Compliance Center

& project SCAPtimony

Presented by
Šimon Lukašík
Software Engineer, Red Hat, inc.

Licensed to the public under a Creative Commons Attribution 4.0 license.

Compliance Center ?

Today's Topics

1. State of the art
2. New requirements
3. SCAPtimony project
4. SCAPtimony within Foreman

State of the art

OpenSCAP

SCAP
SECURITY GUIDE

SCAP
WORKBENCH

Next level requirements

- FISMA Act.
- SCAP, SACM, CDN, SWID
- STIG, PCI DSS
- FIPS 140-2
- ISO 27001/27002
- MLPS, FedRAMP, EU Model Clauses
- United Kingdom G-Cloud
- Australian Government IRAP
- Singapore MTCS Standard
- HIPAA
- FERPA
- CCCPPF

Req: Inventory

- Hardware
- Software
- Configuration

Req: Targeting

- Policy modeling
- Organization defined targeting
- Understanding purpose of target
- Ad-hoc tailoring

Req: Queries

- Is my infrastructure compliant?
- What was the failure on my db server?
- Vulnerabilities assessment (CVEs)
- Where is unpatched openssl?

- Output in standardized forms
- Retention policies
- Can be data trusted

Req: Processes

- Improve managebility
- Monitoring / on-going oversee
- What is the next thing to do / tasking
- Help with best practices
- Trends
- Threat life-cycle
- Define waivers
- Calculate / authorize accepted risk

Req: Other

- Cloud vs. on premise
- Container is an asset too
- API for data import/export
- Devops love ruby
  - Foreman & ManageIQ

Implications

- Deployment will vary
- Use-cases will vary
- Data will fit the same model
- Structured data
- Mostly read-only interface

SCAPtimony

First steps

- Leverage existing OpenSCAP ecosystem
- Configuration compliance
- Database schema
- Basic operation over data

Main entities

- Notion of auditable assets
- Define security/compliance policies
- Reports

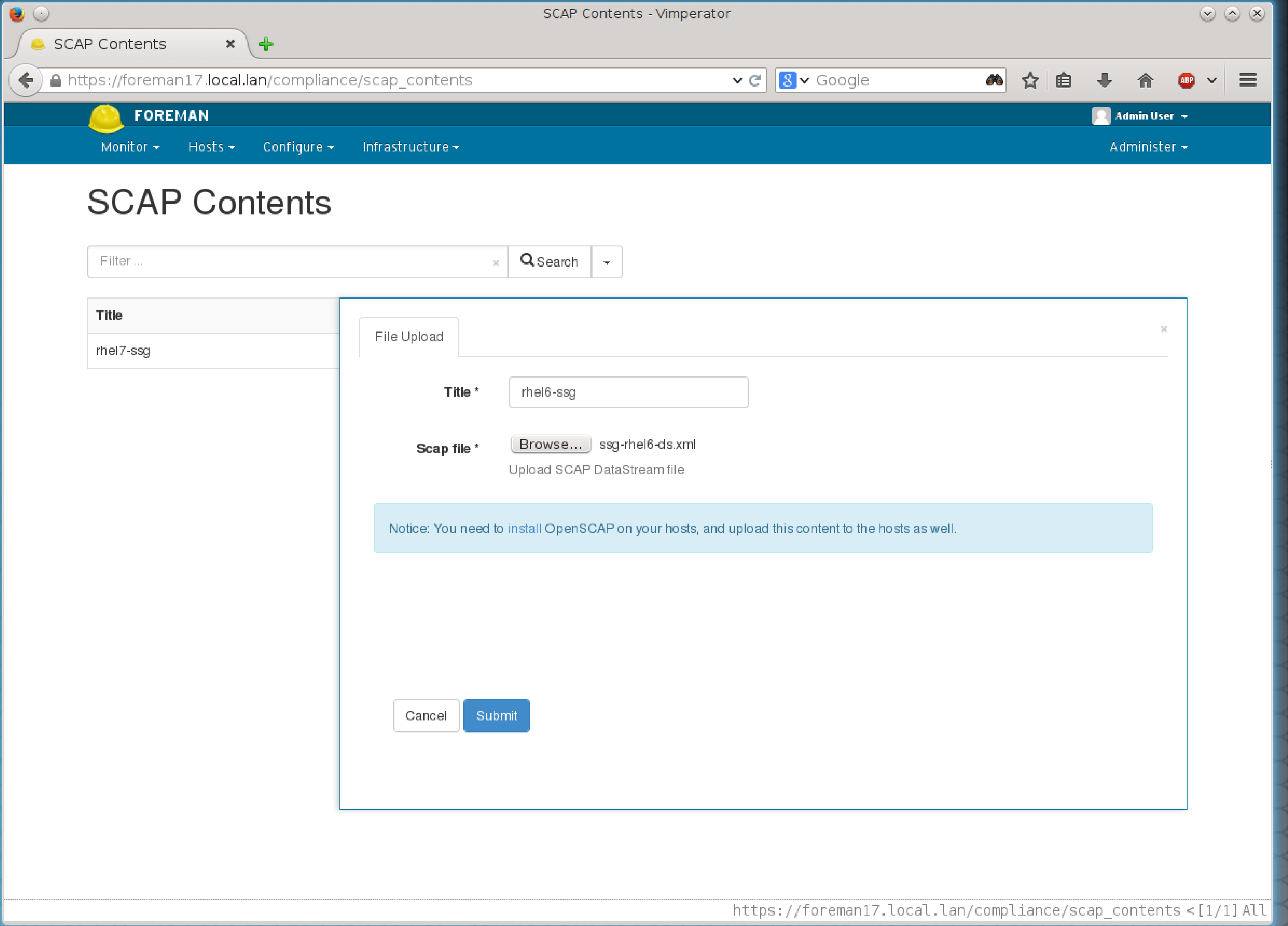
Implementation

- Rails engine
- Mostly models and helpers
  - Translate to SCAP objects
- rubygem-openscap
  - FFI, binds with OpenSCAP primitives
  - OpenSCAP API redesign
- github.com/openscap

SCAPtimony & Foreman

Architecture

- SCAPtimony rails engine
- foreman_openscap rails engine
  - Foreman plug-in
  - Contollers & views
  - Full of concerns
- scoped_search


SCAP Contents - Vimperator
SCAP Contents
https://foreman17.local.lan/compliance/scap_contents
Google
FOREMAN
Admin User
Monitor
Hosts
Configure
Infrastructure
Administer

SCAP Contents

Filter ...
Search
Title
rhel7-ssg
File Upload

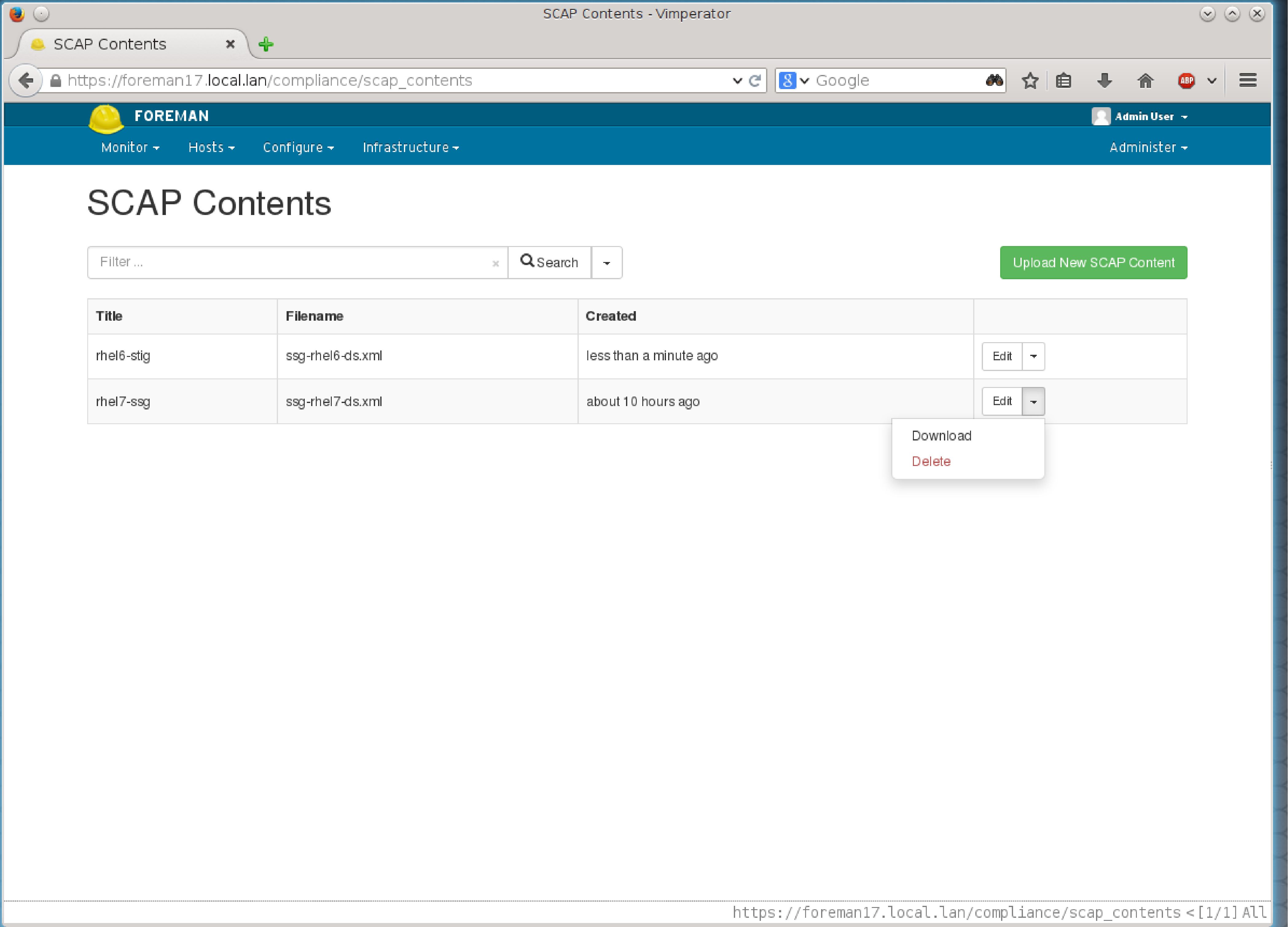
Title * rhel6-ssg

Scap file * Browse... ssg-rhel6-ds.xml

Upload SCAP DataStream file

Notice: You need to install OpenSCAP on your hosts, and upload this content to the hosts as well.

Cancel
Submit
https://foreman17.local.lan/compliance/scap_contents <[1/1] All



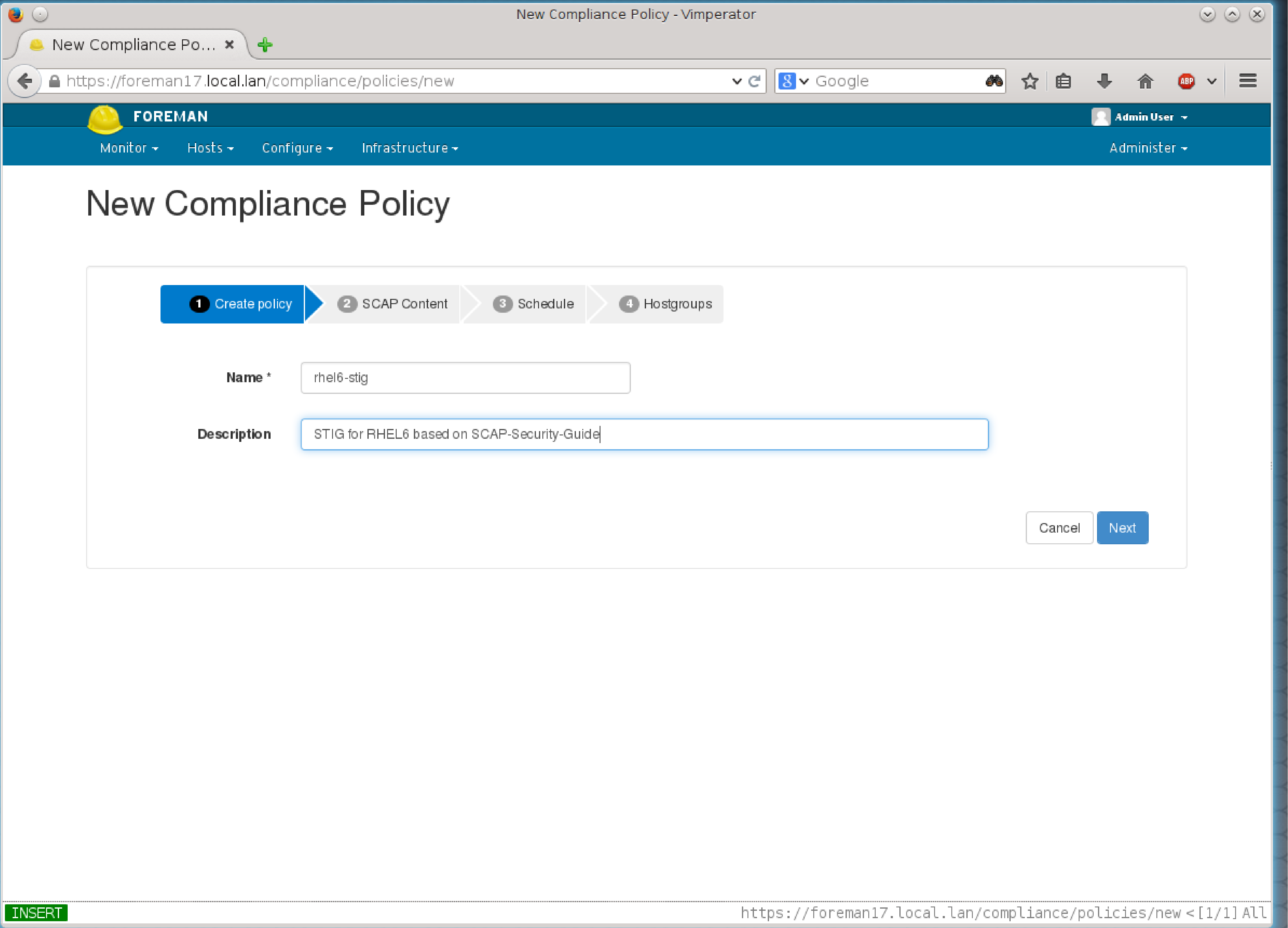
SCAP Contents - Vimperator
SCAP Contents
https://foreman17.local.lan/compliance/scap_contents
Google
FOREMAN
Admin User
Monitor
Hosts
Configure
Infrastructure
Administer

SCAP Contents

Filter ...
Search
Upload New SCAP Content

Title	Filename	Created	
rhel6-stig	ssg-rhel6-ds.xml	less than a minute ago	Edit
rhel7-ssg	ssg-rhel7-ds.xml	about 10 hours ago	Edit

Download
Delete
https://foreman17.local.lan/compliance/scap_contents <[1/1] All

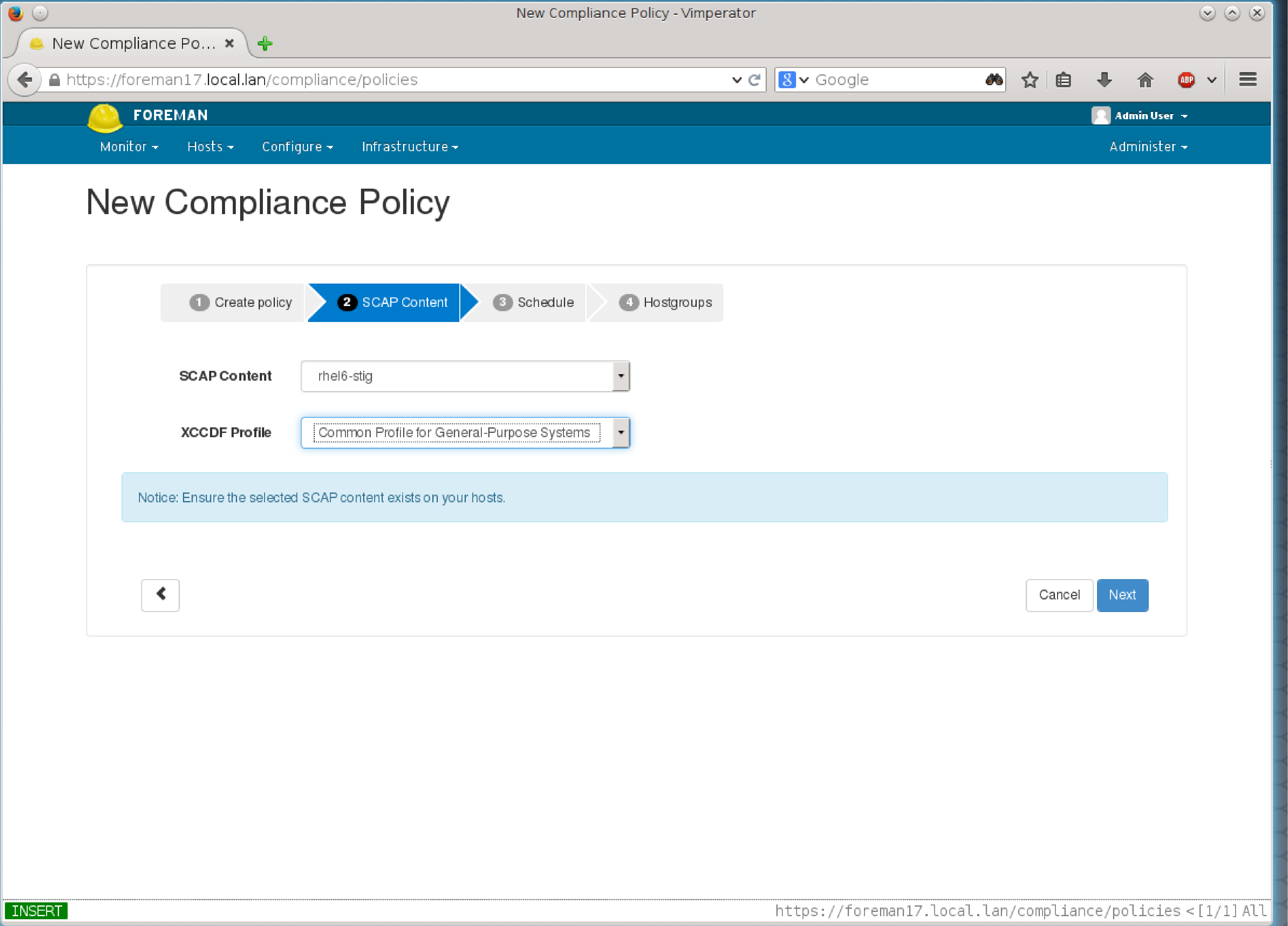


New Compliance Policy

Name * rhel6-stig

Description STIG for RHEL6 based on SCAP-Security-Guide

Cancel
Next
INSERT
https://foreman17.local.lan/compliance/policies/new <[1/1] All

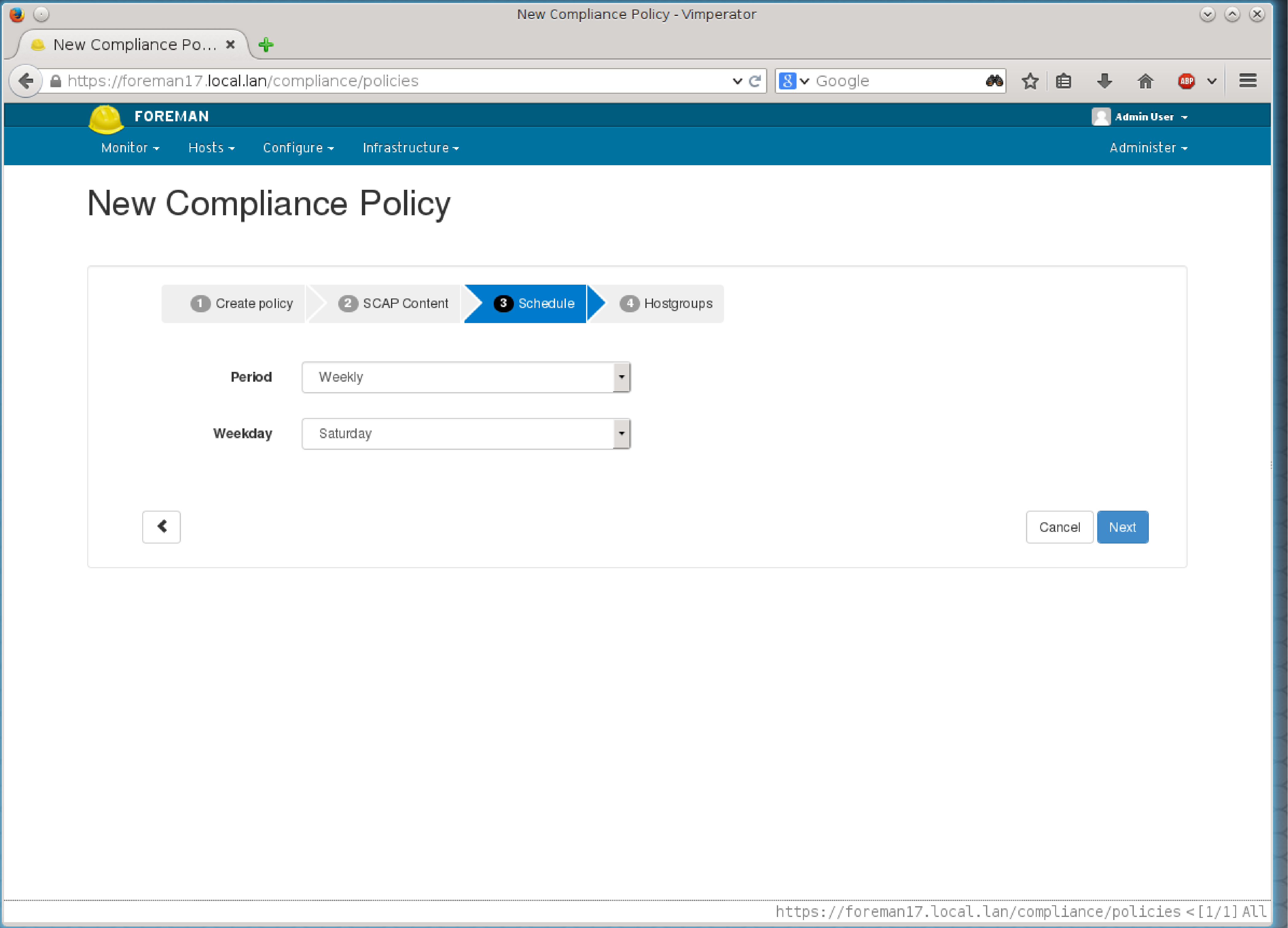


New Compliance Policy

SCAP Content rhel6-stig

XCCDF Profile Common Profile for General-Purpose Systems

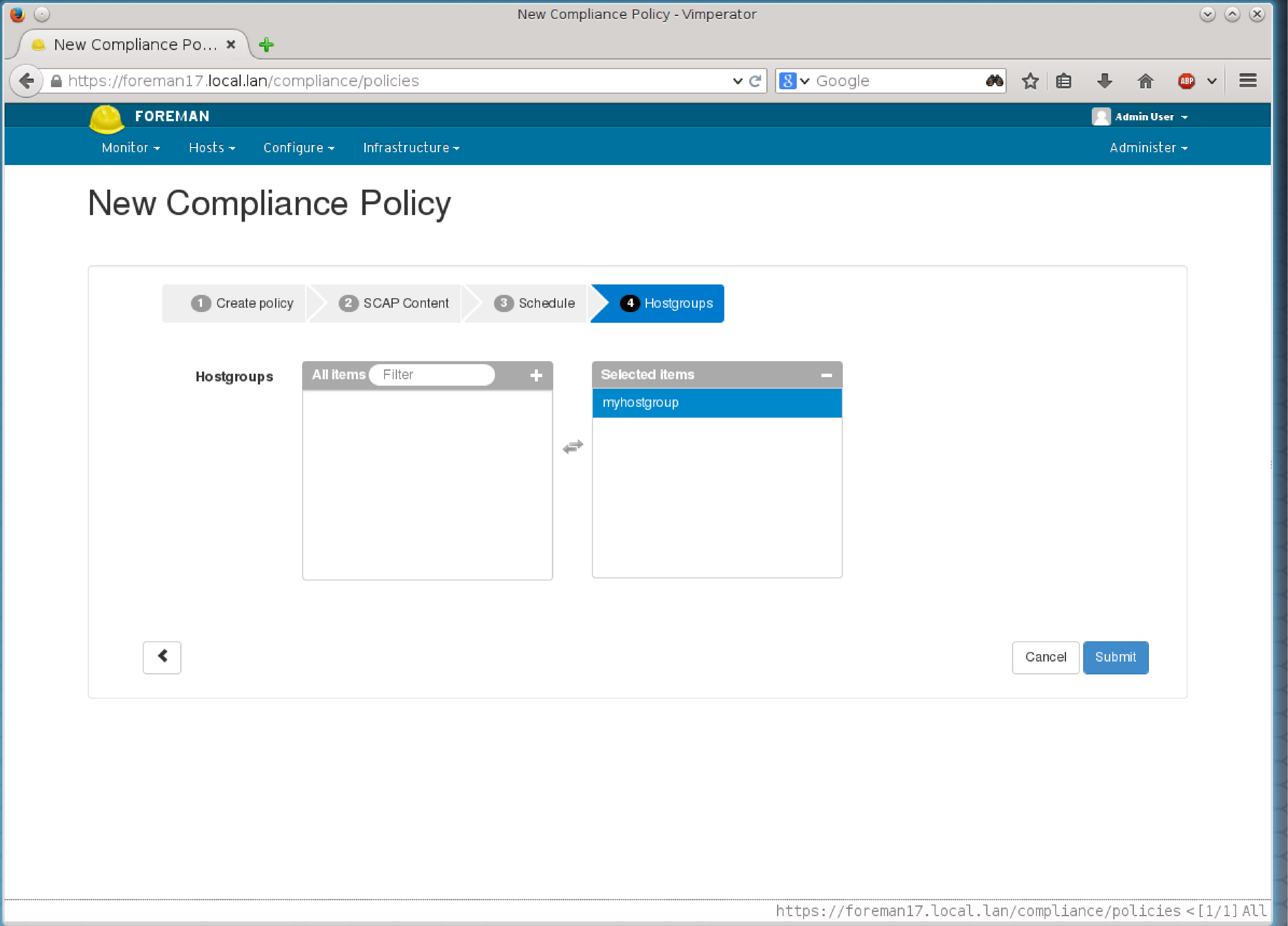
Notice: Ensure the selected SCAP content exists on your hosts.



New Compliance Policy

Period: Weekly

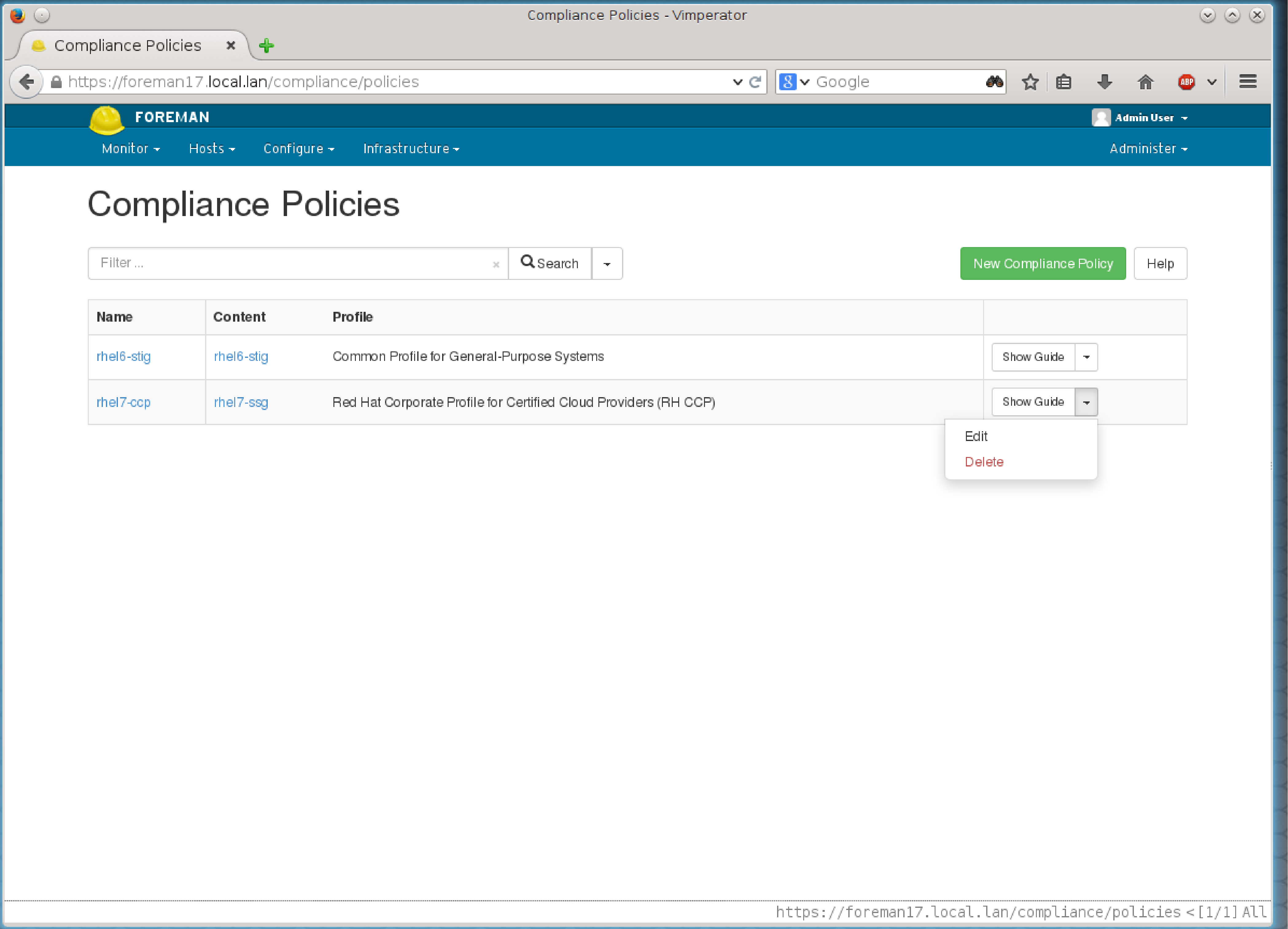
Weekday: Saturday



New Compliance Policy

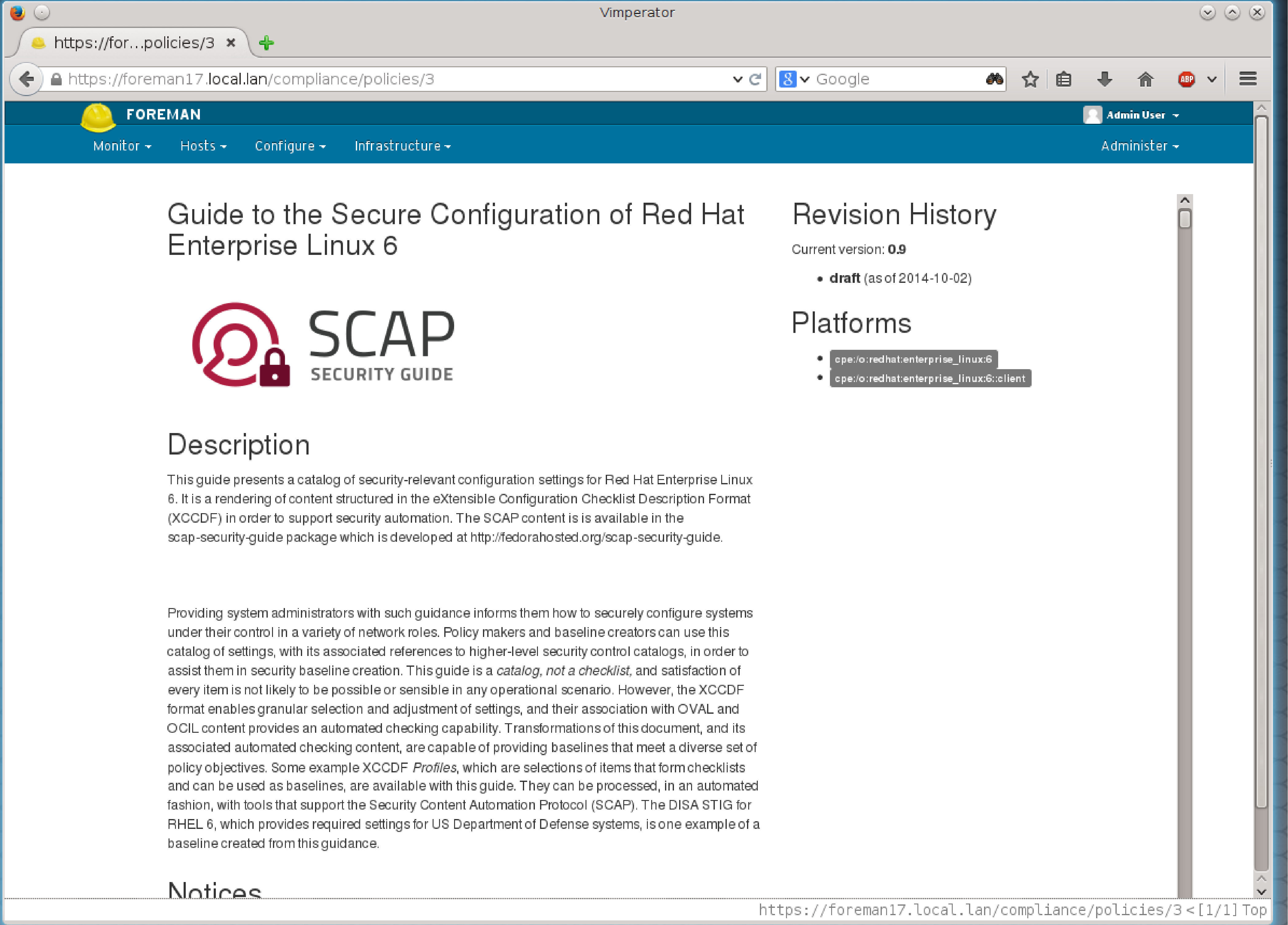
Hostgroups

All items	Selected items
	myhostgroup



Compliance Policies

Name	Content	Profile	
rhel6-stig	rhel6-stig	Common Profile for General-Purpose Systems	Show Guide
rhel7-ccp	rhel7-ssg	Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	Show Guide



Guide to the Secure Configuration of Red Hat Enterprise Linux 6

Revision History

Current version: **0.9**

- **draft** (as of 2014-10-02)

Platforms

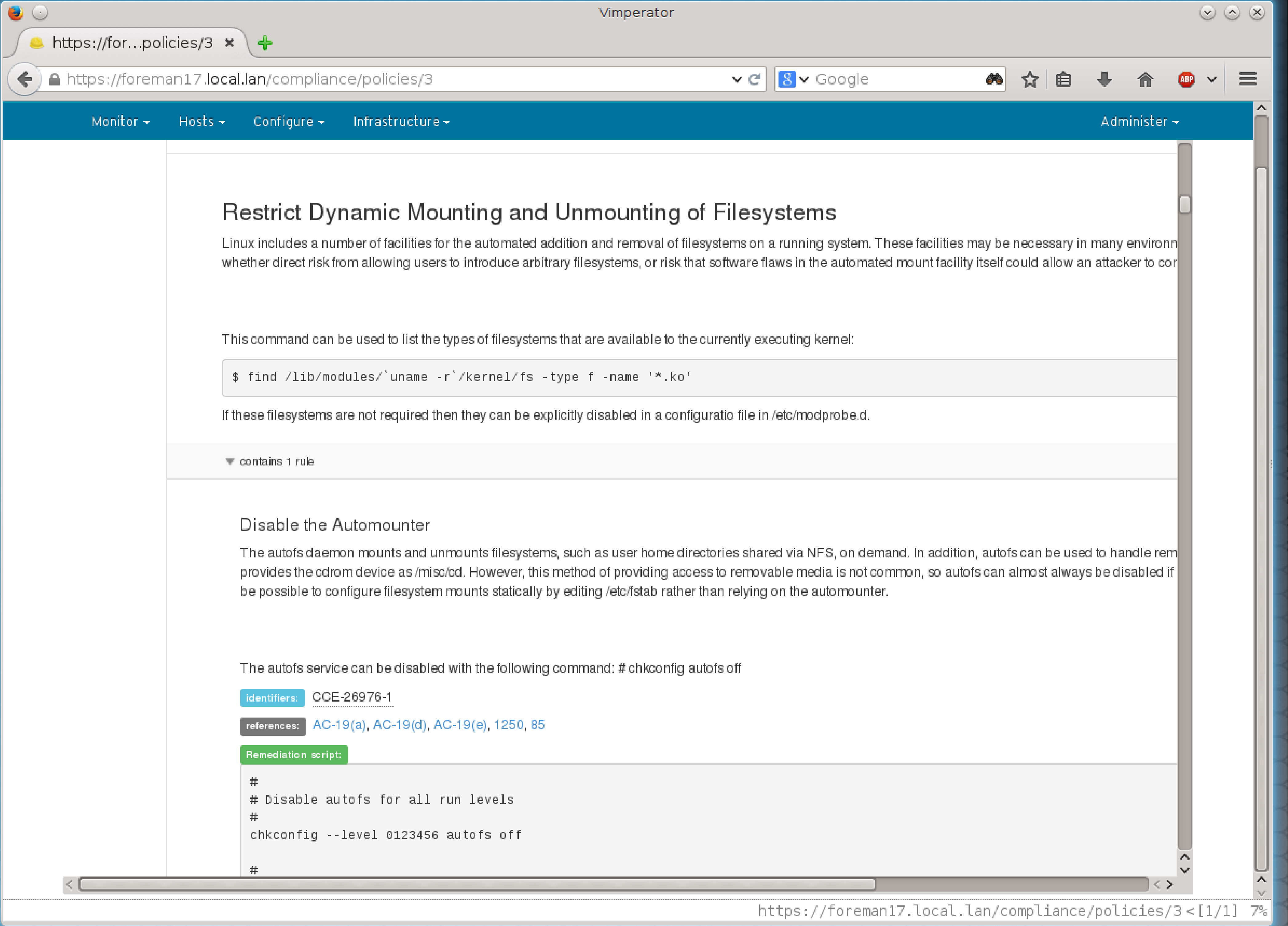
- cpe:/o:redhat:enterprise_linux:6
- cpe:/o:redhat:enterprise_linux:6::client

Description

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 6. 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 http://fedorahosted.org/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 any operational scenario. 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 for RHEL 6, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Notices



Restrict Dynamic Mounting and Unmounting of Filesystems

Linux includes a number of facilities for the automated addition and removal of filesystems on a running system. These facilities may be necessary in many environn
whether direct risk from allowing users to introduce arbitrary filesystems, or risk that software flaws in the automated mount facility itself could allow an attacker to cor

This command can be used to list the types of filesystems that are available to the currently executing kernel:

```
$ find /lib/modules/`uname -r`/kernel/fs -type f -name '*.ko'
```

If these filesystems are not required then they can be explicitly disabled in a configuratio file in /etc/modprobe.d.

▼ contains 1 rule

Disable the Automounter

The autofs daemon mounts and unmounts filesystems, such as user home directories shared via NFS, on demand. In addition, autofs can be used to handle rem
provides the cdrom device as /misc/cd. However, this method of providing access to removable media is not common, so autofs can almost always be disabled if
be possible to configure filesystem mounts statically by editing /etc/fstab rather than relying on the automounter.

The autofs service can be disabled with the following command: # chkconfig autofs off

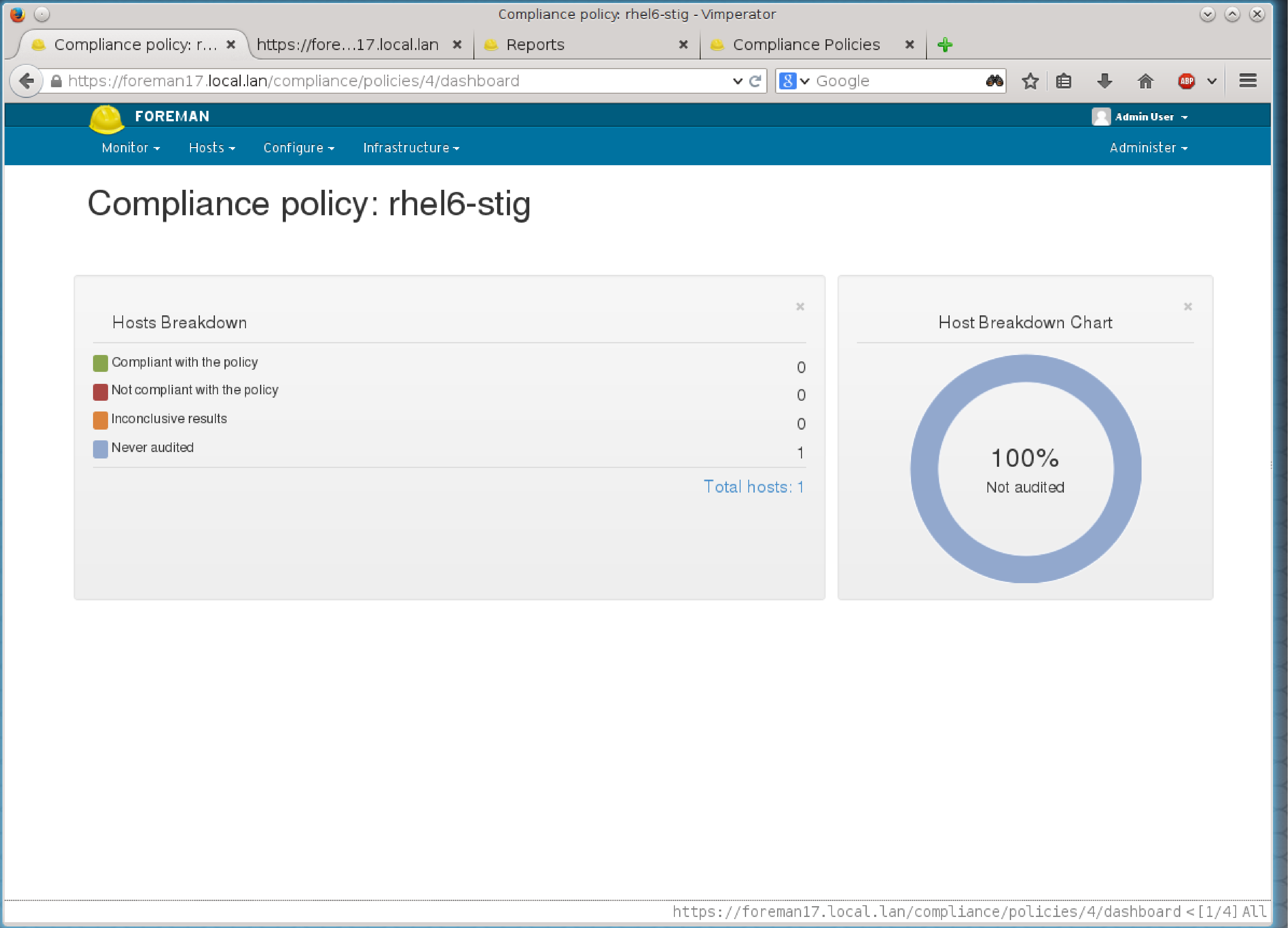
identifiers: CCE-26976-1

references: AC-19(a), AC-19(d), AC-19(e), 1250, 85

Remediation script:

```
#
# Disable autofs for all run levels
#
chkconfig --level 0123456 autofs off

#
```



Compliance policy: rhel6-stig - Vimperator
Compliance policy: r…
https://fore…17.local.lan
Reports
Compliance Policies
https://foreman17.local.lan/compliance/policies/4/dashboard
Google
FOREMAN
Admin User
Monitor
Hosts
Configure
Infrastructure
Administer

Compliance policy: rhel6-stig

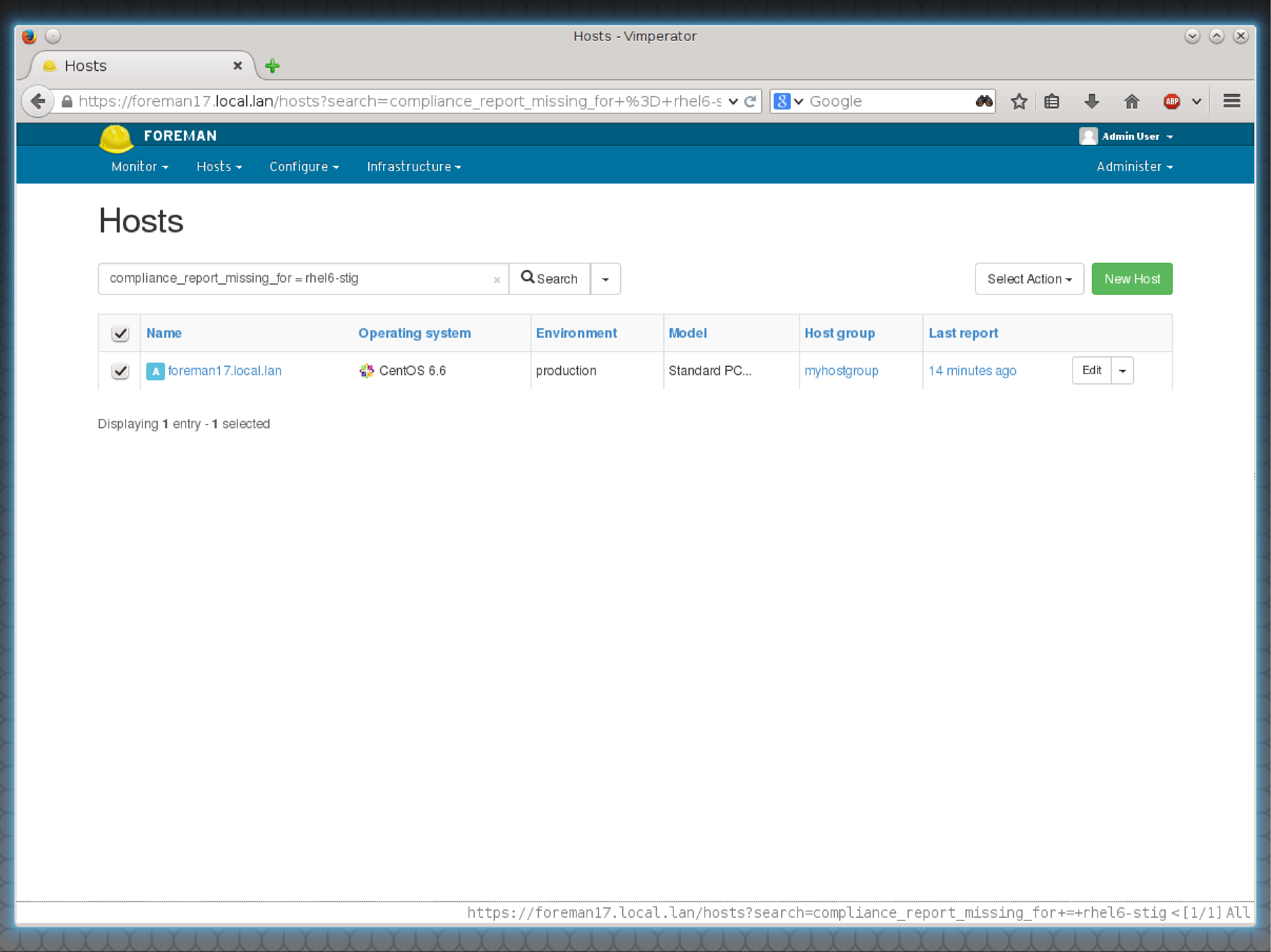
Hosts Breakdown

🟩 Compliant with the policy	0
🟥 Not compliant with the policy	0
🟧 Inconclusive results	0
🟦 Never audited	1

Total hosts: 1

Host Breakdown Chart

100%
Not audited
https://foreman17.local.lan/compliance/policies/4/dashboard <[1/4] All



https://foreman17.local.lan/hosts?search=compliance_report_missing_for+%3D+rhel6-s

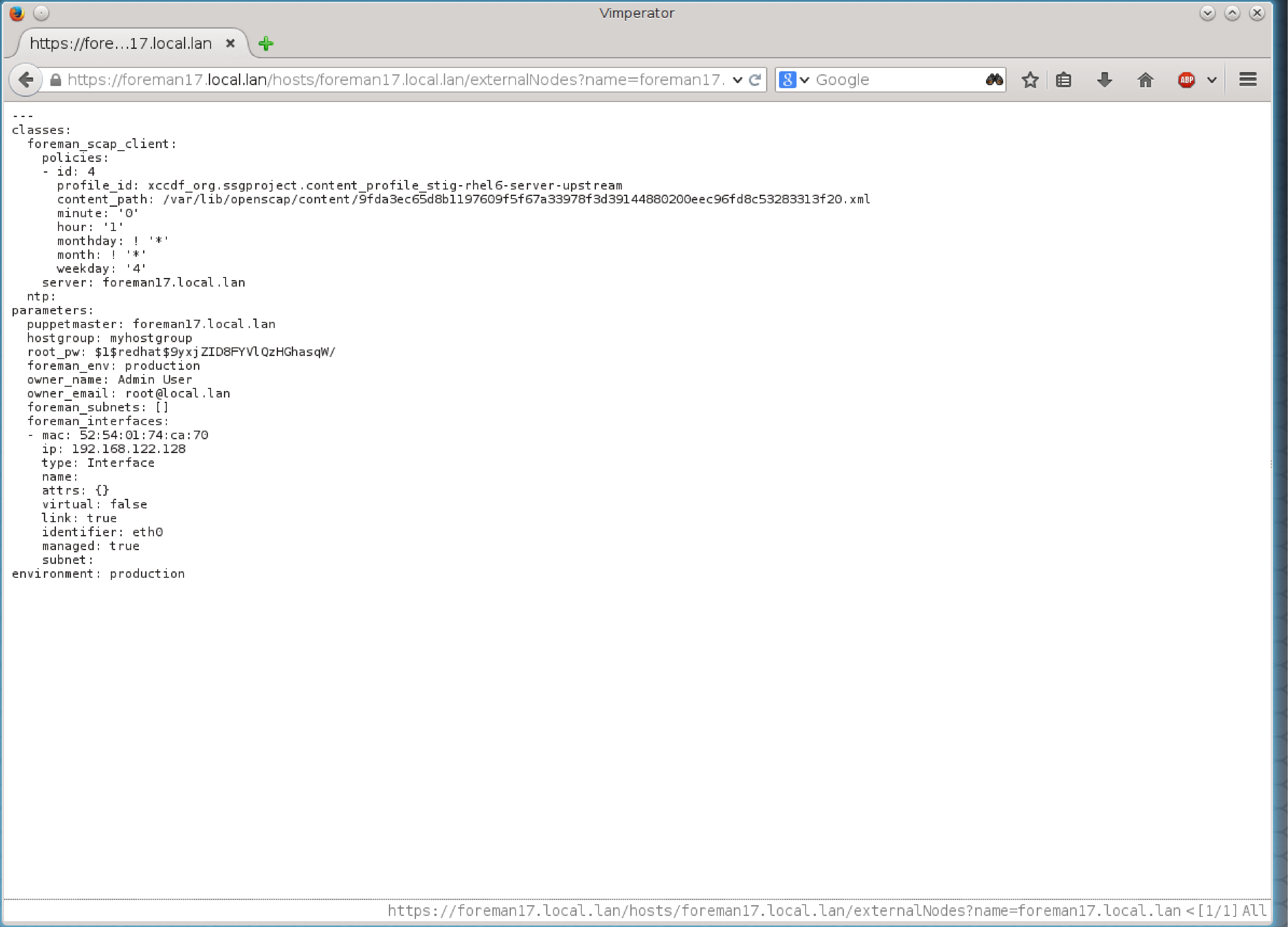
Hosts

compliance_report_missing_for = rhel6-stig

☑	Name	Operating system	Environment	Model	Host group	Last report
☑	A foreman17.local.lan	CentOS 6.6	production	Standard PC...	myhostgroup	14 minutes ago

Displaying **1** entry - **1** selected

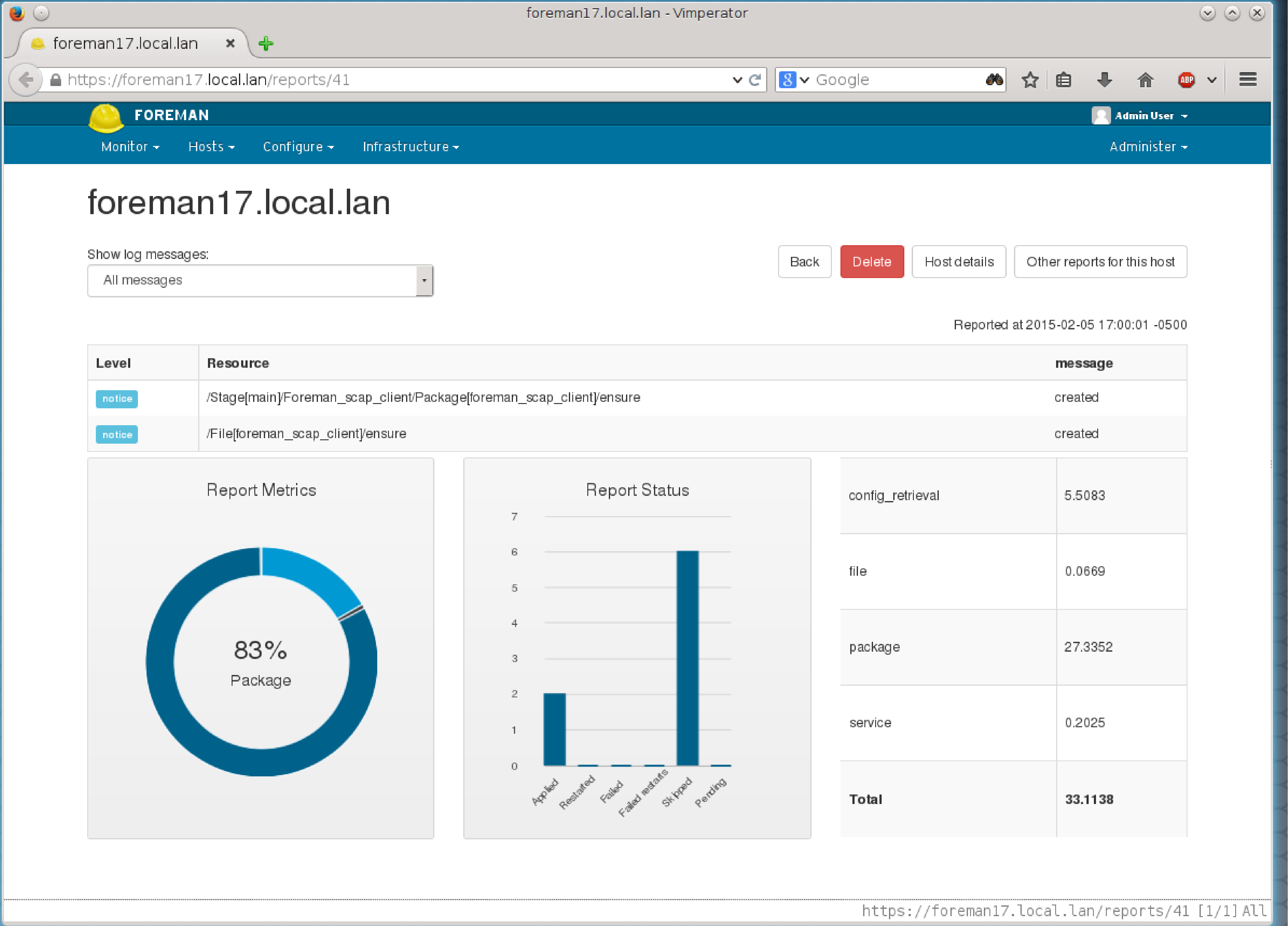
https://foreman17.local.lan/hosts?search=compliance_report_missing_for+=+rhel6-stig < [1/1] All



Vimperator
https://fore…17.local.lan
https://foreman17.local.lan/hosts/foreman17.local.lan/externalNodes?name=foreman17.
Google

```
---
classes:
  foreman_scap_client:
    policies:
    - id: 4
      profile_id: xccdf_org.ssgproject.content_profile_stig-rhel6-server-upstream
      content_path: /var/lib/openscap/content/9fda3ec65d8b1197609f5f67a33978f3d39144880200eec96fd8c53283313f20.xml
      minute: '0'
      hour: '1'
      monthday: ! '*'
      month: ! '*'
      weekday: '4'
    server: foreman17.local.lan
  ntp:
parameters:
  puppetmaster: foreman17.local.lan
  hostgroup: myhostgroup
  root_pw: $1$redhat$9yxjZID8FYVlQzHGhasqW/
  foreman_env: production
  owner_name: Admin User
  owner_email: root@local.lan
  foreman_subnets: []
  foreman_interfaces:
  - mac: 52:54:01:74:ca:70
    ip: 192.168.122.128
    type: Interface
    name:
    attrs: {}
    virtual: false
    link: true
    identifier: eth0
    managed: true
    subnet:
environment: production
```

```
https://foreman17.local.lan/hosts/foreman17.local.lan/externalNodes?name=foreman17.local.lan <[1/1] All
```



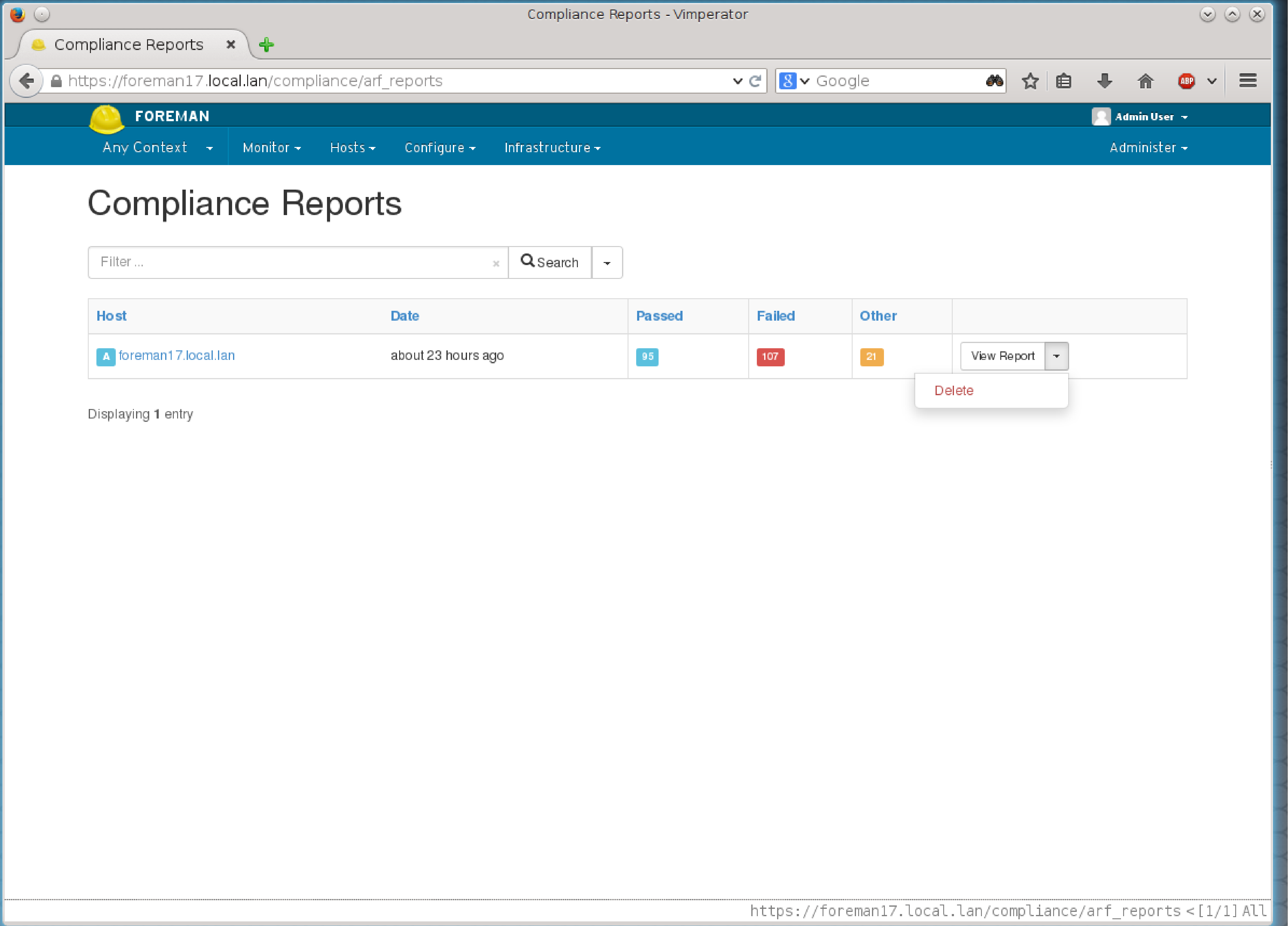
foreman17.local.lan

Show log messages: All messages

Reported at 2015-02-05 17:00:01 -0500

Level	Resource	message
notice	/Stage[main]/Foreman_scap_client/Package[foreman_scap_client]/ensure	created
notice	/File[foreman_scap_client]/ensure	created

config_retrieval	5.5083
file	0.0669
package	27.3352
service	0.2025
Total	**33.1138**

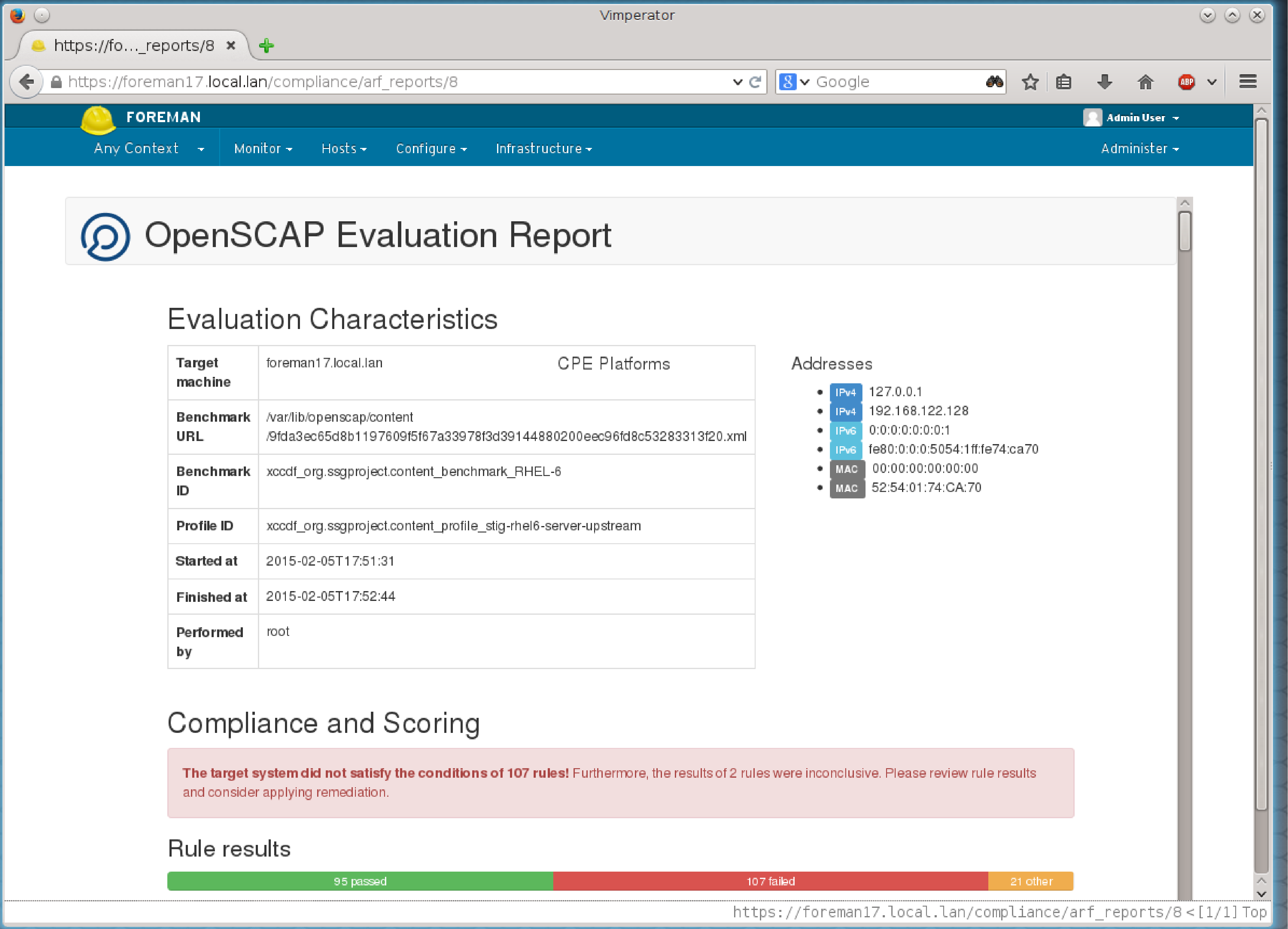

Compliance Reports - Vimperator
Compliance Reports
https://foreman17.local.lan/compliance/arf_reports
Google
FOREMAN
Admin User
Any Context
Monitor
Hosts
Configure
Infrastructure
Administer

Compliance Reports

Host	Date	Passed	Failed	Other	
A foreman17.local.lan	about 23 hours ago	95	107	21	View Report

Displaying **1** entry

https://foreman17.local.lan/compliance/arf_reports <[1/1] All



OpenSCAP Evaluation Report

Evaluation Characteristics

Target machine	foreman17.local.lan
Benchmark URL	/var/lib/openscap/content/9fda3ec65d8b1197609f5f67a33978f3d39144880200eec96fd8c53283313f20.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-6
Profile ID	xccdf_org.ssgproject.content_profile_stig-rhel6-server-upstream
Started at	2015-02-05T17:51:31
Finished at	2015-02-05T17:52:44
Performed by	root

CPE Platforms

Addresses

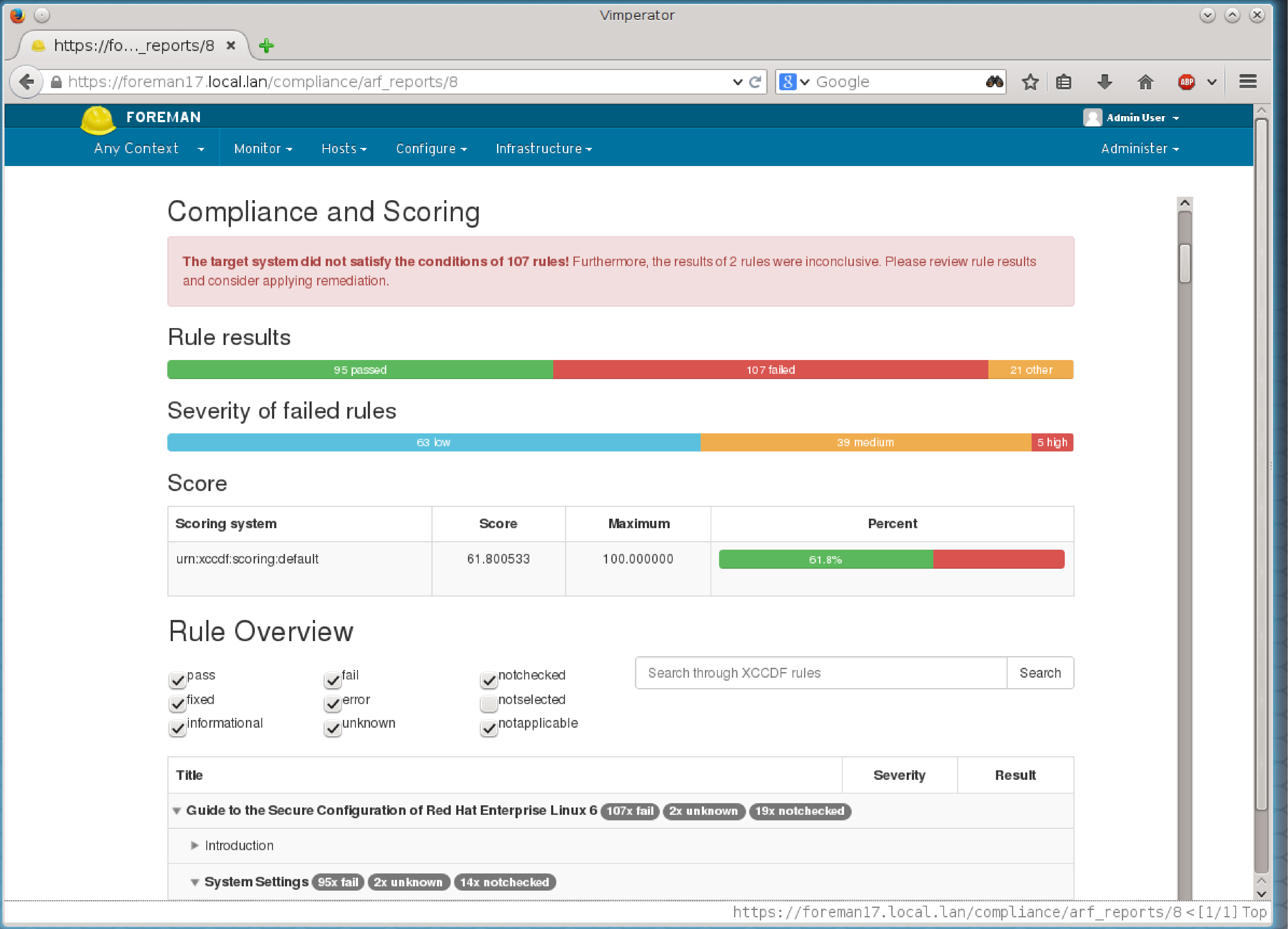
IPv4	127.0.0.1
IPv4	192.168.122.128
IPv6	0:0:0:0:0:0:0:1
IPv6	fe80:0:0:0:5054:1ff:fe74:ca70
MAC	00:00:00:00:00:00
MAC	52:54:01:74:CA:70

Compliance and Scoring

The target system did not satisfy the conditions of 107 rules! Furthermore, the results of 2 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

```
https://foreman17.local.lan/compliance/arf_reports/8 <[1/1] Top
```



Compliance and Scoring

The target system did not satisfy the conditions of 107 rules! Furthermore, the results of 2 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

95 passed | 107 failed | 21 other

Severity of failed rules

63 low | 39 medium | 5 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	61.800533	100.000000	61.8%

Rule Overview

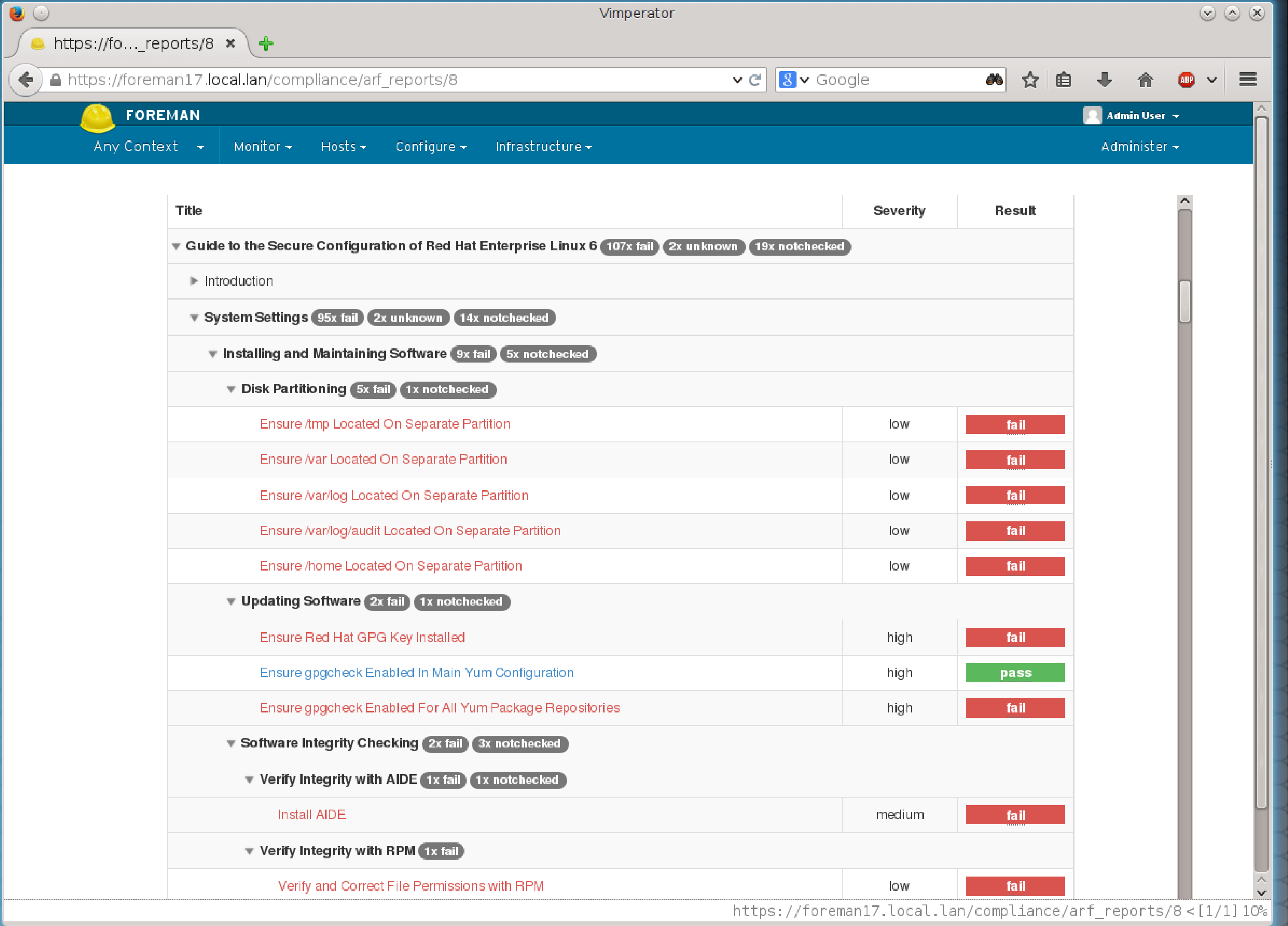
☑ pass
☑ fixed
☑ informational

☑ fail
☑ error
☑ unknown

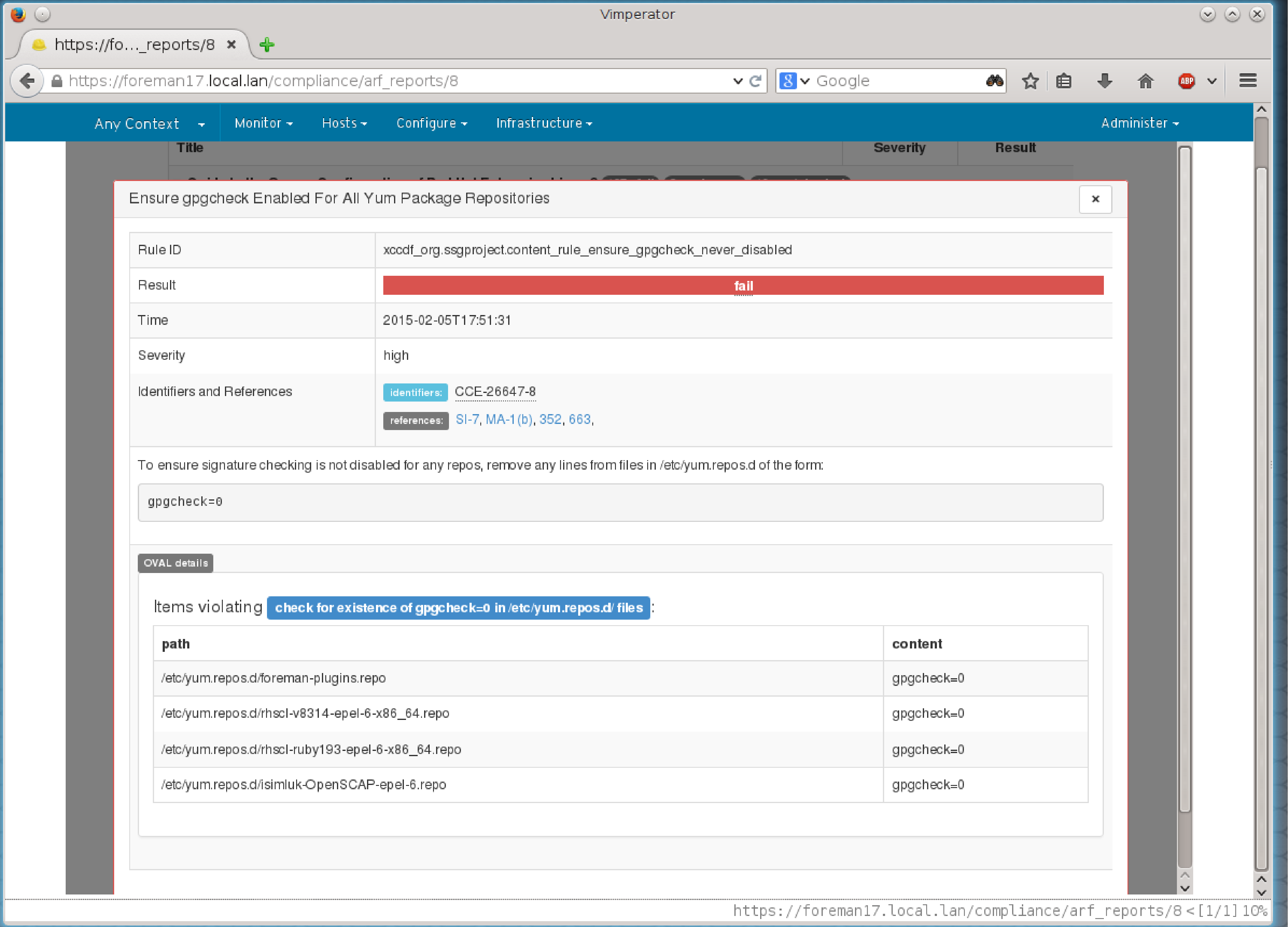
☑ notchecked
☐ notselected
☑ notapplicable

Title	Severity	Result
▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 6 107x fail 2x unknown 19x notchecked		
▶ Introduction		
▼ System Settings 95x fail 2x unknown 14x notchecked		

https://foreman17.local.lan/compliance/arf_reports/8 <[1/1] Top


Vimperator
https://fo..._reports/8
https://foreman17.local.lan/compliance/arf_reports/8
Google
FOREMAN
Admin User
Any Context
Monitor
Hosts
Configure
Infrastructure
Administer
https://foreman17.local.lan/compliance/arf_reports/8 <[1/1] 10%

Title	Severity	Result
▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 6 107x fail 2x unknown 19x notchecked		
▶ Introduction		
▼ System Settings 95x fail 2x unknown 14x notchecked		
▼ Installing and Maintaining Software 9x fail 5x notchecked		
▼ Disk Partitioning 5x fail 1x notchecked		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
Ensure /home Located On Separate Partition	low	fail
▼ Updating Software 2x fail 1x notchecked		
Ensure Red Hat GPG Key Installed	high	fail
Ensure gpgcheck Enabled In Main Yum Configuration	high	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	high	fail
▼ Software Integrity Checking 2x fail 3x notchecked		
▼ Verify Integrity with AIDE 1x fail 1x notchecked		
Install AIDE	medium	fail
▼ Verify Integrity with RPM 1x fail		
Verify and Correct File Permissions with RPM	low	fail


Vimperator
https://fo..._reports/8
https://foreman17.local.lan/compliance/arf_reports/8
Google
Any Context
Monitor
Hosts
Configure
Infrastructure
Administer
Title
Severity
Result
https://foreman17.local.lan/compliance/arf_reports/8 <[1/1] 10%

Ensure gpgcheck Enabled For All Yum Package Repositories

×

Rule ID	xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disabled
Result	fail
Time	2015-02-05T17:51:31
Severity	high
Identifiers and References	identifiers: CCE-26647-8 references: SI-7, MA-1(b), 352, 663,

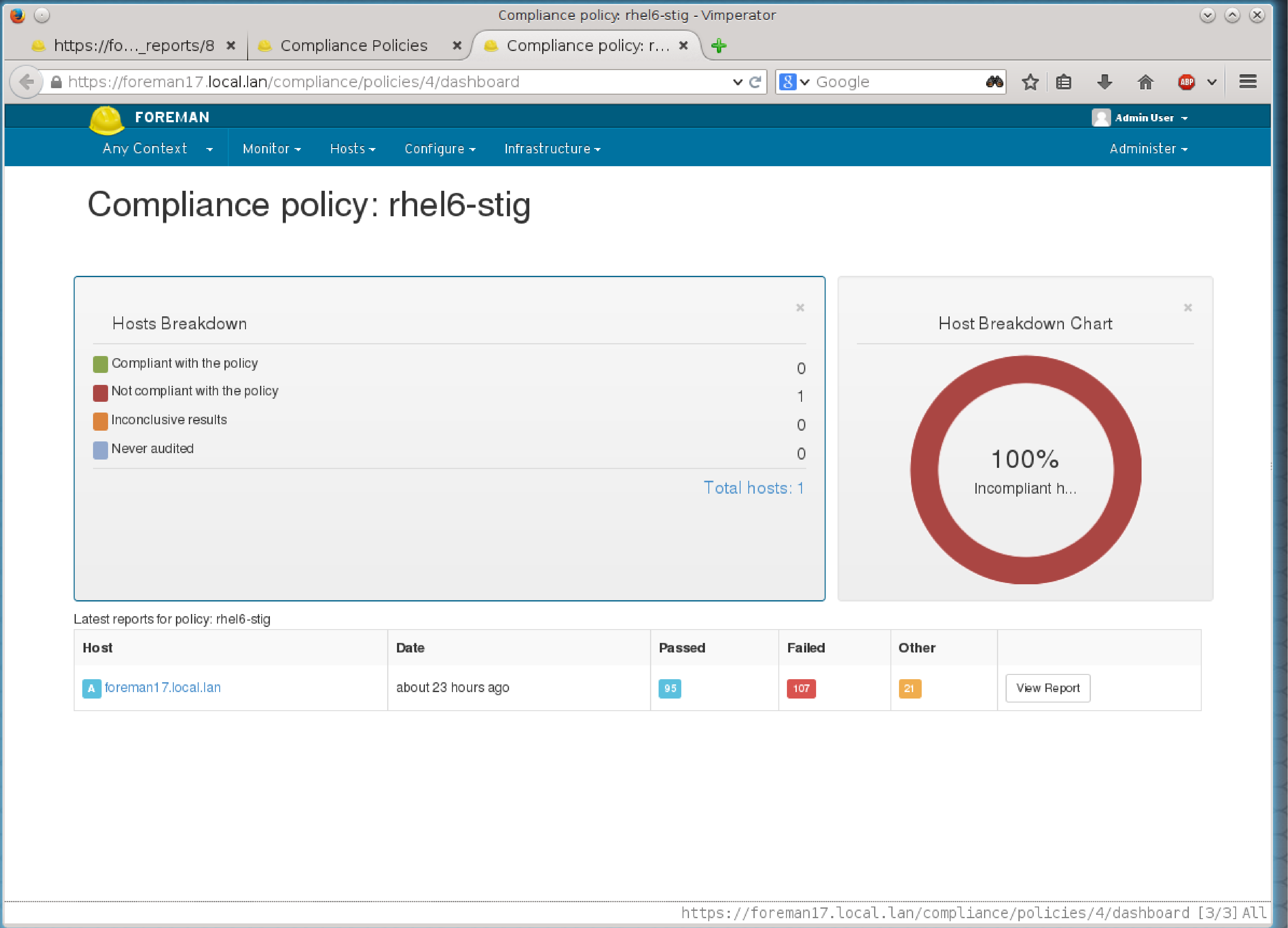
To ensure signature checking is not disabled for any repos, remove any lines from files in /etc/yum.repos.d of the form:

```
gpgcheck=0
```

OVAL details

Items violating check for existence of gpgcheck=0 in /etc/yum.repos.d/ files:

path	content
/etc/yum.repos.d/foreman-plugins.repo	gpgcheck=0
/etc/yum.repos.d/rhscl-v8314-epel-6-x86_64.repo	gpgcheck=0
/etc/yum.repos.d/rhscl-ruby193-epel-6-x86_64.repo	gpgcheck=0
/etc/yum.repos.d/isimluk-OpenSCAP-epel-6.repo	gpgcheck=0


Compliance policy: rhel6-stig - Vimperator
https://fo..._reports/8
Compliance Policies
Compliance policy: r...
https://foreman17.local.lan/compliance/policies/4/dashboard
Google
FOREMAN
Admin User
Any Context
Monitor
Hosts
Configure
Infrastructure
Administer

Compliance policy: rhel6-stig

Hosts Breakdown

🟩 Compliant with the policy	0
🟥 Not compliant with the policy	1
🟧 Inconclusive results	0
🟦 Never audited	0

Total hosts: 1

Host Breakdown Chart

Latest reports for policy: rhel6-stig

Host	Date	Passed	Failed	Other	
A foreman17.local.lan	about 23 hours ago	95	107	21	View Report

https://foreman17.local.lan/compliance/policies/4/dashboard [3/3] All

Summary

1. Compliance tools for endpoins
2. Requirements for compliance center
3. SCAPtimony project
4. SCAPtimony within Foreman

Questions?

Contact:
isimluk@fedoraproject.org

Licensed to the public under a Creative Commons Attribution 4.0 license.