SYSTEM SECURITY & MANAGEMENT

SHAWN WELLS
DIRECTOR, INNOVATION PROGRAMS
unclass: shawn@redhat.com
(+1) 443-534-0130

60 MINUTES, 3 GOALS

1. Review compliance tech + initiatives spanning I4, TS13, DISA, NIST, and Red Hat
    - SCAP Security Guide
    - Security Baselines (CS2, STIG, etc)
    - Emerging Tech

2.

3.

60 MINUTES, 3 GOALS

1. Review compliance tech + initiatives spanning I4, TS13, DISA, NIST, and Red Hat
   - SCAP Security Guide
   - Security Baselines (CS2, STIG, etc)
   - Emerging Tech

2. T3 ATO'd System Management Framework
   - System Provisioning, Patch Management, Monitoring, Conf Mgmt
   - Sponsored by T3 ("go redhat-support")

3.

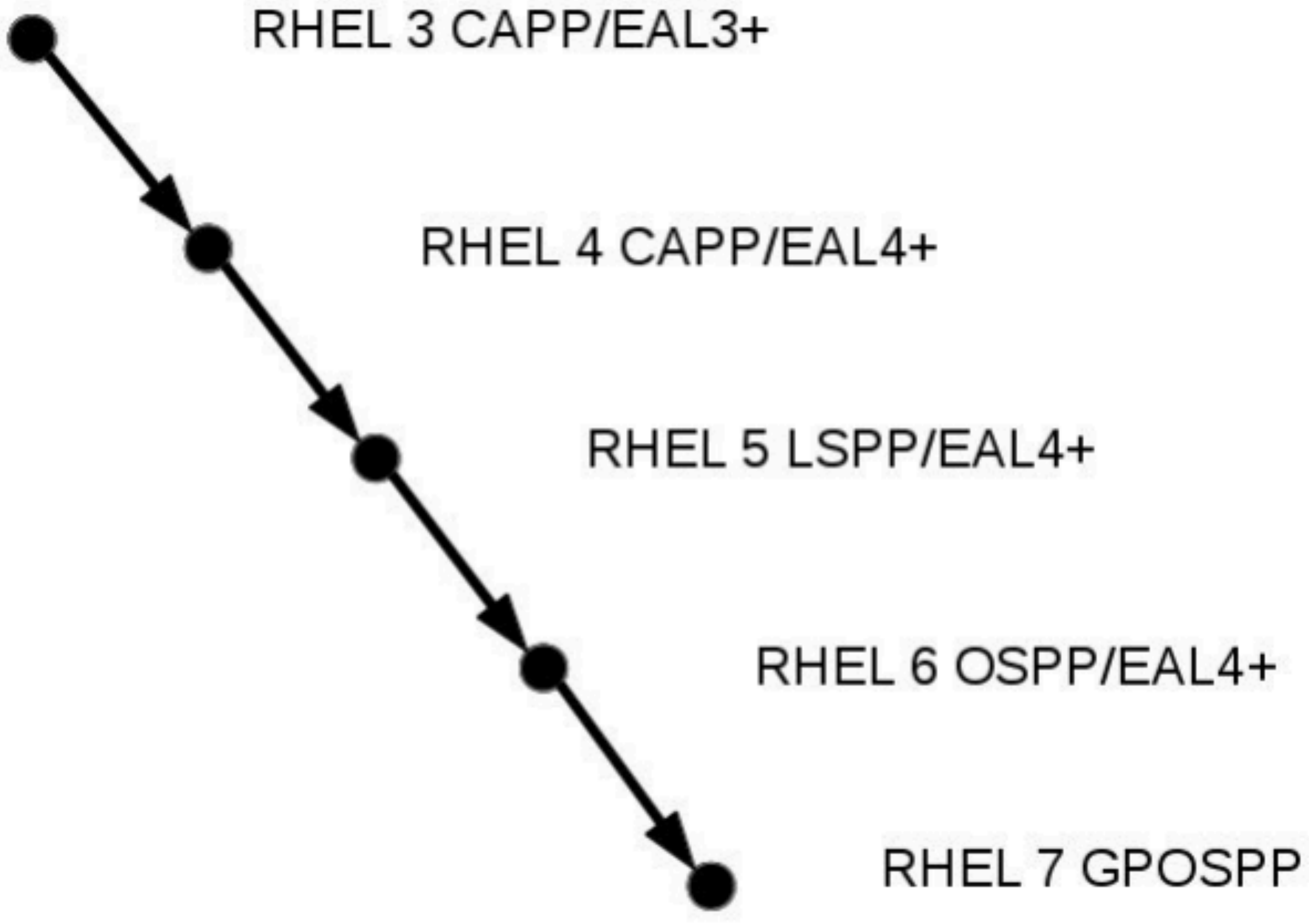
60 MINUTES, 3 GOALS

1. Review compliance tech + initiatives spanning I4, TS13, DISA, NIST, and Red Hat
   - SCAP Security Guide
   - Security Baselines (CS2, STIG, etc)
   - Emerging Tech

2. T3 ATO'd System Management Framework
   - System Provisioning, Patch Management, Monitoring, Conf Mgmt
   - Sponsored by T3 ("go redhat-support")

3. Demonstrate current capabilities

NSA C63 (aka NIAP) & Red Hat: where we've been... and next stop



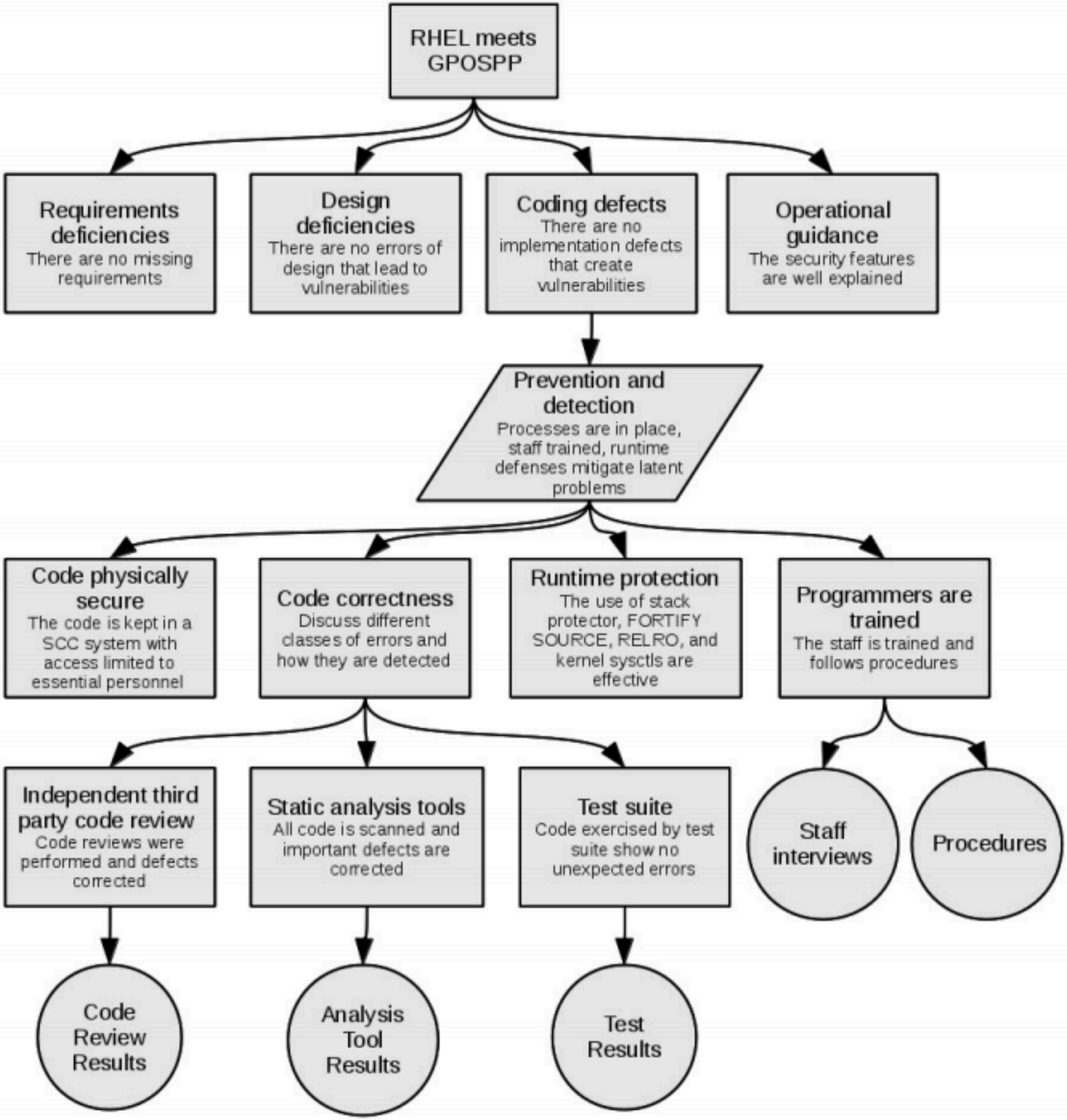
RHEL 3 CAPP/EAL3+

RHEL 4 CAPP/EAL4+

RHEL 5 LSPP/EAL4+

RHEL 6 OSPP/EAL4+

RHEL 7 GPOSPP



RHEL meets GPOSPP

Requirements deficiencies
There are no missing requirements

Design deficiencies
There are no errors of design that lead to vulnerabilities

Coding defects
There are no implementation defects that create vulnerabilities

Operational guidance
The security features are well explained

Prevention and detection
Processes are in place, staff trained, runtime defenses mitigate latent problems

Code physically secure
The code is kept in a SCC system with access limited to essential personnel

Code correctness
Discuss different classes of errors and how they are detected

Runtime protection
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective

Programmers are trained
The staff is trained and follows procedures

Independent third party code review
Code reviews were performed and defects corrected

Static analysis tools
All code is scanned and important defects are corrected

Test suite
Code exercised by test suite show no unexpected errors

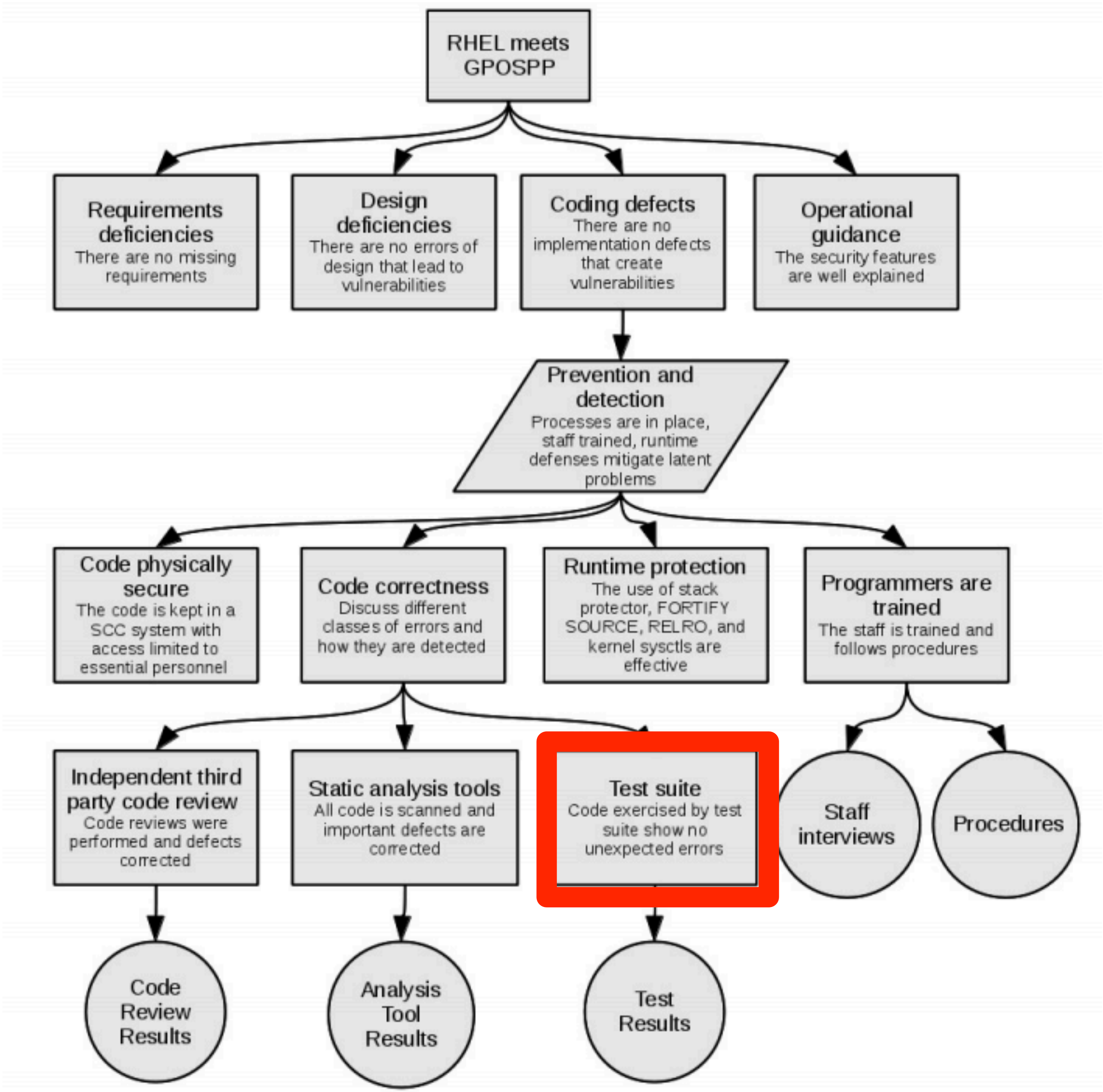
Staff interviews

Procedures

Code Review Results

Analysis Tool Results

Test Results



RHEL meets GPOSPP

Requirements deficiencies
There are no missing requirements

Design deficiencies
There are no errors of design that lead to vulnerabilities

Coding defects
There are no implementation defects that create vulnerabilities

Operational guidance
The security features are well explained

Prevention and detection
Processes are in place, staff trained, runtime defenses mitigate latent problems

Code physically secure
The code is kept in a SCC system with access limited to essential personnel

Code correctness
Discuss different classes of errors and how they are detected

Runtime protection
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective

Programmers are trained
The staff is trained and follows procedures

Independent third party code review
Code reviews were performed and defects corrected

Static analysis tools
All code is scanned and important defects are corrected

Test suite
Code exercised by test suite show no unexpected errors

Staff interviews

Procedures

Code Review Results

Analysis Tool Results

Test Results

SCAP
Security Guide

FSO

I43, I411,
TS13,
T3

NVD

U.S. Federal
AUS Federal
AppSec Engineering

RHEL5 STIG Delay:
1,988 days

RHEL6 STIG Delay:
932 days

STIG Version 1, Release 2, Section 1.1:

"The consensus content was developed using an open source project called SCAP Security Guide. The project's website is https://fedorahosted.org/scap-security-guide/. Except for differences in formatting to accommodate the DISA STIG publising process, the content of the RHEL6 STIG should mirror the SCAP Security Guide content with only minor divergences as updates from multiple sources work through the consensus process"

2.3.4.a. Ensure SELinux Not Disabled in /etc/grub.conf

SELinux can be disabled at boot time by an argument in `/etc/grub.conf`. Remove any instances of `selinux=0` from the kernel arguments in that file to prevent SELinux from being disabled at boot.

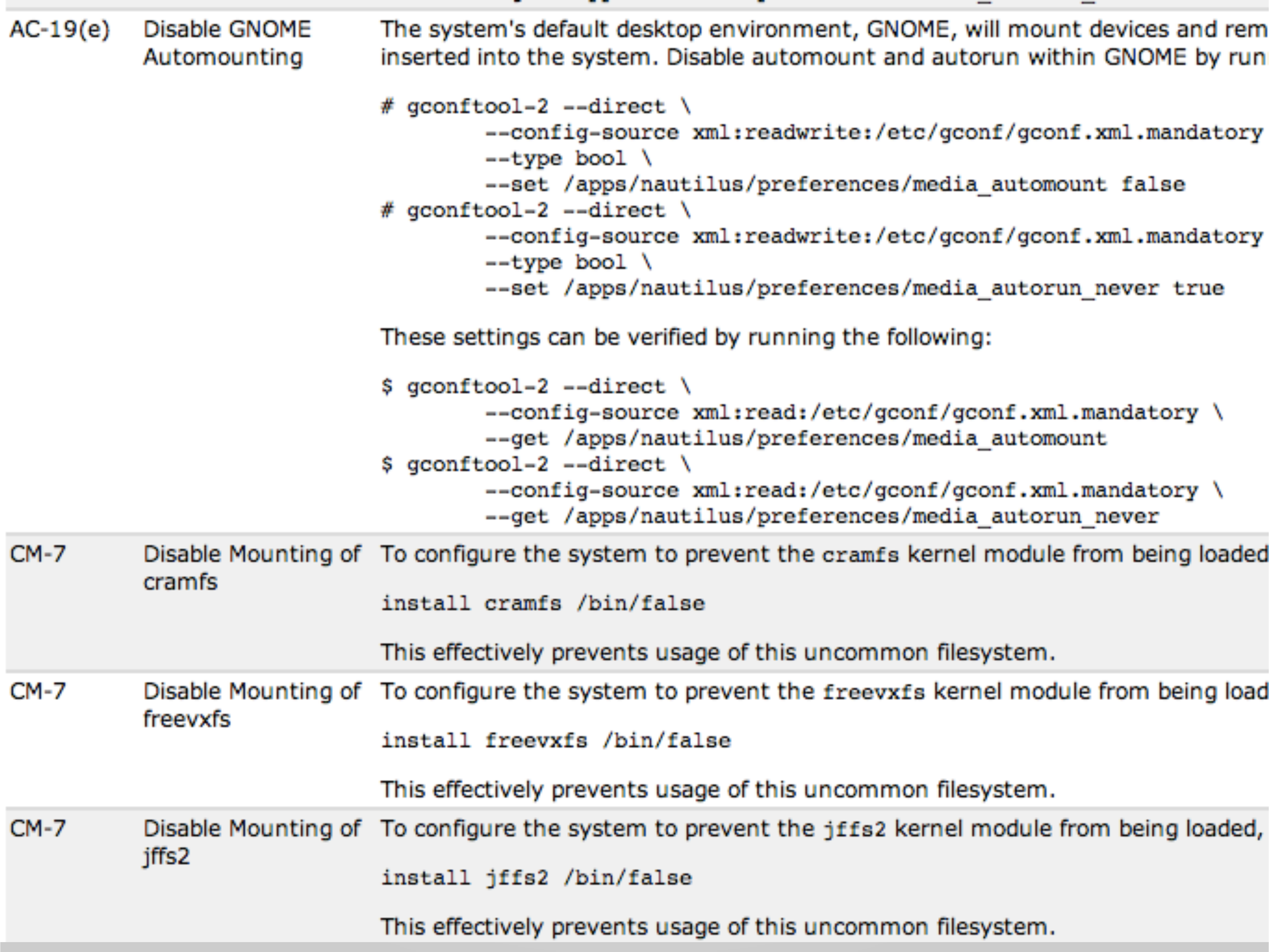
Disabling a major host protection feature, such as SELinux, at boot time prevents it from confining system services at boot time. Further, it increases the chances that it will remain off during system operation.

Security identifiers

- CCE-26956-3

References

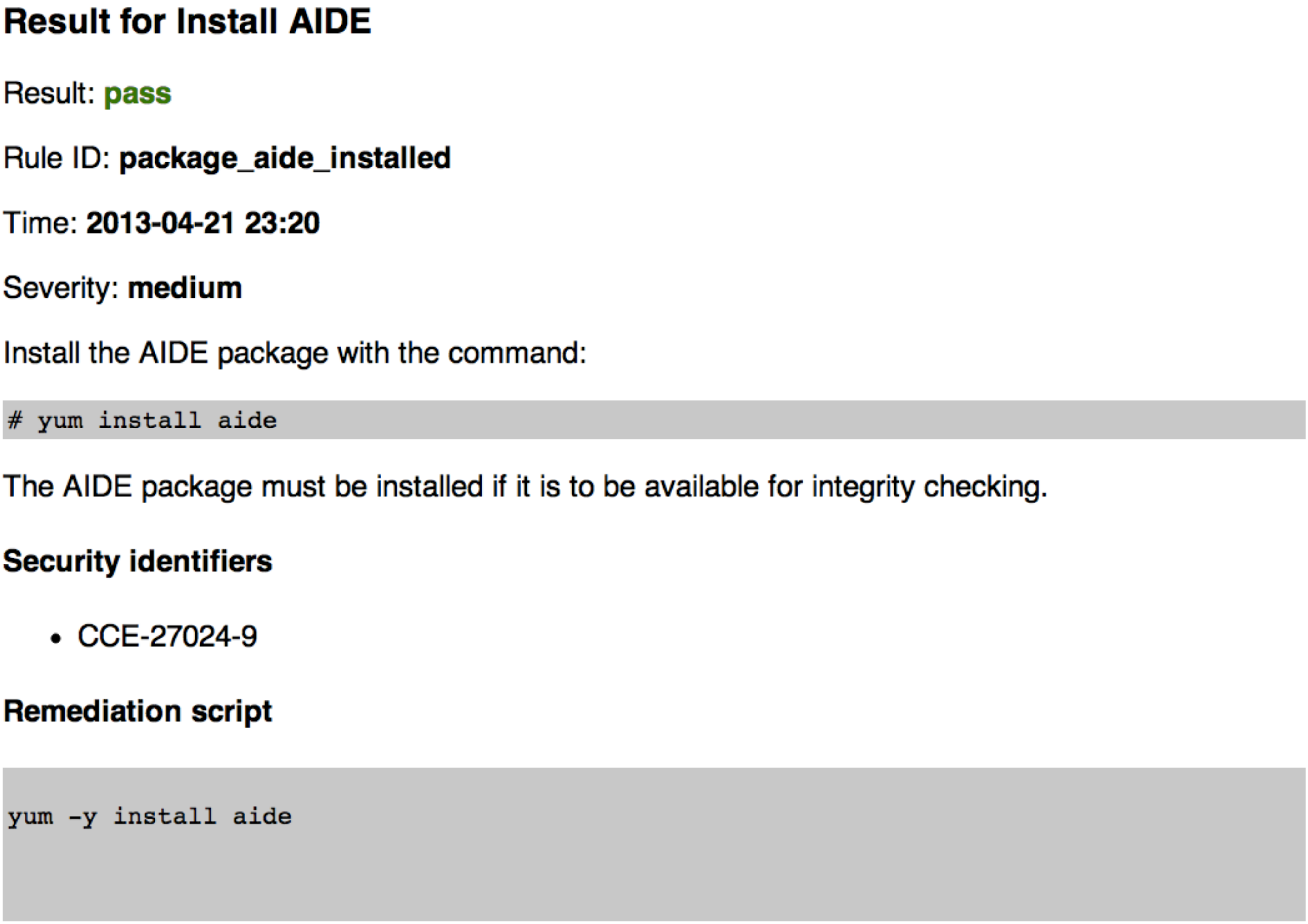
1. *AC-3*. URL: <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>.
2. *AC-3(3)*. URL: <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>.
3. *AC-6*. URL: <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>.
4. *AU-9*. URL: <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>.
5. *22*. URL: <http://iase.disa.mil/cci/index.html>.
6. *32*. URL: <http://iase.disa.mil/cci/index.html>.



<table>
<tr><td>AC-19(e)</td><td>Disable GNOME Automounting</td><td>The system's default desktop environment, GNOME, will mount devices and rem
inserted into the system. Disable automount and autorun within GNOME by run
<pre>
gconftool-2 --direct \
        --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory
        --type bool \
        --set /apps/nautilus/preferences/media_automount false
gconftool-2 --direct \
        --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory
        --type bool \
        --set /apps/nautilus/preferences/media_autorun_never true
</pre>
These settings can be verified by running the following:
<pre>
$ gconftool-2 --direct \
        --config-source xml:read:/etc/gconf/gconf.xml.mandatory \
        --get /apps/nautilus/preferences/media_automount
$ gconftool-2 --direct \
        --config-source xml:read:/etc/gconf/gconf.xml.mandatory \
        --get /apps/nautilus/preferences/media_autorun_never
</pre></td></tr>
<tr><td>CM-7</td><td>Disable Mounting of cramfs</td><td>To configure the system to prevent the <code>cramfs</code> kernel module from being loaded
<pre>
install cramfs /bin/false
</pre>
This effectively prevents usage of this uncommon filesystem.</td></tr>
<tr><td>CM-7</td><td>Disable Mounting of freevxfs</td><td>To configure the system to prevent the <code>freevxfs</code> kernel module from being load
<pre>
install freevxfs /bin/false
</pre>
This effectively prevents usage of this uncommon filesystem.</td></tr>
<tr><td>CM-7</td><td>Disable Mounting of jffs2</td><td>To configure the system to prevent the <code>jffs2</code> kernel module from being loaded,
<pre>
install jffs2 /bin/false
</pre>
This effectively prevents usage of this uncommon filesystem.</td></tr>
</table>

SCAP Security Guide

- Guidance broken into profiles:
  - RHEL6 STIG
  - CS2 ★
  - NIST NVD (JBoss only)
  - FISMA Moderate (in progress)



Result for Install AIDE

Result: pass

Rule ID: **package_aide_installed**

Time: **2013-04-21 23:20**

Severity: **medium**

Install the AIDE package with the command:

```
# yum install aide
```

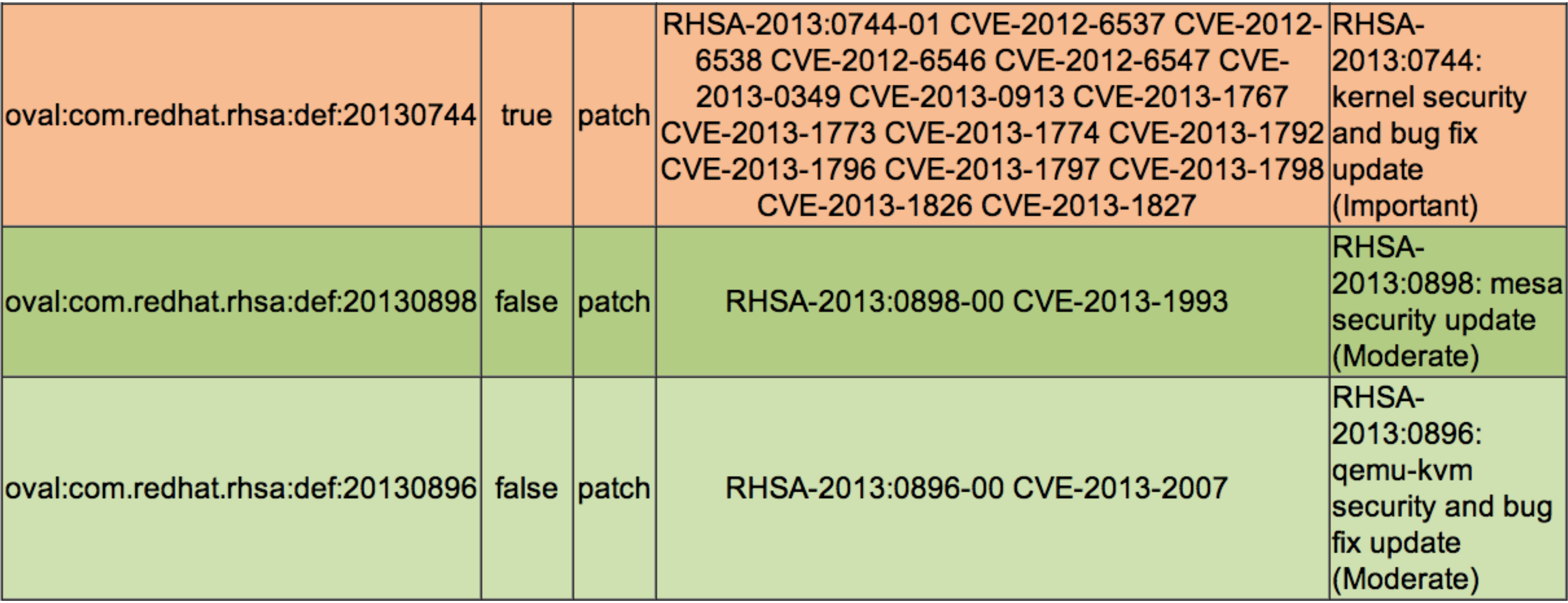
The AIDE package must be installed if it is to be available for integrity checking.

Security identifiers

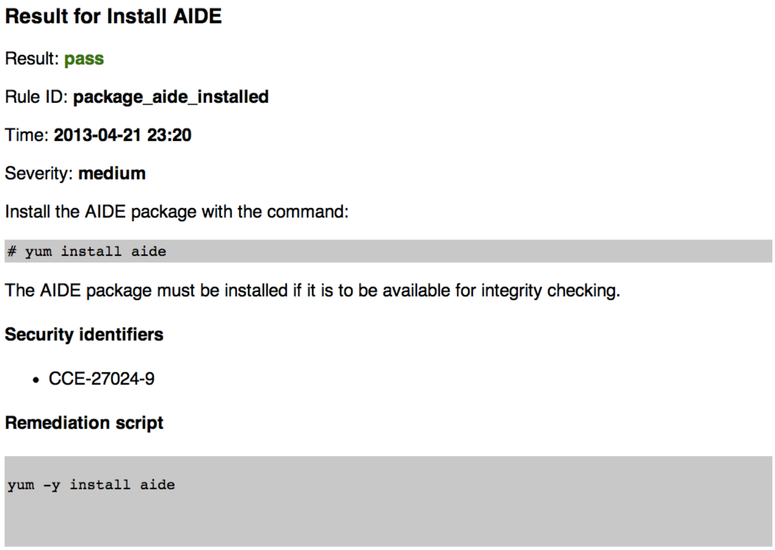
- CCE-27024-9

Remediation script

```
yum -y install aide
```



oval:com.redhat.rhsa:def:20130744	true	patch	RHSA-2013:0744-01 CVE-2012-6537 CVE-2012-6538 CVE-2012-6546 CVE-2012-6547 CVE-2013-0349 CVE-2013-0913 CVE-2013-1767 CVE-2013-1773 CVE-2013-1774 CVE-2013-1792 CVE-2013-1796 CVE-2013-1797 CVE-2013-1798 CVE-2013-1826 CVE-2013-1827	RHSA-2013:0744: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20130898	false	patch	RHSA-2013:0898-00 CVE-2013-1993	RHSA-2013:0898: mesa security update (Moderate)
oval:com.redhat.rhsa:def:20130896	false	patch	RHSA-2013:0896-00 CVE-2013-2007	RHSA-2013:0896: qemu-kvm security and bug fix update (Moderate)



Result for Install AIDE

Result: pass

Rule ID: **package_aide_installed**

Time: **2013-04-21 23:20**

Severity: **medium**

Install the AIDE package with the command:

```
# yum install aide
```

The AIDE package must be installed if it is to be available for integrity checking.

Security identifiers

- CCE-27024-9

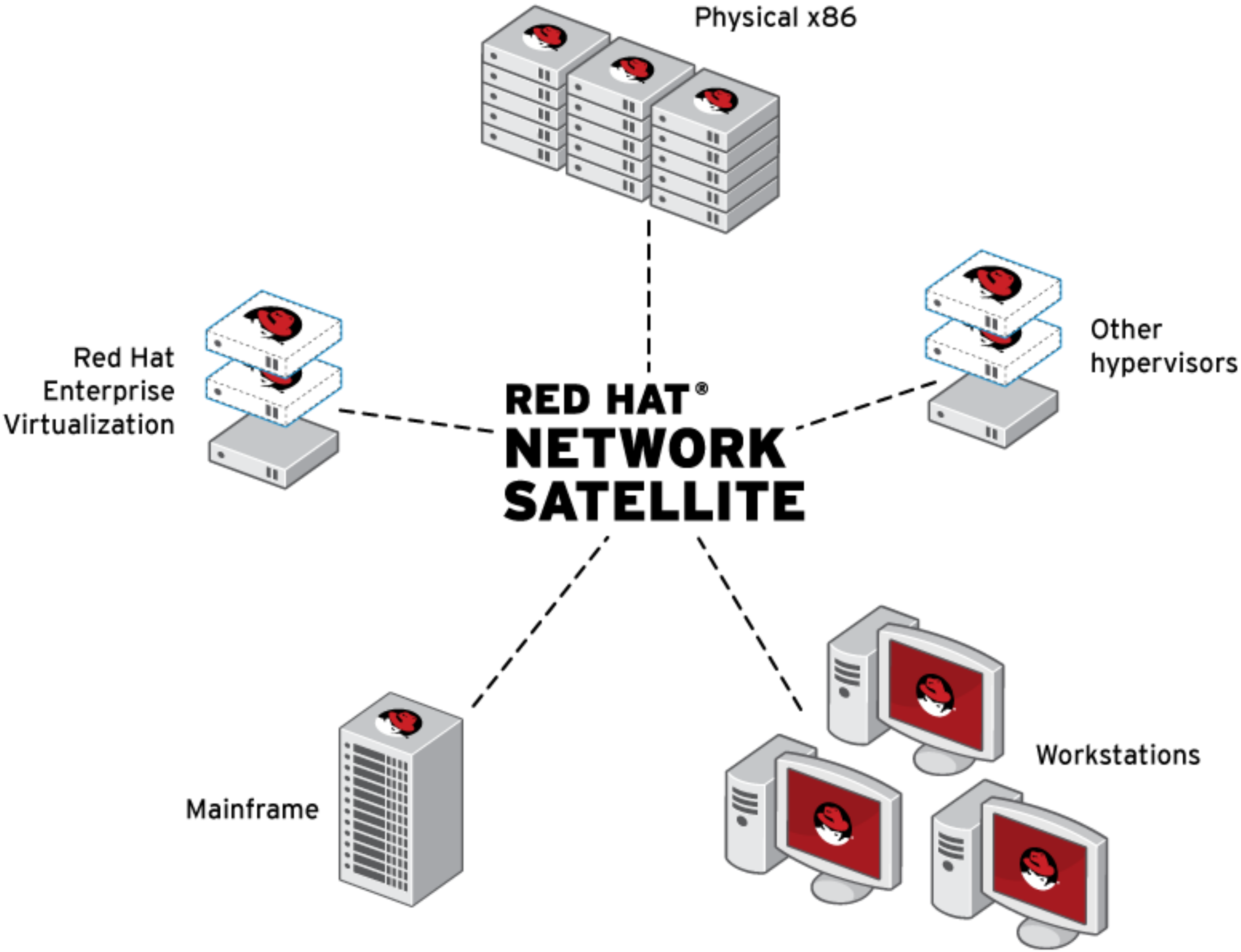
Remediation script

```
yum -y install aide
```

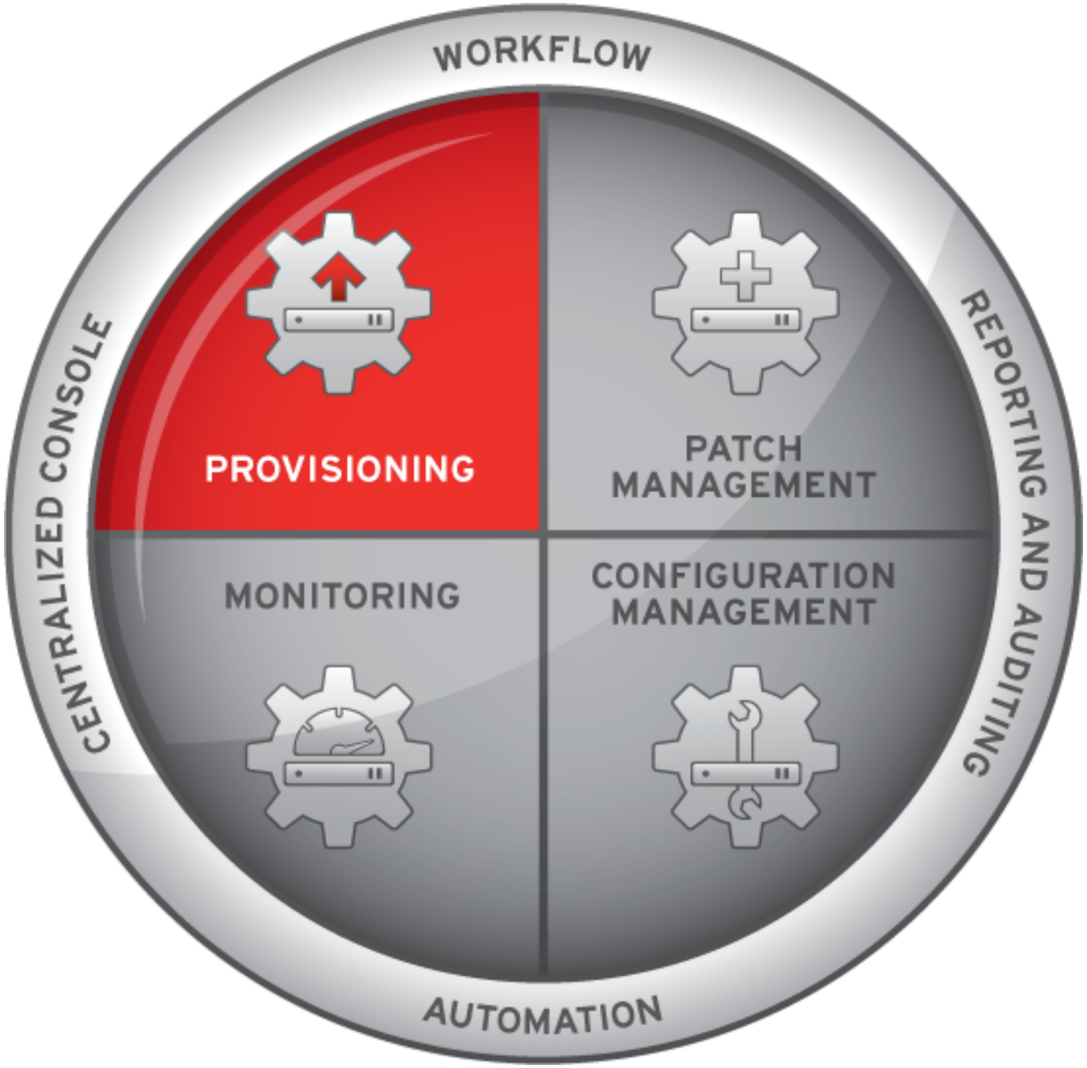
```
<fix system="urn:xccdf:fix:script:sh">
  yum -y install aide
</fix>
```

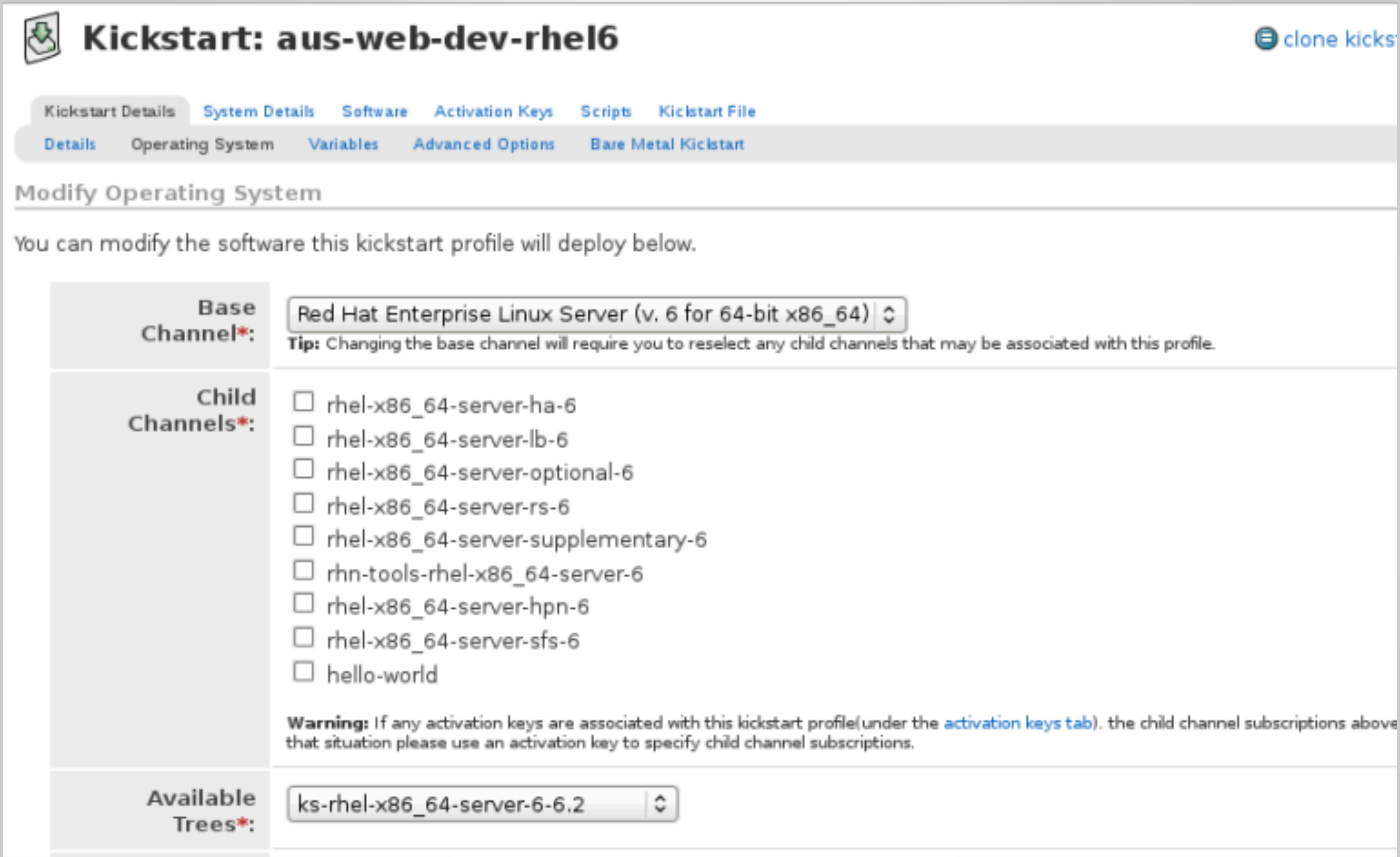
SYSTEMS MANAGEMENT

T3 SYSTEM MANAGEMENT CAPABILITIES



T3 SYSTEM MANAGEMENT CAPABILITIES





Kickstart: aus-web-dev-rhel6

Modify Operating System

You can modify the software this kickstart profile will deploy below.

Base Channel*: Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)

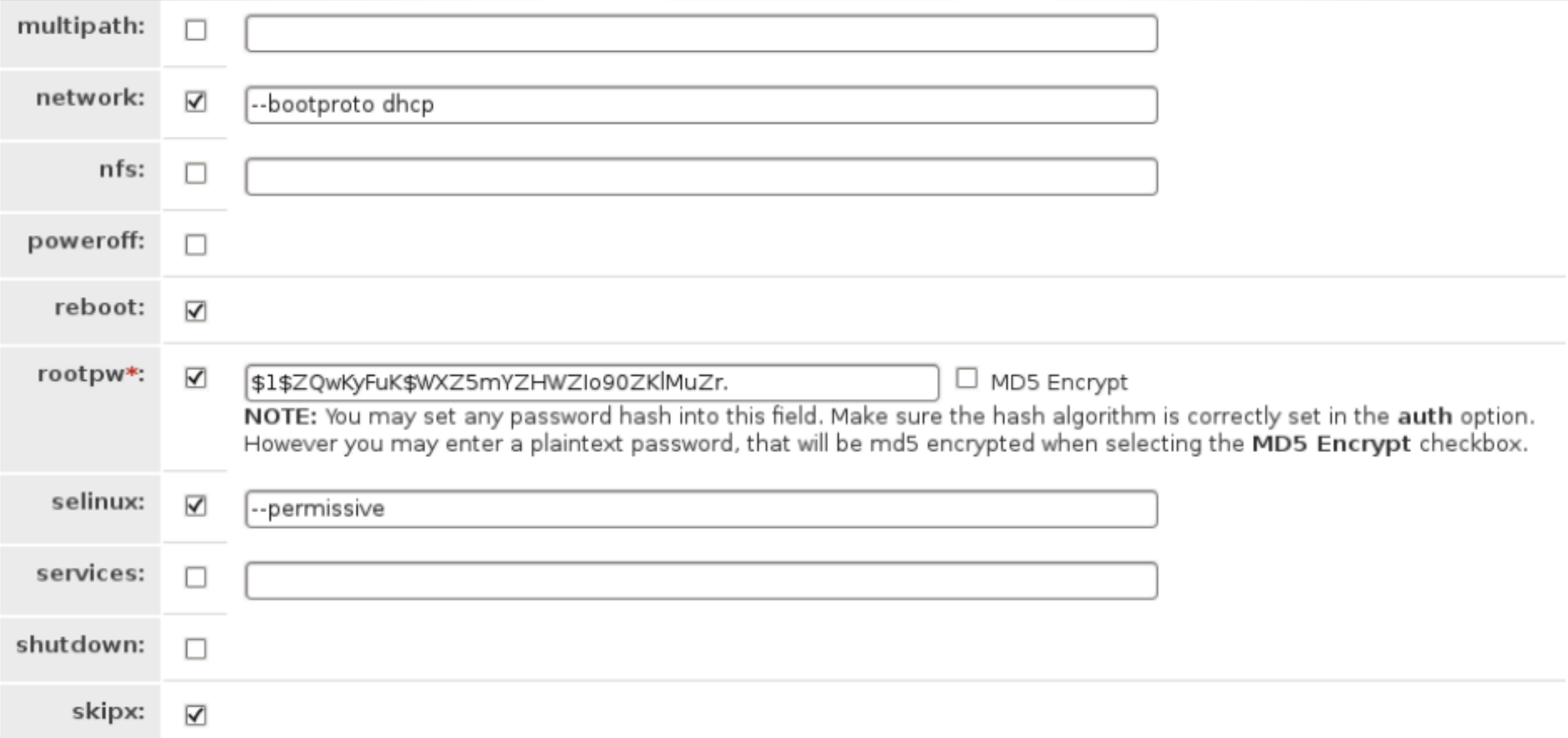
Tip: Changing the base channel will require you to reselect any child channels that may be associated with this profile.

Child Channels*:

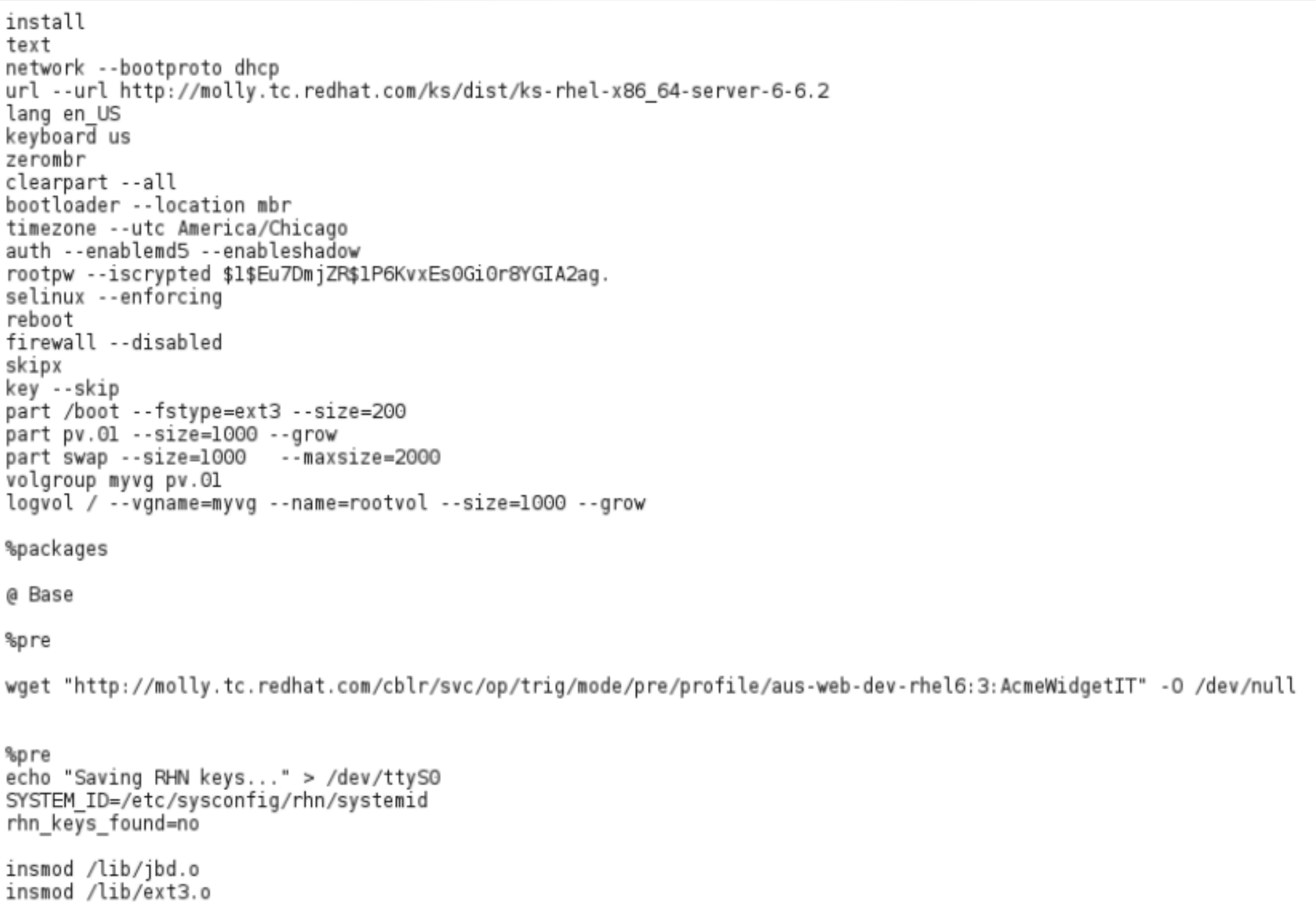
- □ rhel-x86_64-server-ha-6
- □ rhel-x86_64-server-lb-6
- □ rhel-x86_64-server-optional-6
- □ rhel-x86_64-server-rs-6
- □ rhel-x86_64-server-supplementary-6
- □ rhn-tools-rhel-x86_64-server-6
- □ rhel-x86_64-server-hpn-6
- □ rhel-x86_64-server-sfs-6
- □ hello-world

Warning: If any activation keys are associated with this kickstart profile(under the activation keys tab). the child channel subscriptions above
that situation please use an activation key to specify child channel subscriptions.

Available Trees*: ks-rhel-x86_64-server-6-6.2

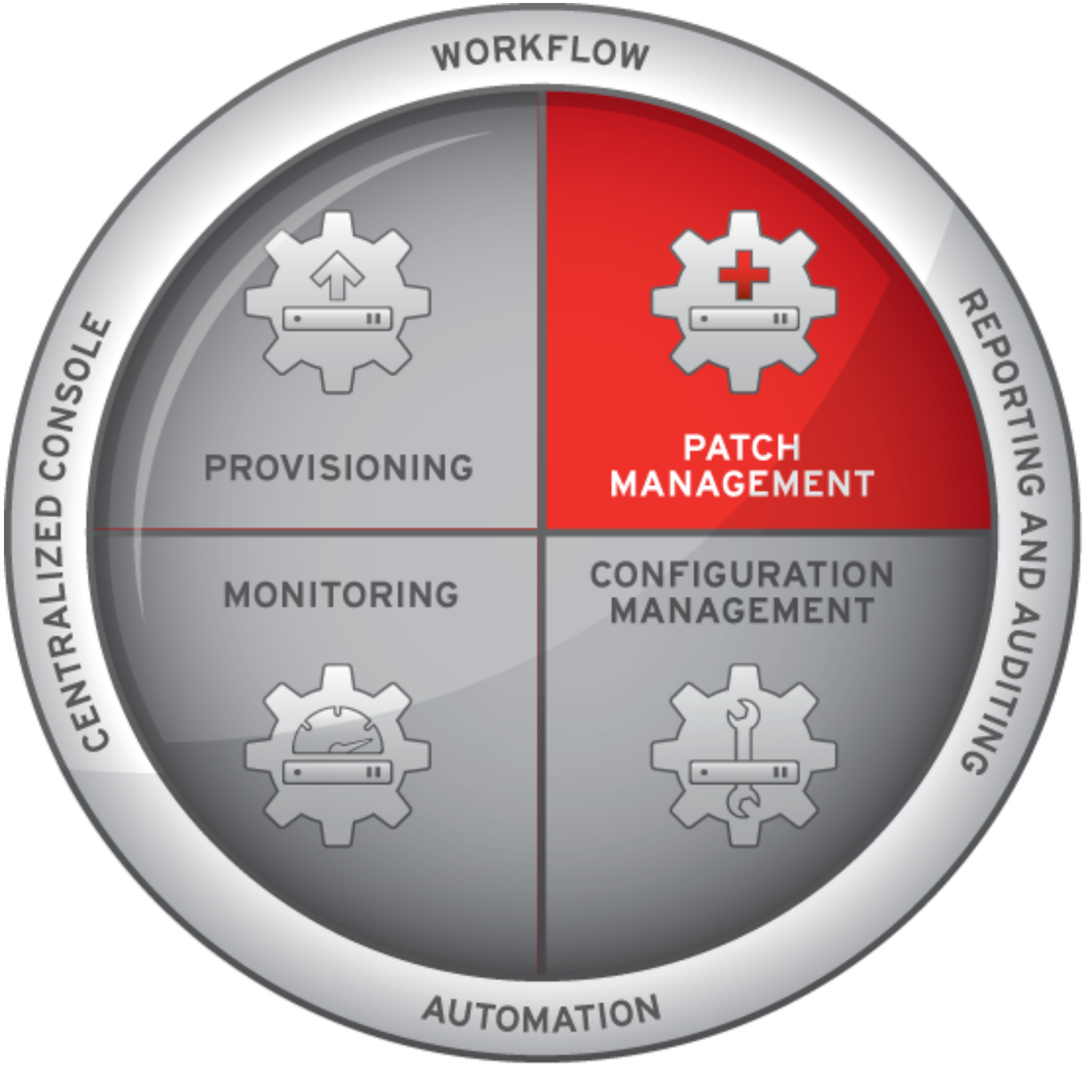


multipath:	□	
network:	☑	--bootproto dhcp
nfs:	□	
poweroff:	□	
reboot:	☑	
rootpw*:	☑	$1$ZQwKyFuK$WXZ5mYZHWZIo90ZKlMuZr. □ MD5 Encrypt **NOTE:** You may set any password hash into this field. Make sure the hash algorithm is correctly set in the **auth** option. However you may enter a plaintext password, that will be md5 encrypted when selecting the **MD5 Encrypt** checkbox.
selinux:	☑	--permissive
services:	□	
shutdown:	□	
skipx:	☑	

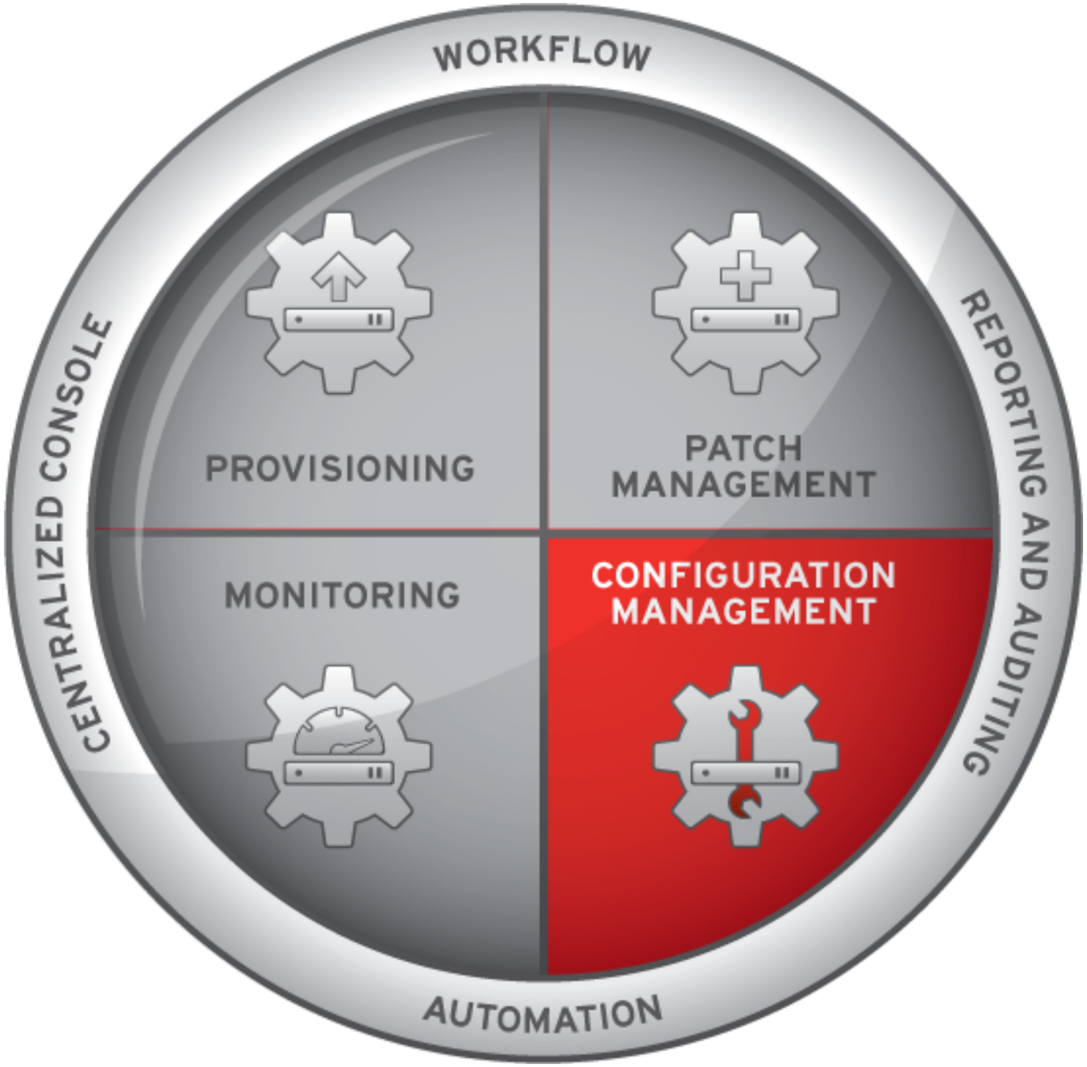


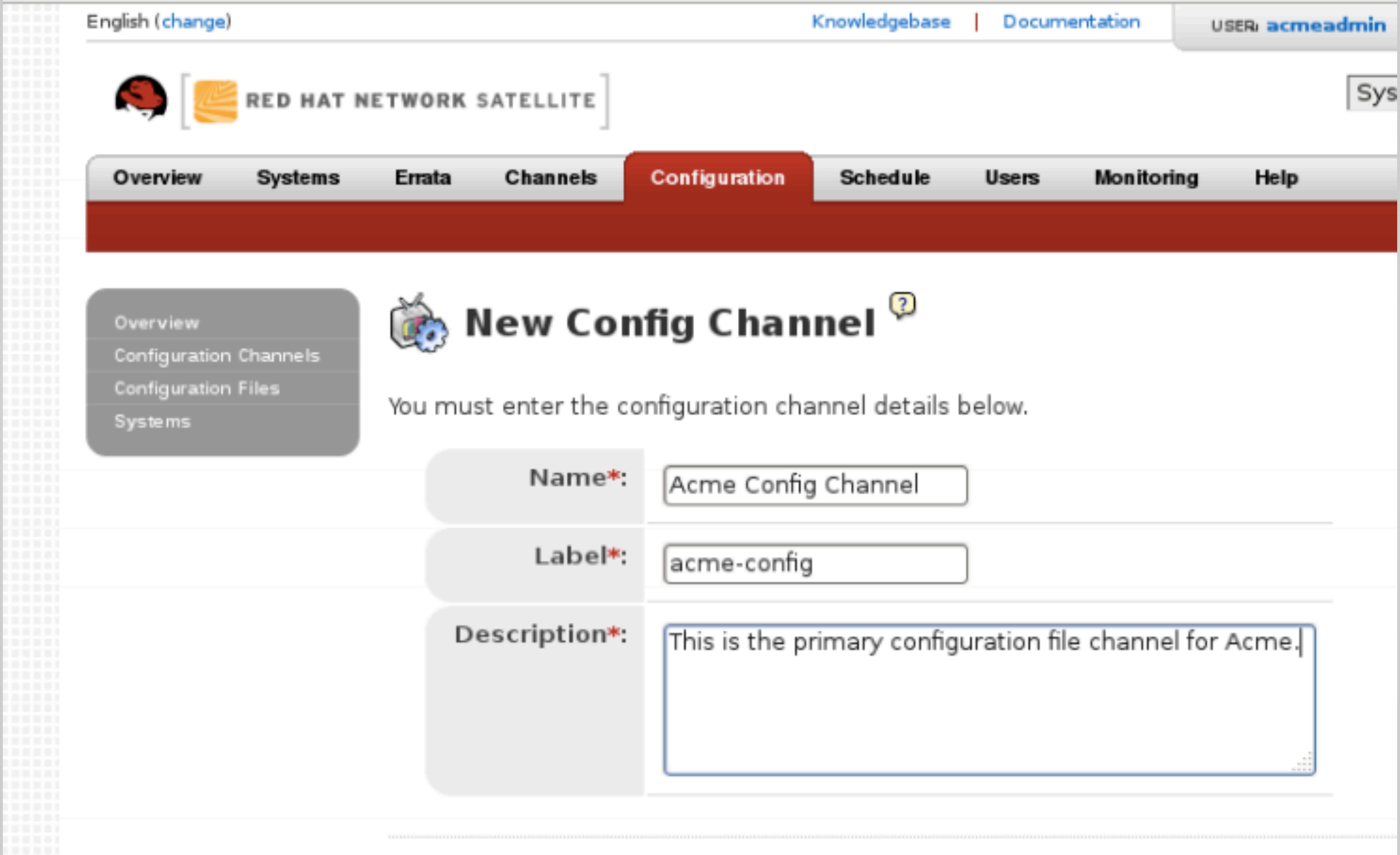
```
install
text
network --bootproto dhcp
url --url http://molly.tc.redhat.com/ks/dist/ks-rhel-x86_64-server-6-6.2
lang en_US
keyboard us
zerombr
clearpart --all
bootloader --location mbr
timezone --utc America/Chicago
auth --enablemd5 --enableshadow
rootpw --iscrypted $1$Eu7DmjZR$1P6KvxEs0Gi0r8YGIA2ag.
selinux --enforcing
reboot
firewall --disabled
skipx
key --skip
part /boot --fstype=ext3 --size=200
part pv.01 --size=1000 --grow
part swap --size=1000   --maxsize=2000
volgroup myvg pv.01
logvol / --vgname=myvg --name=rootvol --size=1000 --grow

%packages

@ Base

%pre

wget "http://molly.tc.redhat.com/cblr/svc/op/trig/mode/pre/profile/aus-web-dev-rhel6:3:AcmeWidgetIT" -O /dev/null


%pre
echo "Saving RHN keys..." > /dev/ttyS0
SYSTEM_ID=/etc/sysconfig/rhn/systemid
rhn_keys_found=no

insmod /lib/jbd.o
insmod /lib/ext3.o
```

T3 SYSTEM MANAGEMENT CAPABILITIES



T3 SYSTEM MANAGEMENT CAPABILITIES

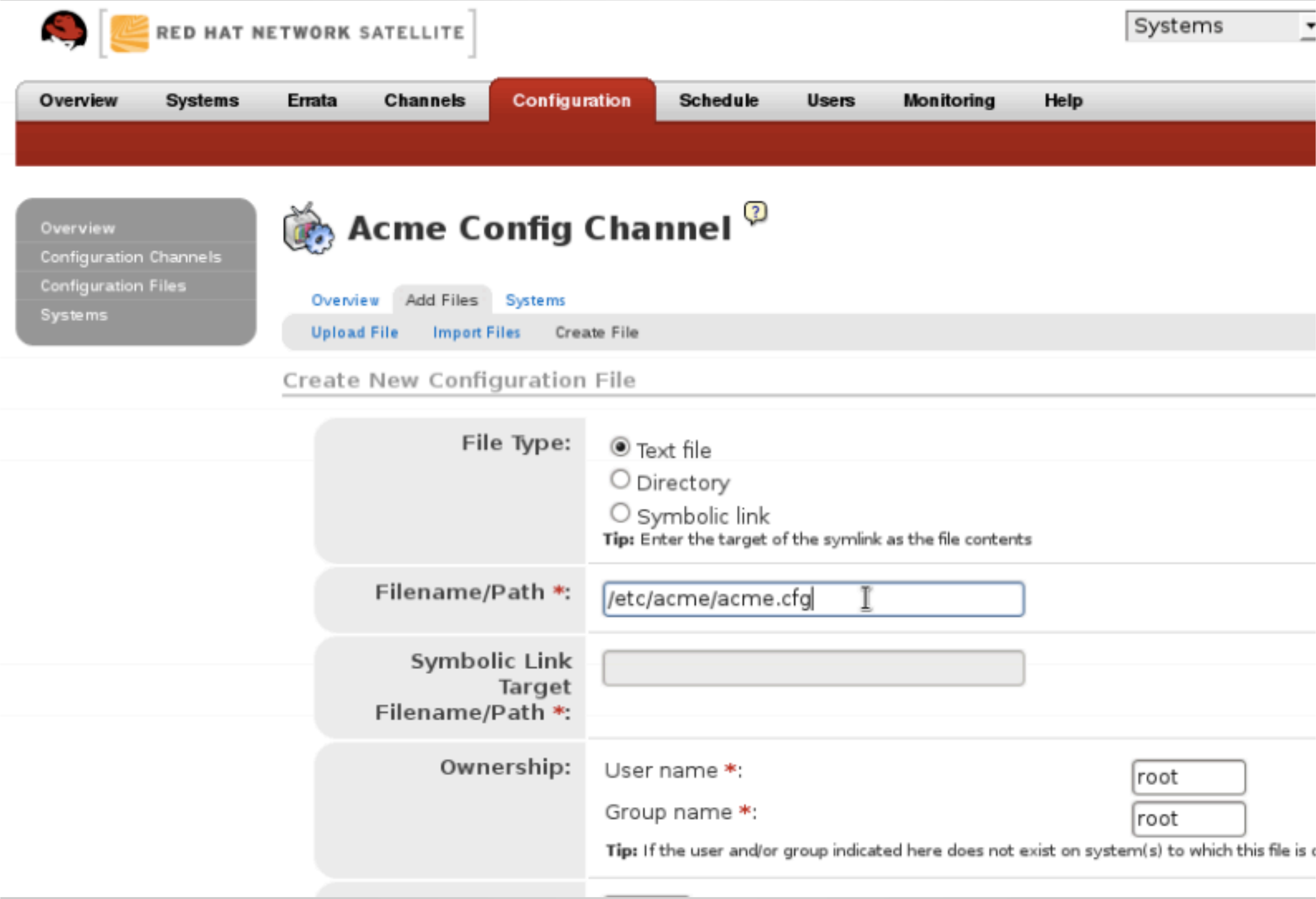




New Config Channel

You must enter the configuration channel details below.

Name*:	Acme Config Channel
Label*:	acme-config
Description*:	This is the primary configuration file channel for Acme.



Acme Config Channel

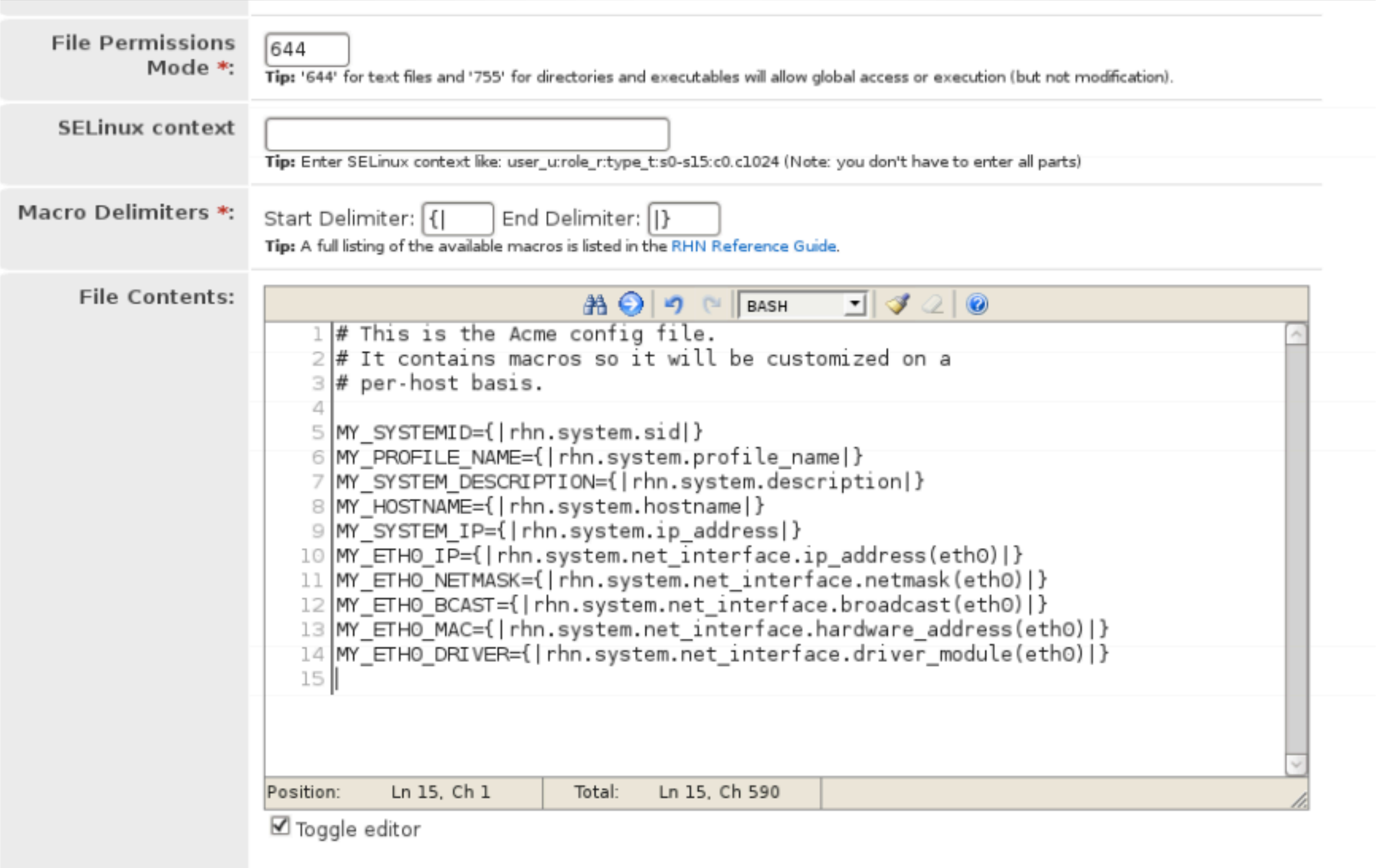
Create New Configuration File

File Type:
● Text file
○ Directory
○ Symbolic link
Tip: Enter the target of the symlink as the file contents

Filename/Path *: /etc/acme/acme.cfg

Symbolic Link Target Filename/Path *:

Ownership:
User name *: root
Group name *: root
Tip: If the user and/or group indicated here does not exist on system(s) to which this file is



File Permissions Mode *: 644

Tip: '644' for text files and '755' for directories and executables will allow global access or execution (but not modification).

SELinux context:

Tip: Enter SELinux context like: user_u:role_r:type_t:s0-s15:c0.c1024 (Note: you don't have to enter all parts)

Macro Delimiters *: Start Delimiter: {| End Delimiter: |}

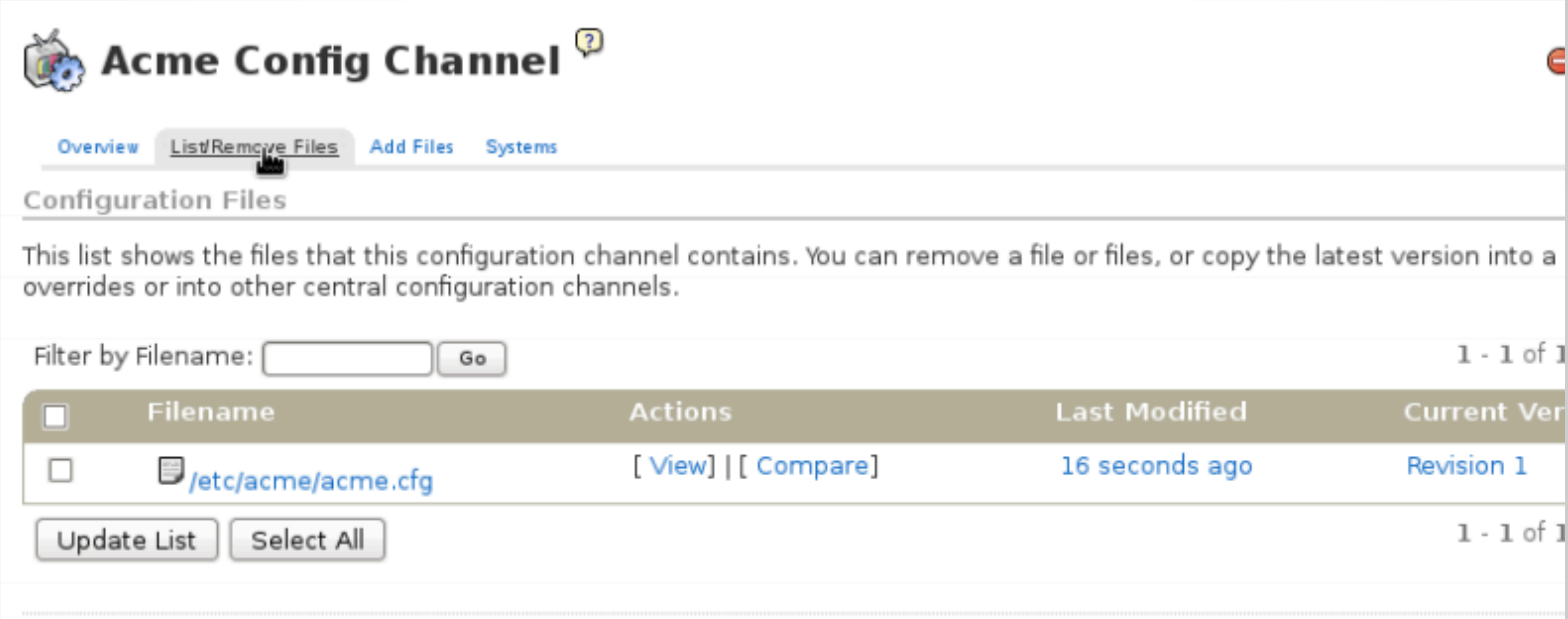
Tip: A full listing of the available macros is listed in the RHN Reference Guide.

File Contents:

```
# This is the Acme config file.
# It contains macros so it will be customized on a
# per-host basis.

MY_SYSTEMID={|rhn.system.sid|}
MY_PROFILE_NAME={|rhn.system.profile_name|}
MY_SYSTEM_DESCRIPTION={|rhn.system.description|}
MY_HOSTNAME={|rhn.system.hostname|}
MY_SYSTEM_IP={|rhn.system.ip_address|}
MY_ETH0_IP={|rhn.system.net_interface.ip_address(eth0)|}
MY_ETH0_NETMASK={|rhn.system.net_interface.netmask(eth0)|}
MY_ETH0_BCAST={|rhn.system.net_interface.broadcast(eth0)|}
MY_ETH0_MAC={|rhn.system.net_interface.hardware_address(eth0)|}
MY_ETH0_DRIVER={|rhn.system.net_interface.driver_module(eth0)|}
```

Position: Ln 15, Ch 1 | Total: Ln 15, Ch 590

☑ Toggle editor



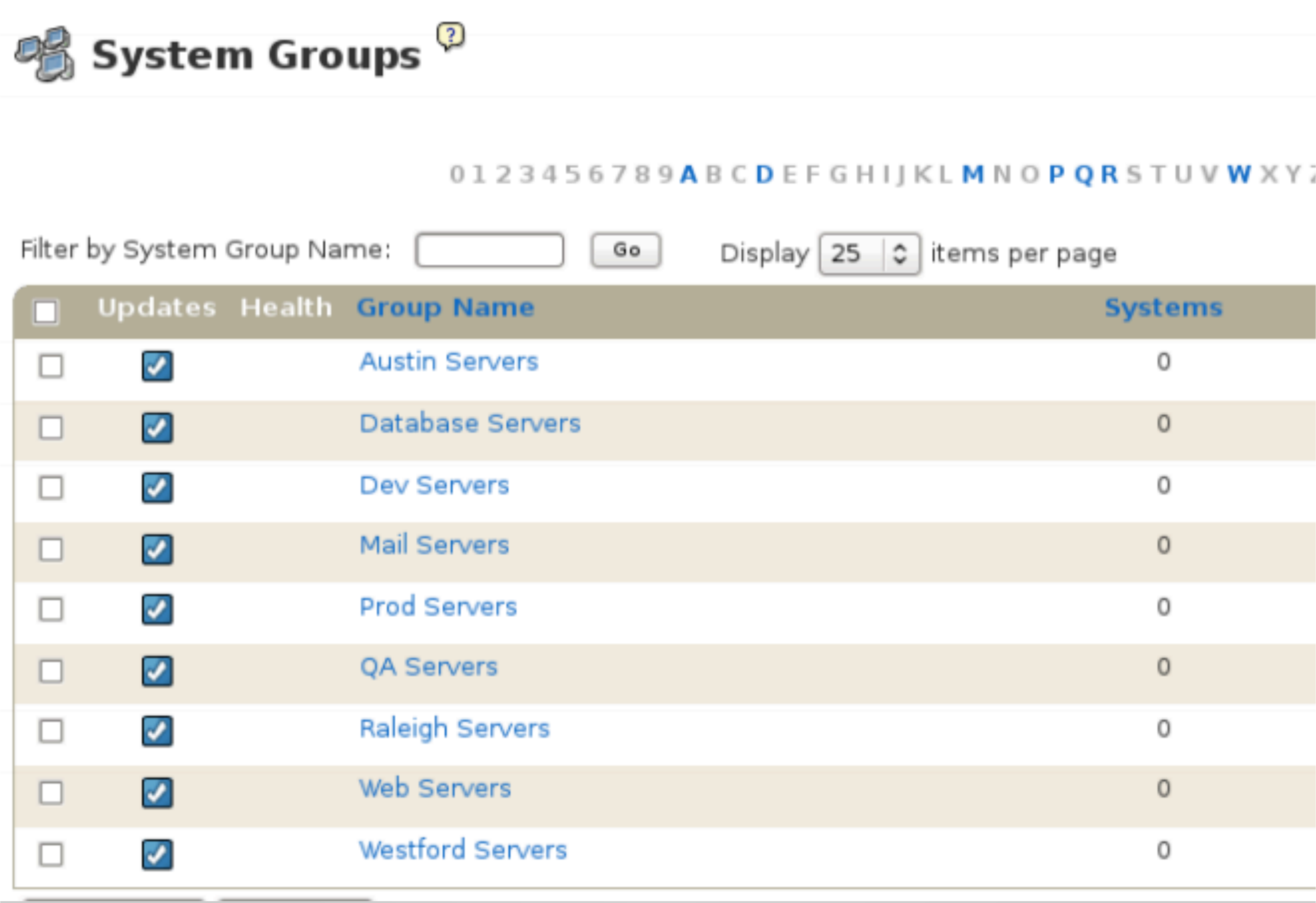
Acme Config Channel

Configuration Files

This list shows the files that this configuration channel contains. You can remove a file or files, or copy the latest version into a overrides or into other central configuration channels.

Filter by Filename:

□	Filename	Actions	Last Modified	Current Ver
□	/etc/acme/acme.cfg	[View] | [Compare]	16 seconds ago	Revision 1



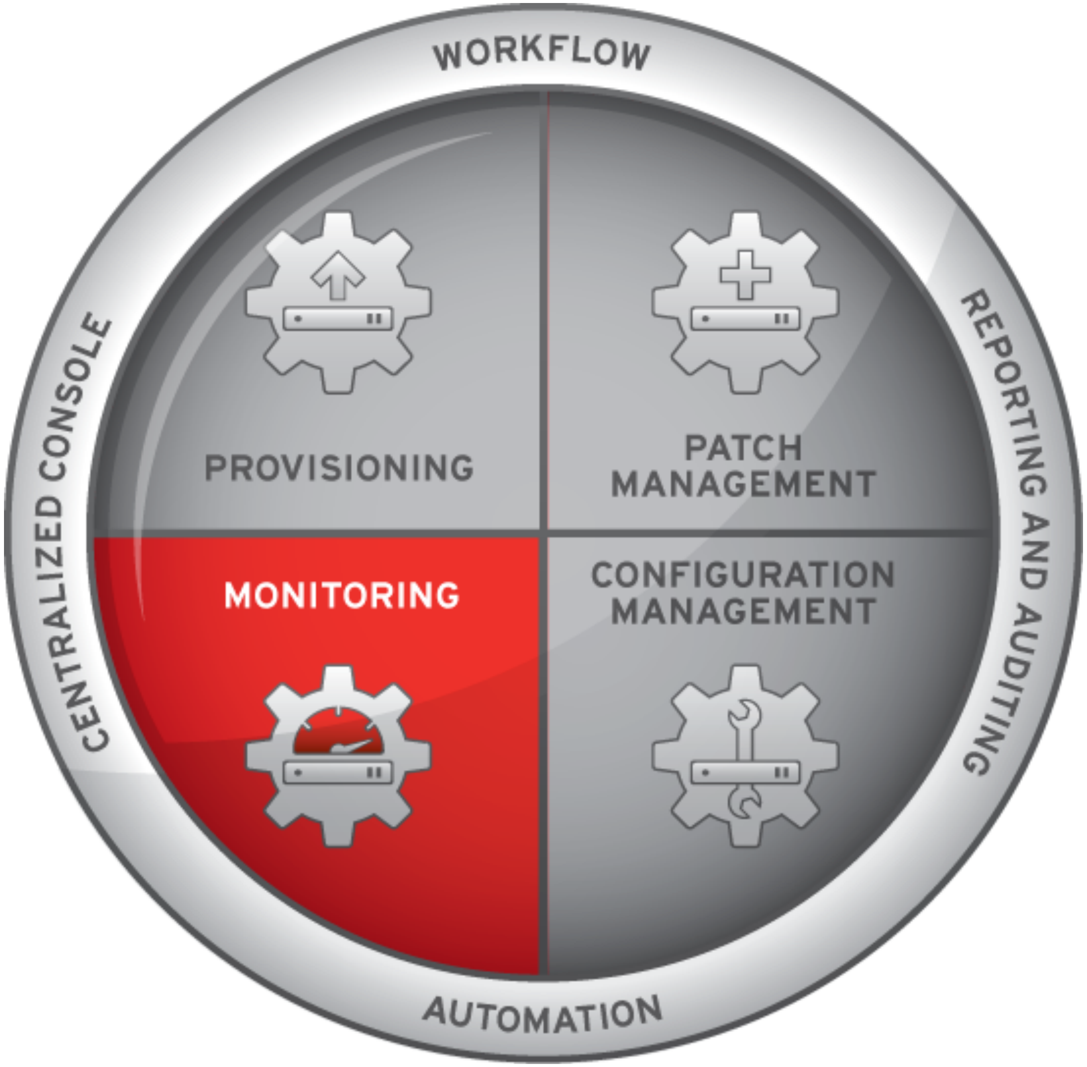
System Groups

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y

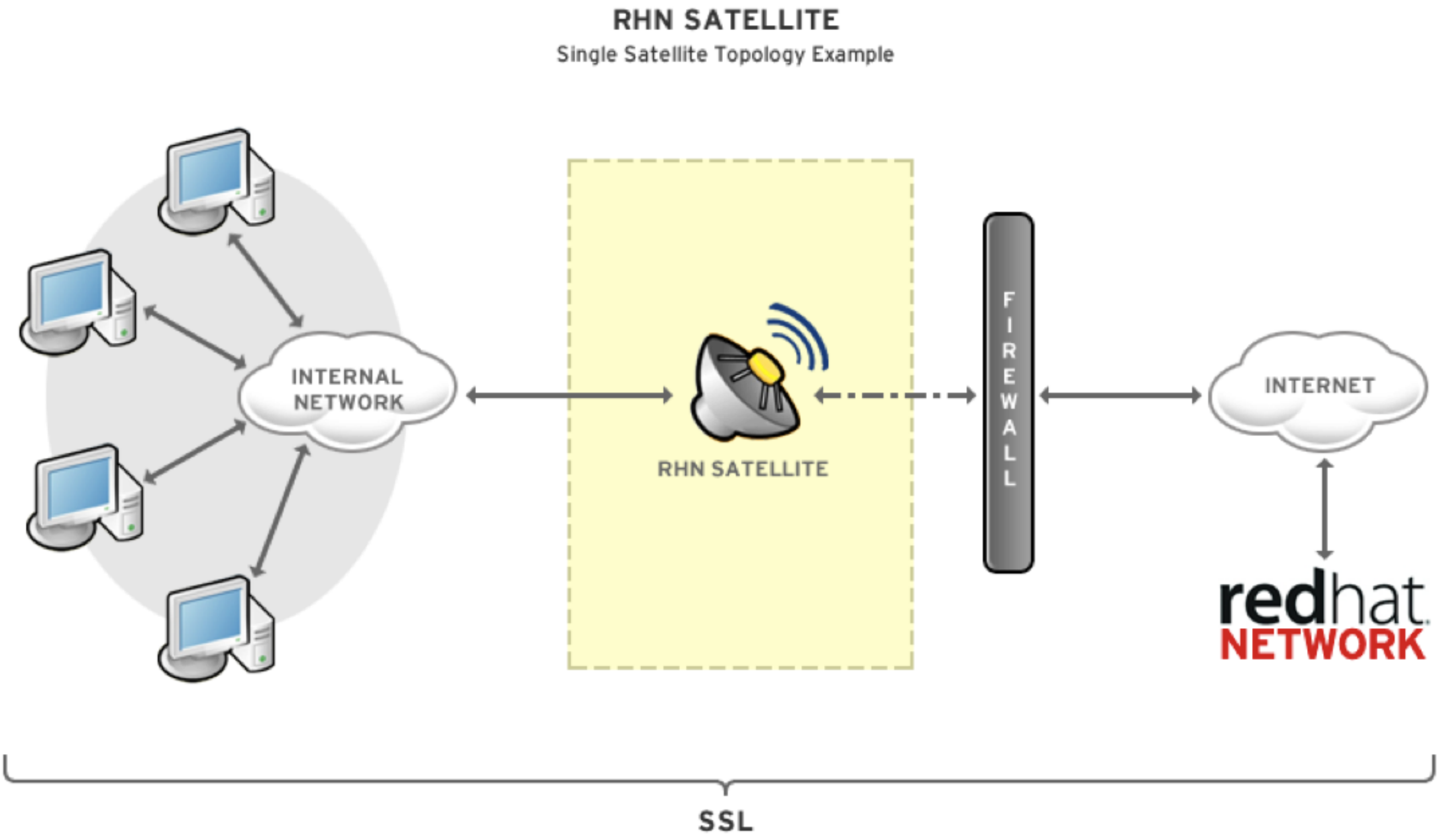
Filter by System Group Name: Go Display 25 items per page

□	Updates	Health	Group Name	Systems
□	☑		Austin Servers	0
□	☑		Database Servers	0
□	☑		Dev Servers	0
□	☑		Mail Servers	0
□	☑		Prod Servers	0
□	☑		QA Servers	0
□	☑		Raleigh Servers	0
□	☑		Web Servers	0
□	☑		Westford Servers	0

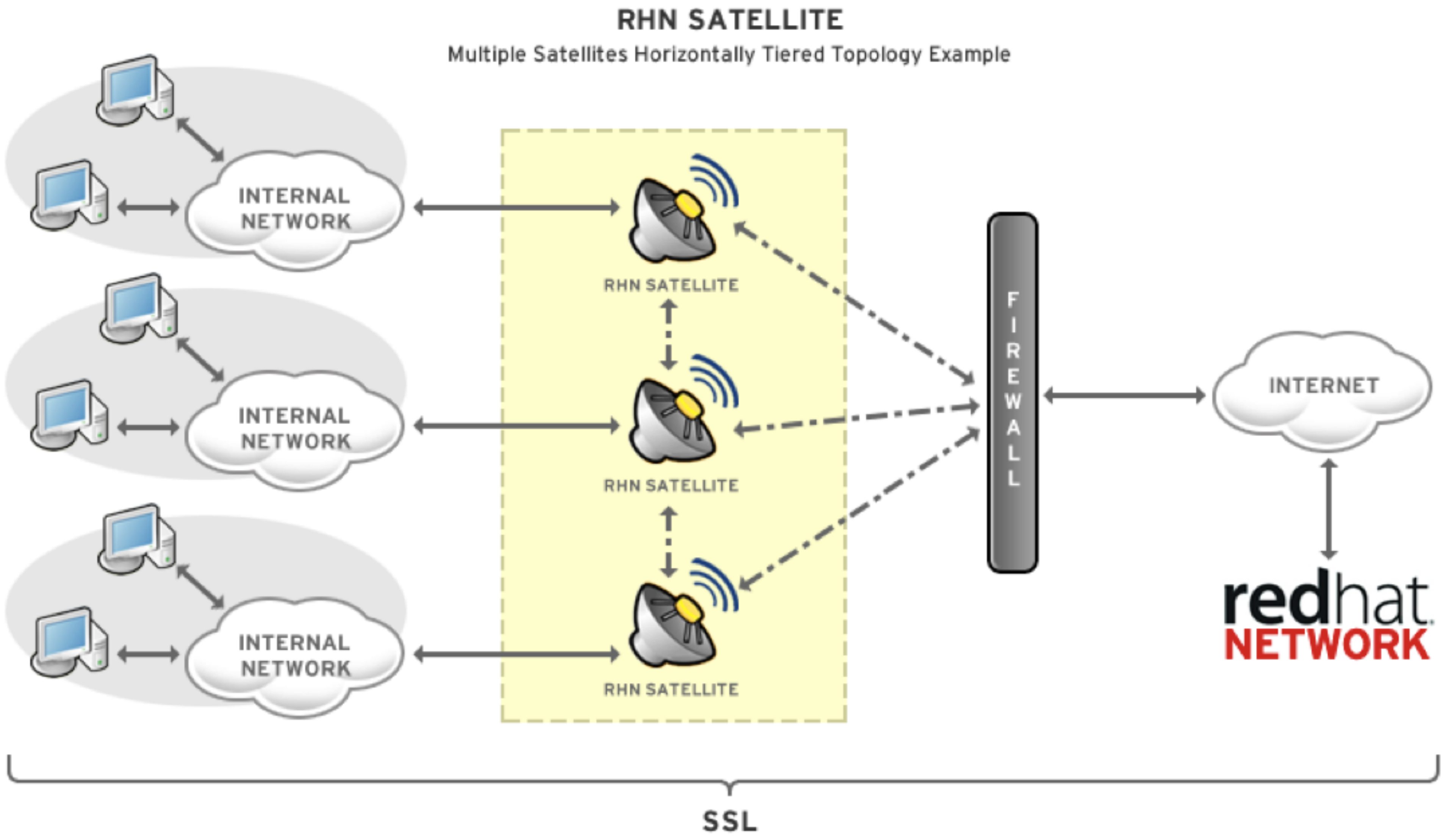
T3 SYSTEM MANAGEMENT CAPABILITIES



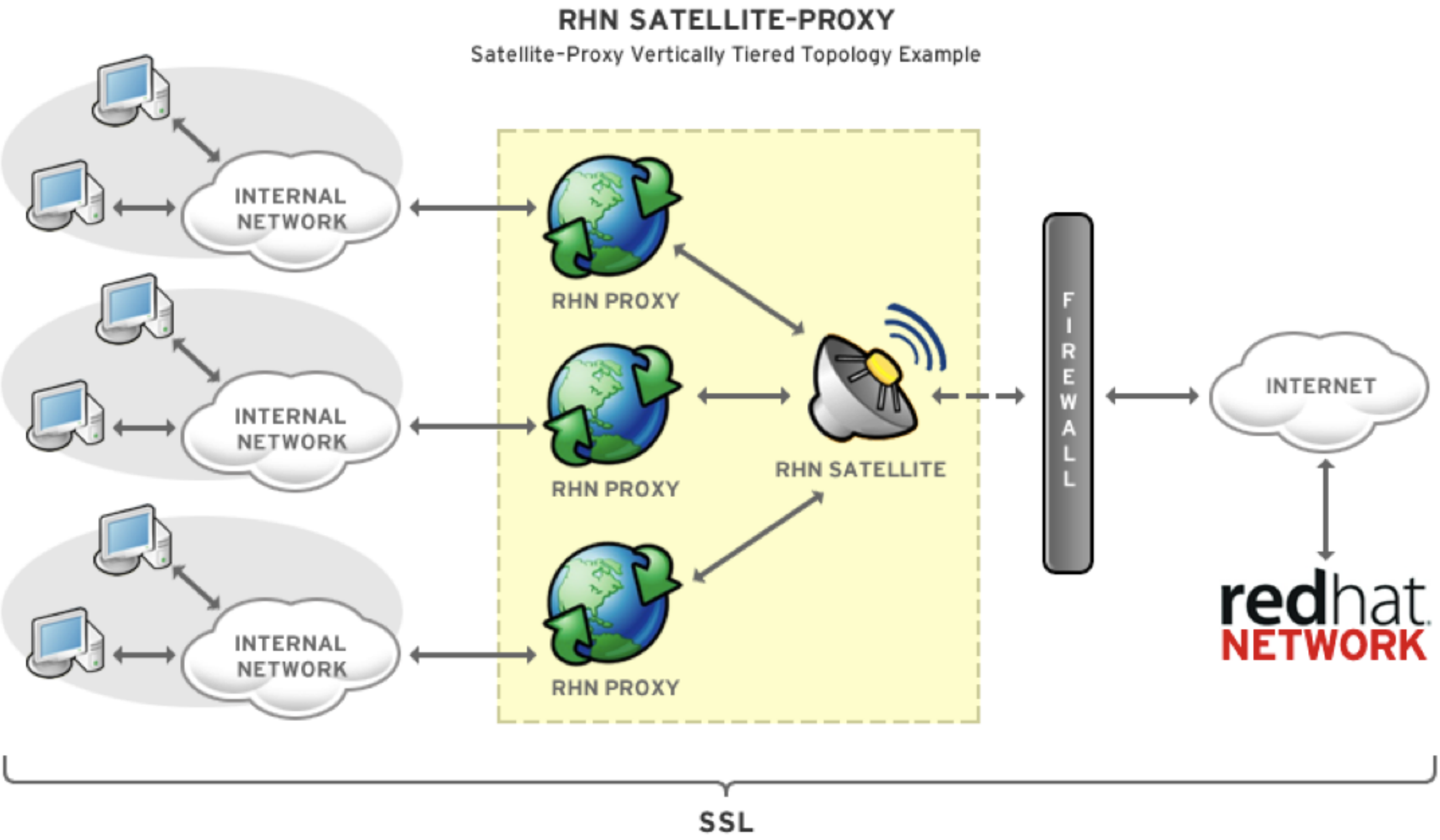
T3 SYSTEM MANAGEMENT CAPABILITIES



T3 SYSTEM MANAGEMENT CAPABILITIES



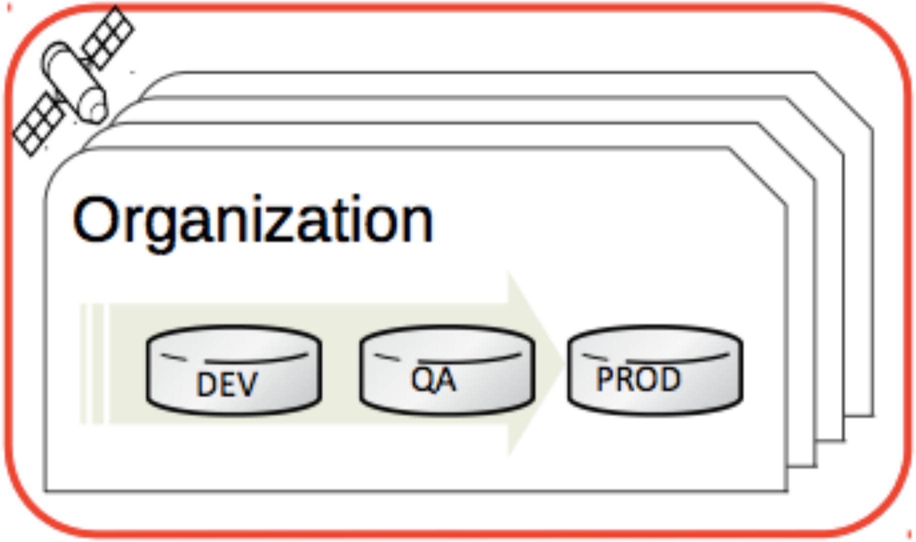
T3 SYSTEM MANAGEMENT CAPABILITIES



T3 RHN Satellite v6: Launching in 2014

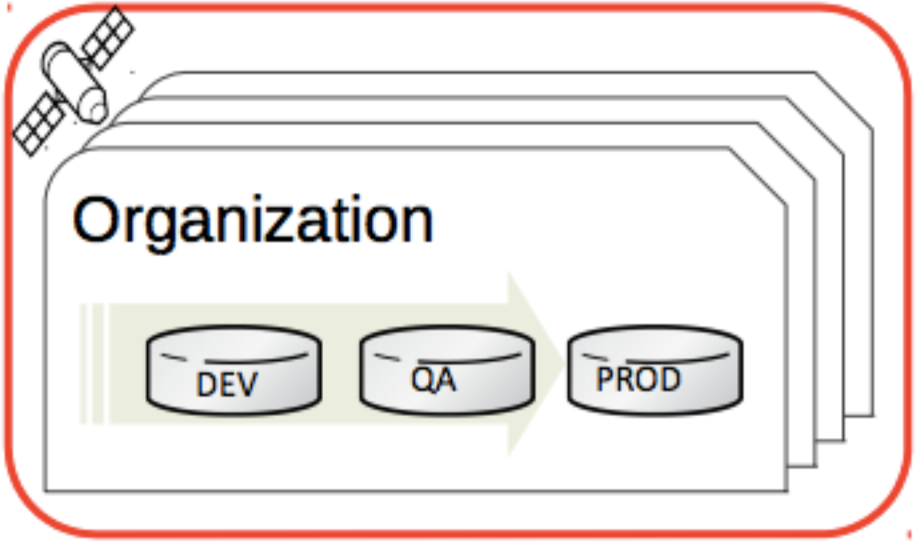
- An entirely new Satellite system
  - Puppet for Configuration
  - Foreman for Provisioning
  - Katello for Content Management
  - Pulp for Repo Management
  - Candlepin for Subscription Management

T3 RHN Satellite v6: Workflow

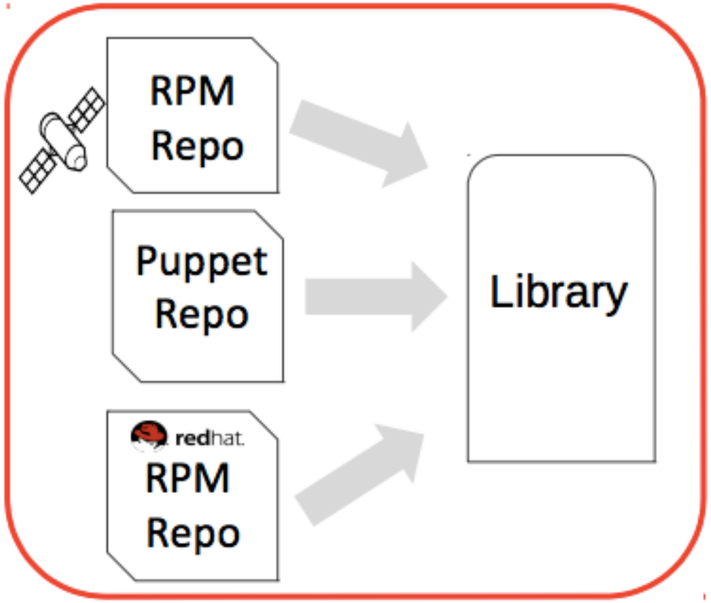


1. Model your Organizations, Environments & Development Lifecycle with promotion paths

T3 RHN Satellite v6: Workflow

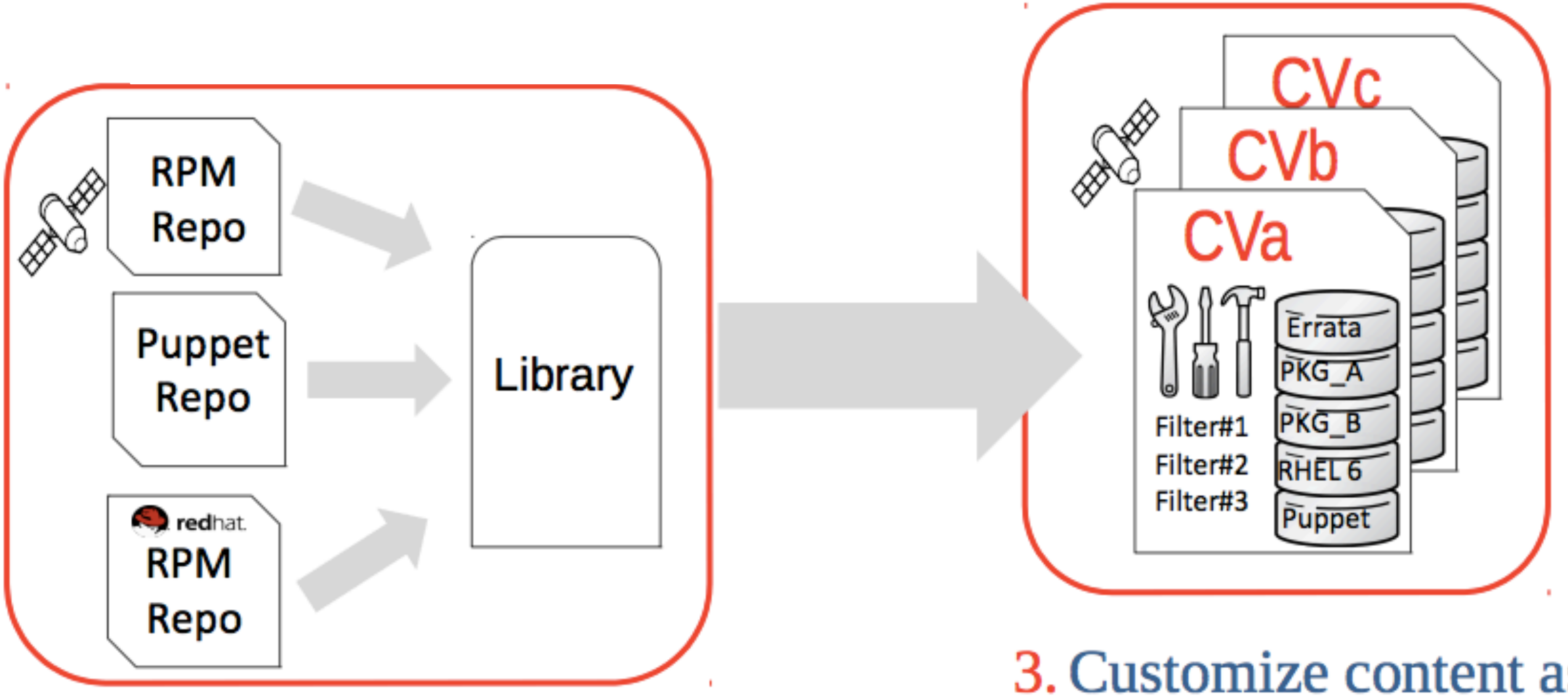


1. Model your Organizations, Environments & Development Lifecycle with promotion paths



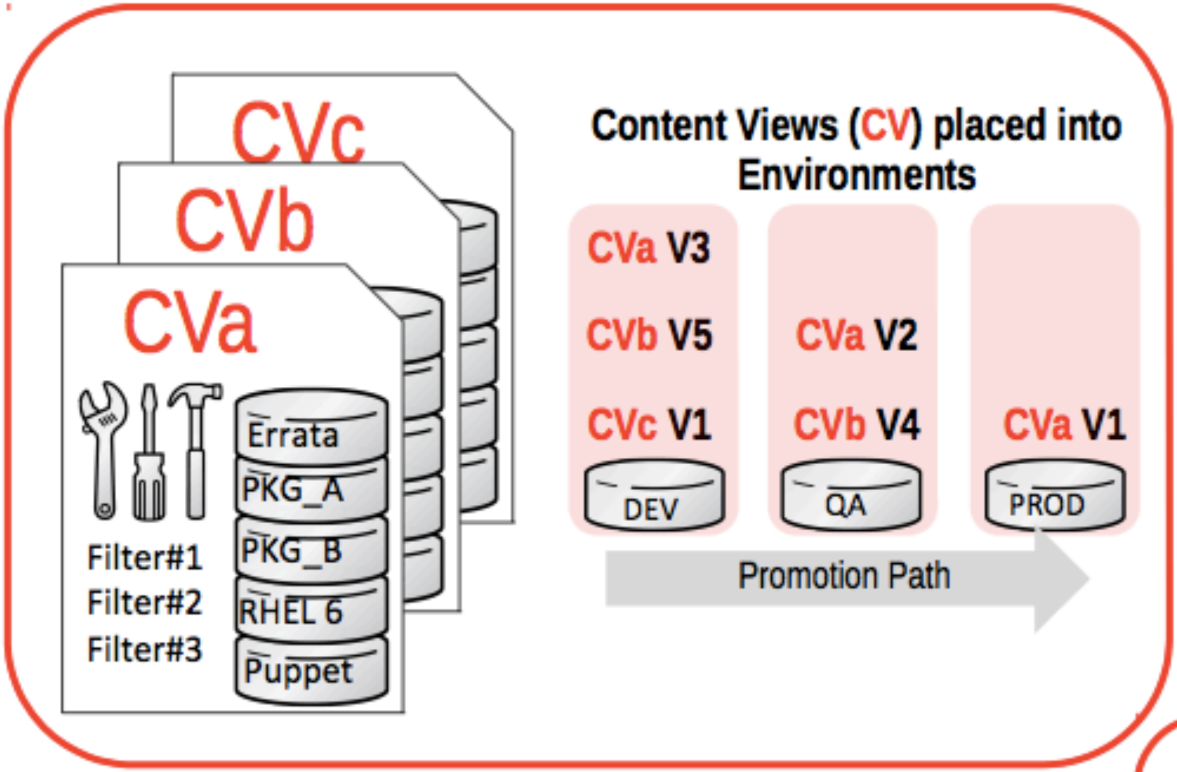
2. Sync content for your workloads

T3 RHN Satellite v6: Workflow

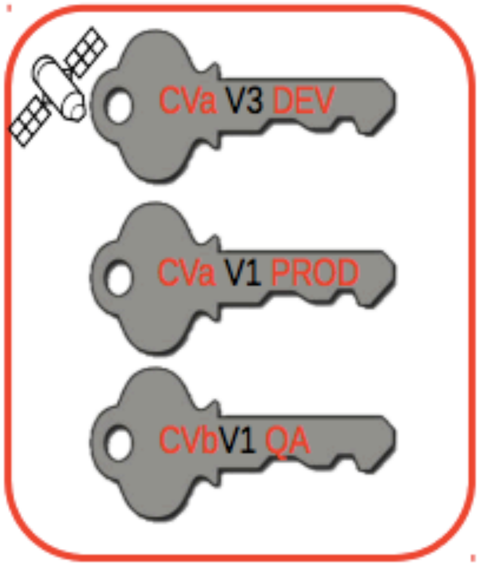


2. Sync content for your workloads

3. Customize content as standardized builds with Content Views (CV)



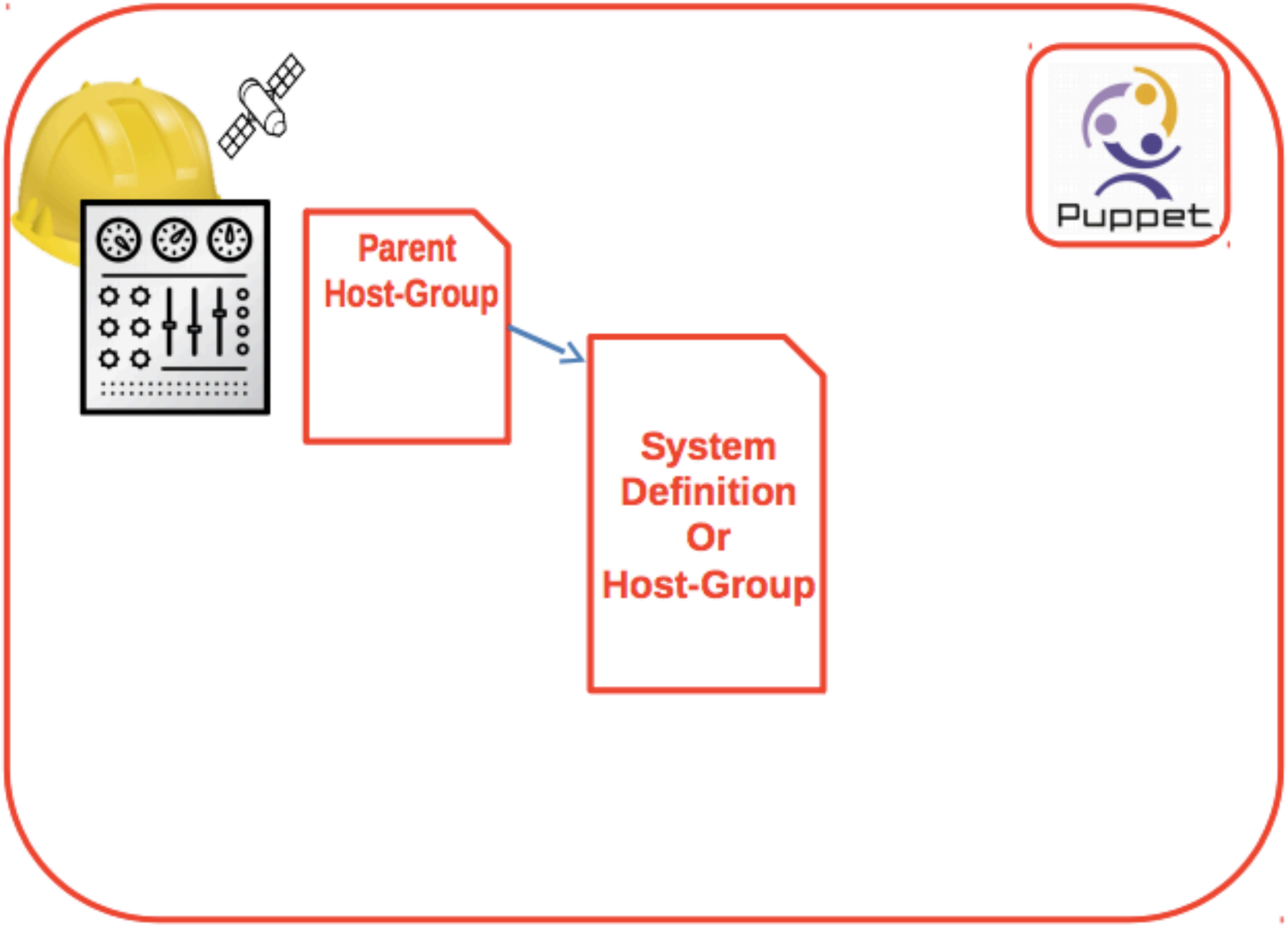
4. Begin promotion cycle by publishing Content Views into Environments. Refresh CV to rerun rules which increments the version



5. Generate activation keys for new system registration

6. Keys get handed off to Foreman for insertion into Kick Start

7. Create Host-Group or “System Definition” to fully specify workload

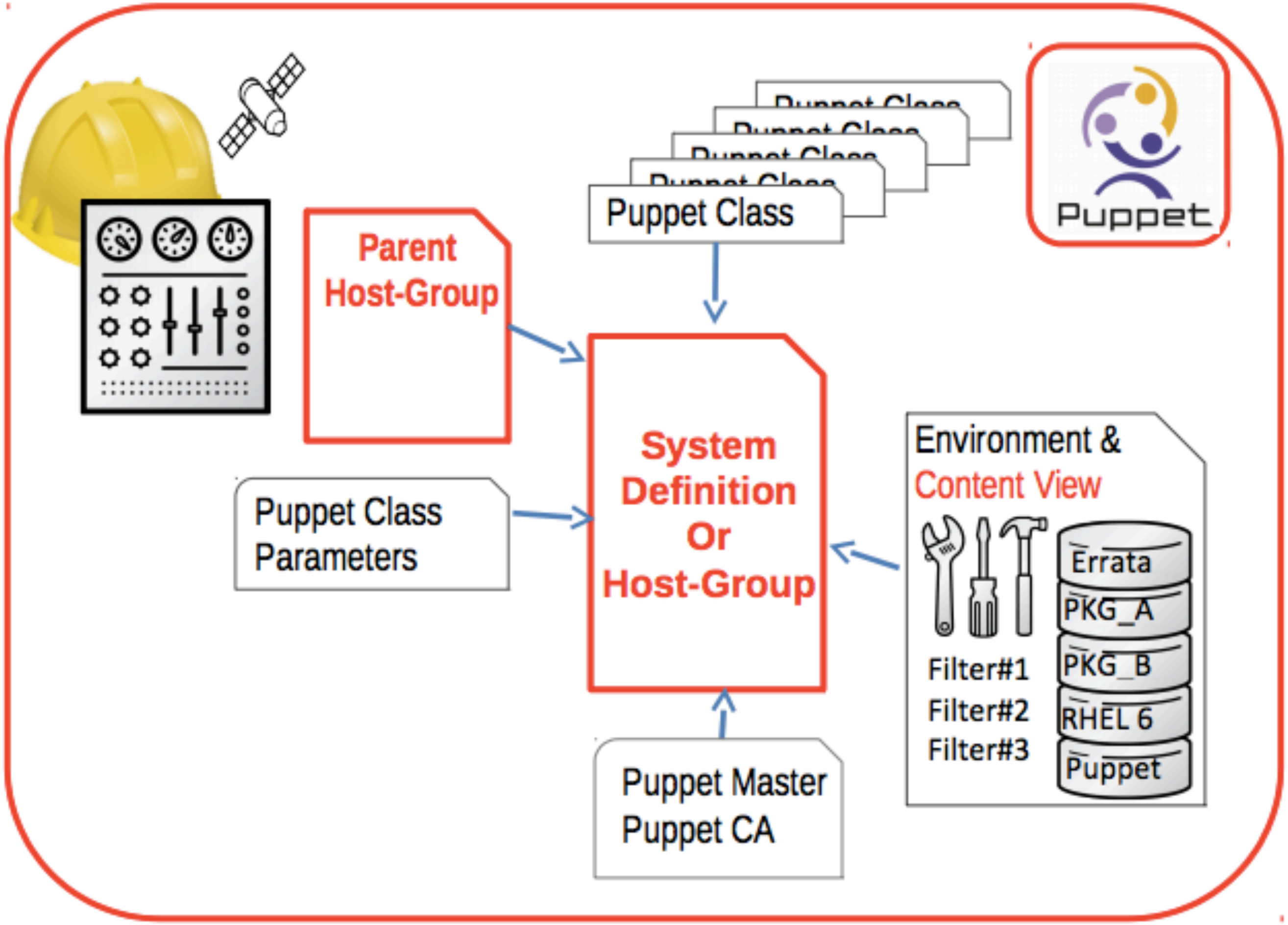


Parent Host-Group

System Definition Or Host-Group

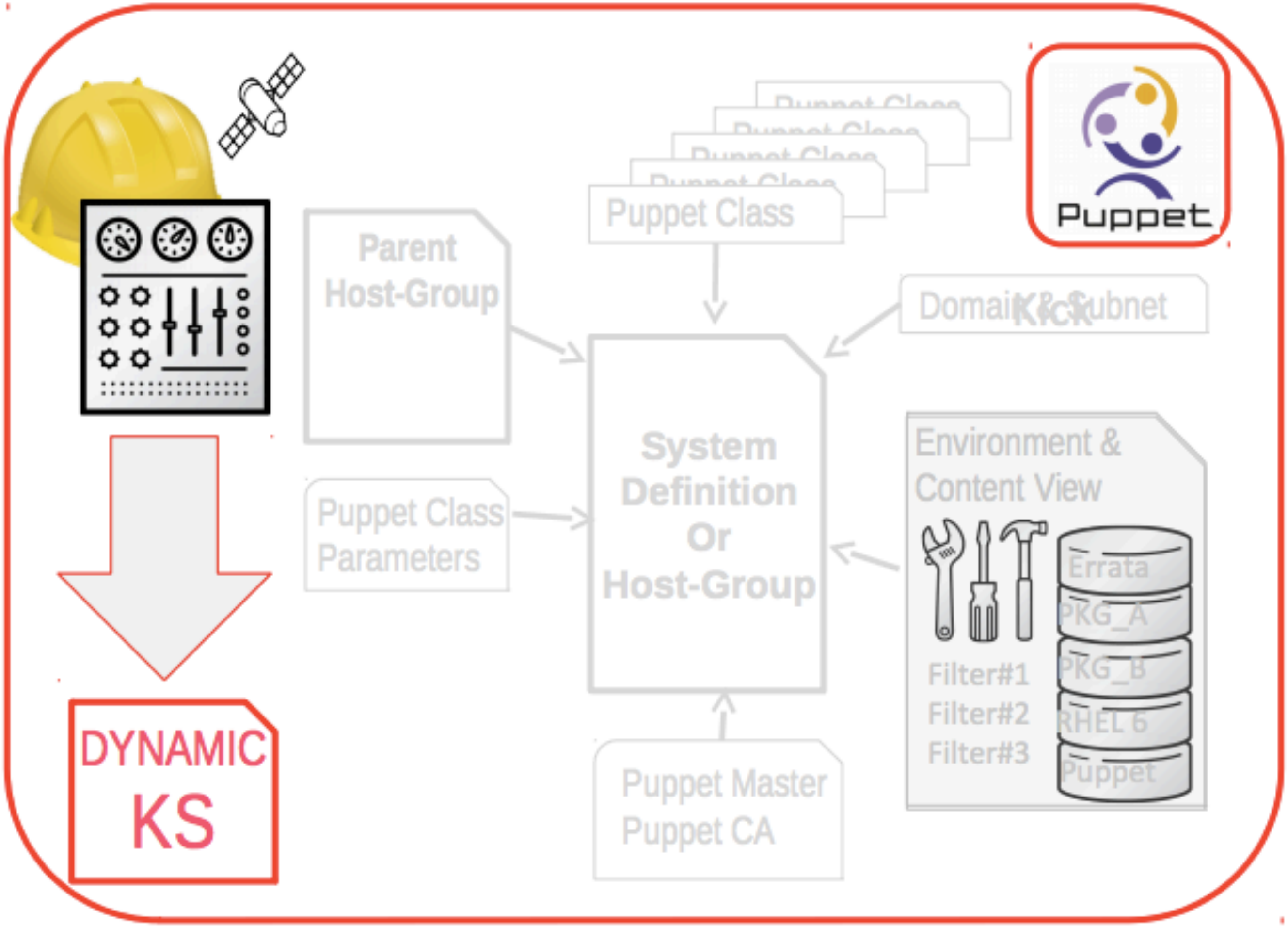
Host Groups can be stacked
e.g.
Apache stacked on RHEL 6.4

7. Create Host-Group or "System Definition" to fully specify workload



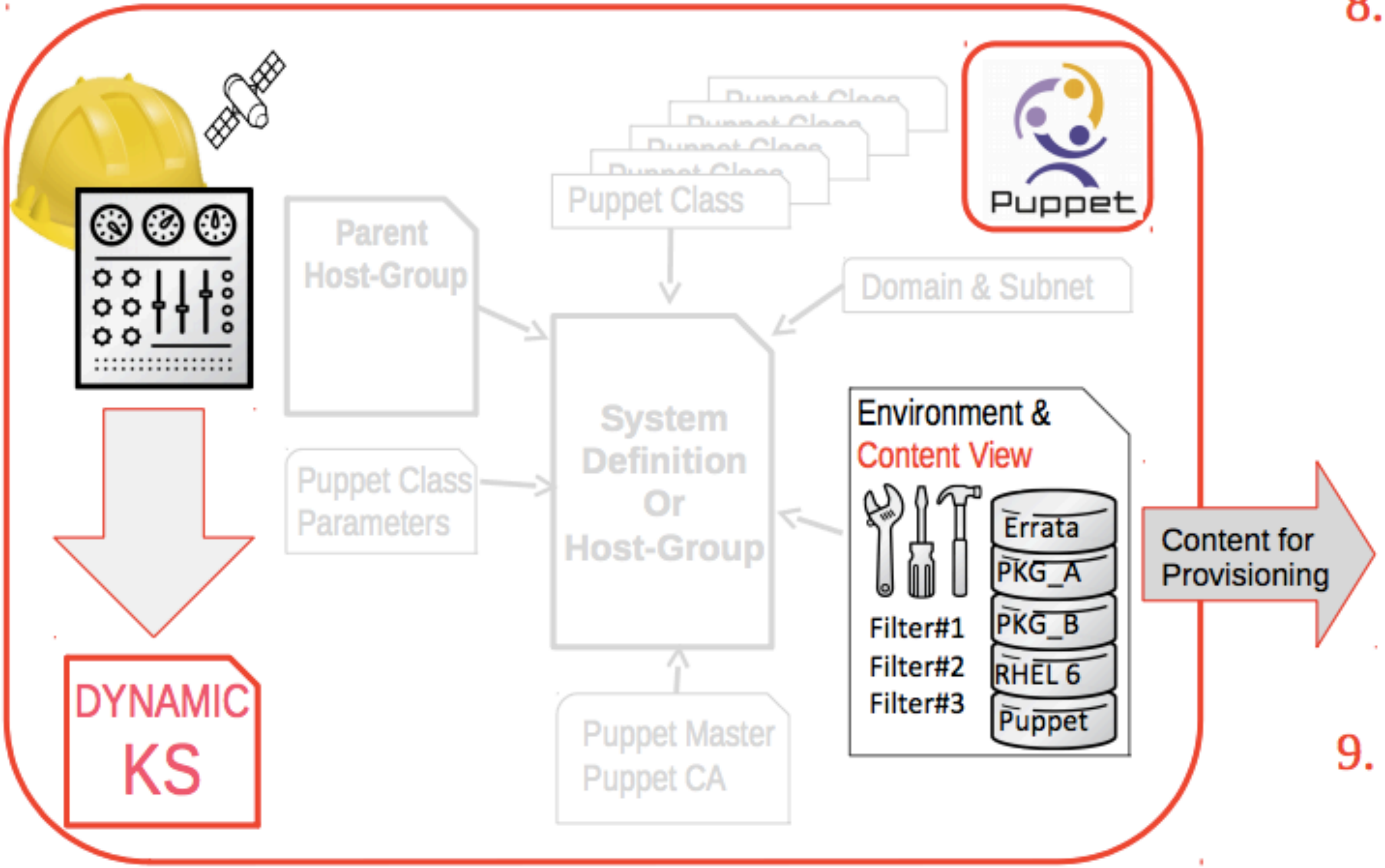
Add Puppet Classes & related artifacts

7. Create Host-Group or "System Definition" to fully specify workload

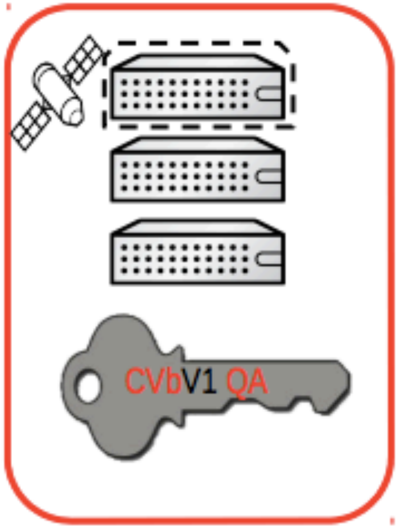


Satellite 6 creates the Kick Start file

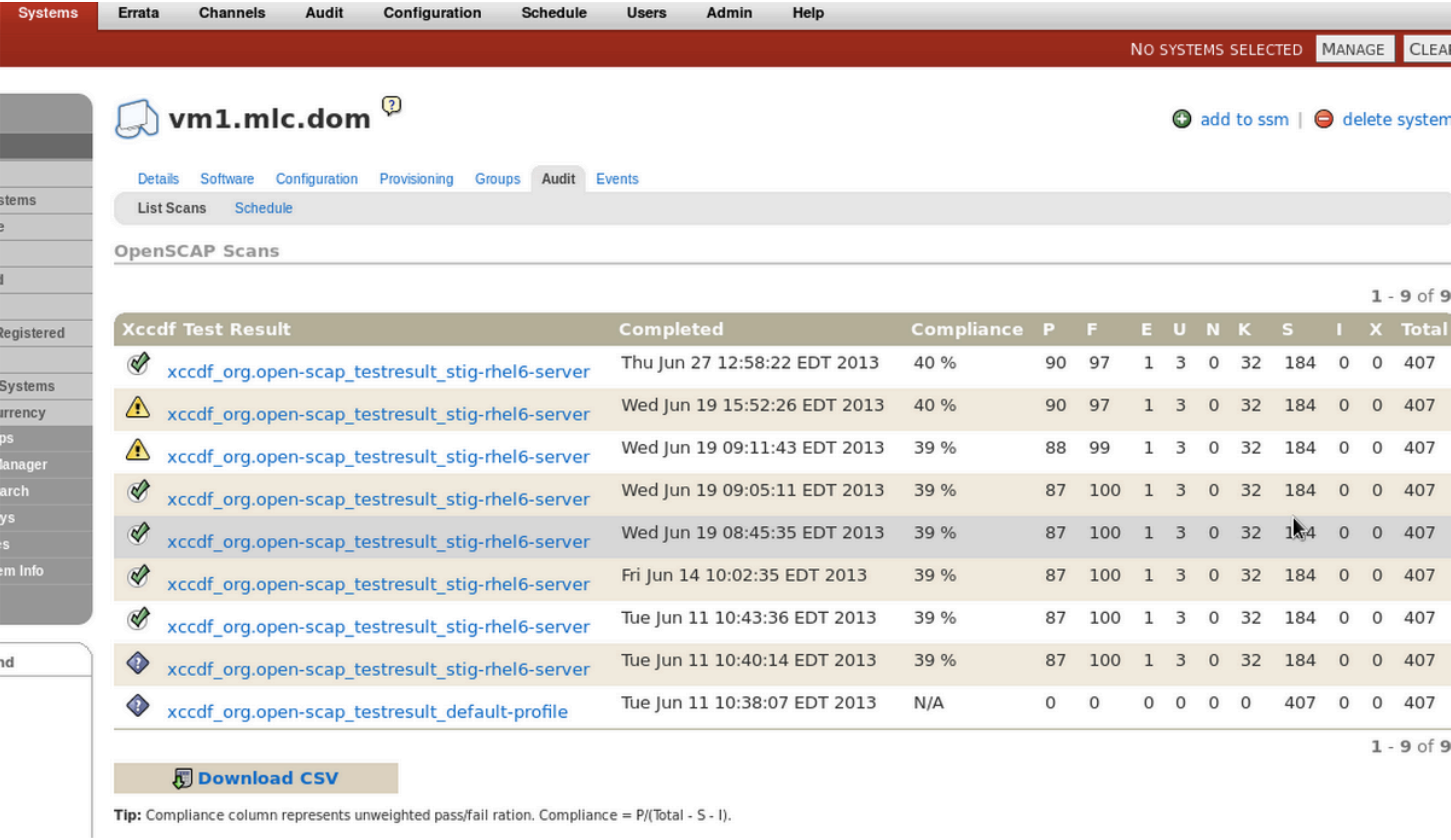
7. Create Host-Group or "System Definition" to fully specify workload



8. System build is automated with KS, PXE & Puppet configuration



9. Systems register back for updates



vm1.mlc.dom

OpenSCAP Scans

1 - 9 of 9

Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
✓ xccdf_org.open-scap_testresult_stig-rhel6-server	Thu Jun 27 12:58:22 EDT 2013	40 %	90	97	1	3	0	32	184	0	0	407
⚠ xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 15:52:26 EDT 2013	40 %	90	97	1	3	0	32	184	0	0	407
⚠ xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 09:11:43 EDT 2013	39 %	88	99	1	3	0	32	184	0	0	407
✓ xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 09:05:11 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
✓ xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 08:45:35 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
✓ xccdf_org.open-scap_testresult_stig-rhel6-server	Fri Jun 14 10:02:35 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
✓ xccdf_org.open-scap_testresult_stig-rhel6-server	Tue Jun 11 10:43:36 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
◆ xccdf_org.open-scap_testresult_stig-rhel6-server	Tue Jun 11 10:40:14 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
◆ xccdf_org.open-scap_testresult_default-profile	Tue Jun 11 10:38:07 EDT 2013	N/A	0	0	0	0	0	0	407	0	0	407

1 - 9 of 9

Download CSV

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

THANK YOU!