Monitoring HPE: Edge Connect (Silver Peak)

HPE: Edge Connect (Silver Peak) PowerPack version 101

Table of Contents

Chapter

1

Introduction

Overview

This manual describes how to monitor HPE: Edge Connect (Silver Peak) devices in SL1 using the *HPE: Edge Connect (Silver Peak)* PowerPack.

The following sections provide an overview of HPE: Edge Connect (Silver Peak) and the *HPE: Edge Connect (Silver Peak)* PowerPack:

This chapter covers the following topics:

> **NOTE:** ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is HPE: Edge Connect (Silver Peak)?

HPE: Edge Connect (Silver Peak) is an SD-WAN management solution that captures data and information from the Silver Peak Unity Orchestrator about devices connected through Unity EdgeConnect. Users can measure the performance and availability of these devices and the connected network, which helps determine potential service delivery issues and maintain compliance.

What Does the HPE: Edge Connect (Silver Peak) PowerPack Monitor?

To monitor HPE: Edge Connect (Silver Peak) using SL1, you must install the *HPE: Edge Connect (Silver Peak)* PowerPack. This PowerPack enables you to discover, model, and collect data about Silver Peak Unity Orchestrator and devices connected via Unity EdgeConnect.

The *HPE: Edge Connect (Silver Peak)* PowerPack includes:

- A sample credential you can use as a template to create SOAP/XML credentials to connect to the Unity Orchestrator you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics, and to collect configuration data for Unity Orchestrator and connected devices
- Device Classes for each of the HPE: Edge Connect (Silver Peak) devices that SL1 monitors
- Event Policies and corresponding alerts that are triggered when New Relic services meet certain status criteria
- A device template for HPE: Edge Connect (Silver Peak) Unity Orchestrator
- A dashboard that displays key metrics for each device

Installing the HPE: Edge Connect (Silver Peak) PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *HPE: Edge Connect (Silver Peak)* PowerPack.

> **TIP:** By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the *Enable Selective PowerPack Field Protection* setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the *System Administration* manual.)

> **IMPORTANT:** The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the [ScienceLogic Support Site](#).
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.

5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.

6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter

2

Configuration and Discovery

Overview

The following sections describe how to configure and discover New Relic services for monitoring by SL1 using the *HPE: Edge Connect (Silver Peak)* PowerPack:

This chapter covers the following topics:

Prerequisites for Monitoring HPE: Edge Connect (Silver Peak)

To configure the SL1 system to monitor Silver Peak Unity Orchestrator and edge devices using the *HPE: Edge Connect (Silver Peak)* PowerPack, you must have the following information about the Unity Orchestrator that you want to monitor:

- The IP address or URL of your Orchestrator

- The username and password for the administrator account on your Orchestrator

Enabling Legacy API Support

Version 9.3.0 of HPE: Edge Connect updated 3 APIs which caused issues with existing Dynamic Applications:

- HPE: Edge Connect Appliance Alarms

- HPE: Edge Connect Orchestrator Alarms Summary Stats

- HPE: Edge Connect Appliance Config

If you are using version 9.3.1 or newer of HPE: Edge Connect (Silver Peak), enable the *enableLegacyApisSupport* setting in the HPE: Edge Connect user interface. Additionally, be sure to follow the steps below and add the *Accept-Encoding:identity* HTTP Header to your credentials to support HPE: Edge Connect Orchestrater versions 9.3.1 and newer.

> **WARNING**: Version 9.3.0 of HPE: Edge Connect is not supported by the HPE: Edge Connect (Silver Peak) PowerPack. ScienceLogic recommends updating to version 9.3.1 or later.

Creating an API Credential for HPE: Edge Connect (Silver Peak)

To configure SL1 to monitor HPE: Edge Connect (Silver Peak), you must create a credential. This credential allows the Dynamic Applications in the *HPE: Edge Connect (Silver Peak)* PowerPack to communicate with your HPE: Edge Connect (Silver Peak) Unity Orchestrator.

> **TIP:** ScienceLogic encourages you to use an API Key for authorization instead of any other method. API key authorization is more efficient and resilient. If you have existing authentication issues, ScienceLogic suggests switching to use an API key authorization. If you need to collect with both Cookie (username/password) AND API key methods, ScienceLogic recommends separating the methods into separate SL1 credentials to avoid confusion.

To configure an API credential to access the Orchestrator:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Locate the **HPE: Edge Connect API Key Example** credential, and then click its wrench icon ( ). The **Edit SOAP/XML Credential** modal appears.

3. Enter values in the following fields:
   - *Profile Name*. Enter a new name for the credential.

   - *URL*. Enter the URL or IP address for the Orchestrator

4. Add the following **HTTP Headers**:

    - content-type: application/json

    - X-Auth-Token: <api_key>

    - Accept-Encoding:identity

5. For all other fields, use the default values.

6. Click the **[Save As]** button.

NOTE: The "Accept-Encoding:identity" HTTP Header is needed to support HPE: Edge Connect Orchestrater versions 9.3.1 and newer. Be sure to create a different credential for each orchestrator you want to discover.

Creating a SOAP/XML Credential for HPE: Edge Connect (Silver Peak)

To configure SL1 to monitor HPE: Edge Connect (Silver Peak), you must create a credential. This credential allows the Dynamic Applications in the *HPE: Edge Connect (Silver Peak)* PowerPack to communicate with your HPE: Edge Connect (Silver Peak) Unity Orchestrator.

TIP: ScienceLogic encourages you to use an API Key for authorization instead of any other method. API key authorization is more efficient and resilient. If you have existing authentication issues, ScienceLogic suggests switching to use an API key authorization. If you need to collect with both Cookie (username/password) AND API key methods, ScienceLogic recommends separating the methods into separate SL1 credentials to avoid confusion.

To configure a SOAP/XML credential to access the Orchestrator:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Locate the **HPE: Edge Connect Cookie Example** credential, and then click its wrench icon ( ). The **Edit SOAP/XML Credential** modal appears.

3. Enter values in the following fields:

    Basic Settings

    - *Profile Name*. Enter a new name for the credential.

    - *URL*. Enter the URL or IP address for the Orchestrator

    - *HTTP Auth User*. Enter the username for the user account on your Orchestrator.

    - *HTTP Auth Password*. Enter the password for the user account on your Orchestrator.

> **NOTE:** As of version 9.2 of the Orchestrator, the API user for the credential in SL1 must be a "non-RBAC" user with read-only permissions and no user role applied.

4. Add the following **HTTP Headers**:

   - cookie_auth:gms/rest/authentication/login
   - content-type: application/json
   - cookie_logout:gms/rest/authentication/logout
   - Accept-Encoding:identity

5. For all other fields, use the default values.

6. Click the **[Save As]** button.

> **NOTE:** The "Accept-Encoding:identity" HTTP Header is needed to support HPE: Edge Connect Orchestrater versions 9.3.1 and newer. Be sure to create a different credential for each orchestrator you want to discover.

Creating a Virtual Device for the Orchestrator

To configure SL1 to monitor HPE: Edge Connect (Silver Peak), you must create a virtual device to represent your Orchestrator. The PowerPack includes a Device Class (HPE: Edge Connect Orchestrator) for the Orchestrator.

To create a virtual device, you must complete the following tasks:

1. Go to the **Device Manager** page (Registry > Devices > Device ManagerDevices > Device Manager).

2. From the **[Actions]** menu, select *Create Virtual Device*.

3. The **Create Virtual Device** modal appears.

4. Supply a value in each of the following fields:

   - *Device Name*. Name of the virtual device. Can be any combination of alphanumeric characters, up to 32 characters in length.
   - *Organization*. Organization to associate with the virtual device. Select from the drop-down list of all organizations in SL1.
   - *Device Class*. The device class to associate with the virtual device. Select *HPE: Edge Connect Orchestrator* from the drop-down list of device classes.
   - *Collector*. Specifies which instance of SL1 will perform auto-discovery and gather data from the device. Can also specify a "virtual" poller. Select from the drop-down list of all collectors in SL1.

5. Select the **[Add]** button to save the new virtual device.

NOTE: For more information about virtual devices, see *Virtual Devices* in the Device Management manual.

Aligning the Virtual Device with the Device Template

When SL1 discovers a device, SL1 applies some default configuration settings to that device. You can edit these settings or use a device template to edit the settings for one or more devices. In this step, you will use the "HPE: Edge Connect Orchestrator Template" to apply a configuration to your HPE: Edge Connect (Silver Peak) Unity Orchestrator.

To use a device template to change the configuration of one or more devices:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

2. In the **Device Manager** page, select the checkbox for your Orchestrator virtual device.

3. In the *Select Actions* field, in the lower right, select the option *Modify by Template*. Click the **[Go]** button.

4. The **Bulk Device Configuration** page appears.

   - In the *Template* field, select "HPE: Edge Connect Orchestrator Template".

   - *Save When Applied & Confirmed*. From the **Bulk Device Configuration** page, you can edit the value in any of the fields in any of the tabs of the device template.

     ○ *If you select this field*, any changes you make to fields in the **Bulk Device Configuration** page will be saved to the template.

     ○ *If you don't select this field*, you can edit the values in any of the fields, and the edited values won't be saved in the device template, but will be applied to the device group.

5. Click the **[Apply]** button to apply the device template and any changed field values to the selected device.

6. The **Device Setting Confirmation** page appears.

   - In this page, you can view any settings in the device template that are different from SL1 default settings.

   - You can click a field to disable it. When you disabled a field, its value will not be applied to the selected device group or selected devices.

   - You can also view a list of devices to which the device template will be applied.

7. To approve the changes and the device list, click the **[Confirm]** button in the **Device Setting Confirmation** page.

8. The device template will be applied to the selected device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the HPE: Edge Connect (Silver Peak) Unity Orchestrator. From the **Device Properties** page for the Orchestrator, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

2. All applicable Dynamic Applications for the service are automatically aligned during discovery.

> **NOTE:** It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

You should see the following Dynamic Applications aligned to the New Relic service:

- REST: Performance Metrics Monitor
- HPE: Edge Connect Appliance Alarms
- HPE: Edge Connect Orchestrator Alarm Summary Stats
- HPE: Edge Connect Orchestrator Performance
- HPE: Edge Connect Orchestrator Alarms
- HPE: Edge Connect Orchestrator Configuration
- HPE: Edge Connect Root Group Discovery

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

1. Click the **[Action]** button, and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:

2. In the **Dynamic Applications** field, select the Dynamic Application you want to align. You can narrow the search, as shown in the example above.

3. In the **Credentials** field, select the credential specified in the table.

4. Click the **[Save]** button.

5. Repeat steps 1-4 for any other unaligned Dynamic Applications.

Configuring the HPE: Edge Connect Appliance Alarms Dynamic Application

The *get-alarm-rest* snippet in the "HPE: Edge Connect Appliance Alarms" Dynamic Application can be customized to modify the appliance alarm API query parameters.

> **CAUTION:** The HPE: Edge Connect (Silver Peak) API is not designed to be effective at polling for alarms. To ensure no alarms are missed, ScienceLogic suggests raising the max alarm value for the appliance alarms API call until no alarms are missed, however, be aware that this will increase the load on the orchestrator and collector. Ideally, you should configure webhooks to consume events from the orchestrator

when available.

To modify the *get-alarm-rest* snippet:

1. Go to the Dynamic Applications Manager page (System > Manage > Applications).

2. Search for the "HPE: Edge Connect Appliance Alarms" Dynamic Application and then click its wrench icon ( ).

3. Select the **[Snippets]** tab.

4. In the Snippet Registry pane, find the ***get-alarm-rest*** snippet and select its wrench icon ( ) *get-alarm-rest*.

5. In the **Snippet Code** field, locate the # SET APPLIANCE ALARMS QUERY CUSTOMIZATIONS HERE # section.

6. The following values can be edited:

    -   CUSTOM_VIEW_FILTER_VALUE

    -   CUSTOM_SEVERITY_FILTER_VALUE

    -   CUSTOM_ORDER_BY_SEVERITY_FILTER_VALUE

    -   CUSTOM_MAX_ALARMS_FILTER_VALUE

7. Click the **[Save]** button.

Viewing HPE: Edge Connect (Silver Peak) Devices

In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the HPE: Edge Connect (Silver Peak) Unity Orchestrator and all connected devices in the following places in the user interface:

-   The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with the Orchestrator, find the Orchestrator and click its plus icon (**+**):

-   The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for the Orchestrator, go to the **Component Map** page and select the map from the list in the left navigation pane. To learn more about the **Component Map** page, see the *Views* manual.

Troubleshooting the HPE: Edge Connect (Silver Peak) PowerPack

This section includes troubleshooting resources and procedures to use with the HPE: Edge Connect (Silver Peak) PowerPack.

CSRF Token Check in HPE: Edge Connect (Silver Peak)

The error message "[REST-PACK]: Critical - AID 2224: Unable to communicate with API: 401 Client Error: Unauthorized. App Name: Silver Peak: Root Group Discovery" occurs when executing the "HPE: Edge Connect (Silver Peak): Root Group Discovery" Dynamic Application. Silver Peak has a default setting enabled called "Enforce CSRF Token Check" that requires a token in the headers of the API request that SL1 makes to the orchestrator, but version 100 of the Silver Peak PowerPack does not support this.

Use cURL commands to correctly identify this issue:

1.
```
curl -X POST -H "Content-Type: application/json; charset=UTF-8" -k -d '
{"user": "xxxxxx", "password":"xxxxxxxxxxxxxxx"}' --cookie-jar
/tmp/silverpeak-cookie-test
https://URL:443/gms/rest/authentication/login
```

2.
```
curl --cookie /tmp/silverpeak-cookie-test -X GET
"https://URL:443/gms/rest/gms/group/root" --insecure
```

The error message "Unable to validate CSRF Token" will display when the second command is executed. In order to disable this setting and allow the HPE: Edge Connect (Silver Peak) PowerPack to function correctly:

1. In HPE: Edge Connect (Silver Peak) Orchestrator, go to the **Advanced Security Settings** page (Configuration > Advanced Security Settings).

2. De-select the *Enforce CSRF Token Check* option.

3. Click *Save*.

Chapter

3

Dashboards

Overview

The following section describes the device dashboards that are included in the *HPE: Edge Connect (Silver Peak)* PowerPack:

This chapter covers the following topics:

Device Dashboards

The *HPE: Edge Connect (Silver Peak)* PowerPack includes dashboards that provide summary information for data collected from Silver Peak Unity Orchestrator and appliances.

HPE: Edge Connect (Silver Peak) Orchestrator Dashboard

The HPE: Edge Connect (Silver Peak) Orchestrator Dashboard displays the following information:

- Orchestrator Alarms
- Tickets and Events
- Count of Appliances, Tunnels, and Active Users
- Top 10 Appliances by Alarm Count
- Top 10 Appliances by Dropped Packets
- Top 10 Appliances by Transmitted Packets

HPE: Edge Connect (Silver Peak) Appliances Dashboard

The HPE: Edge Connect (Silver Peak) Appliance device dashboard displays the following information for the appliance:

- Alarm Count
- Total Alarms
- Tickets and Events
- Top Interfaces by Transmitted Packets
- Top Interfaces by Dropped Packets

ScienceLogic