Red Hat
Smart Management

Security Compliance: A Tale of Two Techniques

Another Installment in the Some Assembly Required Presentation Series

June 10th, 2020

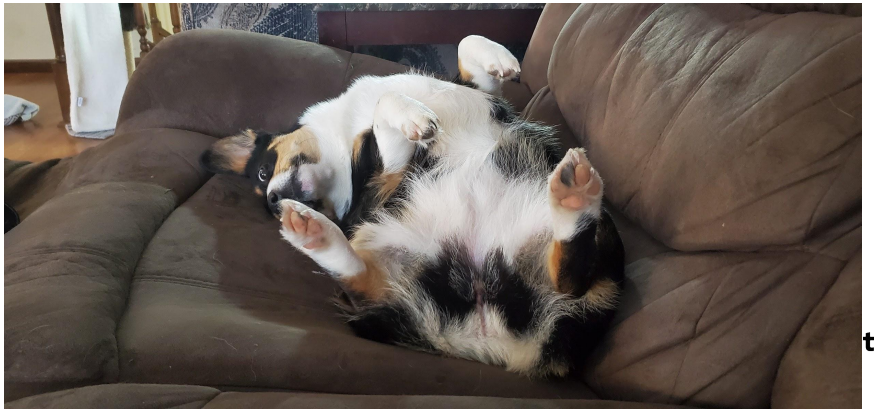
Josh Swanson
Solution Architect

Scott Danielson
Sr. Solution Architect

Red Hat

Josh Swanson

joshswanson@redhat.com



Shameless Plug

https://www.meetup.com/Ansible-Minneapolis/
https://www.youtube.com/channel/UC3IbK0ZyeYF56JBIUeRdU3Q

Thursday, June 18, 2020

Providing Governance to Self-Service Infrastructure Provisioning in the Cloud

Hosted by
Brian Dolan-Goecke and Josh Swanson

Share

Organizer tools

Ansible Minneapolis
Public group

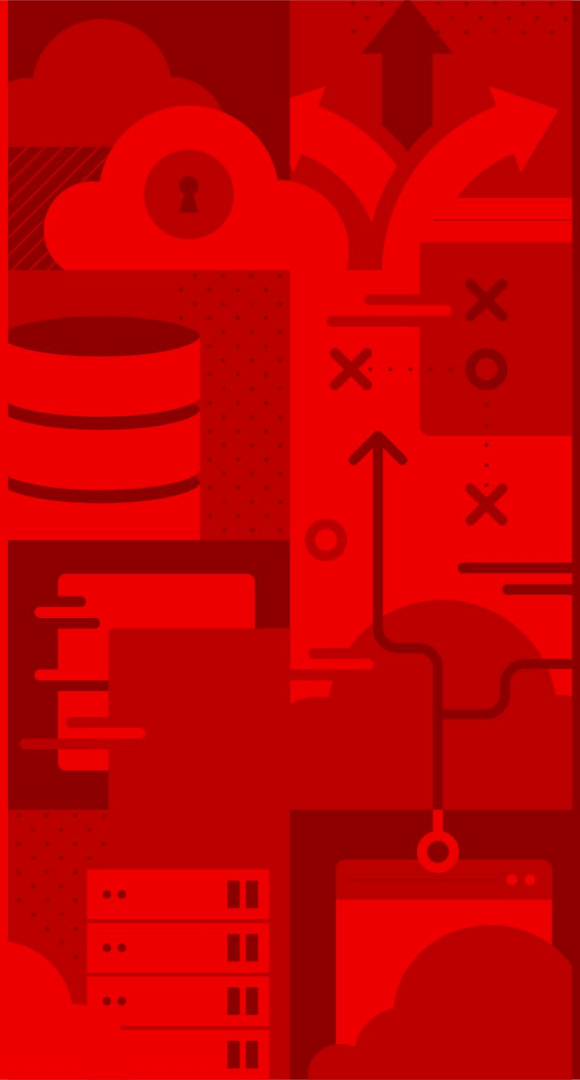
Thursday, June 18, 2020
6:30 PM to 9:30 PM CDT
Every 3rd Thursday of the month
Add to calendar

Online event
https://bluejeans.com/678555292?src=calendarLink

Report this event

Details

Provisioning infrastructure (bare-metal, cloud VMs, serverless) with Ansible allows you to seamlessly transition into configuration management, orchestration and application deployment using the same simple, human readable, automation language. Taking this one step further, running Ansible Automation Platform enables integration with your existing platforms to power self-service automation for people of various skill levels - domain expert, junior architect, operations specialist, etc.



Where Are We Going?

- What is SCAP?
- Getting OpenSCAP content
- Compliance the Satellite Way
- Compliance the Insights Way
- Comparing the Two Workflows
- Using Ansible to Achieve Compliance (Brief Overview)

Red Hat

What is SCAP?

Security Content Automation Protocol

The **Security Content Automation Protocol** (SCAP) is a method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization, including e.g., FISMA compliance. The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP.

http://goo.gl/GBaiIW

SCAP Components

- XCCDF: The Extensible Configuration Checklist Description Format
- OVAL®: Open Vulnerability and Assessment Language
- Asset Identification
- ARF: Asset Reporting Format
- CCE™: Common Configuration Enumeration
- CPE™: Common Platform Enumeration
- CVE®: Common Vulnerabilities and Exposures
- CVSS: Common Vulnerability Scoring System

Helpful links: https://access.redhat.com/articles/1438123 and https://www.open-scap.org/features/scap-components/

What is OpenSCAP?

Open Source Security Compliance Solution

The `oscap` program is a command line tool that allows users to load, scan, validate, edit, and export SCAP documents.

- Homepage of the project: www.open-scap.org
- Manual: Oscap User Manual
- For new contributors: How to contribute

OpenSCAP is an open implementation of SCAP components

Why is OpenSCAP is needed?

Security compliance

In the ever-changing world of computer security where new vulnerabilities are being discovered and patched every day, enforcing security compliance must be a continuous process. The OpenSCAP ecosystem provides tools and customizable policies for a quick, cost-effective and flexible implementation

Vulnerability assessment

A timely inspection of software inventory that identifies such vulnerabilities is a must for any organization in the 21st century, and the OpenSCAP project provides tools for automated vulnerability checking, allowing you to take steps to prevent attacks before they happen.

OpenSCAP umbrella projects

-OpenSCAP Base

- provide oscap command

-OpenSCAP Daemon

- evaluate by schedule

-SCAP Workbench

- graphical utility

-SCAPTimony

- compliance of your infrastructure.

-OSCAP Anaconda Add-on

- an add-on for installer used by Fedora and Red Hat Enterprise Linux 7/8.

-SCAP Security Guide

- OpenSCAP **content** primarily for Red Hat Enterprise Linux

Why OpenSCAP is a good choice?

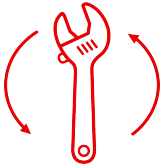
- OpenSCAP has received a NIST certification for its support of SCAP 1.2.
- Red Hat sponsors OpenSCAP
- Red Hat supports OpenSCAP with RHEL Subscriptions
- Red Hat Enterprise Linux 7 and 8 contains OpenSCAP packages
- Red Hat integrates OpenSCAP with Red Hat Products (Satellite/Insights)

Compliance

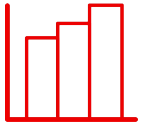
Built on OpenSCAP reporting

Compliance offers

Assess and monitor the degree/level of compliance to a policy for Red Hat products with operational ease



Remediate known issues of non-compliance in the Red Hat environment via Ansible playbooks based on business risk & relevance



Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

Getting OpenSCAP Profiles

Red Hat

Getting OpenSCAP Profiles

Shipped with RHEL

```
[root@rocinante ~]# yum install scap-security-guide
Updating Subscription Management repositories.
...
Dependencies resolved.
Installing:
 scap-security-guide
Installing dependencies:
 xml-common
 openscap-scanner
 GConf2
 openscap
...
Complete!
[root@rocinante ~]# ls /usr/share/xml/scap/ssg/content/
ssg-firefox-cpe-dictionary.xml  ssg-jre-cpe-dictionary.xml  ssg-rhel6-cpe-dictionary.xml  ssg-rhel7-cpe-dictionary.xml  ssg-rhel8-cpe-dictionary.xml
ssg-firefox-cpe-oval.xml        ssg-jre-cpe-oval.xml        ssg-rhel6-cpe-oval.xml        ssg-rhel7-cpe-oval.xml        ssg-rhel8-cpe-oval.xml
ssg-firefox-ds-1.2.xml          ssg-jre-ds-1.2.xml          ssg-rhel6-ds-1.2.xml          ssg-rhel7-ds-1.2.xml          ssg-rhel8-ds-1.2.xml
ssg-firefox-ds.xml              ssg-jre-ds.xml              ssg-rhel6-ds.xml              ssg-rhel7-ds.xml              ssg-rhel8-ds.xml
ssg-firefox-ocil.xml            ssg-jre-ocil.xml            ssg-rhel6-ocil.xml            ssg-rhel7-ocil.xml            ssg-rhel8-ocil.xml
ssg-firefox-oval.xml            ssg-jre-oval.xml            ssg-rhel6-oval.xml            ssg-rhel7-oval.xml            ssg-rhel8-oval.xml
ssg-firefox-xccdf.xml           ssg-jre-xccdf.xml           ssg-rhel6-xccdf.xml           ssg-rhel7-xccdf.xml           ssg-rhel8-xccdf.xml

[root@rocinante jswanson]# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Document type: Source Data Stream
Imported: 2020-02-11T13:41:24

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
Generated: (null)
Version: 1.3
```

Getting OpenSCAP Profiles

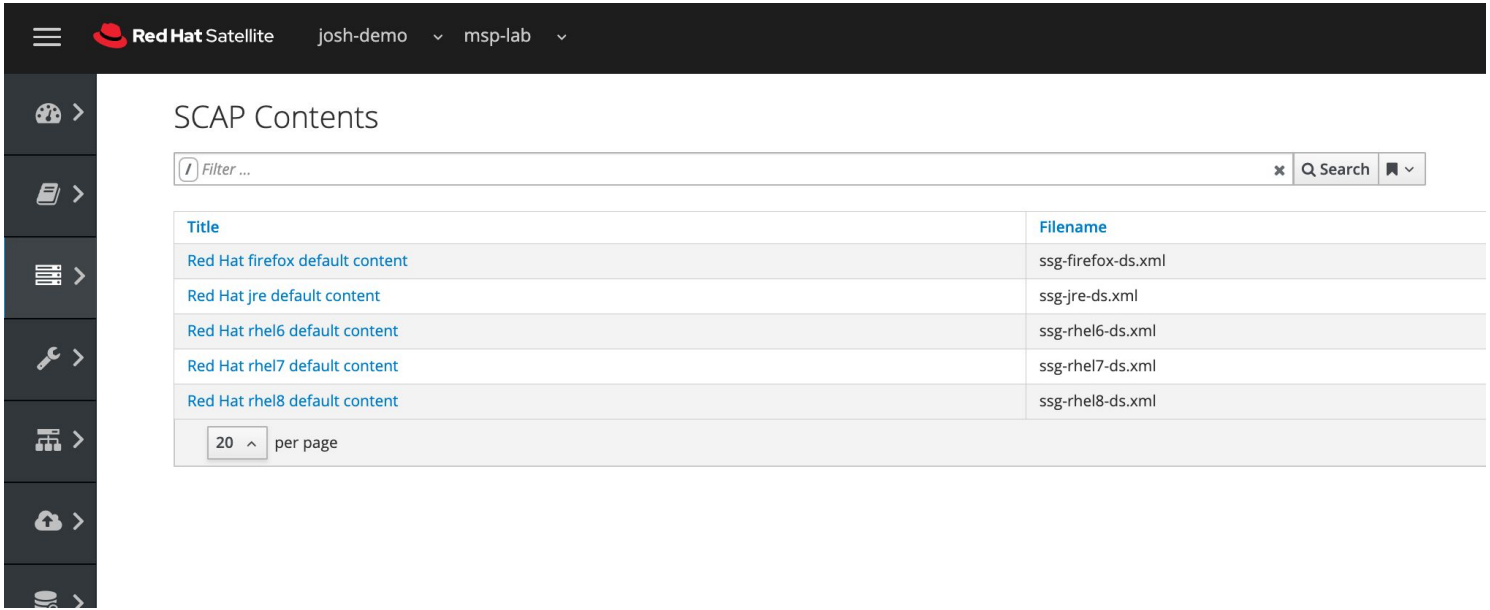
Shipped with RHEL

```
[jswanson@rocinante ~]$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Document type: Source Data Stream
...
                    Profiles:
                              Title: Health Insurance Portability and Accountability Act (HIPAA)
                                        Id: xccdf_org.ssgproject.content_profile_hipaa
                              Title: NIST National Checklist Program Security Guide
                                        Id: xccdf_org.ssgproject.content_profile_ncp
                              Title: OSPP - Protection Profile for General Purpose Operating Systems v4.2.1
                                        Id: xccdf_org.ssgproject.content_profile_ospp
                              Title: VPP - Protection Profile for Virtualization v. 1.0 for Red Hat Enterprise Linux Hypervisor (RHELH)
                                        Id: xccdf_org.ssgproject.content_profile_rhelh-vpp
                              Title: DRAFT - ANSSI DAT-NT28 (high)
                                        Id: xccdf_org.ssgproject.content_profile_anssi_nt28_high
                              Title: DRAFT - ANSSI DAT-NT28 (minimal)
                                        Id: xccdf_org.ssgproject.content_profile_anssi_nt28_minimal
                              Title: Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
                                        Id: xccdf_org.ssgproject.content_profile_rht-ccp
                              Title: Criminal Justice Information Services (CJIS) Security Policy
                                        Id: xccdf_org.ssgproject.content_profile_cjis
                              Title: PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 7
                                        Id: xccdf_org.ssgproject.content_profile_pci-dss
                              Title: DISA STIG for Red Hat Enterprise Linux 7
                                        Id: xccdf_org.ssgproject.content_profile_stig
                              Title: Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
                                        Id: xccdf_org.ssgproject.content_profile_cui
                              Title: Standard System Security Profile for Red Hat Enterprise Linux 7
                                        Id: xccdf_org.ssgproject.content_profile_standard
```

Getting OpenSCAP Datastream Files

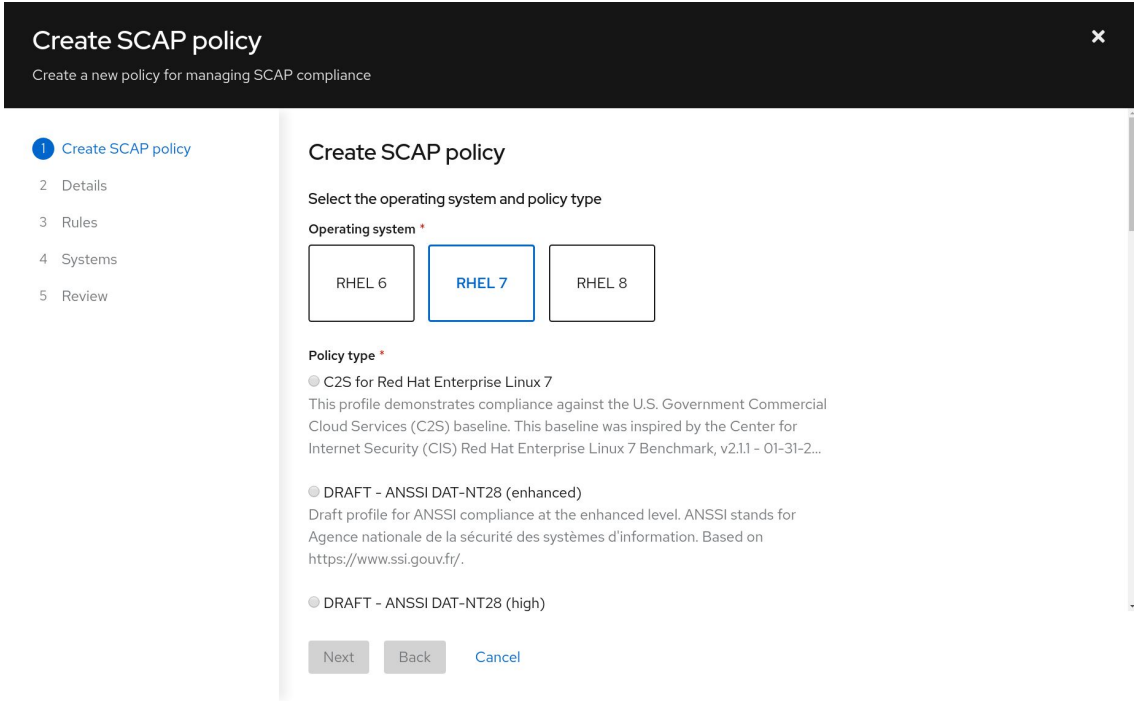
Shipped with Satellite

```
[root@satellite01 ~]# foreman-rake foreman_openscap:bulk_upload:default
```



Getting OpenSCAP Datastream Files

Provided in Compliance on cloud.redhat.com



Getting OpenSCAP Datastream Files

https://nvd.nist.gov/ncp/repository

NIST

NVD MENU

Information Technology Laboratory

NATIONAL CHECKLIST PROGRAM

NVD

NCP

National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.

NCP provides metadata and links to checklists of various formats including checklists that conform to the Security Content Automation Protocol (SCAP). SCAP enables validated security products to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms. Please note that the current search fields have been adjusted to reflect NIST SP 800-70 Revision 4.

Search for Checklists using the fields below. The keyword search will search across the name, and summary.

Checklist Type: Any..... | Content Type: Any..... | Search | Reset

Authority: Any..... | Tool Compatibility: Any.....

Target: Any..... | Keyword:

Order By: Resource (Content Type Ascending)

There are **515** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Name (Version)	Target	Authority	Last Modified	Resources
NIST National Checklist for Red Hat Virtualization Host 4.x (content v0.1.48)	Red Hat Virtualization Host 4.3	Red Hat	01/27/2020	➖ SCAP 1.3 Content - NIST National Checklist for Red Hat Virtualization Host 4.x ➖ Ansible Playbook - [DRAFT] DISA STIG for Red Hat Virtualization Host (RHVH) ➖ Ansible Playbook - VPP - Protection Profile for Virtualization v. 1.0 for Red Hat Virtualization Hypervisor (RHVH) ➖ Machine-Readable Format - OpenControl-formatted NIST 800-53 responses for Red Hat Virtualization Host 4.x
NIST National Checklist for Red Hat Enterprise Linux 7.x (content v0.1.48)	Red Hat Enterprise Linux 7.0 Red Hat Enterprise Linux 7.1 Red Hat Enterprise Linux 7.2 Red Hat Enterprise Linux 7.3	Red Hat	05/12/2020	➖ SCAP 1.3 Content - NIST National Checklist for Red Hat Enterprise Linux 7.x, SCAP 1.3 ➖ Ansible Playbook - CIA Commercial Cloud Services (CIA C2S) ➖ Ansible Playbook - FBI Criminal Justice Information Services (FBI CJIS)

Compliance the Satellite Way

Red Hat

Compliance the Satellite Way Deployment Checklist

- Load in the Ansible OpenSCAP role
- Load in the Ansible OpenSCAP role vars
- Upload the OpenSCAP content files
- Create a new policy
- Deploy the Ansible OpenSCAP role on hosts

Loading in the Ansible Role

Red Hat Satellite josh msp-lab

Monitor
Content
Hosts
Configure
Infrastructure
Insights
Administer

Roles » Changed Ansible roles

Select the changes you want to realize in Satellite

Toggle: New | Obsolete

	Name
☑	theforeman.foreman_scap_client
☐	project-receptor.satellite_receptor_installer

Cancel Update

Loading in the Ansible Role Vars

Red Hat Satellite josh msp-lab

Monitor
Content
Hosts
Configure
Infrastructure
Insights
Administer

Variables » Changed Ansible variables

Select the changes you want to realize in Satellite

Check/Uncheck all Obsolete Update

	Name	Ansible role
☑	foreman_scap_client_state	theforeman.foreman_scap_client
☑	foreman_scap_client_server	theforeman.foreman_scap_client
☑	foreman_scap_client_port	theforeman.foreman_scap_client
☑	foreman_scap_client_policies	theforeman.foreman_scap_client
☑	foreman_scap_client_ca_cert_path	theforeman.foreman_scap_client
☑	foreman_scap_client_host_cert_path	theforeman.foreman_scap_client
☑	foreman_scap_client_host_private_key_path	theforeman.foreman_scap_client
☑	foreman_scap_client_release	theforeman.foreman_scap_client
☑	foreman_scap_client_repo_url	theforeman.foreman_scap_client
☑	foreman_scap_client_repo_state	theforeman.foreman_scap_client
☑	foreman_scap_client_repo_key	theforeman.foreman_scap_client
☑	foreman_scap_client_repo_gpg	theforeman.foreman_scap_client
☑	foreman_scap_client_cron_template	theforeman.foreman_scap_client
☑	foreman_scap_client_cron_splay_seed	theforeman.foreman_scap_client
☑	foreman_scap_client_cron_splay	theforeman.foreman_scap_client
☑	foreman_scap_client_fetch_remote_resources	theforeman.foreman_scap_client
☑	foreman_scap_client_http_proxy_server	theforeman.foreman_scap_client
☑	foreman_scap_client_http_proxy_port	theforeman.foreman_scap_client

Cancel Update

Loading in the Ansible Role Vars

Ansible Variables

Filter ... | Search

Import from satellite01.lab.msp.redhat.com | New Ansible Variable | Documentation

Name	Role	Type	Imported?	Actions
foreman_scap_client_ca_cert_path	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_cron_splay	theforeman.foreman_scap_client	integer	✔	Delete
foreman_scap_client_cron_splay_seed	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_cron_template	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_fetch_remote_resources	theforeman.foreman_scap_client	boolean	✔	Delete
foreman_scap_client_host_cert_path	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_host_private_key_path	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_http_proxy_port	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_http_proxy_server	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_policies	theforeman.foreman_scap_client	array	✔	Delete
foreman_scap_client_port	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_release	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_repo_gpg	theforeman.foreman_scap_client	boolean	✔	Delete
foreman_scap_client_repo_key	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_repo_state	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_repo_url	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_server	theforeman.foreman_scap_client	string	✔	Delete
foreman_scap_client_state	theforeman.foreman_scap_client	string	✔	Delete

20 per page

1-18 of 18 « ‹ 1 of 1 › »

Uploading OpenSCAP Content (Manual)

Scap Contents » Upload new SCAP content file

File Upload | Locations | Organizations

Title * ssg-rhel7-ds

Scap File * Choose File ssg-rhel7-ds.xml

Submit Cancel

Uploading OpenSCAP Content (Manual)

SCAP Contents

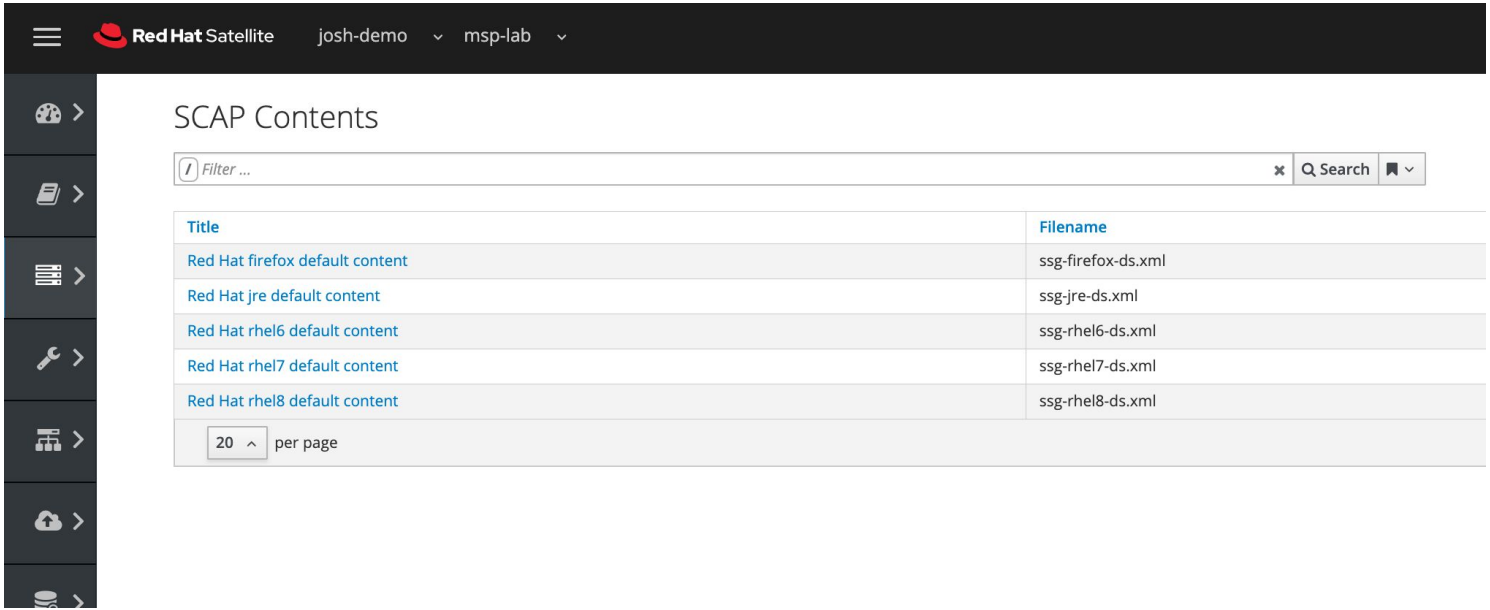
/ Filter ... Search

Title	Filename
ssg-rhel7-ds	ssg-rhel7-ds.xml
ssg-rhel8-ds	ssg-rhel8-ds.xml

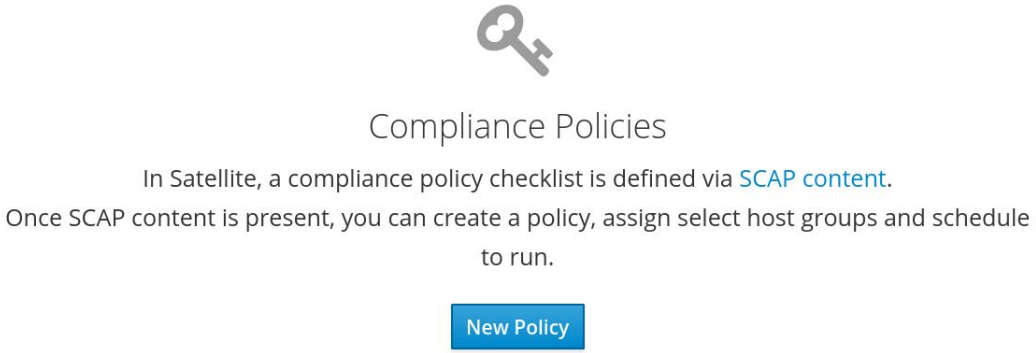
20 per page

Uploading OpenSCAP Content (Manual)

```
[root@satellite01 ~]# foreman-rake foreman_openscap:bulk_upload:default
```



Setting Up Compliance Policies



Setting Up Compliance Policies

Policies » New Compliance Policy

1 Deployment Options | 2 Policy Attributes | 3 SCAP Content | 4 Schedule | 5 Locations | 6 Organizations | 7 Hostgroups

There are significant differences in deployment options. Please make sure you understand them by reading our documentation.

Ansible

Puppet

Manual

Setting Up Compliance Policies

Policies » New Compliance Policy

1 Deployment Options | 2 Policy Attributes | 3 SCAP Content | 4 Schedule | 5 Locations | 6 Organizations | 7 Hostgroups

Name: rhel7 - hipaa

Description: HIPAA on RHEL7 hosts

Setting Up Compliance Policies

Policies » New Compliance Policy

1 Deployment Options | 2 Policy Attributes | 3 SCAP Content | 4 Schedule | 5 Locations | 6 Organizations | 7 Hostgroups

SCAP Content: ssg-rhel7-ds

XCCDF Profile: Health Insurance Portability and Accountability Act (HIPAA)

Tailoring File: Choose Tailoring File

Setting Up Compliance Policies

Policies » New Compliance Policy

1 Deployment Options | 2 Policy Attributes | 3 SCAP Content | 4 Schedule | 5 Locations | 6 Organizations | 7 Hostgroups

Period: Custom

Cron Line: */5 * * * *

You can specify custom cron line, e.g. "0 3 * * *", separate each of 5 values by space

Setting Up Compliance Policies

Policies » New Compliance Policy

1 Deployment Options | 2 Policy Attributes | 3 SCAP Content | 4 Schedule | 5 Locations | 6 Organizations | 7 Hostgroups

Hostgroups

All items *Filter* +

- rhel7-kickstart
- rhel8-kickstart
- rhel8-kickstart/rhel8-hipaa

Selected items −

- rhel7-kickstart/rhel7-hipaa

Setting Up Compliance Policies

Compliance Policies

Filter ... Search

Name	Content	Profile	Tailoring File
rhel7 - hipaa	ssg-rhel7-ds	Health Insurance Portability and Accountability Act (HIPAA)	None

20 per page

Setting Up Compliance Policies

Jobs » Run Ansible roles

Rerun | Rerun failed | Job Task | Cancel Job | Abort Job

Overview | Preview templates

Results

100%
Success

2 | 0 | 0 | 0

Target hosts

Manual selection using **static query**

```
name ^ (hipaa-rhel7-01.josh.lab.msp.redhat.com, hipaa-rhel7-02.josh.lab.msp.redhat.com)
```

Execution order: **alphabetical**

Evaluated at: 2020-04-17 10:18:16 -0500

root
Ansible Roles - Ansible Default effective user

2
Total hosts

Filter ... | Search

Host	Status	Actions
hipaa-rhel7-01.josh.lab.msp.redhat.com	success	Host detail
hipaa-rhel7-02.josh.lab.msp.redhat.com	success	Host detail

20 per page

1-2 of 2 « ‹ 1 of 1 › »

Red Hat

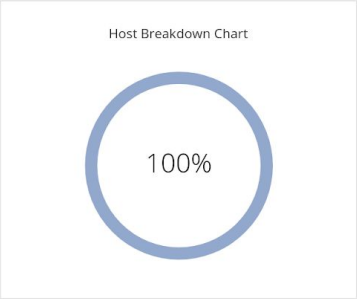
Getting OpenSCAP Datastream Files

```
[root@hipaa-rhel7-01 ~]# cat /etc/cron.d/foreman_scap_client_cron
# DO NOT EDIT THIS FILE MANUALLY
# IT IS MANAGED BY ANSIBLE
# ANY MANUAL CHANGES WILL BE LOST ON THE NEXT ANSIBLE EXECUTION
#
# Executing foreman_scap_client from command line may be useful for debugging purposes.

# foreman_scap_client cron job
*/5 * * * * root /bin/sleep 355; /usr/bin/foreman_scap_client 6 2>&1 | logger -t foreman_scap_client


[root@hipaa-rhel7-01 ~]# ps aux | grep scap
root       7860  0.0  0.0 113184  1200 ?        Ss   15:20   0:00 /bin/sh -c /bin/sleep 355; /usr/bin/foreman_scap_client 6 2>&1 | logger -t foreman_scap_client
root       7903  0.0  0.0 112712   968 pts/1    S+   15:20   0:00 grep --color=auto scap
```

Red Hat

Viewing Overall Compliance

Compliance policy: rhel7 - hipaa



Hosts Breakdown

Compliant with the policy

0

Not compliant with the policy

0

Inconclusive results

0

Never audited

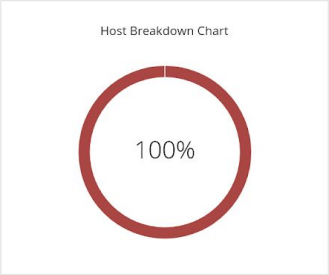
2

Total hosts with policy: 2

Hosts no longer assigned: 0

Viewing Overall Compliance

Compliance policy: rhel7 - hipaa



Hosts Breakdown

Compliant with the policy
0

Not compliant with the policy
2

Inconclusive results
0

Never audited
0

Total hosts with policy: 2

Hosts no longer assigned: 0

Latest reports for policy: rhel7 - hipaa

Host	Policy assigned	Date	Passed	Failed	Other	Actions
hipaa-rhel7-01.josh.lab.msp.redhat.com	✔	less than a minute ago	43	96	2	View Report
hipaa-rhel7-02.josh.lab.msp.redhat.com	✔	2 minutes ago	43	96	2	View Report

20 per page

1-2 of 2 « ‹ 1 of 1 › »

Viewing Compliance Details

Compliance Reports » hipaa-rhel7-01.josh.lab.msp.redhat.com

Show log messages:
All messages

Back | Delete | Host details | View full report | Download XML in bzip | Download HTML

Reported at Apr 17, 10:26 AM for policy rhel7 - hipaa through satellite01.lab.msp.redhat.com

Result	Message	Resource	Severity	Actions
fail	Disable KDump Kernel Crash Analyzer (kdump)	xccdf_org.ssgproject.content_rule_service_kdump_disabled	Medium	Hosts failing this rule
fail	Use Only FIPS 140-2 Validated Ciphers	xccdf_org.ssgproject.content_rule_sshd_use_approved_ciphers	Medium	Hosts failing this rule
fail	Disable SSH Root Login	xccdf_org.ssgproject.content_rule_sshd_disable_root_login	Medium	Hosts failing this rule
pass	Enable Use of Strict Mode Checking	xccdf_org.ssgproject.content_rule_sshd_enable_strictmodes	Medium	Hosts failing this rule
fail	Enable Use of Privilege Separation	xccdf_org.ssgproject.content_rule_sshd_use_priv_separation	Medium	Hosts failing this rule
fail	Enable SSH Warning Banner	xccdf_org.ssgproject.content_rule_sshd_enable_warning_banner	Medium	Hosts failing this rule
pass	Disable Kerberos Authentication	xccdf_org.ssgproject.content_rule_sshd_disable_kerb_auth	Medium	Hosts failing this rule
pass	Disable Compression Or Set Compression to delayed	xccdf_org.ssgproject.content_rule_sshd_disable_compression	Medium	Hosts failing this rule
fail	Disable GSSAPI Authentication	xccdf_org.ssgproject.content_rule_sshd_disable_gssapi_auth	Medium	Hosts failing this rule
pass	Disable Host-Based Authentication	xccdf_org.ssgproject.content_rule_disable_host_auth	Medium	Hosts failing this rule
fail	Set SSH Client Alive Max Count	xccdf_org.ssgproject.content_rule_sshd_set_keepalive	Medium	Hosts failing this rule
fail	Allow Only SSH Protocol 2	xccdf_org.ssgproject.content_rule_sshd_allow_only_protocol2	High	Hosts failing this rule
pass	Disable SSH Support for Rhosts RSA Authentication	xccdf_org.ssgproject.content_rule_sshd_disable_rhosts_rsa	Medium	Hosts failing this rule
fail	Do Not Allow SSH Environment Options	xccdf_org.ssgproject.content_rule_sshd_do_not_permit_user_env	Medium	Hosts failing this rule
fail	Use Only FIPS 140-2 Validated MACs	xccdf_org.ssgproject.content_rule_sshd_use_approved_macs	Medium	Hosts failing this rule
pass	Disable SSH Access via Empty Passwords	xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords	High	Hosts failing this rule
pass	Enable cron Service	xccdf_org.ssgproject.content_rule_service_crond_enabled	Medium	Hosts failing this rule
pass	Disable Quagga Service	xccdf_org.ssgproject.content_rule_service_zebra_disabled	Medium	Hosts failing this rule
pass	Uninstall talk Package	xccdf_org.ssgproject.content_rule_package_talk_removed	Medium	Hosts failing this rule
pass	Uninstall talk-server Package	xccdf_org.ssgproject.content_rule_package_talk-server_removed	Medium	Hosts failing this rule
pass	Uninstall rsh Package	xccdf_org.ssgproject.content_rule_package_rsh_removed	Unknown	Hosts failing this rule
pass	Disable rlogin Service	xccdf_org.ssgproject.content_rule_service_rlogin_disabled	High	Hosts failing this rule
pass	Disable rexec Service	xccdf_org.ssgproject.content_rule_service_rexec_disabled	High	Hosts failing this rule
pass	Disable rsh Service	xccdf_org.ssgproject.content_rule_service_rsh_disabled	High	Hosts failing this rule

Compliance the Insights Way

Red Hat

Red Hat Insights

Now included with all Red Hat Enterprise Linux subscriptions

Buy

Red Hat Enterprise Linux

Get

Red Hat Insights

Red Hat Insights

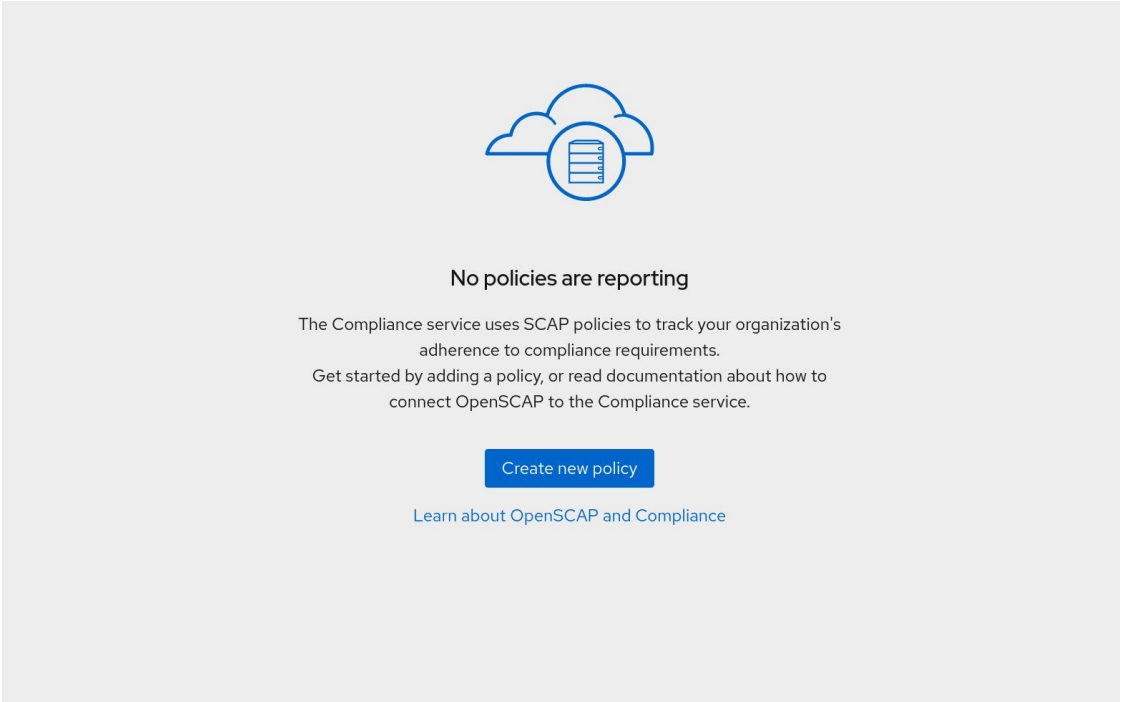
ansible-galaxy install redhatinsights.insights-client

```
roles/requirements.yml
---
- src: redhatinsights.insights-client

rhel_standards.insights.yml
---
- name: deploy redhat insights
  hosts:
    - all
  roles:
    - redhatinsights.insights-client
```

Compliance the Insights Way
Deployment Checklist

- Setup a SCAP policy on cloud.redhat.com
- Install OpenSCAP packages
- Create a cronjob to repeat compliance scanning

Setting Up Compliance Policies



Setting Up Compliance Policies

Create SCAP policy

Create a new policy for managing SCAP compliance

1. Create SCAP policy
2. Details
3. Rules
4. Systems
5. Review

Create SCAP policy

Select the operating system and policy type

Operating system *

RHEL 6 | RHEL 7 | RHEL 8

Policy type *

C2S for Red Hat Enterprise Linux 7
This profile demonstrates compliance against the U.S. Government Commercial Cloud Services (C2S) baseline. This baseline was inspired by the Center for Internet Security (CIS) Red Hat Enterprise Linux 7 Benchmark, v2.1.1 - 01-31-2...

DRAFT - ANSSI DAT-NT28 (enhanced)
Draft profile for ANSSI compliance at the enhanced level. ANSSI stands for Agence nationale de la sécurité des systèmes d'information. Based on https://www.ssi.gouv.fr/.

DRAFT - ANSSI DAT-NT28 (high)

Next | Back | Cancel

Setting Up Compliance Policies

Create SCAP policy

Create a new policy for managing SCAP compliance

1 Create SCAP policy
2 Details
3 Rules
4 Systems
5 Review

Policy details

Policy name *

Health Insurance Portability and Accountability Act (HIPAA)

Reference ID *

xccdf_org.ssgproject.content_profile_hipaa

Description

The HIPAA Security Rule establishes U.S. national standards to protect individuals' electronic personal health information that is created, received, used, or

Compliance threshold

The compliance threshold defines what percentage of rules must be met in order for a system to be determined "compliant".

Compliance threshold (%)

100

Next Back Cancel

Setting Up Compliance Policies

Create SCAP policy

Create a new policy for managing SCAP compliance

1. Create SCAP policy
2. Details
3. Rules
4. Systems
5. Review

Filter by Name | 144 results | 1 - 10 of 144

Selected | Show selected rules | Clear filters

Rule	Severity	Ansible
Verify that Interactive Boot is Disabled CCE-27335-9	Medium	✓
Verify File Hashes with RPM CCE-27157-7	High	✓
Verify Any Configured IPSec Tunnel Connections CCE-80171-2	Medium	No
Verify and Correct File Permissions with RPM	High	✓

Next | Back | Cancel

Setting Up Compliance Policies

Create SCAP policy

Create a new policy for managing SCAP compliance

1. Create SCAP policy
2. Details
3. Rules
4. Systems
5. Review

Systems

Choose systems to scan with this policy. You can add and remove systems later.

Name | hipaa-rhel7 | 1 - 2 of 2

Display name: hipaa-rhel7 | Status: Fresh, Stale | Source: Insights | Clear filters

System name	Policies
hipaa-rhel7-02.josh.lab.msp.redhat.com	
hipaa-rhel7-01.josh.lab.msp.redhat.com	

1 - 2 of 2 | 1 of 1

Next | Back | Cancel

Setting Up Compliance Policies

Create SCAP policy

Create a new policy for managing SCAP compliance

1. Create SCAP policy
2. Details
3. Rules
4. Systems
5. Review

Review

Review your policy before finishing. SCAP security guide, policy type and name cannot be changed after initial creation. Make sure they are correct!

SCAP security guide	Guide to the Secure Configuration of Red Hat Enterprise Linux 7 - 0.1.47
Policy type	Health Insurance Portability and Accountability Act (HIPAA)
Generated ID	xccdf_org.ssgproject.content_profile_hipaa
Number of systems	2

Finish Back Cancel

Setting Up Compliance Policies

SCAP policies

Filter by Name

Create new policy

1 results

Policy name	Operating system	Systems	Business objective
Health Insurance Portability and Accountability Act (HIPAA)	RHEL 7 (SSG 0.1.47)	2	--

Getting OpenSCAP Datastream Files

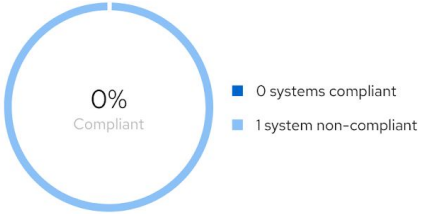
```
[root@msp-rhug-rhel-01 ~]# yum -y install scap-security-guide openscap-scanner openscap
...
Installed:
  GConf2-3.2.6-22.el8.x86_64                                          openscap-1.3.2-6.el8.x86_64
openscap-scanner-1.3.2-6.el8.x86_64                                          scap-security-guide-0.1.48-7.el8.noarch
xml-common-0.6.3-50.el8.noarch
Complete!
[root@msp-rhug-rhel-01 ~]# insights-client --compliance
Running scan for xccdf_org.ssgproject.content_profile_pci-dss... this may take a while
Uploading Insights data.
Successfully uploaded report for msp-rhug-rhel-01.josh.lab.msp.redhat.com.
```

Getting OpenSCAP Datastream Files

Reports > PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8

PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8 report

Delete Report



Policy details

View policy

Operating system	RHEL 8 (SSG 0.1.48)
Compliance threshold	100.0%
Business objective	--

Filter by Name

Remediate

1 - 1 of 1

System name	Rules failed	Compliance score	Last scanned
msp-rhug-rhel-01.josh.lab.msp.redhat.com	76	58%	3 minutes ago

1 - 1 of 1 1 of 1

Getting OpenSCAP Datastream Files

Systems > msp-rhug-rhel-01.josh.lab.msp.redhat.com

msp-rhug-rhel-01.josh.lab.msp.redhat.com

Delete View in Inventory

UUID: feaabdd7-dd9b-4eb0-8f3a-22d3f39decfb

Last seen: 08 Jun 2020 21:17 UTC

PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8

Noncompliant

39 of 115 rules passed (58%)

Profile: xccdf_org.ssgproject.content_profile_pci-dss
SSG version: 0.1.48

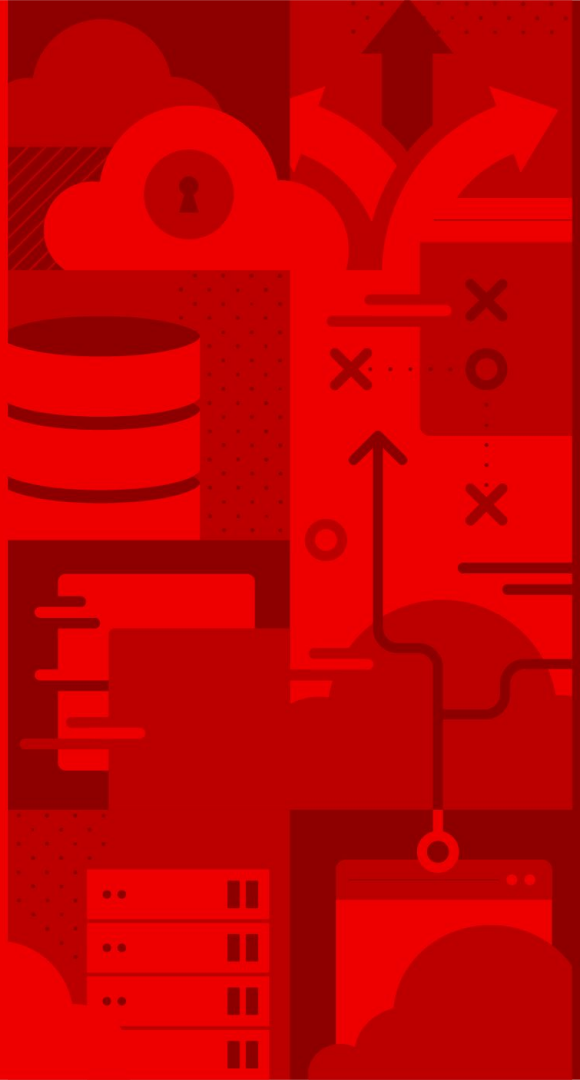
Last scanned: 4 minutes ago

Filter by Name | Remediate | 76 results | 1 - 10 of 76

Passed failed | Clear filters

Rule	Policy	Severity	Passed	Ansible
Verify and Correct File Permissions with RPM CCE-80858-4	PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8	High	!	✓
Set SSH Idle Timeout Interval CCE-80906-1	PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8	Medium	!	✓

Red Hat



Comparing the Two Workflows

Red Hat

Management Flexibility

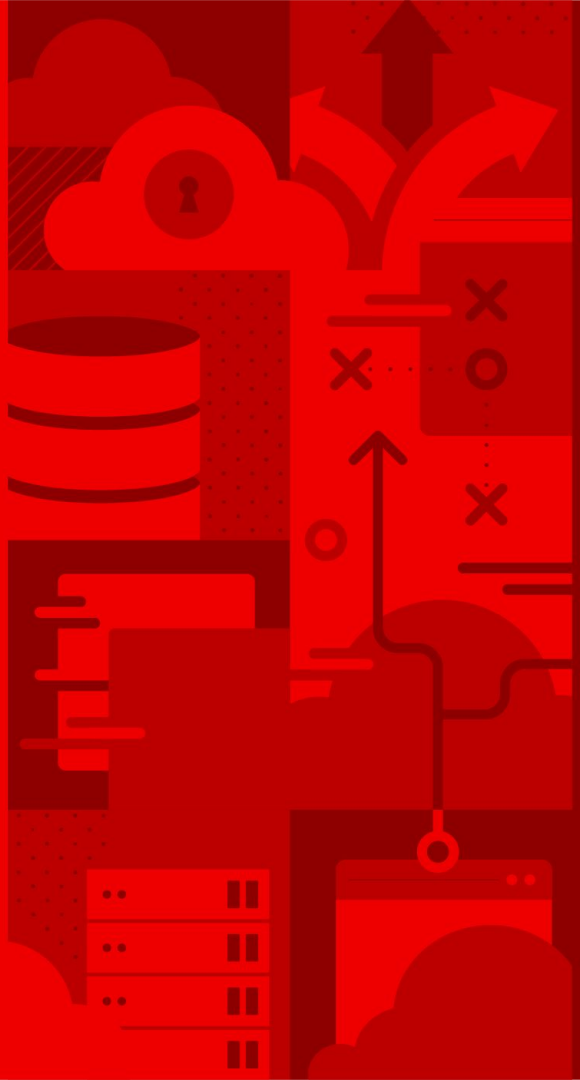
Offering Red Hat Management on-premises or in the cloud

Red Hat Satellite

- Requirements for resource set up and configuration
- Addresses on-prem or disconnected environment
- Limited to viewing hosts registered to the individual Satellite servers
- More footwork before the first compliance scan

cloud.redhat.com Services

- No requirements for resource set up and maintenance
- Adopt new features faster with a software-as-a-service preference
- Single view of all hosts across your RH infrastructure
- Less footwork before the first compliance scan



Using Ansible to Achieve Compliance

Red Hat

Using Ansible to Achieve Compliance

```
[root@rocinante jswanson]# ls /usr/share/scap-security-guide/ansible/
firefox-playbook-default.yml       rhel6-playbook-fisma-medium-rhel6-server.yml  rhel7-playbook-anssi_nt28_enhanced.yml      rhel7-playbook-hipaa.yml       rhel8-playbook-default.yml
firefox-playbook-stig.yml          rhel6-playbook-ftp-server.yml                 rhel7-playbook-anssi_nt28_high.yml          rhel7-playbook-ncp.yml         rhel8-playbook-e8.yml
jre-playbook-default.yml           rhel6-playbook-nist-CL-IL-AL.yml              rhel7-playbook-anssi_nt28_intermediary.yml  rhel7-playbook-ospp.yml        rhel8-playbook-ospp.yml
jre-playbook-stig.yml              rhel6-playbook-pci-dss.yml                    rhel7-playbook-anssi_nt28_minimal.yml       rhel7-playbook-pci-dss.yml     rhel8-playbook-pci-dss.yml
rhel6-playbook-C2S.yml             rhel6-playbook-rht-ccp.yml                    rhel7-playbook-C2S.yml                      rhel7-playbook-rhelh-stig.yml  rhel8-playbook-stig.yml
rhel6-playbook-CS2.yml             rhel6-playbook-server.yml                     rhel7-playbook-cjis.yml                     rhel7-playbook-rhelh-vpp.yml
rhel6-playbook-CSCF-RHEL6-MLS.yml  rhel6-playbook-standard.yml                   rhel7-playbook-cui.yml                      rhel7-playbook-rht-ccp.yml
rhel6-playbook-default.yml         rhel6-playbook-stig.yml                       rhel7-playbook-default.yml                  rhel7-playbook-standard.yml
rhel6-playbook-desktop.yml         rhel6-playbook-usgcb-rhel6-server.yml         rhel7-playbook-e8.yml                       rhel7-playbook-stig.yml
```

Using Ansible to Achieve Compliance

```
[root@rocinante jswanson]# cat /usr/share/scap-security-guide/ansible/rhel8-playbook-pci-dss.yml | head -50
---
################################################################################
#
# Ansible Playbook for PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8
#
# Profile Description:
# Ensures PCI-DSS v3.2.1 security configuration settings are applied.
#
# Profile ID:  pci-dss
# Benchmark ID:  RHEL-8
# Benchmark Version:  0.1.48
# XCCDF Version:  1.1
#
# This file was generated by OpenSCAP 1.3.2 using:
# $ oscap xccdf generate fix --profile pci-dss --fix-type ansible xccdf-file.xml
#
# This Ansible Playbook is generated from an OpenSCAP profile without preliminary evaluation.
# It attempts to fix every selected rule, even if the system is already compliant.
#
# How to apply this Ansible Playbook:
# $ ansible-playbook -i "localhost," -c local playbook.yml
# $ ansible-playbook -i "192.168.1.155," playbook.yml
# $ ansible-playbook -i inventory.ini playbook.yml
#
################################################################################
```

Using Ansible to Achieve Compliance

msp-rhug-rhel-01.josh.lab.msp.redhat.com

Delete | View in Inventory

UUID: a1f480ef-494e-471d-9738-4f102c094ad2
Last seen: 08 Jun 2020 23:34 UTC

Australian Cyber Security Centre (ACSC) Essential Eight

Noncompliant
54 of 96 rules passed (73%)

Profile: xccdf_org.ssgproject.content_profile_e8
SSG version: 0.1.48

Last scanned: 3 minutes ago

Filter by Passed | Remediate | 42 results | 1 - 10 of 42

Passed | Hide passed rules | Clear filters

Rule	Policy	Severity	Passed	Ansible
Verify and Correct File Permissions with RPM CCE-80858-4	Australian Cyber Security Centre (ACSC) Essential Eight	High		
Set hostname as computer node name in audit logs CCE-82897-0	Australian Cyber Security Centre (ACSC) Essential Eight	Medium		

Using Ansible to Achieve Compliance

Australian Cyber Security Centre (ACSC) Essential Eight

Noncompliant

54 of 96 rules passed (73%)

Profile: xccdf_org.ssgproject.content_profile_e8
SSG version: 0.1.48

Last scanned: 4 minutes ago

Filter by Passed | Remediate | 42 results | 1 - 10 of 42

Passed | Hide passed rules | Clear filters

Rule	Policy	Severity	Passed	Ansible
Verify and Correct File Permissions with RPM CCE-80858-4	Australian Cyber Security Centre (ACSC) Essential Eight	High		
Set hostname as computer node name in audit logs CCE-82897-0	Australian Cyber Security Centre (ACSC) Essential Eight	Medium		
Restrict usage of ptrace to descendant processes CCE-80953-3	Australian Cyber Security Centre (ACSC) Essential Eight	Medium		

Using Ansible to Achieve Compliance

Remediate with Ansible

Do you want to modify an existing Playbook or create a new one?

- ○ Existing Playbook (4) — test789
- ◉ Create new Playbook — msp-rhug-compliance-playbook-1

Playbook name

Cancel | Next

Using Ansible to Achieve Compliance

Remediate with Ansible

Playbook name: msp-rhug-compliance-playbook-1

Action	Resolution	Reboot required	Systems	Type
Restrict usage of ptrace to descendant processes	Restrict usage of ptrace to descendant processes	✔	1	Compliance
Set hostname as computer node name in audit logs	Set hostname as computer node name in audit logs	✔	1	Compliance
Verify and Correct File Permissions with RPM	Verify and Correct File Permissions with RPM	✔	1	Compliance

System reboot is required

Auto reboot

Cancel Back Create

Using Ansible to Achieve Compliance

Remediations > msp-rhug-compliance-playbook-1

msp-rhug-compliance-playbook-1

Download playbook

Playbook summary

Total systems

1 system

Playbook settings

Auto reboot: **Enabled** 1 system requires reboot

Turn off auto reboot

Actions | Activity

Search actions | Remove action | 1 - 3 of 3 | 1 of 1

Actions	Resolution	Reboot required	Systems	Type
Restrict usage of ptrace to descendant processes	Restrict usage of ptrace to descendant processes	✔	1	Compliance
Set hostname as computer node name in audit logs	Set hostname as computer node name in audit logs	✔	1	Compliance
Verify and Correct File Permissions with RPM	Verify and Correct File Permissions with RPM	✔	1	Compliance

1 - 3 of 3 | 1 of 1

Red Hat

Using Ansible to Achieve Compliance

```
[jswanson@rocinante ~]$ cat msp-rhug-compliance-playbook-1-1591659597408.yml
---
# Red Hat Insights has recommended one or more actions for you, a system administrator, to review and if you
# deem appropriate, deploy on your systems running Red Hat software. Based on the analysis, we have automatically
# generated an Ansible Playbook for you. Please review and test the recommended actions and the Playbook as
# they may contain configuration changes, updates, reboots and/or other changes to your systems. Red Hat is not
# responsible for any adverse outcomes related to these recommendations or Playbooks.
#
# msp-rhug-compliance-playbook-1
# https://cloud.redhat.com/insights/remediations/3cf2994f-81cf-4d62-8905-e2cc4f5c133d
# Generated by Red Hat Insights on Mon, 08 Jun 2020 23:39:57 GMT
# Created by jswanson_customer

# Set hostname as computer node name in audit logs
# Identifier: (ssg:rhel7|content_profile_e8|xccdf_org.ssgproject.content_rule_auditd_name_format,fix)
# Version: 48db51056597f5613713a8068ac1b4e9bee869d8
- name: Set hostname as computer node name in audit logs
  hosts: 'msp-rhug-rhel-01.josh.lab.msp.redhat.com'
  become: true
  tags:
    - CCE-82359-1
    - auditd_name_format
    - low_complexity
    - low_disruption
    - medium_severity
    - no_reboot_needed
    - restrict_strategy
  tasks:
...
```

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat