Security Automation for Containers and VMs with OpenSCAP

Martin Preisler, Red Hat, Inc., mpreisle@redhat.com
Marek Haicman, Red Hat, Inc., mhaicman@redhat.com

usenix
LISA17
October 29–November 3, 2017 | San Francisco, CA
www.usenix.org/lisa17 #lisa17

GOALS

- Hands on demos of real world use-cases
- Check software flaws - vulnerabilities
- Check configuration flaws - weaknesses
- Customizing existing security policies
- Put machines into compliance - remediate
- Automate everything
- Scale it to an infrastructure level

NON-GOALS

- We have very limited time
- Won’t cover extensive theory
- Won’t cover writing SCAP policies - out of scope

Feel free to catch us after the talk to discuss these!

FOLLOW ALONG!

- You can follow along the demos
- Red Hat Enterprise Linux 7 or CentOS 7 preferred
- Fedora, OpenSUSE, Debian or Ubuntu work in some cases
- We will use various distributions for demos

CHECKING FOR VULNERABILITIES

VULNERABILITY

what is a software vulnerability...

- can be exploited by a threat
- allows attacker to reduce information assurance
- can lead to compromise of security

VULNERABILITIES

Undiscovered vulnerabilities are bad.

- not known to the security community
- every complex system has them
- it’s a lot of effort to use those for exploits
- mitigate with SELinux or AppArmor

VULNERABILITIES

Known vulnerabilities are *much worse*.

- CVE-2017-5638
- details are released to the public
- ready-made exploits often publicly available
  - https://github.com/mazen160/struts-pwn
- mass exploits possible

VULNERABILITIES

Known vulnerabilities sometimes have *fancy names* and logos!

- Shellshock, POODLE, VENOM, …
- Heartbleed
- …
- mainstream visibility

VULNERABILITIES

Not all vulnerabilities are equal.

Let’s prioritize:

- all vulnerabilities are dangerous
- there is not much we can do about the undiscovered ones
- let’s **never** have any **known** ones in our infrastructure!

USE-CASE 1:
AUTOMATICALLY CHECK VULNERABILITIES

SCAP VULNERABILITY SCANNING

A standardized way to scan for vulnerabilities.

- prerequisites: CVE feed, SCAP scanner
- CVE feed contains a database of CVEs
    - with version ranges of affected software
    - supplied by software vendors

SCAP SCANNER - OPENSCAP

open-source SCAP 1.2 implementation

- SCAP is a protocol by NIST
- OpenSCAP is a library
- with a command-line interface **oscap**
- certified by NIST since 2014
- re-certified for new version

OpenSCAP
BASE

VULNERABILITY ASSESSMENT ON RHEL 6

Let’s discuss how to scan a single Red Hat Enterprise Linux 6 machine.

There are three steps to perform:

1. download the CVE data
2. execute the oscap tool
3. review the results

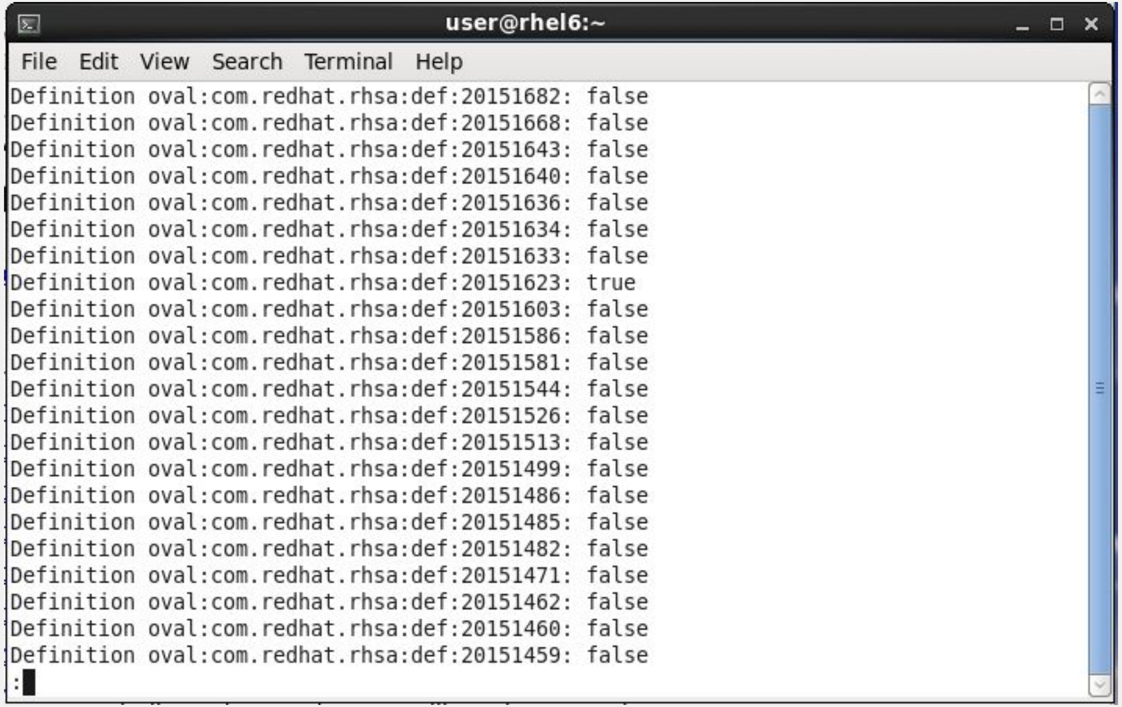
COMMANDS TO SCAN RHEL 6 FOR CVEs

Basic command …

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
# oscap oval eval Red_Hat_Enterprise_Linux_6.xml
```

VULNERABILITY SCAN RESULTS

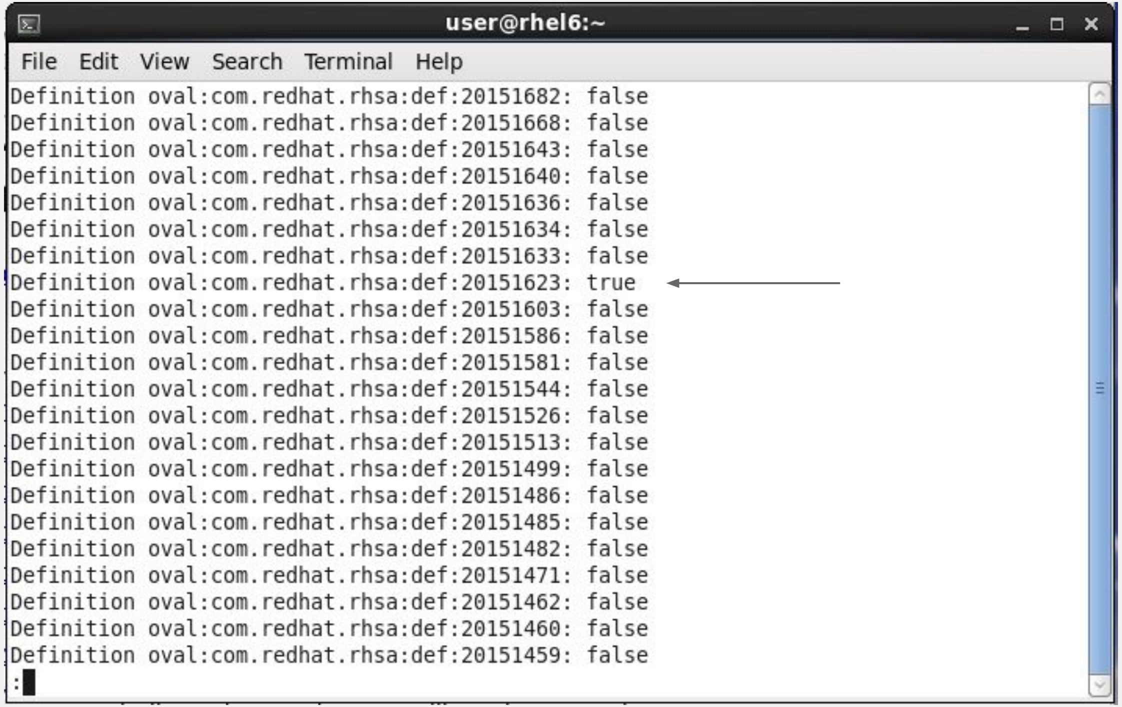
After the command is invoked this is what we can see in stdout.



```
Definition oval:com.redhat.rhsa:def:20151682: false
Definition oval:com.redhat.rhsa:def:20151668: false
Definition oval:com.redhat.rhsa:def:20151643: false
Definition oval:com.redhat.rhsa:def:20151640: false
Definition oval:com.redhat.rhsa:def:20151636: false
Definition oval:com.redhat.rhsa:def:20151634: false
Definition oval:com.redhat.rhsa:def:20151633: false
Definition oval:com.redhat.rhsa:def:20151623: true
Definition oval:com.redhat.rhsa:def:20151603: false
Definition oval:com.redhat.rhsa:def:20151586: false
Definition oval:com.redhat.rhsa:def:20151581: false
Definition oval:com.redhat.rhsa:def:20151544: false
Definition oval:com.redhat.rhsa:def:20151526: false
Definition oval:com.redhat.rhsa:def:20151513: false
Definition oval:com.redhat.rhsa:def:20151499: false
Definition oval:com.redhat.rhsa:def:20151486: false
Definition oval:com.redhat.rhsa:def:20151485: false
Definition oval:com.redhat.rhsa:def:20151482: false
Definition oval:com.redhat.rhsa:def:20151471: false
Definition oval:com.redhat.rhsa:def:20151462: false
Definition oval:com.redhat.rhsa:def:20151460: false
Definition oval:com.redhat.rhsa:def:20151459: false
:
```

VULNERABILITY SCAN RESULTS

After the command is invoked this is what we can see in stdout.



```
Definition oval:com.redhat.rhsa:def:20151682: false
Definition oval:com.redhat.rhsa:def:20151668: false
Definition oval:com.redhat.rhsa:def:20151643: false
Definition oval:com.redhat.rhsa:def:20151640: false
Definition oval:com.redhat.rhsa:def:20151636: false
Definition oval:com.redhat.rhsa:def:20151634: false
Definition oval:com.redhat.rhsa:def:20151633: false
Definition oval:com.redhat.rhsa:def:20151623: true
Definition oval:com.redhat.rhsa:def:20151603: false
Definition oval:com.redhat.rhsa:def:20151586: false
Definition oval:com.redhat.rhsa:def:20151581: false
Definition oval:com.redhat.rhsa:def:20151544: false
Definition oval:com.redhat.rhsa:def:20151526: false
Definition oval:com.redhat.rhsa:def:20151513: false
Definition oval:com.redhat.rhsa:def:20151499: false
Definition oval:com.redhat.rhsa:def:20151486: false
Definition oval:com.redhat.rhsa:def:20151485: false
Definition oval:com.redhat.rhsa:def:20151482: false
Definition oval:com.redhat.rhsa:def:20151471: false
Definition oval:com.redhat.rhsa:def:20151462: false
Definition oval:com.redhat.rhsa:def:20151460: false
Definition oval:com.redhat.rhsa:def:20151459: false
:
```

COMMANDS TO SCAN RHEL 6 FOR CVEs

… with human-readable html report.

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
# oscap oval eval --report /tmp/report.html Red_Hat_Enterprise_Linux_6.xml
# firefox /tmp/report.html
```

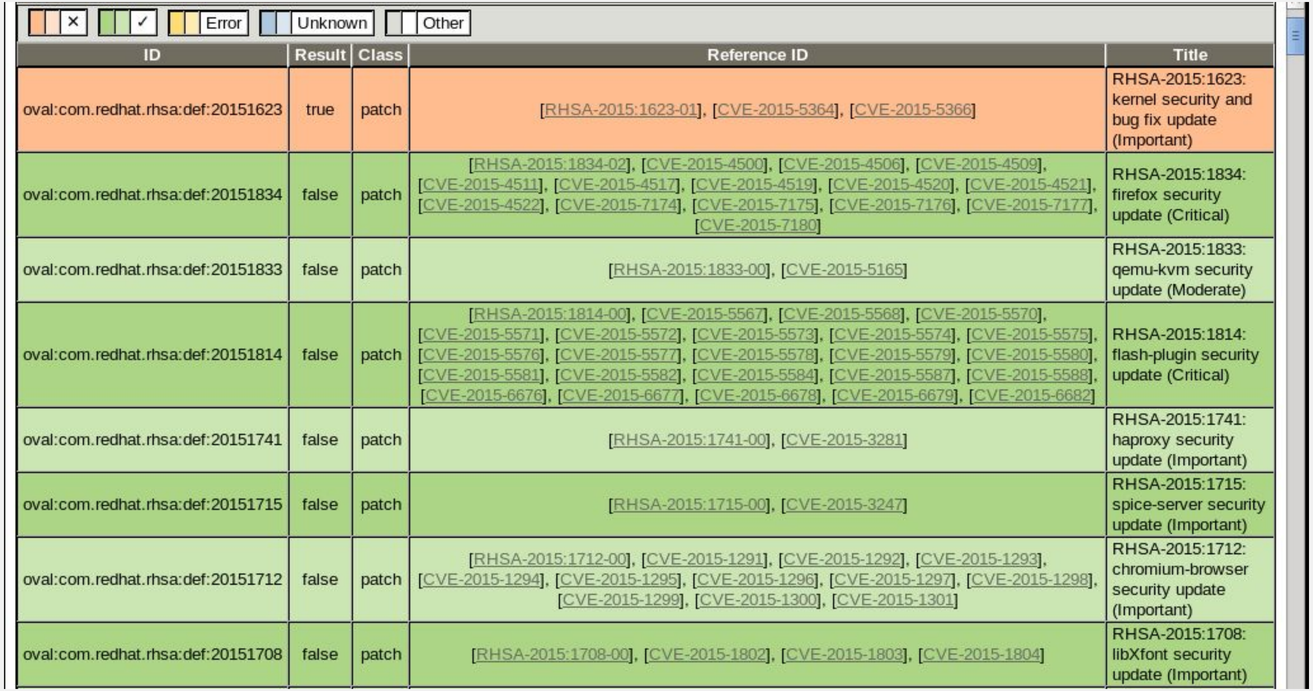
COMMANDS TO SCAN RHEL 6 FOR CVEs

... and machine consumable output.

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
# oscap oval eval --report /tmp/report.html --results /tmp/results.xml
Red_Hat_Enterprise_Linux_6.xml
# firefox /tmp/report.html
```

VULNERABILITY SCAN RESULTS

Let’s see more details by opening the HTML report.

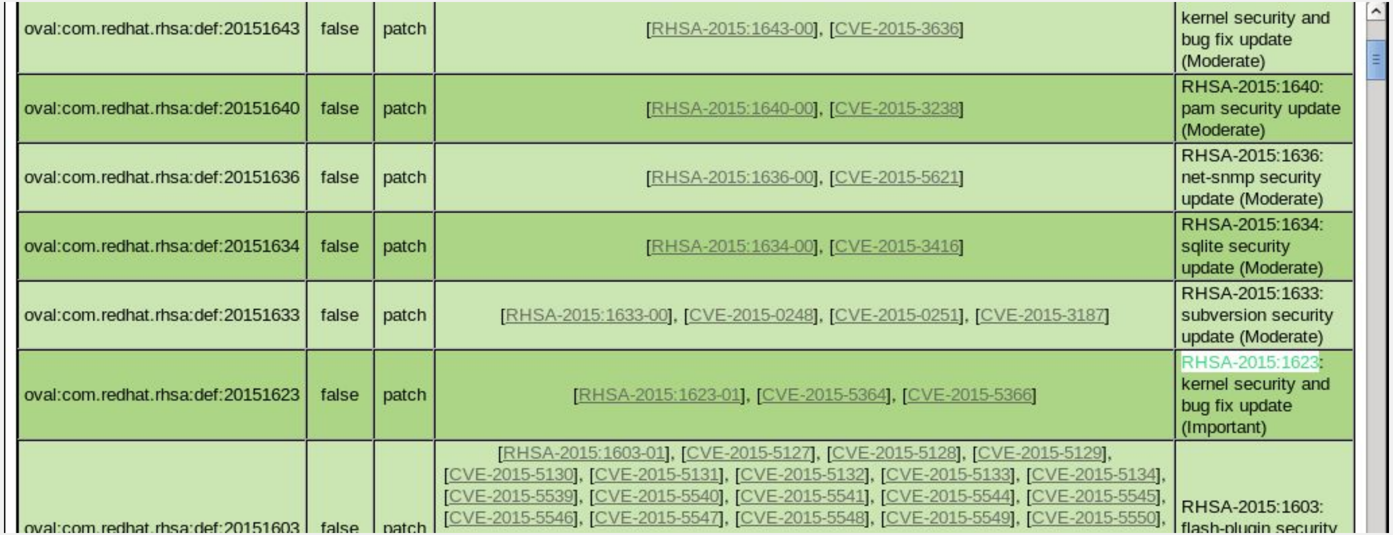


🟧 × 🟩 ✓ 🟨 Error 🟦 Unknown □ Other

ID	Result	Class	Reference ID	Title
oval:com.redhat.rhsa:def:20151623	true	patch	[RHSA-2015:1623-01], [CVE-2015-5364], [CVE-2015-5366]	RHSA-2015:1623: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20151834	false	patch	[RHSA-2015:1834-02], [CVE-2015-4500], [CVE-2015-4506], [CVE-2015-4509], [CVE-2015-4511], [CVE-2015-4517], [CVE-2015-4519], [CVE-2015-4520], [CVE-2015-4521], [CVE-2015-4522], [CVE-2015-7174], [CVE-2015-7175], [CVE-2015-7176], [CVE-2015-7177], [CVE-2015-7180]	RHSA-2015:1834: firefox security update (Critical)
oval:com.redhat.rhsa:def:20151833	false	patch	[RHSA-2015:1833-00], [CVE-2015-5165]	RHSA-2015:1833: qemu-kvm security update (Moderate)
oval:com.redhat.rhsa:def:20151814	false	patch	[RHSA-2015:1814-00], [CVE-2015-5567], [CVE-2015-5568], [CVE-2015-5570], [CVE-2015-5571], [CVE-2015-5572], [CVE-2015-5573], [CVE-2015-5574], [CVE-2015-5575], [CVE-2015-5576], [CVE-2015-5577], [CVE-2015-5578], [CVE-2015-5579], [CVE-2015-5580], [CVE-2015-5581], [CVE-2015-5582], [CVE-2015-5584], [CVE-2015-5587], [CVE-2015-5588], [CVE-2015-6676], [CVE-2015-6677], [CVE-2015-6678], [CVE-2015-6679], [CVE-2015-6682]	RHSA-2015:1814: flash-plugin security update (Critical)
oval:com.redhat.rhsa:def:20151741	false	patch	[RHSA-2015:1741-00], [CVE-2015-3281]	RHSA-2015:1741: haproxy security update (Important)
oval:com.redhat.rhsa:def:20151715	false	patch	[RHSA-2015:1715-00], [CVE-2015-3247]	RHSA-2015:1715: spice-server security update (Important)
oval:com.redhat.rhsa:def:20151712	false	patch	[RHSA-2015:1712-00], [CVE-2015-1291], [CVE-2015-1292], [CVE-2015-1293], [CVE-2015-1294], [CVE-2015-1295], [CVE-2015-1296], [CVE-2015-1297], [CVE-2015-1298], [CVE-2015-1299], [CVE-2015-1300], [CVE-2015-1301]	RHSA-2015:1712: chromium-browser security update (Important)
oval:com.redhat.rhsa:def:20151708	false	patch	[RHSA-2015:1708-00], [CVE-2015-1802], [CVE-2015-1803], [CVE-2015-1804]	RHSA-2015:1708: libXfont security update (Important)

VULNERABILITY SCAN RESULTS

After installing system updates and rebooting the vulnerability is gone.



oval:com.redhat.rhsa:def:20151643	false	patch	[RHSA-2015:1643-00], [CVE-2015-3636]	kernel security and bug fix update (Moderate)
oval:com.redhat.rhsa:def:20151640	false	patch	[RHSA-2015:1640-00], [CVE-2015-3238]	RHSA-2015:1640: pam security update (Moderate)
oval:com.redhat.rhsa:def:20151636	false	patch	[RHSA-2015:1636-00], [CVE-2015-5621]	RHSA-2015:1636: net-snmp security update (Moderate)
oval:com.redhat.rhsa:def:20151634	false	patch	[RHSA-2015:1634-00], [CVE-2015-3416]	RHSA-2015:1634: sqlite security update (Moderate)
oval:com.redhat.rhsa:def:20151633	false	patch	[RHSA-2015:1633-00], [CVE-2015-0248], [CVE-2015-0251], [CVE-2015-3187]	RHSA-2015:1633: subversion security update (Moderate)
oval:com.redhat.rhsa:def:20151623	false	patch	[RHSA-2015:1623-01], [CVE-2015-5364], [CVE-2015-5366]	RHSA-2015:1623: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20151603	false	patch	[RHSA-2015:1603-01], [CVE-2015-5127], [CVE-2015-5128], [CVE-2015-5129], [CVE-2015-5130], [CVE-2015-5131], [CVE-2015-5132], [CVE-2015-5133], [CVE-2015-5134], [CVE-2015-5539], [CVE-2015-5540], [CVE-2015-5541], [CVE-2015-5544], [CVE-2015-5545], [CVE-2015-5546], [CVE-2015-5547], [CVE-2015-5548], [CVE-2015-5549], [CVE-2015-5550],	RHSA-2015:1603: flash-plugin security

COMMANDS TO SCAN RHEL 6 FOR CVEs

Scanning remote machine

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
# oscap-ssh --sudo user@host 22 xccdf eval \
Red_Hat_Enterprise_Linux_6.xml
```

DEMO on Red Hat Enterprise Linux 7.4

ADVANTAGES

A.k.a. “Why don’t you just run `yum check-update`?”

- works offline
- works if a repository is completely missing
- … or outdated
- even if yum is not available

IMPORTANT CAVEATS

Limitations of OpenSCAP vulnerability scanning.

- only detects vulnerabilities in vendor’s packages
    - not in EPEL
    - not in 3rd party vendor repos
    - not in software that doesn’t come from RPMs/deb
- only detects vulnerabilities important enough to be fixed in RHSAs

CVE FEEDS FOR OTHER OSes

- Canonical provides CVE feeds for Ubuntu
  - use https://people.canonical.com/~ubuntu-security/oval/
- SUSE provides CVE feeds for SLES and others
  - use https://support.novell.com/security/oval/

DEMO on openSUSE Leap 42.3

(--skip-valid to save time, validating openSUSE OVAL takes ~4 minutes in the VM)

WHAT ABOUT CONTAINERS?

Scanning containers one by one like this is impractical...

Production deployments are increasingly using containers. This brings new challenges.

- lots of containers and images
- installing the oscap tool in every container is impractical

ONLINE vs. OFFLINE SCANNING

- running oscap on scanned machine is **online scanning**
- offline scanning works without installing OpenSCAP on the target
    - scan a VFS root
    - scan a VM storage image
    - scan a container
- offline scanning is limited
    - cannot query processes, DBus, etc...

OSCAP-DOCKER

Wrapper around oscap, uses offline scanning

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_7.xml
# sudo oscap-docker image $IMAGE_ID oval eval Red_Hat_Enterprise_Linux_7.xml

# sudo oscap-docker image-cve $IMAGE_ID
# sudo oscap-docker container-cve $CONTAINER_ID
```

OSCAP-VM

Wrapper around oscap, uses offline scanning

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_7.xml
# oscap-vm image $VM_IMAGE oval eval Red_Hat_Enterprise_Linux_7.xml
# oscap-vm domain $VM_DOMAIN oval eval Red_Hat_Enterprise_Linux_7.xml
```

ATOMIC SCAN

Scan containers and container images for CVEs.

```
# atomic containers list
# atomic images list

# sudo atomic scan 59d5a49b0f75

59d5a49b0f75 (registry.access.redhat.com/rhel7:latest)

59d5a49b0f75 passed the scan
```

ATOMIC SCAN

```
# sudo atomic scan rhel7.2

rhel7.2 (c453594215e4370)

The following issues were found:

     RHSA-2016:1025: pcre security update (Important)
     Severity: Important
       RHSA URL: https://rhn.redhat.com/errata/RHSA-2016-1025.html
       RHSA ID: RHSA-2016:1025-00
       Associated CVEs:
           CVE ID: CVE-2015-2328
           CVE URL: https://access.redhat.com/security/cve/CVE-2015-2328
           CVE ID: CVE-2016-3191
           CVE URL: https://access.redhat.com/security/cve/CVE-2016-3191

Files associated with this scan are in
/var/lib/atomic/openscap/2016-06-07-10-27-59-394638.
```

DEMO on Red Hat Enterprise Linux 7.4

ATOMIC SCAN WITH MULTIPLE TARGETS

Scan all your containers and container images with a single command.

Three options are available, scan all containers, scan all images and scan both.

- `atomic scan --containers`
- `atomic scan --images`
- `atomic scan --all`

HOW DOES ATOMIC SCAN WORK?

we can't trust what we don't understand...

DETECT OS VERSION

Different operating systems have different CVEs.

SELECT CVE FEED

Based on the OS version we select (optionally even refresh) CVE feed from the vendor.

MOUNT CONTAINER, RUN OSCAP-CHROOT

Atomic does all the mounting.

OpenSCAP compares installed versions with version ranges in the CVE feed.

CHECKING FOR SECURITY COMPLIANCE

TWO TYPES OF SCAP SECURITY POLICIES

SECURITY COMPLIANCE

proper configuration

hardening

USGCB

PCI-DSS

DISA STIG

...

VULNERABILITY ASSESSMENT

detect CVEs

Heartbleed

Shellshock

Ghost

VENOM

...

TWO SCAP USE-CASES

SECURITY COMPLIANCE

is root login over ssh forbidden?

is SELinux enabled and enforcing?

are we using strict password policy?

are obsolete / insecure services disabled?

...?

VULNERABILITY ASSESSMENT

are my machines vulnerable to:

Heartbleed?

Shellshock?

Ghost?

VENOM?

...?

SCAP CONSUMERS

SECURITY COMPLIANCE

Regulatory:

- Government agencies, contractors
- Financial companies
- Health care, Energy
- ...

Pro-active security

VULNERABILITY ASSESSMENT

Everybody who has an attack surface

USE-CASE 2:
SECURITY COMPLIANCE FOR A SINGLE MACHINE

SCAP SCANNER - SCAP WORKBENCH

GUI front-end for OpenSCAP

- uses oscap tool, therefore inherits certifications
- scanning local and remote targets
- content customization (also called SCAP tailoring)
- Linux, Windows and MacOS X support

OpenSCAP BASE

SCAP WORKBENCH

SCAP SECURITY GUIDE

open-source SCAP security policy project

- community project
- content for multiple products - RHEL, Fedora, CentOS, Firefox, ...
- multiple policies for each product - USGCB, PCI-DSS, DISA STIG, ...

SCANNING A SINGLE MACHINE

let’s set-up a Red Hat Enterprise Linux 7.4 machine as close to PCI-DSS as possible

We will need the following to perform a PCI-DSS scan:

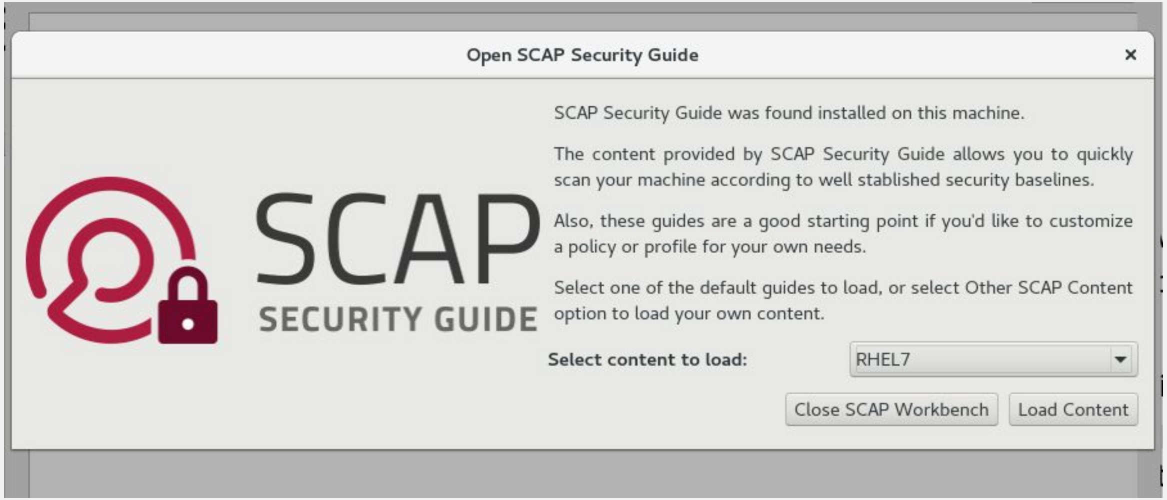
- Red Hat Enterprise Linux 7.4
- OpenSCAP and SCAP Workbench
- PCI-DSS from SCAP Security Guide

INSTALL THE NECESSARY TOOLS

(assuming Red Hat Enterprise Linux 7.4)

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

START SCAP-WORKBENCH



Open SCAP Security Guide

SCAP Security Guide was found installed on this machine.

The content provided by SCAP Security Guide allows you to quickly scan your machine according to well stablished security baselines.

Also, these guides are a good starting point if you'd like to customize a policy or profile for your own needs.

Select one of the default guides to load, or select Other SCAP Content option to load your own content.

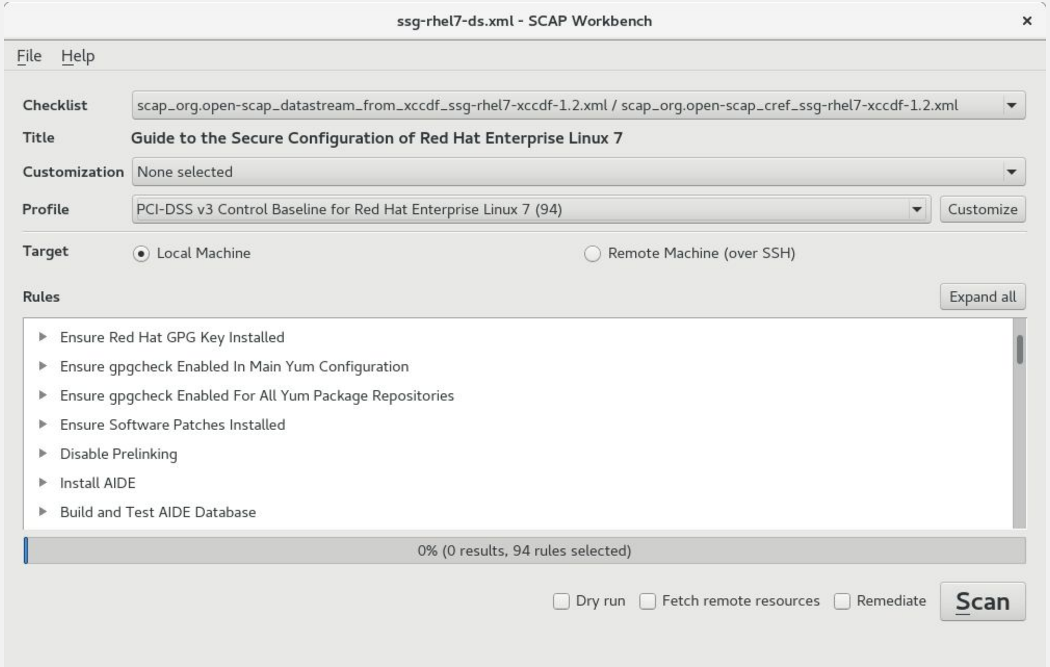
Select content to load: RHEL7

After starting *SCAP Workbench* we will be asked to select the security policy we want to load.

Let’s select security policy for Red Hat Enterprise Linux 7.

INITIAL SCAN

let’s do a quick scan to establish a baseline



ssg-rhel7-ds.xml - SCAP Workbench

Checklist: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml / scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml

Title: Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Customization: None selected

Profile: PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7 (94)

Target: ● Local Machine ○ Remote Machine (over SSH)

Rules

- Ensure Red Hat GPG Key Installed
- Ensure gpgcheck Enabled In Main Yum Configuration
- Ensure gpgcheck Enabled For All Yum Package Repositories
- Ensure Software Patches Installed
- Disable Prelinking
- Install AIDE
- Build and Test AIDE Database

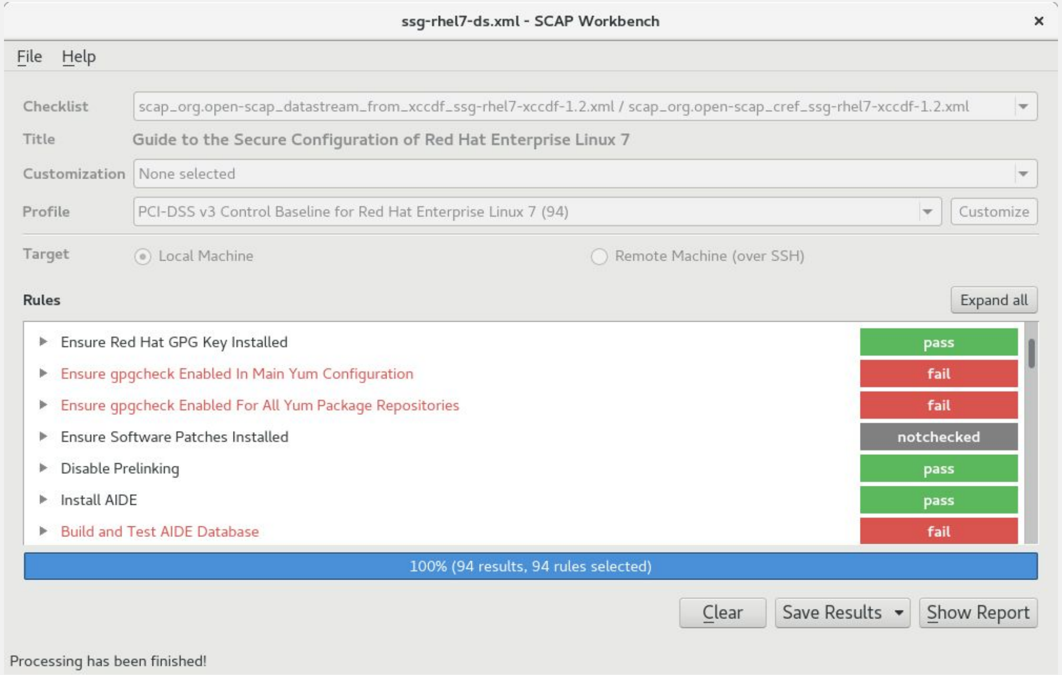
0% (0 results, 94 rules selected)

□ Dry run □ Fetch remote resources □ Remediate

1. select the *PCI-DSS* profile
2. keep *local machine* selected
3. click *Scan*

INITIAL SCAN

let’s do a quick scan to establish a baseline



ssg-rhel7-ds.xml - SCAP Workbench

Checklist: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml / scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml

Title: Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Customization: None selected

Profile: PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7 (94)

Target: ● Local Machine ○ Remote Machine (over SSH)

Rules

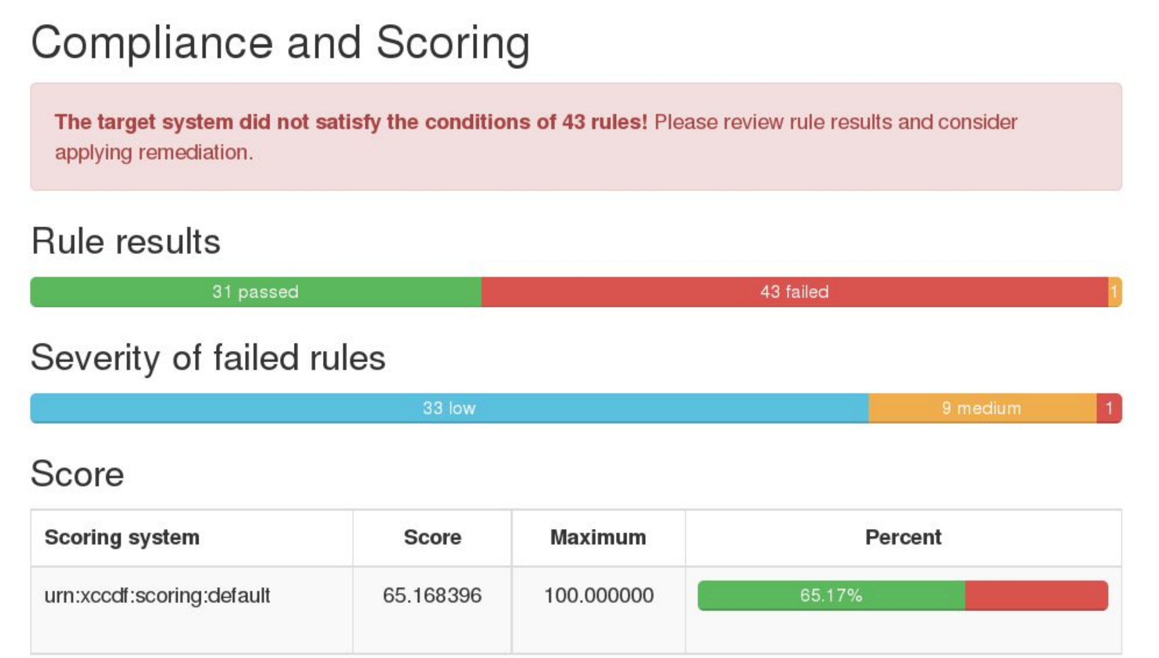
Ensure Red Hat GPG Key Installed	pass
Ensure gpgcheck Enabled In Main Yum Configuration	fail
Ensure gpgcheck Enabled For All Yum Package Repositories	fail
Ensure Software Patches Installed	notchecked
Disable Prelinking	pass
Install AIDE	pass
Build and Test AIDE Database	fail

100% (94 results, 94 rules selected)

Processing has been finished!

1. select the *PCI-DSS* profile
2. keep *local machine* selected
3. click *Scan*

INITIAL RESULTS



Compliance and Scoring

The target system did not satisfy the conditions of 43 rules! Please review rule results and consider applying remediation.

Rule results

31 passed | 43 failed | 1

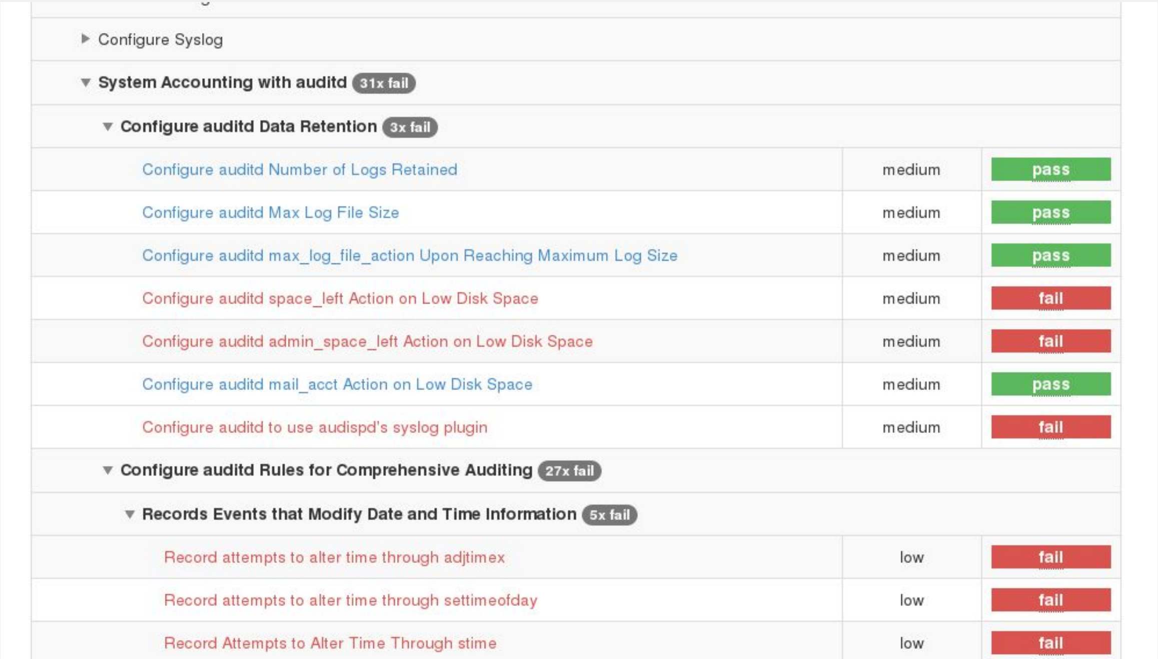
Severity of failed rules

33 low | 9 medium | 1

Score

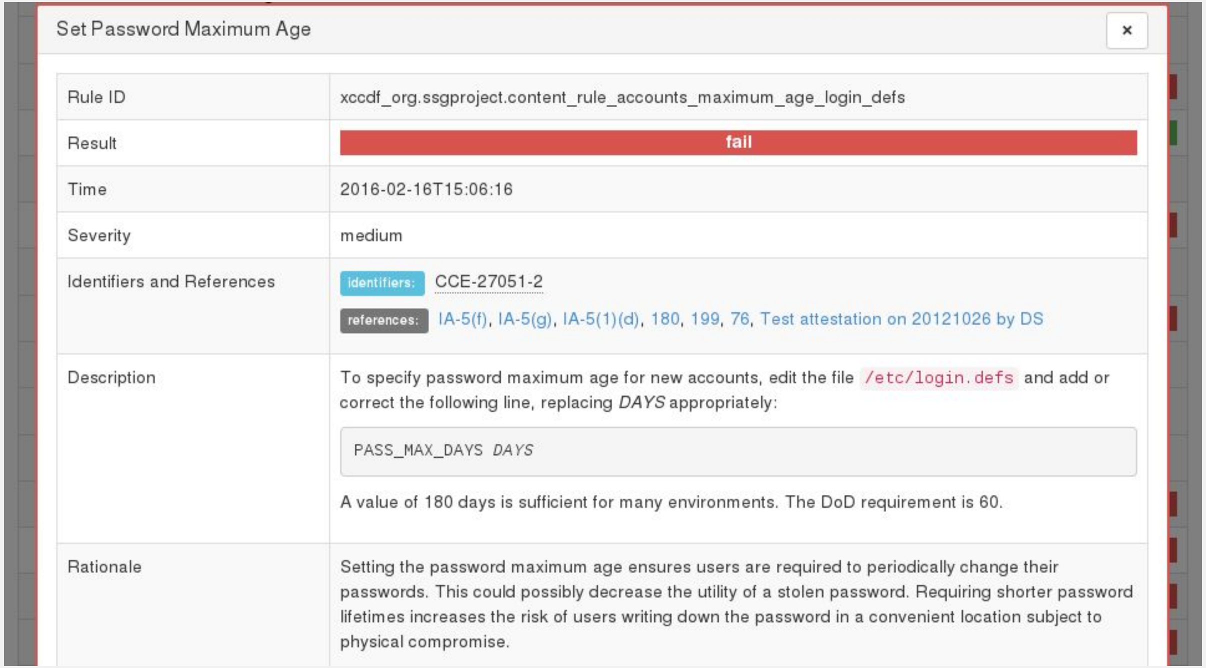
Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	65.168396	100.000000	65.17%

INITIAL RESULTS



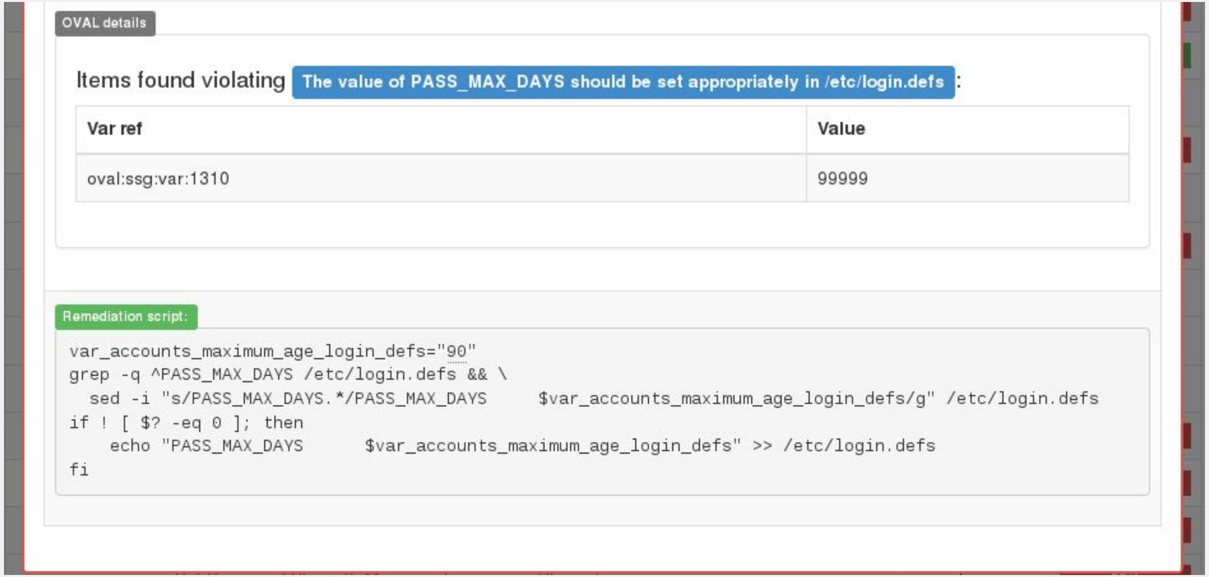
▶ Configure Syslog		
▼ **System Accounting with auditd** 31x fail		
▼ **Configure auditd Data Retention** 3x fail		
Configure auditd Number of Logs Retained	medium	pass
Configure auditd Max Log File Size	medium	pass
Configure auditd max_log_file_action Upon Reaching Maximum Log Size	medium	pass
Configure auditd space_left Action on Low Disk Space	medium	fail
Configure auditd admin_space_left Action on Low Disk Space	medium	fail
Configure auditd mail_acct Action on Low Disk Space	medium	pass
Configure auditd to use audispd's syslog plugin	medium	fail
▼ **Configure auditd Rules for Comprehensive Auditing** 27x fail		
▼ **Records Events that Modify Date and Time Information** 5x fail		
Record attempts to alter time through adjtimex	low	fail
Record attempts to alter time through settimeofday	low	fail
Record Attempts to Alter Time Through stime	low	fail

INITIAL RESULTS



Rule ID	xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs
Result	fail
Time	2016-02-16T15:06:16
Severity	medium
Identifiers and References	identifiers: CCE-27051-2 references: IA-5(f), IA-5(g), IA-5(1)(d), 180, 199, 76, Test attestation on 20121026 by DS
Description	To specify password maximum age for new accounts, edit the file `/etc/login.defs` and add or correct the following line, replacing *DAYS* appropriately: `PASS_MAX_DAYS DAYS` A value of 180 days is sufficient for many environments. The DoD requirement is 60.
Rationale	Setting the password maximum age ensures users are required to periodically change their passwords. This could possibly decrease the utility of a stolen password. Requiring shorter password lifetimes increases the risk of users writing down the password in a convenient location subject to physical compromise.

INITIAL RESULTS

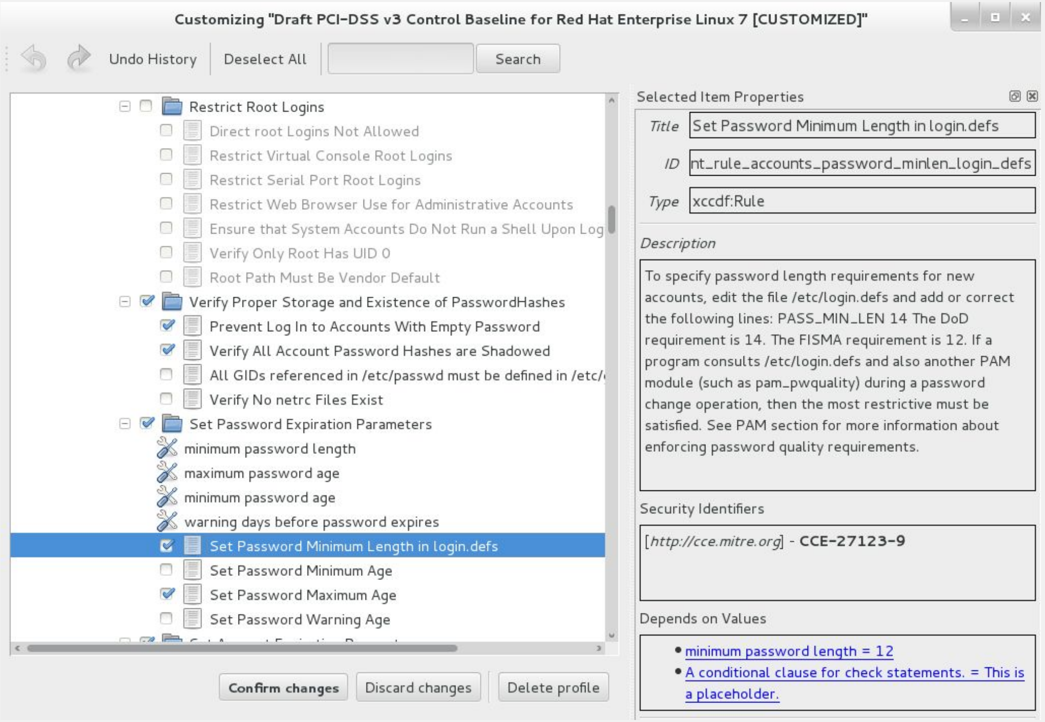


Items found violating The value of PASS_MAX_DAYS should be set appropriately in /etc/login.defs:

Var ref	Value
oval:ssg:var:1310	99999

```
var_accounts_maximum_age_login_defs="90"
grep -q ^PASS_MAX_DAYS /etc/login.defs && \
  sed -i "s/PASS_MAX_DAYS.*/PASS_MAX_DAYS     $var_accounts_maximum_age_login_defs/g" /etc/login.defs
if ! [ $? -eq 0 ]; then
    echo "PASS_MAX_DAYS      $var_accounts_maximum_age_login_defs" >> /etc/login.defs
fi
```

MAKING ADJUSTMENTS


Customizing "Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7 [CUSTOMIZED]"
Undo History
Deselect All
Search
Confirm changes
Discard changes
Delete profile

- ☐ Restrict Root Logins
  - ☐ Direct root Logins Not Allowed
  - ☐ Restrict Virtual Console Root Logins
  - ☐ Restrict Serial Port Root Logins
  - ☐ Restrict Web Browser Use for Administrative Accounts
  - ☐ Ensure that System Accounts Do Not Run a Shell Upon Log
  - ☐ Verify Only Root Has UID 0
  - ☐ Root Path Must Be Vendor Default
- ☑ Verify Proper Storage and Existence of PasswordHashes
  - ☑ Prevent Log In to Accounts With Empty Password
  - ☑ Verify All Account Password Hashes are Shadowed
  - ☐ All GIDs referenced in /etc/passwd must be defined in /etc/
  - ☐ Verify No netrc Files Exist
- ☑ Set Password Expiration Parameters
  - minimum password length
  - maximum password age
  - minimum password age
  - warning days before password expires
  - ☑ Set Password Minimum Length in login.defs
  - ☐ Set Password Minimum Age
  - ☑ Set Password Maximum Age
  - ☐ Set Password Warning Age

Selected Item Properties

Title Set Password Minimum Length in login.defs

ID nt_rule_accounts_password_minlen_login_defs

Type xccdf:Rule

Description

To specify password length requirements for new accounts, edit the file /etc/login.defs and add or correct the following lines: PASS_MIN_LEN 14 The DoD requirement is 14. The FISMA requirement is 12. If a program consults /etc/login.defs and also another PAM module (such as pam_pwquality) during a password change operation, then the most restrictive must be satisfied. See PAM section for more information about enforcing password quality requirements.

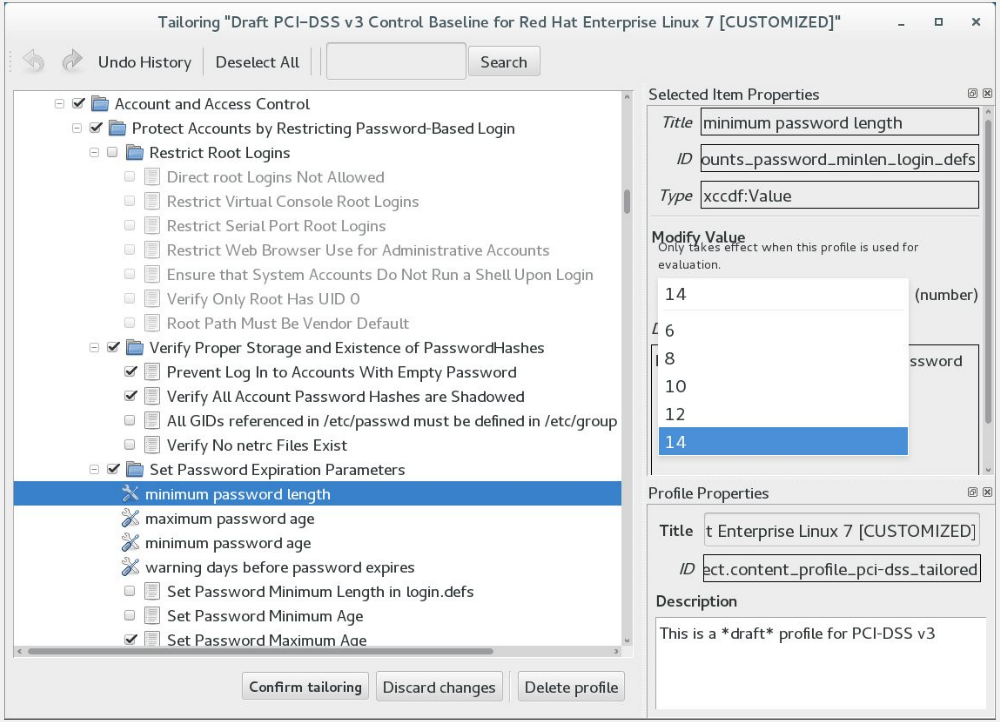
Security Identifiers

[*http://cce.mitre.org*] - **CCE-27123-9**

Depends on Values

- minimum password length = 12
- A conditional clause for check statements. = This is a placeholder.

MAKING ADJUSTMENTS



Tailoring "Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7 [CUSTOMIZED]"

- ☑ Account and Access Control
  - ☑ Protect Accounts by Restricting Password-Based Login
    - □ Restrict Root Logins
      - □ Direct root Logins Not Allowed
      - □ Restrict Virtual Console Root Logins
      - □ Restrict Serial Port Root Logins
      - □ Restrict Web Browser Use for Administrative Accounts
      - □ Ensure that System Accounts Do Not Run a Shell Upon Login
      - □ Verify Only Root Has UID 0
      - □ Root Path Must Be Vendor Default
    - ☑ Verify Proper Storage and Existence of PasswordHashes
      - ☑ Prevent Log In to Accounts With Empty Password
      - ☑ Verify All Account Password Hashes are Shadowed
      - □ All GIDs referenced in /etc/passwd must be defined in /etc/group
      - □ Verify No netrc Files Exist
    - ☑ Set Password Expiration Parameters
      - minimum password length
      - maximum password age
      - minimum password age
      - warning days before password expires
      - □ Set Password Minimum Length in login.defs
      - □ Set Password Minimum Age
      - ☑ Set Password Maximum Age

Selected Item Properties

Title: minimum password length

ID: ounts_password_minlen_login_defs

Type: xccdf:Value

Modify Value

Only takes effect when this profile is used for evaluation.

14 (number)

6
8
10
12
14

ssword

Profile Properties

Title: t Enterprise Linux 7 [CUSTOMIZED]

ID: ect.content_profile_pci-dss_tailored

Description

This is a *draft* profile for PCI-DSS v3

SAVING THE FINAL POLICY

we now have the final security policy, let’s save it for later deployment

Click File → *Save Customization Policy*

Instead of saving the entire policy we will save the difference between stock policy and our final policy. This enables us to get improvements and bug fixes.

TAILORING FILE

The result of Tailoring

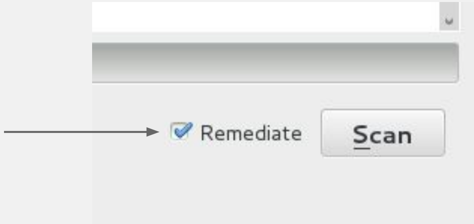
```
<?xml version="1.0" encoding="UTF-8"?>
<xccdf:Tailoring xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2"
id="xccdf_scap-workbench_tailoring_default">
  <xccdf:benchmark href="/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml"/>
  <xccdf:version time="2016-06-02T11:04:09">1</xccdf:version>
  <xccdf:Profile id="xccdf_org.ssgproject.content_profile_pci-dss_customized"
extends="xccdf_org.ssgproject.content_profile_pci-dss">
    <xccdf:title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">PCI-DSS
v3 Control Baseline for Red Hat Enterprise Linux 7 [CUSTOMIZED]</xccdf:title>
    <xccdf:description>...</xccdf:description>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_interval"
selected="true"/>
  </xccdf:Profile>
</xccdf:Tailoring>
```

AUTOMATICALLY FIXING THE ISSUES

Check *Remediate* to automatically fix issues after scanning

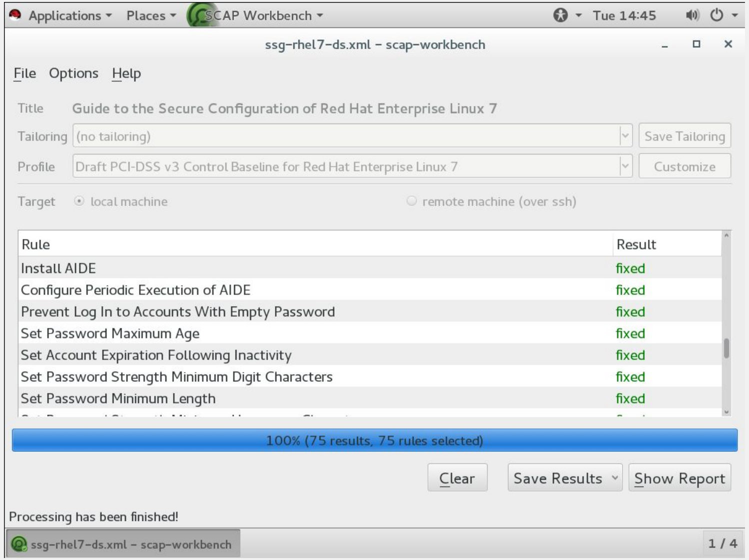
We now have a profile defined, let’s put the machine closer to compliance. Keep this in mind when doing automatic remediation:

- remediation is potentially dangerous
- remediation **cannot be undone**!



REMEDIATION WITH SCAP-WORKBENCH

let’s do a quick scan to establish a baseline



Title Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Tailoring (no tailoring)

Profile Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7

Target ● local machine ○ remote machine (over ssh)

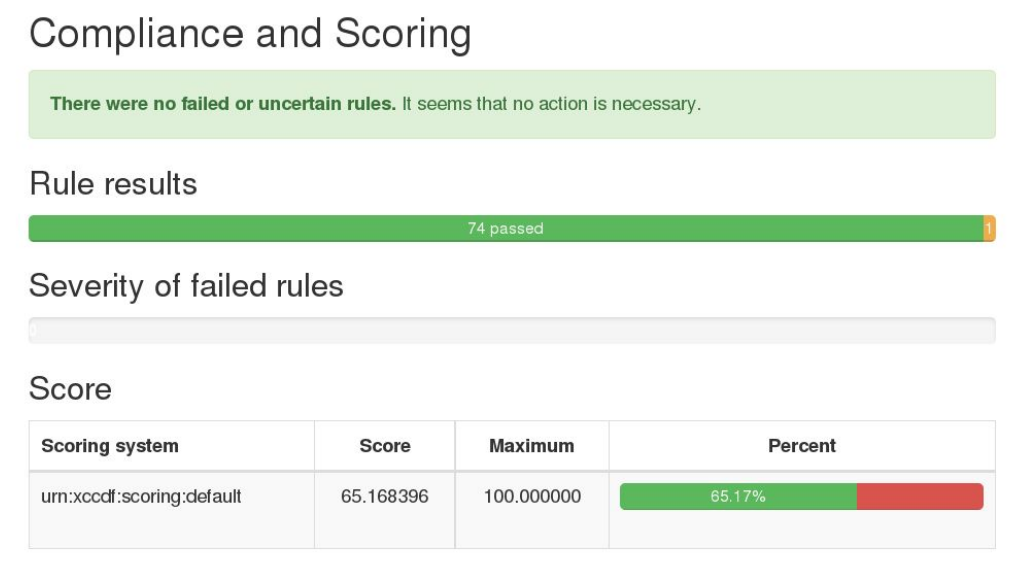
Rule	Result
Install AIDE	fixed
Configure Periodic Execution of AIDE	fixed
Prevent Log In to Accounts With Empty Password	fixed
Set Password Maximum Age	fixed
Set Account Expiration Following Inactivity	fixed
Set Password Strength Minimum Digit Characters	fixed
Set Password Minimum Length	fixed

100% (75 results, 75 rules selected)

Processing has been finished!

- *fixed* means the remediation was successful
- some fixes require reboot
- some rules cannot be automatically fixed - these still show as *failed*

FINAL RESULTS



Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.

Rule results

Severity of failed rules

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	65.168396	100.000000	65.17%

DEMO on Red Hat Enterprise Linux 7.4

COMMAND-LINE COMPLIANCE SCANNING OF RED HAT ENTERPRISE LINUX 7

SCANNING A PHYSICAL MACHINE

Use `oscap`, the OpenSCAP command line interface

```
sudo oscap xccdf eval \
--profile xccdf_org.ssgproject.content_profile_pci-dss \
--results results.xml \
--results-arf arf.xml \
--report report.html \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

SCANNING REMOTE MACHINE

a command-line interface to run oscap on remote machine

```
# oscap-ssh --sudo user@host 22 xccdf eval \
--profile xccdf_org.ssgproject.content_profile_pci-dss \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

SCANNING A CONTAINER

a command-line interface similar to oscap, scans a container “from the outside”

```
# sudo oscap-docker container $ID xccdf eval \
--profile xccdf_org.ssgproject.content_profile_pci-dss \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml

# sudo oscap-docker image $ID xccdf eval \
--profile xccdf_org.ssgproject.content_profile_pci-dss \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

SCANNING A VIRTUAL MACHINE

a command-line interface similar to oscap, scans a VM “from the outside”

```
# sudo oscap-vm domain rhel7 xccdf eval \
--profile xccdf_org.ssgproject.content_profile_pci-dss \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml

# sudo oscap-vm image /var/lib/libvirt/images/rhel7.qcow2 xccdf eval \
--profile xccdf_org.ssgproject.content_profile_pci-dss \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

ATOMIC SCAN

Special case - scanning of container images

```
# sudo atomic scan \
--scan_type configuration_compliance \
--scanner_args \
profile=xccdf_org.ssgproject.content_profile_pci-dss \
rhel7
```

USE-CASE 3: REMEDIATIONS

REMEDIATION WITH CLI TOOLS

SCANNER REMEDIATION

- only failing rules are remedied
- outcome of remediation is part of the report

ROLES REMEDIATION

- performed using content generated by the scanner
- admin can easily review remediation steps before application

REMEDIATION WITH CLI TOOLS

Not every target can be remedied

Tools using **offline scanning** cannot remediate

- `oscap-vm`
- `oscap-docker`

REMEDIATION WITH CLI TOOLS

SCANNER remediation

```
# sudo oscap xccdf eval ...
# oscap-ssh --sudo user@host 22 xccdf eval ...

=== (common part)
--profile xccdf_org.ssgproject.content_profile_pci-dss \
--remediate \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

REMEDIATION WITH CLI TOOLS

Special case - remediation of container images

```
# sudo atomic scan --remediate \
--scan_type configuration_compliance \
--scanner_args \
profile=xccdf_org.ssgproject.content_profile_pci-dss \
rhel7
```

New container image is produced, with hardening layer on top.

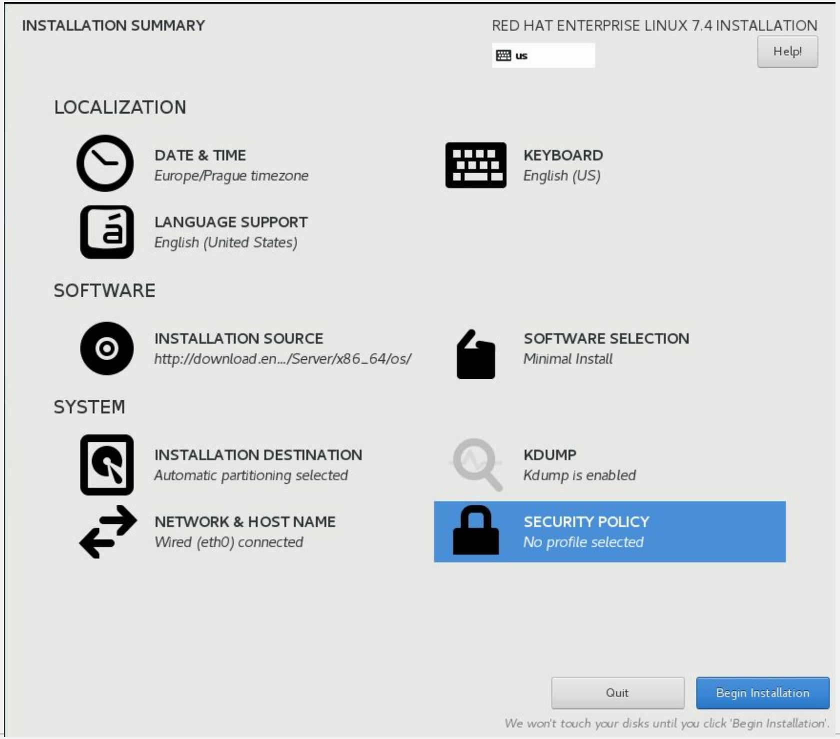
REMEDIATION DURING INSTALLATION

Using OSCAP Anaconda Addon

- install machines in a compliant state
- provision VMs with compliance in mind
    - partitioning
    - passwords
- works only in Anaconda installed

OSCAP ANACONDA ADDON

SCAP integration in the installer GUI



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 7.4 INSTALLATION

LOCALIZATION

DATE & TIME
Europe/Prague timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
http://download.en.../Server/x86_64/os/

SOFTWARE SELECTION
Minimal Install

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

KDUMP
Kdump is enabled

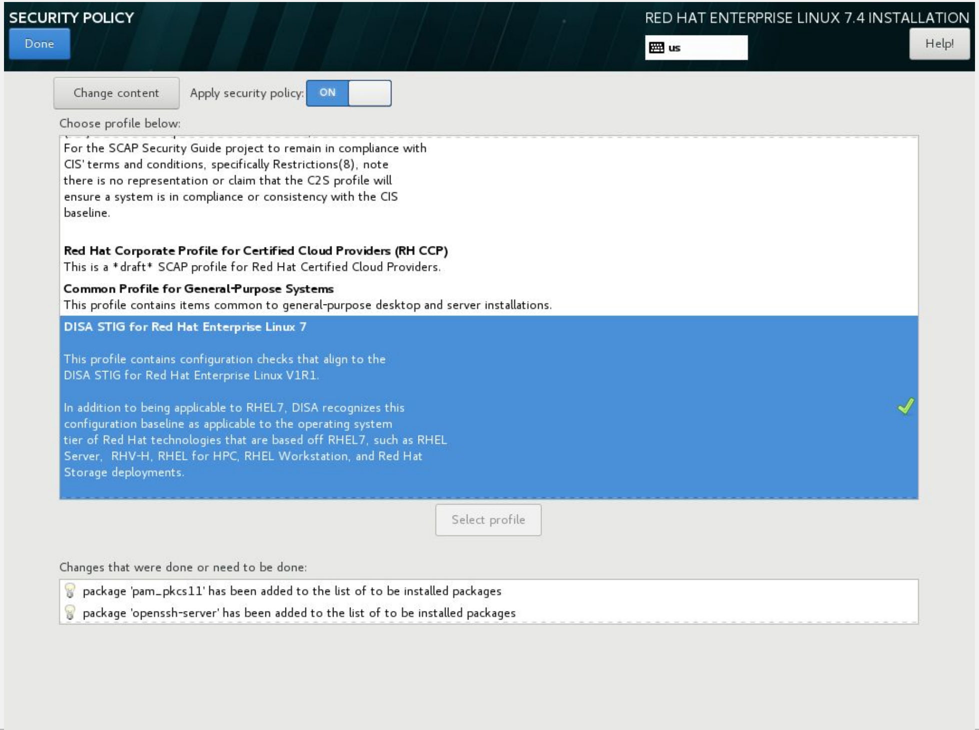
NETWORK & HOST NAME
Wired (eth0) connected

SECURITY POLICY
No profile selected

We won't touch your disks until you click 'Begin Installation'.

OSCAP ANACONDA ADDON

SCAP integration in the installer GUI



Apply security policy: ON

Choose profile below:

For the SCAP Security Guide project to remain in compliance with CIS' terms and conditions, specifically Restrictions(8), note there is no representation or claim that the C2S profile will ensure a system is in compliance or consistency with the CIS baseline.

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.

DISA STIG for Red Hat Enterprise Linux 7 ✓

This profile contains configuration checks that align to the DISA STIG for Red Hat Enterprise Linux V1R1.

In addition to being applicable to RHEL7, DISA recognizes this configuration baseline as applicable to the operating system tier of Red Hat technologies that are based off RHEL7, such as RHEL Server, RHV-H, RHEL for HPC, RHEL Workstation, and Red Hat Storage deployments.

Changes that were done or need to be done:

- package 'pam_pkcs11' has been added to the list of to be installed packages
- package 'openssh-server' has been added to the list of to be installed packages

KICKSTART INTEGRATION

The same functionality is available in kickstart oscap_anaconda_addon block

```
%addon org_fedora_oscap
    content-type = datastream
    content-url = https://www.example.com/scap/ssg-rhel7-ds.xml
    datastream-id = scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
    xccdf-id = scap_org.open-scap_cref_ssg-rhel7-pcidss-xccdf-1.2.xml
    profile =  xccdf_org.ssgproject.content_profile_pci-dss_centric
    fingerprint = 74ce9f0b03a775192a35b202b6d9d1c1
%end
```

REMEDIATION ROLES

REMEDIATION ROLES

Full fix scripts generated by the scanner

WHAT to remediate

- based on scan result
- based on profile - assume all rules failed

FORMAT of remediation

- bash remediation roles
- ansible remediation roles

REMEDIATION ROLES

Profile versus Results based

```
# oscap xccdf generate fix \
--result-id xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_pci-dss \
./result.xml


# oscap xccdf generate fix \
--profile xccdf_org.ssgproject.content_profile_pci-dss \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

BASH REMEDIATION ROLES

Script snippets to put targets into compliance

```
# oscap xccdf generate fix --fix-type bash ...
=====
###############################################################################
# BEGIN fix (2 / 61) for 'xccdf_org.ssgproject.content_rule_aide_build_database'
###############################################################################
(>&2 echo "Remediating rule 2/61:
'xccdf_org.ssgproject.content_rule_aide_build_database'")
/usr/sbin/aide --init
/bin/cp -p /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
# END fix for 'xccdf_org.ssgproject.content_rule_aide_build_database'
```

ANSIBLE REMEDIATION ROLES

Script snippets to put targets into compliance

```
# oscap xccdf generate fix --fix-type ansible ...
=====
# - hosts: localhost # set required host
    tasks:
      - name: "Disable POST password expiration"
        lineinfile:
          create=yes
          dest="/etc/default/useradd"
          regexp="^INACTIVE"
          line="INACTIVE=-1"
```

DEMO on Fedora 26

USE-CASE 4:
SCANNING AN INFRASTRUCTURE

MANY OPTIONS

Every infrastructure is different...

- For small infrastructures:
  - OpenSCAP-daemon
- For large(r) infrastructures:
  - Red Hat Satellite 6 (Foreman)
  - SUSE Manager
  - Red Hat CloudForms (ManageIQ)
  - Red Hat Satellite 5 (Spacewalk)

OPENSCAP-DAEMON

- Continuous scanning, result storage
- Interactive, useful defaults
- Unified task interface, can scan:
  - Local machine
  - Remote machine over SSH
  - Container, container image
  - VMs, VM storage images
  - VFS

OPENSCAP-DAEMON SCAN TARGET

- Unified task interface, can scan:
  - `localhost`
  - `ssh://user@machine:port`
  - `ssh+sudo://user@machine:port`
  - `docker-image://rhel7`
  - `docker-container://furious_einstein`
  - `vm-domain://my_vm`
  - `vm-image:///var/lib/libvirtd/images/my_vm.qcow2`
  - `chroot:///mnt/some_vfs`

OPENSCAP-DAEMON

- Enable the following COPR repo: https://copr.fedorainfracloud.org/coprs/openscapmaint/openscap-latest/

```
# yum install openscap-daemon
# systemctl enable oscapd
# systemctl start oscapd
```

OPENSCAP-DAEMON

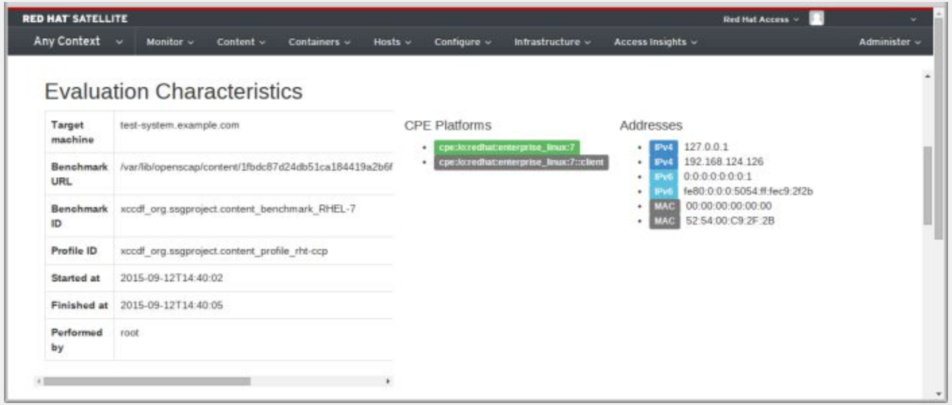
```
# oscapd-cli task

# oscapd-cli task-create -i

# oscapd-cli result

# oscapd-cli task 1 run

# oscapd-cli result 1 1

# oscapd-cli result 1 1 report
```

SCAP IN RED HAT SATELLITE 6

Red Hat Satellite 6 can be used to scan your infrastructure.

Feature highlights:

- upload SCAP content
- assign policies to hosts and hostgroups
- schedule continuous checks
- view HTML reports
- Foreman upstream project



Evaluation Characteristics

Target machine	test-system.example.com
Benchmark URL	/var/lib/openscap/content/1fbdc87d24db51ca184419a2b6f
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID	xccdf_org.ssgproject.content_profile_rht-ccp
Started at	2015-09-12T14:40:02
Finished at	2015-09-12T14:40:05
Performed by	root

CPE Platforms

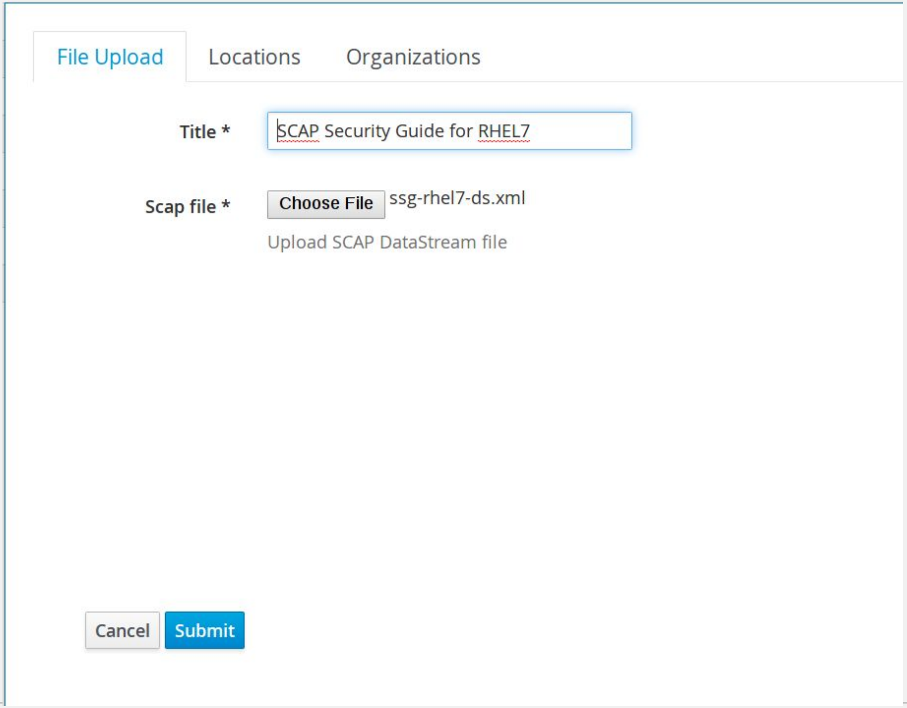
- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.124.126
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:5054:ff:fec9:2f2b
- MAC 00:00:00:00:00:00
- MAC 52:54:00:C9:2F:2B

SCAP IN RED HAT SATELLITE 6

upload SCAP content



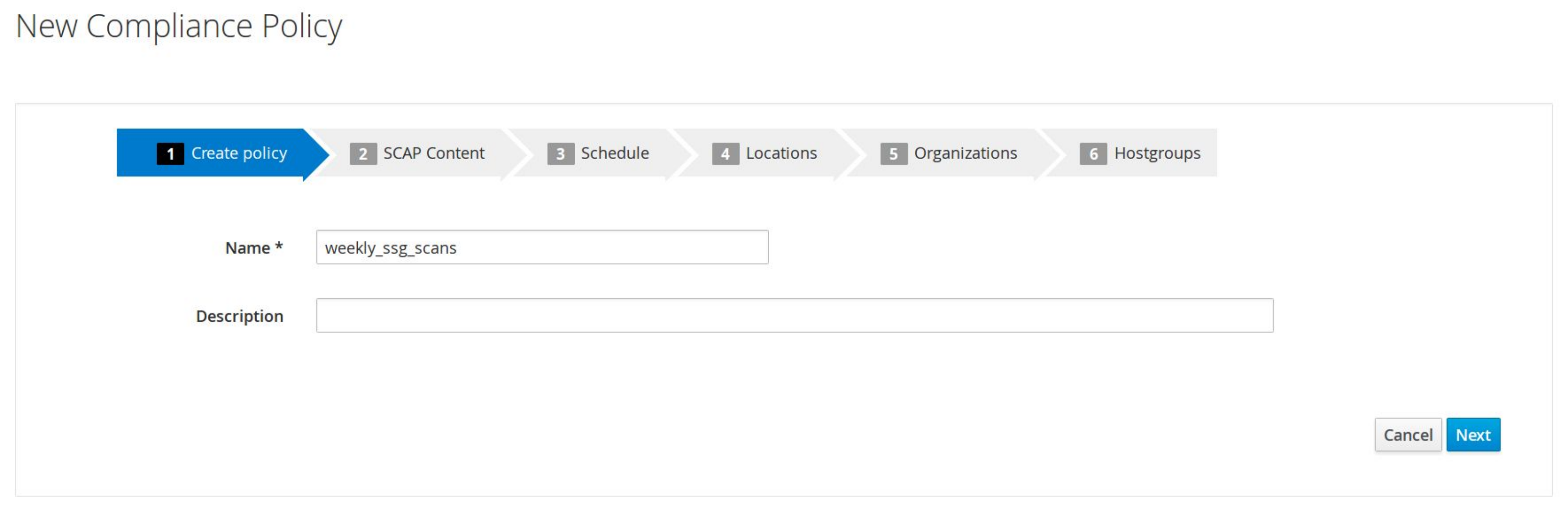
Title * SCAP Security Guide for RHEL7

Scap file * ssg-rhel7-ds.xml

Upload SCAP DataStream file

SCAP IN RED HAT SATELLITE 6

use the uploaded SCAP content to create policies



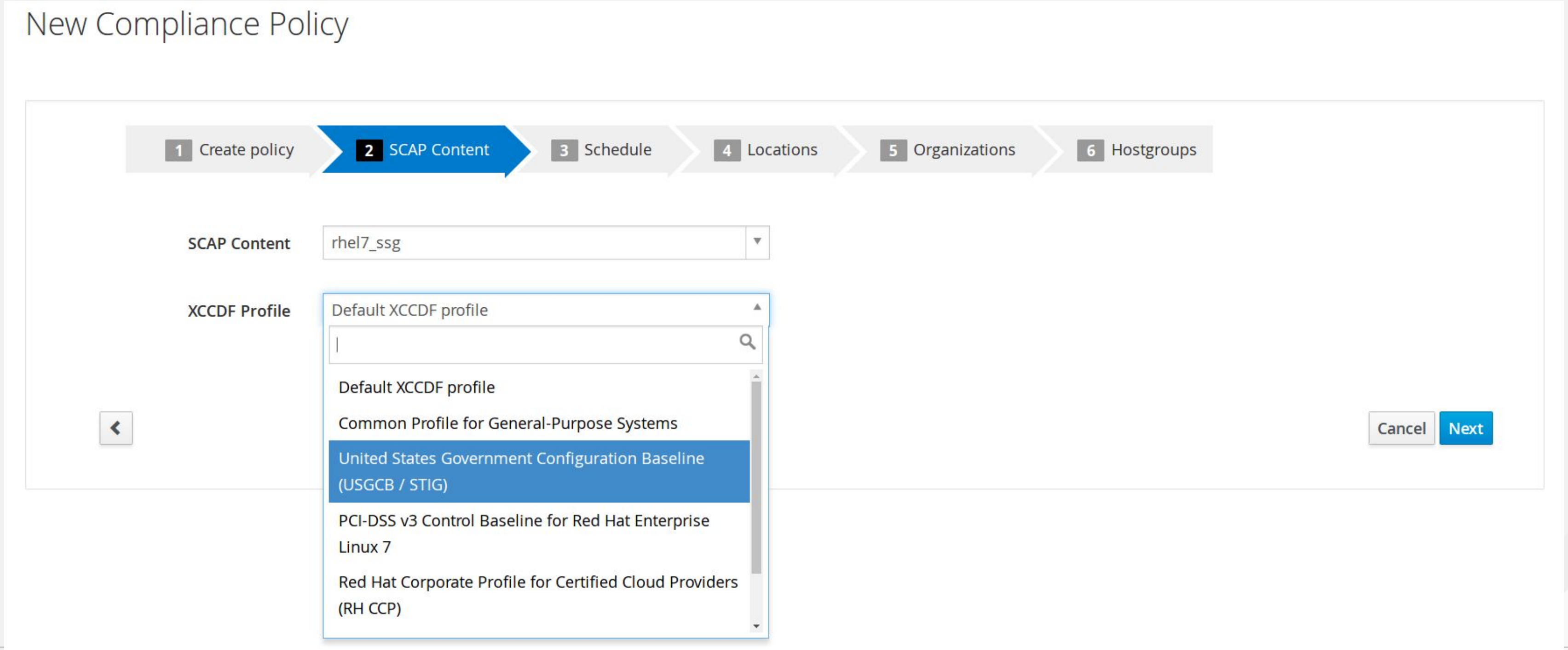
New Compliance Policy

Name * weekly_ssg_scans

Description

SCAP IN RED HAT SATELLITE 6

use the uploaded SCAP content to create policies



New Compliance Policy

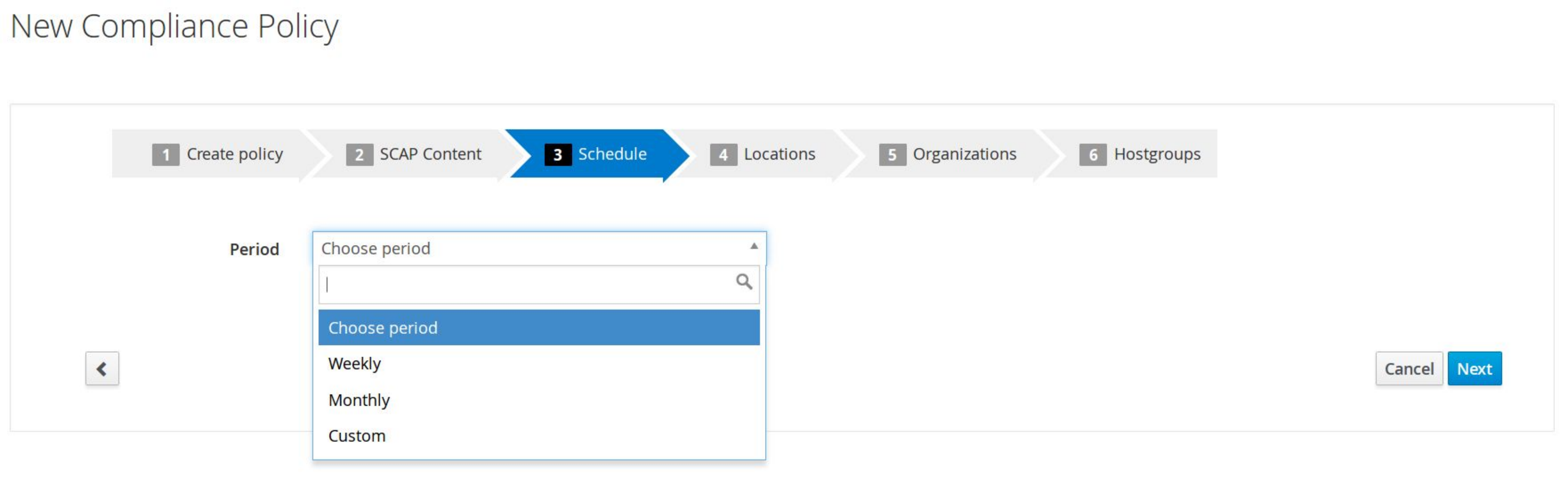
SCAP Content: rhel7_ssg

XCCDF Profile: Default XCCDF profile

- Default XCCDF profile
- Common Profile for General-Purpose Systems
- United States Government Configuration Baseline (USGCB / STIG)
- PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
- Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

SCAP IN RED HAT SATELLITE 6

use the uploaded SCAP content to create policies

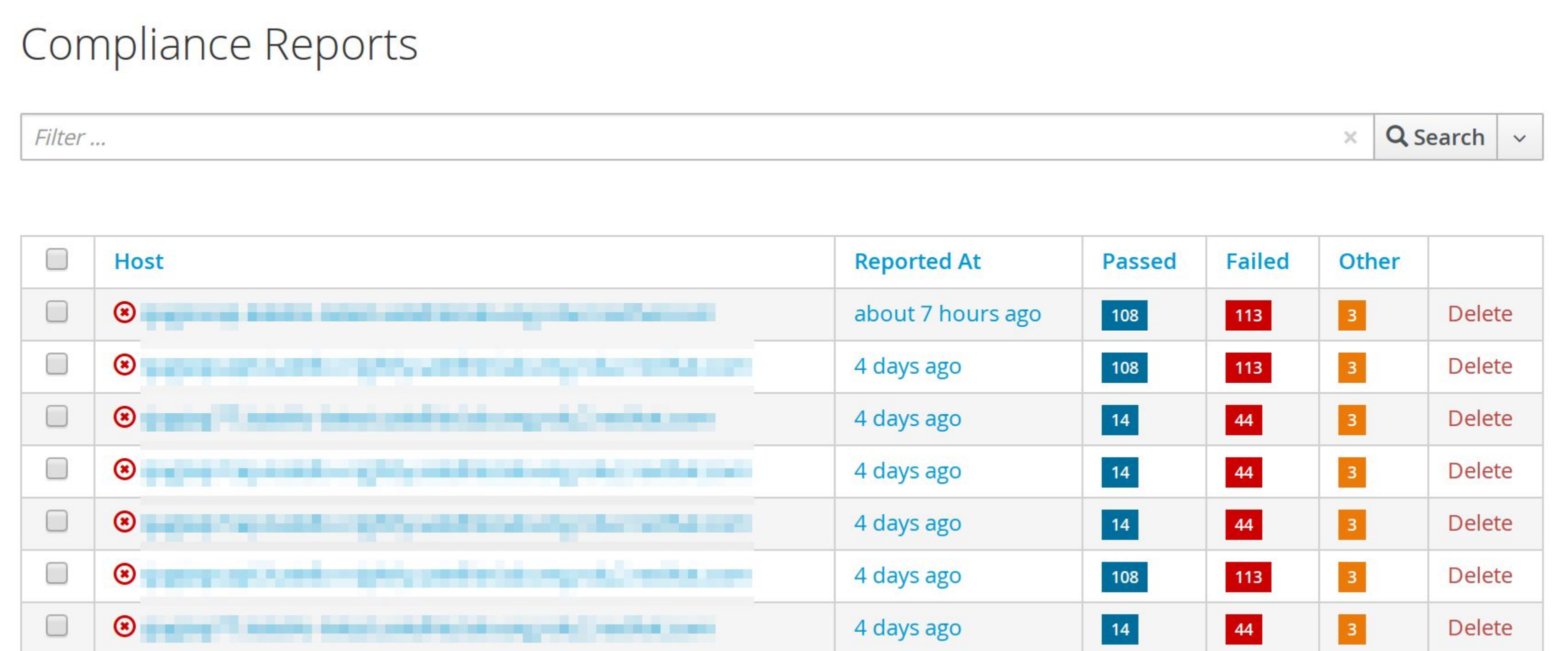


New Compliance Policy

Period: Choose period

SCAP IN RED HAT SATELLITE 6

see past results

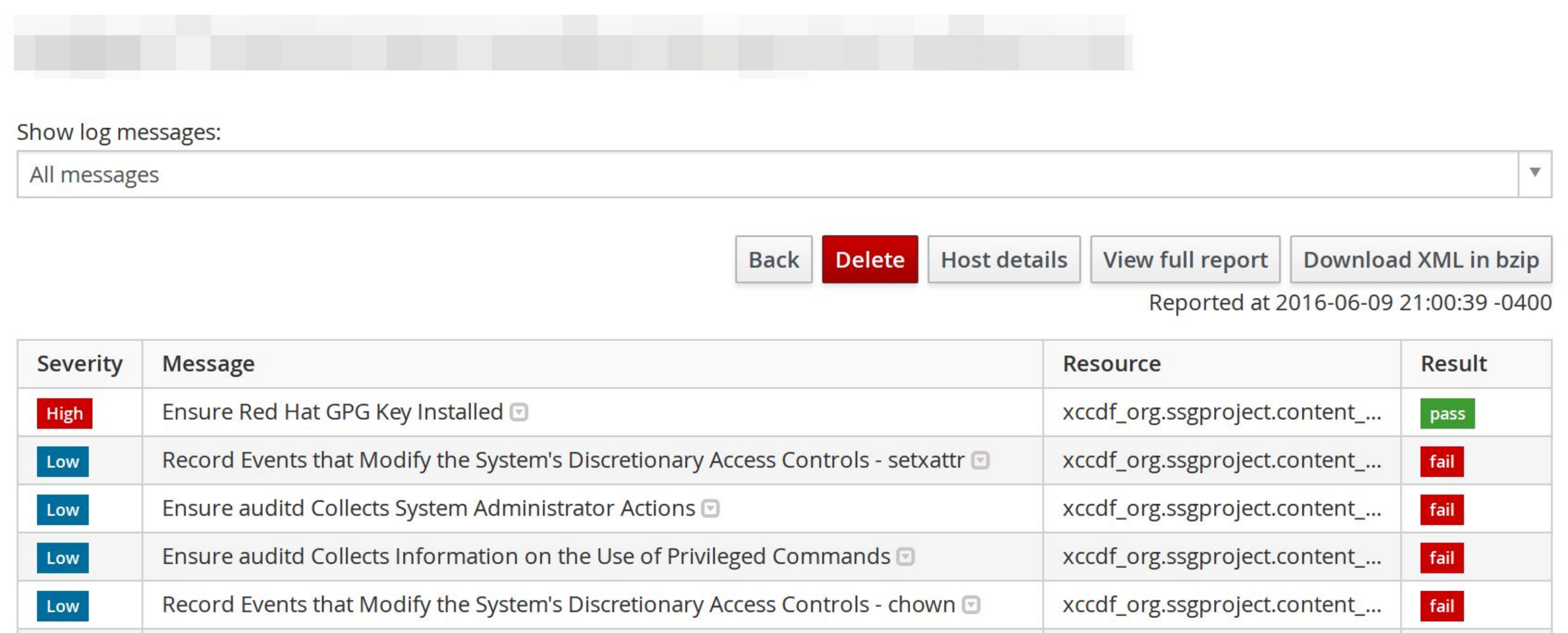


Compliance Reports

□	Host	Reported At	Passed	Failed	Other	
□	⊗ [redacted]	about 7 hours ago	108	113	3	Delete
□	⊗ [redacted]	4 days ago	108	113	3	Delete
□	⊗ [redacted]	4 days ago	14	44	3	Delete
□	⊗ [redacted]	4 days ago	14	44	3	Delete
□	⊗ [redacted]	4 days ago	14	44	3	Delete
□	⊗ [redacted]	4 days ago	108	113	3	Delete
□	⊗ [redacted]	4 days ago	14	44	3	Delete

SCAP IN RED HAT SATELLITE 6

browse and filter in the rule result overview



[redacted]

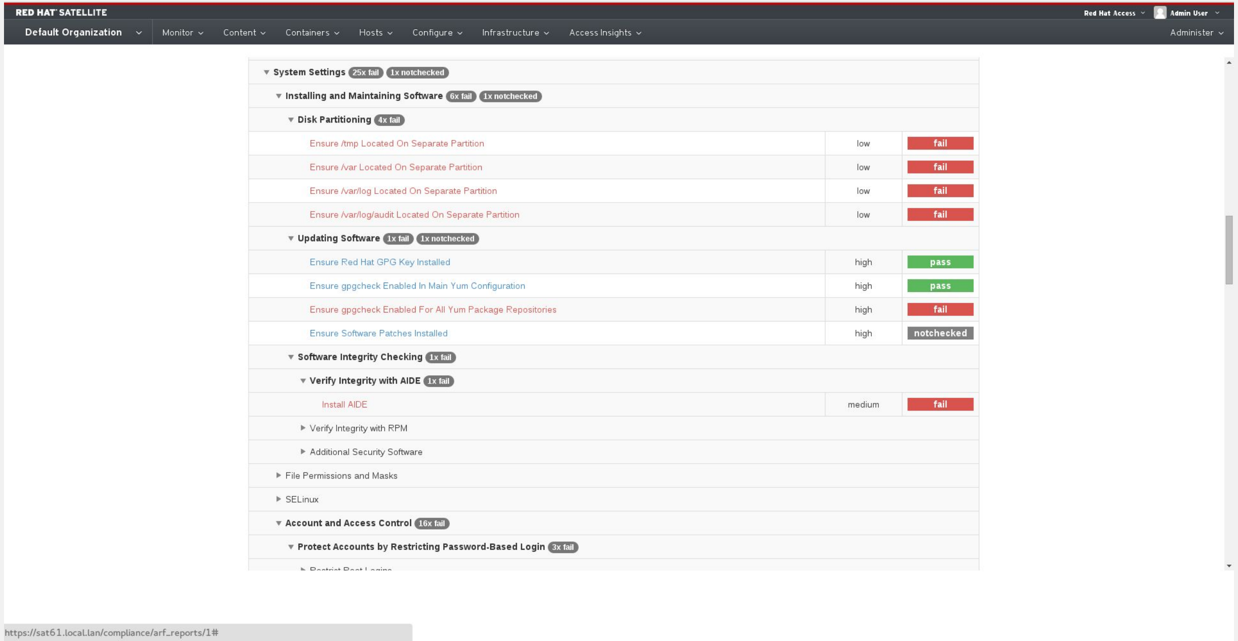
Show log messages: All messages

Reported at 2016-06-09 21:00:39 -0400

Severity	Message	Resource	Result
High	Ensure Red Hat GPG Key Installed	xccdf_org.ssgproject.content_...	pass
Low	Record Events that Modify the System's Discretionary Access Controls - setxattr	xccdf_org.ssgproject.content_...	fail
Low	Ensure auditd Collects System Administrator Actions	xccdf_org.ssgproject.content_...	fail
Low	Ensure auditd Collects Information on the Use of Privileged Commands	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - chown	xccdf_org.ssgproject.content_...	fail

SCAP IN RED HAT SATELLITE 6

browse HTML report for details of a past result



▾ System Settings 25x fail 1x notchecked		
▾ Installing and Maintaining Software 6x fail 1x notchecked		
▾ Disk Partitioning 4x fail		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
▾ Updating Software 1x fail 1x notchecked		
Ensure Red Hat GPG Key Installed	high	pass
Ensure gpgcheck Enabled In Main Yum Configuration	high	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	high	fail
Ensure Software Patches Installed	high	notchecked
▾ Software Integrity Checking 1x fail		
▾ Verify Integrity with AIDE 1x fail		
Install AIDE	medium	fail
▸ Verify Integrity with RPM		
▸ Additional Security Software		
▸ File Permissions and Masks		
▸ SELinux		
▾ Account and Access Control 16x fail		
▾ Protect Accounts by Restricting Password-Based Login 3x fail		
▸ Restrict Root Logins		

https://sat61.local.lan/compliance/arf_reports/1#

SCAP IN RED HAT SATELLITE 6

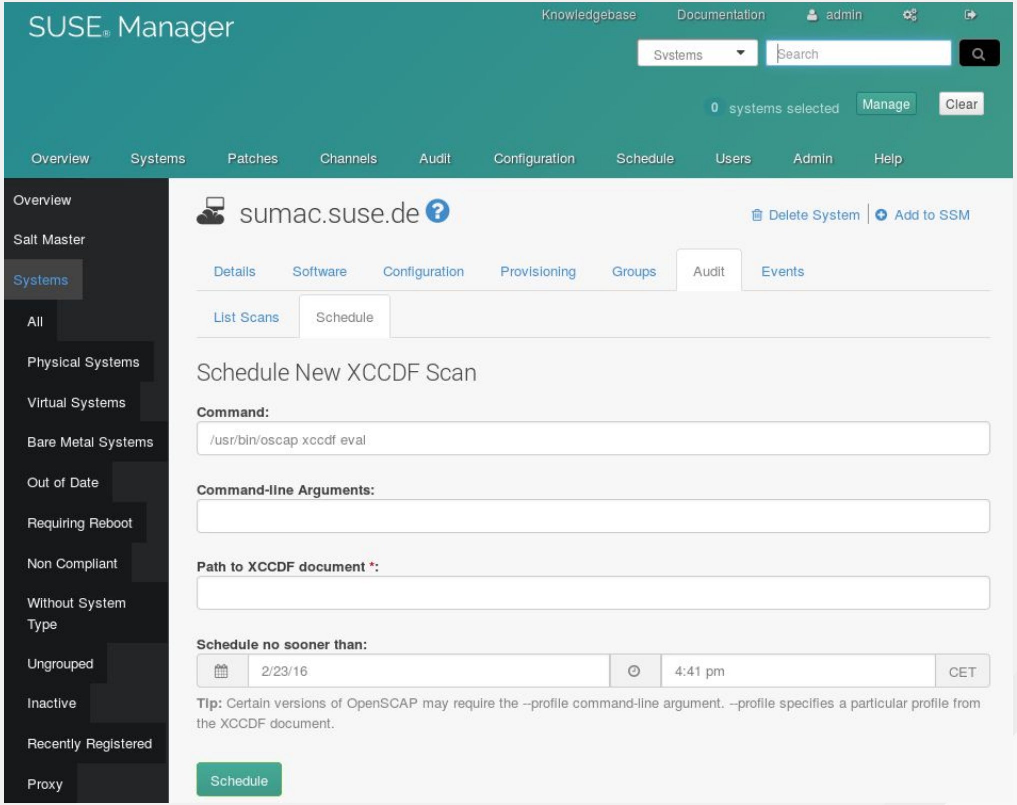
further references...

Red Hat Satellite 6.1 Feature Overview: OpenSCAP

https://www.youtube.com/watch?v=p4uNIzYId-Y

SUSE MANAGER

- Continuous scans
- Result storage
- Low-level compared to Satellite 6



Schedule New XCCDF Scan

Command: /usr/bin/oscap xccdf eval

Command-line Arguments:

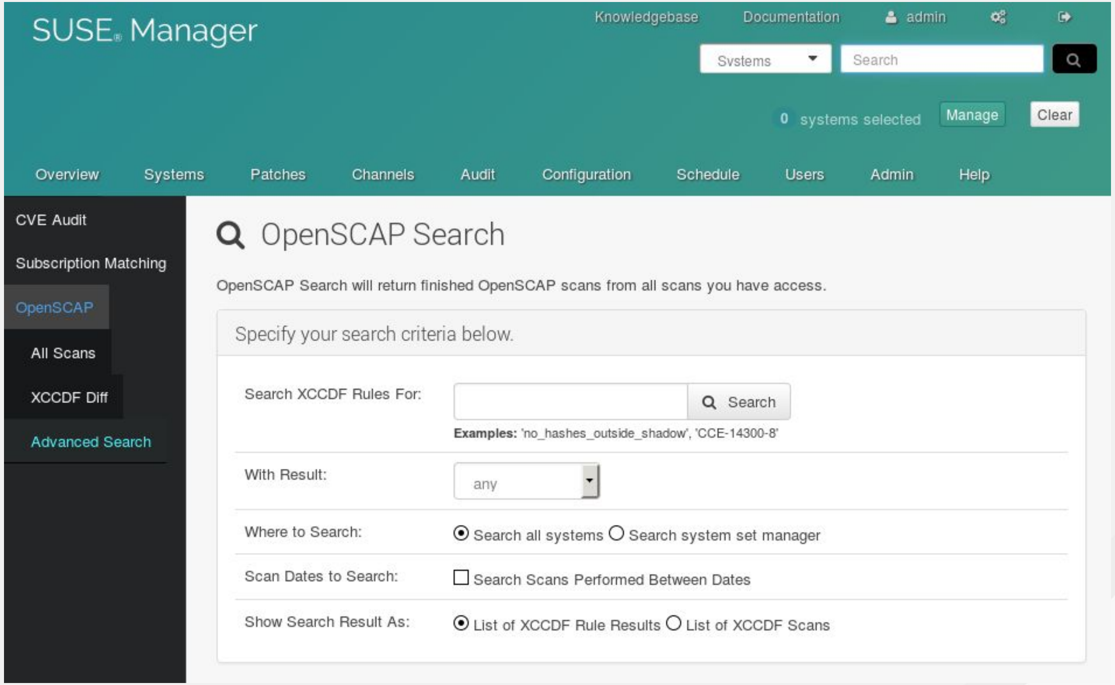
Path to XCCDF document *:

Schedule no sooner than: 2/23/16 4:41 pm CET

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

SUSE MANAGER

- Continuous scans
- Result storage
- Low-level compared to Satellite 6



OpenSCAP Search

OpenSCAP Search will return finished OpenSCAP scans from all scans you have access.

Specify your search criteria below.

Search XCCDF Rules For:

Examples: 'no_hashes_outside_shadow', 'CCE-14300-8'

With Result: any

Where to Search: ● Search all systems ○ Search system set manager

Scan Dates to Search: □ Search Scans Performed Between Dates

Show Search Result As: ● List of XCCDF Rule Results ○ List of XCCDF Scans

COMMUNITY

where to get more answers

- IRC: #openscap on irc.freenode.net
- Mailing lists
- https://www.open-scap.org/
- https://static.open-scap.org/
- Twitter! @OpenSCAP

redhat.

THANK YOU! Questions?

Martin Preisler
mpreisle@redhat.com
Senior Software Engineer, Red Hat, Inc.

Marek Haičman
mhaicman@redhat.com
Quality Engineer, Red Hat, Inc.

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos