



Monitoring Cisco CloudCenter

Beta Version

Cisco: CloudCenter Suite PowerPack version 107

Table of Contents

Introduction	3
What is Cisco CloudCenter?	3
What Does the Cisco: CloudCenter PowerPack Monitor?	4
Installing the Cisco: CloudCenter PowerPack	4
Configuration and Discovery	6
Configuration and Discovery for Standard Cisco CloudCenter Deployments	6
Prerequisites for Monitoring Standard CloudCenter Deployments	7
Creating a Basic/Snippet Credential for Standard Deployments	7
Discovering the CloudCenter Manager Root Tenant for Standard Deployments	8
Discovering the CloudCenter Manager Root Tenant for Standard Deployments in the SL1 Classic User Interface	10
Verifying Discovery and Dynamic Application Alignment	10
Discovering Multiple Tenants for Standard Deployments	11
Creating a Credential for a CloudCenter Manager Tenant	11
Discovering an Additional CloudCenter Manager Tenant	12
Configuration and Discovery for High-Availability Cisco CloudCenter Deployments	13
Prerequisites for Monitoring High-Availability CloudCenter Deployments	13
Creating Credentials for High-Availability Deployments	13
Creating SSH/Key Credentials for CloudCenter Components	14
Creating a Basic/Snippet Credential for RabbitMQ	15
Creating the Master SOAP/XML Credential for High-Availability Discovery	16
Discovering Cisco CloudCenter High-Availability Deployments	19
Discovering Cisco CloudCenter High-Availability Deployments in the SL1 Classic User Interface	21
Verifying Discovery and Dynamic Application Alignment	21
Discovering Multiple Tenants for High-Availability CloudCenter Deployments	22
Creating a Credential for a High-Availability CloudCenter Tenant	22
Discovering an Additional High-Availability CloudCenter Tenant	23
Viewing CloudCenter Component Devices	23
Viewing CloudCenter Component Devices in the SL1 Classic User Interface	24
Merging RabbitMQ and CloudCenter Orchestrator Devices	26
Relationships Between Component Devices	26

Chapter

1

Introduction

Overview

This manual describes how to monitor Cisco: CloudCenter services in SL1 using the Dynamic Applications in the *Cisco: CloudCenter PowerPack*.

The following sections provide an overview of Cisco: CloudCenter and the *Cisco: CloudCenter PowerPack*:

This chapter covers the following topics:

What is Cisco CloudCenter?	3
What Does the Cisco: CloudCenter PowerPack Monitor?	4
Installing the Cisco: CloudCenter PowerPack	4

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 CloudCenter?

Cisco CloudCenter is a cloud-management platform used for deploying and managing applications in data centers, private clouds, and public clouds.

What Does the Cisco: CloudCenter PowerPack Monitor?

The *Cisco: CloudCenter PowerPack* enables you to discover and collect configuration and performance data about standard or high-availability CloudCenter deployments and their components. The *Cisco: CloudCenter PowerPack* can monitor CloudCenter Manager version 4.7 and later.

The *Cisco: CloudCenter PowerPack* includes:

- Sample Credentials you can use as templates to create your own Credentials to monitor CloudCenter deployments
- Dynamic Applications and Run Book Actions to discover, model, and monitor performance metrics and/or collect configuration data for the following CloudCenter components:
 - CloudCenter Clusters
 - CloudCenter Manager
 - CloudCenter Load Balancers
 - CloudCenter Postgres Databases
 - CloudCenter Health Monitor
 - CloudCenter Tenants
 - CloudCenter Application Instances
 - CloudCenter Clouds
 - CloudCenter Regions
 - CloudCenter Orchestrator
 - CloudCenter ELK components
 - RabbitMQ Servers
 - RabbitMQ Load Balancers
- Device Classes for each of the CloudCenter components that SL1 monitors
- Event Policies and corresponding alerts that are triggered when CloudCenter components meet certain status criteria

Installing the Cisco: CloudCenter PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: CloudCenter 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 a Cloud Center Manager for monitoring by SL1 using the *Cisco: CloudCenter PowerPack*:

This chapter covers the following topics:

<i>Configuration and Discovery for Standard Cisco CloudCenter Deployments</i>	6
<i>Configuration and Discovery for High-Availability Cisco CloudCenter Deployments</i>	13
<i>Viewing CloudCenter Component Devices</i>	23
<i>Merging RabbitMQ and CloudCenter Orchestrator Devices</i>	26
<i>Relationships Between Component Devices</i>	26

Configuration and Discovery for Standard Cisco CloudCenter Deployments

The *Cisco: CloudCenter PowerPack* enables you to discover and collect configuration and performance data about standard or high-availability (HA) CloudCenter deployments and their components. The following sections describe the configuration and discovery steps for monitoring standard (non-HA) CloudCenter deployments.

For information about HA deployments, see the section on [Configuration and Discovery for High-Availability Cisco CloudCenter Deployments](#).

Prerequisites for Monitoring Standard CloudCenter Deployments

To configure the SL1 system to monitor standard (non-HA) Cisco CloudCenter deployments using the *Cisco: CloudCenter PowerPack*, you must first have the following information about the CloudCenter Manager that you want to monitor:


- The IP address of the CloudCenter Manager system
- The username and API key for a Cisco CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user. For information about configuring API users in Cisco CloudCenter Manager, see <http://docs.cloudcenter.cisco.com/display/40API/API+Management+Key>.

Creating a Basic/Snippet Credential for Standard Deployments

To configure SL1 to monitor a standard (non-HA) CloudCenter Manager deployment, you must first create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *Cisco: CloudCenter PowerPack* to communicate with your CloudCenter Manager.

The PowerPack includes an example Basic/Snippet credential (**Cisco CloudCenter EXAMPLE**) that you can edit for your own use.

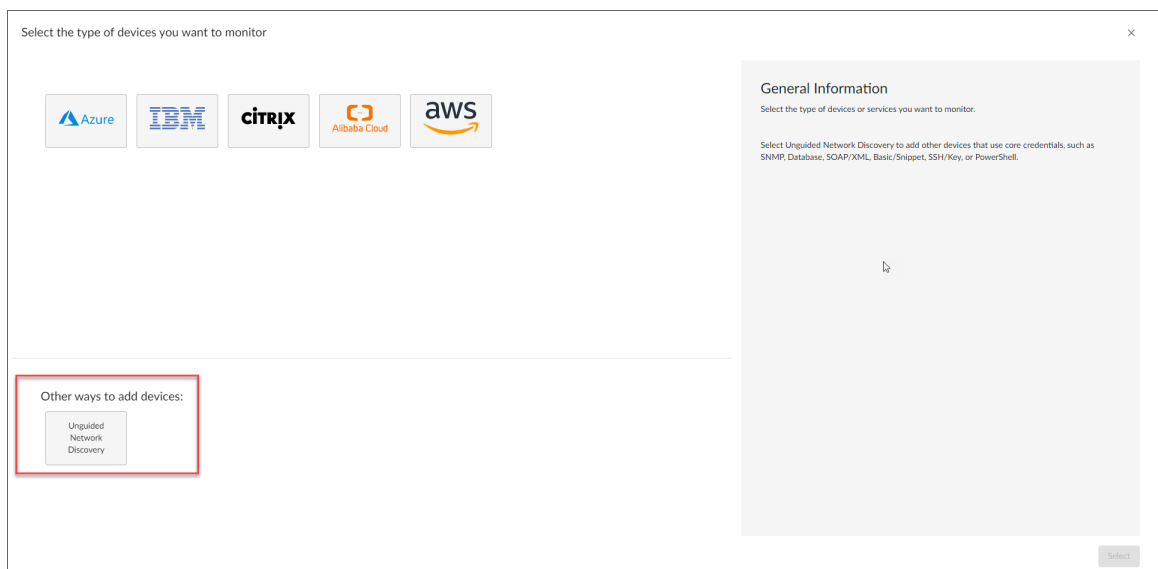
To configure a Basic/Snippet credential to access a CloudCenter Manager:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco CloudCenter EXAMPLE** credential, then click its wrench icon (). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields.
 - **Profile Name**. Type a name for the CloudCenter Manager credential.
 - **Username**. Type the username for a CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user.
 - **Password**. Type the API key for the user you entered in the **Username** field.
4. Leave all other fields set to the default values. Click the **[Save As]** button.

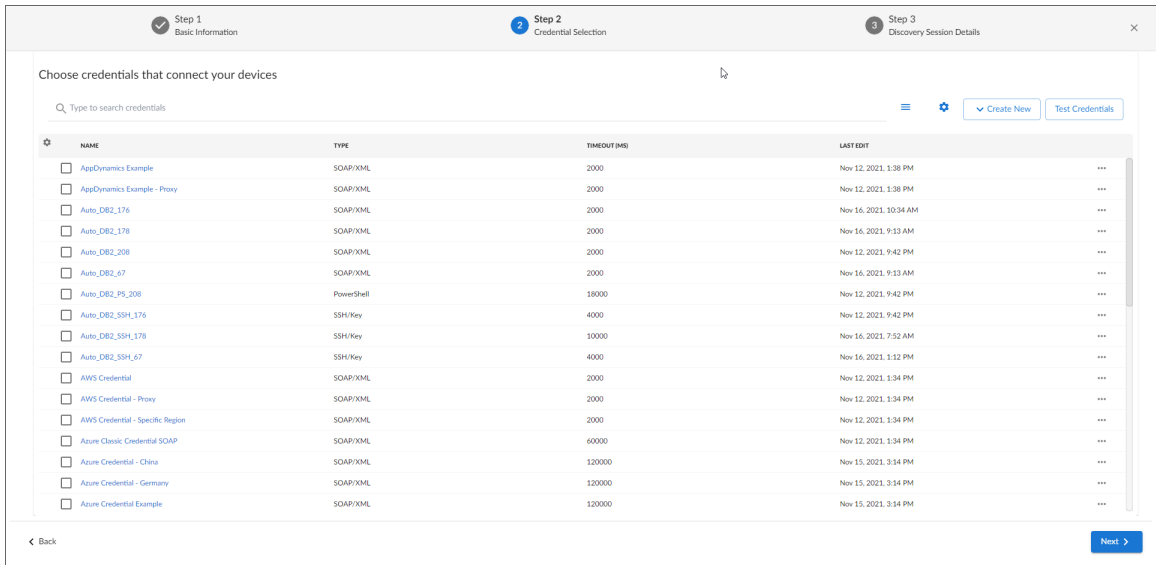
Discovering the CloudCenter Manager Root Tenant for Standard Deployments

To discover CloudCenter Manager, perform the following steps:

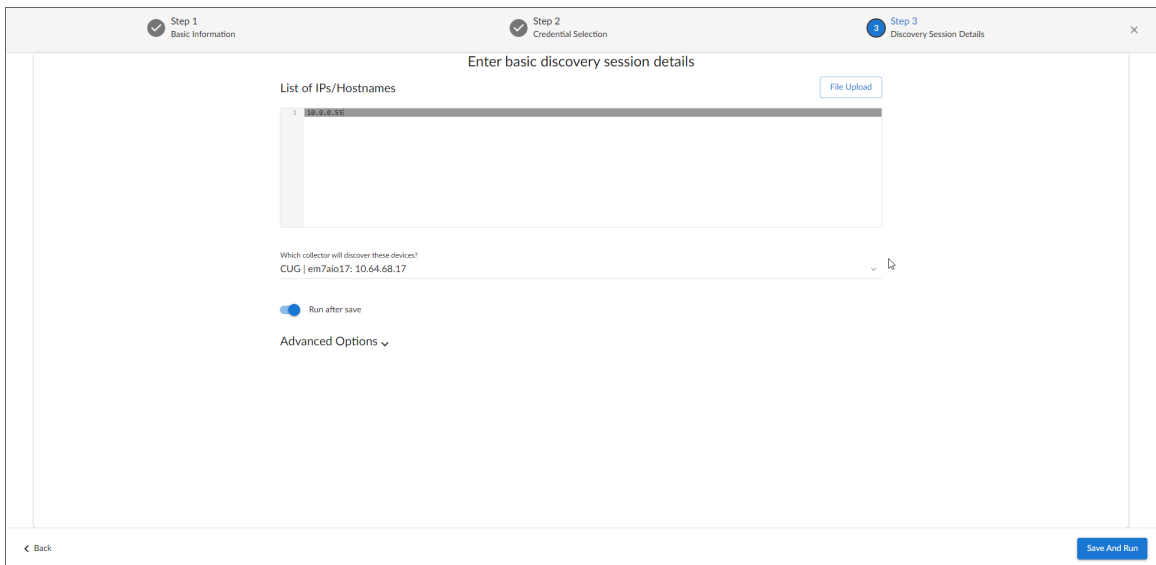
1. On the **Devices** page (📄) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:




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:



- On the **Credentials** page select the Basic/Snippet credential you created for the CloudCenter Manager root tenant. Optionally, if you also have an SNMP credential for the CloudCenter Manager, you can select this credential as well.
- Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



- Complete the following fields:
 - List of IPs/Hostnames.** Enter the IP address for the CloudCenter Manager.
 - Which collector will monitor these devices?.** Required. Select an existing collector to monitor the discovered devices.
 - Run after save.** Select this option to run this discovery session as soon as you save the session.

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 Run]** if you enabled the Run after save setting, or **[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 the CloudCenter Manager Root Tenant for Standard Deployments in the SL1 Classic User Interface

To discover CloudCenter Manager, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button.
3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, define values in the following fields.
 - **IP Address/Hostname Discovery List**. Enter the IP address for the CloudCenter Manager.
 - **SNMP Credentials**. Optionally, select the SNMP credential for the CloudCenter Manager you are discovering.
 - **Other Credentials**. Select the Basic/Snippet credential you created for the CloudCenter Manager root tenant.
 - **Discover Non-SNMP**. Select this checkbox.
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the **Discovery & Credentials** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.
7. The **Discovery Session** window appears. When the device is discovered, click the device icon (🖨) to view the **Device Properties** page for the device.

Verifying Discovery and Dynamic Application Alignment

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

1. From the **Device Properties** page for the CloudCenter Manager device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for CloudCenter Manager 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.

The following Dynamic Applications should be aligned to the device:

- Cisco: CloudCenter CCM Component to Physical Merge
- Cisco: CloudCenter Cluster Discovery
- Cisco: CloudCenter Root Device Reclassification

If the listed Dynamic Applications have not been automatically aligned during discovery, 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.
3. In the **Credentials** field, select the Basic/Snippet credential you created for CloudCenter Manager.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

Discovering Multiple Tenants for Standard Deployments


The Cisco: *CloudCenter* PowerPack can be used to monitor a CloudCenter Manager that includes multiple tenants. To discover multiple tenants, you must follow the steps in the following sections for each tenant in order (in other words, parents must be discovered before their children):

- [Creating a Credential for a CloudCenter Manager Tenant](#)
- [Discovering an additional CloudCenter Manager Tenant](#)

For each tenant, you must use the administrator account for that tenant when you create the credential.

Creating a Credential for a CloudCenter Manager Tenant

To configure a Basic/Snippet credential to access an additional CloudCenter Manager tenant:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the credential you used to discover the root tenant, then click its wrench icon (). The **Edit Basic/Snippet Credential** modal page appears.
3. Enter values in the following fields.
 - **Profile Name**. Enter a new name for the CloudCenter Manager tenant credential.
 - **Username**. Enter the username for a CloudCenter Manager user that is an administrator for the tenant you want to discover. This account must be an API user, not a GUI user.
 - **Password**. Enter the API key for the user you entered in the **Username** field.
4. Leave all other fields set to the default values. Click the **[Save As]** button.

Discovering an Additional CloudCenter Manager Tenant

To discover an additional tenant:

1. From the **Device Properties** page for the CloudCenter Suite root device, click the name of the CloudCenter Cluster device that appears in the **Root Device** field.
2. Click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. Select the checkbox for the "Cisco: CloudCenter Tenant Discovery" Dynamic Application.
4. In the **Select Action** drop-down list, select the credential you created for the tenant.
5. Click **[Go]**.

Configuration and Discovery for High-Availability Cisco CloudCenter Deployments

The *Cisco: CloudCenter PowerPack* enables you to discover and collect configuration and performance data about standard or high-availability (HA) CloudCenter deployments and their components. The following sections describe the configuration and discovery steps for monitoring HA CloudCenter deployments.

For information about standard (non-HA) deployments, see the section on [Configuration and Discovery for Standard Cisco CloudCenter Deployments](#).

Prerequisites for Monitoring High-Availability CloudCenter Deployments

To configure the SL1 system to monitor HA Cisco CloudCenter deployments using the *Cisco: CloudCenter PowerPack*, you must first have the following information about the CloudCenter components that you want to monitor:

- The IP address or hostname for each of the following components:
 - RabbitMQ
 - RabbitMQ Load Balancer
 - Cisco CloudCenter Manager
 - Cisco CloudCenter Manager Load Balancer
 - CloudCenter PostgreSQL database
 - CloudCenter Orchestrator
 - CloudCenter Orchestrator Load Balancer
 - CloudCenter Health Monitor
 - CloudCenter ELK components
- The username and API key for a Cisco CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user. For information about configuring API users in Cisco CloudCenter Manager, see <http://docs.cloudcenter.cisco.com/display/40API/API+Management+Key>.
- The username and password for a RabbitMQ user that has read permission to the RabbitMQ API. For information about configuring users in RabbitMQ, see <https://www.rabbitmq.com/management.html>.
- The usernames and passwords for Cisco CloudCenter users that have API read permissions for each of the other components in the above list.

Creating Credentials for High-Availability Deployments

To configure SL1 to monitor HA Cisco CloudCenter deployments, you must create the following credentials:

- [SSH/Key credentials for CloudCenter Components](#)
- [A Basic/Snippet credential for RabbitMQ](#)
- [A "master" SOAP/XML credential](#) that references the CloudCenter Manager and RabbitMQ credentials and that you will use for discovering the high-availability CloudCenter deployment

Creating SSH/Key Credentials for CloudCenter Components

To configure SL1 to monitor HA Cisco CloudCenter deployments, you must create SSH/Key credentials that allow the Dynamic Applications in the *Cisco: CloudCenter PowerPack* to connect with the various components in your HA CloudCenter.

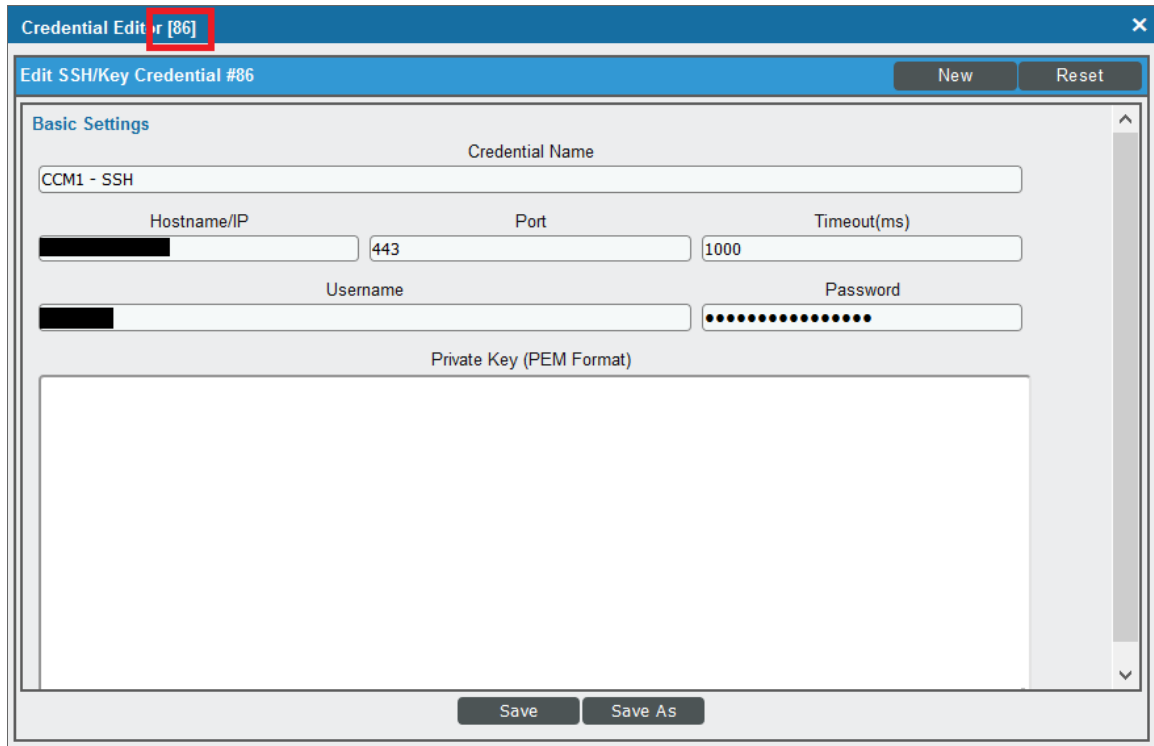
To create an SSH/Key credential to access a CloudCenter component:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create SSH/Key Credential*.
3. Complete the following fields.
 - **Credential Name.** Type a name for the credential.
 - **Hostname/IP.** Type the IP address for the component. **Do not use "%D"**.
 - **Port.** Type the port number required to access the component.
 - **Timeout(ms).** Type the time, in milliseconds, after which SL1 will stop trying to communicate with the component.
 - **Username.** Type the username for a user that has root tenant administration privileges for CloudCenter Manager, or read privileges for other components. This account must be an API user, not a GUI user.
 - **Password.** Type the API key for the user you entered in the **Username** field.
 - **Private Key (PEM Format).** Leave 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 **[Save]**.

5. SL1 assigns the credential an ID number. Take note of the ID number that appears in the Credential Editor heading, as you will need this when [creating the master SOAP/XML credential](#).



6. Repeat these steps for each major component in your HA CloudCenter deployment.

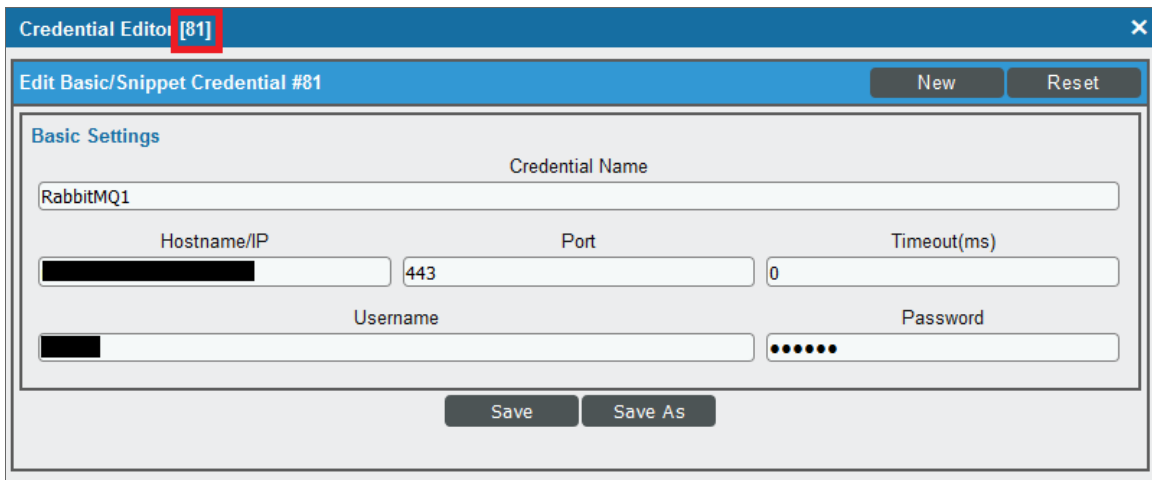
Creating a Basic/Snippet Credential for RabbitMQ

In addition to an SSH/Key credential that allows the Dynamic Applications in the *Cisco: CloudCenter PowerPack* to communicate with your RabbitMQ system, you must also create a Basic/Snippet credential for RabbitMQ. When you discover your HA CloudCenter deployment, these Dynamic Applications will discover and model the CloudCenter RabbitMQ components. These components will later be merged with the physical devices once they are discovered.

NOTE: When monitoring a high-availability CloudCenter deployment, the use of Basic/Snippet credentials will cause RabbitMQ Dynamic Applications to align to RabbitMQ devices, but those Dynamic Applications will not collect data. This is because SL1 discovers the RabbitMQ load balancer devices as the RabbitMQ components, rather than the actual RabbitMQ components themselves. This means that, even if you manually discover the RabbitMQ components, the *Cisco: CloudCenter PowerPack* has no way of linking them with the load balancers. If you would like to collect data for the non-load balancer RabbitMQ components, you can manually align the appropriate credentials.

To create a Basic/Snippet credential to access a RabbitMQ system:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create Basic/Snippet Credential*.
3. Complete the following fields.
 - **Profile Name**. Type a name for the RabbitMQ credential.
 - **Hostname/IP**. Type the hostname or IP address for the RabbitMQ server.
 - **Port**. Type the port number required to access the RabbitMQ server.
 - **Timeout(ms)**. Type the time, in milliseconds, after which SL1 will stop trying to communicate with the RabbitMQ server.
 - **Username**. Type the username for a RabbitMQ user that has read permission to the RabbitMQ API.
 - **Password**. Type the password for the user you entered in the **Username** field.
4. Click **[Save]**.
5. SL1 assigns the credential an ID number. Take note of the ID number that appears in the Credential Editor heading, as you will need this when [creating the master SOAP/XML credential](#).



The screenshot shows a modal window titled "Credential Editor #81" with a close button in the top right corner. Below the title bar is a sub-header "Edit Basic/Snippet Credential #81" and two buttons: "New" and "Reset". The main content area is titled "Basic Settings" and contains the following fields:

- Credential Name**: A text input field containing "RabbitMQ1".
- Hostname/IP**: A text input field with a blacked-out value.
- Port**: A text input field containing "443".
- Timeout(ms)**: A text input field containing "0".
- Username**: A text input field with a blacked-out value.
- Password**: A password input field with six dots.

At the bottom of the form are two buttons: "Save" and "Save As".

Creating the Master SOAP/XML Credential for High-Availability Discovery

After you have created the [SSH/Key](#) and [Basic/Snippet](#) credentials for the various components in your HA CloudCenter, you must create the SOAP/XML credential that will be used as the master credential to discover and model your HA CloudCenter deployment.

A sample credential (**Cisco CloudCenter - HA Example**) that you can use is included in the *Cisco CloudCenter PowerPack*.

To create a SOAP/XML credential for discovering HA Cisco CloudCenter deployments:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Cisco CloudCenter - HA Example** credential and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.

3. Complete the following fields:

Basic Settings

- **Profile Name.** Type a new name for the credential.
- **HTTP Auth User.** Type the username for a CloudCenter Manager user that has root tenant administration privileges. This account must be an API user, not a GUI user.
- **HTTP Auth Password.** Type the API key for the user you entered in the **HTTP Auth User** field.

HTTP Headers

- **HTTP Headers.** Type the following information for each of the CloudCenter components, creating a separate header for each component:
 - **RabbitMQ:** Type the header in the following format:
<Component Name>:<SSH/Key Credential ID>:<Basic/Snippet Credential ID>:<RabbitMQ IP address>:<RabbitMQ Load Balancer IP Address>

Example: If the RabbitMQ has an SSH/Key credential with the ID 60, a Basic/Snippet Credential with the ID 70, an IP address of 10.123.34.45, and a load balancer IP address of 10.22.33.45, then you would type "RabbitMQ:60:70:10.123.34.45:10.22.33.45".
 - **CloudCenter Manager:** Type the header in the following format:
<Component Name>:<SSH/Key Credential ID>:<IP address>

Example: If the CloudCenter Manager has an SSH/Key credential with the ID 80 and an IP address of 10.11.23.45, then you would type "CCM:80:10.11.23.45".
 - **CloudCenter Manager Load Balancer:** Type the header in the following format:
<Component Name>:<SSH/Key Credential ID>:<IP address>

Example: If the CloudCenter Manager Load Balancer has an SSH/Key credential with the ID 90 and an IP address of 10.22.12.34, then you would type "CCMLB:90:10.22.12.34".
 - **PostgreSQL Database:** Type the header in the following format:
<Component Name>:<SSH/Key Credential ID>:<IP address>

Example: If the PostgreSQL database has an SSH/Key credential with the ID 105 and an IP address of 10.32.54.76, then you would type "PostgreSQL:105:10.32.54.76".
 - **CloudCenter Orchestrator:** Type the header in the following format:
<Component Name>:<SSH/Key Credential ID>:<Orchestrator IP address>:<Orchestrator Load Balancer IP Address>

Example: If the CloudCenter Orchestrator has an SSH/Key credential with the ID 120, an IP address of 10.33.22.11, and a load balancer IP address of 10.99.88.77, then you would type "CCO:120:10.33.22.11:10.99.88.77".

- **CloudCenter Orchestrator Load Balancer:** Type the header in the following format:
 <Component Name>:<SSH/Key Credential ID>:<IP address>
Example: If the CloudCenter Orchestrator Load Balancer has an SSH/Key credential with the ID 120 and an IP address of 10.99.88.77, then you would type "CCOLB:120:10.99.88.77".
- **CloudCenter Health Monitor:** Type the header in the following format:
 <Component Name>:<SSH/Key Credential ID>:<IP address>
Example: If the Health Monitor has an SSH/Key credential with the ID 135 and an IP address of 10.56.77.89, then you would type "Monitor:135:10.56.77.89".
- **CloudCenter ELK Components:** Type the header in the following format:
 <ELK Name>:<SSH/Key Credential ID>:<IP address>
Example: If the ELK component has an SSH/Key credential with the ID 85 and an IP address of 10.13.24.57, then you would type "ELK:85:10.13.24.57".

NOTE: If you have more than one of the same component, then you can add numbers to the component name. For example: "CCM1", "CCM2", etc.

NOTE: Component names for load balancers must include "LB".

NOTE: If any of your components use a hostname instead of an IP address, you should include the hostname in place of the IP address.

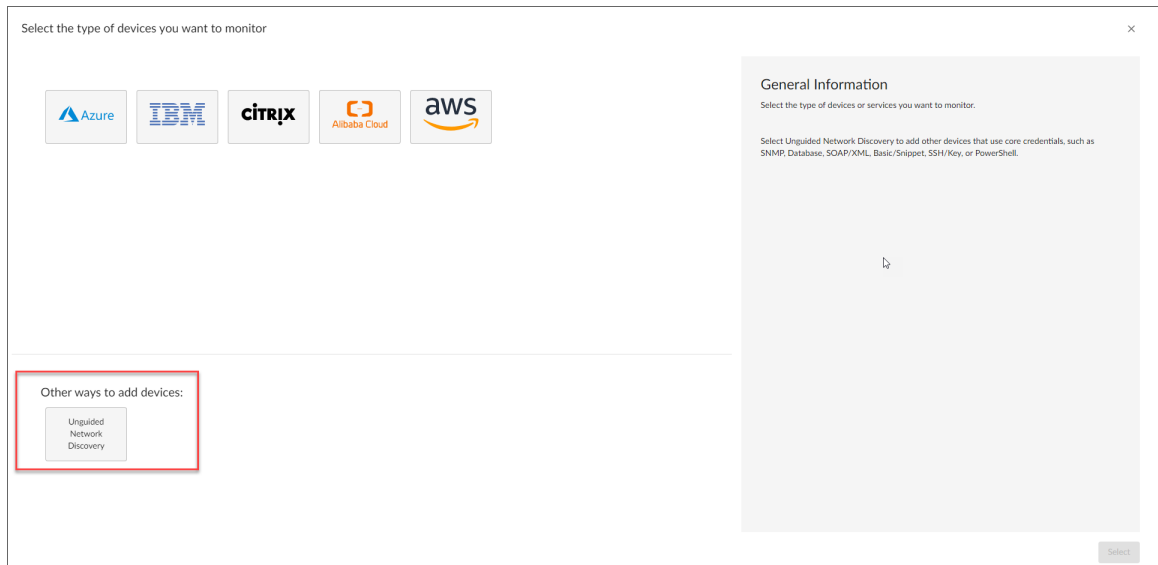
CAUTION: The IP address or hostname used in the header for a given component must match the IP address or hostname in the discovery payload. If any of the headers for any of the components are incorrect, SL1 will be unable to discover and model your HA CloudCenter deployment.

4. For all other fields, use the default values.
5. Click **[Save As]**.
6. In the confirmation message, click **[OK]**.

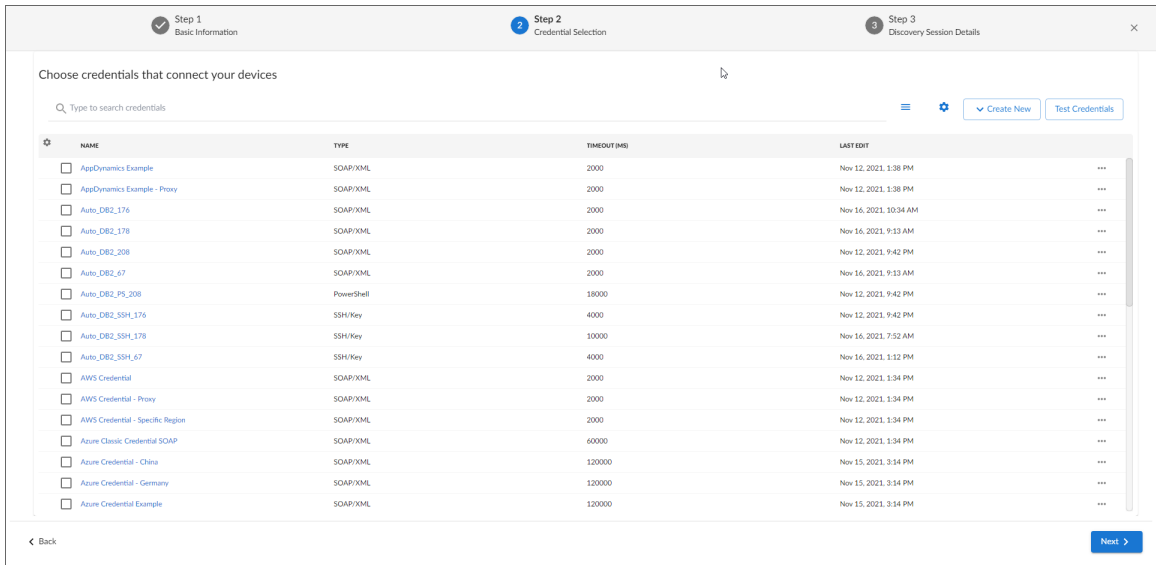
Discovering Cisco CloudCenter High-Availability Deployments

To discover a Cisco CloudCenter HA deployment:

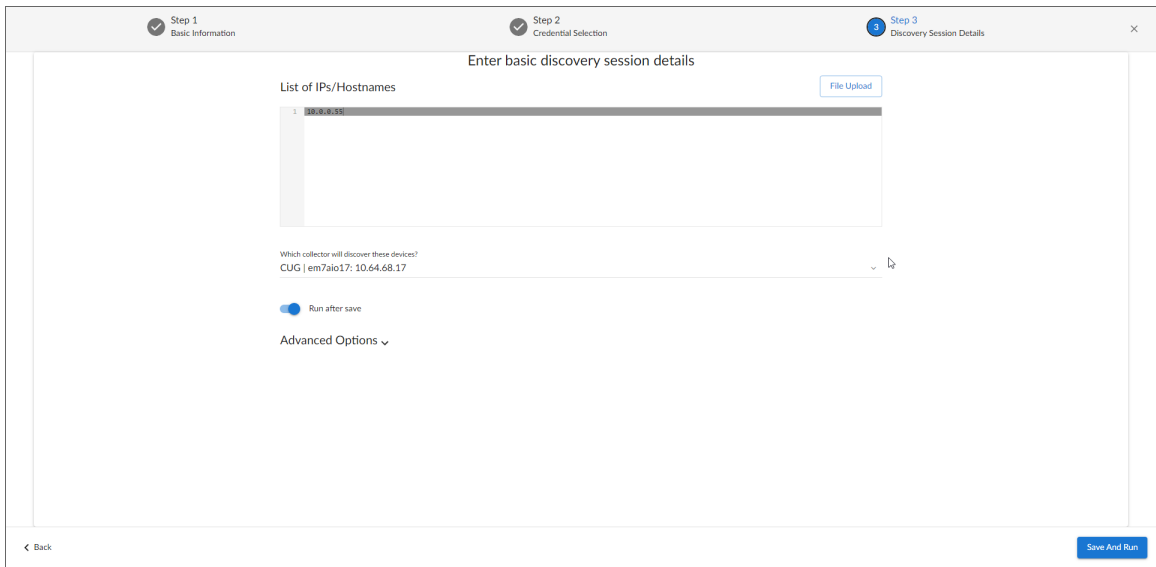
1. On the **Devices** page (🖨️) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



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:



- On the **Credentials** page, select the **SOAP/XML credential** you created for the HA CloudCenter deployment.
- Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



- Complete the following fields:
 - List of IPs/Hostnames.** Type the IP address for the CloudCenter Manager.
 - Which collector will monitor these devices?.** Required. Select an existing collector to monitor the discovered devices.
 - Run after save.** Select this option to run this discovery session as soon as you save the session.
 - 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 Run]** if you enabled the Run after save setting, or **[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 Cisco CloudCenter High-Availability Deployments in the SL1 Classic User Interface

To discover a Cisco CloudCenter HA deployment:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button.
3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, define values in the following fields.
 - **Name**. Type a name for the discovery session.
 - **IP Address/Hostname Discovery List**. Type the IP address for the CloudCenter Manager.
 - **Other Credentials**. Select the **SOAP/XML credential** you created for the HA CloudCenter deployment.
 - **Discover Non-SNMP**. Select this checkbox.
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the **Discovery & Credentials** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (⚡) to run the discovery session.
7. The **Discovery Session** window appears. When the device is discovered, click the device icon (📱) to view the **Device Properties** page for the device.

Verifying Discovery and Dynamic Application Alignment

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

1. From the **Device Properties** page for the CloudCenter HA root device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the CloudCenter root device 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.

The following Dynamic Applications should be aligned to the device:

- Cisco: CloudCenter Component Counts
- Cisco: CloudCenter CCM Discovery
- Cisco: CloudCenter CCM Load Balancer Health
- Cisco: CloudCenter HA Discovery
- Cisco: CloudCenter Tenant Discovery
- Cisco: CloudCenter Tenant Parent Relationships

If the listed Dynamic Applications have not been automatically aligned during discovery, 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.
3. In the **Credentials** field, select the **SOAP/XML credential** you created for CloudCenter.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

Discovering Multiple Tenants for High-Availability CloudCenter Deployments


The *Cisco: CloudCenter PowerPack* can be used to monitor an HA CloudCenter deployment that includes multiple tenants. To discover multiple tenants, you must follow the steps in the following sections for each tenant in order (in other words, parents must be discovered before their children):

- [Creating a Credential for an HA CloudCenter Manager Tenant](#)
- [Discovering an additional HA CloudCenter Manager Tenant](#)

NOTE: For each tenant, you must use the administrator account for that tenant when you create the credential.

Creating a Credential for a High-Availability CloudCenter Tenant

To configure a SOAP/XML credential to access an additional HA CloudCenter tenant:

1. Create any additional **SSH/Key** and **Basic/Snippet** credentials that you might need to reference in the SOAP/XML credential headers.
2. Go to the **Credential Management** page (System > Manage > Credentials).
3. Locate the credential you used to discover the root device for your HA deployment, and then click its wrench icon (). The **Edit SOAP/XML Credential** modal appears.

4. Enter values in the following fields.
 - **Profile Name.** Enter a new name for the credential.
 - For all other fields, follow the instructions described in the [Creating a SOAP/XML Credential for High-Availability Discovery](#) section.
5. Click the **[Save As]** button.

Discovering an Additional High-Availability CloudCenter Tenant

To discover an additional tenant:

1. From the **Device Properties** page for the CloudCenter HA root device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. Select the checkbox for the "Cisco: CloudCenter Tenant Discovery" Dynamic Application.
3. In the **Select Action** drop-down list, select the SOAP/XML credential you created for the tenant.
4. Click **[Go]**.

Viewing CloudCenter Component Devices

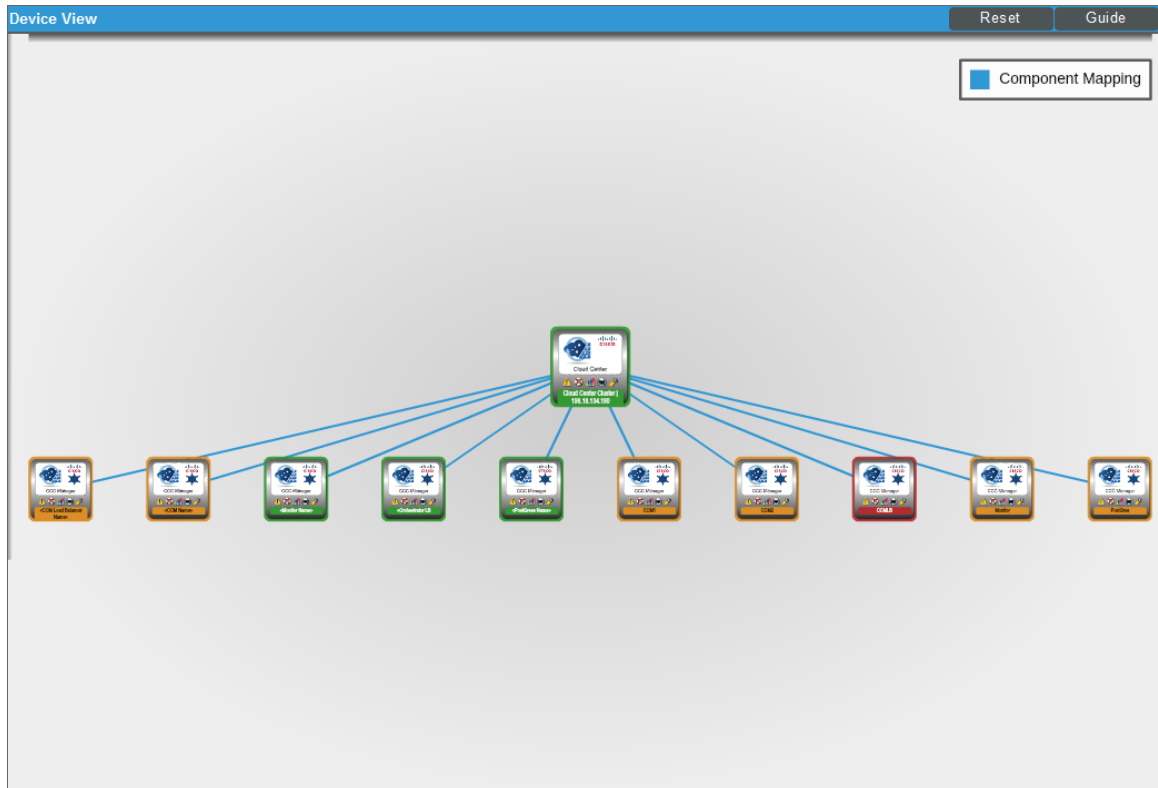
You can view CloudCenter Suite component devices in the following places in the user interface:

- 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 CloudCenter Suite, find the CloudCenter Suite 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 CloudCenter, 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.

Viewing CloudCenter Component Devices in the SL1 Classic User Interface

In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view CloudCenter Suite component devices in the following places in the user interface:

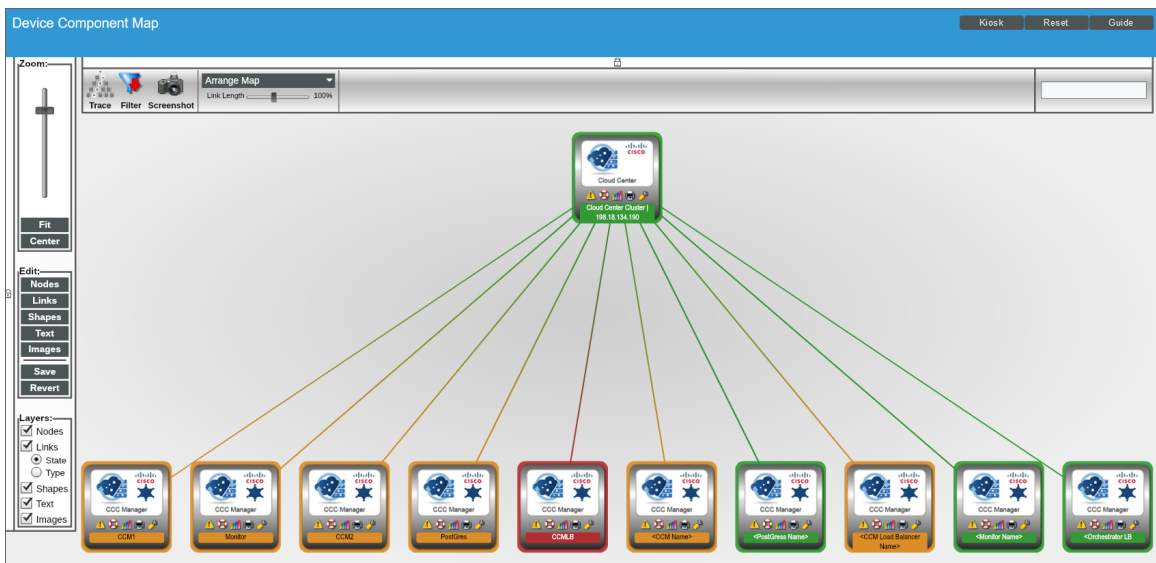
- The **Device View** page displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



- 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 CloudCenter Suite, find the CloudCenter Suite root device and click its plus icon (+):

Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State																																																																																																			
1. + Cisco Systems 198.18.134.190	--	Infrastructure	Cisco Systems Tenant	751	System	Healthy	CUG	Active																																																																																																			
2. - Cloud Center Cluster 198.18.134.190	--	Software	Cisco Systems Cloud Center	745	System	Healthy	CUG	Active																																																																																																			
<table border="1"> <thead> <tr> <th>Device Name</th> <th>IP Address</th> <th>Device Category</th> <th>Device Class Sub-class</th> <th>DID</th> <th>Organization</th> <th>Current State</th> <th>Collection Group</th> <th>Collection State</th> </tr> </thead> <tbody> <tr> <td>1. <CCM Load Balancer Name></td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Manager</td> <td>764</td> <td>System</td> <td>Major</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>2. <CCM Name></td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Manager</td> <td>762</td> <td>System</td> <td>Major</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>3. <Monitor Name></td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Monitor</td> <td>765</td> <td>System</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>4. <Orchestrator LB></td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Loadbalance</td> <td>766</td> <td>System</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>5. <PostGres Name></td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center PostGres</td> <td>763</td> <td>System</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>6. CCM1</td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Manager</td> <td>746</td> <td>System</td> <td>Major</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>7. CCM2</td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Manager</td> <td>748</td> <td>System</td> <td>Major</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>8. CCM LB</td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Loadbalance</td> <td>750</td> <td>System</td> <td>Critical</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>9. Monitor</td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center Monitor</td> <td>747</td> <td>System</td> <td>Major</td> <td>CUG</td> <td>Active</td> </tr> <tr> <td>10. PostGres</td> <td>--</td> <td>Software</td> <td>Cisco Systems Cloud Center PostGres</td> <td>749</td> <td>System</td> <td>Major</td> <td>CUG</td> <td>Active</td> </tr> </tbody> </table>									Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State	1. <CCM Load Balancer Name>	--	Software	Cisco Systems Cloud Center Manager	764	System	Major	CUG	Active	2. <CCM Name>	--	Software	Cisco Systems Cloud Center Manager	762	System	Major	CUG	Active	3. <Monitor Name>	--	Software	Cisco Systems Cloud Center Monitor	765	System	Healthy	CUG	Active	4. <Orchestrator LB>	--	Software	Cisco Systems Cloud Center Loadbalance	766	System	Healthy	CUG	Active	5. <PostGres Name>	--	Software	Cisco Systems Cloud Center PostGres	763	System	Healthy	CUG	Active	6. CCM1	--	Software	Cisco Systems Cloud Center Manager	746	System	Major	CUG	Active	7. CCM2	--	Software	Cisco Systems Cloud Center Manager	748	System	Major	CUG	Active	8. CCM LB	--	Software	Cisco Systems Cloud Center Loadbalance	750	System	Critical	CUG	Active	9. Monitor	--	Software	Cisco Systems Cloud Center Monitor	747	System	Major	CUG	Active	10. PostGres	--	Software	Cisco Systems Cloud Center PostGres	749	System	Major	CUG	Active
Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State																																																																																																			
1. <CCM Load Balancer Name>	--	Software	Cisco Systems Cloud Center Manager	764	System	Major	CUG	Active																																																																																																			
2. <CCM Name>	--	Software	Cisco Systems Cloud Center Manager	762	System	Major	CUG	Active																																																																																																			
3. <Monitor Name>	--	Software	Cisco Systems Cloud Center Monitor	765	System	Healthy	CUG	Active																																																																																																			
4. <Orchestrator LB>	--	Software	Cisco Systems Cloud Center Loadbalance	766	System	Healthy	CUG	Active																																																																																																			
5. <PostGres Name>	--	Software	Cisco Systems Cloud Center PostGres	763	System	Healthy	CUG	Active																																																																																																			
6. CCM1	--	Software	Cisco Systems Cloud Center Manager	746	System	Major	CUG	Active																																																																																																			
7. CCM2	--	Software	Cisco Systems Cloud Center Manager	748	System	Major	CUG	Active																																																																																																			
8. CCM LB	--	Software	Cisco Systems Cloud Center Loadbalance	750	System	Critical	CUG	Active																																																																																																			
9. Monitor	--	Software	Cisco Systems Cloud Center Monitor	747	System	Major	CUG	Active																																																																																																			
10. PostGres	--	Software	Cisco Systems Cloud Center PostGres	749	System	Major	CUG	Active																																																																																																			



- 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 CloudCenter, 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 **Views** manual.



Merging RabbitMQ and CloudCenter Orchestrator Devices

The Dynamic Applications in the *Cisco: CloudCenter PowerPack* create component devices for the RabbitMQ system and CloudCenter Manager. Optionally, you can discover these devices as physical SNMP devices and merge the component device record and physical device record. For information about discovering and monitoring a RabbitMQ system, see the **Monitoring RabbitMQ Systems** manual.

To merge individual devices:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Click the wrench icon () for the physical device that you want to merge with a component device.
3. On the **Device Properties** page, click the **[Actions]** menu and then select *Merge Device*.
4. A list of component devices that are available for merging with the physical device displays. Click the merge icon () for the component device you want to merge with the physical device. Information for the component device then displays in the **Selected Device** panel.
5. Click the **[Merge]** button. A pop-up message appears that asks you to confirm the merge.
6. Click the **[OK]** button.

NOTE: To view an updated list of devices that includes your merged devices, click the **[Reset]** button on the **Device Manager** page.

Relationships Between Component Devices

SL1 can automatically build relationships between CloudCenter component devices and other associated devices:

- If you discover an ACI system using the Dynamic Applications in the *Cisco: ACI PowerPack* version 106 or later, SL1 will automatically create relationships between CloudCenter Applications and ACI Application Network Profiles.
- If you discover an AWS account using the Dynamic Applications in the *Amazon Web Services PowerPack* version 103 or later, SL1 will automatically create relationships between CloudCenter Applications and AWS EC2 Instances.
- If you discover an Azure account using the Dynamic Applications in the *Microsoft: Azure PowerPack* version 103 or later, SL1 will automatically create relationships between CloudCenter Applications and Azure Virtual Machines.
- If you discover a vCenter device using the Dynamic Applications in the *VMware: vSphere Base Pack PowerPack* version 207 or later, SL1 will automatically create relationships between CloudCenter Applications and VMware Virtual Machines.

© 2003 - 2024, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

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>.

ScienceLogic

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

International: +1-703-354-1010