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 - usqovvirginia :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:

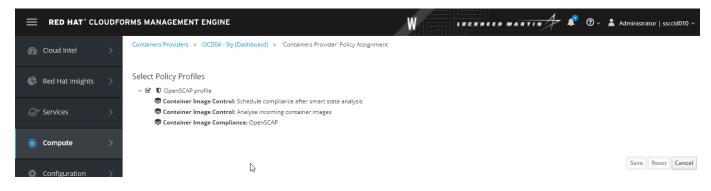
```
/var/www/miq/vmdb/app/models/manageiq/providers/kubernetes/container_manager/scanning
/job.rb
...
class ManageIQ::Providers::Kubernetes::ContainerManager::Scanning::Job <
Job
PROVIDER_CLASS = ManageIQ::Providers::Kubernetes::ContainerManager
INSPECTOR_IMAGE_TAG = '2.1'.freeze
...
```

Assign Compliance Policy

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

RED HAT [®] CLOUDFORMS MANAGEMENT ENGINE					
🕐 Cloud Intel	>	Configuration ~ Policy ~ Authentication ~ L Edit Tags			
Red Hat Insights	>	No filters defined Manage Policies A Check Compliance of Last Known Configuration VIDERS			
.⊕* Services	>				
Compute	>	OCD03hifty OCD04 - Sly			

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

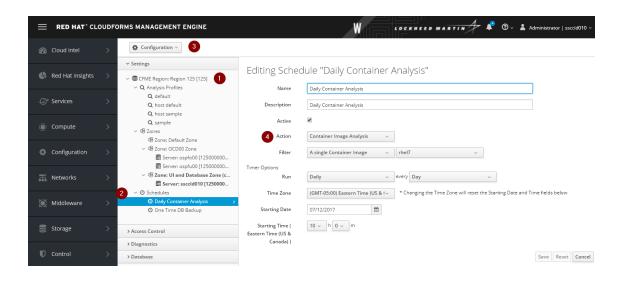


Schedule a Container Image Analysis Job

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

Configuration >								
∨ rhel7	Container Images » rhel	Container Images > rhel7 (Summary)						
	rhel7 (Summa	rhel7 (Summary)						
	Properties		Relationships					
> Properties	Name	Name rhel7		Containers Provider OCD04 - Sly		Sly		
	Tag	latest	Image Registry 💏 registry.acces			access.redhat.com		
> Relationships	Image Id	docker-pullable://registry.access.redhat.com/rhel 7@sha256:cf8211899a606a60aac118240db5137	Projects		iĝi 0			
			Pods		& 0			
		dbdc91868f2ad8a06b0a88757133011f	Containers		© 0			
	Full Name	registry.access.redhat.com/rhel7@sha256:cf8c11 8499a606a60aac118240db5137dbdc91868f2ad8 a06b0a88757133011f	Nodes		a 0			
	Architecture	Architecture amd64			Smart Management			
	Author	Red Hat, Inc.	Lockheed Martin Tags No Lo			kheed Martin Tags have been assigne		
	Command	/bin/bash	d					
	Entrypoint	Entrypoint			Configuration			
	Docker Version	1.10.3	Packages		٥٠ 🕕			
	Exposed Ports	Exposed Ports		OpenSCAP Results		Console Report		
	Size	72184068	OpenSCAP HTML		10 468 Available	Report Download		
			oponoona mi			2		
	Compliance		Environment variables					
	Status	O Compliant as of About 1 Hour Ago	Name	Туре	Value			
	History	D Available	PATH	VALUE	/usr/local/shin:/u	sr/local/bin:/usr/		

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

E RED HAT' CLOUDF	ORMS MANAGEMENT ENGINE	W LOCKNEED WARTIN /	- 🖍 💿 🛓	Administrator ssccld010 ~			
🙆 Cloud Intel >	← Configuration ~ ♥ Policy ~						
Red Hat Insights >	✓ rhel7	Container Images > rhel7 (Openscap) rhel7 (Openscap)					
.⊕* Services >	> Properties	Name Image: Strate S	Result Pass	Severity High			
Compute >	> Relationships	vccdf_com.redhat.rhsa_rule_oval-com.redhat.rhsa-def-20140678 vccdf_com.redhat.rhsa_rule_oval-com.redhat.rhsa-def-20140679	Pass Pass	High High			
🔅 Configuration >		xccdf.com.redhat.rhsa_rule_oval-com.redhat.rhsa-def-20140680 xccdf.com.redhat.rhsa-rule_oval-com.redhat.rhsa-def-20140684 xccdf.com.redhat.rhsa-rule_oval-com.redhat.rhsa-def-20140685	Pass Pass Pass	High High High			
🚡 Networks >		vxcdf_com.redhat.rhsa_rule_ovalcom.redhat.rhsa-def 20140685 vxcdf_com.redhat.rhsa_rule_ovalcom.redhat.rhsa-def 20140686	Pass	High			

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

OpenSCAF	P Evalua	tion Report						
	This file has been g	ally generated X enerated automatically from oval n Characteristic	definitions file.	m OVAL file: c	om.redhat.rhsa-RHEL7.xml			
	Target machine	managelq-img-scan-95cad		CPE Platforms	Addresses			
	Benchmark URL	/tmp/com.redhat.rhsa-RHEL7.ds	xmi.bz2		- 27.0.0.1 - 2004			
	Benchmark ID	xccdf_com.redhat.rhsa_benchm xccdf	ark_generated-					
	Started at	2017-07-13T14:00:52			•			
	Finished at	2017-07-13T14:00:52						
	Performed by		1	2				
Compliance and Scoring								
	There were no i	med of undertain rules, it seems	s mar no action is neo	zasary.				
	Rule results							
Score								
	Scoring system		Score	Maximum	Percent			
	urm:xccdf.scoring;	lefault	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