Dell EMC Avamar vSphere Web Client

Version 19.2

Administration Guide

302-005-842
REV 01
November 2019

DELL EMC

Copyright © 2001-2019 Dell Inc. or its subsidiaries. All rights reserved.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

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

CONTENTS

Preface **5**

Chapter 1 **Introduction** **9**
Avamar Plug-in for vSphere Web Client 10
How Avamar works with VMware 10
Guest backup and restore 10
Image-level backup and restore 10
Supported configurations 11
Guest and image-level backup and restore comparison 11
Changed block tracking 12

Chapter 2 **Configuring the Avamar Plug-in for vSphere Web Client** **15**
Avamar server configuration 16
Register the Avamar Plug-in for vSphere Web Client 16
Unregister the Avamar Plug-in for vSphere Web Client and disable services 17
Access the Avamar Plug-in for vSphere Web Client 18
Access the plug-in by using Avamar Web User Interface 18
Access the plug-in by using the vSphere Client 18
AUI navigation pane 18
Configure localization for the Data Protection Backup and Recovery File-Level Restore UI 20

Chapter 3 **Using the Avamar Plug-in for vSphere Web Client** **23**
Avamar setup 24
Managing backup policies 24
Start an on-demand backup of a backup policy 24
Edit a backup policy 25
Add members to a backup policy 25
Edit policy attributes 26
AUI Activity Monitor 26
Activity Monitor details 27
Monitor backups 29
Cancel backups 30
Restart a backup job 30
View a detailed client session log 30
Monitor restores 31
Cancel restores 31
Monitor replication in the AUI 32
Cancel a replication task 32
Manage clients 32
Add a VMware client 32
Delete a VMware client 34
Enable changed block tracking 34
Managing rules 35
Create a rule 35

Edit a rule....36
Delete a rule....37
Proxy Deployment....38
About proxy deployment....38
Considerations and best practices....39
Deploy proxies....40
Security patch updates for proxies....42

Chapter 4 Backup and Recovery 45
Perform an on-demand backup of a virtual machine by using AUI....46
Set advanced plug-in options in the AUI....47
VMware Image backup plug-in options....49
Restore an instance of a VM backup by using the AUI....51
Restore data to the original virtual machine....52
Restore data to a different virtual machine....53
Restore data to a new virtual machine....55
File-level restore....56
File-level restore supported configurations....57
File level restore troubleshooting and limitations....58
File-level restore in the AUI....59
Perform a file-level restore (FLR) operation by using the Data Protection Backup and Recovery File-Level Restore UI....61

Appendix Plug-in Options 63
How to set plug-in options....64
VMware Image backup plug-in options....64
VMware Image restore plug-in options....67
Windows VMware GLR plug-in options....67

PREFACE

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://support.EMC.com).

Purpose

This guide describes how to install and use the Avamar plug-in for VMware vSphere Web Client to back up and restore VMware image backups on an Avamar server.

Audience

This document is intended for Avamar server administrators who manage VMware environments and are responsible for backing up and restoring VMware images.

Revision history

The following table presents the revision history of this document.

Revision	Date	Description
01	November 15, 2019	GA release of Avamar 19.2

Related documentation

The following publications provide additional information:

- *Avamar for VMware User Guide*
- *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection
- *Avamar Release Notes*
- *Avamar Administration Guide*
- *Avamar Operational Best Practices Guide*

Special notice conventions used in this document

These conventions are used for special notices.

DANGER Indicates a hazardous situation which, if not avoided, results in death or serious injury.

WARNING Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE Addresses practices that are not related to personal injury.

Note: Presents information that is important, but not hazard-related.

Typographical conventions

These type style conventions are used in this document.

Table 1 Typographical conventions

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

Where to get help

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

To access the Avamar support page:

1. Go to https://www.dell.com/support/home/us/en/19.
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.

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

CHAPTER 1

Introduction

This chapter includes the following topics:

- Avamar Plug-in for vSphere Web Client 10
- How Avamar works with VMware 10

Avamar Plug-in for vSphere Web Client

The Avamar Plug-in for vSphere Web Client (Avamar plug-in through vSphere Client) is an Avamar-integrated VMware plug-in that provides an easy to use interface for backing up and restoring VMware image-level backups through a vSphere Web Client. The Avamar plug-in for vSphere Web Client supports image level backup and restore for multiple vCenters.

Note: The Avamar AUI is only supported in stand-alone Windows and Linux environments only.

The optional Data Protection Restore Client provides support for file-level recoveries from inside the VMware guest operating systems within a single vCenter. Before performing file-level recoveries within the VMware guest operating systems, run the following script on the Avamar server:

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

The Avamar Plug-in for vSphere Web Client requires Avamar Proxies to be installed and configured. See the *Avamar for VMware User Guide* for additional details on Avamar Proxy installation and configuration.

Note: NAT network connections between the Avamar utility node and the vCenter are not supported.

How Avamar works with VMware

There are two ways to back up and restore VMware data with Avamar software:

- Guest backup and restore
- Image-level backup and restore

The following sections describe the differences between image-level backups and guest-level backups. The Avamar plug-in for vSphere Web Client only supports image-level backups. Avamar Administrator supports guest backup and restores and image-level backup and restores.

Guest backup and restore

With guest backup and restore, you install an Avamar file system client on each virtual machine. Avamar considers each virtual machine to be a separate client, and you can perform individual backups of each virtual machine.

If databases or specific applications, such as Microsoft Exchange or Microsoft SharePoint, are running on the virtual machine, then you can use an Avamar plug-in to protect the application data.

Image-level backup and restore

Avamar for VMware image-level backups and restores use VMware vStorage API for Data Protection (VADP).

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

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

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

Supported configurations

The following storage architectures are supported:

- Fibre Channel Storage Area Network (SAN) storage hosting VMware File System (VMFS) or Raw Device Mapping (RDM)
- iSCSI SAN storage
- Network File System (NFS)

The image backup process requires temporary creation of a VMware virtual machine snapshot. If the virtual machine is running at the time of backup, this snapshot can impact disk I/O and consume space on the VMware vmfs datastore. Snapshot creation and deletion can take a long time if the virtual machine runs a heavy disk I/O workload during backup.

This requirement also limits the types of virtual disks that are supported to the following:

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

Guest and image-level backup and restore comparison

The following table provides a comparison of guest and image-level backup and restore of VMware data.

Table 2 Comparison of guest and image-level backup and restore

Criterion	Guest backup and restore	Image-level backup and restore
Supported guest OS	All guest operating systems that VMware supports, through the use of Avamar File System clients	All guest operating systems that VMware supports
Avamar software installation	Avamar File System client and optional application plug-in on each virtual machine	Avamar proxy virtual machines on the ESXi host
Avamar server network connection	Required for each virtual machine	Required only for the ESXi host
Deduplication	Data within each virtual machine	Data at image-level
OS consistent	Yes	Yes
Application consistent	Yes	Yes if the guest OS has VMware Tools that are installed
Application-aware backup and restore	Yes, through Avamar plug-ins for applications	No
Virtual machine status for backup	Virtual machine must be running	Virtual machine does not need to be running

Table 2 Comparison of guest and image-level backup and restore (continued)

Criterion	Guest backup and restore	Image-level backup and restore
Backup consumption of CPU, RAM, and disk resources	On the virtual machine	On the ESXi host
Backup customization, including exclusion of certain files or file types	Yes	Yes
Backup of unused file system space	No	Yes
Restore of individual files and folders	Yes	Yes
Disaster recovery requirements	Two-step recovery: 1. Load a known good operating system image on the virtual machine. 2. Restore backup data from Avamar.	One-step restore of backup data from Avamar. However, backups may be a "crash-consistent" snapshot of the full virtual machine image, which might not reliably support a full system restore without data loss.

Changed block tracking

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

Changed block tracking identifies unused space on a virtual disk during the initial backup of the virtual machine, and also empty space that has not changed since the previous backup. Avamar data deduplication performs a similar function. However, using this feature provides valuable I/O reduction earlier in the backup process. Changed block tracking dramatically improves performance if SAN connectivity is not available.

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

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

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

- Virtual machine versions 7 and later
- RDM disks are only supported in virtual compatibility mode. Physical compatibility mode is not supported.
- The same disk cannot be mounted by multiple virtual machines.
- Virtual machines must be configured to support snapshots.

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

- Power on
- Resume after
- Suspend
- Snapshot create
- Snapshot delete
- Snapshot revert

CHAPTER 2

Configuring the Avamar Plug-in for vSphere Web Client

This chapter includes the folllowing topics:

- Avamar server configuration 16
- Register the Avamar Plug-in for vSphere Web Client 16
- Access the Avamar Plug-in for vSphere Web Client 18
- Configure localization for the Data Protection Backup and Recovery File-Level Restore UI .. 20

Avamar server configuration

The Avamar Plug-in for vSphere Web Client is supported in both Avamar Virtual Edition (AVE) and physical Avamar server environments.

The Avamar server must be installed and configured to support VMware image-level backups before the Avamar Plug-in for vSphere Web Client can be used. The *Avamar for VMware User Guide* contains detailed instructions for configuring an Avamar server to support VMware image-level backups.

Register the Avamar Plug-in for vSphere Web Client

After you install Avamar and complete Avamar VMware configuration, register the Avamar Plug-in for vSphere Web Client services with vCenter.

Procedure

1. To start the Avamar Web User Interface, 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 **System**.

   The **System** window is displayed.

3. Click the **Certificate** tab, and perform the following steps:

   a. Click **+IMPORT CERTIFICATE** under the **Trust Certificate** tab.

   The **Import Certificate** dialog box is displayed.

   b. In the **Alias** field, type the name of the vCenter to which the certificate belongs.

   c. To locate and select the certificate, click **Browse**, and then click **NEXT**.

   The **Validation** pane is displayed.

   d. (Optional) To validate the certificate, select the checkbox, and then complete the following steps:

   - In the **IP** field, type the IP address of the vCenter.
   - In the **Port** field, type the port number.
   - Click **Validate**, and then click **FINISH**.

   e. Click **FINISH**.

4. Click the **VMware Plug-in** tab.

5. Locate the vCenter to register with Avamar.

   If the vCenter is not listed, verify that you configured the vCenter for Avamar VMware backups through the Avamar Web User Interface.

6. Enable services:

   a. Click the ⋮ button for that vCenter.

   b. Select **Register**.

      After registration, the **Registered** status changes from false to true.

   The Avamar Plug-in for vSphere automatically registers with the vCenter and becomes available through the vSphere Client.

Unregister the Avamar Plug-in for vSphere Web Client and disable services

If you decide that you no longer want to use the Avamar plug-in for the vSphere Web Client, you can unregister the plug-in and remove the plug-in from vCenter.

Before you begin

Note: The flash-based vCenter plug-in from Avamar releases previous to 7.5.1 is no longer supported. If you upgraded the Avamar server to release 7.5.1 from a previous release and the flash-based plug-in was configured in the previous release, remove the flash-based plug-in from the vCenter managed objects (for example, https://<vcenter_ip>/mob/). To remove the plug-in from vCenter managed objects, go to **Contents** > **ExtensionManager** and copy the plug-in name. Click **UnregisterExtension**, and then paste the plug-in name to unregister.

Procedure

1. To start the Avamar Web User Interface, 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 **System**.

   The **System** window is displayed.

3. Click the **VMware Plug-in** tab.

4. Select the vCenter server.

5. To disable services, click the ⋮ button for that vCenter, and then select **unregister**.

   The Avamar Plug-in for vSphere automatically unregisters from the vCenter and is no longer available through the vSphere Client.

Access the Avamar Plug-in for vSphere Web Client

The Avamar Plug-in for vSphere Web Client is accessed through a web browser and the vSphere Client.

About this task

In order for the Avamar plug-in to be displayed in the vSphere Client homepage, the web client user must log in with the same or greater VC permission as the "dedicated vCenter user account" defined in the *Avamar for VMware User Guide*.

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.

Access the plug-in by using Avamar Web User Interface

Procedure

1. To start the Avamar Web User Interface, 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.

   The **Login** window is displayed.

2. Select **vCenter** as the **Auth Type**.
3. In the **vCenter Username** field, type the name of the dedicated vCenter user.
4. In the **vCenter Password** field, type the password for the dedicated vCenter user.
5. In the **vCenter Server** field, type the IP address or DNS name of the vCenter server to log in to.
6. Click **Log In**.

   The AUI dashboard is displayed.

7. To open the navigation pane from anywhere in the UI, click ≫.

   The navigation pane opens and displays the available menu items.

Access the plug-in by using the vSphere Client

Procedure

1. From the vSphere Client, click **Menu** > **Dell EMC Avamar**

   The Avamar Plug-in for vSphere Web Client dashboard is displayed.

2. To browse to another location in the UI, click an icon in the navigation pane.

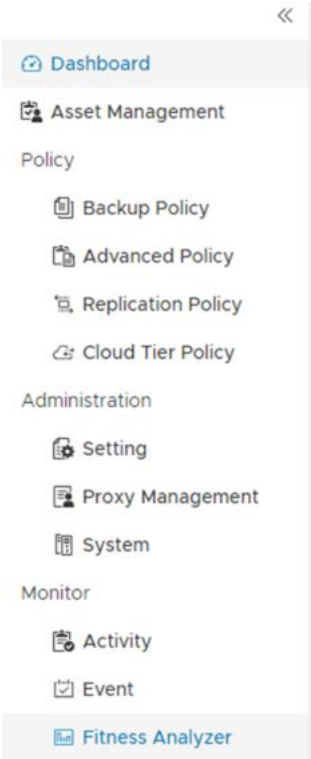
   This action opens the menu item in the main window.

AUI navigation pane

Use the left navigation pane to quickly browse to different panes in the UI. The navigation pane provides links that open other panes to perform tasks in the Avamar Web User Interface.

To open the navigation pane from anywhere in the UI, click ≫. The navigation pane opens and displays the available menu items, as shown in the following illustration.

Figure 1 AUI navigation pane



To browse to another location in the UI, click a link in the navigation pane. This action opens the menu item in the main window.

The links provide access to the following features in the AUI:

Table 3 AUI navigation pane

Navigation link	Icon	Available features
Dashboard		Provides an at-a-glance view of Avamar system status.
Asset Management		Provides the ability to manage Avamar domains and client-related operations: • Create, edit, delete, and refresh Avamar domains. • Add, edit, delete, and sync clients on the Avamar server. • Backup and restore clients.
Backup Policy		Automates backups and enforces consistent rules and system behavior across an entire segment, or group of the user community. The dataset, schedule, and retention policy comprise the backup policy. The backup policy controls backup behavior of all members of the backup policy.
Advanced Policy		Manages application consistent SQL virtual machine backups, including automatic SQL discovery, automatic backup group management, and automatic client SQL

Table 3 AUI navigation pane (continued)

Navigation link	Icon	Available features
		plug-in installation and registration, In an advanced policy, you can also enable the Cloud DR function for SQL virtual machine backups.
Replication Policy		Copies client backups from the source Avamar system to an alternate destination. Replicating backups to an alternate destination protects against data loss if the source Avamar system fails.
Cloud Tier Policy		Moves Avamar backups from Data Domain to the cloud and performs seamless recovery of these backups.
Settings		Assists administrators with adding accounts to the system, and creating and managing schedules, datasets, retention policies, and rules.
Proxy Management		Assists administrators with deploying and managing Avamar proxies 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.
System		Assists administrators with configuring vCenter-to-Avamar authentication, registering the Avamar Plug-in for vSphere Web Client, and adding a Data Domain system to Avamar.
Activity		Provides status and detailed information for backup and replication jobs.
Event		Monitors operational status and server activity. Examples of Avamar events include client registration and activation, successful and failed backups, and hard disk status.
Fitness Analyzer		Opens the Fitness Analyzer portal that provides advanced server reporting and analysis functionality.

Configure localization for the Data Protection Backup and Recovery File-Level Restore UI

Avamar provides localization support for the Data Protection Backup and Recovery File-Level Restore UI.

About this task

To select a language for the UI, complete the following steps:

Procedure

1. In the header pane, click the icon.
2. Select a language from the drop-down list:
   - English

- Simplified Chinese
- Japanese

A confirmation message is displayed.

3. Click **Yes**.

CHAPTER 3

Using the Avamar Plug-in for vSphere Web Client

This chapter includes the following topics:

- Avamar setup 24
- Managing backup policies 24
- AUI Activity Monitor 26
- Manage clients 32
- Managing rules 35
- Proxy Deployment 38

Avamar setup

Prior to using the Avamar Plug-in for vSphere Web Client, Avamar Administrator must be configured with the following:

- Create a schedule
- Create a retention policy
- Create a group in the Virtual Machines domain
- Select proxies to protect virtual machines in the group
- Configure a data set for each VMware Image Dataset or for all virtual disks

Refer to the *Avamar Administration Guide* for details on Avamar policy configuration.

The best practice is to name the Avamar group with a descriptive name (for example, Backup everyday 2 week retention) which provides the VMware administrator with information about the Avamar policy configuration.

After changes are made in Avamar Administrator, use the **Refresh** icon to update changes in the Avamar Plug-in for vSphere Web Client.

Managing backup policies

The **Policies** page provides access to backup policy tasks and information.

The **Policies** page includes a summary of each backup policy on the selected Avamar server.

Backup policy objects contain the following child objects:

- Schedule—when a scheduled backup is performed
- Retention—how long the backup is stored in the backup appliance
- Dataset—optional backup parameters
- Members—add and remove clients from a backup policy

Start an on-demand backup of a backup policy

Protecting an instance assigns the instance to a particular backup policy. You can assign more than one backup policy to an instance.

Procedure

1. In the AUI navigation pane on the left, click ≫, and then click **Backup Policy**.

   The **Policy** page appears.
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, and then click **START BACKUP**.

   The instance receives protection that is based on the schedule and retention period that are specified in the backup policy.

Edit a backup policy

You can edit a backup policy, including setting properties and adding or modifying members, datasets, schedules, and retention.

Procedure

1. In the AUI navigation pane on the left, click ≫, and then click **Backup Policy**.

   The **Policy** page appears.
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, and then click **Edit**.

   The **Policy** wizard is displayed where you can modify the required backup policy settings.

Add members to a backup policy

From the **Members** page of the **Policy** wizard, you can configure backup policy attributes, including applying the backup policy to selected clients or removing a backup policy from selected clients.

About this task

To access the **Members** page of the **Policy** wizard, in the AUI navigation pane on the left, click ≫, click **Backup Policy**.

Complete the following steps from the **Members** pane of the **Policy** wizard.

Procedure

1. In the domain tree, select the domain for the backup policy.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
2. To add a client to a backup policy:

   a. In the list of clients, select the checkbox next to the client that you want to add.

      The client displays with a blue check mark and a status of **Included by User**.
      For a virtual machine backup policy under the vCenter domain, you can also select **Enable Dynamic Rule** and then choose an existing rule from the list, or create a rule to apply to virtual machines that you want to automatically include in the policy. When a client is dynamically included in the policy, the client displays with a green check mark and a status of **Included by Rule**. The *Avamar for VMware User Guide* provides more information about dynamic rules.

   b. Click **NEXT**.

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

3. To remove a client from a backup policy:

   a. In the list of clients, select the X next to the client that you want to remove. The client displays with a status of **Excluded**.

   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.

4. To add a dataset to a backup policy and complete the wizard, click **NEXT**.

   The **Dataset** pane appears.

Edit policy attributes

You can edit attributes for a policy, including the schedule, retention, dataset, and rules.

About this task

Perform the following steps from the **Attributes** window of the **Policy** wizard.

Procedure

1. In the AUI navigation pane on the left, click ≫, and then click **Backup Policy** .

   The **Policy** page appears.
2. In the domain tree, select a domain or subdomain for the client.

   To select a subdomain client, toggle the **Include Sub-domain** switch to on.
3. Select a policy from the list, click ⋮ , and then click **Edit**.

   The **Properties** pane appears.
4. Click **Next**.

   The **Attributes** pane appears.
5. In the **Select Existing Schedule** field, select a schedule type.
6. In the **Select Existing Retention** field, select a retention type.

   Editing an existing retention period allows you to change how long the backup data resides on the protection provider.
7. In the **Select Existing Dataset** field, select a dataset.

   Editing a dataset allows you to change the specific data that is protected.
8. To enable rules, in the **Enable Rule** field, select the check box.

   Rules are used to automatically map auto-discovered virtual machines to domains, and to assign backup policies to auto-discovered virtual machines.
9. In the **Rules** field, select a predefined rule.
10. Click **NEXT**.

    The **Members** window appears.

AUI Activity Monitor

The **Activity Monitor** in the Avamar Web User Interface enables you to monitor backup, restore, backup validation, and replication activity. To perform analysis or troubleshooting, you can view a detailed log of a client session.

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:
  - Completed
  - 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 .

Activity Monitor details

The following tables provide details on the information that is available in the Avamar Web User Interface **Activity Monitor**.

Table 4 Session details available in the Activity Monitor

Field	Description
Status	Status of the backup, restore, or validation activity.
Error Code	If the activity did not successfully complete, a numeric error code appears. To view a detailed explanation, double-click the error code.
Start Time	Date and time that this activity began, adjusted for the prevailing time zone, which is shown in parentheses. Daylight Savings Time (DST) transitions are automatically compensated.
Elapsed Time	Elapsed time for this activity.
End Time	Date and time that this activity completed, adjusted for the prevailing time zone, which is shown in parentheses. Daylight Savings Time (DST) transitions are automatically compensated.
Type	Type of activity. The Avamar Administrator online help provides details on each type.

Table 4 Session details available in the Activity Monitor (continued)

Field	Description
Server	Server on which the activity occurred, either the Avamar server or a Data Domain system.
Progress Bytes	Total number of bytes examined during this activity.
New Bytes	Percentage of new bytes backed up to either the Avamar server or a Data Domain system. Low numbers indicate high levels of data deduplication.

Table 5 Client details available in the Activity Monitor

Field	Description
ID	The unique identifier for the Avamar client.
Client	Avamar client name.
Domain	Full location of the client in the Avamar server.
OS	Client operating system.
Client Release	Avamar client software version. If this activity is a VMware image backup or restore, then this value is the Avamar client software version running on the image proxy client.

Table 6 Policy details available in the Activity Monitor

Field	Description
Sched. Start Time	Date and time that this activity was scheduled to begin.
Sched. End Time	Date and time that this activity was scheduled to end.
Elapsed Wait	Total amount of time that this activity spent in the activity queue. That is, the scheduled start time minus the actual start time.
Policy	Group that started this activity. One of the following values: • If the activity was a scheduled backup, the group that this client was a member of when this scheduled activity started. • **On-demand** is shown for other backup, restore, and validation activities. • If the activity was a scheduled replication, then this value is the replication group.

Table 6 Policy details available in the Activity Monitor (continued)

Field	Description
	• **Admin On-Demand Group** is shown for-demand replication activities.
Plug-in	Plug-in that is used for this activity.
Retention	Retention types that are assigned to this backup. One or more of the following values: • **D**—Daily • **W**—Weekly • **M**—Monthly • **Y**—Yearly • **N**—No specific retention type
Schedule	If the activity was a scheduled backup, the schedule that began this activity. On-Demand or End User Request is shown for all other activities that are started from Avamar Administrator or the client, respectively.
Dataset	Name of the dataset that is used to create the backup. If the activity is a replication job, this column lists the source system name on the destination system, and the destination name on the source system.
WID	Work order ID. Unique identifier for this activity.

Monitor backups

You can monitor backups to ensure a successful completion of restores and troubleshooting of issues. The **Activity Monitor** in the Avamar Web User Interface enables you to view status information for backups.

Procedure

1. In the AUI navigation pane on the left, click ≫, and then click **Activity**.

   The **Activity Monitor** appears with a list of all activities.
2. To filter the results to display only backup activity:

   a. Click ▼ next to the **Activity** column.

   b. Type `On-Demand Backup`.

   c. Press **Enter**.

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.

Procedure

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**.

Restart a backup job

You can restart a completed or failed backup job in the **Activity Monitor** of the Avamar Web User Interface.

Procedure

1. In the AUI navigation pane on the left, click ≫, and then click **Activity**.

   The **Activity Monitor** appears with a list of all activities.
2. Select a backup job in the list, and then click **RESTART**.

   A confirmation dialog box appears.
3. Click **YES**.

Results

The message **Restarted job successfully** will be displayed on the screen.

View a detailed client session log

The **Activity Monitor** in the Avamar Web User Interface enables you to view a detailed log of a client session to perform analysis or troubleshooting.

About this task

For replication sessions, Dell EMC recommends that you review the client logs on the replication source server.

Procedure

1. In the AUI navigation pane on the left, click ≫, and then click **Activity**.

   The **Activity Monitor** appears and displays a list of all activities.
2. Select an activity from the list, and then click **VIEW LOGS**.

   The Log details window appears. By default, the Activity Monitor displays a detailed log of all client backup activity for the past 72 hours.
3. To filter the content based on a search string, in the search field, type the string.
4. To download the log file, click **Download**.

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:
  - Completed
  - 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.

Procedure

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**.

Monitor replication in the AUI

The **Activity** window in the AUI enables you to view status information for both on-demand and scheduled replication activity.

Procedure

1. In the AUI navigation pane on the left, click ≫, and then go to **Monitor** > **Activity**.

   The **Activity Monitor** appears and displays a list of all activities. Replication jobs indicate **Replication Source** in the **Activity** column. Additionally, you can filter the view to display only replication jobs.

2. To filter the results to display only replication activity:

   a. Click ▼ next to the **Activity** column.

   b. Type `Replication Source`.

Cancel a replication task

You can cancel a policy-based replication task in the Activity Monitor any time before it completes. The cancellation might take 5 minutes or longer. The replication may complete before the cancellation finishes.

Procedure

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 replication task from the list.
3. Click **CANCEL**.

   A confirmation dialog box appears.

4. Click **YES**.

Manage clients

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

In the **Asset Management** window, you can add or remove a client, and edit client information.

Add a VMware client

Procedure

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
2. In the **Domain** tree, select a vCenter domain or a subdomain for the client.
3. Click **ADD CLIENT**.

   The **Select VMware Entity** window displays.

4. You can toggle the vCenter hierarchy view in the left pane to list containers by vSphere virtual machines and templates, or by vSphere hosts and clusters.

   - To view by vSphere virtual machines and templates, keep or move the **VM/Tempate** slider to the left. This is the default setting.
   - To view by vSphere hosts and clusters, move the **VM/Tempate** slider to the right. The name changes to **Host/Cluster**.

Note: Resource pools are only visible in the **Host/Cluster** view.

5. In the left pane, expand and select a container in the vCenter.

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

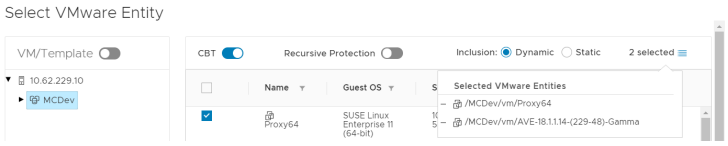
   The VMware entities for the selected object display in a table in the right pane.

6. Select the checkbox next to any folder, resource pool, virtual machine, or vApp in the right pane. Use the filter icons in the **Guest OS**, **Server** and **Location** columns to quickly locate the entity you want to add.

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

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

   Figure 2 Selected VMware Entities drop-down



   Note: The checkbox next to an entity will be disabled in the following cases:

   - The entity has already been added as a client.
   - The entity is the AVE.
   - The entity is a VMware proxy.
   - The entity is a datacenter.
   - The entity is an ESX host.

7. (Optional) When adding a container, select from one of the **Inclusion** options in the right pane:

   - Select **Dynamic** to make this a dynamic container
   - Select **Static** to make this a static container.

8. To enable changed block tracking, move the **CBT** slider to the right/ON position.

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

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

   - Reboot
   - Power on
   - Resume after suspend
   - Migrate

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

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

10. Click **SUBMIT**.

After you finish

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

- Reboot
- Power on
- Resume after suspend
- Migrate

Delete a VMware client

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

About this task

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

Procedure

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

Procedure

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**.

Managing rules

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

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

Create a rule

Rules are used by the Avamar server for domain map and automatic backup policy assignment for autodiscovered VMs.

About this task

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

Procedure

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

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

   This selection allows you to configure multiple different filters to select VMs, and to determine how these filters interact with one another to select the correct virtual machines.

For example, you might create a filter that uses a virtual machine folder path to select virtual machines, and another filter that uses a virtual machine naming convention.

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

- To include only virtual machines that are in the defined folder path and also follow the naming convention, select **All**.
  This step excludes virtual machines that are in the folder path but that do not follow the naming convention. It also excludes virtual machines that follow the naming convention but are not in the folder path
- To include any virtual machines that are either in the virtual machine folder path or that follow the naming convention, select **Any**.

7. To add a filter:
   a. Click +.
      This step adds a row to the list of filters.
   b. In the **Filter** column, select a filter type.
      For example, to create a filter that uses a virtual machine naming convention, select **VM Name**, or to create filter that uses a vCenter VM Tag, select **VM Tag**.
   c. In the **Operator** column, select the operand.
      For example, if VM Name is selected for the filter type and begins with is selected for the operand, then all virtual machines whose names begin with the filter text is selected.
   d. In the **Value** column, type the filter text.
      For example, to create a filter that selects all virtual machines whose names begin with the text string **HR_**, select **VM Name** for the filter type, begins with for the operand, and type **HR_** for the filter text.
8. To create additional filters, click +.
   This step adds a row to the list of filters.
9. To delete an existing filter, click **Delete**.
10. Click **SUBMIT**.
    Changes made to tags may experience a delay of up to 12 hours before being enforced. For this reason, edit tags with caution, or perform a synchronized vCenter operation, which automatically synchronizes the vCenter with the Avamar server.

Edit a rule

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

Procedure

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

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

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

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

   - To include only virtual machines that are in the defined folder path and also follow the naming convention, select **All**.
     This step excludes virtual machines that are in the folder path but that do not follow the naming convention. It also excludes virtual machines that follow the naming convention but are not in the folder path.
   - To include any virtual machines that are either in the virtual machine folder path or that follow the naming convention, select **Any**.

7. To add a filter:

   a. Click +.

      This step adds a row to the list of filters.

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

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

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

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

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

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

8. To create additional filters, click +.

   This step adds a row to the list of filters.

9. To delete an existing filter:

   a. Select the filter.

   b. In the Actions column, click **Delete**.

10. Click **SUBMIT**.

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

Delete a rule

Procedure

1. In the AUI navigation pane on the left, click », and then click **Settings**.
2. Click the **Rule** tab.

3. In the domain tree, select a vCenter domain or subdomain for the client.
4. In the **Setting** page, complete the following tasks:
   a. Select a rule from the list.
   b. Click **DELETE**.

Proxy Deployment

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

Proxy Deployment 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.

Procedure

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 by setting `keep_deploy_failed_proxy = Tru`.

Security patch updates for proxies

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

Best practices and troubleshooting for applying security patch updates to proxies

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

Best practices

- Security updates are only supported for proxies that are managed by the **Proxy Deployment Manager**. For a manually deployed proxy, use the `initproxyappliace.sh` option to register a manually deployed proxy with the **Proxy Deployment Manager**. Older versions of Avamar do not support this form of patching.
- Avamar 19.1 adds support for the package installation tracking feature. Proxy installations from previous releases are not traceable. Dell EMC recommends that you deploy or update proxies to the most recent version by using the proxy upgrade functionality in the **Proxy Deployment Manager**.
- If you update the VAMI or the registered VAMI service (AVAMAR provider: `AvamarVMwareCombined-CIM-linux-sles12sp1-x86_64-`*`version`*`.rpm`), ensure that you manually restart the `vami-sfcb` service on the proxy.

Troubleshooting

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

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

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

```
http:
multipart:
```

```
max-file-size:50000MB
max-request-size:500000MB
```

- If a proxy virtual machine was deleted or powered off from a VMware-side application such as the **vSphere Client**, the proxy is removed from the **Proxy Deployment** tab in the AUI **Proxy Deployment Manager** window. However, the proxy list in the **Proxy Patches** tab still lists the proxy.

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

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

Apply security patch updates to a proxy

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

Before you begin

Review the information in Best practices and troubleshooting for applying security patch updates to proxies on page 42.

Procedure

1. Download the patch files from the provided location.
2. Log in to the AUI or the vSphere Web Client as an administrator.
3. Go to **Proxy Management** > **Proxy Patches**.
4. In the **Available Patches** pane, click **UPLOAD...**

   The **Upload Proxy Patches** dialog displays.
5. Click **BROWSE....** to go to the location of the patch files, and then select the files that you want to upload to the Avamar server patch folder.

   When finished, click **UPLOAD** to save the selections and exit the dialog box. The **Available Patches** pane shows the selected patch files.
6. Select the radio button for the specific patch that you want to apply to the proxy.

   Note: To remove unavailable patch files from this pane, select the file and then click **DELETE**.
7. From the **Proxies List** pane, select the checkbox for the proxy on which you want to install the patch file, and then click **INSTALL PATCH**.

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

Results

An informational message indicates the status of the patch application:

- `Success` indicates that the patch was successfully installed.
- `Success, reboot required` indicates that the patch was successfully installed, but that you must reboot the proxy.
- `Success, restart vami-sfcb service required` indicates that the patch was successfully installed, but that you must restart the `vami-sfcb` service.

- `Failed (view error)` indicates that the patch was not installed. Click the **View Error** link to determine why the failure occurred.
- `Already install, bypass` indicates that this patch is already installed on this proxy.

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

CHAPTER 4

Backup and Recovery

This chapter includes the following topics:

- Perform an on-demand backup of a virtual machine by using AUI 46
- Restore an instance of a VM backup by using the AUI 51
- File-level restore 56

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.

Procedure

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.

   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.

Before you begin

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

Procedure

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**.

   Note: Indexing VMware image backups using the Data Protection Search software is only supported with HotAdd transport mode.

5. To exclude the Windows page file (`pagefile.sys`) from the backup, select **Exclude page file blocks when performing image backup on Windows VM**.

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

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

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

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

8. To store this backup on a Data Domain system, select the **Store backup on Data Domain System** checkbox, then select a Data Domain system from the list.
9. From the **Encryption method to Data Domain system** list, select the encryption method to use for data transfer between the client and the Data Domain system during the backup.

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

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

VMware Image backup plug-in options

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

Table 7 Backup options for Avamar VMware Image plug-in

Setting	Description
Use Changed Block Tracking (CBT) to increase performance	If selected, the VMware changed block tracking feature is used to identify areas of the virtual machine file system that have changed since the last backup and only process those changed areas during the next backup. **Note:** Changed block tracking must be enabled at the virtual machine level in order for this feature to work.
Set Annotionation Tag LastBackupStatus and LastSuccessfulBackup	If selected, enables the Avamar server to report information to the vSphere Web Client or the legacy Windows-based vSphere client about the most recent backup and most recent successful backup. When selected, the following information is displayed in the Annotation list of the vSphere Web Client: • **LastSuccessfulBackupStatus-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.
Exclude page file blocks when performing image backup on Windows VM	If selected, excludes the Windows page file (`pagefile.sys`) from the backup for all the partitions. It is not limited to primary partitions. **Note:** Page file exclusion is supported only for Windows Servers version 2008 R2 and above. For client versions of Windows, this option has no effect; the page file is included in backups of Windows clients, regardless of this setting. **Note:** The proxy uses NBD transport mode internally in order to read the page file blocks. After recognizing the required blocks, the available mode (hotadd/nbdssl/nbd) will be used accordingly for backup or restore operations.

Table 7 Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
Exclude deleted file blocks when performing image backup on Windows VM	If selected, excludes the deleted file blocks from the backup for all the partitions. It is not limited to primary partitions.
Exclude files with path and filter	Excludes the files with path and filter from the backup for all the partitions. It is not limited to primary partitions. Type the full path of the file or folder or the filter path of the files and folders. Separate multiple entries with a comma. To exclude files with path and filter, type the path in the following format: • Start with driver letter • End with "/" to exclude a folder • End without "/" to exclude a file • Use "*" as a wildcard in the filename to exclude all files. Do not use "*" as a wildcard in the file path. For example: ▪ `*:/*/*.TXT` is not supported. ▪ `D:/folder/*.txt` is supported. ▪ `D:/folder/*` is supported.
Store backups on Data Domain system	To store the backup on a Data Domain system instead of the Avamar server, select the checkbox and then select the Data Domain system from the list. **Note:** To enable this option, add a Data Domain system to the Avamar configuration. The *Avamar and Data Domain System Integration Guide* provides instructions.
Encryption method to Data Domain system	Specifies the encryption method for data transfer between the client and the Data Domain system during the backup. As of Avamar release 7.5, the only supported encryption method is "high."
Snapshot delete retry	
Max times to retry snapshot delete	The maximum number of times that a snapshot delete operations should be attempted.
Guest credentials	
Username	Guest operating system user account with sufficient privileges to run scripts.

Table 7 Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
Password	Password for the guest operating system username.
Pre-snapshot Script	
Script file	Full path and filename of the script that will be run before the vmdk snapshot.
Maximum script run time (minutes)	Maximum number of minutes this script is allowed to run before timing out.
Post-snapshot Script	
Script file	Full path and filename of the script that will be run after the backup completes and the vmdk snapshot is removed.
Maximum script run time (minutes)	Maximum number of minutes this script is allowed to run before timing out.
Snapshot quiesce timeout	
Snapshot quiesce timeout (minutes)	Maximum number of minutes to wait before the snapshot quiesce operation is considered to have failed (Windows WMware Image plug-in only)
Microsoft SQL Server authentication	
NT Authentication	Uses the credentials that are entered in Guest Credentials for authentication. User must have administrative privileges and must have write permissions for the files system and read permissions for the Windows registry.
Application Authentication	Uses the SQL Server Username and SQL Server Password to log into the SQL server.
Microsoft SQL Server post action	
Post Action Timeout (minutes)	Maximum number of minutes to wait before post-action operations are considered to have failed. Default is 900 seconds.
Post Action Type of MSSQL	The type of post-action operation to perform. The only available option is LOG Truncation, which performs log truncation after the backup has been performed. When backing up a single VM, all disks of the VM must be selected or log truncation will not occur.

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.

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**.

Procedure

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**.

    The **Summary** pane is displayed.

13. In the **Summay** pane, review the provided information, and then click **FINISH**.

    The following status message is displayed:

    ```
    Restore request initiated.
    ```

Restore data to a different virtual machine

About this task

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

Procedure

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 **Summay** pane, review the provided information, and then click **FINISH**.

    The following status message is displayed:

    ```
    Restore request initiated.
    ```

Restore data to a new virtual machine

About this task

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

Procedure

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 new Virtual Machine**.

b. In the **Post Restore Options** field, select an option.

c. To use Changed Block Tracking (CBT) to increase performance, select **Use CBT to increase performance** check box.

d. In the **Proxy** field, select an option.

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

The **Advanced Config** page appears.

9. In the **Advanced Config** pane, complete the following steps:

   a. In the **vCenter** field, select a vCenter.

   b. In the **VM Name** field, type the name of the virtual machine.

   c. Click **NEXT**.

10. In the **Location** pane, complete the following steps:

    a. Expand the domain name, and then select a destination.

    The selected location appears.

    b. Click **NEXT**.

11. In the **Host/Cluster** pane, complete the following steps:

    a. Expand the domain name, and then select a host or cluster.

    The selected IP address appears.

    b. Click **NEXT**.

12. In the **Resource Pool** pane, complete the following steps:

    a. Expand the domain name, and then select a resource pool.

    The selected resource pool appears.

    b. Click **NEXT**.

13. On the **Datastore** pane, complete the following steps:

    a. Select a datastore.

    b. Click **NEXT**.

14. Click **NEXT**.

    The **Summary** pane is displayed.

15. In the **Summay** pane, review the provided information, and then click **FINISH**.

    The following status message is displayed:

    ```
    Restore request initiated.
    ```

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.

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 8 FLR support partitioning scheme

Partitioning scheme	Guest OS	FLR	Comment
MBR	Windows/Linux	Supported	
EBR (Logical Partition)	Windows/Linux	Supported	
GPT	Windows/Linux	Partial support	Support BTRFS and LVM base on GPT in Linux
MixedGPT	Windows/Linux	Not supported	Hybrid MBR

File system support

The following table outlines the file system support for FLR.

Table 9 File system support for FLR

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

LVM support

The following table outlines the LVM support for FLR.

Table 10 LVM support for FLR

LV type	FLR
Linear LV	Support
Striped LV	Support

Table 10 LVM support for FLR (continued)

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

Multi-device support

The following table outlines multi-device support for FLR.

Table 11 Multi-device support for FLR

RAID	Occur	FLR
RAID 0/Striping	LVM/BTRFS	Support
RAID 1/Mirroring	LVM/BTRFS	Support
RAID 4	LVM	Support
RAID 5	LVM	Support
RAID 6	LVM	Support
RAID10	LVM/BTRFS	Support

File level restore troubleshooting and limitations

Review the following information related to file level restore troubleshooting and limitations:

File level restore limitations

Note the following limitations to file level restore support:

- You cannot restore or browse symbolic links.
- Browsing either a specified directory that is contained within a backup or a restore destination is limited to 50,000 files or folders.
- Restore is limited to 20,000 objects (files or folders) in the same restore operation.
- You can restore files from a Windows backup only to a Windows machine, and files from a Linux backup only to a Linux machine.
- 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: `/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`:

```
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.

RSA 2FA verification errors

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

File-level restore in the AUI

The file level restore (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.

Before you begin

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. It does not support Domain users.
- 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**.

Procedure

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.

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

   a. To select a client, perform the following steps:

      a. Click **SELECT CLIENT**.
      The **Select Client** pane appears.

      b. In the Domain tree, select a domain for the client.

      c. In the **Client** pane, choose a destination client.

      d. Click **OK**.

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

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

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

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

> **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.

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

8. Click **NEXT**.

   The **Summary** pane is displayed.

9. In the **Summay** pane, review the provided information, and then click **FINISH**.

   The following status message is displayed:

   ```
   Restore request initiated.
   ```

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.

Before you begin

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.

Procedure

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: 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: 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**.

APPENDIX

Plug-in Options

This appendix includes the following topics:

- How to set plug-in options 64
- VMware Image backup plug-in options 64
- VMware Image restore plug-in options 67
- Windows VMware GLR plug-in options 67

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.

NOTICE 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 12 Backup options for Avamar VMware Image plug-in

Setting	Description
Use Changed Block Tracking (CBT) to increase performance	If selected, the VMware changed block tracking feature is used to identify areas of the virtual machine file system that have changed since the last backup and only process those changed areas during the next backup. **Note:** Changed block tracking must be enabled at the virtual machine level in order for this feature to work.
Set Annotionation Tag LastBackupStatus and LastSuccessfulBackup	If selected, enables the Avamar server to report information to the vSphere Web Client or the legacy Windows-based vSphere client about the most recent backup and most recent successful backup. When selected, the following information is displayed in the Annotation list of the vSphere Web Client: • **LastSuccessfulBackupStatus-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.
Exclude page file blocks when performing image backup on Windows VM	If selected, excludes the Windows page file (`pagefile.sys`) from the backup for all the partitions. It is not limited to primary partitions.

Table 12 Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
	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. **Note:** The proxy uses NBD transport mode internally in order to read the page file blocks. After recognizing the required blocks, the available mode (hotadd/nbdssl/nbd) will be used accordingly for backup or restore operations.
Exclude deleted file blocks when performing image backup on Windows VM	If selected, excludes the deleted file blocks from the backup for all the partitions. It is not limited to primary partitions.
Exclude files with path and filter	Excludes the files with path and filter from the backup for all the partitions. It is not limited to primary partitions. Type the full path of the file or folder or the filter path of the files and folders. Separate multiple entries with a comma. To exclude files with path and filter, type the path in the following format: • Start with 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.

Table 12 Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
Encryption method to Data Domain system	Specifies the encryption method for data transfer between the client and the Data Domain system during the backup. As of Avamar release 7.5, the only supported encryption method is "high."
Snapshot delete retry	
Max times to retry snapshot delete	The maximum number of times that a snapshot delete operations should be attempted.
Guest credentials	
Username	Guest operating system user account with sufficient privileges to run scripts.
Password	Password for the guest operating system username.
Pre-snapshot Script	
Script file	Full path and filename of the script that will be run before the vmdk snapshot.
Maximum script run time (minutes)	Maximum number of minutes this script is allowed to run before timing out.
Post-snapshot Script	
Script file	Full path and filename of the script that will be run after the backup completes and the vmdk snapshot is removed.
Maximum script run time (minutes)	Maximum number of minutes this script is allowed to run before timing out.
Snapshot quiesce timeout	
Snapshot quiesce timeout (minutes)	Maximum number of minutes to wait before the snapshot quiesce operation is considered to have failed (Windows WMware Image plug-in only)
Microsoft SQL Server authentication	
NT Authentication	Uses the credentials that are entered in Guest Credentials for authentication. User must have administrative privileges and must have write permissions for the files system and read permissions for the Windows registry.
Application Authentication	Uses the SQL Server Username and SQL Server Password to log into the SQL server.
Microsoft SQL Server post action	

Table 12 Backup options for Avamar VMware Image plug-in (continued)

Setting	Description
Post Action Timeout (minutes)	Maximum number of minutes to wait before post-action operations are considered to have failed. Default is 900 seconds.
Post Action Type of MSSQL	The type of post-action operation to perform. The only available option is LOG Truncation, which performs log truncation after the backup has been performed. When backing up a single VM, all disks of the VM must be selected or log truncation will not occur.

VMware Image restore plug-in options

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

Table 13 Restore options for Avamar VMware Image plug-in

Setting	Description
Use Changed Block Tracking (CBT) to increase performance	If selected, the VMware changed block tracking feature is used to identify areas of the virtual machine file system that have changed since the last backup and only process those changed areas during this restore operation. **Note:** Changed block tracking must enabled at the virtual machine level in order for this feature to work.
Encryption method from Data Domain system	Specifies the encryption method for data transfer between the Data Domain system and the client during the restore. As of Avamar release 7.5, the only supported encryption method is "high."

Windows VMware GLR plug-in options

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

Note: GLR does not support Windows dynamic disks.