



# **Red Hat CloudForms 4.6**

## **Managing Providers**

Managing your infrastructure, cloud, and containers providers



# Red Hat CloudForms 4.6 Managing Providers

---

Managing your infrastructure, cloud, and containers providers

Red Hat CloudForms Documentation Team  
[cloudforms-docs@redhat.com](mailto:cloudforms-docs@redhat.com)

## Legal Notice

Copyright © 2018 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Abstract

This guide covers managing your infrastructure, cloud, and containers providers and system managers 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

<b>PREFACE</b>	<b>5</b>
<b>CHAPTER 1. INFRASTRUCTURE PROVIDERS</b>	<b>6</b>
1.1. DISCOVERING INFRASTRUCTURE PROVIDERS	6
1.2. DISCOVERING PHYSICAL INFRASTRUCTURE PROVIDERS	7
1.3. RED HAT VIRTUALIZATION PROVIDERS	7
1.3.1. Enabling Red Hat Virtualization Capacity and Utilization Data Collection	7
1.3.2. Adding a Red Hat Virtualization Provider	8
1.3.3. Authenticating Red Hat Virtualization Hosts	9
1.4. OPENSTACK INFRASTRUCTURE PROVIDERS	10
1.4.1. Adding an OpenStack Infrastructure Provider	10
1.4.1.1. Configuring the Undercloud to Store Events	12
1.5. VMWARE VCENTER PROVIDERS	12
1.5.1. Adding a VMware vCenter Provider	12
1.5.1.1. Using a Non-Administrator Account for vCenter Hosts	13
1.5.2. Authenticating VMware vCenter Hosts	14
1.6. MICROSOFT SCVMM PROVIDERS	15
1.6.1. Authenticating to Microsoft SCVMM	15
1.6.2. Adding a Microsoft SCVMM Provider	15
1.7. REFRESHING PROVIDERS	16
1.8. TAGGING MULTIPLE PROVIDERS	17
1.9. VIEWING A PROVIDER	17
1.10. REMOVING A PROVIDER	19
1.11. VIEWING THE PROVIDER TIMELINE	19
1.12. VIEWING HOSTS AND CLUSTERS	20
1.13. VIEWING VIRTUAL MACHINES AND TEMPLATES	21
<b>CHAPTER 2. CONFIGURATION MANAGEMENT PROVIDERS</b>	<b>22</b>
2.1. RED HAT SATELLITE 6	22
2.1.1. Defining the Workflow	22
2.1.2. Defining the Hostgroup Hierarchy	22
2.1.3. Adding a Satellite 6 Provider	22
2.1.4. Triggering a Refresh of a Satellite 6 Provider	23
2.1.5. Displaying Red Hat Satellite 6 Contents	23
2.1.6. Reprovisioning a Bare Metal Host	23
2.1.7. Tagging a Bare Metal Host	25
<b>CHAPTER 3. AUTOMATION MANAGEMENT PROVIDERS</b>	<b>26</b>
3.1. ANSIBLE	26
3.1.1. Enabling the Embedded Ansible Server Role	26
3.1.2. Verifying the Embedded Ansible Worker State	27
3.1.3. Adding a Playbook Repository	27
3.1.4. Refreshing Repositories	27
3.1.5. Credentials	28
3.1.5.1. Adding Credentials	28
3.1.5.2. Credential Types	28
3.1.5.2.1. Machine	28
3.1.5.2.2. Network	29
3.1.5.2.3. SCM	29
3.1.5.2.4. Amazon	30
3.1.5.2.5. Azure Classic (deprecated)	30
3.1.5.2.6. Azure	30

3.1.5.2.7. Google Compute Engine	30
3.1.5.2.8. OpenStack	31
3.1.5.2.9. Rackspace	31
3.1.5.2.10. Red Hat Virtualization	31
3.1.5.2.11. Satellite 6	31
3.1.5.2.12. VMware	32
3.1.6. Optimizing Ansible Playbooks for Red Hat CloudForms	32
3.1.6.1. Installing Roles on an Embedded Ansible Appliance	32
3.1.6.2. Ansible Service Linking	33
3.1.6.2.1. Example: Linking a virtual machine to a service	33
3.1.6.3. Modifying the Automate Workspace Using the manageiq-automate Role.	34
3.1.6.3.1. Role Variables	34
3.1.6.3.2. Example Playbook	34
3.1.6.4. Callbacks in Multiple Appliance Environments	35
3.2. ANSIBLE TOWER	35
3.2.1. Adding an Ansible Tower Provider	36
3.2.2. Refreshing an Ansible Tower Provider	37
3.2.3. Viewing Ansible Tower Providers and Inventory	38
3.2.4. Viewing Ansible Tower Configured Systems	38
3.2.5. Executing an Ansible Tower Job Template from a Service Catalog	38
3.2.6. Executing an Ansible Tower Job Using a Custom Automate Button	40
<b>CHAPTER 4. CLOUD PROVIDERS</b>	<b>44</b>
4.1. OPENSTACK PROVIDERS	44
4.1.1. Adding OpenStack Providers	44
4.1.1.1. Configuring the Overcloud to Store Events	47
4.2. AZURE PROVIDERS	48
4.2.1. Adding Azure Providers	48
4.2.2. Discovering Azure Providers	50
4.2.3. Disabling Azure Cloud Regions	50
4.3. AMAZON EC2 PROVIDERS	50
4.3.1. Permissions for Amazon EC2 Providers	51
4.3.1.1. Manually Creating an Amazon EC2 Role	51
4.3.2. Adding Amazon EC2 Providers	51
4.3.3. Discovering Amazon EC2 Cloud Providers	52
4.3.4. Enabling Public AMIs from Amazon EC2	52
4.3.5. Enabling AWS Config Notifications	53
4.3.6. Enabling Amazon EC2 Events	54
4.3.6.1. Creating a CloudTrail	54
4.3.6.2. Creating CloudWatch Rules Based on Event Patterns	54
4.3.7. Disabling Amazon Cloud Regions	56
4.4. GOOGLE COMPUTE ENGINE PROVIDERS	57
4.4.1. Adding Google Compute Engine Providers	57
4.4.2. Enabling Google Compute Engine Events	58
4.4.2.1. Configuring Google Compute Engine to Export Events	59
4.4.2.2. Viewing Google Compute Engine Events in Red Hat CloudForms	60
4.5. REFRESHING CLOUD PROVIDERS	61
4.6. TAGGING CLOUD PROVIDERS	61
4.7. REMOVING CLOUD PROVIDERS	61
4.8. EDITING A CLOUD PROVIDER	62
4.9. VIEWING A CLOUD PROVIDER'S TIMELINE	62
<b>CHAPTER 5. NETWORK MANAGERS</b>	<b>64</b>

5.1. ADDING OR VIEWING NETWORK PROVIDERS	64
5.2. REFRESHING NETWORK PROVIDERS	64
5.3. TAGGING NETWORK PROVIDERS	65
5.4. REMOVING NETWORK PROVIDERS	65
5.5. VIEWING A NETWORK PROVIDER'S TIMELINE	65
5.6. USING THE TOPOLOGY WIDGET FOR NETWORK PROVIDERS	66
<b>CHAPTER 6. MIDDLEWARE MANAGEMENT PROVIDERS</b>	<b>68</b>
6.1. ADDING A MIDDLEWARE PROVIDER	68
<b>CHAPTER 7. CONTAINERS PROVIDERS</b>	<b>70</b>
7.1. OBTAINING AN OPENSIFT CONTAINER PLATFORM MANAGEMENT TOKEN	71
7.2. ENABLING OPENSIFT CLUSTER METRICS	71
7.3. ADDING AN OPENSIFT CONTAINER PLATFORM PROVIDER	71
7.4. TAGGING CONTAINERS PROVIDERS	74
7.5. REMOVING CONTAINERS PROVIDERS	75
7.6. PAUSING / RESUMING CONTAINERS PROVIDERS	75
7.7. EDITING A CONTAINERS PROVIDER	76
7.8. HIDING ENVIRONMENT VARIABLES FOR CONTAINERS PROVIDERS	78
7.9. VIEWING A CONTAINERS PROVIDER'S TIMELINE	79
<b>CHAPTER 8. STORAGE MANAGERS</b>	<b>81</b>
8.1. AMAZON ELASTIC BLOCK STORE MANAGERS	81
8.2. OPENSTACK BLOCK STORAGE MANAGERS	81
8.3. OPENSTACK OBJECT STORAGE MANAGERS	81
8.3.1. Viewing Object Stores	82
<b>CHAPTER 9. CROSS-PROVIDERS INSIGHT</b>	<b>83</b>
<b>APPENDIX A. APPENDIX</b>	<b>84</b>
A.1. USING A SELF-SIGNED CA CERTIFICATE	84





## PREFACE

Red Hat CloudForms can manage a variety of external environments, known as providers and managers. A provider or manager is any system that CloudForms integrates with for the purpose of collecting data and performing operations.

In CloudForms, a *provider* is an external virtualization, cloud, or containers environment that manages multiple virtual machines or instances residing on multiple hosts. One example is Red Hat Virtualization, a platform that manages multiple hosts and virtual machines.

In CloudForms, a *manager* is an external management environment that manages more than one type of resource. One example of a manager is OpenStack, which manages infrastructure, cloud, network, and storage resources.

This guide covers working with providers and managers in CloudForms, which include:

- Infrastructure providers
- Configuration management providers
- Automation management providers
- Cloud providers
- Networking management providers
- Middleware management providers
- Container providers
- Storage managers

For information on working with the resources contained by a provider or manager, see [Managing Infrastructure and Inventory](#).

## CHAPTER 1. INFRASTRUCTURE PROVIDERS




In Red Hat CloudForms, an infrastructure provider is a virtual infrastructure environment that you can add to a 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 CloudForms, and how to manage them. Infrastructure providers can be either discovered automatically by CloudForms, or added individually.

The web interface uses virtual thumbnails to represent infrastructure 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

**Table 1.1. Provider 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. DISCOVERING PHYSICAL INFRASTRUCTURE PROVIDERS

In addition to discovering virtual infrastructure providers, CloudForms now has the ability to discover physical infrastructure providers in a given subnet range.

1. Navigate to **Compute** → **Physical Infrastructure** → **Providers**.
2. Click  (**Configuration**), then click  (**Discover Physical Infrastructure Providers**).
3. Select the provider in **Discovery Type**.
4. Enter a **Subnet Range** of IP addresses starting with a **From Address** and ending with a **To Address**.
5. Enter a **Port**.
6. Click **Start**.

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

## 1.3. RED HAT VIRTUALIZATION PROVIDERS

To use a Red Hat Virtualization provider, add it to the appliance and authenticate its hosts. You can also configure capacity and utilization data collection to help track usage and find common issues.

### 1.3.1. Enabling Red Hat Virtualization Capacity and Utilization Data Collection



Configure the following to collect capacity and utilization data from a Red Hat Virtualization provider:

- In CloudForms, enable the capacity and utilization server roles from the settings menu, in **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*.
- For information on selecting clusters and datastores used to collect data, see [Capacity and Utilization Collections](#) in the *General Configuration Guide*.
- In your Red Hat Virtualization environment, install the Data Warehouse and Reports components, and create a Red Hat CloudForms user in the Data Warehouse database:
  - To install the Data Warehouse and Reports components in a Red Hat Virtualization environment, see the [Data Warehouse Guide](#).

- To create a CloudForms user in the Data Warehouse database, see [Data Collection for Red Hat Enterprise Virtualization](#) in the *Deployment Planning Guide*.

### 1.3.2. Adding a Red Hat Virtualization Provider

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

1. Navigate to **Compute** → **Infrastructure** → **Providers**.
2. Click  (**Configuration**), then click  (**Add a New Infrastructure Provider**).
3. Enter a **Name** for the provider.
4. Select **Red Hat Virtualization** from the **Type** list.
5. Select the appropriate **Zone** for the provider. If you do not specify a zone, it is set to **default**.
6. Under **Endpoints** in the **Default** tab, configure the following:

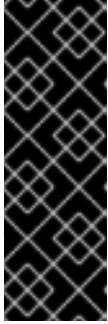
- Enter the **Hostname** or IPv4 or IPv6 address of the Red Hat Virtualization Manager.



#### IMPORTANT

The **Hostname** must be a unique fully qualified domain name.

- Enter the **API Port** if your provider uses a non-standard port for access.
  - Select **Yes** or **No** to **Verify TLS Certificates** to specify whether to authenticate securely to the provider using TLS.
    - If you select **Yes** for **Verify TLS Certificates**, you can either paste a custom certificate in the **Trusted CA Certificates** field in PEM format, or leave the **Trusted CA Certificates** field empty if your Red Hat Virtualization provider has a trusted Certificate Authority.
  - Provide the login credentials for the Red Hat Virtualization administrative user:
    - Enter the user name (formatted as **admin@internal1**) in the **Username** field.
    - Enter the password in the **Password** field.
    - Confirm the password in the **Confirm Password** field.
    - Click **Validate** to confirm CloudForms can connect to the Red Hat Virtualization Manager.
7. Under **Endpoints** in the **C & U Database** tab, you can configure capacity and utilization metrics collection by providing login credentials for the CloudForms user of the Red Hat Virtualization Data Warehouse database. You can also configure this later by editing the provider. Configure the following in the **C & U Database** tab:





## IMPORTANT

To collect capacity and utilization data from a Red Hat Virtualization provider, the capacity and utilization server roles must be enabled in CloudForms. The Red Hat Virtualization environment must also contain the Data Warehouse and Reports components and a CloudForms user. Specific clusters, hosts, and datastores can also be configured for collection. See [Section 1.3.1, “Enabling Red Hat Virtualization Capacity and Utilization Data Collection”](#) for configuration details.

- Enter the database hostname or IPv4 or IPv6 address in **Hostname**.
  - Enter the **API Port** if your provider uses a non-standard port for access.
  - Enter the **Database Name**.
  - 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 CloudForms can connect to the database.
8. Click **Add** to finish adding the Red Hat Virtualization provider.

### 1.3.3. Authenticating Red Hat Virtualization Hosts

After adding a Red Hat 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 Virtualization.
  - 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**.

## 1.4. OPENSTACK INFRASTRUCTURE PROVIDERS

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



### 1.4.1. 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 1.4.1.1, “Configuring the Undercloud to Store Events”](#) for instructions. For more information, see [OpenStack Telemetry \(ceilometer\)](#) in the Red Hat OpenStack Platform *Architecture Guide*.
- To authenticate the provider using a self-signed Certificate Authority (CA), configure the CloudForms appliance to trust the certificate using the steps in [Section A.1, “Using a Self-Signed CA Certificate”](#) before adding the provider.

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**.

**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*.
- The provider you are creating will be able to see projects for the given domain only. To see projects for other domains, add it as another cloud provider. For more information on domain management in OpenStack, see [Domain Management](#) in the Red Hat OpenStack Platform *Users and Identity Management 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. Select a **Security Protocol** method to specify how to authenticate the provider:
    - **SSL without validation**: Authenticate the provider insecurely using SSL.
    - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option. This is the recommended authentication method.
    - **Non-SSL**: Connect to the provider insecurely using only HTTP protocol, without SSL.
  - b. 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)
  - c. In **API Port**, set the public port used by the OpenStack Keystone service. By default, OpenStack uses port 5000 for this.
  - d. Select the appropriate **Security Protocol** used for authenticating with your OpenStack provider.
  - e. 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.
  - f. 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 1.4.1.1, “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.

#### 1.4.1.1. 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. See [Installing the Undercloud](#) and [Configuring the Director](#) in Red Hat OpenStack Platform *Director Installation and Usage* for related details.

## 1.5. VMWARE VCENTER PROVIDERS

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

### 1.5.1. Adding a VMware vCenter Provider

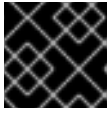
After initial installation and creation of a Red Hat CloudForms environment, add a VMware vCenter provider to the appliance.

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**.

#### 1.5.1.1. Using a Non-Administrator Account for vCenter Hosts

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 created for Red Hat CloudForms. See the [VMware documentation](#) for instructions on how to create a role.

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

Check the entire set of privileges for the following groups:

- 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.

### 1.5.2. 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**.

## 1.6. MICROSOFT SCVMM PROVIDERS

To use a Microsoft System Center Virtual Machine Manager (SCVMM) 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.

### 1.6.1. Authenticating to Microsoft SCVMM

Before you can add a Microsoft SCVMM provider 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.

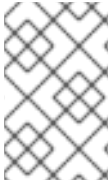
```
Set-ExecutionPolicy RemoteSigned
```

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.



### 1.6.2. Adding a Microsoft SCVMM Provider

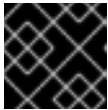
After initial installation and creation of a Red Hat CloudForms environment, add a Microsoft System Center Virtual Machine Manager (SCVMM) provider to the appliance.



## NOTE

To authenticate the provider using a self-signed Certificate Authority (CA), configure the CloudForms appliance to trust the certificate using the steps in [Section A.1, “Using a Self-Signed CA Certificate”](#) before adding the provider.

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 password 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**.

## 1.7. 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**.

## 1.8. 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.



Select a customer tag to assign: Environment *			<Select a value to assign>
	Category	Assigned Value	
	Cost Center *	Cost Center 001	
	Environment *	Quality Assurance	

\* Only a single value can be assigned from these categories

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

## 1.9. 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.

There are two methods of viewing an infrastructure provider's details: the summary screen (default) and the dashboard screen. Use the summary  and dashboard  buttons to toggle between views.

Both the summary and dashboard screens contain a taskbar with **Reload**, **Configuration**, **Policy**, **Monitoring**, and **Authentication** buttons to manage the selected provider.

### Provider Summary Screen

Infrastructure Providers > ECS (Summary)

### ECS (Summary)

Properties	
Host Name	10.64.14.120
Discovered IP Address	
Type	Red Hat Enterprise Virtualization Manager
API Port	443
Aggregate Host CPU Resources	76.6 GHz
Aggregate Host Memory	94 GB
Aggregate Host CPUs	8
Aggregate Host CPU Cores	32
Management Engine GUID	a1e09036-9fd4-11e6-8dfd-001a4a81da03

Status	
Default Credentials	Valid
Last Refresh	Success - About 1 Hour Ago

Relationships	
Hosts & Clusters	Available
VMs & Templates	Available
Clusters	1
Hosts	4
Datastores	3
VMs and Instances	69
Templates	13

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

The provider summary screen displays information about the provider in table format.

- Provider accordion: Displays details about the provider's **Properties** and **Relationships** on the sidebar. Click to expand these lists.
- Provider summary: Displays a provider's **Properties**, **Status**, **Relationships**, and **Smart Management**. Click on an item in the **Relationships** table to see more information about that entity.

## Provider Dashboard Screen

Infrastructure Providers > VMware v5.1 (Dashboard)

2 Clusters
 2 Hosts
 2 Datastores
 74 VMs
 8 Templates

#### Global Utilization

##### CPU

No data available

Last 30 Days

##### Memory

No data available

Last 30 Days

#### Cluster Utilization

##### CPU

No data available

Last 30 Days

##### Memory

No data available

Last 30 Days

#### Recent Hosts

Last 30 Days

Hosts

#### Recent VMs


Last 30 Days


VMs

From the dashboard, you can view:

- Number of clusters, hosts, virtual machines, templates, datastores, resource pools, and other entities on the provider. Click on an entity to see more information about that item.
- Aggregate utilization for CPU, memory, and storage
- Network I/O statistics
- Trends for hosts and virtual machines discovered

To view the dashboard:



1. Navigate to **Compute** → **Infrastructure** → **Providers**.
2. Click the infrastructure provider to view.
3. To access the dashboard view, click  (**Dashboard view**).

To return to the summary view, click  (**Summary view**).

## 1.10. 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**).

## 1.11. 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.

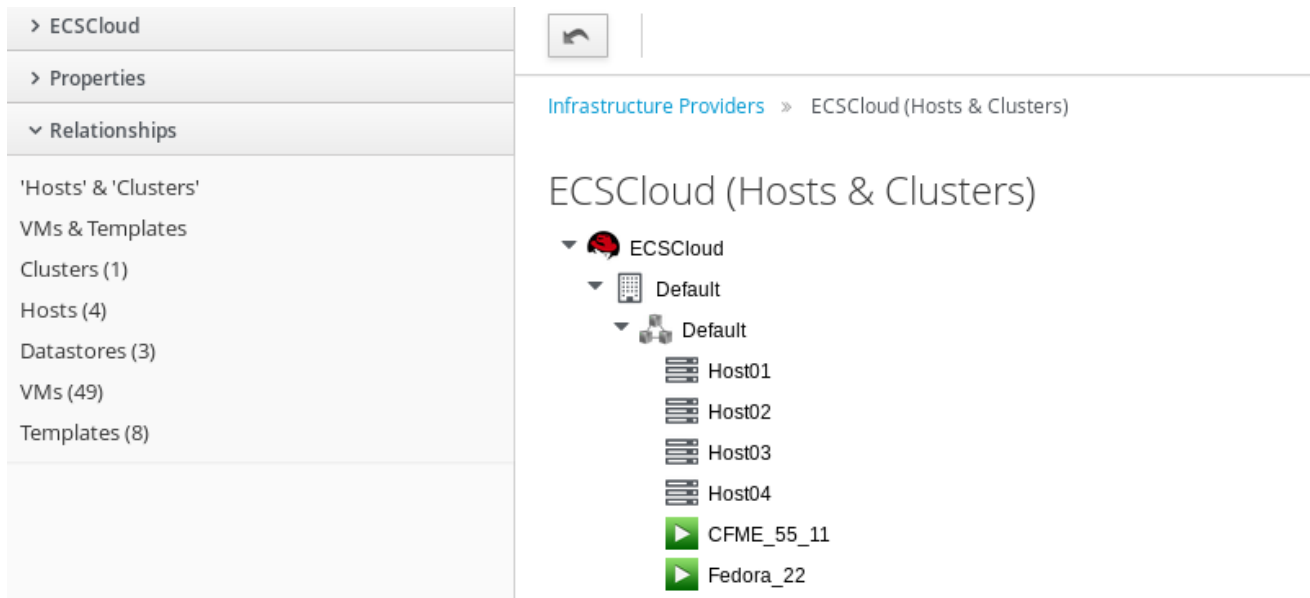
- Use **Show** to select regular Management Events or Policy Events.
- Use the **Interval** dropdown to select hourly or daily data points.
- Use **Date** to type the date for the timeline to display.
- If you select to view a daily timeline, use **Show** to set how many days back to go. The maximum 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.

## 1.12. 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**.





## 1.13. 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

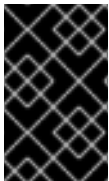
In CloudForms, a configuration management provider is a systems management product that you can add to a CloudForms appliance to manage the lifecycle of your resources. Configuration management providers are useful for uniformly applying changes and updates across providers, and for recording and reporting status and change activity. They can also help eliminate the confusion and error brought about by the existence of different providers.

This chapter describes the different types of configuration management providers available to CloudForms, and how to manage them. Configuration management providers must be added individually to CloudForms.

### 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 Satellite 6 provider added to Red Hat CloudForms.

1. Navigate to **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** → **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.

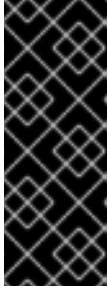
Change between these two views using the accordion menu on the left of the user interface.

#### 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** → **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** → **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.

## CHAPTER 3. AUTOMATION MANAGEMENT PROVIDERS

In Red Hat CloudForms, an automation management provider is a management tool that integrates with CloudForms to simplify automation operations for your resources. This chapter describes the automation management providers that you can use with Red Hat CloudForms, and how to work with them.

Red Hat CloudForms provides automation management features through the following:

**Automate** enables real-time, bi-directional process integration. This provides you with a method to implement adaptive automation for management events and administrative or operational activities.

**Ansible** integration delivers out-of-the-box support for backing service, alert and policy actions using Ansible playbooks. Sync your existing playbook repositories with CloudForms, add credentials to access providers, and create service catalog items for actions ranging from creating and retiring VMs, updating security software, or adding additional disks when space runs low.

**Ansible Tower** is a management tool integrated with CloudForms, designed to help automate infrastructure operations utilizing existing Ansible Tower providers in your inventory. CloudForms allows you to execute Ansible Tower jobs using service catalogs and Automate. 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.

### 3.1. ANSIBLE

Ansible integrates with Red Hat CloudForms to provide automation solutions, using playbooks, for Service, Policy and Alert actions. Ansible playbooks consist of series of *plays* or tasks that define automation across a set of hosts, known as the inventory.

Ranging from simple to complex tasks, Ansible playbooks can support cloud management:

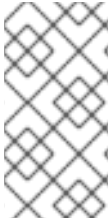
- **Services** - allow a playbook to back a CloudForms service catalog item.
- **Control Actions** - CloudForms policies can execute playbooks as actions based on events from providers.
- **Control Alerts** - set a playbook to launch prompted by a CloudForms alert.

Ansible is built into CloudForms so there is nothing to install. The basic workflow when using Ansible in Red Hat CloudForms is as follows:

1. Enable the **Embedded Ansible** server role.
2. Add a source control repository that contains your playbooks.
3. Establish credentials with your inventory.
4. Back your services, alerts and policies using available playbooks.

#### 3.1.1. Enabling the Embedded Ansible Server Role

In Red Hat CloudForms, the **Embedded Ansible** role is disabled by default. Enable this server role to utilize Ansible Automation Inside.

**NOTE**

Configure your CloudForms appliance network identity (hostname/IP address) before enabling the Embedded Ansible server role. Restart the **evmservd** service on the appliance with the enabled Embedded Ansible server role after making any changes to the hostname or IP address.

1. Navigate to the settings menu, then **Configuration** → **Settings**.
2. Select the desired server under **Zones**.
3. Set the **Server Role** for **Embedded Ansible** to **On**.

### 3.1.2. Verifying the Embedded Ansible Worker State

Verify that the Embedded Ansible worker has started to utilize its features.

1. Navigate to the settings menu, then **Configuration** → **Diagnostics** and click on the desired server.
2. Click on the **Workers** tab.

A table of all workers and current status will appear from which you can confirm the state of your embedded Ansible worker.

### 3.1.3. Adding a Playbook Repository

Add a repository so that Red Hat CloudForms can discover and make available your playbooks.



1. Navigate to **Automation** → **Ansible** → **Repositories**.
2. Click **Add**.
3. Provide a Repository Name in the **Name** field.
4. Add a description for the repository in the **Description** field.
5. Select an **SCM Type** from the drop-down menu.
6. Add a **URL** or IP Address for the repository.
7. Select the appropriate **SCM Credentials** from the drop-down menu.
8. Provide a branch name in the **SCM Branch** field.
9. Check the appropriate box for any **SCM Update Options**.
10. Click **Add**.

Once you have synced a repository, its playbooks will become available to CloudForms.



### 3.1.4. Refreshing Repositories

Red Hat CloudForms allows you to refresh a targeted playbook repository or all repositories in your inventory to ensure your playbooks are current.

Refresh a targeted repository:

1. Navigate to **Automation** → **Ansible** → **Repositories**.
2. Click on a repository.
3. Click  (**Configuration**), then  (**Refresh this Repository**).

Alternately, you can refresh some or all repositories from the list view:

1. Navigate to **Automation** → **Ansible** → **Repositories**.
2. Check those repositories to refresh. Click **Check All** to select all repositories.
3. Click  (**Configuration**), then  (**Refresh Selected Ansible Repositories**).

### 3.1.5. Credentials

Credentials are utilized by Red Hat CloudForms for authentication when running Ansible playbooks against machines, synchronizing with inventory sources, and importing project content from a version control system.



#### 3.1.5.1. Adding Credentials

Red Hat CloudForms can store credentials used by playbooks. Credentials saved in CloudForms are matched and executed with a playbook when run.



#### IMPORTANT

If both CloudForms and a VMware provider are located in the same IPv6-only network, use a DNS-resolvable hostname for the VMware provider in the **vCenter Host** field when adding credentials.

1. Navigate to **Automation** → **Ansible** → **Credentials**.
2. Click  (**Configuration**), then  (**Add a New Credential**).
3. Provide a **Name** for the credential.
4. Select the **Credential Type**. Additional fields will appear depending on the type chosen.
5. Click **Add**.

#### 3.1.5.2. Credential Types

Each credential type used by CloudForms is detailed in the following sections.

##### 3.1.5.2.1. Machine

Machine credentials enable CloudForms to invoke Ansible on hosts under your management. Just like using Ansible on the command line, you can specify the SSH username, optionally provide a password, an SSH key, or a key password. They define SSH and user-level privilege escalation access for playbooks, and are used when running playbooks on a remote host.



- **Username:** The username to be used for SSH authentication.
- **Password:** The actual password to be used for SSH authentication.
- **SSH Private Key:** Copy or drag-and-drop the SSH private key for the machine credential.
- **Private Key Passphrase:** If the SSH Private Key used is protected by a password, you can configure a Key Password for the private key.
- **Privilege Escalation:** Specifies the type of escalation privilege to assign to specific users. Options include **sudo**, **su**, **pbrun**, **pfexec**.
- **Privilege Escalation Username:** Enter the username to use with escalation privileges on the remote system.
- **Privilege Escalation Password:** Enter the actual password to be used to authenticate the user via the selected privilege escalation type on the remote system.
- **Vault Password:** Ansible Vault credentials have only the **Vault Password** attribute that may be configured.



#### NOTE

For more information on Ansible Vault, see [Using Vault in playbooks](#).

#### 3.1.5.2.2. Network

Network credentials are used by Ansible networking modules to connect to and manage networking devices.

Network credentials have several attributes that may be configured:

- **Username:** The username to use in conjunction with the network device.
- **Password:** The password to use in conjunction with the network device.
- **Authorize:** Select this from the Options field to add an Authorize password which signs the RSA key with a password.
- **Authorize password:** If **Authorize** is checked, enter a password in the **Authorize Password** field.
- **SSH Key:** Copy or drag-and-drop the actual SSH Private Key to be used to authenticate the user to the network via SSH.
- **Private key passphrase:** The actual passphrase for the private key to be used to authenticate the user to the network via SSH.

#### 3.1.5.2.3. SCM

SCM (source control) credentials are used with Projects to clone and update local source code repositories from a remote revision control system such as Git, Subversion, or Mercurial.

Source Control credentials have several attributes that may be configured:

- **Username:** The username to use in conjunction with the source control system.

- **Password:** The password to use in conjunction with the source control system.
- **Private key passphrase:** If the SSH private key used is protected by a passphrase, you may configure a key passphrase for the private key.
- **Private Key:** Copy or drag-and-drop the actual SSH Private Key to be used to authenticate the user to the source control system via SSH.

#### 3.1.5.2.4. Amazon

Selecting this credential type enables synchronization of cloud inventory with Amazon Web Services.

- **Access Key:** User credentials that allow for programmatic calls to Amazon Web Services.
- **Secret Key:** The secret key that corresponds to the user access key.
- **STS Token:** Token generated by Amazon Web Services Security Token Service.

#### 3.1.5.2.5. Azure Classic (deprecated)

Selecting this credential type enables synchronization of cloud inventory with Microsoft Windows Azure Classic.

Microsoft Azure credentials have several attributes to configure:

- **Subscription ID:** The Subscription UUID for the Microsoft Azure Classic account.
- **Management Certificate:** The PEM file that corresponds to the certificate you uploaded in the Microsoft Azure Classic console.

#### 3.1.5.2.6. Azure

Selecting this credential type enables synchronization of cloud inventory with Microsoft Azure.

Microsoft Azure credentials have several attributes to configure:

- **Username:** The username to use to connect to the Microsoft Azure account.
- **Password:** The password to use to connect to the Microsoft Azure account.
- **Subscription ID:** The Subscription UUID for the Microsoft Azure account.
- **Tenant ID:** The Tenant ID for the Microsoft Azure account.
- **Client Secret:** The Client Secret for the Microsoft Azure account.
- **Client ID:** The Client ID for the Microsoft Azure account.

#### 3.1.5.2.7. Google Compute Engine

Selecting this credential type enables synchronization of cloud inventory with Google Compute Engine.

Google Compute Engine credentials have several attributes that may be configured:

- **Service Account Email Address:** The email address assigned to the Google Compute Engine service account.

- **RSA Private Key:** The PEM file associated with the service account email.
- **Project:** The GCE assigned identification. It is constructed as two words followed by a three digit number, such as: squeamish-ossifrage-123.

#### 3.1.5.2.8. OpenStack

Selecting this credential type enables synchronization of cloud inventory with Red Hat OpenStack Platform.

OpenStack credentials have several attributes that may be configured:

- **Username:** The username to use to connect to OpenStack.
- **Password (API Key):** The password or API key to use to connect to OpenStack.
- **Host (Authentication URL):** The host to be used for authentication.
- **Project (Tenant Name):** The Tenant name or Tenant ID used for OpenStack. This value is usually the same as the username.
- **Domain name:** The FQDN to be used to connect to OpenStack.

#### 3.1.5.2.9. Rackspace

Selecting this credential type enables synchronization of cloud inventory with Rackspace.

Rackspace credentials have the following attributes that may be configured:

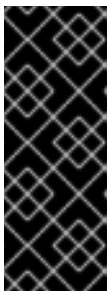
- **Username:** The username to use to connect to vCenter.
- **API Key:** The public key related to the administrator ID.

#### 3.1.5.2.10. Red Hat Virtualization

Selecting this credential type enables synchronization of cloud inventory with Red Hat Virtualization.

Red Hat Virtualization credentials have several attributes that may be configured:

- **Username:** The username to use to connect to Red Hat Virtualization.
- **Password:** The password to use to connect to Red Hat Virtualization.
- **Host (Authentication URL):** The host to be used for authentication.



#### IMPORTANT

- Enter in **Host** the Red Hat Virtualization provider URL, followed by the path **/ovirt\_engine/api**. Example:  
[https://your.rhv.com/ovirt\\_engine/api](https://your.rhv.com/ovirt_engine/api)
- See [Ansible Roles](#) for more information on Ansible Roles available for Red Hat Virtualization.

#### 3.1.5.2.11. Satellite 6

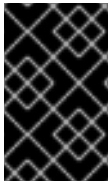
Selecting this credential type enables synchronization of cloud inventory with Red Hat Satellite 6.

Satellite credentials have several attributes that may be configured:

- **Username:** The username to use to connect to Satellite 6.
- **Password:** The password to use to connect to Satellite 6.
- **Satellite 6 Host:** The Satellite 6 URL or IP address to connect to.

#### 3.1.5.2.12. VMware

Selecting this credential type enables synchronization of inventory with VMware vCenter.

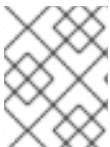


#### IMPORTANT

If both CloudForms and a VMware provider are located in the same IPv6-only network, use a DNS-resolvable hostname for the VMware provider in the **vCenter Host** field when adding credentials.

VMware credentials have several attributes that may be configured:

- **Username:** The username to use to connect to vCenter.
- **Password:** The password to use to connect to vCenter.
- **vCenter Host:** The vCenter hostname or IP address to connect to.



#### NOTE

If the VMware guest tools are not running on the instance, VMware inventory sync may not return an IP address for that instance.

### 3.1.6. Optimizing Ansible Playbooks for Red Hat CloudForms

Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. When designing playbooks for use with CloudForms it is helpful to utilize solutions within the playbook itself to ensure optimal implementation of playbook-backed services or automated processes.

This section is intended to complement the existing documentation on Ansible playbooks and guide administrators through optimizing playbooks for use with CloudForms.

#### 3.1.6.1. Installing Roles on an Embedded Ansible Appliance

Roles are ways of automatically loading certain variable files, tasks, and handlers based on a known file structure. Grouping content by roles also allows easy sharing of roles with other users. Install roles on a Red Hat CloudForms appliance with the Embedded Ansible server role activated to optimize playbooks.

When using this role in a playbook on a CloudForms appliance, add an empty **roles** directory at the root of the playbook. In the **roles** directory, include a **requirements.yml** file with the following contents:

```
---
- src: <ansible-galaxy-role>
```

CloudForms will automatically install the role once it sees the **requirements.yml** file in the playbook.

### 3.1.6.2. Ansible Service Linking

Red Hat CloudForms provides a module allowing inventoried resources such as virtual machines created using Ansible playbooks to link back to the services used to generate them. During service ordering of a playbook the **add\_provider\_vms** module will allow the playbook to connect back to the worker appliance and identify the provider resources it was responsible for generating. Once linked, the newly generated resources are available to CloudForms's life cycle management features.

Linking VMs back to the service that created it requires implementing the following tasks in the playbook used for provisioning:

1. Create a resource and register it.
2. Link the service using the **add\_provider\_vms** method to the newly created resource.

#### 3.1.6.2.1. Example: Linking a virtual machine to a service

In the following playbook task examples, a virtual machine is deployed to Amazon EC2 and linked back to the service. Examples are provided for linking the resource to its service by both an *href slug* and as an object.



#### NOTE

- This example utilizes the ``syncrou.manageiq-vmdb`` role. This role allows CloudForms users to modify and/or change VMDB objects using an Ansible playbook. For information on implementing and utilizing roles when writing Ansible playbooks for CloudForms, see [Section 3.1.6.1, “Installing Roles on an Embedded Ansible Appliance”](#).
- For more information on Ansible Galaxy and roles, see the [Ansible Galaxy documentation](#).
- Note the provider ID in order to successfully link to the service.

1. Create and register the resource.

```
- name: Create Ec2 Instance
  ec2:
    key_name: "{{ key }}"
    instance_tags: {Name: "{{ name }}" }
    group_id: "{{ security_group }}"
    instance_type: "{{ instance_type }}"
    region: "{{ region }}"
    image: "{{ image }}"
    wait: yes
    count: 1
    vpc_subnet_id: "{{ subnet }}"
    assign_public_ip: yes
  register: ec2
```

2. Call the **add\_provider\_vms** method as an action to link to the service via an *href slug* or an object.

■

```

- name: Service Linking via an href slug
  manageiq_vmdb:
    href: "href_slug::services/80"
    action: add_provider_vms
    data:
      uid_ems:
        - "{{ ec2.instances[0].id }}"
      provider:
        id: 24

- name: Service Linking via an object
  manageiq_vmdb:
    vmdb: "{{ vmdb_object }}"
    action: add_provider_vms
    data:
      uid_ems:
        - "{{ ec2.instances[0].id }}"
      provider:
        id: 24

```

### 3.1.6.3. Modifying the Automate Workspace Using the `manageiq-automate` Role.

The **manageiq-automate** role allows users of Red Hat CloudForms Automate to modify and add to the automate workspace via an Ansible playbook.

#### NOTE

When using this role in a playbook on a Red Hat CloudForms appliance with Embedded Ansible activated, add an empty **roles** directory at the root of the playbook. In the **roles** directory, include a **requirements.yml** file with the following contents:

```

---
- src: syncrou.manageiq-automate

```

CloudForms will automatically install the role once it sees the **requirements.yml** file in the playbook.

#### 3.1.6.3.1. Role Variables

The **manageiq\_automate** role employs the following variables when implemented in a playbook run on a CloudForms appliance. Variables are defined in **defaults/main.yml** and **vars/main.yml**.

*auto\_commit*: By default is set to **True**. If set to **False** it will not auto commit back to CloudForms each call to a **set\_** method in the **manageiq\_automate** module.

*manageiq\_validate\_certs*: By default is set to **True**. If passed in via *extra\_vars* or assigned in the playbook variables then the lookup will allow self-signed certificates to be used when using SSL REST API connection URLs.

#### 3.1.6.3.2. Example Playbook

The example below utilizes the **manageiq-automate** role. Using variable substitution, playbook tasks retrieve method parameters which are then used to modify object attributes. A final task uses the **set\_retry** module to update the retry interval.

```

- name: Siphon Method Parameters into an object
  hosts: localhost
  connection: local
  vars:
    - auto_commit: True
    - object: root
    - interval: 600

gather_facts: False
roles:
  - syncrou.manageiq-automate

tasks:
  - name: "Get the list of Method Parameters"
    manageiq_automate:
      workspace: "{{ workspace }}"
      get_method_parameters: yes
      register: method_params

  - name: "Set attributes"
    manageiq_automate:
      workspace: "{{ workspace }}"
      set_attributes:
        object: "{{ object }}"
        attributes: "{{ method_params.value }}"

  - name: Set Retry
    manageiq_automate:
      workspace: "{{ workspace }}"
      set_retry:
        interval: "{{ interval }}"

```

#### 3.1.6.4. Callbacks in Multiple Appliance Environments

In a Red Hat CloudForms multiple appliance environment, enable the Embedded Ansible server role on a dedicated CloudForms appliance. Add **store\_session:sql** to Ansible playbooks to ensure successful callbacks to CloudForms appliances in a multiple appliance environment.

See [Deploying CloudForms at Scale](#) for more information on mutiple appliance environments.

## 3.2. 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:

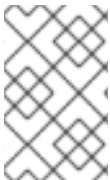
1. Create an Ansible playbook which performs a specific task.
2. A new Ansible Tower job template is created from the playbook, which is then retrieved by Red Hat CloudForms.
3. From the Ansible Tower job template, create a new catalog item in Red Hat CloudForms, optionally with a service dialog that 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](#).

### 3.2.1. Adding an Ansible Tower Provider

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

**NOTE**

Ensure **ENABLE HTTP BASIC AUTH** is set to **On** in the Ansible Tower configuration settings before adding the provider. See [Tower Configuration](#) in the Ansible Tower *Administration Guide*.

1. Navigate to **Automation** → **Ansible Tower** → **Explorer** and click on the **Providers** accordion tab.
2. Under  **Configuration**, click  **Add a new Provider**.
3. In the **Add a new Provider** area:



- a. Enter a **Name** for the new provider.
- b. Add a **Zone** for the provider.
- 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 **Validate** to verify credentials.
7. Click **Add**.

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

### 3.2.2. 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 **Automation** → **Ansible Tower** → **Explorer** and click the **Providers** accordion tab.
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.

### 3.2.3. 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 **Automation** → **Ansible Tower** → **Explorer**.
2. select the **Providers** accordion menu to display a list of **All Ansible Tower 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 **Automation** → **Ansible Tower** → **Explorer** → **Job Templates** accordion menu.

### 3.2.4. Viewing Ansible Tower Configured Systems

To view the systems in your Ansible Tower inventory:

1. Navigate to **Automation** → **Ansible Tower** → **Explorer** → **Configured Systems**.
2. Under **All Ansible Tower Configured Systems**, select **Ansible Tower Configured Systems** to display a list.

### 3.2.5. 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 **Automation** → **Ansible Tower** → **Jobs**.
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.
  - Add configuration information for **Reconfigure Entry Point** and **Retirement Entry Point** as applicable.
  - 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 Conf

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):

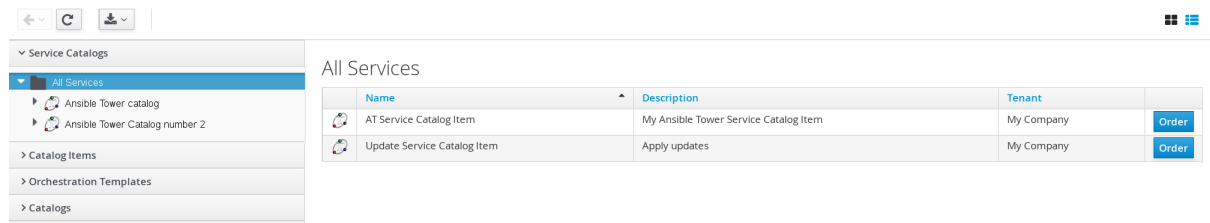
Retirement Entry Point State Machine (NS/CIs /Inst):

**Add** **Cancel**

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

To execute the Ansible Tower job:

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



Name	Description	Tenant	
AT Service Catalog Item	My Ansible Tower Service Catalog Item	My Company	<b>Order</b>
Update Service Catalog Item	Apply updates	My Company	<b>Order</b>

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

### 3.2.6. 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 to 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 **Automation** → **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:  ☒ Display on Button

Button Hover Text:

Button Image:

Dialog:

---

**Object Details**

System/Process:

Message:

Request:

---

**Object Attribute**

Type:

---

**Attribute/Value Pairs**

	Attribute	Value
1	job_template_name	first_job_template
2		
3		
4		
5		

---

**Visibility**


Show:

>

- Click **Add**.

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

1. From **Automation** → **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:  ☒ Display on Button

Button Group Hover Text:

Button Group Image:

---

**Assign Buttons**

Unassigned:

Selected:


Update foo

>

- 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**.

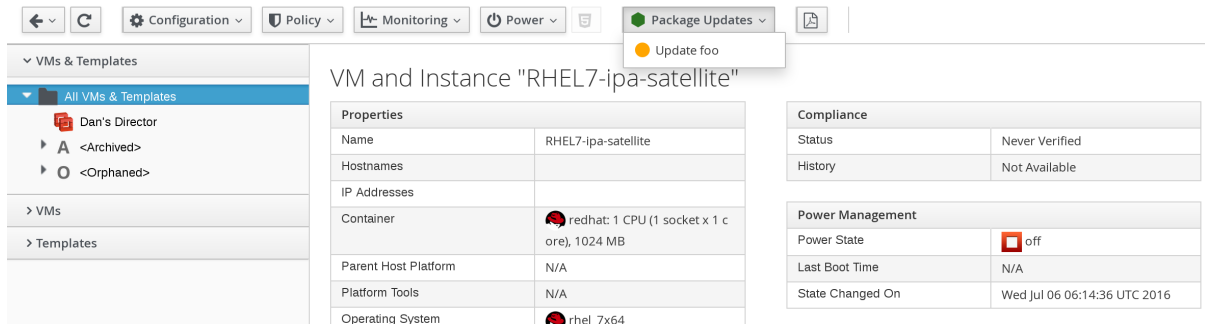
3. Click **Add**.

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.



VM and Instance "RHEL7-ipa-satellite"

Properties	
Name	RHEL7-ipa-satellite
Hostnames	
IP Addresses	
Container	redhat: 1 CPU (1 socket x 1 core), 1024 MB
Parent Host Platform	N/A
Platform Tools	N/A
Operating System	rhel_7x64

Compliance	
Status	Never Verified
History	Not Available

Power Management	
Power State	 off
Last Boot Time	N/A
State Changed On	Wed Jul 06 06:14:36 UTC 2016

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 4. CLOUD PROVIDERS




In CloudForms, a cloud provider is a cloud computing environment that you can add to a 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 CloudForms, and how to manage them. Most cloud providers are added individually to CloudForms. Additionally, Amazon EC2 and Azure cloud providers can be discovered automatically by CloudForms.

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



1. Number of instances
2. Management system software
3. Number of images
4. Authentication status

**Table 4.1. Provider authentication status**

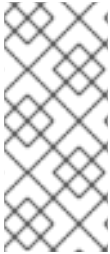
Icon	Description
	Validated: Valid authentication credentials have been added.
	Invalid: Authentication credentials are invalid.
	Unknown: Authentication status is unknown or no credentials have been entered.

### 4.1. OPENSTACK PROVIDERS

#### 4.1.1. 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**

In OpenStack, you must add **admin** as a member of all tenants that users want to access and use in CloudForms.

See [Tenancy](#) in the *Deployment Planning Guide* for more details on tenancy in CloudForms.

When adding an OpenStack cloud or infrastructure provider, you can enable *tenant mapping* in CloudForms to map any existing tenants from that provider. This means CloudForms will create new cloud tenants to match each existing OpenStack tenant; each new cloud tenant and its corresponding OpenStack tenant will have identical resources assignments, with the exception of quotas. Tenant quotas are not synchronized between CloudForms and OpenStack, and are available for reporting purposes only. You can manage quotas in CloudForms but this will not affect the quotas created in OpenStack.

During a provider refresh, CloudForms will also check for any changes to the tenant list in OpenStack. CloudForms will create new cloud tenants to match any new tenants, and delete any cloud tenants whose corresponding OpenStack tenants no longer exist. CloudForms will also replicate any changes to OpenStack tenants to their corresponding cloud tenants.



**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 4.1.1.1, “Configuring the Overcloud to Store Events”](#) for instructions.

For more information, see [OpenStack Telemetry \(ceilometer\)](#) in the Red Hat OpenStack Platform *Architecture Guide*.

**NOTE**

To authenticate the provider using a self-signed Certificate Authority (CA), configure the CloudForms appliance to trust the certificate using the steps in [Section A.1, “Using a Self-Signed CA Certificate”](#) before adding the 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 **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**

Keystone API v3 is required to create cloud tenants on OpenStack cloud providers.

**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*.
- The provider you are creating will be able to see projects for the given domain only. To see projects for other domains, add it as another cloud provider. For more information on domain management in OpenStack, see [Domain Management](#) in the Red Hat OpenStack Platform *Users and Identity Management Guide*.

6. Enter a region number in **Region**.
7. Enter the appropriate **Zone** for the provider. If you do not specify a zone, it is set to **default**.
8. By default, *tenant mapping* is disabled. To enable it, set **Tenant Mapping Enabled** to **Yes**.
9. 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*.

10. In the **Default** tab, under **Endpoints**, configure the host and authentication details of your OpenStack provider:
  - a. Select a **Security Protocol** method to specify how to authenticate the provider:
    - **SSL without validation**: Authenticate the provider insecurely using SSL.
    - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option. This is the recommended authentication method.
    - **Non-SSL**: Connect to the provider insecurely using only HTTP protocol, without SSL.
  - b. 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](#)).

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

- d. In the **Username** field, enter the name of a user in the OpenStack environment.



### IMPORTANT

In environments that use Keystone v3 authentication, the user must have the **admin** role for the relevant domain.

- e. In the **Password** field, enter the password for the user.
- f. Click **Validate** to confirm Red Hat CloudForms can connect to the OpenStack provider.
11. 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 4.1.1.1, “Configuring the Overcloud to Store Events”](#) for details.
  - If you prefer to use the AMQP Messaging bus instead, or eventing is not enabled on Ceilometer, select **AMQP** and configure the following:
    - a. Select a **Security Protocol** method.
    - b. 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.
    - c. In the **API Port**, set the public port used by AMQP. By default, OpenStack uses port 5672 for this.
    - 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** field.
    - e. Click **Validate** to confirm the credentials.
12. 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 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.
- Collecting capacity and utilization data from an OpenStack cloud provider requires selecting the **Collect for All Clusters** option under **Configuration**, in the settings menu. For information, see [Capacity and Utilization Collections](#) in the *General Configuration Guide*.

#### 4.1.1.1. 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:

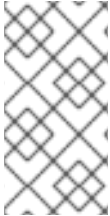
```
parameter_defaults:  
  CeilometerStoreEvents: true
```

3. Please see the below **NOTE**.

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
```



### NOTE

Passing the newly created environment file to the overcloud deployment is environment specific and requires executing commands in particular order depending on use of variables. For further information please see [Director Installation and Usage](#) in the Red Hat OpenStack Platform documentation.

## 4.2. AZURE PROVIDERS

### 4.2.1. 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**.

### 4.2.2. 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 your Azure **Client ID**, **Client Key**, **Azure Tenant ID**, and the **Subscription ID** for that tenant.
5. Click **Start**.

### 4.2.3. Disabling Azure Cloud Regions

Red Hat CloudForms allows administrators to disable Azure cloud regions on the appliance server. You can use this capability to disable certain classified regions. Once disabled, the region will not be available when adding a new Azure provider.

1. From the settings menu, select **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone where the CloudForms server is located, then click on the EVM server.
4. Click on the **Advanced** tab.
5. Search for `:ems_azure:`, and enter the regions you want to disable under `:disabled_regions:`.

Example. To disable the ``us-gov-arizona`` and ``us-gov-texas`` regions:

```
:ems_azure:
:disabled_regions:
- us-gov-arizona
- us-gov-texas
```

6. Click **Save**.

## 4.3. AMAZON EC2 PROVIDERS

### 4.3.1. 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.



#### NOTE

When adding an Amazon EC2 provider in CloudForms with the intention to use the SmartState analysis feature, Red Hat recommends assigning *Admin* group privileges. For situations in which assigning the *Admin* group is unacceptable, manually create an Amazon EC2 policy role using specific permissions. See [Section 4.3.1.1, “Manually Creating an Amazon EC2 Role”](#) for more information.

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)

#### 4.3.1.1. Manually Creating an Amazon EC2 Role

To eliminate the need to assign *Admin* group privileges to the Amazon EC2 provider, create an IAM role following the procedure described in [Creating a Role for an AWS Service \(Console\)](#) in the Amazon Web Services documentation.

Use the following parameters:



1. Select **EC2** as the service the role will use.
2. Attach the following permissions:
  - a. **AmazonEC2FullAccess**
  - b. **AmazonS3FullAccess**
  - c. **AmazonSQSFullAccess**
3. Enter **smartstate** for the **Role name**.

Once the IAM role is created, assign the provider *Power User* privileges as described in [Section 4.3.1, “Permissions for Amazon EC2 Providers”](#).

### 4.3.2. Adding Amazon EC2 Providers





Complete the following procedure to add an Amazon EC2 cloud provider in CloudForms.

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 a **Region**.
6. Select the appropriate **Zone** if you have more than one available.
7. Under **Endpoints**, click the **Default** tab.
  - a. 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**.
  - b. Click **Validate** to validate the credentials.
8. Click the **SmartState Docker** tab.
  - a. Enter the **SmartState Docker User Name** and **SmartState Docker Password**. Here use your **registry.access.redhat.com** credentials required to perform SmartState analysis on AWS. These credentials are required so that you can pull the image from the Red Hat docker registry.
9. Click **Add**.

### 4.3.3. 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**.

### 4.3.4. 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.



**NOTE**

Syncing all public images may require additional memory resources. Also, bear in mind that syncing happens in each configured Amazon EC2 provider, which will require a similar amount of total memory resources.

1. Navigate to the settings menu, then **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.
4. Optionally, configure an array of filters in **public\_images\_filters** to restrict which images are synced. See [http://docs.aws.amazon.com/sdkforruby/api/Aws/EC2/Client.html#describe\\_images-instance\\_method](http://docs.aws.amazon.com/sdkforruby/api/Aws/EC2/Client.html#describe_images-instance_method) for more details.

### 4.3.5. 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 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**. CloudForms automatically connects to this topic.
3. (Optional) Configure the frequency of delta creation in the AWS Management Console.

You can assign 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

### 4.3.6. Enabling Amazon EC2 Events

After adding an Amazon EC2 provider and configuring an SNS topic in [Section 4.3.5, “Enabling AWS Config Notifications”](#), create a CloudTrail, then configure CloudWatch rules on your EC2 provider to automatically get events in CloudForms for monitoring the provider.



#### NOTE

The following procedures are accurate at time of publishing. See the [Amazon AWS documentation](#) for further details on these steps.

#### 4.3.6.1. Creating a CloudTrail

In the CloudTrail area of the AWS Management Console, create a trail and an S3 bucket:

1. Create a **Trail** with a custom name.
2. (Optional) If you want to apply the trail to all of your CloudForms regions, select **Yes** for **Apply trail to all regions**.
3. For **Management Events**, select **Read/Write events: All**.
4. Create a new S3 bucket.

#### 4.3.6.2. Creating CloudWatch Rules Based on Event Patterns

In the CloudWatch area of the AWS Management Console, create three rules: one rule each for EC2, volumes, and snapshots.



#### IMPORTANT

When an SNS topic is deleted and recreated (manually or by CloudForms), CloudWatch rules must be recreated as well, even though the SNS target topic for CloudWatch rules appears to be assigned to these rules. The CloudWatch rule does not send events to this recreated topic until it is recreated too.

To create a CloudWatch rule for EC2:

1. Navigate to **Events** → **Rules** and click **Create rule**.
2. Select the **Event Pattern** radio button to specify the event source.
3. Edit the **Event Pattern Preview** box, and paste and save the following code to create a rule based on a custom event pattern:

```
{
  "source": [
```

```

        "aws.ec2"
      ],
      "detail-type": [
        "AWS API Call via CloudTrail"
      ],
      "detail": {
        "eventSource": [
          "ec2.amazonaws.com"
        ]
      }
    }
  }
}

```

4. Click **Add target** and specify the following attributes:
  - **Type:** SNS Topic
  - **Topic:** AWSConfig\_topic
  - **Input:** Matched event
5. Click **Configure Details** to save these details.
6. Configure a name and description for the rule if desired. Ensure the **Enabled** checkbox is selected for **State**.
7. Click **Create rule** to save the CloudWatch rule.

Repeat the same procedure to create a CloudWatch rule for volumes, pasting the code snippet below to the **Event Pattern Preview** box:

1. Navigate to **Events** → **Rules** and click **Create rule**.
2. Select the **Event Pattern** radio button to specify the event source.
3. Edit the **Event Pattern Preview** box, and paste and save the following code to create a rule based on a custom event pattern:

```

{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EBS Volume Notification"
  ]
}

```

4. Click **Add target** and specify the following attributes:
  - **Type:** SNS Topic
  - **Topic:** AWSConfig\_topic
  - **Input:** Matched event
5. Click **Configure Details** to save these details.

6. Configure a name and description for the rule if desired. Ensure the **Enabled** checkbox is selected for **State**.
7. Click **Create rule** to save the CloudWatch rule.

Repeat the same procedure to create a CloudWatch rule for snapshots, pasting the code snippet below to the **Event Pattern Preview** box:

1. Navigate to **Events** → **Rules** and click **Create rule**.
2. Select the **Event Pattern** radio button to specify the event source.
3. Edit the **Event Pattern Preview** box, and paste and save the following code to create a rule based on a custom event pattern:

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EBS Snapshot Notification"
  ]
}
```

4. Click **Add target** and specify the following attributes:
  - **Type:** **SNS Topic**
  - **Topic:** **AWSConfig\_topic**
  - **Input:** **Matched event**
5. Click **Configure Details** to save these details.
6. Configure a name and description for the rule if desired. Ensure the **Enabled** checkbox is selected for **State**.
7. Click **Create rule** to save the CloudWatch rule.

EC2 can now automatically refresh events in CloudForms.

### 4.3.7. Disabling Amazon Cloud Regions

Red Hat CloudForms allows administrators to disable Amazon cloud regions on the appliance server. Use this capability to disable certain classified regions like AWS GovCloud. Once disabled, the region will not be available when adding an Amazon EC2 provider.

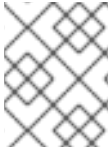
1. From the settings menu, select **Configuration**.
2. Click on the **Settings** accordion, then click **Zones**.
3. Click the zone where the CloudForms server is located, then click on the EVM server.
4. Click on the **Advanced** tab.

5. Search for `:ems_amazon:`, and enter the regions you want to disable under `:disabled_regions:`.

Example. To disable the ``ap-northeast-1`` region:

```
:ems_amazon:
:disabled_regions:
- us-gov-west-1
- ap-northeast-1
```

6. Click **Save**.



#### NOTE

In AWS, Government regions are disabled by default. To enable a disabled region, be sure to do so in the `production.yml` configuration file manually.

## 4.4. GOOGLE COMPUTE ENGINE PROVIDERS

### 4.4.1. 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

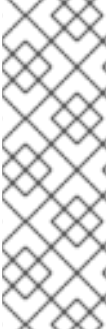
You can generate a private JSON key for your project in **IAM & Admin** → **Service Accounts** in Google Cloud Platform. This key is used to authenticate against your provider.

For additional information, see the Google Cloud 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**.



#### NOTE

Make sure that NTP synchronization is enabled and working. When clocks are not synchronized, the following error will be raised:



**Credential validation was not successful: Authorization failed.**  
**Server message: { "error" : "invalid\_grant", "error\_description" : "Invalid JWT: Token must be a short-lived token and in a reasonable timeframe" }**

### 4.4.2. 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**.

#### 4.4.2.1. 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 ?

Don't export to BigQuery

Save to Cloud Storage bucket ?

Don't export to Cloud Storage

Publish to Cloud Pub/Sub topic ?

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 Cloud 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](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/>.

#### 4.4.2.2. 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.



## 4.5. 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**.



## 4.6. 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.

**Tag Assignment**

Select a customer tag to assign:  <Select a value to assign>



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

\* Only a single value can be assigned from these categories

5. Select a value to assign from the second list.
6. Click **Save**.

## 4.7. 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  (**Configuration**), and then  (**Remove Cloud Providers from the VMDB**).
4. Click **OK**.

## 4.8. 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  (**Configuration**), and then  (**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**.

## 4.9. 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**), 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 **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 5. NETWORK MANAGERS

In Red Hat CloudForms, a network manager is an inventory of networking entities on existing cloud and infrastructure providers managed by your CloudForms appliance.

This provider type exposes software-defined networking (SDN) providers including *OpenStack Network (Neutron)*, *Azure Network*, *Amazon EC2 Network*, and *Google Cloud Network*, which enables software-defined networking inventory collection. 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.

This chapter describes the different types of network managers available to CloudForms, and how to manage them. Network managers are discovered automatically by CloudForms from other connected providers.

### 5.1. ADDING OR VIEWING NETWORK PROVIDERS



#### NOTE

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

Viewing 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*.
2. Click on a provider from the list to view its summary screen.

Network providers summary:

The summary screen includes tables containing information on *Properties*, *Status*, *Relationships*, *Overview*, and *Smart Management*. Click on rows in the *Relationship* and *Overview* tables to see detailed information for individual entities.

Accordion tabs in the sidebar provide access to **Properties** and **Relationships** details.

Click on **Reload**, **Configuration**, **Policy**, and **Monitoring** actions in the taskbar to manage the selected provider.





#### NOTE

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.



### 5.2. 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**.



### 5.3. 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**.



### 5.4. 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**.

### 5.5. 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 and interval, and 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.

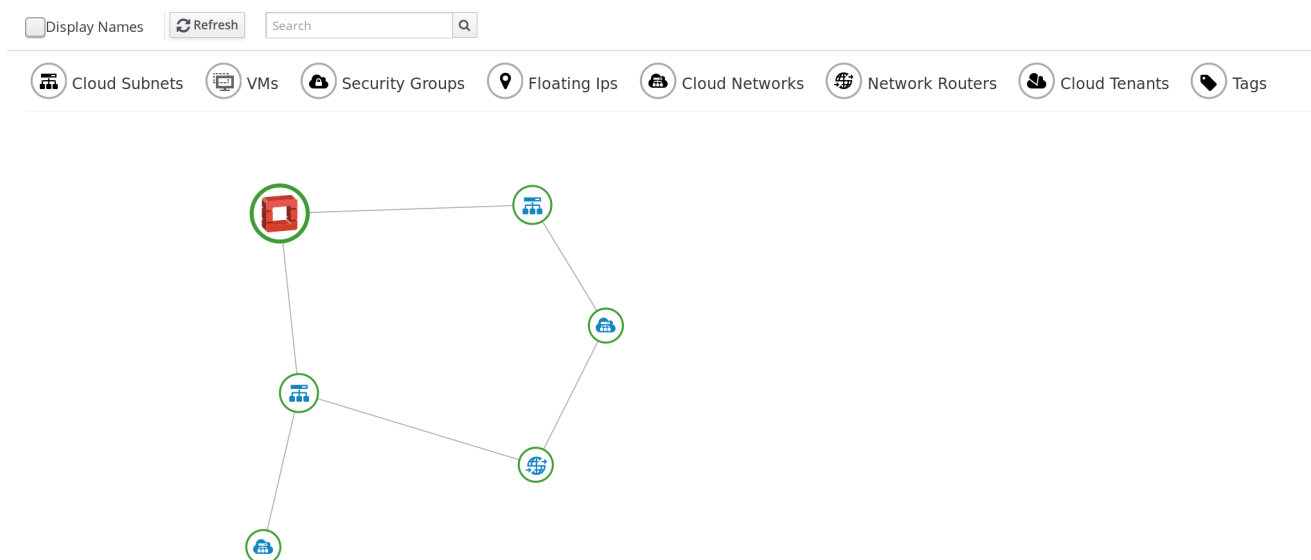
You can also assign policy profiles to network providers, or remove them. The method for doing so is similar to that of any normal policy profile. See [Assigning Policy Profiles to a Network Provider](#) and [Removing Policy Profiles from a Network Provider](#) in the *Policies and Profiles Guide*.

## 5.6. USING THE TOPOLOGY WIDGET FOR NETWORK PROVIDERS

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

The topology graph includes cloud subnets, virtual machines, security groups, floating IP addresses, cloud networks, network routers, cloud tenants, and tags within the overall network provider environment.

Each entity in the graph displays a color indication of its status: green indicates an active entity, while red indicates inactivity or an issue.



### Using the Topology Widget

1. Navigate to **Networks** → **Topology**.
2. Click the desired network provider for viewing the provider summary.

Alternatively, you can open the topology widget from the provider summary page by clicking **Topology** under **Overview**.

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

- Double-click an entity in the graph to navigate to its summary page.
- Drag elements to reposition the graph.
- Click the symbols in the legend at the top of the graph to show or hide entities.
- Click the **Display Names** checkbox to show or hide entity names.
- Click **Refresh** to refresh the display of the network provider entities.
- Enter a search term in the **Search** box to locate an entity by full or partial name.

## CHAPTER 6. MIDDLEWARE MANAGEMENT PROVIDERS

In Red Hat CloudForms, a middleware provider is a middleware management 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 middleware provider that you can add to Red Hat CloudForms, and how to manage them.

The middleware provider extends CloudForms management capabilities to JBoss Middleware application containers running in managed virtual machines, hosts, and Linux containers. The provider delivers inventory, events, metrics, and power operations. Middleware management in CloudForms is a provider based on the Hawkular open source project. When feature complete, the middleware provider will replace the current Red Hat middleware management offering, JBoss Operations Network.





### NOTE

This release of the middleware provider is a Technology Preview. Technology Previews provide early access to upcoming product innovations, allowing you to test new features and provide feedback during the development process. Technology Preview releases are *not* intended for production use. For more information on the support scope for features marked as technology previews, see [Technology Preview Features Support Scope](#).

### 6.1. ADDING A MIDDLEWARE PROVIDER

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

1. Navigate to **Middleware** → **Providers**.
2. Click  (**Configuration**), then click  (**Add a New Middleware Provider**).
3. Enter a **Name** for the provider, for example, Middleware Manager.
4. From the **Type** list, select **Hawkular**.
5. Accept the default **Zone**.
6. Under **Endpoints**, configure the following for the middleware provider:
  - a. Select a **Security protocol** method to specify how to authenticate to the provider. To use SSL to authenticate the provider, the middleware management server must be started with the service option `HAWKULAR_USE_SSL=true`.





### NOTE

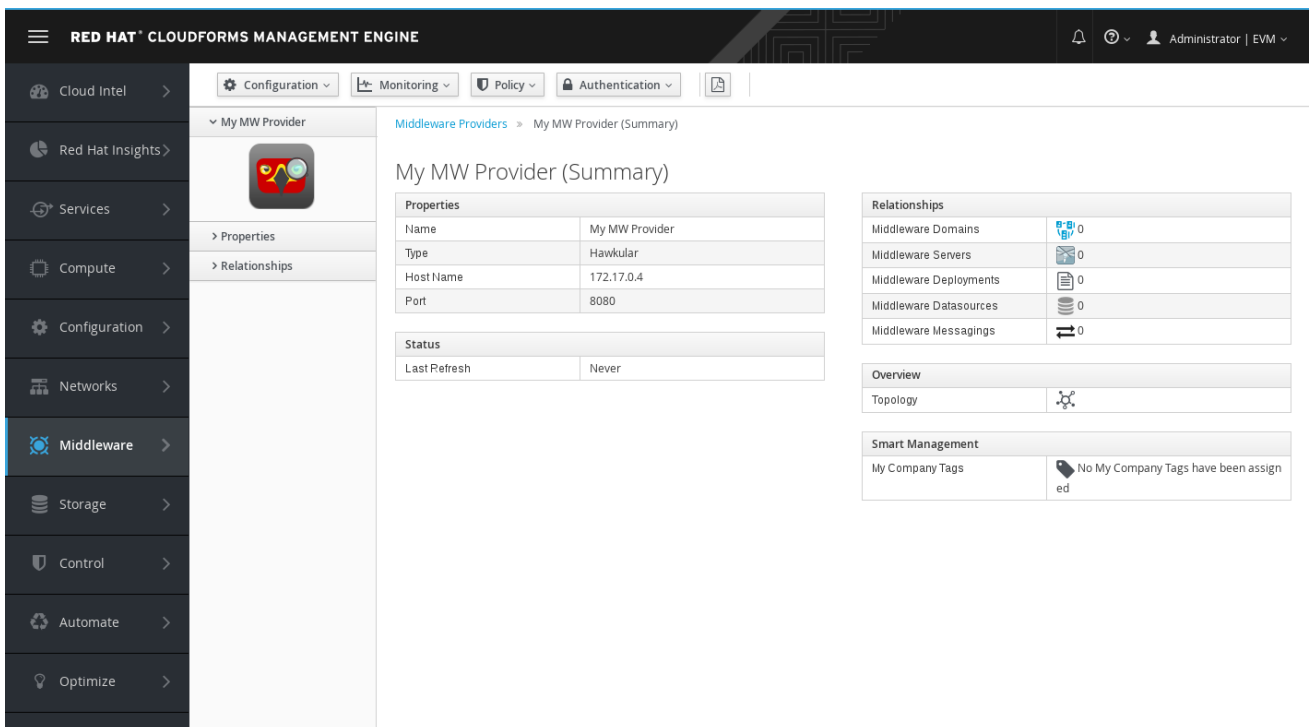
The only supported security protocols for the current release of Hawkular are **SSL without validation** and **Non-SSL**.

- **SSL** (SSL with validation) – Authenticate the provider securely using a trusted certificate authority. This requires that you have already configured your public and private keys in the `/client-secrets` directory as either two .PEM files or as a single .pkcs12 file.
- **SSL trusting custom CA** – Authenticate the provider with a self-signed certificate. For this option, copy your certificate's text to the **Trusted CA Certificates** field in .PEM format.



- **SSL without validation** – Authenticate the provider insecurely (not recommended).
  - **Non-SSL** – Select if you do not want to use SSL.
- b. Enter the **Hostname** or IPv4 or IPv6 address of the machine where you installed the middleware manager.
  - c. Enter the **API Port** of the middleware manager. The default is 8080.
  - d. Enter the **User Name** used to start the middleware manager. This should match the **HAWKULAR\_USERNAME**.
  - e. Enter the **Password** used to start the middleware manager. This should match the **HAWKULAR\_PASSWORD**.
  - f. Reenter the password in the **Confirm Password** field.
  - g. Click **Validate** to confirm that the user has the proper credentials.
7. Click **Add**.
  8. Click  (**Configuration**), then click  (**Refresh Items and Relationships**).

Red Hat CloudForms displays the summary screen:




The screenshot shows the Red Hat CloudForms Management Engine interface. The sidebar on the left contains navigation options: Cloud Intel, Red Hat Insights, Services, Compute, Configuration, Networks, **Middleware**, Storage, Control, Automate, and Optimize. The main content area displays the 'My MW Provider (Summary)' screen. The top navigation bar includes 'Configuration', 'Monitoring', 'Policy', 'Authentication', and a user profile 'Administrator | EVM'. The 'My MW Provider' section shows a summary of the provider's properties and status.

Properties	
Name	My MW Provider
Type	Hawkular
Host Name	172.17.0.4
Port	8080

Status	
Last Refresh	Never

Relationships	
Middleware Domains	0
Middleware Servers	0
Middleware Deployments	0
Middleware Datasources	0
Middleware Messagings	0

Overview	
Topology	

Smart Management	
My Company Tags	No My Company Tags have been assigned

## CHAPTER 7. CONTAINERS PROVIDERS

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

CloudForms can connect to OpenShift Container Platform containers providers and manage them similarly to infrastructure and cloud providers. This allows you to gain control over different aspects of your containers 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 CloudForms connects to a container's 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.



### NOTE




This chapter provides details on managing containers providers. For details on working with the resources within a container environment, see [Container Entities](#) in *Managing Infrastructure and Inventory*.

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



1. Number of nodes
2. Container provider software
3. Power state
4. Authentication status

Table 7.1. Containers provider 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.

## 7.1. OBTAINING AN OPENSIFT CONTAINER PLATFORM MANAGEMENT TOKEN

When deploying OpenShift using **openshift-ansible-3.0.20** (or later versions), the OpenShift Container Platform [service account](#) and [roles](#) required by Red Hat CloudForms are installed by default.



### NOTE

See the [OpenShift Container Platform documentation](#) for a list of the default roles.

Run the following to obtain the token needed to add an OpenShift Container Platform provider:

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



## 7.2. ENABLING OPENSIFT CLUSTER METRICS

Use the OpenShift Cluster Metrics plug-in to collect node, pod, and container metrics into one location. This helps track usage and find common issues.

- Configure Red Hat CloudForms to allow for all three [Capacity & Utilization server roles](#).
- Enable cluster metrics using the [OpenShift Container Platform documentation](#).

## 7.3. ADDING AN OPENSIFT CONTAINER PLATFORM PROVIDER

After initial installation and creation of a Red Hat CloudForms environment, add an OpenShift Container Platform provider using the token obtained in [Section 7.1, “Obtaining an OpenShift Container Platform 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 Container Platform**.
5. Enter the appropriate **Zone** for the provider. If you do not specify a zone, it is set to **default**.
6. From the **Alerts** list, select **Prometheus** to enable external alerts. Selecting **Prometheus** adds an **Alerts** tab to the lower pane to configure the Prometheus service. Alerts are disabled by default.
7. From the **Metrics** list, select **Hawkular** or **Prometheus** to collect capacity and utilization data, or leave as **Disabled**. Selecting **Prometheus** or **Hawkular** adds a **Metrics** tab to the lower pane for further configuration. Metrics are disabled by default.
8. In the **Default** tab, configure the following for the OpenShift provider:
  - a. Select a **Security Protocol** method to specify how to authenticate the provider:
    - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
    - **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.



#### NOTE

You can obtain your OpenShift Container Platform provider's CA certificate for all endpoints (default, metrics, alerts) from `/etc/origin/master/ca.crt`. Paste the output (a block of text starting with `-----BEGIN CERTIFICATE-----`) into the **Trusted CA Certificates** field.

- **SSL without validation**: Authenticate the provider insecurely (not recommended).
- b. Enter the **Hostname** (or IPv4 or IPv6 address) of the provider.



#### IMPORTANT

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

- c. Enter the **API Port** of the provider. The default port is **8443**.
- d. Enter a token for your provider in the **Token** box.



#### NOTE

To obtain a token for your provider, run the **oc get secret** command on your provider; see [Obtaining an OpenShift Container Platform Management Token](#).

For example:

```
# oc get secret --namespace management-infra management-admin-token-8ixxs --template='{{index .data "ca.crt"}}' | base64 --decode
```

- e. Click **Validate** to confirm that Red Hat CloudForms can connect to the OpenShift Container Platform provider.
9. If you selected a metrics service, configure the service details in the **Metrics** tab:
    - a. Select a **Security Protocol** method to specify how to authenticate the service:
      - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
      - **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.



#### NOTE

In OpenShift, the default deployment of the router generates certificates during installation, which can be used with the **SSL trusting custom CA** option. Connecting a Hawkular endpoint with this option requires the CA certificate that the cluster uses for service certificates, which is stored in `/etc/origin/master/service-signer.crt` on the first master in a cluster.

- **SSL without validation**: Authenticate the provider insecurely using SSL. (Not recommended)
- b. Enter the **Hostname** (or IPv4 or IPv6 address) of the provider, or use the **Detect** button to find the hostname.
  - c. Enter the **API Port** if your Hawkular provider uses a non-standard port for access. The default port is **443**.
  - d. Click **Validate** to confirm that Red Hat CloudForms can connect to the metrics endpoint.
10. For the **Prometheus** alerts service, add the Prometheus alerts endpoint in the **Alerts** tab:
    - a. Select a **Security Protocol** method to specify how to authenticate the service:
      - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
      - **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.
      - **SSL without validation**: Authenticate the provider insecurely using SSL. (Not recommended)
    - b. Enter the **Hostname** (or IPv4 or IPv6 address) or alert **Route**.
    - c. Enter the **API Port** if your Prometheus provider uses a non-standard port for access. The default port is **443**.
    - d. Click **Validate** to confirm that CloudForms can connect to the alerts service.

- Click the **Advanced** tab to add image inspector settings for scanning container images on your provider using OpenSCAP.



#### NOTE

- These settings control downloading the image inspector container image from the registry and obtaining the Common Vulnerabilities and Exposures (CVE) information (for effective scanning) via a proxy.
- CVE URL that CloudForms requires to be open for OpenSCAP scanning: <https://www.redhat.com/security/data/metrics/ds/>. This information is based on the source code of OpenSCAP.

- Enter the proxy information for the provider in either **HTTP**, **HTTPS**, or **NO Proxy** depending on your environment.
  - Enter the **Image-Inspector Repository** information. For example, **openshift3/image-inspector**.
  - Enter the **Image-Inspector Registry** information. For example, **registry.access.redhat.com**.
  - Enter the **Image-Inspector Tag** value. A tag is a mark used to differentiate images in a repository, typically by the application version stored in the image.
  - Enter <https://www.redhat.com/security/data/metrics/ds/> in **CVE location**.
- Click **Add**.



#### NOTE



You can also set global default image-inspector settings for all OpenShift providers in the advanced settings menu by editing the values under **ems\_kubernetes**, instead of setting this for each provider.

For example:

```
:image_inspector_registry: registry.access.redhat.com
:image_inspector_repository: openshift3/image-inspector
```



## 7.4. TAGGING CONTAINERS PROVIDERS

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

- Navigate to **Compute** → **Containers** → **Providers**.
- Select the checkboxes for the containers providers to tag.
- Click  (**Policy**), and then  (**Edit Tags**).
- Select a tag to assign from the drop-down menu.

**Tag Assignment**

Select a customer tag to assign: Environment \* <Select a value to assign>



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

\* Only a single value can be assigned from these categories

5. Select a value to assign.
6. Click **Save**.

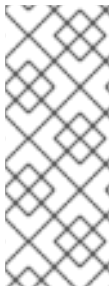
## 7.5. REMOVING CONTAINERS PROVIDERS

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**), and then  (**Remove Containers Providers from the VMDB**).
4. Click **OK**.

## 7.6. PAUSING / RESUMING CONTAINERS PROVIDERS



In CloudForms, you can pause and resume containers providers. This allows users to add a number of potentially resource-intensive providers, then pause and resume those that are not required at a given time. Additionally, when performing maintenance on a provider, you can pause the provider to prevent CloudForms from connecting to it, to avoid generating log errors or collecting partial data.



### NOTE



- While the provider is paused no data will be collected from it. This may cause gaps in inventory, metrics and events.
- Also, the provider itself is not turned off when paused, but only temporarily disables the link between CloudForms and the provider. Resuming the provider re-enables the link between CloudForms and the provider.

To pause a containers provider:

1. Navigate to **Compute** → **Containers** → **Providers**.
2. Click the containers provider that you want to pause.
3. Click  (**Configuration**), and then  (**Pause this Containers Provider**).
4. Click **OK**.

To resume a paused containers provider:



1. Navigate to **Compute** → **Containers** → **Providers**.
2. Click the paused containers provider that you want to resume.

3. Click  (**Configuration**), and then  (**Resume this Containers Provider**).
4. Click **OK**.

## 7.7. EDITING A CONTAINERS PROVIDER

Edit information about a provider such as the name, hostname, IP address or port, and credentials as required. If you have just upgraded your CloudForms environment from an older version, edit the provider to specify the authentication method the provider uses to connect to Red Hat CloudForms.

1. Navigate to **Compute** → **Containers** → **Providers**.
2. Click the containers provider to edit.

3. Click  (**Configuration**), and then  (**Edit Selected Containers Provider**).
4. Edit the **Name** if required.



### NOTE

The **Type** value is unchangeable.

5. Under **Endpoints** in the **Default** tab, edit the following as required:
  - a. Select a **Security Protocol** method to specify how to authenticate the provider:
    - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
    - **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.



### NOTE

You can obtain your OpenShift Container Platform provider's CA certificate for all endpoints (default, metrics, alerts) from `/etc/origin/master/ca.crt`. Paste the output (a block of text starting with `-----BEGIN CERTIFICATE-----`) into the **Trusted CA Certificates** field.

- **SSL without validation**: Authenticate the provider insecurely (not recommended).
- b. Enter the **Hostname** (or IPv4 or IPv6 address) of the provider.



### IMPORTANT

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

- c. Enter the **API Port** of the provider. The default port is **8443**.
- d. Enter a token for your provider in the **Token** box.



**NOTE**

To obtain a token for your provider, run the **oc get secret** command on your provider; see [Obtaining an OpenShift Container Platform Management Token](#).

For example:

```
# oc get secret --namespace management-infra management-admin-token-8ixxs --template='{{index .data "ca.crt"}}' | base64 --decode
```

- e. Click **Validate** to confirm that Red Hat CloudForms can connect to the OpenShift Container Platform provider.
6. Under **Endpoints** in the **Metrics** tab, configure the following for gathering capacity and utilization metrics for Hawkular or Prometheus based on the selection:
    - a. Select a **Security Protocol** method to specify how to authenticate the provider:
      - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
      - **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.
      - **SSL without validation**: Authenticate the provider insecurely using SSL. (Not recommended)
    - b. Enter the **Hostname** (or IPv4 or IPv6 address) of the provider.
    - c. Enter the **API Port** if your provider uses a non-standard port for access. The default port is **443**.
    - d. Click **Validate** to confirm that Red Hat CloudForms can connect to the endpoint.
  7. Under **Endpoints** in the **Alerts** tab, configure the following for Prometheus alerting from the cluster.
    - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
    - **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.
    - **SSL without validation**: Authenticate the provider insecurely using SSL. (Not recommended)
      - a. Enter the **Hostname** (or IPv4 or IPv6 address) of the provider.
      - b. Enter the **API Port** if your provider uses a non-standard port for access. The default port is **443**.
      - c. Click **Validate** to confirm that Red Hat CloudForms can connect to the endpoint.

8. Click **Save**.

## 7.8. HIDING ENVIRONMENT VARIABLES FOR CONTAINERS PROVIDERS

You can restrict users from viewing container provider environment variables by configuring user roles.

This is useful as the environment variables panel can expose sensitive information, such as passwords, that you may not want certain users to view.







### NOTE

The default user roles in CloudForms are read-only. To customize a role's settings, create a new role or a copy of an existing role.

You can view role information and the product features the role can access (marked by a checkmark) by clicking on any role in **Access Control**. Expand the categories under **Product Features** to see further detail.

To configure user access to container environment variables:

1. From the settings menu, select **Configuration**.
2. Click the **Access Control** accordion, then click **Roles**.
3. Select an existing custom role from the **Access Control Roles** list, and click  **(Configuration)**, then  **(Edit the selected Role)**.  
Alternatively, to create a new custom role, select a role from the **Access Control Roles** list, and click  **(Configuration)**, then  **(Copy this Role to a new Role)**.
4. Edit the name for the role if desired.
5. For **Access Restriction for Services, VMs, and Templates**, select if you want to limit users with this role to only see resources owned by the user or their group, owned by the user, or all resources (**None**).
6. Expand the **Product Features (Editing)** tree options to show **Everything** → **Compute** → **Containers** → **Containers Explorer** → **All Containers** → **View Containers**.
7. Clear the **Environment Variables** checkbox to restrict the user role from viewing container environment variables.

Role Information

Name

Access Restriction for Services, VMs, and Templates

Product Features (Editing)



- ☒ ☐ Everything
  - > ☒ ☐ Cloud Intel
  - > ☐ ☐ Red Hat Insights
  - > ☐ ☐ Services
  - > ☒ ☐ Compute
    - > ☒ ☐ Clouds
    - > ☒ ☐ Infrastructure
    - > ☐ ☐ Physical Infrastructure
    - > ☒ ☐ Containers
      - > ☒ ☐ Containers Dashboard
      - > ☒ ☐ Container Providers
      - > ☒ ☐ Projects
      - > ☒ ☐ Routes
      - > ☒ ☐ Services
      - > ☒ ☐ Replicators
      - > ☒ ☐ Pods
      - > ☒ ☐ Containers Explorer
        - > ☒ ☐ Relationships
        - > ☒ ☐ All Containers
          - > ☒ ☐ View Containers
            - ☒ ☐ List
            - ☒ ☐ Timeline
            - ☒ ☐ Environment Variables
          - > ☐ ☐ Modify
          - > ☒ ☐ Operate
    - > ☒ ☐ Nodes

8. Click **Save**.

For more information about user roles, see [Roles](#) in *General Configuration*.

## 7.9. 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.

Click on an item for more detailed information.

## CHAPTER 8. STORAGE MANAGERS

In Red Hat CloudForms, a storage manager is a service providing storage resources that you can manage from a Red Hat CloudForms appliance. This chapter describes the different types of storage managers used by Red Hat CloudForms, and how they are added to Red Hat CloudForms.

There are three types of storage managers currently available to Red Hat CloudForms:

- Amazon Elastic Block Store
- OpenStack Block Storage (**openstack-cinder**)
- OpenStack Object Storage (**openstack-swift**)

### 8.1. AMAZON ELASTIC BLOCK STORE MANAGERS

The Amazon Elastic Block Store service provides and manages persistent block storage resources that Amazon EC2 instances can consume.

To use the Amazon Elastic Block Store service as a storage manager, you must first add an Amazon EC2 cloud provider to your Red Hat CloudForms appliance. The Amazon Elastic Block Store service is automatically discovered by Red Hat CloudForms, and added to the **Storage Managers** list. See [Section 4.3.2, “Adding Amazon EC2 Providers”](#) for instructions on adding an Amazon EC2 cloud provider.



#### NOTE

For information on managing the inventory available to Amazon Elastic Block Store managers, see [Volumes](#) in the *Managing Infrastructure and Inventory* guide.

### 8.2. OPENSTACK BLOCK STORAGE MANAGERS

The OpenStack Block Storage service (**openstack-cinder**) provides and manages persistent block storage resources that OpenStack infrastructure instances can consume.

To use OpenStack Block Storage as a storage manager, you must first add an OpenStack cloud provider to your Red Hat CloudForms appliance and enable events. The Block Storage service will be automatically discovered by Red Hat CloudForms and added to the **Storage Managers** list in Red Hat CloudForms. See [Section 4.1.1, “Adding OpenStack Providers”](#) for instructions on adding a cloud provider and enabling events.



#### NOTE

For information on managing the inventory available to OpenStack Block Storage managers, see [Volumes](#) in the *Managing Infrastructure and Inventory* guide.

### 8.3. OPENSTACK OBJECT STORAGE MANAGERS

The OpenStack Object Storage (**openstack-swift**) service provides cloud object storage.

To use the OpenStack Object Storage service as a storage manager, you must first add an OpenStack cloud provider to your Red Hat CloudForms appliance and enable events. The Object Storage service will be automatically discovered by Red Hat CloudForms and added to the **Storage Managers** list in Red

Hat CloudForms. See [Section 4.1.1, “Adding OpenStack Providers”](#) for instructions on adding a cloud provider and enabling events.

### 8.3.1. Viewing Object Stores

The object store summary page shows details including the object store’s size, parent cloud, storage manager, cloud tenant, and the number of cloud objects on the object store.

In Red Hat CloudForms, view object stores on a object storage manager by following these steps:

1. Navigate to **Storage** → **Object Stores** to display a list of object store containers.
2. Click a container to open a summary page for that object store container.
3. Click **Cloud Objects** to view a list of object stores in the object store container.
4. Click an object store from the list to view the object store’s summary page.

## CHAPTER 9. 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 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 Container Platform Installation and Configuration Guide](#), ensuring you use the desired version of OpenShift.

## APPENDIX A. APPENDIX

### A.1. USING A SELF-SIGNED CA CERTIFICATE

Adding a self-signed Certificate Authority (CA) certificate for SSL authentication requires additional configuration on OpenStack Platform and Microsoft System Center Virtual Machine Manager (SCVMM) providers.



#### NOTE

This procedure is not required for OpenShift Container Platform, Red Hat Virtualization, or middleware manager providers, which have the option to select **SSL trusting custom CA** as a **Security Protocol** in the user interface. These steps are needed only for providers without this option in the user interface.

Before adding the provider, configure the following:

1. Copy your provider's CA certificate in PEM format to **/etc/pki/ca-trust/source/anchors/** on your CloudForms appliance.
2. Update the trust settings on the appliance:

```
# update-ca-trust
```

3. Restart the EVM processes on the server:

```
# rake evm:restart
```

The CA certificate is added to the appliance, and you can add the provider to CloudForms.