



Red Hat CloudForms 4.2

Integration with Red Hat OpenShift Enterprise

**Adding Red Hat OpenShift Enterprise (with Metrics Enabled) as a Container
Provider**

Red Hat CloudForms 4.2 Integration with Red Hat OpenShift Enterprise

Adding Red Hat OpenShift Enterprise (with Metrics Enabled) as a Container Provider

Red Hat CloudForms Documentation Team

cloudforms-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 Red Hat OpenShift Enterprise container services (with metrics enabled) with Red Hat CloudForms. It is intended as an abridged reference for users already familiar with Red Hat CloudForms, Red Hat OpenShift Enterprise, and Red Hat Enterprise Linux.

Table of Contents

1. OVERVIEW	2
2. CONFIGURING OPENSIFT ENTERPRISE METRICS	2
2.1. Configuring Required Service Accounts	2
2.2. Choosing a Storage Option	3
2.3. Deploying the Metrics Components	4
2.4. Applying the Hawkular Metrics Settings to OpenShift Enterprise	4
3. RETRIEVING THE OPENSIFT ENTERPRISE MANAGEMENT TOKEN	5
4. CONFIGURING RED HAT CLOUDFORMS	5
4.1. Configuring CloudForms Capacity and Utilization	6
4.2. Enabling SmartState Analysis	6
5. ADDING THE OPENSIFT DEPLOYMENT AS A CONTAINER PROVIDER	7
6. CONTAINER IMAGE SCANNING	7
6.1. Configuring Image Scanning	7
6.2. Scheduling A Recurring Scan	8
6.3. Working with Images	8
6.3.1. Viewing Results	8
6.3.2. Manual Scanning	9
6.3.3. Evaluating Compliance	9
6.4. OpenSCAP Policy Profile	9
6.4.1. Customizing the Scanning Policy Profile	9
6.5. Controlling OpenShift Pod Execution	10
6.6. Reference	10

1. OVERVIEW

This guide provides a quick walkthrough on adding a Red Hat OpenShift Enterprise deployment to a Red Hat CloudForms container provider catalogue. Each procedure in this guide is covered in greater detail throughout other documents in the [Red Hat CloudForms](#) and [OpenShift Enterprise](#) product documentation; whenever appropriate, we will provide links to the corresponding sections for more detail. This deployment focuses on ensuring that CloudForms can collect metrics from the OpenShift Enterprise deployment upon integration.

This guide assumes that you have:

- Already deployed Red Hat CloudForms, and
- Already deployed OpenShift Enterprise.

For detailed information on how to deploy either product, see:

- [Red Hat CloudForms Installation and Configuration](#)
- [OpenShift Enterprise Installation and Configuration](#)



NOTE

When enabling metrics on OpenShift Enterprise, you can store your metrics data on *persistent* or *non-persistent* storage. With persistent storage, you need to provision a persistent volume specifically for this purpose. See [Persistent Volumes](#) from [OpenShift Enterprise Architecture](#) for more information.

The following sections will describe the required configuration for both products prior to integration ([Section 5, “Adding the OpenShift Deployment as a Container Provider”](#)).

2. CONFIGURING OPENSIFT ENTERPRISE METRICS

In order for CloudForms to collect node, pod, and container metrics on your OpenShift Enterprise, you must first enable *cluster metrics* on your OpenShift deployment. This involves running the OpenShift Metrics services inside your cluster. If cluster metrics are already enabled on OpenShift, skip this section and proceed to [Section 3, “Retrieving the OpenShift Enterprise Management Token”](#).



NOTE

This section is an abridged version of a more detailed chapter, namely [Enabling Cluster Metrics](#) from [OpenShift Enterprise Installation and Configuration](#). Refer to that chapter for more information.

2.1. Configuring Required Service Accounts

Cluster metrics requires the following service accounts:

1. **metrics-deployer**

2. heapster



IMPORTANT

If you deployed OpenShift using **openshift-ansible-3.0.20**, then the service account and roles required for enabling metrics will already be installed. You can skip this section and go to [Section 2.2, “Choosing a Storage Option”](#).

To create these accounts:

1. Log in as an administrator to any node within the OpenShift Enterprise cluster.
2. Open a terminal.
3. Switch to the **openshift-infra** project:

```
$ oc project openshift-infra
```

4. Create a service account for the Metrics Deployer (namely, **metrics-deployer**):

```
$ oc create -f - <<API
apiVersion: v1
kind: ServiceAccount
metadata:
  name: metrics-deployer
secrets:
- name: metrics-deployer
API
```

5. Configure the **metrics-deployer** account to have **edit** permissions to the **openshift-infra** project:

```
$ oadm policy add-role-to-user \
  edit system:serviceaccount:openshift-infra:metrics-deployer
```

The **metrics-deployer** account will be used by the Metrics Deployer, which is described in [Section 2.2, “Choosing a Storage Option”](#).

6. The **heapster** account will be automatically created later on in [Section 2.3, “Deploying the Metrics Components”](#). However, you should pre-emptively grant it **cluster-reader** permission to the **openshift-infra** project:

```
$ oadm policy add-cluster-role-to-user \
  cluster-reader system:serviceaccount:openshift-infra:heapster
```

2.2. Choosing a Storage Option

The *Metrics Deployer* installs and configures the components required for OpenShift Enterprise metrics. By default, the Metrics Deployer uses *self-signed certificates* to secure communication between components. This document assumes that you will use this default; for information on alternative secure communication setups, see [Using Secrets](#) from [OpenShift Enterprise Installation and Configuration](#).

Before deploying OpenShift metrics, choose a storage option:

Persistent storage

With *persistent storage*, OpenShift metrics will be stored on a persistent volume. This offers protection to metrics data by allowing it to survive a pod recreation or restart. OpenShift metrics requires a specifically configured persistent volume; see [Persistent Volumes](#) from [OpenShift Enterprise Architecture](#).

Non-persistent storage

With *non-persistent storage*, you no longer need to provision and configure a volume to store metric data. This makes the deployment easier; however, this option does not offer the same protection as persistent storage.

See [Metrics Data Storage](#) from [OpenShift Enterprise Installation and Configuration](#) for more information.

2.3. Deploying the Metrics Components

OpenShift Enterprise uses *Hawkular Metrics* as its metrics engine. The Metrics Deployer will install the Hawkular Metrics service; however, you need to provide an external hostname at which CloudForms can reach the Hawkular Metrics service. The base configuration of the Metrics Deployer are defined in `/usr/share/openshift/examples/infrastructure-templates/enterprise/metrics-deployer.yaml`.

After choosing a storage option, log in as an administrator to any node within the OpenShift Enterprise cluster. From there, open a terminal and run the corresponding command:

Deploying with persistent storage

```
$ oc new-app \
  -f /usr/share/openshift/examples/infrastructure-
templates/enterprise/metrics-deployer.yaml \
  -p HAWKULAR_METRICS_HOSTNAME=HAWKULARHOST
```

Deploying with non-persistent storage

```
$ oc new-app \
  -f /usr/share/openshift/examples/infrastructure-
templates/enterprise/metrics-deployer.yaml \
  -p HAWKULAR_METRICS_HOSTNAME=HAWKULARHOST \
  -p USE_PERSISTENT_STORAGE=false
```

For either command, replace *HAWKULARHOST* with the external hostname that CloudForms will use to reach the Hawkular Metrics service. *HAWKULARHOST* must be a fully-qualified domain name.

Either of these commands will deploy the required metrics components and create the necessary service accounts. In particular, the metrics components will be configured to also use the specified *HAWKULARHOST* as its public endpoint.

2.4. Applying the Hawkular Metrics Settings to OpenShift Enterprise

After deploying the metrics components, configure OpenShift Enterprise to use them. To do so:

1. Open the OpenShift Master Configuration file – namely, `/etc/origin/master/master-config.yaml`. For more information on this file, see [Master Configuration Files](#) from the [OpenShift Container Platform Installation and Configuration](#).
2. Add a `metricsPublicURL` parameter to the `assetConfig` section. Specify the *HAWKULARHOST* you specified in [Section 2.3, “Deploying the Metrics Components”](#):


```
assetConfig:
  ...
  metricsPublicURL: "https://HAWKULARHOST/hawkular/metrics"
```

3. Restart your OpenShift Enterprise deployment:

```
$ sudo systemctl restart atomic-openshift-master
```

3. RETRIEVING THE OPENSIFT ENTERPRISE MANAGEMENT TOKEN

After enabling cluster metrics on your OpenShift Enterprise deployment, retrieve the *management token* while you are still logged into the OpenShift Enterprise host. This will be required later in [Section 5](#), “Adding the OpenShift Deployment as a Container Provider”.

Refer to the procedure appropriate for your version of OpenShift Enterprise:

OpenShift Enterprise 3.2

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

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

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

OpenShift Enterprise 3.1

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

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

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

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

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

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

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

4. CONFIGURING RED HAT CLOUDFORMS

Configuring CloudForms involves two steps:

1. [Section 4.1, “Configuring CloudForms Capacity and Utilization”](#) , and

2. [Section 4.2, “Enabling SmartState Analysis”](#)

These steps are required to allow CloudForms to collect metrics from OpenShift Enterprise ([Section 2, “Configuring OpenShift Enterprise Metrics”](#)) and use them to perform a SmartState analysis. You can choose different servers to perform either function; the following sections assume that you will.

4.1. 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*.

4.2. Enabling SmartState Analysis



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

Enabling SmartState analysis is similar to [Section 4.1, “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**.

5. ADDING THE OPENSIFT DEPLOYMENT AS A CONTAINER PROVIDER

At this point, you should now be ready to add the OpenShift Deployment to Red Hat CloudForms as a container provider. To do so, prepare the token you retrieved earlier in [Section 3, “Retrieving the OpenShift Enterprise Management Token”](#) and follow the procedure below:

1. Navigate to **Compute** → **Containers** → **Providers**.
2. Click  (**Configuration**), then click  (**Add a New Containers Provider**).
3. Enter a **Name** for the provider.
4. From the **Type** list, select **OpenShift Enterprise**.
5. Enter the appropriate **Zone** for the provider. By default, the zone is set to **default**.
6. In the **Default** tab of the **Endpoints** section, enter the fully qualified domain name of the provider in the **Hostname (or IPv4 or IPv6 address)** field.
7. Enter the **Port** of the provider. The default port is **8443**.
8. In the **Token** and **Confirm Token** fields, enter token obtained earlier in [Section 3, “Retrieving the OpenShift Enterprise Management Token”](#).
9. Click **Validate** to confirm that the Red Hat CloudForms can connect to the OpenShift Enterprise provider using the provided token.
10. Next, click the **Hawkular** tab. From there, enter the **HAWKULARHOST** (from [Section 2.3, “Deploying the Metrics Components”](#)) in the **Hostname (or IPv4 or IPv6 address)** field.
11. Enter the **Port** of the **HAWKULARHOST**. The default port is **443**.
12. Click **Add**.

6. CONTAINER IMAGE SCANNING

6.1. Configuring Image Scanning

Red Hat CloudForms manages vulnerability scanning of container images. When an OpenShift provider is added, OpenShift images from the internal registry are discovered. To enable image scanning, perform the following configuration steps:

1. Navigate to **Compute** → **Containers** → **Providers**.
2. Select the checkboxes of the OpenShift providers on which to enable scanning.
3. From the **Policy** pull-down menu, click **Manage Policies**.
4. Select the **OpenSCAP profile** checkbox.
5. Click **Save**.

This action will trigger a SmartState analysis, or scan, of all images referenced by the OpenShift provider. The initial scan may take several hours to complete, depending on the number and size of images. OpenShift limits the number of scanning pods. Only three images can be scanned simultaneously.

6.2. Scheduling A Recurring Scan

Software vulnerability databases are updated frequently. To apply these updates, a rescan is required. To schedule a recurring scan of container images:

The screenshot shows the 'Adding a new Schedule' form in the Red Hat CloudForms interface. The left sidebar contains a navigation menu with the following items: Settings, CFME Region: Region 0 [0], Analysis Profiles, Zones, Schedules (selected), Access Control, Diagnostics, and Database. The main form area is titled 'Adding a new Schedule' and contains the following fields:

- Name:** OpenSCAP scan
- Description:** Perform vulnerability scan
- Active:** ☒
- Action:** Container Image Analysis
- Filter:** All Container Images for Contain (dropdown), OpenShift (dropdown)
- Timer Options:**
 - Run:** Weekly (dropdown) every Week (dropdown)
 - Time Zone:** (GMT+00:00) UTC (dropdown) * Changing the Time Zone will reset the Starting Date and Time fields below
 - Starting Date:** 05/14/2017 (calendar icon)
 - Starting Time (UTC):** 0 h 0 m

At the bottom right of the form are two buttons: 'Add' and 'Cancel'.

1. From the settings menu, select **Configuration**.
2. From **Settings** → **Zones** in the left pane of the appliance, select **Schedules**.
3. From the drop-down menu, click **Configuration** → **Add a new Schedule**.
4. Type an arbitrary **Name**.
5. Type an arbitrary **Description**.
6. Ensure the **Active** checkbox is selected.
7. In **Action**, select **Container Image Analysis**.
8. In **Filter**, select **All Container Images for Containers Provider**, **OpenShift**.
9. In **Run**, set the schedule as desired.
10. Set the **Time Zone**, **Starting Date**, and **Starting Time**.
11. Click **Add**.

6.3. Working with Images



6.3.1. Viewing Results

Image scanning results are displayed in each image summary page.








1. Select **Compute** → **Containers** → **Container Images**.

2. Click the desired image.

For an OpenSCAP HTML report, locate the **Configuration** section and select **OpenSCAP HTML**.

Configuration	
Packages	 284
OpenSCAP Results	 447
OpenSCAP HTML	Available
Last scan	Fri, 12 May 2017 17:43:26 +0000

For compliance and scanning history information, locate the **Compliance** section and note the **Status** field or select **Available** from the **History** field.

- v  **Compliance Check on:** 2017-05-12 17:44:05 UTC
 - >  **Policy:** Custom OSCAP
 - v  **Policy:** OpenSCAP
 -  **Condition:** Has high severity OpenSCAP rule results
- v  **Compliance Check on:** 2017-04-28 01:26:37 UTC
 - >  **Policy:** Custom OSCAP
 - >  **Policy:** OpenSCAP

6.3.2. Manual Scanning

SmartState analysis scanning may be initiated manually for images. From an image summary page, select **Configuration** → **Perform SmartState Analysis**. Refreshing the image page will reflect the latest scan results and compliance history.

6.3.3. Evaluating Compliance

If the image scan policy has been updated since the last scan, compliance conditions may be re-evaluated. From an image summary page, select **Policy** → **Check Compliance of Last Known Configuration**. Refreshing the image page will reflect the latest compliance history.

6.4. OpenSCAP Policy Profile

Red Hat CloudForms is pre-configured with a default scanning policy profile. This includes conditions to scan and identify compliance, as well as annotate compliance failure. SmartState analysis is performed when new images are added to OpenShift.

6.4.1. Customizing the Scanning Policy Profile

The default OpenSCAP policy profile cannot be edited. To customize scanning policy, copy the default profile as a starting point and edit.

1. Navigate to **Control** → **Explorer**.
2. Select **Policy Profiles** → **All Policy Profiles** → **OpenSCAP Profile**.

3. Select Configuration → Copy this Policy Profile.

The copied profile can be edited as required. Be sure to assign the customized profile to the OpenShift provider.

6.5. Controlling OpenShift Pod Execution

Through the default policy profile, non-compliant images receive the control policy action **Mark as Non-Compliant**. This action annotates the `image` object (not to be confused with the `imagestream` object) with `images.openshift.io/deny-execution=true`. This annotation may be used to prevent nodes from running non-compliant images. Refer to [OpenShift Image Policy documentation](#) for configuration details.

6.6. Reference

More information about OpenSCAP, see visit the [OpenSCAP web site](#).