Red Hat CloudForms 4.5

Installing Red Hat CloudForms on Red Hat OpenStack Platform

How to install and configure Red Hat CloudForms on a Red Hat OpenStack Platform environment

Last Updated: 2018-10-10

Red Hat CloudForms 4.5 Installing Red Hat CloudForms on Red Hat OpenStack Platform

How to install and configure Red Hat CloudForms on a Red Hat OpenStack Platform environment

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

Legal Notice

Abstract

This guide provides instructions on how to install and configure Red Hat CloudForms on a Red Hat OpenStack Platform environment. If you have a suggestion for improving this guide or have found an error, please submit a Bugzilla report at http://bugzilla.redhat.com against Red Hat CloudForms Management Engine for the Documentation component. Please provide specific details, such as the section number, guide name, and CloudForms version so we can easily locate the content.

Table of Contents

CHAPTER 1. INSTALLING RED HAT CLOUDFORMS

Red Hat CloudForms is able to be installed and ready to configure in a few quick steps. After downloading Red Hat CloudForms as a virtual machine image template from the Red Hat Customer Portal, the installation process takes you through the steps of uploading the appliance to a supported virtualization or cloud provider.

IMPORTANT

After installing the Red Hat CloudForms appliance, you must configure the database for Red Hat CloudForms. See Section 2.3, “Configuring a Database for Red Hat CloudForms”.

1.1. OBTAINING THE APPLIANCE

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**.

1.2. UPLOADING THE APPLIANCE ON OPENSTACK

Log in to your OpenStack dashboard to upload your Red Hat CloudForms appliance.

1. Log in to the OpenStack dashboard.
2. In the **Project** tab, navigate to **Compute** → **Images**.
3. Click **Create Image**.
4. In **Name**, enter a name for the image.
5. From **Image Source** list, select **Image Location**. Note that currently only images available via an HTTP URL are supported.
6. In **Image Location**, add an external (HTTP) URL to load the image from. For example, **http://example.com/image.iso**.
7. From the **Format** list, select the image format. For example, **`ISO - Optical Disk Image`**.
8. Specify the **Architecture**. For example, **`i386`** for a 32-bit architecture or **`x86-64`** for a 64-bit architecture.
9. Leave the **Minimum Disk (GB)** and **Minimum RAM (MB)** fields empty.
10. Check the **Public** box to make the appliance available to all users.

11. Check the **Protected** box to protect the image from being accidentally deleted.

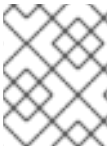
12. Click **Create Image**.

You have successfully uploaded the Red Hat CloudForms appliance.

The appliance image is placed in a queue to be uploaded. It may take some time before the Status of the image changes from Queued to Active.

1.3. ADDING A RULE TO A SECURITY GROUP

Security groups specify what IP traffic is allowed to reach an instance on its public IP address. Security group rules are processed before network traffic reaches firewall rules defined within the guest itself.



NOTE

In the default configuration, the default security group accepts all connections from the default source; all instances within the default group can talk to each other on any port.

1. From the OpenStack dashboard, navigate to **Project** → **Compute** → **Access & Security**.

2. Navigate to **Security Groups** → **Manage Rules** on the row for the default security group.

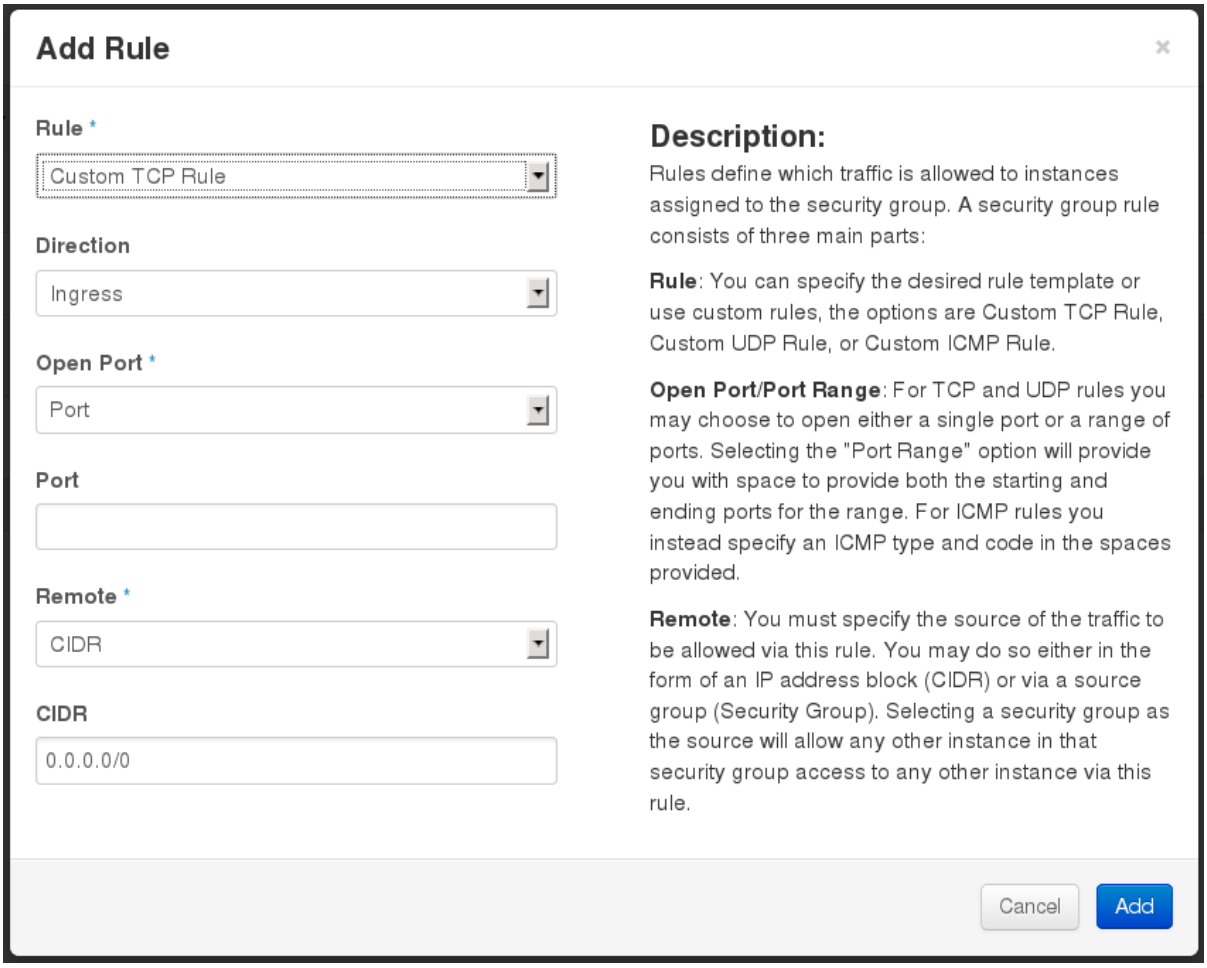
Manage Security Group Rules: default

Security Group Rules

+ Add Rule | ✖ Delete Rules

	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
☐	Egress	IPv4	Any	-	0.0.0.0/0 (CIDR)	Delete Rule
☐	Ingress	IPv6	Any	-	default	Delete Rule
☐	Ingress	IPv4	Any	-	default	Delete Rule
☐	Egress	IPv6	Any	-	::/0 (CIDR)	Delete Rule

3. Click **Add Rule**.



4. Configure the rule.

   a. Select **Rule** → **Custom TCP Rule**.

   b. Select **Direction** → **Ingress**.

   c. Select **Port** from the **Open Port** list.

   d. Specify **443** in the **Port** field.

   e. Select **CIDR** from the **Remote** list.

   f. Specify **`0.0.0.0/0`** in the **CIDR** field.

   g. Click **Add**.

1.4. CREATING A CUSTOM FLAVOR

A flavor is a resource allocation profile that specifies, for example, how many virtual CPUs and how much RAM can be allocated to an instance. You can, for example, run Red Hat CloudForms on a Red Hat OpenStack m1.large flavor, which specifies a virtual machine with 4 cores, 12 GB RAM, and 80 GB disk space. Creating a flavor to run Red Hat CloudForms is optional.

The following procedure demonstrates creating a flavor with the minimum requirements (4 cores, 12 GB RAM, 44 GB disk space) for Red Hat CloudForms. For more information about flavors, see the Red Hat OpenStack Platform Administration User Guide.

1. Log in to the OpenStack dashboard as admin.
2. In the **Admin** tab, navigate to **System** → **Flavors**.
3. Click **Create Flavor** to display the **Create Flavor** dialog.
4. Configure the settings to define a flavor that meets Red Hat CloudForms system requirements.
   a. Enter a name for the flavor.
   b. Enter the following settings:
      - **VCPUs**: 4
      - **RAM MB**: 8192
      - **Root Disk GB**: 45
      - **Ephemeral Disk GB**: 0
      - **Swap Disk MB**: 0
5. Click **Create Flavor**.

A new flavor specific to Red Hat CloudForms is created.

1.5. LAUNCHING THE INSTANCE

1. From the OpenStack dashboard, navigate to **Project** → **Compute** → **Instances**.
2. Click **Launch Instance**.
3. Enter a name for the instance.
4. Select the custom flavor for your instance. The flavor selection determines the computing resources available to your instance. The resources used by the flavor are displayed in the **Flavor Details** pane.
5. Enter **1** in the **Instance Count** field.
6. Select a boot option from the **Instance Boot Source** list:
   - **Boot from image** - displays a new field for **Image Name**. Select the image from the drop-down list.
   - **Boot from snapshot** - displays a new field for **Instance Snapshot**. Select the snapshot from the drop-down list.
   - **Boot from volume** - displays a new field for **Volume**. Select the volume from the drop-down list.
   - **Boot from image (creates a new volume)** - boot from an image and create a volume by choosing **Device Size** and **Device Name** for your volume. Some volumes can be persistent. To ensure the volume is deleted when the instance is deleted, select **Delete on Terminate**.
   - **Boot from volume snapshot (creates a new volume)** - boot from volume snapshot and create a new volume by choosing **Volume Snapshot** from the drop-down list and adding a **Device Name** for your volume. Some volumes can be persistent. To ensure the volume is

deleted when the instance is deleted, select **Delete on Terminate**.

7. Click **Networking** and select a network for the instance by clicking the **+** (plus) button for the network from **Available Networks**.

8. Click **Launch**.

1.6. ADDING A FLOATING IP ADDRESS

When you create an instance, Red Hat OpenStack Platform automatically assigns it a fixed IP address in the network to which the instance belongs. This IP address is permanently associated with the instance until the instance is terminated.

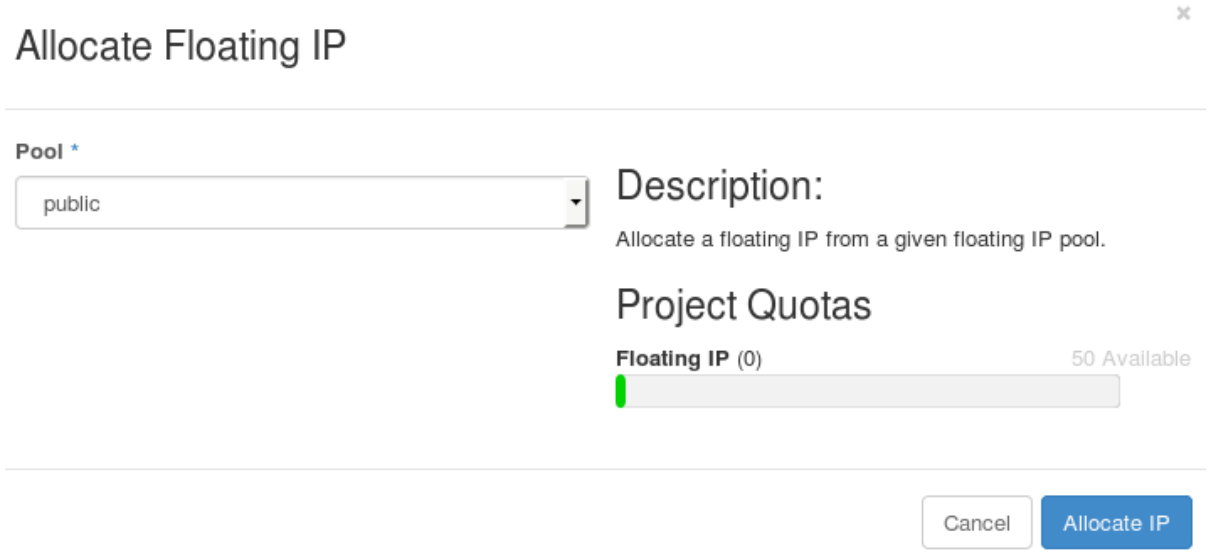
In addition to the fixed address, you can also assign a floating IP address to an instance. Unlike fixed IP addresses, you can modify floating IP addresses associations at any time, regardless of the state of the instances involved.

1. At the command-line on your RHEL OpenStack Platform host, create a pool of floating IP addresses using the **`nova-manage floating create`** command. Replace **IP_BLOCK** with the desired block of IP addresses expressed in CIDR notation.

```
$ nova-manage floating create IP_BLOCK
```

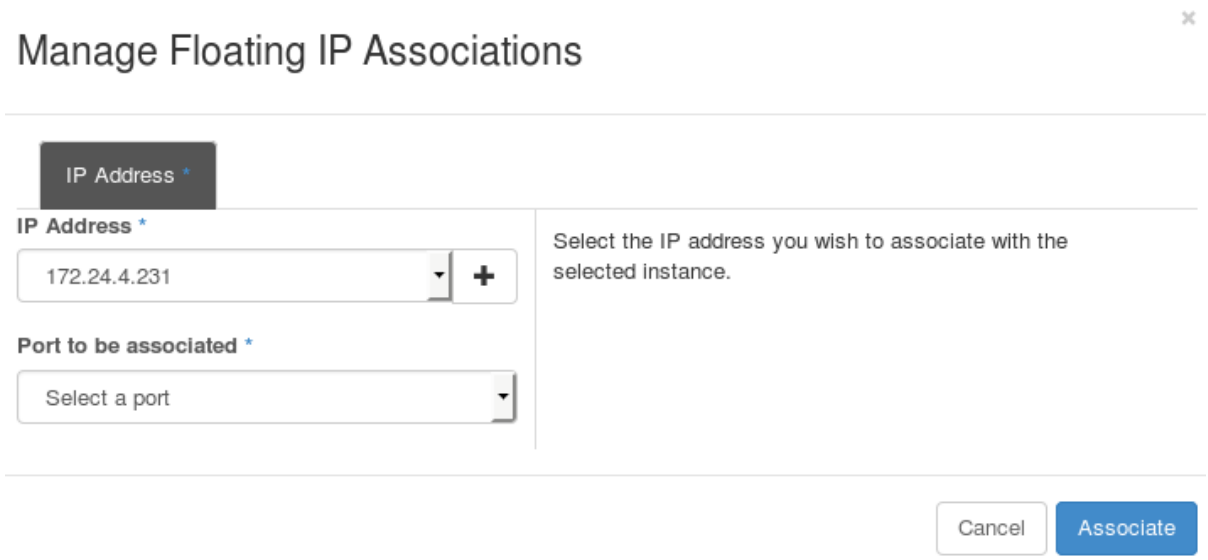
2. In the **Project** tab, navigate to **Compute** → **Access & Security**.

3. Click **Floating IPs** → **Allocate IP To Project**. The **Allocate Floating IP** window is displayed.



4. Click **Allocate IP** to allocate a floating IP from the pool. The allocated IP address appears in the **Floating IPs** table.

5. Select the newly allocated IP address from the **Floating IPs** table. Click **Associate** to assign the IP address to a specific instance.



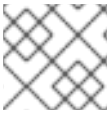
6. Select an instance with which to associate the floating IP Address.
7. Click **Associate** to associate the IP address with the selected instance.

NOTE

To disassociate a floating IP address from an instance when it is no longer required, click **Release Floating IPs**.

CHAPTER 2. CONFIGURING RED HAT CLOUDFORMS

Although the Red Hat CloudForms appliance comes configured to be integrated immediately into your environment, you can make some changes to its configuration.



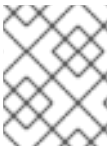
NOTE

The Red Hat CloudForms appliance is intended to have minimal configuration options.

2.1. CHANGING CONFIGURATION SETTINGS

The following procedure describes how to make changes to the configuration settings on the Red Hat CloudForms appliance.

1. Start the appliance and open a terminal console.
2. After starting the appliance, log in with a user name of **`root`** and the default password of **`smartvm`**. This displays the Bash prompt for the **`root`** user.
3. Enter the **`appliance_console`** command. The Red Hat CloudForms appliance summary screen displays.
4. Press **`Enter`** to manually configure settings.
5. Press the number for the item you want to change, and press **`Enter`**. The options for your selection are displayed.
6. Follow the prompts to make the changes.
7. Press **`Enter`** to accept a setting where applicable.



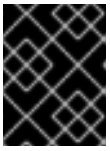
NOTE

The Red Hat CloudForms appliance console automatically logs out after five minutes of inactivity.

2.2. ADVANCED CONFIGURATION 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.

2.3. CONFIGURING A DATABASE FOR RED HAT CLOUDFORMS

Before using Red Hat CloudForms, configure the database options for it. Red Hat CloudForms provides two options for database configuration:

- Install an internal PostgreSQL database to the appliance
- Configure the appliance to use an external PostgreSQL database

2.3.1. Configuring an Internal Database

IMPORTANT

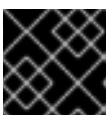
Before installing an internal database, add a disk to the infrastructure hosting your appliance. See the documentation specific to your infrastructure for instructions for adding a disk. As a storage disk usually cannot be added while a virtual machine is running, Red Hat recommends adding the disk before 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. After starting the appliance, log in with a user name of **`root`** and the default password of **`smartvm`**. This displays the Bash prompt for the **`root`** user.
3. Enter the **`appliance_console`** command. The Red Hat CloudForms appliance summary screen displays.
4. Press **Enter** to manually configure settings.
5. Select **5) Configure Database** from the menu.
6. 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.
7. Choose **1) Create Internal Database** for the database location.
8. 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).

9. 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.

10. When prompted, enter a unique number to create a new region.

IMPORTANT

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

11. Create and confirm a password for the database.

Red Hat CloudForms then configures the internal database. This takes a few minutes. After the database is created and initialized, you can log in to CloudForms.

2.3.2. Configuring an External Database

Based on your setup, you will choose to configure the appliance to use an external PostgreSQL database. For example, we can only have one database in a single region. However, a region can be segmented into multiple zones, such as database zone, user interface zone, and reporting zone, where each zone provides a specific function. The appliances in these zones must be configured to use an external database.

The **postgresql.conf** file used with Red Hat CloudForms databases requires specific settings for correct operation. For example, it must correctly reclaim table space, control session timeouts, and format the PostgreSQL server log for improved system support. Due to these requirements, Red Hat recommends that external Red Hat CloudForms databases use a **postgresql.conf** file based on the standard file used by the Red Hat CloudForms appliance.

Ensure you configure the settings in the **postgresql.conf** to suit your system. For example, customize the **shared_buffers** setting according to the amount of real storage available in the external system hosting the PostgreSQL instance. In addition, depending on the aggregate number of appliances expected to connect to the PostgreSQL instance, it may be necessary to alter the **max_connections** setting.

NOTE

- Red Hat CloudForms 4.x requires PostgreSQL version 9.4.
- Because the **`postgresql.conf`** file controls the operation of all databases managed by a single instance of PostgreSQL, do not mix Red Hat CloudForms databases with other types of databases in a single PostgreSQL instance.

1. Start the appliance and open a terminal console.
2. After starting the appliance, log in with a user name of **`root`** and the default password of **`smartvm`**. This displays the Bash prompt for the **`root`** user.
3. Enter the **`appliance_console`** command. The Red Hat CloudForms appliance summary screen displays.
4. Press **Enter** to manually configure settings.
5. Select **5) Configure Database** from the menu.
6. You are prompted to create or fetch a security 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.

NOTE

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

7. Choose **2) Create Region in External Database** for the database location.
8. Enter the database hostname or IP address when prompted.
9. Enter the database name or leave blank for the default (**`vmdb_production`**).
10. Enter the database username or leave blank for the default (**`root`**).
11. Enter the chosen database user's password.
12. Confirm the configuration if prompted.

Red Hat CloudForms will then configure the external database.

2.4. CONFIGURING A WORKER APPLIANCE

You can use multiple appliances to facilitate horizontal scaling, as well as for dividing up work by roles. Accordingly, configure an appliance to handle work for one or many roles, with workers within the appliance carrying out the duties for which they are configured. You can configure a worker appliance through the terminal. The following steps demonstrate how to join a worker appliance to an appliance that already has a region configured with a database.

1. Start the appliance and open a terminal console.

2. After starting the appliance, log in with a user name of **root** and the default password of **smartvm**. This displays the Bash prompt for the **root** user.

3. Enter the **appliance_console** command. The Red Hat CloudForms appliance summary screen displays.

4. Press **Enter** to manually configure settings.

5. Select **5) Configure Database** from the menu.

6. You are prompted to create or fetch a security key. Since this is not the first Red Hat CloudForms appliance, choose **2) Fetch key from remote machine**. For worker and multi-region setups, use this option to copy the security key from another appliance.

NOTE

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

7. Choose **3) Join Region in External Database** for the database location.

8. Enter the database hostname or IP address when prompted.

9. Enter the port number or leave blank for the default (**5432**).

10. Enter the database name or leave blank for the default (**vmdb_production**).

11. Enter the database username or leave blank for the default (**root**).

12. Enter the chosen database user's password.

13. Confirm the configuration if prompted.

CHAPTER 3. LOGGING IN AFTER INSTALLING RED HAT CLOUDFORMS

Once Red Hat CloudForms is installed, you can log in and perform administration tasks.

Log in to Red Hat CloudForms for the first time after installing by:

1. Navigate to the URL for the login screen. (https://xx.xx.xx.xx on the virtual machine instance)
2. Enter the default credentials (Username: **admin** | Password: **smartvm**) for the initial login.
3. Click **Login**.

3.1. CHANGING THE DEFAULT LOGIN PASSWORD

Change your password to ensure more private and secure access to Red Hat CloudForms.

1. Navigate to the URL for the login screen. (https://xx.xx.xx.xx on the virtual machine instance)
2. Click **Update Password** beneath the **Username** and **Password** text fields.
3. Enter your current **Username** and **Password** in the text fields.
4. Input a new password in the **New Password** field.
5. Repeat your new password in the **Verify Password** field.
6. Click **Login**.

APPENDIX A. APPENDIX

A.1. APPLIANCE CONSOLE COMMAND-LINE INTERFACE (CLI)

Currently, the **appliance_console_cli** feature is a subset of the full functionality of the **appliance_console** itself, and covers functions most likely to be scripted using the command-line interface (CLI).

1. After starting the Red Hat CloudForms appliance, log in with a user name of **root** and the default password of **smartvm**. This displays the Bash prompt for the root user.

2. Enter the **appliance_console_cli** or **appliance_console_cli --help** command to see a list of options available with the command, or simply enter **appliance_console_cli --option <argument>** directly to use a specific option.

Table A.1. Database Configuration Options

Option	Description
--region (-r)	region number (create a new region in the database - requires database credentials passed)
--internal (-i)	internal database (create a database on the current appliance)
--dbdisk	database disk device path (for configuring an internal database)
--hostname (-h)	database hostname
--port	database port (defaults to **5432**)
--username (-U)	database username (defaults to **root**)
--password (-p)	database password
--dbname (-d)	database name (defaults to **vmdb_production**)

Table A.2. v2_key Options

Option	Description
--key (-k)	create a new v2_key
--fetch-key (-K)	fetch the v2_key from the given host
--force-key (-f)	create or fetch the key even if one exists

Option	Description
--sshlogin	ssh username for fetching the v2_key (defaults to **root**)
--sshpassword	ssh password for fetching the v2_key

Table A.3. IPA Server Options

Option	Description
--host (-H)	set the appliance hostname to the given name
--ipaserver (-e)	IPA server FQDN
--ipaprincipal (-n)	IPA server principal (default: **admin**)
--ipapassword (-w)	IPA server password
--ipadomain (-o)	IPA server domain (optional). Will be based on the appliance domain name if not specified.
--iparealm (-l)	IPA server realm (optional). Will be based on the domain name of the ipaserver if not specified.
--uninstall-ipa (-u)	uninstall IPA client

NOTE

- In order to configure authentication through an IPA server, in addition to using **Configure External Authentication (httpd)** in the **appliance_console**, external authentication can be optionally configured via the **appliance_console_cli** (command-line interface).
- Specifying **--host** will update the hostname of the appliance. If this step was already performed via the **appliance_console** and the necessary updates made to **/etc/hosts** if DNS is not properly configured, the **--host** option can be omitted.

Table A.4. Certificate Options

Option	Description
--ca (-c)	CA name used for certmonger (default: **ipa**)
--postgres-client-cert (-g)	install certs for postgres client
--postgres-server-cert	install certs for postgres server

Option	Description
--http-cert	install certs for http server (to create certs/httpd* values for a unique key)
--extauth-opts (-x)	external authentication options

NOTE

The certificate options augment the functionality of the **`certmonger`** tool and enable creating a certificate signing request (CSR), and specifying **`certmonger`** the directories to store the keys.

Table A.5. Other Options

Option	Description
--logdisk (-l)	log disk path
--tmpdisk	initialize the given device for temp storage (volume mounted at **`/var/www/miq_tmp`**)
--verbose (-v)	print more debugging info

Example Usage

```
$ ssh root@appliance.test.company.com
```

To create a new database locally on the server using **`/dev/sdb`**:

```
# appliance_console_cli --internal --dbdisk /dev/sdb --region 0 --password
smartvm
```

To copy the v2_key from a host *some.example.com* to local machine:

```
# appliance_console_cli --fetch-key some.example.com --sshlogin root --
sshpassword smartvm
```

You could combine the two to join a region where *db.example.com* is the appliance hosting the database:

```
# appliance_console_cli --fetch-key db.example.com --sshlogin root --
sshpassword smartvm --hostname db.example.com --password
mydatabasepassword
```

To configure external authentication:

-

```
# appliance_console_cli --host appliance.test.company.com
                        --ipaserver ipaserver.test.company.com
                        --ipadomain test.company.com
                        --iparealm TEST.COMPANY.COM
                        --ipaprincipal admin
                        --ipapassword smartvm1
```

To uninstall external authentication:

```
# appliance_console_cli  --uninstall-ipa
```