Dell EMC Avamar Orchestra

Version 19.1

Getting Started Guide

302-005-578

REV 01

DELL EMC

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

Published May 2019

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, 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

Tables 5

Preface 7

Chapter 1 Introduction and Installation 11
About Orchestra 12
Architecture 12
System requirements 13
Installation 14
Obtain the installation package 14
Install Orchestra 14
Install a custom HTTPS certificate 15
Change the default service port 15
Best practices 16
Troubleshooting 16
Enable debug logging 16

Chapter 2 Orchestra Web UI 19
Orchestra Web UI 20
Access the Orchestra Web UI 20
Navigation pane 21
UI header pane 21
View product information 21
Access the Swagger UI 22
Change the Orchestra administrator password 22
Log out of the Orchestra Web UI 22
System pane 22
Monitoring Avamar servers 22
Add an Avamar server 23
Edit an Avamar server 24
Delete an Avamar server 24
Policy pane 24
Viewing policy details 24
Managing backup policies 26
Activity Monitor 32
Activity monitoring 32
View activities in the Activity Monitor 33
View a detailed client session log 34
Monitor backups 34
Restart a backup job 34
Cancel backups 35
Monitor restores 35
Cancel restores 35
Event pane 35
Event monitoring 36
View events in the Event pane 36

Acknowledge system events....37
Task pane.... 37

Chapter 3 Orchestra REST API 39
About the Orchestra REST API.... 40
Orchestra REST API components....40
Authentication tokens....40
About Swagger.... 41
Swagger navigational controls....41
Orchestra REST API examples.... 41
Testing the Orchestra REST API.... 42
Obtain an authentication token....42
Use the authentication token to access the Orchestra REST API.... 43
Using the Orchestra proxy API.... 44
Perform a proxy operation on one Avamar server....45
Perform a proxy operation on all registered Avamar servers.... 47

TABLES

1 Revision history 7
2 Typographical conventions 8
3 System requirements 13
4 Orchestra Web UI navigation pane 21
5 Information available in the System pane 22
6 Policy details 24
7 Settings for each type of schedule 30
8 Information in the Activity Monitor 32
9 Information in the Event pane 36
10 Information available in the Task pane 37
11 Header values and corresponding operational scopes 44

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 provides an introduction to the Avamar Orchestra REST API for multisystems management, including the Orchestra web UI and the Swagger interface.

Audience

This publication is primarily intended for administrators who oversee multiple Avamar servers. Administrators should be familiar with the general principles of the Avamar REST API, and with the basic concepts that are available through the Avamar Web User Interface.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	May 20, 2019	GA release of Avamar 19.1

Related documentation

The following publications provide additional information:

- *Avamar Release Notes*
- *Avamar Administration Guide*
- *Avamar REST API Getting Started 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 2 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.

Documentation

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

- Release notes provide an overview of new features and known limitations for a release.
- Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.
- White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

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

To search the Knowledgebase:

1. Go to https://www.dell.com/support/home/us/en/19.
2. Under the **Support** tab, click **Knowledge Base**.
3. Type either the solution number or keywords in the search box. Optionally, you can limit the search to specific products by typing a product name in the search box and then selecting the product from the list that appears.

Online communities

Go to Community Network at http://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 products.

Live chat

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

Service Requests

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

Note

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

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

Enhancing support

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

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

Comments and suggestions

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

Please include the following information:

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

CHAPTER 1

Introduction and Installation

This chapter contains the following topics:

- About Orchestra 12
- Installation 14
- Best practices 16
- Troubleshooting 16

About Orchestra

The Orchestra REST API extends the native Avamar server REST API to facilitate the management of multiple Avamar servers. After you register each Avamar server with Orchestra, the API provides a single point of interface for management operations that you can perform on the registered servers, individually or as a group:

- Implementing common backup policies.

  Orchestra enables you to centrally define and manage common backup policies across a group of servers, down to the level of datasets, schedules, and retention policies. The common backup policy propagates to each selected server, where it runs like other local policies. Where the master and local copies of a common policy differ, Orchestra can provide a side-by-side comparison.

- Monitoring server events, status, and activities from a centralized location.

  Orchestra regularly collects health information from the registered servers and presents this data in a summary format. You can browse the registered servers to review their activity logs and statistics without having to connect to each server individually.

Orchestra transparently manages the connections to the REST API interfaces of all registered Avamar servers, including the authentication tokens. Use the proxy API to interact directly with individual servers where necessary.

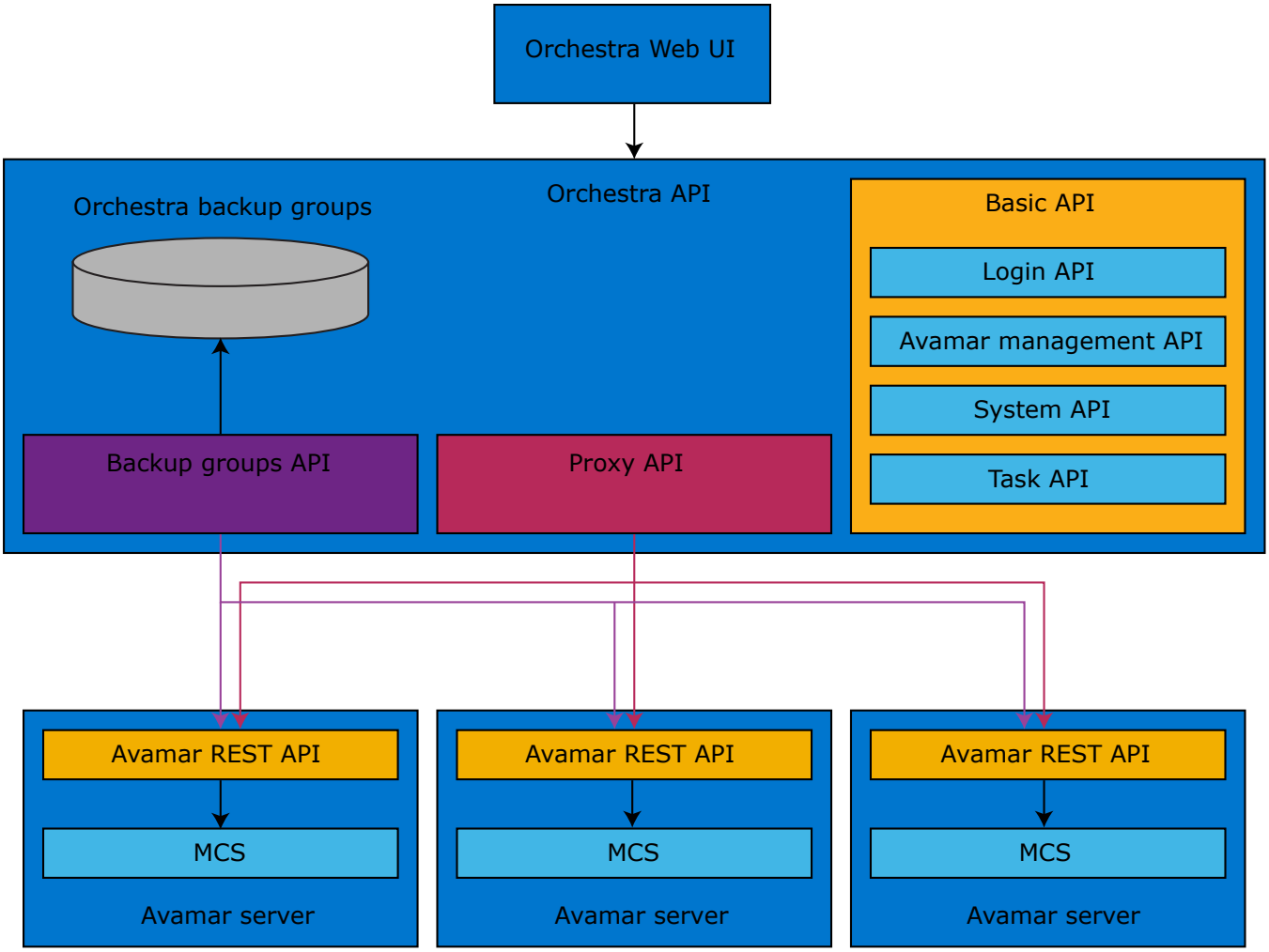
Architecture

Orchestra's multiple APIs provide access to different aspects of Avamar management. From an administrator's perspective, Orchestra web application and REST API translate group operations into appropriate REST API commands for the registered Avamar servers.

Orchestra Web UI on page 19 provides more information about the Orchestra web application. The Orchestra web user interface (web UI) provides a starting point for multiple-systems management and demonstrates the potential of the Orchestra REST API. This interface is closely modeled on the Avamar Web User Interface (AUI).

Orchestra REST API on page 39 provides more information about the different Orchestra APIs, how to learn more about the available commands, and examples of basic commands.

Figure 1 Orchestra architecture



System requirements

The following table defines the minimum system requirements to install Orchestra:

Table 3 System requirements

Requirement	Value
Operating system	SLES 12 (physical or virtual)
Java Runtime Environment	1.8 or later
Memory	8 GB or greater
Processors	Minimum two

To preserve server performance, Dell EMC does not recommend that you install Orchestra on an Avamar utility node.

Installation

The following topics describe how to obtain and install Orchestra installation, and then perform important post-installation configuration.

Obtain the installation package

The Orchestra resides in the Downloads area of Avamar Web Restore.

In a web browser, type `https://AvamarServer/dtlt/home.html`. Navigate to **Downloads** > **Linux for x86 (64 bit)** > **SUSE Linux Enterprise Server 11 (Console)**.

Download `orchestra-version.x86_64.rpm`, where *version* is the installed Avamar software version.

Install Orchestra

Install the Orchestra package on the host and then change the default password.

Procedure

1. Ensure that the firewall rules which protect the Orchestra host allow traffic on the service port, the SSH port, and, optionally, to the Orchestra Web UI.

   The default service port is 9009. The Orchestra Web UI operates over HTTPS.
2. Open a command shell and log in to the Orchestra host as the root user.
3. Using SCP or a USB drive, copy the Orchestra package to a temporary location on the host.

   For example, `/tmp`.
4. Change directory to the temporary location.

   For example, `cd /tmp`.
5. Install the Orchestra package by typing the following command:

   ```
   rpm -ivh orchestra*.rpm
   ```

   The SLES operating system installs and starts the Orchestra service.
6. In a web browser, type `https://orchestrahost:9009`

   where *orchestrahost* is the Orchestra host.

   The Orchestra login page opens.
7. Log in to Orchestra.

   The default username is "admin". The default password is "changeme".
8. In the header pane, click 👤 and then click **Config**.

   The Orchestra configuration page opens.
9. Change the default password to a password of your choice.

Install a custom HTTPS certificate

By default, Orchestra uses a self-signed certificate for HTTPS connections. As part of installation, you can optionally supply a Java keystore file with your own certificate.

Procedure

1. Open a command shell and log in to the Orchestra host as the root user.
2. Using SCP or a USB drive, copy the keystore to the `/opt/orchestra/config` directory on the host.
3. Change directory by typing the following command:

   ```
   cd /opt/orchestra/config
   ```

4. Change the keystore ownership by typing the following command:

   ```
   chown orchestra:orchestra /opt/orchestra/config/keystore.jks
   ```

   where *keystore* is the filename for the keystore that contains your certificate.

5. Using a Linux text editor, such as `vi`, edit `application-production.properties`.
6. Locate and complete the following parameters:

Parameter	Description
`server.ssl.key-store`	The location and name of the keystore that contains your certificate.
`server.ssl.key-store-password`	The password to open the keystore.
`server.ssl.key-password`	The password for the stored certificate.
`server.ssl.key-alias`	The certificate alias.

7. Save and close the file.
8. Restart the Orchestra service by typing the following commands:

   ```
   service orchestra stop
   service orchestra start
   ```

9. Verify that Orchestra supplies the new certificate for HTTPS connections.

Change the default service port

By default, Orchestra listens on port 9009. As part of installation, you can optionally change the port number.

Note

Ensure that the firewall rules which protect the Orchestra host allow traffic on the new service port.

Procedure

1. Open a command shell and log in to the Orchestra host as the root user.
2. Change directory by typing the following command:

```
cd /opt/orchestra/config
```

3. Using a Linux text editor, such as `vi`, edit `application-production.properties`.
4. Locate and uncomment the `server.port` parameter.
5. Change the value for `server.port` to the new service port number.
6. Save and close the file.
7. Restart the Orchestra service by typing the following commands:

```
service orchestra stop
service orchestra start
```

8. Verify that Orchestra responds on the new service port.

Best practices

Observe the following practices for efficient operation:

- Protect the Orchestra host by backing up to an Avamar server, especially the `/opt/orchestra` directory. This practice enables you to recover a lost Orchestra host.
- Do not modify Orchestra policies by using the local tools on an Avamar server, such as through Avamar Administrator or the AUI.

  All Orchestra policies have the unique identification prefix `orchestra-` to distinguish them from policies that are safe to edit through the local Avamar interfaces.
- After installation, control the Orchestra service like any other Linux service. The service responds to the following commands:

```
service orchestra [help|status|stop|start]
```

- When you add or edit an Avamar server, supply credentials for an Avamar software administrative user account under the root domain. For example, the MCUser account.

Troubleshooting

The Orchestra log files reside in the `/opt/orchestra/log` directory.

Examine the `orchestra.log` file for error and warning details.

Enable debug logging

To aid troubleshooting, you can enable extra logging detail and verbosity.

Procedure

1. Open a command shell and log in to the Orchestra host as the root user.
2. Change directory by typing the following command:

```
cd /opt/orchestra/config
```

3. Using a Linux text editor, such as `vi`, edit `application-production.properties`.

4. Locate the line `#logging.level.com.avamar.mc.orchestra=DEBUG`.

   Uncomment this line by removing the `#` symbol.

5. Save and close the file.
6. Restart the Orchestra service by typing the following commands:

   ```
   service orchestra stop
   service orchestra start
   ```

CHAPTER 2

Orchestra Web UI

This chapter contains the following topics:

- Orchestra Web UI 20
- Access the Orchestra Web UI 20
- Navigation pane 21
- UI header pane 21
- System pane 22
- Policy pane 24
- Activity Monitor 32
- Event pane 35
- Task pane 37

Orchestra Web UI

The Orchestra Web User Interface is a web management application that provides a centralized location for managing and monitoring multiple Avamar servers.

The Orchestra Web UI builds on the layout and functionality of the AUI. Many operations in the Orchestra Web UI have counterparts in the AUI. For these reasons, Dell EMC recommends that administrators become familiar with the AUI before using the Orchestra Web UI.

You can use the Orchestra Web UI to monitor backups, restore operations, and system maintenance activities, and to configure backup policies and configure other system settings.

You can administer multiple Avamar servers from the Orchestra Web UI.

The **System** pane appears when you log in to the UI. The **System** pane provides an at-a-glance view of system status for all Avamar servers. A navigation pane provides access to all functionality.

Access the Orchestra Web UI

Access the Orchestra Web UI through a Chrome web browser. To understand how the Orchestra Web UI integrates with the Orchestra REST API, open the Developer Tools in Chrome, and then check the network request for the Orchestra REST API.

Procedure

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

   `https://orchestrahost:9009`

   where *orchestrahost* is the DNS name or IP address of the Orchestra host.

   Note

   If the environment does not meet HTTPS certificate validation requirements, the certificate validation fails and an error message is displayed asking if you want to continue. Ignoring certificate validation might cause security issues.

2. In the **Username** field, type the username for the Orchestra administrator (usually `admin`).
3. In the **Password** field, type the password for the Orchestra administrator.
4. Click **Log In**.

   The **System** pane is displayed.

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

   The navigation pane opens and displays the available menu items.

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 Orchestra Web UI.

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

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 Orchestra Web UI.

Table 4 Orchestra Web UI navigation pane

Navigation link	Icon	Available features
System		Provides an at-a-glance view of server events, status, and activities for all Avamar servers. You can also add, edit, or delete an Avamar server.
Policy		Create and manage groups, datasets, schedules, and retention policies that you can apply to multiple Avamar servers.
Activity		Provides status and detailed information for backup, restore, and backup validation activity.
Event		Monitors operational status and server activity. Example of Avamar events include client registration and activation, successful and failed backups, and hard disk status.
Task		Monitors the status and result of the interactions between Orchestra and the Avamar REST API.

UI header pane

The UI header pane resides at the top of the window. Within the UI header pane, the user menu contains common controls that you can access from any area of the interface.

The user menu provides access to the following information and tasks:

- Version and build details
- Swagger UI
- Password configuration
- Log out of the UI

View product information

To view version and build details, click in the UI header pane, and then click **About**.

Access the Swagger UI

To access the Swagger UI, click in the UI header pane, and then click **Help**.

Change the Orchestra administrator password

Use the following procedure to change the password for the administrator account.

Procedure

1. In the UI header pane, click , and then click **Config**.

   The **Configuration** panel is displayed.
2. In the **Old password** field, type the existing password for the Orchestra administrator.
3. In the **New password** field, type the new password for the Orchestra administrator.
4. In the **Confirm password** field, type the new password again.
5. To save the changes, click **SUBMIT**.

Log out of the Orchestra Web UI

To log out of the UI, click in the UI header pane, and then click **Logout**.

System pane

The **System** pane provides an at-a-glance view of system status for all Avamar servers. It also provides tools for the management of Avamar servers.

Use the **System** pane to monitor server events, status, and activities for an Avamar server. You can also add an Avamar server, remove an Avamar server, or edit the settings for an Avamar server.

Monitoring Avamar servers

The **System** pane provides access to high-level information about each Avamar server.

The following table describes the information that is available in the **System** pane.

Table 5 Information available in the **System** pane

Information	Description
Alias	Unique identifier for the Avamar server.
Host Name	Hostname or IP address of the Avamar server. To access the AUI for a specific Avamar server, click the host name link.
Version	Version of Avamar server software that is installed on the Avamar server.
User	Root or administrator user.
Status	Current state of the Avamar server:

Table 5 Information available in the **System** pane (continued)

Information	Description
	• **Active** indicates the server is healthy and running. • **Inactive** indicates the Orchestra software cannot connect to the Avamar server. If the server is inactive, check the health of the server.
Events	Indicates the number of unacknowledged system errors and warnings that have occurred, as well as certain defined system alerts. The following columns display this information: • **Critical event** • **Error event** • **Warning event** To clear these serious system errors and warnings (that is, reset the count to zero), you must explicitly acknowledge them. You can acknowledge an event from the **Event** pane. To open the **Event** pane and view detailed information about critical, error, or warning events, click the link in its respective column. The *Avamar Administration Guide* provides more information.
Activities	Indicates the number of activities that are in a **Waiting**, **Running**, **Completed**, or **Failed** state. To view detailed information about warning, waiting, running, completed, or failed activities, click the link in its respective column. The *Avamar Administration Guide* provides more information.

Add an Avamar server

To enable management of an Avamar server in the Orchestra Web UI, add an Avamar server.

Procedure

1. In the navigation pane on the left, click ≫, and then click **System**.
2. To add an Avamar server, click +**ADD**.

   The **Add Avamar System** wizard is displayed and opens to the **Connection Information** page.
3. In the **Alias** field, type the alias for the Avamar server.
4. In the **Hostname** field, type the IP address or fully qualified hostname of the Avamar server.
5. In the **Username** field, type the username for an Avamar server.
6. In the **Password** field, type the password for the user.
7. In the **Port** field, type the port number for the Avamar REST API.
8. Click **NEXT**.

   The **Certification Information** pane is displayed.

9. Review the certificate details, and then select **Accept Certificate**.
10. Click **ADD**.

    The Orchestra Web UI adds the Avamar server.

Edit an Avamar server

You can change the connection and certification information for an Avamar server.

Procedure

1. In the navigation pane on the left, click ≫, and then click **System**.
2. Select an Avamar server from the list, and then click **EDIT**.

   The **Edit Avamar System** wizard is displayed where you can modify the connection and certification information for the Avamar server.

Delete an Avamar server

You can delete an Avamar server from the Orchestra Web UI.

Procedure

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

   The **System** pane is displayed.
2. Select the Avamar server that you want to remove, and then click **DELETE**.

   A confirmation message appears.
3. Click **OK**.

Policy pane

The **Policy** pane enables you to create and manage a backup policy that can be applied to multiple Avamar servers.

A 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.

Use the **Policy** pane to add a backup policy, remove a backup policy, or edit an existing backup policy.

Viewing policy details

You can view details for a backup policy that has been assigned to one or more Avamar servers. The policy details that are described in the following table appear in the **Policy details** panel.

Table 6 Policy details

Information	Description
Basic information	
Domain	Full location in the Avamar server.

Table 6 Policy details (continued)

Information	Description
Name	The name of the Orchestra policy that starts with the prefix `orchestra-`
Enabled	Whether Avamar can perform backups for the client. Regardless of this setting, the client can restore files if a previous backup exists in the system.
Override schedule	Defines the available start times for clients that have the **Override group schedules** setting enabled. This schedule is editable. Copies of this schedule are not used with the **Override group schedules** setting.
Avamars	The Avamar servers that have the backup policy assigned to them. If the backup policy exists on the Avamar server, then the **Policy exists on Avamar** column indicates `true`. If the backup policy does not exist on the Avamar server, then this column indicates `false`. This situation might occur if the backup policy fails to publish to the Avamar server, or if the administrative user deletes the policy in the AUI or Avamar Administrator. If settings for a backup policy are the same in Orchestra and on the Avamar server, the **Has difference between Orchestra and Avamar** indicates **true**. If the settings for a backup policy have been modified at the Avamar server level and do not match the settings for the backup policy in Orchestra, the **Has difference between Orchestra and Avamar** column indicates **false**. This situation might occur if the administrative user modifies the backup policy in the AUI or Avamar Administrator. To compare the settings for the backup policy in Orchestra and on the Avamar server, click **VIEW** in the **Actions** column.
Dataset	
Targets	Defines the source data plug-in for the backup policy.
Schedule	
Recurrence type	Defines how often the schedule runs: • Daily • Weekly • Monthly
Delay until	Date and time that the schedule takes effect.
End after	Date and time that the schedule ends.
Backup windows duration	The maximum duration of the schedule.
Scheduled weekdays	The days of the week that the schedule runs.
Start Time	Time that the backup policy is scheduled to begin.

Table 6 Policy details (continued)

Information	Description
Retention	
Retention period	The number of days, weeks, months, or years until a backup expires.

Managing backup policies

The **Policy** pane provides access to backup policy tasks and information.

The **Policy** pane 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

The *Avamar Administration Guide* provides more information about backup policies.

Create a backup policy

You can create a backup policy and assign it to one or more Avamar servers.

When you create a backup policy, you define the dataset, schedule, and retention settings that are applied to a client or a group of clients. A backup policy must contain at least one Avamar client. If the backup policy contains two or more clients, the clients must belong to the same Avamar domain. You can override backup policy settings at the client level.

Procedure

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

   The **Policy** pane is displayed.

2. To add a backup policy, click +**ADD**.

   The **Create Avamar Policy** wizard is displayed and opens to the **Properties** page.

Configure backup policy properties

Configure backup policy properties, including creating a name for the backup policy, enabling the backup policy, setting an override schedule, and applying the policy to one or more Avamar servers.

Complete the following tasks from the **Properties** page of the **Create Avamar Policy** wizard.

To access the **Properties** page of the **Create Avamar Policy** wizard:

- In the navigation pane on the left, click ≫, and then click **Policy**.
- In the **Policy** pane, click +**ADD**.

Procedure

1. In the **Name** field, type a name for the backup policy.

   By default, Orchestra adds the prefix `orchestra-` before the name of the policy.

   Note

   If a backup policy exists with the same name, Orchestra overwrites the existing backup policy.

2. Toggle the **Show Advanced Options** switch to view advanced configuration options.
3. To use this backup policy for scheduled client backups, select the **Enabled** check box.

   Clearing the check box disables backups for the backup policy.

4. To override the assigned schedule for this backup policy, select **Override Schedule**:
   - To skip the next scheduled backup, select **Skip Next Backup**.
   - To perform the next scheduled backup one time only, select **Run Next Backup Once**.
5. Select one or more Avamar servers to which you want to assign the backup policy.
6. To apply the backup policy to selected clients or remove a backup policy from selected clients and complete the wizard, click **NEXT**.

   The **Members** page is displayed.

Add or remove members to a backup policy

You can configure backup policy attributes, including applying the backup policy to selected clients or removing a backup policy from selected clients. You can add clients when you create or add or remove clients when you edit a back policy.

Complete the following steps from the **Members** page of the **Create Avamar Policy** wizard.

To access the **Members** page of the **Create Avamar Policy** wizard, in the navigation pane on the left, click ≫, and then click **Policy**.

Procedure

1. In the drop-down list, select an Avamar server.
2. 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.

3. To add clients to a backup policy:

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

   b. Click **NEXT**.

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

4. To remove clients from a backup policy:
   a. In the list of clients, clear the clients that you want to remove.
   b. Click **NEXT**.

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

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

   The **Dataset** page appears.

Add a dataset to a backup policy

You can configure backup policy attributes, including adding a dataset.

Complete the following tasks from the **Dataset** page of the **Create Avamar Policy** wizard.

To access the **Dataset** page of the **Create Avamar Policy** wizard:

- In the navigation pane on the left, click ≫, and then click **Policy**.
- In the **Policy** pane, click +**ADD**.

Note

When the Avamar server is using Data Domain for back-end storage, the Data Domain system is the default backup storage location.

Procedure

1. From the **Plugin** list, select the plug-ins to use for the backups.

   If you selected more than one client, the **Plugin** list displays all plug-ins for the selected clients. For example, if you select one Windows client and one Linux client, the Windows File System plug-in and Linux File System plug-in appear in the list.

2. Click the **Source Data** tab, and then define the source data plug-ins that contribute data to this dataset:
   a. To back up all available data with the plug in, select the first option.
   b. To type the path to the data to back up:
      - Select the **File/Folder Path** option, and then press **Enter**.
      - Type the path in the **File/Folder Path** field.

      You can limit scheduled backups to a set of data by specifying the path to the data in the dataset. The following rules apply when you type the path:

      - If you are using a file system plug-in, the first occurrence of an asterisk (`*`) in a path is treated as a folder wildcard. For example, to specify the `My Documents` folder for all users on a Windows computer, type **`C:\Documents and Settings\*\My Documents`**.
      - To specify the `Documents` folder for all users on a Macintosh, type **`/Users/*/Documents`**.
      - When you specify a data path, only the first occurrence of an asterisk is treated as a folder wildcard. Subsequent occurrences are interpreted literally.

- The path can include alphanumeric characters (A-Z, a-z, 0–9) and an asterisk (*) as a wildcard. Do not use any of the following characters in the data path: `~!@$^%(){}[]|,`;#:*?<>'"&`

3. Click the **Options** tab, and then set plug in options either by using the graphical controls or by typing option names and values as text entries.

   Plug-in options enable you to further customize the behavior of a dataset. The user guide for each plug-in provides details on the options available for the plugin.

4. To select a Data Domain system to use for back-end storage and complete the wizard, click **NEXT**.

Add a Data Domain system

When the Avamar server is using Data Domain for back-end storage, the Data Domain system is the default backup storage location.

Procedure

1. To automatically select the Data Domain system for the dataset, select the **Auto set Data Domain for dataset** check box.

   Orchestra automatically selects the Data Domain system:

   - If an Avamar server is using only one Data Domain system, this system stores the backup.
   - If an Avamar server is using multiple Data Domain systems, the Avamar server stores the backup on the Data Domain with the largest available capacity.

   Note

   When the Avamar server is not using a Data Domain for back-end storage, the Avamar server stores the backup on the GSAN.

2. To specify the Data Domain system for the dataset:

   a. Select the **Select Data Domain for each Avamar** check box.

   b. In the list, select the Data Domain system to use for each Avamar server.

      If an Avamar server is not using a Data Domain system as a backup target, the Avamar server does not appear in the list. The Avamar server stores the backup on the GSAN.

3. To add a schedule to a backup policy and complete the wizard, click **NEXT**.

   The **Schedule** page is displayed.

Add a schedule to a backup policy

You can configure backup policy attributes, including adding a schedule.

Complete the following tasks from the **Schedule** page of the **Create Avamar Policy** wizard.

To access the **Schedule** page of the **Create Avamar Policy** wizard:

- In the navigation pane on the left, click ≫, and then click **Policy**.
- In the **Policy** pane, click + **ADD**.

Procedure

1. In the **Schedule start date** field, select the date when the schedule should take effect.
2. In the **Schedule end date** field, choose when to discontinue to schedule:
   - To enable a schedule to run indefinitely, select **No End Date**.
   - To discontinue a schedule on a specific date, select **End after** and then select a date from the list.
3. In the **Backup Window** field, type a number of hours.
4. In the **Recurrence Type** field, choose the schedule type:

Table 7 Settings for each type of schedule

Schedule type	Settings
Daily	To select the recurrence pattern by interval, perform the following steps: a. Select **By interval**. b. In the **From** field, select the time when the schedule should take effect. To make a schedule effective immediately, select the current time. c. In the **To** field, select the time when the schedule should end. d. Select the interval. e. Click **ADD**. The selected times appear in the list. f. Click **NEXT**. To select the recurrence pattern by a point in time, perform the following steps: a. Select **By time point**. b. Specify the time. To make a schedule effective immediately, select the current time. c. Click **ADD**. The selected times appear in the list. d. Click **NEXT**. The **Retention** window is displayed **Note** To prevent job overlap, limit the duration of scheduled system activities.
Weekly	a. Select the check box next to the days of the week on which the schedule should run. To select all week days, click **TOGGLE SELECTION**. b. In the **Schedule Time** field, define the activity operating hours. You can type the times, or select the time and use the arrow buttons to change the times. The server workload affects the start time for an activity. Also, the first time that a backup is performed for any client, the backup is

Table 7 Settings for each type of schedule (continued)

Schedule type	Settings
	allowed to continue past the specified end time. This behavior is permitted because initial backups can take longer than subsequent backups of the same client. c. Click **NEXT**. The **Retention** window is displayed
Monthly	a. Choose whether to repeat the activity on a specific calendar date or on a designated day of the week each month: • To repeat the activity on a specific calendar date, select **Day ... of month**, and then select the day from the list. • To repeat the activity on a designated day of the week each month, select **The ... of month** and then select the day from the lists. b. Click **NEXT**. The **Retention** window is displayed

Apply retention to a backup policy

You can configure backup policy attributes, including adding retention.

Complete the following tasks from the **Retention** page of the **Create Avamar Policy** wizard.

To access the **Retention** page of the **Create Avamar Policy** wizard:

- In the navigation pane on the left, click ≫, and then click **Policy**.
- In the **Policy** pane, click +**ADD**.

Note

Best practice is to specify a retention that is greater than or equal to 14 days. When you create a retention policy for less than 14 days, an alert is displayed.

Procedure

1. To delete backups automatically after a specific number of days, weeks, months, or years:
   a. Select **Retention period**.
   b. Specify the number of days, weeks, months, or years.
2. To delete backups automatically on a specific calendar date:
   a. Select **End Date**.
   b. Browse to that date on the calendar.
3. To keep backups for the period that a client is active, select **No End Date**.
4. To review a summary of the backup policy and complete the wizard, click **NEXT**.

   The **Summary** page is displayed.

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 navigation pane on the left, click ≫, and then click **Policy**.

   The **Policy** pane is displayed.

2. Select a backup policy from the list, and then click **EDIT**.

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

Delete a backup policy

You can delete a backup policy from the Orchestra Web UI.

Before you begin

When deleting a backup policy, assign the clients in the backup policy that you would like to delete to a different backup policy so that scheduled backups for the clients can continue uninterrupted.

Procedure

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

   The **Policy** pane is displayed.

2. Select that backup policy that you want to remove, and then click **DELETE**.

   A confirmation message is displayed.

3. Click **OK**.

Activity Monitor

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

Most of the operations that you can perform through the **Activity Monitor** have direct counterparts in the AUI for an individual Avamar server.

Activity monitoring

The **Activity Monitor** provides status and detailed information for backup, restore, and backup validation activity.

Each activity contains the information in the following table:

Table 8 Information in the **Activity Monitor**

Information	Description
Status	Status of the backup, restore, validation, or replication activity.
Client	Avamar client name

Table 8 Information in the **Activity Monitor** (continued)

Information	Description
Started	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.
Processed Byes	Total number of bytes examined during this activity.
Plugin	Plug-in that is used for this activity.
Type	The type of activity.

View activities in the Activity Monitor

You can view activity details for a specific Avamar server and filter the information that appears.

Procedure

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

   The **Activity Monitor** is displayed.

2. To view events for a specific Avamar server, in the **Avamar** drop-down list, select an Avamar server.

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

   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:
     - Waiting
     - Running
     - Completed
     - Failed

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

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

   The *Avamar Administration Guide* provides more information about the details that are available for an activity.

View a detailed client session log

The **Activity Monitor** enables you to view a detailed log of a client session to perform analysis or troubleshooting.

Procedure

1. In the 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 backups

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

Procedure

1. In the 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 **Type** column.

   b. Type `On-Demand Backup`.

   c. Press **Enter**.

Restart a backup job

You can restart a completed or failed backup job in the **Activity Monitor**.

Procedure

1. In the 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.

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 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**.

Monitor restores

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

Procedure

1. In the 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 restore activity:

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

   b. Type `Restore`.

   c. Press **Enter**.

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 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**.

Event pane

The **Event** pane enables you to investigate any system errors or warnings that have occurred. You can also clear any unacknowledged events.

Event monitoring

All Avamar system activity and operational status is reported as events in the **Event** pane. Examples of Avamar events include client registration and activation, successful and failed backups, and hard disk status.

Each event contains the information in the following table:

Table 9 Information in the **Event** pane

Information	Description
Event ID	Unique identifier
Date and time	Date and time the event was reported
Category	Category of event: • SYSTEM • APPLICATION • USER • SECURITY
Type	Type of event: • CRITICAL • ERROR • WARNING • INFORMATION • AUDIT • DEBUG • INTERNAL
Summary	A description of the event
Acknowledge	Whether the event has been acknowledged

View events in the Event pane

You can view event details for a specific Avamar server and filter the information that appears.

Procedure

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

   The **Event** pane is displayed.

2. To view events for a specific Avamar server, in the **Avamar** drop-down list, select an Avamar server.

   The Orchestra Web UI displays a list of unacknowledged serious system errors and warnings that have occurred, as well as certain defined system alerts.

   The **Event** pane provides you with options to filter the information that appears.

   To filter the results, click 🔍 **FILTER**:

- Filter events by date—Specify the range of dates for the events to display by using the **From** and **To** fields.
- Filter events by type—To display only the events for a specific type, in the **Type** list, select the type of events to display.
- Filter events by category—To display only the events for a specific category, in the **Category** list, select the category of events to display.
- Filter events by acknowledgment status—To display only unacknowledged events, select the **Unacknowledged event only** check box.

Acknowledge system events

System events that are configured to require acknowledgment each time they occur, remain in the unacknowledged events list until they are explicitly cleared, or acknowledged, by an Avamar server administrator.

Procedure

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

   The **Event** pane is displayed.
2. Select one or more unacknowledged events from the list, and then click **ACKNOWLEDGE**.

Task pane

The **Task** pane enables you to monitor the status and result of the interactions between Orchestra and the Avamar REST API.

To access the **Task** pane, in the navigation pane on the left, click ≫, and then click **Task**.

A task is an operation performed by Orchestra on one or more Avamar servers, such as configuring a policy and assigning the policy to particular servers. Subtasks are the underlying calls from Orchestra to the Avamar REST API that complete a task. To view subtasks, click > next to the task.

The following table describes the information that is available in the **Task** pane:

Table 10 Information available in the **Task** pane

Information	Description
ID	Unique identifier for the task or subtask.
Name	The name of the task or subtask.
Status	The status of the task or subtask: • QUEUE • RUNNING • SUCCESS • FAIL • PARTIAL SUCCESS
Create Time	The date and time that the task or subtask was created in Orchestra.

Table 10 Information available in the **Task** pane (continued)

Information	Description
Start Time	The date and time that the task or subtask began.
Complete Time	The date and time that the task or subtask completed.
Error	Indicates that a problem occurred during the operation.

Note

Orchestra retains only the last 1000 tasks in memory. Restarting Orchestra clears the list of tasks.

CHAPTER 3

Orchestra REST API

This chapter contains the following topics:

- About the Orchestra REST API 40
- About Swagger 41
- Orchestra REST API examples 41
- Testing the Orchestra REST API 42
- Using the Orchestra proxy API 44

About the Orchestra REST API

The available operations for the Orchestra REST API are related to the operations of the Avamar server REST API. However, Orchestra introduces a level of abstraction that directs calls to all applicable registered servers. A full list of Orchestra functionality is available from the Swagger user interface.

When you interact with Orchestra, the API transparently manages the individual connections to the registered servers. Orchestra obtains, holds, and supplies the required authentication tokens on your behalf. If you need to interact directly with a particular Avamar server, use the proxy API instead of establishing a separate connection.

The *Avamar REST API Getting Started Guide* provides more information about commands that you can issue to individual Avamar servers through the proxy API.

Orchestra REST API components

The Orchestra REST API consists of three separate APIs that implement different areas of functionality.

Basic API

The basic API defines interaction with Orchestra itself. For example, this API contains the functions that control authorization tokens and monitor the status of running Orchestra tasks.

Proxy API

The proxy API handles requests that should be redirected to a particular Avamar server. This way, a calling application does not need to establish a direct link to that server's Avamar REST API interface.

Backup group API

The backup group API defines group operations that occur in parallel on different Avamar servers. For example, creating a backup group across servers and publishing the resulting policy to the selected Avamar servers.

Authentication tokens

Most Orchestra operations require authorization. Orchestra handles authentication like other Avamar REST APIs, where a user authenticates with a username and password. The host provides a corresponding token that lasts for the duration of the session.

An authentication token is an encrypted string that operates like the identifier in a browser cookie. Since HTTP is a stateless protocol, using the authentication token prevents having to supply credentials with every request.

Use the `/api/login` method to supply credentials to the Orchestra host. After you receive an authentication token, supply the token in the header of each subsequent request.

About Swagger

The Swagger user interface (UI) contains a complete listing and description of the available Orchestra REST API functions, including the applicable object models for constructing API calls.

Access the Swagger UI by opening a web browser and typing `https://orchestrahost:9009/swagger-ui.html`, where *orchestrahost* is the IP address or hostname of the Orchestra host.

By default, the Swagger UI shows documentation for the Orchestra basic API. From the **Select a spec** drop-down list, select `Avamar` to see more information about the available API calls for Avamar operations.

Note

With proper authorization, the Swagger UI can construct and call example REST API commands for testing, and return the results for verification. Dell EMC recommends that you issue only API calls that read from the server.

Swagger navigational controls

The Swagger UI presents available operations in themed groups. Expand each group to see the list of related operations.

The list of operations within each group is color-coded to indicate the applicable HTTP method. Click the name of each operation to expand for more detail. The Swagger UI shows the operation URL, the applicable input parameters and syntax, HTTP response codes, and the resulting data structures in the output.

The Swagger UI provides details for the Orchestra and Avamar object models in the section below the list of operation groups. Expand the **Models** list and then expand an object type to see a list of fields and data types. Where a field is of a type that holds a data structure, or provides an enumeration of accepted values, click the > to expand for details.

Almost all REST API operations require an authorization token. To obtain an authorization token, click the **Authorize** button and supply valid login credentials, and then click **Authorize**. The Swagger UI confirms authorization success or failure. Click **Close** to return to the API documentation. The padlock symbol on the **Authorize** button changes from open to closed.

To construct example API calls for any operation, obtain an authorization token. Then, click the operation name to expand the available details and click **Try it out**. The Swagger UI provides text boxes for required and optional input parameters.

When you are finished providing inputs, click **Execute**. The Swagger UI shows the specific syntax for the example, the request URL, and the response from the Orchestra host. You can download the response body for further analysis. To stop running example commands, click **Cancel**.

Orchestra REST API examples

This guide provides several examples of Orchestra REST API syntax that you can safely run on the Orchestra host.

Perform all REST API operations on `https://orchestrahost:9009`, where *orchestrahost* is the hostname or IP address of the Orchestra host.

The descriptions of input and output parameters for some operations may reference object types as defined within the Swagger UI. The object model provides more information about the corresponding definitions and data types.

Note

Authentication token strings have been simplified for these examples. If the authentication token expires, obtain a new token from the authentication operation.

Self-signed security certificates may require the use of `curl -k` to bypass SSL certificate verification.

Testing the Orchestra REST API

The following topics provide examples of REST API calls that test the functionality of the Orchestra host. For example, obtain an authorization token to verify that you have correctly installed and configured the Orchestra API.

Obtain an authentication token

Operation

POST `/api/login`

Description

Authenticates a user to the Orchestra host and returns an encrypted authentication token.

Input parameters

Body: application/json
Credentials

```
{"username":"admin_user", "password":"admin_user_password"}
```

where *admin_user* and *admin_user_password* are the credentials for the Orchestra host that you configured during installation.

The default username is "admin". The default password is "changeme".

Output parameters

Output type:
OAuth2AccessToken

application/json

The `bearer` token type means that any caller with the correct authentication token can use the token for any purpose.

Example request

```
curl -X POST "https://1.2.3.4:9009/api/login" -H "accept: application/
json" -H "Content-Type: application/json" -d '{"username":"admin",
"password":"changeme"}'

POST /api/login HTTP/1.1
accept: application/json
Content-Type: application/json
Content-Length: 43
```

Example response

```
200 OK
Content-Type: application/json;charset=UTF-8
```

```
{
  "access_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.",
  "token_type" : "bearer",
  "refresh_token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.",
  "expires_in" : 43199,
  "scope" : "all",
  "jti" : "f9ae93d6-cef7-4816-900b-43a464b74822"
}
```

Use the authentication token to access the Orchestra REST API

The following operation is a generic example of how to use an authentication token. Token authentication behaves the same way for all Orchestra REST API operations.

Operation

GET `/api/avamars`

Description

Returns a list of all registered Avamar servers.

Input parameters

Header:

Token

```
Authorization: Bearer access_token
Accept: application/json
```

where *access_token* is an encrypted Orchestra authentication token string.

Output parameters

Output type:

Avamar

application/json

The output is an array of Avamar objects, as defined by the object model in the Swagger UI.

Example request

```
curl -X GET "https://1.2.3.4:9009/api/avamars" -H "Authorization:
Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9." -H "Accept: application/
json"

GET /api/avamars HTTP/1.1
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.
Accept: application/json
```

Example response

```
200 OK
Content-Type: application/json;charset=UTF-8

[ {
  "id" : "1554270780@00:10:20:30:40:50",
  "alias" : "serverA",
  "hostname" : "2.3.4.5",
  "port" : 443,
  "username" : "MCUser",
  "password" : "",
  "heartbeat" : {
    "active" : true,
    "tokenCreatedDate" : "2019-04-17T17:59:03.759Z",
    "tokenExpireDate" : "2019-04-18T05:59:02.759Z",
    "lastDetectDate" : "2019-04-17T19:01:03.673Z",
    "failDetectionCount" : 0,
    "failTokenCreationCount" : 0,
    "error" : null
  }
```

```
}, {
  "id" : "1554171012@A0:B0:C0:D0:E0:F0",
  "alias" : "serverB",
  "hostname" : "6.7.8.9",
  "port" : 443,
  "username" : "MCUser",
  "password" : "",
  "heartbeat" : {
    "active" : true,
    "tokenCreatedDate" : "2019-04-17T17:59:03.775Z",
    "tokenExpireDate" : "2019-04-18T05:59:02.775Z",
    "lastDetectDate" : "2019-04-17T19:01:03.656Z",
    "failDetectionCount" : 0,
    "failTokenCreationCount" : 0,
    "error" : null
  } ]
```

Using the Orchestra proxy API

When you perform operations on an Avamar server through the proxy API, an extra `X-Avamar-Id` HTTP header controls the scope of the operation.

Obtain the identifiers for registered Avamar servers by calling `/api/avamars`. Avamar server IDs have the format *numeric_timestamp*@*MAC_address*. For example, `1554270780@00:10:20:30:40:50`.

Supply the `X-Avamar-Id` header with one of the following patterns:

Table 11 Header values and corresponding operational scopes

Header value	Action and scope	Notes
The unique ID that corresponds to a particular Avamar server.	The proxy API forwards the operation to the server's REST API and returns the unchanged HTTP response.	This operation is equivalent to performing the corresponding operation on the server through the Avamar REST API.
Empty value or missing header.	The proxy API forwards the operation to an Avamar server REST API and returns the unchanged HTTP response.	Orchestra uses appropriate criteria to automatically select an active Avamar server, where possible.
`ALL`	The proxy API returns an array of HTTP responses from all registered servers.	
An array of Avamar server IDs.	The proxy API returns an array of HTTP responses from the specified servers.	Supply multiple Avamar server IDs as a semicolon-delimited list. For example, **`1554270780@00:10:20:30:40:50;1554171012@A0:B0:C0:D0:E0:F0`**.

Proxy API operations have the preface `/api/restproxy`, plus the corresponding operation syntax for the Avamar REST API.

Perform a proxy operation on one Avamar server

The following operation is a generic example of how to use the Orchestra proxy API to direct an operation to a single Avamar server.

Operation

GET `/api/restproxy/api/v1/activities`

Description

Returns a list of the current activities on a registered Avamar server.

Input parameters

Header:

```
Authorization: Bearer access_token
Accept: application/json
X-Avamar-Id: avamar_id
```

where:

- *access_token* is an encrypted Orchestra authentication token string.
- *avamar_id* is the unique ID of a registered Avamar server.

Output parameters

Output type:
Activity

application/json

The output is an array of Activity objects, as defined by the object model in the Swagger UI.

Example request

```
curl -X GET "https://1.2.3.4:9009/api/restproxy/api/v1/activities?
recursive=true&page=0&size=20" -H "Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9." -H "Accept: application/json"
-H "X-Avamar-Id: 1554270780@00:10:20:30:40:50"

GET /api/restproxy/api/v1/activities?recursive=true&page=0&size=20
HTTP/1.1
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.
Accept: application/json
X-Avamar-Id: 1554270780@00:10:20:30:40:50
```

Example response

```
200 OK
Content-Type: application/json;charset=UTF-8
X-Avamar-Id: 1554270780@00:10:20:30:40:50
X-Avamar-Name: serverA

{
  "content" : [ {
    "id" : "9155548185887509",
    "wid" : "MOD-1555481858875",
    "cid" : "d5e522cfdd6c4f4671a51712c357aa4e45455bf2",
    "groupId" : null,
    "pluginNumber" : 3001,
    "type" : "On-Demand Backup",
    "state" : "SUCCESS",
    "description" : "Completed",
    "errorCode" : 0,
    "targetCid" : "d5e522cfdd6c4f4671a51712c357aa4e45455bf2",
    "parentWid" : null,
    "proxyName" : null,
    "queuedDate" : "2019-04-17T06:17:38.875Z",
    "scheduledDate" : "2019-04-17T06:17:38.875Z",
```

```
    "activatedDate" : "2019-04-17T06:18:24.679Z",
    "completedDate" : "2019-04-17T06:18:36.191Z",
    "elapsedTime" : 11512,
    "domain" : "/clients/test2",
    "clientName" : "test2",
    "groupFqdn" : "Admin On-Demand Group",
    "pluginName" : "Windows File System",
    "pluginId" : "Windows",
    "timeZone" : null,
    "phase" : 1,
    "phaseName" : null,
    "maxPhase" : 0,
    "estimatedBytes" : 3.4790326272E10,
    "retentionId" : "Default:POLICYID",
    "retention" : "Default Retention",
    "scheduleId" : null,
    "scheduleName" : "Admin On-Demand Schedule",
    "allowOvertime" : true,
    "overtimeOption" : "NEXT_SUCCESS",
    "datasetId" : "MOD-1555481858875",
    "datasetFqdn" : "/Client On-Demand Data",
    "datasetOverride" : false,
    "endStartTime" : 1555568258875,
    "endTime" : 1555568258875,
    "server" : "AVAMAR",
    "datadomain" : null,
    "datadomainId" : null,
    "destinationServer" : null,
    "scheduleRecurrence" : null,
    "retentionTags" : "N",
    "user" : "root",
    "effectiveExpiration" : 1560665858,
    "retentionPolicyOverride" : false,
    "encryption" : "high",
    "hardQuotaExceeded" : false,
    "softQuotaExceeded" : false,
    "sessionId" :
"30640230364febd28558545a754b762bec71af878b24c168974496f5d38f70b887e7d
d937bab85092d856f6fe283db9165ce502902300764b63bd8b5f7f666f56909f121b0c
15ea67faffea053bb00e7b7bb0dc32734f34448ab41eeb01cba40295d9abc900a",
    "containerCid" : null,
    "containerName" : null,
    "dispensedTime" : 1555481903855,
    "stats" : {
      "bytesProcessed" : 4.1650176E8,
      "bytesProtected" : 4.1650176E8,
      "bytesSkipped" : 0.0,
      "bytesExcluded" : 0.0,
      "bytesSent" : 0.0,
      "bytesModified" : 0.0,
      "bytesModifiedSent" : 0.0,
      "bytesModifiedNotSent" : 0.0,
      "overheadBytes" : 385.0,
      "bytesReduced" : 0.0,
      "filesSkipped" : 0.0,
      "filesProcessed" : 5.0,
      "filesModified" : 0.0,
      "percentOfProcessedSent" : 0.0,
      "clientVersion" : "18.2.101-134",
      "clientOs" : "Windows 7 Ultimate Edition Service Pack 1 64-bit",
      "label" : "MOD-1555481858875",
      "labelNumber" : "2"
    },
    "canceling" : false,
    "codeReason" : "Activity completed successfully.",
    "children" : null
  } ]
}
```

Perform a proxy operation on all registered Avamar servers

The following operation is a generic example of how to use the Orchestra proxy API to direct an operation to all registered Avamar servers.

Operation

GET `/api/restproxy/api/v1/events/status`

Description

Returns the event statistics for a registered Avamar server.

Input parameters

Header:

```
Authorization: Bearer access_token
Accept: application/json
X-Avamar-Id: ALL
```

where *access_token* is an encrypted Orchestra authentication token string.

Output parameters

Output type:
application/json

```
[ {
  "taskSucceed" : boolean,
  "httpStatusCode" : integer($int32),
  "responseBody" : EventStatus,
  "avamarVo" : AvamarVO
} ]
```

The output is an array of responses that encapsulate the server identification, return data, and operation status. Here, the output contains EventStatus and AvamarVO objects, as defined by the object model in the Swagger UI.

The AvamarVO indicates the corresponding Avamar server, while the `responseBody` field contains the original return from the Avamar REST API.

Example request

```
curl -X GET "https://1.2.3.4:9009/api/restproxy/api/v1/events/status"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9." -H
"Accept: application/json" -H "X-Avamar-Id: ALL"

GET /api/restproxy/api/v1/events/status HTTP/1.1
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.
Accept: application/json
X-Avamar-Id: ALL
```

Example response

```
200 OK
Content-Type: application/json;charset=UTF-8

[ {
  "taskSucceed" : true,
  "httpStatusCode" : 200,
  "responseBody" : {
    "dataIntegrityAlertsCount" : 0,
    "unackErrorEventCountExclude22426" : 45,
    "unackWarningEventCount" : 0
  },
  "avamarVo" : {
    "id" : "1554270780@00:10:20:30:40:50",
    "alias" : "serverA",
    "hostname" : "2.3.4.5"
  }
}, {
```

```
"taskSucceed" : true,
"httpStatusCode" : 200,
"responseBody" : {
  "dataIntegrityAlertsCount" : 0,
  "unackErrorEventCountExclude22426" : 29,
  "unackWarningEventCount" : 0
},
"avamarVo" : {
  "id" : "1554171012@A0:B0:C0:D0:E0:F0",
  "alias" : "serverB",
  "hostname" : "6.7.8.9"
} ]
```