Image Vulnerability Scanning

[Prerequisites] [Limitations] [Build Image-Inspector] [Configure CloudForms] [Image-Inspector Registry Location] [Assign Compliance Policy] [Schedule a Container Image Analysis Job] [Review Reports] [Resources]

Prerequisites

- Openshift 3.4+
- Openshift added as a "Provider" in CFME 4.5+
    - Requires management-infra project and associated token configured during Provider setup:

```
oc get -n management-infra sa/management-admin
--template='{{range .secrets}}{{printf "%s\n" .name}}{{end}}' |
grep token | awk '{system ("oc get -n management-infra secrets "
$1 " --template='{{.data.token}}' | base64 -d")}'
```

Limitations

- OpenSCAP scans will only work with RHEL 6/7 images

Build Image-Inspector

To incorporate CA chains and/or proxy settings, ensure the image-inspector image is built from the latest source:

1. Clone the repo

```
git clone https://github.com/openshift/image-inspector.git && cd
image-inspector
```

2. Update Dockerfile to include:

```
ENV HTTP_PROXY=http://proxy-lmi.global.lmco.com:80 \
    HTTPS_PROXY=https://proxy-lmi.global.lmco.com:80

RUN curl -k
https://sscgit.ast.lmco.com/projects/CP/repos/openstack-hot/browse/lm
_ca.pem?raw > /etc/pki/ca-trust/source/anchors/lm_ca.pem && \
    /usr/bin/update-ca-trust && \
    echo "proxy=http://proxy-lmi.global.lmco.com:80" >> /etc/yum.conf
```

3. Execute a docker build, tagging the image in the process:
4. Push the image to a locally accessible repository:
5. Test a scan:

Configure CloudForms

These configuration changes require CFME 4.5+

Image-Inspector Registry Location

On each CFME node (UI, Worker, etc.), ensure */var/www/miq/vmdb/config/environments/production.yml* is updated to reflect the location of your pre-built image, which should include appropriate environment variables, CA chains, etc.:

/var/www/miq/vmdb/config/environments/production.yml

```
# This file takes priority over upstream settings in "config/settings.yml".
---
:ems:
  :ems_azure:
    :disabled_regions:
    - usgovarizona
    - usgoviowa
    - usgovtexas
    - usgovvirginia
  :ems_amazon:
    :disabled_regions:
    - us-gov-west-1
  :ems_kubernetes:
    :image_inspector_registry: docker-registry-default.slyapps.ssc.lmco.com
#### Registry location
    :image_inspector_repository: image-inspector/image-inspector ####
Image, which must be tagged 2.1, at least in version CFME 4.5
:product:
  :update_repo_names:
  - cf-me-5.8-for-rhel-7-rpms
  - rhel-server-rhscl-7-rpms
```

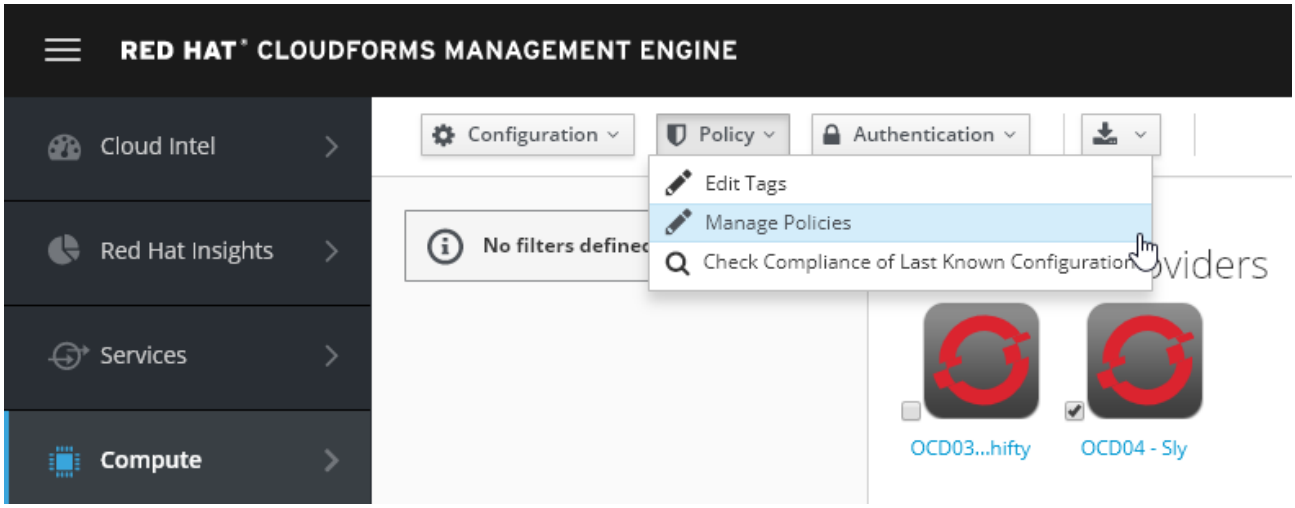
The image tag is still hardcoded to 2.1 so ensure the built image is tagged the same:

/var/www/miq/vmdb/app/models/manageiq/providers/kubernetes/container_manager/scanning/job.rb

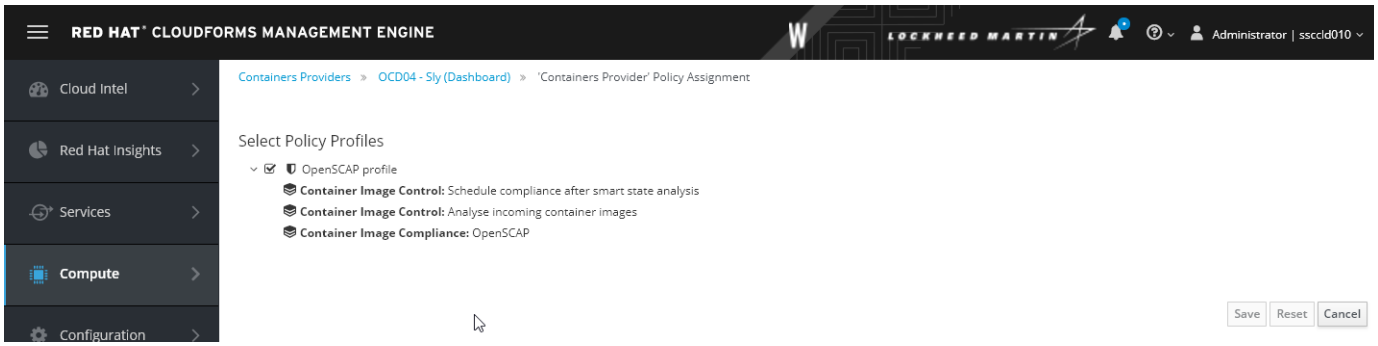
```
...
class ManageIQ::Providers::Kubernetes::ContainerManager::Scanning::Job <
Job
  PROVIDER_CLASS = ManageIQ::Providers::Kubernetes::ContainerManager
  INSPECTOR_IMAGE_TAG = '2.1'.freeze
...
```

Assign Compliance Policy

Navigate to Compute > Containers > Providers. Check one or more providers and navigate to Policy > Manage Policies:

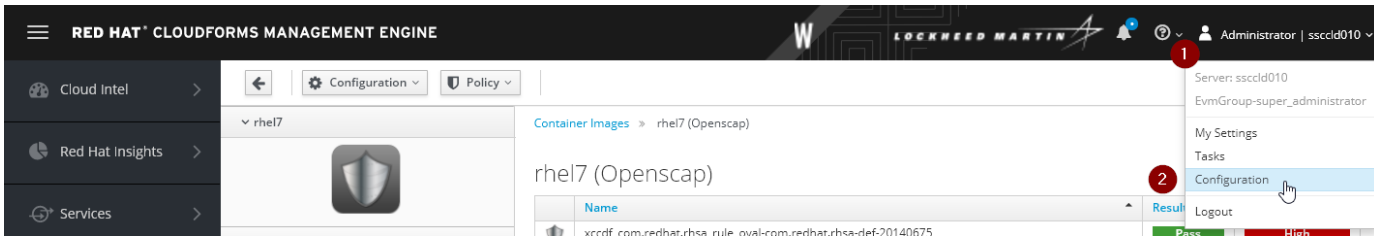


Ensure the OpenSCAP Profiles have been selected and click "Save"

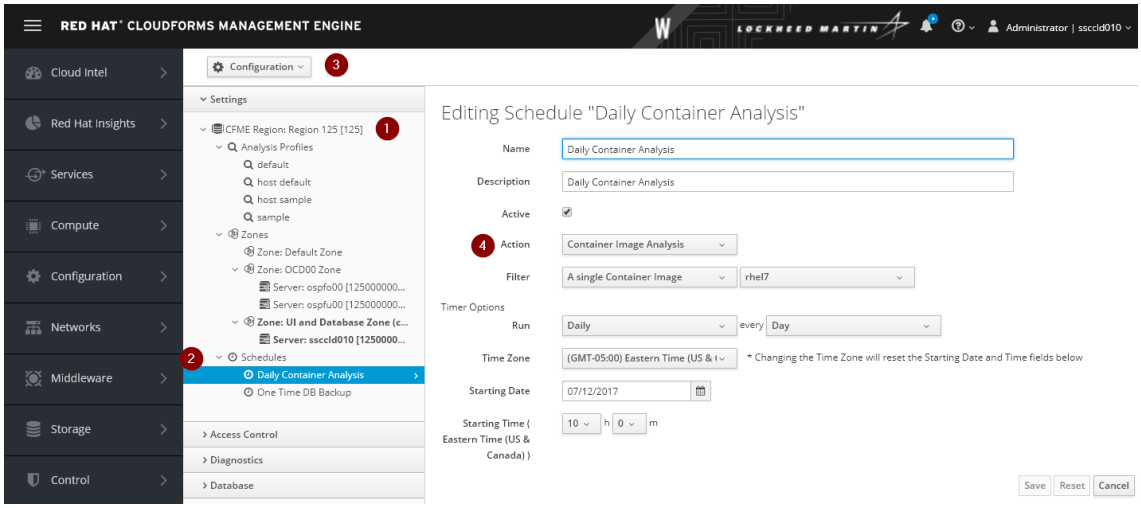


Schedule a Container Image Analysis Job

Navigate to the system "Configuration" page:

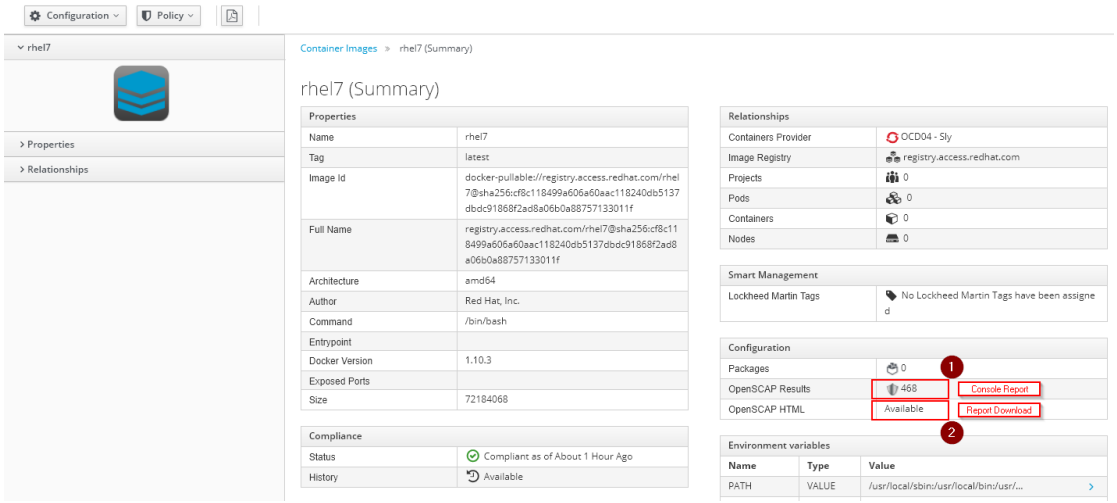


Expand "CFME Region" > "Schedules". Click the "Configuration" menu and select "Add a new Schedule". Complete all fields, and ensure the "Action" is defined as "Container Image Analysis". Optionally, define a filter – it's always good to test single image scanning before bulk image scanning:

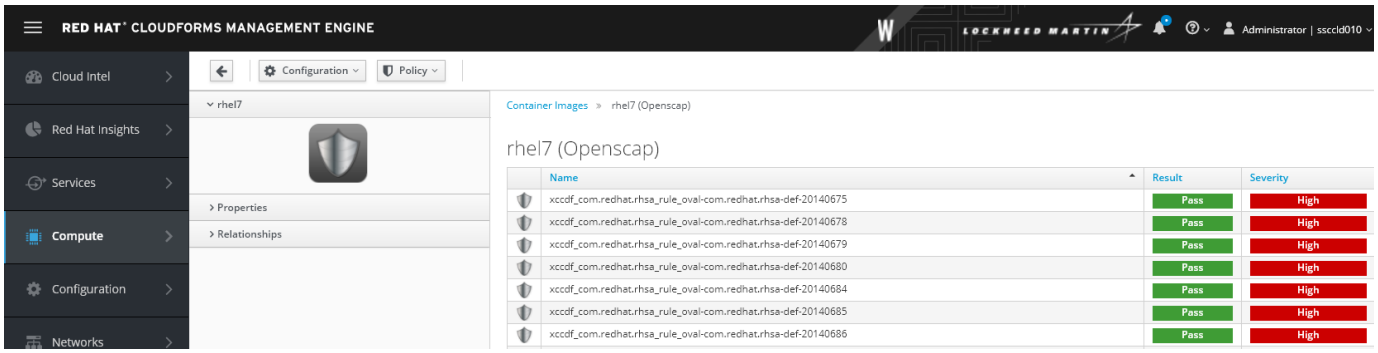


Review Reports

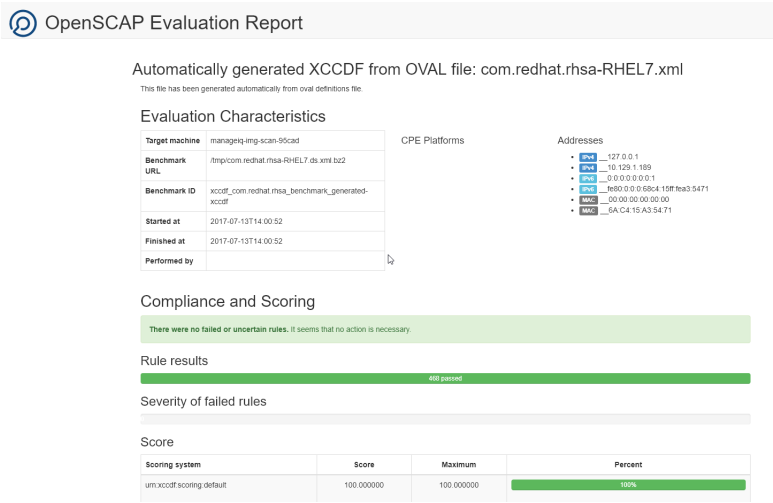
OpenSCAP reports can be reviewed by accessing scanned images (Compute > Containers > Container Images), or by clicking the executed Task. After navigating the the appropriate image, select a method of viewing your OpenSCAP results



To view the in-console OpenSCAP report results click item (1), which should generate a results table:



The OpenSCAP HTML report provides more details, but must be downloaded to view:



OpenSCAP Evaluation Report

Automatically generated XCCDF from OVAL file: com.redhat.rhsa-RHEL7.xml

This file has been generated automatically from oval definitions file.

Evaluation Characteristics

Target machine	manageiq-img-scan-95cad
Benchmark URL	/tmp/com.redhat.rhsa-RHEL7.ds.xml.bz2
Benchmark ID	xccdf_com.redhat.rhsa_benchmark_generated-xccdf
Started at	2017-07-13T14:00:52
Finished at	2017-07-13T14:00:52
Performed by	

CPE Platforms

Addresses

- IPv4 __127.0.0.1
- IPv4 __10.129.1.169
- IPv6 __0:0:0:0:0:0:0:1
- IPv6 __fe80:0:0:0:68c4:15ff:fea3:5471
- MAC __00:00:00:00:00:00
- MAC __6A:C4:15:A3:54:71

Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.

Rule results

468 passed

Severity of failed rules

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	100.000000	100.000000	100%

Resources

- http://www.tigeriq.co/openscap-in-a-secure-environment/
- https://access.redhat.com/documentation/en-us/red_hat_cloudforms/4.5/html/managing_providers/containers_providers