Red Hat CloudForms
4.1
Managing Providers

Managing your infrastructure, cloud, and containers providers

Red Hat CloudForms Documentation
Team

Red Hat CloudForms 4.1 Managing Providers

Managing your infrastructure, cloud, and containers providers

Red Hat CloudForms Documentation Team
cloudforms-docs@redhat.com

Legal Notice

Abstract

This guide covers managing your infrastructure, cloud, and containers providers in Red Hat CloudForms. If you have a suggestion for improving this guide or have found an error, please submit a Bugzilla report at http://bugzilla.redhat.com against Red Hat CloudForms Management Engine for the Documentation component. Please provide specific details, such as the section number, guide name, and CloudForms version so we can easily locate the content.

Table of Contents

CHAPTER 1. INFRASTRUCTURE PROVIDERS

In Red Hat CloudForms, an infrastructure provider is a virtual infrastructure environment that you can add to a Red Hat CloudForms appliance to manage and interact with the resources in that environment. This chapter describes the different types of infrastructure providers that you can add to Red Hat CloudForms, and how to manage them.

The web interface uses virtual thumbnails to represent providers. Each thumbnail contains four quadrants by default, which display basic information about each provider.

1. Number of hosts

2. Management system software

3. Currently unused

4. Authentication status

Icon	Description
	Validated: Valid authentication credentials have been added.
	Invalid: Authentication credentials are invalid.
	Unknown: Authentication status is unknown or no credentials have been entered.

1.1. DISCOVERING INFRASTRUCTURE PROVIDERS

In addition to individually adding providers, you can also discover all infrastructure providers in a given subnet range.

1. Navigate to **Compute → Infrastructure → Providers**.

2. Click ⚙ (**Configuration**), then click 🔍 (**Discover Infrastructure Providers**).

3. Select the types of provider to discover.

4. Enter a **Subnet Range** of IP addresses starting with a **From Address** and ending with a **To Address**. The cursor automatically advances as you complete each octet.

5. Click **Start**.

The appliance searches for all infrastructure providers in the specified subnet range, and adds them to the user interface. However, before you can manage the providers added via discovery, you must edit each provider and specify authentication details.

1.2. RED HAT ENTERPRISE VIRTUALIZATION MANAGER PROVIDERS

To use a Red Hat Enterprise Virtualization Manager provider, add it to the appliance and authenticate its hosts.

1.2.1. Adding a Red Hat Enterprise Virtualization Manager Provider

After initial installation and creation of a Red Hat CloudForms environment, add a Red Hat Enterprise Virtualization Manager provider to the appliance.

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Click ⚙ (**Configuration**), then click ⊕ (**Add a New Infrastructure Provider**).

3. Enter the **Name** of the provider to add. The **Name** is how the device is labeled in the console.

4. Select **Red Hat Enterprise Virtualization Manager** from the **Type** list.

5. Enter the **Host Name or IP address(IPv4 or IPv6)** of the provider.

> **Important**
>
> The **Host Name** must use a unique fully qualified domain name.

6. Enter the **API Port** if your provider uses a non-standard port for access.

7. Select the appropriate **Zone** for the provider. By default, the zone is set to **default**.

8. In the **Credentials** area, under **Default**, provide the login credentials required for the Red Hat Enterprise Virtualization Manager administrative user:

   ≫ Enter the user name, `admin@internal`, in the **Username** field.

   ≫ Enter the password in the **Password** field.

   ≫ Confirm the password in the **Confirm Password** field.

   ≫ Click **Validate** to confirm Red Hat CloudForms can connect to the Red Hat Enterprise Virtualization Manager.

9. Under **C & U Database** tab, provide the login credentials for the Red Hat CloudForms user of the Red Hat Enterprise Virtualization Data Warehouse database:

> **Important**
>
> To collect capacity and utilization data, you must enable the capacity and utilization server roles available under **Settings → Configuration → Server → Server Control**. For more information on capacity and utilization collection, see "Assigning the Capacity and Utilization Server Roles" in the *Deployment Planning Guide*.

> **Important**
>
> To collect capacity and utilization data for a Red Hat Enterprise Virtualization environment, the Data Warehouse and Reports components must be installed in that environment, and you must create a Red Hat CloudForms user in the Data Warehouse database.
>
> To install the Data Warehouse and Reports components in a Red Hat Enterprise Virtualization environment, see the Red Hat Virtualization Installation Guide.
>
> To create a Red Hat CloudForms user in the Data Warehouse database, see Data Collection for Red Hat Enterprise Virtualization 3.3 and 3.4 in the *Deployment Planning Guide*. `

   ⯈ Enter the database user name in the **Username** field.

   ⯈ Enter the user password in the **Password** field.

   ⯈ Confirm the user password in the **Confirm Password** field.

   ⯈ Click **Validate** to confirm Red Hat CloudForms can connect to the database.

10. Click **Save**.

1.2.2. Authenticating Red Hat Enterprise Virtualization Hosts

After adding a Red Hat Enterprise Virtualization infrastructure provider, you must authenticate its hosts to enable full functionality.

1. Navigate to **Compute → Infrastructure → Providers**.

2. Click on a provider to display its summary screen.

3. On the summary screen, click **Hosts** in the **Relationships** information box to display the hosts on that provider.

4. Select the hosts to authenticate. You can select all hosts using the **Check All** option.

5. Click ⚙ (**Configuration**).

6. Click ✎ (**Edit this item**).

7. In the **Credentials** area, enter credentials for the following, as required:

   a. **Default**: This field is mandatory. Users should have privileged access such as, root or administrator.

   b. **Remote Login**: Credentials for this field are required if SSH login is disabled for the **Default** account.

   c. **Web Services**: This tab is used for access to Web Services in Red Hat Enterprise Virtuaization Manager.

   d. **IPMI**: This tab is used for access to IPMI.

8. Click **Validate**.

9. If editing multiple hosts:

   a. Select a host from the **Select Host to validate against** list.

   b. If required, enter credentials for **Remote Login**, **Web Services**, and **IPMI** in their respective tabs; click **Validate**.

   c. Select another host to validate each of these credentials against.

10. Click **Add**.

1.3. OPENSTACK INFRASTRUCTURE PROVIDERS

Enable an OpenStack Infrastructure provider by adding it to the appliance.

1.3.1. Adding an OpenStack Infrastructure Provider

After initial installation and creation of a Red Hat CloudForms environment, add an OpenStack Infrastructure provider to the appliance. Red Hat CloudForms supports operating with the OpenStack `admin` tenant. When creating an OpenStack Infrastructure provider in Red Hat CloudForms, select the OpenStack Infrastructure provider's `admin` user because it is the default administrator of the OpenStack `admin` tenant. When using the `admin` credentials, a user in Red Hat CloudForms provisions into the `admin` tenant, and sees images, networks, and instances that are associated with the `admin` tenant.

> **Note**
>
> You can set whether Red Hat CloudForms should use the Telemetry service or Advanced Message Queueing Protocol (AMQP) for event monitoring. If you choose Telemetry, you should first configure the **ceilometer** service on the undercloud to store events. See Section 1.3.1.1, "Configuring the Undercloud to Store Events" for instructions.
>
> For more information, see OpenStack Telemetry (ceilometer) in the Red Hat OpenStack Platform *Architecture Guide*.

1. Navigate to **Compute → Infrastructure → Providers**.

2. Click ⚙ (**Configuration**), then click ⊕ (**Add a New Infrastructure Provider**).

3. Enter the **Name** of the provider to add. The **Name** is how the device is labeled in the console.

4. Select **OpenStack Platform Director** from the **Type** list.

5. Select the **API Version** of your OpenStack provider's Keystone service from the list. The default is `Keystone v2`.

6. Select the appropriate **Zone** for the provider. By default, the zone is set to **default**.

> **Note**
>
> For more information, see the definition of host aggregates and availability zones in OpenStack Compute (nova) in the Red Hat OpenStack Platform *Architecture Guide*.

7. In the **Default** tab, under **Endpoints**, configure the host and authentication details of your OpenStack provider:

    a. Enter the **Host Name or IP address(IPv4 or IPv6)** of the provider. If your provider is an undercloud, use its hostname (see Setting the Hostname for the System in Red Hat OpenStack Platform *Director Installation and Usage* for more details)

    b. In **API Port**, set the public port used by the OpenStack Keystone service. By default, OpenStack uses port 5000 for this.

    c. Select the appropriate **Security Protocol** used for authenticating with your OpenStack provider.

    d. In the **Username** field, enter the name of an OpenStack user with privileged access (for example, **admin**). Then, provide its corresponding password in the **Password** and **Confirm Password** fields.

    e. Click **Validate** to confirm Red Hat CloudForms can connect to the OpenStack provider.

8. Next, configure how Red Hat CloudForms should receive events from the OpenStack provider. Click the **Events** tab in the **Endpoints** section to start.

    ❯ To use the Telemetry service of the OpenStack provider, select **Ceilometer**. Before you do so, the provider must first be configured accordingly. See Section 1.3.1.1, "Configuring the Undercloud to Store Events" for details.

    ❯ If you prefer to use the AMQP Messaging bus instead, select **AMQP**. When you do: In **Hostname (or IPv4 or IPv6 address)** (of the **Events** tab, under **Endpoints**), enter the public IP or fully qualified domain name of the AMQP host.

        ▪ In the **API Port**, set the public port used by AMQP. By default, OpenStack uses port 5672 for this.

        ▪ In the **Username** field, enter the name of an OpenStack user with privileged access (for example, **admin**). Then, provide its corresponding password in the **Password** and **Confirm Password** fields.

        ▪ Click **Validate** to confirm the credentials.

9. You can also configure SSH access to all hosts managed by the OpenStack infrastructure provider. To do so, click on the **RSA key pair** tab in the **Endpoints** section.

   a. From there, enter the **Username** of an account with privileged access.

   b. If you selected **SSL** in **Endpoints > Default > Security Protocol** earlier, use the **Browse** button to find and set a private key.

10. Click **Add** after configuring the infrastructure provider.

> **Note**
>
> Red Hat CloudForms requires that the adminURL endpoint for all OpenStack services be on a non-private network. Accordingly, assign the adminURL endpoint an IP address of something other than `192.168.x.x`. The adminURL endpoint must be accessible to the Red Hat CloudForms Appliance that is responsible for collecting inventory and gathering metrics from the OpenStack environment. Additionally, all the Keystone endpoints must be accessible, otherwise refresh will fail.

1.3.1.1. Configuring the Undercloud to Store Events

To allow Red Hat CloudForms to receive events from a Red Hat OpenStack Platform environment, you must configure the **notification_driver** option for the Compute service and Orchestration service in that environment. To do so, edit *undercloud.conf*, and set *store_events* to *true* before installing the undercloud. See Installing the Undercloud and Configuring the Director in Red Hat OpenStack Platform *Director Installation and Usage* for related details.

1.4. VMWARE VCENTER PROVIDERS

To use a VMware vCenter provider, add it to the appliance and authenticate its hosts.

1.4.1. Adding a VMware vCenter Provider

After initial installation and creation of a Red Hat CloudForms environment, add a VMware vCenter provider to the appliance.

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Click ⚙ (**Configuration**), then click ⊕ (**Add a New Infrastructure Provider**).

3. Enter the **Name** of the provider to add. The **Name** is how the device is labeled in the console.

4. Select **VMware vCenter** from the **Type** list.

5. Enter the **Host Name or IP address(IPv4 or IPv6)** of the provider.

   > **Important**
   >
   > The **Host Name** must use a unique fully qualified domain name.

6. Select the appropriate **Zone** for the provider. By default, the zone is set to **default**.

7. In the **Credentials** area, under **Default**, provide the login credentials required for the VMware vCenter administrative user:

   - Enter the user name in the **Username** field.

   - Enter the password in the **Password** field.

   - Confirm the password in the **Confirm Password** field.

   - Click **Validate** to confirm Red Hat CloudForms can connect to the VMware vCenter.

8. Click **Add**.

1.4.2. Authenticating VMware vCenter Hosts

The procedure below describes how to authenticate the VMware vCenter hosts.

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Click on a provider to display its summary screen.

3. On the summary screen, click **Hosts** in the Relationships information box to display the hosts on that provider.

4. Select the hosts to authenticate. You can select all hosts using the **Check All** option.

5. Click ⚙ (**Configuration**)

6. Click ✎ (**Edit Selected items**).

7. In the **Credentials** area, under **Default**, provide the VMware ESXi login credentials:

   - Enter the user name in the **Username** field.

   - Enter the password in the **Password** field.

   - Confirm the password in the **Confirm Password** field.

   - Click **Validate** to confirm Red Hat CloudForms can connect to the VMware vCenter host.

8. If editing multiple hosts, select a host from the **Select Host to validate against** list; provide the VMware ESXi login credentials and click **Validate**.

9. Click **Save**.

1.4.2.1. Using a Non-Administrator Account for Host Credentials

After adding a VMware vCenter infrastructure provider, you must authenticate its hosts to enable full functionality. You can use administrator credentials, or create another user assigned to a role (See the VMware documentation for instructions on how to create a role) created for Red Hat CloudForms. The following privileges should be enabled for the non-administrator user:

From the Global group, check:

- Cancel task

- Diagnostics

- Log Event

- Set custom attribute

- Settings

The entire set of privileges for the following groups should be checked:

- Alarms

- Datastores

- dvPort Group

- Host

- Network

- Resource

- Scheduled Task

- Tasks

- Virtual Machine

- vSphere Distributed Switch

Additionally, you must assign the new role to the following objects:

- **Datacenter**: At the Datacenter the Red Hat CloudForms user/group must have at least the read-only role at the Datacenter level (Not Propagated) to be able to see the datacenter. Without this access, relationships cannot be made. Specifically, the datastores will not show up.

- **Cluster**: Each Cluster that the Red Hat CloudForms needs access to must have the new role assigned and propagated.

- **Folders**: Each Folder that Red Hat CloudForms needs access to must have the new role assigned and propagated.

- **Datastores**: Each Datastore that Red Hat CloudForms needs access to must have the new role assigned and propagated.

- **Networking**: Each vLAN or Port Group that Red Hat CloudForms needs access to must have the new role assigned and propagated.

1.5. MICROSOFT SCVMM PROVIDERS

To use a Microsoft System Center Virtual Machine Manager provider, add it to the appliance and set up the SCVMM server for authentication.

> **Note**
>
> To use a SCVMM provider, you must have at least one network adapter available for communication between the host and the SCVMM management server. Make sure that **Used by Management** is checked for this network adapter in the SCVMM host properties.

1.5.1. Authenticating to Microsoft SCVMM

Before you can add a Microsoft SCVMM provide to your Red Hat CloudForms environment, you must enable WinRM to listen for HTTP traffic on Microsoft SCVMM servers. You must also set the appropriate execution policy on the Microsoft SCVMM server to allow PowerShell scripts from the appliance to run remotely.

1. Log in to the Microsoft SCVMM server.

2. Enable WinRM for configuration.

   ```
   winrm quickconfig
   ```

3. Set the following options:

   ```
   winrm set winrm/config/client/auth @{Basic="true"}
   winrm set winrm/config/service/auth @{Basic="true"}
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```

4. For Windows 2012 R2 with PowerShell 4.0, use the following syntax to set these options:

   ```
   winrm set winrm/config/client/auth '@{Basic="true"}'
   winrm set winrm/config/service/auth '@{Basic="true"}'
   winrm set winrm/config/service '@{AllowUnencrypted="true"}'
   ```

5. Enable remote script execution on the SCVMM server using the Set-ExecutionPolicy cmdlet.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   For more information on SCVMM remote script execution policies, see Using the Set-ExecutionPolicy Cmdlet.

If PowerShell returns an error, search for **log_dos_error_results** in the **evm.log** and **scvmm.log** files for information.

1.5.2. Adding a Microsoft System Center Virtual Machine Manager Provider

After initial installation and creation of a Red Hat CloudForms environment, add a Microsoft System Center Virtual Machine Manager provider to the appliance.

1. Navigate to **Compute → Infrastructure → Providers**.

2. Click ⚙ (**Configuration**), then click ⊕ (**Add a New Infrastructure Provider**).

3. Enter the **Name** of the provider to add. The **Name** is how the device is labeled in the console.

4. Select **Microsoft System Center VMM** from the **Type** list.

5. Enter the **Host Name or IP address(IPv4 or IPv6)** of the provider.

> **Important**
>
> The **Host Name** must use a unique fully qualified domain name.

6. Select **Kerberos** or **Basic (SSL)** from the **Security Protocol** list.

    a. For **Kerberos**:

        i. Enter the user name and realm in the **Username** field.

        ii. Enter the password in the **Password** field.

        iii. Enter the password again in the **Confirm Password** field.

    b. For **Basic (SSL)**:

        i. Enter the user name in the **Username** field.

        ii. Enter the pasword in the **Password** field.

        iii. Enter the password again in the **Confirm Password** field.

7. Click **Validate** to confirm that Red Hat CloudForms can connect to the Microsoft System Center Virtual Machine Manager.

8. Click **Add**.

1.6. REFRESHING PROVIDERS

Refresh a provider to find other resources related to it. Use **Refresh** after initial discovery to get the latest data about the provider and the virtual machines it can access. Ensure the provider has credentials to do this. If the providers were added using **Discovery**, add credentials using (**Edit Selected Infrastructure Provider**).

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Select the providers to refresh.

3. Click (Configuration), and then (**Refresh Relationships and Power States**).

4. Click **OK**.

1.7. TAGGING MULTIPLE PROVIDERS

Apply tags to all providers to categorize them together at the same time.

1. Navigate to **Infrastructure → Providers**.

2. Check the providers to tag.

3. Click ⛊ (**Policy**), and then 🏷 (**Edit Tags**).

4. In the **Tag Assignment** area, select a customer tag to assign from the first list, then select a value to assign from the second list.

	Category	Assigned Value
🗑	Cost Center *	Cost Center 001
🗑	Environment *	Quality Assurance

Select a customer tag to assign: [Environment * ⇕] [<Select a value to assign> ⇕]

* Only a single value can be assigned from these categories

5. Select more tags as required; click (**Save**).

1.8. VIEWING A PROVIDER

From a list of providers, you can review a specific provider by clicking on it. This displays various options to access provider information.

Provider Management Screen
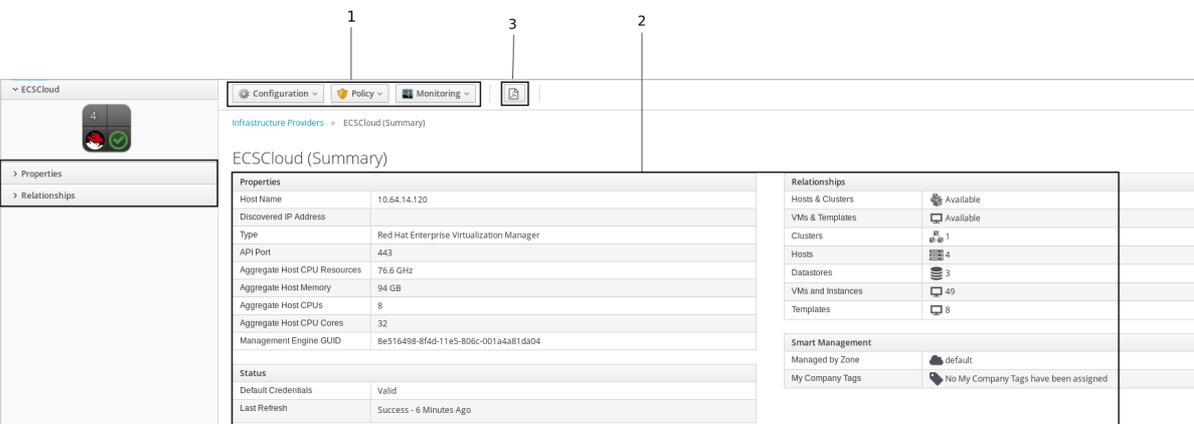
1. **Provider Taskbar**: Choose between Configuration, Policy and Monitoring options for the selected provider.

2. **Provider Summary**: Displays provider summary such as Properties, Relationships, and Smart Management.

3. **Provider Summary PDF**: Generates provider summary in PDF format.

4. **Provider Accordion**: Displays details about Properties and Relationships for the selected provider.

1.9. REMOVING A PROVIDER

If a provider has been decommissioned or requires some troubleshooting, it might require deletion from the VMDB.

Deleting a provider removes the account information from Red Hat CloudForms console. You will no longer be able to view any associated history including chargeback reports generated for the deleted provider. Additionally, if Red Hat CloudForms is the database of record, deleting providers would become a major problem for the other systems relying on it for accurate and consistent billing information. Review all the dependencies carefully before deleting a provider.

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Select the check box for the provider to delete.

3. Click ⚙ (**Configuration**), then 🗑 (**Remove Infrastructure Providers from the VMDB**).

4. Click (**OK**).

1.10. VIEWING THE PROVIDER TIMELINE

View the timeline of events for the virtual machines registered to a provider.

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Click a provider.

3. Click 〰 (**Monitoring**), and then ⊟ (**Timelines**)from the taskbar, or from the provider accordion, click **Properties** → **Timeline**.

4. From **Options**, customize the period of time to display and the types of events to see.

Options

Show	Management Events
Interval	Daily
Date	11/20/2015
Show	7 days back
Level	Summary
Event Groups	Power Activity
	<NONE>
	<NONE>

* Dates/Times on this page are based on time zone: UTC.

» Use **Show** to select regular Management Events or Policy Events.

» Use the **Interval** dropdown to select hourly or daily data points.

» Use **Date** to type the date for the timeline to display.

‣ If you select to view a daily timeline, use **Show** to set how many days back to go. The maximum history is 31 days.

‣ The three **Event Groups** lists allow you to select different groups of events to display. Each has its own color.

‣ From the **Level** list, select a **Summary** event, or a **Detail** list of events. For example, the detail level of a **Power On** event might include the power on request, the starting event, and the actual **Power On** event. If you select **Summary**, only the Power On event displays in the timeline.

1.11. VIEWING HOSTS AND CLUSTERS

Access a tree view of the hosts and clusters for a provider from the **Provider Summary**.

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Click the provider to view the hosts and clusters.

3. Click on the **Relationships** accordion, then click **Hosts & Clusters**.
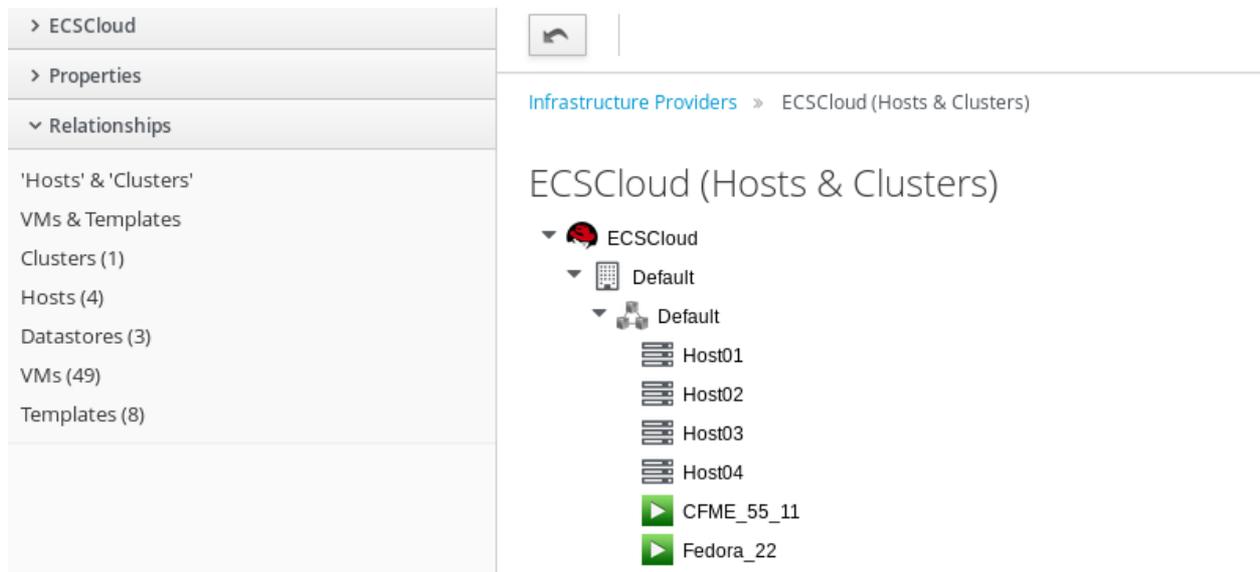
1.12. VIEWING VIRTUAL MACHINES AND TEMPLATES

Access a tree view of the virtual machines and templates for a provider from the **Provider Summary**.

1. Navigate to **Compute** → **Infrastructure** → **Providers**.

2. Click the provider to view the virtual machines and templates.

3. From accordion menu, click **Relationships**, then click **VMs & Templates**.

CHAPTER 2. CONFIGURATION MANAGEMENT PROVIDERS

Currently, Red Hat CloudForms has two configuration management providers integrated in it to review and monitor the configuration items and changes to them to eliminate the confusion and error brought about by the existence of different providers. These configuration systems are used for recording and reporting status and change activity for these configuration items.

2.1. RED HAT SATELLITE 6

Satellite 6 is a subscription and system management tool that provides a way to provision hosts (both virtual and bare metal) and configure them using a set of Puppet modules. Red Hat CloudForms provides functionality to integrate with a Red Hat Satellite 6 server and take advantage of its features. This includes:

- Monitoring the inventory of your Red Hat Satellite 6 server, including independent hosts and hosts provisioned using hostgroups.

- Reprovisioning existing bare metal system hosts to new host groups.

- Applying Red Hat CloudForms policy tags to hosts.

Important

Red Hat CloudForms only reprovisions existing systems in a Red Hat Satellite 6 environment. Provisioning systems from Red Hat Satellite 6's bare metal discovery service is planned for a future release.

2.1.1. Defining the Workflow

This section uses the following workflow:

1. Add Red Hat Satellite 6 server details to Red Hat CloudForms.

2. Refresh the state of your Red Hat Satellite 6 provider in Red Hat CloudForms.

3. Select an existing bare metal host from Red Hat Satellite 6 for reprovisioning.

4. Apply policy tags to Red Hat Satellite 6 hosts.

2.1.2. Defining the Hostgroup Hierarchy

Red Hat CloudForms displays the Red Hat Satellite 6 infrastructure in a host group and host relationship. A host group defines a set of default values that hosts inherit when placed in that group. Hosts can belong to only one host group, but host groups can be nested in hierarchies. You can create a **"base"** or **"parent"** host group that represents all hosts in your organization, and then create nested or **"child"** host groups under that parent to provide specific settings.

2.1.3. Adding a Satellite 6 Provider

To start provisioning bare metal machines, you need at least one Red Hat Satelllite 6 provider added to Red Hat CloudForms.

1. Navigate to **Configuration** → **Configuration Management**.

2. Select **Configuration** → **Add a new Provider**.

3. Enter a **Name** for the provider.

4. Enter a **URL** for the provider. This is the root URL for the Satellite 6 server and can be either an IP address or a hostname. For example, *http://satellite6.example.com*.

5. Select **Verify Peer Certificate** to use encrypted communication with the provider. This requires the **SSL certificates** from your Red Hat Satellite 6 provider.

6. Enter a **Username** for a user on the provider. Ideally, this would be a user in Satellite 6 with administrative access.

7. Enter a **Password**, and then enter it again in **Confirm Password**.

8. Click **Validate** to test your connection with the Red Hat Satellite 6 server.

9. Click **Add** to confirm your settings and save the provider.

Red Hat CloudForms saves the Satellite 6 provider in its database and triggers a refresh of resources detected in the provider.

2.1.4. Triggering a Refresh of a Satellite 6 Provider

Your Satellite 6 provider can still create new hosts independently of Red Hat CloudForms. Your Red Hat CloudForms appliance detects these changes after an automatic refresh period. However, you can trigger a manual refresh to avoid waiting for the automatic refresh.

1. Navigate to **Configuration** → **Configuration Management**.

2. Select your Red Hat Satellite 6 provider using the checkbox, and click **Configuration** → **Refresh Relationships and Power States**. This triggers the refresh.

3. When the refresh is complete, select the Red Hat Satellite 6 provider to check the updated list of hosts groups in the provider.

2.1.5. Displaying Red Hat Satellite 6 Contents

Red Hat CloudForms provides two methods for viewing the contents of a Red Hat Satellite 6 provider:

➤ **Providers** - This presents the Red Hat Satellite 6 contents as a hierarchy of host groups belonging to a provider, and then individual hosts belonging to each provider.

➤ **Configured Systems** - This presents a list of all hosts on your Red Hat Satellite 6 server. This also provides a method to apply predefined filters to organized specific machines.

Change between these two views using the accordion menu on the left of the user interface.

2.1.6. Reprovisioning a Bare Metal Host

This procedure provides an example of reprovisioning an existing bare metal system into a new hostgroup. For this example, your Red Hat Satellite 6 environment requires the following:

❯ An existing bare metal system stored as a host object in your Red Hat Satellite 6 server. This system can be one of the following:

  ▫ A standalone system previously provisioned without a host group.

  ▫ A system previously provisioned using a host group.

❯ A target host group. This host group contains the system configuration to apply to the host when reprovisioning it. This includes:

  ▫ A new operating system installation, including a new partition table.

  ▫ A new networking configuration that the Red Hat Satellite 6 server defines and manages.

  ▫ Registration to any Red Hat subscriptions and repositories assigned to the host group.

  ▫ Application of any Puppet modules assigned to the host group.

1. Navigate to **Configuration → Configuration Management**.

2. Select **Configured Systems** from the accordion menu on the left. This displays the system list.

3. Select one or more hosts to reprovision.

4. Select **Lifecycle → Provision Configured Systems**.

5. Under the **Request** tab, enter the following details:

   a. **E-Mail address**

   b. **First Name**

   c. **Last Name**

   d. This form also contains optional fields for users to enter a plain text **Note** to inform Red Hat CloudForms administrators of any special details, and a field to provide a manager's name in case administrators require approval from a user's manager.

6. Select the **Purpose** tab and select any Red Hat CloudForms policy tags that apply to the system.

7. Select the **Catalog** tab. This screen displays the list of chosen machines to reprovision and their current details. Select a **target host group** from the **Configuration Profile** list. Red Hat CloudForms communicates with Red Hat Satellite to apply the configuration from this host group to the selected host and reprovision the system.

8. Select the **Customize** tab. This screen displays some customizable fields for the selected system. You can change the **Root Password** or change the **Hostname** and **IP Address**. Note that these fields are optional, because the host group in Red Hat Satellite 6 contains this information. The fields here will override the settings from the host group.

Important

Provisioning bare metal systems still requires access to the network that Red Hat Satellite 6 manages. This is because Red Hat Satellite controls PXE booting, kickstarts, and Puppet configuration for bare metal systems. Ensure the IP address you enter in Red Hat CloudForms can access a DHCP service that Red Hat Satellite 6 provides either through the main server or through a Red Hat Satellite 6 Capsule server.

9. Select the **Customize** tab. This screen allows you to either launch the provisioning process immediately on approval or using a schedule. Click **Schedule** to show the date and time fields used to schedule the provisioning.

10. Click **Submit**.

Depending on the request settings on your Red Hat CloudForms appliance, this provisioning request might require approval from an administrator. If not, the provisioning request launches depending on your choice for the schedule.

Note

Previously provisioned hosts might require manual selection of PXE boot from the boot menu, otherwise they might boot to hard disk and not reprovision.

2.1.7. Tagging a Bare Metal Host

Red Hat CloudForms can also control policy settings of bare metal systems from Red Hat Satellite 6 through tagging. Tagging attaches levels of metadata to help define the policy rules required for a set of systems.

1. Navigate to **Configuration → Configuration Management**.

2. Select **Configured Systems** from the accordion menu on the left. This displays the system list.

3. Select one or more hosts to tag.

4. Select **Policy → Edit Tags**.

5. Under **Tag Assignment**, select a tag from **Select a customer tag to assign** and then choose a value from **Select a value to assign**. For example, you can tag this system as located in Chicago by selecting `Location` as the tag and `Chicago` as the value. Once selected, the user interface automatically adds this tag and value to the table below.

6. Click **Save**.

The bare metal system is now configured with a set of policy tags.

2.2. ANSIBLE TOWER

Ansible Tower is a management tool integrated with Red Hat CloudForms, designed to help automate infrastructure operations. Red Hat CloudForms allows you to execute Ansible Tower jobs using service catalogs and Automate. No custom configuration or Ruby scripting is needed in Red

Hat CloudForms, as configuration is done in Ansible Tower using playbooks.

You can use the large library of existing Ansible playbooks as Red Hat CloudForms state machines to automate tasks such as backups, package updates, and maintenance in your Red Hat CloudForms environment. This also includes deploying Red Hat Satellite agents on bare metal machines as required. This can be particularly useful for quickly applying changes across large environments with many virtual machines or instances. Using Ansible Tower, you can schedule Ansible playbook runs and monitor current and historical results, allowing for troubleshooting or identification of issues before they occur.

The basic workflow when using Red Hat CloudForms with an Ansible Tower provider is as follows:

1. Create an Ansible playbook which performs a specific task.

2. A new Ansible Tower job template is created from the playbook, which is then retrieved by Red Hat CloudForms.

3. From the Ansible Tower job template, create a new catalog item in Red Hat CloudForms, optionally with a service dialog that allows the user to enter parameters if needed.

4. The user orders the service from the Red Hat CloudForms user interface, and fills out any additional arguments (for example, limiting the task to run on a specific set of virtual machines).

5. The job executes.

Note

For more information on Ansible playbooks, see the Ansible playbook documentation.

2.2.1. Adding an Ansible Tower Provider

To access your Ansible Tower inventory from Red Hat CloudForms, you must add Ansible Tower as a provider.

1. Navigate to **Configuration** → **Configuration Management** → **Providers**.

2. Under ⚙ **Configuration**, click ⊕ **Add a new Provider**.

3. In the **Add a new Configuration Management Provider** area:
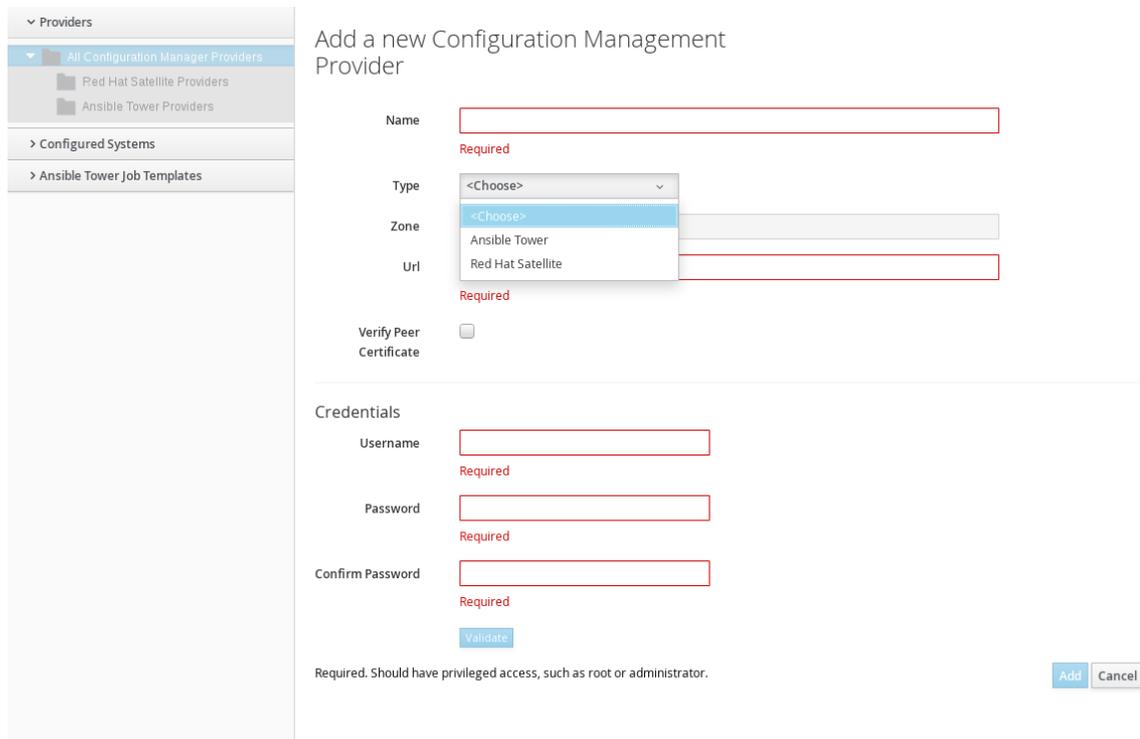
a. Enter a **Name** for the new provider.

b. In the **Type** field, select **Ansible Tower** from the list.

c. Enter the **URL** location or IP address to the Ansible Tower server.

4. Select the **Verify Peer Certificate** checkbox if desired.

5. In the **Credentials** area, provide the **Username** and **Password**, and **Confirm Password**.

6. Click **Add**.

After adding the Ansible Tower provider, refresh its relationships and power states in order to view the current inventory.

2.2.2. Refreshing an Ansible Tower Provider

Refresh relationships of all items related to an existing Ansible Tower configuration management provider including inventory, hosts, virtual machines, and clusters.

You can refresh inventory from Red Hat CloudForms, or by enabling the **Update on Launch** option for inventory groups in Ansible Tower. The **Update on Launch** option allows Ansible Tower to automatically update inventory using a dynamic inventory script before launching an Ansible Tower job from a playbook. See the Ansible Tower documentation for more information.

Important

It can take a long time to retrieve information from providers containing many virtual machines or instances. The Ansible Tower dynamic inventory script can be modified to limit updates to specific items and reduce refresh time.

To refresh an Ansible Tower provider's inventory in Red Hat CloudForms:

1. Navigate to **Configuration** → **Configuration Management** → **Providers**.

2. Select the checkboxes for the Ansible Tower providers to refresh under **All Ansible Tower Providers**.

3. Click ⚙ (**Configuration**), and then ↻ (**Refresh Relationships and Power States**).

4. Click **OK**.

Red Hat CloudForms then queries the Ansible Tower API and obtains an inventory of all available hosts and job templates.

2.2.3. Viewing Ansible Tower Providers and Inventory

Red Hat CloudForms automatically updates its inventory from Ansible Tower. This includes system groups (known as Inventories in Ansible Tower), basic information about individual systems, and available Ansible Tower job templates to be executed from the service catalog or Automate.

> **Note**
>
> To view and access Ansible Tower inventories and job templates in Red Hat CloudForms, you must first create them in Ansible Tower.

To view a list of Ansible Tower providers and inventory:

1. Navigate to **Configuration** → **Configuration Management** → **Providers**.

2. Under **All Configuration Manager Providers**, select the **Ansible Tower Providers** accordion menu to display a list of providers.

3. Select your Ansible Tower provider to expand and list the inventory groups on that Ansible Tower system. The inventory groups can be expanded to view the systems contained within each group, as well as configuration details for these systems.

Similarly, all discovered job templates are accessed under the provider by expanding the **Configuration** → **Configuration Management** → **Ansible Tower Job Templates** accordion menu.

2.2.4. Viewing Ansible Tower Configured Systems

To view the systems in your Ansible Tower inventory:

1. Navigate to **Configuration** → **Configuration Management** → **Configured Systems**.

2. Under **All Configured Systems**, select **Ansible Tower Configured Systems** to display a list.

2.2.5. Executing an Ansible Tower Job Template from a Service Catalog

You can execute an Ansible Tower playbook from Red Hat CloudForms by creating a service catalog item from an Ansible Tower job template.

Important

You must first create the job template in Ansible Tower. The job templates are automatically discovered by Red Hat CloudForms when refreshing your Ansible Tower provider's inventory.

First, create a catalog:

1. Navigate to **Services → Catalogs**.

2. Click (**Configuration**), then (**Add a New Catalog**)

3. Enter a **Name** and **Description** for the catalog.

4. Click **Add**.

Then, create an Ansible Tower service catalog item:

1. Navigate to **Configuration → Configuration Management**.

2. Click **Ansible Tower Job Templates** and select an Ansible Tower job template.

3. Click (**Configuration**), then (**Create Service Dialog from this Job Template**).

4. Enter a **Service Dialog Name** (for example, *ansible_tower_job*)and click **Save**.

5. Navigate to **Services → Catalogs**. Click **Catalog Items**.

6. Click (**Configuration**), then (**Add a New Catalog Item**) to create a new catalog item with the following details, at minimum:

   » For **Catalog Item type**, select **Ansible Tower**.

   » Enter a **Name** for the service catalog item.

   » Select **Display in Catalog**.

   » In **Catalog**, select the catalog you created previously.

   » In **Dialog**, select the service dialog you created previously (in this example, *ansible_tower_job*). **No Dialog** can be selected if the playbook does not require extra variables from the user. To ask the user to enter extra information when running the task, **Service Dialog** must be selected.

   » In **Provider**, select your Ansible Tower provider. This brings up the **Ansible Tower Job Template** option and configures the **Provisioning Entry Point State Machine** automatically.

   » Select your desired **Ansible Tower Job Template** from the list. Generally, this is the Ansible Tower job template previously used to create the service dialog.

Adding a new Service Catalog Item

Basic Info   Details

Name / Description	AT Service Catalog Item	My Ansible Tower Service Catalog It ☑ Display in Catalog
Catalog	Ansible Tower catalog	
Dialog	ansible_tower_job	
Provider	My Ansible Tower Provider Confi	
Ansible Tower Job Template	first_job_template	

Provisioning Entry Point State Machine (NS/CIs /Inst)   /ConfigurationManagement/AnsibleTower/Service/Provisioning/StateMachines/Provision/default   ✕

Reconfigure Entry Point State Machine (NS/CIs /Inst)   ✕

Retirement Entry Point State Machine (NS/CIs /Inst)   ✕

Add   Cancel

7. Click **Add**. The catalog item you created will appear in the **All Service Catalog Items** list.

To execute the Ansible Tower job:

1. Navigate to **Service Catalogs → Ansible Tower catalog**.

Service Catalogs	All Services		
All Services	Name	Description	Tenant
Ansible Tower catalog	AT Service Catalog Item	My Ansible Tower Service Catalog Item	My Company Order
Ansible Tower Catalog number 2	Update Service Catalog Item	Apply updates	My Company Order
Catalog Items			
Orchestration Templates			
Catalogs			

2. Click **Order** for the catalog item.

3. Enter any variables requested and click **Submit**.

Red Hat CloudForms takes you to the **Requests** queue page and show the status of the job.

The service item's details can be viewed in **Services → My Services** in Red Hat CloudForms.

Note

Instead of running a single job at a time, multiple service catalog items can also be grouped together as a catalog bundle to create one deployment with multiple job templates. See Catalogs and Services in *Provisioning Virtual Machines and Hosts* for more information.

2.2.6. Executing an Ansible Tower Job Using a Custom Automate Button

Red Hat CloudForms can execute Ansible Tower jobs on virtual machines or instances using custom buttons in Automate.

Ansible Tower jobs can either be non-customizable, which do not require any extra configuration

from the user, or alternatively, they can allow the user to specify a parameter (for example, a package name to install). In Ansible Tower jobs containing a dialog, Red Hat CloudForms accepts additional information from the user and adds it to the appropriate API call in Automate, and then sends it into Ansible Tower.

Prerequisites

Before creating an Automate button to execute an Ansible Tower job, the following must be configured:

» An Ansible playbook in Ansible Tower. See the Ansible Tower documentation for instructions.

» Ansible Tower must be able reach virtual machines or instances deployed by Red Hat CloudForms at the IP level.

» The virtual machine template must have the Ansible Tower environment's public SSH key injected. For cloud instances, `cloud-init` can be used and the public SSH key can be passed without rebuilding the image.

» Any dynamic inventory scripts used must be configured to return the virtual machine names exactly as they are stored in Red Hat CloudForms, without the UUID appended.

Executing an Ansible Tower Job using a Custom Automate Button

To configure a custom button to execute an Ansible Tower job on a virtual machine or instance, first create the button:

1. Navigate to **Automate → Customization**.

2. Click the **Buttons** accordion menu.

3. Click **VM and Instance → Unassigned Buttons**. This configures the button to run on virtual machines or instances.

4. Click ⚙ (**Configuration**), then click ⊕ (**Add a new Button**).

    » In the **Adding a new Button** screen, configure the **Action** parameters as desired. **Dialog** can be left blank if the playbook does not require extra variables. To ask the user to enter extra information when running the task, **Service Dialog** must be selected.

    » Configure **Object Details** fields with the following request details:

        ▫ For **System/Process**, select **Request**.

        ▫ For **Message**, enter **create**.

        ▫ For **Request**, enter **Ansible_Tower_Job**.

    » Configure **Attribute/Value Pairs** with the following parameters:

        ▫ **job_template_name** is the Ansible Tower job template name to associate with the button. The **job_template_name** field is mandatory; other parameters are provided by the Tower job dialog.

    » Configure **Visibility** to all users, or limit visibility by role as desired.

Adding a new Button

Action

Button Text	Update foo
Button Hover Text	Updates the foo package
Button Image	● Button Image 5
Dialog	<None>

☑ Display on Button

Object Details

System/Process	Request
Message	create
Request	Ansible_Tower_Job

Object Attribute

Type	Vm And Instance

Attribute/Value Pairs

1	job_template_name	first_job_template
2		
3		
4		
5		

Visibility

Show	<To All>

Save Reset Cancel

> Click **Add**.

If you do not have an existing button group to assign the new button to, create a new button group:

1. From **Automate** → **Customization**, navigate to **Buttons** → **VM and Instance** → **Add a new Button Group**, and configure the following:

   > Configure **Basic Info** as desired. For example, name the button group `VM Actions`.

   > In **Assign Buttons**, select the button you just created from the **Unassigned** list and click [>] to assign it to **Selected**.

Adding a new Buttons Group

Basic Info

Button Group Text	Package Updates
Button Group Hover Text	Update packages
Button Group Image	● Button Image 1

☑ Display on Button

Assign Buttons

Unassigned: Selected: Update foo

Add Cancel

> Click **Add**.

To assign the button to an existing button group:

1. Navigate to **Buttons** → **VM and Instance** → **VM Actions** → **Edit this Button Group**.

2. In **Assign Buttons**, select the button you just created from the **Unassigned** list and click

   to assign it to **Selected**.

3. Click **Add**.

To use the button to run an Ansible Tower job on a virtual machine:

1. Navigate to **Compute** → **Infrastructure** → **Virtual Machines**.

2. Select the virtual machine to run the Ansible Tower job template on.

3. Click the **VM Actions** button to show the button you created, and click the button from the list to run the Ansible Tower job template.

4. Click **Submit** to execute the job.

Red Hat CloudForms then confirms the job has been executed.

If you selected a service dialog to run when creating the button, Red Hat CloudForms will then prompt you to enter variables to complete the task. After entering your desired parameters, Red Hat CloudForms takes you to the **Requests** page.

The service item's details can be viewed in **Services** → **My Services** in Red Hat CloudForms.

CHAPTER 3. CLOUD PROVIDERS

In Red Hat CloudForms, a cloud provider is a cloud computing environment that you can add to a Red Hat CloudForms appliance to manage and interact with the resources in that environment. This chapter describes the different types of cloud providers that you can add to Red Hat CloudForms, and how to manage them.

3.1. OPENSTACK PROVIDERS

3.1.1. Adding OpenStack Providers

Red Hat CloudForms supports operating with the OpenStack **admin** tenant. When creating an OpenStack provider in Red Hat CloudForms, select the OpenStack provider's **admin** user because it is the default administrator of the OpenStack **admin** tenant. When using the **admin** credentials, a user in Red Hat CloudForms provisions into the **admin** tenant, and sees images, networks, and instances that are associated with the **admin** tenant.

> **Note**
>
> You can set whether Red Hat CloudForms should use the Telemetry service or Advanced Message Queueing Protocol (AMQP) for event monitoring. If you choose Telemetry, you should first configure the **ceilometer** service on the overcloud to store events. See Section 3.1.1.1, "Configuring the Overcloud to Store Events" for instructions.
>
> For more information, see OpenStack Telemetry (ceilometer) in the Red Hat OpenStack Platform *Architecture Guide*.

1. Navigate to **Compute → Clouds → Providers**.

2. Click ⚙ (**Configuration**), then click ➕ (**Add a New Cloud Provider**).

3. Enter a **Name** for the provider.

4. From the **Type** drop down menu select **OpenStack**.

5. Select the appropriate **API Version** from the list. The default is **Keystone v2**.

   If you select **Keystone v3**, enter the **Keystone V3 Domain ID** that Red Hat CloudForms should use. This is the domain of the user account you will be specifying later in the **Default** tab. If domains are not configured in the provider, enter **default**.

   > **Note**
   >
   > With Keystone API v3, domains are used to determine administrative boundaries of service entities in OpenStack. Domains allow you to group users together for various purposes, such as setting domain-specific configuration or security options. For more information, see OpenStack Identity (keystone) in the Red Hat OpenStack Platform *Architecture Guide*.

6. Select the appropriate **Zone** for the provider. By default, the zone is set to **default**.

> **Note**
>
> For more information, see the definition of host aggregates and availability zones in OpenStack Compute (nova) in the Red Hat OpenStack Platform *Architecture Guide*.

7. In the **Default** tab, under **Endpoints**, configure the host and authentication details of your OpenStack provider:

    a. In **Hostname (or IPv4 or IPv6 address)**, enter the public IP or fully qualified domain name of the OpenStack Keystone service.

    > **Note**
    >
    > The hostname required here is also the **OS_AUTH_URL** value in the **~/overcloudrc** file generated by the director (see Accessing the Overcloud in Red Hat OpenStack Platform *Director Installation and Usage* or the **~/keystonerc_admin** file generated by Packstack (see Evaluating OpenStack: Single-Node Deployment).

    b. In **API Port**, set the public port used by the OpenStack Keystone service. By default, OpenStack uses port 5000 for this.

    c. Select the appropriate **Security Protocol** used for authenticating with your OpenStack provider.

    d. In the **Username** field, enter the name of an OpenStack user with privileged access (for example, **admin**). Then, provide its corresponding password in the **Password** and **Confirm Password** fields.

    e. Click **Validate** to confirm Red Hat CloudForms can connect to the OpenStack provider.

8. Next, configure how Red Hat CloudForms should receive events from the OpenStack provider. Click the **Events** tab in the **Endpoints** section to start.

    » To use the Telemetry service of the OpenStack provider, select **Ceilometer**. Before you do so, the provider must first be configured accordingly. See Section 3.1.1.1, "Configuring the Overcloud to Store Events" for details.

    » If you prefer to use the AMQP Messaging bus instead, select **AMQP**. When you do: In **Hostname (or IPv4 or IPv6 address)** (of the **Events** tab, under **Endpoints**), enter the public IP or fully qualified domain name of the AMQP host.

        ▫ In the **API Port**, set the public port used by AMQP. By default, OpenStack uses port 5672 for this.

        ▫ In the **Username** field, enter the name of an OpenStack user with privileged access (for example, **admin**). Then, provide its corresponding password in the **Password** and **Confirm Password** fields.

        ▫ Click **Validate** to confirm the credentials.

9. Click **Add** after configuring the cloud provider.

Note

To collect inventory and metrics from an OpenStack environment, the Red Hat CloudForms appliance requires that the adminURL endpoint for the OpenStack environment should be on a non-private network. Hence, the OpenStack adminURL endpoint should be assigned an IP address other than **192.168.x.x**. Additionally, all the Keystone endpoints must be accessible, otherwise refresh will fail.

3.1.1.1. Configuring the Overcloud to Store Events

By default, the Telemetry service does not store events emitted by other services in a Red Hat OpenStack Platform environment. The following procedure outlines how to enable the Telemetry service on your OpenStack cloud provider to store such events. This ensures that events are exposed to Red Hat CloudForms when a Red Hat OpenStack Platform environment is added as a cloud provider.

1. Log in to the undercloud host.

2. Create an environment file called *ceilometer.yaml*, and add the following contents:

   ```
   parameter_defaults:
      CeilometerStoreEvents: true
   ```

3. Add the environment file to the *overcloud deploy* command:

   ```
   # openstack overcloud deploy --templates -e ~/ceilometer.yaml
   ```

If your OpenStack cloud provider was not deployed through the undercloud, you can also set this manually. To do so:

1. Log in to your Controller node.

2. Edit */etc/ceilometer/ceilometer.conf*, and specify the following option:

   ```
   store_events = True
   ```

3. Edit */etc/heat/heat.conf*, and specify the following options:

   ```
   notification_driver=glance.openstack.common.notifier.rpc_notifier
   notification_topics=notifications
   ```

4. Edit */etc/nova/nova.conf*, and specify the following options:

   ```
   notification_driver=messaging
   notification_topics=notifications
   ```

5. Restart the Compute service and Orchestration services:

   ```
   # systemctl restart openstack-heat-api.service \
      openstack-heat-api-cfn.service \
      openstack-heat-engine.service \
      openstack-heat-api-cloudwatch.service
   ```

```
# systemctl restart openstack-nova-compute.service
```

3.2. AZURE PROVIDERS

3.2.1. Adding Azure Providers

Red Hat CloudForms supports Microsoft Azure providers. Before CloudForms can be authenticated to Microsoft Azure, you must complete a series of prerequisite steps using the Azure portal; see Create Active Directory application and service principal account using the Azure portal. Follow the steps to set up an Azure Active Directory (Azure AD) and assign the required permissions to it, then create an Azure Active Directory application, and obtain the **Application ID** (Client ID), **Directory ID** (Tenant ID), **Subscription ID**, and **Key Value** (Client Key) that are required to add and connect to the Azure instance as a provider in CloudForms. Currently, all of these steps can be performed using either the Azure Resource Manager or Service Manager (Classic) mode.

> **Note**
>
> In the steps described in Create Active Directory application and service principal account using the Azure portal:
>
> » The **Application ID** obtained during *Get Application ID and Authentication Key* is your **Client ID**. In the same section, after providing a description and a duration for the key, the **VALUE** displayed after clicking **Save** is your **Client Key**. If you choose an expiring key, make sure to note the expiration date, as you will need to generate a new key before that day in order to avoid an interruption.
>
> » The **Directory ID** obtained during *Get Tenant ID* is your **Tenant ID**. In Azure Active Directory (Azure AD), a tenant is a dedicated instance of the Azure AD service and is representative of an organization. It houses the users in a company and the information about them - their user profile data, permissions, groups, applications, and other information related to an organization and its security. To allow Azure AD users to sign in to your application, you must register your application in a tenant of your own which is assigned a Tenant ID (Directory ID).
>
> » During *Assign Application to Role*, select the **Contributor** role and not the **Reader** role.
>
> » To obtain your **Subscription ID**, log in to the Azure portal and click **Subscriptions** on the slide-out menu on the left. Find the appropriate subscription and see your Azure **Subscription ID** associated with it. Note that if the **Subscriptions** tab is not visible, then click on **More services >** to find it. The Azure **Subscription ID** is like a billing unit for all of the services consumed in your Azure account, including virtual machines and storage. The **Subscription ID** is in the form of a Globally Unique Identifier (GUID).

So, after a service principal account (instance of an application in a directory) has been created using the Azure portal, the following four pieces of information will be available within the Azure AD module.

» Directory ID (Tenant ID)

» Subscription ID

» Application ID (Client ID)

» Client Key

You can now use these values in the procedure below to add an Azure cloud instance as a provider to CloudForms.

To Add an Azure Cloud Provider:

1. Navigate to **Compute → Clouds → Providers**.

2. Click (**Configuration**), then click (**Add a New Cloud Provider**).

3. Enter a **Name** for the provider.

4. From the **Type** list, select **Azure**.

5. Select a region from the **Region** list. One provider will be created for the selected region.

6. Enter **Tenant ID**.

7. Enter **Subscription ID**.

8. Enter **Zone**.

9. In the **Credentials** section, enter the **Client ID** and **Client Key**; click **Validate**.

10. Click **Add**.

3.2.2. Discovering Azure Providers

Red Hat CloudForms provides the ability to discover a set of Microsoft Azure providers across all regions.

1. Navigate to **Compute → Clouds → Providers**.

2. Click (**Configuration**), then click (**Discover Cloud Providers**).

3. Select Azure from the **Discover Type** list.

4. In the Credentials section, enter the **Client ID**, **Client Key**, and **Azure Tenant ID**.

5. Click **Start**.

3.3. AMAZON EC2 PROVIDERS

3.3.1. Permissions for Amazon EC2 Providers

Red Hat recommends using Amazon EC2's *Power User* Identity and Access Management (IAM) policy when adding Amazon EC2 as a cloud provider in CloudForms.

This policy allows those in the *Power User* group full access to AWS services except for user administration, meaning a CloudForms API user can access all of the API functionality, but cannot access or change user permissions.

Further limiting API access limitations can limit Automate capabilities, as Automate scripts directly access the AWS SDK to create brand new application functionality.

The AWS services primarily accessed by the CloudForms API include:

- Elastic Compute Cloud (EC2)

- CloudFormation

- CloudWatch

- Elastic Load Balancing

- Simple Notification Service (SNS)

- Simple Queue Service (SQS)

3.3.2. Adding Amazon EC2 Providers

After initial installation and creation of a Red Hat CloudForms environment, add an Amazon EC2 cloud provider by following this procedure:

1. Navigate to **Compute** → **Clouds** → **Providers**.

2. Click (**Configuration**), then click (**Add a New Cloud Provider**).

3. Enter a **Name** for the provider.

4. From the **Type** list, select **Amazon EC2**.

5. Select an **Amazon Region**.

6. Select the appropriate **Zone** if you have more than one available.

7. Generate an **Access Key** in the **Security Credentials** of your Amazon AWS account. The **Access Key ID** acts as your **User ID**, and your **Secret Access Key** acts as your **Password**.

8. Click **Validate** to validate the credentials.

9. Click **Add**.

3.3.3. Discovering Amazon EC2 Cloud Providers

Red Hat CloudForms provides the ability to discover cloud providers associated with a particular set of Amazon EC2 account details.

1. Navigate to **Compute** → **Clouds** → **Providers**.

2. Click (**Configuration**), then click (**Discover Cloud Providers**).

3. Select Amazon EC2 from the **Discover Type** list.

4. Enter your Amazon EC2 **User ID** and **Password**. Reenter your password in the **Verify Password** field.

5. Click **Start**.

3.3.4. Enabling Public AMIs from Amazon EC2

By default, public AMIs from an Amazon EC2 provider are not viewable in Red Hat CloudForms. To make these images viewable, you must edit the main configuration file for the appliance.

1. Navigate to **Settings → Settings → Configuration → Zone → Advanced**.

2. Select the configuration file to edit from the **File** list. If not already automatically selected, select **EVM Server Main Configuration**.

3. Set the **get_public_images** parameter:

   a. Set the parameter to **get_public_images: true** to make public images viewable.

   b. Set the parameter to **get_public_images: false** to make public images not viewable.

3.3.5. Enabling AWS Config Notifications

Amazon's AWS Config notifies subscribers of changes in a region through its Simple Notification Service (SNS). Red Hat CloudForms subscribes to the SNS service for AWS Config deltas and converts the deltas into Red Hat CloudForms events.

1. Enable the AWS Config service in the AWS Management Console. See the AWS Config Developer Guide for more information.

2. Create a new Amazon SNS topic named `AWSConfig_topic`. Red Hat CloudForms automatically connects to this topic.

3. (Optional) Configure the frequency of delta creation in the AWS Management Console.

You can assign Red Hat CloudForms policies to the AWS events listed below. The appliance performs a provider refresh on all these events except for `AWS_EC2_Instance_UPDATE`.

Event	Policies	Refresh
AWS_EC2_Instance_CREATE	src_vm vm_create	ems
AWS_EC2_Instance_UPDATE	N/A	ems
AWS_EC2_Instance_running	src_vm vm_start	ems
AWS_EC2_Instance_stopped	src_vm vm_power_off	ems

Event	Policies	Refresh
AWS_EC2_Instance_shutting-down	src_vm vm_power_off	ems

3.4. GOOGLE COMPUTE ENGINE PROVIDERS

3.4.1. Adding Google Compute Engine Providers

After initial installation and creation of a Red Hat CloudForms environment, add a Google Compute Engine provider by following this procedure.

Prerequisites

To add a Google Compute Engine provider to Red Hat CloudForms, you need:

» A Google Cloud Platform account

» A Google Compute Engine project with the Google Compute Engine API enabled

» A service account JSON key for your project

Note

You can generate a private JSON key for your project in **IAM & Admin → Service Accounts** in Google Compute Platform. This key is used to authenticate against your provider.

For additional information, see the Google Compute Platform documentation at https://cloud.google.com/storage/docs/authentication.

To add a Google Compute Engine provider:

1. Navigate to **Compute → Clouds → Providers**.

2. Click ⚙ (**Configuration**), then click ⊕ (**Add a New Cloud Provider**).

3. Enter a **Name** for the provider.

4. From the **Type** list, select **Google Compute Engine**.

5. Select your **Preferred Region** from the list.

6. Enter your Google Compute Engine Project ID for **Project**.

7. Select the appropriate **Zone** if you have more than one available. Red Hat recommends creating a new zone for your Google Compute Engine provider.

8. Copy your project's **Service Account** JSON key contents to the **Service Account JSON** field.

9. Click **Validate** to validate the credentials.

10. Click **Add**.

3.4.2. Enabling Google Compute Engine Events

After adding Google Compute Engine as a provider in Red Hat CloudForms, enable events for the provider so that you can monitor the system from Red Hat CloudForms.

Events are set up on a per-project basis by using Google Stackdriver logging combined with Google Pub/Sub. Stackdriver logging is a service that aggregates and exposes log events from Google services and applications. Stackdriver exports the log events to Google Pub/Sub, a messaging service. This section describes how to export activity log entries for a Google Compute Engine project so that events are captured in Red Hat CloudForms.

Prerequisites for Exporting Google Compute Engine Events

❯❯ You must have owner permission on the project you are exporting.

❯❯ The Google Cloud Pub/Sub API must be enabled for your project. To enable the API:

1. In Google Cloud Platform, select your project from the top menu bar.

2. Click ☰ to show the **Products and Services** menu. Click **API Manager** to go to https://console.cloud.google.com/apis/library/.

3. In the API Manager **Overview** tab, search for **Pub/Sub** in the **Google APIs** search bar and select **Google Cloud Pub/Sub API** from the results. Click the **Enable** button.

4. If Google Cloud Pub/Sub API is already enabled, the **Enable** button will not show, and instead **Google Cloud Pub/Sub API** will be listed under **Enabled APIs**.

❯❯ The Stackdriver logging service must have permission to publish to your project's Pub/Sub service. To add the required permissions:

1. In Google Cloud Platform, select your project and navigate to ☰ **Products and Services** → **IAM & Admin** → **IAM** to go to https://console.cloud.google.com/iam-admin/iam/.

2. Assign **Logs Configuration Writer** permissions to your project:

   a. If the `cloud-logs@system.gserviceaccount.com` account is already listed under **Members**, ensure **Logs Configuration Writer** is selected under **Role(s)**.

   b. If the `cloud-logs@system.gserviceaccount.com` account is not listed under **Members**:

      i. Click **Add** to add the permissions.

      ii. In the dialog box, enter `cloud-logs@system.gserviceaccount.com` in **Members** to add the Google APIs service account to the permissions list.

      iii. In the **Select a Role** dropdown, select **Logging** → **Logs Configuration Writer** and click **Add**.

3.4.2.1. Configuring Google Compute Engine to Export Events

After you have completed the steps from Prerequisites for Exporting Google Compute Engine Events, set up your Google Compute Engine project to export events to Red Hat CloudForms with the following steps:

1. In Google Cloud Platform, click to show the **Products and Services** menu, and click **Logging** to go to https://console.cloud.google.com/logs/.

2. Select your project from the top menu bar.

3. Click **Exports** from the **Logging** menu.

4. In the **Select service** list, select **Compute Engine**.

5. Under **Export these sources**, click **Add item**, and select `compute.googleapis.com/activity_log` from the list.

6. Under **Select export destinations**, click the **Publish to Cloud Pub/Sub topic** dropdown and click **Add new topic…**

7. In the **Create Cloud Pub/Sub Topic** dialog, enter `manageiq-activity-log` as the **Name**. Click **Create**.

Exports

Select service

Compute Engine ▾

Export these sources

☐ All logs

compute.googleapis.com/activity_log ▾ ✕

+ Add item

Select export destinations

Stream to BigQuery dataset ⑦

Don't export to BigQuery ▾

Save to Cloud Storage bucket ⑦

Don't export to Cloud Storage ▾

Publish to Cloud Pub/Sub topic ⑦

manageiq-activity-log ▾

Save   Revert

8. Click **Save**.

When changes occur to Google Compute Engine instances, Red Hat CloudForms is now notified and reports these changes as events.

> **Note**
>
> For additional information about Google Compute Engine, see the Google Compute Platform documentation:
>
> » For information on setting up a cloud logging export on Google Cloud Platform, see https://cloud.google.com/logging/docs/export/configure_export.
>
> » For information on Google Cloud Pub/Sub API operations and costs, see https://cloud.google.com/pubsub/.

3.4.2.2. Viewing Google Compute Engine Events in Red Hat CloudForms

In Red Hat CloudForms, view events for your Google Compute Engine project by following these

steps:

1. Navigate to **Compute** → **Clouds** → **Providers** and select your Google Compute Engine project.

2. Click **Monitoring** → **Timelines** on the provider summary page to see an events timeline for the project.

3.5. REFRESHING CLOUD PROVIDERS

Refresh a cloud provider to find other resources related to it. Ensure the chosen cloud providers have the correct credentials before refreshing.

1. Navigate to **Compute** → **Clouds** → **Providers**.

2. Select the checkboxes for the cloud providers to refresh.

3. Click ⚙ (**Configuration**), and then 🔄 (**Refresh Relationships and Power States**).

4. Click **OK**.

3.6. TAGGING CLOUD PROVIDERS

Apply tags to all cloud providers to categorize them together at the same time.

1. Navigate to **Compute** → **Clouds** → **Providers**.

2. Select the checkboxes for the Cloud Providers to tag.

3. Click 🛡 (**Policy**), and then ✏ (**Edit Tags**).

4. **Select a customer tag to assign** from the first list.

5. Select a value to assign from the second list.

6. Click **Save**.

3.7. REMOVING CLOUD PROVIDERS

A cloud provider might require removal from the VMDB if it is no longer in use.

1. Navigate to **Compute** → **Clouds** → **Providers**.

2. Check the cloud providers to remove.

3. Click ![gear] (**Configuration**), and then ![trash] (**Remove Cloud Providers from the VMDB**).

4. Click **OK**.

3.8. EDITING A CLOUD PROVIDER

Edit information about a provider such as the name, IP address, and login credentials.

> **Note**
>
> The **Type** value is unchangeable.

To use a different cloud provider, create a new one.

1. Navigate to **Compute** → **Clouds** → **Providers**.

2. Click the cloud provider to edit.

3. Click ![gear] **(Configuration)**, and then ![pencil] **(Edit Selected Cloud Provider)**.

4. Edit the **Basic Information**. This varies depending on the **Type** of provider.

5. Fill out the **Credentials** by typing in a **Username**, **Password**, and a verification of this password (**Confirm Password**).

   ≫ If selecting **Amazon EC2**, generate an **Access Key** in the **Security Credentials** of your Amazon AWS account. The **Access Key ID** acts as your **User ID**, and your **Secret Access Key** acts as your **Password**.

   ≫ If selecting **OpenStack**, use the `Keystone User ID` and `Password` for your login credentials.

6. If editing an OpenStack provider, use the **AMQP** subtab to provide credentials required for the Advanced Message Queuing Protocol service on your OpenStack Nova component.

7. Click **Validate** and wait for notification of successful validation.

8. Click **Save**.

3.9. VIEWING A CLOUD PROVIDER'S TIMELINE

View the timeline of events for instances registered to a cloud provider.

1. Navigate to **Compute** → **Clouds** → **Providers**.

2. Click the desired cloud provider for viewing the timeline.

3. Click ![monitoring] (**Monitoring**), and then ![timelines] (**Timelines**).

4. From **Options**, customize the period of time to display and the types of events to see.

   ≫ Use **Show** to select regular Management Events or Policy Events.

- Use the **Type** list to select hourly or daily data points.

- Use **Date** to type the date for the timeline to display.

- If you select to view a daily timeline, use **Show** to set how many days back to go. The maximum history is 31 days.

- The three **Event Groups** list allow you to select different groups of events to display. Each has its own color.

- From the **Level** list, select a **Summary** event, or a **Detail** list of events.

CHAPTER 4. NETWORK PROVIDERS

Red Hat CloudForms has introduced a new provider type called **Network Managers**. This new provider type exposes software-defined networking (SDN) providers starting with *OpenStack Network (Neutron)*, *Azure Network*, and *Amazon EC2 Network*. The software-defined networking inventory collection is enabled for OpenStack, Amazon and Azure providers. The OpenStack Network provider collects inventory of floating IPs from OpenStack so that IPs can be allocated without querying OpenStack database every time. Also, it refreshes all Neutron data from both OpenStack and OpenStack Infrastructure, and extracts the Neutron logic to a shared place. Note that management via the network providers configuration is currently disabled.

4.1. ADDING OR VIEWING NETWORK PROVIDERS

> **Note**
>
> All supported network providers, that is OpenStack Network, Azure Network, and Amazon EC2 Network, are added or removed automatically upon adding or removing the respective cloud provider.

To view network providers:

1. Navigate to **Networks → Providers** to see a list of all network providers, along with information such as *Name*, *Type*, *EVM Zone*, *Number of Instances*, *Subnets*, and *Region*. Click on a network provider from the list to see additional information about the network provider, and its relationship with the cloud provider, on the summary page.

2. Alternatively, click on a cloud provider to see the cloud provider details and its relationships such as *Network Manager*, *Tenants*, *Instances* among others. In Relationships, click *Network Manager* to see information about the network provider, and its relationship with the cloud provider, on the summary page.

4.2. REFRESHING NETWORK PROVIDERS

Refresh a network provider to find other resources related to it. Ensure the selected network providers have the correct credentials before refreshing.

1. Navigate to **Networks → Providers**.

2. Select the network providers to refresh.

3. Click ⚙ (**Configuration**), and then ↻ (**Refresh Relationships and Power States**).

4. Click **OK**.

4.3. TAGGING NETWORK PROVIDERS

Apply tags to network providers to categorize them together at the same time.

1. Navigate to **Networks → Providers**.

2. Select the network providers to tag.

3. Click (**Policy**), and then (**Edit Tags**).

4. **Select a customer tag to assign** from the first list.

5. Select a value to assign from the second list.

6. Click **Save**.

4.4. REMOVING NETWORK PROVIDERS

Although network providers are added or removed automatically upon adding or removing the respective cloud provider, you can manually remove a network provider if it is no longer in use. This will remove the network provider from the VMDB and any relationship with the cloud provider.

1. Navigate to **Networks → Providers**.

2. Click the network provider to remove.

3. Click (**Configuration**), and then (**Remove this Network Provider from the VMDB**).

4. Click **OK**.

4.5. VIEWING A NETWORK PROVIDER'S TIMELINE

View the timeline of events for instances registered to a network provider.

1. Navigate to **Networks → Providers**.

2. Click the network provider you want to monitor the timeline for.

3. Click (**Monitoring**), and then (**Timelines**).

4. From **Options**, select the event type, interval, customize the period of time to display and the types of events to see.

   » Select *Management Events* or *Policy Events* from the **Show** list.

   » Select an **Interval** between *Hourly* and *Daily*.

   » Select **Date**.

   » If you selected *Daily* for **Interval**, set the number of days in the past to see the event timeline for. The maximum is *31 days back*.

   » Select **Summary** or **Detail** for **Level**.

   » Select the required **Event Groups** from the lists you want to monitor the timeline for.

You can also assign policy profiles to network providers, or remove them. The method for doing so is similar to that of any normal policy profile. See Assigning Policy Profiles to a Network Provider and Removing Policy Profiles from a Network Provider in the *Policies and Profiles Guide*.

CHAPTER 5. CONTAINERS PROVIDERS

A containers provider is a service that manages container resources, and can be added to the Red Hat CloudForms appliance.

The **Compute** → **Containers** area has options to add and manage containers providers. This includes the **Providers** page, which displays all discovered or added containers providers.

Red Hat CloudForms supports adding OpenShift Enterprise as a containers provider.

5.1. OBTAINING AN OPENSHIFT ENTERPRISE MANAGEMENT TOKEN

When deploying OpenShift Enterprise using `openshift-ansible-3.0.20` (or later versions), the service account and roles required by Red Hat CloudForms are installed by default.

To obtain the token to use for the provider definition, follow the instructions below for your OpenShift Enterprise version.

5.1.1. Obtaining a Management Token in OpenShift Enterprise 3.2

Open a terminal and run the following command:

```
# oc sa get-token -n management-infra management-admin
eyJhbGciOiJSUzI1NiI...
```

This command provides the token needed to add an OpenShift Enterprise provider.

5.1.2. Obtaining a Management Token in OpenShift Enterprise 3.1

Open a terminal and perform the following:

1. To obtain the **management** service account token name, run the following command::

   ```
   # oc describe sa -n management-infra management-admin
   ...
   Tokens:   management-admin-token-0f3fh
             management-admin-token-q7a87
   ```

2. Select one of the tokens and run the following command to retrieve the full token output:

   ```
   # oc describe secret -n management-infra management-admin-token-
   0f3fh
   ...
   Data
   ====
   token:   eyJhbGciOiJSUzI1NiI...
   ```

   Replace **management-admin-token-0f3fh** with the name of your token.

This command provides the token needed to add an OpenShift Enterprise provider.

5.2. CONFIGURING OPENSHIFT METRICS

To collect the node, pod, and container metrics, you must run the OpenShift Metrics services inside your cluster. For more information, see Enabling Cluster Metrics in OpenShift Enterprise *Installation and Configuration*.

> **Note**
>
> For metrics collection to work properly, you also need to configure Red Hat CloudForms to allow for all three **Capacity & Utilization** server roles, which are available under **Configure → Configuration → Server → Server Control**. For more information on capacity and utilization collection, see Assigning the Capacity and Utilization Server Roles in the *Deployment Planning Guide*.

5.3. ADDING AN OPENSHIFT ENTERPRISE PROVIDER

After initial installation and creation of a Red Hat CloudForms environment, add an OpenShift Enterprise provider using the token obtained in Section 5.1, "Obtaining an OpenShift Enterprise Management Token" and following the procedure below.

1. Navigate to **Compute → Containers → Providers**.

2. Click ⚙ (**Configuration**), then click ⊕ (**Add a New Containers Provider**).

3. Enter a **Name** for the provider.

4. From the **Type** list, select **OpenShift Enterprise**.

5. Enter the appropriate **Zone** for the provider. By default, the zone is set to `default`.

6. Enter the **Hostname or IP address** of the provider.

   > **Important**
   >
   > The **Hostname** must use a unique fully qualified domain name.

7. Enter the **Port** of the provider. The default port is **8443**.

8. Under **Credentials**, enter the token in the **Token** field. This is the token obtained earlier in Section 5.1, "Obtaining an OpenShift Enterprise Management Token".

   » Click **Validate** to confirm that the Red Hat CloudForms can connect to the OpenShift Enterprise provider using the provided token.

9. Click **Add**.

5.4. TAGGING CONTAINERS PROVIDERS

Apply tags to all containers providers to categorize them together at the same time.

1. Navigate to **Compute → Containers → Providers**.

2. Select the checkboxes for the containers providers to tag.

3. Click ![Policy icon] (**Policy**), and then ![Edit icon] (**Edit Tags**).

4. Select a tag to assign from the drop-down menu.

5. Select a value to assign.

6. Click **Save**.

5.5. REMOVING CONTAINERS PROVIDERS

You may want to remove a containers provider from the VMDB if the provider is no longer in use.

1. Navigate to **Compute → Containers → Providers**.

2. Select the checkboxes for the containers providers to remove.

3. Click ![Configuration icon] (**Configuration**), and then ![Remove icon] (**Remove Containers Providers from the VMDB**).

4. Click **OK**.

5.6. EDITING A CONTAINERS PROVIDER

Edit information about a provider such as the name, hostname, IP address or port, and credentials.

1. Navigate to **Compute → Containers → Providers**.

2. Click the containers provider to edit.

3. Click ![Configuration icon] (**Configuration**), and then ![Edit icon] (**Edit Selected Containers Provider**).

4. Edit the **Basic Information**. This varies depending on the **Type** of provider.

> **Note**
>
> The **Type** value is unchangeable.

To use a different containers provider, create a new one.

5. Edit the **Credentials** by typing in a new **Token**.

6. Click **Validate** and wait for notification of successful validation.

7. Click **Save**.

5.7. VIEWING A CONTAINERS PROVIDER'S TIMELINE

View the timeline of events for instances registered to a containers provider.

1. Navigate to **Compute** → **Containers** → **Providers**.

2. Click the desired containers provider for viewing the timeline.

3. Click (**Monitoring**), and then (**Timelines**).

4. From **Options**, customize the period of time to display and the types of events to see.

   ⯈ Use **Show** to select regular Management Events or Policy Events.

   ⯈ Use the **Interval** dropdown to select hourly or daily data points.

   ⯈ Use **Date** to type the date for the timeline to display.

   ⯈ If you select to view a daily timeline, use **Show** to set how many days back to go. The maximum history is 31 days.

   ⯈ From the **Level** dropdown, select a **Summary** event, or a **Detail** list of events.

   ⯈ The three **Event Groups** dropdowns allow you to select different groups of events to display. Each has its own color.

To see more detail on an item in the timeline, click on it. A balloon appears with a link to the resource.

5.8. INSIGHT AND CONTROL

Red Hat CloudForms can connect to OpenShift Enterprise containers providers and manage them similarly to the way that infrastructure and cloud providers are managed. This allows you to gain control over different aspects of your environment and answer questions, such as:

⯈ How many containers exist in my environment?

⯈ Does a specific node have enough resources?

⯈ How many distinct images are used?

⯈ Which image registries are used?

When Red Hat CloudForms connects to a containers environment, it collects information on different areas of the environment:

⯈ Entities such as pods, nodes, or services.

⯈ Basic relationships between the entities, for example: Which services are serving which pods?

⯈ Advanced insight into relationships, for example: Which two different containers are using the same image?

> Additional information, such as events, projects, routes, and metrics.

You can manage policies for containers entities by adding tags. All containers entities except volumes can be tagged.

5.8.1. Cross-Providers Insight

Cross-providers insight is a feature that connects all layers of infrastructure, cloud, and containers known to Red Hat CloudForms and collects data for analysis.

It supports cross-linking all of the layers available in the following environments:

> OpenStack

> Red Hat Enterprise Virtualization

> VMware vCenter

> Amazon EC2

> Google Cloud Engine

The collected information includes all the data available in other (infrastructure or cloud) providers.

Note

For Amazon EC2 (AWS) and Google Cloud Engine (GCE) support, OpenShift must be installed using the relevant cloud provider. For more information, see the OpenShift Enterprise Installation and Configuration guide.

5.8.2. Working with the Containers Overview Page

The information on all containers providers and entities known to Red Hat CloudForms is summarized on the Containers **Overview** page. The **Overview** page provides links to other summary pages which contain further information on the containers providers and entities.
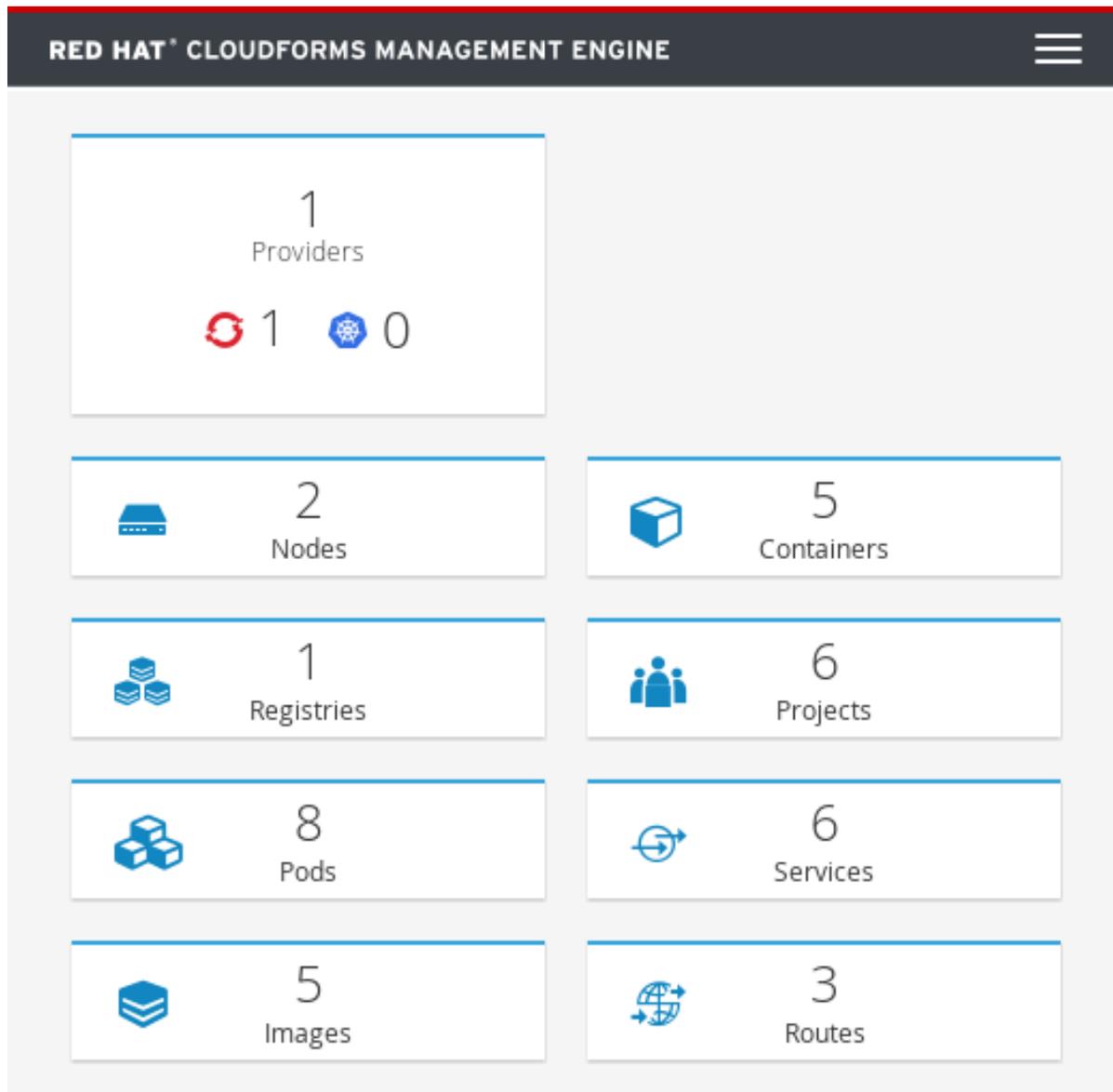
Working with the Containers Overview Page

1. Navigate to **Compute → Containers → Overview**.

2. Click the desired containers entity, or provider, if applicable, for viewing the summary with further information.

5.8.3. Viewing a Containers Provider Summary

A **Containers Provider** summary page allows you to view information on different aspects of a containers provider, for example:

» Status of the provider and its components.

» Relationships between different entities of the containers provider. These relationships are summarized in the **Relationships** box on the right-hand side of the summary page.

RED HAT® CLOUDFORMS MANAGEMENT ENGINE ≡

Relationships	
Projects	6
Routes	3
Services	6
Replicators	4
Pods	8
Containers	5
Nodes	2
Image Registries	1
Images	5

Overview	
Topology	

Smart Management	
Managed by Zone	default
My Company Tags	No My Company Tags have been assigned

※ Additional information on aggregated capacity of all CPU cores of all nodes, and aggregated capacity of all memory of all nodes.

Viewing a Containers Provider Summary

1. Navigate to **Compute** → **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

5.8.4. Viewing a Container Nodes Summary

A **Container Node** summary page allows you to view information on different aspects of a container node, for example:

※ How many entities are on a node?

※ What is the capacity and utilization?

※ What are the versions of the underlying operating system and software?

Viewing a Container Nodes Summary

1. Navigate to **Compute** → **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Nodes**.

4. Click the desired container node for viewing.

5. Alternatively, you can access the desired container node from **Compute** → **Containers** → **Container Nodes**.

5.8.4.1. Viewing a Container Nodes Timeline

You can view the timeline of events for a node. To access the timeline from a container nodes summary page, click [icon] (**Monitoring**), and then [icon] (**Timelines**).

5.8.5. Viewing a Containers Summary

A **Containers** summary page allows you to view information on different aspects of a container, for example:

> What are the relationships of the container to a related node, pod, or image?

> Which node is the container running on?

> Which part of a pod is the container?

> What is the container ID?

> What is the name of the container image? What are other properties of the container image (for example, tag)?

Viewing a Containers Summary

1. Navigate to **Compute** → **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Containers**.

4. Click the desired container for viewing.

5. Alternatively, you can access the desired container from **Compute** → **Containers** → **Containers**.

5.8.6. Viewing a Container Images Summary

A **Container Images** summary page allows you to view information on different aspects of a container image, for example:

> Which containers are using the image?

> Which image registry is the image coming from?

Viewing a Container Images Summary

1. Navigate to **Compute** → **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Images**.

4. Click the desired image for viewing.

5. Alternatively, you can access the desired image from **Compute** → **Containers** → **Container Images**.

5.8.7. Viewing an Image Registries Summary

An **Image Registries** summary page allows you to view information on different aspects of an image registry, for example:

❯ How many images are coming from the registry? What are the images?

❯ Which containers are using images from the registry?

❯ What is the host and port of the registry?

Viewing an Image Registries Summary

1. Navigate to **Compute** → **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Image Registries**.

4. Click the desired image registry for viewing.

5. Alternatively, you can access the desired image registry from **Compute** → **Containers** → **Image Registries**.

5.8.8. Viewing a Pods Summary

A **Pods** summary page allows you to view information on different aspects of a pod, for example:

❯ Which containers are part of the pod?

❯ Which services reference the pod?

❯ Which node does the pod run on?

❯ Is the pod controlled by a replicator?

❯ What is the IP address of the pod?

Viewing a Pods Summary

1. Navigate to **Compute** → **Containers** → **Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Pods**.

4. Click the desired pod for viewing.

5. Alternatively, you can access the desired pod from **Compute → Containers → Pods**.

5.8.9. Viewing a Replicators Summary

A **Replicators** summary page allows you to view information on different aspects of a replicator, for example:

≫ What is the number of requested pods?

≫ What is the number of current pods?

≫ What are the labels and selector for the replicator?

Viewing a Replicators Summary

1. Navigate to **Compute → Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Replicators**.

4. Click the desired replicator for viewing.

5. Alternatively, you can access the desired replicator from **Compute → Containers → Replicators**.

5.8.10. Viewing a Container Services Summary

A **Container Services** summary page allows you to view information on different aspects of a container service, for example:

≫ What are the pods that the container service provides traffic to?

≫ What are the port configurations for the container service?

≫ What are the labels and selector for the container service?

Viewing a Container Services Summary

1. Navigate to **Compute → Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Services**.

4. Click the desired service for viewing.

5. Alternatively, you can access the desired service from **Compute → Containers → Container Services**.

5.8.10.1. Viewing a Volumes Summary

A **Volumes** summary page allows you to view information on the persistent volumes of a container provider, for example:

≫ Which pods is the volume connected to?

≫ What are the volume's connection parameters?

≫ What is the volume's storage capacity?

≫ What are the volume's iSCSI target details (if applicable)?

Viewing a Volumes Summary

1. Navigate to **Compute** → **Containers** → **Volumes**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Volumes**.

4. Click the desired container for viewing.

5. Alternatively, you can access the desired volume from **Containers** → **Volumes**.

5.8.10.2. Viewing a Container Builds Summary

A **Container Builds** summary page allows you to view different aspects of a container build, for example:

≫ What build configuration is the container build based on?

≫ What build instances have been created?

≫ Which phase in the build process has the instance completed?

≫ Which pod does a build instance reside in?

Viewing a Container Builds Summary

1. Navigate to **Compute** → **Containers** → **Container Builds**.

2. Click the desired containers provider for viewing the provider summary.

3. In the **Relationships** box on the right-hand side of the summary page, click**Container Builds**.

4. Click the desired container for viewing.

5. Alternatively, you can access the desired container build from **Containers** → **Container Builds**.

5.8.10.3. Using the Topology Widget

The **Topology** widget is an interactive topology graph, showing the status and relationships between the different entities of the containers providers that Red Hat CloudForms has access to.

≫ The topology graph includes pods, containers, services, nodes, virtual machines, hosts, routes, and replicators within the overall containers provider environment.

≫ Each entity in the graph displays a color indication of its status.

‣ Hovering over any individual graph element will display a summary of details for the individual element.

‣ Double-click the entities in the graph to navigate to their summary pages.

‣ It is possible to drag elements to reposition the graph.

‣ Click the legend at the top of the graph to show or hide entities.

‣ Click **Display Names** on the right-hand side of the page to show or hide entity names.

Using the Topology Widget

1. Navigate to **Compute → Containers → Providers**.

2. Click the desired containers provider for viewing the provider summary.

3. On the provider summary page, click **Topology** in the **Overview** box on the right-hand side of the page.

5.8.11. Running a SmartState Analysis

Perform a SmartState Analysis of a container image to inspect the packages included in an image.

Running a SmartState Analysis

1. Navigate to **Compute → Containers → Container Images**.

2. Check the container image to analyze. You can check multiple images.

3. Click (**Configuration**), and then (**Perform SmartState Analysis**).

The container image is scanned. The process will copy over any required files for the image. After reloading the image page, all new or updated packages are listed.

To monitor the status of container image SmartState Analysis tasks, navigate to **Settings → Tasks**. The status of each task is displayed including time started, time ended, what part of the task is currently running, and any errors encountered.