Dell Avamar for VMware 19.10

User Guide

Dell Inc.

October 2024
Rev. 03

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Figures..8

Tables...9

Preface..10

Chapter 1: Introduction...14

Avamar for VMware data protection overview.. 14

Image backup... 14

Guest backup.. 16

Considerations..17

Changed block tracking..18

Image backup virtual machine quiescing.. 19

Image backup and recovery support in Amazon Web Services (AWS)..19

Chapter 2: Configuration and Setup...21

Best practices..21

(Optional) Configuring support for multiple vCenters.. 22

Installing Avamar Administrator software.. 22

Configure vCenter-to-Avamar authentication..23

Add vCenter authentication certificates to the MCS keystore.. 23

Disabling MCS certificate authentication...24

Creating a dedicated vCenter user account...24

Add a vCenter as an Avamar client in the AUI...26

Register or add a proxy client... 28

Edit vCenter 29

Auto-discovery of virtual machines.. 29

Domain mapping rules for VM auto-discovery...30

Creating a rule..30

Deploying proxies using Proxy Deployment Manager from AUI..30

Proxy Deployment Manager.. 30

Deploy proxies... 32

Add gateway for DualNIC setup.. 34

Upgrading proxies.. 34

Upgrading Avamar proxies... 35

Upgrading older or manually deployed Avamar proxies...35

Maintaining proxies... 38

Reregistering a proxy with an Avamar server.. 38

Changing the proxy guest operating system admin password...38

Changing the proxy guest operating system root password..39

Monitor proxy status.. 39

View Proxy Status...39

Configure email notification for proxy status alert..39

Import custom certificate in Avamar VMware Image Backup Proxy..40

Security patch updates for proxies.. 41

Best practices and troubleshooting for applying security patch updates to proxies.....42
Apply security patch updates to a proxy.....42
Additional Avamar server configuration.....43
Configuring automatic proxy selection.....43
Configuring the MCS to support both guest and image backup.....44

Chapter 3: Administration.....45
Clients and containers.....45
Dynamic versus static containers.....45
Dynamic container behavior.....45
How independent and container protection interact.....46
Add a VMware client.....46
Delete a VMware client.....48
Enable changed block tracking.....48
Viewing protected virtual machines in Avamar Administrator.....49
Viewing a replicated virtual machine name in Avamar Administrator.....49
Monitoring the vCenter connection in Avamar Administrator.....49
Manually synchronize the AUI with vCenter and VM clients.....50
Rename a vCenter client.....50
VMware Image Dataset.....51
Adding guest backup throttling parameters to a dataset in Avamar Administrator.....51
Groups.....52
Default Proxy Group.....52
Default Virtual Machine Group.....52
Virtual machine and proxy relationships within groups.....52
Changing proxy datastore and group assignments in Avamar Administrator.....53

Chapter 4: Backup.....54
Limitations.....54
Perform an on-demand backup of a virtual machine by using AUI 55
Set advanced plug-in options in the AUI.....56
Schedule backups using the AUI Policy wizard.....57
Creating a dataset.....58
Scheduling backups using the Policy wizard.....59
Create a backup policy.....59
Enable a scheduled backup for a backup policy.....59
Automatically include virtual machines in a backup policy using dynamic rules.....60
Log truncation backups.....64
Scheduled backups with Microsoft SQL log truncation.....64
Scheduled backups with Microsoft Exchange log truncation.....65
Monitor backups.....67
Cancel backups.....67
Support for vCenter HA failover for inflight backups.....67
Configure a backup to support VMware encryption.....67
Configure a backup to support VMware CEIP.....68
VMware encryption support limitations.....68
Configure a backup to support vSAN encryption.....69
Enforcement of backups to Data Domain.....70

Chapter 5: Restore.. 71
Image and file-level restore guidelines.. 71
Year 2038.. 71
Monitor restores.. 71
Cancel restores.. 72
Instant access.. 72
Restore an instance of a VM backup by using the AUI.. 74
Image backup overview.. 79
Image-level restore limitations.. 79
Restore the full image or selected drives to the original virtual machine.. 80
Restore the full image or selected drives to a different virtual machine.. 81
Restore the full image or selected drives to a new virtual machine by using Avamar Administrator..... 82
File Level Restore.. 83
Performance improvements for File Level Restore.. 83
File-level restore supported configurations.. 84
RSA SecurID authentication in the AUI.. 85
File Level Restore troubleshooting and limitations.. 87
File Level Restore (FLR) in the AUI.. 88
Restore ACL for non-root user configuration.. 89
Perform a File Level Restore (FLR) operation by using the Data Protection Backup and Recovery File Level Restore (FLR) UI.. 90
Restore VM tags.. 91

Chapter 6: Backup Validation.. 92
Overview.. 92
What is validated.. 92
VM backup validation groups.. 92
Performing an on-demand backup validation.. 92
Scheduling backup validations.. 93

Chapter 7: Protecting the vCenter Management Infrastructure.. 95
vCenter deployments overview.. 95
Best practices for backup and restore.. 95
Protecting an embedded PSC.. 96
Protecting external deployment models.. 96
vCenter server appliance(s) with one external PSC where PSC fails.. 97
vCenter server appliance is lost but the PSC remains.. 97
vCenter server appliance with multiple PSCs where one PSC is lost, one remains.. 98
vCenter server appliance remains but all PSCs fail.. 98
vCenter server appliance remains but multiple PSCs fail.. 98
vCenter server appliance fails.. 98
vCenter server restore workflow.. 99
Platform Services Controller restore workfow.. 100
Command reference.. 100
Support for vCenter HA failover for inflight backups.. 101
Additional considerations.. 101

Chapter 8: Protecting ESX Hosts.. 102

Overview....102
Limitations.... 102
Task List....102
Adding ESX host authentication certificates to the MCS keystore....103
Creating a dedicated ESXi host user account....104
Adding an ESX host as a vCenter client....105
Deploying a proxy in a stand-alone ESX host....106
Deploying a proxy appliance in an ESX host using the vSphere Client.... 106
Manually configuring proxy network settings....107
Registering and activating the proxy with the Avamar server....108
Disassociating an ESX host from a vCenter.... 108

Chapter 9: Avamar Image Backup and Recovery for VMware Cloud on Amazon Web Services (AWS).... 109
Avamar image backup and recovery for VMware Cloud on AWS.... 109
Configure the VMware Cloud on AWS web portal console.... 109
Amazon AWS web portal requirements.... 110
vCenter server inventory requirements....110
Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS....110
Configure vCenter-to-Avamar authentication for VMware Cloud on AWS.... 111
Avamar image backup and restore for VMware Cloud on AWS best practices....111
Unsupported Avamar operations.... 112

Chapter 10: Backing up VMware Cloud Foundation (VCF) Components on VxRail....113
VCF and VxRail overview.... 113
VCF components and backup methods.... 113
Backup prerequisites.... 114
The backup script....114
Quick protection.... 115
Selective protection: SDDC and NSX-T Managers....116
Selective protection: vCenter servers....117
Selective protection: VCF Image-based components....118
Other Operations....118
Backup-script troubleshooting....119

Appendix A: Manually deploying proxies....121
Overview....121
Downloading the proxy appliance template file....121
Deploying the proxy appliance in vCenter....121
Deploying a proxy appliance in vCenter using the vSphere Web Client....122
Registering and activating the proxy with the Avamar server.... 123
Configuring proxy settings in Avamar Administrator.... 124
Performing optional proxy performance optimization.... 124

Appendix B: vSphere Data Ports.... 125
Required data ports.... 125

Appendix C: Using VMware vRealize Log Insight....127
About VMware vRealize Log Insight.... 127

Configuring the Log Central Reporting Service........ 127
Configuring Log Forwarding Agents........ 128

Appendix D: Plug-in Options........ 129
How to set plug-in options........ 129
VMware Image plug-in backup options........ 129
VMware Image plug-in restore options........ 131
Windows VMware GLR plug-in options........ 131

Appendix E: Troubleshooting........ 132
Installation and configuration problems and solutions........ 132
Problems adding vCenter Server as Avamar client........ 132
Proxy network settings........ 132
Error when registering guest backup or Windows recovery target client........ 132
Backup problems and solutions........ 132
Backup does not start........ 132
Exclude the proxy from the virtual machine backup if performing the backup with other VMware software........ 133
Backups fail with No Proxy errors........ 133
Changed block tracking does not take effect........ 136
Proxies are not assigned to backup jobs........ 136
VM snapshot fails backups due to incorrect pre-evaluation of available space........ 136
Backup and restore of vFlash Read Cache enabled VMs will use NBD transport mode........ 136
Exchange log truncation unsupported when VMDK is encrypted via vSphere........ 137
Indexing VMware image backups requires HotAdd transport mode........ 137
Proxy status alert........ 137
Restore problems and solutions........ 138
Preexisting snapshots cause restores to fail........ 138
Restore to new virtual machine not available when physical RDM disks are involved........ 138
FLR browse of a granular disk backup without a partition table is not supported........ 139
Fault tolerance disabled when restore to new virtual machine is performed........ 139
Restore to new virtual machine to Virtual SAN 5.5 will fail........ 139
Powering on an instant access vFlash-VM backup to a host without flash capacity configured fails........ 139
Maximum number of NFS mounts with instant access issue........ 139
FLR on RHEL 5 requires the standard C++ library........ 140
FLR of a folder or file name that contains certain special characters fails........ 140
FLR to user profile fails when Admin Approval Mode is enabled........ 140
A VM-based FLR fails in the virtual machine interface........ 140

Glossary........ 141

Figures

1 Image backup diagram....14
2 Default proxy virtual machine specifications.... 15
3 Example independent and container protection....46
4 Selected VMware Entities drop-down....47
5 Virtual machine and proxy relationships within groups.... 52
6 Example nested container structure....55
7 Example nested container structure....80
8 vCenter server restore workflow.... 99
9 PSC restore workflow....100
10 No proxy error....133
11 No proxy error on activity monitor....134
12 On-demand VMware Image backup fails....134
13 Event details of failed backup....135

Tables

1 Revision history.....10
2 Style conventions.....11
3 Guest backup installation resources.....16
4 Minimum required vCenter user account privileges.....24
5 Example chart for gathering proxy information.....35
6 Example chart for gathering proxy information, continued.....35
7 Virtual machine properties.....36
8 Rule filters.....61
9 Filter operator.....61
10 Examples for rules with regular expressions.....62
11 Required permissions for the Avamar Administrator.....69
12 Image restore toolbar buttons.....79
13 FLR support partitioning scheme.....84
14 File system support for FLR.....84
15 LVM support for FLR.....84
16 Windows Dynamic Disk support for FLR.....85
17 Multidevice support for FLR.....85
18 Minimum required ESXi host user account privileges.....104
19 VCF component of file-based backups.....113
20 VCF components of image-based backups.....114
21 Backup-retention values.....117
22 Error codes and explanations.....119
23 Required vSphere data ports.....125
24 Backup options for Avamar VMware Image plug-in.....129
25 Restore options for Avamar VMware Image plug-in.....131
26 Proxy details.....137

Preface

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

Contact a technical support professional when a product does not function correctly or does not function as described in this document.

ⓘ **NOTE:** This document was accurate at publication time. To find the latest version of this document, go to Dell Support.

Purpose

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

Audience

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

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

A comprehensive discussion of basic Avamar system administration concepts and principles, such as clients, datasets, schedules, retention policies, and backup policies, is beyond the scope of this publication. The *Avamar Administration Guide* provides details.

Revision history

The following table presents the revision history of this document.

Table 1. Revision history

Revision	Date	Description
03	October 2024	Updated the "Required data ports" section.
02	September 2024	Updated the "RSA SecurID authentication in the AUI" section.
01	January 2024	First release of this document for Avamar 19.10

Related documentation

The following Dell publications provide additional information:

- *E-LAB Navigator* at E-Lab Navigator
- *Avamar Release Notes*
- *Avamar Administration Guide*
- *Avamar Operational Best Practices Guide*
- *Avamar Product Security Guide*
- *Avamar Backup Clients User Guide*
- *Avamar for Exchange VSS User Guide*

- *Avamar for IBM DB2 User Guide*
- *Avamar for Lotus Domino User Guide*
- *Avamar for Oracle User Guide*
- *Avamar for SharePoint VSS User Guide*
- *Avamar for SQL Server User Guide*
- *Avamar vSphere Web Client Administration 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*

Typographical conventions

Table 2. Style conventions

Formatting	Description
Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: ● System code ● System output, such as an error message or script ● Pathnames, filenames, prompts, and syntax ● Commands and options
`Monospace italic`	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information 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 resolve a product issue before contacting Customer Support.

To access the Avamar support page:

1. Go to Dell Support.
2. Type a product name in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box.
3. Select the product from the list that appears. When you select a product, the **Product Support** page loads automatically.
4. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Product Support** page.

Documentation

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

- 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 Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to Dell Support.
2. Under the **Support** tab, click **Knowledge Base**.
3. Type either the solution number or keywords in the search box. Optionally, you can limit the search to specific products by typing a product name in the search box and then selecting the product from the list that appears.

Online communities

Go to Community Network at Dell Community for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all products.

Live chat

To engage 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 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 a 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

It is recommended to enable Dell Connectivity and Email Home on all Avamar systems:

- Dell Connectivity automatically generates service requests for high priority events. To configure Dell Connectivity, see *Avamar Administration Guide* for detailed steps.
- Email Home sends configuration, capacity, and general system information to Customer Support.

Comments and suggestions

Feedback helps to improve the accuracy, organization, and overall quality of publications. Perform one of the following steps to provide feedback:

- Go to Content Feedback Portal, and submit a ticket.
- Send feedback to DPADDocFeedback@dell.com.

1

Introduction

Topics:

- Avamar for VMware data protection overview
- Changed block tracking
- Image backup virtual machine quiescing
- Image backup and recovery support in Amazon Web Services (AWS)

Avamar for VMware data protection overview

Avamar offers two basic ways to protect data residing on VMware virtual machines: image backup, and guest backup.

NOTE: The Avamar AUI is only supported in stand-alone Windows, Linux, and Solaris x64 environments.

NOTE: Any references to the Data Domain systems and the Data Domain devices in the document indicate PowerProtect DD appliances.

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.

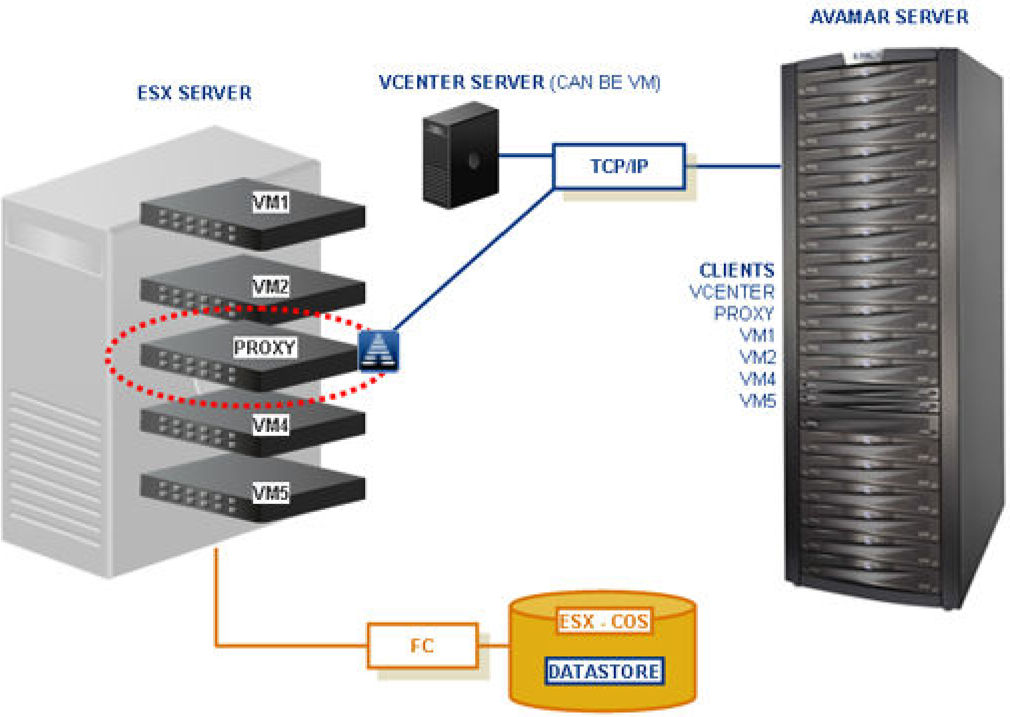


Figure 1. Image backup diagram

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 can perform eight simultaneous backup or restore operations, in any combination.

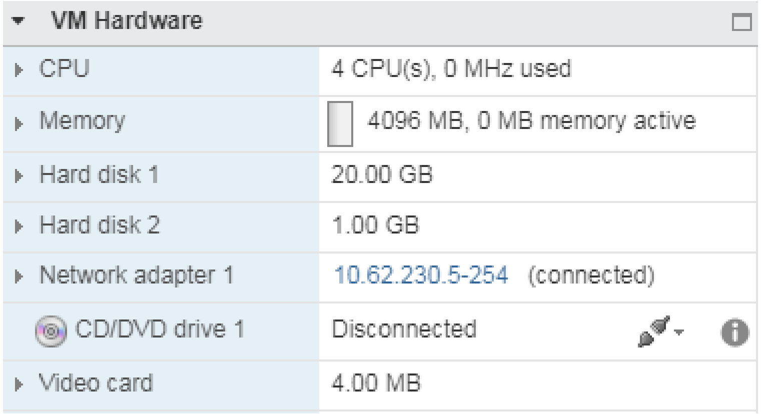
Proxies are allowed in any part of the Avamar Administrator account management tree except the vCenter Server domain or subdomains. Also, you should not activate proxies into the root domain (`/`). Otherwise, this action causes problems during system migration.

Although it is possible to restore across data centers (use a proxy that is deployed in one data center to restore files to a virtual machine in another data center), restores take noticeably longer than if the proxy and the target virtual machine are in the same data center. For best performance, use the Proxy Deployment Manager which recommends the ideal deployment configuration.

Default proxy virtual machine specifications

The following figure outlines the default requirements for the proxy virtual machine.

NOTE: The IP address that is assigned to the network adapter belongs to the guest network.



VM Hardware	
CPU	4 CPU(s), 0 MHz used
Memory	4096 MB, 0 MB memory active
Hard disk 1	20.00 GB
Hard disk 2	1.00 GB
Network adapter 1	10.62.230.5-254 (connected)
CD/DVD drive 1	Disconnected
Video card	4.00 MB

Figure 2. Default proxy virtual machine specifications

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 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 that are 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	*Avamar Backup Clients User Guide*
Linux file systems: ● Debian ● CentOS ● Red Hat ● SUSE ● Ubuntu	*Avamar Backup Clients User Guide*
UNIX file systems: ● HP-UX ● Solaris	*Avamar Backup Clients User Guide*
IBM DB2 databases hosted on IBM AIX, Red Hat and SUSE Linux, and Microsoft Windows	*Avamar for IBM DB2 User Guide*
Lotus Domino databases	*Avamar for Lotus Domino User Guide*
Mac OS X file systems	*Avamar Backup Clients User Guide*
Microsoft Exchange databases	*Avamar for Exchange VSS User Guide*
Microsoft Office SharePoint implementations	*Avamar for SharePoint VSS User Guide*

Table 3. Guest backup installation resources (continued)

Client	Publication
Microsoft SQL Server databases	*Avamar for SQL Server User Guide*
Microsoft Windows file systems	*Avamar Backup Clients User Guide*
Oracle databases hosted on IBM AIX, Red Hat, and SUSE Linux, Sun Solaris, and Microsoft Windows	*Avamar for Oracle User Guide*

Considerations

There are 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 that is 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
- SharePoint 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.

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 that is 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 that are 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 features that are provided by VMware vStorage API for Data Protection (VADP).

Before 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 this issue, 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. 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.

Image backup and recovery support in Amazon Web Services (AWS)

Avamar proxy provides image backup and restore support for VMware Cloud on AWS.

You can use Avamar to seamlessly deploy and manage VMware workloads across all VMware on-premises and AWS environments.

Consider the following points:

- VMware vSphere 6.5 or greater is required.
- There is no network connection between the ESXi host and the Avamar proxy on VMware Cloud on AWS. A vCenter is required for communication.
- User privileges are limited on VMware Cloud on AWS.
- Supports virtual machines that reside in a workload service pool.
- Avamar Virtual Edition support for VMware tags with SSO service.

Prerequisites

Review the following item before you begin:

- If you use NSX-T, configure DNS to resolve to the internal IP address of the vCenter server. Click **SDDC Management** > **Settings** > **vCenter FQDN** and select the private vCenter IP address so that you can directly access the management network over the built-in firewall. Open TCP port 443 for the vCenter server in both the management gateway and the compute gateway. VMware KB article 70846 provides more information.

Limitations

The following features are not supported:

- Application consistent backup
- File-level restore from an image-level backup if using NSX-V. Note that this is not a limitation if using NSX-T.
- Proxy deployment manager. Proxies must be deployed manually.
- Instant access recovery of an image-level backup
- Emergency restores (image restore directly to an ESXi host, bypassing the vCenter).
- Image-level backups and restores using NBD, NBDSSL, or SAN transport mode. Only HotAdd is supported.
- Advanced policy-based data protection for MS-SQL using Avamar.
- Application-aware image backups for MS-SQL and MS-Exchange.
- Image backup and restore when the data center is under a folder.
- Data exclusion
- Proxy appliance that is configured with dual-stack or IPv6-only.
- Restore to new vApp.
- IPV6

Workarounds

- If you use NSX-T and perform an image restore with **Select Post Restore Options** set to `Power on VM with NICs enabled`, the VM network adapter may not connect. To work around this limitation without restarting the VM:
  1. Right-click the VM and select **Edit Settings** > **Network adapter**.
  2. Change the network to `VM Network`.
  3. Click **Apply**.
  4. Click **Edit Settings** > **Network adapter**.
  5. Change the network to `NSX-T Network`.
  6. Click **Connect**.

2

Configuration and Setup

Topics:

- Best practices
- (Optional) Configuring support for multiple vCenters
- Installing Avamar Administrator software
- Configure vCenter-to-Avamar authentication
- Creating a dedicated vCenter user account
- Add a vCenter as an Avamar client in the AUI
- Register or add a proxy client
- Edit vCenter
- Auto-discovery of virtual machines
- Deploying proxies using Proxy Deployment Manager from AUI
- Add gateway for DualNIC setup
- Upgrading proxies
- Maintaining proxies
- Monitor proxy status
- Import custom certificate in Avamar VMware Image Backup Proxy
- Security patch updates for proxies
- Additional Avamar server configuration

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.

Use indirect root login for proxies

Direct root login for proxies is no longer available. Instead, when a procedure requires root access, log in as the admin user, and then change to the root user by typing **`su -`**. This behavior corresponds to the existing root login configuration for the Avamar server.

Network settings

If you do not restore network settings after a restore operation, ensure that you manually configure network settings after the operation completes.

(Optional) Configuring support for multiple vCenters

Avamar 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.

Steps

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 the following command:

   ```
   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" />
      ```

      By default, the `maxJavaHeap` parameter is 2G. Use the following command to change the parameter:

      ```
      entry key="maxJavaHeap" value="-Xmx3G" merge="keep"
      ```
6. Close `mcserver.xml` and save the changes.
7. Start the MCS and the scheduler by typing the following command:

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

Installing Avamar Administrator software

Install Avamar Administrator software on your Windows computer.

Steps

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

   `https://Avamar_server/dtlt/home.html`

   where *Avamar_server* is the DNS name or IP address of the Avamar server.

   The **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.

Configure vCenter-to-Avamar authentication

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

About this task

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.

Add vCenter authentication certificates to the MCS keystore

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

Prerequisites

ⓘ **NOTE:** Importing the same certificate with a different alias name is not permitted.

Steps

1. Log in to the Avamar AUI with Administrator privileges. Open a web browser and type the following URL:

    `https://`*`Avamar_server`*`/aui`

    Where *Avamar_server* is the DNS name or IP address of the Avamar server.

    ⓘ **NOTE:** If your environment does not meet HTTPS certificate validation requirements, the certificate validation fails and an error message appears asking if you want to continue to download packages. Ignoring certificate validation might cause security issues.

    a. In the **Avamar Username** field, type a username with administrative privileges.
    b. In the **Avamar Password** field, type the password for the administrative user.
    c. Select **Avamar** as the **Auth Type**.
    d. Click **Log In**.
2. In the AUI navigation pane on the left, click », and then click **Administration** > **System**.
    The **System** window appears.
3. Select the **Certificate** tab, and then click **+IMPORT CERTIFICATE** under the **Trust Certificate** tab.
    The **Import Certificate** dialog box appears.

    ⓘ **NOTE:** If the vCenter certificate and the Avamar web server certificate are issued by the same CA, you need not import the trusted certificates again for vCenter connection. To check Avamar web server certificate, check the **Raw** field in the private entry details of the **Private Key** tab.
4. Import the vCenter trust certificate by specifying the following information:
    a. In the **Base Information** window, perform the following steps:
        i. Specify the alias name for the vCenter certificate.
        ii. Click the **BROWSE** button to browse and import the vCenter certificate.
        iii. Click **NEXT**.

b. (Optional) On the **Validation** window, specify the IP address of the vCenter, the Port number as **443**, and then click **VALIDATE**.
The **Validation Result** appear window is displayed, where you can view if the validation is successful or failed. If the validation fails, verify the inputs again.

If you skip validation and proceed with importing the certificate, the **IP** and **Port** fields are disabled.

> ⓘ **NOTE:** Although validation is optional, for vCenter authentication certificates, it is recommended that you perform this step to ensure that there is successful communication between Avamar and the vCenter server. The validation only works with the vCenter that has a self-signed certificate or a certificate that is issued by 1-level CA. Skip the validation if your vCenter has a certificate that is issued by multilevel CA.

5. Click **FINISH**.
The successfully imported vCenter certificates are displayed under the **Trust Certificate** tab. You can view and delete the vCenter certificates by clicking the View and Delete icons, respectively.

> ⓘ **NOTE:** To import the parent vCenter trusted certificate, open a web browser and go to **https://*vCenter IP***, then right-click **Download Root CA certificate** in the bottom-right corner of the window and select **Save As...** to extract the file. It is not necessary to restart the MCS after the vCenter certificate is imported to the MCS keystore.

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.

Steps

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 the following command:

   ```
   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 the changes.
7. Start the MCS and the scheduler by typing the following command:

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

Creating a dedicated vCenter user account

We strongly recommend that you set up a separate user account on each vCenter that is strictly dedicated for use with Avamar.

About this task

Using a separate vCenter user account ensures maximum clarity if it becomes necessary to examine vCenter logs. 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.

> ⓘ **NOTE:** The user account must be added to the top (root) level in each vCenter that you intend to protect. If you create the user account at any other level (for example, at a datacenter level), backups fail.

Table 4. Minimum required vCenter user account privileges

Privilege type	Required privileges
Alarms	• Create alarm

Table 4. Minimum required vCenter user account privileges (continued)

Privilege type	Required privileges
	● Edit alarm
Datastore	● Allocate space ● Browse datastore ● Configure datastore ● Low levefile operations ● Move datastore ● Remove datastore ● Delete File ● Rename datastore
Extension	● Register extension ● Unregister extension ● Update extension
Folder	● Create folder
Global	● 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
Resource	● Assign virtual machine to resource pool
Sessions	● Validate session
Tasks	● Create task ● Update task
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 virtuadisk ● Host USB device ● Memory ● Modify device settings ● Raw device ● Reload from path ● Remove disk ● Rename ● Reset guest information ● Set annotation ● Settings ● Swapfile placement

Table 4. Minimum required vCenter user account privileges (continued)

Privilege type	Required privileges
	• Upgrade virtual machine Compatibility
Virtual Machine-Guest Operations	• Guest Operation Modifications • Guest Operation Program Execution • Guest Operation Queries
Virtual Machine-Interaction	• Console interaction • DeviceConnection • Guest operating system management by VIX API • Power off • Power on • Reset • VMware Tools install
Virtual Machine-Inventory	• Create from existing • Create new • Register • Remove • Unregister
VirtuaMachine-Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Clone virtual machine • Mark as template
Virtual Machine-Snapshot Management	• Create snapshot • Remove snapshot • Revert to snapshot
vApp	• Export • Import • vApp application configuration

Add a vCenter as an Avamar client in the AUI

Use the following procedure to add a vCenter as an Avamar client in the AUI.

About this task

> **NOTE:** 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:
>
> 1. Retire the existing vCenter client in the AUI.
> 2. Add the vCenter as a vCenter client by using the procedure below.
> 3. Re-invite the retired vCenter client as a normal client to support guest level backup from the vCenter server.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
2. In the domain tree, select a vCenter domain or a sub-domain for the client.

   To select a sub-domain client, toggle the **Include Sub-domain** switch to on.
3. Click ⋮ next to **ADD CLIENT**, and then select **Add VMware vCenter**.

   The **New vCenter Client** wizard appears.
4. In the **New Client Name or IP** field, type the name of the client and then click **NEXT**.

The **vCenter Information** pane appears.

5. In the **vCenter Information** pane, compete the following information for the vCenter:
    a. In the **User Name** field, type the user account name of the vCenter server administrator.
    b. In the **Password** field, type the password for the vCenter user account.
    c. In the **Verify Password** field, retype the password for the vCenter user account.
    d. In the **Port** field, type the vCenter web services listener data port number.

       443 is the default setting.
    e. Click **NEXT**.

    The **Advanced** pane appears where you can choose to enable the following auto discovery features that include Dynamic VM import by rule or Change Block Tracking.
6. To enable Dynamic VM import by rule, select **Enable Dynamic VM import by rule** and perform the following steps:

    ⓘ **NOTE:** When the VMs are auto-discovered, user defined rules are used by the Avamar software to map the auto-discovered VMs to Avamar domains. User-defined rules are also used to automatically assign backup policies to auto-discovered VMs.

    - To add a rule:
        a. Click **ADD RULE**.
        b. In the **Rule** field, select a rule from the list.
        c. In the **Domain** filed, type the domain that the auto-discovered VM should be included in.

           If the domain entered here does not exist, it is automatically created.
    - To create a rule:

      Rules are used to automatically map auto-discovered VMs to domains, and to assign backup policies to auto-discovered VMs. Rules use one or more filtering mechanisms to determine whether VMs qualify under the rule.

        a. Click **CREATE RULE**.
        b. In the **Rule Name** field, type a name for the rule.
        c. In the **Match Type** field, select whether the rule should match **Any** of the listed filter mechanisms, or **All** of them.

           This selection allows you to configure multiple different filters to select VMs, and to determine how these filters interact with one another to select the correct VMs. For example, you might create a filter that uses a VM folder path to select VMs, and another filter that uses a VM naming convention.

           This option can then be used as follows to determine which VMs are included under this rule:

            ○ To include only VMs that are in the defined folder path and also follow the naming convention, select **All**. This step excludes VMs that are in the folder path but that do not follow the naming convention, and also excludes VMs that follow the naming convention but are not in the folder path.
            ○ To include any VMs that are either in the VM folder path or that follow the naming convention, select **Any**.
        d. In the **Filter** field, select the filter type.

           For example, to create a filter that uses a VM naming convention, select **VM Name**, or to create filter that uses a vCenter VM Tag, select **VM Tag**.

           ⓘ **NOTE:** The **VM Tag** selection is only available with vCenter 6.0 and greater.
        e. In the **Operator** field, select the operand.

           For example, if **VM Name** is selected for the filter type and **begins with** is selected for the operand, then all VMs whose names begin with the filter text is selected.
        f. In the **Value** field, type the filter text.

           For example, to create a filter that selects all VMs whose names begin with the text string `HR_`, select **VM Name** for the filter type, **begins with** for the operand, and type `HR_` for the filter text.
        g. To create additional filters, click the plus sign (**+**).

           This step adds a row to the list of filters. To delete an existing row, click **Delete**.
        h. Click **SUMBIT**.

           Changes made to tags may experience a delay of up to 12 hours before being enforced. For this reason, edit tags with caution, or perform a synchronized vCenter operation, which automatically synchronizes the vCenter with the Avamar server.

Best practice for rule creation is to ensure that rules are mutually exclusive, to avoid the situation where a VM might qualify under multiple rules.

- To enable Change Block Tracking, select **Enable Change Block Tracking**.

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

  Enabling changed block tracking does not take effect until any of the following actions occur on the virtual machine:

  - Restart
  - Power on
  - Resume after suspend
  - Migrate

7. Click **NEXT**.
   The **Optional Information** pane appears.
8. Optional, compete the optional contact information including the contact name, phone number, email, and location, and then click **NEXT**.
   The **Summary** pane appears.
9. Review the client summary information, and then click **ADD**.
   The **Finish** pane appears.
10. Click **FINISH**.

    NOTE: Add IPV6 vCenter to Avamar using FQDN only. IPV6 address is not supported.

Register or add a proxy client

Image-level backup and restore operations require the use of proxy virtual machine clients.

About this task

Client registration is the process of establishing the identity of the proxy virtual machine clients with the Avamar server. Once Avamar “knows” the client, it assigns a unique client ID (CID), which it passes back to the client during activation.

Once the client is added and registered, you can then add a client to the system in a domain and group. This action provides a high degree of control. For example, you can assign a specific dataset, schedule, and retention policy. However, it can be time consuming to add many clients.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
2. To add a proxy virtual machine client, select the **clients** domain in the domain tree.
3. Click ⋮ next to **ADD CLIENT**, and then select **Add VMware Image Proxy**.

   The **New Proxy Client** wizard appears.
4. In the **New Client Name** field, type a unique fully qualified hostname, and then click **NEXT**.

   A proxy can have three different names:

   - The name of the host on which the proxy runs.
   - The DNS name that is assigned to the proxy host.
   - The Avamar client name after the proxy registers and activates with the Avamar server.

   NOTE: To avoid confusion and potential problems, use the same fully qualified hostname for this proxy in all three contexts.

   The **Advanced** pane appears.
5. In the **Advanced** pane, perform the following steps:
   a. In the **vCenter** field, select the vCenter.
   b. To enable auto data store mapping of the proxy, select **Auto DataStore Mapping**.
   c. Click the **Datastores** tab, and then select all vCenter data stores that host machines that you want to protect with this proxy.
   d. Click the **Groups** tab, and then assign this proxy to one or more groups by clicking the checkbox next to each group.

The **Optional Information** pane appears.

6. Optional, complete the optional contact information including the contact name, phone number, email, and location, and then click **NEXT**.
   The **Summary** pane appears.
7. Review the client summary information, and then click **ADD**.
   The **Finish** pane appears.
8. Click **FINISH**.

Edit vCenter

You can edit existing information for vCenter client.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
2. In the hierarchical **Domain** tree, select the vCenter domain.
3. To edit the vCenter client information, Click the overflow menu(⋮), and then select **Edit vCenter**.
   The **Edit Client** dialog box is displayed.
4. Edit the vCenter information. You can edit the name, contact information, or location information for vCenter.
   - In **Basic** tab, you can edit name, domain, and overtime options available for backup.
   - In **Contact** tab, you can edit the information like contact, phone, email address, and location.
   - In **VMware** tab, following information can be edited:
     - **Username** - you can edit the user account name of the vCenter server administrator.
     - **Password** - you can edit the password for the vCenter user account.
     - **Confirm Password** - retype the password for the vCenter user account.
     - **Port** - you can edit the vCenter web services listener data port number. 443 is the default setting.
     - You can enable or disable **Dynamic VM Import by rule** and **Change Block Tracking**
     - You can **ADD RULE** from the existing or **CREATE RULE** for the vCenter client.
5. Click **UPDATE**.

Auto-discovery of virtual machines

With Avamar release 7.4, you can configure Avamar vCenter clients to auto-discover VMs that have been added to the vCenter. When the VMs are auto-discovered, user-defined rules are used by the Avamar software to map the auto-discovered VMs to Avamar domains. User-defined rules are also used to automatically assign backup policies to auto-discovered VMs.

In addition to auto-discovering new VMs, vMotion of VMs from one vCenter to another is also automatically detected by the Avamar software. If the new vCenter hosting the VM is configured in Avamar, the VM is automatically moved from the original vCenter client to the new vCenter client using the same user-defined rules to assign its domain and backup policy. If a VM is deleted from vCenter, it is automatically removed from the vCenter client.

The auto-discover feature is supported with vCenter 5.5 and later releases. However, the vCenter must be at release 6.0 or greater to the use of VM Tags in rules. When protecting ESXi hosts instead of vCenter, only VM names and the root folder are supported in rules.

As tag modification is not triggered by an event, if you are modifying tags on virtual machines, sync with vCenter operation immediately to make the tag change to be effective. If you do not want to do this operation, the change is effective in these situations:

1. Restart Management Console Server.
2. Wait for every 12 hours full scan schedule.
3. Update vCenter, such as add or delete rule domain mapping.

NOTE: Avamar does not support auto-discovery for template VMs.

Domain mapping rules for VM auto-discovery

Domain mapping rules are used during auto-discovery to map new or moved VMs to Avamar domains.

About this task

Rules are selected or created when **Enable dynamic VM import by rule** is selected during configuration of a vCenter client.

Creating a rule

Rules are used to automatically map autodiscovered VMs to domains, and to assign backup policies to autodiscovered VMs. Rules use one or more filtering mechanisms to determine whether VMs qualify under the rule.

About this task

You can apply a rule or create a rule during configuration of a vCenter client.

The *Avamar Administration Guide* provides information about creating rules.

Deploying proxies using Proxy Deployment Manager from AUI

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

About this task

If the proxy is deployed to a Distributed Resource Scheduler (DRS) enabled cluster, the cluster can move the proxy by using storage vMotion. While the proxy is migrating to a different storage, the jobs that are managed by the proxy are at risk. HotAdd does not work for the proxies that are located in a DRS cluster. Therefore, disable DRS for the deployed Avamar Proxy VMs.

For more information, refer to the VMware documentation.

Proxy Deployment Manager

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

Proxy Deployment Manager is the preferred method for deploying proxies. Manual proxy deployment is still supported if necessary.

About proxy deployment

Proxy Deployment 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 ESXi host location for each proxy.

When generating a recommendation, Proxy Deployment 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 then calculates the optimum number of proxies that are required to back up those virtual machines in the time that is allotted by the backup window. Proxy Deployment also considers the datastore and ESXi host topology, and suggests an optimal ESXi 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 resides
- Proxy IP address
- Datastore assignment
- Network settings:
  - Which existing virtual network to use
  - DNS servers
  - Network gateway
  - Network mask
  - NTP

After all proxies are configured, clicking ✓ 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 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 recommendations in order to potentially further optimize proxy deployment at your site. Some of the best practices are also discussed below:

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 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 assumes that each proxy can run eight 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 conservative estimate, several 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 compared to 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.

We recommend 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 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 are 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 does not over allocate proxies beyond the maximum supported.

Proxy PDM support for thin provision

To enable Proxy deployed from PDM to use thin provision disk by default, perform the following step:

Edit `/etc/vcs/dm.properties` on utility or AVE node to update the value of parameter `proxy_disk_provisioning_policy` as following:

```
proxy_disk_provisioning_policy=thin
```

If you do not see this parameter or the value of this parameter is empty or is set to a value other than thin, PDM treats this as Thick Provision Lazy Zeroed.

Deploy proxies

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

About this task

If the proxy is deployed to a Distributed Resource Scheduler (DRS) enabled cluster, the cluster can move the proxy by using storage vMotion. While the proxy is migrating to a different storage, the jobs managed by a proxy are at risk. HotAdd does not work for the proxies that are in a DRS cluster. Therefore, disable DRS for the deployed Avamar Proxy virtual machines.

Steps

1. In the AUI navigation pane on the left, click », and then click **Proxy Management**.

   The **Proxy Deployment** page is displayed.
2. In the **Config** pane, complete the following settings:
   a. Select a **vCenter**.
   b. Set the **Data Change Rate (%)**.
   c. Set the **Backup Window (minutes)**.

   d. To include virtual machines using direct attached storage in this recommendation, select the **Protect Virtual Machines on Local Storage** check box.

      This option ignores virtual machines on clustered-host local storage.

3. Click **CREATE RECOMMENDATION**.

   The recommendation is added to the list in the lower pane.

   The **Recommendations** pane shows the proposed deployment topology. Proposed new proxies are displayed under each ESXi host with the name **New proxy**.

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

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

   b. Click ✎.
      The **New Proxy** dialog box is displayed.

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

   d. Select an Avamar server **Domain** where this proxy resides.

   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**.

5. (Optional) Add **Additional Network Interface** to the Proxy that you intend to deploy:

   > **NOTE:** You must specify the IP address, Network, and Netmask for the additional network interface of the proxy.

   a. Select the **Add Additional Network Interface** checkbox in the **Proxy** wizard.
      When you select the **Add Additional Network Interface** checkbox, the additional fields that are required appear.

   b. Enter the following information for an additional interface and click **SAVE**.

   - IP—Enter the IP address.
   - Network—Select the virtual network from the drop-down.
   - Netmask—Enter the Network mask information.

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

   > **NOTE:** For each proxy you add, you must provide the proxy name, IP address, fully qualified DNS server name or IP address, network gateway, and network mask, else the proxy is skipped. Skipped proxies are denoted with a cross-mark symbol next to the proxy name. Valid proxies are denoted with a checkmark symbol next to the proxy name.

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

   b. Click **New Proxy**.
      The **New Proxy** dialog box is displayed.

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

   d. Select an Avamar server in the **Domain** list where the proxy resides.

   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. Optional, type the NTP server address in the **NTP** field.

   l. Click **SAVE**.

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

   a. In the tree pane, select a proxy.

   b. Click ⊗.

   c. Click **YES**.

8. To update the proxy topology, click ϟ.

9. When the proposed deployment topology is satisfactory, click ✓ to apply the changes and deploy the proxy.

Results

If a proxy fails to deploy, it is deleted from the system. That hostname and IP address are available for subsequent proxy deployments by setting `keep_deploy_failed_proxy = true`.

Add gateway for DualNIC setup

Perform the following steps to add a gateway for DualNIC setup.

Steps

1. Deploy a proxy using Proxy Deployment Manager.

   During **Proxy Deployment**, you must provide an IP address. Assign an IP address from the backup subnet/VLAN. This IP address must follow the normal rules for a new proxy.
2. Go to vSphere Client and select the newly created proxy to add the gateway.
3. Click **LAUNCH WEB CONSOLE** and then click **YES** to confirm the action.
   Proxy Web console page appears.
4. Log in to the web console as a root user.
5. Type `yast2` on the console to open the YaST2 setup.
   YaST2 Control Center appears.
6. Select **System** from the left pane, select **Network Settings** from the right pane and press **Enter** key.
   Network Settings > **Overview** information appears.
7. Go to **Routing** option using right-arrow key and verify if the Default Gateway is the gateway address for the backup network.

   You can set the Default Gateway if it is not available.
8. Use the tab key to select **Add** in the **Routing Table** section and press **Enter** key.
9. Enter the following information:
   - Destination—IP Address for the vCenter Server
   - Device—eth1
   - Gateway—Gateway or Address for the production network
   - Netmask—Use the netmask corresponding to the device
10. Select **OK** and reboot the Proxy Appliance.

Upgrading proxies

This section discusses how to upgrade proxies that run supported releases of the Avamar software.

Avamar 19.4 and later includes an upgrade to the SLES 12 SP5 operating system, including for VMware proxies. This upgrade replaces the previous SLES 11 and SLES 12 operating systems. *Avamar Release Notes* contains important information about this upgrade, including prerequisites that you must meet.

You cannot upgrade VMware proxies from one operating system to another by using the ISO file. Instead, use the Proxy Deployment Manager (PDM), which automatically:

1. Removes the proxies from the Avamar server
2. Powers off the same proxies on the vCenter Server
3. Redeploys the replacement Avamar 19.10 proxies

Upgrading Avamar proxies provides more information.

You can manually remove the proxies on the vCenter Server according to your requirement.

If you manually deployed a proxy for an earlier release, with a different version of the SLES OS, you must record the required information, remove the proxy, and then use the PDM to deploy a new proxy. Upgrading older or manually deployed Avamar proxies provides more information.

ⓘ **NOTE:** The PDM does not list manually deployed proxies. Reregistering a proxy with an Avamar server provides more information about how to use the PDM to manage manually deployed proxies for Avamar 19.1 and later.

The following topics provide instructions that use Avamar Administrator because a few of the previous Avamar releases do not support the Avamar Web User Interface (AUI). Where available, you can use the PDM within the AUI instead. Deploying proxies using Proxy Deployment Manager from AUI provides more information.

Upgrading Avamar proxies

Steps

1. In Avamar Administrator, select **VMware** > **Proxy Deployment Manager**.
   The **Proxy Deployment Manager** window appears.
2. Choose a vCenter, and then click **Create Recommendation**.

   Existing proxies in the topology tree for the selected vCenter that must be upgraded are indicated with a ⚡ symbol, and a tooltip that indicates that the proxy has an update pending.
3. Click **Apply**.

Upgrading older or manually deployed Avamar proxies

This section provides information and procedures for upgrading supported Avamar proxy software from releases before Avamar 7.5.1, or where existing proxies were manually deployed.

Existing proxy configuration

The following information should be gathered before upgrading proxies 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 5. 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 6. 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

The following topics describes how to view the VM configuration.

Steps

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**.
3. For each proxy:
    - 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:

Table 7. Virtual machine properties

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

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window is displayed.
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

Steps

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 link.
The **Administration** window is displayed.
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**.

Restoring datastore assignments and group membership

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
The **Administration** window is displayed.
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.
5. Click the **Groups** tab and verify the proxies that are members of this group, based on the chart created in Existing proxy configuration.
6. Click **OK**.

Re-deploying proxies using the Proxy Deployment Manager

About this task

Where available, you can use the Proxy Deployment Manager within the AUI instead. Deploying proxies using Proxy Deployment Manager from AUI provides more information.

Steps

1. In Avamar Administrator, select **VMware** > **Proxy Deployment Manager**.
The **Proxy Deployment Manager** window appears.
2. Choose a vCenter.
3. Set the **Data change rate** to **0**.
This setting ensures that the **Proxy Deployment Manager** does not recommend proxies that are based on its analysis of the VMware environment.
4. Click **Create Recommendation**.
The tree pane shows the VMware topology. Verify that there are no recommended proxies labeled **New proxy**.
5. For each proxy in the chart that is created in Existing proxy configuration:
    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**.
   The new proxies are deployed. If any failures occur, the operation can be retried by clicking **Apply** again.

Maintaining proxies

This section includes the following topics:

Reregistering a proxy with an Avamar server

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

Steps

1. Launch the vSphere Client or vSphere Web Client, and log in to the vCenter Server.
2. Locate the proxy that 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 that 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 causes an error, and prevents you from registering this client.

13. For proxies that run Avamar 19.1 and later, respond to the Proxy Deployment Manager prompt (`Do you want this proxy to be managed by PDM (Proxy Deploy Manager) in AVE [Y/N]?`).

    This prompt does not appear if the proxy runs Avamar 18.2 or earlier.

    For manually deployed proxies, this prompt controls the registration of the proxy with the Proxy Deployment Manager.

    - To manage the proxy with the Proxy Deployment Manager, type **`y`**, and then press Enter. Supply the vCenter hostname or IP address, and credentials when prompted.
    - Otherwise, type **`n`**, and then press Enter.

Changing the proxy guest operating system admin password

About this task

ⓘ **NOTE:** Direct root login for SSH is disabled.

Steps

1. Open a command shell and log in to the proxy as admin.
2. Type **`passwd`**.
3. Type the current guest operating system admin password, and then press Enter.

4. Type the new guest operating system admin password, and then press Enter.
5. Confirm the new password by typing the password again, and then press Enter.

   NOTE: Once the proxy is deployed, change the password.

Changing the proxy guest operating system root password

Steps

1. Open a command shell and log in to the proxy as admin.
2. Switch user to root by running the following command:

   `su -`
3. Type **`passwd`**.
4. Type the current guest operating system root password, and then press Enter.
5. Type the new guest operating system root password, and then press Enter.
6. Confirm the new password by typing the password again, and then press Enter.

   NOTE: Once the proxy is deployed, change the password.

Monitor proxy status

This section discusses how you can monitor the statuses of proxies in this release of Avamar software.

View Proxy Status

Proxy status in AUI provides the status of the proxies to the Backup Admin.

Steps

1. In the AUI navigation pane on the left, click », and then click **Proxy Management**.

   The **Proxy Deployment** page is displayed.
2. Click the **Proxy Status** tab.
   The **Proxy Status** page is displayed where the statuses of the proxies are displayed.

   The list of proxies is displayed with its corresponding status against it. The legend on the right panel provides information about the possible statuses of the proxies.
3. Click the required proxy to view its detailed service status on the right panel.
   The Remedy section provides information about possible solutions to fix the proxy if it not working as expected.

Configure email notification for proxy status alert

Perform the following steps to configure email notifications for proxy status alerts:

Steps

1. Update the `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` file with the following:

```
<node name="mail">
    <map>
        <entry key="smtpHost" value="mailhubwc.lss.emc.com" />  <Your smtp server>
        <entry key="email_send_debug" value="false" />
        <entry key="email_send_timeout_minutes" value="60" />
        <entry key="admin_mail_sender_address" value="test@avamar.com" />
    </map>
</node>
```

2. Restart MCS.
3. In the AUI navigation pane on the left, click », and then click **Settings**.
   The **Setting** window is displayed.
4. Click the **Profile** tab.
5. Select *High Priority Events*, and click **COPY**.
   The **Copy Profile** dialog box appears.
6. Provide a name for the new copied profile, and select the applicable domain.
7. Click **OK**.
8. Select the newly copied profile, and click **EDIT**.
   The **New Profile** dialog box appears.
9. Update the following:
   - Select the **Send data as events occur** option in the **Properties** section.
   - Clear all event codes, and only select the `25014` event code.
   - Add **Recipient Email Address** in the **Email** section.
10. Click **FINISH** to save the updated to the profile.

Import custom certificate in Avamar VMware Image Backup Proxy

After deploying a proxy appliance in vCenter and registering it with the Avamar server, you can manually replace the default self-signed certificate with a user certificate for port 443, 5480, and 5489 on Avamar VMware Image Backup Proxy.

Prerequisites

Deploy a proxy appliance in vCenter.

Register and activate the proxy with the Avamar server.

Find the `/usr/local/avamarclient/etc/pxychangecert.sh` file on the Avamar VMware Image Backup Proxy.

About this task

NOTE: This is a manual process. If you redeploy or upgrade the proxy manually or using Proxy Deployment Manager (PDM) then you must follow the certificate replacement steps again.

Version supported: Avamar VMware Image Backup Proxy 7.5.1 and later.

To import the custom certificate and replace the existing self-signed certificate on proxy, perform the following steps:

Steps

1. Log in to the proxy using SSH with an admin account and switch to root account using `su` command.
   ```
   195proxy:~ # su -
   ```
2. Grant execute permission for `pxychangecert.sh` script.
   ```
   195proxy:~ # chmod +x pxychangecert.sh
   ```
3. For signed certificate:
   a. From proxy generate a private key and Certificate Signing Request (CSR) files using the following openssl commands:
      ```
      195proxy:~ # mkdir /tmp/certs
      ```
      ```
      195proxy:~ # openssl genrsa -out /tmp/certs/key.pem 3072
      ```
      ```
      195proxy:~ # openssl req -new -key /tmp/certs/key.pem -out /tmp/certs/
      `hostname -f`.csr -subj "/C=US/ST=California/L=Irvine/O=Dell Technologies/OU=Dell EMC/
      CN=`hostname -f`"
      ```

> ⓘ **NOTE:** The `hostname -f ` will set Common Name (CN) to current hostname. Adjust Country (C), State (ST), Location (L), Organization (O), and Organization Unit (OU) as per your requirement or omit `-subj` so that openssl starts an interactive prompt to collect these values.

   b. Upload the `/tmp/certs/<proxy hostname>.csr` file to the commercial or internal Certificate Authority (CA).
   c. The CA must provide a valid signed certificate and a certificate chain file. Upload these the files to `/tmp/certs` directory.

4. For self-signed certificate:

   Run the following openssl command to generate a new private key and a self-signed certificate with expiration duration of one year:

   ```
   195proxy:~ # openssl req -x509 -new -newkey rsa:3072 -nodes -keyout /tmp/certs/
   key.pem -out /tmp/certs/cert.pem -days 365 -subj "/C=US/ST=California/L=Irvine/O=Dell
   Technologies/OU=Dell EMC/CN=`hostname -f `"
   ```

   > ⓘ **NOTE:** You can modify `-days` to adjust the duration of expiration.

5. Ensure matching private key, certificate, and certificate chain are located in the temp location of the proxy, and meet the following requirements:
   a. The private key must not be encrypted.
   b. The certificate must be in x509 format.
   c. The CN of the certificate must match the hostname of this proxy.
   d. The "keyUsage" extension of the certificate or the " keyUsage" must not contain `digitalSignature`, `keyEncipherment`, and `keyAgreement` properties.
   e. The "extendedKeyUsage" extension of the certificate or the "extendedKeyUsage" must not contain `serverAuth` and `clientAuth` properties.
   f. The certificate chain file must contain all trusted root CA for the certificate. If the certificate to be replaced is a self-signed certificate, use the same file for certificate and chain.
6. Replace the certificate by running the following command:

   ```
   195proxy:~ # ./pxychangecert.sh /tmp/certs/key.pem /tmp/certs/cert.pem /tmp/certs/
   chain.pem avam@r
   ```

   Where, **`avam@r`** is the default keystore password.

Results

The old files will be moved to a backup directory.

Example

When you execute the script, old ssl keys are backed up in`/opt/vmware/etc/sfcb/sslbackup/<yyyy-mm-dd-hr.min.ss>` and java keystore is backed up in `/opt/jetty/etc//keybackup/yyyy-mm-dd-hr.min.ss>`

Security patch updates for proxies

Dell periodically provides security roll-up patches to address potential security vulnerabilities with the proxy appliance. It is recommended that you check occasionally to determine if an updated patch for the proxy is available.

> ⓘ **NOTE:** In 19.3, proxy does not install the security-related patch. It is recommended to install the latest security package. Avamar Proxy has a default patch under proxy folder `/tmp/patch`.

The default patches are `sec_os_updates_SLES12SP4-2019-R3-v7.tgz`, `avfwb-7.0.0-3.x86_64.rpm`, and `avhardening-7.0.0-2.x86_64.rpm`.

Best practices and troubleshooting for applying security patch updates to proxies

Review the following items before you apply a security update patch to a proxy:

Best practices

- Security updates are only supported for proxies that are managed by the **Proxy Deployment Manager**. For a manually deployed proxy, use the `initproxyappliace.sh` option to register a manually deployed proxy with the **Proxy Deployment Manager**. Older versions of Avamar do not support this form of patching.
- Avamar 19.3 and later, adds support for the package installation tracking feature. Proxy installations from previous releases are not traceable. Dell Technologies recommends that you deploy or update proxies to the most recent version by using the proxy upgrade functionality in the **Proxy Deployment Manager**.
- If you update the VAMI or the registered VAMI service (Avamar provider: `AvamarVMwareCombined-CIM-linux-sles12sp1-x86_64-`*`version`*`.rpm`), ensure that you manually restart the `vami-sfcb` service on the proxy.

Troubleshooting

- The patch install log resides on the proxy at `/tmp/patch.log`.

  If the installation fails, the proxy fetches the log content and displays the content in the AUI.
- The install patch tracking log resides at `/usr/local/avamarclient/var/patchinstall.log`.
- The install script does not reside on the proxy. If you need to modify this script for troubleshooting purposes, you can find the scripts at the following locations:
  - For the hotfix RPM, the script resides on the Avamar server at `/usr/local/avamar/var/vcs/dm/installpatch.sh`.
  - For the patch TGZ, the `sec_rollup_proxy_install.sh` script resides inside the TGZ package.

  The uploaded patch is saved in the Avamar server at `/usr/local/avamar/var/vcs/dm/patches`.
- To troubleshoot the CIM service, create a new empty file at `/tmp/CIM.log`. The CIM service writes the log entry to this file.
- You can change the upload file size limit by modifying the following lines in the MC REST API service `.yaml` file:

  ```
  http:
  multipart:
  max-file-size:50000MB
  max-request-size:500000MB
  ```
- If a proxy virtual machine was deleted or powered off from a VMware-side application such as the **vSphere Client**, the proxy is removed from the **Proxy Deployment** tab in the AUI **Proxy Deployment Manager** window. However, the proxy list in the **Proxy Patches** tab still lists the proxy.

  Clicking this proxy returns an HTTP 500 error that indicates`No route to host (Host unreachable)`. If you encounter this issue, verify whether the proxy is temporarily unavailable or if the proxy has been permanently removed:

  - If the proxy is temporarily unavailable, power ON the proxy virtual machine, and then retry the operation in the **Proxy Deployment Manager**.
  - If the proxy has been permanently deleted, use the **Asset Management** window in the AUI to remove the proxy, and then retry the operation in the **Proxy Deployment Manager**.

Apply security patch updates to a proxy

If an updated security patch is available, perform the following steps as an administrator to apply the patch to a proxy.

Prerequisites

Review the information in Best practices and troubleshooting for applying security patch updates to proxies.

Steps

1. Download the patch files from the provided location.
2. Log in to the AUI or the vSphere Web Client as an administrator.
3. Go to **Proxy Management** > **Proxy Patches**.
4. In the **Available Patches** pane, click **UPLOAD...**
   The **Upload Proxy Patches** dialog displays.
5. Click **BROWSE....** to go to the location of the patch files, and then select the files that you want to upload to the Avamar server patch folder.
   When finished, click **UPLOAD** to save the selections and exit the dialog box. The **Available Patches** pane shows the selected patch files.
6. Select the radio button for the specific patch that you want to apply to the proxy.

   ⓘ **NOTE:** To remove unavailable patch files from this pane, select the file and then click **DELETE**.

7. From the **Proxies List** pane, select the checkbox for the proxy on which you want to install the patch file, and then click **INSTALL PATCH**.

   ⓘ **NOTE:** You can use the **Filter Proxies by vCenter** drop-down to display proxies from a specific vCenter server. By default, **All vCenters** is selected.

Results

An informational message indicates the status of the patch application:

- `Success` indicates that the patch was successfully installed.
- `Success, reboot required` indicates that the patch was successfully installed, but that you must reboot the proxy.
- `Success, restart vami-sfcb service required` indicates that the patch was successfully installed, but that you must restart the `vami-sfcb` service.
- `Failed (view error)` indicates that the patch was not installed. Click the **View Error** link to determine why the failure occurred.
- `Already install, bypass` indicates that this patch is already installed on this proxy.

After a successful installation, you can click **View** in the **History** column to verify the installed patches on the proxy.

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.

Steps

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 the following command:

   ```
   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 the following command:

```
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.

Steps

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 the following command:

   ```
   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 the following command:

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

3

Administration

Topics:

- Clients and containers
- Add a VMware client
- Delete a VMware client
- Enable changed block tracking
- Viewing protected virtual machines in Avamar Administrator
- Viewing a replicated virtual machine name in Avamar Administrator
- Monitoring the vCenter connection in Avamar Administrator
- Manually synchronize the AUI with vCenter and VM clients
- Rename a vCenter client
- VMware Image Dataset
- Adding guest backup throttling parameters to a dataset in Avamar Administrator
- Groups
- Changing proxy datastore and group assignments in Avamar Administrator

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 the AUI, 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 the AUI, 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 the AUI.

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 the AUI.

Dynamic container behavior

When adding a dynamic container using the **Recursive Protection** checkbox, all the child entities including the subcontainers get added to the AUI. Virtual machines or vApps residing in the subcontainers will get added automatically to the AUI.

If a virtual machine client is deleted from a container in vCenter, and that container was being protected as a dynamic container in the AUI, 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 requires special consideration.

Consider the following nested container structure and scenario:

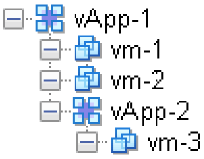


Figure 3. Example independent and container protection

In this example, vm-1 is added to Avamar as a virtual machine client and is independently protected. When the vApp-1 container is added to Avamar, vm-1 is also protected as a member of the vApp-1 container. Avamar recognizes that the same virtual machine exists in two contexts:

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

If the vApp-1 container is retired or deleted, vm-1 continues to exist in Avamar as a stand-alone virtual machine client because it was explicitly added before it was protected as a member of the vApp-1 container. The stand-alone context supersedes the container member context. If you need to retire or delete vm-1, you cannot delete or retire the vApp-1 container. You must also retire or delete the stand-alone instance. If you do not delete the stand-alone instance, vm-1 continues to be protected by scheduled backups.

Add a VMware client

Perform the following steps to add a VMware client:

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
2. In the **Domain** tree, select a vCenter domain or a subdomain for the client.
3. Click **ADD CLIENT**.
   The **Select VMware Entity** window displays.
4. You can toggle the vCenter hierarchy view in the left pane to list containers by vSphere virtual machines and templates, or by vSphere hosts and clusters.
   - To view by vSphere virtual machines and templates, keep or move the **VM/Tempate** slider to the left. This is the default setting.
   - To view by vSphere hosts and clusters, move the **VM/Tempate** slider to the right. The name changes to **Host/Cluster**.

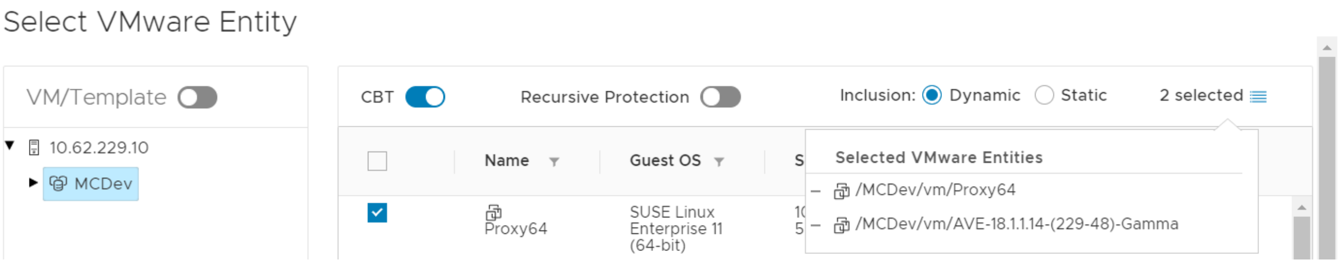
   ⓘ **NOTE:** Resource pools are only visible in the **Host/Cluster** view.
5. In the left pane, expand and select a container in the vCenter.

   Use the filter icon in the **Name** column to search for an entity by name. The search filter limits the list to entities with the same and similar names. You can search for an entity that is located in a folder or subfolder.

   The VMware entities for the selected object display in a table in the right pane.
6. Select the check box next to any folder, resource pool, virtual machine, or vApp in the right pane. Use the filter icons in the **Guest OS**, **Server** and **Location** columns to quickly locate the entity you want to add.

   ⓘ **NOTE:** You can further expand an entity in the table (for example, a folder) to view a container's child entities and select these entities.

All selections appear in the **Selected VMware Entities** drop-down when you hover over the ≡ icon. You can also click the - to the left of an entity in this drop-down to remove the selection.



Select VMware Entity

VM/Template ○

▾ 10.62.229.10
▸ MCDev

CBT ● Recursive Protection ○ Inclusion: ● Dynamic ○ Static 2 selected ≡

☐	Name	Guest OS	S
☑	Proxy64	SUSE Linux Enterprise 11 (64-bit)	1(5

Selected VMware Entities
- /MCDev/vm/Proxy64
- /MCDev/vm/AVE-18.1.1.14-(229-48)-Gamma

Figure 4. Selected VMware Entities drop-down

> **NOTE:** The check box next to an entity will be disabled in the following cases:
> - The entity has already been added as a client.
> - The entity is the AVE.
> - The entity is a VMware proxy.
> - The entity is a data center.
> - The entity is an ESX host.

7. (Optional) When adding a container, select from one of the **Inclusion** options in the right pane:
   - Select **Dynamic** to make this a dynamic container
   - Select **Static** to make this a static container.
8. To enable changed block tracking, move the **CBT** slider to the right/ON position.

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

   > **NOTE:** 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
   > - Migrate

9. To add a dynamic container that uses recursive protection, move the **Recursive Protection** slider to right/ON position.

   This task automatically adds all the child entities, including the subcontainers, virtual machines, and vApps residing in the subcontainers.
10. Click **SUBMIT**.

Next steps

If you enabled changed block tracking for any virtual machine, open the **vSphere Client**, locate the virtual machine, and then perform any of the following actions:

- Reboot
- Power on
- Resume after suspend
- Migrate

Delete a VMware client

Delete a client and all backups of the client. Optionally, choose to delete all replicas that exist on replication destination systems.

About this task

When you delete a client, Avamar permanently deletes all backups that are stored for that client. Only delete a client when you are certain that there is no reason to retain the backups. If there is any doubt, retire the client instead.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
2. In the hierarchical **Domain** tree, select a vCenter domain or a subdomain.
3. In the list of clients, select the client that you want to delete.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
4. Click **MORE ACTIONS** > **Delete Client**.
   The **Delete Client** dialog box appears and displays the number of existing backups for the client.
5. Select **I understand this action is permanent and irreversible**.

   This field is a safety net to avoid unintentionally deleting a client and the backup information of a client.
6. Click **YES**.

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 long backup windows, or excessive back-end storage read and write activity.

About this task

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
- Migrate

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
2. In the hierarchical **Domain** tree, select a vCenter domain or a subdomain.

   To include subdomain clients, toggle the **Include Sub-domain** switch to on.
3. In the list of clients, select the client that you want to edit.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
4. Click **MORE ACTIONS** > **Edit Client**.
   The **Edit Client** dialog box appears and displays the number of existing backups for the client.
5. To enable changed block tracking:
   a. Select the **VMware** tab.
   b. In the **CBT** field, select the check box.
   c. Click **UPDATE**.

Viewing protected virtual machines in Avamar Administrator

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

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window is displayed.
2. Click on vCenter domain.
3. Click the **Account Management** tab.
4. Click the **Protection** tab.

Viewing a replicated virtual machine name in Avamar Administrator

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

About this task

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..

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window is displayed.
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 in Avamar Administrator

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.

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window is displayed.
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 synchronize the AUI with vCenter and VM clients

Although Avamar Administrator automatically synchronizes with any vCenter it monitors at regular intervals, you can also perform a manual synchronization at any time. You can manually synchronize the AUI with both vCenter and VM clients.

Steps

1. To synchronize the AUI with vCenter:
    a. In the AUI navigation pane on the left, click », and then click **Asset Management**.
    b. In the hierarchical **Domain** tree, select a vCenter.
    c. To synchronize the AUI with a vCenter, perform either of the following steps:
        - Click the overflow menu (⋮), and then select **Sync vCenter**.
        - In the **DOMAIN ACTIONS** pane, select **Sync vCenter**.

    d. Click **Yes** to dismiss the confirmation message.
    When the synchronization is complete, the following message is displayed:

    ```
    vCenter data synchronized successfully
    ```

2. To synchronize the AUI with a VM client:
    a. In the AUI navigation pane on the left, click », and then click **Asset Management**.
    b. In the hierarchical **Domain** tree, select a vCenter.
    c. Select the VM client that you want to synchronize, and then click **More Actions** > **Sync Client**.
    d. Click **Yes** to dismiss the confirmation message.
    When the synchronization is complete, the following message is displayed:

    ```
    sync request has been sent to the the server
    ```

Rename a vCenter client

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

About this task

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

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
2. In the domain tree, select the vCenter client.
3. Click **MORE ACTIONS** > **Edit Client**.
   The **Edit Client** window is displayed.
4. In the **Name** field, type the new fully qualified DNS name.
5. Click **UPDATE**.
   A confirmation message is displayed.
6. 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 the following commands:

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

7. Stop the MCS by typing the following command:

   ```
   dpnctl stop mcs
   ```

8. Start the MCS and the scheduler by typing the following command:

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

9. 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 in Avamar Administrator

When performing scheduled guest backups of virtual machines on the same ESX Server, add throttling parameters to the Avamar dataset.

About this task

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.

Steps

1. In Avamar Administrator, select **Tools** > **Manage Datasets**.
   The **Manage All Datasets** window is displayed.
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:

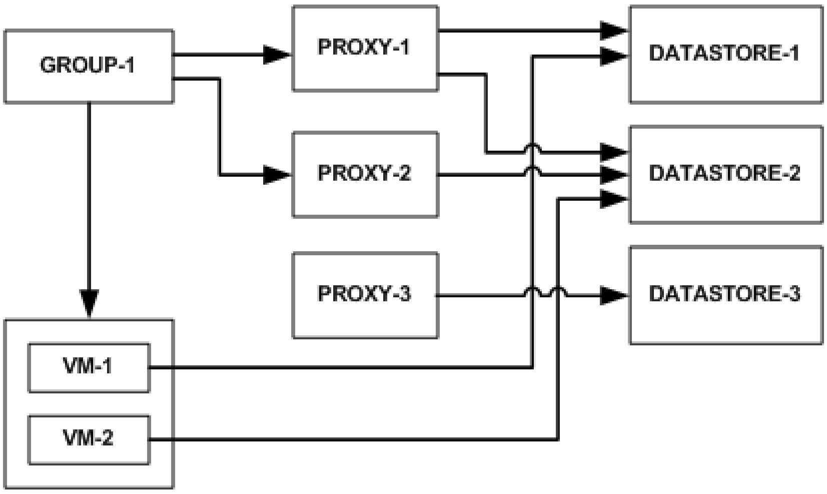


Figure 5. Virtual machine and proxy relationships within groups

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 in Avamar Administrator

Steps

1. In Avamar Administrator, click the **Policy** launcher link.
   The **Policy** window is displayed.
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**.

4

Backup

Topics:

- Limitations
- Perform an on-demand backup of a virtual machine by using AUI
- Set advanced plug-in options in the AUI
- Schedule backups using the AUI Policy wizard
- Log truncation backups
- Monitor backups
- Cancel backups
- Support for vCenter HA failover for inflight backups
- Configure a backup to support VMware encryption
- Configure a backup to support vSAN encryption
- Enforcement of backups to Data Domain

Limitations

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

Updated values are not considered during Proxy Deployment

If you edit the saved values multiple times in the proxy deployment process, it will not replace the initial saved values with the new values. To add the new values, use the **Create Proxy** option instead of **Edit Proxy** option.

All backups must be initiated from the AUI or Avamar Administrator

All image backups must be initiated from the AUI or 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 are 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 virtual disks and physical RDM disks, the backup will successfully process the virtual disks, and bypass the RDM disks, leaving the RDM data unprotected despite completing successfully. Enable the `force_rdm_backup_failure` option in the proxy image plug-in to provide a warning message for this potentially unprotected data. By default, the warning message is disabled. When you enable `force_rdm_backup_failure` option, the following event code and warning message are returned:

```
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:

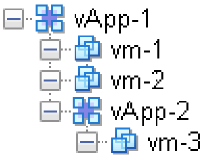


Figure 6. Example nested container structure

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 are 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 backup otherwise that entire backup 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 to ensure maximum data protection.

Perform an on-demand backup of a virtual machine by using AUI

You can perform an instance backup that is independent of existing schedules and policies.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.
3. In the list of clients, select a virtual machine client, VMware folder, resource pool, or vApp.

4. Click **BACKUP**.
   The **Backup** wizard is displayed. In the **Plugins** pane, a list of plug-ins on the client is displayed.
5. In the **Plugin** pane, perform the following steps:
   a. Browse to and select the check box next to the data that you want to back up.
   b. Click **NEXT**.
      The **Basic Configuration** window is displayed.
6. In the **Basic Configuration** pane, perform the following steps:
   a. Select the backup retention policy settings:
      - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period**. 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 until this client remains active in the Avamar server, select **No end date**.
   b. In 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 *Avamar Product Security Guide* provides additional information.
   c. In the **Optionally select a proxy to perform backup** list, select the proxy.

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

      The **More Options** window is displayed.
7. In the **More Options** pane, set the plug-in options:

   Toggle the **Show Advanced Options** switch to view advanced configuration options. Set advanced plug-in options in the AUI provides more information about the advanced backup options.

   VMware Image backup plug-in options provides more information about the basic backup options.
8. Click **FINISH**.
   The following status message is displayed:

   ```
   Backup initiated.
   ```

Set advanced plug-in options in the AUI

Perform the following optional tasks from the **More Options** window when performing an on-demand backup.

Prerequisites

NOTE: You can only perform data exclusion on an application consistent backup. As a result, the target VM must be in a running state.

Steps

1. Toggle the **Show Advanced Options** switch to on.
2. To enable changed block tracking, select the **Use Changed Block Tracking (CBT) to increase performance** checkbox.
3. To enable the Avamar server to report information to the vSphere Client about the most recent backup and most recent successful backup, select the **Set Annotation Tag LastBackupStatus and LastSuccessfulBackup** checkbox.

   When selected, the following information displays in the vSphere Web Client:

   - **LastSuccessfulBackupStatus**: The date and time of the most recent successful backup.
   - **LastBackupStatus**: The date and time of the most recent backup, whether successful or not.
4. To index VMware image backups, select **Index VMware Image Backups**.

   NOTE: Indexing VMware image backups using the Data Protection Search software is only supported with HotAdd transport mode.
5. To exclude the Windows page file (`pagefile.sys`) from the backup, select **Exclude page file blocks when performing image backup on Windows VM**.

ⓘ **NOTE:** Page file exclusion is supported only for Windows Servers version 2008 R2 and above. For client versions of Windows, this option has no effect. The page file is included in backups of Windows clients, regardless of this setting.

6. To exclude deleted file blocks from the backup, select **Exclude deleted file blocks when performing image backup on Windows VM**.
7. For the **Exclude files with path and filter** field, type the files that you want to exclude.

   ⓘ **NOTE:**

   If you exclude a file during backup, and then perform a restore of the entire file system which contained the excluded file, or just a restore of the excluded file, the excluded file will be visible upon restore but will not be usable.

   If you change the exclusion path or filename between backups, the next backup is a full (level 0) backup.

8. 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.
9. 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.
10. For the Windows VMware Image plug-in only, select one or more Snapshot Quiesce Options. The options include the following:
    - Fail backup on snapshot quiesce error.
    - If VMware tools are not running, mark completed backup as 'Complete w/Exception' (applications are not quiesced).
11. For the **Max times to retry snapshot detele** option, type the maximum number of times that a snapshot delete operation should be tried.
12. In **Guest Credentials**, type a virtual machine guest OS user account name and password with sufficient privileges to run scripts before or after the backup.

    For log truncation backups of Exchange servers, guest credentials must have administrator privileges. If multiple VMs are backed up, the same credentials must be used for all VMs.
13. To run a script before the VMDK snapshot:
    a. Type the full path and filename of the script that is run.
    b. Ensure that the script timeout is sufficient for the script to complete.
14. To run a script after the backup completes and the VMDK snapshot is removed:
    a. Type the full path and filename of the script that is run.
    b. Ensure that the script timeout is sufficient for the script to complete.
15. For the Windows VMware Image plug-in only, in the **Snapshot quiesce timeout (minutes)** filed, type the number of minutes to wait before a snapshot quiesce operation is considered to have failed.
16. If performing an image backup of a Microsoft SQL server, select the type of authentication:
    - **NT Authentication** uses the credentials that are entered in **Guest Credentials** for authentication.
    - **Application Authentication** uses the **SQL Server Username** and **SQL Server Password** to log in to the SQL server.
17. If performing an image backup of a Microsoft SQL server, identify the post-action options:
    - Type the maximum number of minutes to wait before post-action operations are considered to have failed in the **Post Action Timeout (minutes)** option.
    - Select the type of post-action operation. **LOG Truncation** performs log truncation after the backup has successfully completed.
    - All disks of the VM must be selected for on-demand backup or log truncation will not occur.
18. If performing an image backup of a Microsoft Exchange server, select the type of post-action operation. **LOG Truncation** performs log truncation after the backup has successfully completed.
19. Click **FINISH**.

Schedule backups using the AUI Policy wizard

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

About this task

You can schedule backups by using the Policy wizard to create a backup policy.

Perform the following steps within the **Policy** wizard.

Steps

1. Assign members to the new backup policy.
2. Assign a dataset to the new backup policy.

   To create a dataset, use the Policy wizard or select **Setting** > **Dataset** > **Add**.
3. Assign a schedule to the new backup policy.

   To create a schedule, use the Policy wizard or select **Setting** > **Schedule** > **Add**.
4. Assign a retention policy to the new backup policy.

   To create a retention policy, use the Policy wizard or select **Setting** > **Retention** > **Add**.
5. Enable scheduling for the backup policy.

Creating a dataset

A dataset specifies the data to include in a scheduled backup and the options to use for the backup. Create at least one dataset for scheduled backups on a client or group of clients. Create multiple datasets to segregate client data.

Steps

1. In the AUI navigation pane on the left, click », and then click **Setting**.
   The **Setting** pane is displayed.
2. Click the **Dataset** tab.
3. Click **ADD**.

   The **Create Dataset** window is displayed.
4. In the **Dataset Name** field, type a name for the dataset.

   The name can include alphanumeric characters (A-Z, a-z, 0–9) and the following special characters: period (.), hyphen (-), and underscore (_), and space. Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
5. In the **Plugins** list, select the **VMware** plug-in appropriate for your operating system.
   The **VMware** plug-in options are displayed.
6. Click the **Options** tab, and then set the plug-in options.

   To view advanced options, select **Show Advanced Options**.

   Plug-in Options provides a detailed list of VMware plug-in options.
7. Click the **Source Data** tab, and then set the plug-in options:
   - To include all virtual machines, select **All virtual disks**.
   - To limit the dataset to specific items, perform the following steps:

   a. In the **File/Folder Path**, type the file path.
   b. Click **ADD**.

   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
   ```
8. Click **SUBMIT**.

Scheduling backups using the Policy wizard

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

About this task

You can schedule backups by using the Policy wizard to create a backup policy.Perform the following steps within the **Policy** wizard. The *Avamar Administration Guide* provides more information about policies, datasets, schedules, and retention policies.

Steps

1. Assign members to the new backup policy.
2. Assign a dataset to the new backup policy.

   To create a dataset, use the Policy wizard or select **Setting** > **Dataset** > **Add**.
3. Assign a schedule to the new backup policy.

   To create a schedule, use the Policy wizard or select **Setting** > **Schedule** > **Add**.
4. Assign a retention policy to the new backup policy.

   To create a retention policy, use the Policy wizard or select **Setting** > **Retention** > **Add**.
5. Enable scheduling for the backup policy.

Create a backup policy

A backup policy is a collection of Avamar clients that use the same dataset, schedule, and retention settings to implement scheduled backups.

About this task

Member clients must all be in the same Avamar domain. When you create a backup policy, you define the dataset, schedule, and retention settings that apply for scheduled backups. From 19.3, during creation of backup policy you can browse the oracle plug-in database during the dataset creation. *Avamar Administration Guide* provides more information for the same. These settings consist of the backup policy, which controls backup behavior for all members of the backup policy unless you override these settings at the client level.

The *Avamar Administration Guide* provides information about creating and editing backup policies, schedules, or retention settings.

Enable a scheduled backup for a backup policy

Scheduled backups occur only for enabled backup policies. Backup policies are disabled by default unless you select the **Enabled** check box on the first page of the **New Policy** wizard. If you did not enable the backup policy when you created it, use the menu options in the **Policy** window to enable backups.

Steps

1. In the AUI navigation pane on the left, click », and then click **Backup Policy**.
   The **Policy** page is displayed.
2. In the domain tree, select a domain or subdomain for the backup policy.

   To select a subdomain for the backup policy, toggle the **Include Sub-domain** switch to on.
3. Select a backup policy from the list.
4. To enable a backup policy, click **MORE ACTIONS** > **Enable Policy**.
5. To disable a backup policy, click **MORE ACTIONS** > **Disable Policy**.

Automatically include virtual machines in a backup policy using dynamic rules

As part of the autodiscovery feature, virtual machines created in vCenter that have been discovered in Avamar can automatically be assigned to backup policies by using dynamic rules. This procedure describes how to configure scheduled policy backups to use dynamic rules.

About this task

ⓘ **NOTE:** Auto-discovery of virtual machines contains information about configuring autodiscovery of virtual machines.

Steps

1. In the left navigation pane of the **AUI**, go to **Policy** > **Backup Policy**, and then select a domain.
2. Click **+ADD** to open the **Policy** wizard, which is used to create the backup policy.
3. On the **Members** page, select **Enable Dynamic rule**, and then perform either of the following:
   - From the list, select an existing rule, or
   - Click **+** to create a rule.

   Virtual machines that match the rule criteria display with a green check mark and a status of **Included by Rule** on the **Members** page, indicating that the virtual machines have been dynamically selected for inclusion in this backup policy.

   You can also add virtual machine clients to this policy that have not been dynamically included. This is also known as static inclusion, as described in the topic Dynamic versus static containers.

   To include a virtual machine in the policy that has not been dynamically added, select the checkbox next to the virtual machine. The entry displays with a blue check mark and a status of **Included by User**, indicating that the virtual machine has been statically selected for inclusion in this backup policy.

   Additionally, you can exclude a virtual machine client that was dynamically included in the policy. To exclude a virtual machine that was dynamically added to the policy, select the X next to the virtual machine. The entry displays with a red X and a status of **Excluded**.

   ⓘ **NOTE:** It is recommended that you do not manually include or exclude clients in a backup policy that uses using virtual machine autodiscovery. As a best practice, reserve backup policies that use automatic member selection (or selection based on dynamic rules) for that purpose only, and create other backup policies for clients that are not autodiscovered virtual machines.

4. Click **NEXT** and complete the remaining steps in the **Policy** wizard.

Results

When you complete this task, the Avamar server applies the backup policy to the selected clients.

Manage rules

The Avamar server uses rules to automatically map autodiscovered virtual machines to domains, and to assign backup policies to these virtual machines. Rules use one or more filtering mechanisms to determine whether virtual machines qualify for inclusion in a policy.

You can use the **AUI** to create a rule, edit an existing rule, or delete a rule.

Create a rule

Avamar server uses rules for domain map and automatic backup policy assignment for autodiscovered virtual machines (VMs).

About this task

When creating rules, ensure that rules are mutually exclusive, to avoid the situation where a VM might qualify under multiple rules.

Steps

1. In the AUI navigation pane on the left, click », and then click **Setting** tab.
2. Click the **Rule** tab.
3. In the domain tree, select a vCenter domain or subdomain for the client.
4. On the **Setting** page, complete the following tasks:
   a. Click **ADD**.

      The **New Rule** window is displayed.
5. In the **Rule Name** field, type a name for the rule.
6. In the **Match Type** field, select whether the rule should match **Any** of the listed filter mechanisms, or **All** of them.

   This selection allows you to configure multiple different filters to select VMs. The selection helps you to determine how these filters interact with one another to select the correct virtual machines. For example, you might create a filter that uses a virtual machine folder path to select virtual machines. You might create another filter that uses a virtual machine naming convention.

   Use this option to determine which virtual machines are included under this rule:

   - To include only virtual machines that are in the defined folder path and also follow the naming convention, select **All**.

     This step excludes virtual machines that are in the folder path but that do not follow the naming convention. It also excludes virtual machines that follow the naming convention but are not in the folder path.
   - To include any virtual machines that are either in the virtual machine folder path or that follows the naming convention, select **Any**.
7. To add a filter:

   a. Click +.

      This step adds a row to the list of filters.

   b. In the **Filter** column, select a filter type.

Table 8. Rule filters

Filter	Meaning
VM Name	Use the VM naming convention to filter.
VM Folder Path	Use the path of the VM folder to filter.
Parent vApp Name	Use the vApp name of the parent VM to filter.
Resource Pool Name	Use the resource pool name of the VM to filter.
Data Center Path	Use the data center path of the VM to filter.
Data Store Name	Use the data store name of the VM to filter.
VM Tag	Use the vCenter VM tag to filter.
Datastore Cluster Name	Use the datastore cluster name of the VM to filter.
ESX Host Cluster	Imports VMs by using the ESX host cluster.
ESX Host Name	Use the ESX Host Name of the VM to filter.
VM Powered On	Use the power-on state of the VM to filter. The value `true` implies that the VM is powered on; `false` implies that the VM is powered off; any other value is considered as `false`.

   c. In the **Operator** column, select the operand.

Table 9. Filter operator

Operand	Meaning
Equals	Checks if the filter is equal to the value that is provided. All VMs whose filter is equal to the value that is provided are selected.

Table 9. Filter operator (continued)

Operand	Meaning
Does Not Equal	Checks if the filter is not equal to the value that is provided. All VMs whose filter is not equal to the value that is provided are selected.
Contains	Checks if the filter contains the value that is provided. All VMs whose filter contains the value that is provided are selected.
Does Not Contain	Checks if the filter does not contain the value that is provided. All VMs whose filter does not contain the value that is provided are selected.
Begins With	Checks if the filter begins with the value that is provided. All VMs whose filter begins with the value that is provided are selected.
Ends With	Checks if the filter ends with the value that is provided. All VMs whose filter ends with the value that is provided are selected.
Matches Regular Expression	Checks if the filter matches the provided regular expression. All VMs whose filter matches the regular expressions that are provided are selected.
Matches	Checks if the filter matches the value that is provided. All VMs whose filter matches the value that is provided are selected.
Does Not Match	Checks if the filter does not match the value that is provided. All VMs whose filter does not match the value that is provided are selected.

d. In the **Value** column, type the filter text.

   For example, to create a filter that selects all virtual machines whose names begin with the text string **HR_**. Select **VM Name** for the filter type, begins with for the operand, and type **HR_** for the filter text.

8. To create additional filters, click +.
   This step adds a row to the list of filters.
9. To delete an existing filter, click **Delete**.
10. Click **SUBMIT**.
    Changes made to tags may experience a delay of up to 12 hours before being enforced. For this reason, edit tags with caution, or perform a synchronized vCenter operation, which automatically synchronizes the vCenter with the Avamar server.

Examples for rules with regular expressions

Matching regular expressions is a powerful functionality to add virtual machines (VMs) to Avamar or backup policy automatically.

About this task

Below example explains how to configure the rules with regular expressions.

Table 10. Examples for rules with regular expressions

Description	Examples	Expression
Match the VMs that start with "vm".	"vm1" or "vm2"	`^vm.*`
Match VMs which do not start with "vm".	"my-vm1" or "my-vm2"	`^(?!vm).*`
Match VMs which end with "vm".	"my-vm1"	`.*vm$`
Match VMs that do not end with "vm".	"my-vm1"	`.*(?<!vm)$`
Match VMs that contain "vm" (case insensitive) in upper or lower cases.	"VM1" or "vm1"	`.*(?i)vm.*`

Table 10. Examples for rules with regular expressions (continued)

Description	Examples	Expression
Match VMs that contain "vm" or Linux.	"vm1", "Linux1"	`.*(vm|Linux).*`
Match VMs that contain "vm" with at least two digits.	"vm01","vm02"	`.*vm(\d){2,}`
Match VMs contain: ● 2~5 Latin character ● one or more digits	"vm1","vm2"	`^[a-zA-Z]{2,5}(\d)+$`
Match VMs which do not contain white space.	N/A	`^\S+$`
Match VMs contain at least one space in the middle.	N/A	`^\w+\s+\w+$`

Edit a rule

When editing a rule, ensure that rules are mutually exclusive, to avoid the situation where a virtual machine might qualify under multiple rules.

Steps

1. In the AUI navigation pane on the left, click », and then click **Setting**.
2. Click the **Rule** tab.
3. In the domain tree, select a vCenter domain or subdomain for the client.
4. In the **Setting** page, complete the following tasks:
   a. Select a folder that contains a VMware entity.
   b. Select a rule from the list that you want to edit, and then click **EDIT**.

      The **Edit Rule** window is displayed.
5. In the **Rule Name** field, type a name for the rule.
6. In the **Match Type** field, select whether the rule should match **Any** of the listed filter mechanisms, or **All** of them.

   This selection allows you to configure multiple different filters to select VMs, and to determine how these filters interact with one another to select the correct virtual machines. For example, you might create a filter that uses a virtual machine folder path to select virtual machines, and another filter that uses a virtual machine naming convention.

   Use this option to determine which virtual machines are included under this rule:

   - To include only virtual machines that are in the defined folder path and also follow the naming convention, select **All**.

     This step excludes virtual machines that are in the folder path but that do not follow the naming convention. It also excludes virtual machines that follow the naming convention but are not in the folder path.
   - To include any virtual machines that are either in the virtual machine folder path or that follows the naming convention, select **Any**.
7. To add a filter:
   a. Click +.

      This step adds a row to the list of filters.

   b. In the **Filter** column, select a filter type.

      For example, to create a filter that uses a virtual machine naming convention, select **VM Name**, or to create filter that uses a vCenter VM Tag, select **VM Tag**.

   c. In the **Operator** column, select the operand.

      For example, if VM Name is selected for the filter type and begins with is selected for the operand, then all virtual machines whose names begin with the filter text is selected.

   d. In the **Value** column, type the filter text.

      For example, to create a filter that selects all virtual machines whose names begin with the text string **HR_**, select **VM Name** for the filter type, begins with for the operand, and type **HR_** for the filter text.

8. To create additional filters, click +.
   This step adds a row to the list of filters.
9. To delete an existing filter:
   a. Select the filter.
   b. In the Actions column, click **Delete**.
10. Click **SUBMIT**.
    Changes made to tags may experience a delay of up to 12 hours before being enforced. For this reason, edit tags with caution, or perform a synchronized vCenter operation, which automatically synchronizes the vCenter with the Avamar server.

Delete a rule

Perform the following steps to delete an existing rule:

Steps

1. In the AUI navigation pane on the left, click », and then click **Setting**.
2. Click the **Rule** tab.
3. In the domain tree, select a vCenter domain or subdomain for the client.
4. In the **Setting** page, complete the following tasks:
   a. Select a rule from the list.
   b. Click **DELETE**.

Log truncation backups

Avamar release 7.4 and greater supports log truncation after a successful Microsoft SQL and Microsoft Exchange image backup has been performed, thereby allowing the backup window to be reduced along with the disk space required for the database logs. The following sections describe how to configure scheduled log truncation backups.

Scheduled backups with Microsoft SQL log truncation

Avamar performs log truncation of a SQL Server Database after the backup has completed.

This section describes how to schedule backups that perform log truncation.

Scheduling backups that contain multiple VMs requires an automated mechanism to select the VMs that are hosting SQL databases. Rules contain filtering mechanisms, such as the VM name or VM tag, that determine which VMs qualify under the rules. Configuring your VMs that host SQL databases correctly from within vCenter, and configuring corresponding rules, allows you to determine which VMs in a multiple VM backup should have log truncation performed.

Full backup required before performing SQL log truncation

A full backup is required before performing log truncation.

If a backup is performed of a database that has never had a full backup, log truncation fails. Performing a full database backup, using either an SQL server native backup or a full Avamar backup, is required before performing log truncation.

Scheduling backups of Microsoft SQL servers for log truncation

Scheduled backups of Microsoft SQL servers for log truncation are configured using the following procedure.

About this task

Follow this procedure to create a dataset for Microsoft SQL server backup and schedule backups of Microsoft Exchange servers for log truncation.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Setting**.
   The **Setting** pane is displayed.
2. Click the **Dataset** tab.
3. Click **ADD**.

   The **Create Dataset** window is displayed.
4. In the **Dataset Name** field, type a name for the dataset.

   The name can include alphanumeric characters (A-Z, a-z, 0–9) and the following special characters: period (.), hyphen (-), and underscore (_), and space. Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
5. In the **Plugins** list, select the **Windows VMware Image** plug-in.
6. Click the **Options** tab, and perform the following steps:
   a. To view advanced options, select the **Show Advanced Options** check box.
   b. In the **Guest Credentials** field, type a virtual machine guest operating system user account name and password with sufficient privileges to run scripts before or after the backup.
   c. In the **Microsoft SQL Server authentication** field, select the type of authentication:
      - **NT Authentication** uses the credentials that are entered in **Guest Credentials** for authentication. You must have Windows Authentication enabled on all SQL Server instances. If log truncation is used, the user who is entered here must have sufficient rights to run log truncation on all databases on all SQL Server instances.
      - **Application Authentication** uses the **SQL Server Username** and **SQL Server Password** to log in to the SQL server. The user credentials that are listed here are used to log in to all SQL Server instances running on the target virtual machine.

   d. In the **Microsoft SQL Server post action** field, identify the post-action options:
      - Type the maximum number of minutes to wait before post-action operations are considered to have failed in the **Post Action Timeout (minutes)** option.
      - Select the type of post-action operation. **LOG Truncation** performs log truncation after the backup has successfully completed.

   e. Complete other information in the Options tab as require.

      The *Avamar Administration Guide* contains further information about creating and configuring datasets.
7. Click the **Source Data** tab, and then select **All virtual disks**:
8. Click **SUBMIT**.
9. If multiple guest VMs are being backed up as part of this backup policy, create a rule that is used to select the appropriate VMs that have log truncation performed.
10. Create a backup policy for the backups.

    During the backup policy creation process, you:

    a. Assign the new dataset to the new backup policy.
    b. Assign a schedule to the new backup policy.
    c. Assign a retention policy to the new backup policy.
    d. If multiple guest VMs are being backed up as part of this backup policy, in the **Members** pane of the Policy wizard, select **Enable Dynamic rule** and select the rule that you previously created.

    The *Avamar Administration Guide* provides more information about backup policies, rules, datasets, schedules, and retention policies.
11. Enable scheduling for the backup policy.

Scheduled backups with Microsoft Exchange log truncation

Avamar performs log truncation of an Exchange Server Database after the backup has completed.

This section describes how to schedule backups that perform log truncation.

Scheduling backups that contain multiple VMs requires an automated mechanism to select the VMs that are hosting Exchange databases. Rules contain filtering mechanisms, such as the VM name or VM tag, that determine which VMs qualify under the rules. Configuring your VMs that host Exchange databases correctly within vCenter, and configuring corresponding rules, allows you to determine which VMs in a multiple VM backup should have log truncation performed.

Log truncation with Microsoft Exchange is supported with the following:

- vSphere 6.5 and greater and ESXi 6.5 and later
- Windows Server 2008 R2 and later
- Exchange 2007 and later
- VMware Tools release 10.1 or later must be installed on the VM hosting the Exchange server

Scheduling backups of Microsoft Exchange servers for log truncation

Scheduled backups of Microsoft Exchange servers for log truncation are configured using the following procedure.

About this task

Follow this procedure to create a dataset for Exchange server backup and schedule backups of Microsoft Exchange servers for log truncation.

Steps

1. In the AUI navigation pane on the left, click », and then click **Setting**.
   The **Setting** pane is displayed.
2. Click the **Dataset** tab.
3. Click **ADD**.

   The **Create Dataset** window is displayed.
4. In the **Dataset Name** field, type a name for the dataset.

   The name can include alphanumeric characters (A-Z, a-z, 0–9) and the following special characters: period (.), hyphen (-), and underscore (_), and space. Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
5. In the **Plugins** list, select the **Windows VMware Image** plug-in.
6. Click the **Options** tab, and perform the following steps:
   a. To view advanced options, select the **Show Advanced Options** check box.
   b. In the **Guest Credentials** field, type a virtual machine guest operating system user account name and password with sufficient privileges to run scripts before or after the backup.
   c. Select the type of post-action operation. **LOG Truncation** performs log truncation after the backup has successfully completed.
   d. Complete other information in the **Options** tab as required.

      The *Avamar Administration Guide* contains further information about creating and configuring datasets.
7. Click the **Source Data** tab, and then select **All virtual disks**:
8. Click **SUBMIT**.
9. If multiple guest VMs are being backed up as part of this backup policy, create a rule that is used to select the appropriate VMs that have log truncation performed.
10. Create a backup policy for the backups.

    During the backup policy creation process, you:

    a. Assign the new dataset to the new backup policy.
    b. Assign a schedule to the new backup policy.
    c. Assign a retention policy to the new backup policy.
    d. If multiple guest VMs are being backed up as part of this backup policy, in the **Members** pane of the Policy wizard, select **Enable Dynamic rule** and then select the rule that you previously created.

    The *Avamar Administration Guide* provides more information about backup policies, rules, datasets, schedules, and retention policies.
11. Enable scheduling for the backup policy.

Monitor backups

You can monitor and view status information for backup and restore operations by using the **Activity Monitor**.

About this task

To access the **Activity Monitor**, open the navigation pane, and then click **Activity**. The **Activity Monitor** appears with a list of all activities.

> ⓘ **NOTE:** The AUI **Activity Monitor** window has been optimized for at least 1366 pixels-wide screens. Display issues might occur for smaller screens. To properly display the AUI, ensure that your display is at least 1366 pixels wide.

The **Activity Monitor** provides you with options to filter the information that appears:

To filter activities by client, start time, plug-in, or type, click ▼ in their respective column.

The **Activity Monitor** displays the date and time that an activity began, and the total number of bytes examined during an activity.

To view activity details, expand the **Details** pane, by clicking «.

Cancel backups

You can cancel a backup any time before it completes. The cancellation might take 5 minutes or longer. The backup might complete before the cancellation finishes.

Steps

1. In the AUI navigation pane on the left, click », and then click **Activity**.
   The **Activity Monitor** appears with a list of activities.
2. Select the backup from the list.
3. Click **CANCEL**.
   A confirmation dialog box is displayed.
4. Click **YES**.

Support for vCenter HA failover for inflight backups

During a vCenter failover period, the Avamar software monitors the failover process and performs the following actions.

1. Automatically detects vCenter failover events and then waits for the vCenter failover to complete.
2. Cancels the hanging backup jobs that were caused by vCenter HA failover.
3. Removes mounted HotAdded disks from the proxy appliance.
4. Restarts all incomplete backups during the vCenter HA failover.

Configure a backup to support VMware encryption

Avamar supports encrypted virtual machine backups.

Prerequisites

- Review the known limitations for configuring a backup to support VMware encryption.
- To backup or restore encrypted virtual machines, ensure that the proxy appliance is also encrypted.
- Ensure that the proxy appliance is manually mapped to the backup policy.

About this task

For details about virtual machine encryption, the VMware *vSphere Security Guide* provides more information.

When backing up an encrypted virtual machine, perform the following steps:

Steps

1. Establish encryption for the virtual machine:
   a. Set up the KMS.
   b. Create the VM encryption policy.
2. Encrypt the proxy appliance.
3. Use a Linux text editor to open `/usr/local/avamarclient/var/vddkconfig.ini`.
4. Locate the value `vixDiskLib.transport.hotadd.NoNFCSession`.
5. Change the value to **0**.

   This change overrides a VMware VDDK issue that inhibits hot-adding an encrypted virtual machine. The VMware Release Notes provide more information.
6. Save and close the file.
7. Set the following permissions for the Avamar admin role:

   Crytopgraphic operations > **Add disk**.

   Crytopgraphic operations > **Direct access**.

Configure a backup to support VMware CEIP

Avamar support enables VDDK CEIP virtual machine backups.

Prerequisites

- Review the known limitations for configuring a backup to support VMware CEIP.
- Ensure that the proxy version >= 19.7.100.

About this task

For details about VMware CEIP, see the VMware VDDK Release Notes. To backup a virtual machine with CEIP, perform the following steps:

Steps

1. Log in to the proxy.
2. Use a Linux text editor to open `/usr/local/avamarclient/var/vddkconfig.ini`.
3. Locate the value `vixDiskLib.phoneHome.EnablePhoneHome`.
   There is no change in `EnablePhoneHome=1` setting in the VDDK configuration file. However, if the vendor details are not set, you must set it to the following values:

   ```
   vixDiskLib.phoneHome.ProductName = "Dell EMC Avamar Proxy"
   ```

   ```
   vixDiskLib.phoneHome.ProductVersion = "19.7.100"
   ```

   If these values are not set, the vendor name and version appears as `Unknown` in VMware analytics. VMware Release Notes provide more information on this.
4. Save and close the file.

VMware encryption support limitations

Consider the following known limitations of Avamar for VMware encryption support.

- As a result of disabling NoNFCSession, backup and restore in VMware Cloud on AWS is not supported. This VMware limitation is addressed in the vddk update.
- When restoring from an encrypted virtual machine and backup, the restored data is unencrypted.
- Restoring virtual machines requires that the target vCenter is configured for the same Key Management Service (KMS) host as the source vCenter.

- Attempts to perform an application-consistent quiesce snapshot on an encrypted virtual machine fails back to a file system-consistent snapshot. This process generates an error message in vCenter, which you can ignore. This process is a VMware limitation.
- When restoring a virtual machine as a new image:
  - By default, new virtual machines are not encrypted. If encryption is wanted, apply the required storage policy.
  - For cases where a boot order other than the default was implemented before the image backup was performed, the original boot order is not restored. In this case, you must select the correct boot device after the restore completes. Alternatively, you can enter the nondefault boot order to the VMX file so that the restored virtual machine starts without any reconfiguration.

    This limitation does not affect virtual machines that use the default boot order.

Configure a backup to support vSAN encryption

Avamar supports encrypted vSAN backups.

Prerequisites

For details about vSAN encryption, the VMware *Administering VMware vSAN Guide* provides more information.

About this task

Before you configure a backup to support vSAN encryption, consider the following points:

- To backup or restore virtual machines that reside on vSAN datastores, deploy the proxy on a vSAN datastore.
- You can use a proxy that is deployed on a vSAN datastore to back up virtual machines from other vSAN datastores (encrypted or non-encrypted) by using hotadd or nbdssl transport modes.
- You can use a proxy that is deployed on a vSAN datastore to back up virtual machines from other non-vSAN datastores by using hotadd or nbdssl transport modes.
- Avamar supports all backup and restore functionality for encrypted vSAN virtual machines.
- Avamar supports restoring an encrypted vSAN virtual machine to a different vCenter that has a non-encrypted datastore.

Steps

1. Set the following permissions for the Avamar administrator:

Table 11. Required permissions for the Avamar Administrator

Object	Permissions	Sub-permissions
Datastore	Allocate Space	
	Browse Datastore	
	Low level file operations	
Virtual Machine	Inventory	All
	Interaction	Power on
	Interaction	Power off
	Interaction	Suspend
	Interaction	Reset
	Interaction	Perform wipe or shrink operations
	Configuration	All
	Provisioning	Allow disk access
	Provisioning	Clone template
	Provisioning	Clone Virtual Machine
	Snapshot	All

Table 11. Required permissions for the Avamar Administrator (continued)

Object	Permissions	Sub-permissions
Folder	Create folder	
	Delete folder	
Global	Act as vCenter Server	
	Disable Methods	
	Enabled Methods	
	System Tag	
Resource	Assign virtual machine to resource pool	
Host	Configuration	Advanced Settings
Network	All	
Profile-driven Storage	All	
Crytopgraphic operations	Add disk	
	Direct access	

2. Create a group for the backup as described in Schedule backups using the AUI Policy wizard.

   NOTE: To backup a vSAN virtual machine, deploy the proxy in the vSAN datastore.

Enforcement of backups to Data Domain

If the Avamar server is configured to enforce backups to a Data Domain system, the server rejects backups that are not destined for the Data Domain. This enforcement covers backups that you configure through the Avamar Administrator and the AUI, as well as from command-line interfaces and other tools.

These backups must have additional flags that indicate the storage target. The *Avamar and Data Domain System Integration Guide* provides more information about backup enforcement and the related client version requirements. Backup enforcement is disabled by default.

5

Restore

Topics:

- Image and file-level restore guidelines
- Image backup overview
- File Level Restore

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 relatively small amounts of data.

If you restore a large number 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). Copy those files to the desired location following the restore.

Year 2038

Avamar 19.2 and later server subsystems support backup retention until February 2106. However, for earlier releases, due to the signed 32-bit integer time format of UNIX and Linux operating systems, the Avamar server subsystems will support backup retention until January 2038 and therefore cannot restore backup after this date.

Newer Avamar releases offer support for longer retention periods:

- Backup retention after 2038 is successful when all Avamar subsystems use unsigned 32-bit integers.
- In Avamar 19.2 and later releases, the Avamar server, client, and plug-ins subsystems all use an unsigned 32-bit integer and will continue to start and retain data until 2106.
- In Avamar 19.1, only the Avamar server subsystem used an unsigned 32-bit integer, and will continue to start until 2106. However, the Avamar client and plug-ins subsystems used a signed 32-bit integer and will only retain data until 2038.
- In Avamar 19.1 and earlier releases, the Avamar server, client, and plug-ins subsystems all used a signed 32-bit integer, and will only continue to start and retain data until 2038.

Therefore, with an Avamar 19.2 and later server subsystem and Avamar 19.2 or later client and plug-ins subsystems, all backup retention succeeds after 2038.

Avamar 19.2 and later clients also support restoring backups where the retention time is after 2038, and where the local (server and client) time is after 2038. Earlier client releases do not support this.

For backups of Windows or Linux clients, do not assign a retention period for a date after February 7, 2106.

Monitor restores

You can monitor and view status information for backup and restore operations in the **Activity Monitor**.

About this task

To access the **Activity Monitor**, open the navigation pane, and then click **Activity**. The **Activity Monitor** appears with a list of all activities.

ⓘ **NOTE:** The AUI **Activity Monitor** window has been optimized for at least 1366 pixels-wide screens. Display issues might occur for smaller screens. To properly display the AUI, ensure that your display is at least 1366 pixels wide.

The **Activity Monitor** provides you with options to filter the information that appears:

To filter activities by client, start time, plug-in, or type, click
▼
in their respective column.

The **Activity Monitor** displays the date and time that an activity began, and the total number of bytes examined during an activity.

To view activity details, expand the **Details** pane, by clicking
«
.

Cancel restores

You can cancel a restore any time before it completes. The cancellation might take 5 minutes or longer. The restore might complete before the cancellation finishes.

Steps

1. In the AUI navigation pane on the left, click », and then click **Activity**.
   The **Activity Monitor** appears with a list of activities.
2. Select the restore from the list.
3. Click **CANCEL**.

   A confirmation dialog box is displayed.
4. Click **YES**.

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 step reduces the amount of time that is 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.
3. The MCS NFS datastore poller automatically unmounts unused Data Domain NFS mounts once daily. Ensure that the NFS mount is unmounted and removed by performing the following:
   - When IA fails due to permission denial for creating VM, DD NFS datastore is mounted in the customer ESXi. The datastore is unmounted automatically every 24 hours. You can also configure unmount time period by changing the following value:

     ```
     <entry key="ddr_nfs_poller_interval_hour" value="24" />
     ```

     in `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`

NOTE: When used with Data Domain systems earlier than release 6.0, to minimize operational impact to the Data Domain system, only one instant access is permitted at a time. For Data Domain systems at release 6.0 or greater, 32 instant access processes are permitted at the same time. With DDOS 7.2 and DD 9400, we can support up to 64 instance access at the same time. If you are using the same ESXi host as the target for multiple instant access processes, then to achieve

32 instant access processes, you must increase the values for the following settings on the ESXi host to the maximum supported values:

- Under NFS, update NFS.MaxVolumes.
- Under Net, update Net.TcpipHeapSize.
- Under Net, update Net.TcpipHeapMax.

VMware KB article 2239 contains further information about increasing the limits for these settings. Refer VMware documentation for concurrent Virtual machine migration limits.

Enable maximum number of instance access to 64 with DDOS7.2 and DD9400

The maximum number of VMware Instant Access restores allowed is 64 from DD OS 7.2 and DD 9400 onwards.

About this task

Perform the following steps to update **mcserver.xml** in Avamar server:

Steps

1. Stop the MCS by typing the following command:

   ```
   dpnctl stop mcs
   ```

2. Open `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` in a UNIX text editor.
3. Change the value from 32 to 64 and restart MCS Services.

   ```
   <node name="ddr_default_ir_limit_by_ddos_version">
   <map>
   <entry key="6.0" value="64" merge="newvalue" />
   </map> </node>
   ```

4. Restart the MCS by typing the following command:

   ```
   dpnctl start mcs
   ```

Restoring the virtual machine

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, 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.
3. In the list of clients, select the virtual machine client or VMware container.

   A list of completed backups for this instance is displayed. Any backup in this list can be used to restore the instance.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup residing on the Data Domain.

   The list of backups for the date range is displayed.
5. Click the **RESTORE** tab.

The **Select Restore Content** dialog box appears and displays a list of volumes that are contained within the backup. The volume names identify the original mount point.

6. In the **Select Restore Content** dialog box, perform the following steps:
   a. In the hierarchy tree, select the virtual disk that you want to restore.
   b. In the Contents pane, select the files that are contained within the folder.
   c. Click **NEXT**.

   The **Restore** wizard is displayed and opens to the **Basic Config** pane.
7. In the **Basic Config** pane, perform the following steps:
   a. In the **Destination** field, select **Instant Acess**.
   b. Click **NEXT**.

   The **Advanced Config** pane appears.
8. In the **Advanced Config** pane, perform the following steps:
   a. In the **VM Name** field, type a unique name for the new virtual machine.
   b. Click **NEXT**.

   The **Location** pane appears.
9. In the **Location** pane, perform the following steps:
   a. In the inventory tree, select a data center and folder location.
   b. Click **NEXT**.

   The **Host/Cluster** pane appears.
10. In the **Host/Cluster** pane, perform the following steps:
    a. In the inventory tree, select a host or cluster.
    b. Click **NEXT**.

    The **Resource Pool** pane appears.
11. In the **Resource Pool** pane, perform the following steps:
    a. In the inventory tree, select a resource pool.
    b. Click **NEXT**.

    The **Summary** pane appears.
12. In the **Summay** pane, review the provided information, and then click **FINISH**.
    The following status message is displayed:

    ```
    Restore request initiated.
    ```

Performing post-restore migration and clean-up

Steps

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 link.
   The **Server** window is displayed.
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**.

Restore an instance of a VM backup by using the AUI

Any successful instance backup can be used to restore a copy of that instance. You can find a backup to restore by date. When you perform the restore, you can restore to either the original location, a different location, or multiple locations.

When you perform the restore, you can restore to either the original virtual machine, to a new virtual machine, or to a different virtual machine.

Selecting a backup instance to restore

About this task

The steps in this procedure apply to the following plug-in types:

- Microsoft Windows File System
- Linux File System
- VMware image
- VMware File Level Restore (FLR)
- Microsoft SQL
- Microsoft Hyper-V
- Microsoft Exchange

For all other plugin types that are not in this list, use Avamar Administrator.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.
3. In the list of clients, select the client computer to recover.

   A list of completed backups for this instance is displayed. Any backup in this list can be used to restore the instance.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **RESTORE** tab.
   The **Select Restore Content** dialog box appears and displays a list of volumes that are contained within the backup. The volume names identify the original mount point.
6. (Optional) To perform a file-level restoration (FLR) of the content, perform the following steps:
   a. Toggle the **FLR** switch to on.

      The list of folders is displayed.
   b. Select the folder or file that you want to restore, and then click **RESTORE**.

   The FLR feature retrieves files from the backup without the need to complete a full restore operation. This feature provides the ability to restore specific files from a volume in a particular backup, or browse the files that are contained in the backup volumes.
7. In the **Select Restore Content** dialog box, perform the following steps:
   a. In the hierarchy tree, select the folder that you want to restore.
   b. In the Contents pane, select the files that are contained within the folder.
   c. Click **NEXT**.

   The **Restore** wizard is displayed and opens to the **Basic Config** page.

   For information about how to restore to the original virtual machine, see Restore data to the original virtual machine.

Restore data to the original virtual machine

About this task

To access the Restore wizard, in the AUI navigation pane on the left, click », and then click **Asset Management** > **Restore**.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.
3. In the list of clients, select the client system to recover.

   A list of completed backups for this instance is displayed. Any backup in this list can be used to restore the instance.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **RESTORE** tab.

   The **Select Restore Content** dialog box appears and displays a list of volumes that are contained within the backup. The volume names identify the original mount point.
6. (Optional) To perform a file-level restoration (FLR) of the content, perform the following steps:
   a. Toggle the **FLR** switch to on.

      The list of folders is displayed.
   b. Select the folder or file that you want to restore, and then click **RESTORE**.

   The FLR feature retrieves files from the backup without the need to complete a full restore operation. This feature provides the ability to restore specific files from a volume in a particular backup, or browse the files that are contained in the backup volumes.
7. In the **Select Restore Content** dialog box, perform the following steps:
   a. In the hierarchy tree, select the folder that you want to restore.
   b. In the **Contents** pane, select the files that are contained within the folder.
   c. Click **NEXT**.

   The **Restore** wizard is displayed and opens to the **Basic Config** page.
8. In the **Destination Client** field:
   a. Select **Restore to Original Virtual Machine**.
   b. Click **NEXT**.

   The **Backups** pane is displayed.
9. In the **Backup Content** pane, perform the following steps:
   a. In the hierarchical Domain tree, select the client that you want to restore.

      The **Contents of Backup** pane displays a list of files that are contained within that folder.
   b. In the right pane, select the virtual machine backup that you want to restore.
   c. Click **NEXT**.

   The **Destination Location** pane is displayed.
10. In the **Destination Location**pane, select **Restore to Original Virtual Machine**.

    The **More Options** pane is displayed.
11. In the **More Options** pane, set the plug-in options:
    a. In the **Post Restore Options** field, select an option.
    b. To restore the virtual machine configuration, select **Restore Virtual Machine Configuration**.
    c. To restore the virtual machine as a new disk, select **Restore as a new disk**.
    d. To use Changed Block Tracking (CBT) to increase performance, select **Use CBT to increase performance**.
    e. In the **Proxy** field, select an option.

    Plug-in Options provides the complete list of plug-in options.
12. Click **NEXT**.

    The **Summary** pane is displayed.
13. In the **Summay** pane, review the provided information, and then click **FINISH**.
    The following status message is displayed:

```
Restore request initiated.
```

Restore data to a different virtual machine

About this task

To access the Restore wizard, in the AUI navigation pane on the left, click », and then click **Asset Management** > **Restore**.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.
3. In the list of clients, select the client system to recover.

   A list of completed backups for this instance is displayed. Any backup in this list can be used to restore the instance.
4. (Optional) To locate backups by date:
   - a. In the right pane, click **VIEW MORE**.
   - b. Click **SEARCH**.
   - c. In the **From** and **To** fields, specify the date range.
   - d. Click **RETRIEVE**.
   - e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **RESTORE** tab.

   The **Select Restore Content** dialog box appears and displays a list of volumes that are contained within the backup. The volume names identify the original mount point.
6. (Optional) To perform a file-level restoration (FLR) of the content, perform the following steps:
   - a. Toggle the **FLR** switch to on.

     The list of folders is displayed.
   - b. Select the folder or file that you want to restore, and then click **RESTORE**.

   The FLR feature retrieves files from the backup without the need to complete a full restore operation. This feature provides the ability to restore specific files from a volume in a particular backup, or browse the files that are contained in the backup volumes.
7. In the **Select Restore Content** dialog box, perform the following steps:
   - a. In the hierarchy tree, select the folder that you want to restore.
   - b. In the Contents pane, select the files that are contained within the folder.
   - c. Click **NEXT**.

   The **Restore** wizard is displayed and opens to the **Basic Config** page.
8. In the **Basic Config** pane, perform the following steps:
   - a. In the **Destination** field, select **Restore to different (existing) Virtual Machine**.
   - b. In the **Post Restore Options** field, select an option.
   - c. To restore the virtual machine as a new disk, select **Restore as a new disk**.
   - d. To use Changed Block Tracking (CBT) to increase performance, select **Use CBT to increase performance** check box.
   - e. In the **Proxy** field, select an option.

   Plug-in Options provides the complete list of plug-in options.

   The **Advanced Config** page appears.
9. In the **Advanced Config** pane, complete the following steps:
   - a. To view hosts, toggle **Host/Cluster** to off.
   - b. To view a cluster, toggle **Host/Cluster** to on.
   - c. In the **Host/Cluster** pane, expand the domain name, and then select a host or cluster.

     The selected IP address appears.
10. Click **NEXT**.

    The **Summary** pane is displayed.
11. In the **Summay** pane, review the provided information, and then click **FINISH**.
    The following status message is displayed:

    ```
    Restore request initiated.
    ```

Restore data to a new virtual machine

About this task

To access the Restore wizard, in the AUI navigation pane on the left, click », and then click **Asset Management** > **Restore**.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.
3. In the list of clients, select the client system to recover.

   A list of completed backups for this instance is displayed. Any backup in this list can be used to restore the instance.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **RESTORE** tab.

   The **Select Restore Content** dialog box appears and displays a list of volumes that are contained within the backup. The volume names identify the original mount point.
6. (Optional) To perform a file-level restoration (FLR) of the content, perform the following steps:
   a. Toggle the **FLR** switch to on.

      The list of folders is displayed.
   b. Select the folder or file that you want to restore, and then click **RESTORE**.

   The FLR feature retrieves files from the backup without the need to complete a full restore operation. This feature provides the ability to restore specific files from a volume in a particular backup, or browse the files that are contained in the backup volumes.
7. In the **Select Restore Content** dialog box, perform the following steps:
   a. In the hierarchy tree, select the folder that you want to restore.
   b. In the Contents pane, select the files that are contained within the folder.
   c. Click **NEXT**.

   The **Restore** wizard is displayed and opens to the **Basic Config** page.
8. In the **Basic Config** pane, perform the following steps:
   a. In the **Destination** field, select **Restore to new Virtual Machine**.
   b. In the **Post Restore Options** field, select an option.
   c. To use Changed Block Tracking (CBT) to increase performance, select **Use CBT to increase performance** check box.
   d. In the **Proxy** field, select an option.

   Plug-in Options provides the complete list of plug-in options.

   The **Advanced Config** page appears.
9. In the **Advanced Config** pane, complete the following steps:
   a. In the **vCenter** field, select a vCenter.
   b. In the **VM Name** field, type the name of the virtual machine.
   c. Click **NEXT**.
10. In the **Location** pane, complete the following steps:
    a. Expand the domain name, and then select a destination.

       The selected location appears.
    b. Click **NEXT**.
11. In the **Host/Cluster** pane, complete the following steps:
    a. Expand the domain name, and then select a host or cluster.

       The selected IP address appears.
    b. Click **NEXT**.

12. In the **Resource Pool** pane, complete the following steps:
    a. Expand the domain name, and then select a resource pool.

       The selected resource pool appears.
    b. Click **NEXT**.
13. On the **Datastore** pane, complete the following steps:
    a. Select a datastore.
    b. Click **NEXT**.
14. Click **NEXT**.

    The **Summary** pane is displayed.
15. In the **Summay** pane, review the provided information, and then click **FINISH**.
    The following status message is displayed:

    ```
    Restore request initiated.
    ```

Image backup overview

Image backup offers three levels of restore functionality: image restore, file-level restore (FLR), 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 12. 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-level restore limitations

The following limitations apply to image-level restores from virtual machine backups.

Virtual machine power state

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

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.

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:

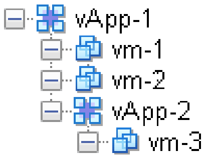


Figure 7. Example nested container structure

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

Two interim solutions exist for this limitation:

- 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

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

Perform the following steps to restore the full image or selected drives to the original virtual machine:

Steps

1. In the **vSphere Client** or **vSphere Web Client**, ensure that the target virtual machine is powered off.
2. In the AUI left navigation pane, click >>, and then click **Asset Management**.
   The **Asset Management** window displays.
3. In the **Domain** pane, select the domain that contains the virtual machine client or VMware container that you want to restore.
4. From the list of clients in the **Asset Management** pane, select the virtual machine client or VMware container.

   The **Client Summary** pane displays backup statistics for the selected object.
5. (Optional) To locate backups by date:
   a. In the **Client Summary** pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
6. Click the **RESTORE** tab.

   The **Restore wizard** appears. If you clicked **RESTORE** from the **Asset Management** pane, the wizard opens on the **Backup List** page, which allows you to select from the available backups for the selected object. If you performed step 5, the wizard opens on the **Content** page, since the backup has already been selected from the list of available backups. The **Content** page displays a list of volumes that are contained within the backup. The volume names identify the original mount point.
7. In the **Content** page:
   a. From the hierarchy tree, select the folder that you want to restore.
   b. Select the files that are contained within the folder.
   c. Click **NEXT**.

   The **Basic Config** page appears.
8. In the **Basic Config** page:

   a. In the **Destination** field, select **Restore to Original Virtual Machine**.
   b. In the **Post Restore Options** field, select an option.
   c. To restore the virtual machine configuration, select the **Restore Virtual Machine Configuration** check box.
   d. To restore the virtual machine as a new disk, select the **Restore as a new disk** checkbox.
   e. To use Changed Block Tracking (CBT) to increase performance, select the **Use CBT to increase performance** check box.
   f. In the **Proxy** field, select an option.
   g. Click **NEXT**.

   The **Summary** pane is displayed.

9. Click **NEXT**.

   The **Summary** pane is displayed.

10. In the **Summay** pane, review the provided information, and then click **FINISH**.
    The following status message is displayed:

    ```
    Restore request initiated.
    ```

11. If the destination virtual machine for the restore is 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.

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

Perform the following steps to restore the full image or selected drives to a different virtual machine:

Steps

1. In the **vSphere Client** or **vSphere Web Client**, ensure that the target virtual machine is powered off.
2. In the AUI left navigation pane, click », and then click **Asset Management**.
   The **Asset Management** window displays.
3. In the **Domain** pane, select the domain that contains the virtual machine client or VMware container that you want to restore.
4. From the list of clients in the **Asset Management** pane, select the virtual machine client or VMware container.

   The **Client Summary** pane displays backup statistics for the selected object.
5. (Optional) To locate backups by date:
   a. In the **Client Summary** pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
6. Click the **RESTORE** tab.

   The **Restore wizard** appears. If you clicked **RESTORE** from the **Asset Management** pane, the wizard opens on the **Backup List** page, which allows you to select from the available backups for the selected object. If you performed step 5, the wizard opens on the **Content** page, since the backup has already been selected from the list of available backups. The **Content** page displays a list of volumes that are contained within the backup. The volume names identify the original mount point.
7. In the **Content** page:
   a. From the hierarchy tree, select the folder that you want to restore.
   b. Select the files that are contained within the folder.
   c. Click **NEXT**.

   The **Basic Config** page appears.
8. In the **Basic Config** page, perform the following steps:
   a. In the **Destination** field, select **Restore to different (existing) Virtual Machine**.
   b. In the **Post Restore Options** field, select an option.
   c. To restore the virtual machine as a new disk, select the **Restore as a new disk** checkbox.

   d. To use Changed Block Tracking (CBT) to increase performance, select the **Use CBT to increase performance** check box.
   e. In the **Proxy** field, select an option.
   f. Click **NEXT**.

   The **Advanced Configuration** pane is displayed.

9. In the **Advanced Config** pane, complete the following steps:
   a. To view hosts, toggle **Host/Cluster** to off.
   b. To view a cluster, toggle **Host/Cluster** to on.
   c. In the **Host/Cluster** pane, expand the domain name, and then select a host or cluster.

      The selected IP address appears.

10. Click **NEXT**.

    The **Summary** pane is displayed.

11. In the **Summay** pane, review the provided information, and then click **FINISH**.
    The following status message is displayed:

```
Restore request initiated.
```

12. If the destination virtual machine for the restore 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.

Restore the full image or selected drives to a new virtual machine by using Avamar Administrator

Steps

1. In Avamar Administrator, click the **Backup & Restore** launcher link.
   The **Backup, Restore and Manage** window is displayed.
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 *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.

File Level Restore

File Level Restore (FLR) enables you to restore individual files and folders from a backup without requiring a full (image-level) restore. You can browse the files contained within a backup volume to select the specific items you want to restore.

NOTE: To use FLR, ensure that the virtual machine is powered on.

NOTE: FLR supports and works on Open VM Tools.

Performance improvements for File Level Restore

By default, Avamar uses the HTTPS (443) protocol to perform FLR. This improves the performance of restores by providing a faster mechanism for file transfer than the previous mechanism using file copy.

If HTTPS (443) is not available, Avamar uses file copy, the previous mechanism, to perform FLR.

The following warning message is displayed during restore:

NOTE: The warning message displayed during restore is seen only on MCGUI FLR.

```
Target VM: client cannot reach proxy: proxy via https due to incorrect network
configuration. Restoration process may take significantly longer time. Press ‘continue’
to start the restore.
```

where:

- *client* is the name of the FLR Guest VM.
- *proxy* is the name of the proxy.

Select **Yes** to continue the restore operation using file copy. The restore takes significantly longer.

ⓘ **NOTE:** This implementation requires the `wget` command. To take advantage of the performance improvement, you must have `wget` installed on the client.

File-level restore supported configurations

The following supported configurations require that both the proxy version and Avamar server to be at Avamar release 7.5 Service Pack 1 or later:

Partitioning scheme

The following table outlines the partitioning scheme for (File-level restore) FLR.

Table 13. FLR support partitioning scheme

Partitioning scheme	Guest operating system	FLR	Comment
MBR	Windows or Linux	Supported	None
EBR (Logical Partition)	Windows or Linux	Supported	None
GPT	Windows or Linux	Supported	None
MixedGPT	Windows or Linux	Not supported	Hybrid MBR

File system support

The following table outlines the file system support for FLR.

Table 14. File system support for FLR

File system type	Guest operating system	Partitioning scheme	Partition ID	Partitionless disk	LVM
ext2	Linux	MBR, EBR, GPT	0x83/Linux file system	Support	Support
ext3	Linux	MBR, EBR, GPT	0x83/Linux file system	Support	Support
ext4	Linux	MBR, EBR, GPT	0x83/Linux file system	Support	Support
ntfs	Windows	MBR, EBR, GPT	0x04/0x07	Support	Support
vfat	Windows	MBR, EBR	0x06/0x0E	Support	Support
xfs	Linux	MBR, EBR, GPT	0x83/Linux file system	Support	Support
reiserfs	Linux	MBR, EBR	0x83	Support	Support
btrfs	Linux	MBR, EBR, GPT	0x83/Linux file system	Support	Support

LVM support

The following table outlines the LVM support for FLR.

Table 15. LVM support for FLR

LV type	FLR
Linear LV	Support
Striped LV	Support

Table 15. LVM support for FLR (continued)

LV type	FLR
Mirrored LV	Support
RAID LV	Support
Thin LV	Support

Windows Dynamic Disk support

The following table outlines the Windows Dynamic Disk support for FLR.

Table 16. Windows Dynamic Disk support for FLR

Volume Type	FLR
Simple	Support
Spanned	Support
Striped	Support
Mirrored	Support
RAID 5	Not Support

Multidevice support

The following table outlines multidevice support for FLR.

Table 17. Multidevice support for FLR

RAID	Occur	FLR
RAID 0/Striping	LVM/BTRFS	Support
RAID 1/Mirroring	LVM/BTRFS	Support
RAID 4	LVM	Support
RAID 5	LVM	Support
RAID 6	LVM	Support
RAID 10	LVM/BTRFS	Support

RSA SecurID authentication in the AUI

Avamar supports RSA SecurID, which is a two-factor authentication technology that is used to protect network resources.

You can use two-factor authentication (2FA) for FLR of guest virtual machine backups in the AUI. Avamar 19.7 and later releases support 2FA on AUI login as well.

Log in to the AUI as an administrator to configure the required RSA server information to store in the Avamar server. This information is then used to verify the connection with the RSA authentication manager.

Once you log in, you can perform the following operations:

- Add the RSA Authentication Manager.
- Add or delete a replication RSA server.

ⓘ **NOTE:** You can only add one RSA Authentication Manager. You can add 0 through 10 replication RSA servers.

Add RSA Manager

To add or edit the RSA Manager, perform the following steps:

About this task

NOTE: Avamar supports only one RSA authentication server at a time.

Steps

1. In the AUI navigation pane on the left, click », and then click **System**.
   The **System** window appears.
2. Select the **RSA Authentication Manager** tab.
3. Click **ADD/EDIT RSA MANAGER**.
   The **RSA Manager** window appears, prompting you to provide the following configuration information for both a new and existing RSA Manager:
   - RSA Client ID—The Avamar server fully qualified domain name (FQDN), which is registered as an agent on the RSA server.
   - RSA Base URL—the RSA server path, which includes the server FQDN and the port to use for communication with the Avamar server.

     For example, in this base url:
     `https://rsaauthmanger.com:5555/mfa/v1_1/` the
     `rsaauthmanger.com` is the
     `hostname` of RSA authentication server.
   - RSA Access ID—the RSA server remote access ID.
   - RSA Access Key—the RSA server remote access key.
   - RSA Root Cert—the Root certificate is required for the Avamar authentication agent to establish a verified HTTPS connection with the RESTful service running on the authentication manager (RSA Manager).
4. After completing the configuration, click **Finish**.
   When you add an RSA Manager, an entry with the RSA server URL appears in the left pane.

Next steps

Add a replication RSA server. Add Replication RSA Server provides information.

Add Replication RSA Server

If the primary server becomes unavailable, adding one or more replication RSA servers enables you to continue RSA 2FA authentication.

About this task

NOTE: Avamar supports one RSA authentication server at a time. If all replication servers and the primary server are not available, authentication fails.

Steps

1. In the AUI navigation pane on the left, click », and then click **System**.
   The **System** window displays.
2. Select the **RSA Authentication Manager** tab.
3. Click **ADD REPLICATION RSA SERVER**.
   The **Add RSA Authentication Manager** window displays.
4. Type the **Replication Server Base URL**, which includes the server FQDN and the port to use for communication with the Avamar server, and then click **Finish**.

Results

An entry for the added replication server now appears below the entry for the RSA Authentication Manger in the left pane of the **System** window. If you want to remove a replication server, select the entry in the left pane and click **DELETE REPLICATION RSA SERVER**, and then confirm the selection.

File Level Restore troubleshooting and limitations

Review the following information that is related to FLR troubleshooting and limitations:

File Level Restore limitations

Note the following limitations to FLR support:

- You cannot restore or browse symbolic links.
- Browsing either a specified directory that is contained within a backup or a restore destination is limited to 50,000 files or folders.
- Restore is limited to 20,000 objects (files or folders) in the same restore operation.
- You can restore files from a Windows backup only to a Windows machine, and files from a Linux backup only to a Linux machine.
- When performing a file-level restore to a `/tmp` location, the Avamar software redirects data to a private `/tmp` location.

  For example: `/tmp/systemd-private-*`
- To overwrite ACLs of an existing file or folder, ensure that the user has ownership rights of the target file or folder that is being overwritten.
- On a Linux virtual machine that is configured with the Logical Volume Manager (LVM), an FLR operation in concurrence with a backup operation sometimes fails, and displays the following error message:

  ```
  Failed to get the file's properties.
  ```
- `fdisk` on a proxy displays the GPT partition as *Linux file system*.
- `/etc/fstab` does not contain GPT *PARTUUID* and *PARTLABLE*.

File Level Restore UI Limitations

- All virtual machine clients must be in `/vCenter/VirtualMachines` subfolder in the AUI. Any other location for the VMs is not supported.
- Only one vCenter is allowed to be configured for the AUI for FLR WEB UI to work.

> **NOTE:** If more than one vCenter is configured in Avamar, you must ensure that the Avamar server's `vcenter-sso-info.cfg` reflects the correct vCenter server for the VC_hostname parameter. For example, the sample file `/usr/local/avamar/var/ebr/server_data/prefs/vcenter-sso-info.cfg`:
>
> ```
> vcenter-sso-hostname=<VC_hostname>
> vcenter-sso-port=7444
> # configure only if more than one vCenter
> vcenter-hostname=<VC_hostname>
> ```

Unsupported virtual disk configurations

FLR does not support the following virtual disk configurations:

- Filesystems that support FLR require a higher kernel than proxy operating system. For example, ext4 sparse_super2, encryption, and project quotas.
- Encrypted or compressed partitions or bootloaders
- Deduplicated NTFS
- Browsing of multiple active disks or partitions. Only the first active disk or partition displays for browsing.

ⓘ **NOTE:** FLR operations on virtual machines with Logical Volume Manager (LVM) configurations are supported only if the LVM configuration is complete. A complete LVM configuration consists of at least one partition that is configured with a type 83/8E-Linux LVM, which consists of one or more physical volumes. These physical volumes contain one or more volume groups that are made up of zero or more logical volumes.

RSA 2FA verification errors

If you enabled **RSA 2FA** for FLR and experience any errors during 2FA verification, these errors likely originate from the RSA server. Contact your RSA administrator for assistance checking the RSA server log and troubleshooting these errors.

File Level Restore (FLR) in the AUI

The FLR feature retrieves files from the backup without the need to complete a full restore operation. This feature provides the ability to restore specific files from a volume in a particular backup, or browse the files that are contained in the backup volumes.

Prerequisites

To perform FLR:

- Ensure that the source VM exists in VMware, and is powered on and registered.
- Ensure that an up-to-date version of VMware Tools is installed and running on the source VM.
- For non-Windows platforms, the user can be part of the Standard or Administrators group. It does not support Domain users.
- For Windows VMs, only a local administrator user can perform FLR. Also, ensure that you disable User Account Control (UAC). The knowledge base article at https://www.dell.com/support/kbdoc/en-us/000171773 provides more information.

About this task

To access the Restore wizard in the AUI left navigation pane, click », and then click **Asset Management** > **Restore**.

Steps

1. In the AUI navigation pane on the left, click », and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain for the client.
3. In the list of clients, select the client system to recover.

   A list of completed backups for this instance is displayed. Any backup in this list can be used to restore the instance.
4. (Optional) To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **From** and **To** fields, specify the date range.
   d. Click **RETRIEVE**.
   e. In the list of backups, select a backup.

   The list of backups for the date range is displayed.
5. Click the **RESTORE** tab.

   The **Select Restore Content** dialog box appears and displays a list of volumes that are contained within the backup. The volume names identify the original mount point.
6. To perform an FLR of the content, perform the following steps:
   a. Toggle the **FLR** switch to on.

      The list of folders is displayed.
   b. Select the folder or file that you want to restore, and then click **RESTORE**.

   The FLR feature retrieves files from the backup without the need to complete a full restore operation. This feature provides the ability to restore specific files from a volume in a particular backup, or browse the files that are contained in the backup volumes.

   The **Basic Config** pane appears.
7. In the **Basic Config** pane, perform the following steps:

a. To select a client, perform the following steps:
   i. Click **SELECT CLIENT**.

      The **Select Client** pane appears.
   ii. In the Domain tree, select a domain for the client.
   iii. In the **Client** pane, choose a destination client.
   iv. Click **OK**.

b. In the **Username** and **Password** fields, type the username and password for the destination client.

   If you enabled **RSA 2FA**, an additional password is required. This password is either a fixed pass code, or the RSA token code/system generated pass code. If you are unsure of the pass code that is required for verification, contact your RSA administrator.

c. In the **Location** field, the path for the restore.

d. (Optional) Select **Restore ACL** to restore ACLs.

e. In the **Proxy** field, select a proxy.

8. Click **NEXT**.

   The **Summary** pane is displayed.

9. In the **Summay** pane, review the provided information, and then click **FINISH**.
   The following status message is displayed:

   ```
   Restore request initiated.
   ```

Restore ACL for non-root user configuration

Prerequisites

If you are a non-root user and want to perform FLR with restore ACL perform the following steps:

About this task

NOTE: The operation is specific to FLR AUI. It is performed from Avamar Web User Interface (AUI) FLR and not from FLR web UI.

Steps

1. Linux VM FLR:
   - As an FLR user you belong to the root group. But you are a non-root user.
   - On proxy edit `/usr/local/avamarclient/bin/config.xml`, add a line

     ```
     <enablesudouserrestore>1</enablesudouserrestore>
     ```

     to the file if the same does not exists.
   - Restart **vmwareflr** service.
   - Copy **binary RestoreAcl** on proxy `/usr/local/avamarclient/bin/RestoreAcl` to target `VM /usr/bin/RestoreAcl`
   - On target `vm /etc/sudoers`, add or modify the following line:

     ```
      restore1
     ALL=(ALL) NOPASSWD:
     /usr/bin/RestoreAcl
     ```

     Where, **restore1** is the FLR user.
   - You have access right for destination folder, if you are a non-root user.

2. Windows VM FLR
   - There are no limitations for domain or local user to restore file with ACL. Only User Account Control (UAC) is disabled for these users.

Perform a File Level Restore (FLR) operation by using the Data Protection Backup and Recovery File Level Restore (FLR) UI

With the **Data Protection Backup and Recovery FLR UI**, a local user can restore specific files and folders from a source VM to the original VM on Windows and Linux VMs. In this mode, you connect to the **Restore Client** from a VM that has been backed up by Avamar.

Prerequisites

To perform FLR:

- Ensure that the source VM exists in VMware, and is powered on and registered.
- Ensure that an up-to-date version of VMware Tools is installed and running on the source VM.
- For non-Windows platforms, the user can be part of the Standard or Administrators group.
- For Windows VMs, ensure that you disable User Account Control (UAC) before performing an FLR. The knowledge base article at https://www.dell.com/support/kbdoc/en-us/000171773 provides more information.

Steps

1. Before performing file-level recoveries within the VMware guest operating systems, run the following script on the Avamar server:

   ```
   ebrserver.pl --init
   ```

2. To start the **Data Protection Backup and Recovery FLR UI**, open a web browser and type the following URL:

   https://*VMware_Backup_Appliance_Host*/flr

   Where *VMware_Backup_Appliance_Host* is the DNS name or IP address of the VMware Backup Appliance from which the VM is backed up.

   NOTE: If a user's environment does not meet HTTPS certificate validation requirements, then certificate validation fails and an error message appears asking the user if they want to continue to download packages. Ignoring certificate validation might cause security issues.

3. In the **Password** field, type the password of the VM that you want to browse and perform file restore operation on.
4. To launch the Data Protection Backup and Recovery FLR UI from the same VM that you want to browse and restore to, click **Login to original VM**.
   The **Select the backups to restore from** pane appears that lists the backups for the VM.
5. To launch the **Data Protection Backup and Recovery FLR UI** from a different VM that you want to browse and restore to:

   a. Select **Login to alternate VM**.
   b. Type the DNS name or IP address of the VMware Backup Appliance of the VM that you want to browse and restore to.

   The **Select the backups to restore from** pane appears that lists the backups for the VM.
6. Select a backup and then click **Next**.
   The **Select items to restore** pane appears.
7. Select the file to restore:

   a. In the left pane, browse the files and folders available for recovery.
   b. In the right pane, select the files and folders that you would like to recover.
   c. Click **Next**.
8. Click **Yes** to confirm that you have selected the correct files and folders.
   The **Select destination to restore to** pane appears.

   NOTE: If the folder hierarchy does not appear. The file system in use on the VM might not be supported.
9. (Optional) Toggle **Restore ACL** to restore ACLs.
10. In the **Select destination** to restore pane, perform the following steps:

    a. Select the folder to which you want to restore the items.
    b. Click **Finish**.

Restore VM tags

For Avamar 19.9 and later, you can back up and restore VM tag information as part of VM metadata. All the tags attached to the VM at the time of backup are backed up.

During the VM restore operation, tags are retrieved from the VM backup and are attached to the restored VM, if not already attached. By default, this feature is enabled, and you can manage it by using two options, `backupvmtags` and `restorevmtags` in the `avvcbimageAll.cmd` file on Avamar proxy.

If you do not want to back up the VM tags, set the value of `backupvmtags` to `false` in the `/usr/local/avamarclient/var/avvcbimageAll.cmd` file. You can also set the value of `backupvmtags` and `restorevmtags` by using free form in the AUI while issuing the work order ID.

During the restore operation, if you select **Restore to Original Virtual Machine** or **Restore to different (existing) Virtal Machine**, there is no impact on the tags which are already attached to the VM. When you select **Restore to new Virtual Machine**, if the backup already has a tag with same name or ID as the one you are trying to restore, then the tag does not get attached to the restored VM.

6

Backup Validation

Topics:

- Overview
- Performing an on-demand backup validation
- Scheduling backup validations

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 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

Perform the following steps to do an on-demand backup validation:

About this task

ⓘ **NOTE:** You can also perform an on-demand backup validation by using the AUI. For more information, see AUI Online Help.

Steps

1. In Avamar Administrator, click the **Backup & Restore** launcher link.
   The **Backup, Restore and Manage** window is displayed.
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 *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 operating system 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.

About this task

ⓘ **NOTE:** You can also create a VM backup validation group by using the AUI. For more information, see AUI Online Help.

Steps

1. In Avamar Administrator, click the **Policy** launcher link.
   The **Policy** window is displayed.
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 *Avamar Product Security Guide* provides details.
   d. Click **Next**.
6. In the **Membership** screen:
   a. Select checkboxes next to the virtual machines that 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.

7

Protecting the vCenter Management Infrastructure

Topics:

- vCenter deployments overview
- Best practices for backup and restore
- Protecting an embedded PSC
- Protecting external deployment models
- vCenter server restore workflow
- Platform Services Controller restore workfow
- Command reference
- Support for vCenter HA failover for inflight backups
- Additional considerations

vCenter deployments overview

This chapter describes how to protect the vCenter server Appliance (VCSA) and the Platform Services Controllers (PSCs). It is intended for virtual administrators who utilize the distributed model of the vCenter server and require protection of the complete vCenter server infrastructure.

You can protect vCenter 6.5 deployments with Avamar by using the proxy appliance. The instructions in this chapter assume that the vCenter server and the PSCs are deployed as virtual machines.

For the restores to complete successfully:

- Ensure that these virtual machines use a fully qualified domain name (FQDN) with correct DNS resolution, or
- Ensure that the host name of the machine is configured as an IP address. Note that if the host name is configured as an IP address, the IP address cannot be changed.

There are mainly two types of vCenter deployments:

- vCenter server Appliance/Windows Virtual Machine with an embedded PSC.
- vCenter server (also multiple) Appliance/Windows virtual machine with an external PSC. This type has two sub categories:
  - vCenter server environment with a single external PSC.
  - vCenter server environment with multiple PSC instances: This environment contains multiple vCenter server instances registered with different external PSC instances that replicate their data.

Best practices for backup and restore

Review the following recommendations and best practices when planning a vCenter virtual machine or its component virtual machine(s) backup.

ⓘ **NOTE:** Backups will not save Distributed switch configurations. The VMware Knowledge Base article at https://kb.vmware.com/s/article/2034602 provides steps to backup and restore the configuration of vSphere Distributed Switches.

- It is recommended to schedule the backup of the vCenter Server when the load on the vCenter server is low, such as during off-hours, to minimize the impact of vCenter virtual machine snapshot creation and snapshot commit processing overhead.
- Ensure that there are no underlying storage problems that might result in long stun times.
- Keep the vCenter virtual machine and all of its component virtual machines in one single isolated protection policy. The protection policy should not be shared with any other virtual machines. This is to ensure that the backup times of all vCenter Server component virtual machines are as close to each other as possible.

- If using one or more external PSCs, it is recommended to have one dedicated proxy associated to the policy group for the entire vCenter Server virtual machines backup. This will ensure that the backup times of all vCenter Server component virtual machines are as close to each other as possible.
- Ensure that the backup start time of the vCenter Server does not overlap with any operations for other protected virtual machines being managed by this vCenter so that there is no impact on other protected virtual machines during snapshot creation and snapshot commit of the vCenter virtual machine.
- If the vCenter Server and PSC instances fail at the same time, you must first restore the Platform Services Controller and then the vCenter Server instances.

Protecting an embedded PSC

The following section describes backup and recovery options for protecting an embedded PSC.

Backup

You can perform a backup of an embedded PSC by using the following guidelines.

1. Create a protection policy, and then add the vCenter virtual machine to the policy.
2. Select the full virtual machine and not individual disks.
3. Run the scheduled or on-demand (ad hoc) policy.

ⓘ **NOTE:** When selecting virtual machines and objects, ensure that you clear the **Enable CBT** option.

Recovery

Depending on the type of failure, you can perform the virtual machine recovery by using one of the following methods.

- Restore to original—This method is valid only when the vCenter Server Appliance (VCSA) is intact and running, but corrupted.
- Recover as a new virtual machine to an ESXi server—Use this method if you have lost your VCSA. This ESXi must be registered with the Avamar server.
- Instant access restores to an ESXi—Use this method if the backup is saved to a Data Domain system. Restores using this method completes more quickly than the other methods.

Once the restore is complete, perform storage migration of this virtual machine to the required datastore, and then unmount the NFS datastore from the ESXi.

For appliance restore, perform any of the above methods depending on the failure type, and then perform the following steps.

1. After the recovery operation, wait until the virtual machine starts up.
2. Log in to the vCenter Server appliance shell as **`root`**.
3. Verify that all PSC and vCenter Server services are running:

   For an appliance, run the `service-control --status -all` command in the appliance shell.

   For a vCenter Server installed on Windows, from the Windows Start menu, select **Control Panel** > **Administrative Tools** > **Services**.

Protecting external deployment models

Review the backup and recovery options for protecting external deployments.

Backup

You can perform a backup by using the following guidelines:

1. Create one policy/group and add the vCenter virtual machine and PSC virtual machine to the group. This will ensure that snapshots are taken at the same time.
2. Ensure that you select the full virtual machine and not individual disks.

3. Run the scheduled or on-demand (ad-hoc) policy.

ⓘ **NOTE:** Ensure that you back up all vCenter Server and PSC instances at the same time

Recovery

Depending on the failure, you can perform virtual machine recovery by using one of the following methods:

- Restore to original — This method is valid only when the VCSA is intact and running, but corrupted.
- Recover as a new virtual machine to an ESXi server — Use this method if you have completely lost your VCSA. Note that this ESXi must be registered with the Avamar server.
- Instant access restore to an ESXi — Use this method if you have completely lost your VCSA and the backup is saved to a Data Domain system. Restores using this method will complete more quickly than the other methods.

Once the restore is complete, perform storage migration of this virtual machine to the desired datastore, and then unmount the NFS datastore from the ESXi.

ⓘ **NOTE:** In the event of a complete environment failure, PSCs should be restored first, followed by the vCenter Server restore.

The following scenarios provide specific instructions based on the number of vCenter server appliances and external PSCs in the environment and the extent of the failure.

vCenter server appliance(s) with one external PSC where PSC fails

Steps

1. Perform an image-level recovery of the PSC by using one of the methods indicated above, and then power ON the virtual machine.
2. Verify that all PSC services are running.
   - For a PSC deployed as an appliance, run the **`service-control --status --all`** command in the appliance shell.
   - For a PSC installed on Windows, from the Windows Start menu, select **Control Panel** > **Administrative Tools** > **Services**.
3. Log into the vCenter server appliance shell as **`root`**.
4. Verify that no vCenter services are running, or stop any vCenter services that are running by typing **`service-control --stop`**.
5. Run the vc-restore script to restore the vCenter virtual machines.
   - For a vCenter server appliance, type **`vcenter-restore -u`** ***`psc_administrator_username`*** **`-p`** ***`psc_administrator_password`***
   - For a vCenter Server installed on Windows, navigate to `C:\Program Files\VMware\vCenter Server\`, and then run **`vcenter-restore -u`** ***`psc_administrator_username`*** **`-p`** ***`psc_administrator_password`***

   where *psc_administrator_username* is the vCenter Single Sign-On administrator user name, which must be in UPN format.
6. Verify that all vCenter services are running and the vCenter Server is started, as specified in step two.
7. Perform a log in test to the vCenter Server.
   If the restore was successful, the login completes successfully.

vCenter server appliance is lost but the PSC remains

Steps

1. Perform an image-level recovery of the lost vCenter server by using one of the following methods, and then power ON.
   - Restore to original — This method is valid only when the VCSA is intact and running, but corrupted.
   - Recover as a new virtual machine to a managed ESXi server — Use this method if you have completely lost your VCSA. Note that this vCenter must be registered with Avamar.
   - Emergency recovery to an ESXi server.
2. After a successful boot, verify that all services are started.
3. Perform a log in test.

vCenter server appliance with multiple PSCs where one PSC is lost, one remains

Steps

1. Repoint the vCenter instance (insert link) to one of the functional PSC in the same SSO domain.

   ⓘ **NOTE:** Log in to all vCenter servers one by one to determine which vCenter log in fails. This will be the vCenter that requires the repoint steps.

2. Run the following command on the vCenter server appliance:

   ```
   cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
   ```

   ⓘ **NOTE:** The square brackets enclose the command options.

3. Perform a log in test on the vCenter server.
4. Deploy the new PSC and join to an active node in the same SSO and site, replacing lost ones.
5. Repoint the vCenter server to the new PSC.

vCenter server appliance remains but all PSCs fail

About this task

ⓘ **NOTE:** In this scenario, none of the vCenter logins (SSO user) have been successful.

Steps

1. Restore the most recent PSC backup and wait for the vCenter services to start
2. Log in to the vCenter server appliance's shell as `root`.
3. Verify that no vCenter services are running, or stop vCenter services.
4. Run the `vc-restore` script to restore the VCSA (refer above for detailed steps).

   ⓘ **NOTE:** If the login test to any vCenter server appliance fails, then the restored PSC is not the PSC that the vCenter server appliance is pointing to, in which case you may be required to perform a repoint, as described above.

5. Deploy the new PSC and join to an active node in the same SSO domain and site.
6. Repoint vCenter connections as required

vCenter server appliance remains but multiple PSCs fail

Steps

1. Restore one PSC.
2. Test the vCenter server appliance login. If the login fails, repoint the vCenter server appliance to an active PSC.
3. Deploy the new PSC and join to an active node in the same SSO domain and site.

vCenter server appliance fails

About this task

ⓘ **NOTE:** If a total failure has occurred (all PSCs and all vCenter server appliances failed), restore one PSC first before restoring the vCenter server appliance.

Steps

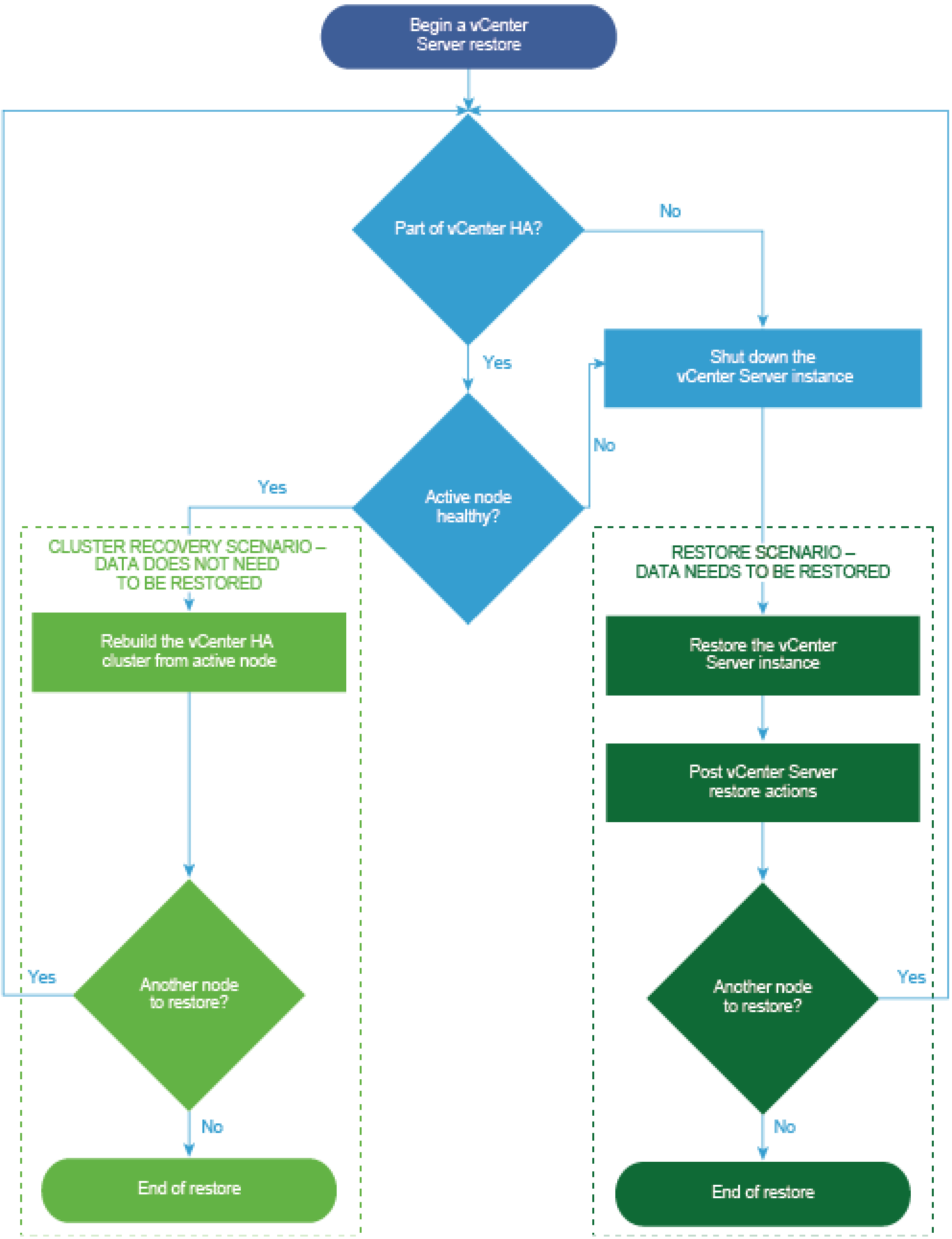
1. Perform an image-level restore of the lost vCenter server by using one of the following methods, and then power ON the vCenter.

- Restore to original — This method is valid only when the vCenter server appliance is intact and running, but corrupted.
- Recover as a new virtual machine to a managed ESXi server — Use this method if you have completely lost your vCenter server appliance. Note that this vCenter must be registered with Avamar.
- Emergency recovery to an ESXi server.

2. After a successful boot, verify that all vCenter services have started.
3. Perform a log in test.
4. If the log in test fails, then this vCenter server appliance is pointing to an inactive PSC. Repoint to an active node.

vCenter server restore workflow

The following diagram shows the restore workflow for a vCenter server.



Begin a vCenter Server restore
Part of vCenter HA?
No
Yes
Shut down the vCenter Server instance
No
Yes
Active node healthy?
CLUSTER RECOVERY SCENARIO – DATA DOES NOT NEED TO BE RESTORED
RESTORE SCENARIO – DATA NEEDS TO BE RESTORED
Rebuild the vCenter HA cluster from active node
Restore the vCenter Server instance
Post vCenter Server restore actions
Yes
Another node to restore?
Another node to restore?
Yes
No
No
End of restore
End of restore

Figure 8. vCenter server restore workflow

Platform Services Controller restore workfow

The following diagram shows the restore workflow for a Platform Services Controller (PSC).

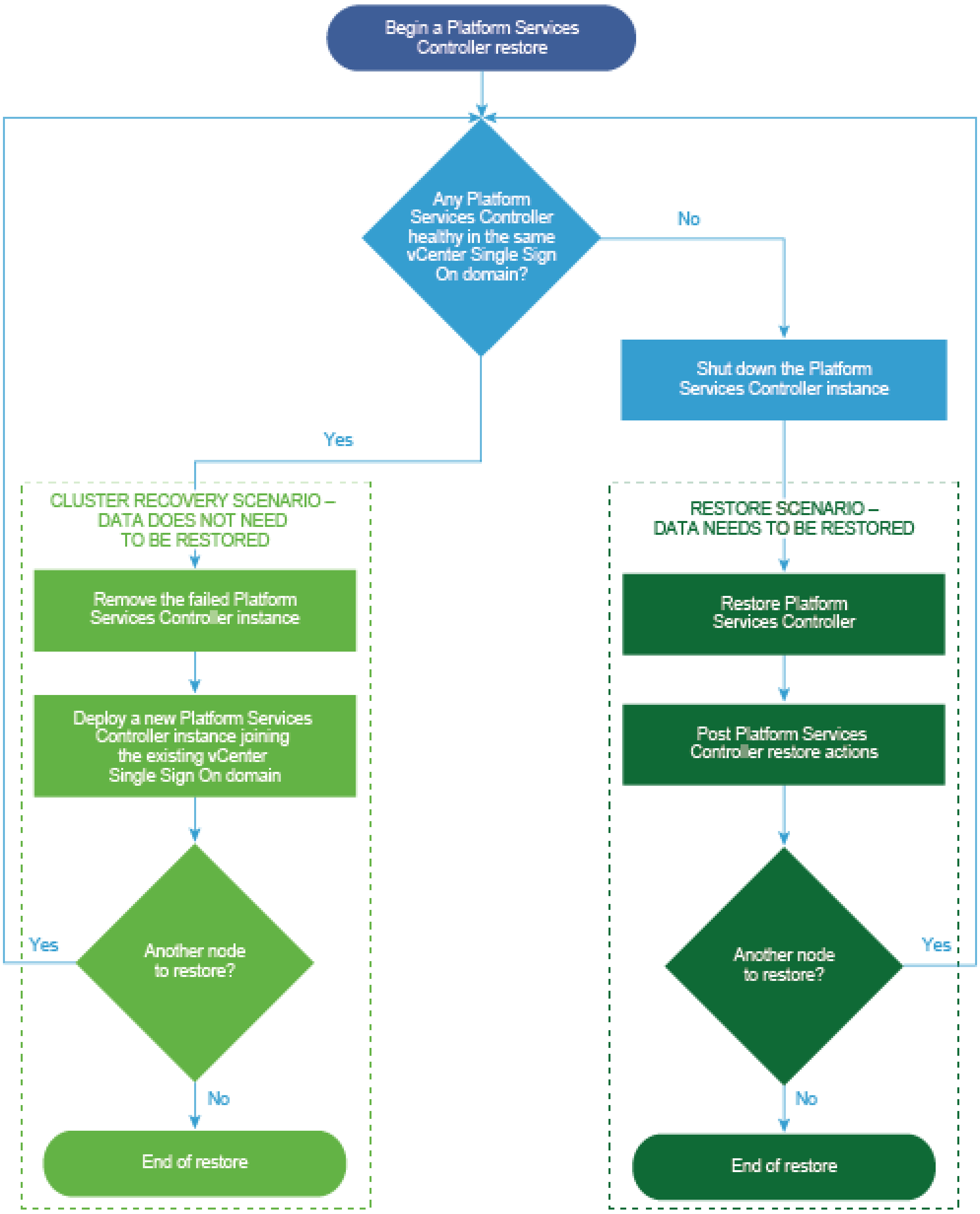

Begin a Platform Services Controller restore
Any Platform Services Controller healthy in the same vCenter Single Sign On domain?
No
Shut down the Platform Services Controller instance
Yes
CLUSTER RECOVERY SCENARIO – DATA DOES NOT NEED TO BE RESTORED
Remove the failed Platform Services Controller instance
Deploy a new Platform Services Controller instance joining the existing vCenter Single Sign On domain
Another node to restore?
Yes
No
End of restore
RESTORE SCENARIO – DATA NEEDS TO BE RESTORED
Restore Platform Services Controller
Post Platform Services Controller restore actions
Another node to restore?
Yes
No
End of restore

Figure 9. PSC restore workflow

Command reference

Use the following command to start or stop services in the vCenter server/PSC, or obtain the status:

```
service-control -status/start/stop -all
```

You can use other Replication topology commands, as in the following example.

Replication topology command

```
/usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h localhost -u PSC_Administrator -w
password
```

NOTE: You can replace **`localhost`** with another PSC FQDN to obtain all of the partnerships in the current vSphere domain.

Support for vCenter HA failover for inflight backups

During a vCenter failover period, the Avamar software monitors the failover process and performs the following actions.

1. Automatically detects vCenter failover events and then waits for the vCenter failover to complete.
2. Cancels the hanging backup jobs that were caused by vCenter HA failover.
3. Removes mounted HotAdded disks from the proxy appliance.
4. Restarts all incomplete backups during the vCenter HA failover.

Additional considerations

Review the following additional considerations when backing up and restoring the vCenter server and PSC.

- Backing up the vCenter server will not save the Distributed switch (vDS) configuration as it is stored on the hosts. As a best practice, back up the vDS configuration by using a script that can be used after restoring the virtual center.
- After restoring the PSC, verify that replication has been performed as designed by using the following commands to display the current replication status of a PSC and any of the replication partners of the PSC:
    - For VCSA, go to `/usr/lib/vmware-vmdir/bin` and type **`./vdcrepadmin -f showpartnerstatus -h localhost -u administrator -w Administrator_Password`**
    - For Windows, open a command prompt and type **`cd "%VMWARE_CIS_HOME%"\vmdird\`**
- For every backup or restore, VDDK reuses the vCenter session instead of creating a new session to increase the performance. This feature works with VDDK 7.0 and later.

The VMware vCenter server documentation, available at https://docs.vmware.com/en/VMware-vSphere/index.html, provides more information about the vCenter server and PSC.

8

Protecting ESX Hosts

Topics:

- Overview
- Adding ESX host authentication certificates to the MCS keystore
- Creating a dedicated ESXi host user account
- Adding an ESX host as a vCenter client
- Deploying a proxy in a stand-alone ESX host
- Disassociating an ESX host from a vCenter

Overview

Image backup can be configured to protect virtual machines residing in stand-alone 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

The following are the known limitations of protecting virtual machines that reside on a standalone ESX host in Avamar:

- Avamar supports ESX 5.5 or later only.
- If you use this feature to restore a virtualized vCenter from an ESX host, before you restore any virtual machines to ESX host, disassociate ESX host from the vCenter server.
- While protecting ESX hosts, the restored virtual machines might have an empty *vc.uuid* in VMX file. Configure this flag to add the restored virtual machines to Avamar.
- Avamar does not support adding ESXi host as a container client.
- File-level restore from an image-level backup is not supported to a stand-alone ESXi host.

Task List

In order to protect virtual machines residing in a stand-alone 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.

About this task

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`.

Steps

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 the following command:

   ```
   dpnctl stop mcs
   ```
3. Switch user to root by running the following command:

   ```
   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 the following command:

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

Creating a dedicated ESXi host user account

We strongly recommend that you set up a separate user account on each ESXi host that is strictly dedicated for use with Avamar.

About this task

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 ESXi host user account ensures maximum clarity if it becomes necessary to examine ESXi host logs.

ⓘ **NOTE:** The user account must be added to the top (root) level in each ESXi host you intend to protect.

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

ⓘ **NOTE:** When creating the user account, select **Propogate to children**, if the option is available.

Table 18. Minimum required ESXi host user account privileges

Privilege type	Required Privileges
Alarms	• Create alarm
Datastore	• Allocate space • Browse datastore • Low-level file operations • Remove file
Extension	• Register extension • Unregister extension • Update extension
Folder	• Create folder
Global	• Cancel task • Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Settings
Host > Configuration	• Connection • Storage partition configuration
Network	• Assign network • Configure
Resource	• Assign virtual machine to resource pool
Sessions	• Validate session
Tasks	• Create task • Update task
vApp	• Import
Virtual machine	
Configuration	• Add existing disk • Add new disk • Add or remove device • Advanced • Change CPU count • Change resource

Table 18. Minimum required ESXi host user account privileges (continued)

Privilege type	Required Privileges
	- 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 Program Execution - Guest Operation Queries
Interaction	- Console interaction - DeviceConnection - Guest operating system management by VIX API - Power off - Power on - Reset - VMware Tools install
Inventory	- Create new - Register - Remove - Unregister
Provisioning	- 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	None

Adding an ESX host as a vCenter client

Prerequisites

NOTE: It is recommended that you do not add the ESX as a container.

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window is displayed.
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 stand-alone ESX host

Prerequisites

1. Add DNS entries for each proxy that 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 system.

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

Steps

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, we strongly recommend 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

Steps

1. Launch the vSphere Client and log in to the ESX host.
2. Locate the proxy that 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 the admin user.
7. Switch to the root user by typing:

```
su -
```

8. Type `/opt/vmware/share/vami/vami_config_net`, and then press **Enter**.
   A **Main Menu** appears.
9. 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.
10. 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.
11. In the **Main Menu**, select **3**, and then press **Enter** to configure the hostname.
12. Type the proxy hostname, and then press **Enter**.
13. In the **Main Menu**, select **2**, and then press **Enter** to configure the default gateway.
14. Type the IPv4 default gateway, and then press **Enter**.
15. Press **Enter** to accept the default IPv6 default gateway.
16. In the **Main Menu**, press **Enter** to show the current configuration.
17. Ensure that the settings are correct.
18. 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.

Prerequisites

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

About this task

ⓘ **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.

Steps

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 Configure vCenter-to-Avamar authentication

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.

Steps

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.

Avamar Image Backup and Recovery for VMware Cloud on Amazon Web Services (AWS)

Topics:

- Avamar image backup and recovery for VMware Cloud on AWS
- Configure the VMware Cloud on AWS web portal console
- Amazon AWS web portal requirements
- vCenter server inventory requirements
- Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS
- Configure vCenter-to-Avamar authentication for VMware Cloud on AWS
- Avamar image backup and restore for VMware Cloud on AWS best practices
- Unsupported Avamar operations

Avamar image backup and recovery for VMware Cloud on AWS

Avamar provides image backup and restore support for VMware Cloud on Amazon Web Services (AWS).

Using Avamar to protect virtual machines that are running in VMware Cloud on AWS is similar to how you protect the virtual machines in an on-premises data center. This section provides information on network configuration requirements, Avamar best practices for VMware Cloud on AWS, and unsupported Avamar operations for VMware Cloud on AWS.

Configure the VMware Cloud on AWS web portal console

Domain Name System (DNS) resolution is critical for Avamar deployment and configuration of the Avamar server, Avamar proxy, and the Data Domain appliance. All infrastructure components should be resolvable through a Fully Qualified Domain Name (FQDN). Resolvable means that components are accessible through both forward (A) and reverse (PTR) lookups.

In the VMware Cloud on AWS web portal console, ensure that the following requirements are met:

- By default, there is no external access to the vCenter Server system in the Software Defined Data Center (SDDC). You can open access to the vCenter Server system by configuring a firewall rule. To enable communication to the vCenter public IP address from the SDDC logical network, set the firewall rule in the compute gateway of VMware Cloud on AWS. If the firewall rule is not configured in the SDDC, the Avamar server does not allow you to add the vCenter Server.
- The default compute gateway firewall rules prevent all virtual machine traffic from reaching the internet. To allow the Avamar Server virtual machine to connect to the internet, create a compute gateway firewall rule. This action allows outbound traffic on the logical network that the Avamar Server virtual machine is connected to.
- Configure DNS to allow machines in the SDDC to resolve Fully Qualified Domain Names (FQDNs) to IP addresses belonging to the internet. If the DNS server is not configured in the SDDC, the Avamar server does not allow you to add the vCenter Server by using the server's public FQDN or IP address.
- It is recommended that you deploy the Data Domain system as a virtual appliance in the Amazon Virtual Private Cloud (VPC). During the SDDC creation, connect the SDDC to an AWS account, and then select a VPC and subnet within that account.
- The Data Domain system running in the Amazon VPC must be connected to the VMware SDDC through the VMware Cloud Elastic Network Interfaces (ENIs). This action allows the SDDC, the services in the AWS VPC, and subnet in the AWS account to communicate without having to route traffic through the internet gateway. For more information about configuring ENIs, see https://vmc.vmware.com/console/aws-link.

- If DDVE is running in the Amazon VPC, configure the inbound and outbound firewall rules of the compute gateway for Data Domain connectivity.
- If using NSX-T, configure the DNS to resolve to the internal IP address of the vCenter server. Navigate to **SDDC Management** > **Settings** > **vCenter FQDN** and select the **Private vCenter IP address** so that you can directly access the management network over the built-in firewall. Additionally, ensure that you open TCP port 443 of the vCenter server in both the management gateway and the compute gateway.

  Also, using NSX-T for file-level restore operations requires you to update the `axionfs.cmd` file on the proxy appliances with the IPv4 address of the Avamar server. After you register and activate the Avamar proxy appliances in the Avamar server, log into each of the Avamar proxy appliances as **`root`**, and then open the `/usr/local/avamar/var/axionfs.cmd` file in a UNIX text editor. Within the file, locate the **`--server`** entry key and update the corresponding value to the IPv4 address of the Avamar server. For example, **`--server=192.168.2.150`**.

Amazon AWS web portal requirements

In the Amazon AWS web portal, ensure that the following requirements are met:

- if Data Domain is running in your Amazon VPC, configure the inbound and outbound firewall rules of your Amazon VPC security group to provide connectivity between the VMware SDDC compute gateway and Data Domain connectivity.
- If you are replicating from one Data Domain system to another, configure the inbound rule for the security group in AWS to allow all traffic from the respective private IPs of the Data Domain Virtual Editions running in your Amazon VPC.
- If you have more than one Data Domain running in AWS to perform replication, both Data Domain systems must have the ability to ping each other using the FQDNs.

vCenter server inventory requirements

In the vCenter server inventory of your SDDC, ensure that the following requirements are met:

- An internal DNS name lookup server must be running inside the vCenter inventory. This is referenced by all the workloads running in the VMware SDDC.
- The internal DNS server must have **Forwarders** enabled to access the Internet. This action is required to resolve the vCenter Server's public FQDN.

  Forwarders are DNS servers that the server can use to resolve DNS queries for records that the server cannot resolve.

Deploy the vProxy OVA on a vCenter server in VMware Cloud on AWS

Perform the following steps to deploy the OVA for the Avamar proxy appliance from a vCenter server by using the HTML5 vSphere Web Client.

Prerequisites

Review the section Configure the VMware Cloud on AWS web portal console

Steps

1. Log in to the HTML5 vSphere Web Client with the cloudadmin account credentials.
2. Click **Menu** > **Hosts and Clusters**.
3. In the inventory pane, expand the vCenter, and then expand the **compute resource pool** inside the SDDC cluster.
4. Right-click the resource pool where you want to deploy the OVA, and then select **Deploy OVF template**.
5. In the **Select an OVF template** window, type a URL path to the OVA package, or click **Choose Files** and navigate to the OVA package location, and then click **Next**.
6. On the **Select a name and folder** window:
   a. Specify a name for the virtual appliance.

    b. Specify the inventory location.
    c. Click **Next**.
7. In the **Select a compute resource** window, select the vApp or resource pool where you want to deploy the OVA, and then click **Next**.
8. In the **Review details** window, review the product details, such as the product name, version, vendor, publisher, and download size, and then click **Next**.
9. In the **Select storage** window, select the disk format and the destination datastore where the virtual appliance files will be stored, and then click **Next**.

   To ensure that the amount of storage space that is allocated to the virtual appliance is available, select **Thick Provision Lazy Zeroed**.
10. In the **Select networks** window, select the **Destination Network**:
    a. Specify the IP address
    b. Click **Next**.
11. In the **Customize Template** window, expand **Networking properties**:
    a. In the **Network IP address** field, type the IP address for the Avamar proxy.
    b. In the **Network Netmask/Prefix** field, specify the netmask for an IPv4 Network IP address.
    c. In the **DNS** field, type the IP address of the DNS servers, separated by commas.
    d. In the **NTP** field, type the IP address of the gateway host.
    e. In the **Default gateway** field, type the IP address of the gateway host.
12. Click **Next**.
    The **Ready to Complete** window appears.
13. In the **Ready to Complete** window, review the deployment configuration details, and then click **Finish**.

Results

The **Deploying template** task appears in the vCenter and provides status information about the deployment.

Configure vCenter-to-Avamar authentication for VMware Cloud on AWS

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

About this task

To import the authentication certificates for VMware Cloud on AWS, perform the following steps:

Steps

1. Download any root certificate from entrust website.

   Go to https://www.entrustdatacard.com/pages/root-certificates-download.
2. Place the root certificate in the Avamar server and follow the instructions in the section Add vCenter authentication certificates to the MCS keystore.
3. Add the vCenter to the Avamar server.

Avamar image backup and restore for VMware Cloud on AWS best practices

Consider the following best practices when using Avamar to protect virtual machines running in VMware Cloud on AWS.

- When deploying or configuring the Avamar server or proxy, ensure that you specify the DNS server IP address that points to the internal DNS server running in the vCenter inventory.
- Ensure that both forward and reverse lookup entries in the internal DNS server are in place for all the required components, such as the Avamar Server, Avamar proxy appliance, and Data Domain Virtual Edition (DDVE).

- If using NSX-T, configure the DNS to resolve to the internal IP address of the vCenter server. Navigate to **SDDC Management** > **Settings** > **vCenter FQDN** and select the **Private vCenter IP address** so that you can directly access the management network over the integrated firewall. Also, ensure that you open TCP port 443 of the vCenter server in both the management gateway and the compute gateway.

  Also, using NSX-T for file-level restore operations requires you to update the `axionfs.cmd` file on the proxy appliances with the IPv4 address of the Avamar server. After you register and activate the Avamar proxy appliances in the Avamar server, log into each of the Avamar proxy appliances as **`root`**, and then open the `/usr/local/avamar/var/axionfs.cmd` file in a UNIX text editor. Within the file, locate the **`--server`** entry key and update the corresponding value to the IPv4 address of the Avamar server. For example, **`--server=192.168.2.150`**.
- Add the vCenter server to the Avamar server by using one of the following options:
  - Public FQDN of the vCenter server
  - Public IP address of the vCenter server.

  It is recommended that you use the FQDN.
- When adding the vCenter server to the Avamar server, specify the login credentials for the cloud admin user.
- When accessing the AUI by using vCenter authentication, add the following parameter in the `/usr/local/avamar/var/mc/server_data/prefs/application-production.properties` file, and then restart the mcs service:

  ```
  vmc.vcenters=VMware Cloud vCenter FQDN
  ```

Unsupported Avamar operations

Avamar image backup and restore in VMware Cloud on AWS does not currently support the following operations:

- Application consistent backup
- Proxy deployment manager. Proxies must be deployed manually.
- File-level restore from an image-level backup if using NSX-V. Note that this operation is supported if using NSX-T.
- Instant access recovery of an image-level backup.
- Emergency restore (image-level restore directly to an ESXi host, bypassing the vCenter).
- Image-level backups and restores using NBD or NBDSSL transport mode.
- Advanced policy based data protection for MS-SQL using Avamar.
- Application aware image backups for MS-SQL and MS-Exchange
- Image backup and restore when the datacenter is under a folder.
- Exclusion of pagefile or user defined files from Windows image backup.
- Proxy appliance that is configured with dual-stack or IPv6-only.
- NBD, NBDSSL, and SAN. Only HotAdd is supported.
- Restore to new vApp.
- IPV6
- Virtual machine template backup
- vCenter plugin is not supported in VMC

10

Backing up VMware Cloud Foundation (VCF) Components on VxRail

This chapter describes how to protect VCF components on VxRail by using CLI backup scripts.

VxRail is the recommended Dell platform for VCF. However, Dell supports the environments that use other VMware-supported vSAN Ready Nodes also.

Topics:

- VCF and VxRail overview
- VCF components and backup methods
- Backup prerequisites
- The backup script
- Quick protection
- Selective protection: SDDC and NSX-T Managers
- Selective protection: vCenter servers
- Selective protection: VCF Image-based components
- Other Operations
- Backup-script troubleshooting

VCF and VxRail overview

VCF integrates a VMware cloud infrastructure with cloud management services by using the vRealize software suite to run enterprise applications. The VCF infrastructure is managed by the SDDC Manager, and it includes vSphere compute, vSAN storage, NSX networking, and a range of security implementations.

Dell VxRail is an all-in-one solution that uses Dell PowerEdge servers and its own VxRail hyperconverged infrastructure (HCI) software to provide a fully functional VCF environment to enterprise customers.

For more information about VCF and VxRail, see the following resources:

- The VMware Cloud Foundation documentation
- The *Dell VxRail Administration Guide* at Dell Online Support
- About VMware Cloud Foundation on Dell VxRail

VCF components and backup methods

Understanding the backup method used by a VCF component aids in understanding how the VCF component is protected by the backup script. The following table shows the VCF components of the different backup methods.

Table 19. VCF component of file-based backups

Backup Method	Component
File based	NSX-T Data Center
	SDDC Manager
	vCenter Server

- Assets of these components are first copied to an external server that uses secure file transfer protocol (SFTP) or another supported protocol. After that, the external server is backed up by Avamar.

Table 20. VCF components of image-based backups

Backup Method	Component	Automatically discovered
Image based	vRealize Suite LifeCycle Manager (vRSLCM)	VCF 4.0
	vRealize Automation	VCF 4.1
	vRealize Business	No
	vRealize Log Insight	VCF 4.1
	vRealize Network Insight	No
	vRealize Operations Manager	VCF 4.1
	VxRail Manager	No
	Workspace ONE Access	VCF 4.1

- Assets of these components that use an image-based backup method are backed up directly by Avamar.
- The **Automatically discovered** column displays the minimum required version of VCF for a component to be automatically discovered, and those components that are not automatically discovered by any version of VCF.
- If using quick protection, the automatically discovered components are automatically protected.

Backup prerequisites

Ensure that you meet the following backup prerequisites:

- You have installed the correct versions of Avamar, hotfixes, and VCF by reviewing the compatibility information at E-Lab Navigator.
- You have discovered any external server that uses SFTP or another supported protocol, and is used in a file-based backup, as a client on the Avamar server.
- You have added the vCenter Server that protects the VxRail and VCF virtual machines to the Avamar server.
- Policies with appropriate datasets are present on the Avamar server. Policies enable you to protect the VxRail and VCF components.
  - At least one policy with datasets that support file system protection is present.
  - At least one policy with datasets that support VMware virtual machine protection is present.
  - A policy with datasets that supports file system protection, and is created for external (SFTP) server backups must have the **Select Files and/or Folders** option that is selected under the **Source Data** section of **Dataset**.

    The option enables you to select required folder or files instead of an entire file system.
- You have set Avamar and the vCenter, SDDC, and NSX-T managers to the same time zone, and synchronized their clocks.
- Avamar and VCF must not contain the backup schedules that back up the same assets simultaneously.
- You have configured policies to ensure that they meet the quiescing and backup job requirements that VMware outlines. VMware Quiescing Recommendations provides information.
- You use only UNIX and Windows file system external backup servers as Avamar clients.
- Proxies are present.
- A backup folder path that an external server uses for a file-based backup is present.
- The user credentials that the backup script uses must resolve to the accounts with the required permissions to access the relevant resources.
- Ensure that the required ports are open in the firewall configuration.

  For example, if you use an SFTP server, the port 22 on the SFTP server must be open to communicate with the vCenter Servers, SDDC Manager, and NSX-T Managers.

The backup script

You use a Avamar script to protect VxRail/VCF components.

The script is accessible from the Avamar command line. It provides a series of guided procedures that automate multiple operations into a single process.

NOTE:

- This script only backs up the data of protected VCF components. It cannot be used to restore any of the data that is backed up.
- To restore the data, use the Avamar and VMware user-interface tools. Ensure that you restore VCF-management data to components in a manner supported by VMware.
- For more information, go to the VMware Validated Design Documentation website and review the backup and restore procedures of the documentation that corresponds to your version of VCF.

Quick protection

This procedure uses default backup settings and values to protect all VCF components at once. If a VCF component is automatically discovered, it is automatically protected. Quick protection requires the least amount of input, but also provides the least amount of choice. For information about the default settings and values used, review the selective-protection procedures that follow.

Steps

1. From a Avamar command line, type the following two commands:

   ```
   cd /usr/local/avamar/bin
   ```

   ```
   ./avamar-vcf-component-protection.sh
   ```

2. Enter the credentials for Avamar server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **1**.

   NOTE: Quick protection uses the same external SFTP server and backup schedule for both the SDDC Manager and vCenter Servers. It also overrides the existing backup configurations of the SDDC and vCenter Servers without prompting.

5. Enter the address of an external SFTP server, including the backup directory path, followed by credentials to access the server. The external SFTP server is also used for vCenter Server configuration.

   The external SFTP server and backup directory path uses the format **sftp://*server_ip_address*:*port_number*/folder/subfolder**. For example:

   ```
   sftp://172.17.62.201:22/upload/backup
   ```

6. Enter the encryption passphrase for the SDDC Manager and vCenter Server backups.

   In quick protection, the encryption passphrase is the same for the SDDC Manager and vCenter Server backups. The encryption passphrase must be 12 - 20 characters in length, and contain at least two lowercase letters, two uppercase letters, two numbers, and a special character.

   NOTE: Store the passphrase in a secure location that is different from the backup files and the VCF environment that you are protecting.

7. Confirm whether you must use common credentials for all vCenter Servers.
   - Enter **y** to provide common credentials for all vCenter Servers.
   - Enter **n** to be prompted for the credentials for each individual server.

   NOTE: In quick protection, all the vCenter Servers are selected for protection. You cannot select individual vCenter Servers.

8. Select the days of the week a backup takes place, and then enter the time of day.

   Type a number that represents a day of the week, where **1** represents Sunday. If selecting multiple days of the week, separate the numbers with a space. For example, to select Sunday and Monday:

   ```
   1 2
   ```

The time of day uses **HH:MM** in the 24-hour format. For example, for 1:25 PM, enter **13:25**.

9. Select the File System and Virtual Machine protection policies to use. If a single protection policy of one type exists, it will be automatically used.
10. Enter the IP address or fully qualified domain name (FQDN) of any image-based VCF component that is not automatically discovered and that you want to protect. For a list of components that are not automatically discovered, see VCF components of image-based backups.

Results

You can monitor the progress of the backup script.

Selective protection: SDDC and NSX-T Managers

This procedure protects just the SDDC and NSX-T manager file-based VCF components, while providing more control over the backup settings used for them than quick protection. To protect other VCF components, refer to the other selective-protection procedures.

Steps

1. From a Avamar command line, type the following two commands:

   ```
   cd /usr/local/avamar/bin
   ```

   ```
   ./avamar-vcf-component-protection.sh
   ```

2. Enter credentials for Avamar server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **2**, and then **1**.
5. To override an existing SDDC Manager backup configuration, enter **y**.
6. To add or modify SDDC Manager backup configuration information, enter the address of an external SFTP server, including the backup directory path, followed by credentials to access the server.

   The external SFTP server and backup directory path uses the format **sftp://*server_ip_address*:*port_number*/folder/subfolder**. For example:

   ```
   sftp://172.17.62.201:22/upload/backup
   ```

7. Enter the encryption passphrase for SDDC Manager backups.

   The encryption passphrase must be between 12 and 32 characters in length and contain at least two lowercase letters, two uppercase letters, two numbers, and a special character.

   ⓘ **NOTE:** The encryption passphrase is required when restoring data. Store this passphrase in a secure location that is separate from the backup files and VCF environment you are protecting.

8. The default SSH fingerprint of the external SFTP server is displayed. Confirm that it should be used, or enter a new one.

   ⓘ **NOTE:** With quick protection, the default SSH fingerprint of the external SFTP server is always used.

9. Select the backup frequency. If you select `HOURLY`, enter the minute of each hour a backup takes place. If you select `WEEKLY`, select the days of the week a backup takes place, and then enter the time of day.

   For a weekly backup frequency, type a number that represents a day of the week, where **1** represents Sunday. If selecting multiple days of the week, separate the numbers with a space. For example, to select Sunday and Monday:

   ```
   1 2
   ```

   The time of day uses the format **HH:MM** in 24-hour notation. For example, to enter 1:25 p.m.:

   ```
   13:25
   ```

10. Enter the backup-retention values described in the following table. The values automatically used by quick protection are also listed.

ⓘ **NOTE:** Backup-retention values are applicable for VCF 4.1 or later.

Table 21. Backup-retention values

Parameter	Value range	Quick-protection default value
Days of daily backups to retain	0–30	7
Days of hourly backups to retain	0–14	7
Backup files to retain	1–600	15
Take backups on state change	Yes or no	Yes

11. Protect the external SFTP server by selecting the File System policy.

Results

You can monitor the progress of the backup script as it protects the selected VCF components.

Selective protection: vCenter servers

This procedure protects just the vCenter server file-based VCF components, while providing more control over the backup settings used for them than quick protection. To protect other VCF components, refer to the other selective-protection procedures.

Steps

1. From a Avamar command line, type the following two commands:

   ```
   cd /usr/local/avamar/bin
   ```

   ```
   ./avamar-vcf-component-protection.sh
   ```

2. Enter credentials for Avamar server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **2** twice.
5. Select the automatically discovered vCenter servers to protect.

   Enter **a** to protect all the servers. Otherwise, enter the numbers that correspond to the individual servers to protect, separating each number with a space.

6. Enter the address of an external server, including the backup directory path, followed by credentials to access the server.

   Supported protocols for the external server are FTP, SFTP, FTPS, HTTP, HTTPS, NFS, and SMB. The external server and backup directory path uses the format ***protocol*://*server_ip_address*:*port_number*/folder/subfolder**. For example:

   ```
   sftp://172.17.62.201:22/upload/backup
   ```

7. Select the days of the week a backup takes place, and then enter the time of day.

   Type a number that represents a day of the week, where **1** represents Sunday. If selecting multiple days of the week, separate the numbers with a space. For example, to select Sunday and Monday:

   ```
   1 2
   ```

   The time of day uses the format **HH:MM** in 24-hour notation. For example, to enter 1:25 p.m.:

   ```
   13:25
   ```

8. Confirm if the backups should be encrypted. If they should be encrypted, enter an encryption password.

   If you enter an encryption password, it must be between 8 and 20 characters in length and contain at least one lowercase letter, one uppercase letter, one number, and one special character.
9. Confirm if historical data should be backed up and the number of backups to retain.

ⓘ **NOTE:** In quick protection, the default is to back up historical data and retain all backups.

10. Confirm if common credentials should be used for all the vCenter servers:
    - Enter **y** to provide common credentials for all vCenter servers.
    - Enter **n** to be prompted for the credentials for each individual server.
11. If there is an existing vCenter server backup configuration, confirm if it should be overridden.

    ⓘ **NOTE:** Should the existing backup configuration fail to be overridden, the vCenter server will be left without a backup configuration.

12. Protect the external server by selecting the File System policy.

Results

You can monitor the progress of the backup script as it protects the selected VCF components.

Selective protection: VCF Image-based components

This procedure protects all of the image-based VCF components, while providing more control over the backup settings used for them than quick protection. The components protected include vRSLCM, VxRail Manager, Workspace ONE Access, and vRealize Suite virtual machines. To protect file-based VCF components, refer to the other selective-protection procedures.

Steps

1. From a Avamar command line, type the following two commands:

   ```
   cd /usr/local/avamar/bin
   ```

   ```
   ./avamar-vcf-component-protection.sh
   ```

2. Enter credentials for Avamar server.
3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **2**, and then **3**.
5. Select an image-based VCF component type to protect.

   ⓘ **NOTE:** You can only select a single component type. To protect more than one component, follow the selective protection steps for each component.

   - If you select vRSLCM, select a discovered vRSLCM server to protect.
   - If you select any other component type, enter the IP address or fully qualified domain name (FQDN) of the server to protect.
6. Protect the image-based VCF component by selecting a Virtual Machine protection policy.

Results

You can monitor the progress of the backup script as it protects the selected VCF component.

Other Operations

The following procedure describes the steps involved in external (SFTP) server password update:

Steps

1. From a Avamar command line, type the following two commands:

   ```
   cd /usr/local/avamar/bin
   ```

   ```
   ./avamar-vcf-component-protection.sh
   ```

2. Enter credentials for Avamar server.

3. Enter the IP address or fully qualified domain name (FQDN) of the SDDC Manager server, and then enter credentials for the SDDC Manager server.
4. From the backup-script main menu, enter **3**.
5. **Update SFTP server password in SDDC/NSX-T Manager backup configuration:**

   To update external SFTP server password in SDDC/NSX-T Manager backup configuration, select **1**.

   a. Next provide the SFTP server password for a given username.
   b. Then confirm the SFTP server fingerprint discovered by the script or enter one manually.

   The script issues a password update request to SDDC Manager and monitor the results.
6. **Update external server password in vCenter Servers backup configuration:**

   To update external server password in vCenter servers backup configuration, select 2.

   a. Confirm if common credentials should be used for all the vCenter servers:
      - Enter **y** to provide common credentials for all vCenter servers.
      - Enter **n** to be prompted for the credentials for each individual server.
   b. Confirm if the backups should be encrypted. If they should be encrypted, enter an encryption password.

      If you enter an encryption password, it must be between 8 and 20 characters in length and contain at least one lowercase letter, one uppercase letter, one number, and one special character.
   c. Next provide the external server password for a given username.

      ⓘ **NOTE:** This step needs to be repeated if separate external servers are used for vCenter servers.

Results

The script issues a password update request and monitor the results.

Backup-script troubleshooting

The following table provides common error codes and messages, along with explanations or recommended areas of investigation to resolve the problem.

Table 22. Error codes and explanations

Error code or message	Explanation or area of investigation

`INVALID_ENCRYPTION_PASSPHRASE`
`Provided encryption passphrase <passphrase> is invalid.`
	The encryption passphrase that is specified for external SFTP server is invalid.

`Validate Backup Location Details FAILED`	The backup location that is specified for the external SFTP server in the SDDC Manager backup configuration does not exist.

`INPUT_PARAM_ERROR`
`Failed to establish SFTP connection to <SFTP server> with username <username> on port <port>.`
	The credentials that are specified for the external SFTP server in the SDDC Manager backup configuration are incorrect.

`INVALID_ARGUMENT`
`The entered backup password does not adhere to the password requirements.`
	The encryption passphrase that is specified in the vCenter server backup configuration is invalid.

Table 22. Error codes and explanations (continued)

Error code or message	Explanation or area of investigation
INVALID_ARGUMENT Plugin error occurred. Access to the backup server is denied. Check your credentials.	The password that is specified for the external server in the vCenter server backup configuration is incorrect.
UNAUTHENTICATED Authentication required. com.vmware.vapi.endpoint.method.authentication.required	The credentials that are specified for the vCenter server are incorrect.
Perform validations for backup server fingerprint FAILED	The SSH fingerprint that is specified for the external SFTP server in the SDDC Manager backup configuration is invalid.
SCHEDULING_SDDC_MANAGER_BACKUPS_FAILED_REASON_UNKNOWN Unexpected error occurred. Provided backup schedule not applied.	Check for errors on the SDCC Manager.
LOCK_NOT_AVAILABLE Lock is not available - SDDC Manager DEPLOYMENT lock to perform Backup & Restore operation.	There are too many pending SDDC Manager jobs. Try running the backup script at another time.

A

Manually deploying proxies

Topics:

- Overview
- Downloading the proxy appliance template file
- Deploying the proxy appliance in vCenter
- Deploying a proxy appliance in vCenter using the vSphere Web Client
- Registering and activating the proxy with the Avamar server
- Configuring proxy settings in Avamar Administrator
- Performing optional proxy performance optimization

Overview

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.

About this task

ⓘ **NOTE:** If adding more than one proxy, you only must perform this task once.

Steps

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 **Avamar Web Restore** page appears.
2. Click **Downloads**.
3. Go to the `VMware vSphere\EMC Avamar VMware Image Backup\FLR Appliance` folder.
4. Click the **AvamarCombinedProxy-linux-sles12sp5_64-*version* .ova** link.
5. Save **AvamarCombinedProxy-linux-sles12sp5_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 system (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.

Prerequisites

1. Add DNS entries for each proxy that 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

Steps

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

   `https://vCenter-server/ui`

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

   The **vSphere Web Client** page appears.
2. For vCenter versions 5.5 and earlier, download and install the vSphere Client Integration Plug-in:

   NOTE:

   These substeps 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.

   These substeps are not required for later versions of vCenter.

   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:

   `https://vCenter-server/ui`

   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, we strongly recommend 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.

Prerequisites

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

About this task

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.

Steps

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 Configure vCenter-to-Avamar authentication

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.

Prerequisites

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

Steps

1. In Avamar Administrator, click the **Administration** launcher link.
   The **Administration** window is displayed.
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.

B

vSphere Data Ports

Topics:

- Required data ports

Required data ports

These are the required data ports in a vSphere environment.

Table 23. 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	Proxies	ESXi hosts	vSphere API	N/A
443	Proxies	vCenter	vSphere API	N/A
443	Avamar MCS	vCenter	vSphere API	N/A
443	Avamar Deployment Manager	ESXi hosts	vSphere API	Used to deploy the proxy.
902	Proxies	ESXi hosts	Network File Copy (NFC)	N/A
5480	Avamar Deployment Manager	Proxies	CIM service	Used to register the proxy.
5488	Avamar Deployment Manager	Proxies	CIM service	Used to register the proxy.
5489	Avamar Deployment Manager	Proxies	CIM service	Used to register the proxy.
7444	Avamar MCS	vCenter	Test vCenter credentials	N/A
8543	Proxies	Avamar server	Snapshot manager	Used for VMware snapshot operations.
27000	Proxies	Avamar server	GSAN communication	Nonsecured communication.
28009	Avamar MCS	Proxies	Access proxy logs	N/A
29000	Proxies	Avamar server	GSAN communication	Secured communication.
30001	Proxies	Avamar MCS	`avagent` to MCS communication	N/A
30009	Avamar MCS	Proxies	`avagent` paging port	Secure communication with VMware proxy.

NOTE: All ports are TCP unless otherwise noted.

C

Using VMware vRealize Log Insight

Topics:

- About VMware vRealize Log Insight
- Configuring the Log Central Reporting Service
- Configuring Log Forwarding Agents

About VMware vRealize Log Insight

You can configure image proxies to forward logs to VMware vRealize Log Insight for centralized log management. This step allows a mechanism for identifying patterns and frequency of error types, and to prevent lost log entries due to log rotation.

Avamar support for Log Insight requires that the vRealize Log Insight appliance is deployed on a vCenter. This feature uses Log Forwarding Agents (LFAs) installed on proxies or other clients to push log content to a Log Central Reporting Service (LCRS). LCRS is installed on a utility node or Avamar Virtual Edition server. The LCRS forwards the logs to the vRealize Log Insight server running on the vCenter.

> **NOTE:**
>
> Each time an Avamar server is upgraded, perform the following steps on the upgraded Avamar server:
>
> 1. Configuring the Log Central Reporting Service
> 2. Configuring Log Forwarding Agents

This appendix describes configuration of the LCRS running on the Avamar server and the LFAs running on proxies and other clients.

Configuring the Log Central Reporting Service

The Log Central Reporting Service (LCRS) runs on the utility node or the Avamar Virtual Server (AVE). Use this procedure to configure the LCRS to forward logging information from proxies to the vRealize Log Insight appliance.

Steps

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, then switch user to root by typing **`su -`**.
   - For a multi-node server, log in to the utility node as admin, then switch user to root by typing **`su -`**.
2. Change to the `/usr/local/emc-lcrs/etc/` directory.
3. Open the `lcrs.ini` in a text editor.
4. Edit this file as follows:

   ```
   server.port=8080
   forward.server=Log_Insight_Server_IP
   forward.port=Log_Insight_Server_port
   forward.messagePerSend=10
   forward.type=LogInsight
   upload.forward=true
   forward.delete=true
   forward.dispatch=true
   ```

   where *Log_Insight_Server_IP* is the IP address of the vRealize Log Insight appliance, and *Log_Insight_Server_port* is the port used by the vRealize Log Insight appliance.
5. Save and close the file.

Configuring Log Forwarding Agents

Follow this procedure to configure Log Forwarding Agents (LFAs).

Steps

1. Log in as admin to the proxy that will be configured to forward log messages to the Log Central Reporting Service (LCRS).
2. Switch user to root by running the following command:

   `su -`

3. Type the following command:

   `/usr/local/avamarclient/etc/proxylfa_setup.sh`

   The following appears:

   ```
   Avamar VMware Log Forwarding Agent Setup
   Main Menu
   ---------
   1) Setup LCRS IP address
   2) Enable Avamar VMware Log Forwarding Agent cron job
   3) Disable Avamar VMware Log Forwarding Agent cron job
   4) quit
   Your choice:
   ```

4. Enter **1** at the prompt to enter the IP address of the Avamar utility node or AVE running the Log Central Reporting Service (LCRS).
5. Enter **2** at the prompt to enable the LFA cron job.

   The cron job forwards the logs from the proxy to the LCRS every 10 minutes.

6. Enter **4** at the prompt to exit the program.

D

Plug-in Options

Topics:

- How to set plug-in options
- VMware Image plug-in backup options
- VMware Image plug-in restore options
- Windows VMware GLR plug-in options

How to set plug-in options

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

Specify plug-in options in the AUI for on-demand backup or restore wizards, or when a dataset for a scheduled backup is created. Set plug-in options with the graphical user interface (GUI) controls (text boxes, check boxes, radio buttons, and so forth). Type an option and its value in the **Key** and **Value** fields.

> **NOTE:** The Avamar software does not check or validate the information that is typed in the **Show Free Form** section of the **More Options** pane. The values in the **Key** and **Value** fields override settings that are specified with the GUI controls for the options.

VMware Image plug-in backup options

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

Table 24. 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.
Set Annotation Tag LastBackupStatus and LastSuccessfulBackup	If selected, enables the Avamar server to report information to the vSphere Web Client or the legacy Windows-based vSphere client about the most recent backup and most recent successful backup. When selected, the following information is displayed in the Annotation list of the vSphere Web Client: ● **LastSuccessfulBackupStatus**: The date and time of the most recent successful backup. ● **LastBackupStatus**: The date and time of the most recent backup, whether successful or not.
Exclude page file blocks when performing image backup on Windows VM	If selected, excludes the Windows page file (`pagefile.sys`) from the backup for all the partitions. It is not limited to primary partitions. **NOTE:** Page file exclusion is supported only for Windows Servers version 2008 R2 and above. For client versions of Windows, this option has no effect; the page file is present in backups of Windows clients, regardless of this setting.

Table 24. Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
	ⓘ **NOTE:** The proxy uses NBD transport mode internally in order to read the page file blocks. After recognizing the required blocks, the available mode (hotadd/nbdssl/nbd) will be used accordingly for backup or restore operations.
Exclude deleted file blocks when performing image backup on Windows VM	If selected, excludes the deleted file blocks from the backup for all the partitions. It is not limited to primary partitions.
Exclude files with path and filter	Excludes the files with path and filter from the backup for all the partitions. It is not limited to primary partitions. Type the full path of the file or folder or the filter path of the files and folders. Separate multiple entries with a comma. To exclude files with path and filter, type the path in the following format: ● Start with the driver letter ● End with "/" to exclude a folder ● End without "/" to exclude a file ● Use "*" as a wildcard in the filename to exclude all files. Do not use "*" as a wildcard in the file path. For example: ○ `*:/*/*.TXT` is not supported. ○ `D:/folder/*.txt` is supported. ○ `D:/folder/*` is supported.
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 *Avamar and Data Domain System Integration Guide* provides instructions.
Encryption method to Data Domain system	Specifies the encryption method for data transfer between the client and the Data Domain system during the backup. As of Avamar release 7.5, the only supported encryption method is "high."
Snapshot delete retry	
Max times to retry snapshot delete	The maximum number of times that a snapshot delete operations should be attempted.
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 must 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.
Snapshot quiesce timeout	
Snapshot quiesce timeout (minutes)	Maximum number of minutes to wait before the snapshot quiesce operation is considered to have failed (Windows VMware Image plug-in only)

Table 24. Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
Microsoft SQL Server authentication	
NT Authentication	Uses the credentials that are entered in Guest Credentials for authentication. User must have administrative privileges and must have write permissions for the file system and read permissions for the Windows registry.
Application Authentication	Uses the SQL Server Username and SQL Server Password to log in to the SQL server.
Microsoft SQL Server post action	
Post Action Timeout (minutes)	The maximum number of minutes to wait before post action operations are considered to have failed. The default is 900 seconds.
Post Action Type of MSSQL	The type of post action operation to perform. The only available option is LOG Truncation, which performs log truncation after the backup has been performed. When backing up a single VM, all disks of the VM must be selected or log truncation does not occur.
Quota limit per backup	
Soft limit size (MBs)	Indicates the soft limit size of a backup. If the size of the backup source exceeds the soft limit, the backup succeeds with a warning. If you provide both the soft and hard limit size, ensure that the soft limit size is smaller than the hard limit size.
Hard limit size (MBs)	Indicates the hard limit size of a backup. If the size of the backup source exceeds the hard limit, the backup fails.

VMware Image plug-in restore options

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

Table 25. 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. As of Avamar release 7.5, the only supported encryption method is "high."

Windows VMware GLR plug-in options

The Windows VMware GLR plug-in option is deprecated. It is recommended to use the File Level Restore (FLR) plug-in through AUI.

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

ⓘ **NOTE:** GLR does not support Windows dynamic disks.

E

Troubleshooting

Topics:

- Installation and configuration problems and solutions
- Backup problems and solutions
- Restore problems and solutions

Installation and configuration problems and solutions

Common installation and configuration problems and solutions are described below.

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 this step does not resolve the problem, turn 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 that are managed by vCenter, once a proxy registers with the Avamar server, it is difficult to change network settings. Otherwise, this step 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 that is used to connect to vCenter might not have sufficient privileges.

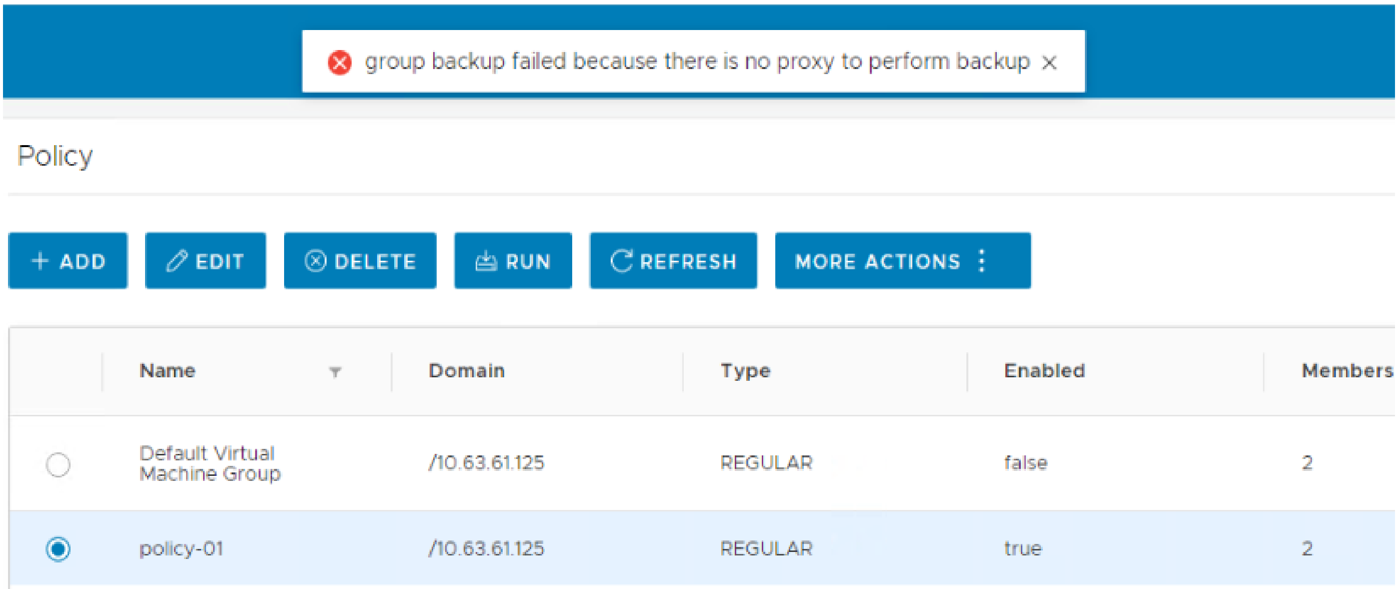
To verify account privileges, log in to the vSphere Client or vSphere Web Client with that username and password. Ensure that you can access datastores on that client. If you cannot, that account does not have the required privileges.

Exclude the proxy from the virtual machine backup if performing the backup with other VMware software

Including the Avamar proxy in a backup consumes a large amount of space. When using other VMware software instead of the Avamar software to perform the virtual machine backup, it is recommended that you exclude the proxy virtual machine from the backup.

Backups fail with No Proxy errors

One or several VM image backups fail with `No Proxy` errors. Following are the error messages that are seen when backup is triggered:



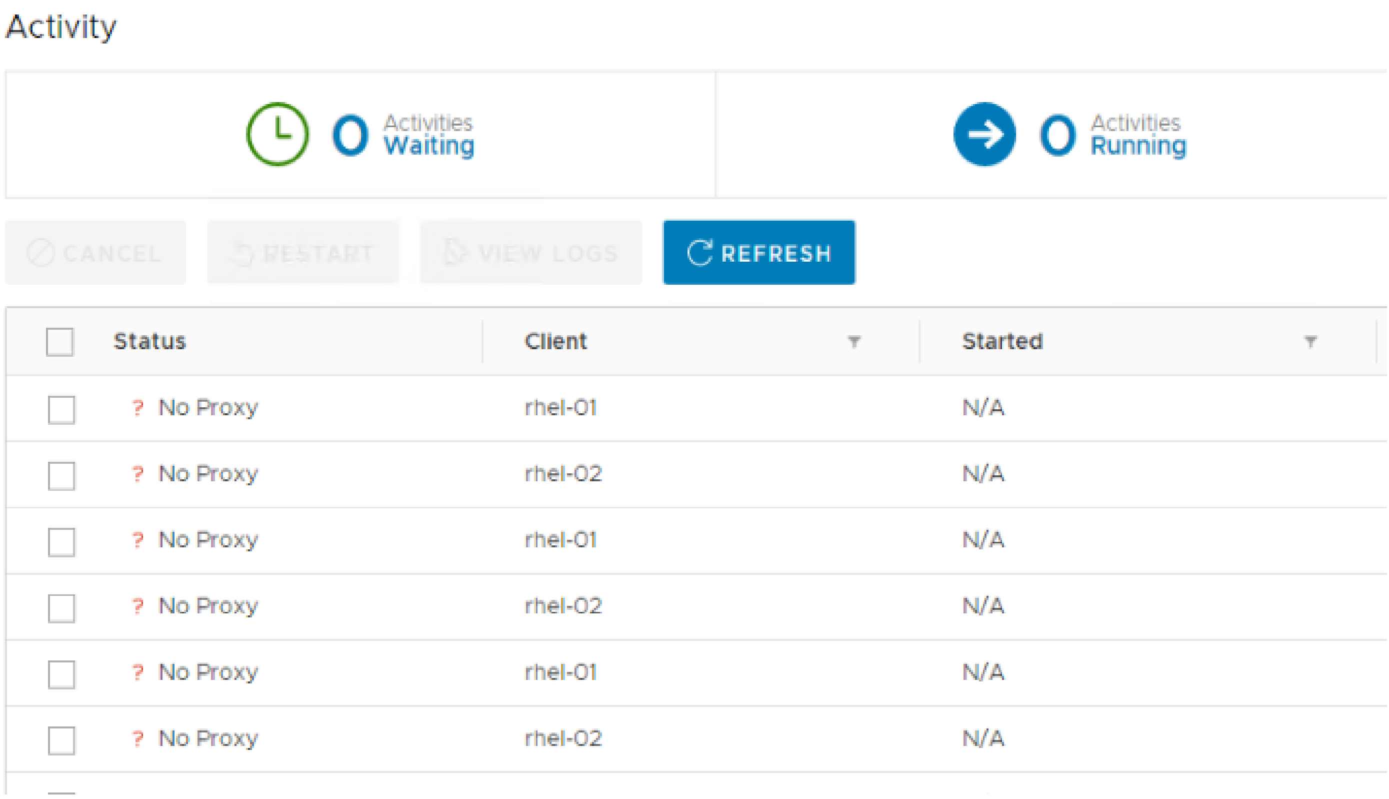
group backup failed because there is no proxy to perform backup

Policy

	Name	Domain	Type	Enabled	Members
○	Default Virtual Machine Group	/10.63.61.125	REGULAR	false	2
●	policy-01	/10.63.61.125	REGULAR	true	2

Figure 10. No proxy error

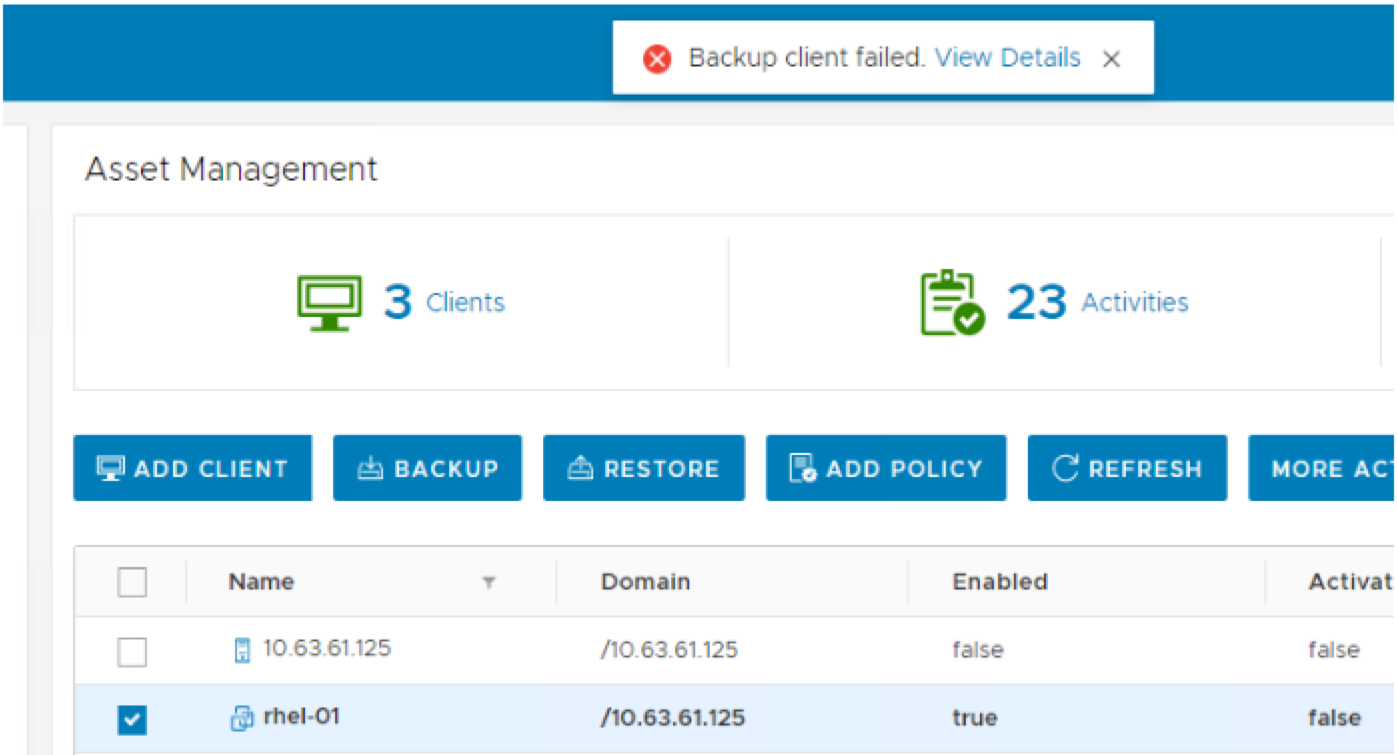
Following is the `No Proxy` error Activity Monitor shows:



□	Status	Client	Started
□	? No Proxy	rhel-01	N/A
□	? No Proxy	rhel-02	N/A
□	? No Proxy	rhel-01	N/A
□	? No Proxy	rhel-02	N/A
□	? No Proxy	rhel-01	N/A
□	? No Proxy	rhel-02	N/A

Figure 11. No proxy error on activity monitor

On-demand VMware Image backup fails with the following appear:

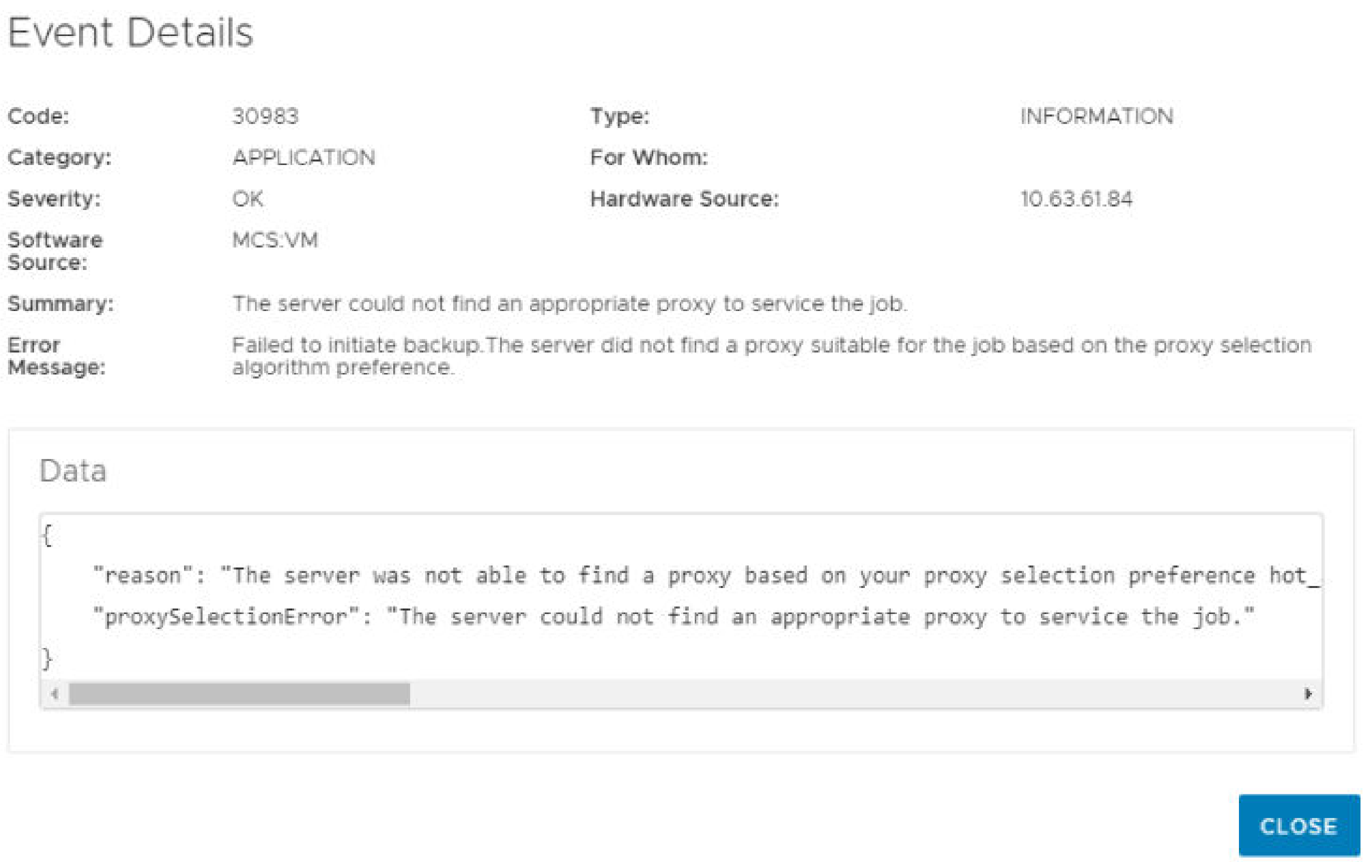


Backup client failed. View Details

□	Name	Domain	Enabled	Activat
□	10.63.61.125	/10.63.61.125	false	false
☑	rhel-01	/10.63.61.125	true	false

Figure 12. On-demand VMware Image backup fails

When you click **View Details**, you get the following details:



Event Details

Code:	30983	Type:	INFORMATION
Category:	APPLICATION	For Whom:	
Severity:	OK	Hardware Source:	10.63.61.84
Software Source:	MCS:VM		
Summary:	The server could not find an appropriate proxy to service the job.		
Error Message:	Failed to initiate backup.The server did not find a proxy suitable for the job based on the proxy selection algorithm preference.		

Data

```
{
    "reason": "The server was not able to find a proxy based on your proxy selection preference hot_
    "proxySelectionError": "The server could not find an appropriate proxy to service the job."
}
```

Figure 13. Event details of failed backup

The earlier mentioned issue occurs due to the following three reasons:

Cause 1

There are no Avamar Image Proxy servers that are configured to protect the datastore where the client `vmdk` files are stored. (This cause usually affects 1 or several VM backup clients.)

The steps to fix this error are:

1. Open Avamar Administrator in AUI.
2. Go to **Asset Management** and click the **clients** tab.
3. Find the failing VM with `No Proxy` and edit it.
4. Go to the **VMware** tab and look at the datastore that the VM is hosted on.
5. Go to the **Administration** window.
6. Edit the proxies and check on the datastore that hosts the VM.
7. Click **Ok** to save the change.

Cause 2

Interruption to the vCenter connection (This cause usually affects all VM clients).

The steps to fix this error are:

1. Verify that Avamar can connect to the vCenter.
2. Go to the **Administration** window and click on the **vCenter root domain.**
3. Click the **vCenter client** connection object and edit the client.
4. Verify the Avamar server IP or Hostname is valid.
5. Verify the vCenter user account that Avamar uses is valid.
6. Click **Ok** to verify Avamar connect to vCenter.

NOTE: If the connection to vCenter was interrupted due to vCenter maintenance or network outage, restart the MCS service on the Avamar server. It clears any vCenter connection caching issues.

Cause 3

The VM itself has no Hard Disks (This cause usually affects 1 or a couple of VMs).

The steps to fix this error are:

1. Open **vCenter**.
2. Find the VM that is failing with `No Proxy`.
3. Edit the VM settings and verify if there are any Hard Disks.

NOTE: If there are no Hard Disks, check with the VM Administrator and contact VMware support. If a backup of the VM is no longer required, retire the VM object in Avamar.

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: restart, power on, resume after suspend, or migrate.

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: restart, power on, resume after suspend, or migrate.

Proxies are not assigned to backup jobs

Any time that you restart the MCS, it might take some time until all proxies reconnect to the MCS and are available for backups. If you stop the MCS and do not restart it within 5 minutes, proxies go into a sleep mode for at least 40 minutes.

To verify that a proxy can 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, override the value 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 in to each proxy, modify the file `/usr/local/avamarclient/avvcbimageAll.cmd` to include the line:

```
-- snapshot_max_change_percent=0
```

This disables this feature.

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

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.

If the Proxy is residing on a host without vFlash resource configured, you may see an error in VC `The available virtual flash resource '0' MB ('0' bytes) is not sufficient for the requested operation` during hot-add attempt and backup falls back to NBD mode and succeeds. This is expected, but if hot-add is strongly desired move the proxy to any host with vflash resource configured.

Exchange log truncation unsupported when VMDK is encrypted via vSphere

When VMDK is encrypted via vSphere, WMware Tools does not use the VSS for application consistent quiescing. The encrypted image backup is file-level consistent instead.

Because the Exchange server log truncation process includes the VSS writer, the VSS writer is not involved in the snapshot quiesce, and log truncation is not triggered.

NOTE: SQL server log truncation does not rely on the VSS writer. SQL log truncation is supported.

Indexing VMware image backups requires HotAdd transport mode

Indexing VMware image backups using the Data Protection Search software can only be completed with HotAdd transport mode.

Proxy status alert

You can configure properties on the proxies that are registered on the Avamar server.

The following properties must be configured in `/etc/vcs/dm.properties`:

Table 26. Proxy details

Property	Description	Possible values	Requires restart if mcserver
enable_status_check_schedule	Indicates if the status checking schedule must be enabled.	true, false	Yes
status_check_schedule_interval	Indicates the frequency at which the status of the proxy must be checked.	30 **NOTE:** The default value is 30 minutes.	Yes
monitor_proxy_mc_event_list	Indicates the status of the monitor proxy mc event list from AUI.	update, retire, and delete.	No
monitor_proxy_vc_event_list	Indicates the status of the monitor proxy in vCenter event.	VmPoweredOffEvent,VmPoweredOnEvent,VmRemovedEvent	No
proxy_status_alert_list	Indicates the status of the proxy alert.	WARNING, ERROR, and UNKNOWN	No

Configure email notification for proxy status alert

Perform the following steps to configure email notifications for proxy status alerts:

Steps

1. Update the `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` file with the following:

```
<node name="mail">
    <map>
        <entry key="smtpHost" value="mailhubwc.lss.emc.com" />  <Your smtp server>
        <entry key="email_send_debug" value="false" />
        <entry key="email_send_timeout_minutes" value="60" />
        <entry key="admin_mail_sender_address" value="test@avamar.com" />
    </map>
</node>
```

2. Restart MCS.
3. In the AUI navigation pane on the left, click ≫, and then click **Settings**.
   The **Setting** window is displayed.
4. Click the **Profile** tab.
5. Select *High Priority Events*, and click **COPY**.
   The **Copy Profile** dialog box appears.
6. Provide a name for the new copied profile, and select the applicable domain.
7. Click **OK**.
8. Select the newly copied profile, and click **EDIT**.
   The **New Profile** dialog box appears.
9. Update the following:
   - Select the **Send data as events occur** option in the **Properties** section.
   - Clear all event codes, and only select the `25014` event code.
   - Add **Recipient Email Address** in the **Email** section.
10. Click **FINISH** to save the updated to the profile.

Restore problems and solutions

Avamar for VMware contains the following common restore problems and solutions.

Preexisting snapshots cause restores to fail

Virtual machine restores fails if a snapshot for that virtual machine exists. In this scenario, 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, clean up existing user created snapshots before restoring to original.

NOTE: Logs may suggest to skip the snapshot check, but do not use `--skip_snapshot_check` flag to override the pre-existing snapshot check.

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.

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

NOTE: As the physical RDM disks were not processed during the backup, data residing on the physical RDM disks cannot be restored at all.

If it is required for you 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 on a disk that does not have a partition table, FLR browsing of the backup fails with the following 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 combination 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.

Maximum number of NFS mounts with instant access issue

When using the instant access feature, if the following error message is displayed, the maximum number of NFS mounts as configured in vSphere may be insufficient.

```
vmir Error <0000>: Mount NFS datastore failed to start with error: Failed to create Data
Domain
```

A related message may be displayed in vSphere as well:

```
vmir Error <0000>: NFS has reached the maximum number of supported volumes.
```

The solution to this problem is to increase the number of NFS mountpoint configured on vSphere. The VMware knowledge base article https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2239 contains information and procedures to increase the number of mount points.

FLR on RHEL 5 requires the standard C++ library

When using HTTPS for enhanced FLR performance on RHEL 5.x, ACLs will be incorrect after restore unless the standard C++ library is installed.

FLR of a folder or file name that contains certain special characters fails

Avamar for VMware does not support a backslash (\), a double quote ("), or an ampersand (&) in folder and file names for an FLR.

FLR to user profile fails when Admin Approval Mode is enabled

When the Microsoft Windows Admin Approval Mode (AAM) is enabled (FilterAdministratorToken=1), the administrator user cannot use FLR to restore a file or folder to an end user's profile.

A restore attempt results in the following error:

```
Unable to browse Destination
The directory cannot be browsed. Please check the directory of the VM
```

To overcome this issue, the administrator user should open the end user's folder from within `C:\Users\`. The following Windows UAC message appears:

```
You don't currently have permission to access this folder.
```

To permanently give the administrator user access to the folder, click **Continue**.

A VM-based FLR fails in the virtual machine interface

When you use the virtual machine interface to perform a VM-based FLR, the operation fails because of the following reasons:

- The virus scanner restrictions on the VM, on which you perform the FLR blocks all the .exe files.
- The security software on the VM blocks file transfers of the .exe files.

Workaround: Disable the firewall.

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.

backup policy
In the AUI, a backup policy specifies a dataset, schedule, and retention settings that are applied to a client or a group of clients. A backup policy must contain at least one Avamar client. If the backup policy contains two or more clients, the clients must belong to the same Avamar domain. You can override backup policy settings at the client level.

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
In Avamar Administration, a group policy is defined as a *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.