EMC® Avamar® Plug-in for vSphere Web Client

Administration Guide

P/N 302-000-856
REV 01

EMC²

PREFACE

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

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

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

Purpose

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

Audience

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

Revision history

The Table 1 presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	June 11, 2014	First release of Avamar 7.1.

Related documentation

The following EMC publications provide additional information:

◆ *EMC Avamar for VMware User Guide*
◆ *EMC Avamar Compatibility and Interoperability Matrix*
◆ *EMC Avamar Release Notes*
◆ *EMC Avamar Administration Guide*
◆ *EMC Avamar Operational Best Practices*

Conventions used in this document

EMC uses the following conventions for special notices:

NOTICE

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

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

IMPORTANT

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

Typographical conventions

EMC uses the following type style conventions in this document:

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

Where to get help

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

To access the Avamar support page:

1. Go to https://support.EMC.com/products.

2. Type a product name in the **Find a Product** box.

3. Select the product from the list that appears.

4. Click the arrow next to the **Find a Product** box.

5. (Optional) Add the product to the **My Products** list by clicking **Add to my products** in the top right corner of the **Support by Product** page.

Documentation

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

◆ Release notes provide an overview of new features and known limitations for a release.

◆ Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.

◆ White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

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

To search the EMC Knowledgebase:

1. Click the **Search** link at the top of the page.

2. Type either the solution number or keywords in the search box.

3. (Optional) Limit the search to specific products by typing a product name in the **Scope by product** box and then selecting the product from the list that appears.

4. Select **Knowledgebase** from the **Scope by resource** list.

5. (Optional) Specify advanced options by clicking **Advanced options** and specifying values in the available fields.

6. Click the search button.

Online communities

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

Live chat

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

Service Requests

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

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

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

Facilitating support

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

◆ ConnectEMC automatically generates service requests for high priority events.

◆ Email Home emails configuration, capacity, and general system information to EMC Customer Support.

Your comments

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

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 that will help us address the documentation issue

CONTENTS

CHAPTER 1
Introduction

The following topics provide an introduction to use the EMC® Avamar® Plug-in for vSphere Web Client to back up and restore data in a VMware environment:

- ◆ "Avamar Plug-in for vSphere Web Client" on page 10
- ◆ "How Avamar works with VMware" on page 10
- ◆ "Changed block tracking" on page 13

Avamar Plug-in for vSphere Web Client

The EMC Avamar Plug-in for vSphere Web Client (called the EMC backup and recovery plug-in through the vSphere Web 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 EMC Data Protection Restore Client provides support for file-level recoveries. For full Avamar backup and restore functionality, use Avamar Administrator.

Note: The Avamar Plug-in for vSphere Web Client supports one vCenter Server per Avamar server. If you need to manage multiple vCenter Servers, use Avamar Administrator.

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

Note: In order to use the Avamar Plug-in for vSphere Web Client, Avamar Administartor must have backup policies configured through Avamar Administator in the VirtualMachines domain. See the *EMC Avamar Administration Guide* for additional details on Avamar policy configuration.

Note: vSphere Data Protection (VDP) and the Avamar Plug-in for vSphere Web Client cannot be installed on the same vCenter Server.

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 using an appliance template (.ova) file.

Supported configurations

◆ The following storage architectures are supported:

• Fiber 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)

Comparing guest and image-level backup and restore

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

Table 1 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 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
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	No
Backup of unused file system space	No	Yes
Restore of individual files and folders	Yes	Yes, through EMC Data Protection Restore Client
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 supports 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, migrate, snapshot create, delete, or revert.

CHAPTER 2
Configuring the Avamar Plug-in for vSphere Web Client

This chapter includes the following topics:

- "Avamar server configuration" on page 16
- "VMware supported software" on page 16
- "Configuring the vcenter-sso-info.cfg file" on page 16
- "Managing the Avamar Plug-in for vSphere Web Client services" on page 17

Avamar server configuration

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 *EMC Avamar 7.0 for VMware User Guide* contains detailed instructions for configuring an Avamar server to support VMware image-level backups.

VMware supported software

The Avamar Plug-in for vSphere Web Client can be used with the following VMware software:

◆ vCenter 5.1 and 5.5 (with associated vSphere Web Client)

◆ ESXi 5.0, ESXi 5.1, and ESXi 5.5

Configuring the vcenter-sso-info.cfg file

The **vcenter-sso-info.cfg** file is used to configure vCenter external SSO (if used) and to select the vCenter to be associated with the Avamar Plug-in for vSphere Web Client if there is more than one vCenter Server registered with the Avamar server.

The **vcenter-sso-info.cfg** file is located in the following directory:

/usr/local/avamar/var/ebr/server_data/prefs/vcenter-sso-info.cfg

The options in the **vcenter-sso-info.cfg** file associated with the Avamar Plug-in for vSphere Web Client are defined in Table 2.

Table 2 vcenter-sso-info.cfg entries for the Avamar Plug-in for vSphere Web Client

vcenter-sso-info.cfg entry	Description
vcenter-sso-hostname=	Required if using external SSO, specifies external SSO hostname.
vcenter-sso-port=	Required if using external SSO, specifies external SSO port.
vcenter-name=	Required to select the vCenter Server for the Avamar Plug-in for vSphere Web Client if there is more than one vCenter Server on the Avamar server.

Managing the Avamar Plug-in for vSphere Web Client services

The following sections describe how to manage the Avamar Plug-in for vSphere Web Client services.

Enabling services on a physical Avamar server

After Avamar is installed and the Avamar VMware configuration is complete, the Avamar Plug-in for vSphere Web Client services must be enabled on the Avamar server.

1. Launch **PuTTY** to open an SSH session with the Avamar server.

2. Log in to Avamar with the **admin** user account.

3. Change to root user with the following command:

   admin@_avamar_server_**:~/>:su -**

4. Provide the root password and press **Enter**.

5. Enter the following command to initiate the Avamar Plug-in for vSphere Web Client services.

   root@_avamar_server_**:~/#:ebrserver.pl --init**

6. An information message appears specifying that initializing the Avamar Plug-in for vSphere Web Client requires a restart of the Tomcat server. Enter **Y** to restart the Tomcat server and start the Avamar Plug-in for vSphere Web Client services.

Enabling services on AVE

After Avamar is installed and the Avamar VMware configuration is complete, the Avamar Plug-in for vSphere Web Client services must be enabled on the AVE virtual machine.

1. To initialize the Avamar Plug-in for vSphere Web Client services, issue the following command from the Avamar server console in the vSphere Client as a root user:

   ebrserver.pl --init

2. After the command is issued, an information message appears specifying that initializing the Avamar Plug-in for vSphere Web Client requires a restart of the Tomcat server. Enter **Y** to restart the Tomcat server and start the Avamar Plug-in for vSphere Web Client services.

Disabling services

If you decide you no longer want to use the Avamar Plug-in for vSphere Web Client (for example, you want to administer the vCenter Server through Avamar Administrator), enter the following command as a root user:

ebrserver.pl --disable

Viewing the Avamar Plug-in for vSphere Web Client activity

Enter the following command to view the status of the Avamar Plug-in for vSphere Web Client as a root user:

```
ebrserver.pl --status
```

Restarting services

After any vCenter configuration (for example, changing the vCenter Server you want to manage by editing the **vcenter-sso-info.cfg** file), you must restart the Avamar Plug-in for vSphere Web Client services with the following command:

```
ebrserver.pl --restart
```

CHAPTER 3
Using the Avamar Plug-in for vSphere Web Client

This chapter includes the following topics:

Avamar setup

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

◆ Under Policies, create a group in the VirtualMachines domain and select proxies to protect virtual machines in the group. If the vCenter is created under any domain except the root domain, the logon to the Avamar Plug-in for vSphere Web Client will fail.

IMPORTANT

The Avamar vSphere Plug-in for vSphere Web Client does not support vCenters with the same name.

◆ The Data Set for each group must be configured to the VMware Image Dataset (or All Virtual Disks).

Note: See the *EMC Avamar Administration Guide* for additional details on Avamar policy configuration.

Note: 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.

Note: All Avamar alerts are displayed and managed through Avamar Administrator and not through the vSphere Web Client.

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

Accessing 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 Web Client.

Note: Web browsers must be enabled with Adobe Flash Player 11.3 or higher to access the vSphere Web Client and Avamar Plug-in for vSphere Web Client functionality

After the Avamar Plug-in for vSphere Web Client is configured, specify an Avamar server through the following steps:

1. Open a web browser and type the following URL to access the vSphere Web Client:

   https://*IP_address_vCenter_Server***:9443/vsphere-client/**

2. Log in with administrative rights.

Note: The administrator who logs into the Avamar Plug-in for vSphere Web Client is able to manage all virtual machine image backups for virtual machines within the vCenter.

3. From the home page, select **EMC Backup and Recovery**.

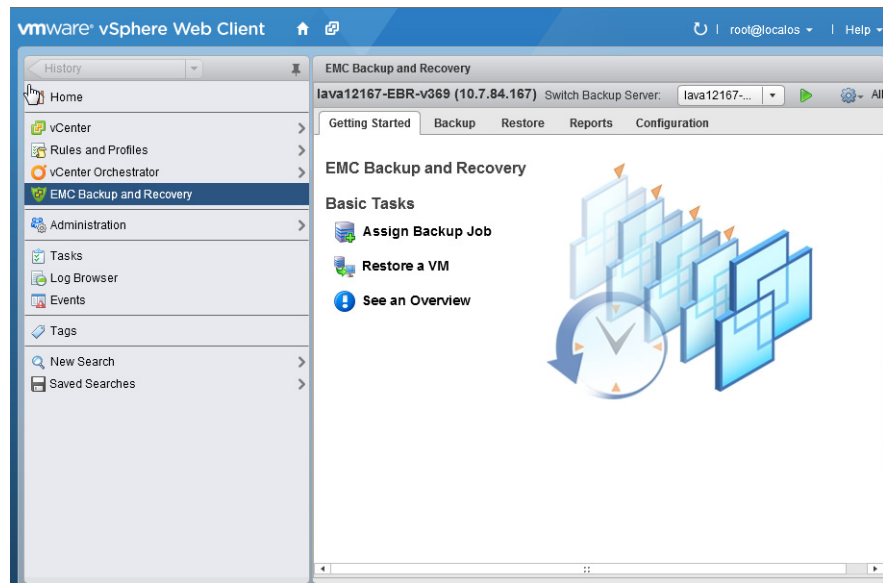   The Welcome to the EMC Backup and Recovery page appears.
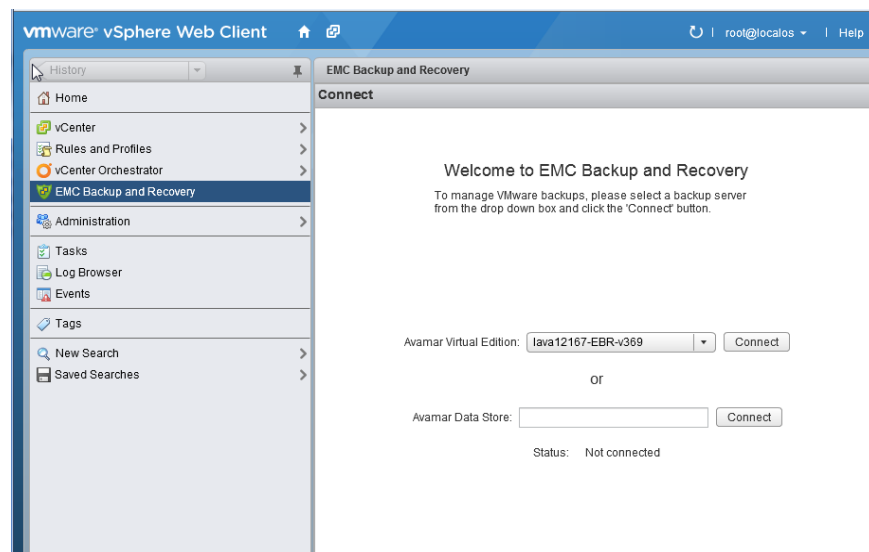
4. Select the Avamar device to connect to, you can select from:

   - **Avamar Virtual Edition** (if you are using AVE, this is automatically configured from the vCenter Server and a drop-down menu is available)

   - **Avamar Data Store** (if you are using physical Avamar, specify the IP address or FQDN of the Avamar server)

5. Click **Connect**.

EMC backup and recovery plug-in user interface

The EMC backup and recovery plug-in user interface is used to manage virtual machine image backups and restores.

EMC backup and recovery plug-in tabs

The EMC backup and recovery plug-in user interface consists of five tabs:

◆ **Getting Started**—Provides an overview of the EMC backup and recovery plug-in functionality and quick links to the Create Backup Job wizard, the Restore wizard, and the Reports tab.

◆ **Backup**—Provides list of Avamar groups configured under the VirtualMachines domain in Avamar Administrator and is used to select virtual machines for backup. See"Backup tab" on page 23 for additional information.

◆ **Restore**—Provides a list of successful backups that can be restored. See "Restore tab" on page 24 for additional information.

◆ **Reports**—Provides backup status reports on the virtual machines on the vCenter Server. See"Reports tab" on page 25 for additional information.

◆ **Configuration**—Displays information about how the EMC backup and recovery plug-in is configured and allows you to edit some of these settings. See "Viewing backup server details" on page 31 for additional information.

Backup tab

The Backup tab displays a list of the backup groups that have been created through Avamar Administrator and is used to select virtual machines for backup.

The Backup tab displays information on the backup jobs as shown in Table 3.

Table 3 Backup tab column descriptions

Column	Description
Name	The name of the backup group (created through Avamar Administrator).
State	The state of the backup group policy, which is enabled or disabled (managed through Avamar Administrator). Disabled backup jobs do not run.
Last Start Time	The start time of the last job.
Duration	The time duration of the most recent job.
Next Runtime	The schedule of the next scheduled job.
Success Count	The number of virtual machines that backed up successfully during the last job, updated after each backup job. The job must run again to reflect changes to a job between backups. For example, if a job reports that 10 virtual machines successfully backed up, the system edits the job so only one virtual machine remains. This number continues to be 10 until the job runs again. If successful, the number changes to one.
Failure Count	The number of virtual machines that did not backup successfully the last time the backup job ran, updated after each backup job. The job must run again to reflect changes to a job between backups. For example, if a job reports that 10 virtual machines failed to back up, the system edits the job so only one virtual machine remains. This number continues to be 10 until the job runs again. If the job fails, the number changes to one.

Using the Backup tab, you can select virtual machines for backup jobs. See "Selecting virtual machines for backup jobs" on page 26 for more information.

Restore tab

The Restore tab displays a list of virtual machines that the EMC backup and recovery plug-in has backed up. By navigating through the list of backups, you can select and restore specific backups.
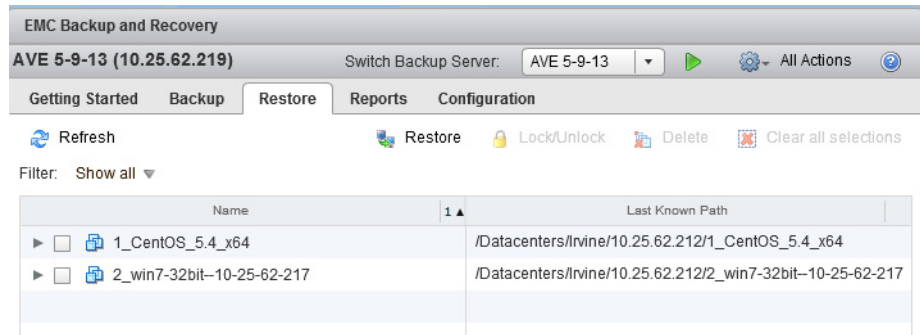
Using the Restore tab you can perform the following operations:

◆ "Restoring backups" on page 28

◆ "Locking and unlocking a backup" on page 29

◆ "Deleting a backup" on page 29

Reports tab

The Reports tab provides overview information about the EMC backup and recovery plug-in and about the virtual machines within the vCenter Server.

See "Viewing information from the Reports tab" on page 30 for more additional information.

Configuration tab

The Configuration tab enables you to view details about the Avamar server and event log details. You can configure email settings and run an integrity check from the Configuration tab.
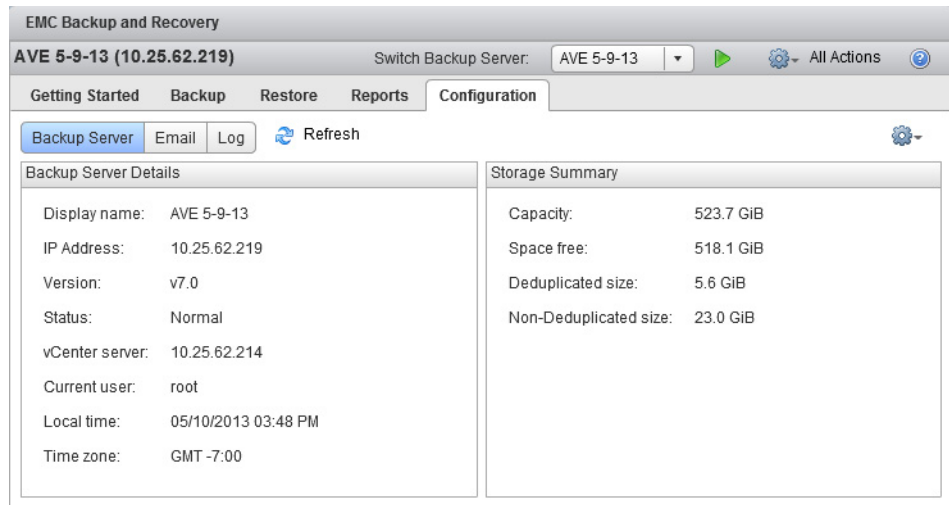
Refer to the following topics for configuration details:

Selecting virtual machines for backup jobs

The following procedure is used to select virtual machines for backup.

1. From **EMC Backup and Recovery** select the **Backup** tab. The Backup tab is populated with Groups configured through Avamar Administrator in the VirtualMachines domain. Select a group and click **Edit**.

2. The **Editing backup job** page displays all virtual machines associated with the vCenter Server associated with the Avamar Plug-in for vSphere Web Client. Select the virtual machines for backup and click **Finish**.

   Note: The EMC backup and recovery plug-in will not back up the following specialized virtual machines: VMware Data Recovery (VDR) Appliances, templates, Secondary fault tolerant nodes, proxies, or Avamar Virtual Edition (AVE) virtual machines. You can select these virtual machines from the wizard. However, when you click Finish, a warning informs you that the backup job excluded these special virtual machines.

Viewing status and backup job details

The Backup tab displays a list of Groups configured through Avamar Administrator in the VirtualMachines domain. By clicking on a backup group, you can see the details of the backup jobs associated with the backup group in the Backup Job Details pane:

◆ **Name**—The name of the backup group.

◆ **Status**—Enabled or disabled.

◆ **Sources**—A list of the virtual machines in the backup job. If more than six virtual machines are in the backup job, a **more** link appears. The **more** link displays the Protected Item List dialog box, which displays a list of all the virtual machines in the backup job.

◆ **Out of Date**—A list of all the virtual machines that failed to back up the last time the job ran. If more than six virtual machines are out of date, a **more** link appears. The **more** link displays the Protected Item List dialog box, which displays a list of all the virtual machines in the backup job.

Restoring backups

Backup jobs are restored with the Restore Job wizard.

1. From **EMC Backup and Recovery** select one of the following options to start the Restore wizard.

    *   Click **Restore a VM** on the Getting Started tab.

    *   Click **Restore** on the Restore tab.

    *   Select a protected virtual machine in the EMC Backup and Recovery Reports tab, and then click the All Actions icon and click **Restore from Last Backup**.

    *   Right-click a protected virtual machine in a vCenter inventory list and then select **All EBR Actions › Restore from Last Backup**. The Select Backup page displays a list of backups.

2. On the **Select Backup** page, select the correct restore point (all restore points for the backup display by date and time). Typically, you only select one restore point at a time. Click **Next**.

3. On the **Set Restore Options** page, confirm that the client and restore point are correct. Select Restore to Original Location or clear the Restore to Original Location checkbox and specify an alternate location (New Name, Destination, and Datastore). Optionally, you can set the virtual machine to **Power On** and **Reconnect NIC** after the restore process completes. Click **Next**.

4. On the **Ready to complete** page, verify the selections. If the settings are correct, click **Finish**. If the settings are not correct, click **Back** to go back to create the correct configuration.

5. A message displays telling you that the restore successfully initiated. Click **OK**.

6. Monitor the Restore progress through the Recent Tasks pane.

Note: If you selected Reconnect NIC during the restore process, confirm the network configuration for the newly created virtual machine. It is possible that the new virtual machine NIC is using the same IP address as the original virtual machine, which will cause conflicts.

Locking and unlocking a backup

During maintenance periods, the EMC backup and recovery plug-in examines the backups, and evaluates whether their retention period has expired. If the retention period has expired, the EMC backup and recovery plug-in removes the expired backup. However, if you want to prevent the EMC backup and recovery plug-in from deleting a backup, you can lock it. The EMC backup and recovery plug-in will not evaluate the retention period on locked backups.

1. From **EMC Backup and Recovery** click the **Restore** tab, and navigate to the backup you want to lock.

2. Click the checkbox next to the backup you want to lock.

3. Click the **Lock/Unlock** icon. Locking a backup overlays a lock icon on the backup icon:.

4. To unlock the backup, click the checkbox next to the backup and click the **Lock/Unlock** icon again. The lock overlay clears and the EMC backup and recovery plug-in evaluates the retention date of the backup during the next maintenance period.

Deleting a backup

The EMC backup and recovery plug-in deletes backups according to the retention policies set in the backup jobs (configured through Avamar Admininstrator). However, you can manually delete backups from the Restore tab by selecting the backup jobs for deletion and clicking the Delete icon.

Viewing information from the Reports tab

The top half of the Reports tab displays the following information:

◆ **Backup Server Status**—The status of Avamar.

◆ **Used Capacity**—A percentage of the total capacity occupied by all backups.

◆ **Integrity Check Status**—This value is either Normal or Out of Date. Normal indicates that a successful integrity check completed in the past two days. Out of Date indicates that an integrity check has not run or has not completed successfully in the past two days.

◆ **Recent Successful Backups**—The number of virtual machines that successfully backed up in the most recently completed backup job.

◆ **Recent Failed Backups**—The number of virtual machines that failed to backup in the most recently completed backup job.

The middle of the Reports tab lists all the virtual machines associated with the vCenter Server. For each virtual machine, you can see the following information:

◆ Virtual machine name

◆ State (The EMC backup and recovery plug-in uses standard VMware state information)

◆ Backup Policies

◆ Last Successful Backup

◆ Status

◆ Date

◆ Backup Job Name

From the bottom section of the Reports tab, you can select a virtual machine from the middle section of the Reports tab and see detailed information about the selected client, which includes:

◆ Virtual Machine Information

  • Name

  • Guest OS

  • Host

  • IP address

  • Virtual Machine State

  • Last Successful Backup

  • Backup Policies (associated with the selected virtual machine)

◆ Last Backup Job

  • Status

  • Date

  • Backup Job

Configuring the EMC backup and recovery plug-in

Use the Configuration tab for the following tasks.

◆

◆

◆

◆

Viewing backup server details

Click the Backup Server tab to view the following backup server details and storage details:

◆ Backup Server Details

- Display name—The name of the Avamar Virtual Edition (AVE) or Avamar server

- IP address—The IP address of the AVE or Avamar server

- Version—The version of Avamar software

- Status—The AVE or Avamar server status

- vCenter server—The FQDN or IP address of the vCenter Server

- Current user—The login name of the user

- Local time—The current local time

- Time zone—The time zone setting

◆ Storage Summary

- Capacity—The used capacity, in GiB

- Space free—The amount of unused space, in GiB

- Deduplicated size—The amount of used deduplicated storage, in GiB

- Non-Deduplicated size—the amount of used non-deduplicated storage, in GiB

Configuring email

The Email tab allows you to configure the EMC backup and recovery plug-in to send SMTP email reports to specified recipients.

1. From **EMC Backup and Recovery,** select the **Configuration** tab.

2. Select **Email.**

3. Click the **Edit** button (in the lower-right corner of the page).

4. Specify the following fields:

    a. **Enable email reports**—Check this box to enable email reports.

    b. **Outgoing mail server**—Enter the name of the SMTP server that you want to use to send email. Enter this name as either an IP address, a hostname, or a fully qualified domain name.

    The default port for non authenticated email servers is 25. The default port of the authenticated mail servers is 587. You can specify a different port by appending a port number to the server name. For example, to specify the use of port 8025 on server "emailserver" type:

    emailserver:8025

    c. (optional) **My server requires me to log in** —Check this box if the SMTP server requires authentication.

    d. **User name**—Enter the user name for authentication with the email server.

    e. **Password**—Enter the password associated with the user name. The EMC backup and recovery plug-in does not validate the password in any way. The EMC backup and recovery plug-in passes the password directly to the email server.

    f. **From address**—Enter the email address the email report will be sent from. Only one address is used.

    g. **To address(es)**—Enter a comma-separated list of up to 10 email addresses.

    h. **Send time**—From the drop-down list, choose the time you want the EMC backup and recovery plug-in to email reports. The default time is 12:00 AM.

    i. **Send day(s)**—Check the days you want the reports sent. You can check any combination of days, from one to all seven.

    j. **Report Locale**—From the drop-down list, select the locale for the email reports.

5. Click the **Save** button.

Note: The EMC backup and recovery plug-in email notification does not support carbon copies (CCs) or blind carbon copies (BCCs), nor does it support SSL certificates.

6. To test the email configuration, click **Send test email.**

Viewing the user interface log

The following steps are used to view the user interface log.

1. From the **Configuration** tab, click **Log**.

   The user interface log details the activities that you have initiated with the user interface which identifies some key status items.

2. Click **Export View** to save the details that display on the screen to file on the machine where the browser is running.

Running an integrity check

Integrity checks verify and maintain data integrity on the deduplication store. The output of an integrity check is a checkpoint. By default, the EMC backup and recovery plug-in creates an integrity check every day during the maintenance window. You can also start the integrity check manually.

1. From the EMC Backup and Recovery Configuration tab, click the All Actions icon, and select **Run integrity check**.

2. A confirmation screen displays, asking if you want to perform a manual integrity check. Click **Yes**.

3. A message displays informing you that the integrity check initiated. Click **OK**.

   The EMC backup and recovery plug-instarts the integrity check.

4. Monitor the integrity check progress through the **Recent Tasks** dialog box.

CHAPTER 4
Using File-Level Restore

This chapter includes the following topics:

Introduction to the EMC Data Protection Restore Client

The EMC backup and recovery plug-in creates image backups of virtual machines. You can restore image backups with the EMC backup and recovery plug-in user interface through the vSphere Web Client. However, if you only want to restore specific files from these virtual machines, then use the EMC Data Protection Restore Client (subsequently referred to as the Restore Client), which is accessed through a web browser.

The Restore Client service is only available to virtual machines backed up by the EMC backup and recovery plug-in. You must log in, either through the vCenter console or some other remote connection, to one of the virtual machines backed up by the EMC backup and recovery plug-in.

The Restore Client allows you to mount specific virtual machine backups as file systems and then "browse" the file system to find the files you want to restore. The ability to restore specific files is called file-level restore (FLR).

Note: The Restore Client does not support Internet Explorer 10.

Note: The Restore Client web browser requires a flash plug- in for FLR UI functionality.

File-level restore supported configurations

You can perform file-level restores on backups of the following file systems:

◆ NTFS (Primary Partition with MBR)

◆ Ext2 (Primary Partition with MBR)

◆ Ext3 (Primary Partition with MBR)

◆ LVM with ext2 (Primary Partition with MBR and a Standalone [without MBR] LVM with ext2)

◆ LVM with ext3 (Primary Partition with MBR and a Standalone [without MBR] LVM with ext3)

File-level restore limitations

File-Level Restore does not support the following virtual disk configurations:

◆ Unformatted disks

◆ Dynamic disks

◆ GUID Partition Table (GPT) disks

◆ ext4 filesystems

◆ FAT16 filesystems

◆ FAT32 filesystems

◆ Extended partitions

◆ Encrypted partitions

◆ Compressed partitions

File-Level Restore does not support the following Windows 8 and Windows Server 2012 configurations:

◆ Deduplicated NTFS

◆ Resilient File System (ReFS)

◆ Extensible Firmware Interface (EFI) boot loader

File-Level Restore also has the following limitations:

◆ You cannot restore or browse symbolic links.

◆ Browsing either a specified directory contained within a backup or a restore destination is limited to 5000 files or folders.

◆ You cannot restore more than 5000 files or folders in the same restore operation.

The following limitations apply to logical volumes managed by the Logical Volume Manager:

◆ You must map one Physical Volume (.vmdk) to exactly one logical volume.

◆ Formatting is limited to ext2 and ext3.

Logging into the Restore Client

The Restore Client operates in one of two modes:

◆ **Basic**—With basic login, you connect to the Restore Client from a virtual machine backed up by the EMC backup and recovery plug-in. You log in to the Restore Client with the same local administrative credentials of the virtual machine. The Restore Client only displays backups for the local virtual machine.

For example, if you were logging in to the Restore Client in Basic mode from a Windows host named "WS44" then you would only be able to mount and browse backups of "WS44."

◆ **Advanced**—With advanced login, you connect to the Restore Client from a virtual machine backed up by the EMC backup and recovery plug-in. You log in to the Restore Client with the local administrative credentials of the virtual machine and you also log in to the vCenter with the vCenter credentials used during registration to the Avamar server. After connecting to the Restore Client, you will be able to mount, browse, and restore files from any virtual machine backed up by the EMC backup and recovery plug-in. All restore files restore to the current virtual machine.

Note: You can only restore files from a Windows backup to a Windows machine, and you can only restore files from a Linux backup to a Linux machine.

Note: The only account that can be used with Windows is administrator. The only account that can be used with Linux is root.

Mounting backups

After you successfully log in, the Manage mounted backups dialog box displays. By default this displays all the available backups. The format of this dialog box varies depending on how you logged in.

◆ If you use basic login, you will see a list of all the backups from the client you logged into that you can mount.

◆ If you used advanced login, you will see a list of all clients that have backed up to the EMC backup and recovery plug-in. Under each client, there is a list of all available backups.

Note: You can mount up to254 VMDK images using the Mount, Unmount, or Unmount all buttons on the lower-right corner of the dialog box.

Filtering backups

In the Manage mounted backups dialog box, you have the option of displaying all the backups or of filtering the list of backups. You can filter the list in the following ways:

◆ **All restore points**—Displays all backups.

◆ **Restore point date**—Displays only backups within the specified date range.

◆ **VM name**—Displays only backups of hosts whose display name contains the text entered in the filter field. This option is not available with basic login because only the backups that belong to the virtual machine are displayed.

Navigating mounted backups

After you have mounted the backups, browse the contents of the backup using the tree display on the left side of the Restore Client user interface. The appearance of the tree varies depending on whether you used basic login or advanced login.

Performing file-level restores

The main screen of the Restore Client allows you to restore specific files by browsing the file system trees.

Note: File-level restore requires that all proxies in the vCenter environment be version 7.0. 6.*x* proxies will disable the file-level restores.

Using the Restore Client with basic login mode

Use the Restore Client on a Windows or Linux virtual machine with basic login mode to access individual files from restore points for that machine, rather than restoring the entire virtual machine.

Prerequisites

◆ Verify that the Avamar Plug-in for vSphere Web Client is configured.

◆ For basic login, you can only login to the Restore Client from a virtual machine backed up by the EMC backup and recovery plug-in.

◆ VMware Tools must be installed on the virtual machine in order to perform file-level restores from backups. Refer to the VMware website for list of operating systems that support VMware Tools.

Procedure

1. Log in remotely using remote desktop, or use the vSphere Web Client to access a virtual machine.

2. Access the Restore Client through:

   https://_Avamar_IP_address_**:8543/flr**

3. In the **Credentials page** under Local Credentials, specify the **Username** and **Password** for the local host (using administrator for Windows or root for Linux).

4. The **Manage** mounted backups dialog box appears. The dialog box lists all the restore points for the client. Select the mount restore point, and click **Mount**.

5. When the mount is complete, the drive icon will appear as a green networked drive.

6. Click **Close**.

7. In the **Mounted Backups** window, browse to and select the folders and files you want to recover.

8. Click **Restore selected files.**

9. In the **Select Destination** dialog box, browse to and select the drive and the destination folder for recovery.

10. Click **Restore**.

11. An initiate restore confirmation dialog box displays. Click **Yes**.

12. A successfully initiated dialog box displays. Click **OK**.

13. Click the **Monitor Restores** tab to view restore status.

14. Confirm the completed job status.

Using the Restore Client with advanced login mode

Use the Restore Client on a Windows or Linux virtual machine with advanced login mode to access virtual machines on a vCenter Server that contain restore points to perform file-level restores.

Procedure

1. Log in remotely using remote desktop, or use the vSphere Web Client to access a virtual machine.

2. Access the Restore Client through:

   https://*Avamar_IP_address***:8543/flr**

3. In the **Credentials page** under Local Credentials, specify the **Username** and **Password** for the local host (using administrator for Windows or root for Linux). Click **Advanced Login** and in the vCenter Credentials field, specify the vCenter administrator **Username** and **Password,** and click **Login**.

4. The **Manage mounted backups** dialog box displays. The dialog box lists the restore points for any virtual machine backed up by the EMC backup and recovery plug-in. Select the restore mount point, and click **Mount**.

5. When the mount is complete, the drive icon will display as a green networked drive.

6. Click **Close**.

7. In the **Mounted Backups** window, browse to and select the virtual machine's folders, and files for recovery.

8. Click **Restore selected files.**

9. In the **Select Destination** dialog box, browse to and select the drive and destination folder for recovery.

10. Click **Restore**.

11. An Initiate Restore confirmation dialog box displays. Click **Yes**.

12. A successfully initiated dialog box appears. Click **OK**.

You can determine when the restore is complete by clicking the **Monitor Restores** tab to view restore status.

Monitoring restores

To monitor current activity and past activity of the EMC Data Protection Restore Client, click the **Monitor Restores button.** The monitor restore screen displays information about current and recently completed restore operations.

The columns in this table are sortable by clicking on the column heading. Click multiple times on a table heading to reverse the sort order, and an up-arrow or down-arrow reflects whether the sort order is ascending or descending.

By default, Monitor Restores shows all the jobs that in are in process or that have completed during the current session. If you want to see jobs that completed or failed in a previous session, check the **Show Completed Activities** box. All past completed and failed jobs display, along with running and pending jobs.