ScienceLogic

Monitoring Cisco Viptela

Cisco: Viptela PowerPack version 200

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Cisco: Viptela devices in SL1 using the *Cisco: Viptela* PowerPack.

The following sections provide an overview of Cisco: Viptela devices and the *Cisco: Viptela* 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 Cisco: Viptela?

Cisco: Viptela provides a cloud-based, software-defined wide area networking (SD-WAN) solution. Cisco: Viptela includes advanced routing, segmentation, and security capabilities for enterprise networks. Cisco: Viptela's cloud-based network management and orchestration technologies help you deploy and manage the latest WAN architectures.

What Does the Cisco: Viptela PowerPack Monitor?

To monitor Cisco: Viptela resources using the ScienceLogic platform, you must install the *Cisco: Viptela* PowerPack. This PowerPack enables you to discover, model, and collect data about Viptela resources.

The *Cisco: Viptela* PowerPack includes:

- Example credentials that you can use as templates to create SOAP/XML credentials to connect to Viptela
- The "Cisco: Viptela vManage Template" for aligning all dynamic applications to the root component device
- Dynamic Applications to discover, model, and monitor performance metrics or collect configuration data for the following Cisco: Viptela resources:
    - vManage
    - vSmart Controller
    - vEdge Routers
    - vBond Orchestrator
- Device Classes for each type of Cisco: Viptela device monitored:
    - ASR1000 Series
    - ISR1000 Series
    - ISR4000 Series
    - vBond Orchestrator
    - vEdge
    - vEdge Cloud
    - vEdge 100
    - vEdge 1000
    - vEdge 5000
    - vEdge 2000
    - vEdge 100-B

    - vEdge 100-M
    - vEdge 100-WM
    - vEdge Container
    - vManage
    - vSmart Controller
- Event Policies and corresponding alerts that are triggered when Viptela resources meet certain status criteria
- Dashboards that display information about Cisco: Viptela component devices

Installing the Cisco: Viptela PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: Viptela* 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 section on ***Global Settings***.

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 Cisco Viptela resources for monitoring by SL1 using the *Cisco: Viptela* PowerPack:

This chapter covers the following topics:

Prerequisite for Monitoring Cisco Viptela

To configure the SL1 system to monitor Cisco Viptela resources using the *Cisco: Viptela* PowerPack, you must first know the credentials (username and password) for a user account that has access to the Cisco Viptela system. The user account must have read-all access.

NOTE: To discover vEdge devices with only "valid" statuses, modify the "Cisco: Viptela vEdge Discovery" Dynamic Application's snippet arguments to filter by "valid" by changing the [*] section to use [?validity==\'valid\']. For example, the serialNumber's snippet argument uses the following:
rest://dataservice/system/device/vedges&silo_args=jpath=data
[?validity==\'valid\'].serialNumber|serialNumber

Configuring a Credential for Cisco Viptela

To configure SL1 to monitor Cisco: Viptela devices, you must first create a credential. This credential allows the Dynamic Applications in the *Cisco: Viptela* PowerPack to use your Cisco: Viptela user account to retrieve information from the *Cisco: Viptela* devices.

Configuring a Universal Credential for Cisco Viptela

To define a universal credential to access Cisco Viptela:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click **[Create New]** and select *Create Cisco sdwan/viptela Credential*. The **Create Credential** modal page appears.
3. Supply values in the following fields:
    - ***Name***. Type a name for your credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (ms)***. Keep the default value of 1500.
    - ***Authentication type***. Keep the default value (Token Authentication).
    - ***Authenticator Override***. Keep the default value (AuthViptela).
    - ***Username***. Type the Cisco: Viptela account username.
    - ***Password***. Type the Cisco: Viptela account password.
    - ***URL***. Type the URL and port for the Cisco: Viptela system, using the following format: *https://URL:443*. For example, https://my.viptela.system:443.

    Proxy Settings

    Toggle on this field if you are using a proxy server to communicate with your Cisco Viptela account, enter the values in the fields listed below:

    - ***Proxy scheme type***. Select *http* or *https* from the drop-down field.
    - ***Proxy Hostname/IP***. Enter the hostname or the IP address associated with your device.
    - ***Proxy Port***. Enter the port number for the proxy server.
    - ***Proxy User***. Enter the username for the proxy server.
    - ***Proxy Password***. Enter the password for the proxy server.

NOTE: The HTTPS proxy scheme is only available using the new universal credential . Existing SOAP/XML credentials do not support switching the scheme.

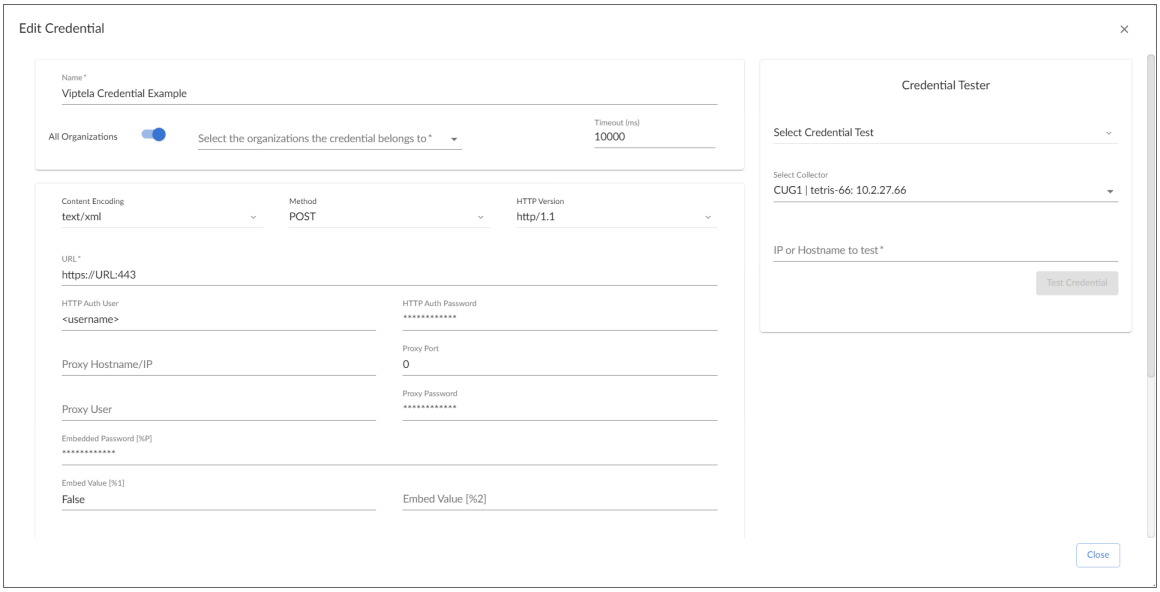
4. Click **[Save & Close]**.

Configuring a SOAP/XML Credential for Cisco Viptela

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure a SOAP/XML credential to access Cisco: Viptela:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate and then click the **Viptela Credential Example - SOAP/XML** credential. The **Edit Credential** modal page appears:



3. Complete the following fields:

   - ***Name***. Type a name for the Cisco: Viptela credential.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***Timeout (ms)***. Keep the default value.
   - ***Content Encoding***. Select *text/xml*.
   - ***Method***. Select POST.
   - ***HTTP Version***. Select HTTP/1.1.
   - ***URL***. Type the URL and port for the Cisco: Viptela system, using the following format: *https://URL:443*. For example, https://my.viptela.system:443.
   - ***HTTP Auth User***. Type the Cisco: Viptela account username.
   - ***HTTP Auth Password***. Type the Cisco: Viptela account password.

4. For the remaining fields, use the default values, and then click the **[Save As]** button.

Configuring a Credential for Cisco Viptela in the SL1 Classic User Interface

To configure SL1 to monitor Cisco: Viptela devices, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Cisco: Viptela* PowerPack) to use your Cisco: Viptela user account to retrieve information from the *Cisco: Viptela* devices.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure a SOAP/XML credential to access Cisco: Viptela:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Viptela Credential Example - SOAP/XML** credential, and then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears.
3. Complete the following fields:
    - ***Profile Name***. Type a name for the Cisco: Viptela credential.
    - ***Content Encoding***. Select *text/xml*.
    - ***Method***. Select POST.
    - ***HTTP Version***. Select HTTP/1.1.
    - ***URL***. Type the URL and port for the Cisco: Viptela system, using the following format: *https://URL:443*. For example, https://my.viptela.system:443.
    - ***HTTP Auth User***. Type the Cisco: Viptela account username.
    - ***HTTP Auth Password***. Type the Cisco: Viptela account password.
    - ***Timeout (seconds)***. Type "10".
4. For the remaining fields, use the default values, and then click the **[Save As]** button.

Cisco Viptela Guided Discovery

You can use the Guided Discovery Framework process in SL1 to guide you through a variety of existing discovery types in addition to traditional SNMP discovery. This process, which is also called "guided discovery", lets you choose a discovery type based on the type of devices you want to monitor. The Guided Discovery workflow includes a button for Cisco Viptela.

To run a Guided Discovery:

1. On the **Devices** page () or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.
2. Select the **[Cisco]** button. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Credential Selection** page appears.

NOTE: During the guided discovery process, you cannot click **[Next]** until the required fields are filled on the page, nor can you skip to future steps. However, you can revisit previous steps that you have already completed.

4. On the **Credential Selection** page of the guided discovery process, select the Cisco Viptela universal credential that you configured, and then click **[Next]**. The **Root Device Details** page appears.
5. Complete the following fields:
    - ***Root Device Name***. Type the name of the root device for the Cisco Viptela root device you want to monitor.
    - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered device.
    - ***Collector Group Name***. Select an existing collector group to communicate with the discovered device. This field is required.
6. Click **[Next]**. SL1 creates the Cisco Viptela root device with the appropriate Device Class assigned to it and aligns the relevant Dynamic Applications. The **Final Summary** page appears.
7. Click **[Close]**.

TIP: This PowerPack uses the snippet framework in order to function. Not all values returned in an API call in a Dynamic Application may have a collection object. For more information about how collections can be modified, added, or deleted using the snippet framework, see the *Snippet Framework* documentation.

NOTE: The results of a guided discovery do not display on the **Discovery Sessions** page (Devices > Discovery Sessions).

Creating a Cisco Viptela Virtual Device

Because the Cisco: Viptela service does not have a static IP address, you cannot discover a Cisco: Viptela device using discovery unless you use guided discovery. Instead, you must create a ***virtual device*** that represents the Cisco: Viptela service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Cisco: Viptela service:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.

3. Complete the following fields:
    - ***Device Name***. Type a name for the device.
    - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
    - ***Device Class***. Select *Cisco Systems Viptela | vManage*.
    - ***Collector***. Select the collector group that will monitor the device.
4. Click **[Add]** to create the virtual device.

Aligning Dynamic Applications to the Virtual Device

A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *Cisco: Viptela* PowerPack includes the "Cisco: Viptela vManage Template," which enables the SL1 to align all Dynamic Applications to the root component device.

Configuring the Device Template

Before you can use the "Cisco: Viptela vManage Template," you need to configure the template so that each dynamic application in the template aligns with the ***credential you created earlier***.

To configure the Viptela device template:

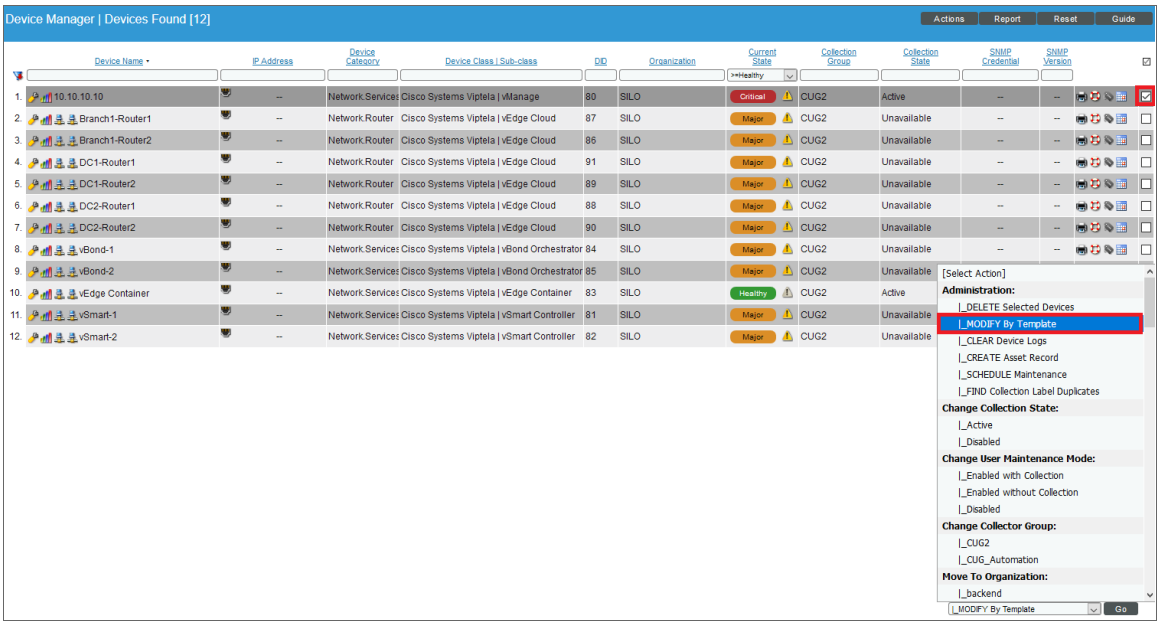
1. Go to the **Configuration Templates** page (Devices > Templates).
2. Locate the "Cisco: Viptela vManage Template" and click its wrench icon (). The **Device Template Editor** modal page appears.
3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.
4. In the ***Credentials*** drop-down list, select the credential that you created for Viptela.
5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the credential you created in the ***Credentials*** field.
6. Repeat step 5 until you have selected that credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.
7. Click **[Save]**.

Using the Device Template to Align Dynamic Applications to the Component Device

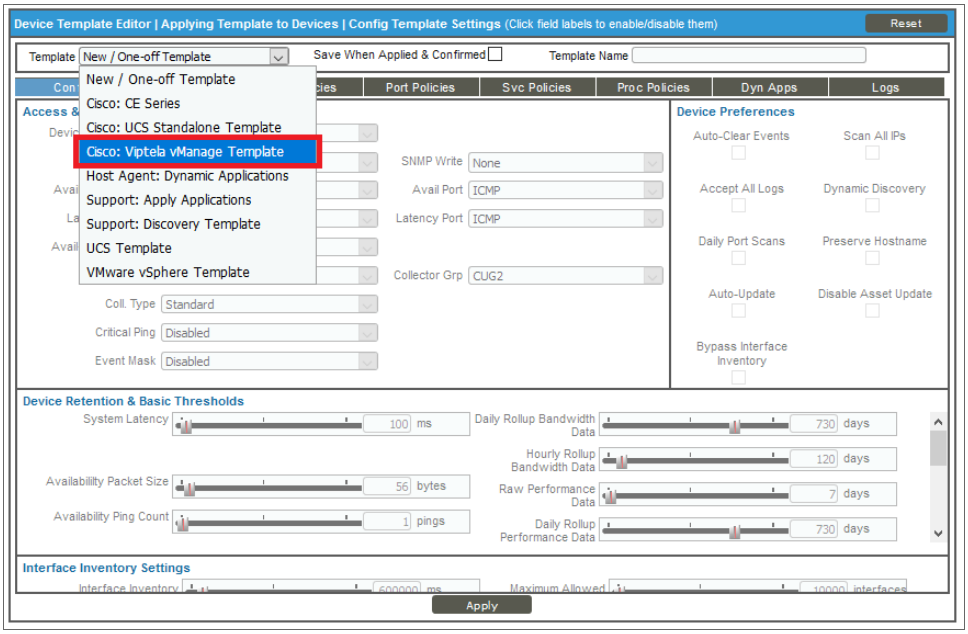
After you have configured the "Cisco: Viptela vManage Template" so that each dynamic application in the template aligns with the credential you created, you can use that template to align the Dynamic Applications to the root component device for Cisco: Viptela.

To use the "Viptela vManage Template" to align Dynamic Applications:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. On the **Device Manager** page, select the checkbox for the root component device.



3. In the ***Select Actions*** field, in the lower right, select the option *MODIFY by Template* and click the **[Go]** button. The **Device Template Editor** page appears:



4. Complete the following fields:

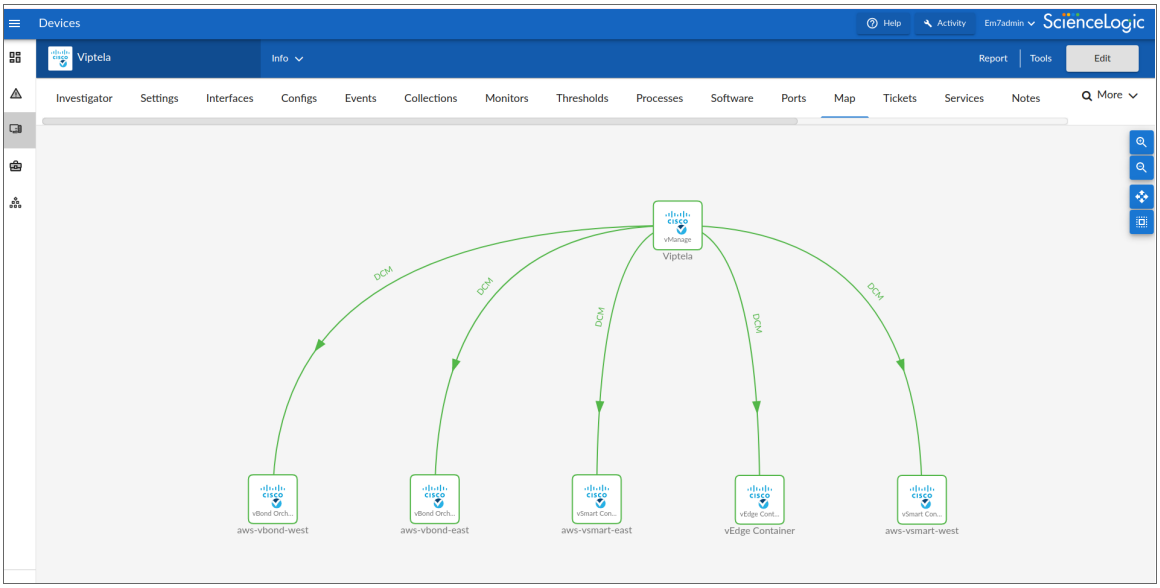
- In the ***Template*** drop-down list, select *Cisco: Viptela vManage Template*.
- In the ***Credentials*** drop-down list, select the credential you created earlier.

5. Click the **[Apply]** button, and then click **[Confirm]** to align the Dynamic Applications to the root component device.

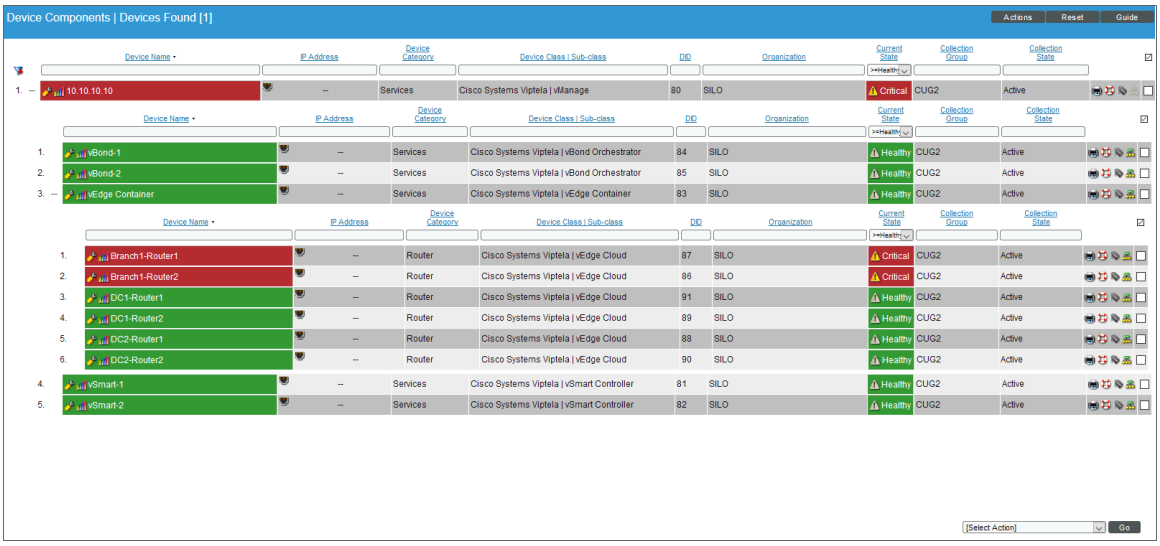
Viewing Information About the Cisco Viptela System

You can view your Cisco Viptela devices in the following places in the user interface:

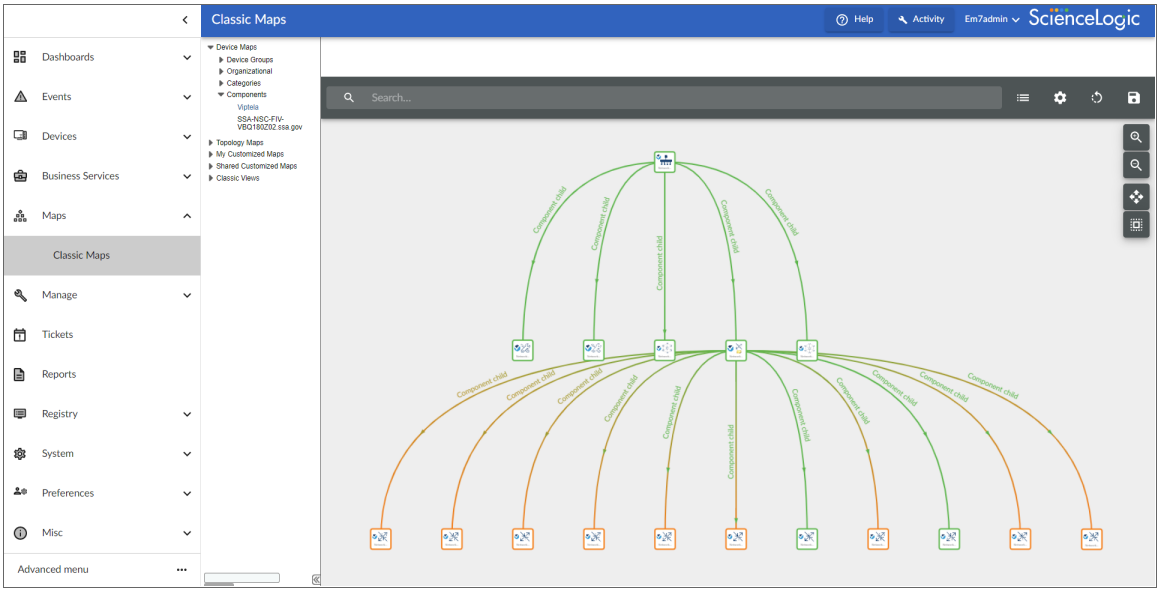
- The **[Map]** tab of the **Device Investigator** for a selected device on the **Devices** page displays a map of that device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device.



- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1. The **Device Components** page displays all root devices and component devices 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 a Cisco Viptela device, find the device and click its plus icon (**+**).



- The **Classic Maps** page (Maps > Classic Maps) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. From this page, go to Device Maps > Component to easily visualize and manage root nodes and their components. SL1 automatically updates the **Classic Maps** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a Cisco Viptela device, go to the **Classic Maps** page and select the map from the list in the left NavBar. To learn more about the **Classic Maps** page, see the ***Maps*** manual.



Chapter 3

Dashboards

Overview

The *Cisco: Viptela* PowerPack contains dashboards that present data related to different aspects of a Cisco Viptela system.

This chapter covers the following topics:

Cisco Viptela vEdge Dashboard

The *Cisco: Viptela* PowerPack includes a dashboard that provides summary information for vEdge Router component devices.

The Cisco: Viptela vEdge dashboard displays the following information:

- Vitals: CPU system percentage, disk use percentage, and memory utilization percentage
- Packet loss count
- Total bandwidth by interface
- Tx drops by interface
- Rx drops by interface
- Tx errors by interface
- Rx errors by interface
- Tx bandwidth by interface
- Rx bandwidth by interface

Cisco Viptela vManage Dashboard

The *Cisco: Viptela* PowerPack includes a dashboard that provides summary information for vManage component devices.

The Cisco: Viptela vManage dashboard displays the following information:

- CPU utilization
- Memory utilization
- Disk usage
- New event counts

Cisco Viptela vSmart and vBond Dashboard

The *Cisco: Viptela* PowerPack includes a dashboard that provides summary information for vSmart and vBond component devices.

The Cisco: Viptela vSmartvBond dashboard displays the following information:

- CPU utilization
- Memory utilization
- Disk usage
- Process counts

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010