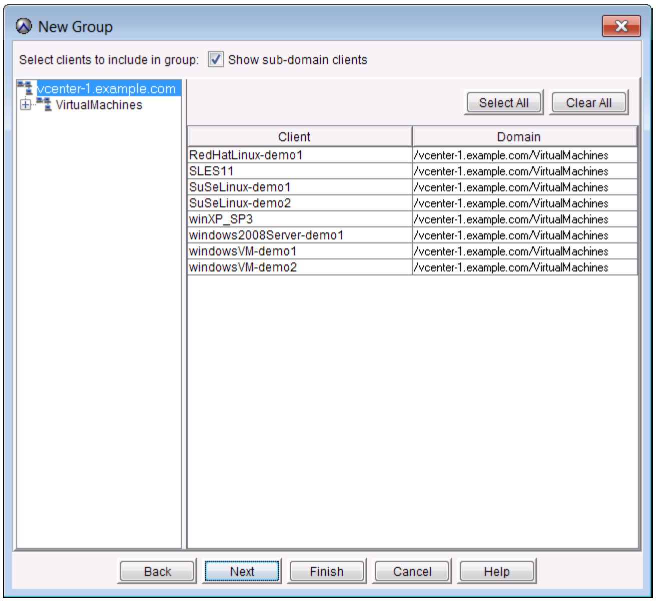
12. Select a retention policy from the **Select An Existing Retention Policy** list.

NOTICE

You cannot edit retention policies from this screen. Detailed retention policy properties are shown so that you can review them before you make a selection. The *EMC Avamar Administration Guide* provides details about editing retention policies.

13. Click **Next**.

    The next New Group wizard screen appears.



Select clients to include in group: ☑ Show sub-domain clients

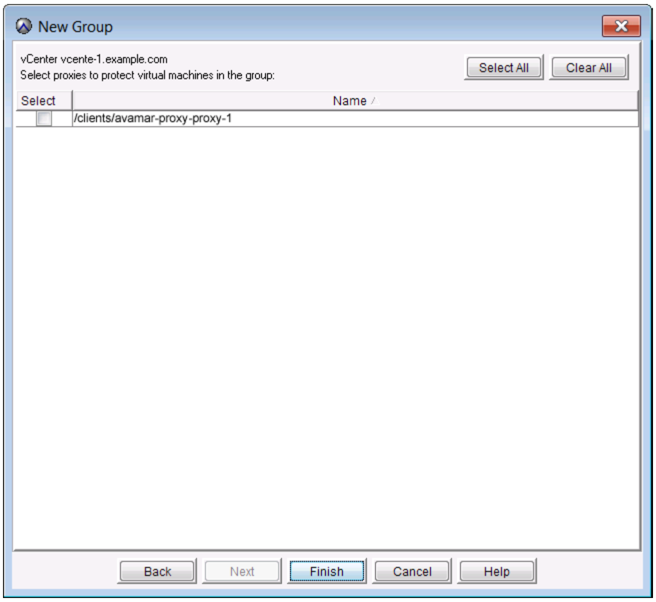
Client	Domain
RedHatLinux-demo1	/vcenter-1.example.com/VirtualMachines
SLES11	/vcenter-1.example.com/VirtualMachines
SuSeLinux-demo1	/vcenter-1.example.com/VirtualMachines
SuSeLinux-demo2	/vcenter-1.example.com/VirtualMachines
winXP_SP3	/vcenter-1.example.com/VirtualMachines
windows2008Server-demo1	/vcenter-1.example.com/VirtualMachines
windowsVM-demo1	/vcenter-1.example.com/VirtualMachines
windowsVM-demo2	/vcenter-1.example.com/VirtualMachines

14. Select one or more virtual machine clients in the data table.

    Note: Click **Show sub-domain clients** to show all available virtual machine clients.

15. Click **Next**.

    The next New Group wizard screen appears.



vCenter vcente-1.example.com
Select proxies to protect virtual machines in the group:

Select	Name
□	/clients/avamar-proxy-proxy-1

16. Select one or more proxies in the data table.

17. Click **Finish**.

    The New Group dialog box closes.

Editing a vCenter group

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Select the **Policy Management** tab.
3. Select the **Groups** tab.
4. Select a vCenter group and click **Edit**.

   The Edit Group dialog box appears.

5. Edit the group settings.

   "Adding a vCenter group" on page 60 provides details about vCenter group settings.

6. Click **OK**.

   The Edit Group dialog box closes.

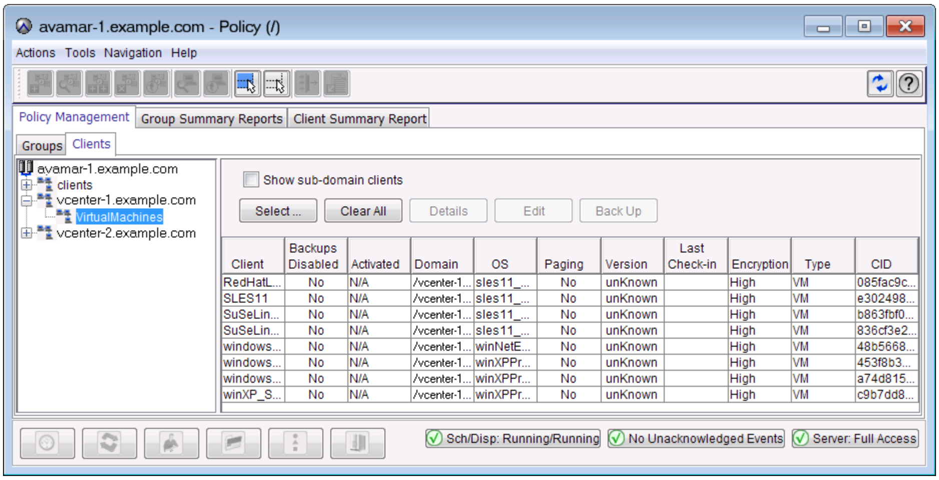
Editing proxy datastore and group settings

This topic describes how to change proxy datastore and group settings. The *EMC Avamar Administration Guide* provides details about editing other client policy settings.

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Select the **Policy Management** tab.
3. Select the **Clients** tab.



□ Show sub-domain clients

Client	Backups Disabled	Activated	Domain	OS	Paging	Version	Last Check-in	Encryption	Type	CID
RedHatL...	No	N/A	/vcenter-1...	sles11_...	No	unKnown		High	VM	085fac9c...
SLES11	No	N/A	/vcenter-1...	sles11_...	No	unKnown		High	VM	e302498...
SuSeLin...	No	N/A	/vcenter-1...	sles11_...	No	unKnown		High	VM	b863fbf0...
SuSeLin...	No	N/A	/vcenter-1...	sles11_...	No	unKnown		High	VM	836cf3e2...
windows...	No	N/A	/vcenter-1...	winNetE...	No	unKnown		High	VM	48b5668...
windows...	No	N/A	/vcenter-1...	winXPPr...	No	unKnown		High	VM	453f8b3...
windows...	No	N/A	/vcenter-1...	winXPPr...	No	unKnown		High	VM	a74d815...
winXP_S...	No	N/A	/vcenter-1...	winXPPr...	No	unKnown		High	VM	c9b7dd8...

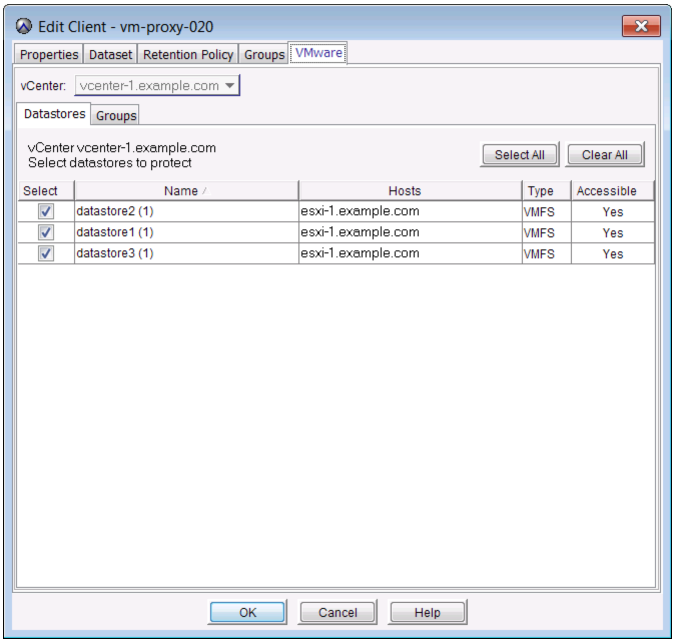
Note: Click **Show sub-domain clients** to show all available proxies.

4. Select a proxy and click **Edit**.

   The Edit Client dialog box appears.

5. Select the **VMware** tab.

6. Select the **Datastores** tab.



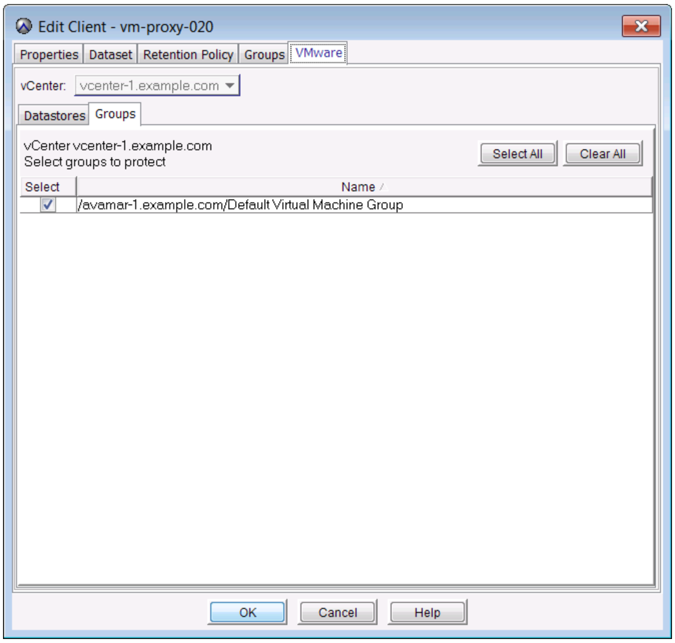
vCenter: vcenter-1.example.com

vCenter vcenter-1.example.com
Select datastores to protect

Select	Name	Hosts	Type	Accessible
☑	datastore2 (1)	esxi-1.example.com	VMFS	Yes
☑	datastore1 (1)	esxi-1.example.com	VMFS	Yes
☑	datastore3 (1)	esxi-1.example.com	VMFS	Yes

7. Select one or more datastores.

8. Select the **Groups** tab.



vCenter: vcenter-1.example.com

vCenter vcenter-1.example.com
Select groups to protect

Select	Name
☑	/avamar-1.example.com/Default Virtual Machine Group

9. Select one or more groups.

10. Click **OK**.

    The Edit Client dialog box closes.

Best practices

The following topics describe best practices to follow when configuring and using Avamar for VMware image backup and restore.

EMC Avamar Compatibility and Interoperability Matrix

Before upgrading the vCenter infrastructure, refer to the *EMC Avamar Compatibility and Interoperability Matrix* to ensure that Avamar supports that version.

Use 64-bit VMware vCenter

For best resuts, use 64-bit VMware vCenter whenever possible.

Verify ESX and vCenter certificates

Use properly registered certificates from a trusted provider that match DNS names for ESX and vCenter.

Use fully-qualified ESX Server hostnames

When adding new ESX Servers to 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.

Recommendations for high change-rate clients

Use the guest backup or Data Domain backend for high change-rate clients.

Changed block tracking recomendations

If a virtual machine contains over 10,000 changed blocks, it is generally faster to back up that client with changed block tracking disabled.

Use throttling parameters for group guest backups

When performing scheduled guest backups of virtual machines on the same ESX Server, add throttling parameters to the Avamar dataset. The reason for doing this is that Avamar tries 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 on the same ESX Server, this can spike CPU usage, which will have an adverse effect on overall ESX Server performance.

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. Select the **Options** tab.
5. Click **Show Advanced Options**.

6. Type a nonzero value in the **Network usage throttle (Mbps)** field.

   Begin with a low value such as 20. Then monitor the next backup session to verify that this has resolved any ESX Server CPU usage issues.

7. Click **OK**.

   The Edit Dataset dialog box closes.

CHAPTER 4
Backup

This chapter provides instructions for backing up virtual machines. Topics in this chapter include:

Limitations

All backups must be initiated from Avamar Administrator

All VMware image backups must be initiated from Avamar Administrator. You cannot initiate backups from the virtual machine or proxy.

Changing virtual machine disk configuration forces a full backup

Changing a virtual machine's disk configuration (either adding or removing a disk), causes the next entire image backup to be processed as a full backup (that is, all virtual disks are processed and changed block tracking is not used), which will require additional time to complete. Backups of specific disks are not affected, unless that disk is previously unknown to Avamar.

Virtual machines with independent disks must not be suspended

If a virtual machine is configured with an independent disk, it must not be in a suspended state when a backup is initiated, or the backup will fail.

Version 8 or 9 virtual machines with disks on multiple datastores

If backing up a hardware version 8 or 9 virtual machine that has multiple disks residing on different datastores, not all datastores will be checked for orphaned snapshots. The backup will also complete without error even if some disks were not backed up.

The only known remedy is to reconfigure the virtual machine such that all virtual disks reside on the same datastore.

Backups involving physical RDM disks

When backing up a virtual machine that has both virtual disks and physical RDM disks, the backup will successfully process the virtual disks, bypass the RDM disks, and complete with the following event code:

Event Code: 30929

Category: Application

Severity: Process

Summary: Virtual machine client contains disks that cannot be backed up or restored.

vApp backups fail if any subvirtual machine fails to backup

When backing up a vApp, all virtual machines within the vApp must successfully complete the back up otherwise that entire back up will not be recorded. Backups for virtual machines that did successfully complete are found in the ContainerClients domain. All backup failures should be promptly investigated and remedied in order to ensure maximum data protection.

Consecutive backups of the same virtual machine might fail if initiated too quickly

If consecutive backups of the same virtual machine are initiated too quickly, the second backup might fail with the following error:

```
avvcbimage Error <9647>: create snapshot failed with error:The object
has already been deleted or has not been completely created on query
#1
```

Do not initiate immediately consecutive backups of the same virtual machine.

ContainerClients domain

The ContainerClients domain is a special system domain, which is populated with virtual machines residing in VMware container entities. Avamar assumes that when you add a VMware container to Avamar, that you will always manage the container and all virtual machines within it as a single object. Therefore, if only you add these virtual machines to a backup group as individual machines, rather than adding the parent VMware container, they will not be backed up.

Nested container limitations

When backing up a VMware container that contains other containers (that is, a nested container structure), , Avamar only backs up the top-level of the hierarchy. Consider the following example nested container structure:

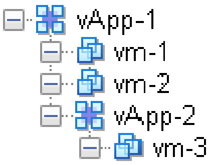


Figure 4 Example nested container structure

When vApp-1 is backed up to Avamar, the vApp backup image will only contain virtual machine backup images for vm-1 and vm-2. When vApp-1 backup is restored, only vm-1 and vm-2 data will be restored. vApp-2 and vm-3 containers will also be present but will not contain any data.

Two interim solutions exist for this limitation:

- Flatten the container structure.

  For example, move vm-3 under vApp-1. Then all three virtual machines will be backed up when vApp-1 is backed up.

- Add both vApp-1 and vApp-2 to Avamar as separate container entities so that they can be backed up separately.

  When restoring, restore vApp-1 first, then restore vApp-2 into vApp-1

Backup of .vmx and nvram files might fail because the ESX server has an exclusive lock

When using vCenter 4.1 U1 or earlier, backups of .vmx and nvram files might fail because the ESX server maintains an exclusive lock on these files. If the vCenter attempts to use an ESX server other than the one that has the exclusive lock on the file to back up the files, then the server without the lock cannot read the .vmx and nvram files to back them up. This issue is fixed in vCenter 4.1 U2.

To work around this issue, add the --x22=8192 option to the dataset for scheduled group backups, or to the **Backup Command Line Options** dialog box for on-demand backups. This allows the backup to complete even if the .vmx file is not backed up.

Because the .vmx file contains the VM configuration information, when restoring the backup, you can select **Restore to original virtual machine** or **Restore to existing virtual machine**, but you cannot select **Restore to a new virtual machine**. To restore to a new virtual machine, you must manually create a new virtual machine with the same configuration as the original virtual machine, then use the **Restore to existing virtual machine** command to restore the backup to the new virtual machine. Restoring to a manually created virtual machine issues new virtual NIC MAC addresses and new virtual disk serial numbers, which may cause license activation issues with virtual machines running Windows.

vApp backups fail if any subvirtual machine fails to backup

When backing up a vApp, all virtual machines within the vApp must successfully complete the back up otherwise that entire back up will not be recorded. Backups for virtual machines that did successfully complete are found in the ContainerClients domain. All backup failures should be promptly investigated and remedied in order to ensure maximum data protection.

Performing an on-demand backup

To perform an on-demand backup:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Click the **Backup** tab.

3. Select an Avamar domain in the upper tree.

4. Select a a virtual machine client, VMware folder, resource pool, or vApp in the lower tree.

5. In the **Browse for File, Folders, or Directories** pane, do one of the following for each selection made in step 4:

   - Select the top (root) folder to back up the entire image.
   - Select one or more disks to only back up those specific virtual disks.

6. Select **Actions › Backup Now...**

   The On Demand Backup Options dialog box appears.

7. Select one of the following retention policies for this backup:

   - **Retention period**—Automatically 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**—Automatically 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**—Keep this backup for as long as this client remains active in the Avamar server.

8. Select one of the following encryption methods for client/server data transfer during this backup:

   - **High**—Strongest available encryption setting.
   - **Medium**—Medium strength encryption.
   - **None**—No encryption.

   Note: The exact encryption technology and bit strength used for any particular client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

9. Click **OK**.

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

10. Click **Close**.

Scheduling backups

To schedule recurring VMware image backups:

1. Create a dataset for the backups.
2. Create a group for the backups. During the group creation process, you:
   a. Assign the new dataset to the new group.
   b. Assign a schedule to the new group.
   c. Assign a retention policy to the new group.
   d. Add virtual machine clients to the new group.
3. Enable scheduling for the group.

A thorough discussion of groups, group policy, datasets, schedules, and retention policies is beyond the scope of this guide. The *EMC Avamar Administration Guide* provides details.

CHAPTER 5
Restore

This chapter provides instructions for restoring a complete image, selected drives, or specific folders or files from an Avamar backup. Topics in this chapter include:

Overview

Avamar offers two levels of restore functionality:

- Image restore—restores an entire backup image or selected drives to the original virtual machine, another existing virtual machine, or a new virtual machine.
- File-level restore—restores specific folders or files from an image backup.

Two buttons are provided above the Select for Restore contents pane, which are not shown if a normal (non-VMware Image) backup is selected:

Clicking the Browse for Image Restore button initiates an image restore.

Clicking the Browse for Granular Restore button initiates a file-level restore.

When performing a VMware image restore, the Restore Options dialog box is slightly 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.

When performing a file-level restore, the procedure is substantially the same as restoring selected folders or files from a normal (non-VMware Image) backup.

Guidelines for performing image restores versus file-level restores

Avamar provides two distinct mechanisms for restoring virtual machine data:

? Image restores, which can restore an entire image or selected drives
- File-level restores, which can to restore specific folders or files

Image restores are less resource intensive and are best used for restoring large amounts of data quickly.

File-level restores are more resource intensive and are best used to restore a relatively small amounts of data. Also, when performing any file-level restore, you cannot restore more than 5,000 folders or files, nor can you browse more than 14,498 folders or files in the same file-level restore operation.

Therefore, if you must restore or browse large numbers of folders or files, you will experience better performance if you restore an entire image or selected drives to a temporary location (for example, a new temporary virtual machine), then copy those files to the desired location following the restore.

Limitations

The following limitations apply to restore operations:

All restores must be initiated from Avamar Administrator

All VMware restores must be initiated from the Avamar Administrator graphical management console or the Management Console Command Line Interface (MCCLI). It is not possible to initiate restores from the virtual machine or proxy.

Server software upgrades require proxy reboots

All Avamar server software upgrades require that all proxies be rebooted. The server software upgrades primarily affect file-level restores (which will not complete until the proxy is rebooted), but is a good practice to immediately reboot all proxies following any server software upgrade.

Virtual machine power state

When restoring an entire image or selected drives, as described in "Nested container limitations" on page 79, "Restoring the full image or selected drives to a different (existing) virtual machine" on page 81, and "Restoring the full image or selected drives to a new virtual machine" on page 83, the target virtual machine must be powered off.

When restoring specific files or folders, as described in "Restoring specific folders or files to the original virtual machine" on page 84 or "Restoring specific folders or files to a different virtual machine" on page 87, the target virtual machine must be powered on.

Restore to original virtual machine limitations

The "Nested container limitations" on page 79 feature is not available when restoring from a template backup. It is also disabled if any 6.1 or older proxies are detected in the environment.

Virtual machine template restores

When restoring a virtual machine template with a 6.0 proxy or using the instant access feature, the virtual machine image is properly restored but is not converted to a template. The solution for this limitation is manually change the restored virtual machine to a template in vSphere.

Restores involving physical RDM disks

When attempting to restore data from a backup taken from a virtual machine with physical RDM disks, "Restoring the full image or selected drives to a new virtual machine" on page 83 is not available. "Restore to new virtual machine not available when physical RDM disks are involved" on page 97 troubleshooting topic provides detailed information and an interim solution.

File-level restore limitations

The following limitations apply to file-level restore as described in "Restoring specific folders or files to the original virtual machine" on page 84 or "Restoring specific folders or files to a different virtual machine" on page 87:

- In order to restore specific folders or files to the original virtual machine, all proxies in the vCenter environment must be version 6.1 or later.

  If any 6.0 or older proxies are detected in the vCenter environment, restoring specific folders or files to the original virtual machine will not be available. However, restoring specific folders or files to a different virtual machine will be available, as described in "Restoring specific folders or files to a different virtual machine" on page 87, will be available.

- VMware Tools must be installed on the target virtual machine. For best results, ensure that all virtual machines are running the latest available version of VMware Tools. Older versions are known to cause failures when browsing during the file-level restore operation.

- The following virtual disk configurations are not supported:

  - Unformatted disks
  - Dynamic disks (Windows) / Multi-Drive Partitions (that is, any partition that consists of 2 or more virtual disks)
  - GUID Partition Table (GPT) disks
  - FAT16 file systems
  - FAT32 file systems
  - Deduplicated NTFS
  - Resilient File System (ReFS)
  - EFI bootloader
  - Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
  - Encrypted partitions
  - Compressed partitions

  Note: In some cases (most notably extended partitions), it may be possible to restore the entire backup image to a temporary virtual machine as described in"Restoring the full image or selected drives to a different (existing) virtual machine" on page 81 or "Restoring the full image or selected drives to a new virtual machine" on page 83, then selectively copy the folders or files you need.

- ACLs are not restored.

- Symbolic links cannot be restored or browsed.

- You cannot restore more than 5,000 folders or files in the same file-level restore operation.

- You cannot browse more than 14,498 folders or files in the same file-level restore operation.

- When restoring files or folders to the original virtual machone, only SCSI disks are supported; IDE disks are not supported.
- In vCenter 5.x, zero-byte files cannot be restored. Attempting to do so might cause the restore to fail.
- Encrypted folders or files cannot be restored. Attempting to do so might cause the restore to fail.
- Progress bytes are not displayed in the Activity Monitor.

Nested container limitations

When restoring a VMware container that contains other containers (that is, a nested container structure), Avamar only restores the top-level of the hierarchy. Consider the following example nested vApp structure:

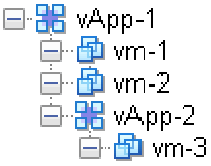


Figure 5 Example nested container structure

When vApp-1 is backed up to Avamar, the vApp backup image will only contain virtual machine backup images for vm-1 and vm-2. When vApp-1 backup is restored, only vm-1 and vm-2 will be present.

Two interim solutions exist for this limitation:

1. Flatten the vApp structure.

   For example, move vm-3 under vApp-2. Then all three virtual machines will be backed up when vApp-1 is backed up.

2. Add both vApp-1 and vApp-2 as separate Avamar clients.

   When restoring, restore vApp-1 first, then restore vApp-2 into vApp-1

Restoring the full image or selected drives to the original virtual machine

NOTICE

If restoring from a template backup, the restore to original virtual machine feature is disabled. It is also disabled if any 6.1 or older proxies are detected in the environment.

To restore the full image or selected drives to the original virtual machine:

1. From the vSphere Client, ensure that the target virtual machine is powered off.
2. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

3. Click the **Restore** tab.

4. Select a client in the clients tree.
5. Locate and select a backup.
6. Click the **Browse for Image Restore** button directly above the contents pane.
7. In the contents pane, do one of the following:
   - Select the **All virtual disks** folder checkbox to restore the entire image.
   - Select one or more drives to only restore those specific drives.
8. Select **Actions › Restore Now...**

   The Restore Options dialog box appears.
9. Select **Restore to original virtual machine** as the restore destination.

   Note: When restoring an image backup to the original virtual machine, the **Configure Destination** button is disabled.
10. (Optional) If you want to restore VMware configuration files, select **Restore virtual machine configuration**.
11. Select one of the following encryption methods for client/server data transfer during this restore:
    - **High**—Strongest available encryption setting.
    - **Medium**—Medium strength encryption.
    - **None**—No encryption.

    Note: The exact encryption technology and bit strength used for any particular client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.
12. Click **More Options**.

    The Restore Command Line Options dialog box appears.
13. Select or clear **Use Changed Block Tracking (CBT) to increase performance.**
14. Select one of the following settings in the **Select Post Restore Options** list:
    - **Do not power on VM after restore.**
    - **Power on VM with NICs enabled.**
    - **Power on VM with NICs disabled.**
15. (Optional) To include additional plug-in options with this restore, configure the Enter Attribute and Enter Attribute Value settings as described in“Plug-in Options” on page 105.
16. 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 advising you that the restored virtual machine might not boot if the virtual machine configuration has changed since the backup was taken.

17. Click **OK**.

    The previous message dialog box closes, and the following message appears:

    ```
    Restore initiated.
    ```

18. Click **Close** to dismiss the message.

Restoring the full image or selected drives to a different (existing) virtual machine

1. In the vSphere Client, ensure that the target virtual machine is powered off.
2. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
3. Click the **Restore** tab.
4. Select a client in the clients tree.
5. Locate and select a backup.
6. Click the **Browse for Image Restore** button directly above the contents pane.
7. In the contents pane:
   - Select the **All virtual disks** folder checkbox to restore the entire image.
   - Select one or more drives to only restore those specific drives.
8. Select **Actions › Restore Now...**

   The Restore Options dialog box appears.
9. Select **Restore to a different (existing) virtual machine** as the restore destination.

   Note: When restoring an image backup to a different (existing) virtual machine, the **Restore virtual machine configuration** option is disabled.
10. Click **Configure Destination**

    The Configure Virtual Machine dialog box appears.
11. Click **Browse**

    The Select VMware Entity 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.
12. Select the destination virtual machine and click **OK**.

The Select VMware Entity dialog box closes.

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

    The Configure Virtual Machine dialog box closes.

14. Switch to **Restore Options** dialog box.

15. Select one of the following encryption methods for client/server data transfer during this restore:

    - **High**—Strongest available encryption setting.
    - **Medium**—Medium strength encryption.
    - **None**—No encryption.

    Note: The exact encryption technology and bit strength used for any particular client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

16. Click **More Options**.

    The Restore Command Line Options dialog box appears.

17. Select or clear **Use Changed Block Tracking (CBT) to increase performance.**

18. Select one of the following settings in the **Select Post Restore Options** list:

    - **Do not power on VM after restore.**
    - **Power on VM with NICs enabled.**
    - **Power on VM with NICs disabled.**

19. (Optional) To include additional plug-in options with this restore, configure the Enter Attribute and Enter Attribute Value settings as described in“Plug-in Options” on page 105.

20. 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 advising you that the restored virtual machine might not boot if the target virtual machine configuration is incompatible with the backup.

21. Click **OK**.

    The previous message dialog box closes, and the following message appears:

    ```
    Restore initiated.
    ```

22. Click **Close**.

Restoring the full image or selected drives to a new virtual machine

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Click the **Restore** tab.

3. Select a client in the clients tree.

4. Locate and select a backup.

5. Click the **Browse for Image Restore** button directly above the contents pane.

6. In the contents pane:

   - Select the **All virtual disks** folder checkbox to restore the entire image.

   - Select one or more drives to only restore those specific drives.

7. Select **Actions › Restore Now...**

   The Restore Options dialog box appears.

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

   Note: When restoring an image backup to a new virtual machine, the **Restore virtual machine configuration** option is selected and disabled because these configuration files are always required to configure the new virtual machine.

9. Click **Configure Destination.**

   The Configure Virtual Machine dialog box appears.

10. Click **Browse.**

    The New Virtual Machine wizard appears.

11. Type a name for the new virtual machine in the **Virtual Machine Name** field.

12. In the tree, select a datacenter and folder location for this new virtual machine.

13. Click **Next.**

    The next New Virtual Machine wizard screen appears.

14. In the tree, select a host/cluster location for this new virtual machine.

15. Click **Finish.**

    The New Virtual Machine wizard screen closes.

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

    The Configure Virtual Machine dialog box closes.

17. Switch to **Restore Options** dialog box.

18. Select one of the following encryption methods for client/server data transfer during this restore:

    - **High**—Strongest available encryption setting.
    - **Medium**—Medium strength encryption.
    - **None**—No encryption.

    Note: The exact encryption technology and bit strength used for any particular client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

19. Click **More Options**.

    The Restore Command Line Options dialog box appears.

20. Select or clear **Use Changed Block Tracking (CBT) to increase performance.**
21. Select one of the following settings in the **Select Post Restore Options** list:

    - **Do not power on VM after restore.**
    - **Power on VM with NICs enabled.**
    - **Power on VM with NICs disabled.**

22. (Optional) To include additional plug-in options with this restore, configure the Enter Attribute and Enter Attribute Value settings as described in“Plug-in Options” on page 105.
23. Click **OK**.

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

    ```
    Restore initiated.
    ```

24. Click **Close**.

Restoring specific folders or files to the original virtual machine

This topic describes how to restore specific folders and files to the original virtual machine.

Where folders and files are actually restored

This topic explains where folder and files will actually be restored on Windows and Linux virtual machines.

Windows virtual machines

When restoring specific folders or files to the original Windows virtual machine (that is, the same virtual machine from which the backup was originally taken), the folders and files are restored to the current drive letter as it exists on the virtual machine at the time of restore (that is, not the folder from which it was originally backed up).

Additionally, file-level restore does not support restoring to original partitions that are currently mapped to a folder, instead of a drive letter. If this is attempted, the following error message will appear:

```
Failed to correlate the VMDK(s) to a Drive Letter
```

Linux virtual machines

For best results when restoring specific folders or files to the original Linux virtual machine (that is, the same virtual machine from which the backup was originally taken), ensure that all partitions on all VMDKs are correctly mounted and that the fstab file, which persists partition remounting on reboot, is correct. This will ensure that files and folders are restored to original locations at the time of backup.

If partitions are not mounted correctly, or the fstab file is not correct, partitions will be prefixed with standard Linux disk designations (for example, sda, sdb, sdc1, sdc2, and so forth). In these situations, folders and files are restored to the relative path from root in the original backup.

Restore procedure

NOTICE

File-level restore requires that all proxies in the vCenter environment be version 6.1 or later. If any 6.0 proxies are detected, file-level restores will be disabled.

NOTICE

You cannot restore more than 5,000 folders or files, nor can you browse more than 14,498 folders or files in the same file-level restore operation. "Guidelines for performing image restores versus file-level restores" on page 76 provides details.

To restore backup data to its original virtual machine location:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

3. Click the **Restore** tab.
4. Select a client in the clients tree.
5. Locate and select a backup.
6. Click the **Browse for Granular Restore** button.
7. Select one or more folders or files you want to restore.
8. Select **Actions › Restore Now...**

   The Restore Options dialog box appears.

9. Select **Restore everything to its original location.**

10. Select one of the following encryption methods for client/server data transfer during this restore:

    - **High**—Strongest available encryption setting.
    - **Medium**—Medium strength encryption.
    - **None**—No encryption.

    Note: The exact encryption technology and bit strength used for any particular client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

11. Click **More Options**.

    The Restore Command Line Options dialog box appears.

12. Select or clear **Use Changed Block Tracking (CBT) to increase performance.**
13. Select one of the following settings in the **Select Post Restore Options** list:

    - **Do not power on VM after restore.**
    - **Power on VM with NICs enabled.**
    - **Power on VM with NICs disabled.**

14. (Optional) To include additional plug-in options with this restore, configure the Enter Attribute and Enter Attribute Value settings as described in“Plug-in Options” on page 105.
15. Click **OK**.

    The Restore Command Line Options dialog box closes.

16. In the Restore Options dialog box, click **OK**.

    The Restore Options dialog box closes.

    The Restore Request dialog box appears showing that a restore request has been initiated.

17. Click **Close**.

    The Restore Request dialog box closes.

Restoring specific folders or files to a different virtual machine

NOTICE

File-level restore requires that all proxies in the vCenter environment be version 6.1 or later. If any 6.0 proxies are detected, file-level restores will be disabled.

NOTICE

You cannot restore more than 5,000 folders or files, nor can you browse more than 14,498 folders or files in the same file-level restore operation. "Guidelines for performing image restores versus file-level restores" on page 76 provides details.

To restore backup data to a different virtual machine location:

1. In the vSphere Client, ensure that the target virtual machine is powered on and fully operational.
2. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
3. Click the **Restore** tab.
4. Select a client in the clients tree.
5. Locate and select a backup.
6. Click the **Browse for Granular Restore** button.
7. Select one or more folders or files you want to restore.
8. Select **Actions › Restore Now...**

   The Restore Options dialog box appears.
9. Select **Restore everything to a different location.**
10. Select the target location for the restored data:

    a. Click **Browse** next to the **Absolute Destination** box.

       The Browse for Restore Client dialog box appears.

    b. Locate and select the destination client.

    c. In the Browse for Folders or Directories pane, expand the tree by clicking **+**.

       The Log into Virtual Machine dialog box appears.

    d. Type virtual machine client login credentials in the User name and Password fields.

       Note: These login credentials must have administration privileges on the virtual machine guest operating system.

    e. Click **Log On**.

       The Log into Virtual Machine dialog box closes.

    f. In the Browse for Restore Client dialog box, browse to and select the destination folder that will receive the restored data.

g. Click **OK**.

   The Browse for Restore Client dialog box closes.

11. In the Restore Options dialog box, select one of the following encryption methods for client/server data transfer during this restore:

    - **High**—Strongest available encryption setting.
    - **Medium**—Medium strength encryption.
    - **None**—No encryption.

    Note: The exact encryption technology and bit strength used for any particular client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

12. Click **More Options**.

    The Restore Command Line Options dialog box appears.

13. Select or clear **Use Changed Block Tracking (CBT) to increase performance.**

14. Select one of the following settings in the **Select Post Restore Options** list:

    - **Do not power on VM after restore.**
    - **Power on VM with NICs enabled.**
    - **Power on VM with NICs disabled.**

15. (Optional) To include additional plug-in options with this restore, configure the Enter Attribute and Enter Attribute Value settings as described in“Plug-in Options” on page 105.

16. Click **OK**.

    The Restore Command Line Options dialog box closes.

17. In the Restore Options dialog box, click **OK**.

    The Restore Options dialog box closes.

    The Restore Request dialog box appears showing that a restore request has been initiated.

18. Click **Close**.

    The Restore Request dialog box closes.

Instant access

If restoring an entire virtual machine from backups stored on a Data Domain system, a special feature called “instant access” is available. Instant access is similar to “Restoring the full image or selected drives to a new virtual machine”as described on page 83, except that the restored virtual machine can be booted directly from the Data Domain system. This reduces the amount of time required to restore an entire virtual machine.

The instant access process works as follows:

1. “Task 1: Restore the virtual machine” on page 89:
   - Instant access is initiated.
   - Selected VMware backup is copied to temporary NFS share on the Data Domain system.
2. “Task 2: Postrestore migration and clean-up” on page 91:
   - From the vSphere Client, power on the virtual machine and initiate a vMotion of the virtual machine to a datastore within the vCenter.
   - When the vMotion is complete, the restored virtual machine files no longer exist on the Data Domain system (they have been vMotioned away).
   - From Avamar Administrator, ensure that the Data Domain NFS share has been deleted.

NOTICE

In order to minimize operational impact to the Data Domain system, only one instant access is permitted at a time. Therefore, it is important to fully clean up and unmount the NFS share after each instant access so that subsequent instant access are not impacted.

Prerequisites

Instant access requires the following:

- Avamar 7.0 or later
- Data Domain Operating System 5.2.1, 5.3.x, and 5.4.x

Task 1: Restore the virtual machine

To restore a virtual machine with instant access, perform the following:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
2. Click the **Restore** tab.
3. Select a client in the clients tree.
4. Locate and select a backup.

5. Click the **Browse for Image Restore** button directly above the contents pane.
6. In the contents pane, select the **All virtual disks** folder checkbox to restore the entire image.
7. Select **Actions › Instant Access.**

   The Restore Options dialog box appears.

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

   Note: When initiating an instant access, the **Restore to original virtual machine** and **Restore to a different (existing) virtual machine** destinations are disabled. The **Restore virtual machine configuration** option is selected and disabled because these configuration files are always required to configure the new virtual machine.

9. Click **Configure Destination.**

   The New Virtual Machine wizard appears.

10. In the **Name and Location** screen, complete the following:

    a. Type a unique name for the new virtual machine in the **Name** field.

    b. Select a datacenter and folder location for this new virtual machine in the Inventory tree.

11. Click **Next.**

    The Summary screen appears.

12. Ensure that the information is correct.
13. Click **Finish.**

    The New Virtual Machine wizard closes.

14. From the **Restore Options** dialog box, complete the following:

    a. Ignore the **Encryption method** setting.

    Note: Because no client/server data transfer takes place, the **Encryption method** setting has no effect.

    b. (Optional) To include additional plug-in options with this restore, click **More Options** and configure the Enter Attribute and Enter Attribute Value settings as described in“Plug-in Options” on page 105.

15. Click **OK.**

    The Restore Command Line Options dialog box closes.

16. Click **OK.**

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

    ```
    Restore request initiated.
    ```

17. Click **Close.**

Task 2: Postrestore migration and clean-up

NOTICE

In order to minimize operational impact to the Data Domain system, only one instant access is permitted at a time. Therefore, it is important to fully clean up and unmount the NFS share after each instant access so that subsequent instant access are not impacted.

To complete the instant access, perform the following:

1. Launch the vSphere Client and log in to the vCenter Server.

   The vSphere Client window appears.

2. Locate the virtual machine you restored in "Task 1: Restore the virtual machine" on page 89.

3. Use vMotion to migrate that virtual machine from the Data Domain NFS share to a datastore within the vCenter.

   When the vMotion is complete, the restored virtual machine files should no longer exist on the Data Domain system (they have been vMotioned away).

   Additionally, the MCS NFS datastore poller automatically unmounts unused Data Domain NFS mounts once daily.

   However, it is still a good practice to ensure that the NFS mount has been unmounted and removed by performing steps 4–7.

4. In Avamar Administrator, click the **Server** launcher button.

   The server window appears.

5. Select the **Data Domain NFS Datastores** tab.

6. Ensure that there is no entry relating to the virtual machine you restored in "Task 1: Restore the virtual machine" on page 89.

7. If an entry is found in step 6, select it and click **Unmount/Remove**.

CHAPTER 6
Troubleshooting

This chapter contains the following topics:

Installation and configuration problems and solutions

The following topics describe common configuration problems and their solutions.

Problems adding vCenter Server as Avamar client

If you encounter problems adding a vCenter Server as an Avamar client, ensure that:

- vCenter hostname, username, and password are correct.
- 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 as described on "Turning off certificate authentication for all vCenter-to-Avamar MCS communications" on page 28.

Proxy network settings

If a proxy was deployed with an incorrect IP address or DNS entry, it might have registered with the Avamar server as localhost instead of the correct hostname.

Because proxies are virtual appliances managed by vCenter, once a proxy registers with the Avamar server, it is difficult to change network settings. Doing so would involve deleting it from the Avamar server, changing the network settings in vCenter, then reactivating it with the Avamar server.

In most cases, the most efficient remedy is to deploy a new proxy with the correct settings, then delete the old proxy from both Avamar and vCenter.

Refer to your vCenter documentation for specific instructions regarding changing virtual appliance network settings.

Backup problems and solutions

The following topics describe common backup problems and solutions.

Backup does not start

If a backup activity fails to start:

- Ensure that an Avamar Image Backup Proxy has been correctly deployed as described in "Deploying proxies" on page 32.
- 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 in to 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.

Backups fail with "No Proxy" or "No VM" errors

If backups fail with "No Proxy" or "No VM" errors, try manually synchronizing Avamar Administrator with the vCenter hosting the virtual machines or proxies, as described in "Manually synchronizing Avamar Administrator with a vCenter" on page 58.

Backup snapshot errors

If backing up virtual machines with multiple disks hosted on different datastores on pre 5.x ESX Servers, you might encounter the following error:

```
"Too many extra snapshot files (%d) were found on the VMs datastore.
   This can cause a problem for the backup or restore."
```

To resolve this condition, you must perform a new backup of the affected virtual machine and include the skip_datastore_check option in the Backup Options dialog box. This will force that backup operation to ignore the snapshot check, which will enable the backup to successfully complete.

To perform a backup using the skip_datastore_check plug-in option:

1. Initiate an on-demand backup of the affected virtual machin as described in "Performing an on-demand backup" on page 72.
2. When you reach the point in the procedure that instructs you to set backup options in the Backup Options dialog box, perform the following additional steps:
   a. Click **More Options**.

      The backup Command Line Options dialog box appears.

   a. Click **More**.

      The Enter Attribute and Enter Attribute Value fields appear.

   b. Type **[avvcbimage]skip_datastore_check** in the Enter Attribute field.
   c. Type **true** in the Enter Attribute Value field.
   d. Click **+**.

      [avvcbimage]skip_datastore_check=true appears in the plug-in options list.

   e. Click **OK**.

      The Backup Command Line Options dialog box closes.
3. Proceed with the remainder of the restore procedure.

Changed block tracking does not take effect

Enabling changed block tracking in Avamar Administrator does not take effect until any of the following actions occur on the virtual machine: reboot, power on, resume after suspend, or migrate.

Therefore, if you enable changed block tracking but do not experience the expected performance increase, use the vSphere Client or vSphere Web Client to locate any virtual machines for which you have enabled changed block tracking, and then perform any of the following actions: reboot, power on, resume after suspend, or migrate.

Restore problems and solutions

The following topics describe common restore problems and solutions.

Preexisting snapshots cause restores to fail

Virtual machine restores will fail if a snapshot for that virtual machine already exists. When this occurs, the restore operation will return an error message similar to the following:

```
2012-12-07 09:30:26 avvcbimage FATAL <0000>: The pre-existing
   snapshots from VMX '[VNXe3300-Datastore1]
   vm-example/vm-example.vmx' will not permit a restore.
2012-12-07 09:30:26 avvcbimage FATAL <0000>: If necessary, use the
   '--skip_snapshot_check' flag to override this pre-existing snapshot
   check.
2012-12-07 09:30:26 avvcbimage Error <9759>: createSnapshot: snapshot
   creation failed
```

To resolve this condition, you must perform a new restore of the affected virtual machine and include the skip_snapshot_check plug-in option in the Restore Options dialog box. This will force that restore operation to overwrite the existing snapshot, which will enable the restore to successfully complete.

To perform a restore using the skip_snapshot_check plug-in option:

1. Initiate an image restore of the affected virtual machine as described in one of the following procedures:
   - "Nested container limitations" on page 79
   - "Restoring the full image or selected drives to a different (existing) virtual machine" on page 81
   - "Restoring the full image or selected drives to a new virtual machine" on page 83
2. When you reach the point in the procedure that instructs you to set restore options in the Restore Options dialog box, perform the following additional steps:

   a. Click **More Options**.

   The Restore Command Line Options dialog box appears.

   a. Click **More**.

   The Enter Attribute and Enter Attribute Value fields appear.

   b. Type **[avvcbimage]skip_snapshot_check** in the Enter Attribute field.

   c. Type **true** in the Enter Attribute Value field.

   d. Click **+**.

   [avvcbimage]skip_snapshot_check=true appears in the plug-in options list.

   e. Click **OK**.

   The Restore Command Line Options dialog box closes.
3. Proceed with the remainder of the restore procedure.

Restore to new virtual machine not available when physical RDM disks are involved

If you back up a virtual machine that has both virtual disks and physical Raw Device Mapping (RDM) disks, the backup will successfully process the virtual disks, bypass the RDM disks.

However, when restoring data from one of these backups, you can restore the data to the original virtual machine, or redirect it to another existing virtual machine. However, you cannot restore data to a new virtual machine.

Note that because the physical RDM disks were not processed during the backup, data residing on the physical RDM disks cannot be restored at all.

If you need to restore data to a new virtual machine, you must:

1. Manually create a new virtual machine in vCenter.

   This new virtual machine must have the same number of virtual disks as the original virtual machine from which the backup was taken.

2. Manually add the new virtual machine to Avamar, as described in "Adding clients and containers" on page 52.

3. Restore the data to this virtual machine, as described in "Restoring the full image or selected drives to a different (existing) virtual machine" on page 81 or "Restoring specific folders or files to a different virtual machine" on page 87.

CHAPTER 7
Protecting the vCenter Management Infrastructure

This chapter describes how to protect the vCenter management infrastructure with Avamar. Topics in this chapter include:

Overview

This chapter covers how to protect the vCenter management infrastructure (not the virtual machines within that environment).

The vCenter runs on a 32- or 64-bit Windows host. It also comprises 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 methodology for protecting vCenter management infrastructure is to implement guest backup on each virtual host. The dataset should only back up the following important 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

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- or 64-bit Windows virtual machine).

Backing up the vCenter management infrastructure

The methodology for protecting vCenter management infrastructure is to implement guest backup 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. The *EMC Avamar Administration Guide* provides details.

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

- “Task 1: Implement guest backups” on page 101
- “Task 2: Define a custom dataset for vCenter backups” on page 101
- “Task 3: Add a backup client for vCenter database hosts” on page 102

Task 1: Implement guest backups

To protect the vCenter management infrastructure with guest backup:

- Install and register Avamar Client for Windows software on the vCenter host as described in the *EMC 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 *EMC Avamar for SQL Server User Guide*.

Task 2: Define a custom dataset for vCenter backups

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

Table 5 Important vCenter management infrastructure components

Component	Default Location
License files	The exact location depends on the specific VMware and Windows version, but is 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	The exact location depends on the specific VMware and Windows version, but is 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	The exact location depends on the specific VMware and Windows version, but is 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	The exact location depends on the specific VMware and Windows version, but is typically one of the following folders: • C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\sysprep • C:\ProgramData\VMWare\VMware VirtualCenter\sysprep

Use of a custom dataset 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- to a 64-bit Windows virtual machine).

1. In Avamar Administrator, select **Tools › Manage Datasets**.

   The Manage All Datasets window appears.

2. Click **New**.

   The New Dataset dialog box appears.

3. Type a name for this new dataset (for example, vCenter-1).

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

4. Click the **Source Data** tab.

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

5. Select **Enter Explicitly** and select the **Windows File System** plug-in from the **Select Plug-In Type** list.

6. In the list of backup targets at the bottom of the dialog box, delete every entry except for the Windows File System plug-in by selecting an entry and clicking **-**.

7. Add each vCenter management infrastructure component to the dataset as follows:

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

8. 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 *EMC Avamar for SQL Server 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 plug-in **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 from Avamar backups

Recovering vCenter management infrastructure from 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. The *EMC Avamar Administration Guide* provides details.

APPENDIX A
vSphere Data Ports

This appendix lists Avamar port usage in a typical vSphere environment. Topics in this chapter include:

Communication ports

All ports are TCP.

Table 6 vSphere communication ports

		VMware		Avamar	
		vCenter	ESX Server	Proxies	Backup Clients
VMware	vCenter	n/a	*V	443‹	n/a
	ESX Server	*V	n/a	902‹	n/a
Avamar	Proxies	n/a	n/a	n/a	n/a
	MCS	› 443	n/a	› 28002 28001‹	› 28002 28001‹

Legend:
*V= Defined by VMware
‹ or › indicates port direction

Listen ports

All ports are TCP unless specifically designated as UDP.

Table 7 vSphere listen ports

		Initiator			
		VMware		Avamar	
		vCenter	ESX Server	Proxies	Utility Node
VMware	vCenter	n/a	*V	443	443
	ESX Server	*V	n/a	902	n/a
Avamar	Proxies	n/a	n/a	n/a	28002
	Utility Node	n/a	n/a	137 (UDP) 138 (UDP) 139 445 27000 28001-28009 29000	n/a

Legend:
*V= Defined by VMware

APPENDIX B
Plug-in Options

The following topics provide information about backup and restore plug-in options for various Avamar for VMware image backup and restore plug-ins:

How to set plug-in options

Plug-in options enable you to control specific actions for on-demand backups, restores, and scheduled backups. The plug-in options that are available depend on the operation type and client plug-in type.

You specify plug-in options for on-demand backup or restore operations or when you create a dataset for a scheduled backup. You can set options by using the graphical controls and by typing options and values in the Enter Attribute and Enter Attribute Value fields.

NOTICE

No error checking or validation is performed on free text entries. Additionally, free text entries override settings made using the graphical controls.

Detailed instructions on how to access and set plug-in options during a backup or restore are available in "Backup" on page 69 and "Restore" on page 75.

Linux VMware Image plug-in options

This topic describes the available options for the Avamar Linux VMware Image plug-in.

Table 8 Linux VMware image backup options

Setting	Description
Use Changed Block Tracking (CBT) to increase performance	If selected, the VMware changed block tracking feature is used to identify areas of the virtual machine file system that have changed since the last backup and only process those changed areas during the next backup. **Note:** Changed block tracking must be enabled at the virtual machine level in order for this feature to work.
Store backup on Data Domain system	To store the backup on a Data Domain system instead of the Avamar server, select the checkbox and then select the Data Domain system from the list. **Note:** To enable this option, add a Data Domain system to the Avamar configuration. The *EMC Avamar and Data Domain Integration Guide* provides instructions.

Table 9 Linux VMware image restore options

Setting	Description
Use Changed Block Tracking (CBT) to increase performance	If selected, the VMware changed block tracking feature is used to identify areas of the virtual machine file system that have changed since the last backup and only process those changed areas during this restore operation. **Note:** Changed block tracking must enabled at the virtual machine level in order for this feature to work.

Windows VMware Image plug-in options

This topic describes the available options for the Avamar Windows VMware Image plug-in.

Table 10 Windows VMware image backup options

Setting	Description
Use Changed Block Tracking (CBT) to increase performance	If selected, the VMware changed block tracking feature is used to identify areas of the virtual machine file system that have changed since the last backup and only process those changed areas during the next backup. **Note:** Changed block tracking must be enabled at the virtual machine level in order for this feature to work.
Store backup on Data Domain system	To store the backup on a Data Domain system instead of the Avamar server, select the checkbox and then select the Data Domain system from the list. **Note:** To enable this option, add a Data Domain system to the Avamar configuration. The *EMC Avamar and Data Domain Integration Guide* provides instructions.

Table 11 Windows VMware image restore options

Setting	Description
Use Changed Block Tracking (CBT) to increase performance	If selected, the VMware changed block tracking feature is used to identify areas of the virtual machine file system that have changed since the last backup and only process those changed areas during this restore operation. **Note:** Changed block tracking must enabled at the virtual machine level in order for this feature to work.

Linux VMware File-level Restore plug-in options

Backup operations are not supported by the Avamar Linux VMware File-level Restore plug-in, and no user-configurable restore options are available.

Windows VMware File-level Restore plug-in options

Backup operations are not supported by the Avamar Windows VMware File-level Restore plug-in, and no user-configurable restore options are available.

INDEX