Red Hat CloudForms 5.0

Scanning Container Images in CloudForms with OpenSCAP

Configuring OpenSCAP in CloudForms for Scanning Container Images

Last Updated: 2020-08-05

Red Hat CloudForms 5.0 Scanning Container Images in CloudForms with OpenSCAP

Configuring OpenSCAP in CloudForms for Scanning Container Images

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

Legal Notice

Copyright © 2020 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, the Red Hat 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 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

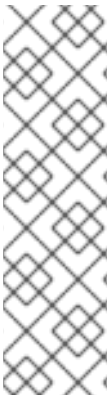
This document provides information about using OpenSCAP scanning capabilities in Red Hat CloudForms to ensure compliance of container images on OpenShift Container Platform. The content provides workflows on running scans for identifying and marking non-compliant container images and generating reports based on scanning results.

Table of Contents

CHAPTER 1. OVERVIEW

OpenSCAP is an auditing tool used for hardening the security of your enterprise. This tool is built upon the knowledge and resources provided by the many experienced security experts active in the upstream OpenSCAP ecosystem. For more information about OpenSCAP, see https://www.open-scap.org/.

Red Hat CloudForms supports OpenSCAP. It provides a built-in OpenSCAP policy profile for managing the security of your container images. These policies ensure that new container images from any provider within CloudForms are scanned against the latest Common Vulnerabilities and Exposures (CVE) content distributed by Red Hat.

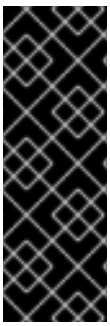


NOTE

- See Red Hat's Security Data page for more details about this content. In particular, the SCAP source data stream files index provides examples of security advisories used by the built-in OpenSCAP policy profile. Each of these security advisories have a severity ranging from low to critical. With the built-in OpenSCAP policy profile, any image that fails a security check against an advisory with at least a high severity is marked as non-compliant.
- For more information about control and compliance policies, and creating and assigning policy profiles in CloudForms, see the Policies and Profiles Guide.

CloudForms can initiate scanning of container images in the following ways:

- Manual scanning of images via SmartState analysis.
- Scheduled scanning of images using the OpenSCAP policy profile.
- Scanning new images in the registry when an OpenShift Container Platform provider is added.



IMPORTANT

For image scanning to work, make sure your CloudForms appliance has the **SmartProxy** and **SmartState Analysis** roles enabled:

1. From the Settings menu, navigate to **Configuration → Server**.
2. Under Server Control, ensure **SmartState Analysis** and **SmartProxy** roles are enabled.

CHAPTER 2. SCANNING CONTAINER IMAGES MANUALLY

When running SmartState analysis on container images, scanning containers are created on the target provider. The container image being inspected is pulled, mounted, and analyzed for vulnerabilities.

To run a single scan via SmartState analysis:

1. Navigate to **Compute → Containers → Container Images**.
2. Select the images to scan and click **Configuration → Perform SmartState Analysis**.

You can follow the scan status by navigating to **Tasks → All Tasks** from the settings menu.

2.1. VIEWING SCANNING RESULTS

Once complete, you can view the container image scanning results displayed on the summary page for each image.

1. Select **Compute → Containers → Container Images**.
2. Click the desired image.
3. Locate the **Configuration** section on the container image summary page and select **OpenSCAP HTML** to view an OpenSCAP HTML report.

CHAPTER 3. SCHEDULING A SCAN OF CONTAINER IMAGES

To fully utilize OpenSCAP scanning in CloudForms for container image compliance, assign the built-in OpenSCAP policy profile to containers providers, then schedule an OpenSCAP compliance check on container images for the assigned providers.

3.1. ASSIGNING THE BUILT-IN OPENSCAP POLICY PROFILE TO A CONTAINER PROVIDER

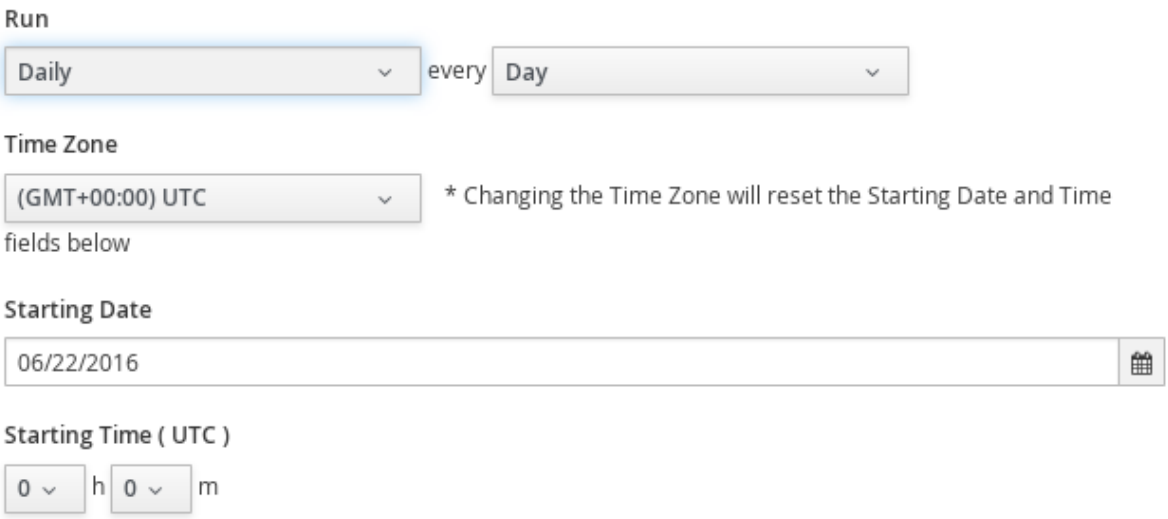
The OpenSCAP policy profile included with Red Hat CloudForms is not automatically assigned. You still need to assign it to a containers provider.

1. Navigate to **Compute → Containers → Providers**, check the providers you need to assign the OpenSCAP policy profile to.
2. Click  (**Policy**), and then click  (**Manage Policies**).
3. From the **Select Policy Profiles** area, click on the triangle next to **OpenSCAP profile** to expand it and see its member policies.
4. Select **OpenSCAP profile**. It turns blue to show its assignment state has changed.
5. Click **Save**.

3.2. SCHEDULING AN OPENSCAP COMPLIANCE CHECK FOR CONTAINER IMAGES

Once you have assigned the built-in OpenSCAP policy profile to a container provider, you can schedule a compliance check against the policy profile.

1. From the settings menu, select **Configuration**.
2. Click the **Settings** accordion, and select **Schedules**.
3. Click  (**Configuration**),  (**Add a new Schedule**).
4. In the **Adding a new Schedule** area, enter a name and description for the schedule.
5. Select **Active** to enable this scan.
6. From the **Action** list, select **Container Image Analysis**.
7. From the **Filter** list, select **All Container Images for Containers Provider**; a new list will appear. From this list, choose the provider where you enabled the OpenSCAP policy profile.
8. From the **Run** list, select how often you want the analysis to run. Your options after that depend on which run option you choose.



- Select **Once** to run the analysis just one time.
- Select **Daily** to run the analysis on a daily basis. You are prompted to select how many days you want between each analysis.
- Select **Hourly** to run the analysis hourly. You are prompted to select how many hours you want between each analysis.

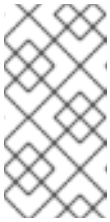
9. Select the time zone for the schedule.
10. Enter or select a date to begin the schedule in **Starting Date**.
11. Select a starting time based on a 24-hour clock in the selected time zone.
12. Click **Add**.

CHAPTER 4. CONFIGURING IMAGE SCANNING WHEN ADDING AN OPENSHIFT CONTAINER PLATFORM PROVIDER

When you add an OpenShift Container Platform node as a containers provider, container images from the internal registry are discovered. To enable scanning of newly discovered images in the registry against the latest CVE content distributed by Red Hat, configure the image-inspector settings under advanced settings when adding an OpenShift Container Platform containers provider. These settings control downloading the image-inspector container image from the registry and obtaining the CVE information (for effective scanning) via a proxy.

4.1. ADDING AN OPENSHIFT CONTAINER PLATFORM PROVIDER

1. Navigate to **Compute → Containers → Providers**.
2. Click  (**Configuration**), then click  (**Add a New Containers Provider**).
3. Enter a **Name** for the provider.
4. From the **Type** list, select **OpenShift Container Platform**.
5. Enter the appropriate **Zone** for the provider. If you do not specify a zone, it is set to **default**.
6. From the **Alerts** list, select **Prometheus** to enable external alerts. Selecting **Prometheus** adds an **Alerts** tab to the lower pane to configure the Prometheus service. Alerts are disabled by default.
7. From the **Metrics** list, select **Hawkular** or **Prometheus** to collect capacity and utilization data, or leave as **Disabled**. Selecting **Prometheus** or **Hawkular** adds a **Metrics** tab to the lower pane for further configuration. Metrics are disabled by default.
8. In the **Default** tab, configure the following for the OpenShift provider:
   a. Select a **Security Protocol** method to specify how to authenticate the provider:
      - **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
      - **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.

        NOTE

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

      - **SSL without validation**: Authenticate the provider insecurely (not recommended).

   b. Enter the **Hostname** (or IPv4 or IPv6 address) of the provider.

IMPORTANT

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

c. Enter the **API Port** of the provider. The default port is **8443**.

d. Enter a token for your provider in the **Token** box.

NOTE

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

For example:

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

e. Click **Validate** to confirm that Red Hat CloudForms can connect to the OpenShift Container Platform provider.

9. For the **Prometheus** alerts service, add the Prometheus alerts endpoint in the **Alerts** tab:

a. Select a **Security Protocol** method to specify how to authenticate the service:

- **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
- **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.
- **SSL without validation**: Authenticate the provider insecurely using SSL. (Not recommended)

b. Enter the **Hostname** (or IPv4 or IPv6 address) or alert **Route**.

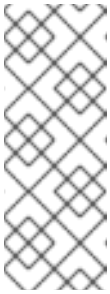
c. Enter the **API Port** if your Prometheus provider uses a non-standard port for access. The default port is **443**.

d. Click **Validate** to confirm that CloudForms can connect to the alerts service.

10. If you selected a metrics service, configure the service details in the **Metrics** tab:

a. Select a **Security Protocol** method to specify how to authenticate the service:

- **SSL**: Authenticate the provider securely using a trusted Certificate Authority. Select this option if the provider has a valid SSL certificate and it is signed by a trusted Certificate Authority. No further configuration is required for this option.
- **SSL trusting custom CA**: Authenticate the provider with a self-signed certificate. For this option, copy your provider's CA certificate to the **Trusted CA Certificates** box in PEM format.



NOTE

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

- **SSL without validation**: Authenticate the provider insecurely using SSL. (Not recommended)

b. Enter the **Hostname** (or IPv4 or IPv6 address) of the provider, or use the **Detect** button to find the hostname.

c. Enter the **API Port** if your Hawkular or Prometheus provider uses a non-standard port for access. The default port is **443**.

d. Click **Validate** to confirm that Red Hat CloudForms can connect to the metrics endpoint.

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

NOTE

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

a. Enter the proxy information for the provider in either **HTTP**, **HTTPS**, or **NO Proxy** depending on your environment.

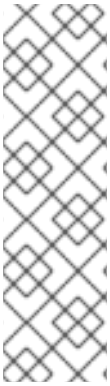
b. Enter the **Image-Inspector Repository** information. For example, **openshift3/image-inspector**.

c. Enter the **Image-Inspector Registry** information. For example, **registry.access.redhat.com**.

d. Enter the **Image-Inspector Tag** value. A tag is a mark used to differentiate images in a repository, typically by the application version stored in the image.

e. Enter **https://www.redhat.com/security/data/metrics/ds/** in **CVE location**.

12. Click **Add**.



NOTE

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

For example:

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

With the above configuration:

- New container images discovered will automatically be scanned.
- All OpenShift Container Platform provider images will be scanned as per the schedule you set.
- Images with high severity failures will be marked as non-compliant. Also, OpenShift Container Platform will attempt to label non-compliant images as non-secure and prevent their execution. This requires additional configuration in OpenShift Container Platform, see https://docs.openshift.com/container-platform/3.11/admin_guide/image_policy.html.

You can define additional policies in CloudForms that would be executed once a compliance check failed or succeeded. To do that, copy the OpenSCAP policy profile and create new profiles based on that; see Chapter 5, *Creating a Customized OpenSCAP Policy Profile* . For example, a user can choose to define all images with any severity failure as non-compliant, creating a very hardened system.

Additionally, to generate a report on container images for failed OpenSCAP rule results, see Chapter 6, *Generating OpenSCAP Scanning Reports*.

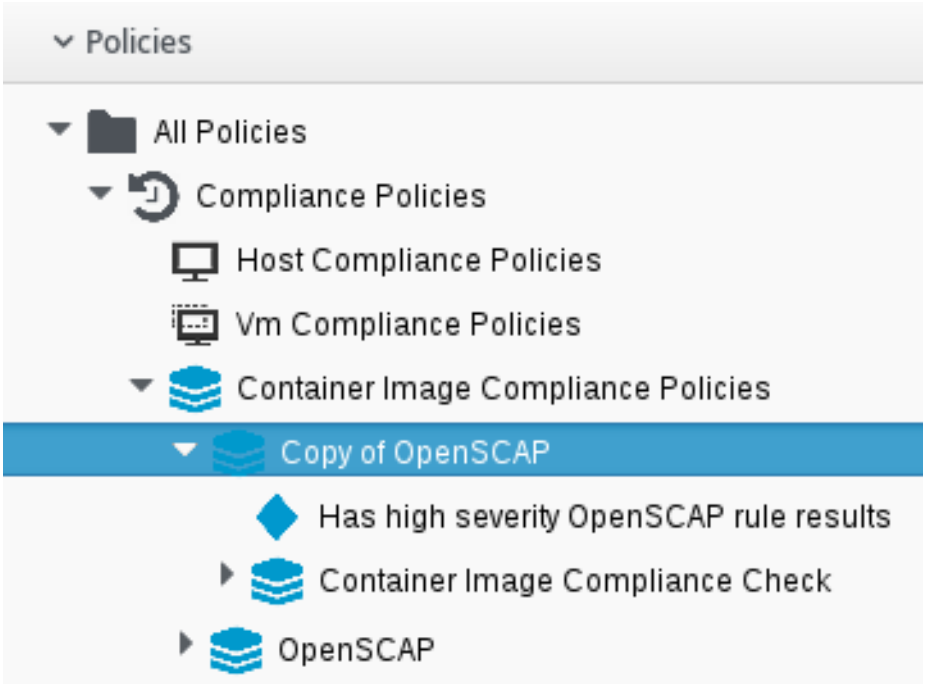
CHAPTER 5. CREATING A CUSTOMIZED OPENSCAP POLICY PROFILE

The built-in OpenSCAP policy profile cannot be edited. You can, however, assign *edited* copies of its policies to a new policy profile. This will allow you to create a customized version of the built-in OpenSCAP policy profile.

To do so, you will first have to copy the policy you want to customize:

1. Navigate to **Control → Explorer**.
2. Click the **Policies** accordion, and select **Container Image Compliance Policies**, then click **OpenSCAP**.
3. Click (**Configuration**), and an option to copy the policy should appear; for example, (**Copy this Container Image Policy**).
4. Click **OK** to confirm.

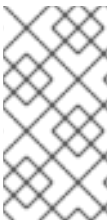
The new policy is created with a prefix of **Copy of** in its description, and it can be viewed in the Policies accordion.



You can now edit the copied policy. After editing copied policies, you can add them to a new policy profile. For instructions on how to edit policies, create a new policy profile, and add policies to it, see the Policies and Profiles guide. Once you have a customized policy profile, you can assign it to a containers provider.

CHAPTER 6. GENERATING OPENSCAP SCANNING REPORTS

You can output the results of an OpenSCAP scan of images to a report for an overview of the security risk level of images. The **Images by Failed OpenSCAP Rule Results** is included with CloudForms and shows whether the image has passed or failed OpenSCAP policy criteria, and the security risk.



NOTE

You can also create a copy of this report and edit it to contain additional information, such as the project name where the image is used, to produce more useful results. See Editing a Report and See Reportable Fields in Red Hat CloudForms in *Monitoring, Alerts, and Reporting* for instructions on customizing reports.

To create a report showing image compliance:

1. Navigate to **Overview → Reports**.
2. Click the **Reports → All Reports** accordion.
3. Navigate to **Configuration Management → Containers → Images by Failed OpenSCAP Rule Results** for a report showing which images have failed the OpenSCAP compliance.
4. Click  **Queue**.
5. The report generation is placed in the queue and its status shows in the reports page.

		Queued At	Run At	Source	Username	Group	Status
☐	⏵	03/12/18 04:31:57 UTC		Requested by user	ocpadmin	EvmGroup-container_administrator_updated	Queued
☐	→	03/07/18 08:43:25 UTC	03/07/18 08:44:00 UTC	Requested by user	ocpadmin	EvmGroup-container_administrator_updated	Complete

6. Click  **(Refresh this page)** to update the status.
7. Navigate to the **Saved Reports** accordion, and click the report when it is completed.
8. Click on the report download buttons for the type of export you want. The report is automatically named with the type of report and date.
   - Click  **(Download this report in text format)** to download as text.
   - Click  **(Download this report in CSV format)** to download as a comma-separated file.
   - Click  **(Download this report in PDF format)** to download as PDF.