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
COMPLIANCE
Common Criteria (CC)

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 (e.g. Integrated Circuits IC’s)

EAL7: Formally Verified Design and Tested
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/scappproducts.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.


- 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

Security Policy

Choose profile below:

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.

Changes that were done or need to be done:
- 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**
  
  ```bash
  # 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
### Guide to the Secure Configuration of Red Hat Enterprise Linux 7

<table>
<thead>
<tr>
<th>Rule</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure /var/log Located On Separate Partition</td>
<td></td>
</tr>
<tr>
<td>Ensure /var/log/audit Located On Separate Partition</td>
<td></td>
</tr>
<tr>
<td>Disable the Automounter</td>
<td></td>
</tr>
<tr>
<td>Ensure rsyslog is Installed</td>
<td></td>
</tr>
<tr>
<td>Enable rsyslog Service</td>
<td></td>
</tr>
<tr>
<td>Record attempts to alter time through adjtimex</td>
<td></td>
</tr>
<tr>
<td>Record attempts to alter time through settimeofday</td>
<td></td>
</tr>
<tr>
<td>Record Attempts to Alter Time Through stime</td>
<td></td>
</tr>
<tr>
<td>Record Attempts to Alter Time Through clock_settime</td>
<td></td>
</tr>
<tr>
<td>Record Attempts to Alter the localtime File</td>
<td></td>
</tr>
<tr>
<td>Record Events that Modify User/Group Information</td>
<td></td>
</tr>
<tr>
<td>Record Events that Modify the System's Network Environment</td>
<td></td>
</tr>
<tr>
<td>Record Events that Modify the System's Mandatory Access Controls</td>
<td></td>
</tr>
<tr>
<td>Record Events that Modify the System's Discretionary Access Controls</td>
<td></td>
</tr>
<tr>
<td>Record Events that Modify the System's Discretionary Access Controls</td>
<td></td>
</tr>
</tbody>
</table>

**Tailoring:** (no tailoring)

**Profile:** Common Profile for General-Purpose Systems

**Target:** local machine

---

**scap-workbench**
scap-workbench scanning...
scap-workbench tailoring...
OpenSCAP in Satellite 6

- **Requirements**
  
  ```bash
  # mkdir -p /etc/puppet/environments/RHUG/modules
  ```

- **Click on Configure → Environments**
- **Import from Satellite button**
- **Select “RHUG”**
- **Click 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
OpenSCAP in Satellite 6

- New Compliance Policy
- Hosts → Policy
OpenSCAP in Satellite 6

- New Compliance Policy – select SCAP Content
OpenSCAP in Satellite 6

- New Compliance Policy – select schedule
OpenSCAP in Satellite 6

- New Compliance Policy – select Location/Organization ...
- Select Hostgroups
OpenSCAP in Satellite 6

- Assign Policy to Hosts
- Hosts → All Hosts → Select Action
- Assign Compliance Policy
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
OpenSCAP in Satellite 6

```
node2.openshift.skinnerlabs.com

Show log messages:
- All messages

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Resource</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Ensure /var/log Located On Separate Partition</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Ensure /var/log/audit Located On Separate Partition</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Disable the Automounter</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Pass</td>
</tr>
<tr>
<td>Medium</td>
<td>Ensure rsyslog is Installed</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Pass</td>
</tr>
<tr>
<td>Medium</td>
<td>Enable rsyslog Service</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Pass</td>
</tr>
<tr>
<td>Low</td>
<td>Record attempts to alter time through adjtime</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Record attempts to alter time through settimeofday</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Record Attempts to Alter Time Through strftime</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Record Attempts to Alter Time Through clock_settime</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Record Attempts to Alter the localtime File</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Record Events that Modify User/Group Information</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Record Events that Modify the System’s Network Environment</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
<tr>
<td>Low</td>
<td>Record Events that Modify the System’s Mandatory Access Controls</td>
<td>xccdf_org.ssgproject.content...</td>
<td>Fail</td>
</tr>
</tbody>
</table>

Reported at 2016-09-20 15:10:10 -0500
```
OpenSCAP in Satellite 6

<table>
<thead>
<tr>
<th>Title</th>
<th>Severity</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guide to the Secure Configuration of Red Hat Enterprise Linux 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installing and Maintaining Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Partitioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure /var/log Located On Separate Partition</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Ensure /var/log/audit Located On Separate Partition</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Updating Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Integrity Checking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Permissions and Masks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OpenSCAP in Satellite 6

<table>
<thead>
<tr>
<th>Rule ID</th>
<th>xccdf_org.ssgproject.content_rule_partition_for_var_log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>fail</td>
</tr>
<tr>
<td>Time</td>
<td>2016-06-20T15:09:59</td>
</tr>
<tr>
<td>Severity</td>
<td>low</td>
</tr>
<tr>
<td>Identifiers and References</td>
<td>CCE-26987.0, AU-9, SC-32, <a href="http://iase.disa.mil/stigs/cci/Pages/Index.aspx">http://iase.disa.mil/stigs/cci/Pages/Index.aspx</a>, Test attestation on 20120928 by MM</td>
</tr>
<tr>
<td>Description</td>
<td>System logs are stored in the /var/log directory. Ensure that it has its own partition or logical volume at installation time, or migrate it using LVM.</td>
</tr>
<tr>
<td>Rationale</td>
<td>Placing /var/log in its own partition enables better separation between log files and other files in /var/.</td>
</tr>
</tbody>
</table>

Items not found violating /var/log on own partition
Object oavl:ssg:obj:1021 of type partition_object

Mount point
/var/log
OpenSCAP in Satellite 6

- Hosts → Reports
OpenSCAP in CloudForms
CONTAINER SCANNING WITH CLOUDFORMS
Policy Profile "OpenSCAP profile"

Policies

- **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

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Scopes / Expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has high severity OpenSCAP rule results</td>
<td>Expression FIND Image.Openscap Rule Results : Result = &quot;fail&quot; CHECK ANY Severity = &quot;High&quot;</td>
</tr>
</tbody>
</table>

Events

<table>
<thead>
<tr>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container Image Compliance Check</td>
<td>Mark as Non-Compliant</td>
</tr>
</tbody>
</table>
### Images

<table>
<thead>
<tr>
<th>Name</th>
<th>Provider</th>
<th>Tag</th>
<th>Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>openshift3/ose-docker-registry</td>
<td>zoseaio</td>
<td>v3.2.1.13</td>
<td>docker://sha256:</td>
</tr>
<tr>
<td>openshift3/ose-haproxy-router</td>
<td>zoseaio</td>
<td>v3.2.1.13</td>
<td>docker://sha256:</td>
</tr>
<tr>
<td>registry.access.redhat.com/openshift3/image-inspector</td>
<td>zoseaio</td>
<td>2.0</td>
<td>docker://sha256:</td>
</tr>
<tr>
<td>registry.access.redhat.com/openshift3/metrics-cassandra</td>
<td>zoseaio</td>
<td>3.2.1</td>
<td>docker://sha256:</td>
</tr>
<tr>
<td>registry.access.redhat.com/openshift3/metrics-deployer</td>
<td>zoseaio</td>
<td>3.2.1</td>
<td>docker://sha256:</td>
</tr>
</tbody>
</table>
Overview

POD: MANAGEIQ-IMG-SCAN-CF3DA

CONTAINER: IMAGE-INSPECTOR

- Image: openshift3/image-inspector
- Ports: 8080/TCP
2016/09/18 22:43:35 package webdav requires Go version 1.5 or greater
2016/09/18 22:44:00 Serving Image content /var/tmp/image-inspector-174896965 on webdav://0.0.0.0:8080/api/v1/content/
# openshift3/oсуe-haproxy-router (Summary)

## Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>openshift3/oсуe-haproxy-router</td>
</tr>
<tr>
<td>Tag</td>
<td>v3.2.1.13</td>
</tr>
<tr>
<td>Image Id</td>
<td>docker://sha256:f8ее807bd101b9b6b35bf85132f6a9bca76436b823d77fd67d841118cacb76562</td>
</tr>
<tr>
<td>Full Name</td>
<td>openshift3/oсуe-haproxy-router:v3.2.1.13</td>
</tr>
</tbody>
</table>

## Compliance

<table>
<thead>
<tr>
<th>Status</th>
<th>Never Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>Not Available</td>
</tr>
</tbody>
</table>

## Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Containers Provider</td>
<td>zoseaio</td>
</tr>
<tr>
<td>Image Registry</td>
<td>Unknown image source</td>
</tr>
<tr>
<td>Projects</td>
<td>1</td>
</tr>
<tr>
<td>Pods</td>
<td>1</td>
</tr>
<tr>
<td>Containers</td>
<td>1</td>
</tr>
<tr>
<td>Nodes</td>
<td>1</td>
</tr>
</tbody>
</table>

## Smart Management

No Jozwiak Tags have been assigned

## Configuration

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packages</td>
<td>0</td>
</tr>
<tr>
<td>OpenSCAP Results</td>
<td>1076</td>
</tr>
<tr>
<td>OpenSCAP HTML</td>
<td>Available</td>
</tr>
<tr>
<td>OpenSCAP Failed Rules Summary</td>
<td>Medium: 1</td>
</tr>
</tbody>
</table>
Evaluation Characteristics

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

CPE Platforms

<table>
<thead>
<tr>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
</tr>
<tr>
<td>IPv4</td>
</tr>
<tr>
<td>IPv6</td>
</tr>
<tr>
<td>IPv6</td>
</tr>
<tr>
<td>MAC</td>
</tr>
<tr>
<td>MAC</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Scoring system</th>
<th>Score</th>
<th>Maximum</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:xccdf:scoring:default</td>
<td>99.907066</td>
<td>100.000000</td>
<td>99.91%</td>
</tr>
</tbody>
</table>
Resources

- RHEL 7 Security Guide

- Satellite 6.2 Security Compliance

- CloudForms 4.1 OpenSCAP Integration
### Checklist

1.4.2. Threats to Server Security
1.4.3. Threats to Workstation and Home PC Security
1.5. Common Exploits and Attacks

### Tailoring

This combo box informs you about the current checklist version.