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.
Figures.............................................................................................................. 8

Tables.................................................................................................................. 9

Preface.................................................................................................................. 10

Chapter 1: Introduction.......................................................................................... 14
  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...................................................................... 20
  Best practices....................................................................................................... 20
  (Optional) Configuring support for multiple vCenters......................................... 21
  Installing Avamar Administrator software............................................................ 21
  Configuring vCenter-to-Avamar authentication.................................................... 22
    Adding vCenter authentication certificates to the MCS keystore....................... 22
    Disabling MCS certificate authentication......................................................... 23
  Creating a dedicated vCenter user account........................................................... 23
  Register or add a VMware vCenter client............................................................. 25
  Auto-discovery of virtual machines..................................................................... 27
    Domain mapping rules for VM auto-discovery.................................................. 27
    Creating a rule.................................................................................................... 28
  Deploying proxies............................................................................................... 28
    Proxy Deployment Manager............................................................................. 28
    Deploy proxies.................................................................................................. 30
  Upgrading proxies............................................................................................... 31
    Upgrading Avamar proxies............................................................................... 31
    Upgrading Avamar proxies from supported releases before 7.5.1.................. 32
  Maintaining proxies............................................................................................ 34
    Reregistering a proxy with an Avamar server.................................................. 34
    Changing the proxy guest operating system admin password......................... 35
    Changing the proxy guest operating system root password........................... 35
  Additional Avamar server configuration.............................................................. 35
    Configuring automatic proxy selection............................................................ 35
    Configuring the MCS to support both guest and image backup...................... 36

Chapter 3: Administration...................................................................................... 37
  Clients and containers......................................................................................... 37
Chapter 4: Backup .......................................................... 45
  Limitations ............................................................................. 45
  Perform an on-demand backup of a virtual machine by using AUI ................................................................. 46
  Set advanced plug-in options in the AUI .................................................. 47
  Scheduling backups using the AUI Policy wizard ............................................. 48
    Creating a dataset ...................................................................... 49
    Creating a backup policy .......................................................... 49
    Enabling a scheduled backup for a backup policy ............................... 49
    Automatically including virtual machines in a backup policy ............... 50
  Log truncation backups .................................................................. 51
    Scheduled backups with Microsoft SQL log truncation ....................... 51
    Scheduled backups with Microsoft Exchange log truncation ............... 52
  Monitoring backups ..................................................................... 53
  Cancel backups ........................................................................ 53
  Support for vCenter HA failover for inflight backups ......................... 54
  Configure a backup to support VMware encryption .............................. 54
    VMware encryption support limitations ....................................... 54
  Configure a backup to support vSAN encryption .................................. 55
  Enforcement of backups to Data Domain .......................................... 56

Chapter 5: Restore .............................................................. 57
  Image and file-level restore guidelines ............................................. 57
  Monitor restores ........................................................................ 57
  Cancel restores .......................................................................... 58
  Instant access ............................................................................ 58
  Restore an instance of a VM backup by using the AUI ......................... 60
  Image backup overview .............................................................. 64
  Image-level restore limitations ..................................................... 64
  Restoring the full image or selected drives to the original virtual machine ................................................................................. 65
  Restoring the full image or selected drives to a different virtual machine ......................................................................................... 66
<table>
<thead>
<tr>
<th>Figures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Image backup diagram.................................................................14</td>
</tr>
<tr>
<td>2. Default proxy virtual machine specifications.................................15</td>
</tr>
<tr>
<td>3. Example independent and container protection.................................38</td>
</tr>
<tr>
<td>4. Virtual machine and proxy relationships within groups......................43</td>
</tr>
<tr>
<td>5. Example nested container structure..................................................46</td>
</tr>
<tr>
<td>6. Example nested container structure..................................................65</td>
</tr>
</tbody>
</table>
1. Revision history................................................................................................................................................................ 10
2. Typographical conventions............................................................................................................................................. 11
3. Guest backup installation resources....................................................................................................................... 16
4. Minimum required vCenter user account privileges................................................................................................. 23
5. Example chart for gathering proxy information...................................................................................................... 32
6. Example chart for gathering proxy information, continued.......................................................................................... 32
7. Virtual machine properties........................................................................................................................................ 33
8. Required permissions for the Avamar Administrator.................................................................................................. 55
9. Image restore toolbar buttons........................................................................................................................................ 64
10. FLR support partitioning scheme............................................................................................................................ 70
11. File system support for FLR..................................................................................................................................... 70
12. LVM support for FLR................................................................................................................................................. 70
13. Multi-device support for FLR.................................................................................................................................. 71
14. Important vCenter management infrastructure components..................................................................................... 79
15. Minimum required ESX host user account privileges.............................................................................................. 84
16. Required vSphere data ports...................................................................................................................................... 97
17. Backup options for Avamar VMware Image plug-in................................................................................................. 100
18. Restore options for Avamar VMware Image plug-in................................................................................................. 102
As part of an effort to improve the product lines, revisions of the software and hardware are periodically released. 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 the 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 Online Support (https://www.dell.com/support).

### Purpose

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

### Audience

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

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

A comprehensive discussion of basic Avamar system administration concepts and principles, such as clients, datasets, schedules, retention policies, 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>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05</td>
<td>June, 2020</td>
<td>Updated &quot;Performance improvements for file-level restore&quot; section.</td>
</tr>
<tr>
<td>04</td>
<td>April, 2020</td>
<td>Added the &quot;Perform a file-level restore (FLR) operation by using the Data Protection Backup and Recovery File-Level Restore UI&quot; sub-section to the &quot;File-level restore (FLR)&quot; section.</td>
</tr>
<tr>
<td>03</td>
<td>November 15, 2019</td>
<td>Added a port to &quot;Required data ports.&quot;</td>
</tr>
<tr>
<td>02</td>
<td>January 25, 2018</td>
<td>Updates to proxy upgrade procedures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updates to &quot;Unsupported Avamar operations&quot; for Avamar image backup and restore in VMware Cloud on AWS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added prerequisite related to NSX-T in the section &quot;Configure the VMware Cloud on AWS web portal console.&quot;</td>
</tr>
<tr>
<td>01</td>
<td>December 14, 2018</td>
<td>GA release of Avamar 18.2.</td>
</tr>
</tbody>
</table>

### Related documentation

The following Dell EMC publications provide additional information:
Typographical conventions

These type style conventions are used in this document.

Table 2. Typographical conventions

<table>
<thead>
<tr>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>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)</td>
</tr>
<tr>
<td>Italic</td>
<td>Used for full titles of publications that are referenced in text</td>
</tr>
<tr>
<td>Monospace</td>
<td>Used for:</td>
</tr>
<tr>
<td></td>
<td>- System code</td>
</tr>
<tr>
<td></td>
<td>- System output, such as an error message or script</td>
</tr>
<tr>
<td></td>
<td>- Pathnames, filenames, prompts, and syntax</td>
</tr>
<tr>
<td></td>
<td>- Commands and options</td>
</tr>
<tr>
<td>Monospace italic</td>
<td>Used for variables</td>
</tr>
<tr>
<td>Monospace bold</td>
<td>Used for user input</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose optional values</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{ }</td>
<td>Braces enclose content that the user must specify, such as x or y or z</td>
</tr>
<tr>
<td>...</td>
<td>Ellipses indicate nonessential information that is omitted from the example</td>
</tr>
</tbody>
</table>

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:

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:
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 https://www.dell.com/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 ConnectEMC and Email Home on all Avamar systems:

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

Comments and suggestions

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

Please include the following information:

- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Other details to help address documentation issues
Introduction

Topics:

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

Data protection overview

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

- Image backup
- Guest backup

NOTE: The Avamar AUI is only supported in stand-alone environments.

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. Additionally, you should not activate proxies into the root domain (/). Otherwise, this action causes problems during system migration.

Although it is possible to restore across datacenters (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.]

**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 just as if it were a physical machine, then registering and activating that client with an Avamar server. No special configuration is required.

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

The following table lists Avamar client guides, which provide detailed instructions for installing Avamar client software in virtual machines.

Table 3. Guest backup installation resources

<table>
<thead>
<tr>
<th>Client</th>
<th>Publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM AIX file systems</td>
<td>Avamar Backup Clients User Guide</td>
</tr>
</tbody>
</table>
| Linux file systems:  
  - Debian  
  - CentOS  
  - Red Hat  
  - SUSE  
  - Ubuntu | Avamar Backup Clients User Guide |
| Novell NetWare file systems | Avamar Backup Clients User Guide |
| UNIX file systems:  
  - FreeBSD  
  - HP-UX  
  - SCO Open Server and UnixWare  
  - 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 |
| Microsoft SQL Server databases | Avamar for SQL Server User Guide |
| Microsoft Windows file systems | Avamar Backup Clients User Guide |
Table 3. Guest backup installation resources (continued)

<table>
<thead>
<tr>
<th>Client</th>
<th>Publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle databases hosted on IBM AIX, Red Hat, and SUSE Linux, Sun Solaris, and Microsoft Windows</td>
<td>Avamar for Oracle User Guide</td>
</tr>
</tbody>
</table>

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.

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 restore (image 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
- Data exclusion
- Proxy appliance configured with dual-stack or IPv6-only.
- NBD, NBDSSL, and SAN. Only HotAdd is supported.
- VMware tag based rule selection criteria for dynamic policy
- Restore to new vApp
- IPV6
- Virtual machine template backup
Topics:

- Best practices
- (Optional) Configuring support for multiple vCenters
- Installing Avamar Administrator software
- Configuring vCenter-to-Avamar authentication
- Creating a dedicated vCenter user account
- Register or add a VMware vCenter client
- Auto-discovery of virtual machines
- Deploying proxies
- Upgrading proxies
- Maintaining 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

Starting in Avamar 18.1, 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`
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:
        ```xml
        <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`:
         ```xml
         <entry key="maxJavaHeap" value="-Xmx2G" />
         ```
         By default, the `maxJavaHeap` parameter is 2G. Use the following command to change the parameter:
         ```shell
         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:
   ```shell
   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.

Configuration and Setup
Configuring 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.

Adding 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.

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 under the Trust Certificate tab.

   The Import Certificate dialog box appears.

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. On the Validation window, specify the IP address of the vCenter, the Port number as 443, and then click the VALIDATE button.

   The Validation Result pop-up window is displayed where you can view if the validation is successful or failed. If the validation is failed, verify the inputs again.

5. Click the FINISH button.

   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:** 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`
4. Find the `ignore_vc_cert` entry key.
5. Change the `ignore_vc_cert` setting to `true`.
   `<entry key="ignore_vc_cert" value="true" /></entry>`
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

<table>
<thead>
<tr>
<th>Privilege type</th>
<th>Required privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>- Create alarm&lt;br&gt;- Edit alarm</td>
</tr>
<tr>
<td>Datastore</td>
<td>- Allocate space&lt;br&gt;- Browse datastore&lt;br&gt;- Configure datastore&lt;br&gt;- Low level filesystem operations&lt;br&gt;- Move datastore&lt;br&gt;- Remove datastore&lt;br&gt;- Delete File&lt;br&gt;- Rename datastore</td>
</tr>
<tr>
<td>Extension</td>
<td>- Register extension&lt;br&gt;- Unregister extension&lt;br&gt;- Update extension</td>
</tr>
<tr>
<td>Folder</td>
<td>- Create folder</td>
</tr>
<tr>
<td>Global</td>
<td>- Cancel task</td>
</tr>
<tr>
<td>Privilege type</td>
<td>Required privileges</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>Disable methods</td>
</tr>
<tr>
<td></td>
<td>Enable methods</td>
</tr>
<tr>
<td></td>
<td>Licenses</td>
</tr>
<tr>
<td></td>
<td>Log event</td>
</tr>
<tr>
<td></td>
<td>Manage custom attributes</td>
</tr>
<tr>
<td></td>
<td>Set custom attribute</td>
</tr>
<tr>
<td></td>
<td>Settings</td>
</tr>
<tr>
<td>Host</td>
<td>Configuration &gt; Storage partition configuration</td>
</tr>
<tr>
<td>Network</td>
<td>Assign network</td>
</tr>
<tr>
<td></td>
<td>Configure</td>
</tr>
<tr>
<td>Resource</td>
<td>Assign virtual machine to resource pool</td>
</tr>
<tr>
<td>Sessions</td>
<td>Validate session</td>
</tr>
<tr>
<td>Tasks</td>
<td>Create task</td>
</tr>
<tr>
<td></td>
<td>Update task</td>
</tr>
<tr>
<td>Virtual Machine-Configuration</td>
<td>Add existing disk</td>
</tr>
<tr>
<td></td>
<td>Add new disk</td>
</tr>
<tr>
<td></td>
<td>Add or remove device</td>
</tr>
<tr>
<td></td>
<td>Advanced</td>
</tr>
<tr>
<td></td>
<td>Change CPU count</td>
</tr>
<tr>
<td></td>
<td>Change resource</td>
</tr>
<tr>
<td></td>
<td>Configure managed by</td>
</tr>
<tr>
<td></td>
<td>Disk change tracking</td>
</tr>
<tr>
<td></td>
<td>Disk Lease</td>
</tr>
<tr>
<td></td>
<td>Extend virtual disk</td>
</tr>
<tr>
<td></td>
<td>Host USB device</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td>Modify device settings</td>
</tr>
<tr>
<td></td>
<td>Raw device</td>
</tr>
<tr>
<td></td>
<td>Reload from path</td>
</tr>
<tr>
<td></td>
<td>Remove disk</td>
</tr>
<tr>
<td></td>
<td>Rename</td>
</tr>
<tr>
<td></td>
<td>Reset guest information</td>
</tr>
<tr>
<td></td>
<td>Set annotation</td>
</tr>
<tr>
<td></td>
<td>Settings</td>
</tr>
<tr>
<td></td>
<td>Swapfile placement</td>
</tr>
<tr>
<td></td>
<td>Upgrade virtual machine Compatibility</td>
</tr>
<tr>
<td>Virtual Machine-Guest Operations</td>
<td>Guest Operation Modifications</td>
</tr>
<tr>
<td></td>
<td>Guest Operation Program Execution</td>
</tr>
<tr>
<td></td>
<td>Guest Operation Queries</td>
</tr>
<tr>
<td>Virtual Machine-Interaction</td>
<td>Console interaction</td>
</tr>
<tr>
<td></td>
<td>DeviceConnection</td>
</tr>
<tr>
<td></td>
<td>Guest operating system management by VIX API</td>
</tr>
<tr>
<td></td>
<td>Power off</td>
</tr>
<tr>
<td></td>
<td>Power on</td>
</tr>
<tr>
<td></td>
<td>Reset</td>
</tr>
<tr>
<td></td>
<td>VMware Tools install</td>
</tr>
</tbody>
</table>
Table 4. Minimum required vCenter user account privileges (continued)

<table>
<thead>
<tr>
<th>Privilege type</th>
<th>Required privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine-Inventory</td>
<td>- Create from existing</td>
</tr>
<tr>
<td></td>
<td>- Create new</td>
</tr>
<tr>
<td></td>
<td>- Register</td>
</tr>
<tr>
<td></td>
<td>- Remove</td>
</tr>
<tr>
<td></td>
<td>- Unregister</td>
</tr>
<tr>
<td>Virtual Machine-Provisioning</td>
<td>- Allow disk access</td>
</tr>
<tr>
<td></td>
<td>- Allow read-only disk access</td>
</tr>
<tr>
<td></td>
<td>- Allow virtual machine download</td>
</tr>
<tr>
<td></td>
<td>- Clone virtual machine</td>
</tr>
<tr>
<td></td>
<td>- Mark as template</td>
</tr>
<tr>
<td>Virtual Machine-Snapshot</td>
<td>- Create snapshot</td>
</tr>
<tr>
<td>Management</td>
<td>- Remove snapshot</td>
</tr>
<tr>
<td></td>
<td>- Revert to snapshot</td>
</tr>
<tr>
<td>vApp</td>
<td>- Export</td>
</tr>
<tr>
<td></td>
<td>- Import</td>
</tr>
<tr>
<td></td>
<td>- vApp application configuration</td>
</tr>
</tbody>
</table>

Register or add a VMware vCenter client

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

About this task

Client registration is the process of establishing the identity of the vCenter client 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. 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, complete 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:
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** field, 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:
     o 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.
     o 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 **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.
   - 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:

o Restart
o Power on
o Resume after suspend
o Migrate

7. Click **NEXT**.
   - The **Optional Information** pane appears.
8. Optional, complete 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.

Results

Adding a vCenter client in the AUI automatically:

- Adds the vCenter client to the Default Group.
  
  However, this client is not activated as normal Avamar clients are. Therefore, no backups are performed for it on behalf of the Default Group.

- Creates vCenter Server domain hierarchy.

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

- Creates a Default Virtual Machine Group.

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

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

1. Retire the existing vCenter client in the AUI.
2. Add the vCenter as a vCenter client (using this procedure).
3. Re-invite the retired vCenter client as a normal client to support guest level backup from the vCenter Server.

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 use 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

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 ESX 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 ESX host topology, and suggests an optimal ESX host location for each proxy so that all datastores are protected.

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

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

- Proxy name
- Avamar server domain where the proxy 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 best practices are also discussed.

Data change rate

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

Even though empirical field data routinely reports client data change rates of 3-4% per day, by default Proxy Deployment 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 8 concurrent backup jobs and process 500 GB of data per hour.

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

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

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

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

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

Protecting against proxy over commit

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

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 will be level-1 incremental or changed block backups, not level-0 full backups.

Level-0 backups inherently take longer and use more proxy resources. Therefore, large new virtual machine deployments can adversely affect the ability to complete all required backups in the time allotted by the backup window.
For this reason, whenever possible phase-in large new virtual machine deployments in order to give the system an opportunity to ingest the necessary level-0 backups.

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

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

## 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 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 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 ESX 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 other proxies that you want to deploy:

   **NOTE:** You must be prepared to specify the proxy name, IP address, fully qualified DNS server name or IP address, network gateway and network mask for each proxy you add.
   - a. In the tree pane, select an ESX host.
   - b. Click **New Proxy**.
     The **New Proxy** dialog box 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.

6. (Optional) Delete any proxies that you do not want to deploy:
   a. In the tree pane, select a proxy.
   b. Click
   c. Click YES.

7. To update the proxy topology, click 🔄.

8. 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 completely deleted from the system. That hostname and IP address are available for subsequent proxy deployments.

Upgrading proxies

This section discusses how to upgrade proxies that run supported releases of the Avamar software. For Avamar proxies running release 7.3.x or older, past releases of this publication provide more information.

About this task

- If you deployed the proxy with the Proxy Deployment Manager, use Upgrading Avamar proxies on page 31.
- If you manually deployed the proxy, you must record the required information, remove the existing proxy, and then re-deploy a new proxy. Upgrading Avamar proxies from supported releases before 7.5.1 on page 32 provides more information.

**NOTE:**

The Proxy Deployment Manager may not list manually-deployed proxies.

You can only use an ISO to upgrade to a release that runs the same version of the SLES OS. Therefore, you cannot use an ISO to upgrade a proxy from an earlier release (on SLES 11 SP3) to release 7.5.1 or later (on SLES 12 SP1). If you manually deployed a proxy for an earlier release with a different version of the SLES OS, you must remove the proxy and then use the Proxy Deployment Manager to deploy a new proxy.

The following topics provide instructions that use Avamar Administrator, as some past Avamar releases do not support the Avamar Web User Interface (AUI). Where available, you can use the Proxy Deployment Manager within the AUI instead. Deploying proxies on page 28 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 as well as a tooltip that indicates that the proxy has an update pending.

3. Click Apply.
Upgrading Avamar proxies from supported releases before 7.5.1

This section provides information and procedures for upgrading supported Avamar proxy software when existing proxies are at a release level before 7.5.1.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Host</th>
<th>Datastore</th>
<th>Network</th>
<th>Folder</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy1</td>
<td>vcenter.com/host1</td>
<td>DS2</td>
<td>NW1</td>
<td>/proxies</td>
<td>x.x.x.x</td>
</tr>
<tr>
<td>Proxy2</td>
<td>vcenter.com/host2</td>
<td>DS2</td>
<td>NW1</td>
<td>/proxies</td>
<td>x.x.x.x</td>
</tr>
</tbody>
</table>

Table 6. Example chart for gathering proxy information, continued

<table>
<thead>
<tr>
<th>Gateway</th>
<th>DNS</th>
<th>Netmask</th>
<th>Domain</th>
<th>Datastore protecting</th>
<th>Groups protecting</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.x.x.x</td>
<td>x.x.x.x.x</td>
<td>x.x.x.x</td>
<td>/clients</td>
<td>DS1,DS2</td>
<td>Default Virtual Machine Group</td>
</tr>
<tr>
<td>x.x.x.x</td>
<td>x.x.x.x.x</td>
<td>x.x.x.x</td>
<td>/clients</td>
<td>DS1,DS2</td>
<td>Other Group</td>
</tr>
</tbody>
</table>

Viewing 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>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vami.ip0.EMC_Avamar_Virtual_Machine_Combined_Proxy</td>
<td>IP address</td>
</tr>
<tr>
<td>vami.gateway.EMC_Avamar_Virtual_Machine_Combined_Proxy</td>
<td>Gateway</td>
</tr>
<tr>
<td>vami.DNS.EMC_Avamar_Virtual_Machine_Combined_Proxy</td>
<td>DNS servers</td>
</tr>
<tr>
<td>vami.netmask0.EMC_Avamar_Virtual_Machine_Combined_Proxy</td>
<td>Netmask</td>
</tr>
</tbody>
</table>

### 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 **Account Management** tab.
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* on page 32.
5. Click the **Groups** tab and verify the proxies that are members of this group, based on the chart created in *Existing proxy configuration* on page 32.
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* on page 28 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* on page 32:
   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

**About this task**

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 you want to reregister.
3. Right click **Power > Shut Down Guest**.
4. Click **Yes** to confirm that you want to shut down the guest operating system.
5. Right click **Power > Power Off**.
6. Click **Yes** to confirm that you want to power off the proxy virtual machine.
7. Right-click **Open Console**.
   A console window appears.
8. Right click **Power > Power On**.
9. Monitor the console window until the following message appears:
   Please press a key now if you want to re-register this proxy with Avamar Administrator.
   Continuing in 10 seconds...
10. Click inside the console window and press Enter.
11. Type the Avamar server DNS name, and then press Enter.
12. Type an Avamar server domain name, and then press Enter.

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

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

### Changing the proxy guest operating system admin password

**About this task**

*NOTE: The root account for ssh login 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 click Enter.
4. Type the new guest operating system admin password, and then click Enter.
5. Confirm the new password by typing the password again, and then click 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 typing:
   ```
   su -
   ```
3. Type `passwd`.
4. Type the current guest operating system root password, and then click Enter.
5. Type the new guest operating system root password, and then click Enter.
6. Confirm the new password by typing the password again, and then click Enter.

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

### 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:
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

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
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 synchronizing the AUI with a vCenter
- Renaming 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:

![Diagram of nested containers]

**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**

**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.

   **NOTE:** The *Avamar for VMware User Guide* provides information about VMware vCenter, Image Proxy, and virtual machine client types.

   The Select VMware Entity pane is displayed.

4. In the Select VMware Entity window, complete the following tasks:
   - To view the vSphere virtual machines and templates, toggle the Host/Cluster switch to off.
   - To view the vSphere hosts and clusters, toggle the Host/Cluster switch to on.

   The vCenter inventory list displays on the right pane according to the VMware entity that was selected in the left pane.

   **NOTE:** Resource pools are not visible in the vSphere virtual machines and templates view. They are only visible in the hosts and clusters view.

   a. To select a folder, resource pool, virtual machine, or vApp, in the right pane, click ➔.

   The VMware entities is displayed in the lower pane.

   b. When adding a container, in the right pane, toggle the Dynamic switch to on to make this a dynamic container.

   This setting enables dynamic policies.

   c. When adding a container, in the right pane, toggle the Static switch to on to make this a static container.

   d. To enable changed block tracking, in the right pane, toggle the CBT switch to on.

   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:
To add a dynamic container that uses recursive protection, in the right pane, toggle the Recursive switch to on. This task automatically adds all the child entities, including the subcontainers, virtual machines, and vApps residing in the subcontainers.

5. Click OK.
6. If you enabled change block tracking:
   a. In the vSphere Client, locate the virtual machine.
   b. Perform any of the following actions for each virtual machine:
      • Reboot
      • Power on
      • Resume after suspend
      • Migrate

7. To remove a folder, resource pool, virtual machine, or vApp, in the lower pane, click .
8. Click YES.

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 client's backups.
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 synchronizing the AUI with a vCenter

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

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.
3. 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.
4. Click Yes to dismiss the confirmation message.

Renaming a vCenter client

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

```
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:

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.
Topics:

- Limitations
- Perform an on-demand backup of a virtual machine by using AUI
- Set advanced plug-in options in the AUI
- Scheduling backups using the AUI Policy wizard
- Log truncation backups
- Monitoring 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.

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 will be checked for orphaned snapshots. The only known remedy is to reconfigure the virtual machine such that all virtual disks reside on the same datastore.

Backups involving physical RDM disks

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

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

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

Nested container limitations

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

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

Figure 5. Example nested container structure

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

Two interim solutions exist for this limitation:

- Flatten the container structure.
  - For example, move vm-3 under vApp-1. Then all three virtual machines will be backed up when vApp-1 is backed up.
- Add both vApp-1 and vApp-2 to Avamar as separate container entities so that they can be backed up separately.
  - When restoring, restore vApp-1 first, then restore vApp-2 into vApp-1

vApp backups fail if any subvirtual machine fails to backup

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

The **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.

**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-com.dellemc.avamar**: The date and time of the most recent successful backup.
- **LastBackupStatus-com.dellemc.avamar**: The date and time of the most recent backup, whether successful or not.

4. To index VMware image backups, select **Index VMware Image Backups**.
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 try a restore of the excluded file, the excluded is visible but unstable.

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 delete 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) field, 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.

**Scheduling 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. The Avamar Administration Guide provides more information about policies, datasets, schedules, and retention settings.

**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 Settings > Dataset > Add.
3. Assign a schedule to the new backup policy.
   - To create a schedule, use the Policy wizard or select Settings > Schedule > Add.
4. Assign a retention policy to the new backup policy.
   - To create a retention policy, use the Policy wizard or select Settings > 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 Settings. 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 (_). 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
7. Click SUBMIT.

Creating 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. These settings comprise 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.

Enabling 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 including virtual machines in a backup policy

As part of the autodiscovery feature, virtual machines that have been autodiscovered are automatically assigned to backup policies by using rules. In this way, backup policies can be automatically assigned to VMs when they are created in vCenter. This procedure describes how to configure scheduled backups to use rules to automatically assign backup policies to autodiscovered VMs.

About this task

NOTE: Auto-discovery of virtual machines on page 27 contains information about configuring autodiscovery of VMs.

Steps

1. Create a backup policy.
2. In the Members page of the Policy wizard, select Enable Dynamic rule.
3. From the Rule drop-down list, perform either of the following step:
   - Select an existing rule.
   - Select New Rule....
     If New Rule... is selected, create a rule.
4. To add a client to the backup policy that has not been automatically assigned, perform the following steps:
   a. In the list of clients, select the client that you want to add.
   b. Click NEXT.

   NOTE: It is generally not good practice to manually include clients in a backup policy that is using VM autodiscovery. Best practice is to reserve backup policies that are using automatic member selection for that purpose only, and create other backup policies for clients that are not autodiscovered VMs.

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

5. To exclude clients in this backup policy that have been automatically assigned, perform the following steps:
   a. In the list of clients, clear the client that you want to remove.
   b. Click NEXT.

   This step removes the association between selected clients and the backup policy. When you complete the task, the backup policy no longer applies to the selected clients.

   NOTE: It is generally not good practice to manually exclude clients in a backup policy that is using VM autodiscovery. Best practice is to properly configure rules and VMs so that only those VMs that should be in this backup policy are automatically assigned to it.

6. Click NEXT.

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

The Avamar Administration Guide provides more information about creating rules.
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 Settings. 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 (_). 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 Settings.

   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 (_). 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.

Monitoring 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:

- Filter activities by duration—By default, the Activity Monitor displays the most recent 5,000 client activities. To select a different duration, in the Filter activities by duration drop-down list, select Last 24 hours or Last 72 hours.

- Filter activities by domain—By default, the Activity Monitor displays all activities regardless of domain. To display only the activities for a specific domain, in the Filter activities by domain drop-down list, select a domain or subdomain.

- Filter activities by status—By default, the Activity Monitor displays all activities regardless of status.

To display only activities with a specific status, at the top of the Activity Monitor, select one of the following options:

- Canceled
- Completed
- Completed with Exceptions
- Failed
- Running
- Waiting

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 bug that inhibits hot-adding an encrypted virtual machine. The [VMware Release Notes](https://www.vmware.com/support/relnotes/vddk.html) 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**.

**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 will fail back to a file system-consistent snapshot. This process generates an error message in vCenter, which you can ignore. This is a VMware limitation.
When restoring a virtual machine as a new image:
  - By default, new virtual machines are not encrypted. If encryption is desired, 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 non-default 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 nbddssl 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 nbddssl 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>
<thead>
<tr>
<th>Table 8. Required permissions for the Avamar Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object</strong></td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Datastore</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Virtual Machine</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Folder</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Global</td>
</tr>
</tbody>
</table>
Table 8. Required permissions for the Avamar Administrator (continued)

<table>
<thead>
<tr>
<th>Object</th>
<th>Permissions</th>
<th>Sub-permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Disable Methods</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabled Methods</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Tag</td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Assign virtual machine to resource pool</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>Configuration</td>
<td>Advanced Settings</td>
</tr>
<tr>
<td>Network</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Profile-driven Storage</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Cryptographic operations</td>
<td>Add disk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Direct access</td>
<td></td>
</tr>
</tbody>
</table>

2. Create a group for the backup as described in Scheduling backups.

**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.
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.

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:

- Filter activities by duration—By default, the Activity Monitor displays the most recent 5,000 client activities. To select a different duration, in the Filter activities by duration drop-down list, select Last 24 hours or Last 72 hours.
- Filter activities by domain—By default, the Activity Monitor displays all activities regardless of domain. To display only the activities for a specific domain, in the Filter activities by domain drop-down list, select a domain or subdomain.
- Filter activities by status—By default, the Activity Monitor displays all activities regardless of status.

To display only activities with a specific status, at the top of the Activity Monitor, select one of the following options:

- Canceled
- Completed
- Completed with Exceptions
- Failed
- Running
- Waiting

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.

**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. 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.

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 Access**.
   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 **Summary** 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.
   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 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.
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.
13. In the Summary 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 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.
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 Summary 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 client computers, 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.
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 Summary 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>
<thead>
<tr>
<th>Table 9. Image restore toolbar buttons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td><img src="image.png" alt="Image Restore" /></td>
</tr>
<tr>
<td><img src="image.png" alt="Granular Restore" /></td>
</tr>
<tr>
<td><img src="image.png" alt="Mount Windows VMDK" /></td>
</tr>
</tbody>
</table>

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 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 will be present.

Two interim solutions exist for this limitation:
- Flatten the container structure.
  
  For example, move vm-3 under vApp-1. Then all three virtual machines will be backed up when vApp-1 is backed up.
- Add both vApp-1 and vApp-2 to Avamar as separate container entities so that they can be backed up separately.

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

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

Steps
1. In the vSphere Client or vSphere Web Client, ensure that the target virtual machine is powered off.
2. In the AUI navigation pane on the left, click ➤, and then click Asset Management.
   
   The **Asset Management** window is displayed.
3. In the domain tree, select the domain that contains the virtual machine client or VMware container.
4. 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.
5. (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.
6. 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.
7. (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.
8. 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.
9. In the **Basic Configuration** field, perform the following steps:
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 check box.
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.

10. Click NEXT.

The Summary pane is displayed.

11. In the Summary pane, review the provided information, and then click FINISH.

The following status message is displayed:

Restore request initiated.

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

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

#### Steps

1. In the vSphere Client or vSphere Web Client, ensure that the target virtual machine is powered off.
2. In the AUI navigation pane on the left, click ➞, and then click Asset Management.

   The Asset Management window is displayed.
3. In the domain tree, select the domain that contains the virtual machine client or VMware container.
4. 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.
5. (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.
6. 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.
7. (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.
8. 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.
9. In the Basic Configuration field, 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.

66 Restore
e. In the **Proxy** field, select an option.
f. Click **NEXT**.

The **Advanced Configuration** pane is displayed.

### 10. 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.

11. Click **NEXT**.

The **Summary** pane is displayed.

12. In the **Summary** pane, review the provided information, and then click **FINISH**.

The following status message is displayed:

**Restore request initiated.**

13. 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.

---

### Mounting Windows VMDKs from an image backup

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

### Configuring the recovery target machine

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

#### Prerequisites

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

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

#### Steps

2. Using instructions in the Avamar Backup Clients User Guide, register the recovery target machine as a client with the same Avamar server storing the image backup to be mounted.
3. Install the Windows VMware GLR plug-in software:
   a. Log in to the recovery target machine with Windows administrator privileges.
   b. Download the `AvamarVMWareGLR-windows-x86_64-version.msi` install package from the Avamar server.
   c. Open the install package, and then follow the on-screen instructions.
   d. Reboot the computer.

### Restoring and mounting the Windows VMDKs

#### Prerequisites

Ensure that the recovery target machine has been properly configured:

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

#### Steps

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

   The Backup, Restore and Manage window is displayed.
3. Click the **Restore** tab.
The upper left pane contains a list of domains.

4. Select a virtual machine client or VMware container:
   a. Select the domain that contains the virtual machine client or VMware container. You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.
      A list of Avamar clients appears in the pane under the domains list.
   b. From the list of clients, select the virtual machine client or VMware container.

5. Select a backup:
   a. Click the By Date tab.
   b. Select the backup date from the calendar. Valid backups occurred on dates with a yellow highlight. A list of backups on that date appears in the Backups table next to the calendar.
   c. Select a backup from the Backups table.

6. In the contents pane, select a virtual disk.

7. Click the Mount Windows VMDK button (△). The Select Destination Client dialog box appears.

8. Click Browse next to the Client box. The Browse for Restore Destination Client dialog box appears.

9. Select the recovery target virtual machine, and then click OK. The Browse Backup Status dialog box appears.

10. Click OK to confirm that the operation should continue. The Restore Browse Options dialog box appears.

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

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

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 (егодня) 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.

Performance improvements for file-level restore

With Avamar 7.4 and later, the HTTPS (443) protocol is used by default to perform file-level restore. 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, the previous mechanism, using file copy, will be used to perform the file-level restore. The following warning message will be displayed during restore:

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 will take 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>
<thead>
<tr>
<th>Partitioning scheme</th>
<th>Guest OS</th>
<th>FLR</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBR</td>
<td>Windows/Linux</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>EBR (Logical Partition)</td>
<td>Windows/Linux</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>GPT</td>
<td>Windows/Linux</td>
<td>Partial support</td>
<td>Support BTRFS and LVM base on GPT in Linux</td>
</tr>
<tr>
<td>MixedGPT</td>
<td>Windows/Linux</td>
<td>Not supported</td>
<td>Hybrid MBR</td>
</tr>
</tbody>
</table>

**File system support**

The following table outlines the file system support for FLR.

<table>
<thead>
<tr>
<th>File system type</th>
<th>Guest OS</th>
<th>Partitioning scheme</th>
<th>Partition ID</th>
<th>Partitionless disk</th>
<th>LVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext2</td>
<td>Linux</td>
<td>MBR, EBR</td>
<td>0x83</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>ext3</td>
<td>Linux</td>
<td>MBR, EBR</td>
<td>0x83</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>ext4</td>
<td>Linux</td>
<td>MBR, EBR</td>
<td>0x83</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>ntfs</td>
<td>Windows</td>
<td>MBR, EBR, GPT</td>
<td>0x04/0x07</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>vfat</td>
<td>Windows</td>
<td>MBR, EBR</td>
<td>0x06/0x0E</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>xfs</td>
<td>Linux</td>
<td>MBR, EBR</td>
<td>0x83</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>reiserfs</td>
<td>Linux</td>
<td>MBR, EBR</td>
<td>0x83</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>btrfs</td>
<td>Linux</td>
<td>MBR, EBR, GPT</td>
<td>0x83</td>
<td>Support</td>
<td>Support</td>
</tr>
</tbody>
</table>

**LVM support**

The following table outlines the LVM support for FLR.

<table>
<thead>
<tr>
<th>LV type</th>
<th>FLR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear LV</td>
<td>Support</td>
</tr>
<tr>
<td>Striped LV</td>
<td>Support</td>
</tr>
<tr>
<td>Mirrored LV</td>
<td>Support</td>
</tr>
<tr>
<td>RAID LV</td>
<td>Support</td>
</tr>
<tr>
<td>Thin LV</td>
<td>Support</td>
</tr>
</tbody>
</table>
Multi-device support

The following table outlines multi-device support for FLR.

### Table 13. Multi-device support for FLR

<table>
<thead>
<tr>
<th>RAID</th>
<th>Occur</th>
<th>FLR</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0/Striping</td>
<td>LVM/BTRFS</td>
<td>Support</td>
</tr>
<tr>
<td>RAID 1/Mirroring</td>
<td>LVM/BTRFS</td>
<td>Support</td>
</tr>
<tr>
<td>RAID 4</td>
<td>LVM</td>
<td>Support</td>
</tr>
<tr>
<td>RAID 5</td>
<td>LVM</td>
<td>Support</td>
</tr>
<tr>
<td>RAID 6</td>
<td>LVM</td>
<td>Support</td>
</tr>
<tr>
<td>RAID10</td>
<td>LVM/BTRFS</td>
<td>Support</td>
</tr>
</tbody>
</table>

File-level restore limitations

File-level restore has the following limitations:

- 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.
- The vCenter must be added to the root domain in the AUI. Any other location for the vCenter domain is not supported.
- When performing a file-level restore to a /tmp location, the Avamar software redirects data to a private /tmp location.

For example:

```bash
tmp/systemd-private-*
```

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

**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`:

```bash
vcenter-sso-hostname=<VC_hostname>
vcenter-sso-port=7444
# configure only if more than one vCenter
vcenter-hostname=<VC_hostname>
```

Unsupported virtual disk configurations

File-level restore does not support the following virtual disk configurations:

- Filesystems that support FLR require a higher kernel than proxy operating system (3.12)
  - XFS Free Inode B-Tree (finobt)
  - Ext4 sparse_supper2(3.16), metdata_csum(3.18), encrypt(4.1), project(4.5)
- Windows Dynamic disks
- Encrypted/compressed partitions or bootloaders
- Deduplicated NTFS
- Unformatted disks
- Browsing of multiple active disks/partitions. Only the first active disk/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 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 one or more logical volumes.
Perform a file-level restore (FLR) operation by using 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 file-level restores:
- 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, only a local administrator user can perform file-level restore. Additionally, ensure that you disable User Account Control (UAC). The knowledgebase article at https://support.emc.com/kb/477118 provides more information.

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 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. 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.
   c. In the Basic Config pane, 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.
   d. In the Username field, type the username for the destination client.
   e. In the Password field, type the password for the destination client.
   f. In the Location field, the path for the restore.
   g. (Optional) Select Restore ACL to restore ACLs.
Perform a file-level restore (FLR) operation by using the Data Protection Backup and Recovery File-Level Restore UI

With the Data Protection Backup and Recovery File-Level Restore 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 file-level restores:

- 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, only a local administrator user can perform file-level restore. Additionally, ensure that you disable User Account Control (UAC) before performing a file-level restore. The knowledgebase article at https://support.emc.com/kb/477118 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 File-Level Restore 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 File-Level Restore 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 File-Level Restore 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:](image)
   **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.

   ![NOTE:](image)
   **NOTE:** If the **Restore ACL** option is selected, the user performing the restore must have file ownership of the original file to perform the restore. If the file ownership has changed since the backup was performed and the user performing the restore does not have proper file ownership, the restore fails.

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**.
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

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:

   a. Click More Options. The Validate Command Line Options dialog box appears.

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

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

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

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

   e. Click OK.

15. Click OK on the Validate Options box. The following status message appears: Restore request initiating.

16. Click Close.

Scheduling backup validations

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

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.


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 you want to be members of this validation group.

b. Click Next.

7. In the Location screen:
   a. Click Configure Location.
   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.
Protecting the vCenter Management Infrastructure

Topics:
- Overview
- Backing up the vCenter management infrastructure
- Recovering vCenter management infrastructure from Avamar backups
- Support for vCenter HA failover for inflight backups

Overview

This topic discusses how to protect the vCenter management infrastructure (not the virtual machines within that environment). The vCenter runs on a 32-bit or 64-bit Windows host. It also comprises a database server which can run on a different host. Some optional vSphere components require additional databases that can be hosted on the same host as vCenter or on different database server hosts.

NOTE: For more information about protecting vCenter 6.5 deployments with Avamar using the VMware image backup proxy appliance, refer to the Backup and Restore of the vCenter Server using the Avamar VMware Image Protection Solution whitepaper.

The methodology for protecting vCenter management infrastructure is to implement guest backup on each virtual host. The dataset should only back up the following important vCenter management infrastructure components:
- License files
- SSL certificates
- Audit logs
- Windows guest customization (sysprep) files
- Database-hosted configuration settings
- UpdateManager database
- Site Recovery Manager (SRM) database

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

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

Backing up the vCenter management infrastructure

About this task

The methodology for protecting vCenter management infrastructure is to implement guest backup on each virtual host using a custom dataset that only backs up important vCenter management infrastructure components.

You should then add the vCenter Avamar clients to a group and schedule these backups at regular intervals.
Implementing guest backups of vCenter management infrastructure

Steps
1. Install and register Avamar Client for Windows software on the vCenter host as described in the Avamar Backup Clients User Guide.
2. Install and register the correct Avamar database software on each database host as described in various database-specific documentation such as the Avamar for SQL Server User Guide.

Creating a dataset for vCenter management infrastructure backups

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

About this task

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

Steps
1. In Avamar Administrator, select Tools > Manage Datasets. The Manage All Datasets window is displayed.
2. Click New. The New Dataset dialog box appears.
3. Type a name for this new dataset (for example, vCenter-1).
4. Click the Source Data tab.
5. Select Enter Explicitly, and then select the Windows File System plug-in from the Select Plug-In Type list.
6. In the list of backup targets at the bottom of the dialog box, delete every entry except for the Windows File System plug-in by selecting an entry, and then clicking -.
7. Add each vCenter management infrastructure component to the dataset:
   a. Select Files and/or Folders and click ...
      The Select Files And/Or Folders dialog box appears.
   b. Locate a vCenter management infrastructure component and select it.

Table 14. Important vCenter management infrastructure components

<table>
<thead>
<tr>
<th>Component</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>License files</td>
<td>The exact location depends on the specific VMware and Windows version, but is typically one of the following folders: C:\Program Files(x86)\VMware\Infrastructure\VirtualCenter Server\licenses\site C:\Program Files\VMware\VMware License Server\Licenses</td>
</tr>
<tr>
<td>SSL certificates</td>
<td>The exact location depends on the specific VMware and Windows version, but is typically one of the following folders: C:\Documents and Settings\All Users\Application Data\VMware\VirtualCenter\SSL C:\ProgramData\VMware\VirtualCenter\SSL</td>
</tr>
<tr>
<td>Audit logs</td>
<td>The exact location depends on the specific VMware and Windows version, but is typically one of the following folders:</td>
</tr>
</tbody>
</table>
Table 14. Important vCenter management infrastructure components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows guest customization (sysprep)</td>
<td>The exact location depends on the specific VMware and Windows version, but is typically one of the following folders:</td>
</tr>
<tr>
<td>files</td>
<td>C:\Documents and Settings\All Users \Application Data\VMware\VMware VirtualCenter\Logs</td>
</tr>
<tr>
<td></td>
<td>C:\ProgramData\VMWare\VMware VirtualCenter\Logs</td>
</tr>
</tbody>
</table>

8. Click OK.

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

Adding a backup client for vCenter database hosts

About this task

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

Steps

1. Install Avamar database backup agents on the database hosts as described in the database-specific documentation, such as the Avamar for SQL Server User Guide.
2. Configure a scheduled backup to protect the databases.
   - You should truncate vCenter database transaction logs after each backup. This step can be done by selecting the Truncate database log option in the SQL Server plug-in. Truncating database transaction logs ensures that logs will not grow too large, and consume excessive amounts of space on the Avamar server.

Recovering vCenter management infrastructure from Avamar backups

About this task

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

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.
Protecting ESX Hosts

Topics:

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

Overview

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

There are two primary uses for this feature:

1. Support for minimal customer configurations.
   
   Some customer sites use a simple VMware topology, comprising a single ESX host, with one or more virtual machines residing on that ESX host. These sites typically do not implement a vCenter management layer. However, the virtual machines residing on a standalone ESX host still must be backed up in order to protect against data loss. Adding the standalone ESX host as an Avamar vCenter client enables those virtual machines to be backed up with image backup, rather than guest backup.

2. Virtual vCenter disaster recovery.

   Adding an ESX host as an Avamar vCenter client can be useful when virtual machines residing on a particular ESX host must be restored, but the vCenter is not operational. This is often the case when a virtual vCenter must be recovered from Avamar backups. Adding the standalone ESX host as an Avamar vCenter client enables the vCenter management infrastructure virtual machines to be restored so that the vCenter can be restarted.

Limitations

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.

Task List

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

1. Ensure that the Avamar server can communicate and authenticate with the ESX host.

   Add the ESX host certificate to the Avamar MCS keystore. Otherwise, you must disable certificate authentication for all MCS communications.

2. (Optional) Create a dedicated user account on the ESX host for use with Avamar.

3. Add the ESX host to Avamar as a vCenter client.

   This enables dynamic discovery of virtual machines residing on that ESX host, so that they can be backed up with image backup rather than guest backup.

4. Deploy one or more proxies on the ESX host.

5. Perform on-demand or scheduled image backups of virtual machines residing on that ESX host.
Adding ESX host authentication certificates to the MCS keystore

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

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 typing 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 ESX host user account

We strongly recommend that you set up a separate user account on each ESX 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 ESX host user account ensures maximum clarity if it becomes necessary to examine ESX host logs.
**NOTE:** The user account must be added to the top (root) level in each ESX host you intend to protect.

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

### Table 15. Minimum required ESX host user account privileges

<table>
<thead>
<tr>
<th>Privilege type</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>• Create alarm</td>
</tr>
<tr>
<td>Datastore</td>
<td>• Allocate space</td>
</tr>
<tr>
<td></td>
<td>• Browse datastore</td>
</tr>
<tr>
<td></td>
<td>• Low level file operations</td>
</tr>
<tr>
<td></td>
<td>• Remove file</td>
</tr>
<tr>
<td>Extension</td>
<td>• Register extension</td>
</tr>
<tr>
<td></td>
<td>• Unregister extension</td>
</tr>
<tr>
<td></td>
<td>• Update extension</td>
</tr>
<tr>
<td>Folder</td>
<td>• Create folder</td>
</tr>
<tr>
<td>Global</td>
<td>• Cancel task</td>
</tr>
<tr>
<td></td>
<td>• Disable methods</td>
</tr>
<tr>
<td></td>
<td>• Enable methods</td>
</tr>
<tr>
<td></td>
<td>• Licenses</td>
</tr>
<tr>
<td></td>
<td>• Log event</td>
</tr>
<tr>
<td></td>
<td>• Manage custom attributes</td>
</tr>
<tr>
<td></td>
<td>• Settings</td>
</tr>
<tr>
<td>Host &gt; Configuration</td>
<td>• Connection</td>
</tr>
<tr>
<td></td>
<td>• Storage partition configuration</td>
</tr>
<tr>
<td>Network</td>
<td>• Assign network</td>
</tr>
<tr>
<td></td>
<td>• Configure</td>
</tr>
<tr>
<td>Resource</td>
<td>• Assign virtual machine to resource pool</td>
</tr>
<tr>
<td>Sessions</td>
<td>• Validate session</td>
</tr>
<tr>
<td>Tasks</td>
<td>• Create task</td>
</tr>
<tr>
<td></td>
<td>• Update task</td>
</tr>
<tr>
<td>vApp</td>
<td>• Import</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>• Add existing disk</td>
</tr>
<tr>
<td></td>
<td>• Add new disk</td>
</tr>
<tr>
<td></td>
<td>• Add or remove device</td>
</tr>
<tr>
<td></td>
<td>• Advanced</td>
</tr>
<tr>
<td></td>
<td>• Change CPU count</td>
</tr>
<tr>
<td></td>
<td>• Change resource</td>
</tr>
<tr>
<td></td>
<td>• Disk change tracking</td>
</tr>
<tr>
<td></td>
<td>• Disk Lease</td>
</tr>
<tr>
<td></td>
<td>• Extend virtual disk</td>
</tr>
<tr>
<td></td>
<td>• Host USB device</td>
</tr>
<tr>
<td></td>
<td>• Memory</td>
</tr>
<tr>
<td></td>
<td>• Modify device settings</td>
</tr>
<tr>
<td></td>
<td>• Raw device</td>
</tr>
</tbody>
</table>
Table 15. Minimum required ESX host user account privileges (continued)

<table>
<thead>
<tr>
<th>Privilege type</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Reload from path</td>
</tr>
<tr>
<td></td>
<td>• Remove disk</td>
</tr>
<tr>
<td></td>
<td>• Rename</td>
</tr>
<tr>
<td></td>
<td>• Reset guest information</td>
</tr>
<tr>
<td></td>
<td>• Settings</td>
</tr>
<tr>
<td></td>
<td>• Swapfile placement</td>
</tr>
<tr>
<td></td>
<td>• Upgrade virtual machine compatibility</td>
</tr>
<tr>
<td>Guest Operations</td>
<td>• Guest Operation Modifications</td>
</tr>
<tr>
<td></td>
<td>• Guest Operation Program Execution</td>
</tr>
<tr>
<td></td>
<td>• Guest Operation Queries</td>
</tr>
<tr>
<td>Interaction</td>
<td>• Console interaction</td>
</tr>
<tr>
<td></td>
<td>• DeviceConnection</td>
</tr>
<tr>
<td></td>
<td>• Guest operating system management by VIX API</td>
</tr>
<tr>
<td></td>
<td>• Power off</td>
</tr>
<tr>
<td></td>
<td>• Power on</td>
</tr>
<tr>
<td></td>
<td>• Reset</td>
</tr>
<tr>
<td></td>
<td>• VMware Tools install</td>
</tr>
<tr>
<td>Inventory</td>
<td>• Create new</td>
</tr>
<tr>
<td></td>
<td>• Register</td>
</tr>
<tr>
<td></td>
<td>• Remove</td>
</tr>
<tr>
<td></td>
<td>• Unregister</td>
</tr>
<tr>
<td>Provisioning</td>
<td>• Allow disk access</td>
</tr>
<tr>
<td></td>
<td>• Allow read-only disk access</td>
</tr>
<tr>
<td></td>
<td>• Allow virtual machine download</td>
</tr>
<tr>
<td></td>
<td>• Mark as Template</td>
</tr>
<tr>
<td>Snapshot Management</td>
<td>• Create snapshot</td>
</tr>
<tr>
<td></td>
<td>• Remove snapshot</td>
</tr>
<tr>
<td></td>
<td>• Revert to snapshot</td>
</tr>
<tr>
<td></td>
<td>• Management</td>
</tr>
<tr>
<td>State</td>
<td></td>
</tr>
</tbody>
</table>

Adding an ESX host as a vCenter client

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.
Deploying a proxy in a standalone ESX host

Prerequisites
1. Add DNS entries for each proxy you intend to deploy.
   During proxy deployment, you will be asked to assign a unique IP address to each proxy. The ESX host performs a reverse DNS lookup of that IP address to ensure that it is resolvable to a hostname. For best results, configure all required DNS entries for proxies you plan to deploy before proceeding with the remainder of this procedure.
2. Download the proxy appliance template file from the Avamar server.
3. Install the vSphere Client on your Windows computer.

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

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 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 Configuring vCenter-to-Avamar authentication on page 22

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 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 will be 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 on page 89

**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.

2. Place the root certificate in the Avamar server and follow the instructions in the section **Adding vCenter authentication certificates to the MCS keystore** on page 22.

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 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.

- 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 cloudadmin 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.
- VMware tag based rule selection criteria for dynamic policy
- Restore to new vApp
- IPV6
- Virtual machine template backup
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

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

Downloading the proxy appliance template file

Download the proxy appliance template file from the Avamar server.

About this task

NOTE: If adding more than one proxy, you only need to 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. Navigate to the VMware vSphere\EMC Avamar VMware Image Backup\FLR Appliance folder.

4. Click the AvamarCombinedProxy-linux-sles12sp1-x86_64-version.ova link.

5. Save AvamarCombinedProxy-linux-sles12sp1-x86_64-version.ova to a temporary folder, such as C:\Temp, or the desktop.

Deploying the proxy appliance in vCenter

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

Prerequisites

1. Add DNS entries for each proxy you intend to deploy.
   
   During proxy deployment, you will be asked to assign a unique IP address to each proxy. The vCenter performs a reverse DNS lookup of that IP address to ensure that it is resolvable to a hostname. For best results, configure all required DNS entries for proxies you plan to deploy before proceeding with the remainder of this procedure.

2. Download the proxy appliance template file from the Avamar server.
Deploying a proxy appliance in vCenter using the vSphere Web Client

Steps

1. Connect to the vCenter Server by opening a web browser, and then typing the following URL:
   
   `http://vCenter-server:9443/`

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

   The vSphere Web Client page appears.

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

   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.
   c. Follow the onscreen instructions.

3. Reconnect to the vCenter Server by opening a web browser, and then typing the following URL:
   
   `http://vCenter-server:9443/`

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

   The vSphere Web Client page appears.

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

5. Select Home > vCenter > Hosts and Clusters.

6. Select Actions > Deploy OVF Template.

7. Allow plug-in access control.

   The Deploy OVF Template wizard appears.

8. In the Source screen:
   a. Select Local file, and then click Browse.
   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.
   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.
    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.

---

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

---

**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.

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:
   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 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 Configuring vCenter-to-Avamar authentication on page 22.
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.
## Required data ports

These are the required data ports in a vSphere environment.

### Table 16. Required vSphere data ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Source</th>
<th>Destination</th>
<th>Function</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Avamar Administrator</td>
<td>Proxies</td>
<td>SSH</td>
<td>Diagnostic support. Optional, but recommended.</td>
</tr>
<tr>
<td>53</td>
<td>Proxies</td>
<td>DNS server</td>
<td>DNS</td>
<td>UDP+TCP.</td>
</tr>
<tr>
<td>443</td>
<td>Avamar Deployment Manager</td>
<td>ESXi hosts</td>
<td>vSphere API</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Proxies</td>
<td>ESXi hosts</td>
<td>vSphere API</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Proxies</td>
<td>vCenter</td>
<td>vSphere API</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Avamar MCS</td>
<td>vCenter</td>
<td>vSphere API</td>
<td></td>
</tr>
<tr>
<td>902</td>
<td>Proxies</td>
<td>ESX hosts</td>
<td>VDDK</td>
<td></td>
</tr>
<tr>
<td>5489</td>
<td>Avamar Deployment Manager</td>
<td>Proxies</td>
<td>CIM service</td>
<td>Used to register the proxy.</td>
</tr>
<tr>
<td>7444</td>
<td>Avamar MCS</td>
<td>vCenter</td>
<td>Test vCenter credentials</td>
<td></td>
</tr>
<tr>
<td>8543</td>
<td>Proxies</td>
<td>Avamar server</td>
<td>Snapshot manager</td>
<td>Used for VMware snapshot operations.</td>
</tr>
<tr>
<td>27000</td>
<td>Proxies</td>
<td>Avamar server</td>
<td>GSAN communication</td>
<td>Non-secured communication.</td>
</tr>
<tr>
<td>28009</td>
<td>Avamar MCS</td>
<td>Proxies</td>
<td>Access proxy logs</td>
<td></td>
</tr>
<tr>
<td>28102-28109</td>
<td>Avamar MCS</td>
<td>Proxies</td>
<td>avagent paging port</td>
<td>Avamar 7.0 and 7.1.</td>
</tr>
<tr>
<td>29000</td>
<td>Proxies</td>
<td>Avamar server</td>
<td>GSAN communication</td>
<td>Secured communication.</td>
</tr>
<tr>
<td>30001</td>
<td>Proxies</td>
<td>Avamar MCS</td>
<td>avagent to MCS communication</td>
<td>Avamar 7.2.</td>
</tr>
<tr>
<td>30102-30109</td>
<td>Avamar MCS</td>
<td>Proxies</td>
<td>avagent paging port</td>
<td>Avamar 7.2.</td>
</tr>
</tbody>
</table>

**NOTE:** All ports are TCP unless otherwise noted.
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 typing the following command:
   ```bash
   su -
   ```
3. Type the following command:
   ```bash
   /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.
Topics:
- How to set plug-in options
- VMware Image backup plug-in options
- VMware Image restore plug-in 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 backup plug-in options
These backup options are available for the Avamar VMware Image plug-in.

Table 17. Backup options for Avamar VMware Image plug-in

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Changed Block Tracking (CBT) to increase performance</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Changed block tracking must be enabled at the virtual machine level in order for this feature to work.</td>
</tr>
<tr>
<td>Set Annotation Tag LastBackupStatus and LastSuccessfulBackup</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• LastSuccessfulBackupStatus-com.dellemc.avamar: The date and time of the most recent successful backup.</td>
</tr>
<tr>
<td></td>
<td>• LastBackupStatus-com.dellemc.avamar: The date and time of the most recent backup, whether successful or not.</td>
</tr>
<tr>
<td>Exclude page file blocks when performing image backup on Windows VM</td>
<td>If selected, excludes the Windows page file (pagefile.sys) from the backup for all the partitions. It is not limited to primary partitions.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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</td>
</tr>
</tbody>
</table>
### Table 17. Backup options for Avamar VMware Image plug-in (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include file blocks when performing image backup on Windows VM</td>
<td>If selected, includes the deleted file blocks from the backup for all partitions. It is not limited to primary partitions.</td>
</tr>
</tbody>
</table>
| Exclude files with path and filter           | Excludes the files with path and filter from the backup for all 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 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                        | The maximum number of times that a snapshot delete operations should be attempted. |

### Guest credentials

<table>
<thead>
<tr>
<th>Username</th>
<th>Guest operating system user account with sufficient privileges to run scripts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Password for the guest operating system username.</td>
</tr>
</tbody>
</table>

### Pre-snapshot Script

| Script file       | Full path and filename of the script that will be run before the vmdk snapshot. |
Table 17. Backup options for Avamar VMware Image plug-in (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum script run time (minutes)</td>
<td>Maximum number of minutes this script is allowed to run before timing out.</td>
</tr>
<tr>
<td>Post-snapshot Script</td>
<td></td>
</tr>
<tr>
<td>Script file</td>
<td>Full path and filename of the script that will be run after the backup completes and the vmdk snapshot is removed.</td>
</tr>
<tr>
<td>Maximum script run time (minutes)</td>
<td>Maximum number of minutes this script is allowed to run before timing out.</td>
</tr>
<tr>
<td>Snapshot quiesce timeout</td>
<td>Maximum number of minutes to wait before the snapshot quiesce operation is considered to have failed (Windows VMware Image plug-in only)</td>
</tr>
<tr>
<td>Microsoft SQL Server authentication</td>
<td></td>
</tr>
<tr>
<td>NT Authentication</td>
<td>Uses the credentials that are entered in Guest Credentials for authentication. User must have administrative privileges and must have write permissions for the files system and read permissions for the Windows registry.</td>
</tr>
<tr>
<td>Application Authentication</td>
<td>Uses the SQL Server Username and SQL Server Password to log into the SQL server.</td>
</tr>
<tr>
<td>Microsoft SQL Server post action</td>
<td></td>
</tr>
<tr>
<td>Post Action Timeout (minutes)</td>
<td>Maximum number of minutes to wait before post-action operations are considered to have failed. Default is 900 seconds.</td>
</tr>
<tr>
<td>Post Action Type of MSSQL</td>
<td>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 will not occur.</td>
</tr>
</tbody>
</table>

Table 18. Restore options for Avamar VMware Image plug-in

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Changed Block Tracking (CBT) to increase performance</td>
<td>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.</td>
</tr>
<tr>
<td>Encryption method from Data Domain system</td>
<td>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 &quot;high.&quot;</td>
</tr>
</tbody>
</table>

VMware Image restore plug-in options

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

Windows VMware GLR plug-in options

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

**Backups fail with “No Proxy” or “No VM” errors**

If backups fail with “No Proxy” or “No VM” errors, try manually synchronizing Avamar Administrator with the vCenter hosting the virtual machines or proxies.

**Changed block tracking does not take effect**

Enabling changed block tracking in Avamar Administrator does not take effect until any of the following actions occur on the virtual machine: 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, VMware 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.

**Restore problems and solutions**

These are common restore problems and solutions.

**Preexisting snapshots cause restores to fail**

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

```
2012-12-07 09:30:26 avvcbimage FATAL <0000>: The pre-existing snapshots from VMX '[VNXe3300-Datastore1] vm-example/vm-example.vmx' will not permit a restore.
```

```
2012-12-07 09:30:26 avvcbimage FATAL <0000>: If necessary, use the '--skip_snapshot_check' flag to override this pre-existing snapshot check.
```

```
2012-12-07 09:30:26 avvcbimage Error <9759>: createSnapshot: snapshot creation failed
```

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

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

1. Initiate an image restore of the affected virtual machine.
2. When you reach the point in the procedure that instructs you to set restore options in the Restore Options dialog box, perform the following additional steps:
   a. Click More Options.
      The Restore Command Line Options dialog box appears.
   b. Click More.
   c. Type `[avvcbimage]skip_snapshot_check` in the Enter Attribute field.
   d. Type `true` in the Enter Attribute Value field.
   e. Click +.
      The `[avvcbimage]skip_snapshot_check=true` entry appears in the plug-in options list.
   f. Click OK.
3. Proceed with the remainder of the restore procedure.

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

If you back up a virtual machine that has both virtual disks and physical Raw Device Mapping (RDM) disks, the backup will successfully process the virtual disks, bypass the RDM disks.
However, when restoring data from one of these backups, you can restore the data to the original virtual machine, or redirect it to another existing virtual machine. However, you cannot restore data to a new virtual machine.

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

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

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

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

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

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

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

**Fault tolerance disabled when restore to new virtual machine is performed**

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

**Restore to new virtual machine to Virtual SAN 5.5 will fail**

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

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

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

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

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

**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.

**File-level restore 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.

**File-level restore of a folder or file name containing certain special characters fails**

The use of the backslash (\) or the double quote (") in folder or file names is not supported with FLR.

**File-level restore 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**.
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.

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

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.

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.

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

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.

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).

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

**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.

**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.

**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.

**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.

**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.

**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.