



Introduction to openSCAP

Luc de Louw <ldelouw@redhat.com>
Sr. Linux Consultant
2013-06-06

The basics – What is SCAP?

Stands for “*Security Content Automation Protocol*”

- SCAP is a standardized compliance checking solution
It is a line of specifications maintained by the National Institute of Standards and Technology (NIST) for maintaining system security for IT systems.
- openSCAP is the open source implementation

More abbreviations (The most important ones)

- XCCDF: Extensible Configuration Checklist Description Format
- OVAL: Open Vulnerability and Assessment Language
- CVE: Common Vulnerabilities and Exposures
- CCE: Common Configuration Enumeration

XCCDF

- Used for Security Policies

OVAL

- Vulnerability detection
- Patch detection

CCE

- Tracks systems against specific configuration requirements

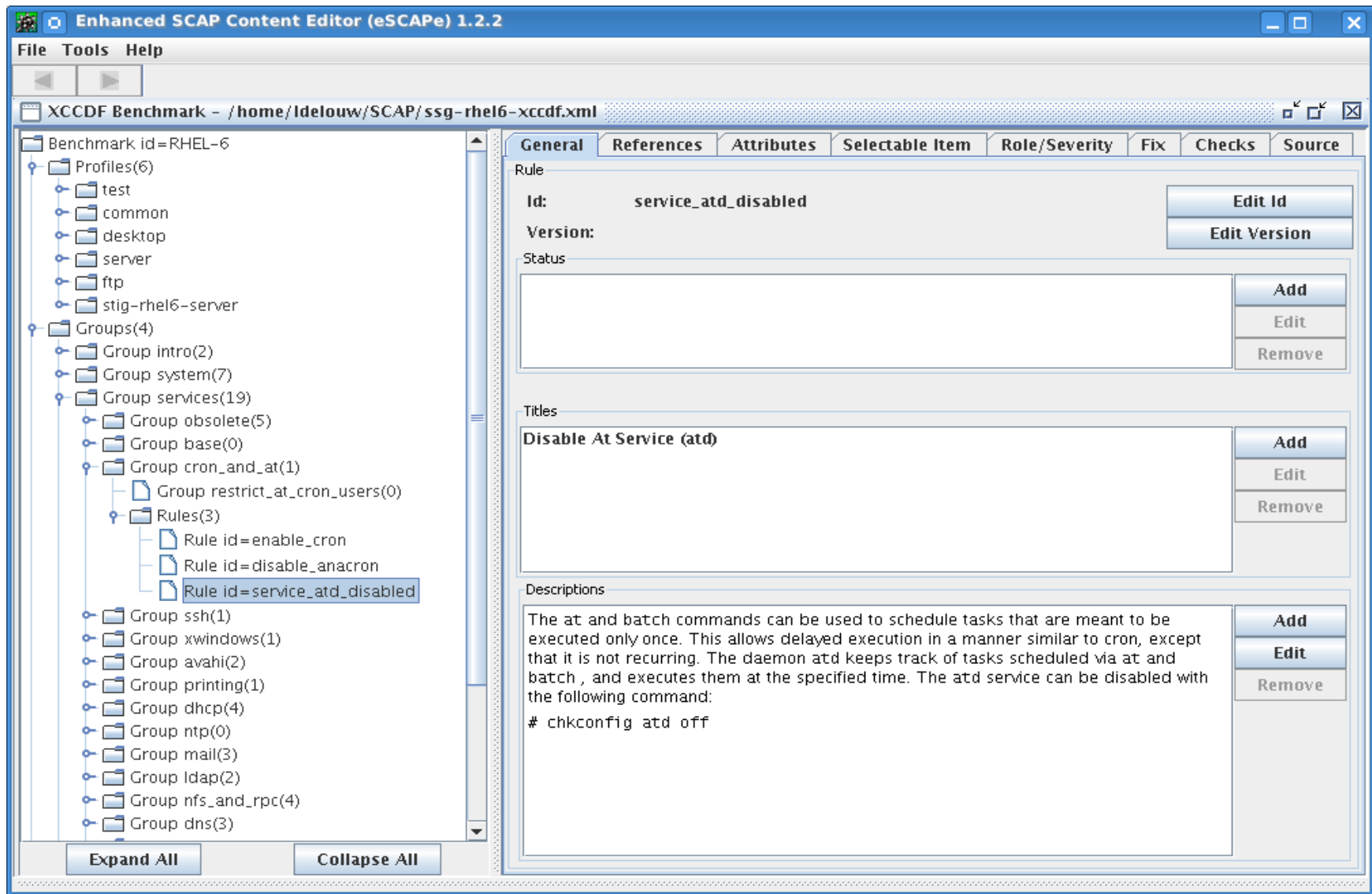
Do not reinvent the wheel

- Use existing OVALs and customize them to your needs
- Find them at NIST ->
http://usgcb.nist.gov/usgcb/rhel/download_rhel5.html
- Find them at Red Hat ->
<https://www.redhat.com/security/data/oval/>
- If you like XML, use vim or emacs
- The use of special tools such as “Enhanced SCAP Editor” is the better choice.

Enhanced SCAP Editor

- Opensource GPL v3
- Java based
- Runs on different platforms
- Some nice wizards


Enhanced SCAP Editor



RHN Satellite integration in Version 5.5

[Overview](#) **[Systems](#)** [Errata](#) [Channels](#) [Audit](#) [Configuration](#) [Schedule](#) [Users](#) [Admin](#) [Help](#)

[Overview](#)
[Systems](#)
[All](#)
[Virtual Systems](#)
[Out of Date](#)
[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](#)

 **ipa1.example.com** 

[Details](#) [Software](#) [Configuration](#) [Provisioning](#) [Groups](#) **[Audit](#)** [Events](#)

[List Scans](#) [Schedule](#)


Schedule New XCCDF Scan

Command:	<input type="text" value="/usr/bin/oscaped eval"/>
Command-line Arguments:	<input type="text" value="--profile RHEL6-Default"/>
Path to XCCDF document*:	<input type="text" value="/usr/share/openscap/scap-rhel6-xccdf.xml"/>
Schedule no sooner than:	<div><div>June</div><div>5</div><div>2013</div><div>11</div><div>:</div><div>45</div><div>PM</div><div>EDT</div></div>

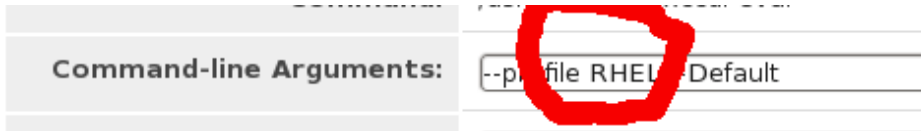
Tip: Certain versions of OpenSCAP may require the --profile command-line argument. --profile specifies a particular profile from the XCCDF document.

10

RED HAT CONFIDENTIAL | Introduction in openSCAP

 redhat.

RHN Satellite (cont) – Pitfall!





- Just omit the = when passing a parameter!
- Is this a bug?




RHN Satellite (cont.)

[Overview](#) **[Systems](#)** [Errata](#) [Channels](#) [Audit](#) [Configuration](#) [Schedule](#) [Users](#) [Admin](#) [Help](#)

[Overview](#)
Systems
All
Virtual Systems
Out of Date
Untitled
Ungrouped
Inactive
Recently Registered
Proxy
Duplicate Systems
System Currency
System Groups
System Set Manager

 **ipa1.example.com** 
[Details](#) [Software](#) [Configuration](#) [Provisioning](#) [Groups](#) **[Audit](#)** [Events](#)
[List Scans](#) [Schedule](#)

OpenSCAP Scans

Xccdf Test Result	Completed	Compliance	P	F
 xccdf_org.open-scap_testresult_server	Thu Jun 06 06:18:34 CEST 2013	44 %	79	86
 xccdf_org.open-scap_testresult_server	Thu Jun 06 06:11:56 CEST 2013	44 %	78	87
 xccdf_org.open-scap_testresult_server	Thu Jun 06 06:05:22 CEST 2013	43 %	77	88

Command Line Tools

- `/usr/bin/oscap`

```
root@ipa1 ~]# oscap info  
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xmlDocument type: XCCDF  
Checklist
```

```
Checklist version: 1.1
```

```
Status: draft
```

```
Generated: 2013-05-01
```

```
Imported: 2013-05-02T05:59:06
```

```
Resolved: true
```

```
Profiles:
```

```
    test
```

```
    common
```

```
    desktop
```

```
    server
```

```
    ftp
```

```
    stig-rhel6-server
```

Command Line Tools (cont)

```
root@ipa1 ~]# /usr/bin/osc const xccdf eval --profile=server  
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```

```
Title    Ensure /tmp Located On Separate Partition  
Rule     partition_for_tmp  
Ident    CCE-26435-8  
Result   fail
```

```
[..]
```

```
Title    Verify User Who Owns passwd File  
Rule     userowner_passwd_file  
Ident    CCE-26953-0  
Result   pass
```

Thanks for listening
Let's have a Demo now