



OPENSAP AND SATELLITE 6

Michael Lessard

Senior Solutions Architect

mlessard@redhat.com

 [michaellessard](#)

What is SCAP?

<http://goo.gl/GBailW>

WHAT IS SCAP ?

Security Content Automation Protocol

The 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 GOAL : BE PROACTIVE

SCAP COMPONENTS

SCAP encompassed several underlying standards. The component standards of SCAP include:

Languages:

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

Enumerations:

- CCE: Common Configuration Enumeration: an enumeration of security-relevant configuration elements for applications and operating systems
- CPE: Common Platform Enumeration: Is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets
- CVE®: Common Vulnerabilities and Exposures: is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."

Metrics:

- CVSS: Common Vulnerability Scoring System: metrics to assign a score to software vulnerabilities to help users prioritize risk.
- CCSS: Common Configuration Scoring System: metrics to assign a score to security-relevant configuration elements to help users prioritize responses.

CHECKLIST
LANGUAGE

XCCDF

CHECK INSTRUCTION
LANGUAGES

OVAL

OCIL

ENUMERATIONS

CCE

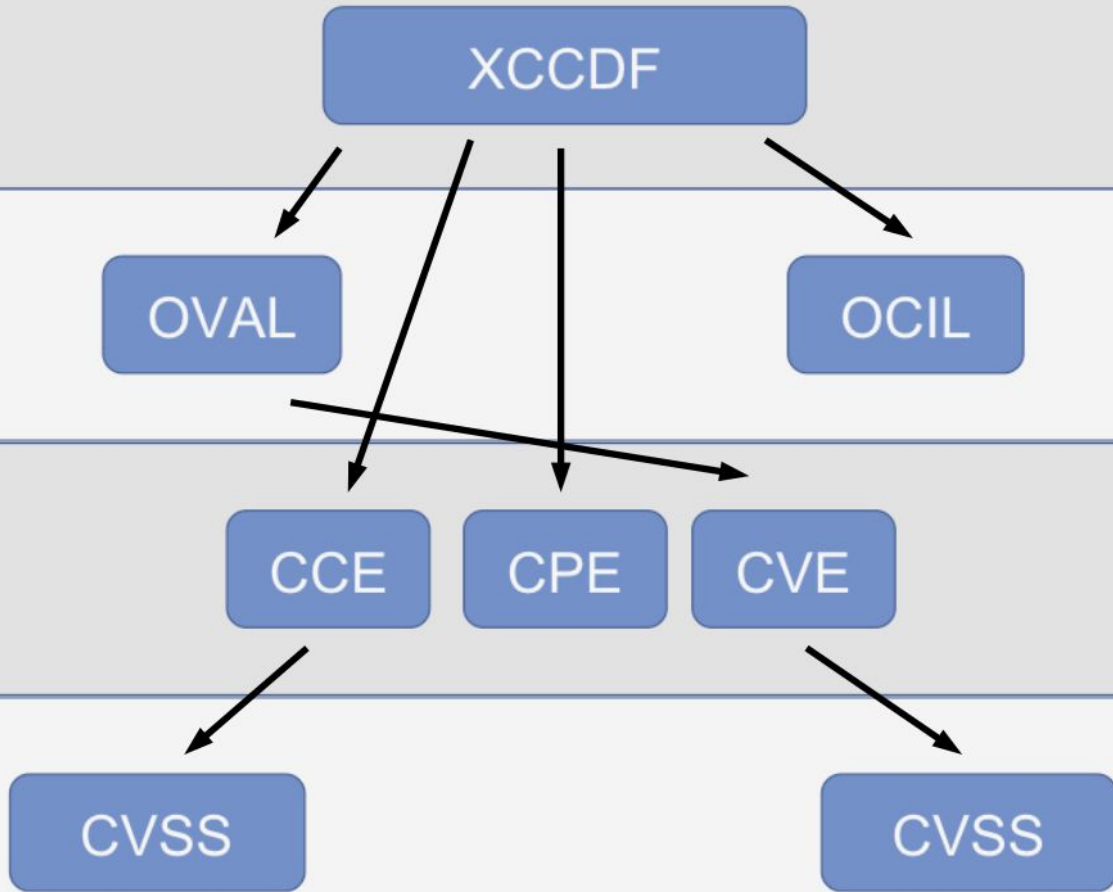
CPE

CVE

RISK MEASUREMENT

CVSS

CVSS



What is OPENSCAP?

WHAT IS OPENS CAP ?

A framework of libraries and tools to improve the accessibility of SCAP and enhance the usability of the information it represents.

OpenSCAP components:

- Library - OpenSCAP library provides API to SCAP document processing and evaluation.
- Toolkit - SCAP scanner (oscap) is a command line tool that provides various SCAP capabilities; for instance: configuration scanner, vulnerability scanner, SCAP content validation and transformation etc.

On 04/29/2014 OpenSCAP project received SCAP 1.2 certification from NIST.

- <http://nvd.nist.gov/scapproducts.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.

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.

Openscap and Satellite 6

CONFIGURE OPENSCAP FOR SATELLITE 6 (1/4)

```
[root@satellite ~]# satellite-installer --enable-foreman-plugin-openscap
[root@satellite ~]# yum install puppet-foreman_scap_client
[root@satellite ~]# systemctl restart foreman-proxy
[root@satellite ~]# mkdir -p /etc/puppet/environments/production/modules
```

1. Load the openscap content to the Satellite server

```
[root@satellite ~]# foreman-rake foreman_openscap:bulk_upload:default
```

2. Import the foreman_scap_client puppet class to your Satellite server

- In the Satellite web ui, select Any organization and any location
- Go to the Configure -> Environments.
- Click the Import button.

CONFIGURE OPENS CAP FOR SATELLITE 6 (2/4)

3. Create new SCAP Content.

- Go to the Hosts -> Compliance -> SCAP contents page.
- Upload the DataStream file if you are using custom content. **Note:** Red Hat preloads the content of the **SCAP Security Guide** as a courtesy, so you do not need to upload that.
- If you do not see the preloaded SCAP content, you may need to change your Satellite organization to "Any Context". Then assign the appropriate organization

CONFIGURE OPENS CAP FOR SATELLITE 6 (3/4)

4. Create a new Policy.

- Go to the Hosts -> Compliance -> Policies page.
- Assign 'SCAP Content' to the Policy
- Select 'XCCDF Profile' from your SCAP Content
- Define a periodic scan schedule.
- Assign Hostgroups to the policy (hosts you want to audit should be assigned with one of the hostgroups).

CONFIGURE OPENS CAP FOR SATELLITE 6 (4/4)

(Optional)

5. Select particular hosts for a compliance audit.

- Go to the Hosts -> All hosts page
- Select a host
- Use the Select Action -> Assign Compliance Policy button
- Select the policy you want to apply to the host

FORCE OPENS CAP EXECUTION

To test a policy

On a host

```
[root@host1 ~]# puppet agent -t
```

```
[root@host1 ~]# foreman_scap_client 1 (or check in /var/spool/cron/root for id)
```

On Satellite

```
[root@satellite ~]# smart-proxy-openscap-send  
(log : /var/log/foreman-proxy/openscap-send.log)
```

Hosts -->> Reports

(you should see the report)

demo.mlc.dom

Show log messages:

[Back](#)
[Delete](#)
[Host details](#)
[View full report](#)
[Download XML in bz1](#)

Reported at 2017-01-26 16:07:37 UTC

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
Low	Record Events that Modify the System's Discretionary Access Controls - chmod □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - chown □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - fchmod □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - fchmodat □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - fchown □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - fchownat □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - fremovexattr □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - fsetxattr □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - lchown □	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - lremovexattr □	xccdf_org.ssgproject.content_...	fail

Compliance and Scoring

The target system did not satisfy the conditions of 29 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	75.000000	100.000000	 75%

Rule Overview

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

REFERENCE

Satellite 6.2 Openscap doc

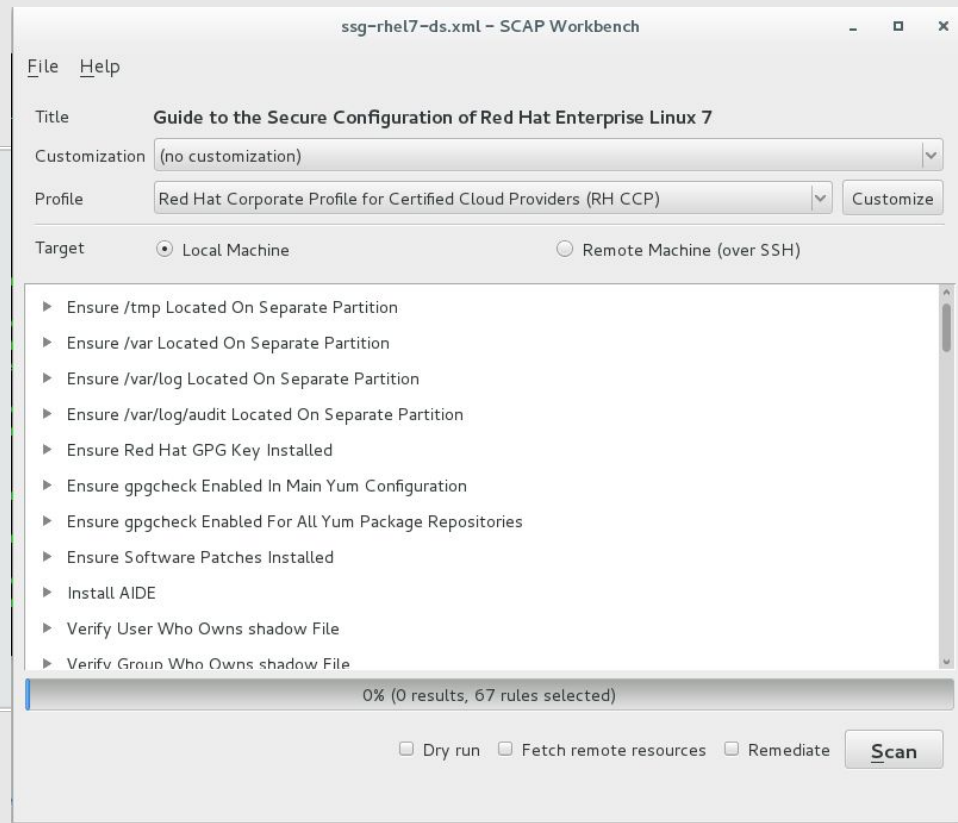
<http://red.ht/2kGaMdZ>

Customize a SCAP security guide

SCAP WORKBENCH

To launch a local openscap scan or to edit a scap profile, you can use scap workbench

```
# yum install openscap-workbench
```



SCAP Tailoring

Details on how to use tailoring option with openscap-workbench

<https://www.open-scap.org/resources/documentation/customizing-scap-security-guide-for-your-use-case/>

Tailoring file are not supported yet with Satellite 6.2

https://bugzilla.redhat.com/show_bug.cgi?id=1292510

SCAP Tailoring with Satellite 6 workaround

You will need to merge the files using this script :






<https://github.com/mpreisler/combine-tailoring/blob/master/combine-tailoring.py>

```
./combine-tailoring.py /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml  
ssg-rhel7-ds-tailoring.xml --output ssg-rhel7-ds-merged.xml
```

The ssg-rhel7-ds-merged.xml can be uploaded to Satellite 6, the customized profile will show up in the profile selector dialog.

SCAP Contents

   Search [Upload New SCAP Content](#) [Help](#)

Title	Filename	Created	
michael-test	ssg-rhel7-ds-merged.xml	14 days ago	Edit 
Red Hat firefox default content	ssg-firefox-ds.xml	6 months ago	Edit 
Red Hat jre default content	ssg-jre-ds.xml	6 months ago	Edit 
Red Hat rhel7 default content	ssg-rhel7-ds.xml	about 1 year ago	Edit 
Red Hat rhel7 default content	ssg-rhel7-ds.xml	6 months ago	Edit 



THANK YOU



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos