



OpenSCAP Scanning in Satellite 6 and CloudForms

RHUG Q3.2016

Marc Skinner

Principal Solutions Architect

Mike Dahlgren

Senior Solutions Architect

9/21/2016

AGENDA

Security and Compliance

What is SCAP?

OpenSCAP in Satellite 6

OpenSCAP in CloudForms

Security and Compliance



KEY HELP PART TESTED METRICS DEVICES PRIVACY COVER PROVIDE TRENDS COMPANY MALWARE PHYSICAL EVENT
PENETRATION PERFORM UPDATED REVIEWED REGULATION DOCUMENTED CLIENT SITE CONTINUITY ACCESS RECORDS ENDSURE FOCUS
FRAMEWORK ADDRESSED FRAMEWORK APPLICATIONS INCLUDE PREVIOUS WRITTEN RISK VULNERABILITY CURRENT FILLING
PRACTICES PROCESS SCOPE SECURITY INFORMATION MANAGEMENT EXTERNAL REPAIR COMPUTER FOR
COMPLIANCE LOGS AGREED RESULTS GOVERNANCE ACCEPTED REPORT OPERATED PERFORMING
NETWORK SURVEY GUIDE RECOVERY MEETING CHECK BUSINESS BACKUP STAFF INCIDENTS DISASTER
AUDITED PROBLEM DEFICIENCIES AUDIT PASSEWORDS FIREWALL VULNERABILITY ASSESSMENT DISCOVERED WEAKNESSES GENERAL HEADQUARTERS
TECHNICAL SYSTEM POLICY FINANCIAL INTERNAL GAIN ORGANIZATION ASKED ACCOMPLISH HISTORICAL DETERMINE CONTROLS ANSWERS BEST REVIEW DOWNTIME
SUMMARY DAILY PROCEDURES AUDITORS MEASURABLE EXAMINATION APPROPRIATE ACCORDANCE STANDARDS COMPLETE EFFECTIVE INSIGHT OVERALL
OBJECTIVES CONDUCT IMPORTANT ANALYSIS FINDINGS SETTINGS EXAMINE ACTUALLY OVERVIEW

Common Criteria (CC)

AAAA
ANTI-ACRONYM ASSOCIATION OF AMERICA

Protection Profile(PP)

Security Target (ST)

Security Functional Req. (SFRs)

{Requirements}

{Properties}

{Combined Function}

EVALUATION ASSURANCE LEVEL (EAL)



EAL1: Functionally Tested

EAL2: Structurally Tested

(vSphere 5.1-5.5)

EAL3: Methodically Tested and Checked

EAL4: Methodically Designed, Tested and Reviewed

(vSphere 5.0, RHEL6, WIN2k8)

EAL5: Semiformally Designed and Tested

(e.g. Smart Card Readers)

EAL6: Semiformally Verified Design and Tested

EAL7: Formally Verified Design and Tested

(e.g. Integrated Circuits IC's)

Without Testing...

**EAL's
DO NOT =
SECURITY**



- Security Technical Implementation Guide (STIGs)
+ PostgreSQL
- United States Gov Config Baseline (USGCB)
- Federal Information Processing (FIPS140)
- Payment Card Industry (PCI)



Security policies available in the SCAP Security Guide

The SCAP Security Guide is not just one security policy, but a whole number of them. For each platform, there are several profiles which provide security policies implemented according to security baselines. You can view the guide by clicking the respective platform.

Other profiles can be derived from existing profiles using the SCAP Workbench. For more information, please see

[Customization](#)

These guides to secure configuration of following platforms with following profiles are currently available:

[Fedora Linux](#) ▾

[Red Hat Enterprise Linux 7](#) ▾

[U.S. Government Commercial Cloud Services \(C2S\)](#)

[CNSSI 1253 Low/Low/Low Control Baseline for Red Hat Enterprise Linux 7](#)

[Common Profile for General-Purpose Systems](#)

[Criminal Justice Information Services \(CJIS\) Security Policy](#)

[Payment Card Industry – Data Security Standard \(PCI-DSS\) v3](#)

[Red Hat Corporate Profile for Certified Cloud Providers \(RH CCP\)](#)

[STIG for Red Hat Enterprise Linux 7 Server](#)

[STIG for Red Hat Enterprise Linux 7 Server Running GUIs](#)

[STIG for Red Hat Enterprise Linux 7 Workstation](#)

[Standard System Security Profile](#)

[United States Government Configuration Baseline \(NIAP OSPP v4.0, USGCB, STIG\)](#)

What is SCAP?

What is SCAP?

- **Security Content Automation Protocol (SCAP)** is a collection of standards managed by **National Institute of Standards and Technology (NIST)**. It was created to provide a standardized approach to maintaining the security of enterprise systems, such as automatically verifying the presence of patches, checking system security configuration settings, and examining systems for signs of compromise.
- The key step in the implementation of SCAP within the organization is having the security policy in the form of SCAP.
- It is a collection of data formats.

What is SCAP?

- For each of the SCAP components mentioned, the standard defines a document format with syntax and semantics of the internal data structures.
- All the component standards are based on **Extensible Markup Language (XML)** and each component standard defines its own XML name-space
- Any tool which is certified against SCAP 1.2 is **required** to understand all of the previous versions of the component standards.

SCAP Components

- SCAP languages:
 - **OVAL®**: A language for making logical assertions about the state of an endpoint system – describing the desired state.
 - **XCCDF**: A language to express, organize, and manage security guidance that references OVAL.
 - **OCIL**: Open Checklist Interactive Language: a language to provide a standard way of querying for a human user.
 - **ARF**: Asset Reporting Format: a language to express the transport format of information about assets, and the relationships between assets and reports.

What is OpenSCAP?

- A **framework of libraries and tools** to improve the accessibility of SCAP and enhance the usability of the information it represents.
- On 04/29/2014 OpenSCAP project received SCAP 1.2 certification from NIST.
 - <http://nvd.nist.gov/scaproducts.cfm>

What tooling is available for SCAP?

- **OpenSCAP:** suite of open source tools and libraries for security automation
- **OpenSCAP Scanner:** command line tool for configuration and vulnerability measurements
- **SCAP Workbench:** a GUI tool for scanning and content tailoring, GUI front-end for OpenSCAP
- **SCAP Security Guide:** The project provides pre-built profiles for common configuration requirements, such as DoD STIG, PCI, CJIS, and the Red Hat Certified Cloud Provider standards.

What tooling is available for SCAP?

- **OSCAP Anaconda:** An add-on for the Anaconda installer that enables administrators to feed security policy into the installation process and ensure that systems are compliant from the very first boot.
- **Red Hat Satellite:** Centralized systems life-cycle manager with enterprise vulnerability measurements.
- **Red Hat CloudForms:** to manage security through the full life cycle of systems and apps in open hybrid cloud environments (want to scan Amazon AMIs?).
- **Red Hat Atomic:** The ability to scan Docker container images.

What is the SCAP Security Guide?

- The project provides practical security hardening advice for Red Hat products and also links it to compliance requirements in order to ease deployment activities, such as certification and accreditation.
- The project started in 2011 as open collaboration of U.S. Government bodies to develop next generation of **United States Government Baseline (USGCB)** available for Red Hat Enterprise Linux 6.
- In addition to the policy for Red Hat Enterprise Linux 6 and 7, there are policies growing for other Red Hat products, such as JBoss Application Server
- Take policy requirements and present them as machine readable formats.

RHEL 7

Optional Security Policy

The screenshot shows the 'SECURITY POLICY' configuration window during the Red Hat Enterprise Linux 7.2 installation. The window title is 'Red Hat Enterprise Linux 7.2 installation on host 192.168.33.226 - TigerVNC'. The top right corner shows 'RED HAT ENTERPRISE LINUX 7.2 INSTALLATION' and a 'Help!' button. A 'Done' button is in the top left. Below the title bar, there is a 'Change content' button and a toggle for 'Apply security policy:' which is currently set to 'ON'. The main area is titled 'Choose profile below:' and lists several profiles with their descriptions:

- Default**: The implicit XCCDF profile. Usually, the default contains no rules.
- Standard System Security Profile**: This profile contains rules to ensure standard security base of Red Hat Enterprise Linux 7 system.
- Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7**: This is a *draft* profile for PCI-DSS v3
- Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)**: This is a *draft* SCAP profile for Red Hat Certified Cloud Providers
- Common Profile for General-Purpose Systems**: This profile contains items common to general-purpose desktop and server installations.
- Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server**: This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

At the bottom of the profile list is a 'Select profile' button. Below this, a section titled 'Changes that were done or need to be done:' shows a lightbulb icon and the text 'No profile selected'.

OpenSCAP in Satellite 6

Three Steps Needed

- Client configuration
- Satellite 6 configuration
- SCAP content

Prepare RHEL 7 Client

- Requirements

```
# yum -y install puppet puppet-foreman_scap_client
```

```
# systemctl start puppet
```

```
# systemctl enable puppet
```

```
# puppet agent -t --server sat6.i.skinnerlabs.com
```

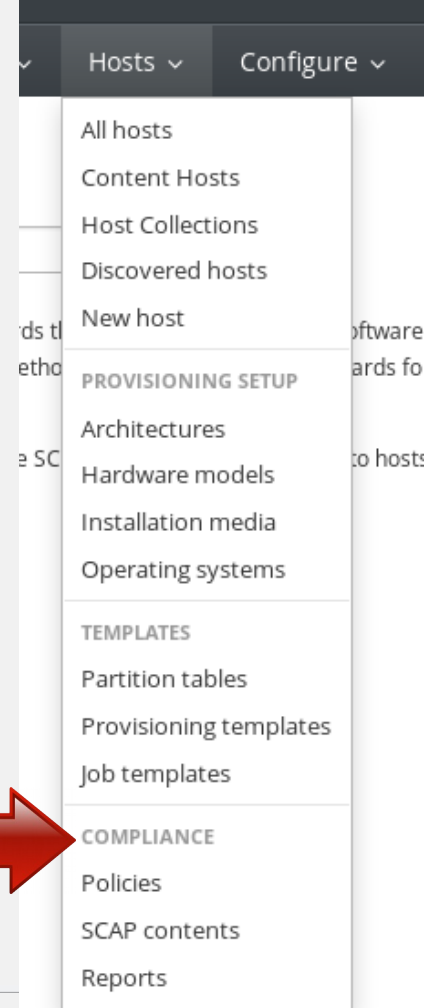
Prepare Satellite 6

- Requirements

```
# satellite-installer --enable-foreman-plugin-openscap
```

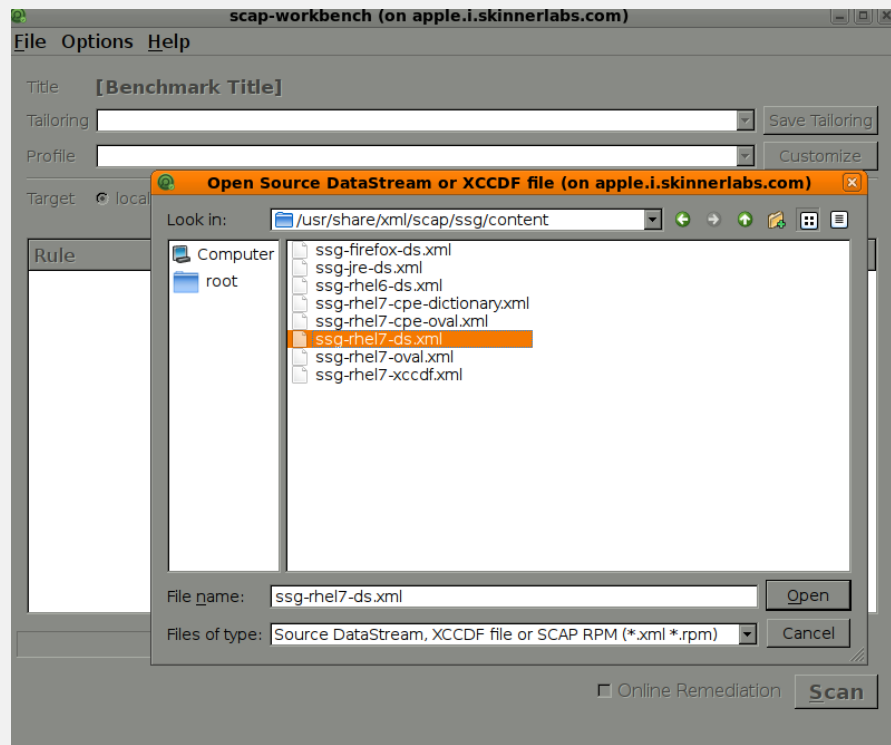
```
# yum -y install puppet-foreman_scap_client
```

```
# foreman-rake foreman_openscap:bulk_upload:default
```



RHEL7 SCAP Content

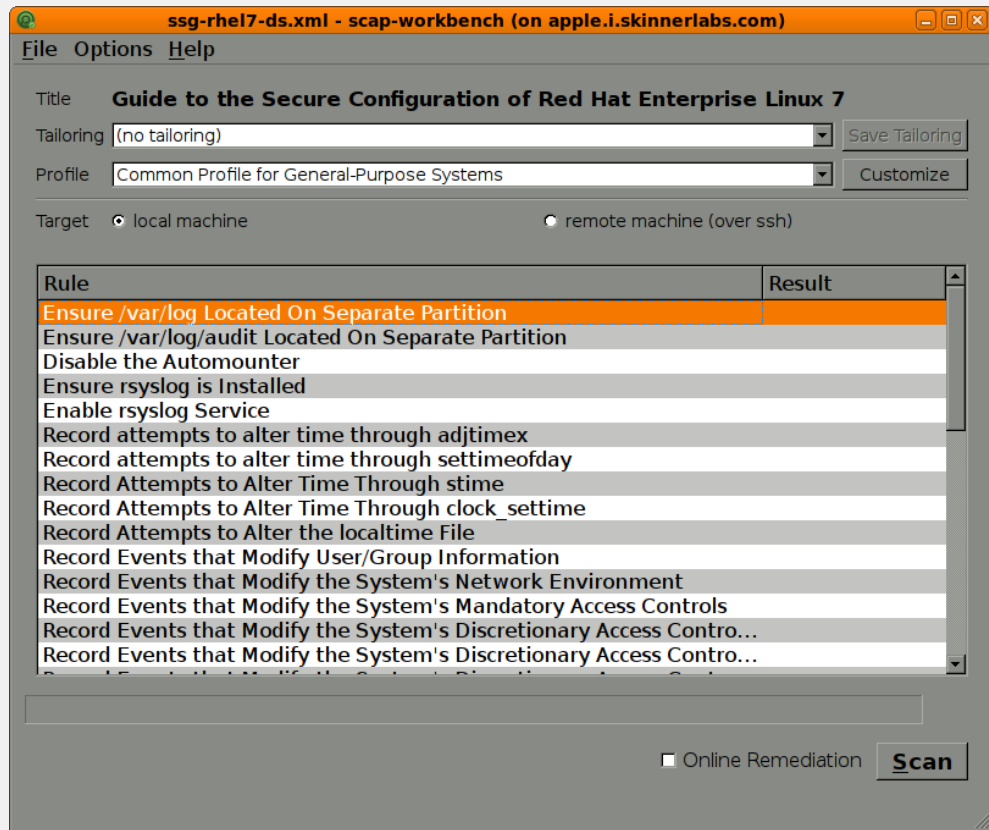
- Requirements
 - # yum install scap-workbench
 - # yum install scap-security-guide
 - # scap-workbench



RHEL7 SCAP

- **Profiles**
 - Common Profile for General-Purpose Systems
 - Draft PCI-DSS v3 Control Baseline for RHEL7
 - Red Hat Corporate Profile for Certified Cloud Provider
 - Standard System Security Profile
 - Pre-release Draft STIG for RHEL7

scap-workbench



scap-workbench scanning...

The screenshot shows the scap-workbench application window titled "ssg-rhel7-ds.xml - scap-workbench (on apple.i.skinnerlabs.com)". The interface includes a menu bar (File, Options, Help) and a configuration section with the following details:

- Title: Guide to the Secure Configuration of Red Hat Enterprise Linux 7
- Tailoring: (no tailoring) [Save Tailoring]
- Profile: Common Profile for General-Purpose Systems [Customize]
- Target: local machine remote machine (over ssh)

The main area displays a table of scan results:

Rule	Result
Record Events that Modify the System's Discretionary Access Contro...	fail
Record Events that Modify the System's Discretionary Access Contro...	fail
Record Events that Modify the System's Discretionary Access Contro...	fail
Ensure auditd Collects Unauthorized Access Attempts to Files (unsuc...	fail
Ensure auditd Collects Information on the Use of Privileged Comma...	fail
Ensure auditd Collects Information on Exporting to Media (successful)	fail
Ensure auditd Collects File Deletion Events by User	fail
Ensure auditd Collects System Administrator Actions	fail
Ensure auditd Collects Information on Kernel Module Loading and U...	fail
Disable Automatic Bug Reporting Tool (abrtd)	fail
Disable ntpdate Service (ntpdate)	pass
Disable Odd Job Daemon (oddjobd)	pass
Disable Apache Qpid (qpidd)	pass
Disable Network Router Discovery Daemon (rdisc)	pass
Disable At Service (atd)	fail

Below the table is a progress bar showing 100% completion (38 results, 38 rules selected). At the bottom, there are buttons for "Clear", "Save Results", and "Show Report", along with the message "Processing has been finished!".

scap-workbench tailoring...

The screenshot displays the Scap Workbench Tailoring application window. The title bar reads "Tailoring 'Common Profile for General-Purpose Systems [TAILORED]' (on apple.i.skinnerlabs.com)". The interface includes a toolbar with "Undo History", "Deselect All", and "Search" buttons. The main area is a tree view showing a hierarchy of configuration items:

- Guide to the Secure Configuration of Red Hat Enterprise Linux 7
 - A conditional clause for check statements.
 - Introduction
 - General Principles
 - Encrypt Transmitted Data Whenever Possible
 - Minimize Software to Minimize Vulnerability
 - Run Different Network Services on Separate Systems
 - Configure Security Tools to Improve System Robustness
 - Least Privilege
 - How to Use This Guide
 - Read Sections Completely and in Order
 - Test in Non-Production Environment
 - Root Shell Environment Assumed
 - Formatting Conventions
 - Reboot Required
 - System Settings
 - Installing and Maintaining Software
 - Disk Partitioning
 - Ensure /tmp Located On Separate Partition
 - Ensure /var Located On Separate Partition
 - Ensure /var/log Located On Separate Partition
 - Ensure /var/log/audit Located On Separate Partition
 - Ensure /home Located On Separate Partition
 - Encrypt Partitions
 - Updating Software
 - Ensure Red Hat GPG Key Installed
 - Ensure gpgcheck Enabled In Main Yum Configuration
 - Ensure gpgcheck Enabled For All Yum Package Repos
 - Ensure Software Patches Installed
 - Software Integrity Checking
 - Verify Integrity with AIDE
 - Install AIDE

At the bottom of the window are three buttons: "Confirm tailoring", "Discard changes", and "Delete profile".

On the right side, there are two panels:

- Selected Item Properties:** Shows fields for Title, ID, and Type, all currently empty. The Description field is also empty.
- Profile Properties:** Shows fields for Title (General-Purpose Systems [TAILORED]), ID (common_tailored-RHUG), and Description (This profile contains items common to general-purpose desktop and server installations).

OpenSCAP in Satellite 6

- Requirements

```
# mkdir -p /etc/puppet/environments/RHUG/modules
```

- Click on Configure → Environments

- Import from Satellite button

- Select “RHUG”

- Click Update

Changed environments

Select the changes you want to realize in Satellite

Toggle: [New](#) | [Updated](#) | [Obsolete](#)

<input checked="" type="checkbox"/>	Environment	Operation	Puppet Modules
<input type="checkbox"/>	KT_SkinnerLabs_LAB_RHEL7_VM2_11	Add:	access_insights_client , foreman_scap_client , and stdlib
<input type="checkbox"/>	KT_SkinnerLabs_Library_RHEL7_VM2_11	Add:	access_insights_client , foreman_scap_client , and stdlib
<input checked="" type="checkbox"/>	RHUG	Add:	access_insights_client , foreman_scap_client , and stdlib
<input type="checkbox"/>	example_env	Add:	access_insights_client , foreman_scap_client , and stdlib
<input type="checkbox"/>	production	Add:	access_insights_client , foreman_scap_client , and stdlib

Cancel

Update

OpenSCAP in Satellite 6

- Upload SCAP content into Satellite
- Grab content from RPM file: scap-security-guide
- Hosts → SCAP Contents
- /usr/share/xml/scap/ssg
- ssg-rhel7-ds.xml

Upload new SCAP content file

File Upload Locations Organizations

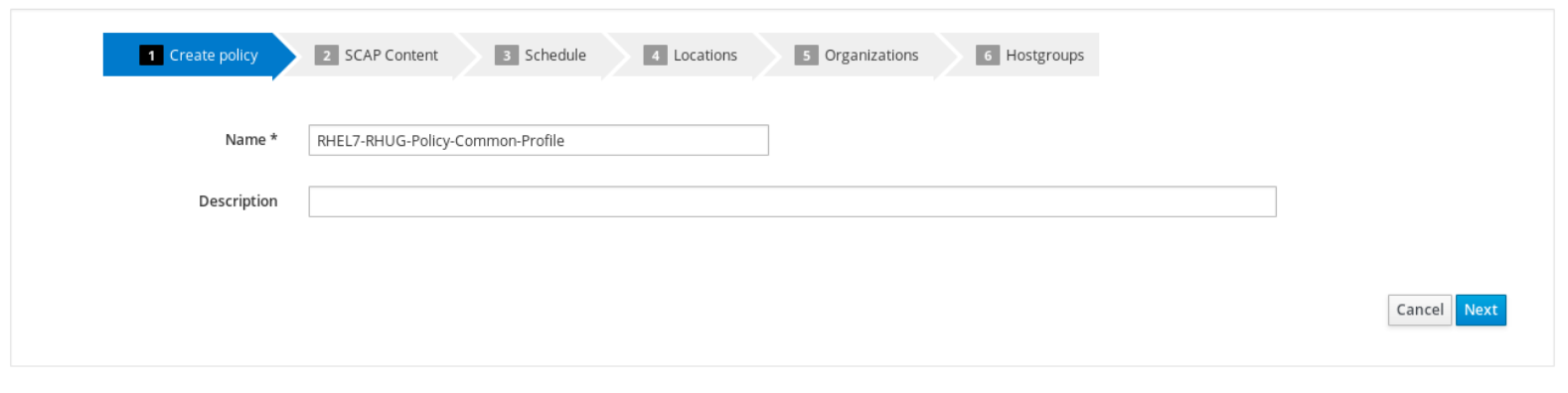
Title *

Scap file * No file selected.
Upload SCAP DataStream file

OpenSCAP in Satellite 6

- New Compliance Policy
- Hosts → Policy

New Compliance Policy



1 Create policy

2 SCAP Content

3 Schedule

4 Locations

5 Organizations

6 Hostgroups

Name *

Description

Cancel Next

OpenSCAP in Satellite 6

- **New Compliance Policy – select SCAP Content**

New Compliance Policy

1 Create policy 2 SCAP Content 3 Schedule 4 Locations 5 Organizations 6 Hostgroups

SCAP Content: RHEL7-RHUG-default

XCCDF Profile: Common Profile for General-Purpose Systems

- Default XCCDF profile
- Standard System Security Profile
- Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
- Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
- Common Profile for General-Purpose Systems**
- Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server

Cancel Next

OpenSCAP in Satellite 6

- New Compliance Policy – select schedule

New Compliance Policy

The screenshot displays the 'New Compliance Policy' wizard interface. At the top, a progress bar shows six steps: 1. Create policy, 2. SCAP Content, 3. Schedule (highlighted in blue), 4. Locations, 5. Organizations, and 6. Hostgroups. Below the progress bar, there are two input fields: 'Period' with a dropdown menu set to 'Custom', and 'Cron line' with a text input field containing '15 * * * *'. To the right of the 'Cron line' field is a help text: 'You can specify custom cron line, e.g. "0 3 * * *", separate each of 5 values by space'. At the bottom left is a back arrow button, and at the bottom right are 'Cancel' and 'Next' buttons.

OpenSCAP in Satellite 6

- New Compliance Policy – select Location/Organization ...
- Select Hostgroups

New Compliance Policy

1 Create policy 2 SCAP Content 3 Schedule 4 Locations 5 Organizations 6 Hostgroups

Hostgroups

All Items Filter +

RHUG-OpenSCAP

Rhlab-VM

Selected Items

OpenShift

<

Cancel Submit

OpenSCAP in Satellite 6

- Assign Policy to Hosts
- Hosts → All Hosts → Select Action
- Assign Compliance Policy

Assign Compliance Policy - The following hosts are about to be changed

Name	Host group	Environment	Location	Organization
node2.openshift.skinnerlabs.com	OpenShift	RHUG	Default Location	SkinnerLabs
master1.openshift.skinnerlabs.com	OpenShift	RHUG	Default Location	SkinnerLabs
node1.openshift.skinnerlabs.com	OpenShift	RHUG	Default Location	SkinnerLabs

Keep selected hosts for a future action

RHEL7-RHUG-Policy-Commq

Cancel Submit

Select Action

- Change Group
- Build Hosts
- Change Environment
- Edit Parameters
- Disable Notifications
- Enable Notifications
- Disassociate Hosts
- Rebuild Config
- Assign Organization
- Assign Location
- Change Owner
- Change Puppet Master
- Change Puppet CA
- Change Power State
- Delete Hosts
- Assign Compliance Policy
- Unassign Compliance Policy
- Run Job

OpenSCAP in Satellite 6

- Wait 15 minutes or run manually on each client
- `# foreman_scap_client 3`

- Policy number can be found in `/etc/foreman_scap_client/config.yaml`

OpenSCAP in Satellite 6

- Hosts → Policies → Your Policy

Compliance policy: RHEL7-RHUG-Policy-Common-Profile

Hosts Breakdown

- Compliant with the policy
0
- Not compliant with the policy
3
- Inconclusive results
0
- Never audited
0

Total hosts: 3

Host Breakdown Chart



Latest reports for policy: RHEL7-RHUG-Policy-Common-Profile

Host	Date	Passed	Failed	Other	
node2.openshift.skinnerlabs.com	less than a minute ago	9	20	0	View Report
node1.openshift.skinnerlabs.com	less than a minute ago	9	20	0	View Report
master1.openshift.skinnerlabs.com	4 minutes ago	9	20	0	View Report



OpenSCAP in Satellite 6

node2.openshift.skinnerlabs.com

Show log messages:

All messages



View full report

Download XML in bzip

Reported at 2016-09-20 15:10:10 -0500

Severity	Message	Resource	Result
Low	Ensure /var/log Located On Separate Partition	xccdf_org.ssgproject.content_...	fail
Low	Ensure /var/log/audit Located On Separate Partition	xccdf_org.ssgproject.content_...	fail
Low	Disable the Automounter	xccdf_org.ssgproject.content_...	pass
Medium	Ensure rsyslog is Installed	xccdf_org.ssgproject.content_...	pass
Medium	Enable rsyslog Service	xccdf_org.ssgproject.content_...	pass
Low	Record attempts to alter time through adjtimex	xccdf_org.ssgproject.content_...	fail
Low	Record attempts to alter time through settimeofday	xccdf_org.ssgproject.content_...	fail
Low	Record Attempts to Alter Time Through stime	xccdf_org.ssgproject.content_...	fail
Low	Record Attempts to Alter Time Through clock_settime	xccdf_org.ssgproject.content_...	fail
Low	Record Attempts to Alter the localtime File	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify User/Group Information	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Network Environment	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Mandatory Access Controls	xccdf_org.ssgproject.content_...	fail

OpenSCAP in Satellite 6

Title	Severity	Result
▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 7 29x fail		
▶ Introduction		
▼ System Settings 29x fail		
▼ Installing and Maintaining Software 2x fail		
▼ Disk Partitioning 2x fail		
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
▶ Updating Software		
▶ Software Integrity Checking		
▼ File Permissions and Masks		



OpenSCAP in Satellite 6

Ensure /var/log Located On Separate Partition

Rule ID	xccdf_org.ssgproject.content_rule_partition_for_var_log
Result	fail
Time	2016-09-20T15:09:59
Severity	low
Identifiers and References	identifiers: CCE-26967-0 references: AU-9 , SC-32 , http://iase.disa.mil/stigs/cci/Pages/index.aspx , Test attestation on 20120928 by MM
Description	System logs are stored in the <code>/var/log</code> directory. Ensure that it has its own partition or logical volume at installation time, or migrate it using LVM.
Rationale	Placing <code>/var/log</code> in its own partition enables better separation between log files and other files in <code>/var/</code> .

OVAL details

Items not found violating `/var/log on own partition` :

Object `oval:ssg:obj:1021` of type `partition_object`

Mount point
<code>/var/log</code>

OpenSCAP in Satellite 6

- Hosts → Reports

Compliance Reports

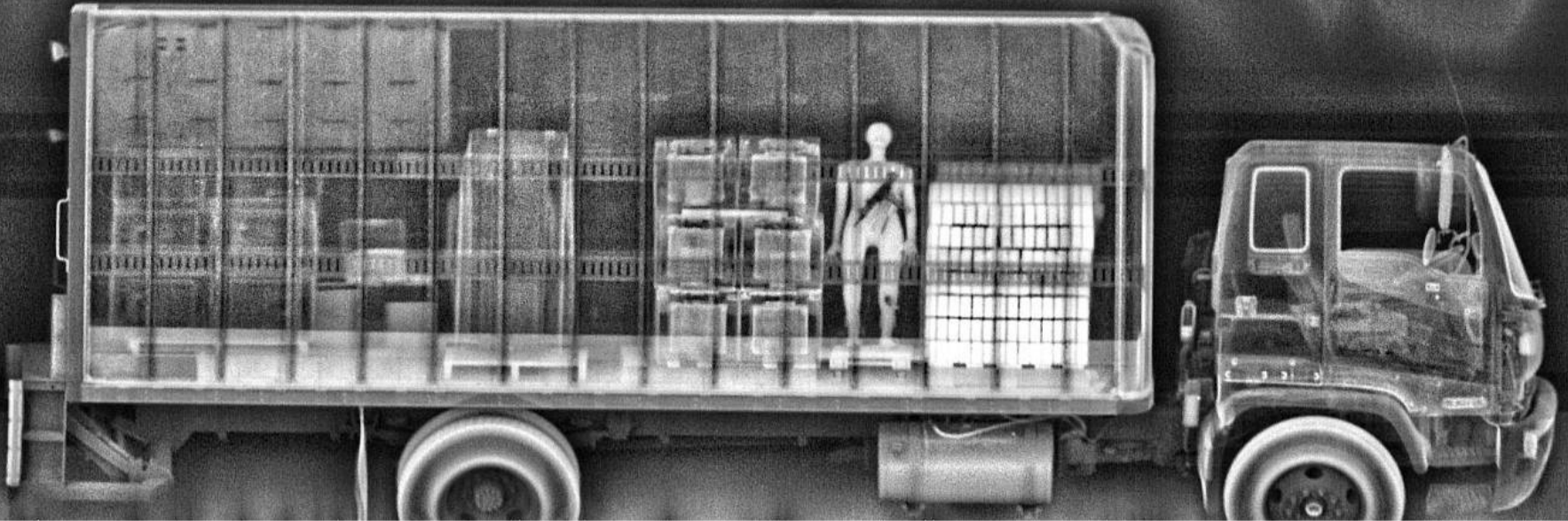
Filter ... × Q Search ▾

<input type="checkbox"/>	Host	Reported At	Passed	Failed	Other	
<input type="checkbox"/>	master1.openshift.skinnerlabs.com	4 minutes ago	9	29	0	Delete
<input type="checkbox"/>	node2.openshift.skinnerlabs.com	4 minutes ago	9	29	0	Delete
<input type="checkbox"/>	node1.openshift.skinnerlabs.com	4 minutes ago	9	29	0	Delete
<input type="checkbox"/>	node2.openshift.skinnerlabs.com	9 minutes ago	9	29	0	Delete
<input type="checkbox"/>	node1.openshift.skinnerlabs.com	9 minutes ago	9	29	0	Delete
<input type="checkbox"/>	master1.openshift.skinnerlabs.com	12 minutes ago	9	29	0	Delete
<input type="checkbox"/>	node1.openshift.skinnerlabs.com	16 minutes ago	9	29	0	Delete
<input type="checkbox"/>	node2.openshift.skinnerlabs.com	16 minutes ago	9	29	0	Delete

Displaying all 8 entries

OpenSCAP in CloudForms

CONTAINER SCANNING WITH CLOUDFORMS



Cloud Intel >

Red Hat Insights >

Services >

Compute >

Configuration >

Networks >

Control >

Automate >

Optimize >

← ↻ ⚙ Configuration ▾

▾ Policy Profiles

▾ All Policy Profiles

▾ OpenSCAP profile

▾ **Image Compliance:** OpenSCAP

◆ Has high severity OpenSCAP rule results

▾ **Container Image Compliance Check**

⊗ Mark as Non-Compliant

▾ **Image Control:** Analyse incoming container images

▾ **Container Image Discovered**

⊗ Initiate SmartState Analysis for Container Image

> Policies

> Events

> Conditions



> Actions

> Alert Profiles

> Alerts

Policy Profile "OpenSCAP profile"

Policies

	Image Compliance: OpenSCAP
	Image Control: Analyse incoming container images

Notes


 No notes have been entered.

Policy "OpenSCAP"

Basic Information

Active	Yes
Created	By Username admin on 05/25/16 at 21:06:01 UTC


Scope

 No Policy scope defined, the scope of this policy includes all elements.

Conditions

	Description	Scopes / Expressions
	Has high severity OpenSCAP rule results	ExpressionFIND Image.Openscap Rule Results : Result = "fail" CHECK ANY Severity = "High"

Events

	Description	Actions
	Container Image Compliance Check	✘ Mark as Non-Compliant

Cloud Intel >

Red Hat Insights >

Services >

Compute >

Configuration >

Networks >

Control >

Automate >

Configuration ▾

Policy ▾



Perform SmartState Analysis

No filters defined.

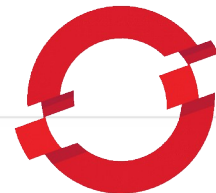
Images

		Name ▲	Provider	Tag	Id
<input type="checkbox"/>		openshift3/ose-docker-registry	zoseaio	v3.2.1.13	docker://sha256:
<input checked="" type="checkbox"/>		openshift3/ose-haproxy-router	zoseaio	v3.2.1.13	docker://sha256:
<input type="checkbox"/>		registry.access.redhat.com/openshift3/image-inspector	zoseaio	2.0	docker://sha256:
<input type="checkbox"/>		registry.access.redhat.com/openshift3/metrics-cassandra	zoseaio	3.2.1	docker://sha256:
<input type="checkbox"/>		registry.access.redhat.com/openshift3/metrics-deployer	zoseaio	3.2.1	docker://sha256:



Overview

Overview



Filter by label

Add



Browse


POD: MANAGEIQ-IMG-SCAN-CF3DA

created 24



CONTAINER: IMAGE-INSPECTOR

 Image: openshift3/image-inspector

 Ports: 8080/TCP



Settings



Overview



Browse

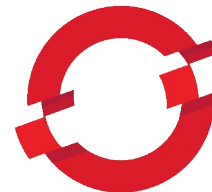


Settings

Pods » manageiq-img-scan-cf3da

manageiq-img-scan-cf3da created 27 minutes ago

manageiq.org true name manageiq-img-scan-cf3da



Details Environment Metrics Logs Terminal Events

Container: image-inspector — Running Log from 9/18/16 9:43 PM

```
1 | 2016/09/18 22:43:35 package webdav requires Go version 1.5 or greater
2 | 2016/09/18 22:43:35 Image openshift3/ose-haproxy-router:v3.2.1.13 is available, skipping image pull
3 | 2016/09/18 22:43:36 Extracting image openshift3/ose-haproxy-router:v3.2.1.13 to /var/tmp/image-inspector-174896965
4 | 2016/09/18 22:43:46 OpenSCAP scanning /var/tmp/image-inspector-174896965. Placing results in /var/tmp/image-inspector-scan-results-954348512
5 | 2016/09/18 22:44:00 Serving image content /var/tmp/image-inspector-174896965 on webdav://0.0.0.0:8080/api/v1/content/
```

Cloud Intel >

Red Hat Insights >

Services >

Compute >

Configuration >

Networks >

Control >

Automate >

Optimize >

Settings >

⚙ Configuration ▾

🛡 Policy ▾



Images » openshift3/ose-haproxy-router (Summary)

openshift3/ose-haproxy-router (Summary)

Properties	
Name	openshift3/ose-haproxy-router
Tag	v3.2.1.13
Image Id	docker://sha256:f8e807bd101b9b6b35bf85132f6a9bca76436b823d77fd67d841118cacb76562
Full Name	openshift3/ose-haproxy-router:v3.2.1.13

Compliance	
Status	Never Verified
History	Not Available

Relationships	
Containers Provider	zoseaio
Image Registry	Unknown image source
Projects	1
Pods	1
Containers	1
Nodes	1

Smart Management	
Jozwiak Tags	No Jozwiak Tags have been assigned

Configuration	
Packages	0
OpenSCAP Results	1076
OpenSCAP HTML	Available

OpenSCAP Failed Rules Summary	
Medium	1



Evaluation Characteristics

Target machine	manageiq-img-scan-cf3da
Benchmark URL	/tmp/com.redhat.rhsa-RHEL6.ds.xml.bz2
Benchmark ID	xccdf_com.redhat.rhsa_benchmark_generated-xccdf
Started at	2016-09-18T22:43:58
Finished at	2016-09-18T22:43:58

CPE Platforms

Addresses

- IPv4 __127.0.0.1
- IPv4 __10.1.0.6
- IPv6 __0:0:0:0:0:0:1
- IPv6 __fe80:0:0:0:42:aff:fe01:6
- MAC __00:00:00:00:00:00
- MAC __02:42:0A:01:00:06

Compliance and Scoring

The target system did not satisfy the conditions of 1 rules! Please review rule results and consider applying remediation.

Rule results

1075 passed

Severity of failed rules

1 medium

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	99.907066	100.000000	99.91%

Resources

- RHEL 7 Security Guide

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-Compliance_and_Vulnerability_Scanning.html

- Satellite 6.2 Security Compliance

<https://access.redhat.com/documentation/en/red-hat-satellite/6.2/paged/host-configuration-guide/chapter-4-security-compliance-management>

- CloudForms 4.1 OpenSCAP Integration

<https://access.redhat.com/documentation/en/red-hat-cloudforms/4.1/policies-and-profiles-guide/policies-and-profiles-guide#openscap>



THANK YOU



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos

Fedora Orange

