Avamar 7.3 for VMware

User Guide

302-002-865

REV 02

Published April 2018

Dell 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.“ DELL 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 DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Published in the USA.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

FIGURES

TABLES

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Some versions of the software or hardware currently in use do not support every function that this document describes. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document contact an EMC technical support professional.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.EMC.com) to find 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

Revision	Date	Description
02	April 23, 2018	Updated port tables.
01	April, 2016	GA release of Avamar 7.3

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 Guide*
- *EMC Avamar Product Security Guide*
- *EMC Avamar Backup Clients User Guide*

- *EMC Avamar for Exchange VSS User Guide*
- *EMC Avamar for IBM DB2 User Guide*
- *EMC Avamar for Lotus Domino User Guide*
- *EMC Avamar for Oracle User Guide*
- *EMC Avamar for SharePoint VSS User Guide*
- *EMC Avamar for SQL Server User Guide*

The following VMware publications provide additional information:

- *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*

Special notice conventions used in this document

EMC uses the following conventions to alert the reader to particular information.

NOTICE

The Notice convention emphasizes important information about the current topic.

Note

The Note convention addresses specific information that is related to the current topic.

Typographical conventions

In this document, EMC uses the typographical conventions that are shown in the following table.

Table 2 Typographical conventions

Convention	Example	Description
Bold typeface	Click **More Options**.	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what a user specifically selects or clicks).
Italic typeface	*EMC Avamar Administration Guide*	Use for full titles of publications that are referenced in text.
Monospace font	`Event Type = INFORMATION`	Use for: • System code

Table 2 Typographical conventions (continued)

Convention	Example	Description
	`Event Severity = OK Event Summary = New group created`	• System output, such as an error message or script • Pathnames, file names, prompts, and syntax • Commands and options
Monospace font with italic typeface	Type ***`Avamar_server`***, where *Avamar_server* is the DNS name or IP address of the Avamar server.	Use for variables.
Monospace font with bold typeface	Type **`yes`**.	Use for user input.
Square brackets	**`[--domain=String(/)] --name=String`**	Square brackets enclose optional values.
Vertical bar	**`[--domain=String(/)] | --name=String`**	Vertical bar indicates alternate selections - the bar means “or”.
Braces	**`{[--domain=String(/)] | --name=String}`**	Braces enclose content that the user must specify.
Ellipses	`valid hfs ...`	Ellipses indicate nonessential information that is 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 upper 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 to supplement the information in 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 **Search** 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 **Search**.

Online communities
Go to EMC Community Network at http://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 an EMC sales representative for details about obtaining a valid support agreement or with questions about an 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**.

Enhancing 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 sends configuration, capacity, and general system information to EMC Customer Support.

Comments and suggestions
Comments and suggestions help EMC to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to DPAD.Doc.Feedback@emc.com.

Please include the following information:

- Product name and version
- Document name, part number, and revision (for example, 01)

- Page numbers
- Other details to help address documentation issues

CHAPTER 1

Introduction

This chapter includes the following topics:

Data protection overview

EMC® Avamar® offers two basic ways to protect data residing on VMware virtual machines:

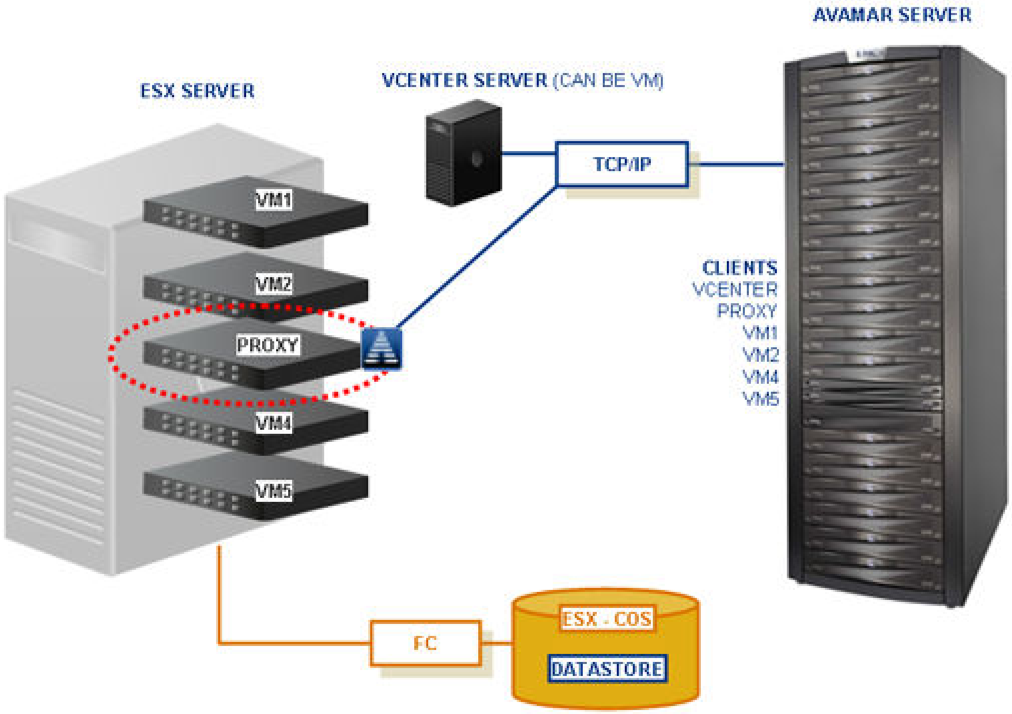
- Image backup
- Guest backup

Image backup

Image backup uses VMware vStorage API for Data Protection (VADP) to protect virtual machine data.

Image backup is fully integrated with vCenter Server to provide detection of virtual machine clients, and enable efficient centralized management of backup jobs.

Figure 1 Image backup diagram



Proxies

Image backups and restores require deployment of proxy virtual machines within the vCenter.

Proxies run Avamar software inside a Linux virtual machine, and are deployed using an appliance template (`.ova`) file or the Proxy Deployment Manager.

Once deployed, each proxy provides these 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

Each proxy is capable of performing eight simultaneous backup or restore operations, in any combination.

Proxies are allowed in any part of the Avamar Administrator account management tree except the vCenter Server domain or subdomains. Additionally, you should not activate proxies into the root domain (`/`), as this will cause problems during system migration.

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 take noticeably longer than if the proxy and the target virtual machine are both located in the same datacenter. Therefore, for best performance, use the Proxy Deployment Manager to recommend the ideal deployment configuration.

Snapshots

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

If the virtual machine is running at the time of backup, this snapshot can impact disk I/O and consume disk space on the datastore in which the virtual machine resides. Snapshot creation and deletion can take a long time if the virtual machine runs a heavy disk I/O workload during backup

Avamar image backup supports the following types of virtual disks:

- Flat (version 1 and 2)
- Raw Device Mapped (RDM) in virtual mode only (version 1 and 2)
- Sparse (version 1 and 2)

Other virtual disk types are not supported.

Supported storage architectures

Image backup fully supports the following storage architectures:

- Fiber channel SAN storage hosting VMFS or RDMS
- iSCSI SAN storage
- NFS

Image backup system limitations

The following system-wide limitations apply to image backups.

Special characters are not allowed in datacenter, datastore, folder, or virtual machine names

Because of a known limitation in the vCenter software, when special characters are used in the datacenter, datastore, folder, or virtual machine names, the `.vmx` file is not included in the backup.

This issue is seen when special characters like %, &, *, $, #, @, !, \, /, :, *, ?, ", <, >, |, ;, ',+,=,?,~ are used.
As a long-term solution for this issue, upgrade the VMware software to a version where this issue is resolved. However, until a fix is provided by VMware, rename the datacenter, datastore, folder, or virtual machine names without using these special characters.

Avamar server upgrades require proxy reboots
After you upgrade Avamar server software, you must manually reboot all proxies connected to that server.

Guest backup

Guest backup protects virtual machine data by installing Avamar client software on the 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.

Note

When registering virtual machine clients protected by guest backup, do not register them to a vCenter domain. Doing so prevents the administrator 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 table lists Avamar client guides, which provide detailed instructions for installing Avamar client software in virtual machines.

Table 3 Guest backup installation resources

Client	Publication
IBM AIX file systems	*EMC Avamar Backup Clients User Guide*
Linux file systems: • Debian • CentOS • Red Hat • SUSE • Ubuntu	*EMC Avamar Backup Clients User Guide*
Novell NetWare file systems	*EMC Avamar Backup Clients User Guide*
UNIX file systems: • FreeBSD • HP-UX • SCO Open Server and UnixWare • 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 VSS User Guide*
Microsoft Office SharePoint implementations	*EMC Avamar for SharePoint VSS User Guide*
Microsoft SQL Server databases	*EMC Avamar for SQL Server User Guide*
Microsoft Windows file systems	*EMC Avamar Backup Clients User Guide*

Table 3 Guest backup installation resources (continued)

Client	Publication
Oracle databases hosted on IBM AIX, Red Hat, and SUSE Linux, Sun Solaris, and Microsoft Windows	*EMC Avamar for Oracle User Guide*

Considerations

These are the various considerations of using either image or guest backup to protect virtual machine data.

General use case guidelines

For virtual machines hosted in a vCenter, image backup enables you to protect multiple virtual machines with the least amount of effort.

On Windows Vista/2008 and later virtual machines, image backups are fully application-consistent and sufficient for most use cases involving Microsoft Exchange, Microsoft Office SharePoint, and Microsoft SQL Server. However, because image backup is limited to functionality offered by the VMware vStorage API for Data Protection (VADP), some deployments might require more advanced functionality than that offered by VADP. In these situations, the additional functionality provided by guest backup might offer a better solution.

The following deployments are known to benefit from using guest backup instead of image backup:

- Exchange Database Availability Groups (DAGs)
- SharePoint Server Farms
- SQLServer Clusters
- Exchange, SharePoint and SQLServer deployments requiring log truncation

Guest backup is the only way to protect virtual machines that are not hosted in a vCenter (for example, desktops and laptops).

Ease of implementation

Image backup:

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

Guest backup:

- 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.

Efficiency

Image backup:

- Offers moderate deduplication efficiency.
- Does not consume guest virtual machine CPU, RAM, and disk resources during backups.
- Does consume ESX Server CPU, RAM, and disk resources during backups.

Guest backup:

- Offers the highest level of data deduplication efficiency.
- Does consume small amounts of guest virtual machine CPU, RAM, and disk resources during backups.
- Does not consume ESX Server CPU, RAM, and disk resources during backups.

Backup and restore

Image backup:

- Image backups are supported for all machines currently supported by VMware.
- Backups can comprise an entire virtual machine image (all drives) or selected drives (`.vmdk` files).
- Individual folder and file restores supported for both Windows and Linux virtual machines.
- Backups are not optimized (temp files, swap files, and so forth are included).
- Unused file system space is backed up.
- Virtual machines need not have a network connection to Avamar server.
- Virtual machines need not be running for backups to occur.

Guest backup:

- Backups are highly optimized (temp files, swap files, and so forth are 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 for all supported virtual machines (not just Linux and Windows)
- Backup and restore jobs can execute pre- and post-processing scripts.
- Virtual machines must have a network connection to Avamar server.
- Virtual machines must be running for backups to occur.

Required VMware knowledge

Image backup requires moderate VMware knowledge. Integrators should have working knowledge of the 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.

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

Using both image and guest backup

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.

In order to support using both image and guest backup to protect the same virtual machine, you must configure the Avamar MCS to allow duplicate client names.

Changed block tracking

Changed block tracking is a VMware feature that tracks which 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 types of virtual disk formats:

- Virtual machine versions 7 and later
  The earlier virtual machine 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. vCenter online help provides 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 does not take effect until any of the following actions occur on the virtual machine: reboot, power on, resume after suspend, or migrate.

Image backup virtual machine quiescing

Image backup does not provide any additional virtual machine quiescing capabilities other than those provided by VMware vStorage API for Data Protection (VADP).

Prior to performing an image 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 Vista/2008 and later virtual machines that are running VMware Tools. Additionally, for application-consistent quiescing to be available, the following conditions must be met:

- This issue is seen when special characters like

  %, &, *, $, #, @, !, \, /, :, *, ?, ", <, >, |, ;, '
  etc are contained in names of vSphere entities like virtual machine name, cluster name, datastore/folder/file name etc.

  The UUID attribute must be enabled. This is enabled by default on virtual machines created on ESX hosts.
- The virtual machine must use only SCSI disks.
- The virtual machine cannot use dynamic disks.

CHAPTER 2

Configuration and Setup

This chapter includes the following topics:

Best practices

Follow these best practices when configuring your system.

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 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
When protecting high change rate clients, such as database hosts, use guest backup, or store image backups on a Data Domain system.

(Optional) Configuring support for multiple vCenters

By default, Avamar 7.1 and later servers support protecting up to 15 vCenters with no additional configuration required. However, if you will be protecting more than 15 vCenters, or if your Avamar server was upgraded from the previous version, some manual configuration is required.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For 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. Ensure that the max_number_of_vcenters setting is equal to or greater than the number of vCenters you intend to protect:

   a. Find the max_number_of_vcenters entry key.

   b. Change the max_number_of_vcenters setting to ***num***, where *num* is an integer equal to or greater than the number of vCenters you intend to protect.

   For example, this setting allows as many as 15 vCenters to be protected by this Avamar server:

   ```
   <entry key="max_number_of_vcenters" value="15" />
   ```
5. If protecting 50 or more vCenters, also change the maxJavaHeap setting to -**Xmx2G**:

   a. Find the maxJavaHeap entry key.

   b. Change the maxJavaHeap setting to **-Xmx2G**:

   ```
   <entry key="maxJavaHeap" value="-Xmx2G" />
   ```

6. Close `mcserver.xml` and save your changes.
7. Start the MCS and the scheduler by typing:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

Installing Avamar Administrator software

Install Avamar Administrator software on your Windows computer.

Procedure

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

   `https://`*`Avamar-server`*

   where *Avamar-server* is the Avamar server network hostname or IP address.

   The **EMC Avamar Web Restore** page appears.
2. Click **Downloads**.
3. Navigate to the folder containing 32-bit Windows software installation packages.
4. Locate the Java Runtime Environment (JRE) install package (it is typically the last entry in the folder).
5. If the JRE on the client computer is older than the JRE hosted on the Avamar server, download and install the newer JRE:

   a. Click the **jre-*version*-windows-i586-p** link.

   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.
6. Click the **AvamarConsoleMultiple-windows-x86-*version*.exe** link.
7. Open the installation file, or download the file, and then open it from the saved location.
8. Follow the onscreen instructions to complete the Avamar Administrator software installation.

Configuring vCenter-to-Avamar authentication

Configure vCenter-to-Avamar authentication for each vCenter you intend to protect.

The most secure method for configuring vCenter-to-Avamar authentication is to add vCenter authentication certificates to the Avamar MCS keystore. You must do this for each vCenter you intend to protect .

If you do not want to add vCenter authentication certificates to the Avamar MCS keystore, you must disable certificate authentication for all vCenter-to-Avamar MCS communications.

Adding vCenter authentication certificates to the MCS keystore

Configure vCenter-to-Avamar authentication by adding a vCenter authentication certificate to the MCS keystore. Do this for each vCenter you intend to protect.

This procedure uses the java `keytool` utility, which manages certificate keys. The `keytool` utility is located in the Java bin folder (`/usr/java/`*`version`*`/bin`), where *version* is the 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`.

Procedure

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

   The following table lists the default locations for vCenter certificates.

   Table 4 Default vCenter certificate locations

vCenter host OS	Default certificate location
Windows 2008 and above	`C:\ProgramData\VMware \vCenterServer\cfg\certs`
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. Copy the MCS keystore to `/tmp` by typing:

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

   This creates a temporary version of the live MCS keystore in `/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. Type the keystore password.
8. Type **`yes`**, and press **Enter** to trust this certificate.
9. (Optional) If you will be protecting more than one vCenter with this Avamar server, add those vCenter certificates now.

10. 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.

11. Copy the temporary MCS keystore to the live location by typing:

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

12. Exit the root subshell by typing **exit**.
13. Start the MCS and the scheduler by typing:

    ```
    dpnctl start mcs
    dpnctl start sched
    ```

Disabling MCS certificate authentication

If you do not want to add vCenter authentication certificates to the Avamar MCS keystore, you must disable certificate authentication for all vCenter-to-Avamar MCS communications.

Procedure

1. Open a command shell and log in by using one of the following methods:
    - For a single-node server, log in to the server as admin.
    - For 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. Find the ignore_vc_cert entry key.
5. Change the ignore_vc_cert setting to **true**.

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

6. Close mcserver.xml and save your changes.
7. Start the MCS and the scheduler by typing:

    ```
    dpnctl start mcs
    dpnctl start sched
    ```

Creating a dedicated vCenter user account

EMC strongly recommends that you set up a separate user account on each vCenter 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.

Note

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

Procedure

1. Create a vCenter user account with privileges listed in the following table.

   Note

   You must create this user account at the vCenter level. If you create it at any other level (for example, at a datacenter level), backups will fail.

Table 5 Minimum required vCenter user account privileges

Privilege type	vCenter 6.0	vCenter 5.5/5.5U2	vCenter 5.1
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 • 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
Extension	• Register extension • Unregister extension • Update 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 • Set custom attribute • Settings	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Set custom attribute • Settings	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Set custom attribute • Settings
Host			• Configuration > Storage partition configuration
Network	• Assign network • Configure	• Assign network • Configure	• Assign network • Configure

Table 5 Minimum required vCenter user account privileges (continued)

Privilege type	vCenter 6.0	vCenter 5.5/5.5U2	vCenter 5.1
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
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 • Configure managed by • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Set annotation • Settings • Swapfile placement • Upgrade virtual machine compatibility	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Configure managed by • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Set annotation • Settings • Swapfile placement • Upgrade virtual machine compatibility	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource • Configure managed by • Disk change tracking • Disk Lease • Extend virtual disk • Host USB device • Memory • Modify device settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility
Guest Operations	• Guest Operation Modifications	• Guest Operation Modifications	• Guest Operation Modifications

Table 5 Minimum required vCenter user account privileges (continued)

Privilege type	vCenter 6.0	vCenter 5.5/5.5U2	vCenter 5.1
	• Guest Operation Program Execution • Guest Operation Queries	• Guest Operation Program Execution • Guest Operation Queries	• 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	• Console interaction • DeviceConnection • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install
Inventory	• Create from existing • Create new • Register • Remove • Unregister	• Create from existing • Create new • Register • Remove • Unregister	• Create from existing • Create new • Register • Remove • Unregister
Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Clone virtual machine • Mark as template	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Clone virtual machine • Mark as template	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Clone virtual machine • Mark as Template
Snapshot Management	• Create snapshot • Remove snapshot • Revert to snapshot	• Create snapshot • Remove snapshot • Revert to snapshot	• Create snapshot • Remove snapshot • Revert to snapshot

Adding a vCenter client

You must add each vCenter you intend to protect as an Avamar client in Avamar Administrator.

Procedure

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

   The **Administration** window appears.

2. Click the **Account Management** tab.
3. In the tree, select the top-level (root) domain, and then select **Actions** > **Account Management** > **New Client(s)**.

The **New Client**dialog box appears.

4. Complete the following settings:

    a. Select **VMware vCenter** in the **Client Type** list.

    b. Type the vCenter fully qualified DNS name or IP address in the **New Client Name or IP** field.

    c. Type the vCenter web services listener data port number in the **Port** field.

    443 is the default setting.

    d. Type the vCenter user account name in the **User Name** field.

    e. Type the vCenter user account password in the **Password** field.

    f. Type the vCenter user account password again in the **Verify Password** field.

    g. (Optional) Type a contact name in the **Contact** field.

    h. (Optional) Type a contact telephone number in the **Phone** field

    i. (Optional) Type a contact email address in the **Email** field.

    j. (Optional) Type a contact location in the **Location** field.

5. Click **OK**.

Results

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 vCenter Server domain hierarchy.
- Creates a VirtualMachines subdomain within that vCenter Server domain hierarchy.
- 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.

If the vCenter was already registered as a normal backup client (for example, to support guest level backup), attempting to add that same vCenter as a vCenter client will fail because the system will not allow you to register the same client twice. If this occurs, you must:

1. Retire the existing vCenter client in Avamar Administrator.
2. Add the vCenter as a vCenter client (using this procedure).
3. Reinvite the retired vCenter client as a normal client to support guest level backup from the vCenter Server.

Deploying proxies

Deploy one or more proxies on each vCenter you intend to protect with image backup.

Proxy Deployment Manager

Proxy Deployment Manager is an Avamar Administrator feature that assists administrators with deploying and managing Avamar proxies in vCenter environments.

Beginning with Avamar 7.2, Proxy Deployment Manager is the preferred method for deploying proxies. Manual proxy deployment is still supported if necessary.

When you select a vCenter from the list, the tree pane shows the vCenter topology. Any existing proxies that were previously deployed with Proxy Deployment Manager are shown beneath ESX hosts.

The **Recent Tasks** pane shows status for all deployment tasks in the past two hours.

You can cancel tasks that have not completed by selecting the task and clicking **Cancel**.

Functional overview

Proxy Deployment Manager assists administrators with proxy deployment by offering a recommendation as to the number of proxies that should be deployed in each vCenter, and a recommended ESX host location for each proxy.

When generating a recommendation, Proxy Deployment Manager performs a static point-in-time analysis of the virtual infrastructure. This analysis gathers data about the virtual infrastructure, such as the number of virtual machines, the number of datastores, and the number of virtual machines hosted in each datastore.

Users specify a data change rate and backup window duration for their site.

Proxy Deployment manager then calculates the optimum number of proxies required to back up those virtual machines in the time allotted by the backup window. Proxy Deployment Manager also considers the datastore and ESX host topology, and suggests an optimal ESX host location for each proxy so that all datastores are protected.

This calculated proxy deployment topology is offered as a recommendation. This recommendation can be accepted as offered, or modified to meet specific site requirements.

Before proxies can be deployed, each recommended proxy must be configured by specifying:

- Proxy name
- Avamar server domain where the proxy will reside
- Proxy IP address
- Datastore assignment
- Network settings:
  - Which existing virtual network to use
  - DNS server(s)
  - Network gateway
  - Network mask

After all proxies are configured, clicking **Apply** creates the proxy virtual machines with the specified configuration settings.

You can generate new proxy deployment recommendations at any time. This is useful for periodically reevaluating and optimizing proxy deployments when significant changes have occurred in the virtual infrastructure.

Considerations and best practices

Proxy Deployment Manager has been intentionally designed to ensure broad compatibility with most customer environments. This necessitated making certain design assumptions about typical customer environments and reasonable proxy capabilities in those environments. Understanding these design assumptions can help you to better understand Proxy Deployment Manager's recommendations in order to potentially further optimize proxy deployment at your site. Some best practices are also discussed.

Data change rate

The data change rate is the percentage of a client file system that actually changes between backups. Data change rates directly impact the number of proxies required to successfully back up all required virtual machines in the time allotted by the backup window. More data to be backed up requires more time, more proxies, or both.

Even though empirical field data routinely reports client data change rates of 3-4% per day, by default Proxy Deployment Manager assumes a client data change rate of 12% per day. The intentionally conservative use of 12% as a design assumption provides a buffer.

If client data change rates at your site are routinely lower or higher than these assumed values, you can add or delete proxies as needed. You can also shorten or lengthen the backup window.

Proxy data ingestion rate

Proxy data ingestion rate is another parameter that directly impacts the number of proxies required to successfully back up all required virtual machines in the time allotted by the backup window. By default, Proxy Deployment Manager assumes that each proxy can run 8 concurrent backup jobs and process 500 GB of data per hour.

While an assumed proxy data ingestion rate of 500 GB per hour is a very conservative estimate, a number of factors at each customer site directly affect the actual proxy data ingestion rate. Some of these factors are the:

- Avamar server architecture (physical Avamar server using a Data Domain system for back end storage versus a virtual Avamar server hosted in vCenter)
- Type of storage media used for proxy storage
- Network infrastructure and connectivity speed
- SAN infrastructure and connectivity speed

If proxy data ingestion rates at your site are routinely lower or higher than 500 GB per hour, you can add or delete proxies as needed. You can also shorten or lengthen the backup window.

If your site consistently experiences substantially different proxy data ingestion rates (that is, either substantially lower or higher than 500 GB per hour), you can permanently change the default proxy data ingestion rate setting, which will affect all future proxy deployment recommendations. To do this:

1. Open a command shell and log in to the Avamar server as user **`admin`**.
2. Switch user to root by typing `su -` .
3. Open `/etc/vcs/dm.properties` in a UNIX text editor.
4. Change the `proxy_ingest_rate_gb_per_hour` setting.
5. Save your changes and close `/etc/vcs/dm.properties`.

Protecting against proxy over commit
By default, each Avamar proxy is configured to allow 8 concurrent backup jobs. This setting is known to work well for most customer sites.

EMC recommends against increasing the number of concurrent jobs to more than 8 because it can lead to a condition in which too many backup jobs are queued for a given proxy (proxy over commit). This causes uneven distribution of backup jobs among proxies, and can also cause a bottleneck in which backup jobs to take longer to complete than they otherwise might.

Some sites might benefit from configuring some proxies to allow fewer concurrent backup jobs. This generally requires deploying additional proxies, but can result in more even distribution of backup jobs among proxies, as opposed to concentrating or clustering backups in a certain area of the virtual infrastructure.

Optimization for level-1 incremental change block backups
When Proxy Deployment Manager generates a proxy deploy recommendation, it does so by calculating how many proxies are required to sustain normal backup operations. One of the assumptions about normal backup operation is that backups will be level-1 incremental or changed block backups, not level-0 full backups.

Level-0 backups inherently take longer and use more proxy resources. Therefore, large new virtual machine deployments can adversely affect the ability to complete all required backups in the time allotted by the backup window.

For this reason, whenever possible phase-in large new virtual machine deployments in order to give the system an opportunity to ingest the necessary level-0 backups.

If a phased-in deployment is not possible, another approach is to tolerate the failed backups that will occur due to proxy over commit. Once the system begins to settle, proxy resources will be under committed, and those virtual machines will eventually be backed up. Administrators should monitor the situation closely to ensure that the system does settle and that the virtual machines eventually do successfully back up.

Note

Avamar will attempt to deploy proxies where needed, but it is impossible to know all details about the environment so it is important you verify the proxy deployment manager does not over allocate proxies beyond the maximum supported.

Deploying proxies with Proxy Deployment Manger

Procedure

1. In Avamar Administrator, select **VMware** > **Proxy Deployment Manger**.

   The **Proxy Deployment Manger** window appears.

2. **Choose a vCenter**.
3. Complete the following settings:

   a. Set the **Data change rate**.

      The default data change rate of 12% (**.12**) is a conservative setting that is known to work with most customer sites.

   b. Set the **Backup window minutes**.

   c. To include virtual machines using direct attached storage in this recommendation, select **Protect VM's on local storage**.

      This will ignore VM's on clustered-host local storage.

4. Click **Create Recommendation**.

   The tree pane shows the proposed deployment topology. Proposed new proxies appear under each ESX host with the name **New proxy**.

5. For each recommended proxy you intend to deploy, configure the proxy as follows:

   a. In the tree pane, select a **New proxy**.

   b. Click **Edit**.

      The **New Proxy** dialog box appears.

   c. Type the proxy name in the **Name** field.

   d. Select an Avamar server **Domain** where this proxy will reside.

   e. Type the IP address in the **IP** field.

   f. Select a datastore from the **Datastore** list.

   g. Select a virtual network from the **Network** list.

   h. Type the fully qualified DNS server name or IP address in the **DNS String** field.

   i. Type the network gateway IP address in the **Gateway** field.

   j. Type the network mask in the **Netmask** field.

   k. Click **Save**.

6. (Optional) Add other proxies you want to deploy:

   Note

   You must be prepared to specify the proxy name, IP address, fully qualified DNS server name or IP address, network gateway and network mask for each proxy you add.

   ---

   a. In the tree pane, select an ESX host.

   b. Click **New Proxy**.

      The **New Proxy** dialog box appears.

   c. Type the proxy hostname in the **Name** field.

   d. Select an Avamar server **Domain** where this proxy will reside.

   e. Type the IP address in the **IP** field.

   f. Select a datastore from the **Datastore** list.

   g. Select a virtual network from the **Network** list.

   h. Type the fully qualified DNS server name or IP address in the **DNS String** field.

   i. Type the network gateway IP address in the **Gateway** field.

   j. Type the network mask in the **Netmask** field.

   k. Click **Save**.

7. (Optional) Delete any proxies you do not want to deploy:

   a. In the tree pane, select a proxy.

   b. Click **Delete**.

   c. Click **Yes** to confirm the deletion.

8. When the proposed deployment topology is satisfactory, click **Apply** to deploy the proxies.

Results

If a proxy fails to deploy for any reason, it is completely deleted from the system. That hostname and IP address will be available for subsequent proxy deployments.

(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 or chained permission 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 or chained permission 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 or chained permission file.
4. Open `/usr/local/avamarclient/var/avvcbimageAll.cmd` in a UNIX text editor.
5. Append the following entry to the end of the file:

   ```
   --ssl_server_authentication_file=/usr/local/
   avamarclient/bin/certificate-file
   ```

   where *certificate-file* is the actual certificate name.
6. Save the changes and close `avvcbimageAll.cmd`.
7. Open `/usr/local/avamarclient/var/avvmwfileAll.cmd`in a UNIX text editor.
8. Append the following entry to the end of the file:

   ```
   --ssl_server_authentication_file=/usr/local/
   avamarclient/bin/certificate-file
   ```

   where *certificate-file* is a standalone certificate or chained permission file.

9. Save the changes and close `avvmwfileAll.cmd`.
10. Open `/etc/vmware/config` in a UNIX text editor.
11. Append the following lines to the end of the file:

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

    where *certificate-file* is a standalone certificate or chained permission file.
12. Save the changes and close `config` in a UNIX text editor.
13. Open `/usr/local/avamarclient/var/vddkconfig.ini`in a UNIX text editor.
14. Find the `vixDiskLib.linuxSSL.verifyCertificates=0` entry.
15. Change the value of the `vixDiskLib.linuxSSL.verifyCertificates=0` entry to `1`.

    ```
    vixDiskLib.linuxSSL.verifyCertificates=1
    ```
16. Save the changes and close `vddkconfig.ini`.
17. Ensure that there are no running backup or restore jobs on this proxy.
18. Restart the `avagent` and `vmwareflr` services by typing:

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

After you finish

Repeat this procedure for each Avamar proxy.

Upgrading proxies

Upgrading Avamar proxies from release 7.2 or newer

Use this procedure to upgrade Avamar proxies from release 7.2 or newer to release 7.3 or newer.

Procedure

1. In Avamar Administrator, select **VMware** > **Proxy Deployment Manger**.

   The **Proxy Deployment Manger** window appears.
2. Choose a vCenter.

   Existing proxies in the topology tree for the selected vCenter that need to be upgraded will be indicated with a **!** symbol as well as a tooltip that indicates that the proxy has an update pending.
3. Click Apply to upgrade the proxies.

Upgrading Avamar proxies from releases prior to release 7.2

This section provides information and procedures for upgrading Avamar proxy software when existing proxies are at a release level prior to release 7.2.

7.0 proxy compatibility with upgraded 7.3 servers

You cannot use both 7.0 and 7.3 proxies with the same Avamar server.

Each 7.0 proxy hosts eight separate `avagent` plug-ins, each of which can process one backup or restore job. Each 7.0 proxy can therefore process as many as eight simultaneous backup or restore jobs.

Each 7.3 proxy hosts a single `avagent` plug-in, but that single `avagent` plug-in can perform up to eight simultaneous backup or restore jobs. The maximum simultaneous job limitation is still eight.

In order to precisely control the maximum number of simultaneous jobs allowed for each proxy, Avamar 7.3 introduced a new setting in `mcserver.xml`: `max_jobs_per_proxy`. The default setting is 8.

You cannot use both 7.0 and 7.3 proxies with the same Avamar server. This is because the Avamar server `max_jobs_per_proxy` setting is global. It applies to every proxy in the environment. Therefore, in a heterogeneous environment comprising both 7.0 and 7.3 proxies, a `max_jobs_per_proxy=8` setting would work fine for 7.3 proxies, but might result in 7.0 proxies attempting to process as many as 64 simultaneous backup or restore jobs (that is, eight jobs for each of the eight `avagent` processes). This might cause degraded performance. Similarly, a `max_jobs_per_proxy=1` setting would work fine for 7.0 proxies, but would limit 7.3 proxies to performing only one backup or restore job at a time. This would drastically underutilize each 7.3 proxy.

These proxy compatibility issues only affect customers who upgrade their Avamar 7.0 servers to 7.3. Customers deploying new 7.3 servers in their environments will deploy new 7.3 proxies. Customers using existing 7.0 servers will already have 7.0 proxies in their environment, and can deploy additional 7.0 proxies to support that server.

EMC suggests the following solutions for these proxy compatibility issues:

- If 7.3 proxies will be deployed, the preferred solution is to upgrade all existing 7.0 proxies to 7.3.
- If new 7.3 proxies will never be simultaneously deployed with the existing 7.0 proxies, change the `mcserver.xml` `max_jobs_per_proxy` setting to **1**.

Existing proxy configuration

The following information should be gathered prior to upgrading proxies in order to restore the proxy settings to the values that existed prior to the upgrade:

- VM container
  - Name
  - Host
  - Datastore
  - Network
  - Folder
- VM client
  - IP address
  - Gateway
  - DNS servers
  - Netmask

- Policy
  - Domain
  - Datastores protecting
  - Group membership

The following example charts demonstrate how this information should be gathered prior to upgrading proxies:

Table 6 Example chart for gathering proxy information

Name	Host	Datastore	Network	Folder	IP
Proxy1	vcenter.com/ host1	DS2	NW1	/proxies	x.x.x.x
Proxy2	vcenter.com/ host2	DS2	NW1	/proxies	x.x.x.x

Table 7 Example chart for gathering proxy information, continued

Gateway	DNS	Netmask	Domain	Datastore protecting	Groups protecting
x.x.x.x	x.x.x.x,x.x.x.x	x.x.x.x	/clients	DS1,DS2	Default Virtual Machine Group
x.x.x.x	x.x.x.x,x.x.x.x	x.x.x.x	/clients	DS1,DS2	Other Group

Viewing VM configuration

Procedure

1. In the vSphere Client or vSphere Web Client, navigate to **VMs and Templates** view.
2. Locate existing proxies. For each proxy:

   a. Note the VM and folder names.

   b. Select the **Summary** tab.

   c. Note the host, storage (datastore) and network.

   d. Right click and select **Edit Settings...**.

   - If using the vSphere Web Client, navigate to the **vApp Options** tab and note the IP, gateway, DNS, and netmask.
   - If using the vSphere Client (Windows):

   a. Navigate to the **Options** tab.

   b. Select **vApp Options > Advanced**.

   The right pane shows the vApp option fields.

   c. Click **Properties > Properties** in the right pane.

   The **Advanced Properties Configuration** window appears.

d. From the Properties table, note the IP address, gateway, DNS, and netmask values from the **Value** column corresponding to the following keys in the **Key** column:

Key	Value
vami.ip0.EMC_Avamar_Virtual_Machine_Combined_Proxy	IP address
vami.gateway.EMC_Avamar_Virtual_Machine_Combined_Proxy	Gateway
vami.DNS.EMC_Avamar_Virtual_Machine_Combined_Proxy	DNS servers
vami.netmask0.EMC_Avamar_Virtual_Machine_Combined_Proxy	Netmask

Viewing datastore assignments and group membership

Procedure

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

   The **Administration** window appears.
2. Click the **Account Management** tab.
3. Locate the proxy and note the domain.
4. Select a proxy and click **Edit**.

   The **Edit Client** dialog box appears.
5. Click the **Datastores** tab and note which datastores are selected.
6. Click the **Groups** tab and note which groups are selected.
7. Uncheck all groups in preparation for deleting this proxy.
8. Click **OK**.

Removing existing proxies

Procedure

1. In the vSphere Client or Web Client, locate existing proxies.
2. For each proxy:

   a. Right click and select **Power > Power off**.

   b. Wait for the proxy to power off, then right-click and select **Delete from Disk**.

   The **Confirm Delete** confirmation windows appears.

   c. Click **Yes**.
3. In Avamar Administrator, click the **Administration** launcher button.

   The **Administration** window appears.
4. Click the **Account Management** tab.
5. Locate existing proxies, and for each proxy:

   a. Right click and select **Retire Client...**.

   The **Retire Client** window appears.

   b. Click **OK**.

Re-deploying proxies using the Proxy Deployment Manager

Procedure

1. In Avamar Administrator, select **VMware** > **Proxy Deployment Manger**.

   The **Proxy Deployment Manger** window appears.

2. Choose a vCenter.
3. Set the **Data change rate** to **0**.

   This ensures that the Proxy Development Manager will not recommend proxies based on its analysis of your VMware environment.

4. Click **Create Recommendation**.

   The tree pane shows your VMware topology. Verify that there are no recommended proxies labeled **New proxy**.

5. For each proxy in the chart created in Existing proxy configuration on page 40:

   a. Locate and select the host in the Proxy Deployment Manager.

   b. Click **New Proxy...**.

      The **New Proxy** window appears.

   c. Complete the **Name**, **Domain**, **IP**, **Datastore**, **Network**, **DNS**, **Gateway**, and **Netmask** based on the information in the chart.

   d. Click **Save**.

6. Click **Apply** to deploy the proxies.

   The new proxies will be deployed and registered. If any failures occur, the operation can be retried by clicking **Apply** again.

Restoring datastore assignments and group membership

Procedure

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

   The **Administration** window appears.

2. Click the **Account Management** tab.
3. Select the updated proxy and click **Edit**.

   The **Edit Client** dialog box appears.

4. Click the **Datastores** tab and verify the Datastore protecting the client, based on the chart created in Existing proxy configuration on page 40.
5. Click the **Groups** tab and verify the proxies that are members of this group, based on the chart created in Existing proxy configuration on page 40.
6. Click **OK**.

Maintaining proxies

Reregistering a proxy with an Avamar server

Use these instructions to reregister an existing proxy with an Avamar server.

Procedure

1. Launch the vSphere Client or vSphere Web Client, and log in to the vCenter Server.
2. Locate the proxy you want to reregister.
3. Right click **Power** > **Shut Down Guest**.
4. Click **Yes** to confirm that you want to shut down the guest operating system.
5. Right click **Power** > **Power Off**.
6. Click **Yes** to confirm that you want to power off the proxy virtual machine.
7. Right-click**Open Console**.

   A console window appears.
8. 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 window and press **Enter**.
11. Type the Avamar server DNS name, and then press **Enter**.
12. Type an Avamar server domain name, and then press **Enter**.

    The default domain is “clients.” However, your Avamar system administrator may have defined other domains, and subdomains. Consult your Avamar system administrator for the 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.

Changing the proxy guest operating system root password

Procedure

1. Open a command shell and log in to the proxy as root.
2. Type `passwd`.
3. Type the current guest operating system root password, and then press **Enter**.
4. Type the new guest operating system root password, and then press **Enter**.
5. Confirm the new password by typing it again, and then pressing **Enter**.

Additional Avamar server configuration

Configuring automatic proxy selection

The automatic intelligent proxy selection feature provides three different algorithms for determining which proxy to use to backup and restore operations. The algorithm can only be configured by manually modifying the `mcserver.xml` proxy_selection_algorithm setting.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For 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. Find the `proxy_selection_algorithm` entry key.
5. Change the `proxy_selection_algorithm` setting to one of the following values:
   - `hot_add_preferred`—The MCS intelligently prefers and automatically selects proxies based on hot-add capabilities. If none are found, then the MCS will fall back to using proxies without hot-add capabilities. This is the default setting.
   - `hot_add_only`—The MCS intelligently prefers and automatically selects proxies based on hot-add capabilities. If none are found, then the MCS will pause the backup or restore operation and wait for a hot-add capable proxy to become available.
   - `ignore_associated_datastores`—This setting causes known proxy-datastore associations to be ignored during the selection process. This allows the MCS to select a proxy from a larger pool of available proxies. Like the `hot_add_preferred` setting, proxies with hot-add capabilities are still preferred over proxies without hot-add capabilities. But if no hot-add capable proxies are found, then the MCS will fall back to using proxies without hot-add capabilities.

   For example:

   `<entry key=" proxy_selection_algorithm" value="`**`hot_add_only`**`" />` configures the automatic proxy selection mechanism to use the hot_add_only algorithm.
6. Close `mcserver.xml` and save your changes.
7. Start the MCS and the scheduler by typing:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

Configuring the MCS to support both guest and image backup

In order to support using both image and guest backup to protect the same virtual machine, you must configure the Avamar MCS to allow duplicate client names.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For 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. Find the `allow_duplicate_client_names` entry key.
5. Change the `allow_duplicate_client_names` setting to **`true`**.

   ```
   <entry key="allow_duplicate_client_names" value="true" />
   ```
6. Close `mcserver.xml` and save your changes.
7. Start the MCS and the scheduler by typing:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

CHAPTER 3

Administration

This chapter includes the following topics:

Clients and containers

Image backup can be used to 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.

Note

Empty containers such as a folder or resource pool are allowed to be added to MCS. When VMs or vApps are added to a container, they are automatically protected by Avamar. During a backup, MCS will skip a container if it is empty.

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 using the **Recursive Protection** checkbox, all the child entities including the subcontainers get added to Avamar Administrator. Virtual machines or vApps residing in the subcontainers will get added automatically to Avamar Administrator.

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.

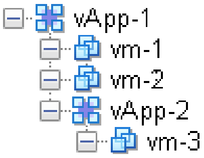
If you need to delete or retire one or more virtual machine clients from an Avamar dynamic container, you must first change that container to a static container. An alternative method is to move those virtual machine clients to another container in vCenter.

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



- vApp-1
  - vm-1
  - vm-2
  - vApp-2
    - vm-3

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 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 various icons to communicate VMware entity type and state.

Table 8 Avamar Administrator icons and what they mean

Icon	Description
vCenter Servers	
🖥	Activated. This is the same icon used to show nonvirtual machine clients.
R🖥	Replicated. This icon is only visible in the 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, this can be the normal state for a vCenter Server.
Virtual machine clients	

Table 8 Avamar Administrator icons and what they mean (continued)

Icon	Description
	Powered off.
	Template.
Proxies	
	Activated and enabled.
×	Disabled
R	Replicated. This icon is only visible in the REPLICATE domain.
?	Unactivated.
Other entities	
	vCenter folder.
	vApp.
	Resource pool.

Adding clients and containers

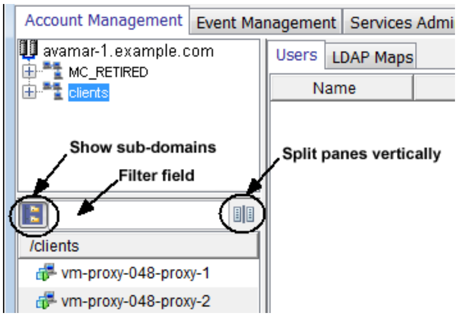
Procedure

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

   The **Administration** window appears.

2. Click 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 equivalent to the vSphere Virtual Machines and Template view.
   - The **Hosts & Clusters** tab is equivalent to the vSphere 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, select 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. In the right properties pane, select a folder, resource pool, virtual machine or vApp.
8. If adding a container, set the **Dynamic** checkbox to make this a dynamic container, or set the **Static** checkbox to make this a static container.
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**.
11. (Optional) If adding a client, type the following contact information:
    a. **Contact** name.
    b. Contact telephone (**Phone**) number.
    c. Contact **Email** address.
    d. Contact **Location**.
12. Click **OK**.
13. Click **OK** to dismiss the confirmation message.
14. If you enabled changed block tracking:
    a. In the vSphere Client or vSphere Web Client, locate the virtual machine.
    b. Perform any of the following actions for each virtual machine: reboot, power on, resume after suspend, or migrate.

Editing clients and containers

Procedure

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

   The **Policy** window appears.
2. Click the **Policy Management** tab, and then 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 **Datastores** 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.
   - When editing a virtual machine client, datastores on which that virtual machine resides are shown.

- When editing a container, the **Properties** tab shows a **Dynamic Mode** checkbox, which is used to enable or disable dynamic inclusion for that container.

Viewing protected virtual machines

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

Procedure

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

   The **Administration** window appears.
2. Click on vCenter domain.
3. Click the **Account Management** tab.
4. Click the **Protection** tab.

Viewing a replicated virtual machine name

This feature is used to view the virtual machine name of any virtual machine in the REPLICATE domain.

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

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

Procedure

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

   The **Administration** window appears.
2. Click the **Account Management** tab.
3. In the tree, select a virtual machine client in the REPLICATE domain.
4. Select **Actions** > **Account Management** > **View Information**.

   A dialog box appears, which shows the virtual machine name.
5. Click **OK**.

Monitoring the vCenter connection

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

Procedure

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

   The **Administration** window appears.
2. Click the **Services Administration** tab.
3. Double-click the **VMware vCenter Connection Monitor** services entry.

   The **VMware vCenter Connection Monitor** dialog box appears. Valid connection states are Active and Idle.

Results

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, Avamar Administrator cannot display the 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.

Procedure

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

   The **Administration** window appears.
2. Click the **Account Management** tab.
3. In the tree, select a vCenter.
4. Select **Actions** > **Account Management** > **Sync. with vCenter.**.
5. Click **Yes** to dismiss the confirmation message.

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.

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.

Procedure

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

   The **Administration** window appears.
2. Click the **Account Management** tab.
3. In the tree, select the vCenter client.
4. Select **Actions** > **Account Management** > **Edit Client**.

   The **Edit Client** dialog box appears.
5. In the **New Client Name or IP** box, type the new fully qualified DNS name.
6. Click **OK**.
7. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:

     a. Log in to the utility node as admin.

   b. Load the admin OpenSSH key by typing:

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

   c. When prompted, type the `admin_key` passphrase and press **Enter**.

8. Stop the MCS by typing `dpnctl stop mcs`.
9. Start the MCS and the scheduler by typing:

```
dpnctl start mcs
dpnctl start sched
```

10. Reboot every Avamar proxy in this vCenter:

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

    b. Locate an Avamar proxy.

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

    d. Click **Yes** to confirm that you want to shut down the guest operating system.

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

    f. Click **Yes** to confirm that you want to power off the virtual machine.

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

VMware Image Dataset

The VMware Image Dataset is the default dataset for protecting VMware entities with image backup.

In many respects, the VMware Image Dataset is simpler than most other datasets:

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

Adding guest backup throttling parameters to a dataset

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.

Procedure

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

   The **Manage All Datasets** window appears.

2. Select a dataset from the list and click **Edit**.

   The**Edit Dataset** dialog box appears.

3. Click the **Options** tab, and then click **Show Advanced Options**.
4. If the client supports Network usage throttle, 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.

5. Click **OK**.

Groups

Groups have important behavioral differences when used with image backup and restore.

Default Proxy Group

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

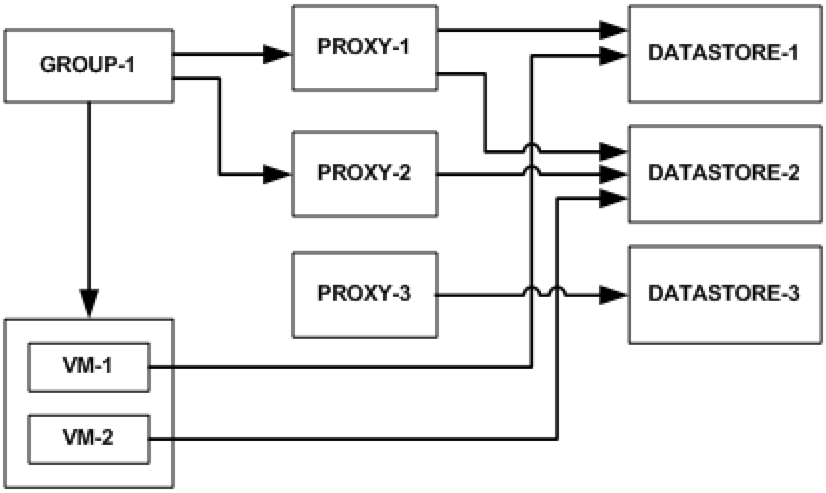
Default Virtual Machine Group

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.

Virtual machine and proxy relationships within groups

Consider the following simplified example configuration:

Figure 3 Virtual machine and proxy relationships within 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 group (GROUP-1) is created, to which virtual machines VM-1 and VM-2 are added.

In order to protect these virtual machines, proxies must also be added to the group as follows:

- PROXY-1, because it is assigned to both DATASTORE-1 and DATASTORE-2, can protect both VM-1 and VM-2.
- PROXY-2, because it is only assigned to DATASTORE-2, is optional as long as Proxy-1 exists in the group.
- PROXY-3, because it is only assigned to DATASTORE-3, cannot protect either VM-1 or VM-2.

Every 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`.

Changing proxy datastore and group assignments

Procedure

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

   The **Policy** window appears.
2. Click the **Policy Management** tab, and then click the **Clients** tab.
3. Select a proxy and click **Edit**.

   Note

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

   The **Edit Client** dialog box appears.
4. Click the **VMware** tab, and then click the **Datastores** tab.
5. Select one or more datastores.
6. Click the **Groups** tab.
7. Select one or more groups.
8. Click **OK**.

CHAPTER 4

Backup

This chapter includes the following topics:

Limitations

These are the known limitations of Avamar for VMware image backup.

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

Changing a virtual machine's 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.

Version 8 or higher 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 only known remedy is to reconfigure the virtual machine such that all virtual disks reside on the same datastore.

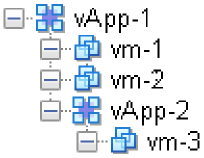
Backups involving physical RDM disks
When backing up a virtual machine that has both virtual disks and physical RDM disks, the backup will successfully process the virtual disks, bypass the RDM disks, and complete with the following event code:

```
Event Code: 30929
Category: Application
Severity: Process
Summary: Virtual machine client contains disks that cannot be
backed up or restored.
```

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

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

Procedure

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

   The **Backup, Restore and Manage** window appears.
2. Click the **Backup** tab.

   The top-left pane contains a list of domains.
3. Select a domain in the upper tree, and then select a virtual machine client, VMware folder, resource pool, or vApp in the lower tree.
4. In the **Browse for File, Folders, or Directories** pane, select the data to back up:

   - Select the top (root) folder to back up the entire image.
   - Select one or more disks to only back up those specific virtual disks.
5. Select **Actions** > **Backup Now**.

   The **On Demand Backup Options** dialog box appears.
6. Select the backup retention setting:

   - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period** and then specify the number of days, weeks, months, or years for the retention period.
   - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
   - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.
7. From the **Avamar encryption method** list, select the encryption method to use for data transfer between the client and the Avamar server during the backup.

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.
8. (Optional) **Optionally select a proxy to perform backup**.

   The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.

9. (Optional) Set plug-in options:

   a. Click **More Options**.

      The **Backup Command Line Options** dialog box appears.

   b. Select the **Show Advanced Options** checkbox.

   c. To enable changed block tracking, select the **Use Changed Block Tracking (CBT) to increase performance** checkbox.

   d. To store this backup on a Data Domain system, select the **Store backup on Data Domain System** checkbox, then select a Data Domain system from the list.

   e. From the **Encryption method to Data Domain system** list, select the encryption method to use for data transfer between the client and the Data Domain system during the backup.

   f. To run a script before or after the backup, type a virtual machine guest OS user account name and password with sufficient privileges to run scripts.

   g. To run a script before the vmdk snapshot, type the full path and filename of the script that will be run. Also ensure that the script timeout is sufficient for the script to complete.

   h. To run a script after the backup completes and the vmdk snapshot is removed, type the full path and filename of the script that will be run. Also ensure that the script timeout is sufficient for the script to complete.

   i. Click **OK**.

   These settings are all optional. In most cases, system default settings are the optimum settings for on-demand image backups.

10. Click **OK**.

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

11. Click **OK**.

Scheduling backups

Scheduled backups run automatically to ensure that backups occur on an ongoing basis. You can schedule backups to run daily, weekly, or monthly.

Procedure

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.

      By default, dataset entries use absolute path notation. For example:

      ```
      [datastore1] VM1/VM1.vmdk
      ```

      However, you can use relative path notation to ensure that a particular `.vmdk` is always included in a backup, even if that virtual machine is migrated to another datastore using Storage vMotion. For example, the following equivalent dataset entry uses relative path notation:

      ```
      \[.*\] VM1/VM1.vmdk
      ```

   b. Assign a schedule to the new group.
   c. Assign a retention policy to the new group.
   d. Add one or more clients to the new group.

   The *EMC Avamar Administration Guide* provides more information about groups, group policy, datasets, schedules, and retention policies.

3. Enable scheduling for the group.

Monitoring backups

You can monitor backups to ensure that the backups complete successfully and to troubleshoot issues. The Activity Monitor in Avamar Administrator enables you to view status information for both on-demand and scheduled backups.

Procedure

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

   The **Activity** window appears.
2. Click the **Activity Monitor** tab.

   A list of all activities appears.
3. To filter the results to display only backup activity, select **Actions** > **Filter**.

   The **Filter Activity** dialog box appears.
4. Select **All Backups** from the **Type** list.
5. Click **OK**.

Canceling backups

You can cancel a backup any time before it completes. The cancellation might take five minutes or longer. The backup may complete before the cancellation finishes.

Procedure

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

   The **Activity** window appears.
2. Click the **Activity Monitor** tab.

   A list of all activities appears.
3. Select the backup from the list.
4. Select **Actions** > **Cancel Activity**.

   A confirmation message appears.
5. Click **Yes**.

CHAPTER 5

Restore

This chapter includes the following topics:

Overview

Image backup offers three levels of restore functionality: image restore, file-level restore, and the capability to mount specific drives from a Windows image backup in order to support application-level recovery.

Three buttons are provided above the **Select for Restore** contents pane, which are not shown if a non-VMware image backup is selected:

Table 9 Image restore toolbar buttons

Button	Tooltip	Description
	Browse for Image Restore	Initiates an image restore.
	Browse for Granular Restore	Initiates a file-level restore.
	Mount Windows VMDK	Mounts selected drives in a Windows image backup in order to support application-level recovery.

When performing an image restore, the **Restore Options** dialog box is slightly different from the typical **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.

Image and file-level restore guidelines

Avamar provides two distinct mechanisms for restoring virtual machine data: image restores, which can restore an entire image or selected drives, and file-level restores, which can 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.

If you restore a 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

These are the limitations of restoring data from an image backup.

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

Virtual machine power state
When using image restore to restore an entire image or selected drives, the target virtual machine must be powered off.

When using file-level restore to restore specific files or folders, the target virtual machine must be powered on and have VMTools installed and running the current or most up to date version.

Restores involving physical RDM disks
When restoring data from a backup taken from a virtual machine with physical RDM disks, you cannot restore that data to a new virtual machine.

File-level restore limitations
The following limitations apply to file-level restores:

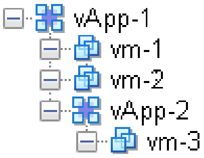
- VMware Tools must be installed on the target virtual machine. For best results, ensure that all virtual machines are running the latest available version of VMware Tools. Older versions are known to cause failures when browsing during the file-level restore operation.
- The following virtual disk configurations are not supported:
  - Dynamic disks (Windows)
  - Deduplicated NTFS
  - Resilient File System (ReFS)
  - All Extended Partition not of type 0x05
  - Encrypted partitions or bootloaders
  - Compressed partitions or bootloaders
- ACLs are not restored for Microsoft Windows clients (ACLs are restored for Linux files and folders).
- Symbolic links cannot be restored or browsed.
- 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.

Note

In some cases (most notably extended partitions), it may be possible to restore the entire backup image to a temporary virtual machine, then selectively copy the folders or files you need.

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



vApp-1
vm-1
vm-2
vApp-2
vm-3

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:

- 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

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

Procedure

1. In the vSphere Client or vSphere Web 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.

   The upper left pane contains a list of domains.
4. Select a virtual machine client or VMware container:

   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.

   b. From the list of clients, select the virtual machine client or VMware container.
5. Select a backup:

   a. Click the **By Date** tab.

   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.

   c. Select a backup from the **Backups** table.
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 original virtual machine** as the restore destination.

   Note

   When restoring an image backup to the original virtual machine, the **Configure Destination** button is disabled (grayed out).

10. (Optional) If you want to restore VMware configuration files, select **Restore virtual machine configuration**.
11. (Optional) **Optionally select a proxy to perform restore**.

    The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.
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. From the **Encryption method from Data Domain system** list, select the encryption method to use for data transfer between the Data Domain system and the client during the restore.
15. 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**.
16. (Optional) To include additional plug-in options with this restore, type **Enter Attribute** and **Enter Attribute Value** settings.
17. Click **OK** on the **Restore Command Line Options** dialog box.
18. Click **OK** on the **Restore Options** dialog box.

    The following status message appears: `Restore initiated`.
19. Click **OK**.
20. If the restore target virtual machine will be using changed block tracking for future backups, enable changed block tracking by performing any of the following actions on that virtual machine: reboot, power on, resume after suspend, or migrate.

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

Procedure

1. In the vSphere Client or vSphere Web 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.

   The upper left pane contains a list of domains.
4. Select a virtual machine client or VMware container:

   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.

   b. From the list of clients, select the virtual machine client or VMware container.
5. Select a backup:

   a. Click the **By Date** tab.

   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.

   c. Select a backup from the **Backups** table.
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 (grayed out).
10. Click **Configure Destination**.

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

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

Note

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

13. Click **OK** on the **Configure Virtual Machine** dialog box.
14. From the **Avamar encryption method** list, select the encryption method to use for data transfer between the Avamar server and the client during the restore.

    The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.
15. (Optional) **Optionally select a proxy to perform restore**.

    The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.
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. From the **Encryption method from Data Domain system** list, select the encryption method to use for data transfer between the Data Domain system and the client during the restore.
19. 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**.
20. (Optional) To include additional plug-in options with this restore, type **Enter Attribute** and **Enter Attribute Value** settings.
21. Click **OK** on the **Restore Command Line Options** dialog box.
22. Click **OK** on the **Restore Options** dialog box.

    The following status message appears: `Restore initiated`.
23. Click **OK**.
24. If the restore target virtual machine will be using changed block tracking for future backups, enable changed block tracking by performing any of the following actions on that virtual machine: reboot, power on, resume after suspend, or migrate.

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

Procedure

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

   The **Backup, Restore and Manage** window appears.

2. Click the **Restore** tab.

   The upper left pane contains a list of domains.

3. Select a virtual machine client or VMware container:

   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.

   b. From the list of clients, select the virtual machine client or VMware container.

4. Select a backup:

   a. Click the **By Date** tab.

   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.

   c. Select a backup from the **Backups** table.

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 (grayed out) because these configuration files are always required to configure the new virtual machine.

9. Specify a location and settings for the new virtual machine:

   a. Click **Configure Destination**.

      The **Configure Virtual Machine** dialog box appears.

   b. Click **Browse**.

      The **New Virtual Machine** wizard appears.

   c. In the **Name and Location** screen, type a unique **Name** for the new virtual machine, select a datacenter and folder location in the inventory tree, and then click **Next**.

   d. In the **Summary** screen, review the information, and then **Finish**.

   e. Click **OK** on the **Configure Virtual Machine** dialog box.

10. From the **Avamar encryption method** list, select the encryption method to use for data transfer between the Avamar server and the client during the restore.

    The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

11. (Optional) **Optionally select a proxy to perform restore**.

    The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.

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. From the **Encryption method from Data Domain system** list, select the encryption method to use for data transfer between the Data Domain system and the client during the restore.
15. 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**.
16. (Optional) To include additional plug-in options with this restore, type **Enter Attribute** and **Enter Attribute Value** settings.
17. Click **OK** on the **Restore Command Line Options** dialog box.
18. Click **OK** on the **Restore Options** dialog box.

    The following status message appears: `Restore initiated`.

19. Click **OK**.
20. If the restore target virtual machine will be using changed block tracking for future backups, enable changed block tracking by performing any of the following actions on that virtual machine: reboot, power on, resume after suspend, or migrate.

Restoring specific folders or files to the original virtual machine

Before you begin

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

Where folders and files are actually restored differs according to the target virtual machine operating system:

- 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.

Procedure

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

   The **Backup, Restore and Manage** window appears.
3. Click the **Restore** tab.

   The upper left pane contains a list of domains.
4. Select a virtual machine client or VMware container:

   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.

   b. From the list of clients, select the virtual machine client or VMware container.
5. Select a backup:

   a. Click the **By Date** tab.

   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.

   c. Select a backup from the **Backups** table.
6. Click the **Browse for Granular Restore** button ().
7. **Optionally select a proxy to perform browse and restore**, and then click **OK**.

   The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.
8. Select one or more folders or files you want to restore.
9. Select **Actions** > **Restore Now**.

   The **Restore Options** dialog box appears.
10. Select **Restore everything to its original location**.
11. From the **Avamar encryption method** list, select the encryption method to use for data transfer between the Avamar server and the client during the restore.

    The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.
12. Click **More Options**.

    The **Restore Command Line Options** dialog box appears.

13. (Optional) If restoring Linux folders or files, select **Restore Access Control List (ACL)** to restore Linux ACLs.
14. (Optional) To include additional plug-in options with this restore, type **Enter Attribute** and **Enter Attribute Value** settings.
15. Click **OK** on the **Restore Command Line Options** dialog box.
16. Click **OK** on the **Restore Options** dialog box.

    The following status message appears: `Restore initiated`.
17. Click **OK**.

Restoring specific folders or files to a different virtual machine

Before you begin

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

Procedure

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

   The **Backup, Restore and Manage** window appears.
3. Click the **Restore** tab.

   The upper left pane contains a list of domains.
4. Select a virtual machine client or VMware container:

   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.

   b. From the list of clients, select the virtual machine client or VMware container.
5. Select a backup:

   a. Click the **By Date** tab.

   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.

   c. Select a backup from the **Backups** table.
6. Click the **Browse for Granular Restore** button ().
7. **Optionally select a proxy to perform browse and restore**, and then click **OK**.

   The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.

8. Select one or more folders or files you want to restore.
9. Select **Actions** > **Restore Now**.

   The **Restore Options** dialog box appears.
10. Select **Restore everything to a different location**.
11. Select the target virtual machine that will receive 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 target virtual machine that will receive the restored data.

    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**.

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

    g. Click **OK**.
12. Click **More Options**.

    The **Restore Command Line Options** dialog box appears.
13. (Optional) If restoring Linux folders or files, select **Restore Access Control List (ACL)** to restore Linux ACLs.
14. (Optional) To include additional plug-in options with this restore, type **Enter Attribute** and **Enter Attribute Value** settings.
15. Click **OK** on the **Restore Command Line Options** dialog box.
16. Click **OK** on the **Restore Options** dialog box.

    The following status message appears: `Restore initiated`.
17. Click **OK**.

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 an image backup to a new virtual machine, 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.

Instant access comprises the following tasks:

1. Restoring the virtual machine:

- Instant access is initiated.
- Selected VMware backup is copied to temporary NFS share on the Data Domain system.

2. Performing post-restore migration and clean-up:
   - From the vSphere Client or vSphere Web Client, power on the virtual machine, and then use Storage vMotion to migrate the virtual machine from the Data Domain NFS share to a datastore within the vCenter.
   - When Storage vMotion is complete, the restored virtual machine files no longer exist on the Data Domain system.
   - From Avamar Administrator, ensure that the Data Domain NFS share has been deleted.

Note

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 unmount the NFS share after each instant access so that subsequent instant access operations are not impacted.

Restoring the virtual machine

Before you begin

Instant access requires the following:

- Avamar 7.0 or later
- Data Domain Operating System 5.2.1 and above. Please refer to the Avamar compatibility matrix for supported versions of DDOS

Procedure

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

   The **Backup, Restore and Manage** window appears.
2. Click the **Restore** tab.

   The upper left pane contains a list of domains.
3. Select a virtual machine client or VMware container:
   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.

   b. From the list of clients, select the virtual machine client or VMware container.
4. Select a backup residing on the Data Domain:
   a. Click the **By Date** tab.

   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.

   c. Select a backup from the **Backups** table.

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 restoring an image backup to a new virtual machine, the **Restore virtual machine configuration** option is selected and disabled (grayed out) because these configuration files are always required to configure the new virtual machine.

   ---

9. Specify a location and settings for the new virtual machine:

   a. Click **Configure Destination.**

      The **Configure Virtual Machine** dialog box appears.

   b. Click **Browse**.

      The **New Virtual Machine** wizard appears.

   c. In the **Name and Location** screen, type a unique **Name** for the new virtual machine, select a datacenter and folder location in the inventory tree, and then click **Next**.

   d. In the **Summary** screen, review the information, and then **Finish**.

   e. Click **OK** on the **Configure Virtual Machine** dialog box.
10. Ignore the **Avamar encryption method** setting.

    Because no client/server data transfer takes place, the **Avamar encryption method** setting has no effect.
11. (Optional) **Optionally select a proxy to perform restore**.

    The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.
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, type **Enter Attribute** and **Enter Attribute Value** settings.
16. Click **OK** on the **Restore Command Line Options** dialog box.
17. Click **OK** on the **Restore Options** dialog box.

The following status message appears: `Restore initiated`.

18. Click **OK**.

Performing post-restore migration and clean-up

Procedure

1. Launch the vSphere Client or vSphere Web Client, and log in to the vCenter Server.
2. Locate the virtual machine you restored.
3. Use Storage vMotion to migrate that virtual machine from the Data Domain NFS share to a datastore within the vCenter.

   When Storage vMotion is complete, the restored virtual machine files no longer exist on the Data Domain system.

   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 the remainder of this procedure.
4. In Avamar Administrator, click the **Server** launcher button.

   The **Server** window appears.
5. Click the **Data Domain NFS Datastores** tab.
6. Ensure that there is no entry for the virtual machine you restored.

   If an entry is found, select it, and then click **Unmount/Remove**.

Mounting Windows VMDKs from an image backup

Avamar provides a mechanism for mounting VMDKs from VMware image backups of Windows virtual machines. This feature is typically used to enable third party tools such as Kroll OnTrack PowerControls to perform data mining and advanced data recovery.

Configuring the recovery target machine

This task configures a physical or virtual Windows machine to be a recovery target for mounting Windows VMDKs from an image backup.

Before you begin

The recovery target machine must be a 64-bit Windows physical or virtual machine.

Note

Recovery targets can be physical or virtual machines. If you intend to use a virtual machine as a recovery target, install the Avamar software directly on the virtual machine just as you would if implementing guest backup.

Procedure

1. Using instructions in the *EMC Avamar Backup Clients User Guide*, install Avamar Windows client software on the recovery target machine.
2. Using instructions in the *EMC Avamar Backup Clients User Guide*, register the recovery target machine as a client with the same Avamar server storing the image backup to be mounted.

3. Install the Windows VMware GLR plug-in software:
   a. Log in to the recovery target machine with Windows administrator privileges.
   b. Download the **AvamarVMWareGLR-windows-x86_64-*version*.msi** install package from the Avamar server.
   c. Open the install package, and then follow the on screen instructions.
   d. Reboot the computer.

Restoring and mounting the Windows VMDKs

Before you begin

Ensure that the recovery target machine has been properly configured:

- The Avamar Windows client, and Windows VMware GLR plug-in software is installed
- The recovery target machine is registered and activated as a client with the same Avamar server storing the image backup from which the VMDK will be mounted

Procedure

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

   The **Backup, Restore and Manage** window appears.
3. Click the **Restore** tab.

   The upper left pane contains a list of domains.
4. Select a virtual machine client or VMware container:
   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.
   b. From the list of clients, select the virtual machine client or VMware container.
5. Select a backup:
   a. Click the **By Date** tab.
   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.
   c. Select a backup from the **Backups** table.
6. In the contents pane, select a virtual disk.
7. Click the **Mount Windows VMDK** button ().

   The **Select Destination Client** dialog box appears.
8. Click **Browse** next to the **Client** box.

The **Browse for Restore Destination Client** dialog box appears.

9. Select the recovery target virtual machine, and then click **OK**.

   The **Browse Backup Status** dialog box appears.

10. Click **OK** to confirm that the operation should continue.

    The **Restore Browse Options** dialog box appears.

11. Select a time out value from the **Amount of time to leave VMDKs mounted** list, and then click **OK**.

Results

A folder path appears in the right backup contents pane. The Windows VMDK is now mounted to that folder.

Monitoring restores

You can monitor restores to ensure that the restores complete successfully and to troubleshoot issues. The Activity Monitor in Avamar Administrator enables you to view status information for restores.

Procedure

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

   The **Activity** window appears.

2. Click the **Activity Monitor** tab.

   A list of all activities appears.

3. To filter the results to display only restore activity, select **Actions** > **Filter**.

   The **Filter Activity** dialog box appears.

4. Select **Restore** from the **Type** list.
5. Click **OK.**

Canceling restores

You can cancel a restore any time before the restore completes. The cancellation might take five minutes or longer. The restore may complete before the cancellation finishes.

Procedure

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

   The **Activity** window appears.

2. Click the **Activity Monitor** tab.

   A list of all activities appears.

3. Select the restore from the list.
4. Select **Actions** > **Cancel Activity**.

   A confirmation message appears.

5. Click **Yes**.

CHAPTER 6

Backup Validation

This chapter includes the following topics:

Overview

For image backups, the backup validation mechanism is similar to restoring a virtual machine backup to a new virtual machine, except that once the backup is validated, the new virtual machine is automatically deleted from vCenter.

Backup validations can be initiated for a single virtual machine backup as needed (on-demand), or scheduled for an entire group of virtual machines. Scheduled backup validations always use the latest completed backup for each virtual machine group member.

What is validated

The default validation verifies that the virtual machine powers on and that the operating system starts following the restore.

Backup validations also provide an optional capability for running a user-defined script in order to perform custom application-level verifications. The script must exist in the backup to be validated. You cannot run external scripts during a backup validation.

Supported script types are shell scripts for Linux virtual machines, and DOS batch files for Windows virtual machines. Perl scripts are not supported.

VM Backup Validation groups

Scheduled backup validations are implemented using special VM Backup Validation groups. These groups are only used to perform automated backup validations, they cannot be used for any other purpose.

VM Backup Validation groups differ from other groups as follows:

- VM Backup Validation groups do not have retention policies assigned to them.
- The dataset assigned to each VM Backup Validation group is automatically created when the group is created. The dataset name is the same as the VM Backup Validation group name.
- Each VM Backup Validation group also stores a location where new virtual machines are temporarily created during the backup validation (that is, an ESX host or cluster, datastore, and folder).

Performing an on-demand backup validation

Procedure

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

   The **Backup, Restore and Manage** window appears.

2. Click the **Manage** tab.
3. Select a virtual machine client or VMware container:

   a. Select the domain that contains the virtual machine client or VMware container.

      You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

      A list of Avamar clients appears in the pane under the domains list.

   b. From the list of clients, select the virtual machine client or VMware container.

4. Select a backup:

   a. Click the **By Date** tab.

   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight.

      A list of backups on that date appears in the **Backups** table next to the calendar.

   c. Select a backup from the **Backups** table.

5. Select **Actions** > **Validate Backup**.

   The **Validate Options** dialog box appears.

6. Click **Configure Destination**.

   The **Configure Location** wizard appears.

7. Select a vCenter, and then click **Next**.

8. Type an inventory location name, select a datacenter folder in the tree, and then click **Next**.

9. Select a host or cluster and then click **Next**.

10. Select a resource pool and then click **Next**.

11. Select a datastore and then click **Next**.

12. At the **Summary screen**, click **Finish**.

13. From the **Avamar encryption method** list, select the encryption method to use for data transfer between the client and the Avamar server during the backup validation.

    The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

14. (Optional) To run a user-defined script as part of the validation:

    Note

    The script must already be in the backup to be validated. You cannot run external scripts during a backup validation.

    a. Click **More Options**.

       The **Validate Command Line Options** dialog box appears.

    b. Type a virtual machine guest OS user account name and password with sufficient privileges to run scripts.

    c. Type the full path and filename of the validation script.

       Note

       If this is a Windows virtual machine, type `exit /B` ***`exitcode`*** after the script path and filename, where *exitcode* is a user-defined exit message.

    d. Ensure that the **Maximum script run time (minutes)** setting allows sufficient time for the script to complete.

    e. Click **OK**.

15. Click **OK** on the **Validate Options** box.

    The following status message appears: `Restore request initiating.`

16. Click **Close**.

Scheduling backup validations

To schedule backup validations for an entire group of virtual machines, create a VM Backup Validation Group.

Procedure

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

   The **Policy** window appears.

2. Click the **Policy Management** tab, and then click the **Groups** tab.
3. In the tree, select a location for the group.
4. Select **Actions** > **Group** > **New** > **VM Backup Validation Group**.

   The **New VM Backup Validation Group** wizard appears.

5. In the **General** screen:

   a. Type a **Group name**.

   b. Select or clear the **Disabled** checkbox.

   Select this checkbox to delay the start of scheduled backups for this group. Otherwise, clear this checkbox to enable scheduled backups for this group the next time the assigned schedule runs.

   c. Select an **Avamar encryption method** for client/server data transfers during the backup validation.

   Note

   The encryption technology and bit strength for a 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. Click **Next**.

6. In the **Membership** screen:

   a. Select checkboxes next to the virtual machines you want to be members of this validation group.

   b. Click **Next**.

7. In the **Location** screen:

   a. Click **Configure Location**.

   The **Configure VM Backup Validation Location** wizard appears.

   b. Select a vCenter, and then click **Next**.

   c. Select a datacenter folder in the tree, and then click **Next**.
   d. Select a host or cluster, and then click **Next**.
   e. Select a resource pool, and then click **Next**.
   f. Select a datastore, and then click **Next**.
   g. In the **Summary** screen, review your settings, and then click **Finish**.
   h. Click **Next**.

8. In the **Schedule** screen, select a schedule from the list, and then click **Next**.
9. In the **Overview** screen, review your settings, and then click **Finish**.
10. Ensure that the scheduler is running.

CHAPTER 7

Protecting the vCenter Management Infrastructure

This chapter includes the following topics:

Overview

This topic discusses 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 a 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.

Implementing guest backups of vCenter management infrastructure

Procedure

1. Install and register Avamar Client for Windows software on the vCenter host as described in the *EMC Avamar Backup Clients User Guide*.
2. 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*.

Creating a dataset for vCenter management infrastructure backups

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

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).

Procedure

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).
4. Click the **Source Data** tab.
5. Select **Enter Explicitly**, and then 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 then clicking **-**.
7. Add each vCenter management infrastructure component to the dataset:

   a. Select **Files and/or Folders** and click **...**

   The **Select Files And/Or Folders** dialog box appears.

   b. Locate a vCenter management infrastructure component and select it.

Table 10 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`

Table 10 Important vCenter management infrastructure components (continued)

Component	Default Location
	`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`

c. Click **OK**.

d. Repeat these steps for each important vCenter management infrastructure component.

8. Click **OK**.

Adding a backup client for vCenter database hosts

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

Procedure

1. 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*.
2. 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 **Truncate database log** option in the SQL Server plug-in . 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. *EMC Avamar Administration Guide*

CHAPTER 8

Protecting ESX Hosts

This chapter includes the following topics:

Overview

Image backup can be configured to protect virtual machines residing in standalone ESX hosts.

There are two primary uses for this feature:

1. Support for minimal customer configurations.
   Some customer sites use a simple VMware topology, comprising a single ESX host, with one or more virtual machines residing on that ESX host. These sites typically do not implement a vCenter management layer. However, the virtual machines residing on a standalone ESX host still must be backed up in order to protect against data loss. Adding the standalone ESX host as an Avamar vCenter client enables those virtual machines to be backed up with image backup, rather than guest backup.
2. Virtual vCenter disaster recovery.
   Adding an ESX host as an Avamar vCenter client can be useful when virtual machines residing on a particular ESX host must be restored, but the vCenter is not operational. This is often the case when a virtual vCenter must be recovered from Avamar backups. Adding the standalone ESX host as an Avamar vCenter client enables the vCenter management infrastructure virtual machines to be restored so that the vCenter can be restarted.

Limitations

These are the known limitation of protecting virtual machines residing in a standalone ESX host in Avamar.

ESX versions
Support for this feature is limited to ESX 5.0 or higher. Older versions are not supported.

Virtual vCenter disaster recovery
If you are using this feature for the purpose of recovering a virtualized vCenter from an ESX host, you must first disassociate that ESX host from the vCenter before restoring any virtual machines to that ESX host.

Task List

In order to protect virtual machines residing in a standalone ESX host, perform the following tasks:

1. Ensure that the Avamar server can communicate and authenticate with the ESX host.
   Add the ESX host certificate to the Avamar MCS keystore. Otherwise, you must disable certificate authentication for all MCS communications.
2. (Optional) Create a dedicated user account on the ESX host for use with Avamar.
3. Add the ESX host to Avamar as a vCenter client.
   This enables dynamic discovery of virtual machines residing on that ESX host, so that they can be backed up with image backup rather than guest backup.
4. Deploy one or more proxies on the ESX host.
5. Perform on-demand or scheduled image backups of virtual machines residing on that ESX host.

Adding ESX host authentication certificates to the MCS keystore

Add an ESX host authentication certificate to the MCS keystore. Do this for each ESX host you intend to protect.

This procedure uses the java `keytool` utility, which manages certificate keys. The `keytool` utility is located in the Java bin folder (`/usr/java/`*`version`*`/bin`), where *version* is the 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`.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For 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 `/etc/vmware/ssl/rui.crt` from the ESX host machine to `/tmp` on the Avamar utility node or single-node server.
5. Copy the MCS keystore to `/tmp` by typing:

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

   This creates a temporary version of the live MCS keystore in `/tmp`.
6. Add the default ESX host 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. Type the keystore password.
8. Type **`yes`**, and press **Enter** to trust this certificate.
9. (Optional) If you will be protecting more than one ESX host with this Avamar server, add those ESX host certificates now.
10. 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.
11. Copy the temporary MCS keystore to the live location by typing:

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

12. Exit the root subshell by typing **`exit`**.

13. Start the MCS and the scheduler by typing:

```
dpnctl start mcs
dpnctl start sched
```

Creating a dedicated ESX host user account

EMC strongly recommends that you set up a separate user account on each ESX host 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 ESX host user account ensures maximum clarity if it becomes necessary to examine ESX host logs.

Note

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

Procedure

1. Create a ESX host user account with privileges listed in the following table.

Table 11 Minimum required ESX host user account privileges

Privilege type	ESX 5.5	ESX 5.0
Alarms	• Create alarm	• Create alarm
Datastore	• Allocate space • Browse datastore • Low level file operations • Remove file	• Allocate space • Browse datastore • Low level file operations • Remove file
Extension	• Register extension • Unregister extension • Update extension	• Register extension • Unregister extension • Update extension
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
Host > Configuration	• Connection	• Connection

Table 11 Minimum required ESX host user account privileges (continued)

Privilege type	ESX 5.5	ESX 5.0
	• Storage partition configuration	• Storage partition configuration
Network	• Assign network • Configure	• Assign network • Configure
Resource	• Assign virtual machine to resource pool	• Assign virtual machine to resource pool
Sessions	• Validate session	• Validate session
Tasks	• Create task • Update task	• Create task • Update task
vApp	• Import	• Import
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 settings • 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 settings • Raw device • Reload from path • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual machine compatibility
Guest Operations	• Guest Operation Modifications	• Guest Operation Modifications

Table 11 Minimum required ESX host user account privileges (continued)

Privilege type	ESX 5.5	ESX 5.0
	• Guest Operation Program Execution • Guest Operation Queries	• 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 • Power off • Power on • Reset • VMware Tools install
Inventory	• Create new • Register • Remove • Unregister	• Create new • Register • Remove • Unregister
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
Snapshot Management	• Create snapshot • Remove snapshot • Revert to snapshot • Management	
State		• Create snapshot • Remove snapshot • Revert to snapshot

Adding an ESX host as a vCenter client

Procedure

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

   The **Administration** window appears.
2. Click the **Account Management** tab.

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

   The **New Client** dialog box appears.
4. Complete the following settings:
   a. Select **VMware vCenter** in the **Client Type** list.
   b. Type the ESX host fully qualified DNS name or IP address in the **New Client Name or IP** field.
   c. Type the ESX host web services listener data port number in the **Port** field.

      443 is the default setting.
   d. Type the ESX host administrative user account name in the **User Name** field.
   e. Type the ESX host administrative user account password in the **Password** field.
   f. Type the ESX host administrative user account password again in the **Verify Password** field.
   g. (Optional) Type a contact name in the **Contact** field.
   h. (Optional) Type a contact telephone number in the **Phone** field
   i. (Optional) Type a contact email address in the **Email** field.
   j. (Optional) Type a contact location in the **Location** field.
5. Click **OK**.

Deploying a proxy in a standalone ESX host

Before you begin

1. Add DNS entries for each proxy you intend to deploy.
   During proxy deployment, you will be asked to assign a unique IP address to each proxy. The ESX host 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.
2. Download the proxy appliance template file from the Avamar server.
3. Install the vSphere Client on your Windows computer.

Deploying a proxy appliance in an ESX host using the vSphere Client

Procedure

1. Launch the vSphere Client and log in to the ESX host.
2. Select **File** > **Deploy OVF Template**.

   The **Deploy OVF Template** wizard appears.
3. In the **Source** screen:
   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.

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

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

e. Click **Next**.

4. In the **OVF Template Details** screen:

a. Ensure that the template information is correct.

b. Click **Next**.

5. In the **Name and Location** screen:

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.
- The DNS name assigned to the proxy virtual machine.
- The Avamar client name after the proxy registers and activates with server.

Note

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 three contexts.

b. Click **Next**.

6. In the **Resource Pool** screen:

a. Select an ESX host or a resource pool.

b. Click **Next**.

7. In the **Storage** screen:

a. Select a storage location for this proxy.

b. Click **Next**.

8. In the **Disk Format** screen:

a. Select a disk format for this proxy.

b. Click **Next**.

9. In the **Network Mapping** screen:

a. Select a destination network from list.

b. Click **Next**.

10. In the **Ready To Complete** screen:

a. Ensure that the information is correct.

b. Click **Finish**.

Manually configuring proxy network settings

Procedure

1. Launch the vSphere Client and log in to the ESX host.
2. Locate the proxy you want to configure.
3. Right-click **Open Console**.

   A console window appears.
4. In the console **Main Menu**, press `2` to quit.
5. In the welcome screen, select **Log in**, and then press **Enter**.
6. Log in as root:

   a. Type `root`, and then press **Enter**.

   b. Type the root password, and then press **Enter**.
7. Type `/opt/vmware/share/vami/vami_config_net`, and then press **Enter**.

   A **Main Menu** appears.
8. In the **Main Menu**, select **6**, and then press **Enter** to configure the IP address for eth0.

   You can configure an IPv6 address, a static IPv4 address, or a dynamic IPv4 address. Follow the on-screen prompts to configure the correct address type for your site.
9. In the **Main Menu**, select **4**, and then press **Enter** to configure DNS.

   Follow the on-screen prompts to specify the primary and secondary DNS servers in use at your site.
10. In the **Main Menu**, select **3**, and then press **Enter** to configure the hostname.
11. Type the proxy hostname, and then press **Enter**.
12. In the **Main Menu**, select **2**, and then press **Enter** to configure the default gateway.
13. Type the IPv4 default gateway, and then press **Enter**.
14. Press **Enter** to accept the default IPv6 default gateway.
15. In the **Main Menu**, press **Enter** to show the current configuration.
16. Ensure that the settings are correct.
17. Press `1` to exit the program.

Registering and activating the proxy with the Avamar server

Register and activate each proxy deployed in vCenter with the Avamar server.

Before you begin

1. Deploy the proxy appliance in vCenter.
2. Add the ESX host as a vCenter client in Avamar.

Note

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.

Perform this task for every proxy you deploy in an ESX host.

Procedure

1. From the vSphere client, locate and select an Avamar image backup proxy.
2. Right-click **Power** > **Power On**.
3. Right-click**Open Console**.

   A console window appears.
4. From the **Main Menu**, type `1`, and then press **Enter**.
5. Type the Avamar server DNS name, and then press **Enter**.
6. Type an Avamar server domain name, and then press **Enter**.

   The default domain is “clients.” However, your Avamar system administrator may have defined other domains, and subdomains. Consult your Avamar system administrator for the 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.
7. From the **Main Menu**, type `2`, and then press **Enter** to quit.
8. (optional) If proxy certificate authentication is required, see Configuring vCenter-to-Avamar authentication on page 27

Disassociating an ESX host from a vCenter

Only perform this task if you are restoring virtual machines to an ESX host while the associated vCenter is not operational.

Procedure

1. Launch the vSphere Client or vSphere Web Client, and log in to the ESX host.
2. Click the **Summary** tab.
3. In the **Host Management** pane, click **Disassociate host from vCenter Server**.
4. Click **Yes** to confirm the action.

APPENDIX A

Manually deploying proxies

This appendix includes the following topics:

Overview

Beginning with Avamar 7.2, the Proxy Deployment Manager is the preferred method for deploying proxies. Manual proxy deployment is still supported if necessary.

Downloading the proxy appliance template file

Download the proxy appliance template file from the Avamar server.

Note

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

Procedure

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

   ```
   https://Avamar-server
   ```

   where *Avamar-server* is the Avamar server network hostname or IP address.

   The **EMC Avamar Web Restore** page appears.
2. Click **Downloads**.
3. Navigate to the **VMware vSphere** > **EMC Avamar VMware Image Backup/FLR Appliance** folder.
4. Click the **AvamarCombinedProxy-linux-sles11_64-*version*.ova** link.
5. Save **AvamarCombinedProxy-linux-sles11_64-*version*.ova** to a temporary folder, such as `C:\Temp`, or the desktop.

Deploying the proxy appliance in vCenter

Use either the vSphere Client running on a Windows computer (also known as the "thick client"), or the vSphere Web Client to deploy one or more proxies in each vCenter you intend to protect with image backup.

Before you begin

1. Add DNS entries for each proxy you intend to deploy.
   During proxy deployment, you will be asked to assign a unique IP address to each proxy. The 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.
2. Download the proxy appliance template file from the Avamar server.

Deploying a proxy appliance in vCenter using the vSphere Web Client

Procedure

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

```
http://vCenter-server:9443/
```

where *vCenter-server* is the vCenter Server network hostname or IP address.

The **vSphere Web Client** page appears.

2. Download and install the vSphere 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.

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

      The installation wizard appears.

   c. Follow the onscreen instructions.

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

   ```
   http://vCenter-server:9443/
   ```

   where *vCenter-server* is the vCenter Server network hostname or IP address.

   The **vSphere Web Client** page appears.

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

5. Select **Home** > **vCenter** > **Hosts and Clusters**.

6. Select **Actions** > **Deploy OVF Template**.

7. Allow plug-in access control.

   The **Deploy OVF Template** wizard appears.

8. In the **Source** screen:

   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.

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

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

   e. Click **Next**.

9. In the **OVF Template Details** screen:

   a. Ensure that the template information is correct.

   b. Click **Next**.

10. In the **Select name and Location** screen:

    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.

Note

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 three contexts.

---

b. In the tree, select a datacenter and folder location for this proxy.

c. Click **Next**.

11. In the **Select a resource** screen:

a. Select an ESX host, cluster, vApp or resource pool.

b. Click **Next**.

12. In the **Select Storage** screen:

a. Select a storage location for this proxy.

b. Click **Next**.

13. In the **Setup networks** screen:

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

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

c. Click **Next**.

14. In the **Customize template** screen:

Note

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 **Customize template** screen are correct.

---

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

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

c. If not using DHCP, type a valid IP address for this proxy in the **Isolated Network IP Address** field

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

e. Click **Next**.

15. In the **Ready To Complete** screen:

a. Ensure that the information is correct.

b. Click **Finish**

Registering and activating the proxy with the Avamar server

Register and activate each proxy deployed in vCenter with the Avamar server.

Before you begin

1. Deploy the proxy appliance in vCenter.
2. Add the ESX host as a vCenter client in Avamar.

Note

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.

Perform this task for every proxy you deploy in an ESX host.

Procedure

1. From the vSphere client, locate and select an Avamar image backup proxy.
2. Right-click **Power** > **Power On**.
3. Right-click**Open Console**.

   A console window appears.
4. From the **Main Menu**, type `1`, and then press **Enter**.
5. Type the Avamar server DNS name, and then press **Enter**.
6. Type an Avamar server domain name, and then press **Enter**.

   The default domain is “clients.” However, your Avamar system administrator may have defined other domains, and subdomains. Consult your Avamar system administrator for the 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.

   ---
7. From the **Main Menu**, type `2`, and then press **Enter** to quit.
8. (optional) If proxy certificate authentication is required, see Configuring vCenter-to-Avamar authentication on page 27

Configuring proxy settings in Avamar Administrator

After deploying a proxy appliance in vCenter and registering it with the Avamar server, configure datastore, group and optional contact settings in Avamar Administrator.

Before you begin

1. Deploy a proxy appliance in vCenter.
2. Register and activate the proxy with the Avamar server.

Procedure

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

   The **Administration** window appears.
2. Click the **Account Management** tab.
3. In the tree, select the proxy, and then select **Actions** > **Account Management** > **Client Edit**.

   The **Edit Client** dialog box appears.
4. Click the **Datastores** tab, and then select all vCenter datastores that host virtual machines you want to protect with this proxy.
5. Click the **Groups** tab, and then assign this proxy to one or more groups by clicking the **Select** checkbox next to each group.
6. (Optional) provide contact information:

   a. Type a contact name in the **Contact** field.

   b. Type a contact telephone number in the **Phone** field.

   c. Type a contact email address in the **Email** field.

   d. Type a contact location in the **Location** field.
7. Click **OK**.

Performing optional proxy performance optimization

By default, Avamar proxies are configured with four virtual CPU sockets and one core per socket. However, if your ESXi host has two or more physical CPUs, changing the proxy configuration to four virtual CPU sockets and two cores per socket will achieve better backup and restore performance.

APPENDIX B

vSphere Data Ports

This appendix includes the following topics:

Required data ports

These are the required data ports in a vSphere environment.

Table 12 Required vSphere data ports

Port	Source	Destination	Function	Additional information
22	Avamar Administrator	Proxies	SSH	Diagnostic support. Optional, but recommended.
53	Proxies	DNS server	DNS	UDP+TCP
443	Avamar Deployment Manager	ESXi hosts	vSphere API	
443	Proxies	ESXi hosts	vSphere API	
443	Proxies	vCenter	vSphere API	
443	Avamar MCS	vCenter	vSphere API	
902	Proxies	ESX hosts	VDDK	
5489	Avamar Deployment Manager	Proxies	CIM service	Used to register the proxy.
7444	Avamar MCS	vCenter	Test vCenter credentials	
27000	Proxies	Avamar server	GSAN communication	Non-secured communication
28009	Avamar MCS	Proxies	Access proxy logs	
28102 - 28109	Avamar MCS	Proxies	`avagent` paging port	Avamar 7.0 and 7.1
29000	Proxies	Avamar server	GSAN communication	Secured communication
30001	Proxies	Avamar MCS	`avagent` to MCS communication	Avamar 7.2
30102-30109	Avamar MCS	Proxies	`avagent` paging port	Avamar 7.2

Note

All ports are TCP unless otherwise noted.

APPENDIX C

Plug-in Options

This appendix includes the following topics:

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 plug-in type.

You specify plug-in options in Avamar Administrator for on-demand backup or restore operations, or when you create a dataset for a scheduled backup. You set plug-in options with the graphical user interface (GUI) controls (text boxes, checkboxes, radio buttons, and so forth). In addition to using the GUI controls for the options, you can type an option and its value in the **Enter Attribute** and **Enter Attribute Value** fields.

NOTICE

The Avamar software does not check or validate the information that you type in the **Enter Attribute** and **Enter Attribute Value** fields. In addition, the values in the **Enter Attribute** and **Enter Attribute Value** fields override settings that you specify with the GUI controls for the options.

VMware Image plug-in options

These backup and restore options are available for the Avamar VMware Image plug-in.

Table 13 Backup options for Avamar VMware Image plug-in

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 backups 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 EMC Data Domain System Integration Guide* provides instructions.

Table 13 Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
Encryption method to Data Domain system	Specifies the encryption method for data transfer between the client and the Data Domain system during the backup.
Guest credentials	
Username	Guest operating system user account with sufficient privileges to run scripts.
Password	Password for the guest operating system username.
Pre-snapshot Script	
Script file	Full path and filename of the script that will be run before the vmdk snapshot.
Maximum script run time (minutes)	Maximum number of minutes this script is allowed to run before timing out.
Post-snapshot Script	
Script file	Full path and filename of the script that will be run after the backup completes and the vmdk snapshot is removed.
Maximum script run time (minutes)	Maximum number of minutes this script is allowed to run before timing out.

Table 14 Restore options for Avamar VMware Image plug-in

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.
Encryption method from Data Domain system	Specifies the encryption method for data transfer between the Data Domain system and the client during the restore.

Windows VMware GLR plug-in options

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

APPENDIX D

Troubleshooting

This appendix includes the following topics:

Installation and configuration problems and solutions

These are common installation and configuration problems and 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 the vCenter.

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

Proxy network settings

If a proxy is 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.

The vCenter documentation provides instructions for changing virtual appliance network settings.

Error when registering guest backup or Windows recovery target client

If a virtual machine has been added to the Avamar server because it resides in a vCenter domain, and you want to also protect that same virtual machine using guest backup, or use that same virtual machine as a recovery target for mounting Windows VMDKs, then you must change the `mcserver.xml` `allow_duplicate_client_names` preference setting to true.

Backup problems and solutions

These are 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.
- Ensure that the datastore for the source virtual machine has been selected on a running proxy server.

If that does not resolve the problem, the account used to connect to vCenter might not have sufficient privileges. To verify account privileges, log in to the vSphere Client or vSphere Web 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.

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.

Proxies are not assigned to backup jobs

Any time you restart the MCS, it might take some time until all proxies reconnect to the MCS and are available for backups. Additionally, if you stop the MCS and do not restart it within five minutes, proxies go into a sleep mode for at least 40 minutes.

To verify that a proxy is able to connect to the MCS, view that proxy's avagent.log file and ensure that messages similar to the following appear at the end of the log history:

```
2014-03-20 20:34:33 avagent Info <5964>:
Requesting work from 10.7.245.161
2014-03-20 20:34:33 avagent Info <5264>:
Workorder received: sleep
2014-03-20 20:34:33 avagent Info <5996>:
Sleeping 15 seconds
```

VM snapshot fails backups due to incorrect pre-evaluation of available space.

The "snapshot_max_change_percent" flag tells the proxy to pre-evaluate free datastore space to ensure that there is enough storage for the VM snapshot. The default value is set to 5%. If the proxy incorrectly fails the backup due to the perceived lack of storage, the value can be overridden by either changing the percentage to "0" by the user of the policy, or by permanently overriding the value in the proxy command file.

To permanently override this check in the proxy, log into each proxy, modify the file "/usr/local/avamarclient/avvcbimageAll.cmd" to include the line:

```
-- snapshot_max_change_percent=0
```

This will disable this feature.

Backup and restore of vFlash Read Cache enabled VMs will use NBD transport mode

Backup and restore of vFlash Read Cache enabled VMs will use NBD transport mode by default

vCenter will display the error:

```
The
device or operation specified at index '0' is not supported for the
current virtual machine version 'vmx-07'. A minimum version of
'vmx-10' is required for this operation to succeed
```

If hot-add is desired then please upgrade the proxy hardware version to vmx-10 or above.

Restore problems and solutions

These are 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.
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.
   b. Click **More**.
   c. Type **`[avvcbimage]skip_snapshot_check`** in the **Enter Attribute** field.
   d. Type **`true`** in the **Enter Attribute Value** field.
   e. Click **+**.
   The [avvcbimage]skip_snapshot_check=true entry appears in the plug-in options list.

f. Click **OK**.

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.
2. This new virtual machine must have the same number of virtual disks as the original virtual machine from which the backup was taken.
3. Manually add the new virtual machine to Avamar.
4. Restore the data to this virtual machine.

FLR browse of a granular disk backup without a partition table is not supported

When a non-LVM granular disk backup is performed of a disk that does not have a partition table, FLR browsing of the backup will fail with the error:

```
Failed to mount disks. Verify that all the disks on the VM have
valid/supported partitions.
```

The workaround for this issue is to perform a full image backup of all disks on the VM, then restore the files or folders from the disk that does not have a partition table.

Fault tolerance disabled when restore to new virtual machine is performed

When a fault-tolerant virtual machine is restored to a new virtual machine, fault tolerance is disabled. You will need to enable fault tolerance after the machine is restored to a new virtual machine. VMware documentation contains information regarding how to enable fault tolerance.

Restore to new virtual machine to Virtual SAN 5.5 will fail

Restore to new virtual machine to a Virtual SAN 5.5 will fail with the message `unable to access file` if the restore is of a multiple disk VM using a mix of datastore types (VSAN and VMFS or NFS and the restore of first disk is to a non-VSAN datastore. To workaround this issue, select a VSAN datastore for the first disk of the VM. This issue is not seen in VSAN 6.0.

Powering on an instant access vFlash-VM backup to a host without flash capacity configured fails

Powering on an instant access vFlash-VM backup to a host without flash capacity configured fails with the following error:

```
The available virtual flash resource '0' MB ('0' bytes) is not
sufficient for the requested operation
```

To workaround this issue, disable flash cache in VM before powering on.

GLOSSARY

A

activation The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

See also client activation

application-consistent The state of a virtual machine in which the virtual file system writes have been completed and all running applications have been quiesced.

Avamar Administrator A graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or Linux client computer.

Avamar server The server component of the Avamar client/server system. Avamar server is a fault-tolerant, high-availability system that efficiently stores the backups from all protected clients. It also provides essential processes and services required for data restores, client access, and remote system administration. Avamar server runs as a distributed application across multiple networked storage nodes.

B

backup A point-in-time copy of client data that can be restored as individual files, selected data, or as an entire backup.

C

changed block tracking (CBT) A VMware feature that tracks which virtual machine file system blocks have changed between backups.

client activation The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

See also activation

client registration The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during *client activation*.

See also registration

crash-consistent The state of a virtual machine that is consistent with what would occur by interrupting power to a physical computer. Because file system writes might or might not be in progress when power is interrupted, there is always the possibility of some data loss when backing up a crash-consistent file system.

D

datacenter In VMware vSphere environments, a datacenter comprises the basic physical building blocks. These physical building blocks include virtualization servers, storage networks and arrays, IP networks, and a management server. Each vSphere vCenter can manage multiple datacenters.

Data Domain system Disk-based deduplication appliances and gateways that provide data protection and disaster recovery (DR) in the enterprise environment.

dataset A policy that defines a set of files, directories, and file systems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

datastore In VMware vSphere environments, a datastore is the storage resources used by a datacenter.

E

ESX/ESXi Server A virtualization layer run on physical servers that abstracts processor, memory, storage, and resources into multiple virtual machines. ESX Servers provide an integrated service console; ESXi Servers do not.

F

file system-consistent The state of a virtual machine in which the virtual file system has been quiesced (that is, all file system writes have been completed).

G

group A level of organization in Avamar Administrator for one or more Avamar clients. All clients in an Avamar group use the same group policies, which include the *dataset*, *schedule*, and *retention policy*.

group policy The *dataset*, *schedule*, and *retention policy* for all clients in an Avamar group.

guest backup A method of protecting a virtual machine in which backup software is installed directly in the guest operating system just as if it were a physical machine.

I

image backup A method for protecting virtual machines hosted in a vCenter in which a backup is taken of entire virtual disk images. Avamar for VMware image backup is fully integrated with vCenter Server to provide detection of virtual machine clients, and enable efficient centralized management of backup jobs

M

MCS Management console server. The server subsystem that provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by *Avamar Administrator*.

P

plug-in Avamar client software that recognizes a particular kind of data resident on that client.

plug-in options Options that you specify during backup or restore to control backup or restore functionality.

proxy A virtual machine that is used to perform image backups, image restores, and file-level restores of other virtual machines. Proxies run Avamar software inside a Linux virtual machine, and are deployed in a vCenter using an appliance template (.ova) file.

R

registration The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during *client activation*.

See also client registration

restore An operation that retrieves one or more file systems, directories, files, or data objects from a backup and writes the data to a designated location.

retention The time setting to automatically delete backups on an Avamar server. Retention can be set to permanent for backups that should not be deleted from an Avamar server. Retention is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

S

schedule The ability to control the frequency and the start and end time each day for backups of clients in a group. A schedule is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

Storage vMotion A VMware feature the enables migration of a live virtual machine from one datastore to another.

V

vCenter Server A centralized single point of management and control for one or more VMware datacenters.

vSphere Client A VMware software application used to control and manage a vCenter. The vSphere Client is also known as the "thick client."

vSphere Web Client A VMware web interface used to control and manage a vCenter.