EMC® Avamar® 7.4 and Service Packs Plug-in for vSphere Web Client

Administration Guide

EMC²

CONTENTS

CONTENTS

TABLES

TABLES

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.

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

Note

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

Purpose

This 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 following table presents the revision history of this document.

Revision	Date	Description
01	December, 2016	DA release of Avamar 7.4.
02	March, 2017	GA release of Avamar 7.4 Service Pack 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 Guide*

Special notice conventions used in this document
EMC uses the following conventions to alert the reader to particular information.

> **NOTICE**

The Notice convention emphasizes important information about the current topic.

Note

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

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

Table 1 Typographical conventions

Convention	Example	Description
Bold typeface	Click **More Options**.	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what a user specifically selects or clicks).
Italic typeface	*EMC Avamar Administration Guide*	Use for full titles of publications that are referenced in text.
Monospace font	`Event Type = INFORMATION Event Severity = OK Event Summary = New group created`	Use for: • System code • System output, such as an error message or script • Pathnames, file names, prompts, and syntax • Commands and options
Monospace font with italic typeface	Type *Avamar_server*, where *Avamar_server* is the DNS name or IP address of the Avamar server.	Use for variables.
Monospace font with bold typeface	Type `yes`.	Use for user input.
Square brackets	`[--domain=String(/)] --name=String`	Square brackets enclose optional values.
Vertical bar	`[--domain=String(/)] | --name=String`	Vertical bar indicates alternate selections - the bar means "or".

Table 1 Typographical conventions (continued)

Convention	Example	Description
Braces	`{[--domain=`*`String`*`(/)]` `| --name=`*`String`*`}`	Braces enclose content that the user must specify.
Ellipses	`valid hfs ...`	Ellipses indicate nonessential information that is omitted from the example.

Where to get help

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

To access the Avamar support page:

1. Go to https://support.EMC.com/products.
2. Type a product name in the **Find a Product** box.
3. Select the product from the list that appears.
4. Click the arrow next to the **Find a Product** box.
5. (Optional) Add the product to the **My Products** list by clicking **Add to my products** in the upper right corner of the **Support by Product** page.

Comments and suggestions

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

Please include the following information:

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

CHAPTER 1

Introduction

This chapter includes the following topics:

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.

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.

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.

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

In order to use the Avamar Plug-in for vSphere Web Client, Avamar Administrator must have backup policies configured through Avamar Administrator in the VirtualMachines domain (subdomains are not supported). 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.

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 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

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

Criterion	Guest backup and restore	Image-level backup and restore
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 requiremens	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, migrate, snapshot create, delete, or revert.

CHAPTER 2

Configuring the Avamar Plug-in for vSphere Web Client

This chapter includes the folllowing topics:

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 proxy virtual client must be running on the same vCenter as the Avamar Plug-in for vSphere Web Client.

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

For successful configuration of Avamar plugin for vSphere Web Client, vCenter client must be registered as main domain in Avamar server. If it is registered under any other domain as sub-domain, plugin configuration fails.

vCenter configuration file settings

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 the following table.

Table 3 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-hostname =	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.

Procedure

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 with the following command:

   ```
   admin@avamar_server:~/>:su -
   ```

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

5. Initiate the Avamar Plug-in for vSphere Web Client services by typing the following command:

   ```
   root@avamar_server:~/#:ebrserver.pl --init
   ```

   An information message appears specifying that initializing the Avamar Plug-in for vSphere Web Client requires a restart of the Tomcat server.

6. Type **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.

Procedure

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
   ```

   An information message appears specifying that initializing the Avamar Plug-in for vSphere Web Client requires a restart of the Tomcat server.

2. Type **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), type the following command as a root user:

```
ebrserver.pl --disable
```

Viewing the Avamar Plug-in for vSphere Web Client activity

Type 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

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

See the *EMC Avamar Administration Guide* for additional 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.

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.

Procedure

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.

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:

   - **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 following table describes the tabs in the EMC backup and recovery plug-in user interface.

Table 4 User interface tabs

Tab	Description
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 a list of Avamar groups configured under the VirtualMachines domain in Avamar Administrator and is used to select virtual machines for backup.
Restore	Provides a list of successful backups that can be restored.
Reports	Provides backup status reports on the virtual machines on the vCenter Server.
Configuration	Displays information about how the EMC backup and recovery plug-in is configured and allows you to edit some of these settings.

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. Using the Backup tab, you can select virtual machines for backup jobs.

The **Backup** tab displays information on the backup jobs as shown in the following table.

Table 5 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

Table 5 Backup tab column descriptions (continued)

Column	Description
	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.

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
- Locking and unlocking a backup
- Deleting a backup

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.

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.

Selecting virtual machines for backup jobs

Procedure

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.

2. Select a group and click **Edit.**

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

3. Select the virtual machines for backup and click **Finish.**

Note

The EMC backup and recovery plug-in does 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.

The following table lists the details that appear for each backup jobs.

Table 6 Backup job details

Field	Description
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

Procedure

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. 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.

3. Click **Next.**

4. On the **Set Restore Options** page, confirm that the client and restore point are correct.

5. 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.

6. Click **Next.**

7. On the **Ready to complete** page, verify the selections and click **Finish**.

    A message indicates that the restore successfully initiated.

8. Click **OK.**

9. Monitor the restore progress through the **Recent Tasks** pane.

After you finish

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.

Procedure

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.

Procedure

1. On the **Restore** tab, select the backup job to delete.

2. Click the **Delete** icon.

Viewing information from the Reports tab

The **Reports** tab provides system status and virtual machine information.

Top section of the Reports tab

The top half of the **Reports** tab displays the system status information in the following table.

Table 7 Reports tab — top section details

Field	Description
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 back up in the most recently completed backup job.

Middle section of the Reports tab

The middle of the **Reports** tab lists all the virtual machines associated with the vCenter Server. The following information appears for each virtual machine:

- 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

Bottom section of the Reports tab

The bottom section of the **Reports** tab displays detailed information about the virtual machine selected in the middle section of the **Reports** tab. The following information appears for the selected virtual machine:

- 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

EMC Backup and Recovery plug-in Configuration tab

Use the **Configuration** tab for the following tasks:

- Viewing backup server details

- Configuring email

- Viewing the user interface log

- Running an integrity check

Backup server details

The **Backup Server** tab displays backup server and storage details.

The following table describes the backup server details that appear on the **Backup Server** tab.

Table 8 Backup server details

Field	Description
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

Table 8 Backup server details (continued)

Field	Description
Local time	The current local time
Time zone	The time zone setting

The following table describes the storage details that appear on the **Backup Server** tab.

Table 9 Storage details

Field	Description
Capacity	The used capacity in GiB
Space free	The amount of unused space in GiB
Deduplicated size	The amount of deduplicated storage in GiB
Non-Deduplicated size	The amount of used non-deduplicated storage in GiB

Configuring email

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

Procedure

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. Select **Enable email reports** to enable email reports.
5. In **Outgoing mail server**, specify the IP address, hostname, of FQDN of the SMTP server to use to send the email.

   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`.
6. (Optional) Select **My server requires me to log in** if the SMTP server requires authentication, and then specify the username and password for authentication.

   The EMC backup and recovery plug-in passes the username and password directly to the mail server without any validation.
7. In **To address(es)**, type a comma-separated list of as many as 10 email addresses to which to send the reports.
8. From the **Send time** list, select the time at which to email the reports.
9. In **Send day(s)**, select the checkbox next to the days on which to send the reports.
10. From the **Report Locale** list, select the locale for the email reports.
11. Click **Save**.

> **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.

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

Viewing the user interface log

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

Procedure

1. From the **Configuration** tab, click **Log.**
2. Click **Export View** to export the data to a local file.

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 automatically creates an integrity check every day during the maintenance window. You can also start the integrity check manually.

Procedure

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

   A confirmation message appears.

2. Click **Yes.**
3. 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

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

File-level restore supported configurations

The following supported configurations require that both the proxy version and Avamar server to be at Avamar release 7.4 Service Pack 1 or later:

- NTFS (Primary Partition with MBR)
- Ext2 (Primary Partition with MBR)
- Ext3 (Primary Partition with MBR)
- Ext4 (Primary Partition with MBR)
- XFS (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)
- LVM with ext4 (Primary Partition with MBR and a Standalone [without MBR] LVM with ext4)
- LVM with XFS (Primary Partition with MBR and a Standalone [without MBR] LVM with XFS)
- Extended partition of type 0x05
- Striped LVM
- GUID Partition Table (GPT) disks (only basic disks)

File-level restore limitations

File-level restore with Restore Client Web UI 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 5,000 files or folders.
- Restore is limited to 5,000 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.

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

- Unformatted disks

- Dynamic disks (Windows)

- FAT16 filesystems

- FAT32 filesystems

- Extended partitions not of type 0x05

- Encrypted partitions or bootloaders

- Compressed partitions or bootloaders

- Parity LVM

- Mirrored LVM

- Deduplicated NTFS

- Resilient File System (ReFS)

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 configured with a type 8E-Linux LVM, which consists of one or more physical volumes that contains one or more volume groups made up of one or more logical volumes.

Restore Client Login

The Restore Client operates in either user or admin modes.

User

With user 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.

Admin

With admin login, you connect to the Restore Client from a virtual machine backed up by the EMC backup and recovery plug-in. You log in with the vCenter credentials used during registration to the Avamar server. After connecting to the Restore Client, you can browse and restore files to and from all virtual machines backed up by the EMC backup and recovery plug-in.

Performing file-level restores

The main screen of the Restore Client enables 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.*x*.

Restoring specific folders or files to the original virtual machine in User mode

To restore specific folders and files to the original virtual machine on Windows and Linux virtual machines, select the **User** tab in the **EMC Data Protection Restore**

Client login page. In this mode, you connect to the **EMC Data Protection Restore Client** from a virtual machine that has been backed up by the proxy appliance.

Procedure

1. Open a browser on the virtual machine to which the files will be restored and enter the following URL:

   ```
   https://Avamar_IP_address:8543/flr
   ```

   where *Avamar_IP_address* is the IP address of the Avamar server.

   Note

   For recoveries in User mode, you must connect to the Avamar server from a web browser on the virtual machine that will receive FLR data.

2. Select the **User** tab.

3. Log in to the **EMC Data Protection Restore Client** with the user credentials of the virtual machine to which you are logged in.

   The **Select the backup(s) to restore from** page displays, with a list of backups for the local virtual machine. Use the drop-down list to view the available backups. You can view all backups, or only backups on a specific date or within a specific range.

4. Highlight the desired backup, and double-click or drag-and-drop the backup to move it to the **Selected Items** pane.

5. Click **Next**.

   The **Restore Options** page is displayed.

   Note

   If a folder hierarchy does not appear, the **EMC Data Protection Restore Client** may not support the file system in use on the virtual machine. The section File-level restore supported configurations on page 32 provides more information.

6. On the **Restore Options** page, select the folder to which items should be restored.

7. Click **Next**.

8. On the **Select items to restore** page, browse and select files and folders desired for recovery.

   To mark an item for recovery, double-click or drag-and-drop the item to move it to the **Selected Items** pane. Items marked for recovery will appear in the **Selected Items** pane.

9. Click **Finish**.

10. Click **Yes** when you are prompted to continue the restore.

After you finish

To monitor the progress of the restore operation, click the arrow button located at the lower right of the **Restore client** screen. When you select the arrow button, the **Restore Monitor** panel slides up. Click the **Refresh** button refresh the contents.

Restoring specific folders or files from a different virtual machine in Admin mode

To restore folders and files from a different virtual machine, select the **Admin** tab in the **EMC Data Protection Restore Client** login page. Once connected, you can browse, select, and restore files and folders from any virtual machine that you backed up. You can then restore items to the virtual machine on which you are currently logged in, or to any available destination virtual machine.

Procedure

1. Open a browser on the virtual machine to which the files will be restored and enter the following URL:

   ```
   https://Avamar_IP_address:8543/flr
   ```

   where *Avamar_IP_address* is the IP address of the Avamar server.

2. Select the **Admin** tab.

3. Log in to the **EMC Data Protection Restore Client** with the user credentials that you used to register the vCenter server to the Avamar server.

   The **Select Backups** page displays, with a list of all virtual machines that have been backed up. Available backups appear under each virtual machine.

4. On the **Select Backups** page:

   a. Use the arrows to the right of the entry to view the available backups.

   b. Highlight the desired backup and double-click or drag-and-drop the backup to move it to the **Selected Items** pane.

5. Click **Next**.

   The **Restore Options** page is displayed.

6. On the **Restore Options** page, select a destination virtual machine.

7. Log in to the selected destination virtual machine.

8. Select the restore location or create a new destination folder on the selected destination.

   The **Select items to restore page** is displayed.

9. On the **Select items to restore** page, browse and select files and folders desired for recovery.

   To mark an item for recovery, double-click or drag-and-drop the item to move it to the **Selected Items** pane. Items marked for recovery will appear in the **Selected Items** pane.

10. Click **Finish**.

11. Click **Yes** when you are prompted to continue the restore.

After you finish

To monitor the progress of the restore operation, click the arrow button located at the lower right of the **Restore client** screen. When you select the arrow button, the **Restore Monitor** panel slides up. Click the **Refresh** button refresh the contents.