Red Hat CloudForms 5.0

Installing Red Hat CloudForms on Amazon Elastic Compute Cloud (Amazon EC2)

How to install and configure Red Hat CloudForms on Amazon Elastic Compute Cloud (Amazon EC2)
Red Hat CloudForms 5.0 Installing Red Hat CloudForms on Amazon Elastic Compute Cloud (Amazon EC2)

How to install and configure Red Hat CloudForms on Amazon Elastic Compute Cloud (Amazon EC2)

Red Hat CloudForms Documentation Team
cloudforms-docs@redhat.com
Abstract
This guide provides instructions on how to install and configure Red Hat CloudForms on Amazon EC2. 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

1.1. OBTAINING THE APPLIANCE .......................................................... 3
1.2. REQUIREMENTS ............................................................................ 3
   1.2.1. CloudForms Requirements ...................................................... 3
   1.2.2. Amazon EC2 Requirements ................................................... 3
1.3. UPLOADING THE APPLIANCE TO AN AMAZON S3 BUCKET .......... 3
1.4. CONFIGURING AMAZON EC2 TO IMPORT THE APPLIANCE ......... 4
1.5. ACCESSING THE APPLIANCE CONSOLE ..................................... 6
1.6. CONFIGURING A DATABASE .......................................................... 6
   1.6.1. Configuring an Internal Database .......................................... 7
   1.6.2. Configuring an External Database ......................................... 8
1.7. CONFIGURING A WORKER APPLIANCE ..................................... 9

## APPENDIX A. APPENDIX

A.1. APPLIANCE CONSOLE COMMAND-LINE INTERFACE (CLI) ........ 11
Installing Red Hat CloudForms consists of the following steps:

1. Downloading the appliance for your environment as a virtual machine snapshot template.
2. Setting up a virtual machine based on the appliance.
3. Configuring the CloudForms appliance.

After you have completed all the procedures in this guide, you will have a working environment on which additional customizations and configurations can be performed.

### 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.
5. From the list of installers and images, click the Download Now link for CFME EC2 Virtual Appliance.

### 1.2. Requirements

Below are the two sets of requirements for installing Red Hat CloudForms on Amazon EC2.

#### 1.2.1. CloudForms Requirements

- 44 GB of space on the chosen datastore.
- 12 GB RAM.
- 4 vCPUs.

#### 1.2.2. Amazon EC2 Requirements

- An Amazon S3 bucket to store the disk image that will be imported to AWS as a snapshot.
- A VM import service role (IAM role) named vimport.

For information on creating an Amazon S3 bucket and a VM Import Service Role, see the Amazon EC2 documentation.

### 1.3. Uploading the Appliance to an Amazon S3 Bucket

From your local file system, you can now upload the CloudForms appliance VHD image obtained in Section 1.1, “Obtaining the Appliance” to the Amazon S3 bucket, using your choice of tool.
1.4. CONFIGURING AMAZON EC2 TO IMPORT THE APPLIANCE

**IMPORTANT**
These are the procedural steps as of the time of writing. For the latest information on importing a virtual machine as an image, see the Amazon EC2 documentation.

1. Install the AWS client on the computer you want to interact with the AWS API from.
   ```
   $ pip install awscli
   ```

2. Configure and download your AWS secret/access key by following the steps in the *Managing Access Keys for Your AWS Account* documentation.

3. Configure the AWS client with your access/secret key. For example:
   ```
   $ aws configure
   AWS Access Key ID [******]: ACCESS_KEY
   AWS Secret Access Key [******]: SECRET_KEY
   Default region name [None]:
   Default output format [None]:
   ```

4. Create the `trust-policy.json` file for the `vmimport` role. For example:
   ```json
   {
   "Version": "2012-10-17",
   "Statement": [
   { "Effect": "Allow",
     "Principal": { "Service": "vmie.amazonaws.com" },
     "Action": "sts:AssumeRole",
     "Condition": { "StringEquals": { "sts:ExternalId": "vmimport" } }
   }
   ]
   }
   ```

5. Create the `vmimport` role using the `trust-policy.json` file that you just created.
   ```
   $ aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json
   ```

   **NOTE**
   This user must have permissions to create and modify IAM roles.

6. Create the `role-policy.json` file. Be sure to use the exact S3 bucket name. For example:
   ```
   ```
"Version": "2012-10-17",
"Statement": [ 
  { 
    "Effect": "Allow",
    "Action": [ 
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  },
  { 
    "Effect": "Allow",
    "Action": [ 
      "s3:CreateBucket",
      "s3:DeleteBucket",
      "s3:DeleteObject",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource": ["arn:aws:s3:::BUCKET_TO_UPLOAD_IMAGE","arn:aws:s3:::BUCKET_TO_UPLOAD_IMAGE/*"]
  },
  { 
    "Effect": "Allow",
    "Action": [ 
      "iam:CreateRole",
      "iam:PutRolePolicy"
    ],
    "Resource": "*"
  },
  { 
    "Effect": "Allow",
    "Action": [ 
      "ec2:CancelConversionTask",
      "ec2:CancelExportTask",
      "ec2:CreateImage",
      "ec2:CreateInstanceExportTask",
      "ec2:CreateTags",
      "ec2:DeleteTags",
      "ec2:DescribeConversionTasks",
      "ec2:DescribeExportTasks",
      "ec2:DescribeExportImageTasks",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstances",
      "ec2:DescribeTags",
      "ec2:ExportImage",
      "ec2:ImportInstance",
      "ec2:ImportVolume",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ec2:ImportImage",
      "ec2:ImportSnapshot"
    ],
    "Resource": "*"
  }
]
7. Apply the `vmimport` role to the CloudForms appliance image you uploaded to the S3 bucket.

```
$ aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json
```

== Configuring Red Hat CloudForms

After installing CloudForms and running it for the first time, you must perform some basic configuration. To configure CloudForms, you must at a minimum:

1. Add a disk to the infrastructure hosting your appliance.
2. Configure the database.

Configure the CloudForms appliance using the internal appliance console.

1.5. ACCESSING THE APPLIANCE CONSOLE

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

1.6. CONFIGURING A DATABASE

CloudForms uses a database to store information about the environment. Before using CloudForms, configure the database options for it; CloudForms provides the following two options for database configuration:

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

1.6.1. 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/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.

### 1.6.2. 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 requires PostgreSQL version 9.5.
- 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.

### 1.7. 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.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--key (-k)</td>
<td>create a new v2_key</td>
</tr>
<tr>
<td>--fetch-key (-K)</td>
<td>fetch the v2_key from the given host</td>
</tr>
<tr>
<td>--force-key (-f)</td>
<td>create or fetch the key even if one exists</td>
</tr>
</tbody>
</table>
```
--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

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

**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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ca (-c)</td>
<td>CA name used for certmonger (default: ipa)</td>
</tr>
<tr>
<td>--postgres-client-cert (-g)</td>
<td>install certs for postgres client</td>
</tr>
<tr>
<td>--postgres-server-cert</td>
<td>install certs for postgres server</td>
</tr>
</tbody>
</table>
--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>
<thead>
<tr>
<th>Table A.5. Other Options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--logdisk (-l)</td>
<td>log disk path</td>
</tr>
<tr>
<td>--tmpdisk</td>
<td>initialize the given device for temp storage (volume mounted at <code>/var/www/miq_tmp</code>)</td>
</tr>
<tr>
<td>--verbose (-v)</td>
<td>print more debugging info</td>
</tr>
</tbody>
</table>

### 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
    --ipapincipal admin
    --ipapassword smartvm1
```
To uninstall external authentication:

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