Red Hat
Enterprise Linux

A Deep Dive into OpenSCAP

Marc Skinner
Principal Solutions Architect

Red Hat

Security and Compliance

KEY
HELP
PART
TESTED
UPDATED
METRICS
DEVICES
COVER
PRIVACY
PROVIDE
TRENDS
PENETRATION
PERFORM
REVIEWED
SPECIFIC
REGULATION
COMPANY
MALWARE
PHYSICAL
FRAMEWORK
DOCUMENTED
EVENT
ADDRESSED
CLIENT
SITE
CONTINUITY
APPLICATIONS
INCLUDE
RECORDS
PRACTICES
PROCESS
ACCESS
ENSURE
FOCUS
QUESTIONS
PREVIOUS
WRITTEN
FORMAL
SECURITY
PLACE
COMMENT
SOLUTIONS
RISK
SCOPE
INFORMATION
INDUSTRY
CURRENT
RESOURCES
FOLLOW
CORRECTED
MANAGEMENT
EXTERNAL
ORDER
COMPUTER
FAIR
BRIEFING
REQUIREMENTS
COMPLIANCE
RESULTS
GOVERNANCE
ACCEPTED
REPORT
SURVEY
GUIDE
RECOVERY
MEETING
EMPLOYEES
OPERATING
USUALLY
ASSETS
LOGS
NETWORK
PROBLEM
DEFICIENCIES
CHECK
BACKUP
AUDITED
BUSINESS
AGREED
FIREWALL
STAFF
INCIDENTS
DISASTER
PASSWORDS
VULNERABILITY
OPERATIONS
TOOLS
DATA
MANAGER
CHANGES
FINANCIAL
AUDIT
ORGANIZATION
ASSESSMENT
CONSISTENT
DISCOVERED
WEAKNESSES
MEASURE
GENERAL
TECHNICAL
SYSTEM
POLICY
GAIN
INTERNAL
ASKED
ACCOMPLISH
HISTORICAL
EXECUTIVE
DEFINED
MEASURABLE
DETERMINE
ANSWERS
REVIEW
SCANS
ACTIVITIES
CONTROLS
BEST
SUMMARY
COMPLETE
INSIGHT
EXAMINATION
EFFECTIVE
APPROPRIATE
PLAN
OVERALL
PROCEDURES
AUDITORS
ACCORDANCE
STANDARDS
ACTUALLY
DAILY
QUESTIONNAIRES
EXAMINE
OVERVIEW
FINDINGS
SETTINGS
IMPORTANT
OBJECTIVES
CONDUCT
ANALYSIS

What is IT Security?

The implementation of technical controls to protect company assets and data

- Configuring and running a host based firewall
- Using encryption protocols when connecting to a database
- Running anti-virus/malware agent on your desktop

CIA Triad: Confidentiality / Integrity / Accessibility

What is IT Compliance?

The art of aligning with a third party's regulatory guidance

- Industry Regulations : HIPAA
- Government Policies: FISMA
- Security Frameworks: CISA

*** Compliance is only finished when the third party is satisfied ***

Security and Compliance: Equally Critical

- Compliance helps build your security baseline
- Security enforces and maintains your compliance

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.

- It is a collection of data formats.

What is SCAP?

- SCAP components define standards in 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 Release 1.3 is current

What is SCAP?

- SCAP components:
  - **DataStream:** single file SCAP format
  - **CPE:** Common Platform Enumeration
  - **CVE:** Common Vulnerabilities and Exposures
  - **CWE:** Common Weakness Enumeration

- SCAP languages:
  - **OVAL:** Open Vulnerability and Assessment Language
  - **XCCDF:** Extensible Configuration Checklist Description Format
  - **ARF**: Asset Reporting Format

What is OpenSCAP?

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

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 to name just a few

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.

What is SCAP Security Guide?

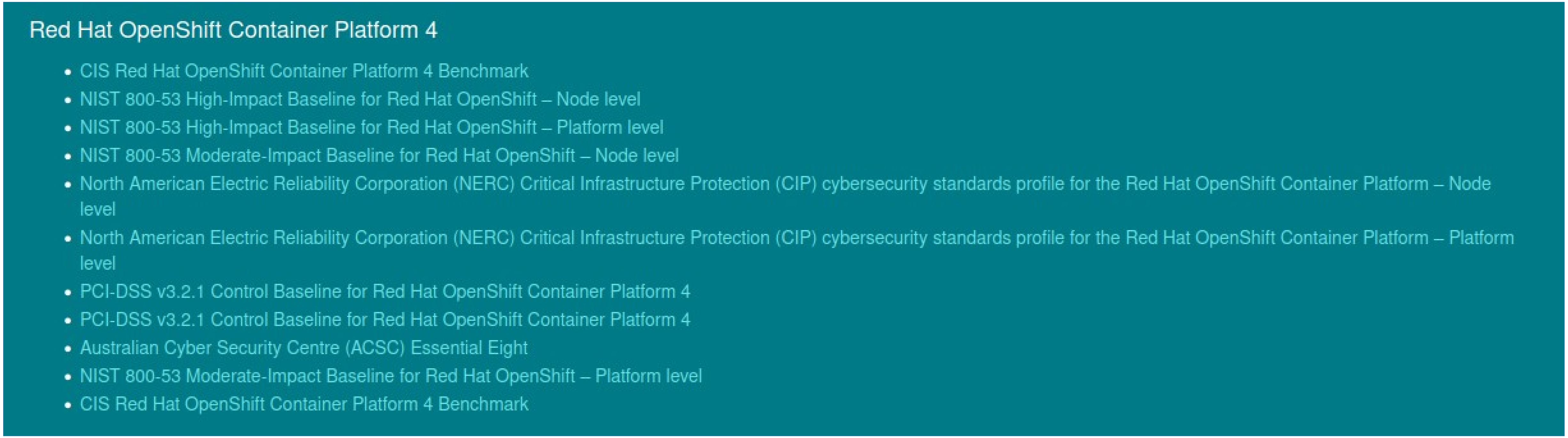
- The project provides practical security hardening advice for Red Hat products and also links it to compliance requirements in order to ease deployment activities, such as certification and accreditation.

- The project started in 2011 as open collaboration of U.S. Government bodies to develop next generation of **United States Government Baseline** (USGCB) available for Red Hat Enterprise Linux 6.

- Take policy requirements and present them as machine readable formats.

- Hosted on the open-scap.org website

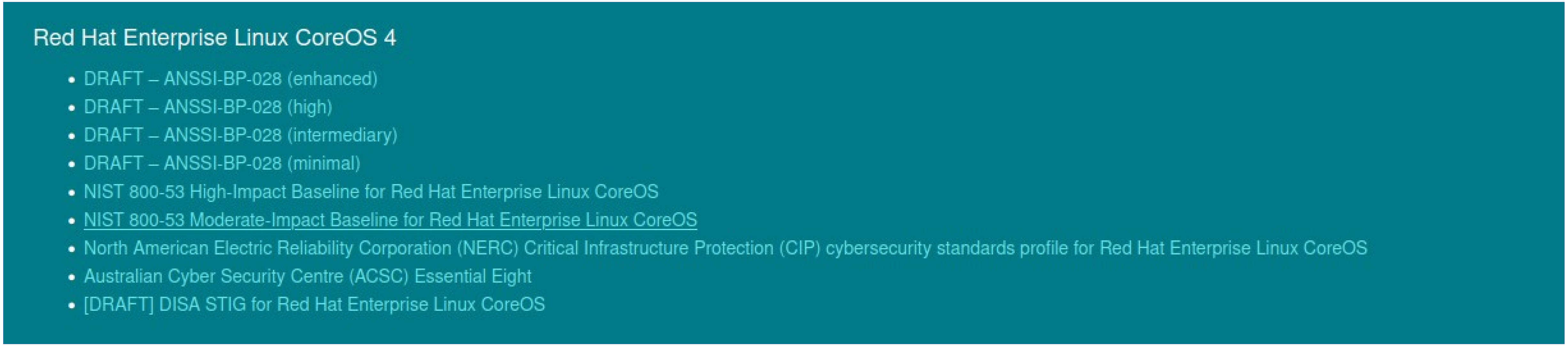
Choosing a Security Policy for Red Hat



Red Hat OpenShift Container Platform 4

- CIS Red Hat OpenShift Container Platform 4 Benchmark
- NIST 800-53 High-Impact Baseline for Red Hat OpenShift – Node level
- NIST 800-53 High-Impact Baseline for Red Hat OpenShift – Platform level
- NIST 800-53 Moderate-Impact Baseline for Red Hat OpenShift – Node level
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity standards profile for the Red Hat OpenShift Container Platform – Node level
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity standards profile for the Red Hat OpenShift Container Platform – Platform level
- PCI-DSS v3.2.1 Control Baseline for Red Hat OpenShift Container Platform 4
- PCI-DSS v3.2.1 Control Baseline for Red Hat OpenShift Container Platform 4
- Australian Cyber Security Centre (ACSC) Essential Eight
- NIST 800-53 Moderate-Impact Baseline for Red Hat OpenShift – Platform level
- CIS Red Hat OpenShift Container Platform 4 Benchmark

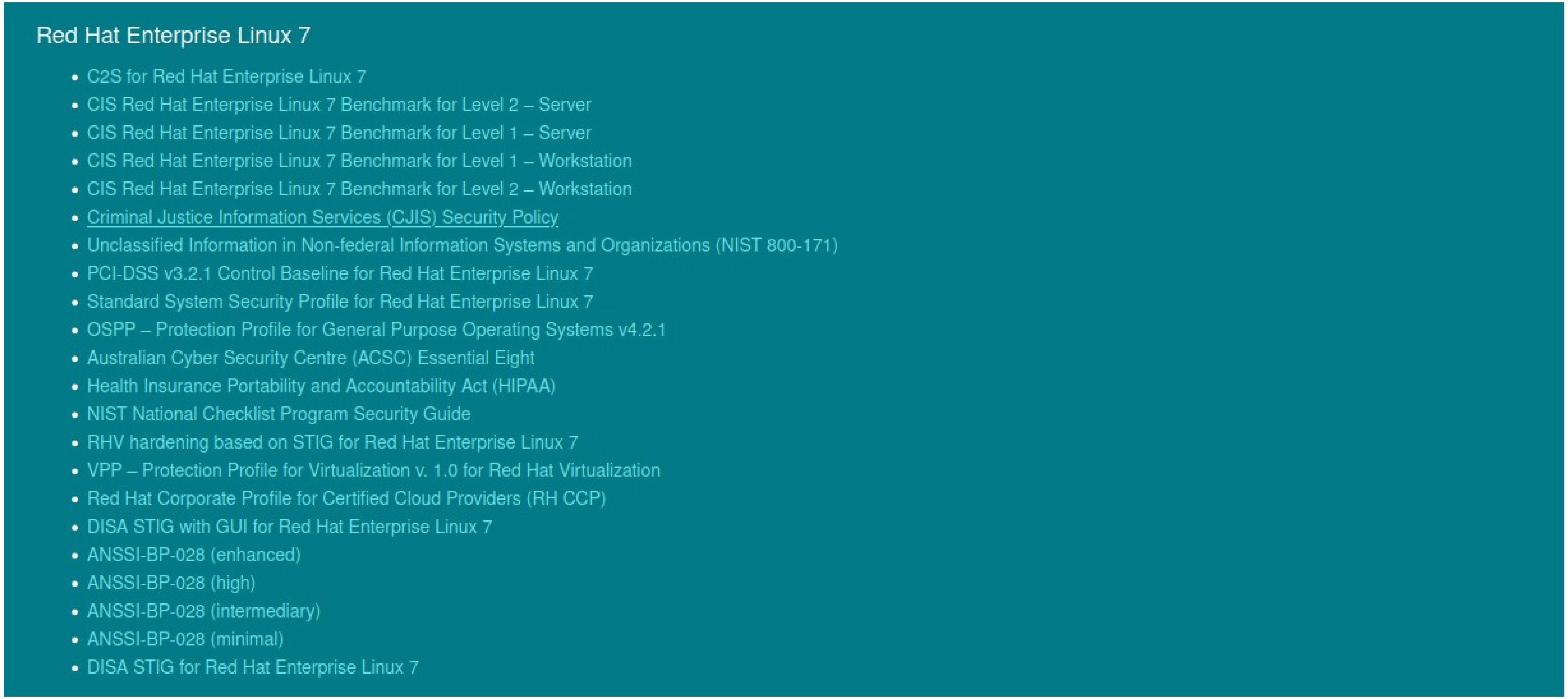
Choosing a Security Policy for Red Hat



Red Hat Enterprise Linux CoreOS 4

- DRAFT – ANSSI-BP-028 (enhanced)
- DRAFT – ANSSI-BP-028 (high)
- DRAFT – ANSSI-BP-028 (intermediary)
- DRAFT – ANSSI-BP-028 (minimal)
- NIST 800-53 High-Impact Baseline for Red Hat Enterprise Linux CoreOS
- NIST 800-53 Moderate-Impact Baseline for Red Hat Enterprise Linux CoreOS
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity standards profile for Red Hat Enterprise Linux CoreOS
- Australian Cyber Security Centre (ACSC) Essential Eight
- [DRAFT] DISA STIG for Red Hat Enterprise Linux CoreOS

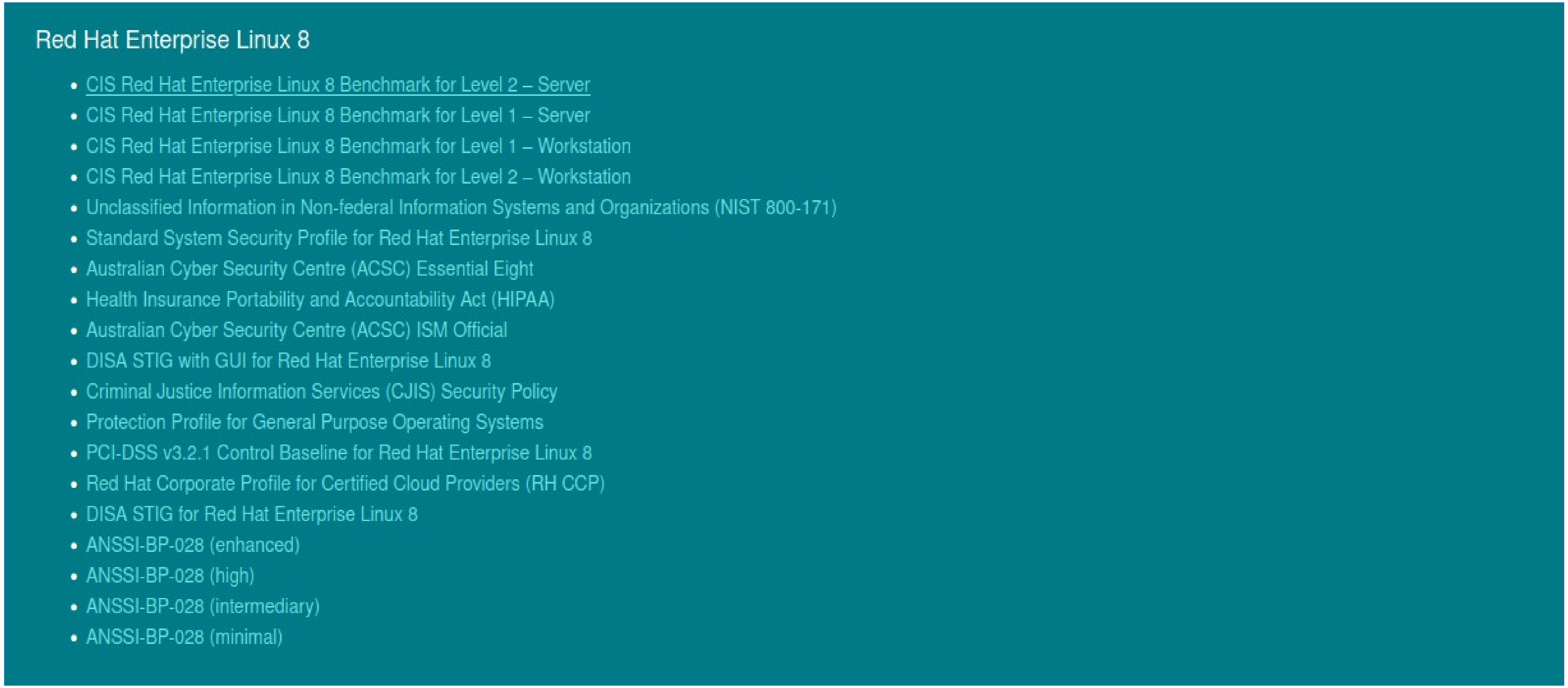
Choosing a Security Policy for Red Hat



Red Hat Enterprise Linux 7

- C2S for Red Hat Enterprise Linux 7
- CIS Red Hat Enterprise Linux 7 Benchmark for Level 2 – Server
- CIS Red Hat Enterprise Linux 7 Benchmark for Level 1 – Server
- CIS Red Hat Enterprise Linux 7 Benchmark for Level 1 – Workstation
- CIS Red Hat Enterprise Linux 7 Benchmark for Level 2 – Workstation
- Criminal Justice Information Services (CJIS) Security Policy
- Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
- PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 7
- Standard System Security Profile for Red Hat Enterprise Linux 7
- OSPP – Protection Profile for General Purpose Operating Systems v4.2.1
- Australian Cyber Security Centre (ACSC) Essential Eight
- Health Insurance Portability and Accountability Act (HIPAA)
- NIST National Checklist Program Security Guide
- RHV hardening based on STIG for Red Hat Enterprise Linux 7
- VPP – Protection Profile for Virtualization v. 1.0 for Red Hat Virtualization
- Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
- DISA STIG with GUI for Red Hat Enterprise Linux 7
- ANSSI-BP-028 (enhanced)
- ANSSI-BP-028 (high)
- ANSSI-BP-028 (intermediary)
- ANSSI-BP-028 (minimal)
- DISA STIG for Red Hat Enterprise Linux 7

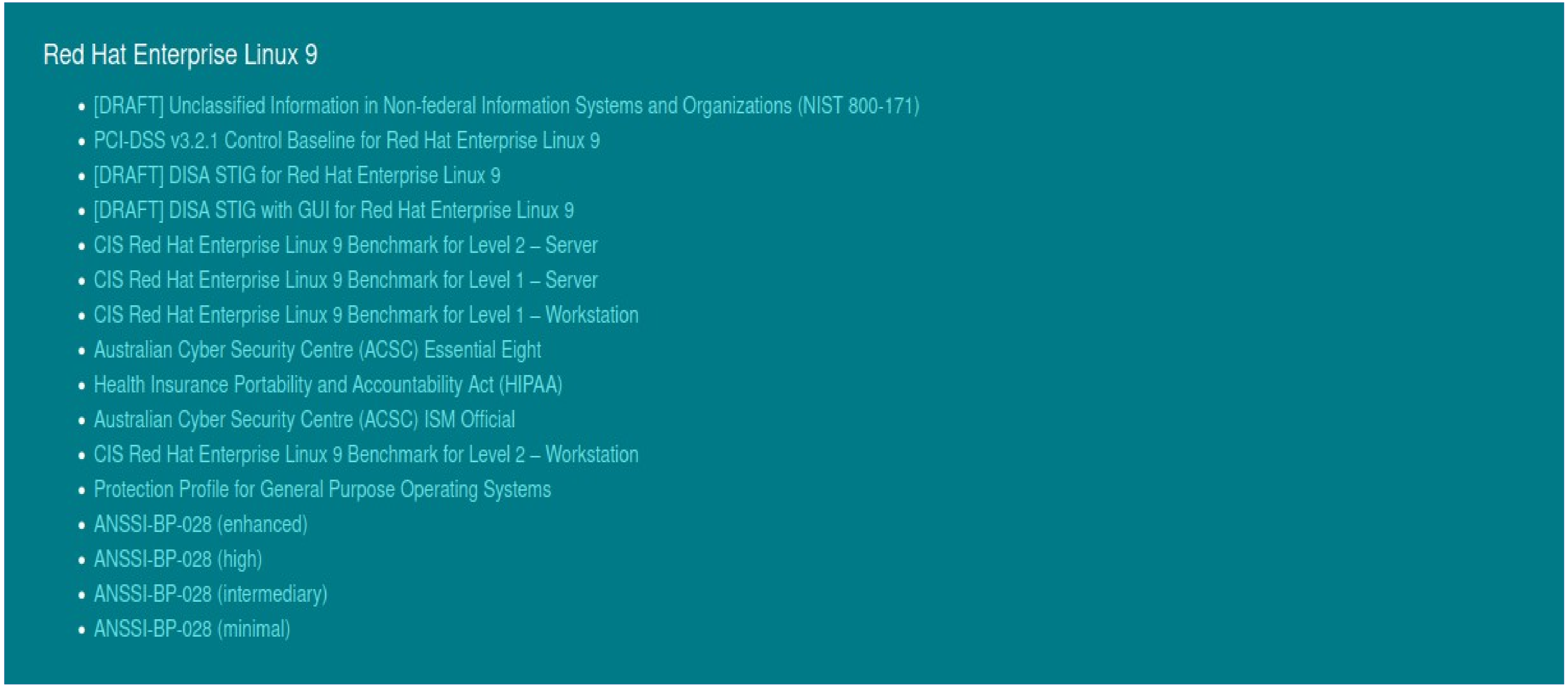
Choosing a Security Policy for Red Hat



Red Hat Enterprise Linux 8

- CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 – Server
- CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 – Server
- CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 – Workstation
- CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 – Workstation
- Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
- Standard System Security Profile for Red Hat Enterprise Linux 8
- Australian Cyber Security Centre (ACSC) Essential Eight
- Health Insurance Portability and Accountability Act (HIPAA)
- Australian Cyber Security Centre (ACSC) ISM Official
- DISA STIG with GUI for Red Hat Enterprise Linux 8
- Criminal Justice Information Services (CJIS) Security Policy
- Protection Profile for General Purpose Operating Systems
- PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8
- Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
- DISA STIG for Red Hat Enterprise Linux 8
- ANSSI-BP-028 (enhanced)
- ANSSI-BP-028 (high)
- ANSSI-BP-028 (intermediary)
- ANSSI-BP-028 (minimal)

Choosing a Security Policy for Red Hat



Red Hat Enterprise Linux 9

- [DRAFT] Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
- PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9
- [DRAFT] DISA STIG for Red Hat Enterprise Linux 9
- [DRAFT] DISA STIG with GUI for Red Hat Enterprise Linux 9
- CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 – Server
- CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 – Server
- CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 – Workstation
- Australian Cyber Security Centre (ACSC) Essential Eight
- Health Insurance Portability and Accountability Act (HIPAA)
- Australian Cyber Security Centre (ACSC) ISM Official
- CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 – Workstation
- Protection Profile for General Purpose Operating Systems
- ANSSI-BP-028 (enhanced)
- ANSSI-BP-028 (high)
- ANSSI-BP-028 (intermediary)
- ANSSI-BP-028 (minimal)

OpenSCAP on the command line

Installation

Requirements

- Security Policy files (scap-security-guide)
- OpenScap Scanner (oscap)

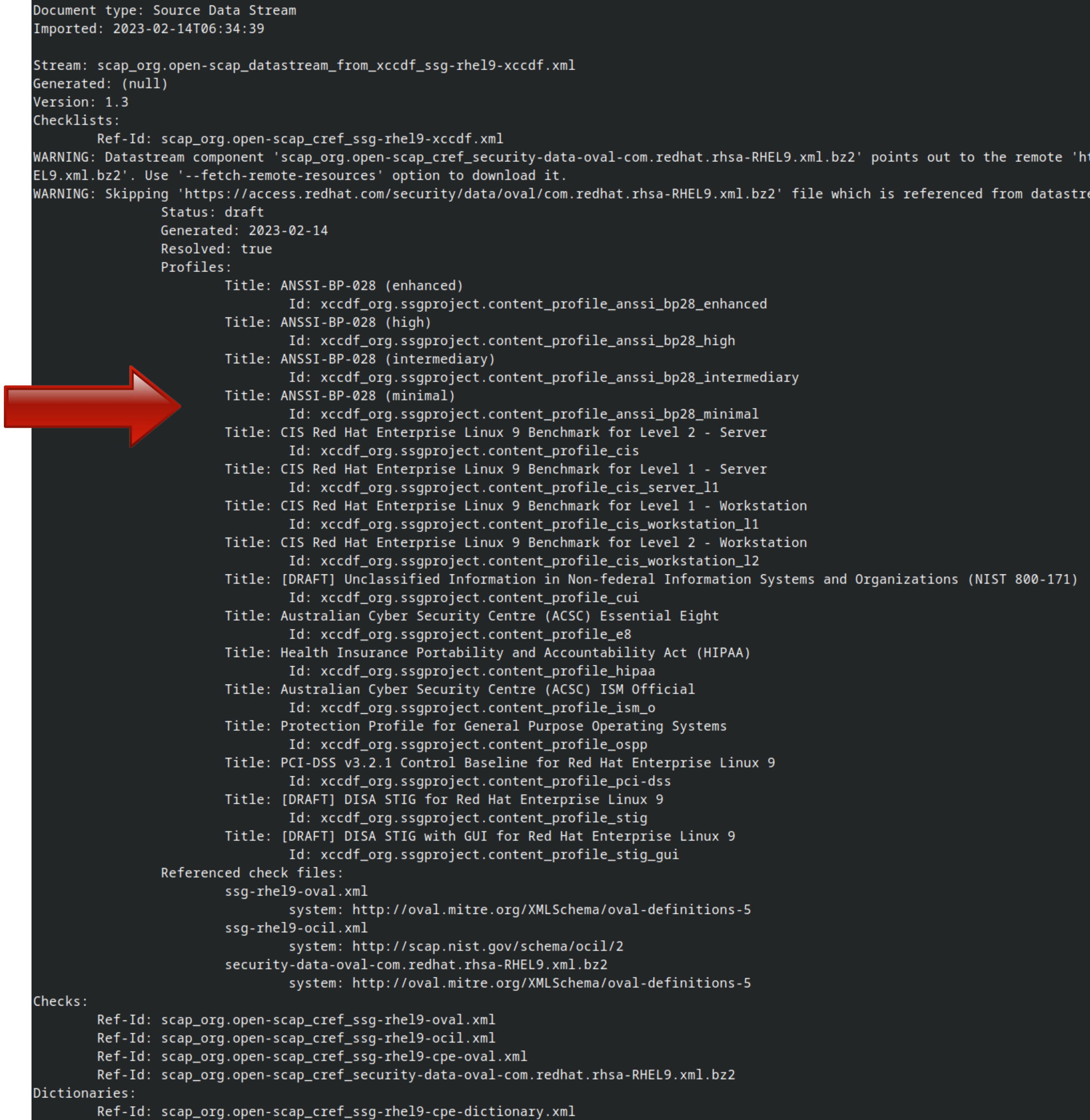
```
# dnf -y install scap-security-guide
```

- Installs the RHEL security policy: /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml
- Installs RHEL Kickstart examples: /usr/share/scap-security-guide/kickstart
- Installs Ansible Remediation playbooks: /usr/share/scap-security-guide/ansible
- Installs the openscap-scanner package: oscap

What Policy do we want to use?

View our options:

```
# cd /usr/share/xml/scap/ssg/content
# oscap info ssg-rhel9-ds.xml
```

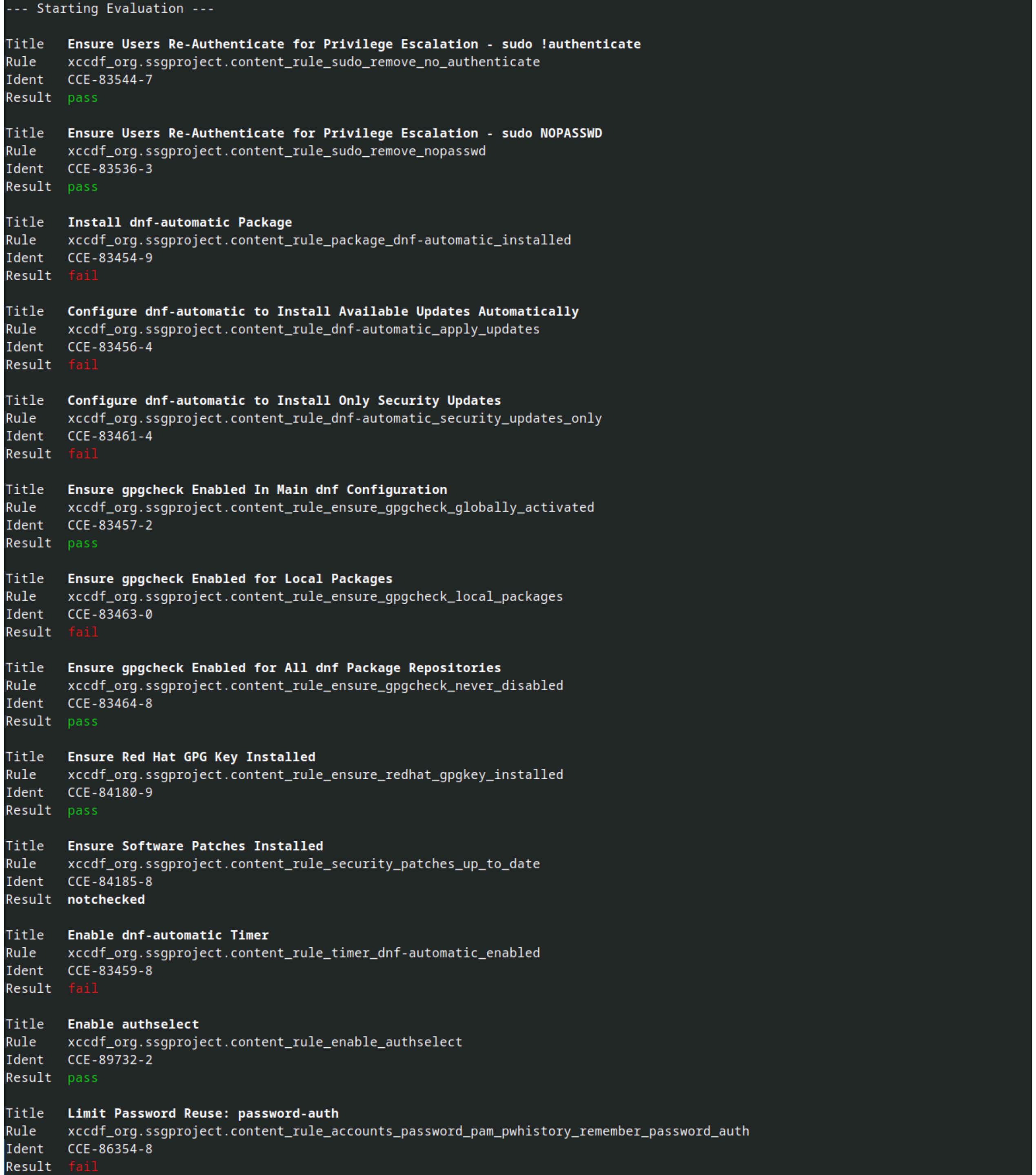


```
Document type: Source Data Stream
Imported: 2023-02-14T06:34:39

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel9-xccdf.xml
Generated: (null)
Version: 1.3
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel9-xccdf.xml
WARNING: Datastream component 'scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-RHEL9.xml.bz2' points out to the remote 'ht
EL9.xml.bz2'. Use '--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL9.xml.bz2' file which is referenced from datastre
                Status: draft
                Generated: 2023-02-14
                Resolved: true
                Profiles:
                        Title: ANSSI-BP-028 (enhanced)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced
                        Title: ANSSI-BP-028 (high)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_high
                        Title: ANSSI-BP-028 (intermediary)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary
                        Title: ANSSI-BP-028 (minimal)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Server
                                Id: xccdf_org.ssgproject.content_profile_cis
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 - Server
                                Id: xccdf_org.ssgproject.content_profile_cis_server_l1
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 - Workstation
                                Id: xccdf_org.ssgproject.content_profile_cis_workstation_l1
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Workstation
                                Id: xccdf_org.ssgproject.content_profile_cis_workstation_l2
                        Title: [DRAFT] Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
                                Id: xccdf_org.ssgproject.content_profile_cui
                        Title: Australian Cyber Security Centre (ACSC) Essential Eight
                                Id: xccdf_org.ssgproject.content_profile_e8
                        Title: Health Insurance Portability and Accountability Act (HIPAA)
                                Id: xccdf_org.ssgproject.content_profile_hipaa
                        Title: Australian Cyber Security Centre (ACSC) ISM Official
                                Id: xccdf_org.ssgproject.content_profile_ism_o
                        Title: Protection Profile for General Purpose Operating Systems
                                Id: xccdf_org.ssgproject.content_profile_ospp
                        Title: PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9
                                Id: xccdf_org.ssgproject.content_profile_pci-dss
                        Title: [DRAFT] DISA STIG for Red Hat Enterprise Linux 9
                                Id: xccdf_org.ssgproject.content_profile_stig
                        Title: [DRAFT] DISA STIG with GUI for Red Hat Enterprise Linux 9
                                Id: xccdf_org.ssgproject.content_profile_stig_gui
                Referenced check files:
                        ssg-rhel9-oval.xml
                                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
                        ssg-rhel9-ocil.xml
                                system: http://scap.nist.gov/schema/ocil/2
                        security-data-oval-com.redhat.rhsa-RHEL9.xml.bz2
                                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
Checks:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel9-oval.xml
        Ref-Id: scap_org.open-scap_cref_ssg-rhel9-ocil.xml
        Ref-Id: scap_org.open-scap_cref_ssg-rhel9-cpe-oval.xml
        Ref-Id: scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-RHEL9.xml.bz2
Dictionaries:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel9-cpe-dictionary.xml
```

Run OpenScap Scan

Run and save html report

# cd /usr/share/xml/scap/ssg/content
# oscap xccdf eval --profile **xccdf_org.ssgproject.content_profile_anssi_bp28_minimal** --report /root/report.html ssg-rhel9-ds.xml

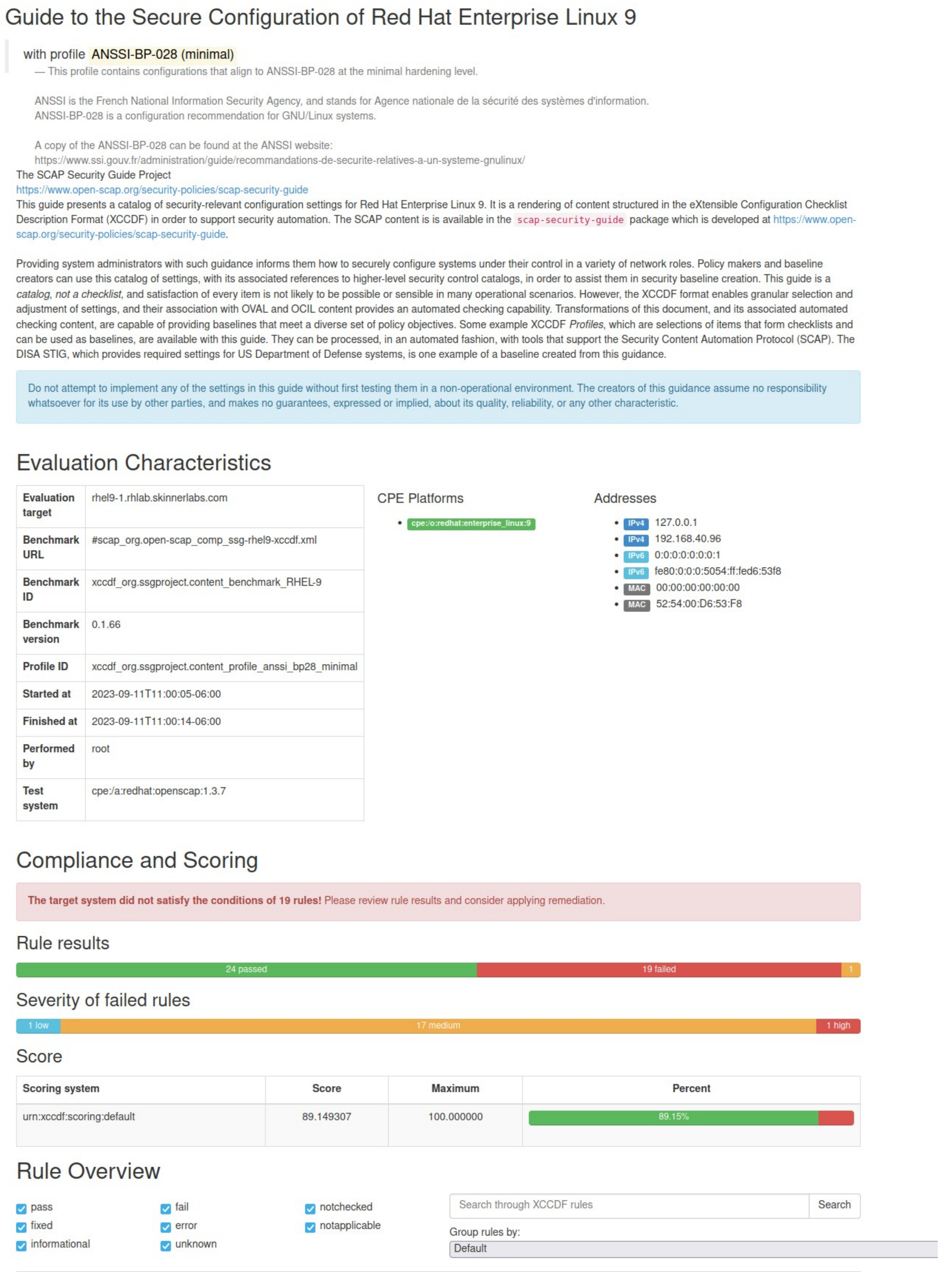


```
--- Starting Evaluation ---

Title   Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate
Rule    xccdf_org.ssgproject.content_rule_sudo_remove_no_authenticate
Ident   CCE-83544-7
Result  pass

Title   Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD
Rule    xccdf_org.ssgproject.content_rule_sudo_remove_nopasswd
Ident   CCE-83536-3
Result  pass

Title   Install dnf-automatic Package
Rule    xccdf_org.ssgproject.content_rule_package_dnf-automatic_installed
Ident   CCE-83454-9
Result  fail

Title   Configure dnf-automatic to Install Available Updates Automatically
Rule    xccdf_org.ssgproject.content_rule_dnf-automatic_apply_updates
Ident   CCE-83456-4
Result  fail

Title   Configure dnf-automatic to Install Only Security Updates
Rule    xccdf_org.ssgproject.content_rule_dnf-automatic_security_updates_only
Ident   CCE-83461-4
Result  fail

Title   Ensure gpgcheck Enabled In Main dnf Configuration
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_activated
Ident   CCE-83457-2
Result  pass

Title   Ensure gpgcheck Enabled for Local Packages
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_local_packages
Ident   CCE-83463-0
Result  fail

Title   Ensure gpgcheck Enabled for All dnf Package Repositories
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disabled
Ident   CCE-83464-8
Result  pass

Title   Ensure Red Hat GPG Key Installed
Rule    xccdf_org.ssgproject.content_rule_ensure_redhat_gpgkey_installed
Ident   CCE-84180-9
Result  pass

Title   Ensure Software Patches Installed
Rule    xccdf_org.ssgproject.content_rule_security_patches_up_to_date
Ident   CCE-84185-8
Result  notchecked

Title   Enable dnf-automatic Timer
Rule    xccdf_org.ssgproject.content_rule_timer_dnf-automatic_enabled
Ident   CCE-83459-8
Result  fail

Title   Enable authselect
Rule    xccdf_org.ssgproject.content_rule_enable_authselect
Ident   CCE-89732-2
Result  pass

Title   Limit Password Reuse: password-auth
Rule    xccdf_org.ssgproject.content_rule_accounts_password_pam_pwhistory_remember_password_auth
Ident   CCE-86354-8
Result  fail
```

View OpenScap Report

- Open report.html in browser

- Show report rule sorting
- Show remediation of rule failure



Guide to the Secure Configuration of Red Hat Enterprise Linux 9

> with profile ANSSI-BP-028 (minimal)
>
> — This profile contains configurations that align to ANSSI-BP-028 at the minimal hardening level.
>
> ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information.
> ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.
>
> A copy of the ANSSI-BP-028 can be found at the ANSSI website:
> https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 9. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Evaluation target	rhel9-1.rhlab.skinnerlabs.com
Benchmark URL	#scap_org.open-scap_comp_ssg-rhel9-xccdf.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-9
Benchmark version	0.1.66
Profile ID	xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
Started at	2023-09-11T11:00:05-06:00
Finished at	2023-09-11T11:00:14-06:00
Performed by	root
Test system	cpe:/a:redhat:openscap:1.3.7

CPE Platforms

- cpe:/o:redhat:enterprise_linux:9

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.40.96
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:5054:ff:fed6:53f8
- MAC 00:00:00:00:00:00
- MAC 52:54:00:D6:53:F8

Compliance and Scoring

The target system did not satisfy the conditions of 19 rules! Please review rule results and consider applying remediation.

Rule results

24 passed 19 failed 1

Severity of failed rules

1 low 17 medium 1 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	89.149307	100.000000	89.15%

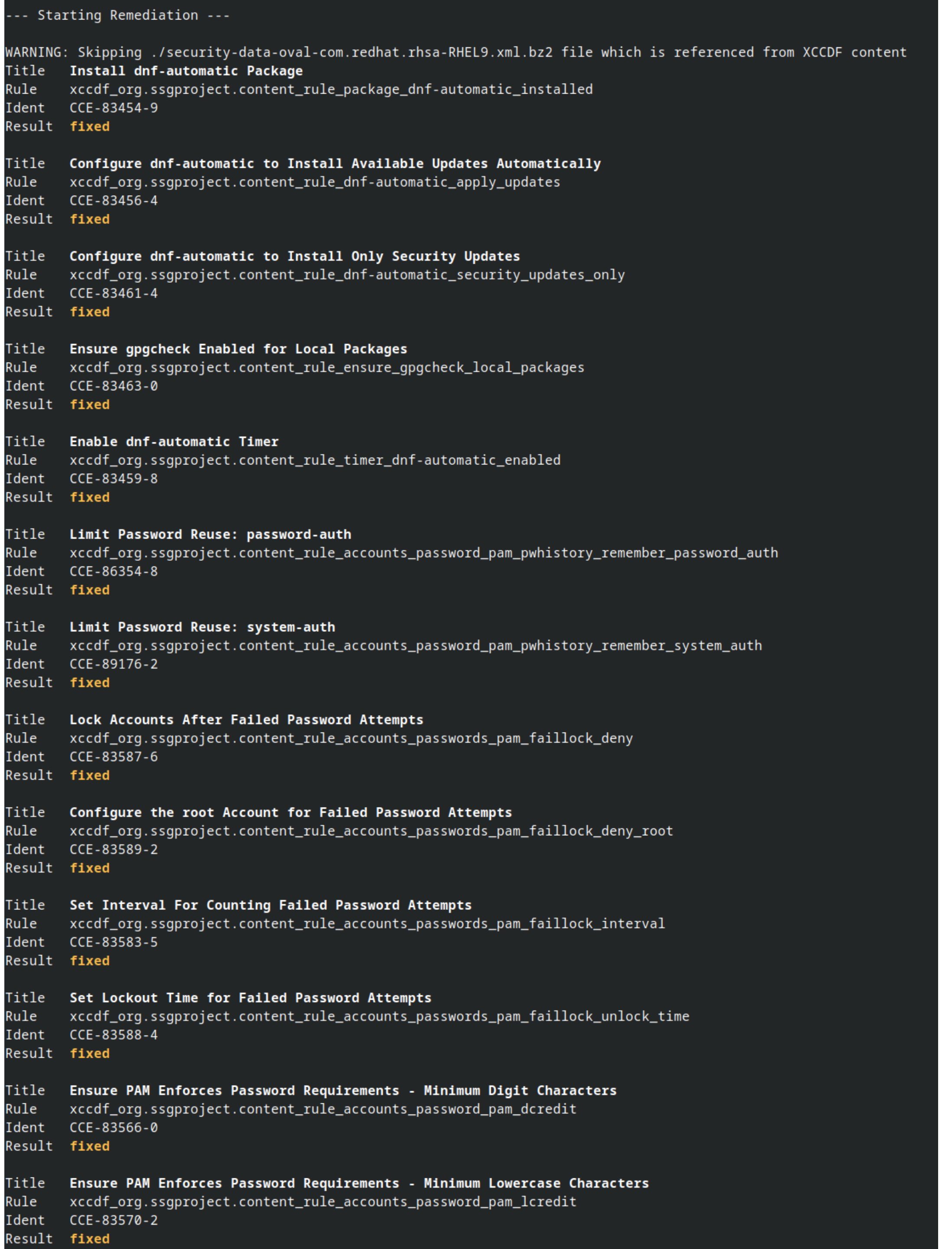
Rule Overview

☑ pass
☑ fixed
☑ informational
☑ fail
☑ error
☑ unknown
☑ notchecked
☑ notapplicable

Remediate OpenScap Scan

Run remediation

```
# cd /usr/share/xml/scap/ssg/content
# oscap xccdf eval --profile
```
xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
```
--remediate ssg-rhel9-ds.xml
```



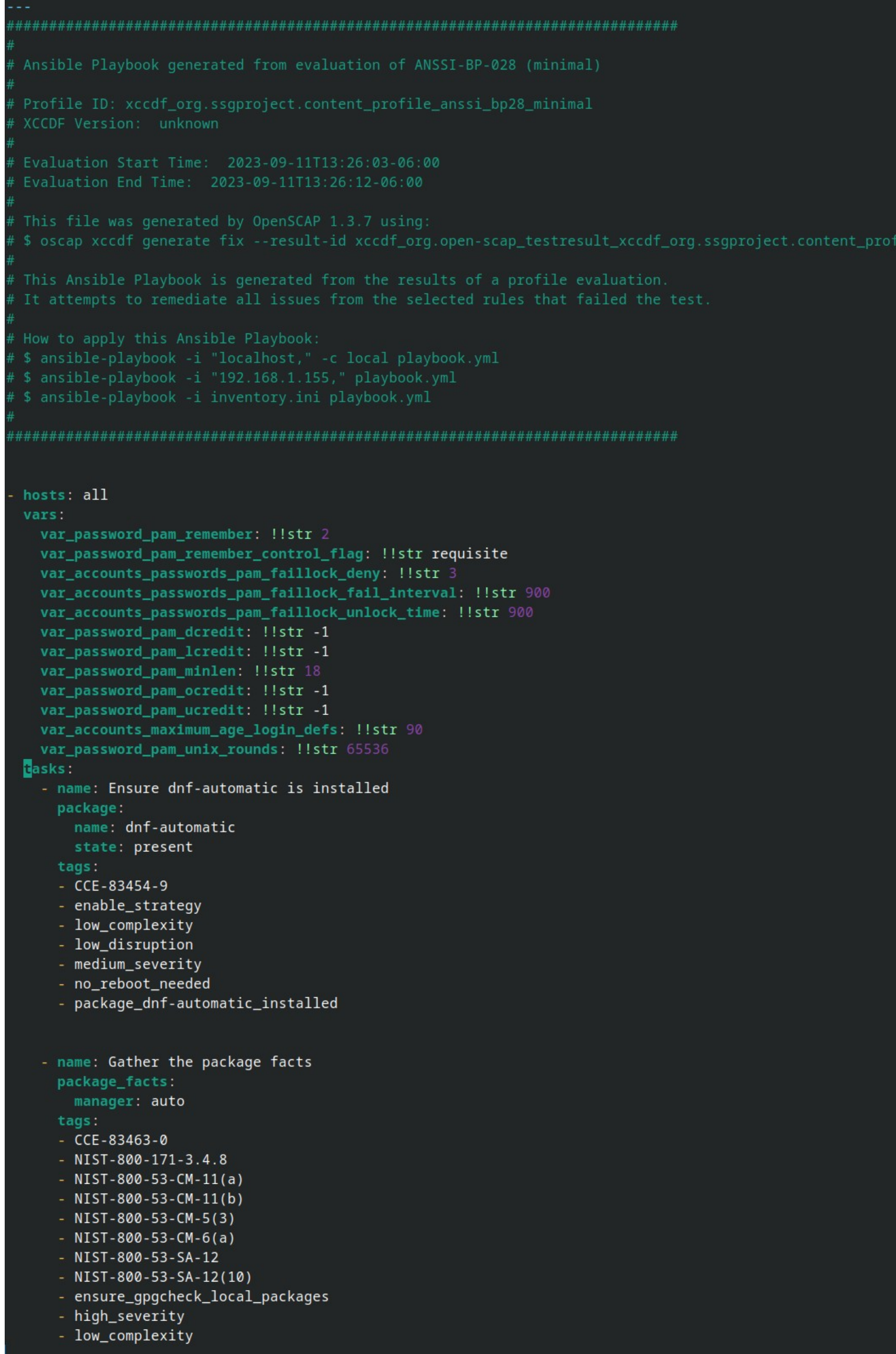
```
--- Starting Remediation ---

WARNING: Skipping ./security-data-oval-com.redhat.rhsa-RHEL9.xml.bz2 file which is referenced from XCCDF content
Title   Install dnf-automatic Package
Rule    xccdf_org.ssgproject.content_rule_package_dnf-automatic_installed
Ident   CCE-83454-9
Result  fixed

Title   Configure dnf-automatic to Install Available Updates Automatically
Rule    xccdf_org.ssgproject.content_rule_dnf-automatic_apply_updates
Ident   CCE-83456-4
Result  fixed

Title   Configure dnf-automatic to Install Only Security Updates
Rule    xccdf_org.ssgproject.content_rule_dnf-automatic_security_updates_only
Ident   CCE-83461-4
Result  fixed

Title   Ensure gpgcheck Enabled for Local Packages
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_local_packages
Ident   CCE-83463-0
Result  fixed

Title   Enable dnf-automatic Timer
Rule    xccdf_org.ssgproject.content_rule_timer_dnf-automatic_enabled
Ident   CCE-83459-8
Result  fixed

Title   Limit Password Reuse: password-auth
Rule    xccdf_org.ssgproject.content_rule_accounts_password_pam_pwhistory_remember_password_auth
Ident   CCE-86354-8
Result  fixed

Title   Limit Password Reuse: system-auth
Rule    xccdf_org.ssgproject.content_rule_accounts_password_pam_pwhistory_remember_system_auth
Ident   CCE-89176-2
Result  fixed

Title   Lock Accounts After Failed Password Attempts
Rule    xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_deny
Ident   CCE-83587-6
Result  fixed

Title   Configure the root Account for Failed Password Attempts
Rule    xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_deny_root
Ident   CCE-83589-2
Result  fixed

Title   Set Interval For Counting Failed Password Attempts
Rule    xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_interval
Ident   CCE-83583-5
Result  fixed

Title   Set Lockout Time for Failed Password Attempts
Rule    xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_unlock_time
Ident   CCE-83588-4
Result  fixed

Title   Ensure PAM Enforces Password Requirements - Minimum Digit Characters
Rule    xccdf_org.ssgproject.content_rule_accounts_password_pam_dcredit
Ident   CCE-83566-0
Result  fixed

Title   Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters
Rule    xccdf_org.ssgproject.content_rule_accounts_password_pam_lcredit
Ident   CCE-83570-2
Result  fixed
```

Generate Ansible Remediation Playbook

Run Scan
# cd /usr/share/xml/scap/ssg/content
# oscap xccdf eval --profile **xccdf_org.ssgproject.content_profile_anssi_bp28_minimal** --results /root/scan-results.xml ssg-rhel9-ds.xml

Get Result ID
# oscap info /root/scan-results.xml | grep "Result ID"
xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_anssi_bp28_minimal

Generate Ansible Playbook
#oscap xccdf generate fix --fix-type ansible --result-id **xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_anssi_bp28_minimal** --output /root/ansible-remediate.yml /root/scan-results.xml



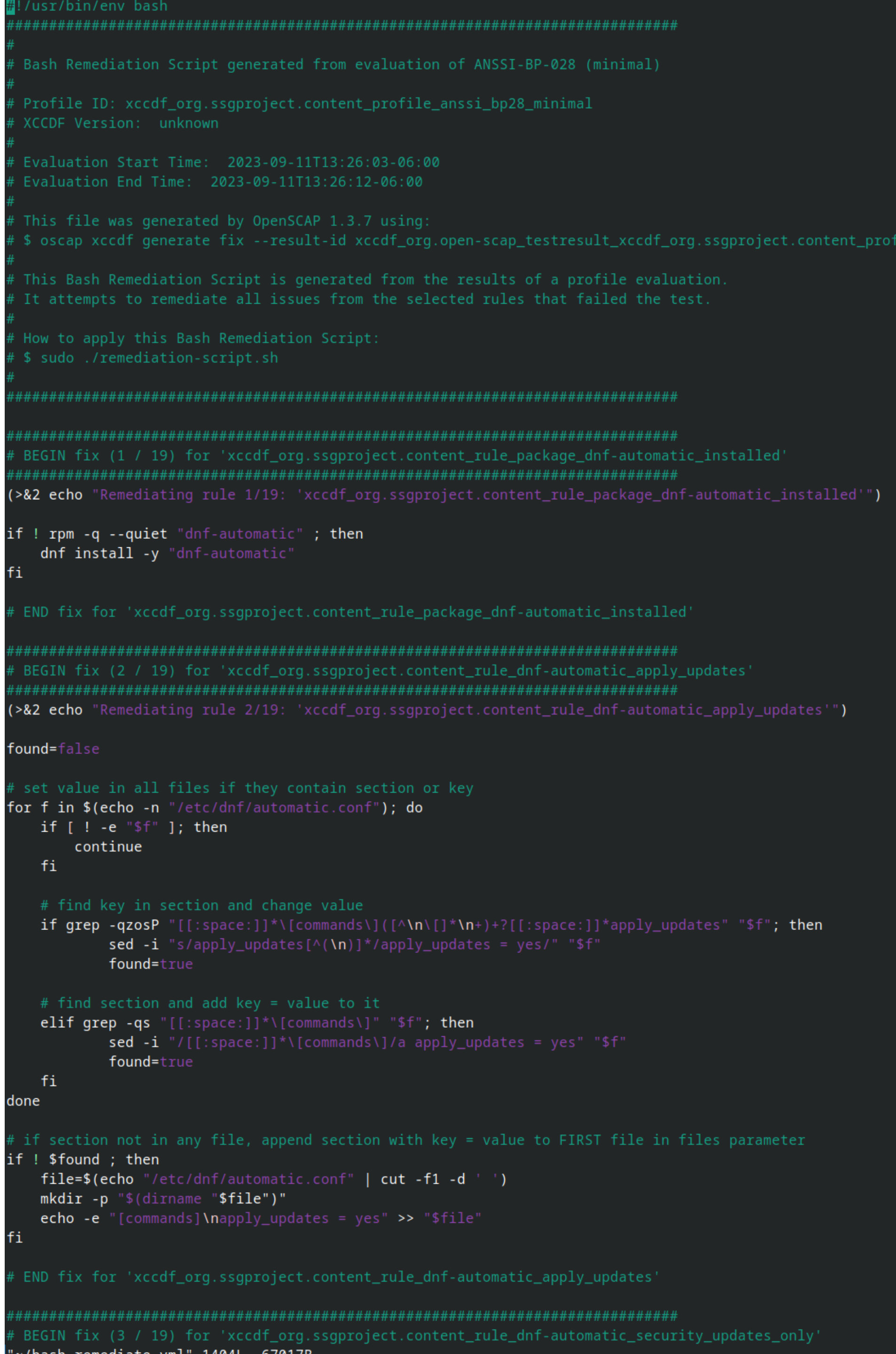
```
---
###############################################################################
#
# Ansible Playbook generated from evaluation of ANSSI-BP-028 (minimal)
#
# Profile ID: xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
# XCCDF Version:  unknown
#
# Evaluation Start Time:  2023-09-11T13:26:03-06:00
# Evaluation End Time:  2023-09-11T13:26:12-06:00
#
# This file was generated by OpenSCAP 1.3.7 using:
# $ oscap xccdf generate fix --result-id xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_prof
#
# This Ansible Playbook is generated from the results of a profile evaluation.
# It attempts to remediate all issues from the selected rules that failed the test.
#
# 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
#
###############################################################################


- hosts: all
  vars:
    var_password_pam_remember: !!str 2
    var_password_pam_remember_control_flag: !!str requisite
    var_accounts_passwords_pam_faillock_deny: !!str 3
    var_accounts_passwords_pam_faillock_fail_interval: !!str 900
    var_accounts_passwords_pam_faillock_unlock_time: !!str 900
    var_password_pam_dcredit: !!str -1
    var_password_pam_lcredit: !!str -1
    var_password_pam_minlen: !!str 18
    var_password_pam_ocredit: !!str -1
    var_password_pam_ucredit: !!str -1
    var_accounts_maximum_age_login_defs: !!str 90
    var_password_pam_unix_rounds: !!str 65536
  tasks:
    - name: Ensure dnf-automatic is installed
      package:
        name: dnf-automatic
        state: present
      tags:
      - CCE-83454-9
      - enable_strategy
      - low_complexity
      - low_disruption
      - medium_severity
      - no_reboot_needed
      - package_dnf-automatic_installed


    - name: Gather the package facts
      package_facts:
        manager: auto
      tags:
      - CCE-83463-0
      - NIST-800-171-3.4.8
      - NIST-800-53-CM-11(a)
      - NIST-800-53-CM-11(b)
      - NIST-800-53-CM-5(3)
      - NIST-800-53-CM-6(a)
      - NIST-800-53-SA-12
      - NIST-800-53-SA-12(10)
      - ensure_gpgcheck_local_packages
      - high_severity
      - low_complexity
```

Generate BASH Remediation Playbook

Run Scan
# cd /usr/share/xml/scap/ssg/content
# oscap xccdf eval --profile **xccdf_org.ssgproject.content_profile_anssi_bp28_minimal** --results /root/scan-results.xml ssg-rhel9-ds.xml

Get Result ID
# oscap info /root/scan-results.xml | grep "Result ID"
xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_anssi_bp28_minimal

Generate BASH Playbook
#oscap xccdf generate fix --fix-type bash --result-id **xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_anssi_bp28_minimal** --output /root/bash-remediate.sh /root/scan-results.xml



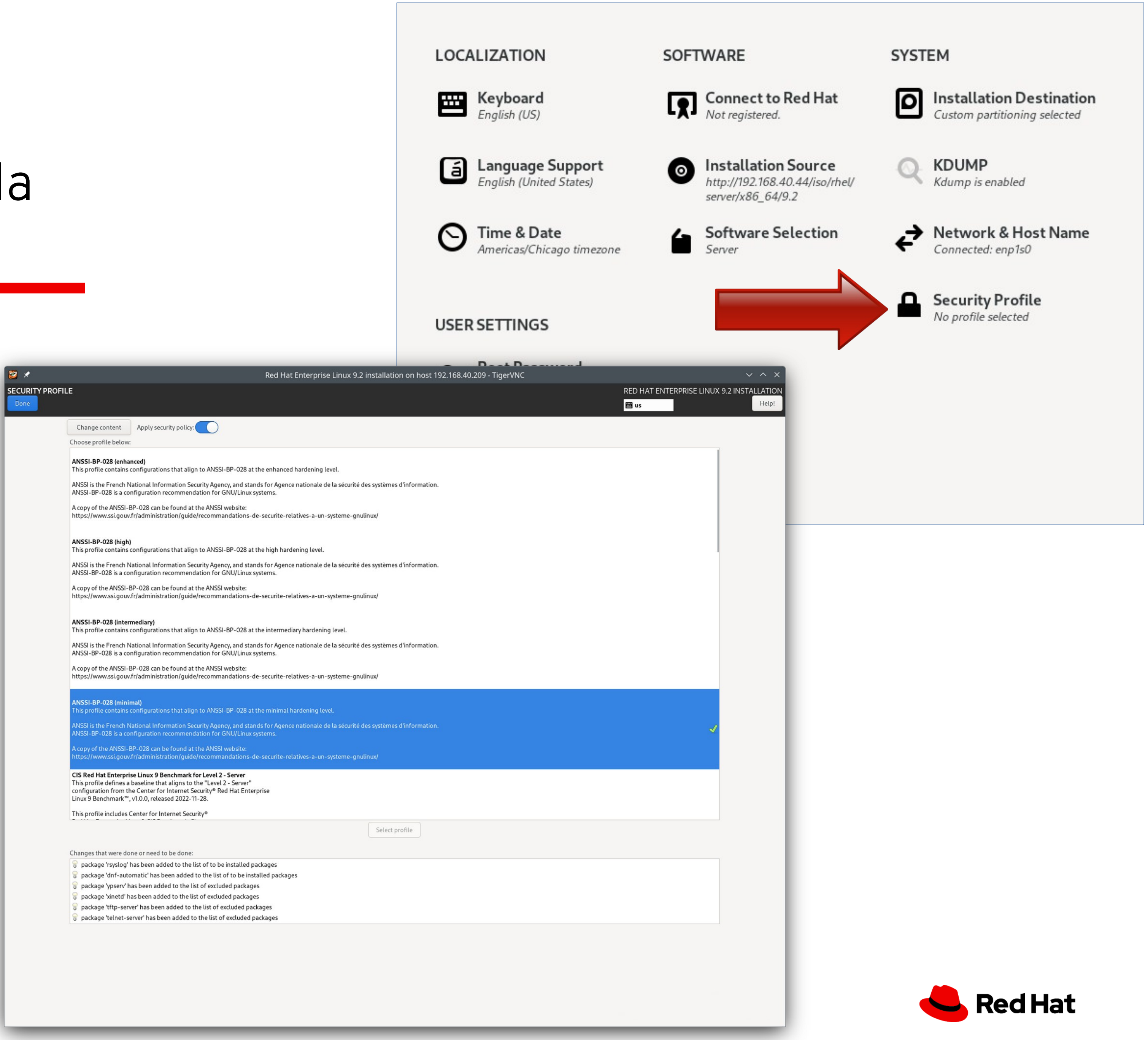
```
#!/usr/bin/env bash
###############################################################################
#
# Bash Remediation Script generated from evaluation of ANSSI-BP-028 (minimal)
#
# Profile ID: xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
# XCCDF Version:  unknown
#
# Evaluation Start Time:  2023-09-11T13:26:03-06:00
# Evaluation End Time:  2023-09-11T13:26:12-06:00
#
# This file was generated by OpenSCAP 1.3.7 using:
# $ oscap xccdf generate fix --result-id xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_prof
#
# This Bash Remediation Script is generated from the results of a profile evaluation.
# It attempts to remediate all issues from the selected rules that failed the test.
#
# How to apply this Bash Remediation Script:
# $ sudo ./remediation-script.sh
#
###############################################################################

###############################################################################
# BEGIN fix (1 / 19) for 'xccdf_org.ssgproject.content_rule_package_dnf-automatic_installed'
###############################################################################
(>&2 echo "Remediating rule 1/19: 'xccdf_org.ssgproject.content_rule_package_dnf-automatic_installed'")

if ! rpm -q --quiet "dnf-automatic" ; then
    dnf install -y "dnf-automatic"
fi

# END fix for 'xccdf_org.ssgproject.content_rule_package_dnf-automatic_installed'

###############################################################################
# BEGIN fix (2 / 19) for 'xccdf_org.ssgproject.content_rule_dnf-automatic_apply_updates'
###############################################################################
(>&2 echo "Remediating rule 2/19: 'xccdf_org.ssgproject.content_rule_dnf-automatic_apply_updates'")

found=false

# set value in all files if they contain section or key
for f in $(echo -n "/etc/dnf/automatic.conf"); do
    if [ ! -e "$f" ]; then
        continue
    fi

    # find key in section and change value
    if grep -qzosP "[[:space:]]*\[commands\]([^\n\[]*\n+)+?[[:space:]]*apply_updates" "$f"; then
            sed -i "s/apply_updates[^(\n)]*/apply_updates = yes/" "$f"
            found=true

    # find section and add key = value to it
    elif grep -qs "[[:space:]]*\[commands\]" "$f"; then
            sed -i "/[[:space:]]*\[commands\]/a apply_updates = yes" "$f"
            found=true
    fi
done

# if section not in any file, append section with key = value to FIRST file in files parameter
if ! $found ; then
    file=$(echo "/etc/dnf/automatic.conf" | cut -f1 -d ' ')
    mkdir -p "$(dirname "$file")"
    echo -e "[commands]\napply_updates = yes" >> "$file"
fi

# END fix for 'xccdf_org.ssgproject.content_rule_dnf-automatic_apply_updates'

###############################################################################
# BEGIN fix (3 / 19) for 'xccdf_org.ssgproject.content_rule_dnf-automatic_security_updates_only'
"~/bash-remediate.xml" 1404L, 67017B
```

OpenSCAP during installation

Installation with Anaconda

Select “Security Profile” from main Installation screen

Choose Security Profile from list and click on “Select profile” button



LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/Chicago timezone

USER SETTINGS

SOFTWARE

Connect to Red Hat
Not registered.

Installation Source
http://192.168.40.44/iso/rhel/server/x86_64/9.2

Software Selection
Server

SYSTEM

Installation Destination
Custom partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Connected: enp1s0

Security Profile
No profile selected

Red Hat Enterprise Linux 9.2 installation on host 192.168.40.209 - TigerVNC

SECURITY PROFILE

RED HAT ENTERPRISE LINUX 9.2 INSTALLATION

Apply security policy: ●

Choose profile below:

ANSSI-BP-028 (enhanced)
This profile contains configurations that align to ANSSI-BP-028 at the enhanced hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information.
ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

ANSSI-BP-028 (high)
This profile contains configurations that align to ANSSI-BP-028 at the high hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information.
ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

ANSSI-BP-028 (intermediary)
This profile contains configurations that align to ANSSI-BP-028 at the intermediary hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information.
ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

ANSSI-BP-028 (minimal) ✓
This profile contains configurations that align to ANSSI-BP-028 at the minimal hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information.
ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Server
This profile defines a baseline that aligns to the "Level 2 - Server"
configuration from the Center for Internet Security® Red Hat Enterprise
Linux 9 Benchmark™, v1.0.0, released 2022-11-28.

This profile includes Center for Internet Security®

Changes that were done or need to be done:

- package 'rsyslog' has been added to the list of to be installed packages
- package 'dnf-automatic' has been added to the list of to be installed packages
- package 'ypserv' has been added to the list of excluded packages
- package 'xinetd' has been added to the list of excluded packages
- package 'tftp-server' has been added to the list of excluded packages
- package 'telnet-server' has been added to the list of excluded packages

Installation with Kickstart

Kickstart Stanza

```
%addon com_redhat_oscap
    content-type = scap-security-guide
    profile = xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
%end
```

Remember

```
# dnf -y install scap-security-guide
```

Installs RHEL Kickstart examples: /usr/share/scap-security-guide/kickstart

OpenSCAP in Satellite 6

Satellite 6 Client Requirements

Install scap-security-guide

```
# dnf -y install scap-security-guide
```

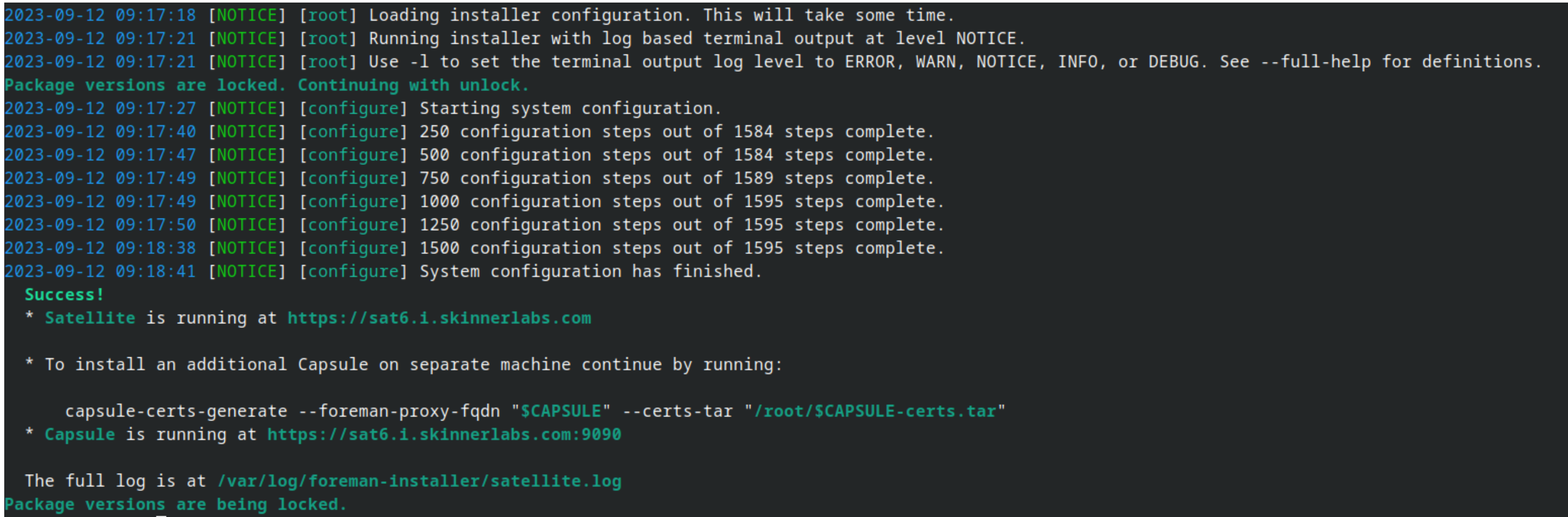
Join Satellite 6 Client repository

```
# subscription-manager repos --enable=satellite-client-6-for-rhel-9-x86_64-rpms
```

Preparing Satellite 6

Enable SCAP Content

#satellite-installer --enable-foreman-plugin-openscap --enable-foreman-proxy-plugin-openscap --foreman-proxy-plugin-openscap-puppet-module true



```
2023-09-12 09:17:18 [NOTICE] [root] Loading installer configuration. This will take some time.
2023-09-12 09:17:21 [NOTICE] [root] Running installer with log based terminal output at level NOTICE.
2023-09-12 09:17:21 [NOTICE] [root] Use -l to set the terminal output log level to ERROR, WARN, NOTICE, INFO, or DEBUG. See --full-help for definitions.
Package versions are locked. Continuing with unlock.
2023-09-12 09:17:27 [NOTICE] [configure] Starting system configuration.
2023-09-12 09:17:40 [NOTICE] [configure] 250 configuration steps out of 1584 steps complete.
2023-09-12 09:17:47 [NOTICE] [configure] 500 configuration steps out of 1584 steps complete.
2023-09-12 09:17:49 [NOTICE] [configure] 750 configuration steps out of 1589 steps complete.
2023-09-12 09:17:49 [NOTICE] [configure] 1000 configuration steps out of 1595 steps complete.
2023-09-12 09:17:50 [NOTICE] [configure] 1250 configuration steps out of 1595 steps complete.
2023-09-12 09:18:38 [NOTICE] [configure] 1500 configuration steps out of 1595 steps complete.
2023-09-12 09:18:41 [NOTICE] [configure] System configuration has finished.
  Success!
  * Satellite is running at https://sat6.i.skinnerlabs.com

  * To install an additional Capsule on separate machine continue by running:

      capsule-certs-generate --foreman-proxy-fqdn "$CAPSULE" --certs-tar "/root/$CAPSULE-certs.tar"
  * Capsule is running at https://sat6.i.skinnerlabs.com:9090

  The full log is at /var/log/foreman-installer/satellite.log
Package versions are being locked.
```

Preparing Satellite 6

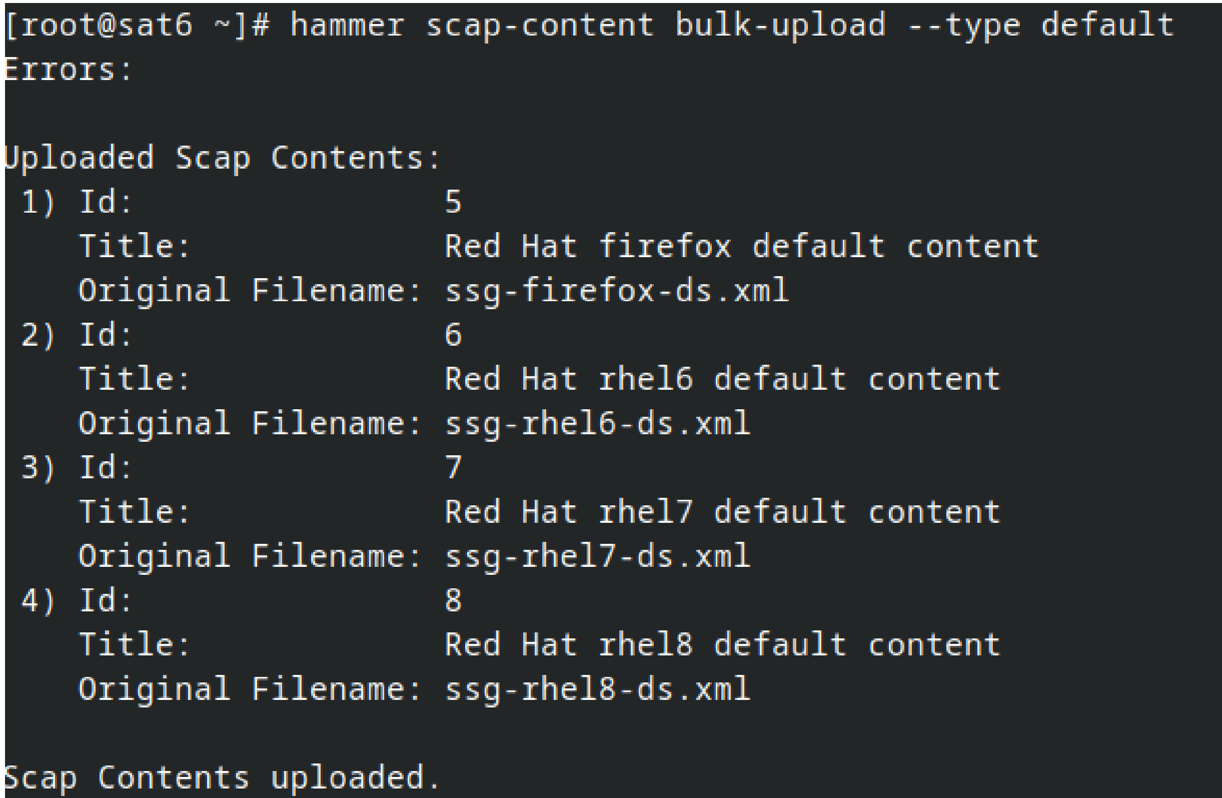
Import Default SCAP Content

hammer scap-content bulk-upload --type default

SCAP Content

- Firefox
- RHEL6
- RHEL7
- RHEL8

Where is RHEL9?

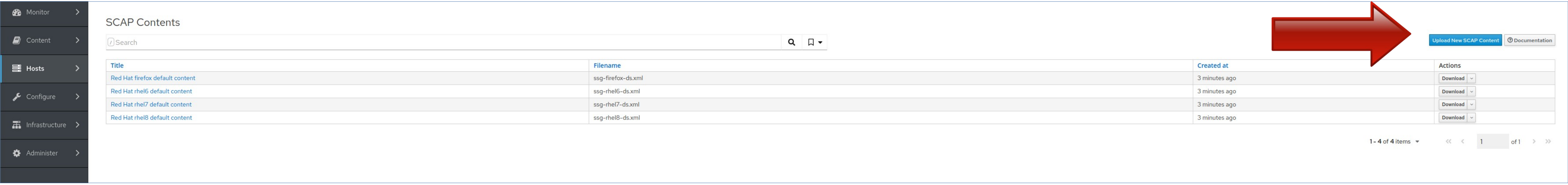


```
[root@sat6 ~]# hammer scap-content bulk-upload --type default
Errors:

Uploaded Scap Contents:
 1) Id:                5
    Title:             Red Hat firefox default content
    Original Filename: ssg-firefox-ds.xml
 2) Id:                6
    Title:             Red Hat rhel6 default content
    Original Filename: ssg-rhel6-ds.xml
 3) Id:                7
    Title:             Red Hat rhel7 default content
    Original Filename: ssg-rhel7-ds.xml
 4) Id:                8
    Title:             Red Hat rhel8 default content
    Original Filename: ssg-rhel8-ds.xml

Scap Contents uploaded.
```

Preparing Satellite 6

Import RHEL9 SCAP Content

- Install scap-security-guide.rpm onto a RHEL9 system
- Manually copy /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml file to a workstation
- Use Satellite UI to import file from workstation

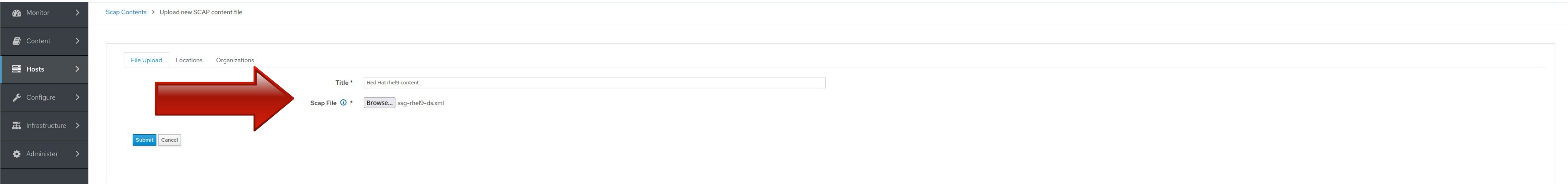


SCAP Contents

Title	Filename	Created at	Actions
Red Hat firefox default content	ssg-firefox-ds.xml	3 minutes ago	Download
Red Hat rhel6 default content	ssg-rhel6-ds.xml	3 minutes ago	Download
Red Hat rhel7 default content	ssg-rhel7-ds.xml	3 minutes ago	Download
Red Hat rhel8 default content	ssg-rhel8-ds.xml	3 minutes ago	Download

1 - 4 of 4 items

1 of 1



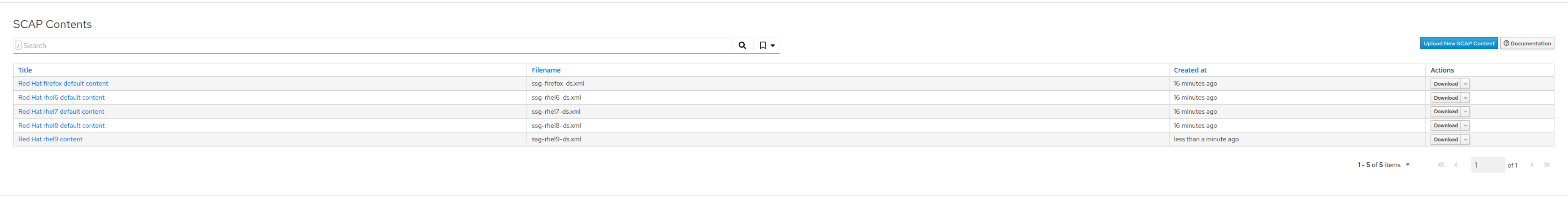
Scap Contents > Upload new SCAP content file

Title * Red Hat rhel9 content

Scap File * ssg-rhel9-ds.xml

Preparing Satellite 6

All SCAP Content



SCAP Contents

Title	Filename	Created at	Actions
Red Hat firefox default content	ssg-firefox-ds.xml	16 minutes ago	Download
Red Hat rhel6 default content	ssg-rhel6-ds.xml	16 minutes ago	Download
Red Hat rhel7 default content	ssg-rhel7-ds.xml	16 minutes ago	Download
Red Hat rhel8 default content	ssg-rhel8-ds.xml	16 minutes ago	Download
Red Hat rhel9 content	ssg-rhel9-ds.xml	less than a minute ago	Download

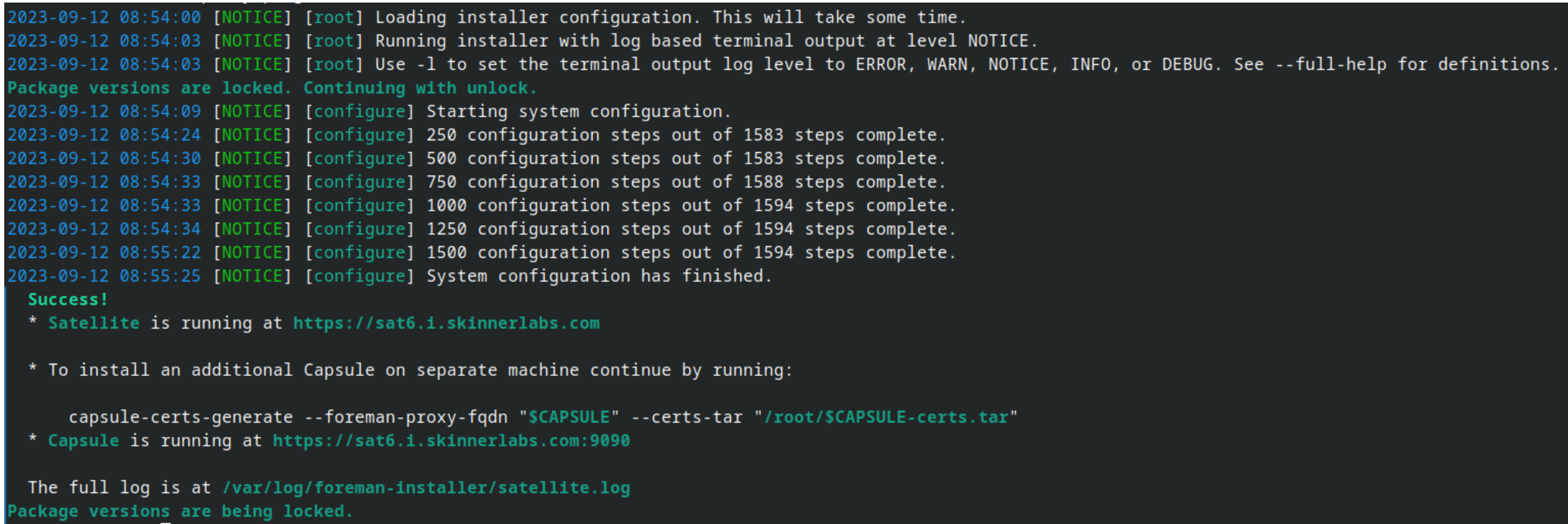
1 - 5 of 5 items

1 of 1

Preparing Satellite 6

Enable Ansible Integration

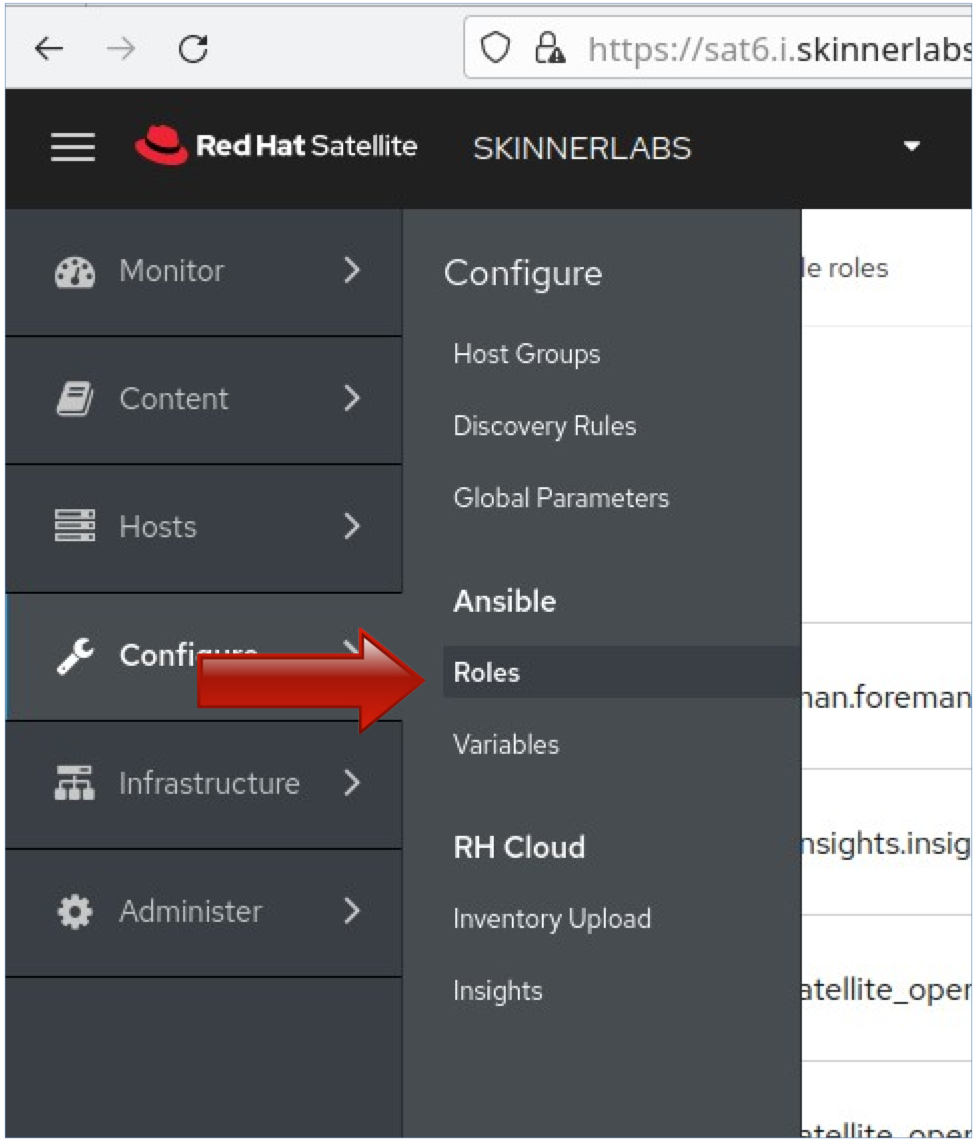
#satellite-installer --enable-foreman-plugin-ansible --enable-foreman-proxy-plugin-ansible



```
2023-09-12 08:54:00 [NOTICE] [root] Loading installer configuration. This will take some time.
2023-09-12 08:54:03 [NOTICE] [root] Running installer with log based terminal output at level NOTICE.
2023-09-12 08:54:03 [NOTICE] [root] Use -l to set the terminal output log level to ERROR, WARN, NOTICE, INFO, or DEBUG. See --full-help for definitions.
Package versions are locked. Continuing with unlock.
2023-09-12 08:54:09 [NOTICE] [configure] Starting system configuration.
2023-09-12 08:54:24 [NOTICE] [configure] 250 configuration steps out of 1583 steps complete.
2023-09-12 08:54:30 [NOTICE] [configure] 500 configuration steps out of 1583 steps complete.
2023-09-12 08:54:33 [NOTICE] [configure] 750 configuration steps out of 1588 steps complete.
2023-09-12 08:54:33 [NOTICE] [configure] 1000 configuration steps out of 1594 steps complete.
2023-09-12 08:54:34 [NOTICE] [configure] 1250 configuration steps out of 1594 steps complete.
2023-09-12 08:55:22 [NOTICE] [configure] 1500 configuration steps out of 1594 steps complete.
2023-09-12 08:55:25 [NOTICE] [configure] System configuration has finished.
  Success!
  * Satellite is running at https://sat6.i.skinnerlabs.com

  * To install an additional Capsule on separate machine continue by running:

      capsule-certs-generate --foreman-proxy-fqdn "$CAPSULE" --certs-tar "/root/$CAPSULE-certs.tar"
  * Capsule is running at https://sat6.i.skinnerlabs.com:9090

  The full log is at /var/log/foreman-installer/satellite.log
Package versions are being locked.
```

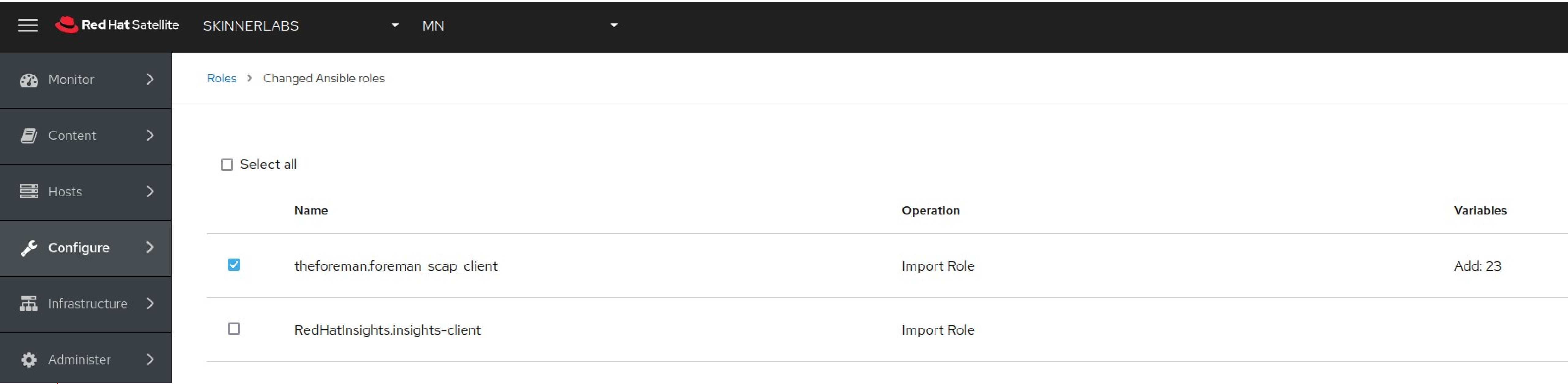
Preparing Satellite 6

Import Ansible SCAP Client Roles



Preparing Satellite 6

Select Ansible SCAP Client Roles

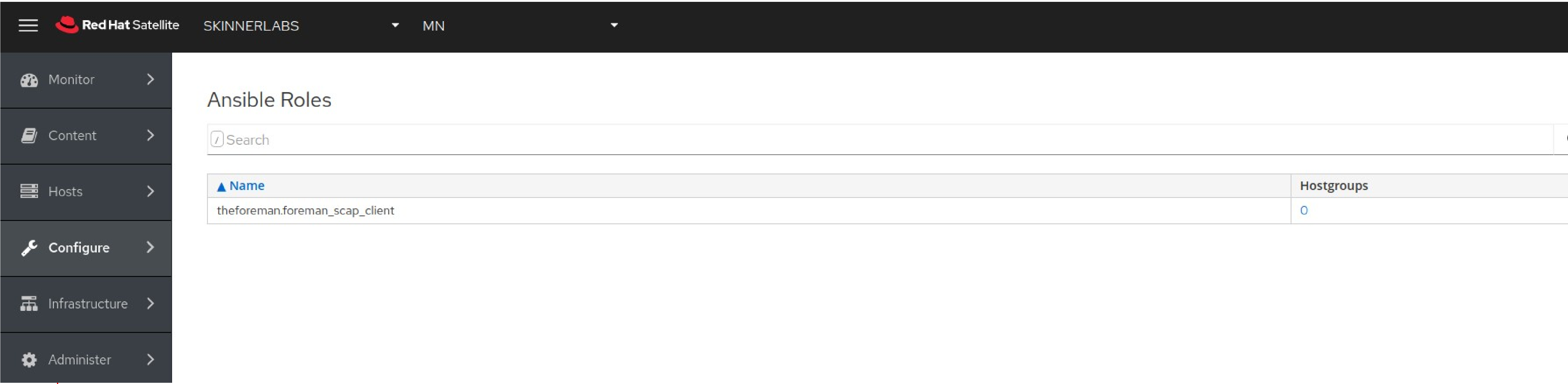


☐ Select all

	Name	Operation	Variables
☑	theforeman.foreman_scap_client	Import Role	Add: 23
☐	RedHatInsights.insights-client	Import Role	

Preparing Satellite 6

Ansible SCAP Client Roles Imported!

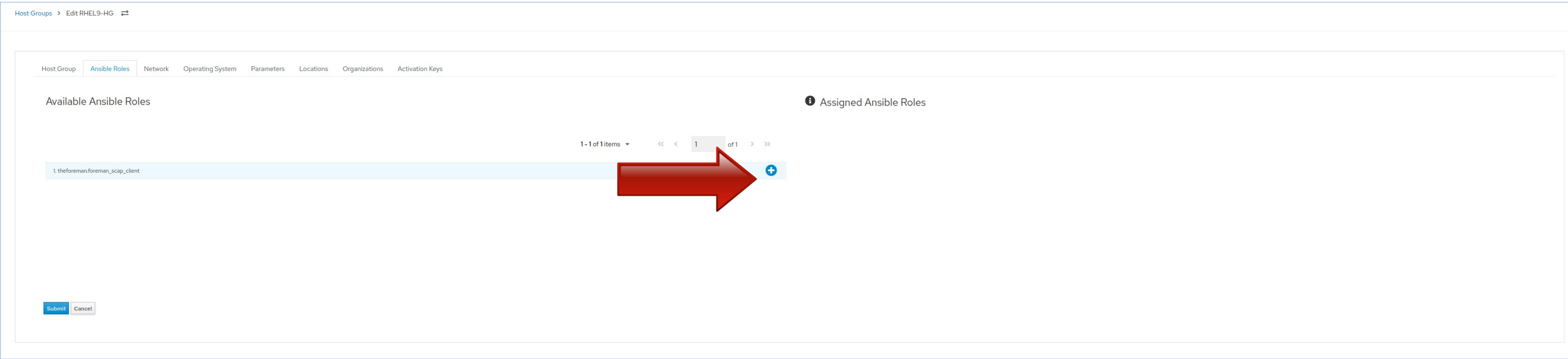


Ansible Roles

▲ Name	Hostgroups
theforeman.foreman_scap_client	0

Satellite 6 Host Groups

Create Host Group and Assign Ansible Roles



Available Ansible Roles

Assigned Ansible Roles

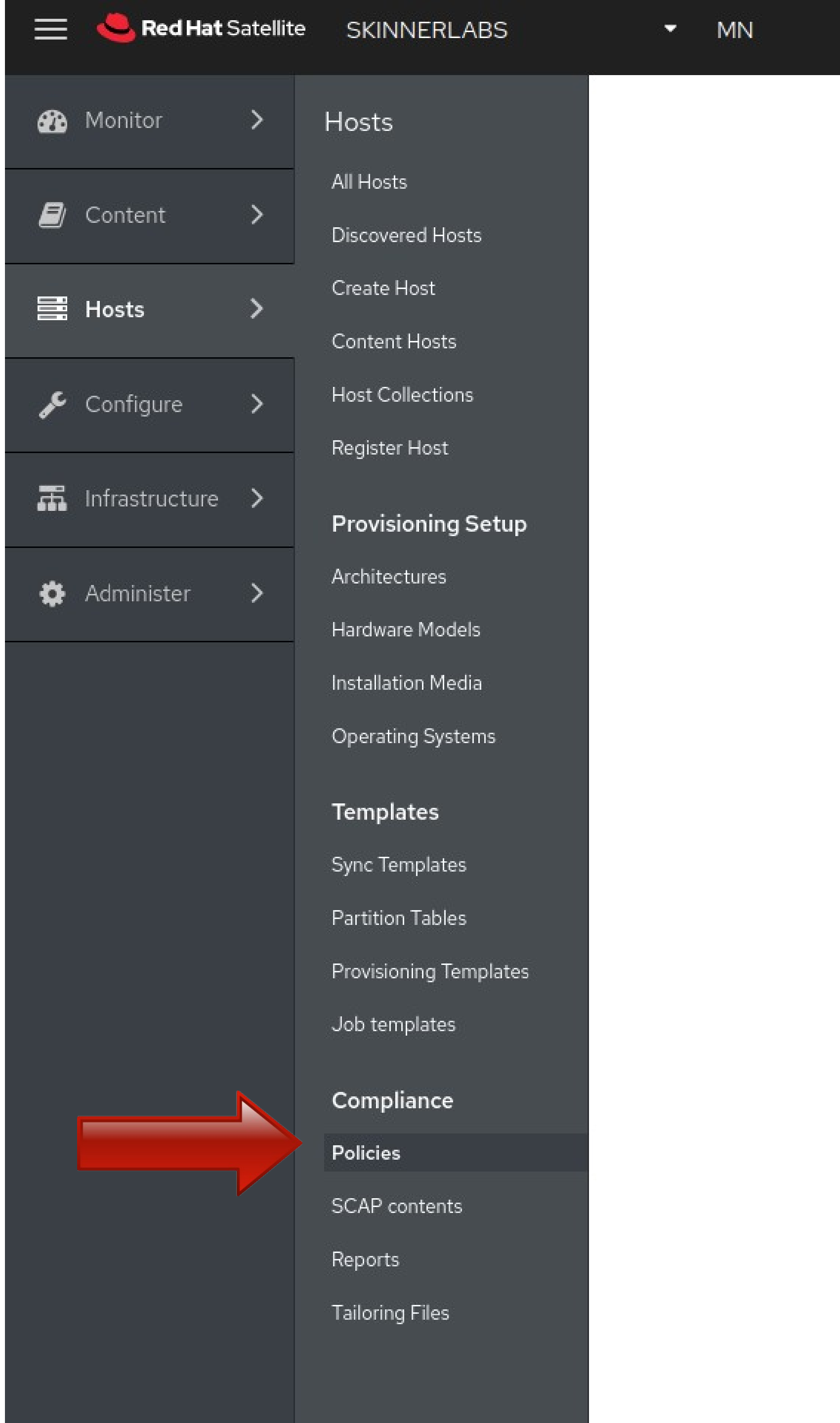
1 - 1 of 1 items

1 of 1

1. theforeman.foreman_scap_client

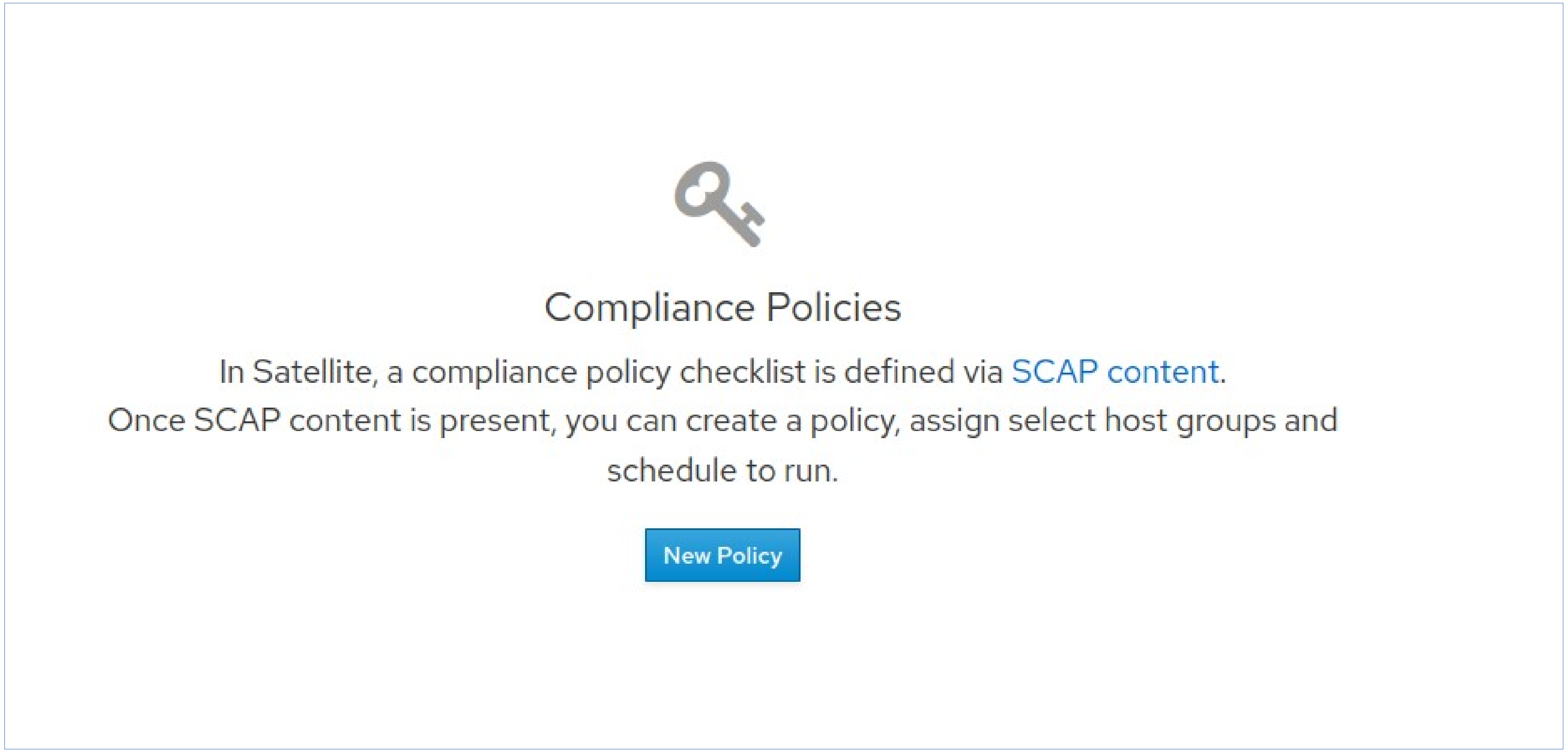
Preparing Satellite 6

Create Policy



Preparing Satellite 6

Create Policy

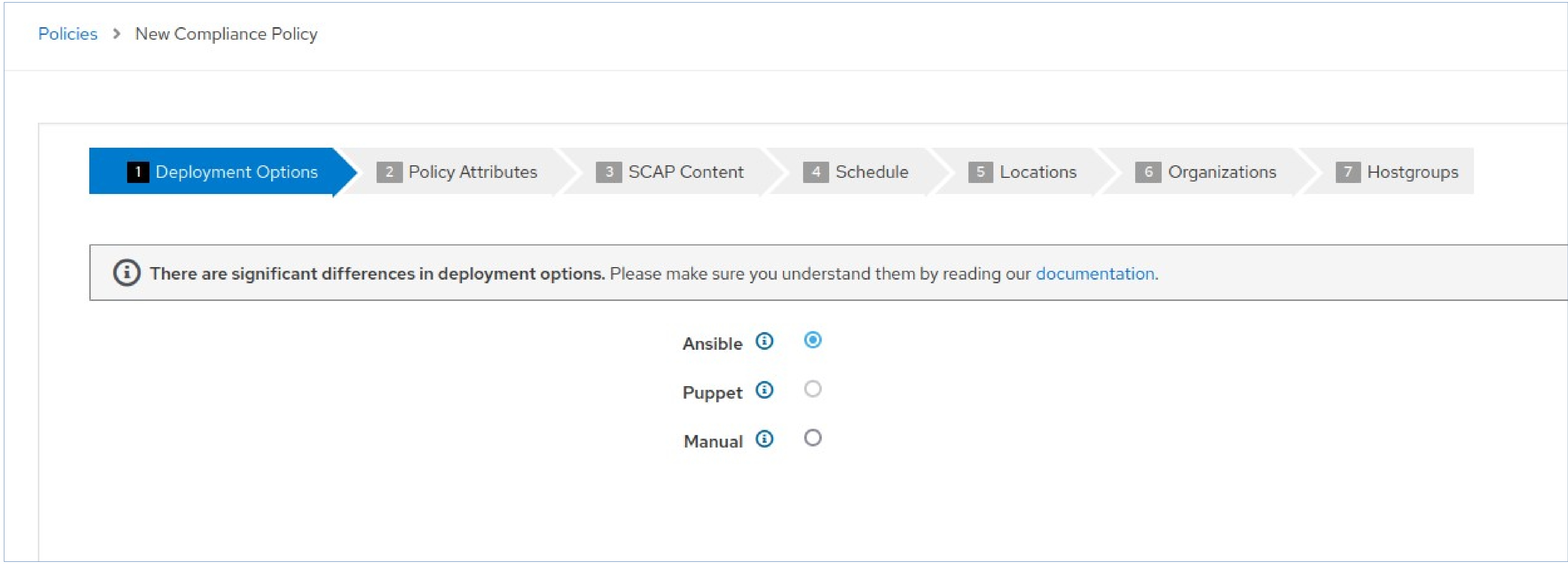


Compliance Policies

In Satellite, a compliance policy checklist is defined via SCAP content.
Once SCAP content is present, you can create a policy, assign select host groups and schedule to run.

Preparing Satellite 6

Create Policy :: Deployment Options



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

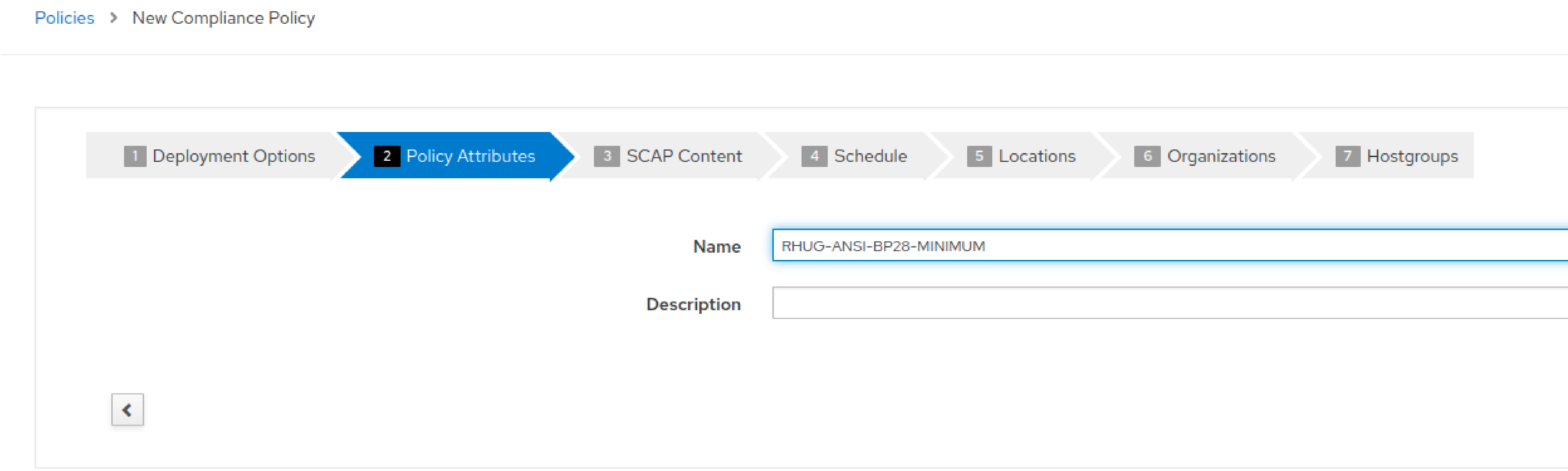
Ansible ●

Puppet ○

Manual ○

Preparing Satellite 6

Create Policy :: Policy Attributes

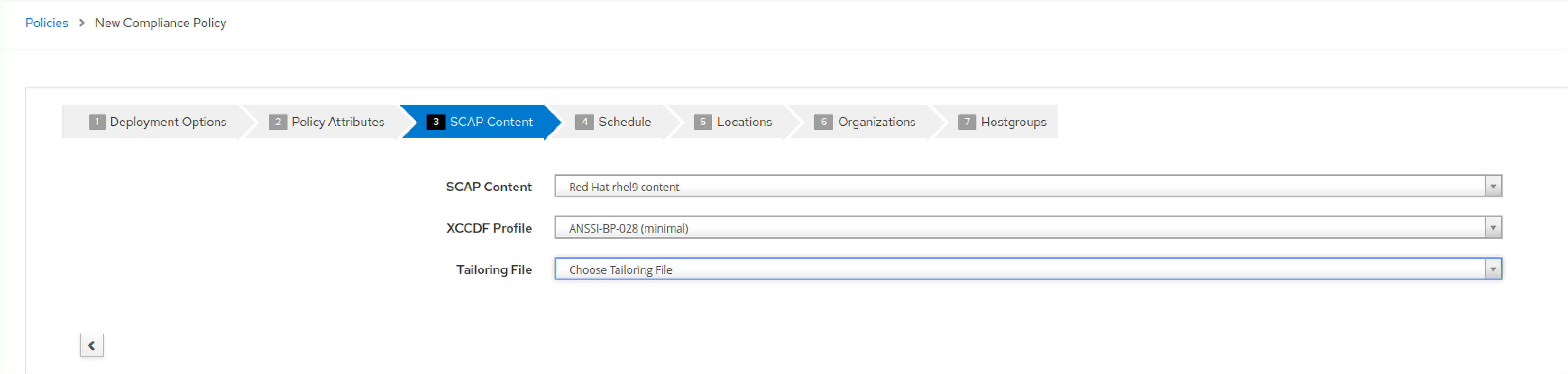


Name: RHUG-ANSI-BP28-MINIMUM

Description:

Preparing Satellite 6

Create Policy :: SCAP Content

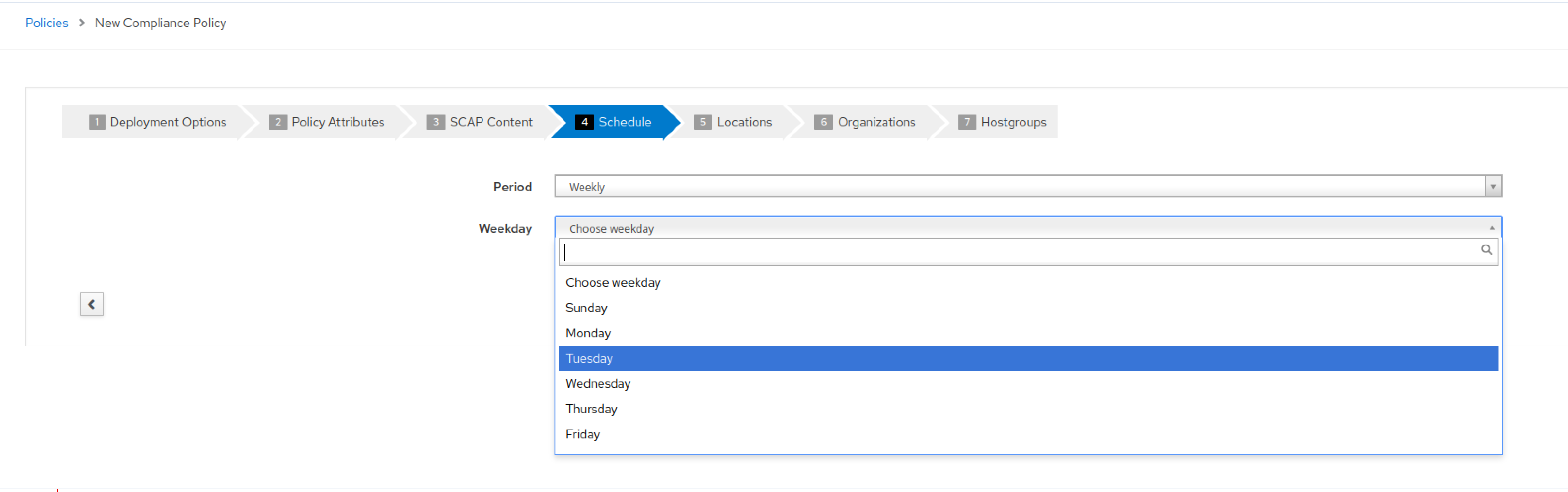


Policies > New Compliance Policy

SCAP Content	Red Hat rhel9 content
XCCDF Profile	ANSSI-BP-028 (minimal)
Tailoring File	Choose Tailoring File

Preparing Satellite 6

Create Policy :: Schedule



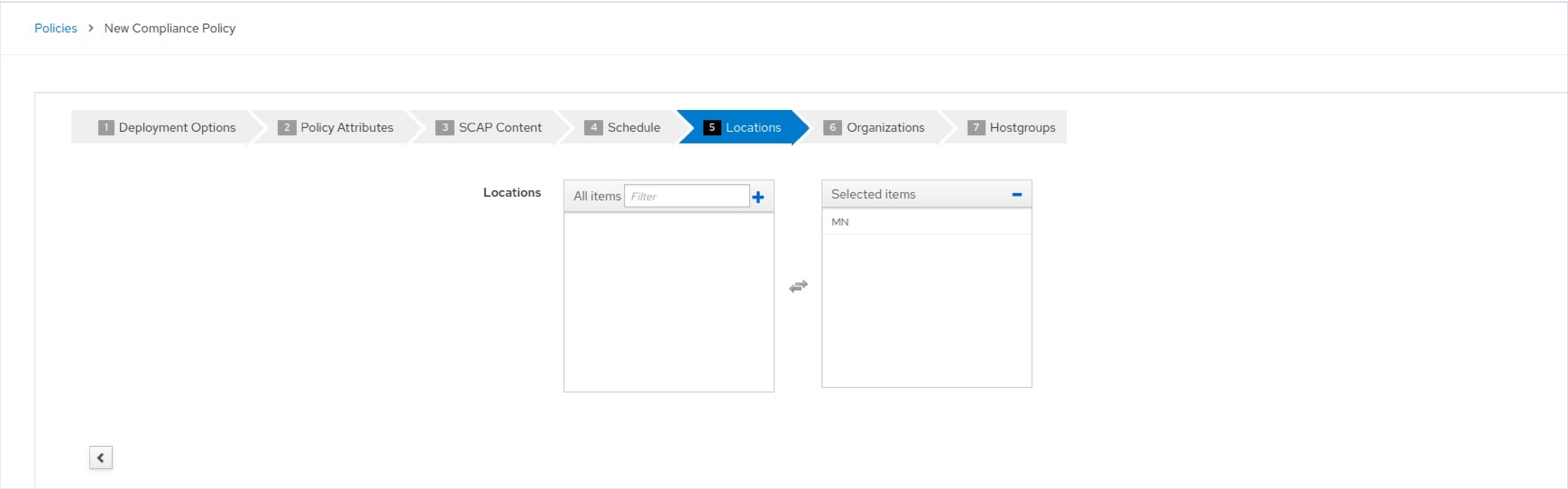
Policies > New Compliance Policy

Period: Weekly

Weekday: Choose weekday

Preparing Satellite 6

Create Policy :: Locations



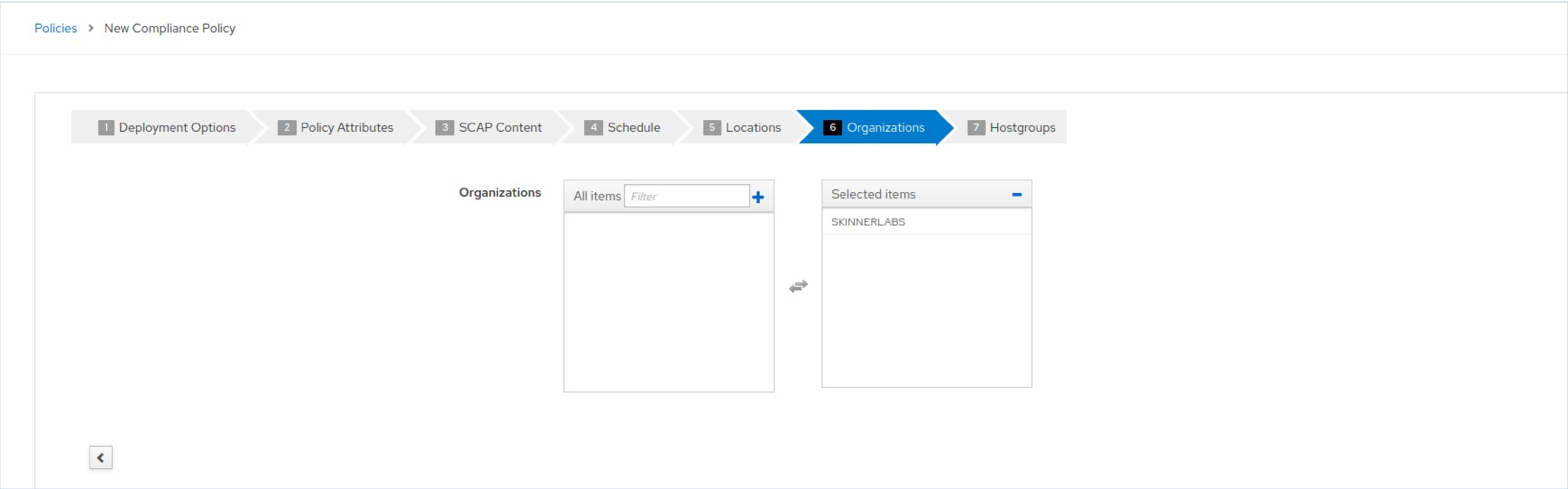
Policies > New Compliance Policy

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

Locations

Preparing Satellite 6

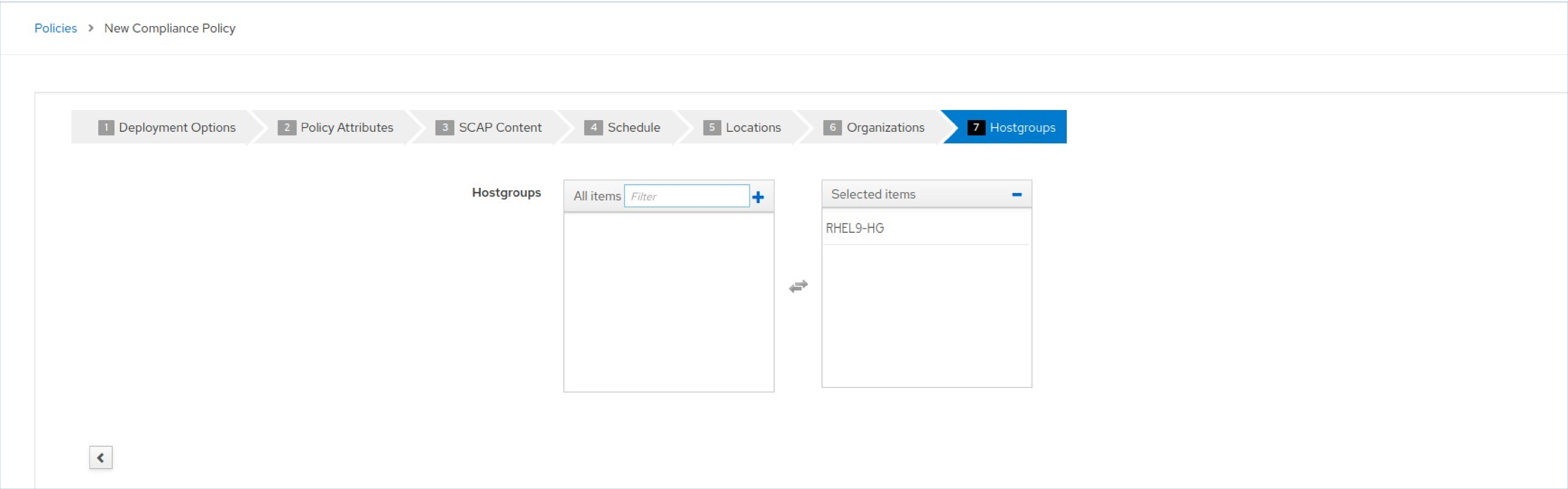
Create Policy :: Organizations



Organizations: SKINNERLABS

Preparing Satellite 6

Create Policy :: Hostgroups



Policies > New Compliance Policy

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

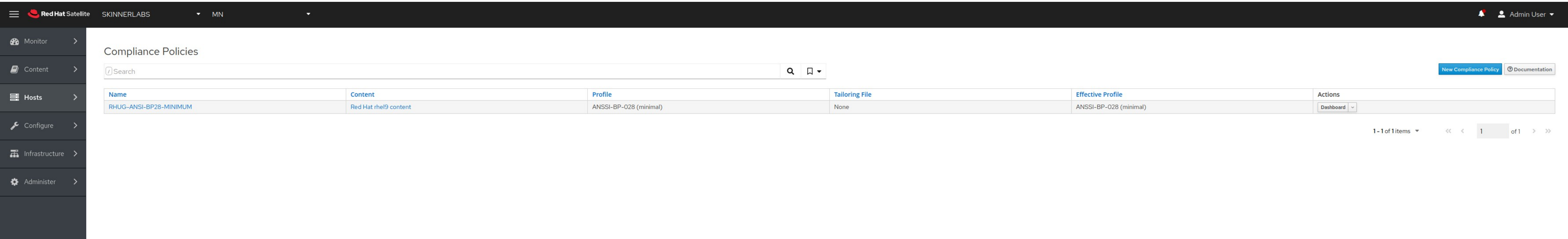
Hostgroups

All items: Filter (empty)

Selected items: RHEL9-HG

Preparing Satellite 6

Policy Created



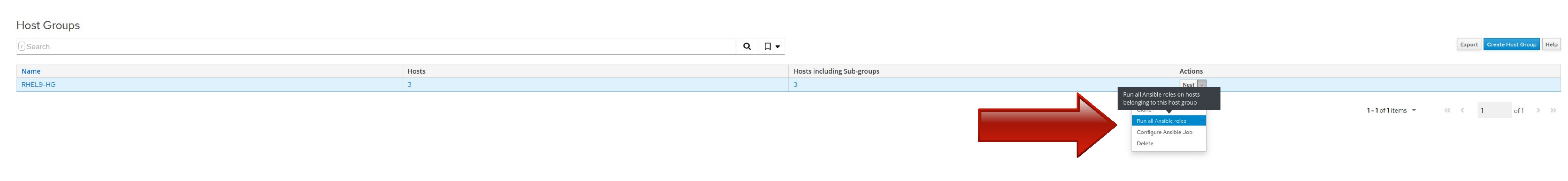
Compliance Policies

Name	Content	Profile	Tailoring File	Effective Profile	Actions
RHUG-ANSI-BP28-MINIMUM	Red Hat rhel9 content	ANSSI-BP-028 (minimal)	None	ANSSI-BP-028 (minimal)	Dashboard

1 - 1 of 1 items 1 of 1

Run OpenSCAP scan from Satellite 6

- Click on Actions … “Run all Ansible Roles”
- This will connect to each host in the Host Group, run the Ansible Playbook to configure the scheduled OpenSCAP scan, and generate a report back to Satellite



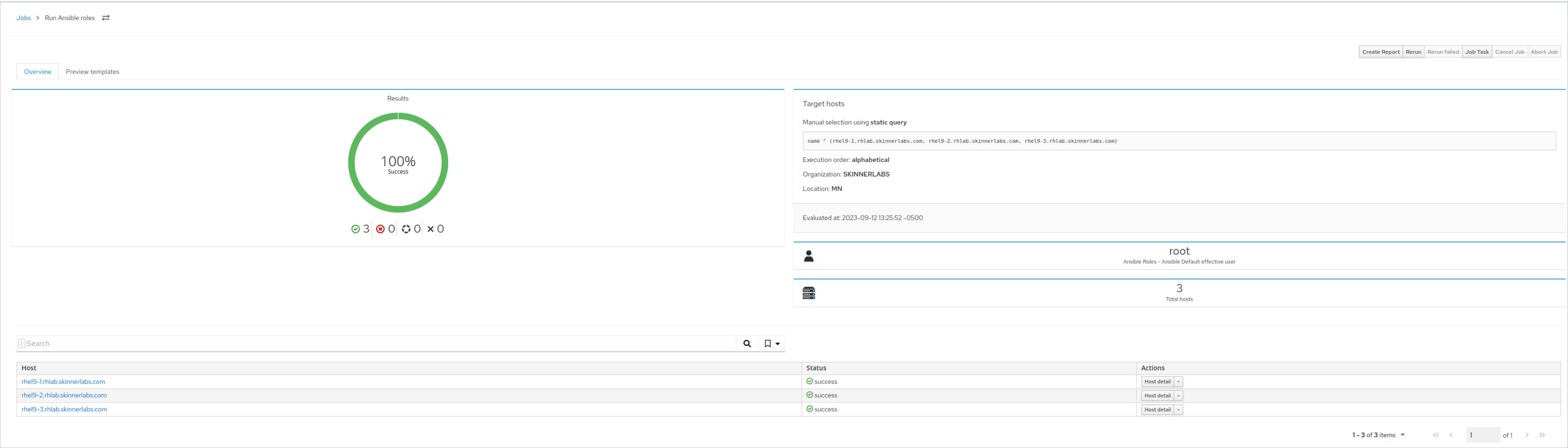
Host Groups

Name	Hosts	Hosts including Sub-groups	Actions
RHEL9-HG	3	3	Nest

Run all Ansible roles on hosts belonging to this host group

Run OpenSCAP scan from Satellite 6

- 3 Hosts = 3 Ansible jobs = 100% Success!



Target hosts

Manual selection using **static query**

```
name ^ (rhel9-1.rhlab.skinnerlabs.com, rhel9-2.rhlab.skinnerlabs.com, rhel9-3.rhlab.skinnerlabs.com)
```

Execution order: **alphabetical**

Organization: **SKINNERLABS**

Location: **MN**

Evaluated at: 2023-09-12 13:25:52 -0500

root
Ansible Roles - Ansible Default effective user

3
Total hosts

Host	Status	Actions
rhel9-1.rhlab.skinnerlabs.com	✓ success	Host detail
rhel9-2.rhlab.skinnerlabs.com	✓ success	Host detail
rhel9-3.rhlab.skinnerlabs.com	✓ success	Host detail

1 - 3 of 3 items 1 of 1

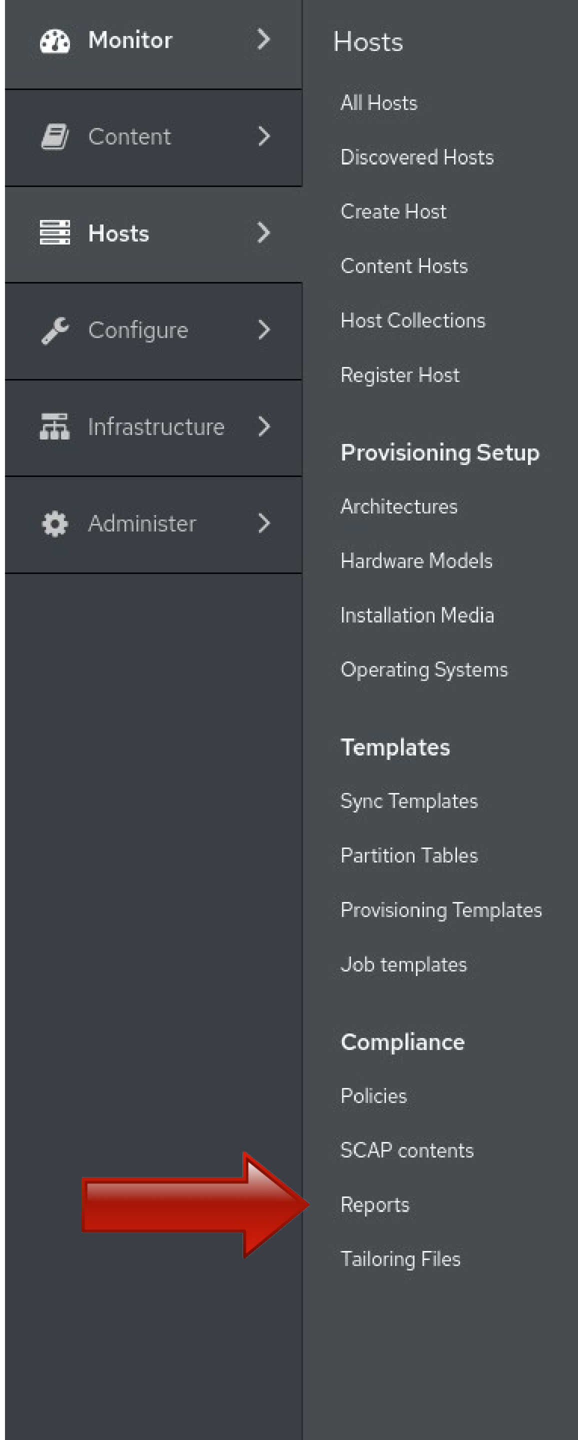
Run OpenSCAP scan manually → Satellite 6

- I don’t want to wait for a scheduled cron job on host/client
- Manually run it from client – look at /etc/cron.d/foreman_scap_client_cron file for details

```
# /usr/bin/foreman_scap_client ds 1 2>&1 | logger -t foreman_scap_client
```

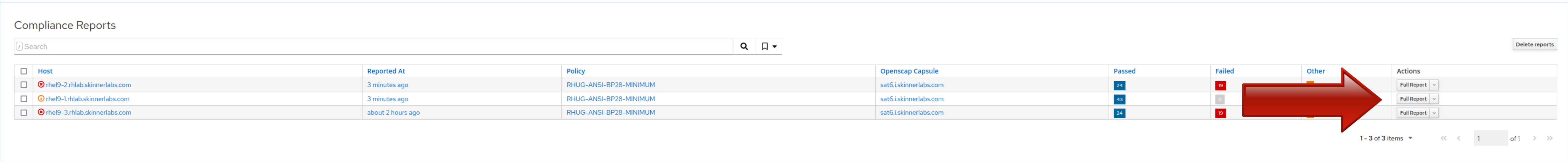
Satellite 6 OpenScap Reports

- Click on “Reports”



Satellite 6 OpenScap Reports

- Click on “Full Report”



Compliance Reports

Search

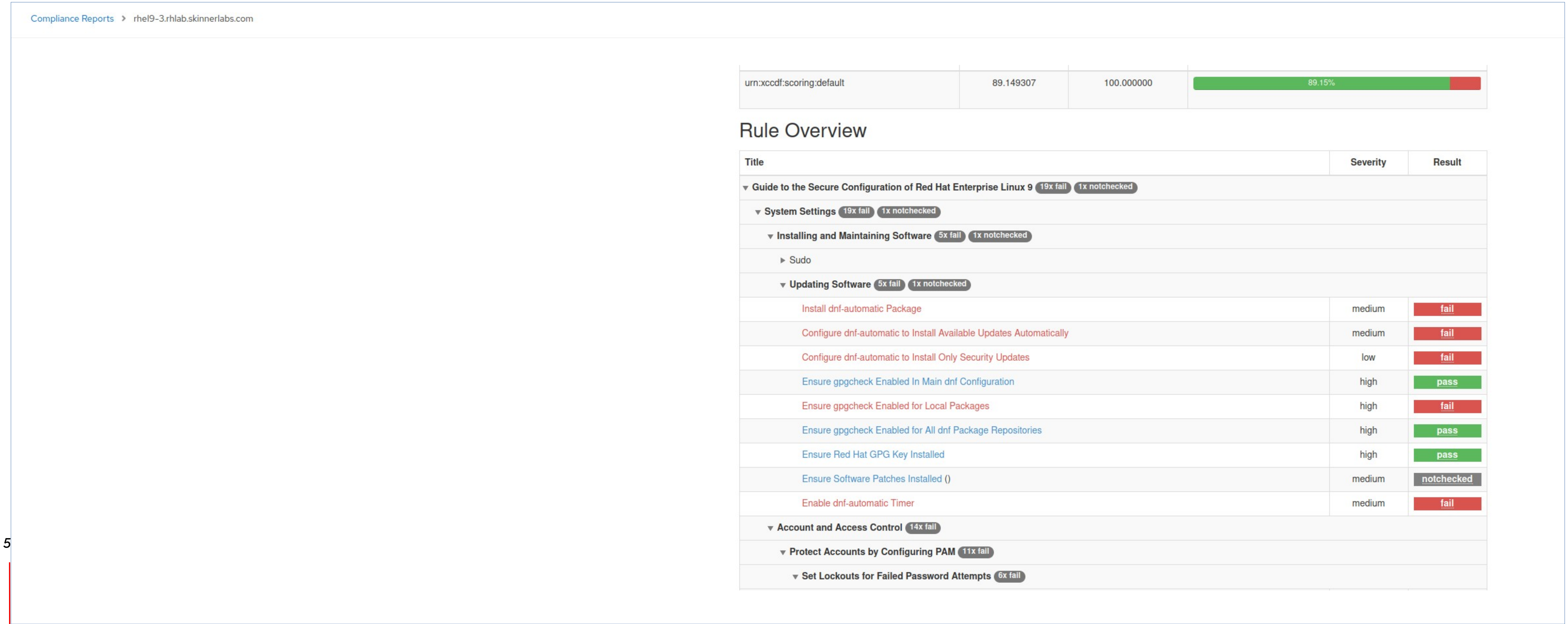
Delete reports

□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other	Actions
□	rhel9-2.rhlab.skinnerlabs.com	3 minutes ago	RHUG-ANSI-BP28-MINIMUM	sat6.i.skinnerlabs.com	24	19		Full Report
□	rhel9-1.rhlab.skinnerlabs.com	3 minutes ago	RHUG-ANSI-BP28-MINIMUM	sat6.i.skinnerlabs.com	43	0		Full Report
□	rhel9-3.rhlab.skinnerlabs.com	about 2 hours ago	RHUG-ANSI-BP28-MINIMUM	sat6.i.skinnerlabs.com	24	19		Full Report

1 - 3 of 3 items

1 of 1

Satellite 6 OpenScap Reports



Compliance Reports › rhel9-3.rhlab.skinnerlabs.com

urn:xccdf:scoring:default	89.149307	100.000000	89.15%

Rule Overview

Title	Severity	Result
▾ Guide to the Secure Configuration of Red Hat Enterprise Linux 9 19x fail 1x notchecked		
▾ System Settings 19x fail 1x notchecked		
▾ Installing and Maintaining Software 5x fail 1x notchecked		
▸ Sudo		
▾ Updating Software 5x fail 1x notchecked		
Install dnf-automatic Package	medium	fail
Configure dnf-automatic to Install Available Updates Automatically	medium	fail
Configure dnf-automatic to Install Only Security Updates	low	fail
Ensure gpgcheck Enabled In Main dnf Configuration	high	pass
Ensure gpgcheck Enabled for Local Packages	high	fail
Ensure gpgcheck Enabled for All dnf Package Repositories	high	pass
Ensure Red Hat GPG Key Installed	high	pass
Ensure Software Patches Installed ()	medium	notchecked
Enable dnf-automatic Timer	medium	fail
▾ Account and Access Control 14x fail		
▾ Protect Accounts by Configuring PAM 11x fail		
▾ Set Lockouts for Failed Password Attempts 6x fail		

SCAP Workbench

What is SCAP Workbench?

- A GUI to customize/tailor SCAP profiles
- Very common to start with a security profile, and need to customize

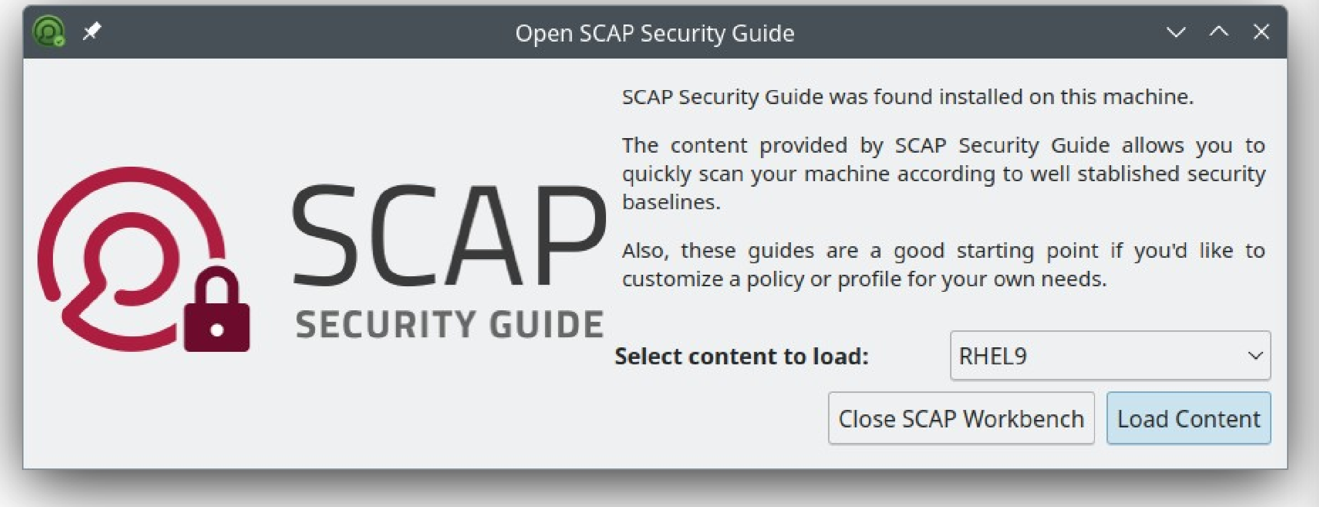
Install SCAP Workbench

- On RHEL Workstation

```
# dnf -y install scap-workbench
```

This will install: scap-workbench, scap-security-guide and openscap tooling

Start SCAP Workbench

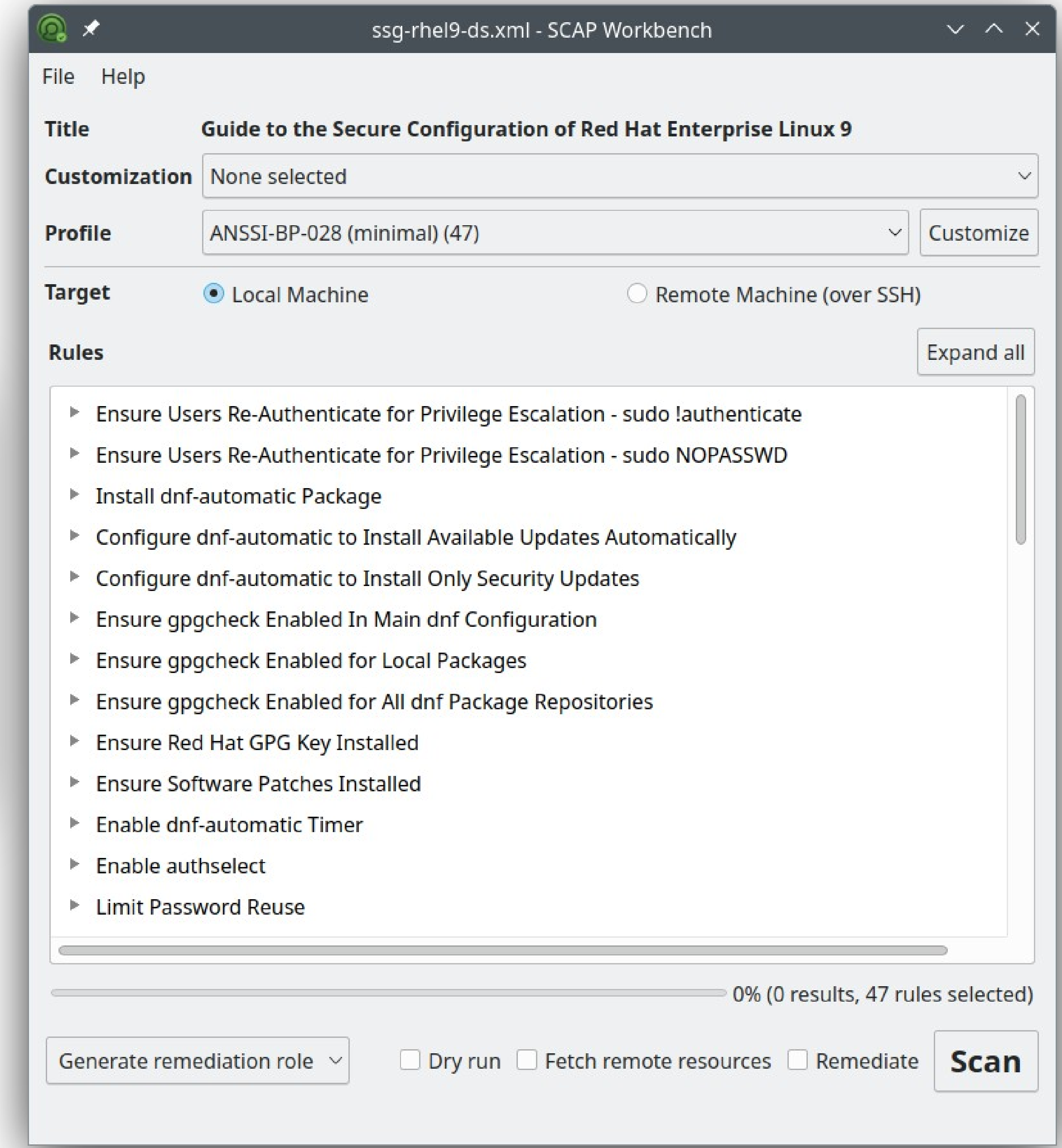


SCAP Security Guide was found installed on this machine.

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 content to load: RHEL9



Title Guide to the Secure Configuration of Red Hat Enterprise Linux 9

Customization None selected

Profile ANSSI-BP-028 (minimal) (47)

Target ● Local Machine ○ Remote Machine (over SSH)

Rules

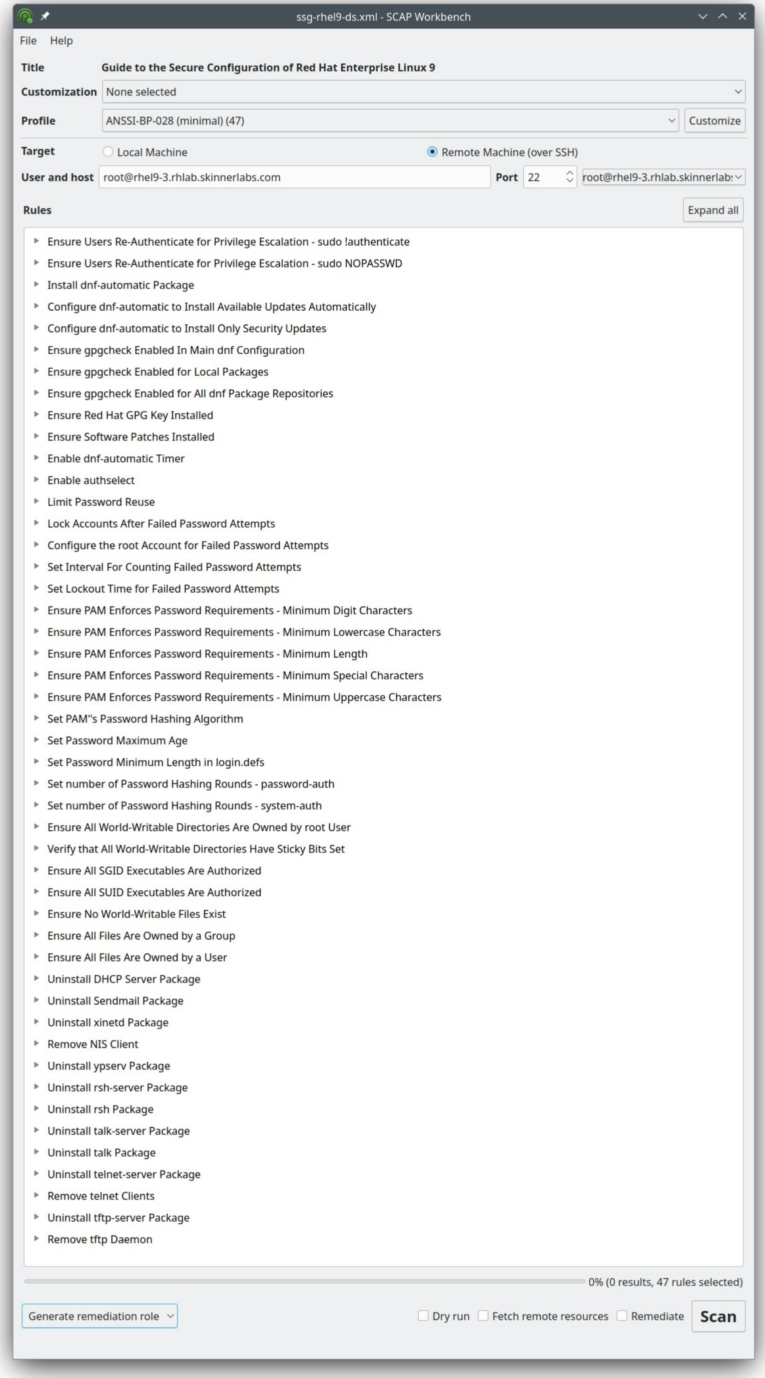
- Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate
- Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD
- Install dnf-automatic Package
- Configure dnf-automatic to Install Available Updates Automatically
- Configure dnf-automatic to Install Only Security Updates
- Ensure gpgcheck Enabled In Main dnf Configuration
- Ensure gpgcheck Enabled for Local Packages
- Ensure gpgcheck Enabled for All dnf Package Repositories
- Ensure Red Hat GPG Key Installed
- Ensure Software Patches Installed
- Enable dnf-automatic Timer
- Enable authselect
- Limit Password Reuse

0% (0 results, 47 rules selected)

□ Dry run □ Fetch remote resources □ Remediate

Using SCAP Workbench

- Select Profile
- Select Target
  - Scan local or Remote Machine
- Click on “Scan” button



Title Guide to the Secure Configuration of Red Hat Enterprise Linux 9

Customization None selected

Profile ANSSI-BP-028 (minimal) (47)

Target ○ Local Machine ● Remote Machine (over SSH)

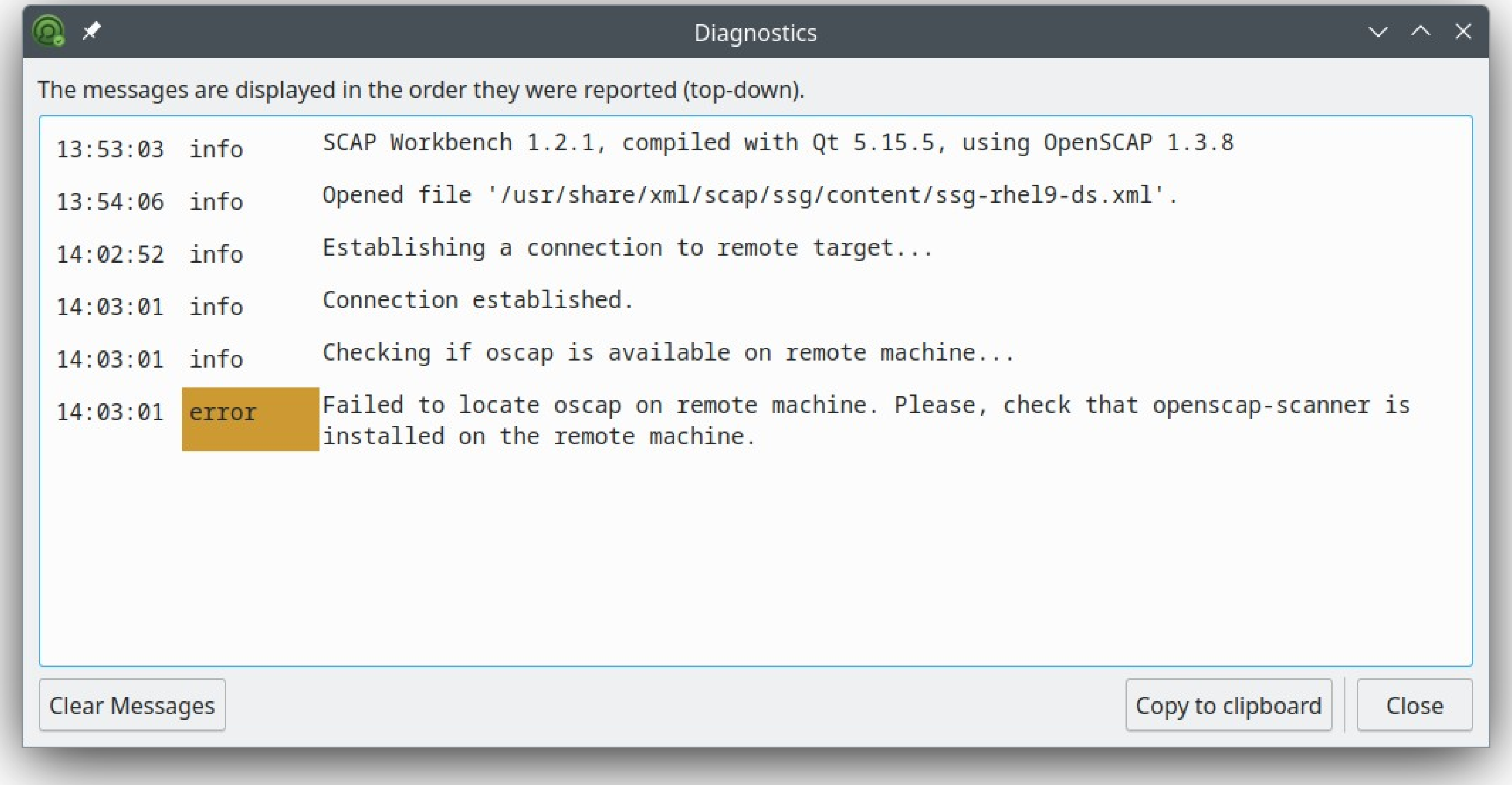
User and host root@rhel9-3.rhlab.skinnerlabs.com **Port** 22 root@rhel9-3.rhlab.skinnerlab:

Rules

- Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate
- Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD
- Install dnf-automatic Package
- Configure dnf-automatic to Install Available Updates Automatically
- Configure dnf-automatic to Install Only Security Updates
- Ensure gpgcheck Enabled In Main dnf Configuration
- Ensure gpgcheck Enabled for Local Packages
- Ensure gpgcheck Enabled for All dnf Package Repositories
- Ensure Red Hat GPG Key Installed
- Ensure Software Patches Installed
- Enable dnf-automatic Timer
- Enable authselect
- Limit Password Reuse
- Lock Accounts After Failed Password Attempts
- Configure the root Account for Failed Password Attempts
- Set Interval For Counting Failed Password Attempts
- Set Lockout Time for Failed Password Attempts
- Ensure PAM Enforces Password Requirements - Minimum Digit Characters
- Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters
- Ensure PAM Enforces Password Requirements - Minimum Length
- Ensure PAM Enforces Password Requirements - Minimum Special Characters
- Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters
- Set PAM"s Password Hashing Algorithm
- Set Password Maximum Age
- Set Password Minimum Length in login.defs
- Set number of Password Hashing Rounds - password-auth
- Set number of Password Hashing Rounds - system-auth
- Ensure All World-Writable Directories Are Owned by root User
- Verify that All World-Writable Directories Have Sticky Bits Set
- Ensure All SGID Executables Are Authorized
- Ensure All SUID Executables Are Authorized
- Ensure No World-Writable Files Exist
- Ensure All Files Are Owned by a Group
- Ensure All Files Are Owned by a User
- Uninstall DHCP Server Package
- Uninstall Sendmail Package
- Uninstall xinetd Package
- Remove NIS Client
- Uninstall ypserv Package
- Uninstall rsh-server Package
- Uninstall rsh Package
- Uninstall talk-server Package
- Uninstall talk Package
- Uninstall telnet-server Package
- Remove telnet Clients
- Uninstall tftp-server Package
- Remove tftp Daemon

0% (0 results, 47 rules selected)

Using SCAP Workbench

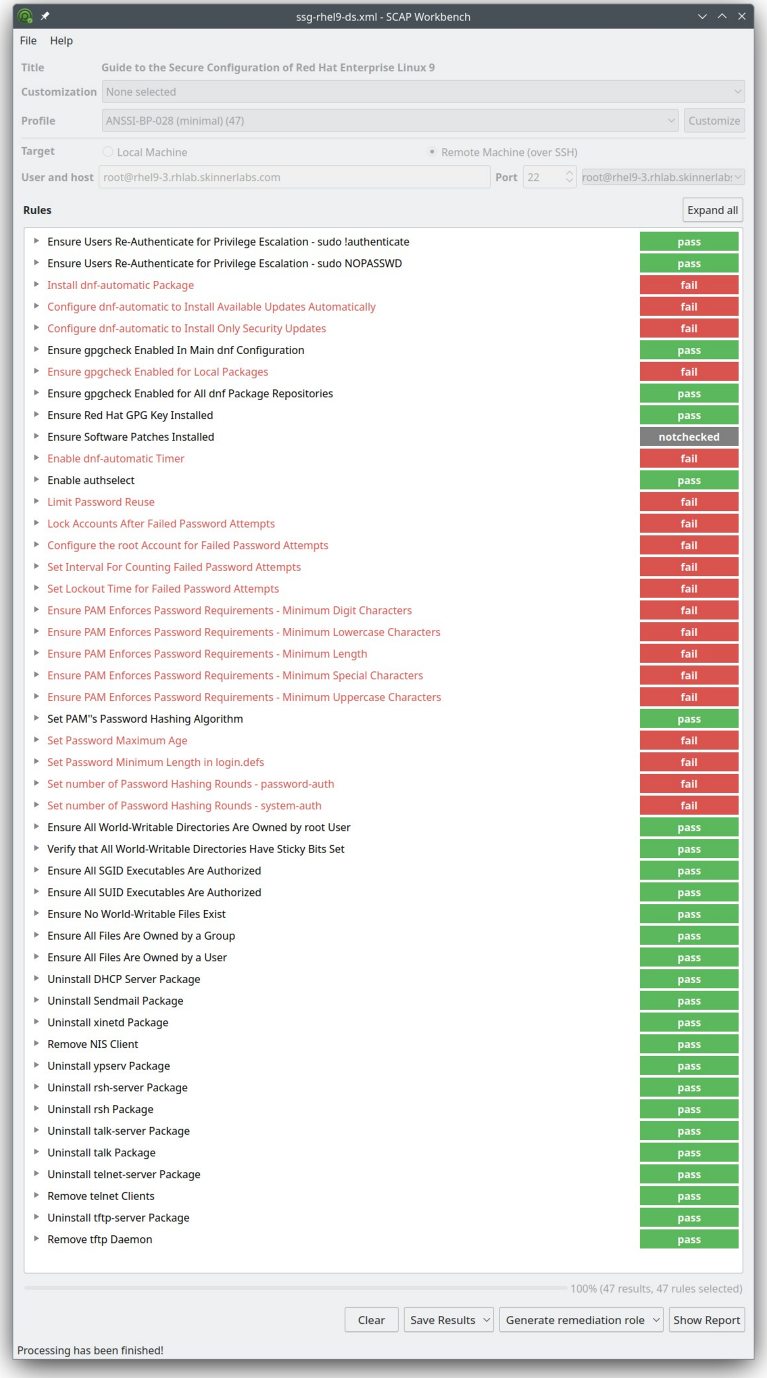


The messages are displayed in the order they were reported (top-down).

```
13:53:03  info     SCAP Workbench 1.2.1, compiled with Qt 5.15.5, using OpenSCAP 1.3.8
13:54:06  info     Opened file '/usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml'.
14:02:52  info     Establishing a connection to remote target...
14:03:01  info     Connection established.
14:03:01  info     Checking if oscap is available on remote machine...
14:03:01  error    Failed to locate oscap on remote machine. Please, check that openscap-scanner is
                   installed on the remote machine.
```

Using SCAP Workbench

- Customize
- Expand all
- Save Results
  - XCCDF
  - ARF
  - HTML
- Generate remediation
  - Bash
  - Ansible
  - Puppet
- Show Report
  - Generate HTML report



Title: Guide to the Secure Configuration of Red Hat Enterprise Linux 9

Customization: None selected

Profile: ANSSI-BP-028 (minimal) (47)

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

User and host: root@rhel9-3.rhlab.skinnerlabs.com Port: 22 root@rhel9-3.rhlab.skinnerlab:

Rules

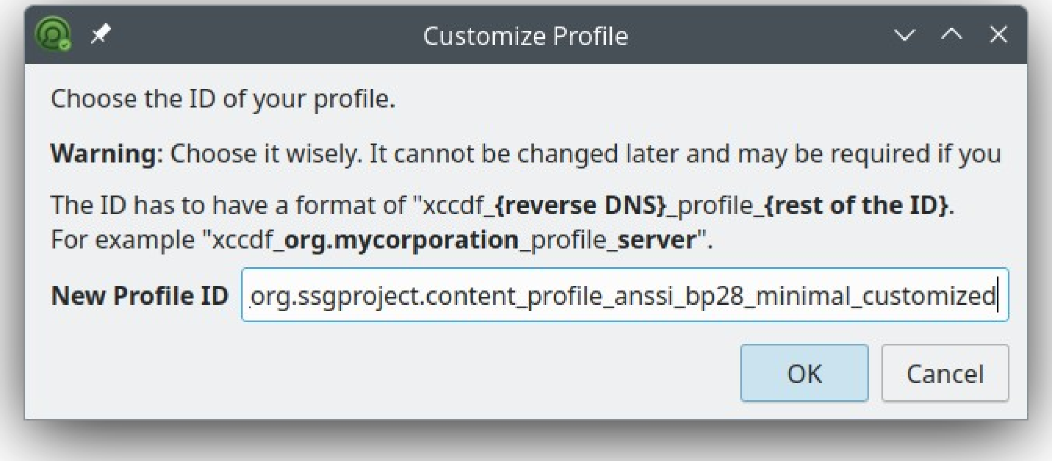
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate	pass
Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD	pass
Install dnf-automatic Package	fail
Configure dnf-automatic to Install Available Updates Automatically	fail
Configure dnf-automatic to Install Only Security Updates	fail
Ensure gpgcheck Enabled In Main dnf Configuration	pass
Ensure gpgcheck Enabled for Local Packages	fail
Ensure gpgcheck Enabled for All dnf Package Repositories	pass
Ensure Red Hat GPG Key Installed	pass
Ensure Software Patches Installed	notchecked
Enable dnf-automatic Timer	fail
Enable authselect	pass
Limit Password Reuse	fail
Lock Accounts After Failed Password Attempts	fail
Configure the root Account for Failed Password Attempts	fail
Set Interval For Counting Failed Password Attempts	fail
Set Lockout Time for Failed Password Attempts	fail
Ensure PAM Enforces Password Requirements - Minimum Digit Characters	fail
Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters	fail
Ensure PAM Enforces Password Requirements - Minimum Length	fail
Ensure PAM Enforces Password Requirements - Minimum Special Characters	fail
Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	fail
Set PAM''s Password Hashing Algorithm	pass
Set Password Maximum Age	fail
Set Password Minimum Length in login.defs	fail
Set number of Password Hashing Rounds - password-auth	fail
Set number of Password Hashing Rounds - system-auth	fail
Ensure All World-Writable Directories Are Owned by root User	pass
Verify that All World-Writable Directories Have Sticky Bits Set	pass
Ensure All SGID Executables Are Authorized	pass
Ensure All SUID Executables Are Authorized	pass
Ensure No World-Writable Files Exist	pass
Ensure All Files Are Owned by a Group	pass
Ensure All Files Are Owned by a User	pass
Uninstall DHCP Server Package	pass
Uninstall Sendmail Package	pass
Uninstall xinetd Package	pass
Remove NIS Client	pass
Uninstall ypserv Package	pass
Uninstall rsh-server Package	pass
Uninstall rsh Package	pass
Uninstall talk-server Package	pass
Uninstall talk Package	pass
Uninstall telnet-server Package	pass
Remove telnet Clients	pass
Uninstall tftp-server Package	pass
Remove tftp Daemon	pass

100% (47 results, 47 rules selected)

Processing has been finished!

Using SCAP Workbench

- Customize
- Change minimum password length from 15 to 20



Choose the ID of your profile.

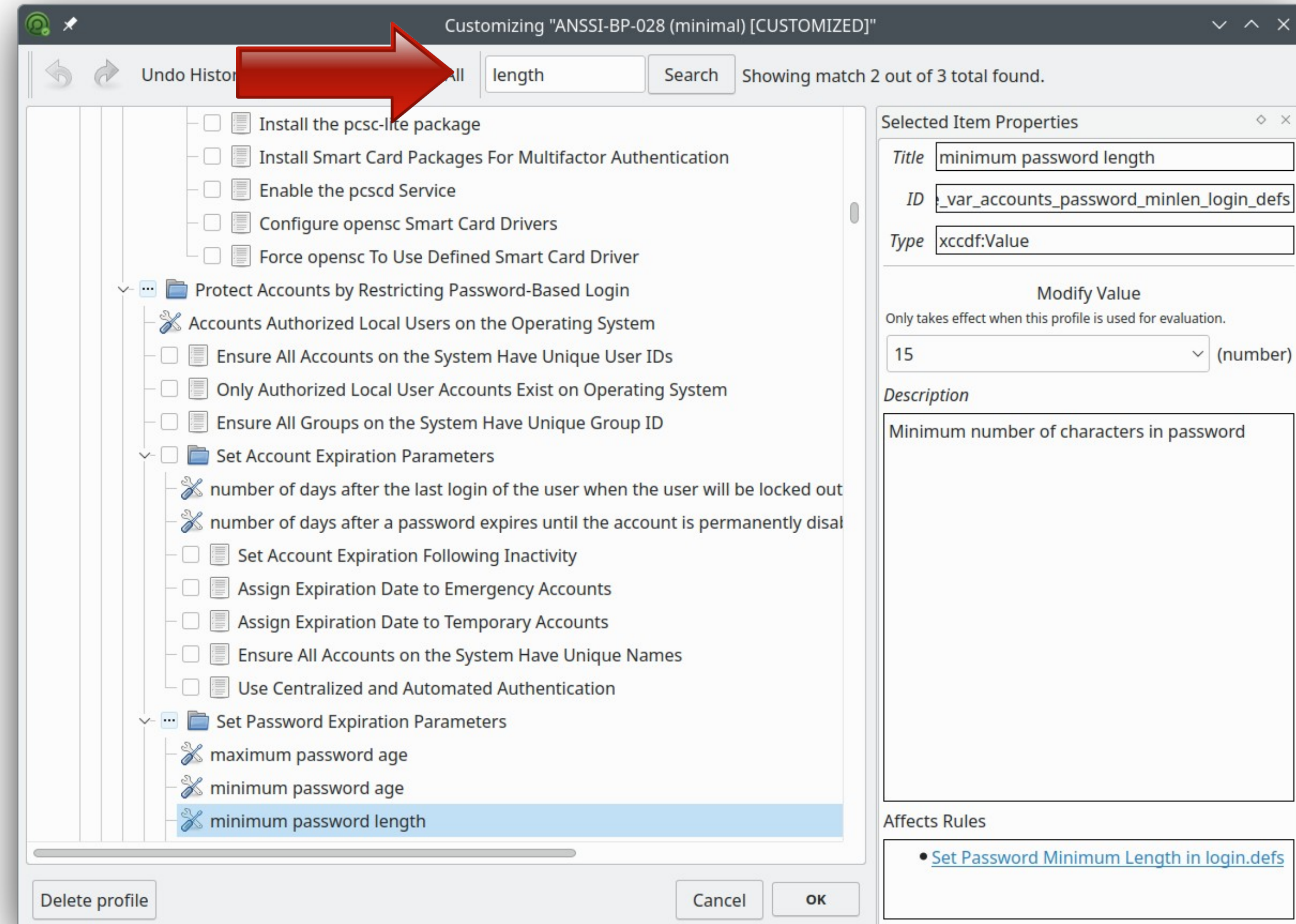
Warning: Choose it wisely. It cannot be changed later and may be required if you

The ID has to have a format of "xccdf_**{reverse DNS}**_profile_**{rest of the ID}**.
For example "xccdf_**org.mycorporation**_profile_**server**".

New Profile ID org.ssgproject.content_profile_anssi_bp28_minimal_customized

Using SCAP Workbench

- Search for “length”
- Second match allows to modify value



Customizing "ANSSI-BP-028 (minimal) [CUSTOMIZED]"

length

Showing match 2 out of 3 total found.

- □ Install the pcsc-lite package
- □ Install Smart Card Packages For Multifactor Authentication
- □ Enable the pcscd Service
- □ Configure opensc Smart Card Drivers
- □ Force opensc To Use Defined Smart Card Driver
- Protect Accounts by Restricting Password-Based Login
  - Accounts Authorized Local Users on the Operating System
  - □ Ensure All Accounts on the System Have Unique User IDs
  - □ Only Authorized Local User Accounts Exist on Operating System
  - □ Ensure All Groups on the System Have Unique Group ID
  - □ Set Account Expiration Parameters
    - number of days after the last login of the user when the user will be locked out
    - number of days after a password expires until the account is permanently disal
    - □ Set Account Expiration Following Inactivity
    - □ Assign Expiration Date to Emergency Accounts
    - □ Assign Expiration Date to Temporary Accounts
    - □ Ensure All Accounts on the System Have Unique Names
    - □ Use Centralized and Automated Authentication
  - Set Password Expiration Parameters
    - maximum password age
    - minimum password age
    - minimum password length

Selected Item Properties

Title minimum password length

ID _var_accounts_password_minlen_login_defs

Type xccdf:Value

Modify Value

Only takes effect when this profile is used for evaluation.

15 (number)

Description

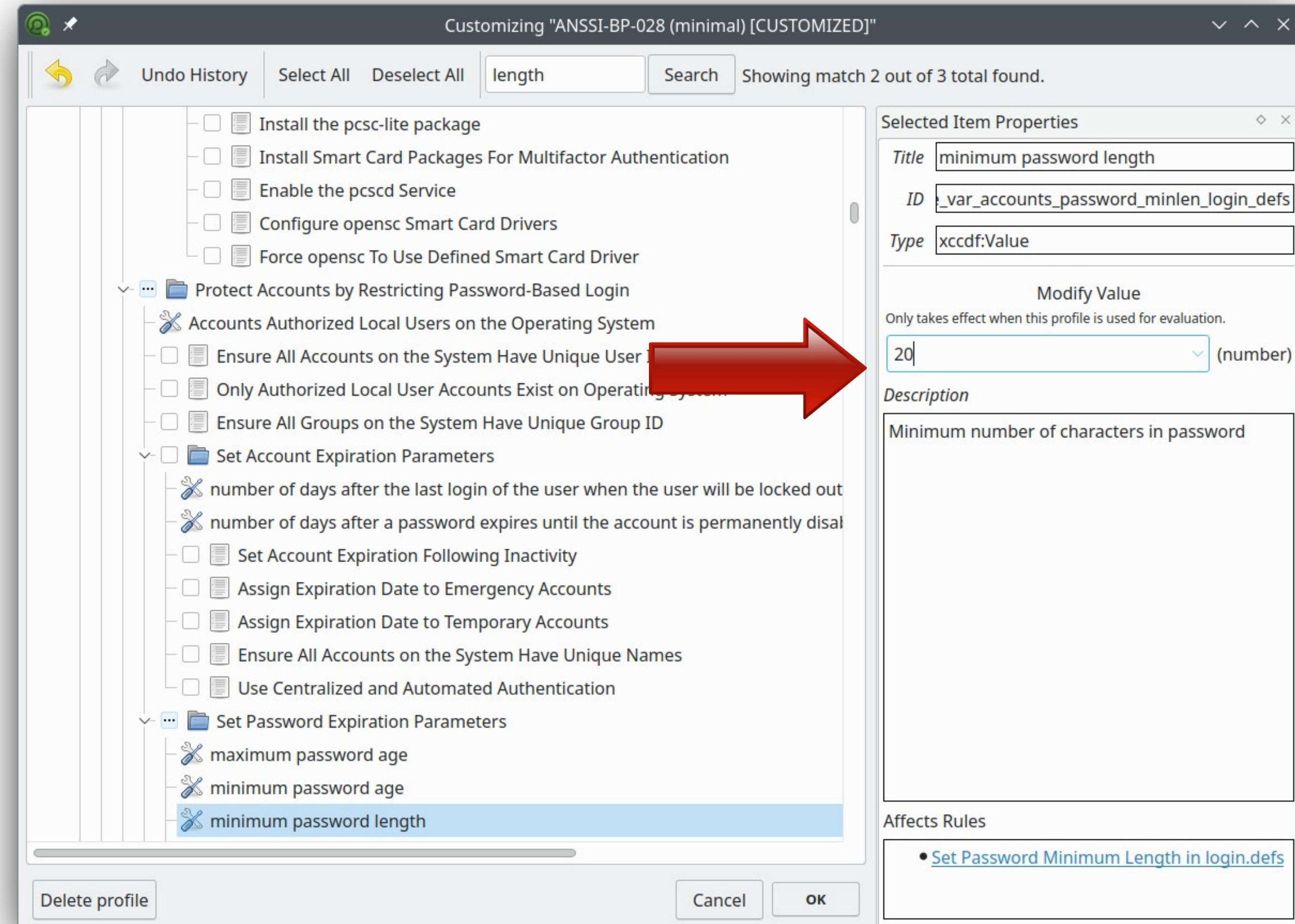
Minimum number of characters in password

Affects Rules

- Set Password Minimum Length in login.defs

Using SCAP Workbench

- Change value from 15 to 20
- Save Options
  - Save all into directory
  - Save all as an RPM
  - Save only customization



Customizing "ANSSI-BP-028 (minimal) [CUSTOMIZED]"

length

Showing match 2 out of 3 total found.

- ☐ Install the pcsc-lite package
- ☐ Install Smart Card Packages For Multifactor Authentication
- ☐ Enable the pcscd Service
- ☐ Configure opensc Smart Card Drivers
- ☐ Force opensc To Use Defined Smart Card Driver
- Protect Accounts by Restricting Password-Based Login
  - Accounts Authorized Local Users on the Operating System
  - ☐ Ensure All Accounts on the System Have Unique User I
  - ☐ Only Authorized Local User Accounts Exist on Operati
  - ☐ Ensure All Groups on the System Have Unique Group ID
  - ☐ Set Account Expiration Parameters
    - number of days after the last login of the user when the user will be locked out
    - number of days after a password expires until the account is permanently disal
    - ☐ Set Account Expiration Following Inactivity
    - ☐ Assign Expiration Date to Emergency Accounts
    - ☐ Assign Expiration Date to Temporary Accounts
    - ☐ Ensure All Accounts on the System Have Unique Names
    - ☐ Use Centralized and Automated Authentication
  - Set Password Expiration Parameters
    - maximum password age
    - minimum password age
    - minimum password length

Selected Item Properties

Title: minimum password length

ID: _var_accounts_password_minlen_login_defs

Type: xccdf:Value

Modify Value

Only takes effect when this profile is used for evaluation.

20 (number)

Description

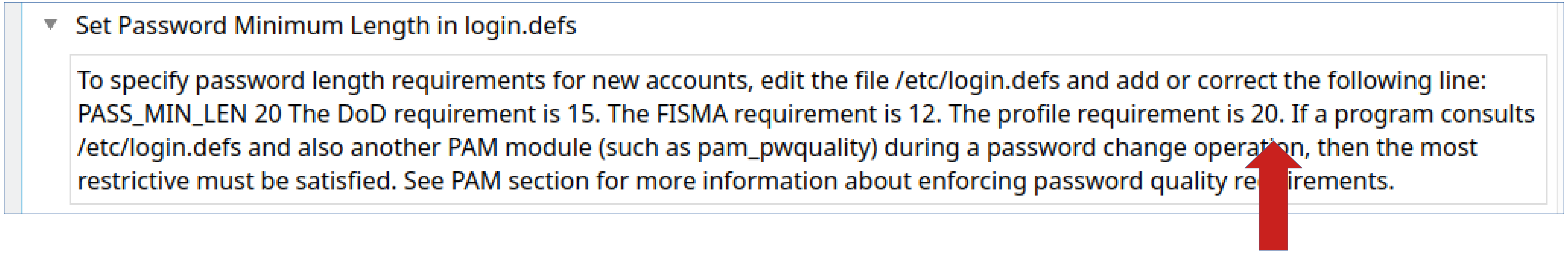
Minimum number of characters in password

Affects Rules

- Set Password Minimum Length in login.defs

Using SCAP Workbench

- Tailored Policy



Set Password Minimum Length in login.defs

To specify password length requirements for new accounts, edit the file /etc/login.defs and add or correct the following line: PASS_MIN_LEN 20 The DoD requirement is 15. The FISMA requirement is 12. The profile requirement is 20. 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.

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.

in linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat