# Security for the Cloud with SCAP

Martin Preisler, Ján Lieskovský

Red Hat, Inc.

# Everything is indeed on fire!

- let’s fight the fires!
- software flaws - vulnerabilities
- configuration flaws - weaknesses

# Vulnerabilities

- **undiscovered vulnerabilities are bad**

But not all that bad, everybody has them.

It’s a lot of effort to use those for exploits.

# Vulnerabilities

- undiscovered vulnerabilities are bad
- **known vulnerabilities are much worse**

CVE-2016-1283

Details are publicly available.

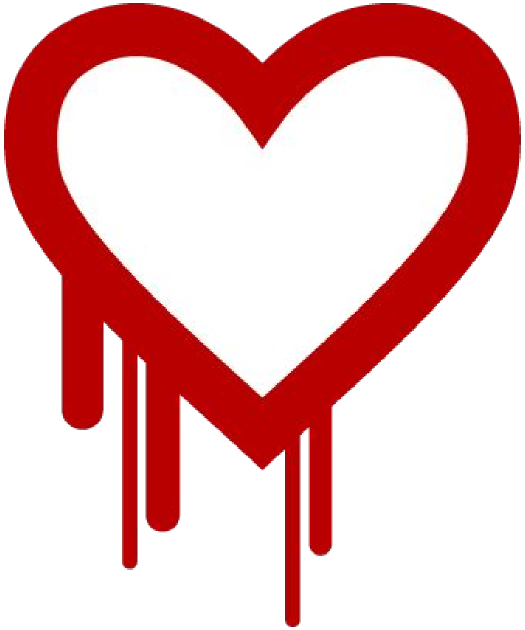
# Vulnerabilities

- undiscovered vulnerabilities are bad
- known vulnerabilities are much worse
- **some are so bad that they have fancy names**

Shellshock, POODLE, VENOM, ...

# Vulnerabilities

- undiscovered vulnerabilities are bad
- known vulnerabilities are much worse
- some are so bad that they have fancy names
- **… and logos**



# Vulnerabilities

- vulnerabilities are dangerous
- nothing we can do about unknown vulnerabilities
- let’s **never** have any **known ones** in our infrastructure!

# We are in the cloud age!

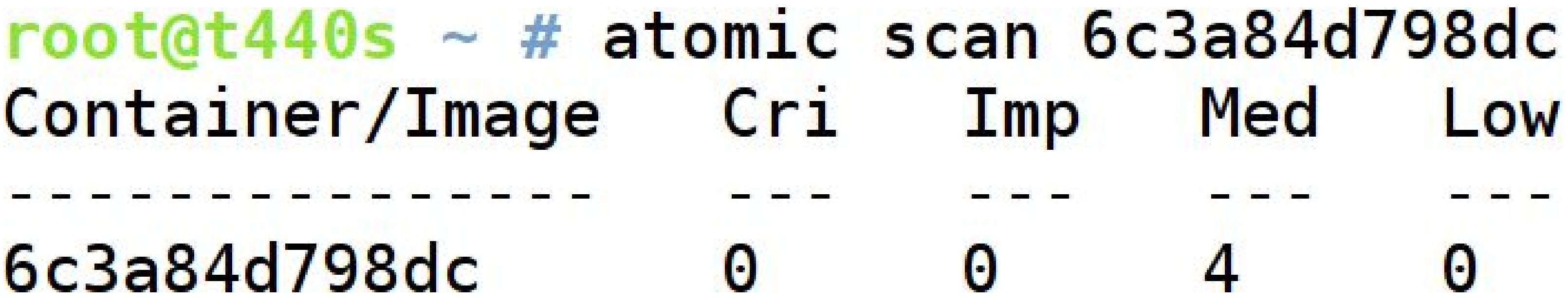
- production deployments are getting complex
- containers are everywhere
- single-purpose containers → many different containers

# We need automation!

Need to automatically check all our containers for vulnerabilities!

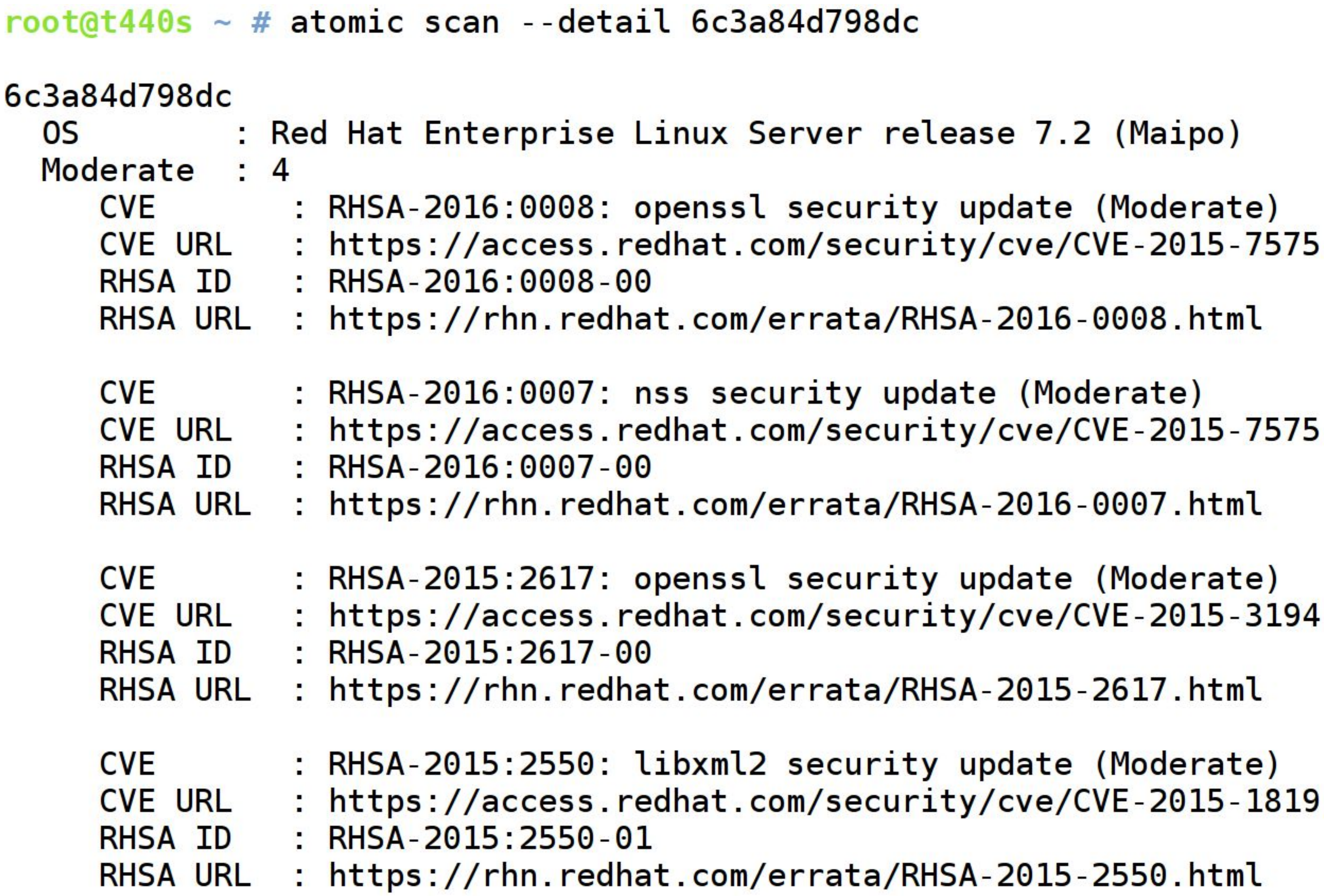
# atomic scan

- new feature in atomic
- scan a container or container image for CVEs
- scan containers or images en masse
- outputs summary, detailed results, json



```
root@t440s ~ # atomic scan 6c3a84d798dc
Container/Image   Cri   Imp   Med   Low
---------------   ---   ---   ---   ---
6c3a84d798dc      0     0     4     0
```

# atomic scan



```
root@t440s ~ # atomic scan --detail 6c3a84d798dc

6c3a84d798dc
  OS          : Red Hat Enterprise Linux Server release 7.2 (Maipo)
  Moderate    : 4
     CVE         : RHSA-2016:0008: openssl security update (Moderate)
     CVE URL     : https://access.redhat.com/security/cve/CVE-2015-7575
     RHSA ID     : RHSA-2016:0008-00
     RHSA URL    : https://rhn.redhat.com/errata/RHSA-2016-0008.html

     CVE         : RHSA-2016:0007: nss security update (Moderate)
     CVE URL     : https://access.redhat.com/security/cve/CVE-2015-7575
     RHSA ID     : RHSA-2016:0007-00
     RHSA URL    : https://rhn.redhat.com/errata/RHSA-2016-0007.html

     CVE         : RHSA-2015:2617: openssl security update (Moderate)
     CVE URL     : https://access.redhat.com/security/cve/CVE-2015-3194
     RHSA ID     : RHSA-2015:2617-00
     RHSA URL    : https://rhn.redhat.com/errata/RHSA-2015-2617.html

     CVE         : RHSA-2015:2550: libxml2 security update (Moderate)
     CVE URL     : https://access.redhat.com/security/cve/CVE-2015-1819
     RHSA ID     : RHSA-2015:2550-01
     RHSA URL    : https://rhn.redhat.com/errata/RHSA-2015-2550.html
```

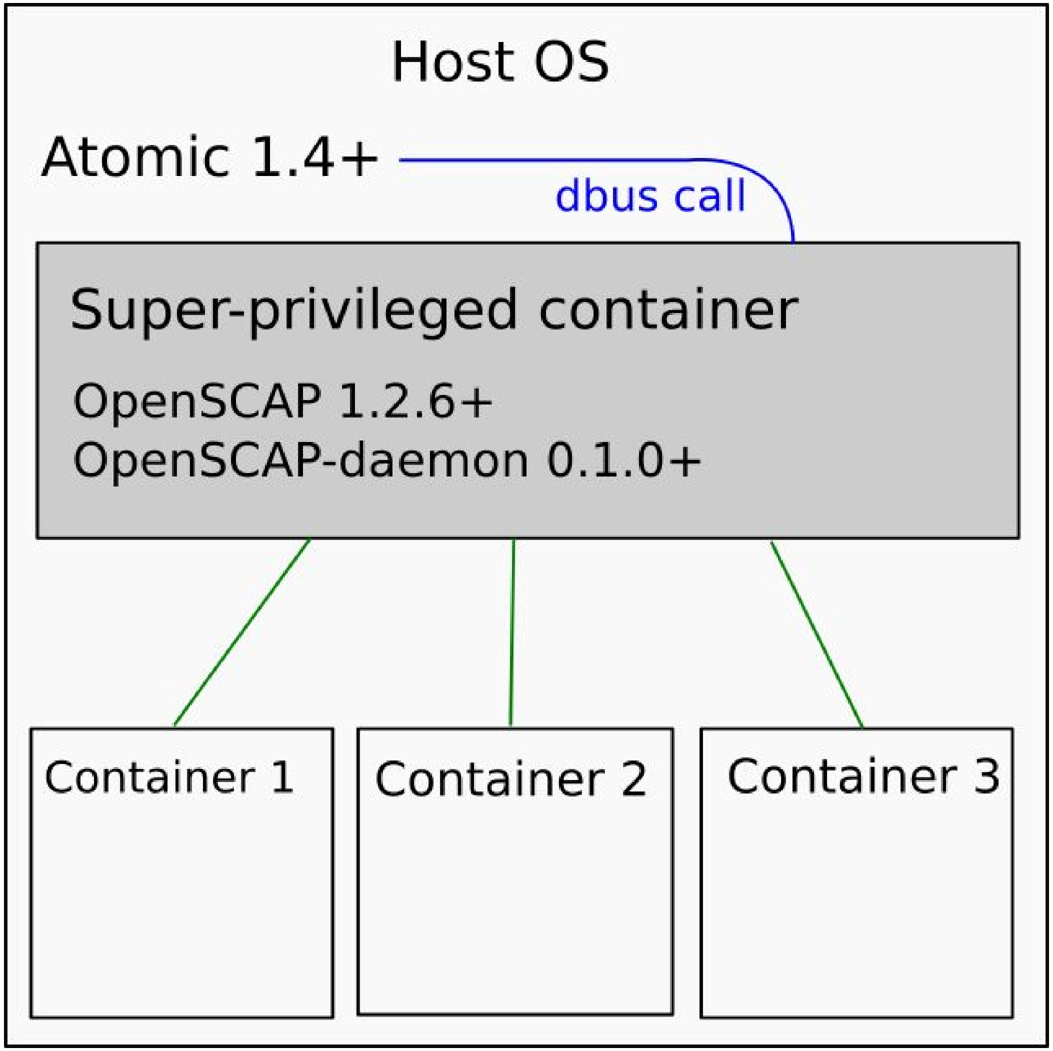
# atomic scan with multiple targets

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

# So… How does this work?

1. detect the OS version
2. get the appropriate CVE feed
3. evaluate with OpenSCAP
4. parse the results

# atomic scan in SPC



# Security?

- security is a very broad term
- secure a system according to a **security policy**
  - **avoid unpatched vulnerable software**
  - get the configuration right - hardening

# Security?

- security is a very broad term
- secure a system according to a **security policy**
  - avoid unpatched vulnerable software
  - **get the configuration right - hardening**

# What is a security policy?

- what it means to secure a system
- set of rules to follow
  - description
  - rationale
  - how to check
  - how to fix
- text - PDF, spreadsheet, …
- very often comes from standard organizations or government bodies
- can be very useful for pro-active security

| PCI DSS Requirements | Testing Procedures | Guidance |
|---|---|---|
| **1.1.5** Description of groups, roles, and responsibilities for management of network components | **1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components. | This description of roles and assignment of responsibilities ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged. |
| | **1.1.5.b** Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented. | |
| **1.1.6** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.<br>Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2. | **1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols. | Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed.<br>If insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed. |
| | **1.1.6.b** Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. | |
| | **1.1.6.c** Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port. | |

# What is SCAP?

- **S**ecurity **C**ontent **A**utomation **P**rotocol
- NIST standard
- express security policies with machine readable code
- several data-formats specified
- XCCDF and OVAL are the main components

## Network Configuration and Firewalls

group

Most machines must be connected to a network of some sort, and this brings with it the substantial risk of network attack. This section discusses the security impact of decisions about networking which must be made when configuring a system.

This section also discusses firewalls, network access controls, and other network security frameworks, which allow system-level rules to be written that can limit an attackers' ability to connect to your system. These rules can specify that network traffic should be allowed or denied from certain IP addresses, hosts, and networks. The rules can also specify which of the system's network services are available to particular hosts or networks.

▼ contains 1 rule

## IPSec Support

group

Support for Internet Protocol Security (IPsec) is provided in Red Hat Enterprise Linux 7 with Libreswan.

▼ contains 1 rule

### Install libreswan Package

rule

The Libreswan package provides an implementation of IPsec and IKE, which permits the creation of secure tunnels over untrusted networks. The `libreswan` package can be installed with the following command:

```
$ sudo yum install libreswan
```

**Rationale:**

Providing the ability for remote users or systems to initiate a secure VPN connection protects information when it is transmitted over a wide area network.

**identifiers:** CCE-RHEL7-CCE-TBD

**references:** AC-17, MA-4, SC-9, 1130, 1131, Req-4

**Remediation script:**

```
yum -y install libreswan
```

# Two types of SCAP security policies

- **Vulnerability Assessment**
- detect CVEs
- Heartbleed
- Shellshock
- Ghost
- VENOM
- ...

- **Security Compliance**
- proper configuration
- USGCB
- DISA STIG
- PCI DSS
- ...

# Two main use-cases

- **Vulnerability Assessment**
- are my machines vulnerable?
  - to Heartbleed?
  - to Shellshock?
  - to Ghost?
  - to VENOM?
  - ...

- **Security Compliance**
- is root login over ssh forbidden?
- is /tmp on a separate partition?
- are we using strict password policy?
- no obsolete/insecure services?
  - telnet, rsh
- ...

# OpenSCAP

- SCAP 1.2 implementation
- stable and mature project, started by Red Hat in 2009
- certified by NIST since 2014
- open source - LGPL 2.1+
- library and a command-line tool
- GUI frontend - SCAP Workbench
- https://www.open-scap.org/

OpenSCAP BASE

SCAP WORKBENCH

# Scanning a single machine

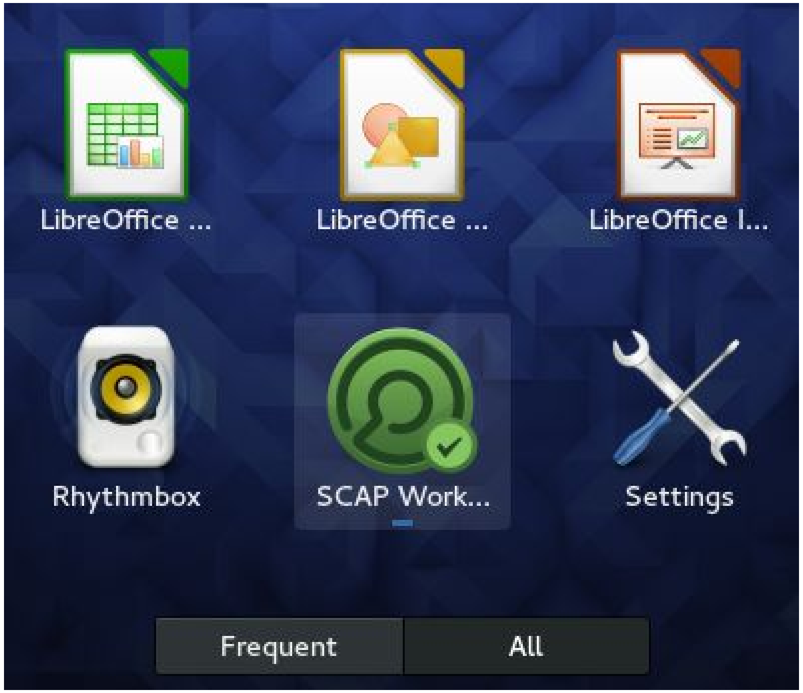
- Fedora 23
- OpenSCAP + SCAP Workbench
- Common profile from SCAP Security Guide

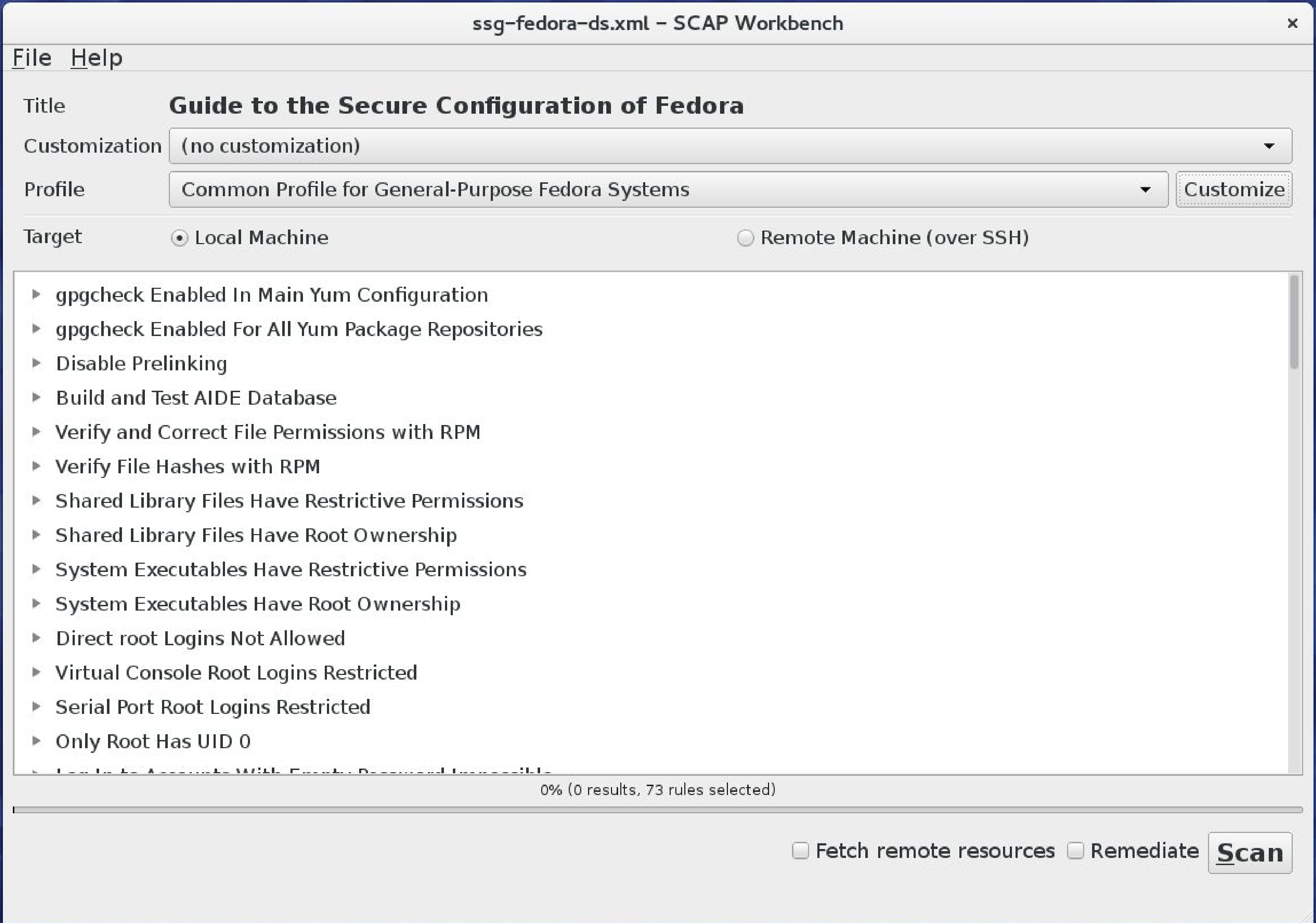
# Install and start SCAP Workbench

(Assuming Fedora 23)

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

```
$ scap-workbench
```





ssg-fedora-ds.xml – SCAP Workbench

Title: Guide to the Secure Configuration of Fedora

Customization: (no customization)

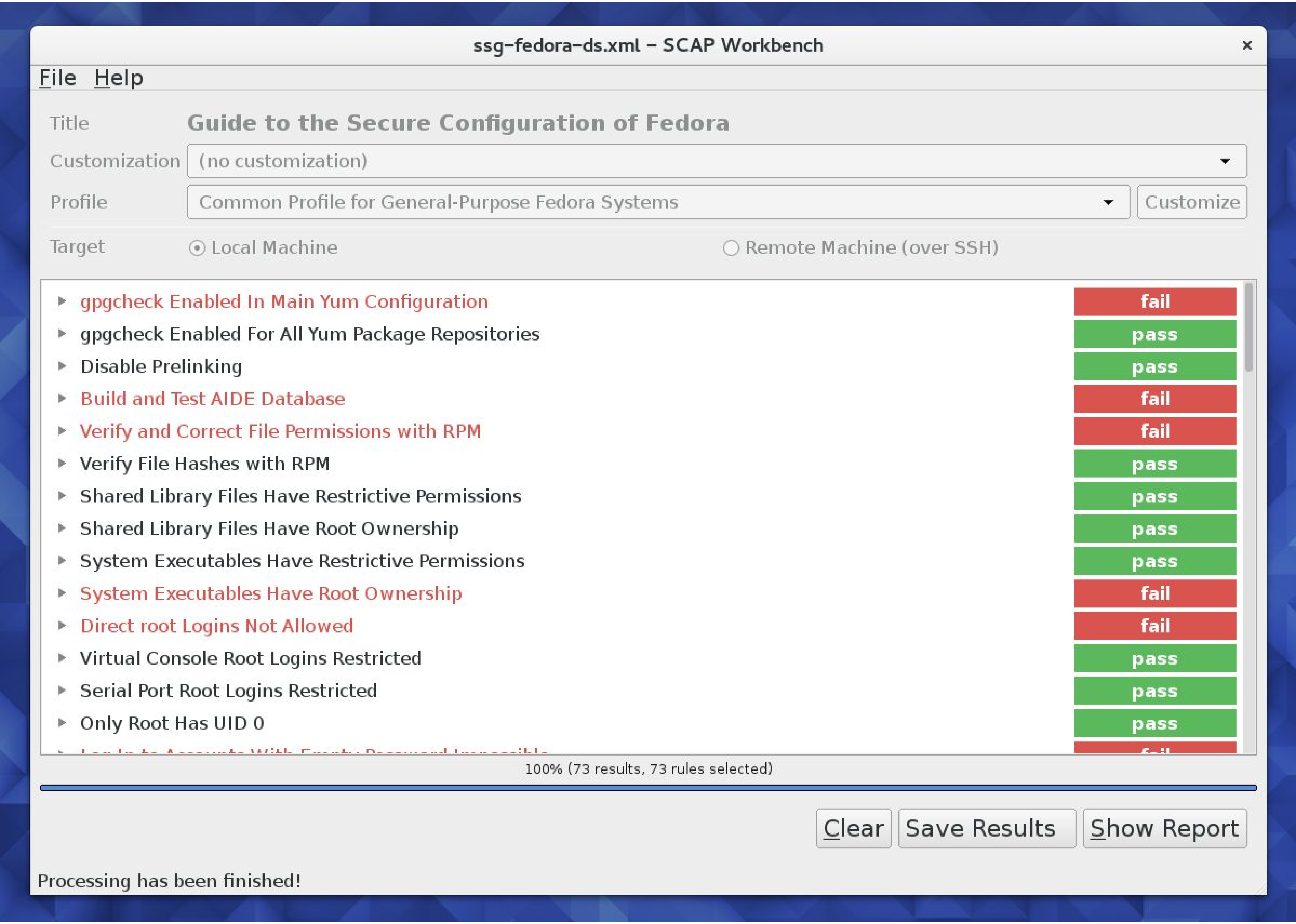
Profile: Common Profile for General-Purpose Fedora Systems

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

- gpgcheck Enabled In Main Yum Configuration
- gpgcheck Enabled For All Yum Package Repositories
- Disable Prelinking
- Build and Test AIDE Database
- Verify and Correct File Permissions with RPM
- Verify File Hashes with RPM
- Shared Library Files Have Restrictive Permissions
- Shared Library Files Have Root Ownership
- System Executables Have Restrictive Permissions
- System Executables Have Root Ownership
- Direct root Logins Not Allowed
- Virtual Console Root Logins Restricted
- Serial Port Root Logins Restricted
- Only Root Has UID 0
- Log In to Accounts With Empty Password Impossible

0% (0 results, 73 rules selected)

□ Fetch remote resources □ Remediate



Title: Guide to the Secure Configuration of Fedora

Customization: (no customization)

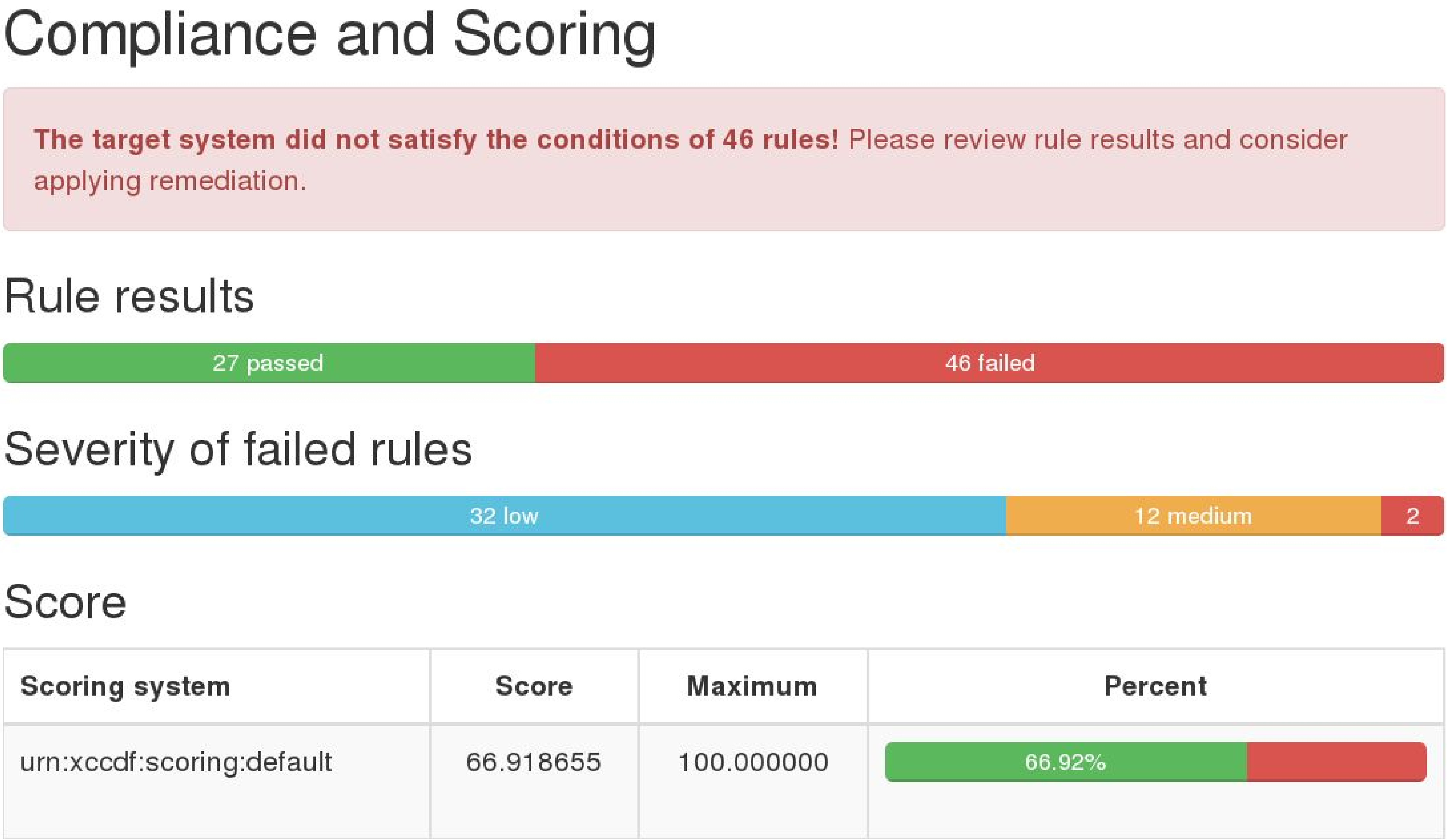
Profile: Common Profile for General-Purpose Fedora Systems

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

| | |
|---|---|
| ▸ gpgcheck Enabled In Main Yum Configuration | fail |
| ▸ gpgcheck Enabled For All Yum Package Repositories | pass |
| ▸ Disable Prelinking | pass |
| ▸ Build and Test AIDE Database | fail |
| ▸ Verify and Correct File Permissions with RPM | fail |
| ▸ Verify File Hashes with RPM | pass |
| ▸ Shared Library Files Have Restrictive Permissions | pass |
| ▸ Shared Library Files Have Root Ownership | pass |
| ▸ System Executables Have Restrictive Permissions | pass |
| ▸ System Executables Have Root Ownership | fail |
| ▸ Direct root Logins Not Allowed | fail |
| ▸ Virtual Console Root Logins Restricted | pass |
| ▸ Serial Port Root Logins Restricted | pass |
| ▸ Only Root Has UID 0 | pass |
| ▸ Log In to Accounts With Empty Password Impossible | fail |

100% (73 results, 73 rules selected)

Processing has been finished!



# Compliance and Scoring

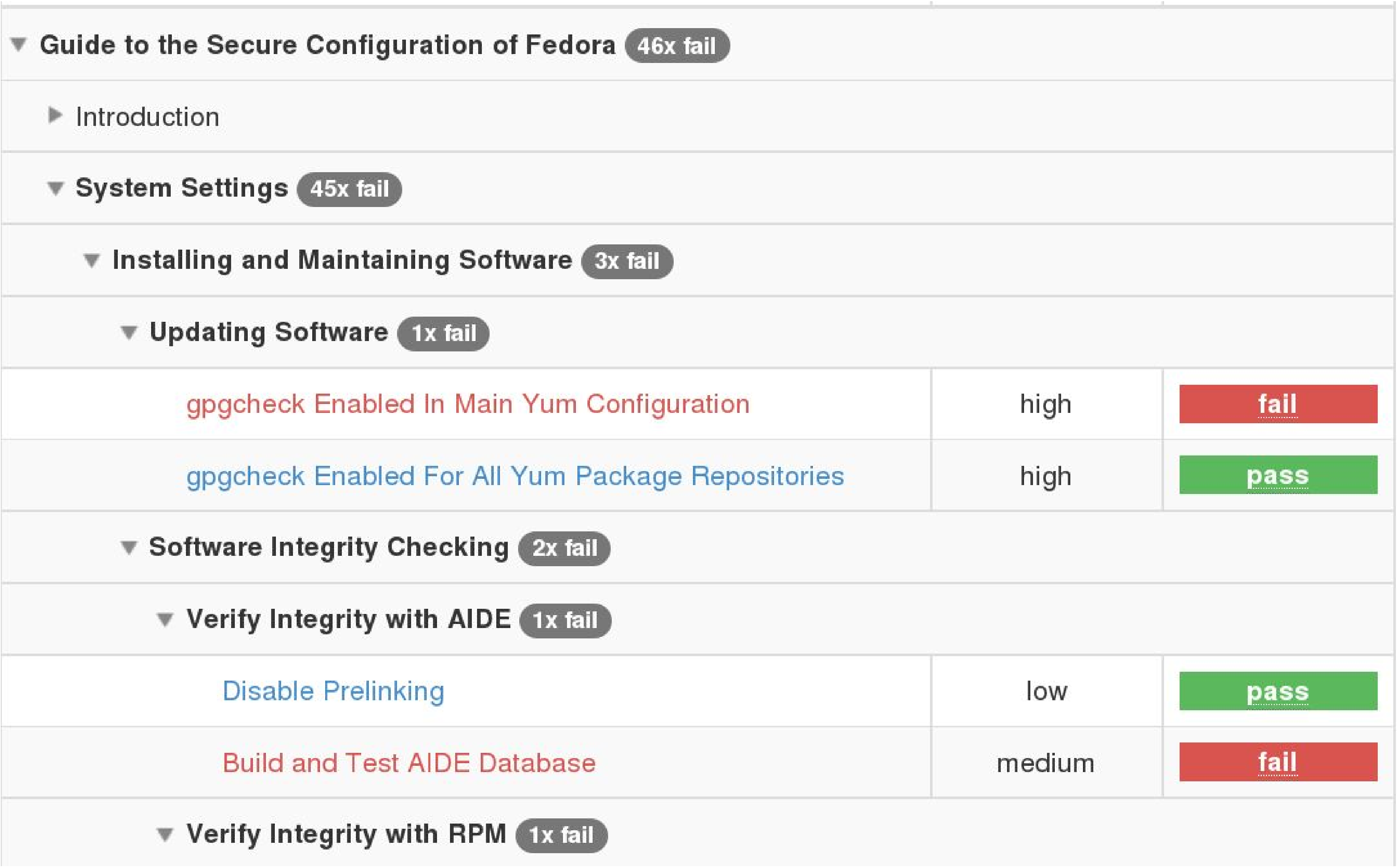
**The target system did not satisfy the conditions of 46 rules!** Please review rule results and consider applying remediation.

## Rule results

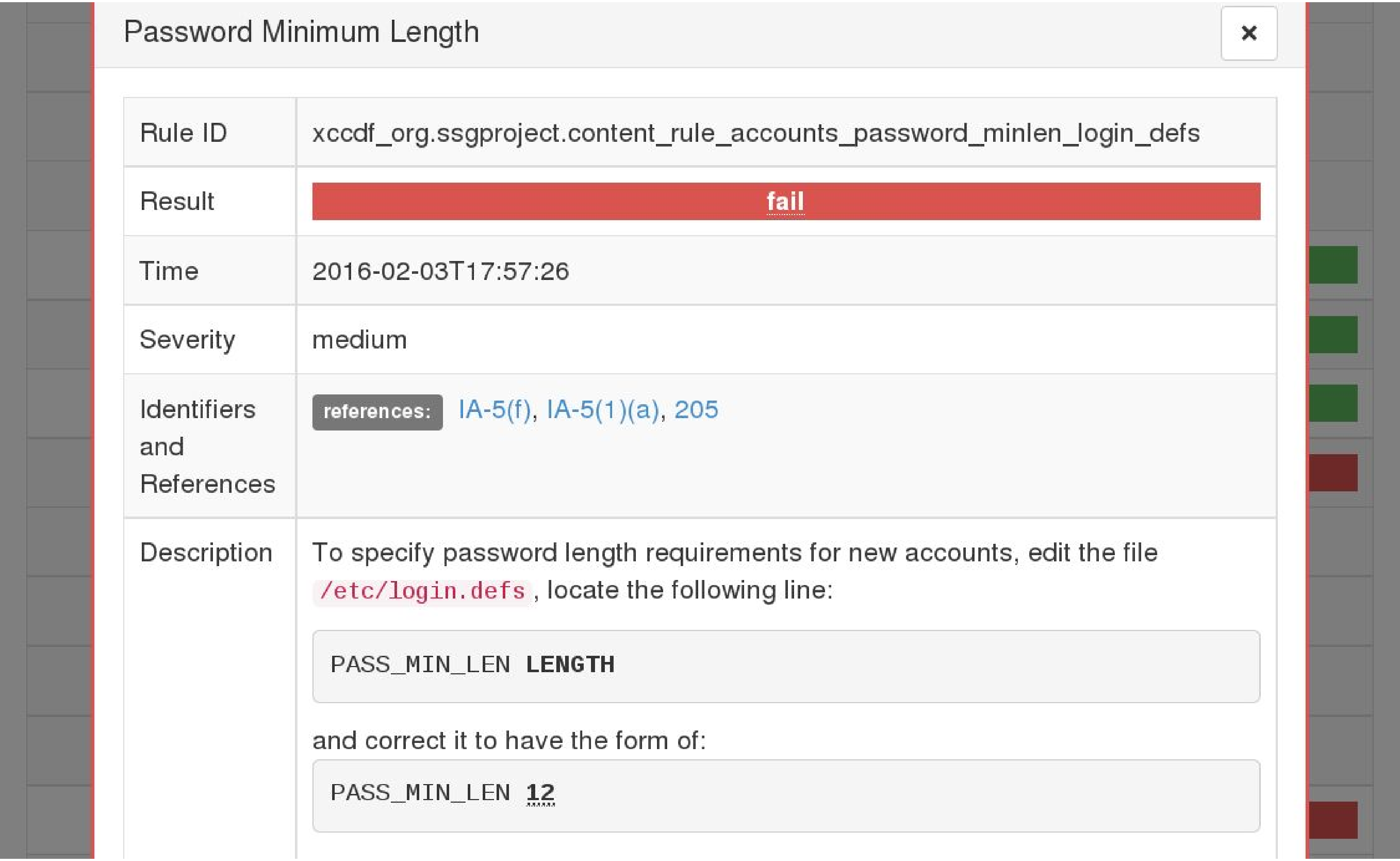
## Severity of failed rules

## Score

| Scoring system | Score | Maximum | Percent |
|---|---|---|---|
| urn:xccdf:scoring:default | 66.918655 | 100.000000 | 66.92% |

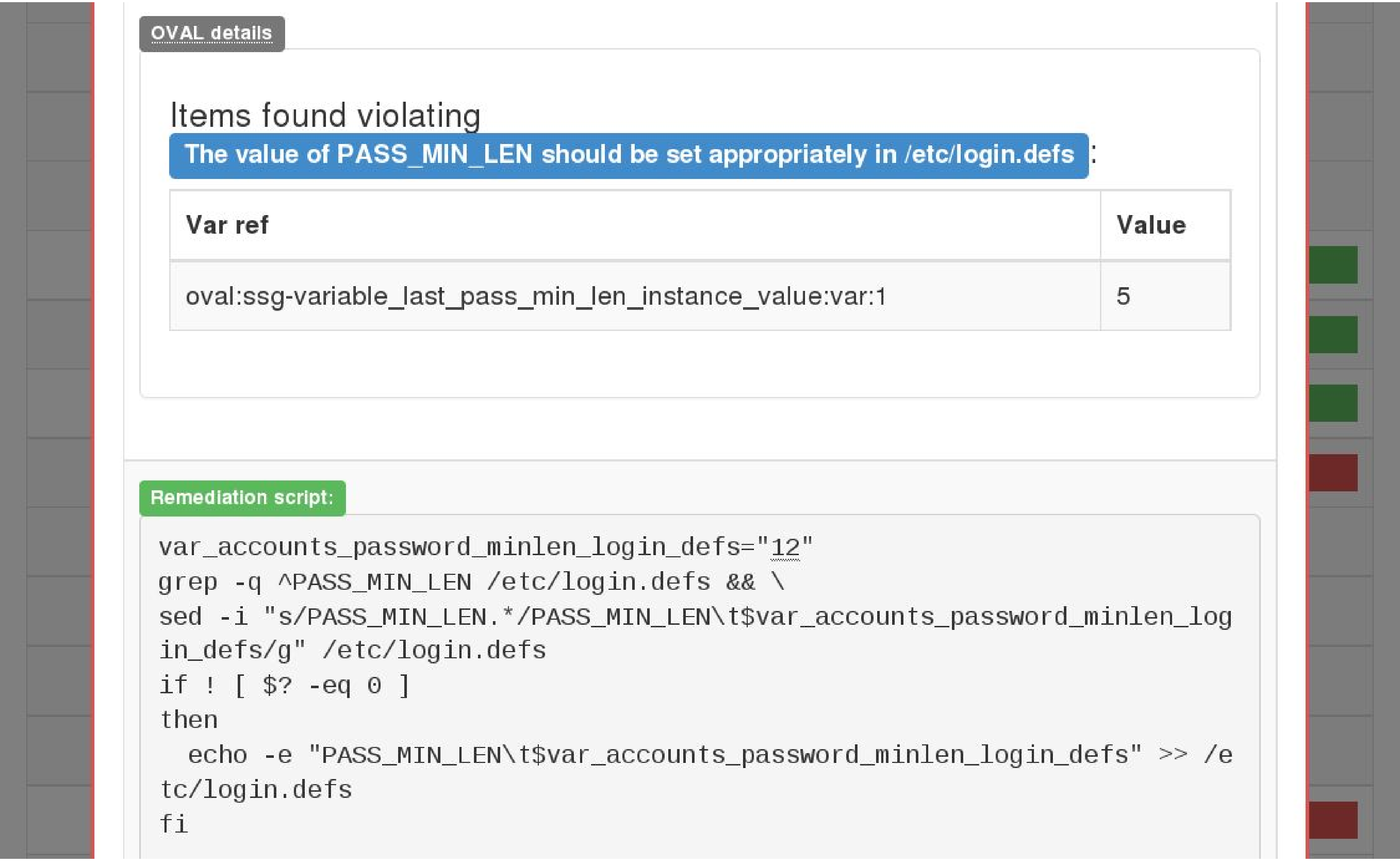


| | | |
|---|---|---|
| ▼ **Guide to the Secure Configuration of Fedora** 46x fail | | |
| ▶ Introduction | | |
| ▼ **System Settings** 45x fail | | |
| ▼ **Installing and Maintaining Software** 3x fail | | |
| ▼ **Updating Software** 1x fail | | |
| gpgcheck Enabled In Main Yum Configuration | high | fail |
| gpgcheck Enabled For All Yum Package Repositories | high | pass |
| ▼ **Software Integrity Checking** 2x fail | | |
| ▼ **Verify Integrity with AIDE** 1x fail | | |
| Disable Prelinking | low | pass |
| Build and Test AIDE Database | medium | fail |
| ▼ **Verify Integrity with RPM** 1x fail | | |



## Password Minimum Length

| | |
|---|---|
| Rule ID | xccdf_org.ssgproject.content_rule_accounts_password_minlen_login_defs |
| Result | fail |
| Time | 2016-02-03T17:57:26 |
| Severity | medium |
| Identifiers and References | references: IA-5(f), IA-5(1)(a), 205 |
| Description | To specify password length requirements for new accounts, edit the file `/etc/login.defs`, locate the following line:<br>`PASS_MIN_LEN LENGTH`<br>and correct it to have the form of:<br>`PASS_MIN_LEN 12` |



OVAL details

Items found violating

The value of PASS_MIN_LEN should be set appropriately in /etc/login.defs:

| Var ref | Value |
|---|---|
| oval:ssg-variable_last_pass_min_len_instance_value:var:1 | 5 |

Remediation script:

```
var_accounts_password_minlen_login_defs="12"
grep -q ^PASS_MIN_LEN /etc/login.defs && \
sed -i "s/PASS_MIN_LEN.*/PASS_MIN_LEN\t$var_accounts_password_minlen_login_defs/g" /etc/login.defs
if ! [ $? -eq 0 ]
then
  echo -e "PASS_MIN_LEN\t$var_accounts_password_minlen_login_defs" >> /etc/login.defs
fi
```

# Why the need for security policies?

- Linux distributions are multi-purpose (classroom workstation vs HPC server vs airport laptop)
- High-level 3rd-party standards (e.g. PCI DSS) vs concrete hardening steps
- Desire for automation

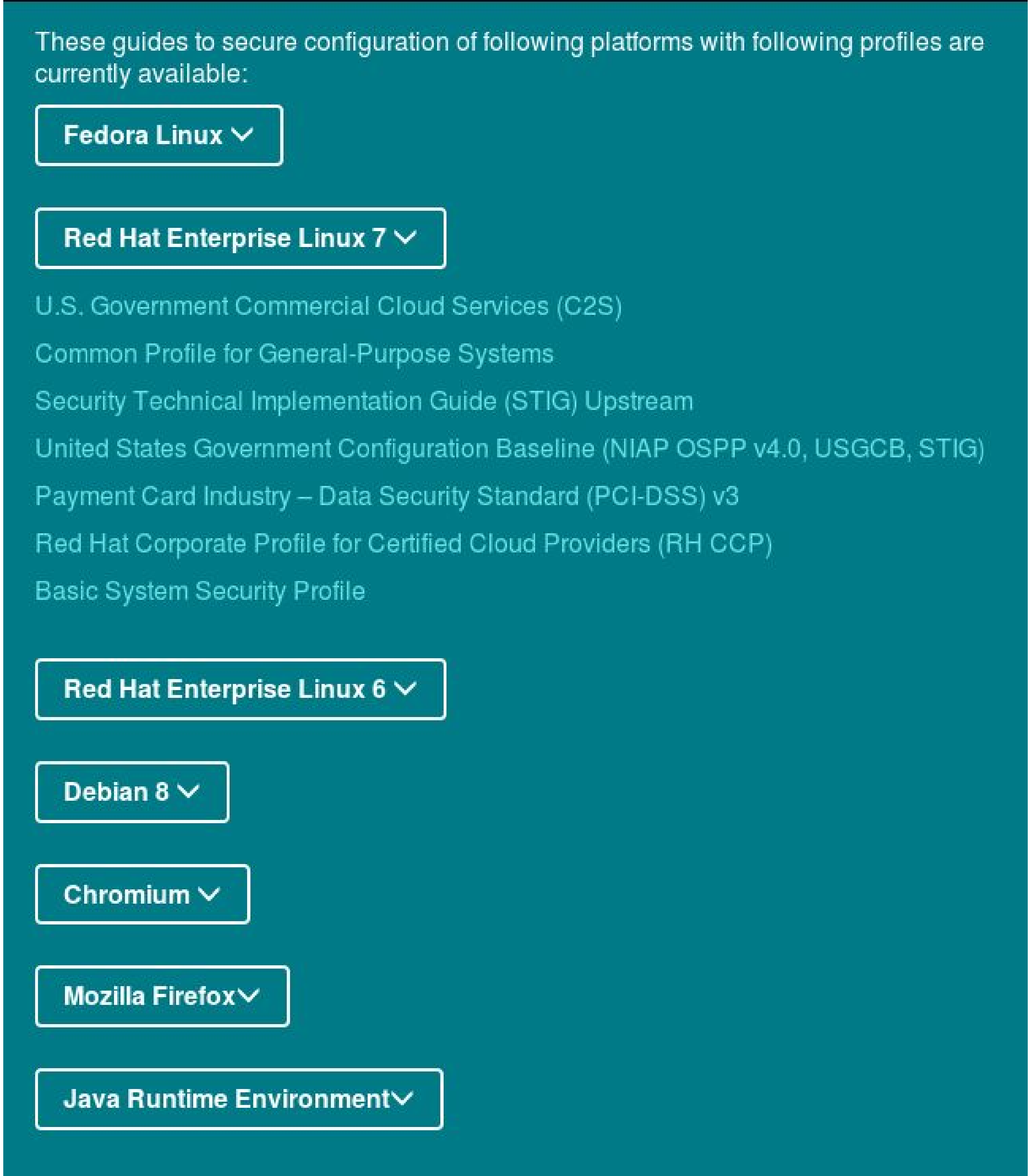
# Introducing SCAP Security Guide (SSG)

- Suite of policies expressed in SCAP format
- Suitable for both:
  - Machines (XML, ARF)
  - Humans (HTML)

# Introducing SCAP Security Guide (SSG)

- Provides all content necessary for automated assessment of systems
- Community project
- Open source - public domain

SCAP
SECURITY GUIDE



These guides to secure configuration of following platforms with following profiles are currently available:

**Fedora Linux**

**Red Hat Enterprise Linux 7**

U.S. Government Commercial Cloud Services (C2S)

Common Profile for General-Purpose Systems

Security Technical Implementation Guide (STIG) Upstream

United States Government Configuration Baseline (NIAP OSPP v4.0, USGCB, STIG)

Payment Card Industry – Data Security Standard (PCI-DSS) v3

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

Basic System Security Profile

**Red Hat Enterprise Linux 6**

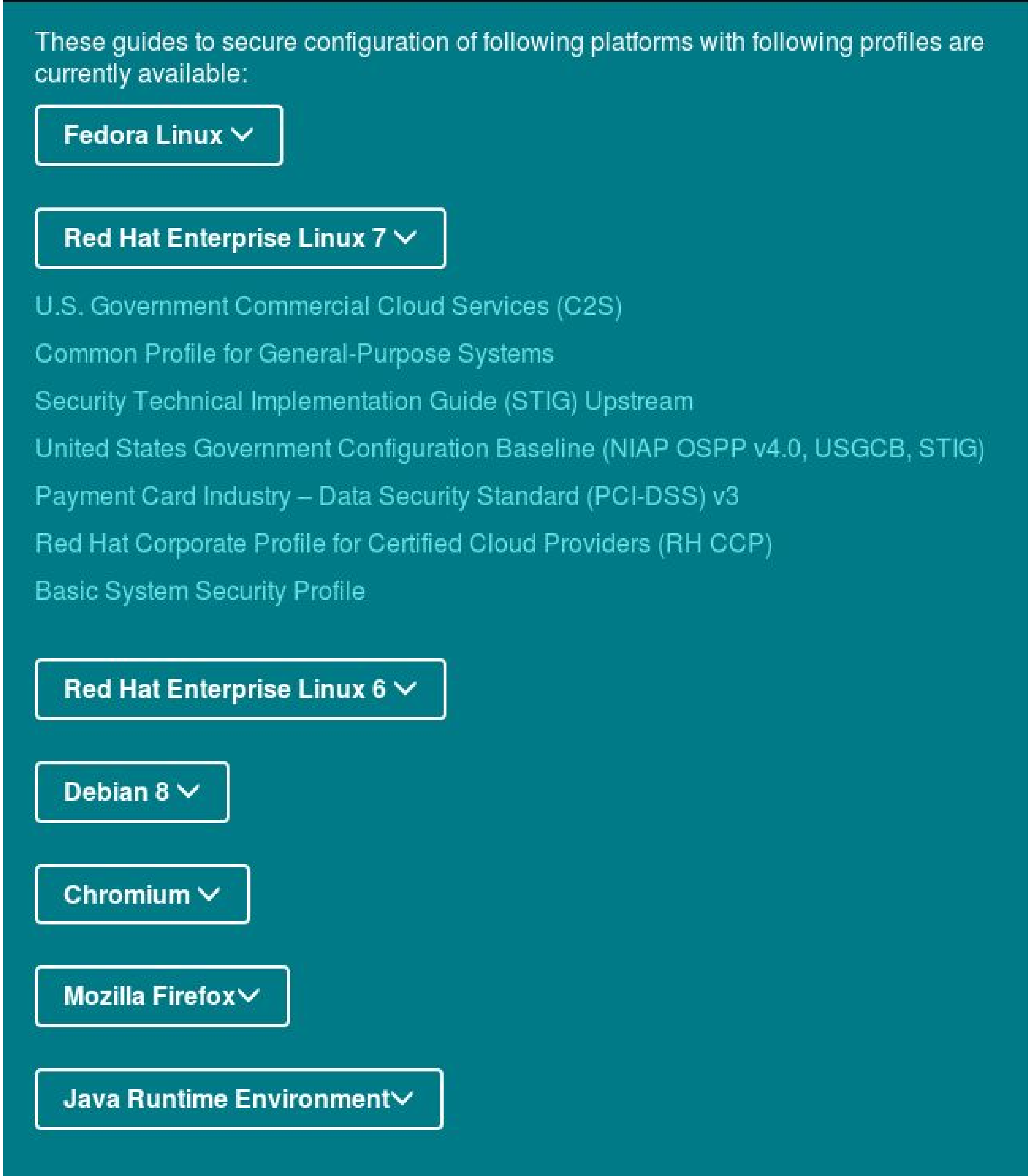
**Debian 8**

**Chromium**

**Mozilla Firefox**

**Java Runtime Environment**

Missing some?



These guides to secure configuration of following platforms with following profiles are currently available:

Fedora Linux

Red Hat Enterprise Linux 7

U.S. Government Commercial Cloud Services (C2S)

Common Profile for General-Purpose Systems

Security Technical Implementation Guide (STIG) Upstream

United States Government Configuration Baseline (NIAP OSPP v4.0, USGCB, STIG)

Payment Card Industry – Data Security Standard (PCI-DSS) v3

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

Basic System Security Profile

Red Hat Enterprise Linux 6

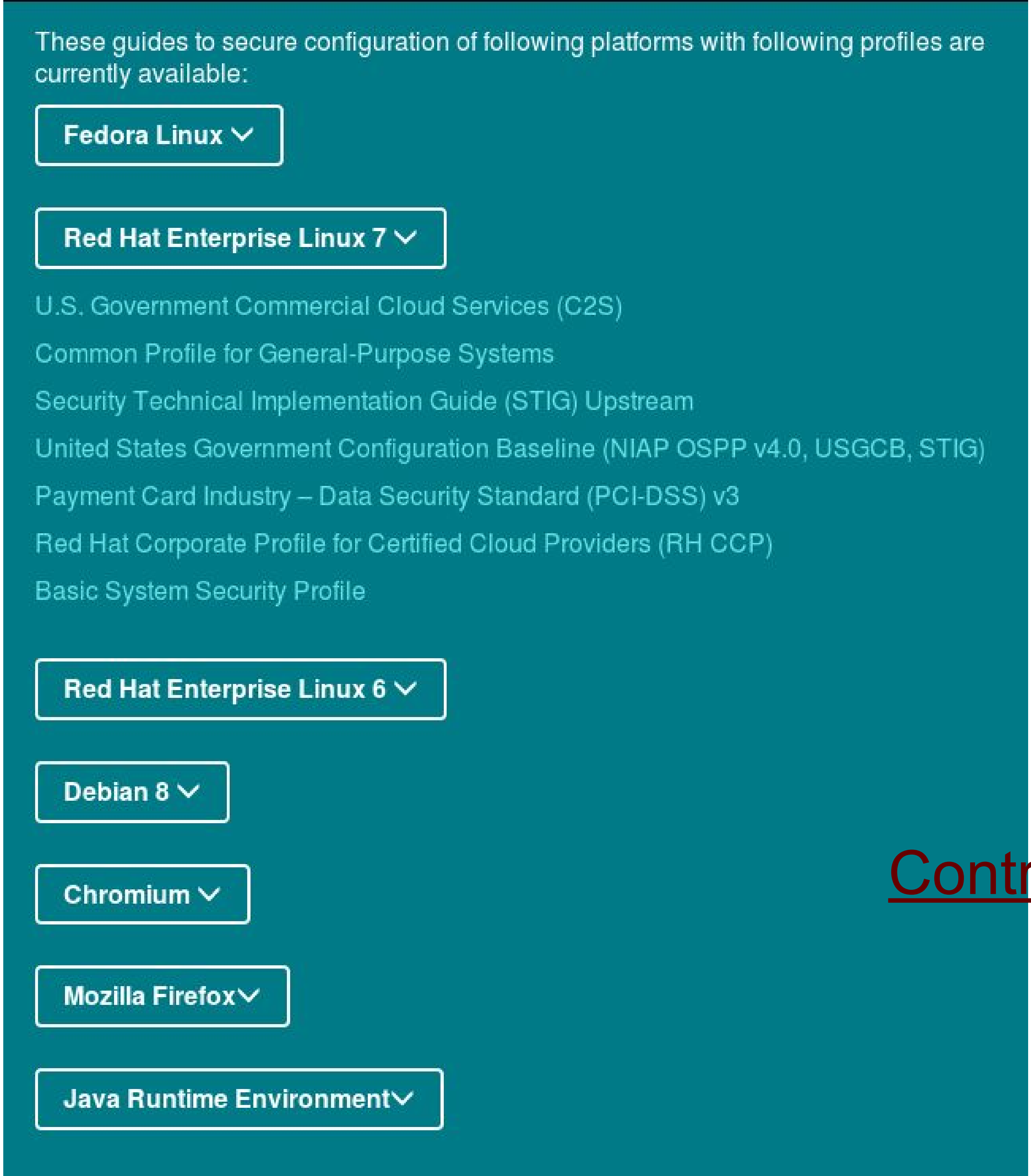
Debian 8

Chromium

Mozilla Firefox

Java Runtime Environment

Missing some?



These guides to secure configuration of following platforms with following profiles are currently available:

U.S. Government Commercial Cloud Services (C2S)

Common Profile for General-Purpose Systems

Security Technical Implementation Guide (STIG) Upstream

United States Government Configuration Baseline (NIAP OSPP v4.0, USGCB, STIG)

Payment Card Industry – Data Security Standard (PCI-DSS) v3

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

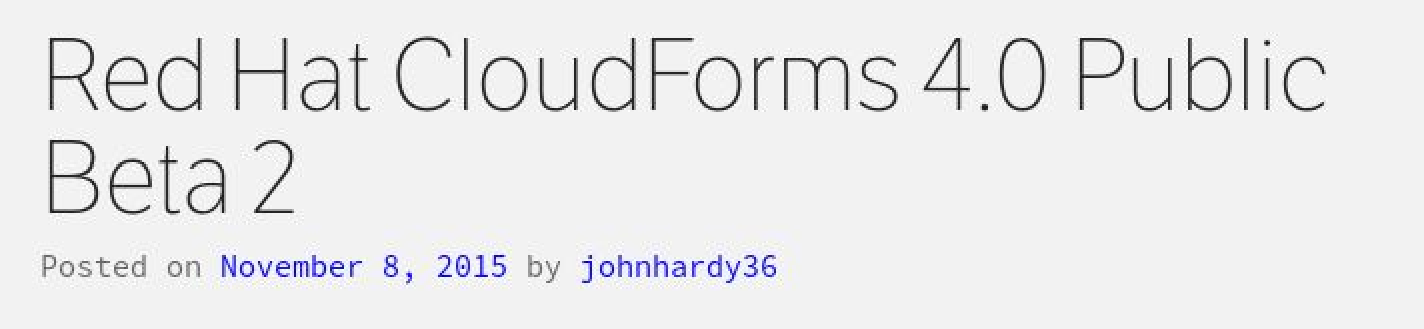
Basic System Security Profile

Contribute!!!

# Meet security policies

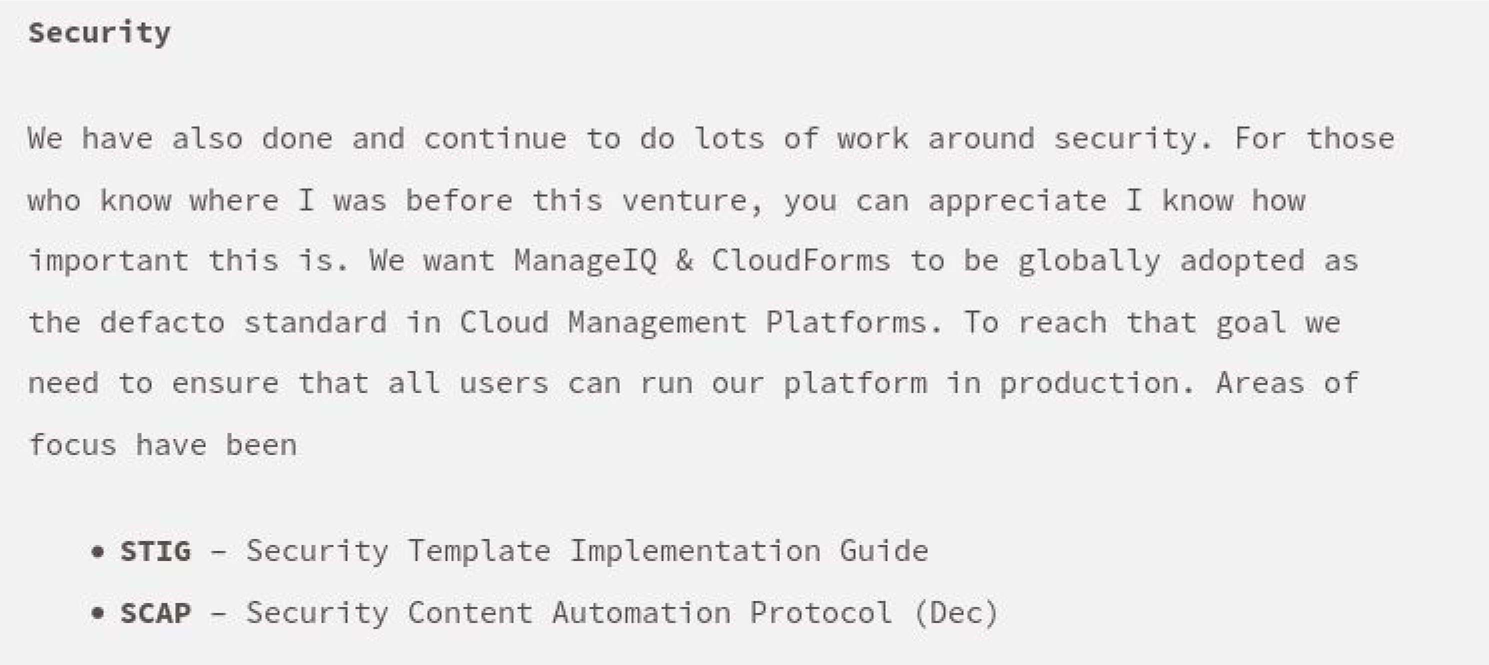
- Bad news
- Good news

# Meet security policies (in the clouds)



## Red Hat CloudForms 4.0 Public Beta 2

Posted on November 8, 2015 by johnhardy36

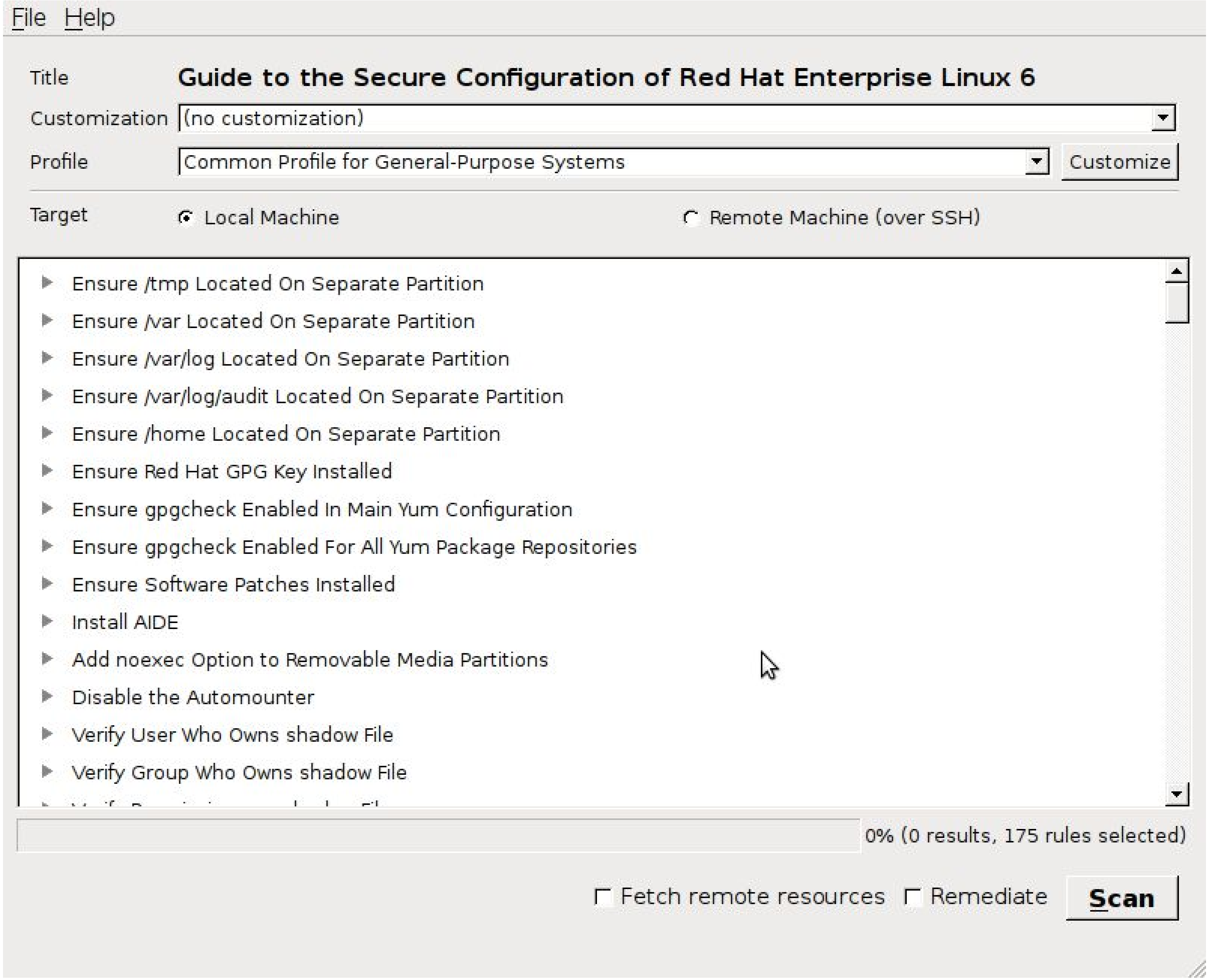


**Security**

We have also done and continue to do lots of work around security. For those who know where I was before this venture, you can appreciate I know how important this is. We want ManageIQ & CloudForms to be globally adopted as the defacto standard in Cloud Management Platforms. To reach that goal we need to ensure that all users can run our platform in production. Areas of focus have been

- **STIG** – Security Template Implementation Guide
- **SCAP** – Security Content Automation Protocol (Dec)

# Meet security policies (on localhost)



Title: Guide to the Secure Configuration of Red Hat Enterprise Linux 6

Customization: (no customization)

Profile: Common Profile for General-Purpose Systems

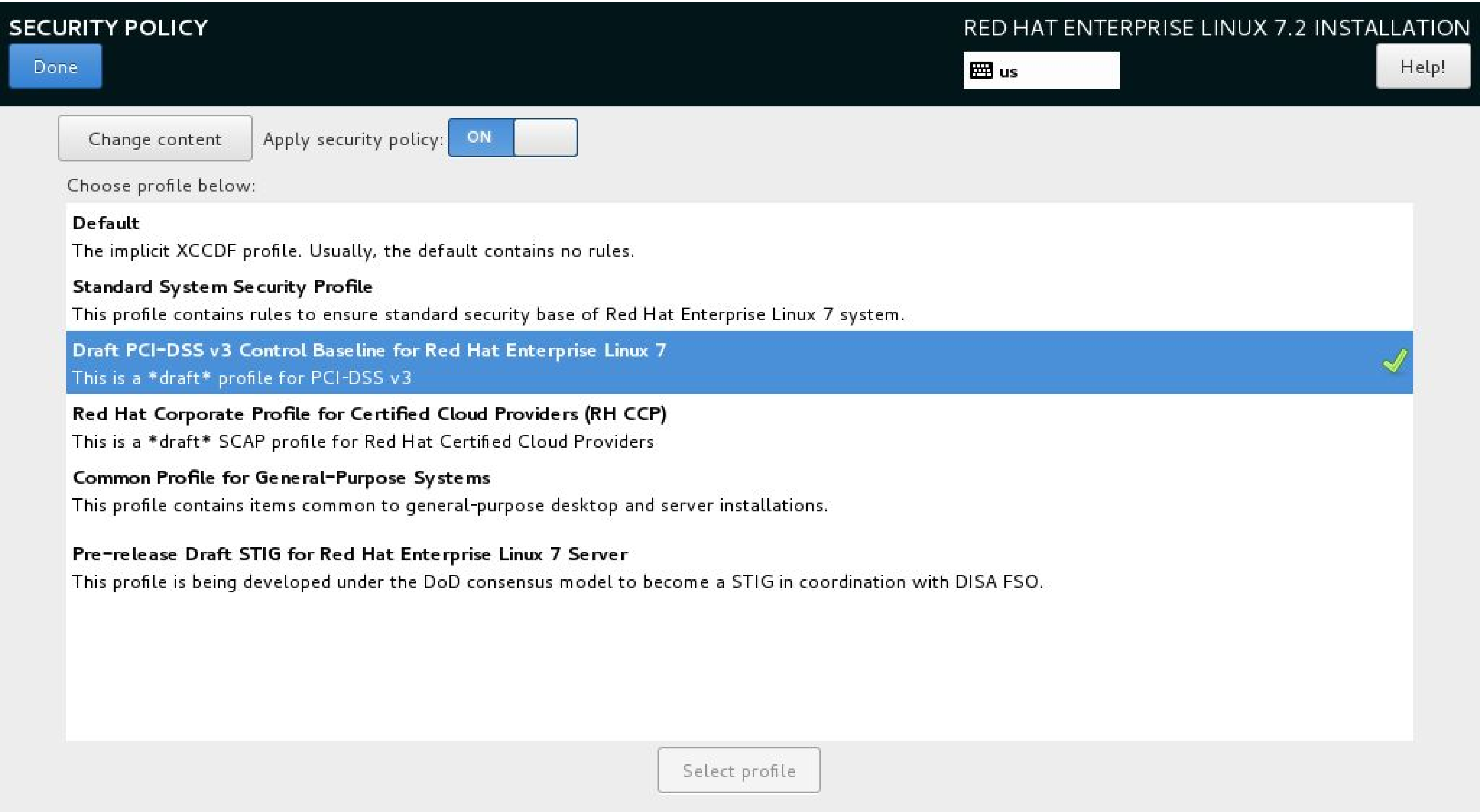
Target: ● Local Machine ○ Remote Machine (over SSH)

- Ensure /tmp Located On Separate Partition
- Ensure /var Located On Separate Partition
- Ensure /var/log Located On Separate Partition
- Ensure /var/log/audit Located On Separate Partition
- Ensure /home Located On Separate Partition
- Ensure Red Hat GPG Key Installed
- Ensure gpgcheck Enabled In Main Yum Configuration
- Ensure gpgcheck Enabled For All Yum Package Repositories
- Ensure Software Patches Installed
- Install AIDE
- Add noexec Option to Removable Media Partitions
- Disable the Automounter
- Verify User Who Owns shadow File
- Verify Group Who Owns shadow File

0% (0 results, 175 rules selected)

☐ Fetch remote resources ☐ Remediate

# Meet security policies (during OS install)



Apply security policy: ON

Choose profile below:

**Default**
The implicit XCCDF profile. Usually, the default contains no rules.

**Standard System Security Profile**
This profile contains rules to ensure standard security base of Red Hat Enterprise Linux 7 system.

**Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7** ✓
This is a *draft* profile for PCI-DSS v3

**Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)**
This is a *draft* SCAP profile for Red Hat Certified Cloud Providers

**Common Profile for General-Purpose Systems**
This profile contains items common to general-purpose desktop and server installations.

**Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server**
This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

# Meet security policies (during OS install)

```
...
%addon org_fedora_oscap
     content-type = scap-security-guide
     profile = pci-dss
%end
...
```

# Firefox policy preview

| Policy Example #1 |
|---|
| Disable SSL Version 2.0  in Firefox |
| Disable SSL Version 3.0 in Firefox |
| Enable TLS Usage in Firefox |
| .. |

# Firefox policy preview

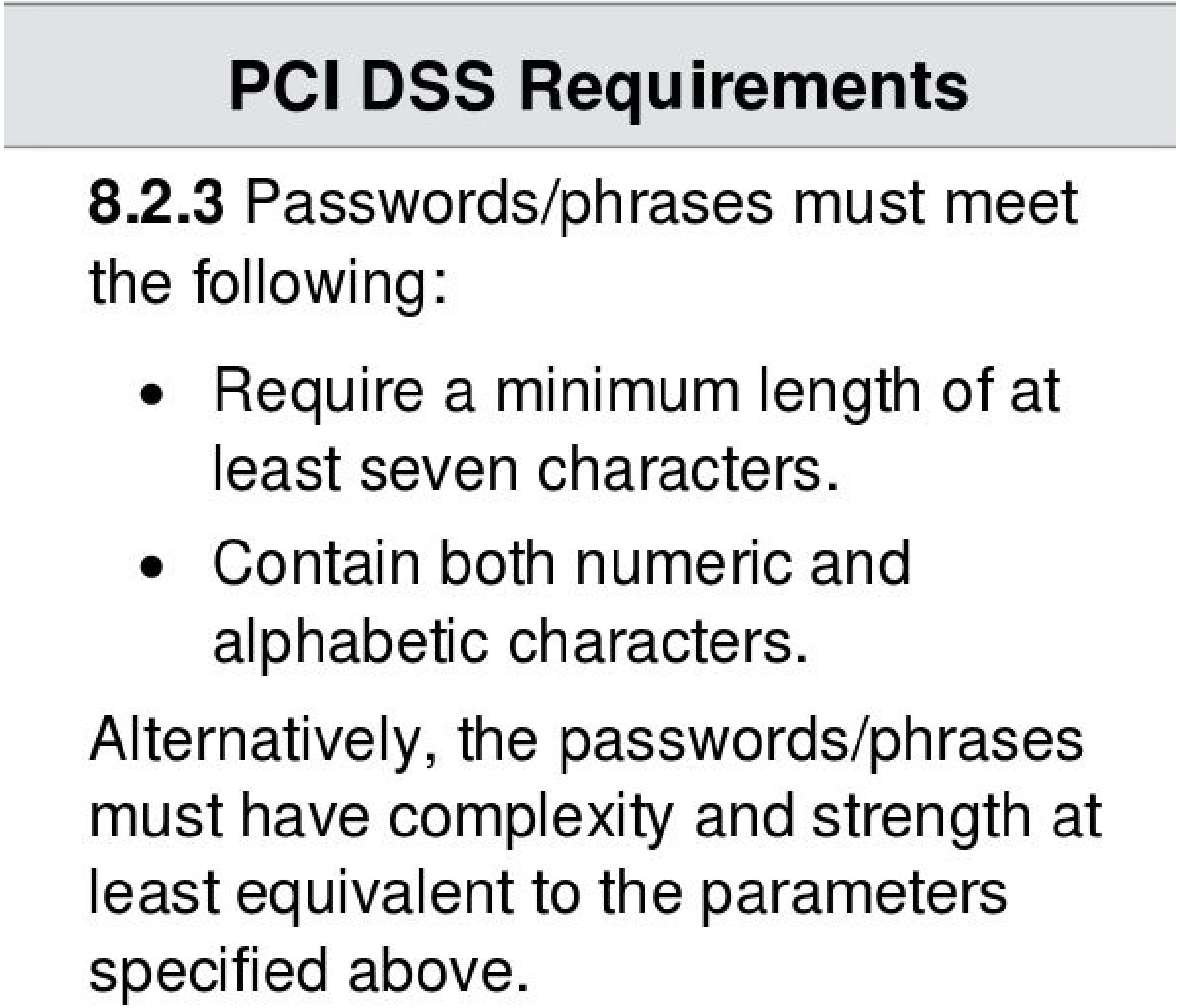
| Policy Example #2 |
|---|
| Enable Certificate Validation |
| .. |

# Firefox policy preview

| Policy Example #3 |
|---|
| Enable Firefox Pop-up Blocker |
| .. |

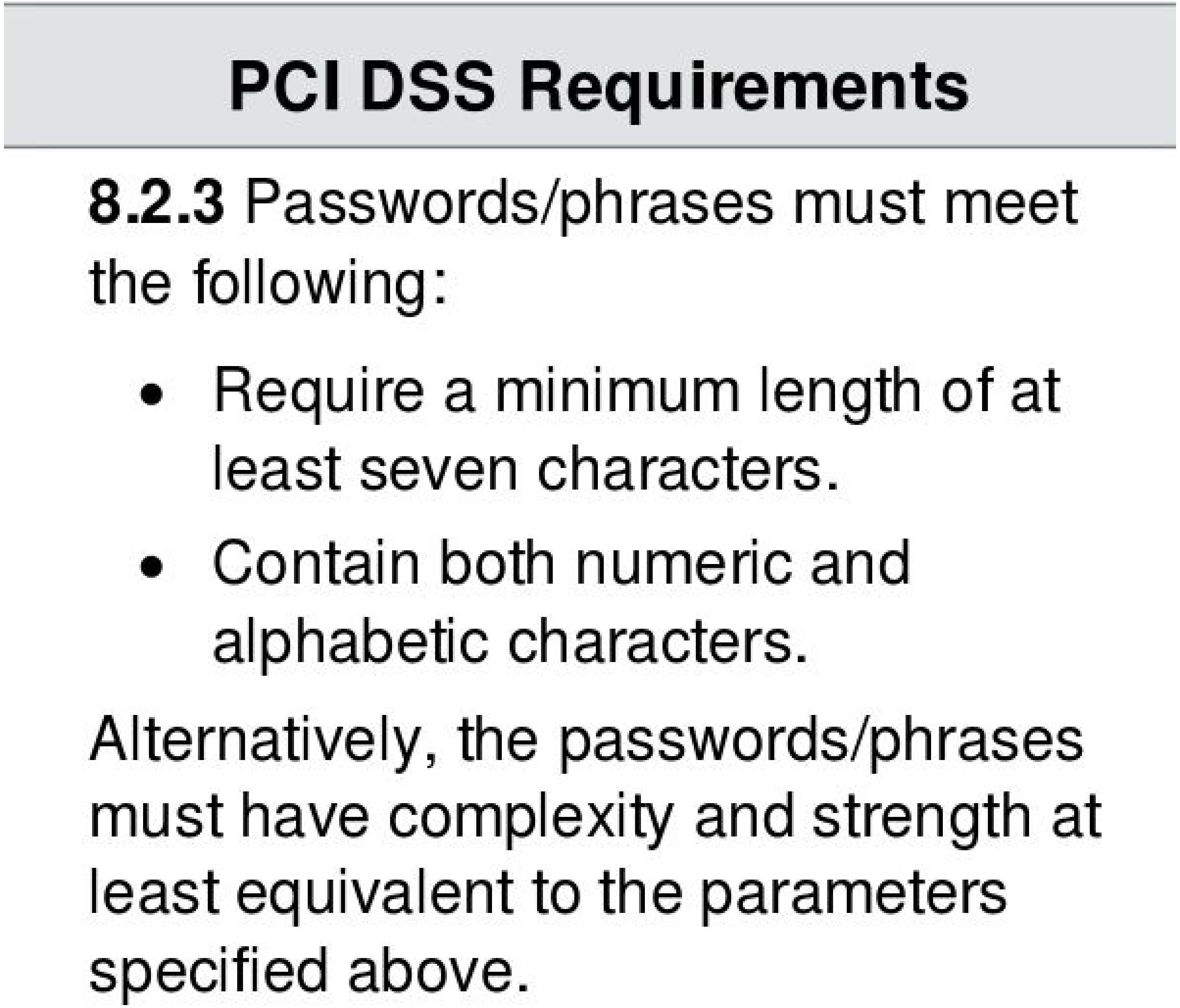
How were these policies created?

# Why to customize policy?



| PCI DSS Requirements |
|---|
| **8.2.3** Passwords/phrases must meet the following:<br>• Require a minimum length of at least seven characters.<br>• Contain both numeric and alphabetic characters.<br>Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above. |

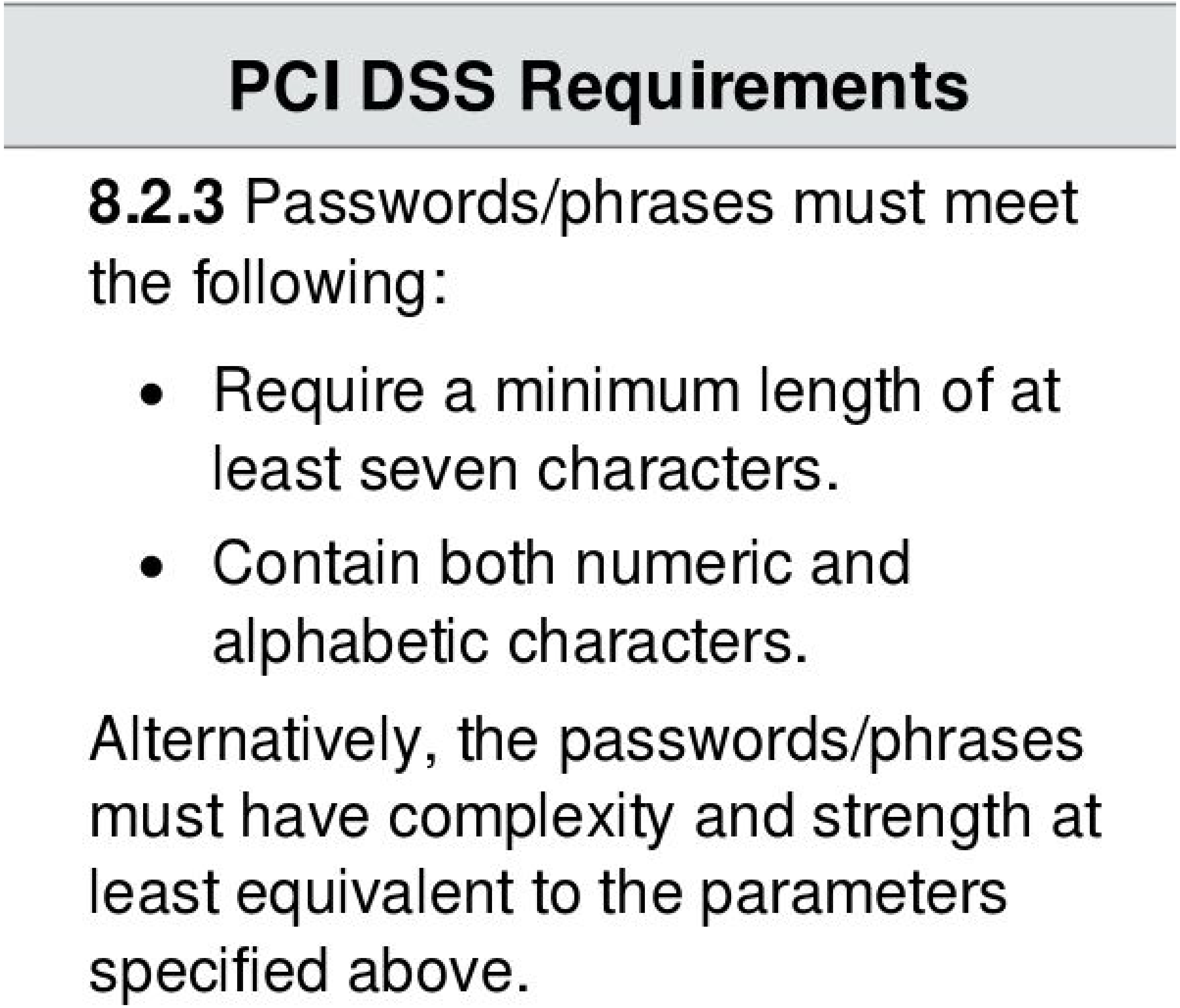
# Why to customize policy?



| PCI DSS Requirements |
|---|
| **8.2.3** Passwords/phrases must meet the following:<br>• Require a minimum length of at least seven characters.<br>• Contain both numeric and alphabetic characters.<br>Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above. |

- **To strengthen (weaken) the existing policy!**

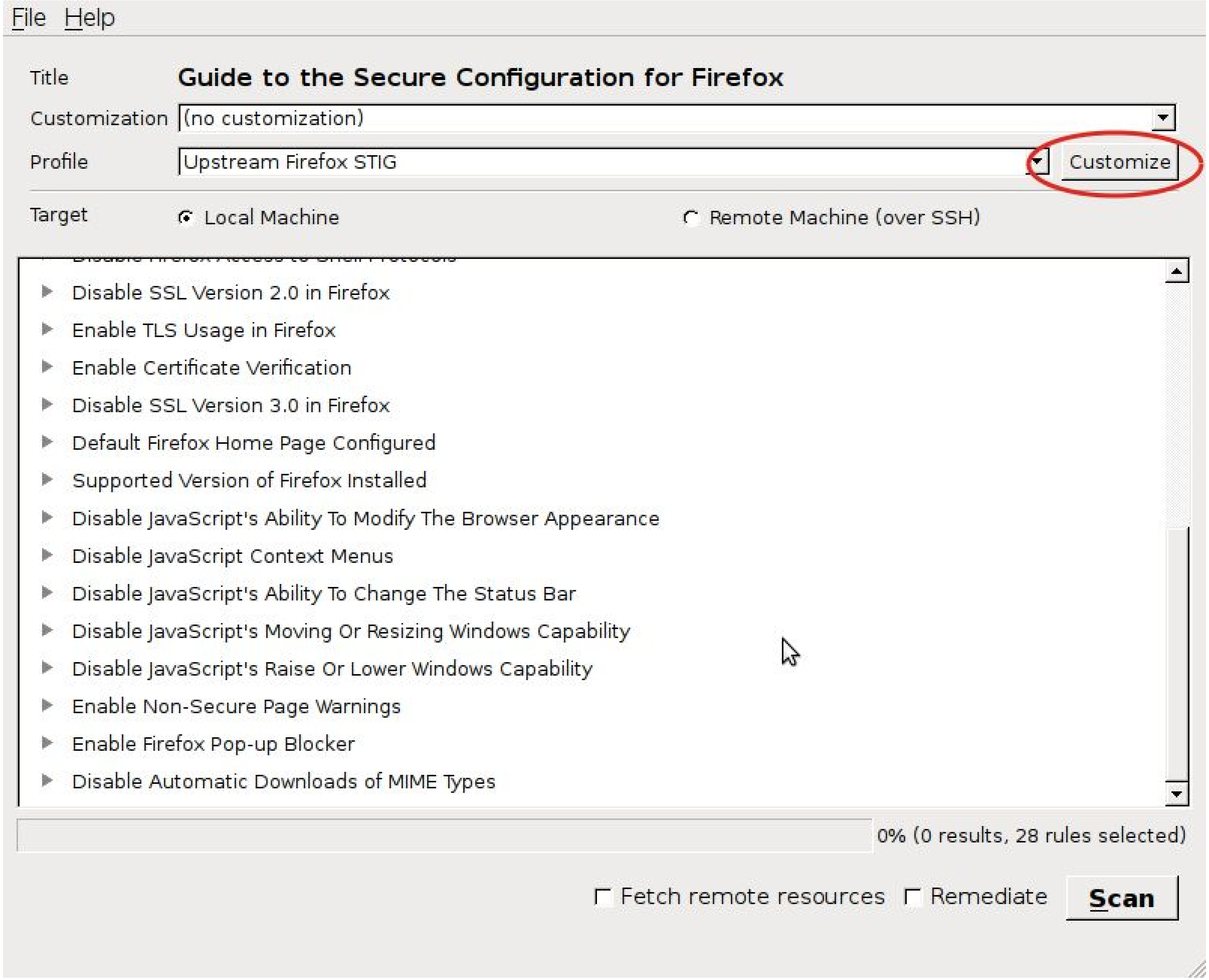
# Why to customize policy?



| PCI DSS Requirements |
|---|
| **8.2.3** Passwords/phrases must meet the following:<br>• Require a minimum length of at least seven characters.<br>• Contain both numeric and alphabetic characters.<br>Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above. |

- **To create own one!**

# Customizing policies



Title: Guide to the Secure Configuration for Firefox

Customization: (no customization)

Profile: Upstream Firefox STIG

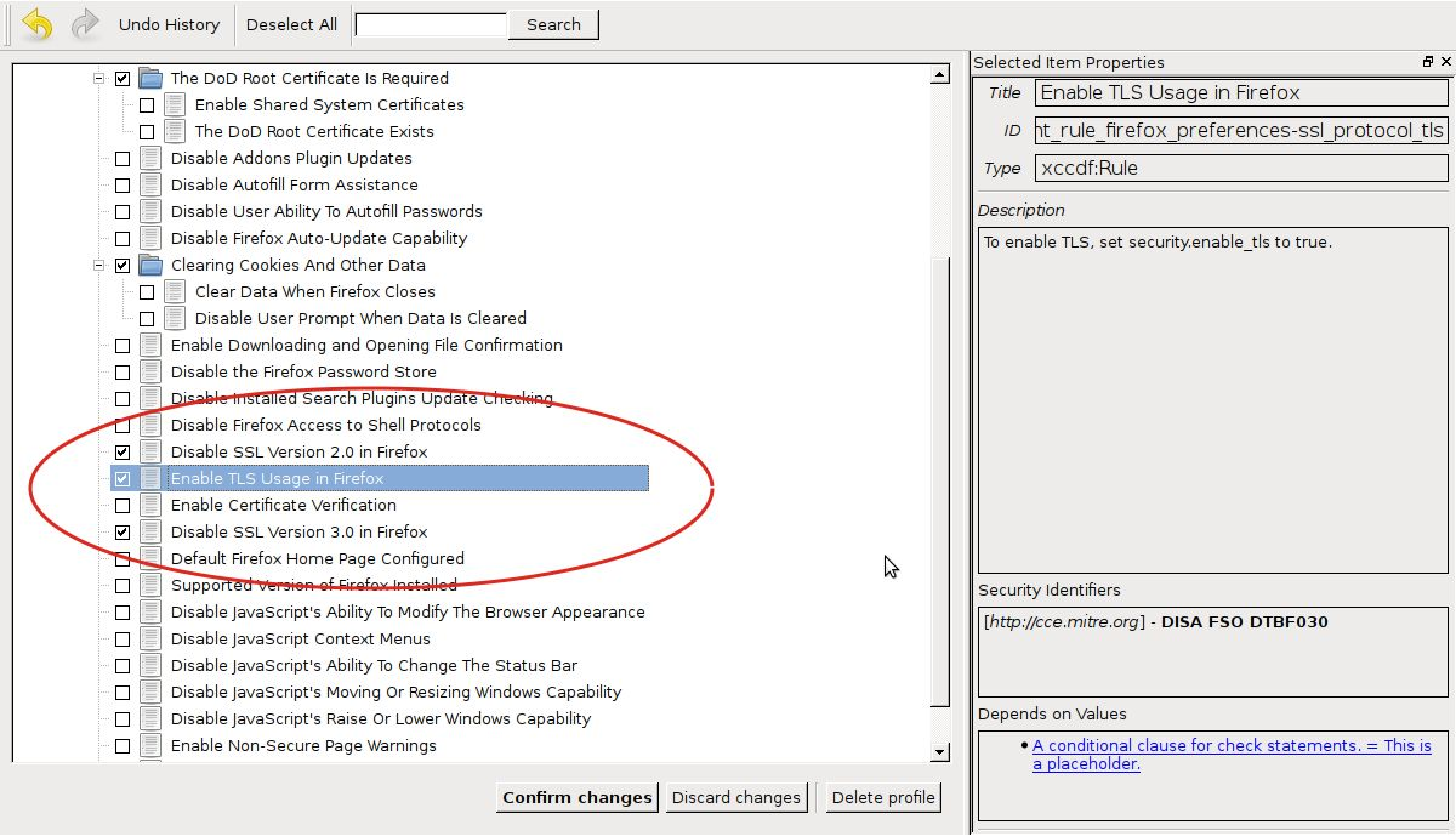
Target: ● Local Machine ○ Remote Machine (over SSH)

- Disable Firefox Access to Shell Protocols
- Disable SSL Version 2.0 in Firefox
- Enable TLS Usage in Firefox
- Enable Certificate Verification
- Disable SSL Version 3.0 in Firefox
- Default Firefox Home Page Configured
- Supported Version of Firefox Installed
- Disable JavaScript's Ability To Modify The Browser Appearance
- Disable JavaScript Context Menus
- Disable JavaScript's Ability To Change The Status Bar
- Disable JavaScript's Moving Or Resizing Windows Capability
- Disable JavaScript's Raise Or Lower Windows Capability
- Enable Non-Secure Page Warnings
- Enable Firefox Pop-up Blocker
- Disable Automatic Downloads of MIME Types

0% (0 results, 28 rules selected)

□ Fetch remote resources □ Remediate

# Customizing policies #2



- ☑ The DoD Root Certificate Is Required
  - ☐ Enable Shared System Certificates
  - ☐ The DoD Root Certificate Exists
- ☐ Disable Addons Plugin Updates
- ☐ Disable Autofill Form Assistance
- ☐ Disable User Ability To Autofill Passwords
- ☐ Disable Firefox Auto-Update Capability
- ☑ Clearing Cookies And Other Data
  - ☐ Clear Data When Firefox Closes
  - ☐ Disable User Prompt When Data Is Cleared
- ☐ Enable Downloading and Opening File Confirmation
- ☐ Disable the Firefox Password Store
- ☐ Disable Installed Search Plugins Update Checking
- ☐ Disable Firefox Access to Shell Protocols
- ☑ Disable SSL Version 2.0 in Firefox
- ☑ Enable TLS Usage in Firefox
- ☐ Enable Certificate Verification
- ☑ Disable SSL Version 3.0 in Firefox
- ☐ Default Firefox Home Page Configured
- ☐ Supported Version of Firefox Installed
- ☐ Disable JavaScript's Ability To Modify The Browser Appearance
- ☐ Disable JavaScript Context Menus
- ☐ Disable JavaScript's Ability To Change The Status Bar
- ☐ Disable JavaScript's Moving Or Resizing Windows Capability
- ☐ Disable JavaScript's Raise Or Lower Windows Capability
- ☐ Enable Non-Secure Page Warnings

Selected Item Properties

*Title* Enable TLS Usage in Firefox

*ID* nt_rule_firefox_preferences-ssl_protocol_tls

*Type* xccdf:Rule

*Description*

To enable TLS, set security.enable_tls to true.

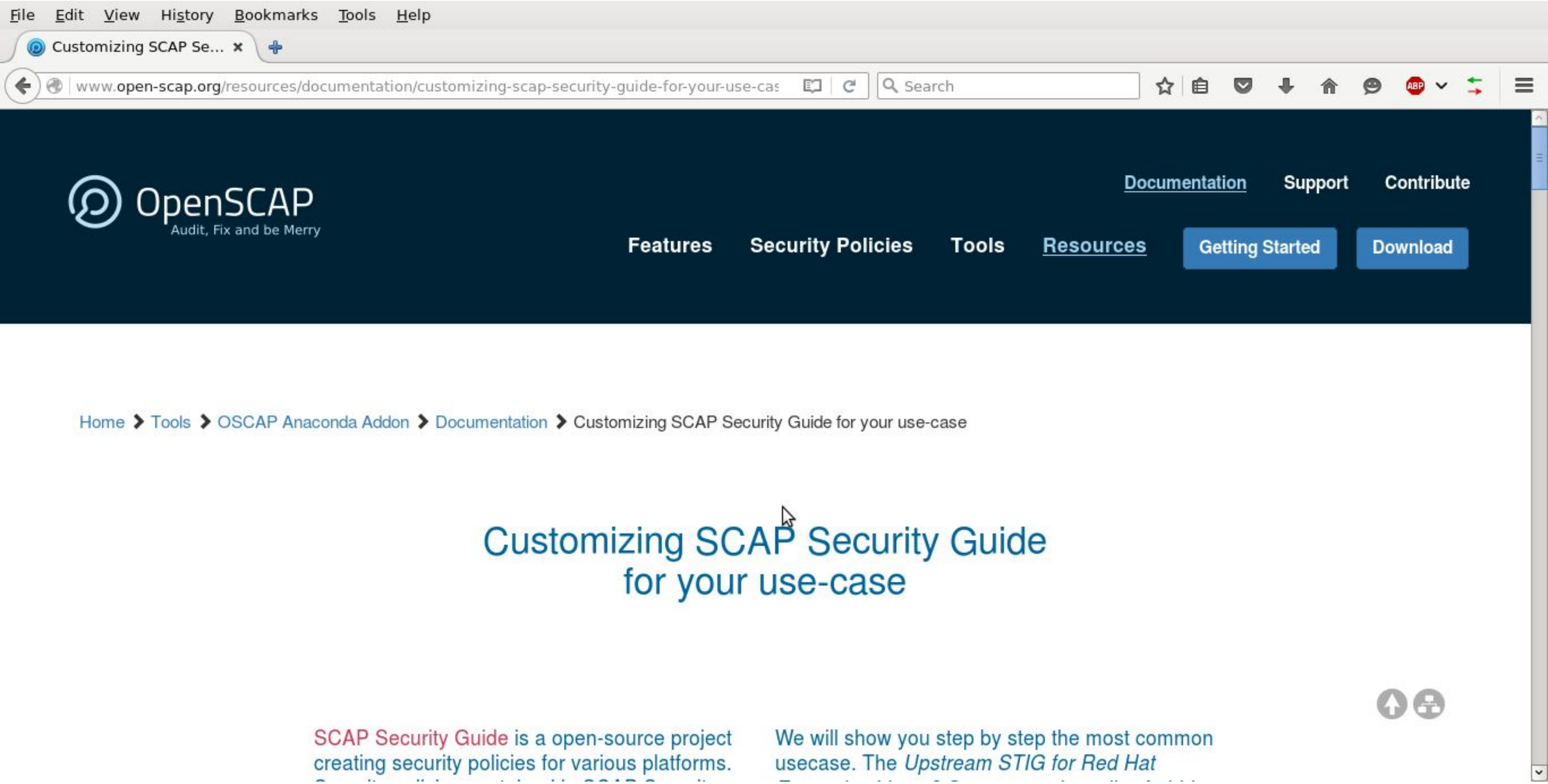
Security Identifiers

[*http://cce.mitre.org*] - **DISA FSO DTBF030**

Depends on Values

- A conditional clause for check statements. = This is a placeholder.

# Customizing policies - Further information



Home > Tools > OSCAP Anaconda Addon > Documentation > Customizing SCAP Security Guide for your use-case

## Customizing SCAP Security Guide for your use-case

SCAP Security Guide is a open-source project creating security policies for various platforms.

We will show you step by step the most common usecase. The *Upstream STIG for Red Hat*

# Is there something left for the future?

SURE THING!!!

# Is there something left for the future?

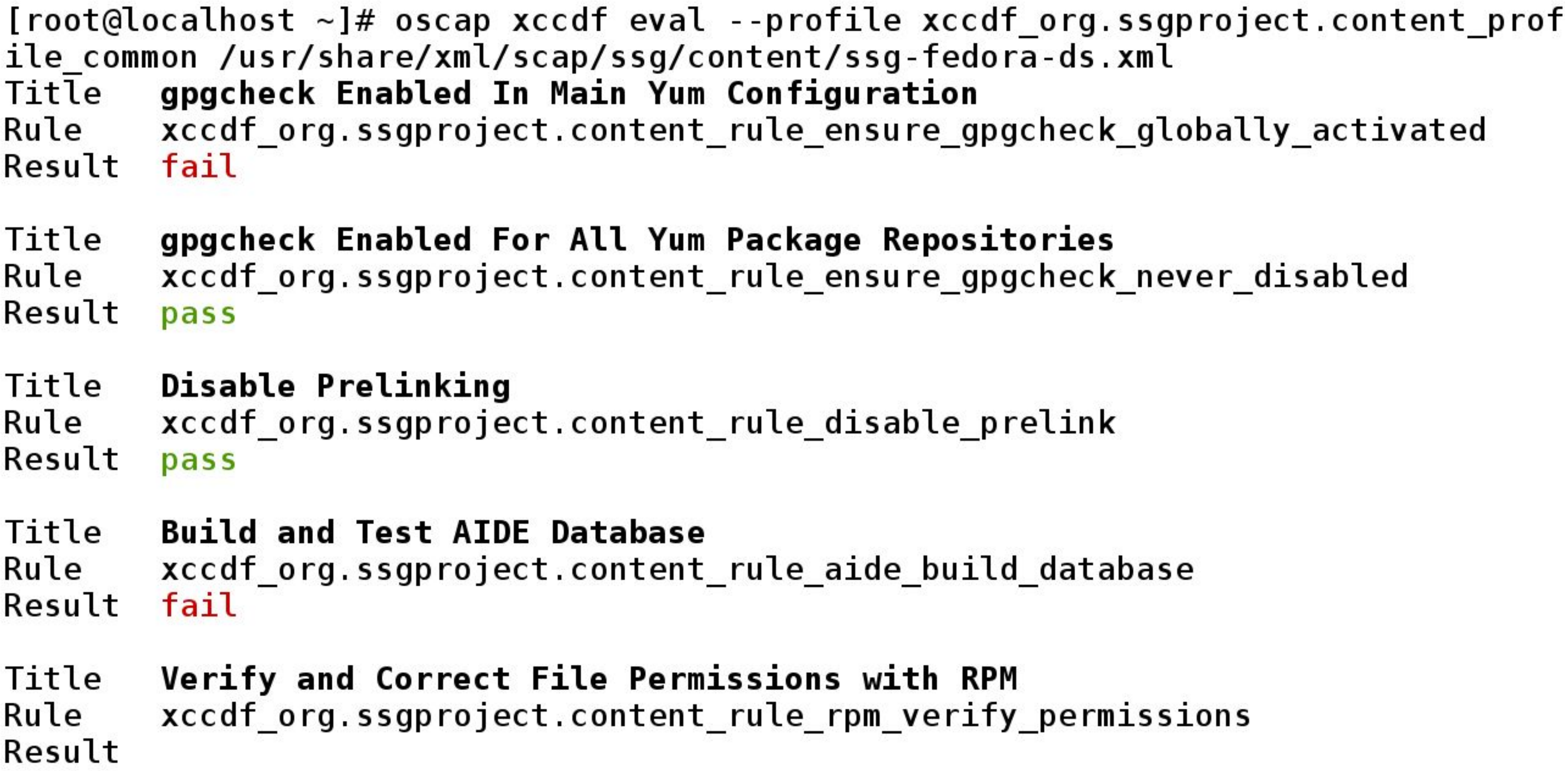
We want policies and tools to be integrated with even more technologies:

Docker, OpenShift, OpenStack, RHEV, …

Got interested? Let’s talk!

# Scanning without GUI tools

# oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_common /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml



```
[root@localhost ~]# oscap xccdf eval --profile xccdf_org.ssgproject.content_prof
ile_common /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
Title   gpgcheck Enabled In Main Yum Configuration
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_activated
Result  fail

Title   gpgcheck Enabled For All Yum Package Repositories
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disabled
Result  pass

Title   Disable Prelinking
Rule    xccdf_org.ssgproject.content_rule_disable_prelink
Result  pass

Title   Build and Test AIDE Database
Rule    xccdf_org.ssgproject.content_rule_aide_build_database
Result  fail

Title   Verify and Correct File Permissions with RPM
Rule    xccdf_org.ssgproject.content_rule_rpm_verify_permissions
Result
```

# oscap-docker, oscap-vm

- command-line tools
- scan containers and container images
- scan virtual machines
- no need to install any tools inside the containers / VMs

# Continuous scans

- Scanning a single machine, VM or container is just a learning step
- So far we have only seen one-off solicited scans
- Doing manual scans of a few machines is workable but doesn’t scale
- Continuous compliance to the rescue

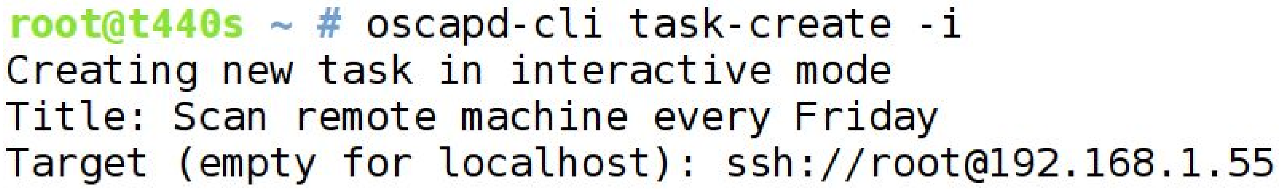
“Scan every Sunday around midnight”

# OpenSCAP-daemon

- a service!
- provides a dbus interface
- oscapd-cli
- “task” is a central concept of the daemon
- tasks usually evaluate some resource
  - local machine
  - container, container image
  - VM
  - remote machine
- tasks can be evaluated on demand
- tasks can be planned and repeated

# Creating Tasks

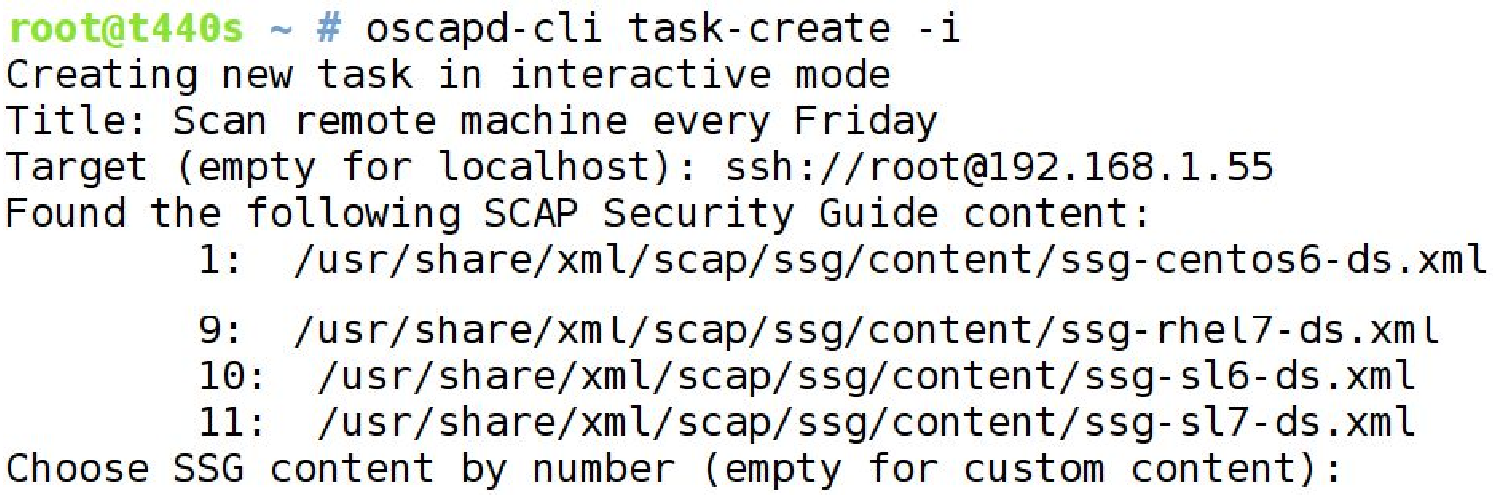
- interactive interfaces
- no need to remember any IDs!



```
root@t440s ~ # oscapd-cli task-create -i
Creating new task in interactive mode
Title: Scan remote machine every Friday
Target (empty for localhost): ssh://root@192.168.1.55
```

# Creating Tasks

- interactive interfaces
- no need to remember any IDs!

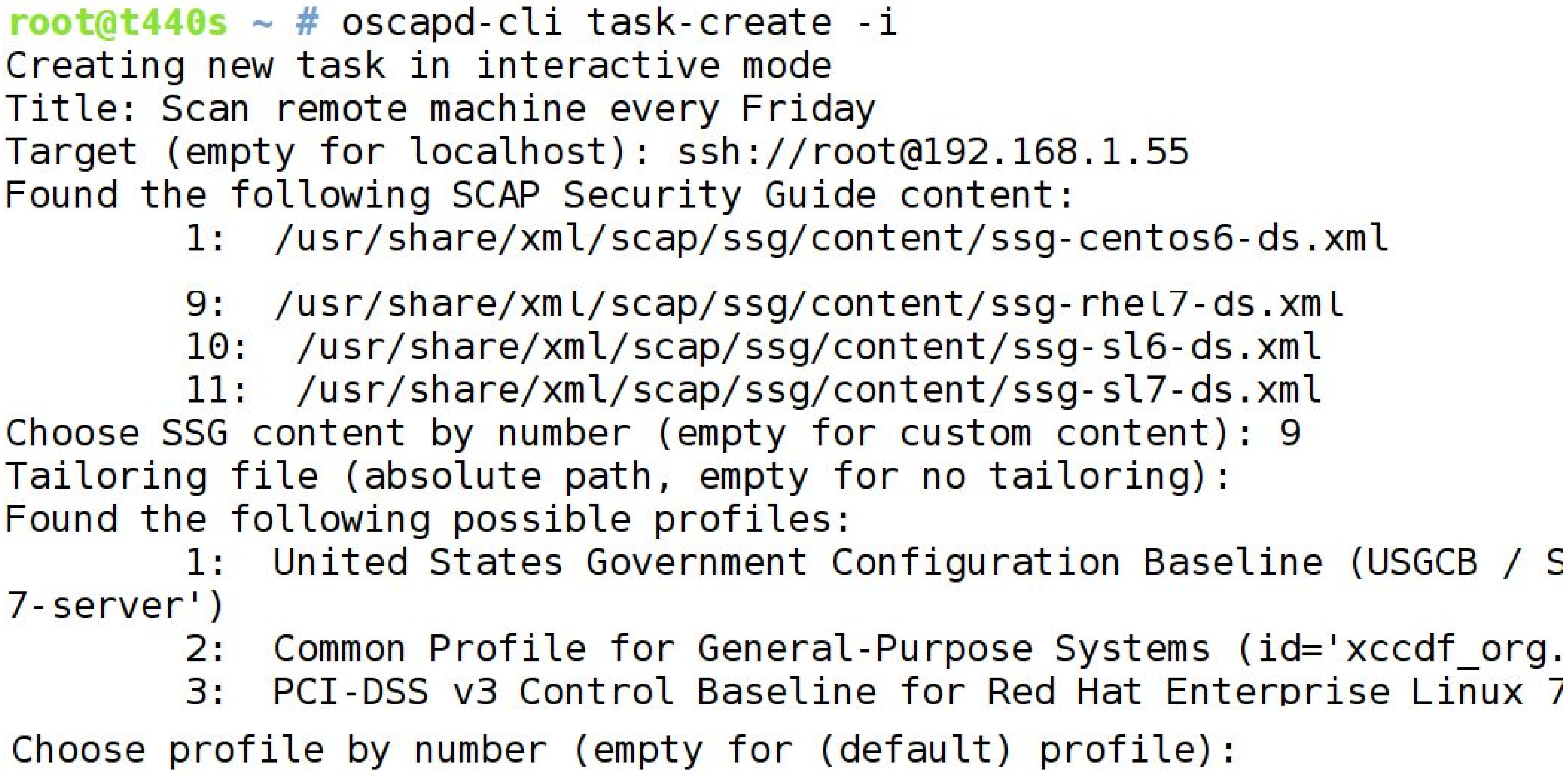


```
root@t440s ~ # oscapd-cli task-create -i
Creating new task in interactive mode
Title: Scan remote machine every Friday
Target (empty for localhost): ssh://root@192.168.1.55
Found the following SCAP Security Guide content:
        1:  /usr/share/xml/scap/ssg/content/ssg-centos6-ds.xml

        9:  /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
        10:  /usr/share/xml/scap/ssg/content/ssg-sl6-ds.xml
        11:  /usr/share/xml/scap/ssg/content/ssg-sl7-ds.xml
Choose SSG content by number (empty for custom content):
```

# Creating Tasks

- interactive interfaces
- no need to remember any IDs!



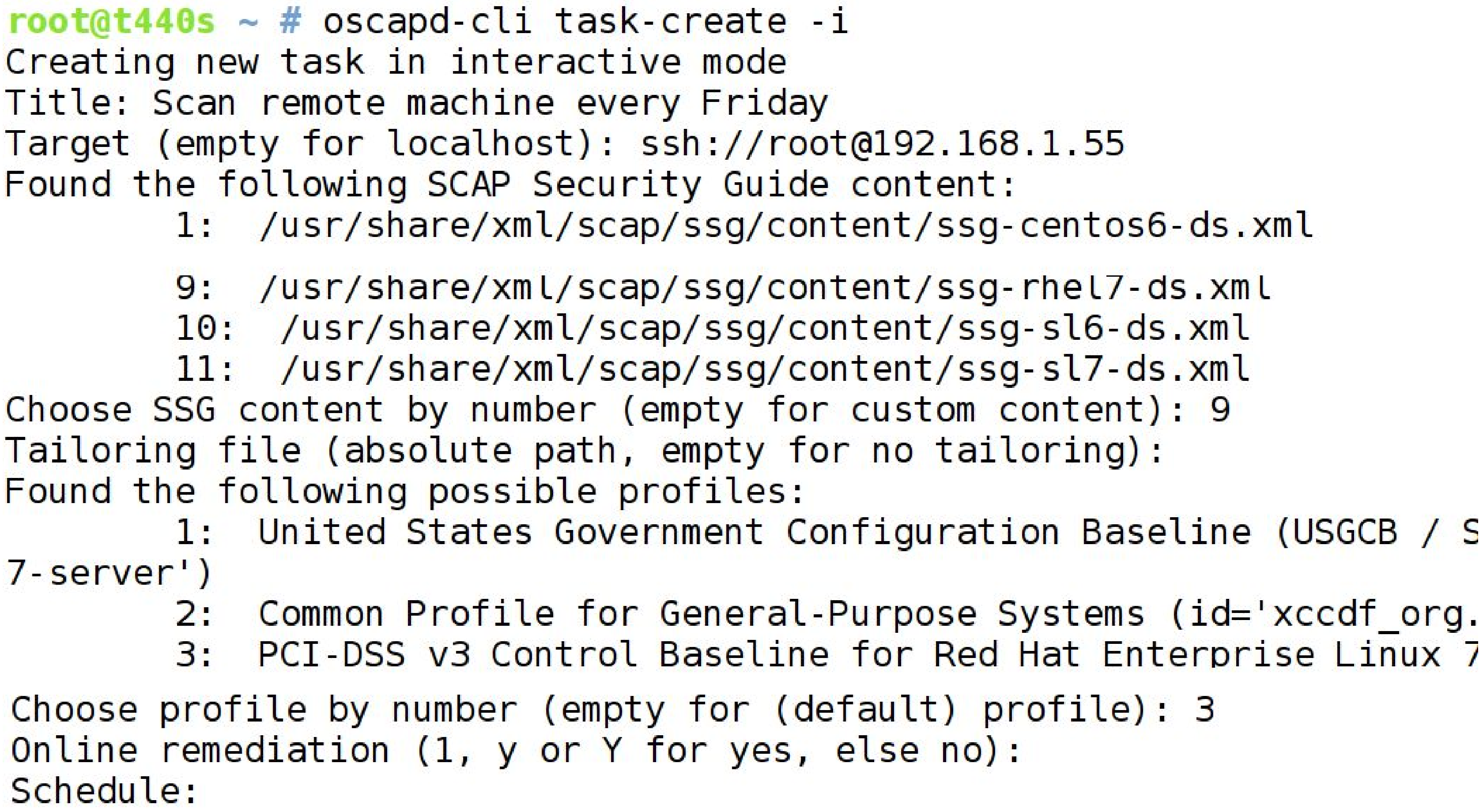
```
root@t440s ~ # oscapd-cli task-create -i
Creating new task in interactive mode
Title: Scan remote machine every Friday
Target (empty for localhost): ssh://root@192.168.1.55
Found the following SCAP Security Guide content:
        1:  /usr/share/xml/scap/ssg/content/ssg-centos6-ds.xml

        9:  /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
        10:  /usr/share/xml/scap/ssg/content/ssg-sl6-ds.xml
        11:  /usr/share/xml/scap/ssg/content/ssg-sl7-ds.xml
Choose SSG content by number (empty for custom content): 9
Tailoring file (absolute path, empty for no tailoring):
Found the following possible profiles:
        1:  United States Government Configuration Baseline (USGCB / S
7-server')
        2:  Common Profile for General-Purpose Systems (id='xccdf_org.
        3:  PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7

Choose profile by number (empty for (default) profile):
```

# Creating Tasks

- interactive interfaces
- no need to remember any IDs!

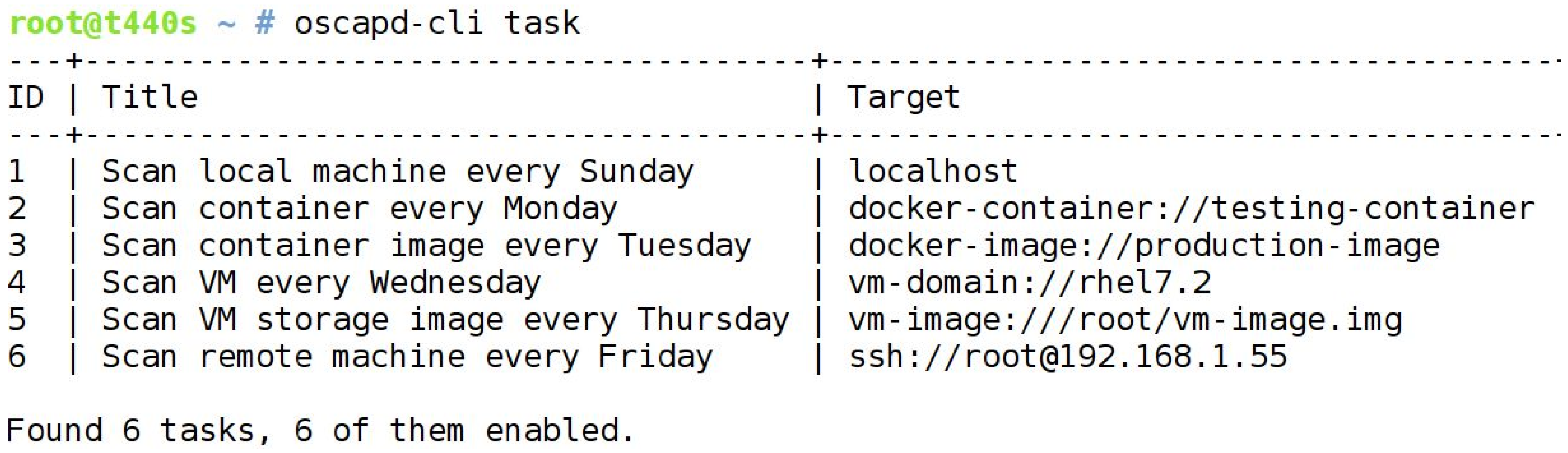


```
root@t440s ~ # oscapd-cli task-create -i
Creating new task in interactive mode
Title: Scan remote machine every Friday
Target (empty for localhost): ssh://root@192.168.1.55
Found the following SCAP Security Guide content:
        1:  /usr/share/xml/scap/ssg/content/ssg-centos6-ds.xml

        9:  /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
        10:  /usr/share/xml/scap/ssg/content/ssg-sl6-ds.xml
        11:  /usr/share/xml/scap/ssg/content/ssg-sl7-ds.xml
Choose SSG content by number (empty for custom content): 9
Tailoring file (absolute path, empty for no tailoring):
Found the following possible profiles:
        1:  United States Government Configuration Baseline (USGCB / S
7-server')
        2:  Common Profile for General-Purpose Systems (id='xccdf_org.
        3:  PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7

Choose profile by number (empty for (default) profile): 3
Online remediation (1, y or Y for yes, else no):
Schedule:
```

# Task Overview



```
root@t440s ~ # oscapd-cli task
---+--------------------------------------+---------------------------------------
ID | Title                                | Target
---+--------------------------------------+---------------------------------------
1  | Scan local machine every Sunday      | localhost
2  | Scan container every Monday          | docker-container://testing-container
3  | Scan container image every Tuesday   | docker-image://production-image
4  | Scan VM every Wednesday              | vm-domain://rhel7.2
5  | Scan VM storage image every Thursday | vm-image:///root/vm-image.img
6  | Scan remote machine every Friday     | ssh://root@192.168.1.55

Found 6 tasks, 6 of them enabled.
```

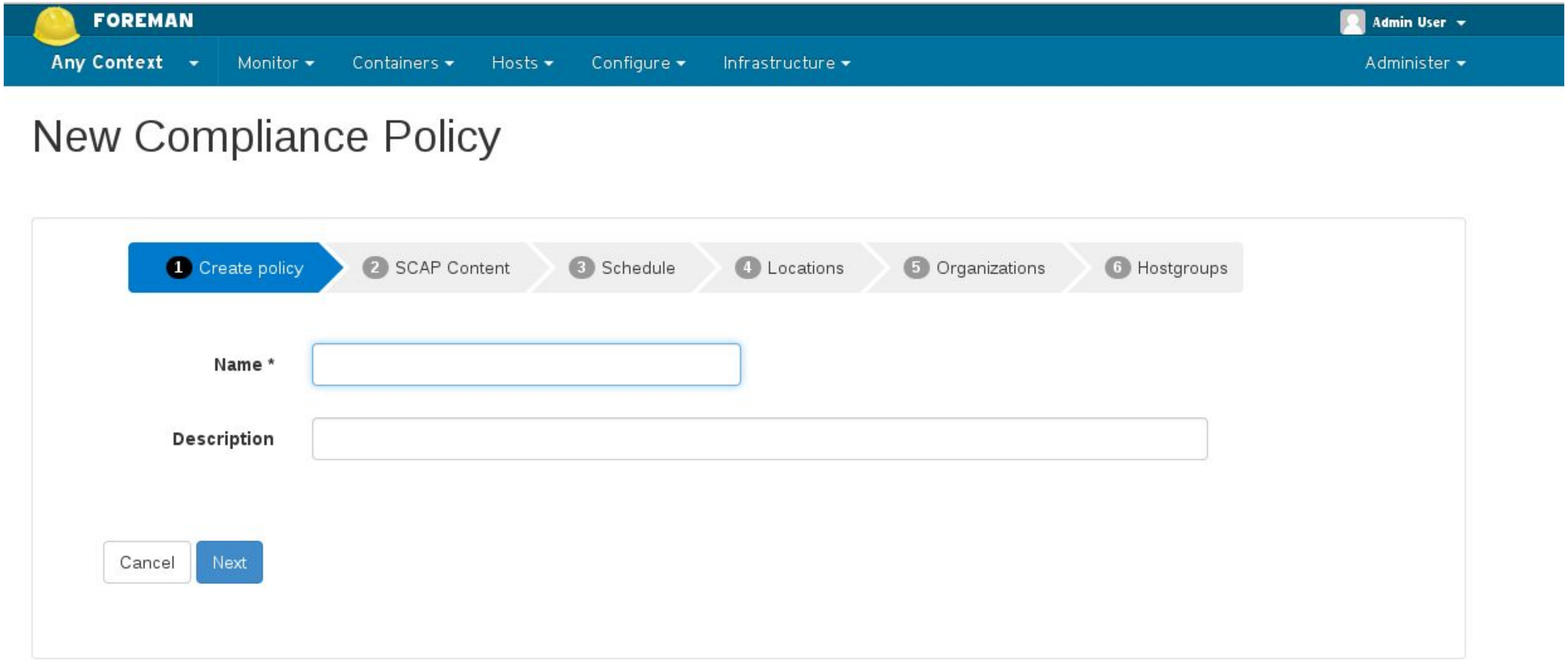
# Querying results

- oscapd-cli result 1
  - overview of all results for task 1
- oscapd-cli result 1 1 arf
  - get ARF of result 1 of task 1
- oscapd-cli result 1 1 report
  - get HTML report of result 1 of task 1
- oscapd-cli result 1 1 {stdout,stderr,exit_code}
  - get other outputs from the oscap tool

# Foreman

- OpenSCAP-daemon is a very new project
- OpenSCAP-daemon is for smaller deployments
- Foreman is older and more production ready
- Foreman is more suitable for large deployments

# Foreman

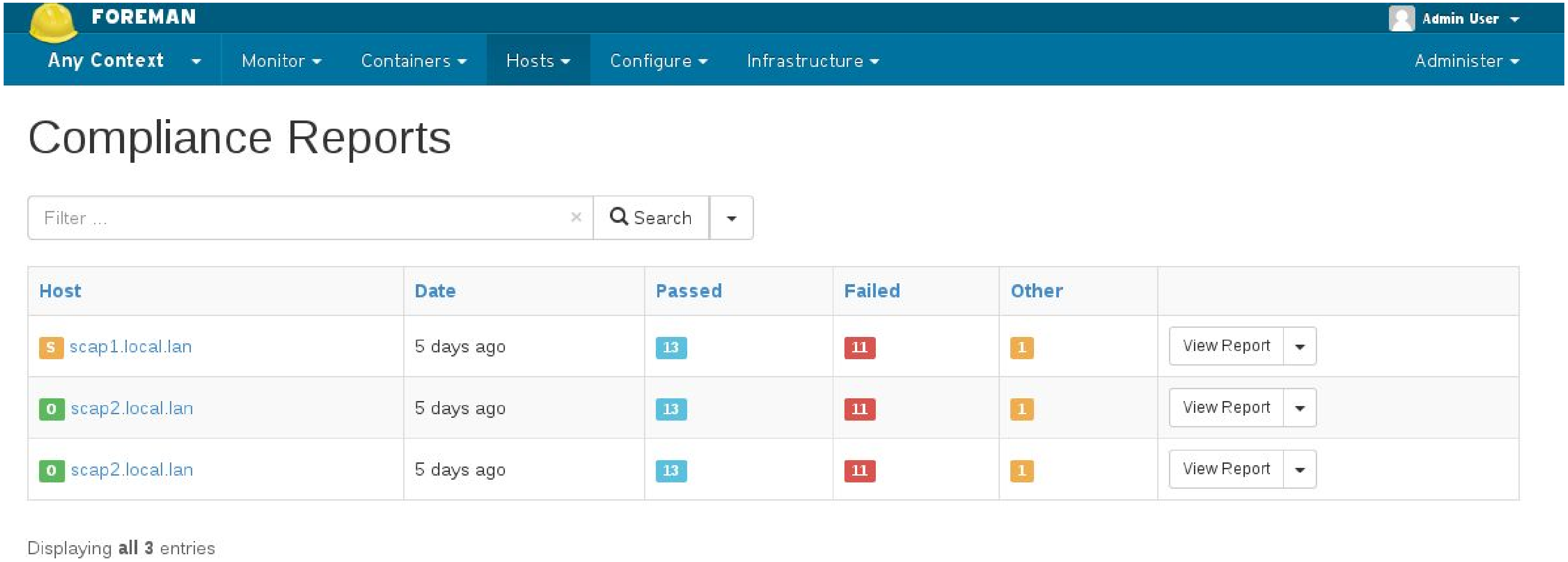


New Compliance Policy

Name *

Description

# Foreman

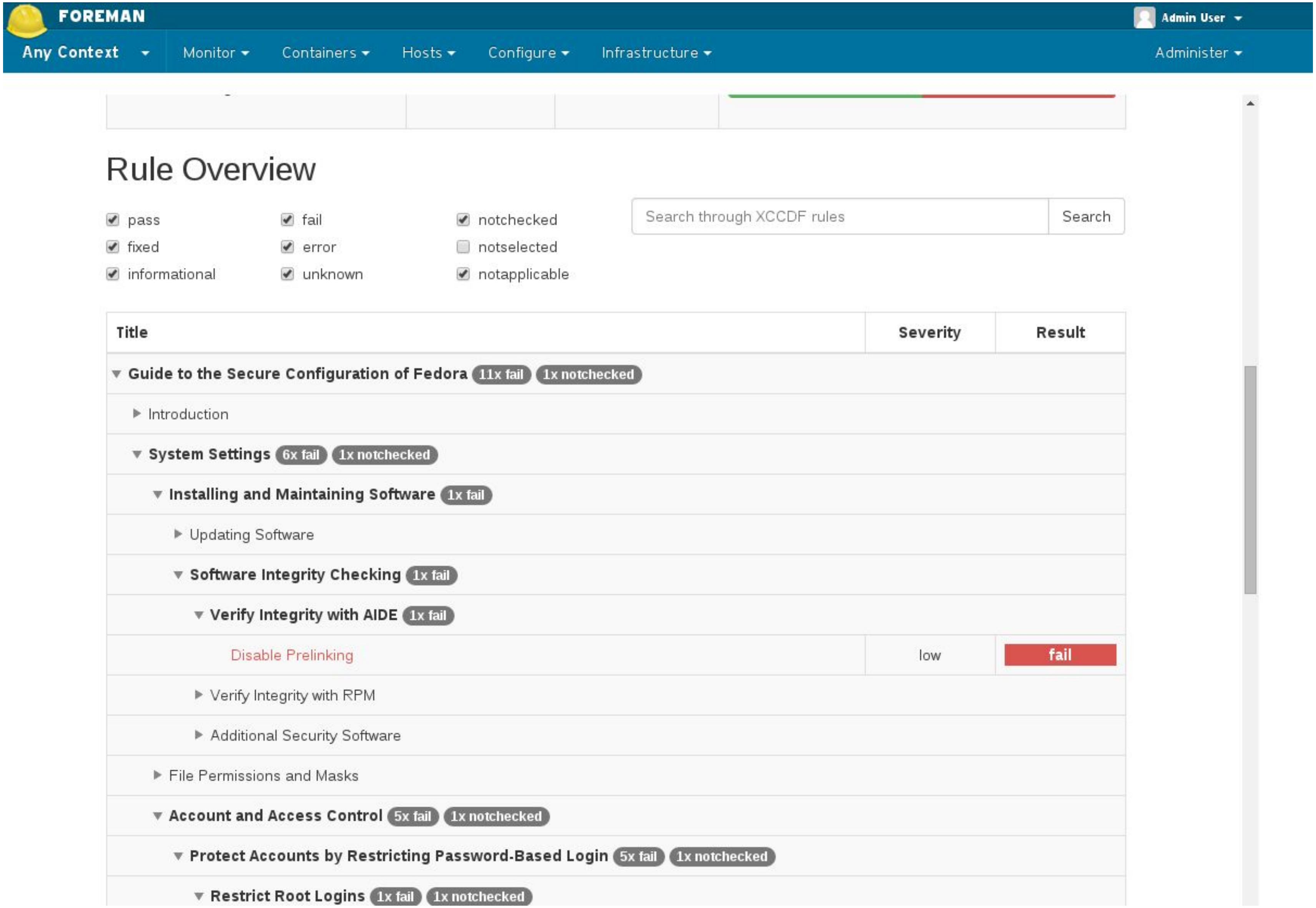


## Compliance Reports

| Host | Date | Passed | Failed | Other | |
|---|---|---|---|---|---|
| S scap1.local.lan | 5 days ago | 13 | 11 | 1 | View Report |
| O scap2.local.lan | 5 days ago | 13 | 11 | 1 | View Report |
| O scap2.local.lan | 5 days ago | 13 | 11 | 1 | View Report |

Displaying **all 3** entries

# Foreman



## Rule Overview

☑ pass
☑ fixed
☑ informational

☑ fail
☑ error
☑ unknown

☑ notchecked
□ notselected
☑ notapplicable

Search through XCCDF rules | Search

| Title | Severity | Result |
|---|---|---|
| ▼ **Guide to the Secure Configuration of Fedora** 11x fail 1x notchecked | | |
| ▶ Introduction | | |
| ▼ **System Settings** 6x fail 1x notchecked | | |
| ▼ **Installing and Maintaining Software** 1x fail | | |
| ▶ Updating Software | | |
| ▼ **Software Integrity Checking** 1x fail | | |
| ▼ **Verify Integrity with AIDE** 1x fail | | |
| Disable Prelinking | low | fail |
| ▶ Verify Integrity with RPM | | |
| ▶ Additional Security Software | | |
| ▶ File Permissions and Masks | | |
| ▼ **Account and Access Control** 5x fail 1x notchecked | | |
| ▼ **Protect Accounts by Restricting Password-Based Login** 5x fail 1x notchecked | | |
| ▼ **Restrict Root Logins** 1x fail 1x notchecked | | |

# Thanks for your attention!

- Questions?

- https://www.open-scap.org/
- https://github.com/OpenSCAP
- twitter: @OpenSCAP