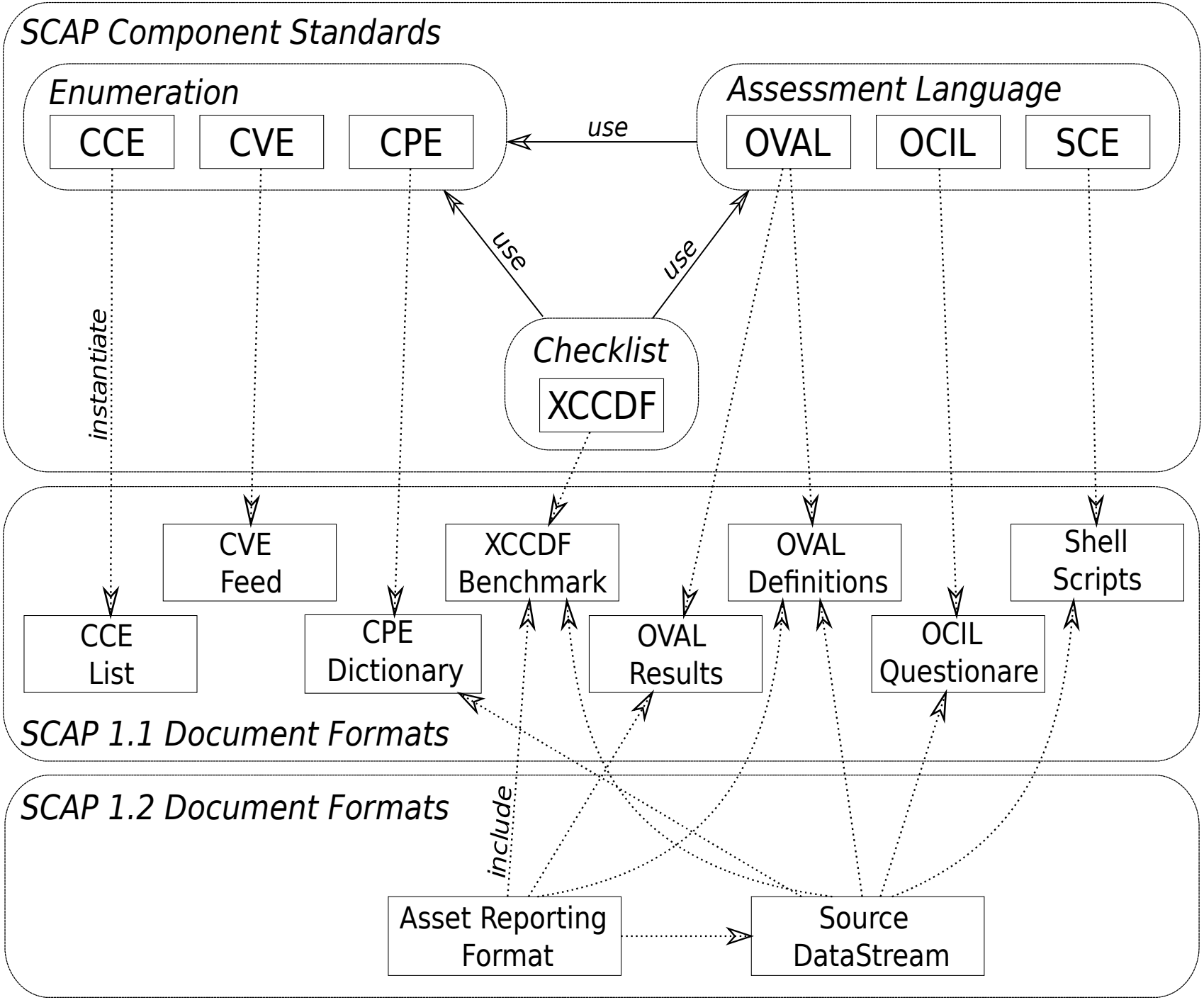
SCAP
Otevřený standard pro bezpečnostní audit

Šimon Lukašík

ukázka

scap.nist.gov


SCAP Component Standards
Enumeration
CCE
CVE
CPE
use
Assessment Language
OVAL
OCIL
SCE
use
use
instantiate
Checklist
XCCDF
CVE Feed
XCCDF Benchmark
OVAL Definitions
Shell Scripts
CCE List
CPE Dictionary
OVAL Results
OCIL Questionare
SCAP 1.1 Document Formats
SCAP 1.2 Document Formats
include
Asset Reporting Format
Source DataStream

MEETING IN PROGRESS

DON'T WORRY.

SECURITY

No acronyms. No security. No problem.

Foreman
OpenSCAP

Ruby Gem
OpenSCAP

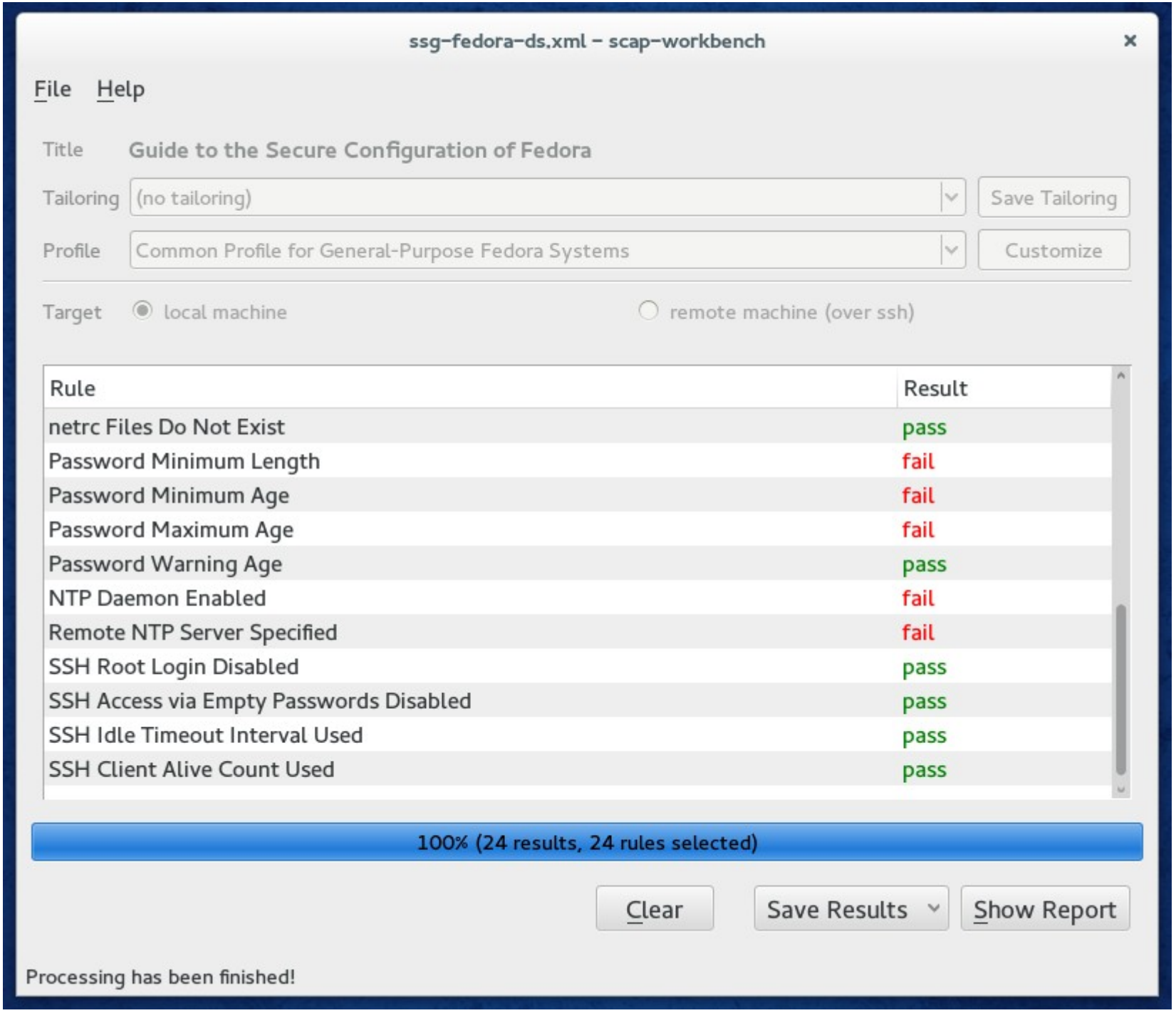
Puppet
OpenSCAP

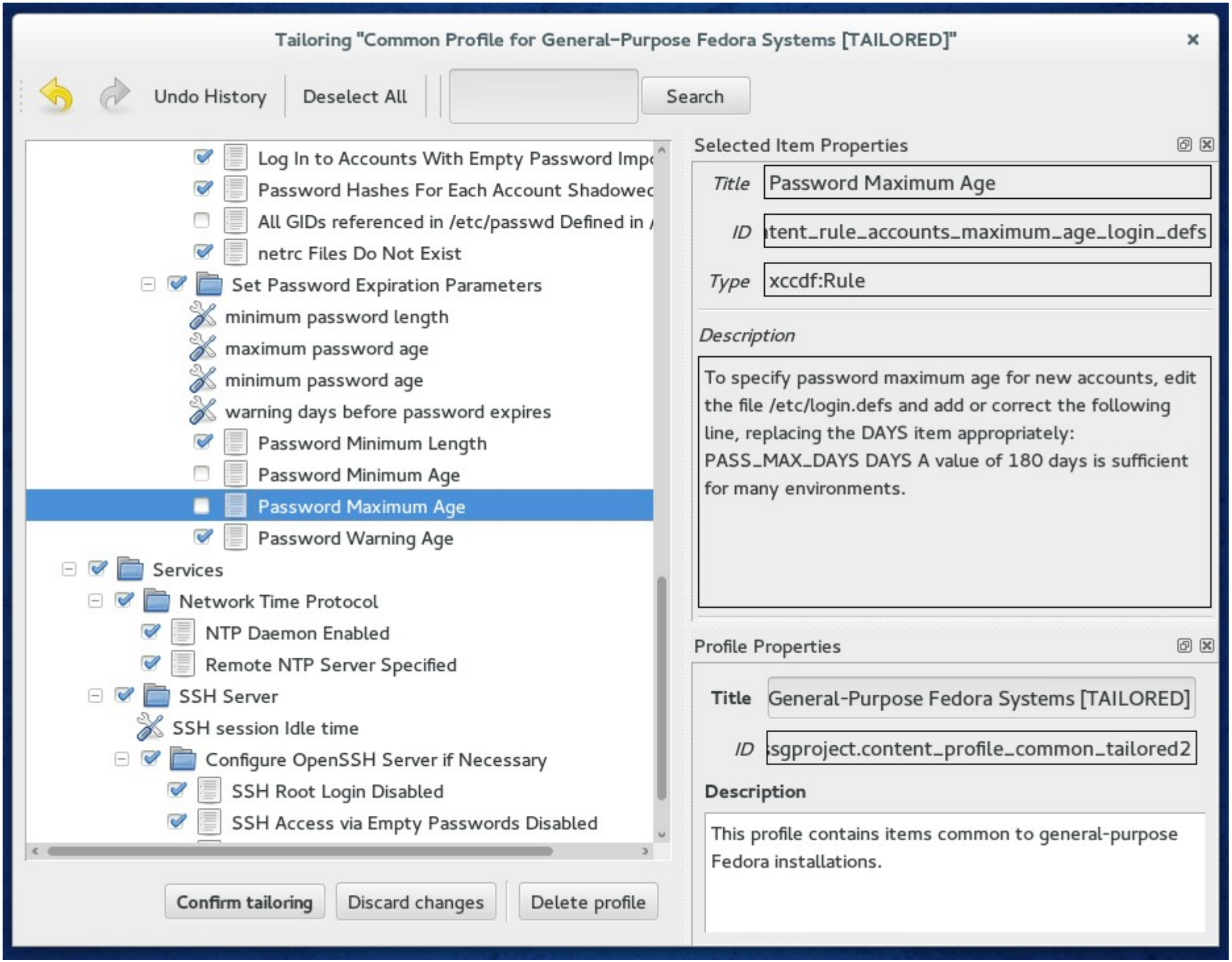
SCAPtimony

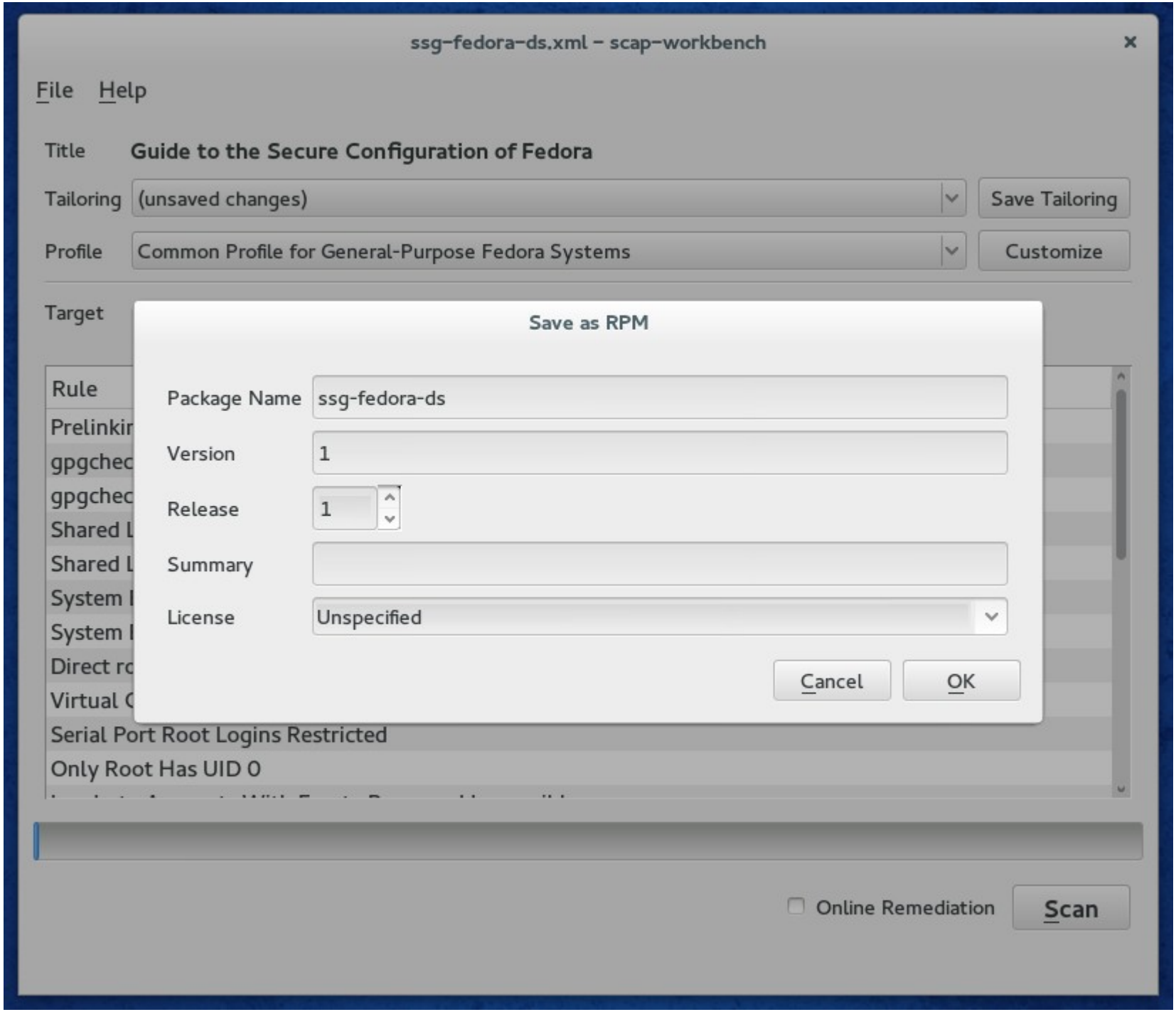
open-scap.org

github.com/OpenSCAP/scap-security-guide

github.com/OpenSCAP/scap-workbench


ssg-fedora-ds.xml – scap-workbench
File Help
Title Guide to the Secure Configuration of Fedora
Tailoring (no tailoring)
Save Tailoring
Profile Common Profile for General-Purpose Fedora Systems
Customize
Target local machine
remote machine (over ssh)
Rule
Result
netrc Files Do Not Exist pass
Password Minimum Length fail
Password Minimum Age fail
Password Maximum Age fail
Password Warning Age pass
NTP Daemon Enabled fail
Remote NTP Server Specified fail
SSH Root Login Disabled pass
SSH Access via Empty Passwords Disabled pass
SSH Idle Timeout Interval Used pass
SSH Client Alive Count Used pass
100% (24 results, 24 rules selected)
Clear
Save Results
Show Report
Processing has been finished!


Tailoring "Common Profile for General-Purpose Fedora Systems [TAILORED]"
Undo History
Deselect All
Search
Log In to Accounts With Empty Password Impo
Password Hashes For Each Account Shadowed
All GIDs referenced in /etc/passwd Defined in /
netrc Files Do Not Exist
Set Password Expiration Parameters
minimum password length
maximum password age
minimum password age
warning days before password expires
Password Minimum Length
Password Minimum Age
Password Maximum Age
Password Warning Age
Services
Network Time Protocol
NTP Daemon Enabled
Remote NTP Server Specified
SSH Server
SSH session Idle time
Configure OpenSSH Server if Necessary
SSH Root Login Disabled
SSH Access via Empty Passwords Disabled
Selected Item Properties
Title
Password Maximum Age
ID
tent_rule_accounts_maximum_age_login_defs
Type
xccdf:Rule
Description
To specify password maximum age for new accounts, edit the file /etc/login.defs and add or correct the following line, replacing the DAYS item appropriately: PASS_MAX_DAYS DAYS A value of 180 days is sufficient for many environments.
Profile Properties
Title
General-Purpose Fedora Systems [TAILORED]
ID
sgproject.content_profile_common_tailored2
Description
This profile contains items common to general-purpose Fedora installations.
Confirm tailoring
Discard changes
Delete profile


ssg-fedora-ds.xml – scap-workbench
File
Help
Title
Guide to the Secure Configuration of Fedora
Tailoring
(unsaved changes)
Save Tailoring
Profile
Common Profile for General-Purpose Fedora Systems
Customize
Target
Save as RPM
Package Name
ssg-fedora-ds
Version
1
Release
1
Summary
License
Unspecified
Cancel
OK
Rule
Serial Port Root Logins Restricted
Only Root Has UID 0
Online Remediation
Scan

spacewalk.redhat.com

Overview
Systems
All
Virtual Systems
Out of Date
Requiring Reboot
Unentitled
Ungrouped
Inactive
Recently Registered
Proxy
Duplicate Systems
System Currency
System Groups
System Set Manager
Advanced Search
Activation Keys
Stored Profiles
Custom System Info
Kickstart

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

remove from ssm | delete system

Details Software Groups Virtualization Audit Events

List Scans Schedule

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

Download CSV

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

OSCAP Anaconda Addon

fedorahosted.org/oscap-anaconda-addon

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

Quit

Begin Installation

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

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

SPOKE NAME

Done

FEDORA 20130115 INSTALLATION

PRE-RELEASE / TESTING

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:

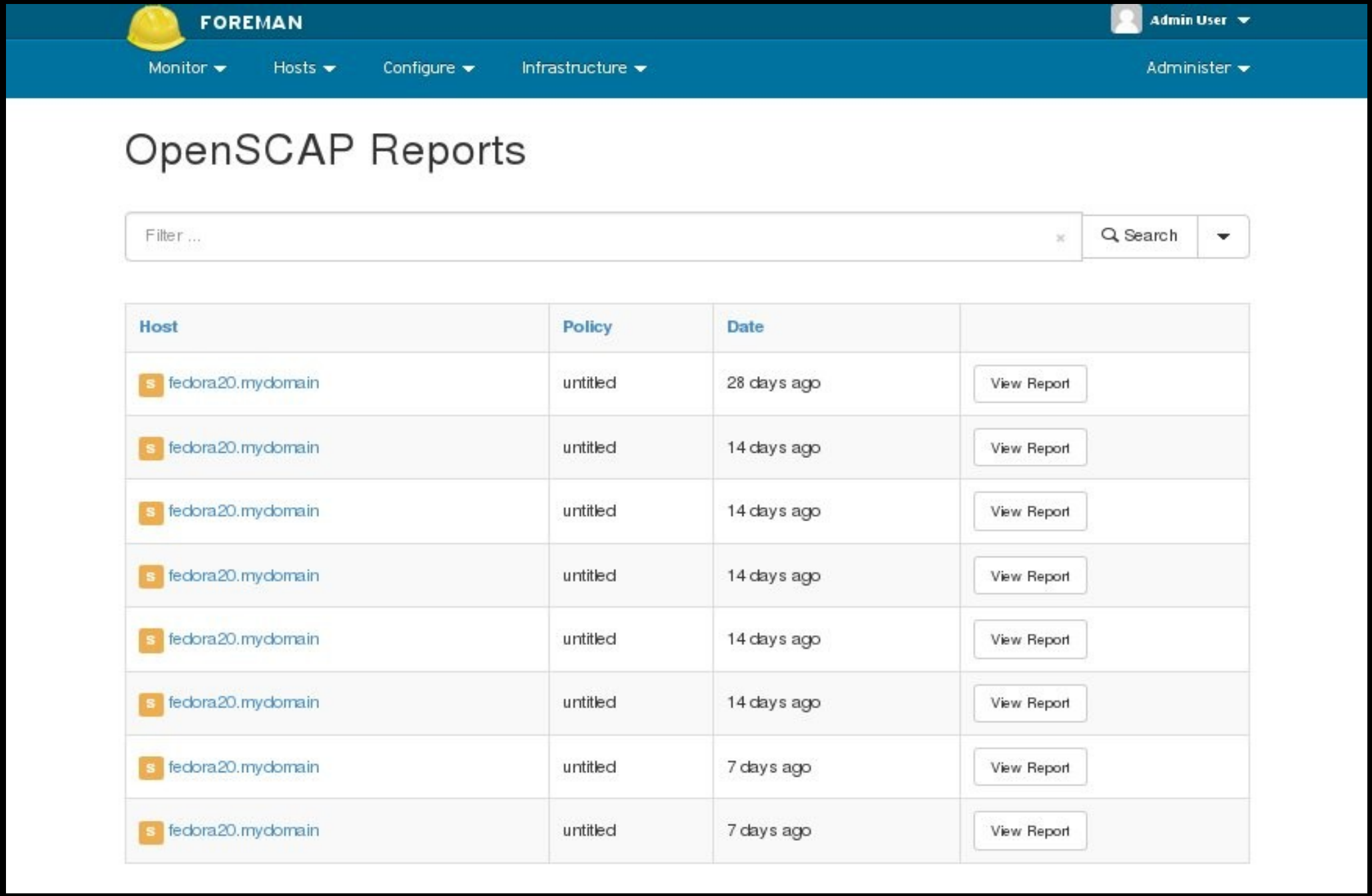
- /tmp is not on a separate partition
- /var/log is not on a separate partition
- root password may be not strong enough

github.com/OpenSCAP/ruby-openscap

github.com/OpenSCAP/puppet-openscap

github.com/OpenSCAP/scaptimony

github.com/OpenSCAP/foreman_openscap


FOREMAN
Admin User
Monitor
Hosts
Configure
Infrastructure
Administer
OpenSCAP Reports
Filter ...
Search
Host
Policy
Date
fedora20.mydomain
untitled
28 days ago
14 days ago
7 days ago
View Report

Děkuji za pozornost

isimluk.livejournal.com
twitter.com/isimluk