



Red Hat OpenStack Platform 10

QuickStart Guide for CloudForms with Red Hat OpenStack Platform

Getting started with CloudForms on Red Hat OpenStack Platform

Red Hat OpenStack Platform 10 QuickStart Guide for CloudForms with Red Hat OpenStack Platform

Getting started with CloudForms on Red Hat OpenStack Platform

OpenStack Team
rhos-docs@redhat.com

Legal Notice

Copyright © 2017 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 document provides a quick guide for integrating an Red Hat OpenStack Platform cloud deployment with Red Hat CloudForms. It is intended as an abridged reference for users already familiar with Red Hat CloudForms, Red Hat OpenStack Platform, and Red Hat Enterprise Linux.

Table of Contents

CHAPTER 1. INTRODUCTION TO RED HAT CLOUDFORMS	4
1.1. ARCHITECTURE	4
1.2. REQUIREMENTS	5
1.2.1. Virtual Hardware Requirements	5
1.2.2. Database Requirements	5
1.2.3. Browser Requirements	6
1.2.4. Additional Requirements	6
1.3. TERMINOLOGY	7
1.4. GETTING SUPPORT	9
CHAPTER 2. KEY RED HAT CLOUDFORMS FEATURES FOR OPENSTACK CLOUD PROVIDERS	11
CHAPTER 3. INSTALLING AND CONFIGURING RED HAT CLOUDFORMS	12
3.1. OBTAINING AND INSTALLING THE RED HAT CLOUDFORMS APPLIANCE	12
3.2. CONFIGURING RED HAT CLOUDFORMS	12
3.3. CONFIGURING GENERAL APPLIANCE SETTINGS	13
3.4. CONFIGURING A DATABASE FOR RED HAT CLOUDFORMS	14
3.5. CONFIGURING GENERAL RED HAT CLOUDFORMS SETTINGS	15
3.6. REGISTERING YOUR APPLIANCE	16
3.7. CONFIGURING CLOUDFORMS METRICS FOR SMARTSTATE ANALYSIS	18
3.7.1. Configuring CloudForms Capacity and Utilization	18
3.7.2. Enabling SmartState Analysis	18
CHAPTER 4. ADDING AN OPENSTACK INFRASTRUCTURE PROVIDER	20
4.1. CONFIGURING THE UNDERCLOUD TO STORE EVENTS	22
CHAPTER 5. ADDING AN OPENSTACK CLOUD PROVIDER	23
5.1. CONFIGURING THE OVERCLOUD TO STORE EVENTS	25
CHAPTER 6. PERFORMING A SMARTSTATE ANALYSIS	27
CHAPTER 7. USING THE TOPOLOGY WIDGET	28
CHAPTER 8. MANAGING POLICIES	29
8.1. CREATING A HOST COMPLIANCE POLICY	29
8.2. CREATING A VIRTUAL MACHINE CONTROL POLICY	31
CHAPTER 9. MANAGING INSTANCES	33
9.1. PROVISIONING AN OPENSTACK INSTANCE FROM AN IMAGE	33
CHAPTER 10. MANAGING STORAGE	35
10.1. MANAGING BLOCK STORAGE	35
10.2. MANAGING OBJECT STORAGE	37
CHAPTER 11. CATALOGS AND SERVICES	38
11.1. CREATING A SERVICE DIALOG	38
11.2. CREATING A CATALOG	40
11.2.1. Creating a Catalog Item	40
11.2.2. Ordering a Catalog Item	41
CHAPTER 12. REPORTS	42
12.1. GENERATING A SINGLE REPORT	42
12.2. SCHEDULING A REPORT	43
12.3. VIEWING REPORTS	43

CHAPTER 13. CHARGEBACK	44
13.1. CREATING CHARGEBACK RATES	44
13.2. ASSIGNING CHARGEBACK RATES	44
13.3. CREATING A CHARGEBACK REPORT	45
APPENDIX A. USING A SELF-SIGNED CA CERTIFICATE	46
APPENDIX B. CUSTOMIZING PROVISIONING DIALOGS	47
APPENDIX C. CREATING CUSTOM BUTTONS FOR CLOUD TENANTS	48
C.1. CREATING A CUSTOM BUTTON GROUP	48
C.2. CREATING A CUSTOM BUTTON	48
APPENDIX D. MANAGING KEYPAIRS	50

CHAPTER 1. INTRODUCTION TO RED HAT CLOUDFORMS

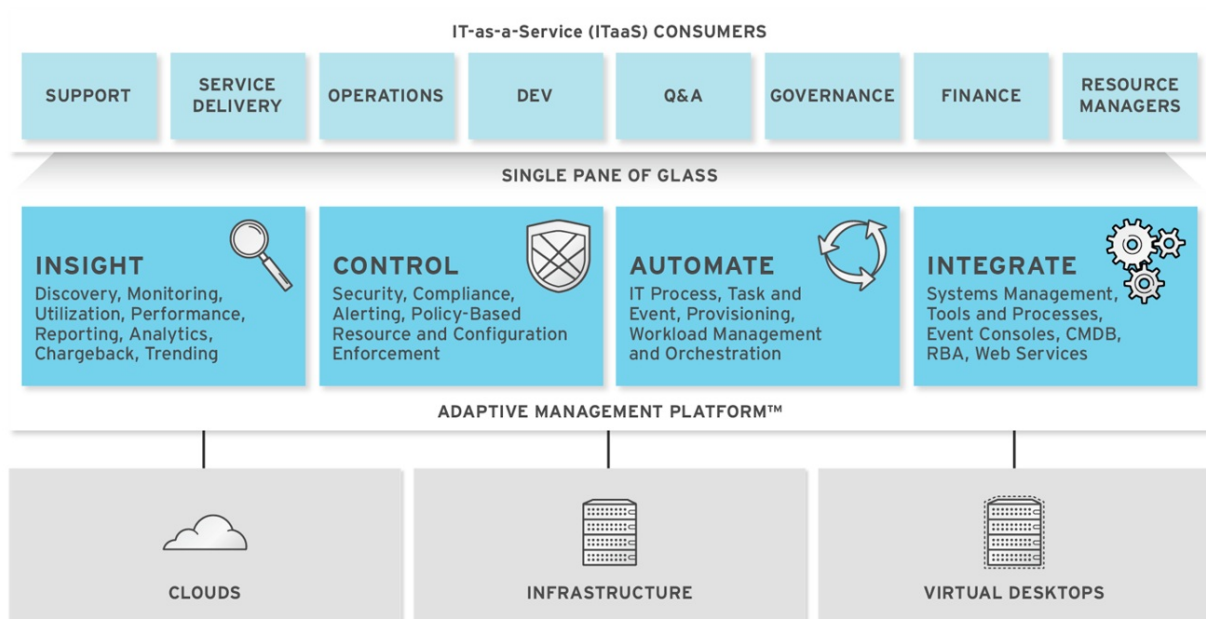
Red Hat CloudForms delivers the insight, control, and automation that enterprises need to address the challenges of managing virtual environments. This technology enables enterprises with existing virtual infrastructures to improve visibility and control, and those starting virtualization deployments to build and operate a well-managed virtual infrastructure.

Red Hat CloudForms provides the following feature sets:

- **Insight:** Discovery, Monitoring, Utilization, Performance, Reporting, Analytic, Chargeback, and Trending.
- **Control:** Security, Compliance, Alerting, and Policy-Based Resource, and Configuration Enforcement.
- **Automate:** IT Process, Task and Event, Provisioning, and Workload Management and Orchestration.
- **Integrate:** Systems Management, Tools and Processes, Event Consoles, Configuration Management Database (CMDB), Role-based Administration (RBA), and Web Services.

1.1. ARCHITECTURE

The diagram below describes the capabilities of Red Hat CloudForms. Its features are designed to work together to provide robust management and maintenance of your virtual infrastructure.



The architecture comprises the following components:

- The Red Hat CloudForms appliance (appliance) which is supplied as a secure, high-performance, preconfigured virtual machine. It provides support for HTTPS communications.
- The Red Hat CloudForms Server (Server) resides on the appliance. It is the software layer that communicates between the SmartProxy and the Virtual Management Database. It includes support for HTTPS communications.

- The Virtual Management Database (VMDB) resides either on the appliance or another computer accessible to the appliance. It is the definitive source of intelligence collected about your Virtual Infrastructure. It also holds status information regarding appliance tasks.
- The Red Hat CloudForms Console (Console) is the Web interface used to view and control the Server and appliance. It is consumed through Web 2.0 mash-ups and web services (WS Management) interfaces.
- The SmartProxy can reside on the appliance or on an ESX Server. If not embedded in the Server, the SmartProxy can be deployed from the appliance. A SmartProxy agent must be configured in each storage location, and must be visible to the appliance. The SmartProxy acts on behalf of the appliance communicating with it over HTTPS on standard port 443.

1.2. REQUIREMENTS

To use Red Hat CloudForms, certain virtual hardware, database, and browser requirements must be met in your environment.

1.2.1. Virtual Hardware Requirements

The Red Hat CloudForms appliance requires the following virtual hardware at minimum:

- 4 VCPUs
- 12 GB RAM
- 44 GB HDD + optional database disk

1.2.2. Database Requirements

Red Hat recommends allocating the virtual machine disk fully at the time of creation. Three main factors affect the size of your database over time:

- Virtual Machine Count: the most important factor in the calculation of virtual machine database (VMDB) size over time.
- Host Count: the number of hosts associated with the provider.
- Storage Count: the number of individual storage elements as seen from the perspective of the provider or host. It is not the total number of virtual disks for all virtual machines.

Use the following table as a guideline to calculate minimum requirements for your database:

Virtual Machine Count	Host Count	Storage Count	Estimated VMDB Size in GB	
			1 year	2 year
100	5	50	3.5	5
500	10	100	17	25
5000	50	500	173	251

**NOTE**

When enabling capacity and utilization for metrics gathering over a period of time, it is recommended that the VMDB size scale accordingly. Evaluate the number of instances in your provider inventory and storage duration requirements to plan for increased VMDB sizing requirements.

Use the following information to plan for your increased VMDB needs when working with metrics gathering:

- Realtime metrics data are stored for 4 hours.
- Rollup metrics data are stored for 6 months.

Example:

	Minute	Hour	Day
OpenStack Provider Instance	3 Realtime Metrics	181 (3 records * 60 minutes = 180 Realtime Metrics + 1 hourly Rollup Metric)	4,345 (3 records * 60 minutes * 24 hours = 4320 Realtime Metrics + 1 daily Rollup Metric)

- Metrics data storage times can be configured by editing the Advanced Settings.

1.2.3. Browser Requirements

To use Red Hat CloudForms, the following browser requirements must be met:

- One of the following web browsers:
 - Mozilla Firefox for versions supported under Mozilla's Extended Support Release (ESR)
 - Internet Explorer 10 or higher
 - Google Chrome for Business
- A monitor with minimum resolution of 1280x1024.

**IMPORTANT**

Due to browser limitations, Red Hat supports logging in to only one tab for each multi-tabbed browser. Console settings are saved for the active tab only. For the same reason, Red Hat CloudForms does not guarantee that the browser's **Back** button will produce the desired results. Red Hat recommends using the breadcrumbs provided in the Console.

1.2.4. Additional Requirements

Additionally, the following must be configured to use Red Hat CloudForms:

- The Red Hat CloudForms appliance must already be installed and activated in your enterprise environment.

- The SmartProxy must have visibility into the virtual machines and cloud instances that you want to control.
- For more information, see [SmartProxies](#) in the CloudForms *General Configuration* guide.

1.3. TERMINOLOGY

The following terms are used throughout this document. Review them before proceeding.

Account Role

The level of access a user has to different parts and functions of the Red Hat CloudForms console. There are a variety of Account Roles, which can be assigned to users to restrict or allow access to parts of the console and virtual infrastructure.

Action

An execution that is performed after a condition is evaluated.

Alert

Red Hat CloudForms alerts notify administrators and monitoring systems of critical configuration changes and threshold limits in the virtual environment. The notification can take the form of either an email or an SNMP trap.

Analysis Profile

A customized scan of hosts, virtual machines, or instances. You can collect information from categories, files, event logs, and registry entries.

Cloud

A pool of on-demand and highly available computing resources. The usage of these resources are scaled depending on the user requirements and metered for cost.

Red Hat CloudForms Appliance

A virtual machine where the virtual management database (VMDB) and Red Hat CloudForms reside.

Red Hat CloudForms Console

A web-based interface into the Red Hat CloudForms appliance.

Red Hat CloudForms Role

A designation assigned to a Red Hat CloudForms server that defines what a Red Hat CloudForms server can do.

Red Hat CloudForms Server

The application that runs on the Red Hat CloudForms appliance and communicates with the SmartProxy and the VMDB.

Cluster

Hosts that are grouped together to provide high availability and load balancing.

Condition

A control policy test triggered by an event, which determines a subsequent action.

Discovery

Process run by the Red Hat CloudForms server which finds virtual machine and cloud providers.

Drift

The comparison of a virtual machine, instance, host, cluster to itself at different points in time.

Event

A trigger to check a condition.

Event Monitor

Software on the Red Hat CloudForms appliance which monitors external providers for events and sends them to the Red Hat CloudForms server.

Host

A computer running a hypervisor, capable of hosting and monitoring virtual machines. Supported hypervisors include RHEV-H, VMware ESX hosts, Windows Hyper-V hosts.

Instance/Cloud Instance

A on-demand virtual machine based upon a predefined image and uses a scalable set of hardware resources such as CPU, memory, networking interfaces.

Managed/Registered VM

A virtual machine that is connected to a host and exists in the VMDB. Also, a template that is connected to a provider and exists in the VMDB. Note that templates cannot be connected to a host.

Managed/Unregistered VM

A virtual machine or template that resides on a repository or is no longer connected to a provider or host and exists in the VMDB. A virtual machine that was previously considered registered may become unregistered if the virtual machine was removed from provider inventory.

Provider

An external management system that CloudForms integrates in order to collect data and perform operations.

Policy

A combination of an event, a condition, and an action used to manage a virtual machine.

Policy Profile

A set of policies.

Refresh

A process run by the Red Hat CloudForms server which checks for relationships of the provider or host to other resources, such as storage locations, repositories, virtual machines, or instances. It also checks the power states of those resources.

Regions

A region is the collection of zones that share the same database for reporting and charting. A master region may be added to synchronize multiple VMDBs into one VMDB for higher-level reporting, providing a "single pane of glass" view.

Resource

A host, provider, instance, virtual machine, repository, or datastore.

Resource Pool

A group of virtual machines across which CPU and memory resources are allocated.

Repository

A place on a datastore resource which contains virtual machines.

SmartProxy

The SmartProxy is a software agent that acts on behalf of the Red Hat CloudForms appliance to perform actions on hosts, providers, storage and virtual machines.

The SmartProxy can be configured to reside on the Red Hat CloudForms appliance or on an ESX server version. The SmartProxy can be deployed from the Red Hat CloudForms appliance, and provides visibility to the VMFS storage. Each storage location must have a SmartProxy with visibility to it. The SmartProxy acts on behalf of the Red Hat CloudForms appliance. If the SmartProxy is not embedded in the Red Hat CloudForms server, it communicates with the Red Hat CloudForms appliance over HTTPS on standard port 443.

SmartState Analysis

Process run by the SmartProxy which collects the details of a virtual machine or instance. Such details include accounts, drivers, network information, hardware, and security patches. This process is also run by the Red Hat CloudForms server on hosts and clusters. The data is stored in the VMDB.

SmartTags

Descriptors that allow you to create a customized, searchable index for the resources in your clouds and infrastructure.

Storage Location

A device, such as a VMware datastore, where digital information resides that is connected to a resource.

Tags

Descriptive terms defined by a Red Hat CloudForms user or the system used to categorize a resource.

Template

A template is a copy of a preconfigured virtual machine, designed to capture installed software and software configurations, as well as the hardware configuration, of the original virtual machine.

Unmanaged Virtual Machine

Files discovered on a datastore that do not have a virtual machine associated with them in the VMDB. These files may be registered to a provider that the Red Hat CloudForms server does not have configuration information on. Possible causes may be that the provider has not been discovered or that the provider has been discovered, but no security credentials have been provided.

Virtual Machine

A software implementation of a system that functions similar to a physical machine. Virtual machines utilize the hardware infrastructure of a physical host, or a set of physical hosts, to provide a scalable and on-demand method of system provisioning.

Virtual Management Database (VMDB)

Database used by the Red Hat CloudForms appliance to store information about your resources, users, and anything else required to manage your virtual enterprise.

Virtual Thumbnail

An image in the web interface representing a resource, such as a provider or a virtual machine, showing the resource's properties at a glance. Each virtual thumbnail is divided into quadrants, which provide information about the resource, such as its software and power state.

Zones

Red Hat CloudForms Infrastructure can be organized into zones to configure failover and to isolate traffic. Zones can be created based on your environment. Zones can be based on geographic location, network location, or function. When first started, new servers are put into the default zone.

1.4. GETTING SUPPORT

If you experience difficulty with a procedure described in this documentation, visit the Red Hat Customer Portal at <http://access.redhat.com>. Through the Customer Portal, you can:

- search or browse through a knowledgebase of technical support articles about Red Hat products
- submit a support case to Red Hat Global Support Services (GSS)
- access other product documentation

Red Hat also hosts a large number of electronic mailing lists for discussion of Red Hat software and technology. You can find a list of publicly available mailing lists at

<https://www.redhat.com/mailman/listinfo>. Click on the name of any mailing list to subscribe to that list or to access the list archives.

CHAPTER 2. KEY RED HAT CLOUDFORMS FEATURES FOR OPENSTACK CLOUD PROVIDERS

Red Hat CloudForms provides several interface features specific to OpenStack cloud providers:

- The CloudForms **Topology** widget ([Chapter 7, Using the Topology Widget](#)) provides an interactive visualization of the OpenStack cloud.
- CloudForms provides a user interface for managing OpenStack storage resources ([Chapter 10, Managing Storage](#)).
- *Custom buttons*, which allows you to provide automation for specific actions to OpenStack tenants ([Appendix C, Creating Custom Buttons for Cloud Tenants](#)).

When adding an OpenStack cloud provider, you can also:

- Enable *tenant mapping*. This creates a one-to-one association between tenants in CloudForms and OpenStack.
- Connect to OpenStack through the Keystone V3 API. This API enables multiple OpenStack identity domains. Domains are high-level containers for projects, users, and groups. Users of different domains can be represented in different authentication back ends.

For information about tenant mapping and the Keystone V3 API, see [Chapter 5, Adding an OpenStack Cloud Provider](#).

CHAPTER 3. INSTALLING AND CONFIGURING RED HAT CLOUDFORMS

Red Hat CloudForms can be installed on a number of virtualization platforms, such as [VMware vSphere](#), and [Red Hat Enterprise Virtualization](#). This chapter describes how to install and configure Red Hat CloudForms on *Red Hat OpenStack Platform*.

3.1. OBTAINING AND INSTALLING THE RED HAT CLOUDFORMS APPLIANCE

First, download the appliance from the Red Hat Customer Portal:

1. Go to access.redhat.com and log in to the Red Hat Customer Portal using your customer account details.
2. Click **Downloads** in the menu bar.
3. Click **A-Z** to sort the product downloads alphabetically.
4. Click **Red Hat CloudForms** to access the product download page. The latest version of each download displays by default.
5. From the list of installers and images under **Product Software**, choose **OpenStack Virtual Appliance** option with the latest version and click **Download Now**.

Afterwards, upload or install the appliance image as a virtual machine or instance on a supported virtualization environment or cloud provider. See the [Installation and Upgrade](#) section for information on different supported *Red Hat CloudForms* deployment methods.

Whichever deployment method you choose, ensure that *Red Hat CloudForms* is configured with connectivity to the OpenStack management network.

TIP

See [Uploading the Appliance on OpenStack](#) for instructions on deploying *Red Hat CloudForms* as an instance on the overcloud.

3.2. CONFIGURING RED HAT CLOUDFORMS

After deploying the appliance, log in with the root password **smartvm**. If you deployed the appliance as a virtual machine, you can log in through **virsh**:

```
[root@kvm-host ~]# virsh console my-cfme
Connected to domain my-cfme
...
Welcome to the CFME Virtual Appliance.

You can browse to http://localhost.localdomain/

Red Hat Enterprise Linux Server 7.2 (Maipo)
Kernel 3.10.0-327.36.1.el7.x86_64 on an x86_64
localhost login: root
Password:
Last login: Thu Oct 13 23:03:53 on tty2
```


Welcome to the Appliance Console

For a menu, please type: appliance_console
[root@localhost ~]#

3.3. CONFIGURING GENERAL APPLIANCE SETTINGS

After logging in, you can use the following menu items for advanced configuration of the appliance:

- Use **Set DHCP Network Configuration** to use DHCP to obtain the IP address and network configuration for your Red Hat CloudForms appliance. The appliance is initially configured as a DHCP client with bridged networking.
- Use **Set Static Network Configuration** if you have a specific IP address and network settings you need to use for the Red Hat CloudForms appliance.
- Use **Test Network Configuration** to check that name resolution is working correctly.
- Use **Set Hostname** to specify a hostname for the Red Hat CloudForms appliance.



IMPORTANT

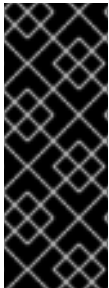
A valid fully qualified hostname for the Red Hat CloudForms appliance is required for SmartState analysis to work correctly,

- Use **Set Timezone** to configure the time zone for the Red Hat CloudForms appliance.
- Use **Set Date and Time** to configure the date and time for the Red Hat CloudForms appliance.
- Use **Restore Database from Backup** to restore the Virtual Management Database (VMDB) from a previous backup.
- Use **Setup Database Region** to create regions for VMDB replication.
- Use **Configure Database** to configure the VMDB. Use this option to configure the database for the appliance after installing and running it for the first time.
- Use **Configure Database Replication** to configure a primary or standby server for VMDB replication.
- Use **Configure Database Maintenance** to configure the VMDB maintenance schedule.
- Use **Configure Application Database Failover Monitor** to start or stop VMDB failover monitoring.
- Use **Extend Temporary Storage** to add temporary storage to the appliance. The appliance formats an unpartitioned disk attached to the appliance host and mounts it at `/var/www/miq_tmp`. The appliance uses this temporary storage directory to perform certain image download functions.
- Use **Configure External Authentication (httpd)** to configure authentication through an IPA server.
- Use **Generate Custom Encryption Key** to regenerate the encryption key used to encode plain text password.

- Use **Harden Appliance Using SCAP Configuration** to apply Security Content Automation Protocol (SCAP) standards to the appliance. You can view these SCAP rules in the `/var/www/miq/lib/appliance_console/config/scap_rules.yml` file.
- Use **Stop EVM Server Processes** to stop all server processes. You may need to do this to perform maintenance.
- Use **Start EVM Server Processes** to start the server. You may need to do this after performing maintenance.
- Use **Restart Appliance** to restart the Red Hat CloudForms appliance. You can either restart the appliance and clear the logs or just restart the appliance.
- Use **Shut Down Appliance** to power down the appliance and exit all processes.
- Use **Summary Information** to go back to the network summary screen for the Red Hat CloudForms appliance.
- Use **Quit** to leave the Red Hat CloudForms appliance console.

3.4. CONFIGURING A DATABASE FOR RED HAT CLOUDFORMS

Red Hat CloudForms supports the use of an internal or external database. The following instructions are suitable for configuring an *internal* database. For instructions on how to configure an external database instead, see [Configuring an External Database](#).



IMPORTANT

Before installing an internal database, add a disk to the infrastructure hosting your appliance. See the documentation specific to your infrastructure for instructions for adding a disk. As a storage disk usually cannot be added while a virtual machine is running, Red Hat recommends adding the disk before starting the appliance. Red Hat CloudForms only supports installing of an internal VMDB on blank disks; installation will fail if the disks are not blank.

1. Start the appliance and open a terminal console.
2. Enter the **appliance_console** command. The Red Hat CloudForms appliance summary screen displays.
3. Press **Enter** to manually configure settings.
4. Select **5) Configure Database** from the menu.
5. You are prompted to create or fetch an encryption key.
 - If this is the first Red Hat CloudForms appliance, choose **1) Create key**.
 - If this is not the first Red Hat CloudForms appliance, choose **2) Fetch key from remote machine** to fetch the key from the first appliance. For worker and multi-region setups, use this option to copy key from another appliance.

**NOTE**

All CloudForms appliances in a multi-region deployment must use the same key.

6. Choose **1) Create Internal Database** for the database location.
7. Choose a disk for the database. This can be either a disk you attached previously, or a partition on the current disk.

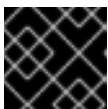
**IMPORTANT**

Red Hat recommends using a separate disk for the database.

If there is an unpartitioned disk attached to the virtual machine, the dialog will show options similar to the following:

- ```
1) /dev/vdb: 20480
2) Don't partition the disk
```

- Enter **1** to choose **/dev/vdb** for the database location. This option creates a logical volume using this device and mounts the volume to the appliance in a location appropriate for storing the database. The default location is **/var/opt/rh/rh-postgresql95/lib/pgsql**, which can be found in the environment variable **\$APPLIANCE\_PG\_MOUNT\_POINT**.
  - Enter **2** to continue without partitioning the disk. A second prompt will confirm this choice. Selecting this option results in using the root filesystem for the data directory (not advised in most cases).
8. Enter **Y** or **N** for **Should this appliance run as a standalone database server?**
    - Select **Y** to configure the appliance as a database-only appliance. As a result, the appliance is configured as a basic PostgreSQL server, without a user interface.
    - Select **N** to configure the appliance with the full administrative user interface.
  9. When prompted, enter a unique number to create a new region.

**IMPORTANT**

Creating a new region destroys any existing data on the chosen database.

10. Create and confirm a password for the database.

Red Hat CloudForms then configures the internal database.

### 3.5. CONFIGURING GENERAL RED HAT CLOUDFORMS SETTINGS

After configuring the general settings for the appliance and creating a database for it, you can now launch Red Hat CloudForms. To do this, use the **Start EVM Server Processes** option from the appliance console ([Section 3.3, “Configuring General Appliance Settings”](#)). Once you launch Red Hat CloudForms, note the **Hostname** and **IP Address** displayed on the appliance console screen.

Open the Red Hat CloudForms web-based user interface by accessing either **Hostname** and **IP Address** on a web browser. At the login screen, use the following credentials:

- Username: **admin**
- Password: **smartvm**



#### NOTE

You can also change the password of the **admin** account from the login screen. To do so, click the **Update Password** link.

You can access and configure most Red Hat CloudForms settings through the **Configuration** menu. You can access this menu through **Administrator | EVM > Configuration**.

The options under the **Configuration** menu allow you to configure global options for your Red Hat CloudForms environment, view diagnostic information, and view analytics on the servers in the environment. The menu displays the Red Hat CloudForms environment at the enterprise, zone, and server levels.

There are four main areas:

- **Settings**  
This menu allows you to configure global settings for your Red Hat CloudForms infrastructure. You can also create analysis profiles and schedules for these profiles.
- **Access Control**  
This menu contains options for configuring users, groups, roles, and tenants.
- **Diagnostics**  
This menu displays the status of your servers and their roles and provides access to logs.
- **Database**  
specify the location of your Virtual Machine Database (VMDB) and its login credentials.

## 3.6. REGISTERING YOUR APPLIANCE

Before you can access and apply package updates, you must register and subscribe the Red Hat CloudForms appliance to either Red Hat Content Delivery Network (CDN) or to a Red Hat Satellite server.

You need the following to register your appliance:

- Your Red Hat account login or Red Hat Network Satellite login
- A Red Hat subscription that covers your product

To register your appliance with Red Hat Subscription Management or Red Hat Satellite 6, first configure the region with your registration details. These settings will apply to all appliances in this region.

To configure registration for a region:

1. Log in to the appliance as the **admin** user.
2. From the settings menu, select **Configuration**.

3. Select **Region** in the accordion menu and click the **Red Hat Updates** tab.
4. Click **Edit Registration**.
5. Configure registration details for the Red Hat CloudForms appliance using one of two available options:
  - a. To register with Red Hat Subscription Management:
    - i. In **Register to**, select **Red Hat Subscription Management**.
    - ii. Enter the **Red Hat Subscription Management Address**. The default is `subscription.rhn.redhat.com`.
    - iii. Enter the **Repository Name(s)**. The default is `cf-me-5.8-for-rhel-7-rpms rhel-server-rhsc1-7-rpms`, which are the Red Hat CloudForms repository and the Red Hat Software Collections repository.
    - iv. To use a HTTP proxy, select **Use HTTP Proxy** and enter your proxy details.
    - v. Enter your Red Hat account information and click **Validate**.
    - vi. After your credentials are validated, click **Save**.
  - b. To register with Red Hat Satellite 6:
    - i. In **Register to**, select **Red Hat Satellite 6**.
    - ii. Enter the **Red Hat Satellite 6 Address**. The default is `subscription.rhn.redhat.com`.
    - iii. Enter the **Repository Name(s)**. The default is `cf-me-5.8-for-rhel-7-rpms rhel-server-rhsc1-7-rpms`, which are the Red Hat CloudForms repository and the Red Hat Software Collections repository.
    - iv. To use a HTTP proxy, select **Use HTTP Proxy** and enter your proxy details.
    - v. Enter your Red Hat Satellite account information and click **Validate**.
    - vi. After your credentials are validated, click **Save**.

Your appliance now appears in the **Appliance Updates** list as **Not registered**.

To register your appliance:

1. Select the appliance from the **Appliance Updates** list.
2. Click **Register** to subscribe the appliance and attach subscriptions.

Registering and attaching subscriptions takes a few minutes. The subscription process is complete when the appliance reports that it is **Subscribed** under **Update Status**, and **Registered** under **Last Message**.

You can now apply updates to your appliance.

**NOTE**

To update your appliances, see [Updating Red Hat CloudForms](#) in *Migrating to Red Hat CloudForms 4.5*.

## 3.7. CONFIGURING CLOUDFORMS METRICS FOR SMARTSTATE ANALYSIS

You can also configure CloudForms to perform a *SmartState Analysis*. This type of analysis collects details such as accounts, drivers, network information, hardware, and security patches on assets managed by the OpenStack provider. Enabling SmartState Analysis involves two steps:

1. [Section 3.7.1, “Configuring CloudForms Capacity and Utilization”](#), and
2. [Section 3.7.2, “Enabling SmartState Analysis”](#)

These steps are required to allow CloudForms to collect metrics from OpenStack and use them to perform a SmartState analysis. You can choose different servers to perform either function; the following sections assume that you will.

### 3.7.1. Configuring CloudForms Capacity and Utilization

For metrics collection to work properly, you also need to configure Red Hat CloudForms to allow for all three **Capacity & Utilization** server roles, which are available from the settings menu under **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*.

To enable these server roles:

1. From the settings menu, select **Configuration**, then select the server to configure from **Settings** → **Zone** in the accordion menu on the left.
2. Navigate to the **Server Roles** list in the **Server** → **Server Control** section. From there, set the required capacity and utilization roles to **ON**, namely:
  - a. **Capacity & Utilization Coordinator**
  - b. **Capacity & Utilization Data Collector**
  - c. **Capacity & Utilization Data Processor**
3. Click **Save**.

Data collection is enabled immediately. However, the first collection begins 5 minutes after the server is started, and every 10 minutes after that. Therefore, the longest the collection takes after enabling the Capacity & Utilization Collector role is 10 minutes. The first collection from a particular provider may take a few minutes since Red Hat CloudForms is gathering data points going one month back in time.

For more information, see [Capacity and Utilization Collection](#) from the *Deployment Planning Guide*.

### 3.7.2. Enabling SmartState Analysis

After enabling the required server roles, enable SmartState analysis. See [Smart State Analysis Support](#) from the Support Matrix and [Running a SmartState Analysis](#) in the Managing Providers guide for more information.

Enabling SmartState analysis is similar to [Section 3.7.1, “Configuring CloudForms Capacity and Utilization”](#), in that the procedure also involves enabling server roles on a specific server. To do so:

1. From the settings menu, select **Configuration**.
2. Select the server to configure from **Settings** → **Zone** in the left pane of the appliance.
3. Navigate to the **Server Roles** list in the **Server** → **Server Control** section. From there, set the appropriate SmartState roles to **ON**. Namely:
  - a. **SmartProxy**
  - b. **SmartState Analysis**
4. Click **Save**.



## CHAPTER 4. 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 4.1, “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 [Appendix A, 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 4.1, “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.

## 4.1. CONFIGURING THE UNDERCLOUD TO STORE EVENTS

To allow Red Hat CloudForms to receive events from a Red Hat OpenStack Platform environment, you must configure the **notification\_driver** option for the Compute service and Orchestration service in that environment. To do so, edit *undercloud.conf*, and set *store\_events* to *true* before installing the undercloud. See [Installing the Undercloud](#) and [Configuring the Director](#) in Red Hat OpenStack Platform *Director Installation and Usage* for related details.

## CHAPTER 5. ADDING AN OPENSTACK CLOUD PROVIDER

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.

When adding an OpenStack cloud or infrastructure provider, you can enable *tenant mapping* in Red Hat CloudForms to map any existing tenants from that provider. This means Red Hat CloudForms will create new cloud tenants to match each of existing OpenStack tenants; each new cloud tenant and its corresponding OpenStack tenant will have identical user memberships, quotas, access/security rules, and resources assignments.

During a provider refresh, Red Hat CloudForms will also check for any changes to the tenant list in OpenStack. Red Hat CloudForms will create new cloud tenants to match any new tenants, and delete any cloud tenants whose corresponding OpenStack tenants no longer exist. Red Hat 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 5.1, “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 [Appendix A, 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** drop down menu select **OpenStack**.
5. Select the appropriate **API Version** from the list. The default is **Keystone v2**.  
If you select **Keystone v3**, enter the **Keystone V3 Domain ID** that Red Hat CloudForms should use. This is the domain of the user account you will be specifying later in the **Default** tab. If domains are not configured in the provider, enter **default**.

**NOTE**

- With Keystone API v3, domains are used to determine administrative boundaries of service entities in OpenStack. Domains allow you to group users together for various purposes, such as setting domain-specific configuration or security options. For more information, see [OpenStack Identity \(keystone\)](#) in the Red Hat OpenStack Platform *Architecture Guide*.
- 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. By default, *tenant mapping* is disabled. To enable it, set **Tenant Mapping Enabled** to **Yes**.
7. 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*.

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

- e. 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.

- f. In the **Password** and **Confirm Password** fields, enter the password for the user.
  - g. Click **Validate** to confirm Red Hat CloudForms can connect to the OpenStack provider.
9. 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 5.1, “Configuring the Overcloud to Store Events”](#) for details.
    - If you prefer to use the AMQP Messaging bus instead, select **AMQP**. When you do: In **Hostname (or IPv4 or IPv6 address)** (of the **Events** tab, under **Endpoints**), enter the public IP or fully qualified domain name of the AMQP host.
      - In the **API Port**, set the public port used by AMQP. By default, OpenStack uses port 5672 for this.
      - In the **Username** field, enter the name of an OpenStack user with privileged access (for example, **admin**). Then, provide its corresponding password in the **Password** and **Confirm Password** fields.
      - Click **Validate** to confirm the credentials.
  10. 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*.

## 5.1. CONFIGURING THE OVERCLOUD TO STORE EVENTS

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

1. Log in to the undercloud host.

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

```
parameter_defaults:
 CeilometerStoreEvents: true
```

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

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

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

1. Log in to your Controller node.
2. Edit */etc/ceilometer/ceilometer.conf*, and specify the following option:

```
store_events = True
```

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

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

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

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

5. Restart the Compute service and Orchestration services:



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

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



## CHAPTER 6. PERFORMING A SMARTSTATE ANALYSIS

Red Hat CloudForms can analyze a cloud Instance or infrastructure host to collect metadata such as user accounts, applications, software patches, and other internal information. This key CloudForms feature is called SmartState Analysis. SmartState analysis can be initiated manually or automatically using Control Policies.

To manually initiate SmartState analysis on an instance:

1. Navigate to **Compute** → **Clouds** → **Instances**.
2. Click on an instance in the **All Instances by Provider** nsection.
3. Click  (**Configuration**), and then  (**Perform SmartState Analysis**). A pop-up window will appear to confirm the action.
4. Click **OK**. The SmartState analysis will be initiated for the selected instance.

To manually initiate SmartState analysis on an Infrastructure host:

1. Navigate to **Compute** → **Infrastructure** → **Providers**.
2. Select a node in the **Nodes** section.
3. Click  (**Configuration**), and then  (**Perform SmartState Analysis**). A pop-up window will appear to confirm the action.
4. Click **OK**. The SmartState analysis will be initiated for the selected node.

## CHAPTER 7. USING THE TOPOLOGY WIDGET

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

- The topology graph includes instances, nodes, and other cloud resources within the overall OpenStack cloud provider environment.
- Each entity in the graph displays a color indication of its status.
- Hovering over any individual graph element will display a summary of details for the individual element.
- Double-click the entities in the graph to navigate to their summary pages.
- It is possible to drag elements to reposition the graph.
- Click the legend at the top of the graph to show or hide entities.
- Click **Display Names** on the right-hand side of the page to show or hide entity names.

To view an OpenStack provider through the **Topology** widget:

1. Navigate to **Compute** → **Cloud** → **Providers**.
2. Click the desired OpenStack cloud provider for viewing the provider summary.
3. On the provider summary page, click **Topology** in the **Overview** box on the right-hand side of the page.



## CHAPTER 8. MANAGING POLICIES

Policies are used to manage your virtual environment. There are two types of policies available: compliance and control. Compliance policies are used to harden your virtual infrastructure, making sure that your security requirements are adhered to. Control policies are used to check for a specific condition and perform an action based on the outcome. For example:

- Prevent virtual machines from running without an administrator account.
- Prevent virtual machines from starting if certain patches are not applied.
- Configure the behavior of a production virtual machine to only start if it is running on a production host.
- Force a SmartState Analysis when a host is added or removed from a cluster.

CloudForms policies are associated with cloud instances using virtual machine analysis profiles. These are the steps required to create a custom virtual machine analysis profile, and assigning it to a cloud instance for use with SmartState analysis, via a control policy.





### NOTE

For more detailed information about CloudForms policies, see [Assigning a Custom Analysis Profile to a Virtual Machine](#) and [Policies and Profiles Guide](#).

The following subsections demonstrate how to create host compliance and instance control policies.

### 8.1. CREATING A HOST COMPLIANCE POLICY

The following procedure describes how to create a compliance policy that checks whether firewalls are enabled on infrastructure provider nodes. Nodes with disabled firewalls are marked *non-compliant*.

1. Navigate to **Control** → **Explorer**.
2. Expand the **Policies** accordion, and click **Compliance Policies**.
3. Select **Host Compliance Policies**.
4. Click  (**Configuration**),  (**Add a New Host/Node Compliance Policy**).
5. Type in a **Description** for the policy.

| Basic Information |                                     |
|-------------------|-------------------------------------|
| Description       | Check VM for Compliance             |
| Active            | <input checked="" type="checkbox"/> |

6. Uncheck **Active** if you do not want this policy processed even when assigned to a resource.
7. Add **Host / Node.Firewall Rules : Active CONTAINS "true"** to the *scope* of the policy . To do so:
  - a. In drop-down below the **Scope** section, choose **Field**. When you do, a new drop-down will

appear below it; from there, select **Host/Node.Firewall.Rules: Active**.

b. A new drop-down will appear; from there, select **true**.



c. Click  (**Commit expression element changes**) to add the scope.

8. In the **Notes** area, add a detailed explanation of the policy.

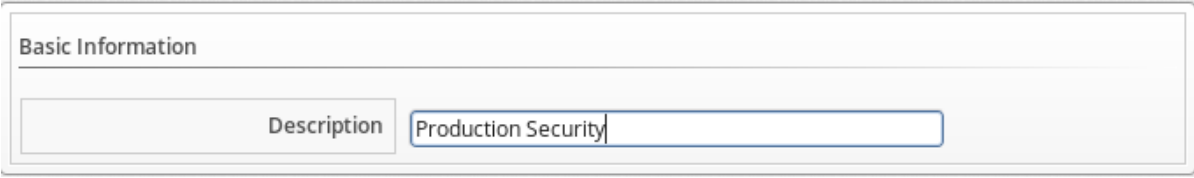
9. Click **Add**. The policy will be added and listed under **Host Compliance Policies** in the **Policies** accordion.

Next, create a *policy profile* and assign this new compliance policy to it:

1. Navigate to **Control** → **Explorer**.


2. Click on the **Policy Profiles** accordion, then click  (**Configuration**), then  (**Add a New Policy Profile**).

3. In the **Basic Information** area, type in a unique description for the policy profile.



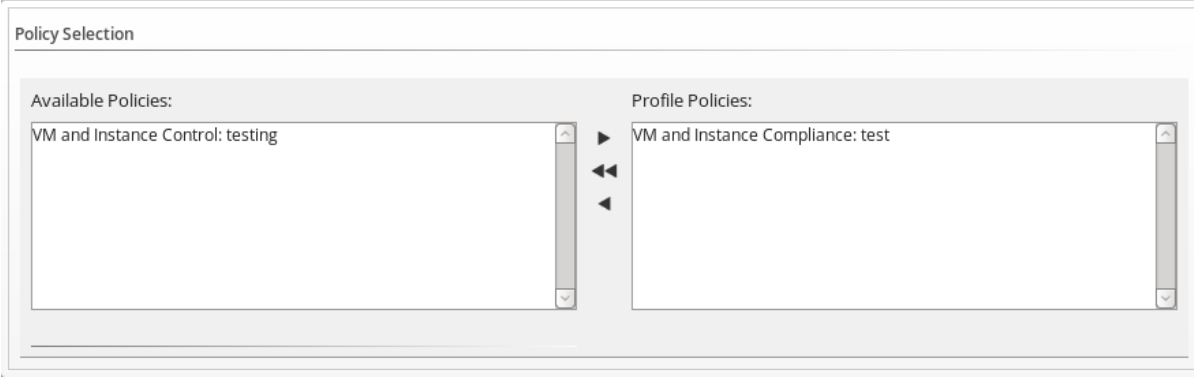
The screenshot shows the 'Basic Information' section of a policy profile configuration. There is a 'Description' label and a text input field containing the text 'Production Security'.

4. From **Available Policies** in the **Policy Selection** area select all the policies you need to apply to this policy profile. Use the **Ctrl** key to select multiple policies.



The screenshot shows the 'Policy Selection' area. On the left, under 'Available Policies', there is a list with two items: 'VM and Instance Compliance: test' and 'VM and Instance Control: testing'. On the right, under 'Profile Policies', the list is empty. Arrows between the two lists indicate the ability to move policies from available to the profile.

5. Click  to add the **Policies**.





The screenshot shows the 'Policy Selection' area after one policy has been added to the profile. The 'Available Policies' list now only contains 'VM and Instance Control: testing'. The 'Profile Policies' list now contains 'VM and Instance Compliance: test'.

6. Add to the **Notes** area if required.




7. Click **Add**.

At this point, you can now add the new policy profile to the infrastructure provider hosts:



1. Navigate to **Compute** → **Infrastructure** → **Providers**, verify the provider you need to assign the policy profiles to.
2. Click  (**Policy**), and then click  (**Manage Policies**).
3. From the **Select Policy Profiles** area, you can click on the triangle next to a desired policy profile to expand it and see its member policies.
4. Check the policy profiles you require to apply to the provider. It turns blue to show its assignment state has changed.
5. Click **Save**.

## 8.2. CREATING A VIRTUAL MACHINE CONTROL POLICY

The process of creating a *control policy* is similar to that of a compliance policy. A control policy is driven by events after certain conditions are met. The following control policy will start a SmartState analysis on an instance every 24 hours:



1. Navigate to **Control** → **Explorer**.
2. Expand the **Policies** accordion, and click **Control Policies**.
3. Select **Vm Control Policies**.
4. Click  (**Configuration**), then  (**Add a New VM and Instance Control Policy**).
5. Enter a **Description**. This will be the name given to your VM control policy.
6. Uncheck **Active** if you do not want this policy processed even when assigned to a resource.
7. Add **VM and Instance : Last Analysis Time IS "Yesterday"** to the scope of the policy. To do so:
  - a. In drop-down below the **Scope** section, choose **Field**. When you do, a new drop-down will appear below it; from there, select **VM and Instance : Last Analysis Time**.
  - b. A new drop-down will appear; from there, select **true**.
  - c. Click  (**Commit expression element changes**) to add the scope.
8. Click **Add**. The policy is added and listed under **Vm Control Policies** in the **Policies** accordion.

You can now associate events, conditions, and actions to this control policy. To do so:



1. Navigate to **Control** → **Explorer**.
2. Click the **Policies** accordion, and select the control policy you just created.
3. Click  (**Configuration**),  (**Edit this Policy's Condition assignments**).
4. In the **VM Operation** section, select **VM Power On**.

5. Click **Save**. The **VM Power On** event should appear under your policy.



You can now associate an action to the **VM Power On** event. To do so:

1. Select the **VM Power On** event.
2. Click  (**Configuration**), then  (**Edit Actions for this Policy Event**).
3. In the **Order of Actions if ALL Conditions are True** section, select **Generate Log Message** and **Initiate SmartState Analysis for VM**.
4. Click **Save**.

Next, create a policy profile and assign this new control policy to it:

1. Navigate to **Control** → **Explorer**.
2. Click on the **Policy Profiles** accordion, then click  (**Configuration**), then  (**Add a New Policy Profile**).
3. Enter **Most Recent SmartState** in the **Description** field.
4. In the **Policy Selection** area, choose the control policy you created earlier. This should have **VM and Instance Control** in its name. Add this policy to the **Profile Policies** box.
5. Click **Add**.

At this point, you should now be able to add the policy profile to the cloud providers.



1. Navigate to **Compute** → **Cloud** → **Providers**.
2. Select the overcloud you added in [Chapter 5, Adding an OpenStack Cloud Provider](#).
3. Click  (**Policy**), then  (**Manage Policies**).
4. Under **Select Policy Profiles**, select **Most Recent SmartState**.
5. Click **Save**.

## CHAPTER 9. MANAGING INSTANCES

Cloud instance provisioning goes through three phases:

1. **Request:** This includes ownership information, tags, virtual hardware requirements, the operating system, and any customization required. See [Provisioning Requests](#) from the [Provisioning Virtual Machines and Hosts](#) guide for more details.
2. **Approval:** Provisioning requests are then approved or denied. This phase can happen automatically or manually. See [Provisioning Request Approval Methods](#) from the [Provisioning Virtual Machines and Hosts](#) guide for more details.
3. **Provision:** Approved provisioning requests are executed. See [Working with Provisioning Requests](#) from the [Provisioning Virtual Machines and Hosts](#) guide for more details.

### 9.1. PROVISIONING AN OPENSTACK INSTANCE FROM AN IMAGE

1. Navigate to **Compute** → **Clouds** → **Instances**.
2. Click  (**Lifecycle**), then click  (**Provision Instances**).
3. Select an OpenStack image from the list presented. These images must be available on your OpenStack provider.
4. Click **Continue**.
5. On the **Request** tab, enter information about this provisioning request. In **Request Information**, type in at least a first and last name and an email address. This email is used to send the requester status emails during the provisioning process for items such as auto-approval, quota, provision complete, retirement, request pending approval, and request denied. The other information is optional. If the Red Hat CloudForms Server is configured to use LDAP, you can use the **Look Up** button to populate the other fields based on the email address.



#### NOTE

Parameters with a \* next to the label are required to submit the provisioning request. To change the required parameters, see [Appendix B, Customizing Provisioning Dialogs](#).

6. Click the **Purpose** tab to select the appropriate tags for the provisioned instance.
7. Click the **Catalog** tab for basic instance options.
  - a. To change the image to use as a basis for the instance, select it from the list of images.
  - b. Select the **Number of Instances** to provision.
  - c. Type a **Instance Name** and **Instance Description**.
8. Click the **Environment** tab to select the instance's **Tenant**, **Availability Zones**, **Cloud Network**, **Security Groups**, and **Public IP Address**. If no specific Tenant is required, select the **Choose Automatically** checkbox.
9. Click the **Properties** tab to set provider options such as flavors and security settings.

- a. Select a flavor from the **Instance Type** list.
  - b. Select a **Guest Access Key Pair** for access to the instance. For more information about key pairs, see [Appendix D, Managing Keypairs](#).
10. Click the **Volumes** tab to provision any volumes with the instance. Volumes are useful for augmenting ephemeral storage of instances with persistent, general-purpose block storage:
  - a. Fill in the **Volume Name** and **Size (gigabytes)** fields.
  - b. If you want the volume to be deleted once the instance terminates (thereby making it non-persistent), check **Delete on Instance Terminate**.
  - c. To provision and add multiple volumes to the instance, click **Add Volume**. Doing so will add new fields you can fill in.  
For more information about persistent storage in OpenStack, see the Red Hat OpenStack Platform *Storage Guide*.
11. Click the **Customize** tab to set additional instance options.
  - a. Under **Credentials**, enter a **Root Password** for the **root** user access to the instance.
  - b. Enter a **IP Address Information** for the instance. Leave as **DHCP** for automatic IP assignment from the provider.
  - c. Enter any **DNS** information for the instance if necessary.
  - d. Select a **Customize Template** for additional instance configuration. Select from the Cloud-Init scripts stored on your appliance.
12. Click the **Schedule** tab to set the provisioning and retirement date and time.
  - a. In **Schedule Info**, choose whether the provisioning begins upon approval, or at a specific time. If you select **Schedule**, you will be prompted to enter a date and time.
  - b. In **Lifespan**, select whether to power on the instances after they are created, and whether to set a retirement date. If you select a retirement period, you will be prompted for when to receive a retirement warning.
13. Click **Submit**.

The provisioning request is sent for approval. For the provisioning to begin, a user with the admin, approver, or super admin account role must approve the request. The admin and super admin roles can also edit, delete, and deny the requests. You will be able to see all provisioning requests where you are either the requester or the approver.

After submission, the appliance assigns each provision request a **Request ID**. If an error occurs during the approval or provisioning process, use this ID to locate the request in the appliance logs. The Request ID consists of the region associated with the request followed by the request number. As regions define a range of one trillion database IDs, this number can be several digits long.

### Request ID Format

Request 99 in region 123 results in Request ID 1230000000000099.

## CHAPTER 10. MANAGING STORAGE

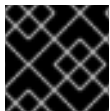
Two types of storage managers are currently available to Red Hat CloudForms: OpenStack Block Storage (**openstack-cinder**) and OpenStack Object Storage (**openstack-swift**). OpenStack Block Storage provisions and manages block storage, whereas OpenStack Object Storage manages object storage within the cloud. These storage managers are discovered automatically by Red Hat CloudForms after adding an OpenStack cloud provider.

For more information, see [Storage Managers](#) from the [Managing Providers](#) guide.

### 10.1. MANAGING BLOCK STORAGE



The OpenStack Block Storage service (**openstack-cinder**) provides and manages persistent block storage resources that OpenStack infrastructure instances can consume. CloudForms provides an interface for managing these resources (volumes, volume backups, and volume snapshots).

To create a volume:





#### IMPORTANT

After creating a volume, only the volume name can be edited.



1. Navigate to **Storage** → **Block Storage** → **Volumes**.
2. Click  (**Configuration**), then click  (**Add a new Cloud Volume**).
3. Select the OpenStack Block Storage manager from the **Storage Manager** list.
4. Enter a **Volume Name**.
5. Enter the size of the volume in gigabytes (GB).
6. Under **Placement**, select the cloud tenant to attach it to.
7. Click **Add**.

The volume appears in the list of volumes after it has been provisioned.



To attach a volume to an instance (for example, one created through [Section 9.1, “Provisioning an OpenStack Instance from an Image”](#)):

1. Navigate to **Storage** → **Block Storage** → **Volumes**.
2. Select the volume to attach.
3. Click  (**Configuration**), then click  (**Attach selected Cloud Volume to an Instance**) to open the **Attach Cloud Volume** screen.
4. Select an instance from the list.
5. Optionally, enter a **Device Mountpoint**.
6. Click **Attach**.

To view a timeline of storage manager events:

1. Navigate to **Storage** → **Storage Managers**.
2. Select your OpenStack Cinder manager to go to the Cinder manager's summary page.
3. Click  (**Monitoring**), and then  (**Timelines**) to view the events timeline for the manager.
4. A timeline of either management events or policy events can be viewed.
  - a. To view management events, select **Management Events**.
  - b. Specify the type of event to view.
  - c. Specify the timeline for the events to view.
  - d. Click **Apply**.
5. To view policy events, select **Policy Events**.
  - a. Specify if you want to view successful events, failed events, or both.
  - b. Specify the timeline for the events to view.
  - c. Click **Apply**.

To back up a volume:

1. Navigate to **Storage** → **Block Storage** → **Volumes**.
2. Click the volume you want to back up to open the volume's summary page.
3. Click  (**Configuration**), then click  (**Create a Backup of this Cloud Volume**).
4. Enter a name for the backup in **Backup Name**.
5. (Optional) Select **Incremental?** to take an incremental backup of the volume instead of a full backup.



#### NOTE

You can take an incremental backup of a volume if you have at least one existing full backup of the volume. An incremental volume saves resources by capturing only changes made to the volume since its last backup. See [Create an Incremental Volume Backup](#) in the *Storage Guide* for more information.

6. Click **Save**.

View a volume's backups by clicking **Cloud Volume Backups** on the volume's summary page.





#### NOTE

See [Back Up and Restore a Volume](#) in the *Storage Guide* for more information about backups.



To take a volume snapshot:

1. Navigate to **Storage** → **Block Storage** → **Volumes**.
2. Click the volume to snapshot to open the volume's summary page.
3. Click  (**Configuration**), then click  (**Create a Snapshot of this Cloud Volume**).
4. Enter a name for the snapshot in **Snapshot Name**.
5. Click **Save**.

Click **Cloud Volume Snapshots** on the summary page of a volume to view the snapshots for that volume.



#### NOTE

See [Create, Use, or Delete Volume Snapshots](#) in the *Storage Guide* for more information about snapshots.

For more information about available options for block storage resources in CloudForms, see [OpenStack Block Storage Managers](#) (from the [Managing Providers](#) guide).

## 10.2. MANAGING OBJECT STORAGE

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

To view the summary page of an object store:

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 11. CATALOGS AND SERVICES

In [Section 9.1, “Provisioning an OpenStack Instance from an Image”](#), you provisioned instance manually by entering values in provisioning dialogs such as name, size, image, CPUs, etc. *Catalogs* are used to create groups of instances for provisioning. CloudForms enables users to provision instances via a single **Order** button.

Creating a *service catalog* involves:

1. Creating a **Service Dialog**. This is a UI interface element that allows users to interact with the service (for example, a drop-down list).
2. Creating a **Catalog Item** for each instance that will be part of the service.
3. Creating a *method* for the **Service Dialog**. This method defines what each option means to each individual cloud instances for the service. This method is called from a service provisioning instance in the **Automate** model.











### NOTE

For more information about catalogs and services, see [Catalogs and Services](#) from the [Provisioning Virtual Machines and Hosts](#) guide.

### 11.1. CREATING A SERVICE DIALOG

When provisioning a service, input will be needed from the requester. **Service Dialogs** are used to take input from the user. This input is connected to a method in the **Automate** model that defines how user input is translated into the provision request. Before creating a **Service Dialog**, be sure to plan what items you need the user to input.

1. Navigate to **Automate** → **Customization**.
2. Click the **Service Dialogs** accordion.
3. Click  (**Configuration**), and then  (**Add a new Dialog**).
4. In **Dialog Information**, enter a **Label** and **Description**. Check the boxes for the buttons you want available at the bottom of the dialog form. The description will appear as hover text. As you enter the **Label** of the dialog, it should appear in the **Dialog** pane on the left.
  - a. Click  (**Add**), then  (**Add a New Tab to this Dialog**).
  - b. Enter a **Label** and **Description** for this tab.  
As you enter the **Label** of the tab, it should appear in the **Dialog** pane on the left under the dialog you are creating.
  - c. Click  (**Add**), then  (**Add a New Box to this Tab**).
  - d. Enter a **Label** and **Description** for this box.  
As you enter the **Label** of the box, it should appear in the **Dialog** pane on the left under the tab you are creating.
5. Add an element to this box. Elements are controls that accept input.

- a. Click  (**Add**), then  (**Add a New Element to this Box**).
- b. Enter a **Label**, **Name**, and **Description** for this element.



### IMPORTANT

**Name** must use only alphanumeric characters and underscores without spaces. It is also used to retrieve the value of this element in the method used with the dialog and must start with **dialog\_service\_type**

- c. Select a **Type** for an element type. All **Type** options have a **Required** and **Default Value** field. Check **Required** or set **Required** to **true** if the element is required to proceed. You can also specify a default value. The rest of the options presented are based on which type of element you select.



| Element Types          | Additional Info                                                                                                                                                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check Box              | Check <b>Default Value</b> if you want this check box checked by default.                                                                                                                                                                                       |
| Date Control           | Use <b>Date Control</b> to create a field where users can select a date. If you want users to be able to select a date and time, use the <b>Date/Time Control</b> option.                                                                                       |
| Date/Time Control      | Use <b>Date/Time Control</b> to create a field where users can select a date and time. Only one <b>Date Control</b> or <b>Date/Time Control</b> element can be present in a dialog.                                                                             |
| Drop Down Dynamic List | Use <b>Drop Down Dynamic List</b> if you want the list options to be created using automate methods. Use <b>Entry Point (NS/Cls/Inst)</b> to select an automate instance. Check <b>Show Refresh Button</b> to allow users to refresh the list options manually. |
| Radio Button           | This element type serves the same purpose as <b>Drop Down List</b> but displays options using radio buttons.                                                                                                                                                    |
| Tag Control            | Select a <b>Category</b> of tags you want assigned to the virtual machines associated with this service dialog. Check <b>Single Select</b> if only one tag can be selected.                                                                                     |
| Text Area Box          | Provides text area for users to enter some text. You can also leave a message to users by typing in the <b>Default Value</b> field or leave it as blank.                                                                                                        |
| Text Box               | This element type serves the same purpose as <b>Text Area Box</b> with the option to check <b>Protected</b> so the text is shown as asterisks (*), instead of plain text.                                                                                       |

6. Continue adding the dialog items you need. You can switch between dialogs, tabs, boxes, and elements by selecting their respective labels from the **Dialog** pane on the left.



- Click **Add**. Your dialog should appear in the **Service Dialogs** accordion.

## 11.2. CREATING A CATALOG

A catalog is a way to organize or categorize catalog items and bundles. Before you can associate a catalog item into a catalog, create an empty catalog first:

- Navigate to **Services** → **Catalogs**.
- Click the **Catalogs** accordion.
- Click  (**Configuration**), and then  (**Add a New Catalog**).
- Enter a **Name** and **Description**, leaving everything else blank.
- Click **Add**.

### 11.2.1. Creating a Catalog Item

- Navigate to **Services** → **Catalogs**.
- Click the **Catalog Items** accordion.
- Click  (**Configuration**), and then  (**Add a New Catalog Item**).
- Select **OpenStack** from the **Catalog Item Type** drop-down.
- In the **Basic Info** subtab:
  - Type a **Name/Description**.
  - Check **Display in Catalog** to edit **Catalog**, **Dialog**, and **Entry Point(NS/CIs/Inst)** options.
    - Provisioning Entry Point (Domain/NS/CIs/Inst)** requires you to select an Automate instance to run upon provisioning. Navigate to **ManageIQ/Service/Provisioning/State-Machines/ServiceProvision\_Template/CatalogItemInitialization** and click **Apply**.
    - Retirement Entry Point (Domain/NS/CIs/Inst)** requires you to select an Automate instance to run upon retirement. Navigate to **ManageIQ/Service/Provisioning/State-Machines/ServiceProvision\_Template/CatalogItemTermination** and click **Apply**.



#### NOTE

The entry point must be a State Machine since the **Provisioning Entry Point** list is filtered to only show State Machine class instances. No other entry points will be available from the **Provisioning Entry Point** field.

You can only choose from the catalogs and dialogs you have already created. If you haven't done so, leave the values blank and edit later.

- In the **Details** subtab, write a **Long Description** for the catalog item.
- In the **Request Info** subtab, select provisioning options that apply to the provider chosen.

8. Click **Add**.

### 11.2.2. Ordering a Catalog Item

1. Navigate to **Services** → **Catalogs**.
2. Click the **Service Catalogs** accordion, and select the service to provision.
3. Click **Order**.

## CHAPTER 12. REPORTS


Red Hat CloudForms provides a large group of default reports organized into categories. Each category has its own set of subfolders. These reports have been constructed to help you view the most commonly requested and significant data.



The categories of predefined reports available on Red Hat CloudForms are:


- **Configuration Management:** hardware, application, network, service, user account, operating system, and snapshot information for all of your items.
- **Migration Readiness:** information related to items required to migrate a virtual machine.
- **Operations:** free space on registered and unregistered virtual machines, power states for virtual machines, and SmartState analysis status.  
This category also provides reports relating to the operation of Red Hat CloudForms, such as user IDs and snapshots taken by Red Hat CloudForms.
- **VM Sprawl:** usage information and disk waste.
- **Relationships:** virtual machine, folder, and cluster relationships.
- **Events:** operations and configuration management events.
- **Performance by Asset Type:** performance of your virtual infrastructure.  
You must be capturing capacity and utilization data to get this information.
- **Running Processes:** information on processes running on a virtual machine.  
You must have domain credentials entered for the zone to collect the information for these reports, and the virtual machine must have been analyzed at least once.
- **Trending:** projections of datastore capacity, along with host CPU and memory use.
- **Tenants:** quotas report aggregated by each tenant that shows quota name, total quota, in use, allocated, and available. The report currently lists all tenants and there is no nesting information available by parent and child tenants.
- **Provisioning:** provisioning activity based on the approver, datastore, requester, and virtual machine.

For more detailed information on managing reports, see [Monitoring, Alerts, and Reporting](#).

### 12.1. GENERATING A SINGLE REPORT


1. Navigate to **Cloud Intel** → **Reports**
2. Click the **Reports** accordion and select the report you want to view.
3. Click  (**Queue**).
4. The report generation is placed on the queue and its status shows in the reports page.

|                                                                                     | Queued At             | Run At                | Source            | User ID | Status   |
|-------------------------------------------------------------------------------------|-----------------------|-----------------------|-------------------|---------|----------|
|  | 10/21/11 14:14:11 UTC |                       | Requested by user | admin   | Queued   |
|  | 10/21/11 14:00:08 UTC | 10/21/11 14:00:22 UTC | Requested by user | admin   | Finished |

5. Click  (**Reload current display**) to update the status.
6. When a report has finished generating, click on its row to view it.

## 12.2. SCHEDULING A REPORT

You can view historical data by creating reports on a scheduled basis. In addition, scheduled reports can be emailed directly to users:

1. Navigate to **Cloud Intel** → **Reports**
2. Click the **Reports** accordion and select the report you want to view.
3. Click  (**Configuration**), then **Add a new Schedule**.
4. Fill in the **Basic Information** section.
5. Configure the **Report Selection**.
6. Configure the report's schedule and frequency in the **Timer** section.
7. Click **Save**.

## 12.3. VIEWING REPORTS

Once you have created a schedule for a report, you can view it at any time after the first scheduled time has occurred.

1. Navigate to **Cloud Intel** → **Reports**.
2. Click the **Saved Reports** accordion or the **Reports** accordion.
3. Click on the instance of the report you want to view.



## CHAPTER 13. CHARGEBACK

The *chargeback* feature allows you to calculate monetary virtual machine charges based on owner or company tag. To use this feature you must be collecting capacity and utilization data. For information on server control settings and capacity & utilization collection settings, see [Section 3.7.1, “Configuring CloudForms Capacity and Utilization”](#).

### 13.1. CREATING CHARGEBACK RATES

Red Hat CloudForms allows you to create your own set of computing and storage costs to use for billing.

Chargeback rates can be configured at a single rate or in tiers, where one rate is assigned to one usage range, and another rate is assigned to a different usage range. You can also assign fixed and variable rates per tier if desired.

1. Navigate to **Cloud Intel** → **Chargeback**.
2. Click the **Rates** accordion and select **Compute** to create a CPU chargeback rate.
3. Click  (**Configuration**) and  (**Add a new Chargeback Rate**).
4. Type in a **Description** for the chargeback rate.
5. Select **Currency** and fill in the **Rate Details**.

Rate Details

\* Caution: The value Range end will not be included in the tier.

| Group       | Description          | Per Time | Per Unit | Range |          | Rate  |          | Actions | Currency |
|-------------|----------------------|----------|----------|-------|----------|-------|----------|---------|----------|
|             |                      |          |          | Start | Finish   | Fixed | Variable |         |          |
| CPU         | Allocated CPU Count  | Hourly   |          | 0.0   | Infinity | 1.0   | 0.0      | Add     | USD      |
| CPU         | Used CPU             | Hourly   | MHz      | 0.0   | Infinity | 0.0   | 0.02     | Add     | USD      |
| Cpu Cores   | Used CPU Cores       | Hourly   |          | 0.0   | Infinity | 1.0   | 0.02     | Add     | USD      |
| Disk I/O    | Used Disk I/O        | Hourly   | KBps     | 0.0   | Infinity | 0.0   | 0.005    | Add     | USD      |
| Fixed       | Fixed Compute Cost 1 | Hourly   |          | 0.0   | Infinity | 0.0   | 0.0      | Add     | USD      |
| Fixed       | Fixed Compute Cost 2 | Hourly   |          | 0.0   | Infinity | 0.0   | 0.0      | Add     | USD      |
| Memory      | Allocated Memory     | Hourly   | MB       | 0.0   | Infinity | 0.0   | 0.0      | Add     | USD      |
| Memory      | Used Memory          | Hourly   | MB       | 0.0   | Infinity | 0.0   | 0.02     | Add     | USD      |
| Network I/O | Used Network I/O     | Hourly   | KBps     | 0.0   | 100.0    | 0.5   | 0.0      | Add     | USD      |
|             |                      |          |          | 100.0 | Infinity | 0.5   | 0.005    | Delete  |          |

6. Click **Add**.

### 13.2. ASSIGNING CHARGEBACK RATES

After assigning a chargeback rate, assign it to a cloud provider.






1. Navigate to **Cloud Intel** → **Chargeback**.
2. Click the **Assignments** accordion, and click either **Compute** or **Storage**.
3. In the **Basic Info** area, select **Selected Cloud/Infrastructure Providers**.
4. Select the chargeback rate you created in [Section 13.1, “Creating Chargeback Rates”](#).



5. Click **Save**.

## 13.3. CREATING A CHARGEBACK REPORT

Red Hat CloudForms allows you to create chargeback reports to monitor costs you charged.

1. Navigate to **Cloud Intel** → **Reports**.
2. Click the **Reports** accordion.
3. Click  (**Configuration**),  (**Add a new Report**).
4. On the **Columns** tab, fill out the **Basic Report Info** area.
  - Type a unique name in **Menu Name** for how you want the report described in the menu list.
  - Type the **Title** to display on the report.
5. Add fields in the **Configure Report Columns** area.
  - From the **Base the report on** list, select **Chargebacks**.
  - Select the fields to include in the report from the **Available Fields** list, then click  (**Move selected fields down**). In addition to the fields, you can also select any tags that you have created and assigned.
  - Change the order of the fields in the report by clicking  (**Move selected fields up**) or  (**Move selected fields down**).
6. Click the **Formatting** tab to set the size of paper for a PDF and column header format.
  - From the **PDF Output** area, select the page size from the **Page Size** list.
  - From **Specify Column Headers and Formats**, type the text to display for each field. For each numeric field, you can also set the numeric format.
7. Click the **Filter** tab to set filters for the data displayed in the report.
  - From **Chargeback Filters**, select how you want the costs to show, the tag category, the tag, and how you want the items grouped.
  - From **Chargeback Interval**, select the time interval. You must have a full interval worth of data in order to select an option other than **Partial** in the **Daily Ending With** list.
8. Click the **Preview** tab, and then **Load** to see what the report will look like.
9. When you are satisfied that you have the report that you want, click **Add** to create the new report.

The new report is created. To make the report accessible from the **Report** menu, you must add it to a report menu.

## APPENDIX A. 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.

## APPENDIX B. CUSTOMIZING PROVISIONING DIALOGS

The default set of provisioning dialogs shows all possible options. However, Red Hat CloudForms also provides the ability to customize which tabs and fields are shown. You can decide what fields are required to submit the provisioning request or set default values.

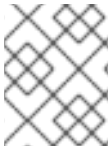
For each type of provisioning, there is a dialog that can be created to adjust what options are presented. While samples are provided containing all possible fields for provisioning, you can remove what fields are shown but cannot add new fields or tabs.

Edit the dialogs to:

1. Hide or show provisioning tabs.
2. Hide or show fields. If you hide an attribute, the default will be used, unless you specify otherwise.
3. Set default values for a field.
4. Specify if a field is required to submit the request.
5. Create custom dialogs for specific users.

## APPENDIX C. CREATING CUSTOM BUTTONS FOR CLOUD TENANTS

CloudForms also allows you to create *custom buttons* for cloud tenants. This is useful for providing shortcuts to functionalities and features frequently used by specific tenants.



### NOTE

This capability is made possible through the *Automate* model. See [Understanding the Automate Model](#) from the [Scripting Actions in CloudForms](#) guide for more details.

The following subsections summarize the two main steps for creating a custom button for cloud tenants.

### C.1. CREATING A CUSTOM BUTTON GROUP



A *button group* is a label for a collection of buttons under an *object type*. To create a button group:

1. Navigate to **Automate** → **Customization**.
2. Click the **Buttons** accordion.
3. From the **Object Types** tree, select the type of object you want to create the button group for.



### NOTE

When creating a button group for OpenStack tenants, select **Cloud Tenant** as your object type.

4. Click  (**Configuration**),  (**Add a new Button Group**).
5. Type in a **Button Group Text** and **Button Group Hover Text**, and select the **Button Group Image** you want to use.
6. If custom buttons have already been created, assign them to the button group. If not, see [Section C.2, “Creating a Custom Button”](#) to create custom buttons.
7. Click **Add**.

The button group will show in the **Cloud Tenant** object type. When it does, create a custom button for any tenant within the OpenStack Cloud (see [Section C.2, “Creating a Custom Button”](#)).



### C.2. CREATING A CUSTOM BUTTON

1. Navigate to **Automate** → **Customization**.
2. Click the **Buttons** accordion.
3. From the **Object Types** tree, select the type of object you want to create the button for.


**NOTE**

When creating a button for OpenStack tenants, select **Cloud Tenant** as your object type.

4. Click **Unassigned Buttons**.

5. Click  (**Configuration**), then  (**Add a new Button**).

**NOTE**

If  (**Add a new Button**) is not available, that means you have not created a button group for that object. To continue, create a button group first. See [Section C.1, “Creating a Custom Button Group”](#)

6. In **Action**, type in a **Button Text** and **Button Hover Text**, and select the **Button Image** you want to use.
7. Select a **Dialog** if applicable.
8. In **Object Details**, select **Request** from the **/System/Process/** dropdown. By default, the message is **create**. Do not change it.
9. Type in a **Request** name for the **/System/Process/Request** instance.
10. Type in the **Attribute/Value Pairs** fields if applicable.
11. Under **Visibility**, select which **Account Roles** you want to have access to this button.
12. Click **Add** when you have confirmed that the button accomplishes the task you want.



The button will show in the object type you added the button to. See [Invoking Automate](#) from the [Scripting Actions in CloudForms](#) guide for more in-depth coverage.

## APPENDIX D. MANAGING KEYPAIRS

Key pairs allow you to manage SSH access between a user and provisioned instance. For more information about key pairs in OpenStack, see [Manage Key Pairs](#) in the *Instances and Images Guide*.

To manage key pairs, navigate to **Compute** → **Clouds** → **Key Pairs**. From there, you can view a list of available key pairs. Click on a key pair to view its details.

To create a new key pair:

1. Navigate to **Compute** → **Clouds** → **Key Pairs**.
2. Click  (**Configuration**),  (**Add a new Key Pair**).
3. Enter a **Name** for the key pair.
4. If you want to use a public key, copy its contents into the **Public Key (optional)** field.
5. Select which cloud provider on which to create the key pair. The key pair will then be available for use by instances in that provider.
6. Click **Add**.