Monitoring Cisco Cloud Services Platform

Cisco: Cloud Services Platform PowerPack version 107

Table of Contents

Chapter

1

Introduction

Overview

This manual describes how to monitor Cisco Cloud Services Platform (CSP) clusters in SL1 using the *Cisco: Cloud Services Platform* PowerPack.

The following sections provide an overview of Cisco Cloud Services Platform (CSP) devices and the *Cisco: Cloud Services Platform* 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 Cloud Services Platform?

Cisco Cloud Services Platform is a platform for virtualizing data center network functions. The hardware and software platform includes REST APIs, a command-line interface, and a web user interface for creating and managing virtual machines.

What Does the Cisco: Cloud Services Platform PowerPack Monitor?

To monitor Cloud Servies Platform (CSP) devices using SL1, you must install the *Cisco: Cloud Services Platform* PowerPack. This PowerPack enables you to discover, model, and collect data about CSP clusters, nodes, and services.

The *Cisco: Cloud Services Platform* PowerPack includes:

- Four example credentials (two SNMP credentials, a Basic/Snippet credential, and an SSH/Key credential) you can use to create the credentials that enable you to collect data from CSP devices

- Dynamic Applications to discover and monitor the CSP component devices

- Device Classes for each type of CSP component device SL1 monitors

- Event Policies and corresponding alerts that are triggered when CSP component devices meet certain status criteria

- Run Book Actions and Policies that align the correct device class to CSP component devices based on GUID and that merge CSP component devices with the appropriate physical components

- Device dashboards for each type of discovered CSP component device

Installing the Cisco: Cloud Services Platform PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: Cloud Services Platform* 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 Cisco Cloud Services Platform (CSP) clusters for monitoring by SL1 using the *Cisco: Cloud Services Platform* PowerPack:

This chapter covers the following topics:

Prerequisites for Monitoring CSP Clusters

To configure the SL1 system to monitor CSP clusters using the *Cisco: Cloud Services Platform* PowerPack, you must have the following information about the clusters that you want to monitor:

- Username and password of a user with REST API read access and a role of operator-group or admin-group

- SNMP community string with read privileges and the port set to 161

> **NOTE**: For more information about these requirements, see
> http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/config_guide/b_Cisco_CSP_2100_Config_Guide.html.

Additionally, you must establish a Net-SNMP public community string with the port set to 1610. To do so:

1. Log in to the command line of the CSP device as an administrative user.

2. Run the following commands:

```
netsnmp agent port 1610
```

```
netsnmp community public
```

Creating SNMP Credentials for CSP Clusters

Before you can discover and monitor Cloud Services Platform (CSP) clusters in SL1, you must first create two SNMP credentials (one for port 161 and another for port 1610) in SL1. These credentials, along with a *Basic/Snippet credential* and *SSH/Key credential* that you must also create, enable SL1 to collect data from the clusters. Two example SNMP credentials that you can edit for your own use are included in the *Cisco: Cloud Services Platform* PowerPack.

> **NOTE**: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the *Duplicate* option for sample credential(s). ScienceLogic recommends that you use *the classic user interface and the Save As button* to create new credentials from sample credentials. This will prevent you from overwriting the sample credential(s).

> **NOTE**: For more information about the configuration required for the two SNMP credentials, see the *Prerequisites* section.

To configure the port 161 SNMP credential for CSP:

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

2. Locate the **Cisco: CSP SNMP Port 161 Example** credential, click its **[Actions]** icon (⋯) and select *Duplicate*. A copy of the credential, called **Cisco: CSP SNMP Port 161 Example copy** appears.

3. Click the **[Actions]** icon (⋯) for the **Cisco: CSP SNMP Port 161 Example copy** credential and select *Edit/Test*.The **Edit Credential** page appears. Enter values in the following fields:

- *Name*. Enter a new name for the 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.
- *SNMP Community (Read Only)*. Enter the port 161 community string for the CSP cluster.

4. Use the default values for the other fields on this page.

5. Click the **[Save & Close]** button.

To configure the port 1610 SNMP credential for CSP:

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

2. Locate the **Cisco: CSP SNMP Port 1610 Example** credential, click its **[Actions]** icon (⋯) and select *Duplicate*. A copy of the credential, called **Cisco: CSP SNMP Port 1610 Example copy** appears.

3. Click the **[Actions]** icon (•••) for the **Cisco: CSP SNMP Port 1610 Example copy** credential and select
    Edit/Test.The **Edit Credential** page appears. Enter values in the following fields:

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

-   *SNMP Community (Read Only)*. Enter the port 1610 community string for the CSP cluster.

4. Use the default values for the other fields on this page.

5. Click the **[Save & Close]** button.

Creating SNMP Credentials for CSP Clusters in the SL1 Classic User Interface

Before you can discover and monitor Cloud Services Platform (CSP) clusters in SL1, you must first create two
SNMP credentials (one for port 161 and another for port 1610) in SL1. These credentials, along with a
Basic/Snippet credential and *SSH/Key credential* that you must also create, enable SL1 to collect data from
the clusters. Two example SNMP credentials that you can edit for your own use are included in the *Cisco: Cloud
Services Platform* PowerPack.

> **NOTE:** For more information about the configuration required for the two SNMP credentials, see the
> *Prerequisites* section.

To configure the port 161 SNMP credential for CSP:

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

2. Locate the **Cisco: CSP SNMP Port 161 Example** credential, then click its wrench icon (🔧). The **Edit
    SNMP Credential** modal page appears.

3. Make entries in the following fields:

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

   - *SNMP Community (Read Only)*. Enter the port 161 community string for the CSP cluster.

4. Use the default values for the other fields on this page.

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

6. When the confirmation message appears, click **[OK]**.

To configure the port 1610 SNMP credential for CSP:

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

2. Locate the **Cisco: CSP SNMP Port 1610 Example** credential, then click its wrench icon (🔧). The **Edit SNMP Credential** modal page appears.

3. Make entries in the following fields:

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

   - *SNMP Community (Read Only)*. Enter the port 1610 community string for the CSP cluster.

4. Use the default values for the other fields on this page.

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

6. When the confirmation message appears, click **[OK]**.

Creating a Basic/Snippet Credential for CSP Clusters

Some Dynamic Applications in the *Cisco: Cloud Services Platform* PowerPack collect data from CSP clusters using the REST API. These Dynamic Applications require a Basic/Snippet credential to enable SL1 to communicate with the cluster. An example Basic/Snippet credential that you can edit for your own use is included in the *Cisco: Cloud Services Platform* PowerPack.

NOTE: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the *Duplicate* option for sample credential(s). ScienceLogic recommends that you use *the classic user interface and the Save As button* to create new credentials from sample credentials. This will prevent you from overwriting the sample credential(s).

NOTE: For more information about the configuration required for the Basic/Snippet credential, see the *Prerequisites* section.

To create a Basic/Snippet credential to monitor CSP:

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

2. Locate the **Cisco: CSP Example** credential, click its **[Actions]** icon (⋯) and select *Duplicate*. A copy of the credential, called **Cisco: CSP Example copy** appears.

3. Click the **[Actions]** icon (⋯) for the **Cisco: CSP Example copy** credential and select *Edit/Test*. The **Edit Credential** page appears. Enter values in the following fields:

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

- *Username*. Enter the username for a user with REST API read access to the CSP cluster and a role of operator-group or admin-group.

- *Password*. Enter the password for the REST API user.

4. Use the default values for the other fields on this page.

5. Click the **[Save & Close]** button.

Creating a Basic/Snippet Credential for CSP Clusters in the SL1 Classic User Interface

Some Dynamic Applications in the *Cisco: Cloud Services Platform* PowerPack collect data from CSP clusters using the REST API. These Dynamic Applications require a Basic/Snippet credential to enable SL1 to communicate with the cluster. An example Basic/Snippet credential that you can edit for your own use is included in the *Cisco: Cloud Services Platform* PowerPack.

> **NOTE:** For more information about the configuration required for the Basic/Snippet credential, see the *Prerequisites* section.

To create a Basic/Snippet credential to monitor CSP:

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

Creating a Basic/Snippet Credential for CSP Clusters

2. Locate the **Cisco: CSP Example** credential, and then click its wrench icon (🔧). The **Edit Basic/Snippet Credential** modal page appears.

3. Enter values in the following fields:

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

   - *Username*. Enter the username for a user with REST API read access to the CSP cluster and a role of operator-group or admin-group.

   - *Password*. Enter the password for the REST API user.

4. Use the default values for the other fields on this page.

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

6. When the confirmation message appears, click **[OK]**.

Creating an SSH/Key Credential for CSP Clusters

Some Dynamic Applications in the *Cisco: Cloud Services Platform* PowerPack collect data from CSP clusters from the command line interface instead of the API. These Dynamic Applications require an SSH/Key credential to enable SL1 to communicate with the cluster. An example SSH/Key credential that you can edit for your own use is included in the *Cisco: Cloud Services Platform* PowerPack.

> **NOTE**: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the *Duplicate* option for sample credential(s). ScienceLogic recommends that you use *the classic user interface and the Save As button* to create new credentials from sample credentials. This will prevent you from overwriting the sample credential(s).

> **NOTE:** This functionality utilizes MD5 password encryption. As such, it is not currently available for use in Federal Information Processing Standard (FIPS)-compliant installations of SL1. If you attempt to discover CSP cluster data using an SSH/Key credential in FIPS-compliant installations of SL1, the cluster component device will not be created and an exception error message appears in the system log.

To create an SSH/Key credential to monitor CSP:

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

2. Locate the **Cisco: CSP 2100 CLI Example** credential, click its **[Actions]** icon (⋯) and select *Duplicate*. A copy of the credential, called **Cisco: CSP 2100 CLI Example copy** appears.

3. Click the **[Actions]** icon (⋯) for the **Cisco: CSP 2100 CLI Example copy** credential and select *Edit/Test*.The **Edit Credential** page appears. Enter values in the following fields:

- *Name*. Type a new name for the 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 setting.
- *Hostname/IP.* Type the IP address or hostname of the CSP cluster you want to monitor.
- *Port.* Type the SSH port number for the CSP cluster you want to monitor.
- *Username*. Type the username for a user with administrator access to the CSP cluster command line interface.
- *Password*. Type the user's password.
- *Private Key (PEM Format)*. Keep this field blank.

> **NOTE:** The private key can have a maximum of 64 characters per line. Therefore, you cannot use keys in the OpenSSH format, because that format uses 70 characters per line. When you attempt to save the credential, SL1 will validate that the private key entered is in the correct format. You will be able to save the credential only if the private key is correctly formatted.

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

Creating an SSH/Key Credential for CSP Clusters in the SL1 Classic User Interface

Some Dynamic Applications in the *Cisco: Cloud Services Platform* PowerPack collect data from CSP clusters from the command line interface instead of the API. These Dynamic Applications require an SSH/Key credential to enable SL1 to communicate with the cluster. An example SSH/Key credential that you can edit for your own use is included in the *Cisco: Cloud Services Platform* PowerPack.

> **NOTE**: This functionality utilizes MD5 password encryption. As such, it is not currently available for use in Federal Information Processing Standard (FIPS)-compliant installations of SL1. If you attempt to discover CSP cluster data using an SSH/Key credential in FIPS-compliant installations of SL1, the cluster component device will not be created and an exception error message appears in the system log.

To create an SSH/Key credential to monitor CSP:

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

2. Locate the **Cisco: CSP 2100 CLI Example** credential, and then click its wrench icon ( ). The **Edit SSH/Key Credential** modal page appears.

3. Enter values in the following fields:

   - *Credential Name*. Type a new name for the credential.

   - *Hostname/IP.* Type the IP address or hostname of the CSP cluster you want to monitor.

   - *Port.* Type the SSH port number for the CSP cluster you want to monitor.

   - *Timeout(ms).* Keep the default setting.

   - *Username*. Type the username for a user with administrator access to the CSP cluster command line interface.

   - *Password*. Type the user's password.

   - *Private Key (PEM Format)*. Keep this field blank.

> **NOTE**: The private key can have a maximum of 64 characters per line. Therefore, you cannot use keys in the OpenSSH format, because that format uses 70 characters per line. When you attempt to save the credential, SL1 will validate that the private key entered is in the correct format. You will be able to save the credential only if the private key is correctly formatted.

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

5. When the confirmation message appears, click **[OK]**.

Discovering CSP Clusters

When you discover your Cloud Services Platform (CSP) cluster with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor the CSP cluster and all of its associated component devices.

To discover your CSP cluster, perform the following steps:

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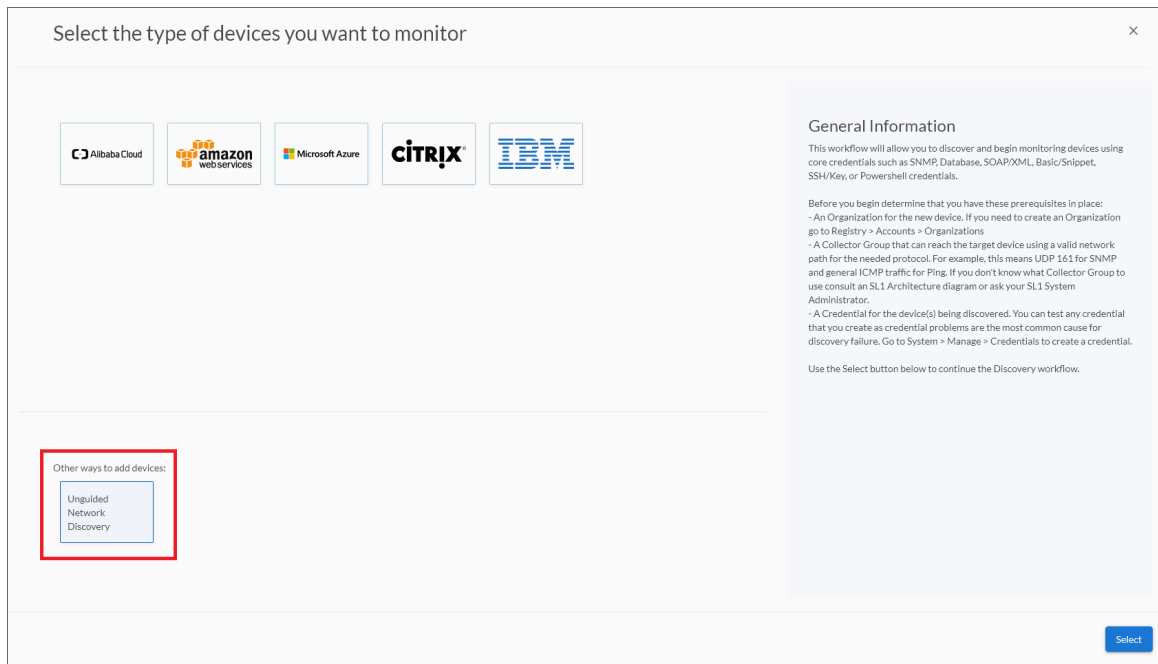
2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.

3. Click **[Select]**. The **Add Devices** page appears:

4. Complete the following fields:

   - *Name*. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.

   - *Description*. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.

   - *Select the organization to add discovered devices to*. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:
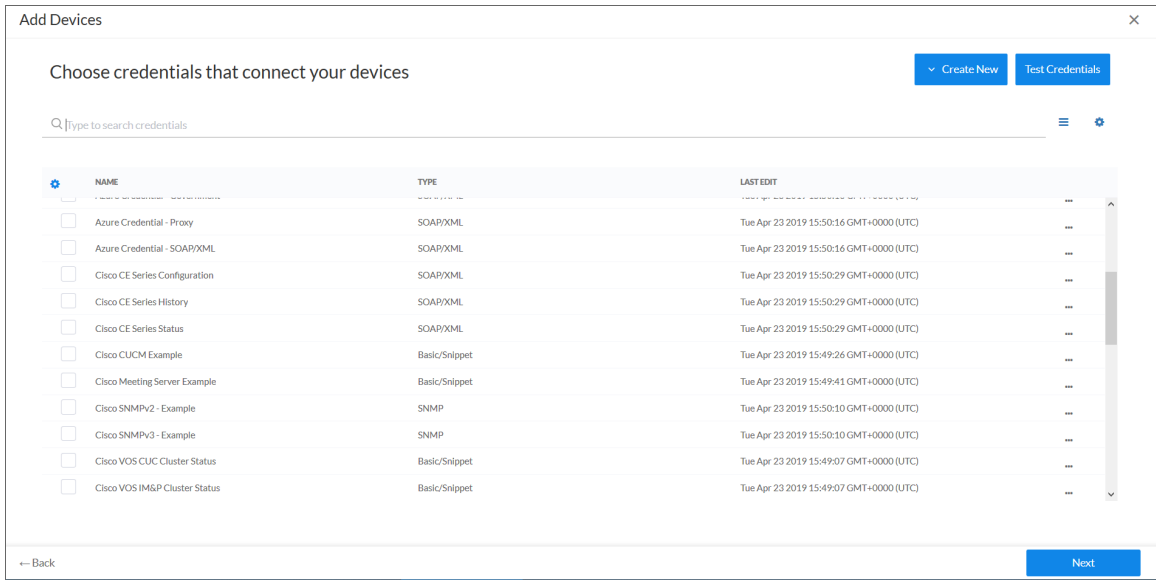
6. On the **Credentials** page, locate and select the two SNMP credentials that you created (one for port 161 and the other for port 1610), and the Basic/Snippet credential and the SSH/Key credential for each of the CSP nodes you want to discover.

NOTE: You must include a minimum of three credentials (one SNMP credential and two Basic/Snippet credentials) for each CSP node with unique credential information.

---

7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:
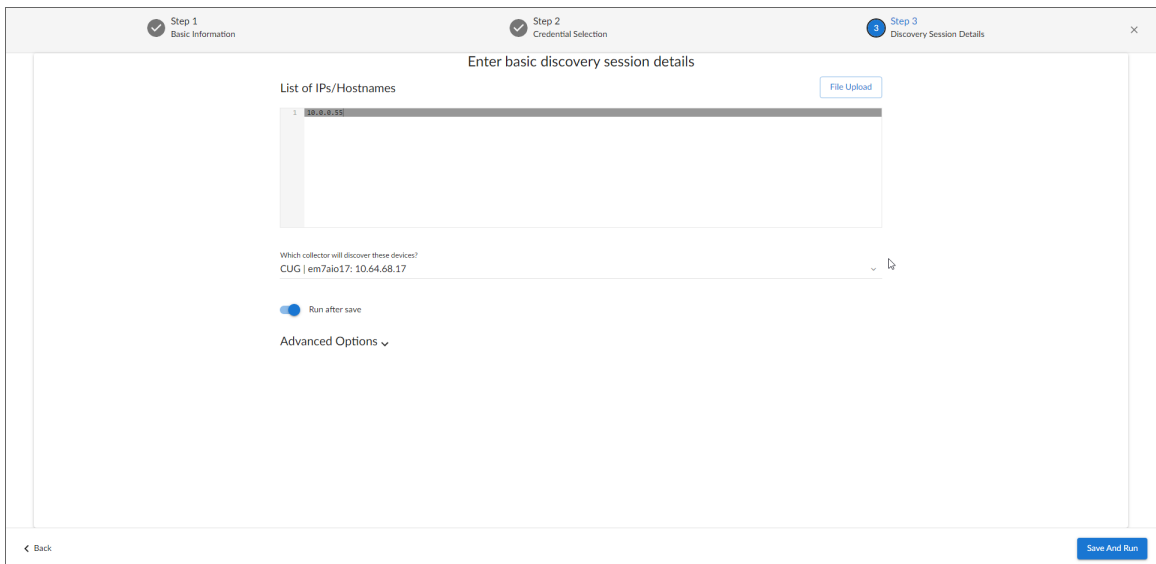
8. Complete the following fields:

    - *List of IPs/Hostnames*. Type the IP address of each CSP node you want to discover.

    - *Which collector will monitor these devices?*. Select an existing collector to monitor the discovered devices. Required.

    - *Run after save*. Select this option to run this discovery session as soon as you click **[Save and Close]**.

        In the **Advanced options** section, click the down arrow icon (∨) to complete the following fields:

        ◦ *Discover Non-SNMP*. Enable this setting.

9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.

10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

Discovering CSP Clusters in the SL1 Classic User Interface

When you discover your Cloud Services Platform (CSP) cluster with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor the CSP cluster and all of its associated component devices.

To discover your CSP cluster, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).

2. Click the **[Create]** button. The **Discovery Session Editor** page appears.

3. Supply values in the following fields:

    - *IP Address/Hostname Discovery List*. Enter the IP address of each CSP node you want to discover.

    - *SNMP Credentials*. Select the two SNMP credentials that you created (one for port 161 and the other for port 1610) for each of the CSP nodes you want to discover.

    - *Other Credentials*. Select the Basic/Snippet credential and the SSH/Key credential for each of the CSP nodes you want to discover.

    - *Discover Non-SNMP*. Select this checkbox.

NOTE: You must include a minimum of three credentials (one SNMP credential and two Basic/Snippet credentials) for each CSP node with unique credential information.

---

4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the *Discovery & Credentials* manual.

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

6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (⚡) for the discovery session you created.

7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

Viewing CSP Component Devices

When SL1 discovers your CSP cluster, SL1 creates component devices that represent each component in the cluster.

In addition to the **Devices** page, you can view all associated component devices in the following places in the user interface:

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular 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.
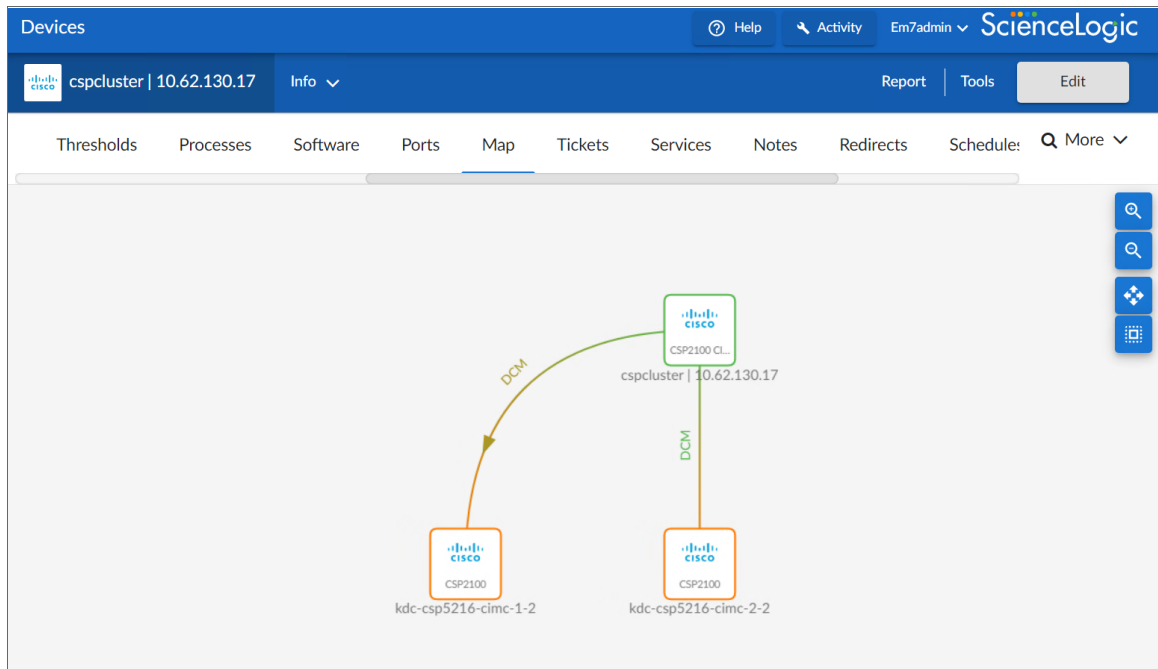
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1. The **Device Components** page displays all root devices and component devices in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with your CSP cluster, find the root device 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 your CSP cluster, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the *Maps* manual.
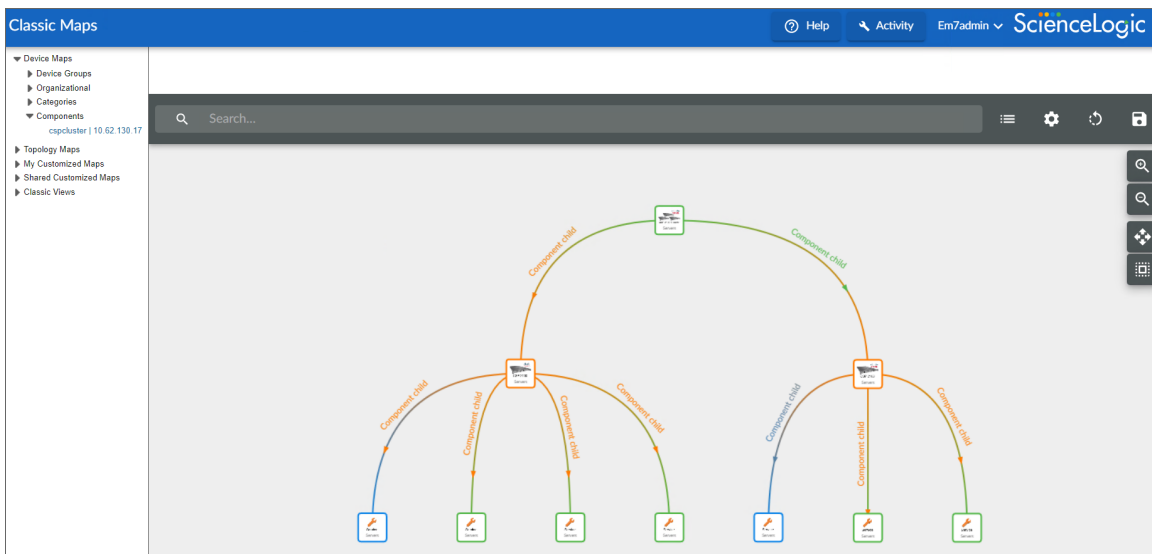
Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between CSP-2100 nodes and Cisco UCS Standalone servers.

Relationships Between Component Devices

Chapter

3

Dashboards

Overview

The following sections describe the device dashboards that are included in the *Cisco: Cloud Services Platform* PowerPack.

> **NOTE**: These dashboards appear only in the SL1 classic user interface.

This chapter covers the following topics:

Device Dashboards

The *Cisco: Cloud Services Platform* PowerPack includes device dashboards that provide summary information for Cisco Cloud Services Platform (CSP) 2100 component devices. Each of the device dashboards in the *Cisco: Cloud Services Platform* PowerPack are set as the default device dashboard for the equivalent device class.

Cisco: CSP 2100 Cluster

The Cisco: CSP 2100 Cluster device dashboard displays the following information:

- Gauges that indicate:

  - The number of nodes in the cluster

- ◦ The number of services in the cluster that are currently powered off

- ◦ The number of services in the cluster that are currently powered on

- The number of services over a specified period of time

- Cluster resource utilization over a specified period of time

- Cluster CPU utilization over a specified period of time

- RAM utilization over a specified period of time

- Cluster disk utilization over a specified period of time

Cisco: CSP 2100 Node

The Cisco: CSP 2100 Node device dashboard displays the following information:

- Gauges that indicate:

  - ◦ The number of services in the node that are currently powered on

  - ◦ The number of services in the node that are currently powered off

- A list of tickets and events relating to the node

- Node vitals over a specified period of time

- The top 5 physical interfaces in the node based on bandwidth utilization

- Node resource utilization over a specified period of time

- The top 5 services in the node based on memory utilization

- The top 5 services in the node based on CPU load

- The top 5 services in the node based on disk space utilization

Cisco: CSP 2100 Service

The Cisco: CSP 2100 Service device dashboard displays the following information:

- The service's power status (i.e., on or off) over a specified period of time

- A list of tickets and events relating to the service

- Service resource consumption over a specified period of time

- Service resource memory consumption over a specified period of time

- Service resource disk consumption over a specified period of time

- The top service interfaces based on packets in and out over the previous hour

- The top service interfaces based on dropped packets in and out over the previous hour

- The top service interfaces based on errors in and out over the previous hour

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.