



RHN Satellite OpenSCAP Primer

Marc Skinner

What is OpenSCAP?

- Open source implementation of SCAP
 - SCAP: Standardized compliance checking solution developed by NIST for maintaining system security.
- Specifically, it is an auditing tool
 - Utilizes XCCDF: Extensible Configuration Checklist Description Format
 - ??? - Standard way of defining content to scan
- How to use?
 - RHN Satellite version 5.5 includes OpenSCAP
 - Need SCAP content – rules to scan
 - From scratch?
 - From online resources like NIST
 - From RH



Walk through example

- Install Red Hat provided SCAP definitions on Satellite
 - Join RHEL 6 Optional Channel
 - Install openscap-content RPM
 - [root@sat ~]# rpm -ql openscap-content
 - /usr/share/openscap/scap-oval.xml
 - /usr/share/openscap/scap-rhel6-oval.xml
 - /usr/share/openscap/scap-rhel6-xccdf.xml
 - /usr/share/openscap/scap-xccdf.xml
 - scp scap-rhel6-xccdf.xml and scap-rhel6-oval.xml to client
- Client
 - Join RHEL 6 RHN Tools Channel
 - Install spacewalk-oscapp RPM from Satellite
 - Install osad if you haven't – osad lets you schedule tasks in Satellite
 - Start osad or you'll have to manually rhn_check



On Satellite :: Schedule scan

 openscap.cloud. [redacted]

[+ add to ssm](#) | [- delete system](#)

[Details](#) [Software](#) [Configuration](#) [Provisioning](#) [Groups](#) [Audit](#) [Events](#)

[List Scans](#) [Schedule](#)

Schedule New XCCDF Scan

Command:	/usr/bin/oscaped eval
Command-line Arguments:	<input type="text" value="--profile RHEL6-Default"/>
Path to XCCDF document*:	<input type="text" value="/usr/local/scap/scap-rhel6-xccdf.xml"/>
Schedule no sooner than:	February 20 2013 11:33 PM EST

Schedule

Tip: Certain versions of OpenSCAP may require the --profile command-line argument. --profile specifies a particular profile from the XCCDF document.



List Scans :: Baseline, then Pass

OpenSCAP Scans

1 - 3 of 3

Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
OSCAP-Test-RHEL6-Default	Wed Feb 20 22:30:08 CST 2013	96 %	71	3	0	0	0	0	69	0	0	143
OSCAP-Test-RHEL6-Default	Wed Feb 20 09:57:51 CST 2013	96 %	71	3	0	0	0	0	69	0	0	143
OSCAP-Test-default-profile	Wed Feb 20 09:45:09 CST 2013	N/A	0	0	0	0	0	0	143	0	0	143

1 - 3 of 3

[Download CSV](#)

Tip: Compliance column represents unweighted pass/fail ration. Compliance = $P / (Total - S - I)$.

Xccdf Legend

- P - Pass
- F - Fail
- E - Error
- U - Unknown
- N - Not applicable
- K - Not checked
- S - Not selected
- I - Informational
- X - Fixed



Break Client

- `service auditd stop`
- `chkconfig auditd off`



Client changes :: Scan Fails

openscap.cloud.l[REDACTED]





[+ add to ssm](#) | [- delete system](#)

[Details](#) [Software](#) [Configuration](#) [Provisioning](#) [Groups](#) [Audit](#) [Events](#)

[List Scans](#) [Schedule](#)

OpenSCAP Scans

1 - 4 of 4

Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
 OSCAP-Test-RHEL6-Default	Wed Feb 20 22:42:22 CST 2013	95 %	70	4	0	0	0	0	69	0	0	143
 OSCAP-Test-RHEL6-Default	Wed Feb 20 22:30:08 CST 2013	96 %	71	3	0	0	0	0	69	0	0	143
 OSCAP-Test-RHEL6-Default	Wed Feb 20 09:57:51 CST 2013	96 %	71	3	0	0	0	0	69	0	0	143
 OSCAP-Test-default-profile	Wed Feb 20 09:45:09 CST 2013	N/A	0	0	0	0	0	0	143	0	0	143

1 - 4 of 4

 [Download CSV](#)

Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

N - Not applicable

K - Not checked

S - Not selected

I - Informational

X - Fixed



Client side :: Manual run for detailed report

- `oscap xccdf eval --results result2.xml --report report2.html --oval-results --profile RHEL6-Default scap-rhel6-xccdf.xml scap-rhel6-oval.xml`

OVAL: Open Vulnerability and Assessment Language

```
(root) openscap.cloud - Konsole
File Edit View Bookmarks Settings Help
Rule ID: rule-1103
Title: Configure number of sent router solicitations
Result: pass
Rule ID: rule-1104
Title: Configure whether to accept router preference
Result: pass
Rule ID: rule-1105
Title: Configure whether to accept path information
Result: pass
Rule ID: rule-1106
Title: Configure whether to accept default router information
Result: pass
Rule ID: rule-1107
Title: Configure whether to autoconfigure addresses
Result: pass
Rule ID: rule-1108
Title: Configure number of duplicate address detection probes
Result: pass
Rule ID: rule-1109
Title: Configure maximum number of autoconfigured addresses
Result: pass
Rule ID: rule-1111
Title: ip6tables service is enabled
Result: pass
Rule ID: rule-1112
Title: iptables service is enabled
Result: pass
Rule ID: rule-1120
Title: Rsyslog service is enabled
Result: pass
Rule ID: rule-1121
Title: User ownership of System Log Files
Result: pass
```



For failure details, look at html report on client

Result for Auditd service is enabled

Result: **fail**

Rule ID: **rule-1127**

Time: **2013-02-20 22:43**

Severity: **medium**

The auditd service should be enabled.

Security identifiers

- CCE-4292-9

Check whether the auditd service is enabled in runlevels 3 and 5

service name	runlevel	start	kill
auditd	3	false	true
auditd	5	false	true

[results summary](#)

XCCDF Result Report, Generated by OpenSCAP on 2013-02-20 22:43

CCE: Common Configuration Enumeration
<http://cce.mitre.org>



Inspect SCAP template for rule details

```
.  
. .  
.  
<Rule id="rule-1127" selected="false" weight="10.000000" severity="medium">  
  <status date="2010-07-01">accepted</status>  
  <title xml:lang="en-US">Auditd service is enabled</title>  
  <description xml:lang="en-US">The auditd service should be  
enabled.</description>  
  <ident system="http://cce.mitre.org">CCE-4292-9</ident>  
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">  
    <check-content-ref name="oval:org.open-scap.rhel6:def:1127" href="scap-rhel6-  
oval.xml"/>  
  </check>  
</Rule>
```



In Conclusion

- Create SCAP rules
- Deploy
- Baseline
- Schedule scans
- Stay in compliance



Resources:

http://www.open-scap.org/page/Main_Page

<http://cce.mitre.org/>

<http://oval.mitre.org/>

<http://scap.nist.gov/specifications/xccdf/>

https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Network_Satellite/5.5/html/User_Guide/chap-Red_Hat_Network_Satellite-User_Guide-OpenSCAP.html

