System Compliance Checks

Šimon Lukašík
Martin Preisler

Agenda

- What is computer compliance
- Automation -- SCAP
- SCAP Content creation
- Existing SCAP content
- opensource SCAP projects
- scap-workbench
- Anaconda integration
- Spacewalk integration

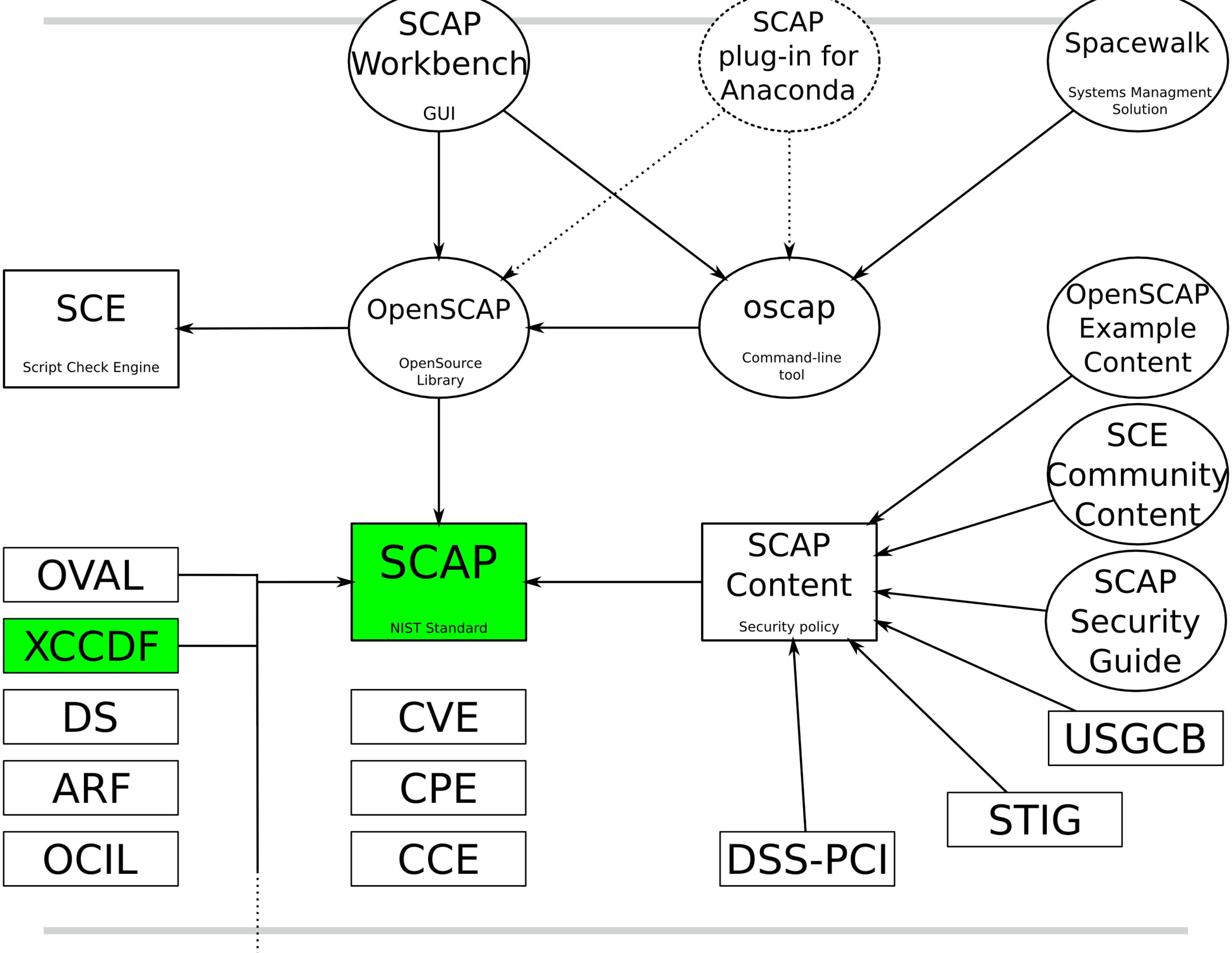
Compliance audit

- Proactive security
- Security policy
- Computers follow all rules in a policy
- Why would you do that?
  - Government regulations
  - FISMA Act.
  - ISO/EIC 27000 standard series

MEETING IN PROGRESS
SMEP
DISA
SMAP
SHA
MDF
CWE
ICANN
SSL
CWSS
CA
NIST
ASLR
SSSD
CEE
AES
XCCDF
ECID
NIAP
OVAL
RHEL
MITRE
DES
FIPS
STIG
GS
GCB
CCE
MCS
NSS
GCM
DSS
GPOS
NTLM
PAM
CC
MLS
OFB
HBSS
DISA
RNG
DAC
API
SCAP
XTS
TNC
EUID
ECC
MAC
WTF?!
DON'T WORRY.

SECURITY

No acronyms. No security. No problem.



SCAP Workbench
GUI

SCAP plug-in for Anaconda

Spacewalk
Systems Managment Solution

SCE
Script Check Engine

OpenSCAP
OpenSource Library

oscap
Command-line tool

OpenSCAP Example Content

SCE Community Content

SCAP Security Guide

SCAP
NIST Standard

SCAP Content
Security policy

OVAL

XCCDF

DS

ARF

OCIL

CVE

CPE

CCE

USGCB

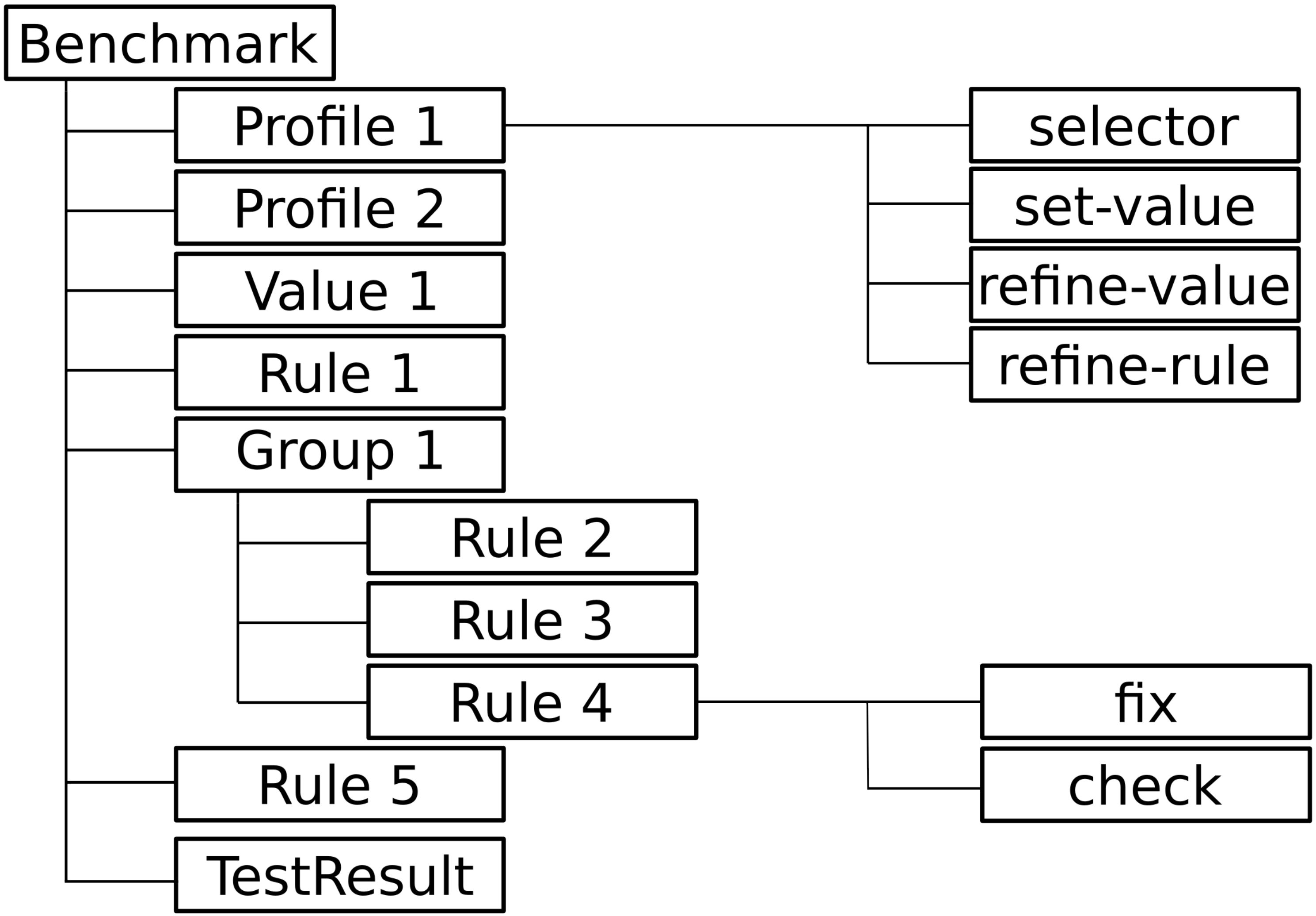
STIG

DSS-PCI

What is SCAP?

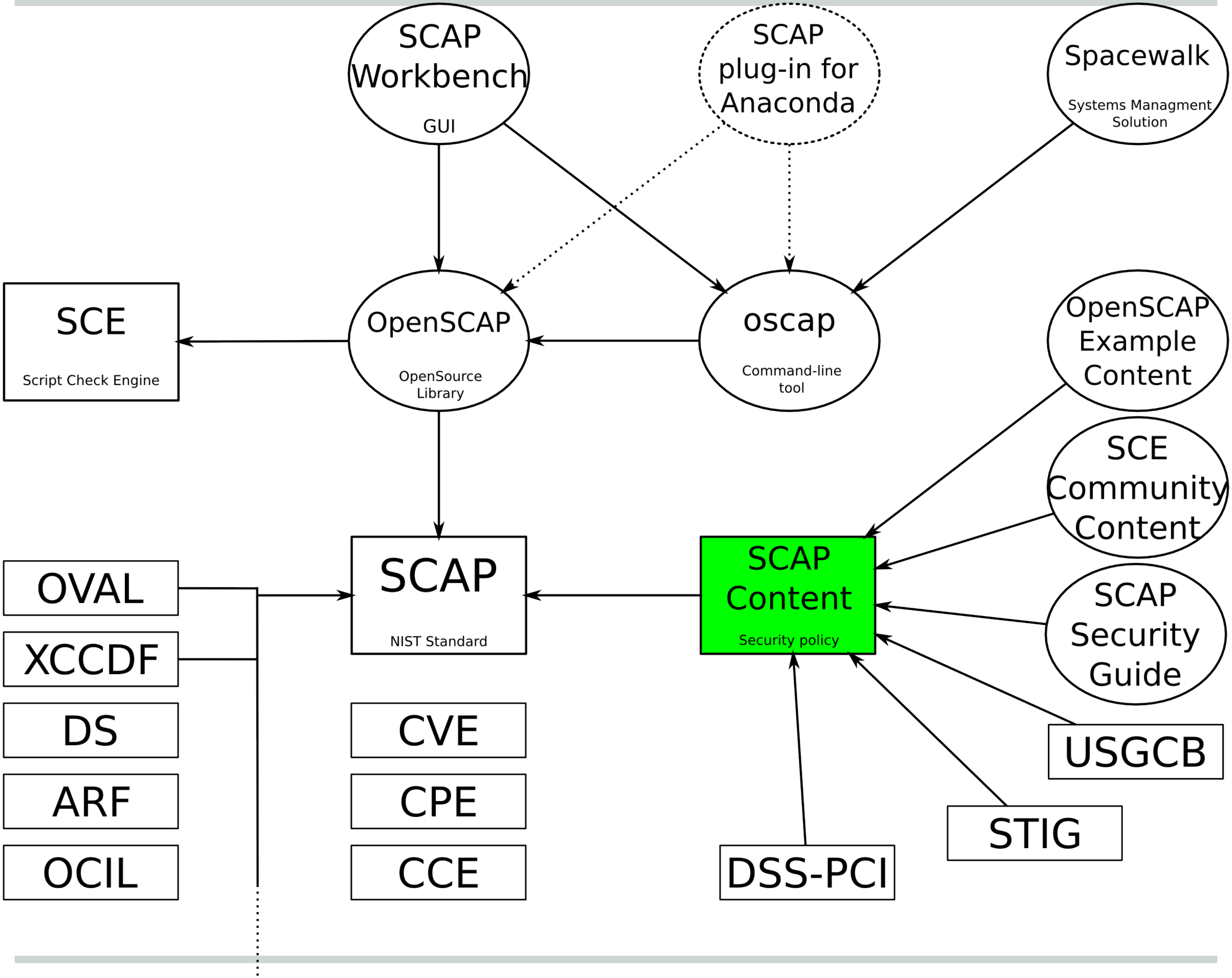
- Group of many standards
- Automated compliance checking
- Governed by NIST
  - http://scap.nist.gov/
  - Industry standard
- Current version: 1.2
- Component Standards: XCCDF, OVAL, OCIL, AI, DataStream, ARF, CCE, CPE, CVE, CVSS, TMSAD

XCCDF structure



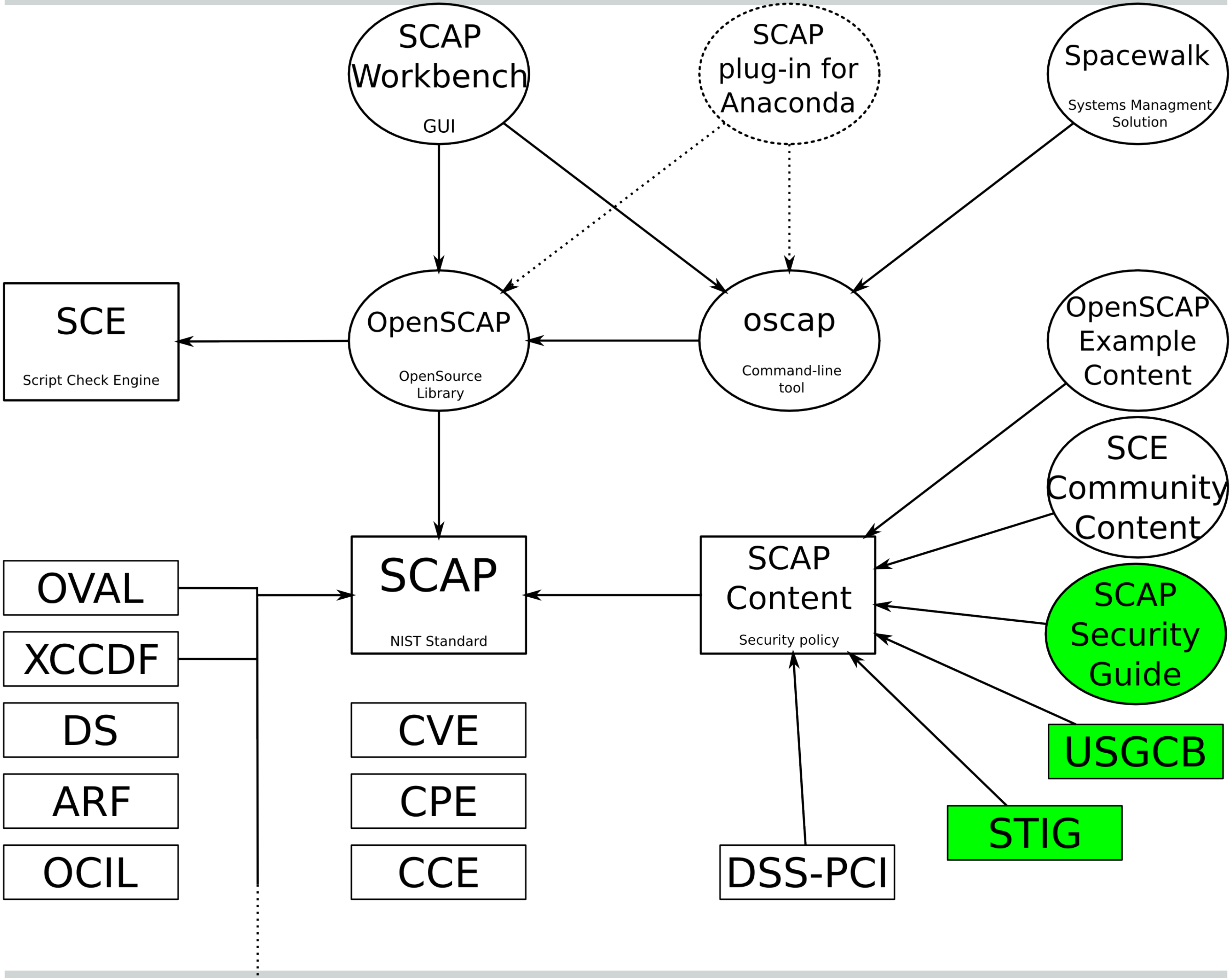
Example of XCCDF Rule

```
<Rule id="sshd_disable_root_login">
  <title>Disable SSH Root Login</title>
  <ident>CCE-27100-7</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref
            href="ssg-rhel6-oval.xml"
            name="oval:ssg:def:905"/>
    </check>
</Rule>
```


SCAP Workbench
GUI
SCAP plug-in for Anaconda
Spacewalk
Systems Managment Solution
SCE
Script Check Engine
OpenSCAP
OpenSource Library
oscap
Command-line tool
OpenSCAP Example Content
SCE Community Content
SCAP Security Guide
OVAL
XCCDF
DS
ARF
OCIL
SCAP
NIST Standard
SCAP Content
Security policy
CVE
CPE
CCE
USGCB
STIG
DSS-PCI

SCAP Security Policy Customization

- Hand editing
  - cross referencing IDs is hard
- GUI tool editing
  - does not scale to multiple authors
  - very problematic versioning - few huge files
  - editing being dropped from workbench
- Generating from smaller files
  - used by SSG
  - easier collaboration of multiple authors
  - easier versioning



SCAP Workbench

GUI

SCAP plug-in for Anaconda

Spacewalk

Systems Managment Solution

SCE

Script Check Engine

OpenSCAP

OpenSource Library

oscap

Command-line tool

OpenSCAP Example Content

SCE Community Content

SCAP

NIST Standard

SCAP Content

Security policy

SCAP Security Guide

OVAL

XCCDF

DS

ARF

OCIL

CVE

CPE

CCE

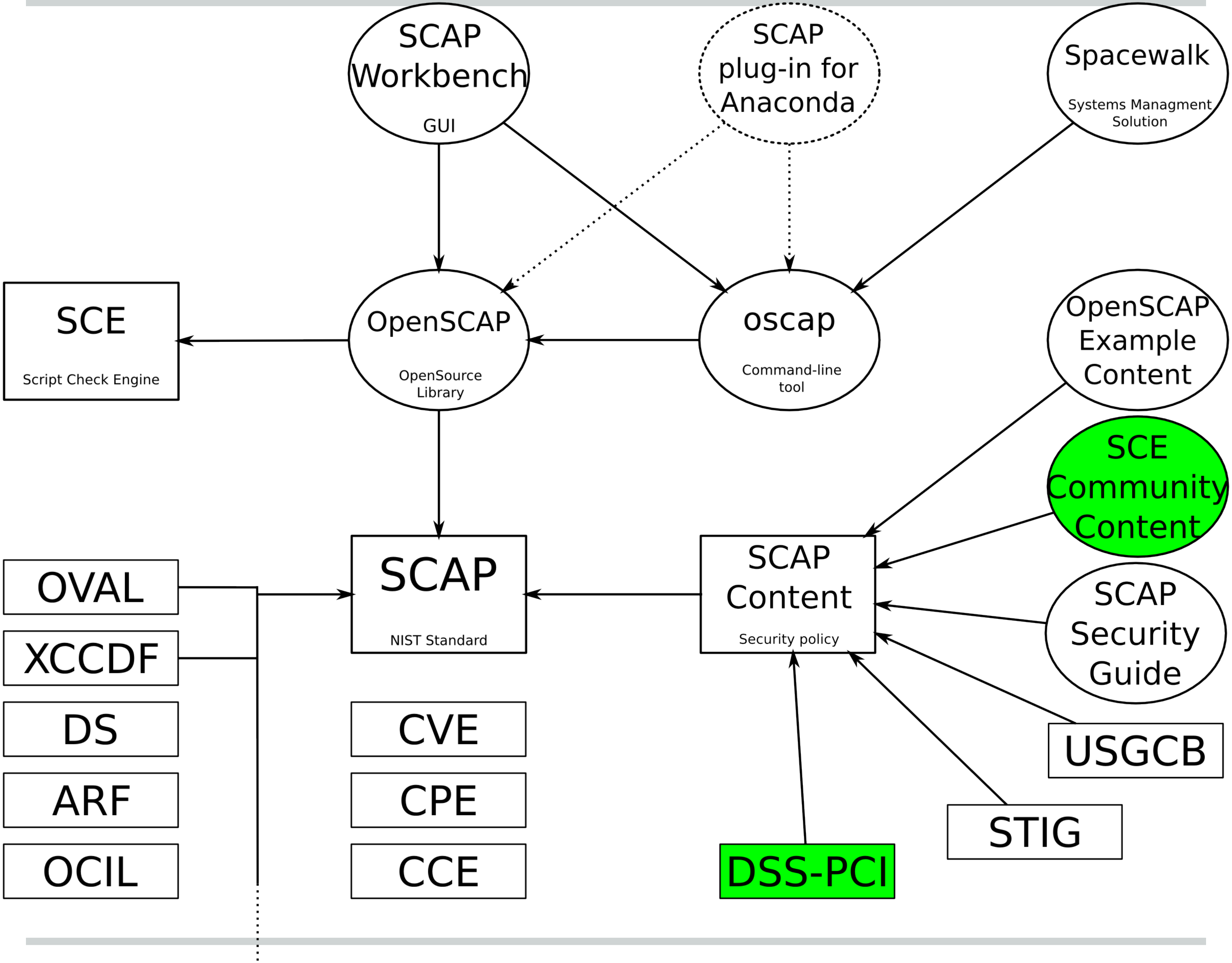
USGCB

STIG

DSS-PCI

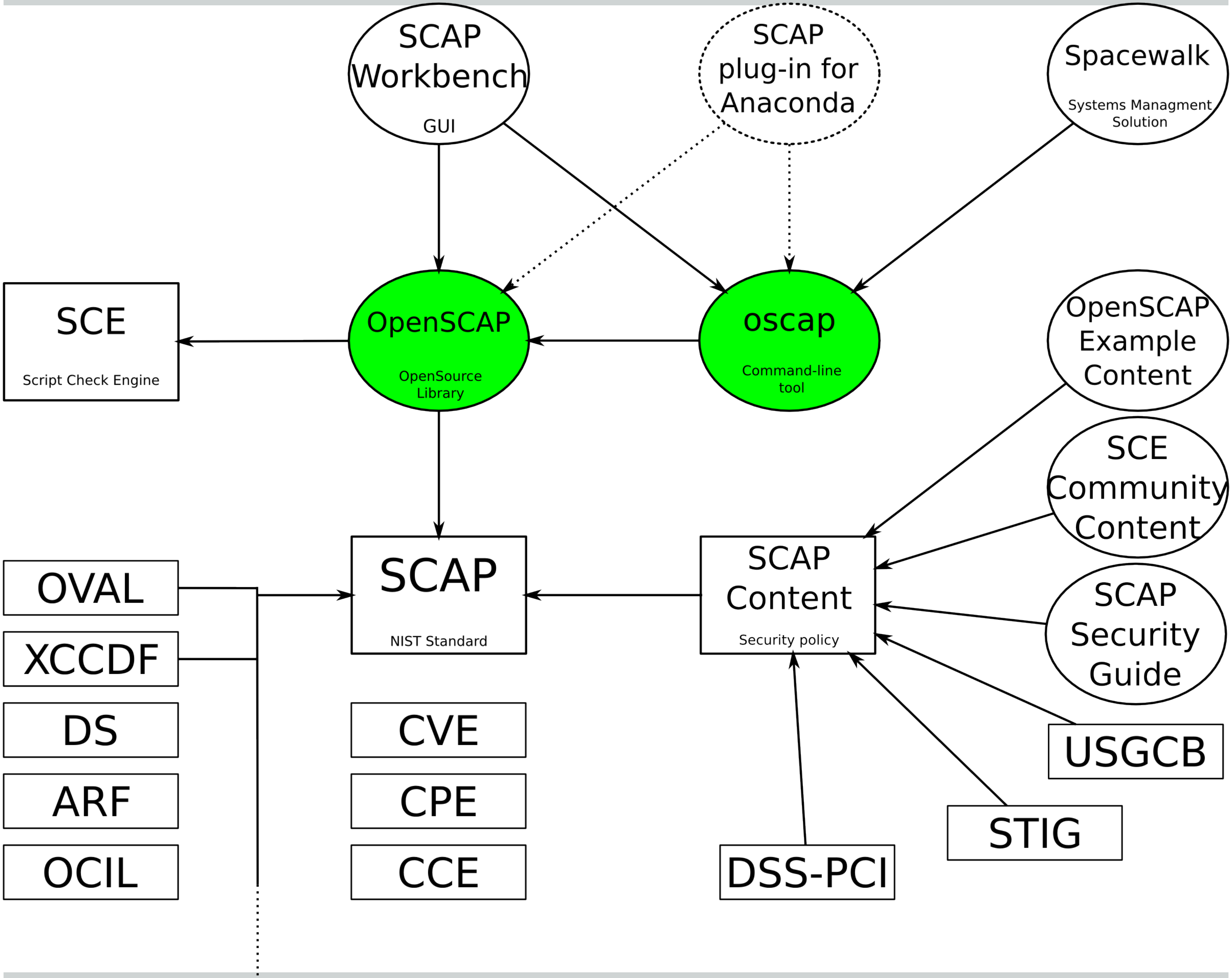
SCAP Security Guide

- Uses OVAL for checks
- Multiple security baselines in a single SCAP content
- Red Hat Enterprise Linux 6
  - Server, DISA STIG Server
  - Desktop
  - FTP Server
- JBoss Enterprise Application Server


SCAP Workbench
GUI
SCAP plug-in for Anaconda
Spacewalk
Systems Managment Solution
SCE
Script Check Engine
OpenSCAP
OpenSource Library
oscap
Command-line tool
OpenSCAP Example Content
SCE Community Content
OVAL
XCCDF
DS
ARF
OCIL
SCAP
NIST Standard
SCAP Content
Security policy
SCAP Security Guide
CVE
CPE
CCE
USGCB
STIG
DSS-PCI

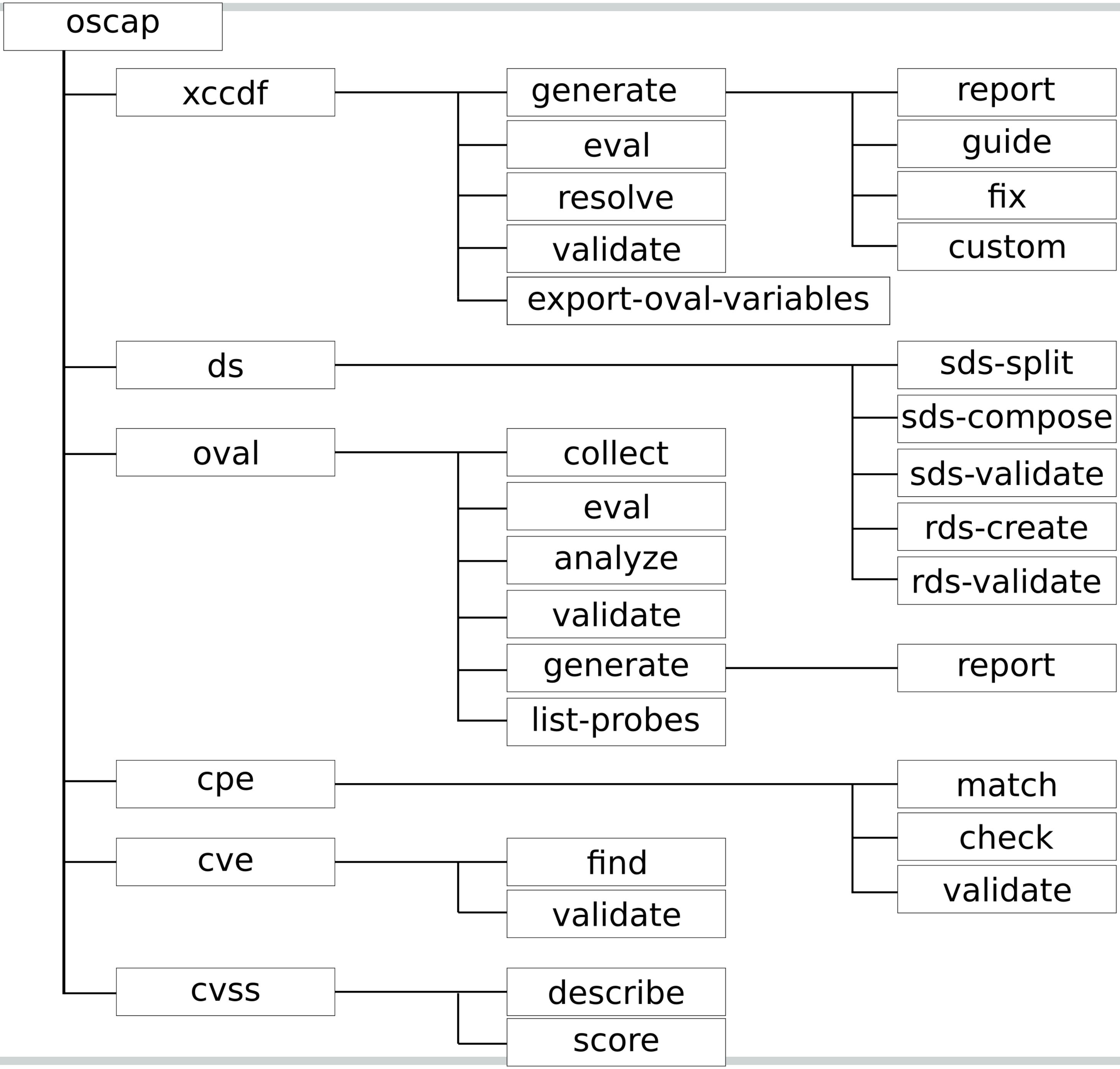
SCE Community Content

- Uses bash scripts
- DSS-PCI is being added
- Fix tags are revised and added

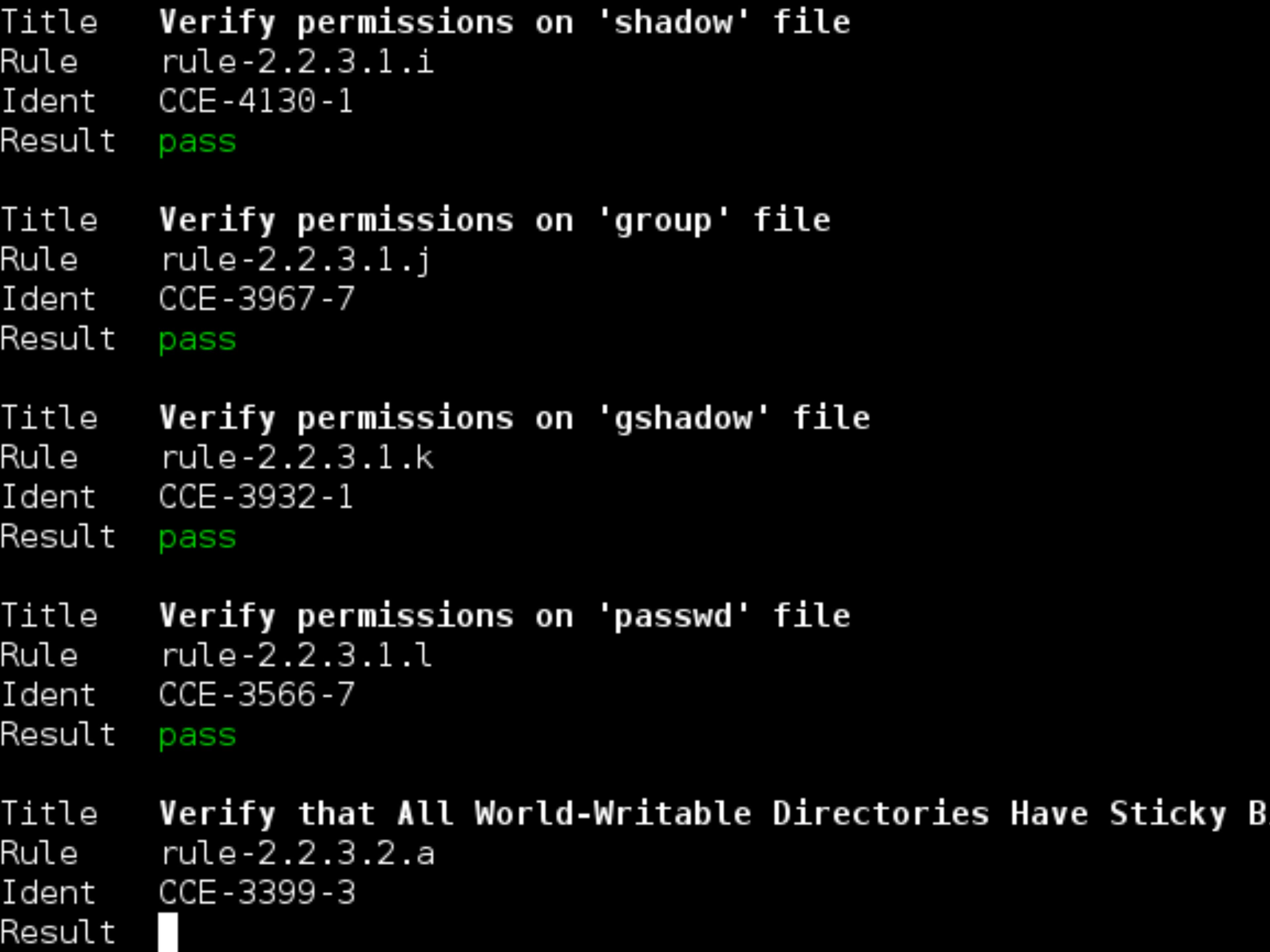

SCAP Workbench
GUI
SCAP plug-in for Anaconda
Spacewalk
Systems Managment Solution
SCE
Script Check Engine
OpenSCAP
OpenSource Library
oscap
Command-line tool
OpenSCAP Example Content
SCE Community Content
SCAP Security Guide
OVAL
XCCDF
DS
ARF
OCIL
SCAP
NIST Standard
CVE
CPE
CCE
SCAP Content
Security policy
USGCB
STIG
DSS-PCI

OpenSCAP

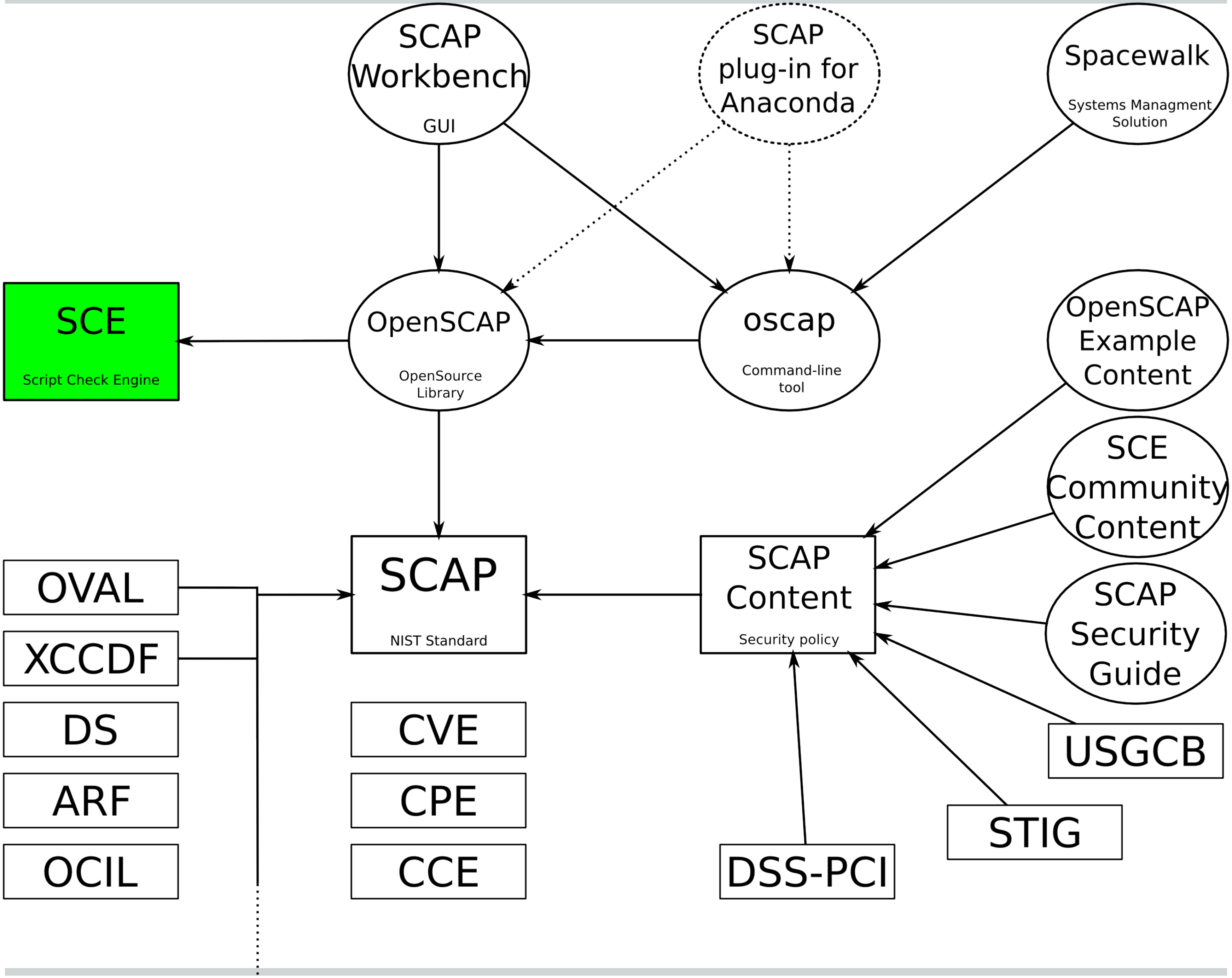
- LGPL library
- SCAP 1.2 support
  - XCCDF 1.2
  - OVAL 5.10.1
  - CPE applicability
  - datastream support
  - preview of remediation
- High-level API
- oscap command line tool



oscap
xccdf
generate
report
guide
fix
custom
eval
resolve
validate
export-oval-variables
ds
sds-split
sds-compose
sds-validate
rds-create
rds-validate
oval
collect
eval
analyze
validate
generate
report
list-probes
cpe
match
check
validate
cve
find
validate
cvss
describe
score

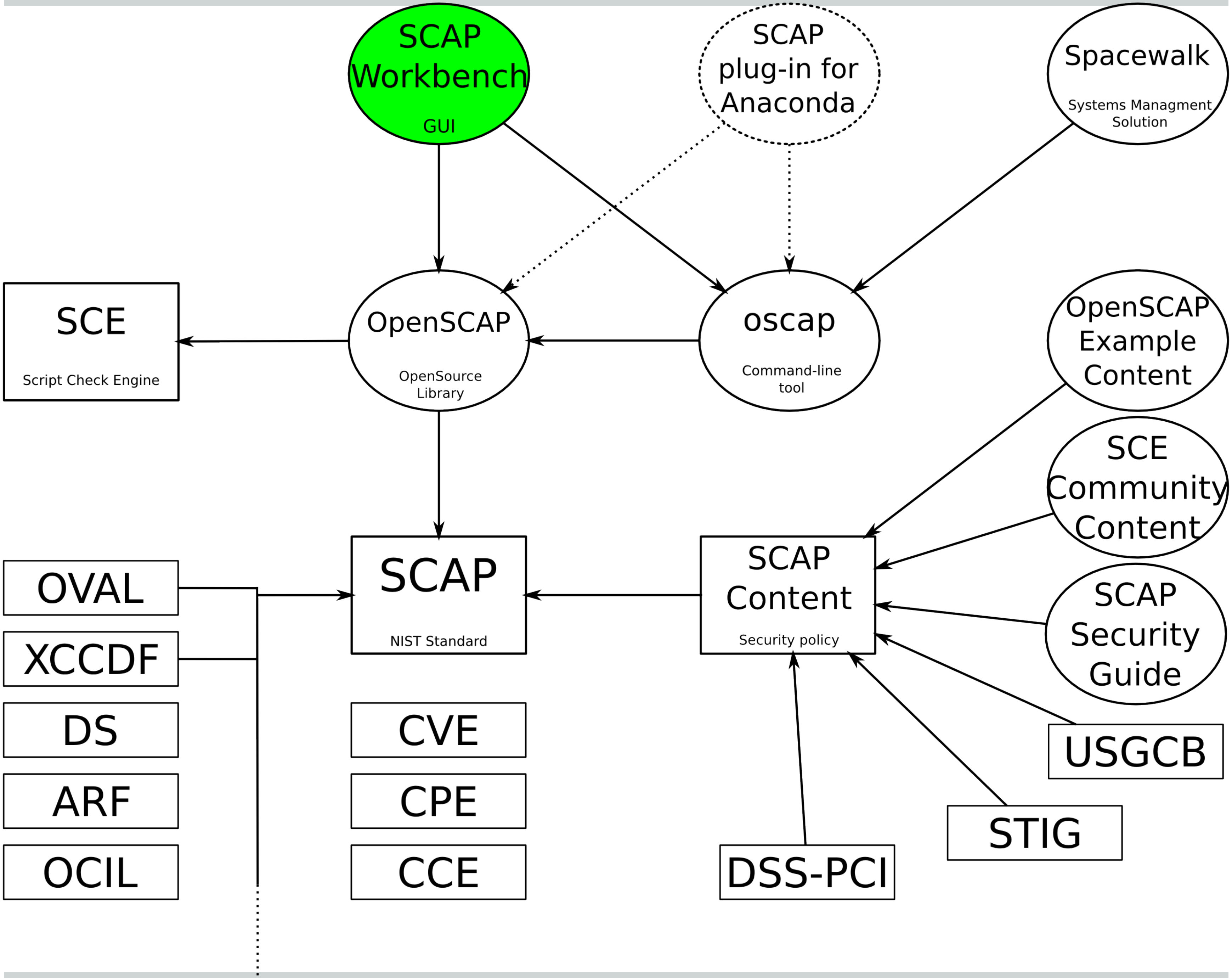


```
Title   Verify permissions on 'shadow' file
Rule    rule-2.2.3.1.i
Ident   CCE-4130-1
Result  pass

Title   Verify permissions on 'group' file
Rule    rule-2.2.3.1.j
Ident   CCE-3967-7
Result  pass

Title   Verify permissions on 'gshadow' file
Rule    rule-2.2.3.1.k
Ident   CCE-3932-1
Result  pass

Title   Verify permissions on 'passwd' file
Rule    rule-2.2.3.1.l
Ident   CCE-3566-7
Result  pass

Title   Verify that All World-Writable Directories Have Sticky B
Rule    rule-2.2.3.2.a
Ident   CCE-3399-3
Result  
```


SCAP Workbench
GUI
SCAP plug-in for Anaconda
Spacewalk
Systems Managment Solution
SCE
Script Check Engine
OpenSCAP
OpenSource Library
oscap
Command-line tool
OpenSCAP Example Content
SCE Community Content
OVAL
XCCDF
DS
ARF
OCIL
SCAP
NIST Standard
SCAP Content
Security policy
SCAP Security Guide
CVE
CPE
CCE
USGCB
STIG
DSS-PCI

SCE: Script Check Engine

- Our own simple standard
- Use any executable file as a check
- Map exit code to XCCDF result
- Configure time option in openscap
  - defaults to disabled
- Two independent implementations
  - openscap
  - jOVAL


SCAP Workbench
GUI
SCAP plug-in for Anaconda
Spacewalk
Systems Managment Solution
SCE
Script Check Engine
OpenSCAP
OpenSource Library
oscap
Command-line tool
OpenSCAP Example Content
SCE Community Content
SCAP Security Guide
OVAL
XCCDF
DS
ARF
OCIL
SCAP
NIST Standard
CVE
CPE
CCE
SCAP Content
Security policy
USGCB
STIG
DSS-PCI

Issues of scap-workbench

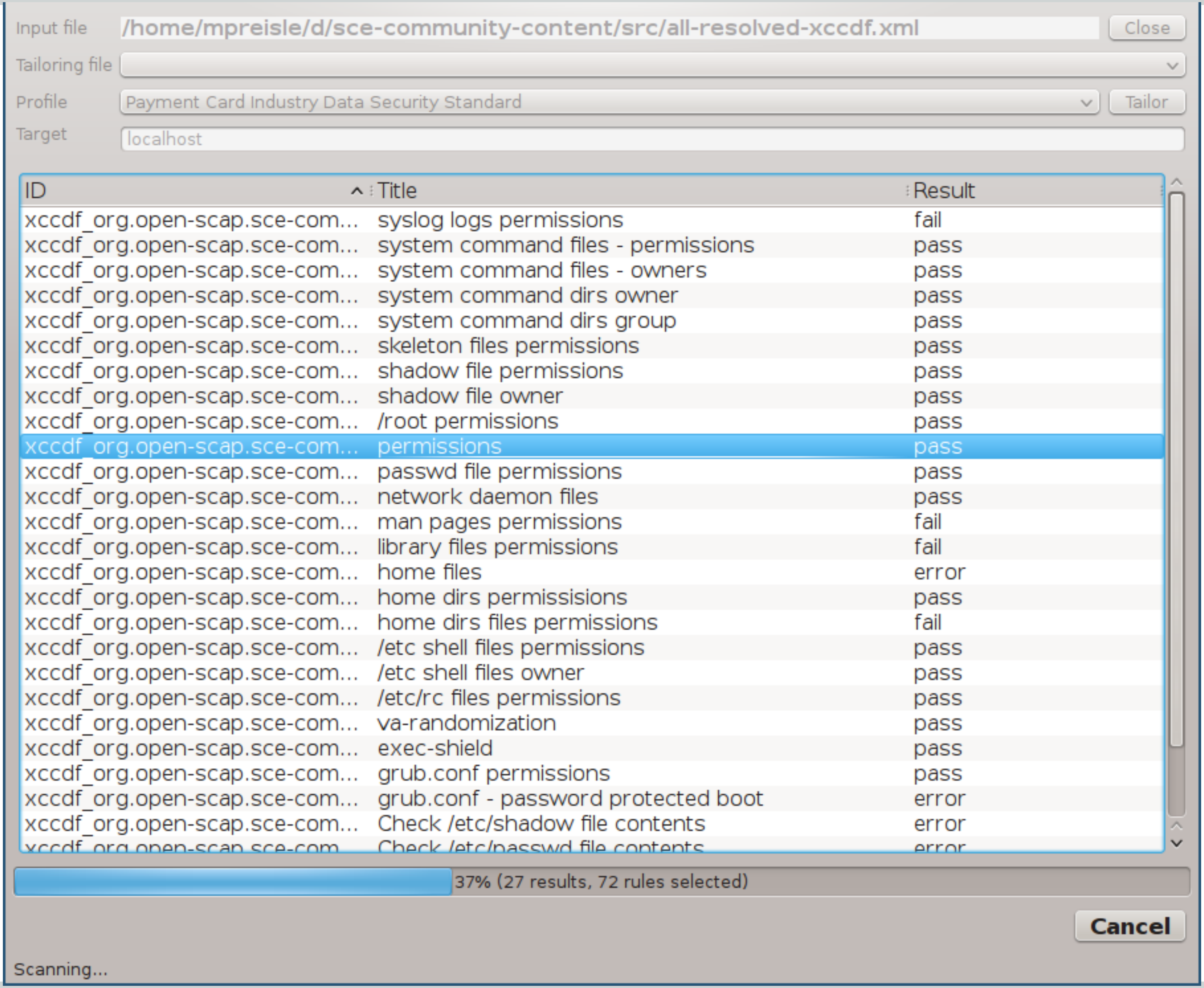
- Tailoring not according to specification
- No datastream support
- No remote scanning support
- Prone to openscap changes
- Python bindings breakage
- Large codebase
  - a substantial part of it is the editor

Redesigning scap-workbench

- Much smaller codebase
  - in C++, using Qt4
- Uses high-level API from openscap
  - less opportunity for breakage
  - datastream support
- Scans via the 'oscap' tool
  - less opportunity for breakage
  - only the 'oscap' tool needs to be certified

Typical scanner usage

1. Open content
2. Select profile
3. Select target machine
4. Scan
5. Collect results



Input file /home/mpreisle/d/sce-community-content/src/all-resolved-xccdf.xml

Tailoring file

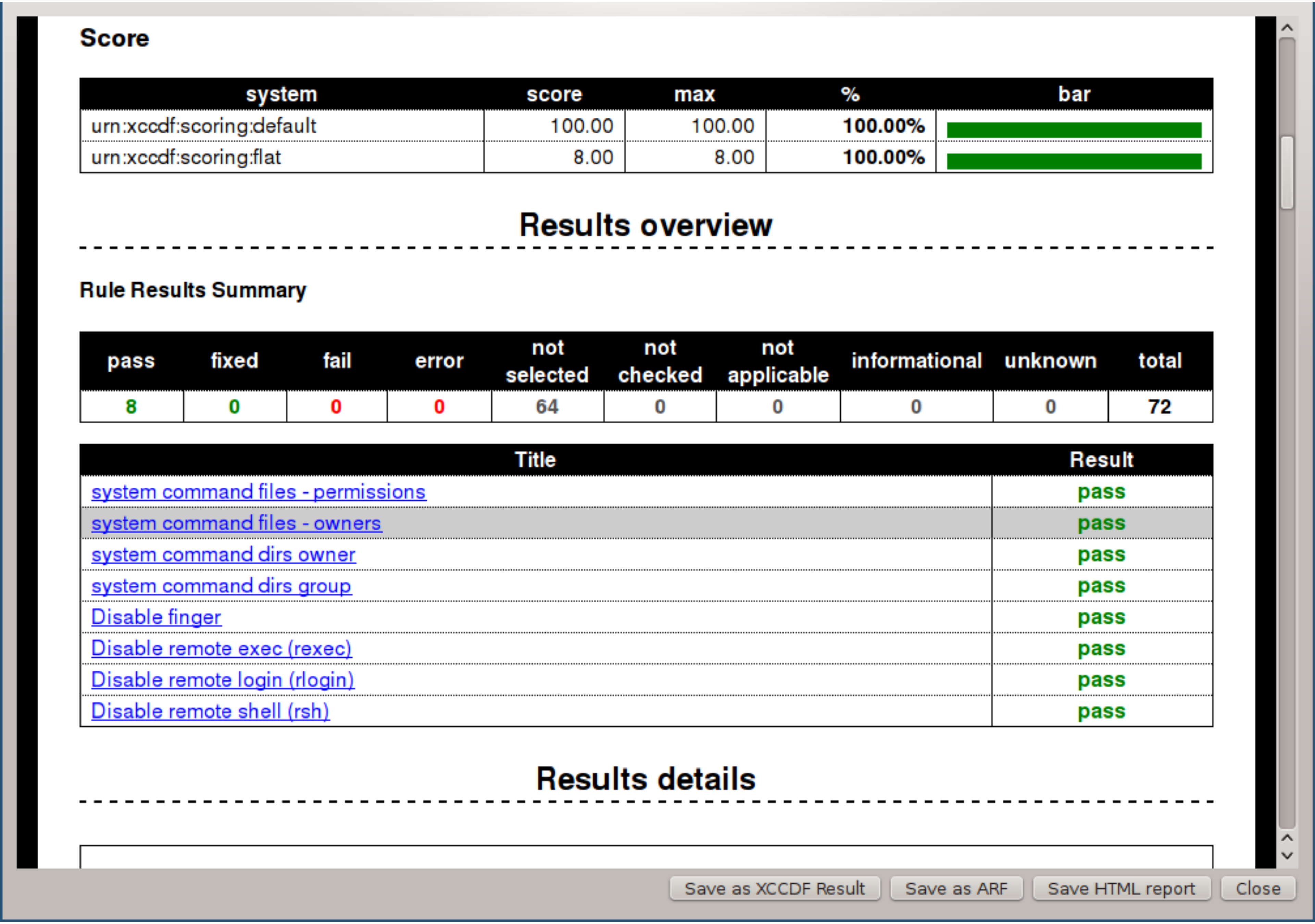
Profile Payment Card Industry Data Security Standard

Target localhost

ID	Title	Result
xccdf_org.open-scap.sce-com...	syslog logs permissions	fail
xccdf_org.open-scap.sce-com...	system command files - permissions	pass
xccdf_org.open-scap.sce-com...	system command files - owners	pass
xccdf_org.open-scap.sce-com...	system command dirs owner	pass
xccdf_org.open-scap.sce-com...	system command dirs group	pass
xccdf_org.open-scap.sce-com...	skeleton files permissions	pass
xccdf_org.open-scap.sce-com...	shadow file permissions	pass
xccdf_org.open-scap.sce-com...	shadow file owner	pass
xccdf_org.open-scap.sce-com...	/root permissions	pass
xccdf_org.open-scap.sce-com...	permissions	pass
xccdf_org.open-scap.sce-com...	passwd file permissions	pass
xccdf_org.open-scap.sce-com...	network daemon files	pass
xccdf_org.open-scap.sce-com...	man pages permissions	fail
xccdf_org.open-scap.sce-com...	library files permissions	fail
xccdf_org.open-scap.sce-com...	home files	error
xccdf_org.open-scap.sce-com...	home dirs permissions	pass
xccdf_org.open-scap.sce-com...	home dirs files permissions	fail
xccdf_org.open-scap.sce-com...	/etc shell files permissions	pass
xccdf_org.open-scap.sce-com...	/etc shell files owner	pass
xccdf_org.open-scap.sce-com...	/etc/rc files permissions	pass
xccdf_org.open-scap.sce-com...	va-randomization	pass
xccdf_org.open-scap.sce-com...	exec-shield	pass
xccdf_org.open-scap.sce-com...	grub.conf permissions	pass
xccdf_org.open-scap.sce-com...	grub.conf - password protected boot	error
xccdf_org.open-scap.sce-com...	Check /etc/shadow file contents	error
xccdf_org.open-scap.sce-com...	Check /etc/passwd file contents	error

37% (27 results, 72 rules selected)

Scanning...



Score

system	score	max	%	bar
urn:xccdf:scoring:default	100.00	100.00	**100.00%**	🟩
urn:xccdf:scoring:flat	8.00	8.00	**100.00%**	🟩

Results overview

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
8	0	0	0	64	0	0	0	0	72

Title	Result
system command files - permissions	pass
system command files - owners	pass
system command dirs owner	pass
system command dirs group	pass
Disable finger	pass
Disable remote exec (rexec)	pass
Disable remote login (rlogin)	pass
Disable remote shell (rsh)	pass

Results details

Remote scanning

- Requires oscap and sshd on remote machine

How does it work?

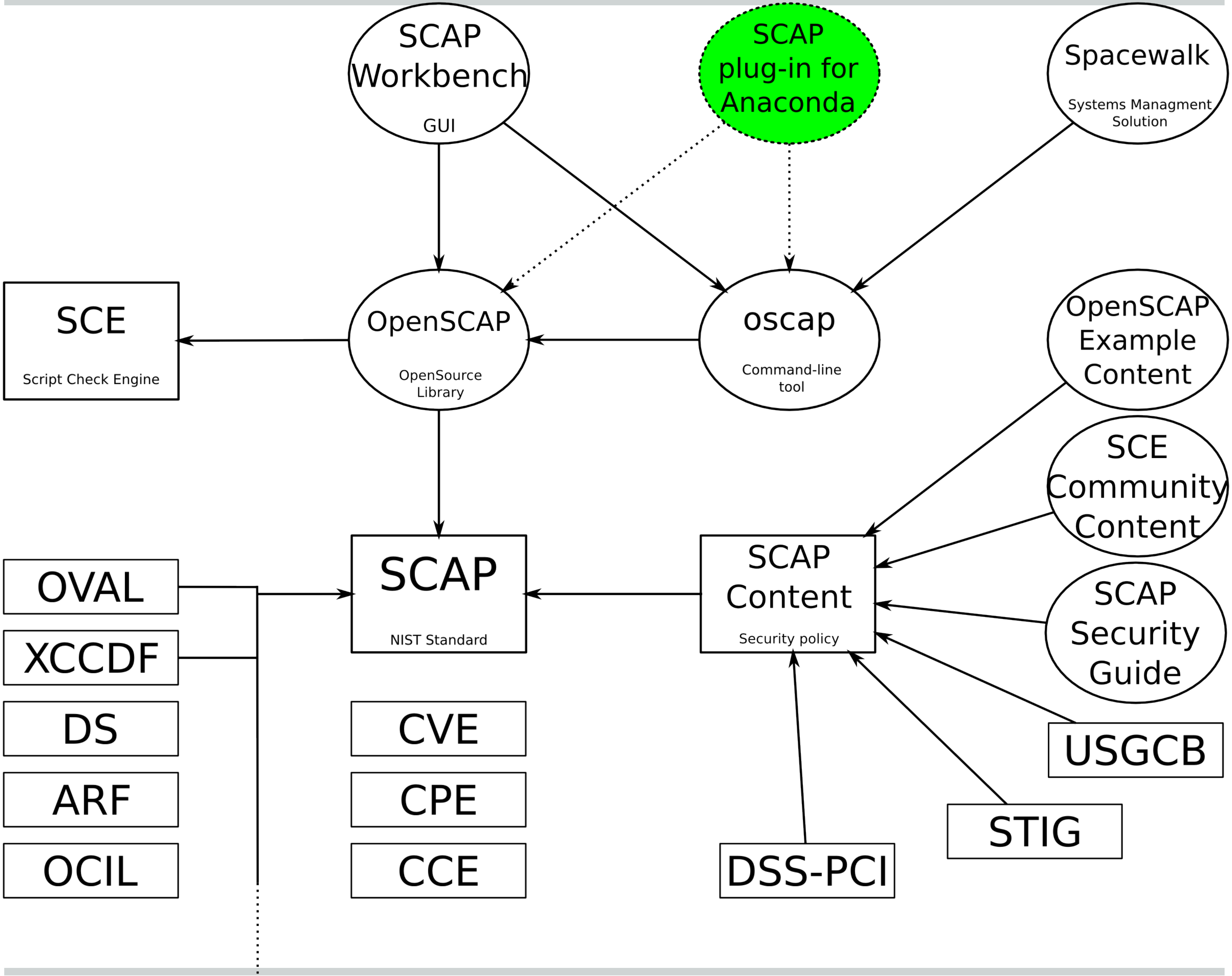
1. Copy local content over
2. Run oscap on the remote machine
3. Transfer results to the local machine
4. Interpret results locally

Features to avoid in workbench

- Scanning multiple machines at once
  - use Spacewalk instead
- Content editing
  - very hard to implement
  - proven not to be useful for complex content

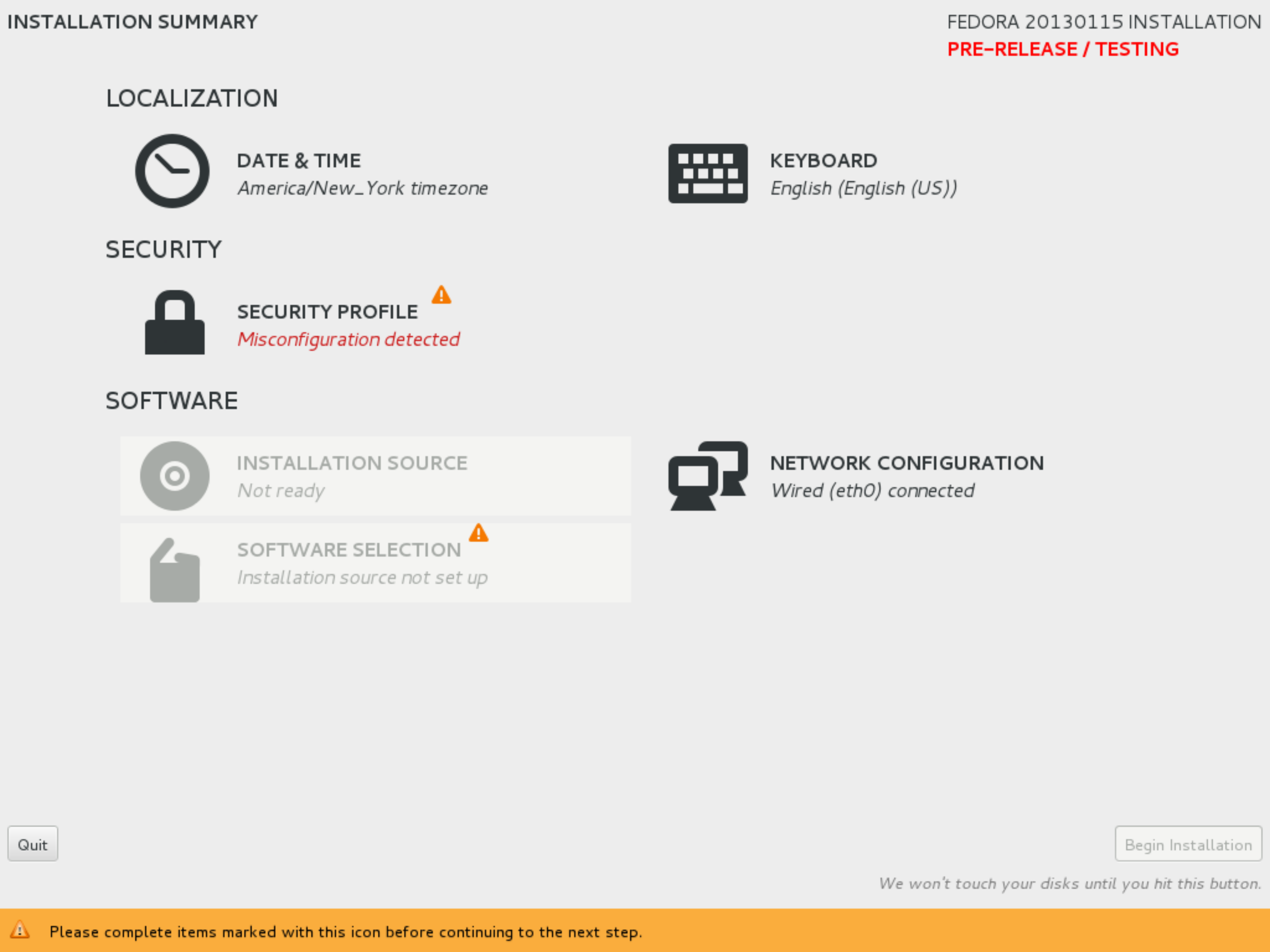
Where to find the new workbench?

- 'rewrite' branch in the workbench repo
    - git://git.fedorahosted.org/git/scap-workbench.git
- Suggestions and testing appreciated :-)
- Might be moved elsewhere in the future


SCAP Workbench
GUI
SCAP plug-in for Anaconda
Spacewalk
Systems Managment Solution
SCE
Script Check Engine
OpenSCAP
OpenSource Library
oscap
Command-line tool
OpenSCAP Example Content
SCE Community Content
SCAP Security Guide
SCAP
NIST Standard
SCAP Content
Security policy
OVAL
XCCDF
DS
ARF
OCIL
CVE
CPE
CCE
USGCB
STIG
DSS-PCI

Anaconda plug-in

- *Not fully implemented yet*
- Kickstart addon
- Making sure a machine is in compliance before it boots
- Value in integration and ease of use



INSTALLATION SUMMARY

FEDORA 20130115 INSTALLATION
PRE-RELEASE / TESTING

LOCALIZATION

DATE & TIME
America/New_York timezone

KEYBOARD
English (English (US))

SECURITY

SECURITY PROFILE ⚠
Misconfiguration detected

SOFTWARE

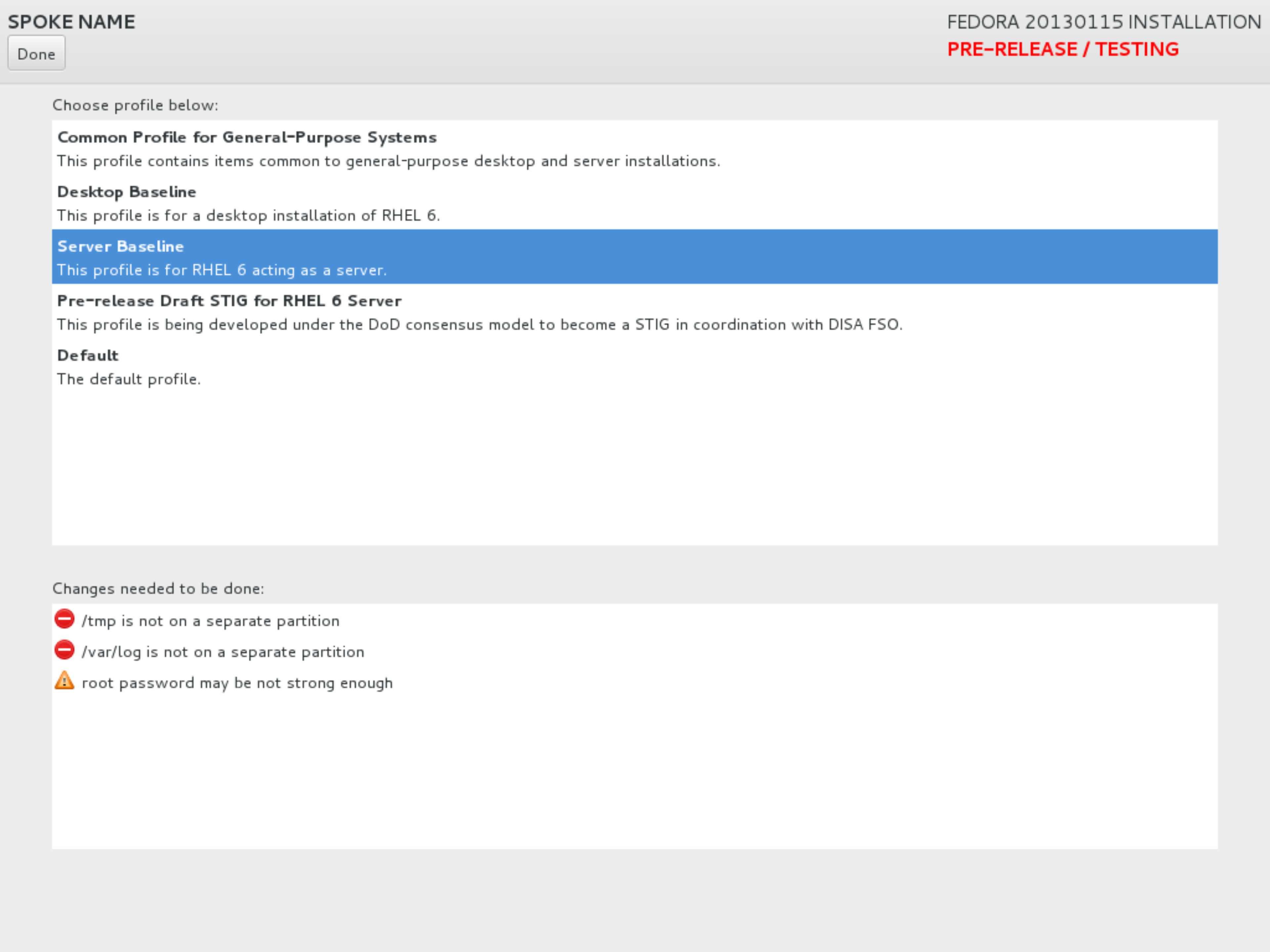
INSTALLATION SOURCE
Not ready

NETWORK CONFIGURATION
Wired (eth0) connected

SOFTWARE SELECTION ⚠
Installation source not set up

We won't touch your disks until you hit this button.

⚠ Please complete items marked with this icon before continuing to the next step.



Choose profile below:

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

Desktop Baseline
This profile is for a desktop installation of RHEL 6.

Server Baseline
This profile is for RHEL 6 acting as a server.

Pre-release Draft STIG for RHEL 6 Server
This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

Default
The default profile.

Changes needed to be done:

⛔ /tmp is not on a separate partition

⛔ /var/log is not on a separate partition

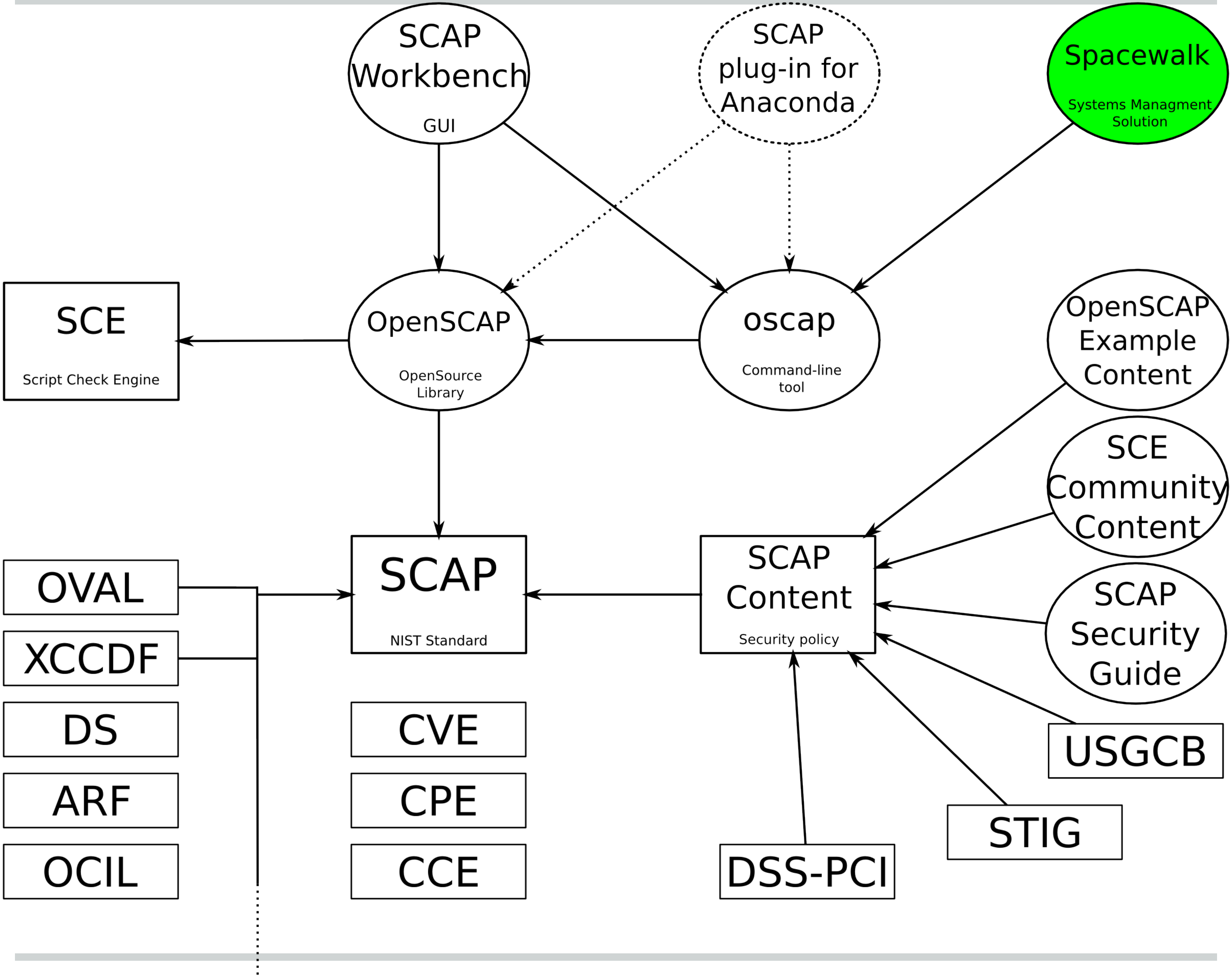
⚠ root password may be not strong enough

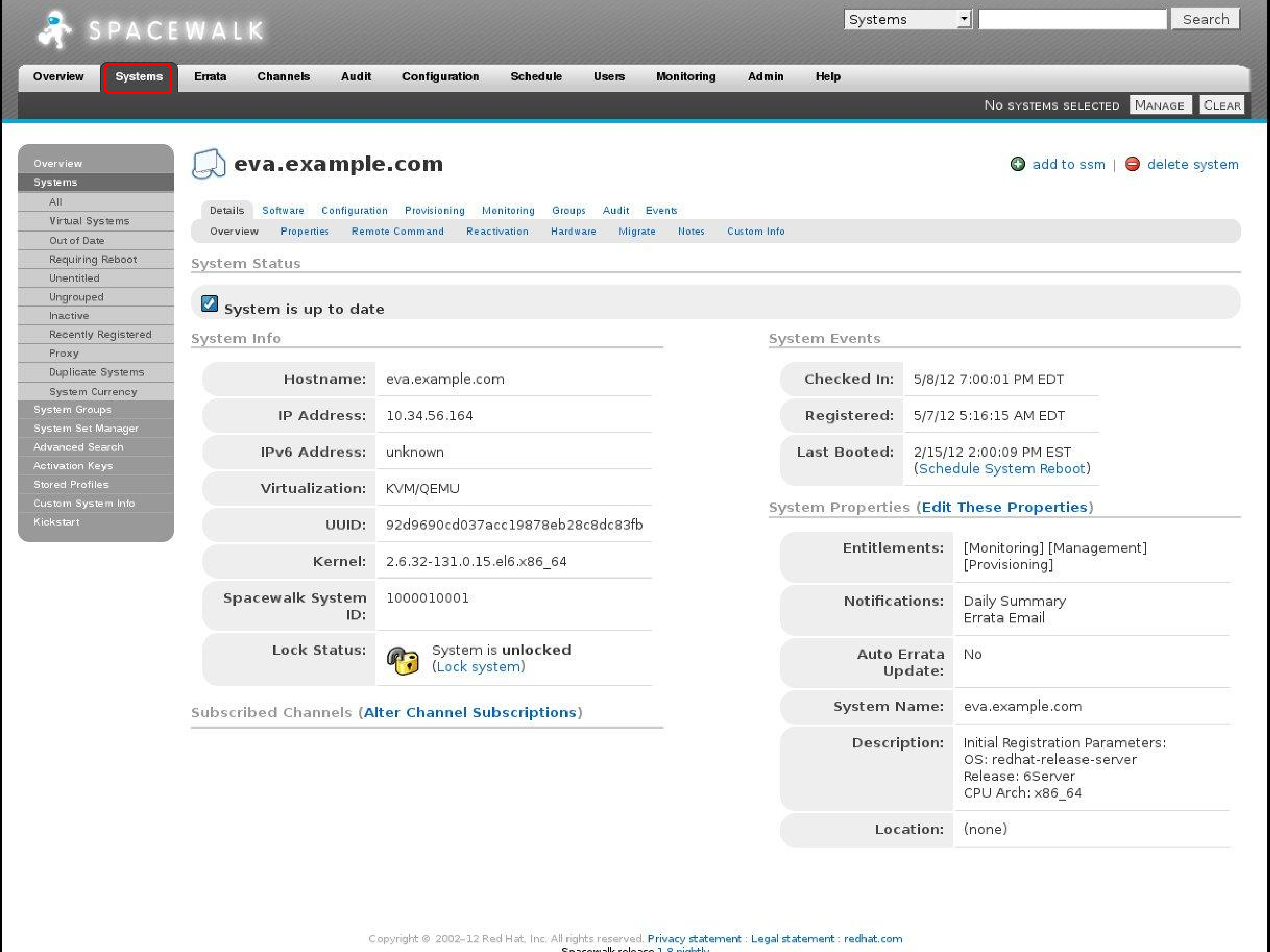
Concerns & Issues

- Content has to be Anaconda-ready
  - special flags for remediation of partitioning
- Limited scanning possibilities inside chroot
  - services aren't running
  - we can only test config files

First boot scan

- Scan using XCCDF profile selected
- Show results, allow remediation
- This is a full scan, all services are running


SCAP Workbench
GUI
SCAP plug-in for Anaconda
Spacewalk
Systems Managment Solution
SCE
Script Check Engine
OpenSCAP
OpenSource Library
oscap
Command-line tool
OpenSCAP Example Content
SCE Community Content
SCAP Security Guide
OVAL
XCCDF
DS
ARF
OCIL
SCAP
NIST Standard
CVE
CPE
CCE
SCAP Content
Security policy
USGCB
STIG
DSS-PCI



eva.example.com

System Status

☑ System is up to date

System Info

Hostname:	eva.example.com
IP Address:	10.34.56.164
IPv6 Address:	unknown
Virtualization:	KVM/QEMU
UUID:	92d9690cd037acc19878eb28c8dc83fb
Kernel:	2.6.32-131.0.15.el6.x86_64
Spacewalk System ID:	1000010001
Lock Status:	System is **unlocked** (Lock system)

Subscribed Channels (Alter Channel Subscriptions)

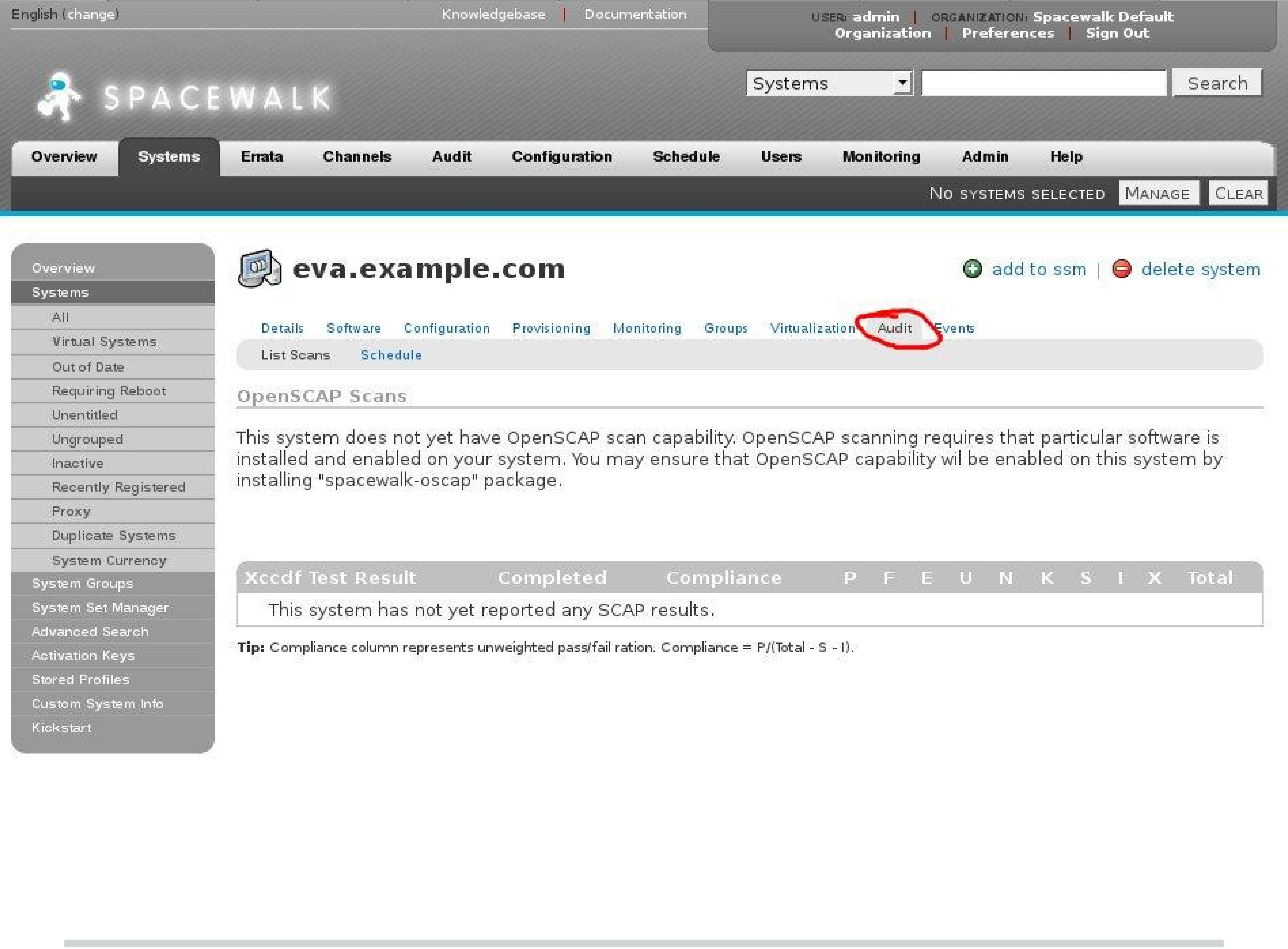
System Events

Checked In:	5/8/12 7:00:01 PM EDT
Registered:	5/7/12 5:16:15 AM EDT
Last Booted:	2/15/12 2:00:09 PM EST (Schedule System Reboot)

System Properties (Edit These Properties)

Entitlements:	[Monitoring] [Management] [Provisioning]
Notifications:	Daily Summary Errata Email
Auto Errata Update:	No
System Name:	eva.example.com
Description:	Initial Registration Parameters: OS: redhat-release-server Release: 6Server CPU Arch: x86_64
Location:	(none)

Spacewalk release 1.8 nightly

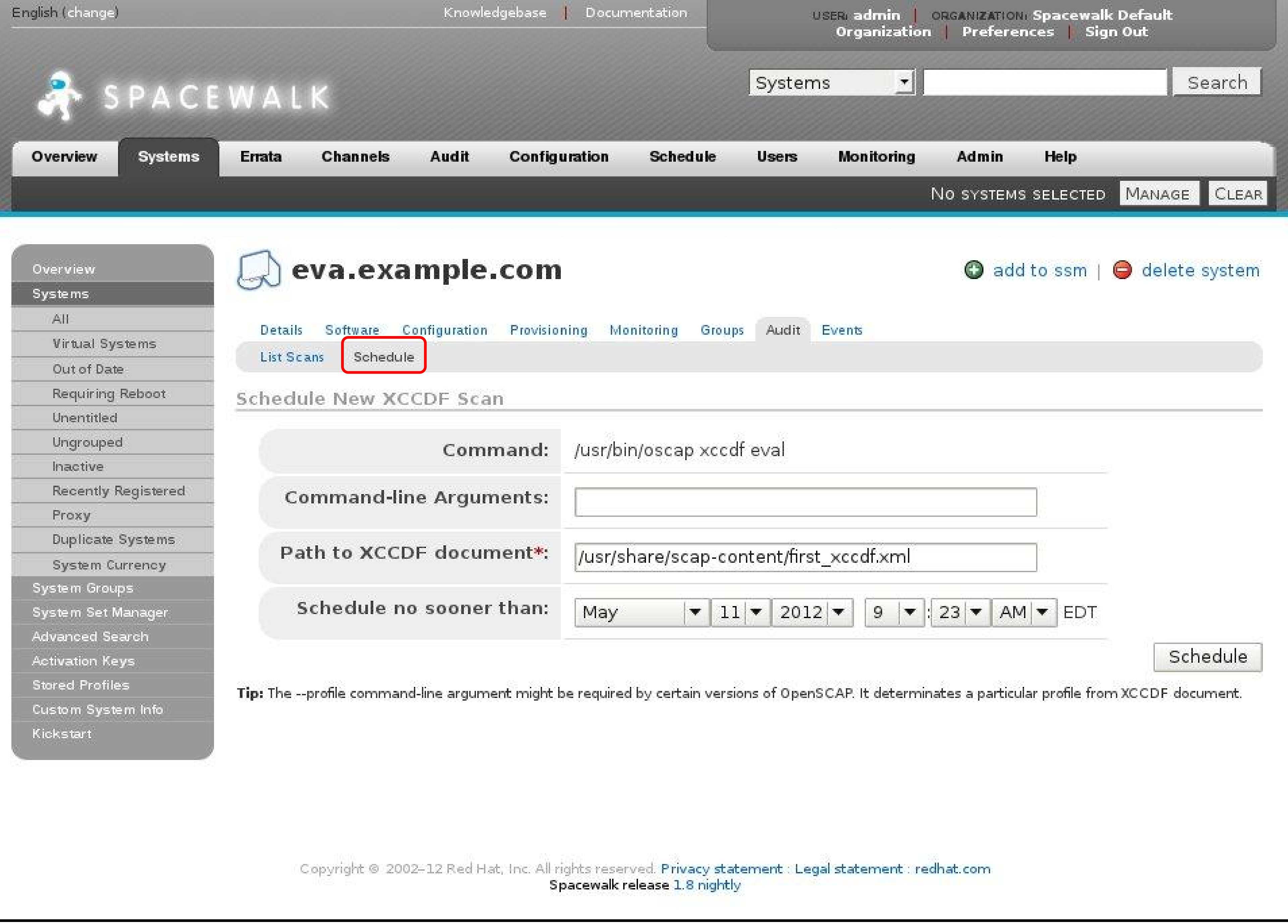


OpenSCAP Scans

This system does not yet have OpenSCAP scan capability. OpenSCAP scanning requires that particular software is installed and enabled on your system. You may ensure that OpenSCAP capability wil be enabled on this system by installing "spacewalk-oscap" package.

Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
This system has not yet reported any SCAP results.												

Tip: Compliance column represents unweighted pass/fail ration. Compliance = P/(Total - S - I).

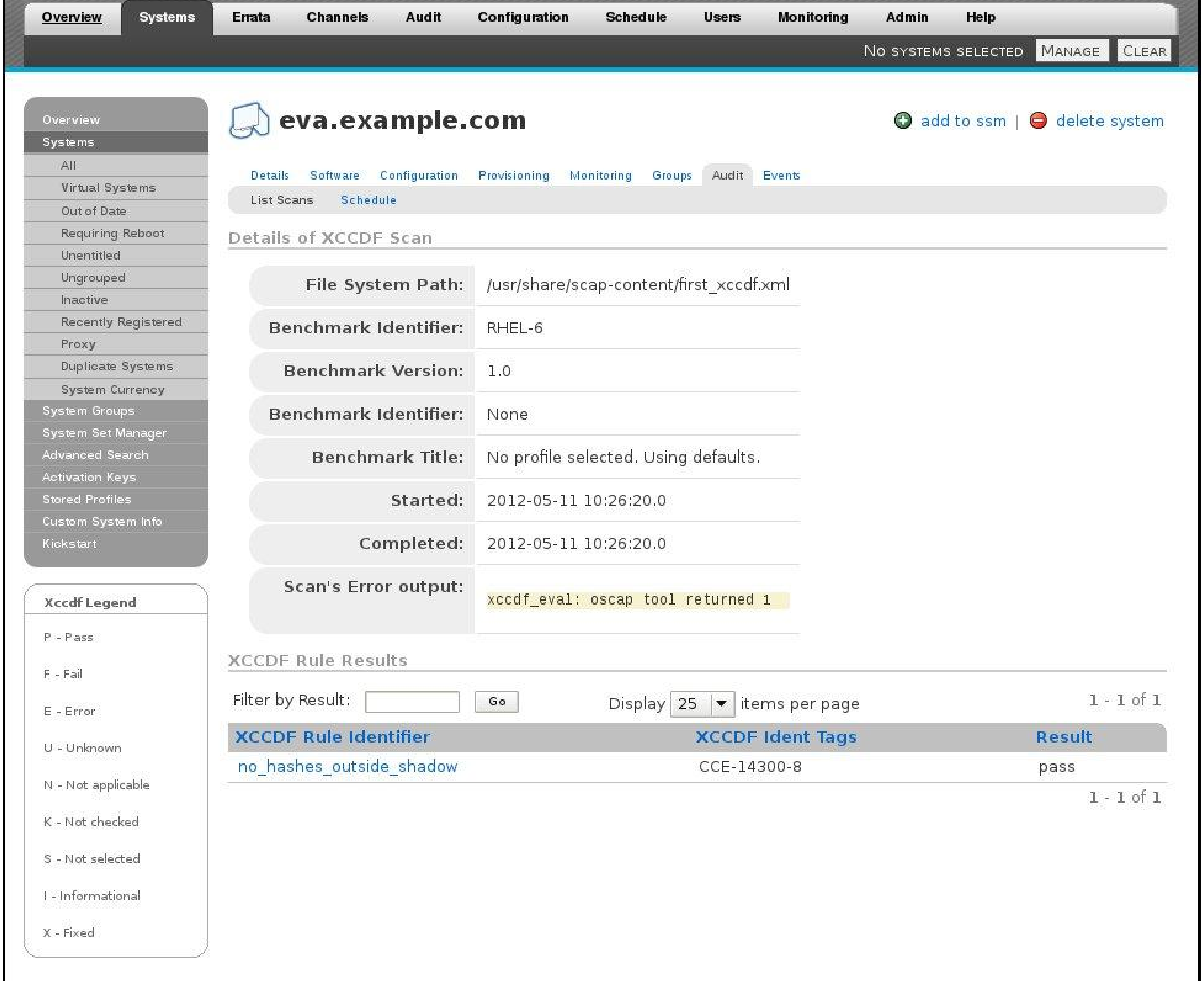


eva.example.com

Schedule New XCCDF Scan

Command:	/usr/bin/oscap xccdf eval
Command-line Arguments:	
Path to XCCDF document*:	/usr/share/scap-content/first_xccdf.xml
Schedule no sooner than:	May 11 2012 9 : 23 AM EDT

Tip: The --profile command-line argument might be required by certain versions of OpenSCAP. It determinates a particular profile from XCCDF document.



eva.example.com

Details of XCCDF Scan

File System Path:	/usr/share/scap-content/first_xccdf.xml
Benchmark Identifier:	RHEL-6
Benchmark Version:	1.0
Benchmark Identifier:	None
Benchmark Title:	No profile selected. Using defaults.
Started:	2012-05-11 10:26:20.0
Completed:	2012-05-11 10:26:20.0
Scan's Error output:	`xccdf_eval: oscap tool returned 1`

XCCDF Rule Results

Filter by Result:

Display 25 items per page

1 - 1 of 1

XCCDF Rule Identifier	XCCDF Ident Tags	Result
no_hashes_outside_shadow	CCE-14300-8	pass

1 - 1 of 1

Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

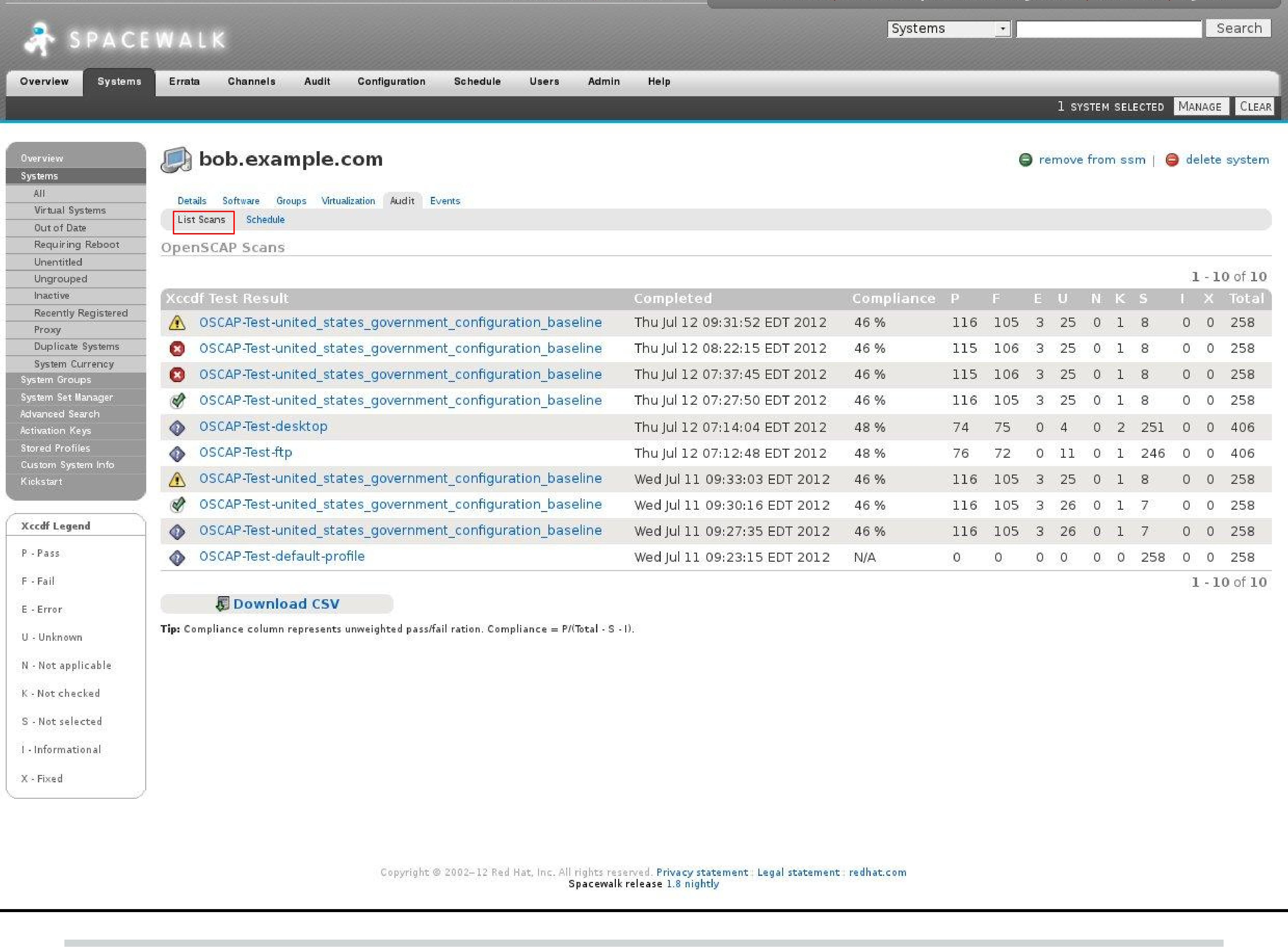
N - Not applicable

K - Not checked

S - Not selected

I - Informational

X - Fixed



bob.example.com

OpenSCAP Scans

1 - 10 of 10

	Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
⚠	OSCAP-Test-united_states_government_configuration_baseline	Thu Jul 12 09:31:52 EDT 2012	46 %	116	105	3	25	0	1	8	0	0	258
✖	OSCAP-Test-united_states_government_configuration_baseline	Thu Jul 12 08:22:15 EDT 2012	46 %	115	106	3	25	0	1	8	0	0	258
✖	OSCAP-Test-united_states_government_configuration_baseline	Thu Jul 12 07:37:45 EDT 2012	46 %	115	106	3	25	0	1	8	0	0	258
✓	OSCAP-Test-united_states_government_configuration_baseline	Thu Jul 12 07:27:50 EDT 2012	46 %	116	105	3	25	0	1	8	0	0	258
◆	OSCAP-Test-desktop	Thu Jul 12 07:14:04 EDT 2012	48 %	74	75	0	4	0	2	251	0	0	406
◆	OSCAP-Test-ftp	Thu Jul 12 07:12:48 EDT 2012	48 %	76	72	0	11	0	1	246	0	0	406
⚠	OSCAP-Test-united_states_government_configuration_baseline	Wed Jul 11 09:33:03 EDT 2012	46 %	116	105	3	25	0	1	8	0	0	258
✓	OSCAP-Test-united_states_government_configuration_baseline	Wed Jul 11 09:30:16 EDT 2012	46 %	116	105	3	26	0	1	7	0	0	258
◆	OSCAP-Test-united_states_government_configuration_baseline	Wed Jul 11 09:27:35 EDT 2012	46 %	116	105	3	26	0	1	7	0	0	258
◆	OSCAP-Test-default-profile	Wed Jul 11 09:23:15 EDT 2012	N/A	0	0	0	0	0	0	258	0	0	258

1 - 10 of 10

Tip: Compliance column represents unweighted pass/fail ration. Compliance = P/(Total - S - I).

Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

N - Not applicable

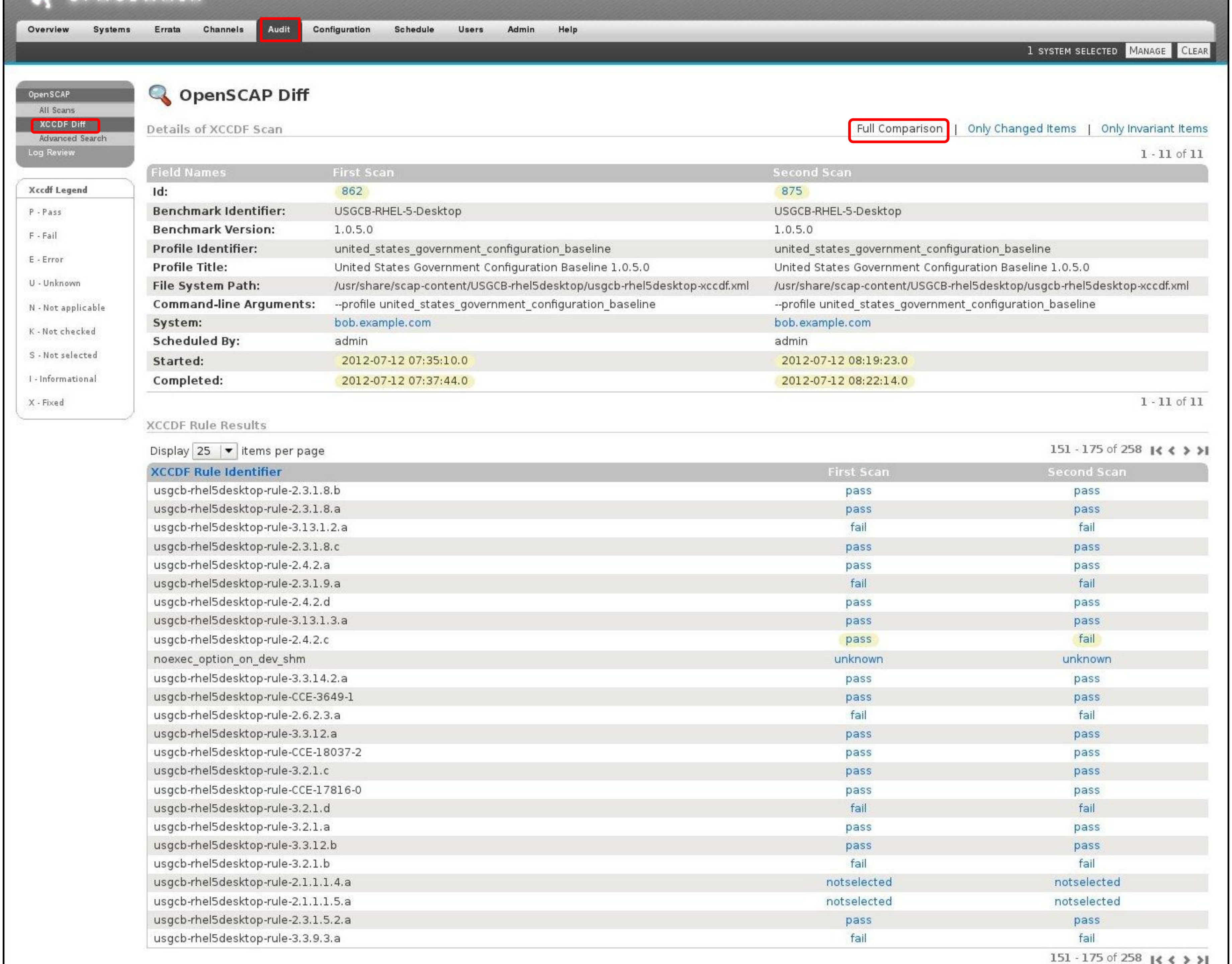
K - Not checked

S - Not selected

I - Informational

X - Fixed

Spacewalk release 1.8 nightly



Xccdf Legend

P - Pass
F - Fail
E - Error
U - Unknown
N - Not applicable
K - Not checked
S - Not selected
I - Informational
X - Fixed

OpenSCAP Diff

Details of XCCDF Scan

Full Comparison | Only Changed Items | Only Invariant Items

1 - 11 of 11

Field Names	First Scan	Second Scan
Id:	862	875
Benchmark Identifier:	USGCB-RHEL-5-Desktop	USGCB-RHEL-5-Desktop
Benchmark Version:	1.0.5.0	1.0.5.0
Profile Identifier:	united_states_government_configuration_baseline	united_states_government_configuration_baseline
Profile Title:	United States Government Configuration Baseline 1.0.5.0	United States Government Configuration Baseline 1.0.5.0
File System Path:	/usr/share/scap-content/USGCB-rhel5desktop/usgcb-rhel5desktop-xccdf.xml	/usr/share/scap-content/USGCB-rhel5desktop/usgcb-rhel5desktop-xccdf.xml
Command-line Arguments:	--profile united_states_government_configuration_baseline	--profile united_states_government_configuration_baseline
System:	bob.example.com	bob.example.com
Scheduled By:	admin	admin
Started:	2012-07-12 07:35:10.0	2012-07-12 08:19:23.0
Completed:	2012-07-12 07:37:44.0	2012-07-12 08:22:14.0

1 - 11 of 11

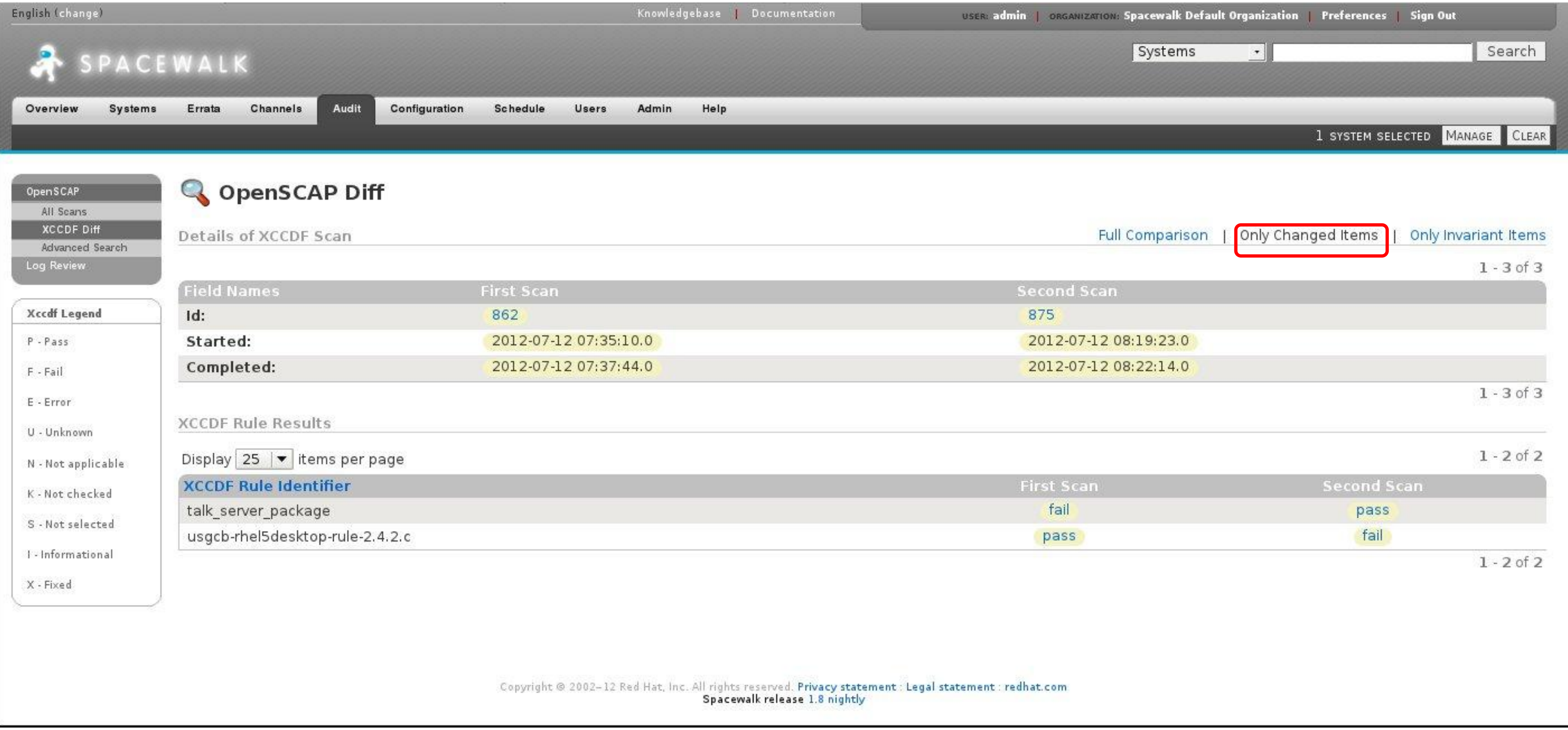
XCCDF Rule Results

Display 25 items per page

151 - 175 of 258

XCCDF Rule Identifier	First Scan	Second Scan
usgcb-rhel5desktop-rule-2.3.1.8.b	pass	pass
usgcb-rhel5desktop-rule-2.3.1.8.a	pass	pass
usgcb-rhel5desktop-rule-3.13.1.2.a	fail	fail
usgcb-rhel5desktop-rule-2.3.1.8.c	pass	pass
usgcb-rhel5desktop-rule-2.4.2.a	pass	pass
usgcb-rhel5desktop-rule-2.3.1.9.a	fail	fail
usgcb-rhel5desktop-rule-2.4.2.d	pass	pass
usgcb-rhel5desktop-rule-3.13.1.3.a	pass	pass
usgcb-rhel5desktop-rule-2.4.2.c	pass	fail
noexec_option_on_dev_shm	unknown	unknown
usgcb-rhel5desktop-rule-3.3.14.2.a	pass	pass
usgcb-rhel5desktop-rule-CCE-3649-1	pass	pass
usgcb-rhel5desktop-rule-2.6.2.3.a	fail	fail
usgcb-rhel5desktop-rule-3.3.12.a	pass	pass
usgcb-rhel5desktop-rule-CCE-18037-2	pass	pass
usgcb-rhel5desktop-rule-3.2.1.c	pass	pass
usgcb-rhel5desktop-rule-CCE-17816-0	pass	pass
usgcb-rhel5desktop-rule-3.2.1.d	fail	fail
usgcb-rhel5desktop-rule-3.2.1.a	pass	pass
usgcb-rhel5desktop-rule-3.3.12.b	pass	pass
usgcb-rhel5desktop-rule-3.2.1.b	fail	fail
usgcb-rhel5desktop-rule-2.1.1.1.4.a	notselected	notselected
usgcb-rhel5desktop-rule-2.1.1.1.5.a	notselected	notselected
usgcb-rhel5desktop-rule-2.3.1.5.2.a	pass	pass
usgcb-rhel5desktop-rule-3.3.9.3.a	fail	fail

151 - 175 of 258



Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

N - Not applicable

K - Not checked

S - Not selected

I - Informational

X - Fixed

OpenSCAP Diff

Details of XCCDF Scan

Full Comparison | Only Changed Items | Only Invariant Items

1 - 3 of 3

Field Names	First Scan	Second Scan
Id:	862	875
Started:	2012-07-12 07:35:10.0	2012-07-12 08:19:23.0
Completed:	2012-07-12 07:37:44.0	2012-07-12 08:22:14.0

1 - 3 of 3

XCCDF Rule Results

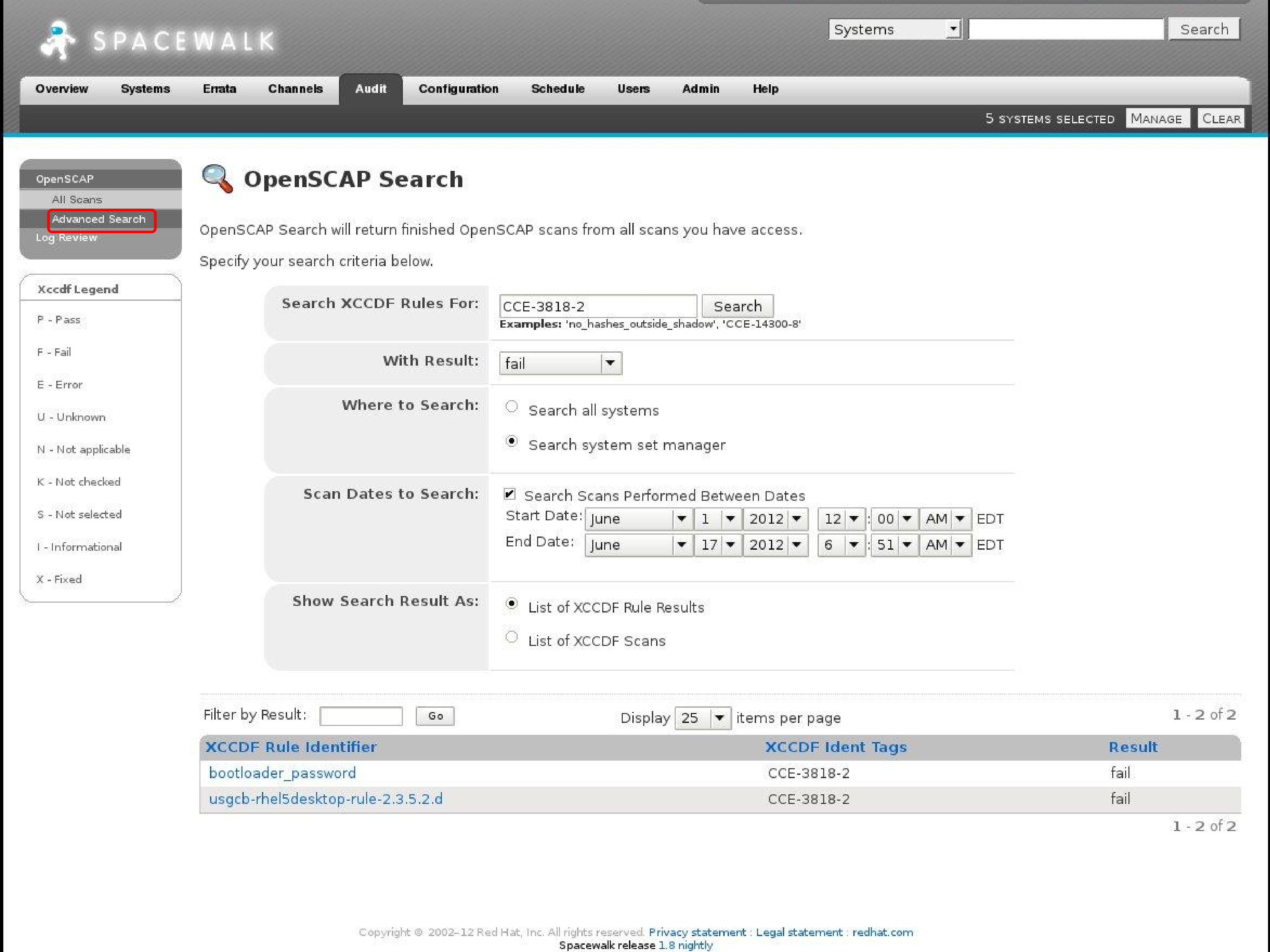
Display 25 items per page

1 - 2 of 2

XCCDF Rule Identifier	First Scan	Second Scan
talk_server_package	fail	pass
usgcb-rhel5desktop-rule-2.4.2.c	pass	fail

1 - 2 of 2

Copyright © 2002–12 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
Spacewalk release 1.8 nightly



Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

N - Not applicable

K - Not checked

S - Not selected

I - Informational

X - Fixed

OpenSCAP Search

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

Specify your search criteria below.

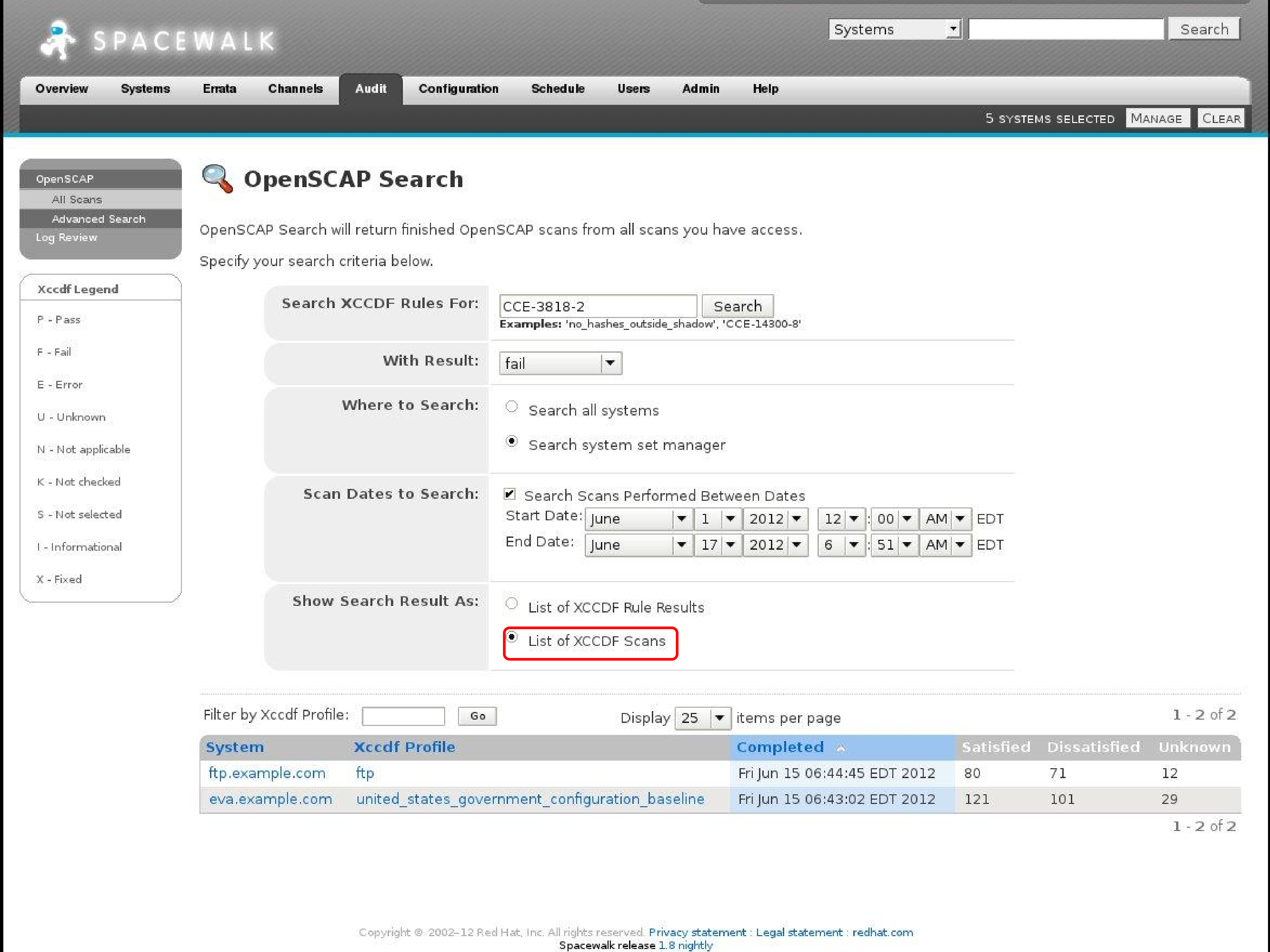
Search XCCDF Rules For:	CCE-3818-2 [Search] **Examples:** 'no_hashes_outside_shadow', 'CCE-14300-8'
With Result:	fail
Where to Search:	○ Search all systems ● Search system set manager
Scan Dates to Search:	☑ Search Scans Performed Between Dates Start Date: June 1 2012 12 : 00 AM EDT End Date: June 17 2012 6 : 51 AM EDT
Show Search Result As:	● List of XCCDF Rule Results ○ List of XCCDF Scans

Filter by Result: [ ] Go   Display 25 items per page   1 - 2 of 2

XCCDF Rule Identifier	XCCDF Ident Tags	Result
bootloader_password	CCE-3818-2	fail
usgcb-rhel5desktop-rule-2.3.5.2.d	CCE-3818-2	fail

1 - 2 of 2

Copyright © 2002–12 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
Spacewalk release 1.8 nightly



Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

N - Not applicable

K - Not checked

S - Not selected

I - Informational

X - Fixed

OpenSCAP Search

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

Specify your search criteria below.

Search XCCDF Rules For: CCE-3818-2 Search
Examples: 'no_hashes_outside_shadow', 'CCE-14300-8'

With Result: fail

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

Scan Dates to Search:
☑ Search Scans Performed Between Dates
Start Date: June 1 2012 12 : 00 AM EDT
End Date: June 17 2012 6 : 51 AM EDT

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

Filter by Xccdf Profile: Go   Display 25 items per page   1 - 2 of 2

System	Xccdf Profile	Completed	Satisfied	Dissatisfied	Unknown
ftp.example.com	ftp	Fri Jun 15 06:44:45 EDT 2012	80	71	12
eva.example.com	united_states_government_configuration_baseline	Fri Jun 15 06:43:02 EDT 2012	121	101	29

1 - 2 of 2

Copyright © 2002-12 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
Spacewalk release 1.8 nightly

Lifecycle

- Obtaining content
  - official
  - custom
- Tailoring
- Machine installation
  - **Anaconda** scan before the machine boots
  - **Kickstart**
- Production
  - periodic scanning with **scap-workbench** or **spacewalk**

Short-term future plans

- Lowering SCAP's entry barrier
  - new scap-workbench
  - ready to go content
- Implementing missing pieces in lifecycle
  - Anaconda integration
- Remediation

Thanks for your attention

Questions?

- #openscap at irc.freenode.net
- open-scap-list@redhat.com