Compliance, Security Automation, and Remediation with Red Hat CloudForms, Red Hat Satellite, and Ansible Tower by Red Hat

RED HAT SUMMIT

Lucy Huh Kerner
Senior Cloud Solutions Architect
Red Hat U.S. Public Sector

Matt Micene
Solutions Architect
DLT Solutions

GOAL

- **Create a Security Compliant host at Provisioning time by 2 methods:**
  - Red Hat Satellite 6 + OpenSCAP
  - Red Hat CloudForms + Red Hat Satellite + Ansible Tower by Red Hat

- **Automate ongoing Security Remediation and Compliance with:**
  - Red Hat CloudForms + Red Hat Satellite + OpenSCAP
  - Red Hat CloudForms + Ansible Tower by Red Hat
  - Red Hat CloudForms Control/Policy Engine + Red Hat Insights

WHY AUTOMATE COMPLIANCE ?

Compliance, what's it good for?

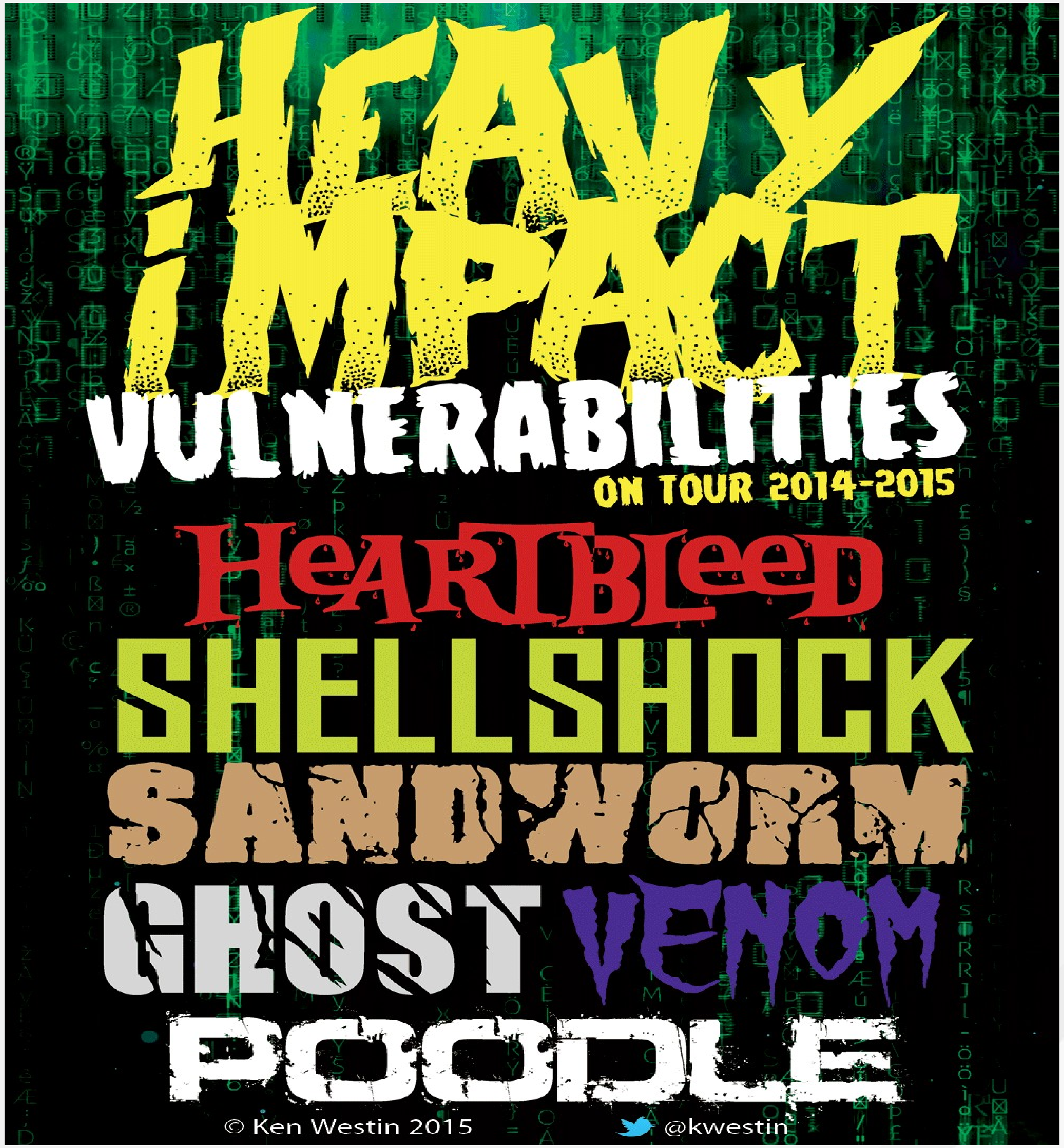
CA DOJ recommends CIS Critical Security Controls as “minimum level of information security” to meet standard of reasonableness

– California Breach Report https://oag.ca.gov/breachreport2016#findings

“Patch management and associated vulnerability management processes represent the biggest problem areas, because they’re rarely well documented and automated.”

– Anton Chuvakin [http://blogs.gartner.com/anton-chuvakin/2014/02/13/highlights-from-verizon-pci-report-2014/]

ZDNET TOLD ME OUR SERVERS HAVE POODLES
I'LL NEED YOU TO PATCH ALL THE BASHES
imgflip.com



Poster created by Ken Westin, 2015, used with permission of author. Hi Ken!

WHAT IS SCAP?

SCAP = Security Content Automation Protocol (latest is version 1.2), Specification: *NIST SP 800-126 Rev. 2*

- **CCE™:** Common Configuration Enumeration
- **CPE™:** Common Platform Enumeration
- **CVE®:** Common Vulnerabilities and Exposures
- **CVSS:** Common Vulnerability Scoring System
- **CCSS:** Common Configuration Scoring System
- **XCCDF:** The Extensible Configuration Checklist Description Format
- **OVAL®:** Open Vulnerability and Assessment Language
- **OCIL:** Open Checklist Interactive Language
- **AI:** Asset Identification
- **ARF:** Asset Reporting Format

WHAT IS OpenSCAP?

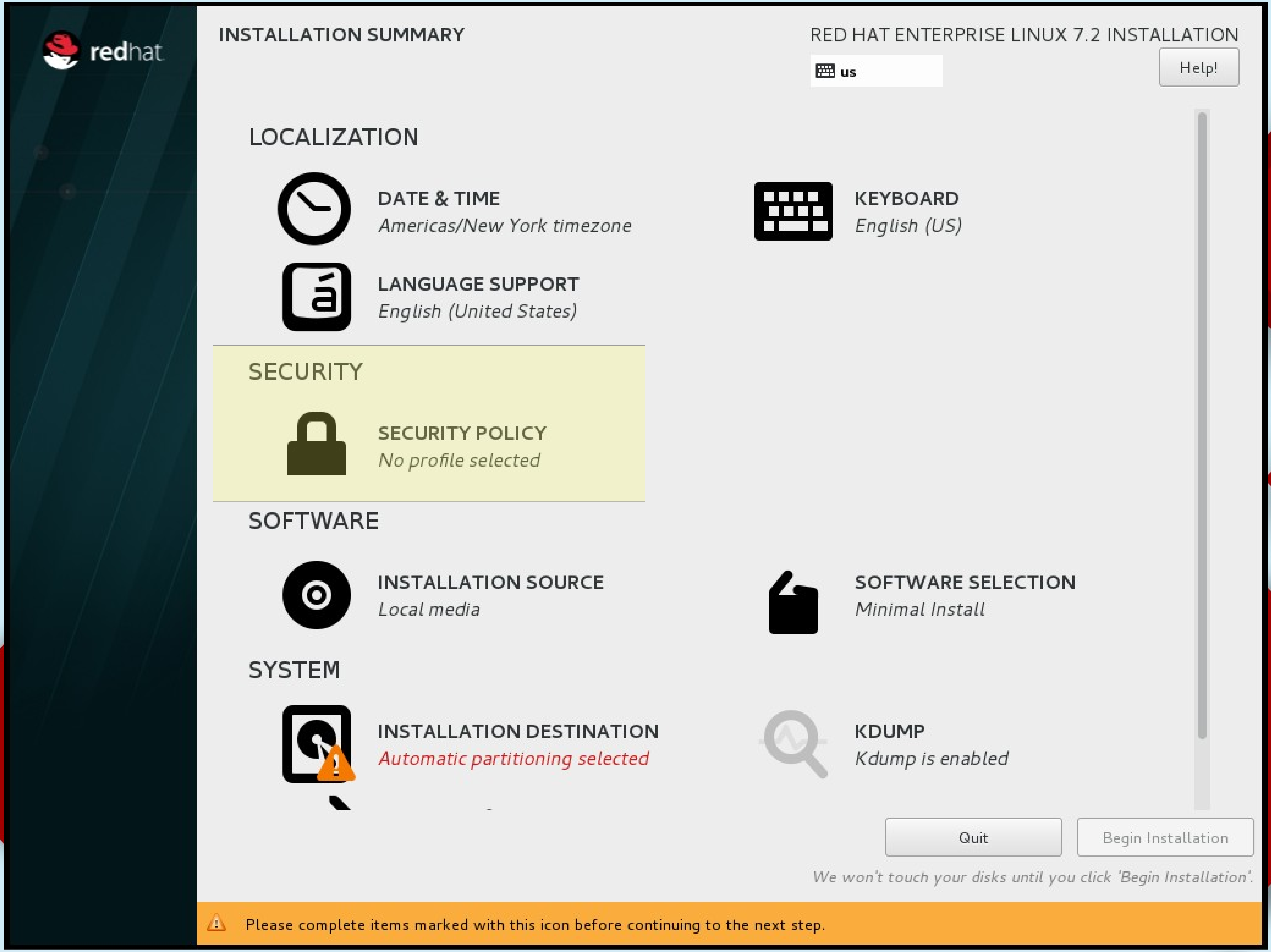
NIST **validated** SCAP scanner by Red Hat

redhat	OpenSCAP 1.0	- Authenticated Configuration Scanner - Common Vulnerabilities and Exposures (CVE)	- Red Hat Enterprise Linux 5.9 Desktop, (x86_64) - Red Hat Enterprise Linux 5.9 Desktop, (x86)	April 17, 2014

https://nvd.nist.gov/scapproducts.cfm

METHOD #1:
Create a Security Compliant host at Provisioning time with:
Red Hat Satellite 6 + OpenSCAP

Kickstarting SCAP



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION

LOCALIZATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY POLICY
No profile selected

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

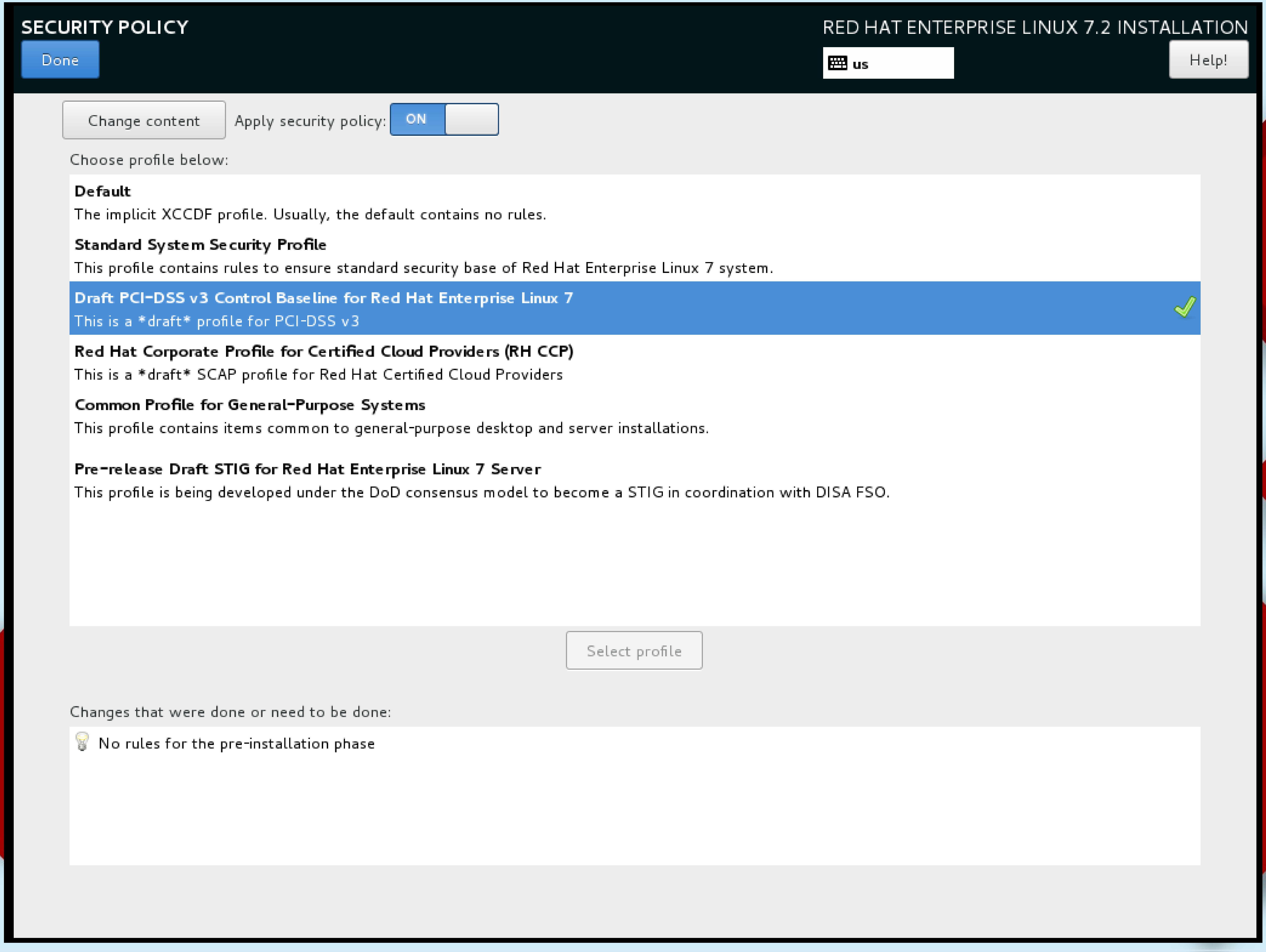
SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

KDUMP
Kdump is enabled

We won't touch your disks until you click 'Begin Installation'.

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



Apply security policy: ON

Choose profile below:

Default
The implicit XCCDF profile. Usually, the default contains no rules.

Standard System Security Profile
This profile contains rules to ensure standard security base of Red Hat Enterprise Linux 7 system.

Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7 ✓
This is a *draft* profile for PCI-DSS v3

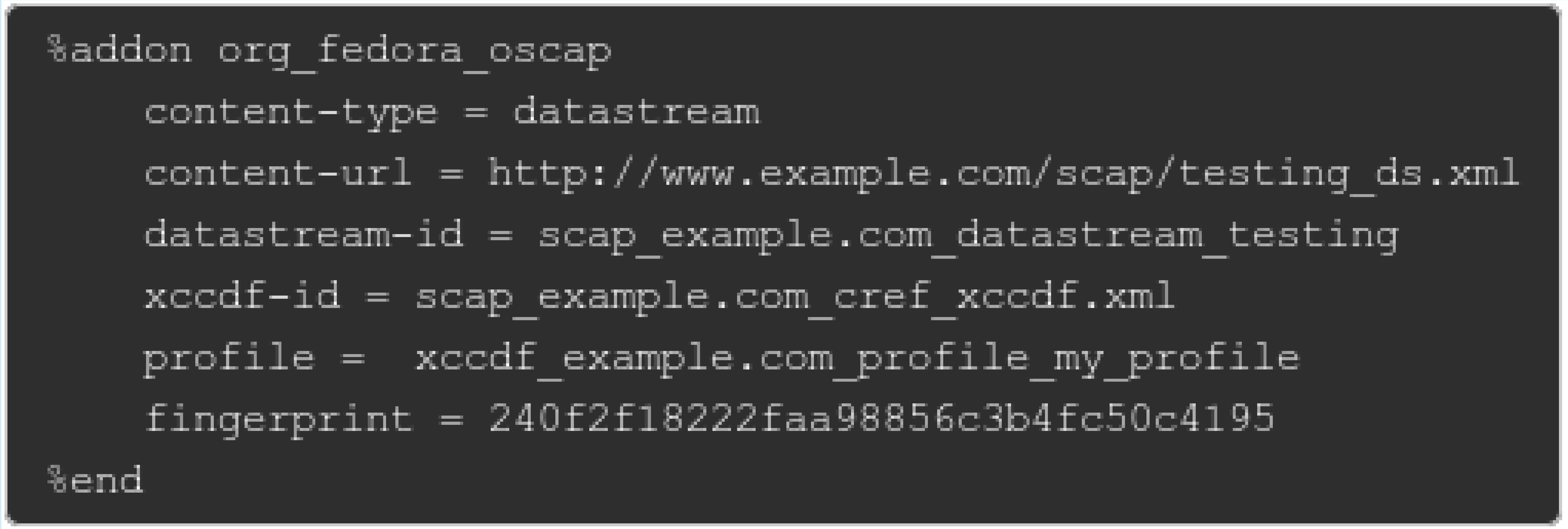
Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
This is a *draft* SCAP profile for Red Hat Certified Cloud Providers

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

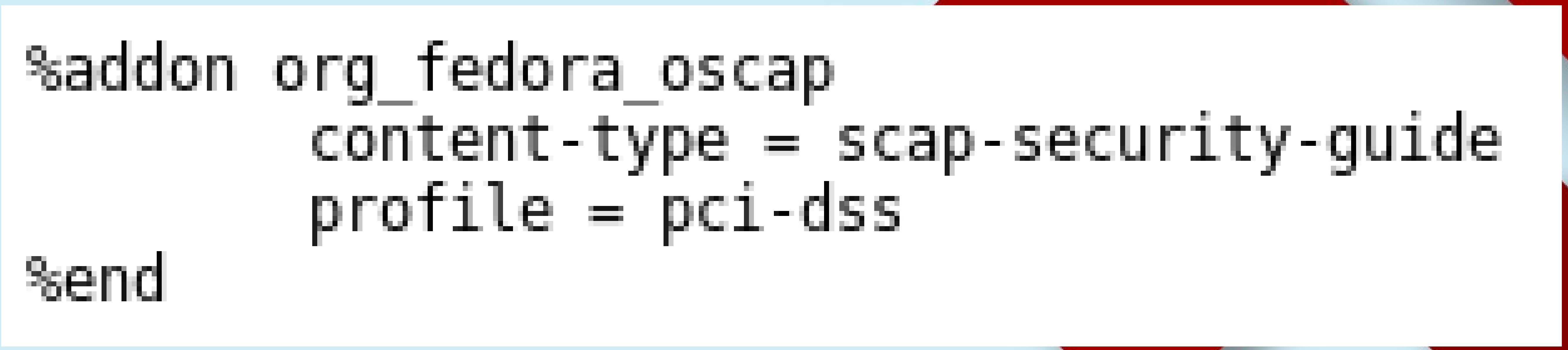
Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server
This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

Changes that were done or need to be done:

No rules for the pre-installation phase



```
%addon org_fedora_oscap
    content-type = datastream
    content-url = http://www.example.com/scap/testing_ds.xml
    datastream-id = scap_example.com_datastream_testing
    xccdf-id = scap_example.com_cref_xccdf.xml
    profile =  xccdf_example.com_profile_my_profile
    fingerprint = 240f2f18222faa98856c3b4fc50c4195
%end
```



```
%addon org_fedora_oscap
        content-type = scap-security-guide
        profile = pci-dss
%end
```

RED HAT SATELLITE
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights
Host Group
Puppet Classes
Network
Operating System
Parameters
Locations
Organizations
Activation Keys
Reset Puppet Enviror

New Host Group

Parent: RHEL 7 Base

Name *: PCI

Lifecycle Environment: DEV

Content View: RHEL7_base

Puppet Environment: KT_DLT_Solutions_development_rhel7_base_2

Capsule Settings

Content Source: sat6-local.lab.dlt.com — Use this as a source

Puppet CA: sat6-local.lab.dlt.com — Use this puppet serv

Puppet Master: sat6-local.lab.dlt.com — Use this puppet serv

New Host Group

Included Classes

- foreman_scap_client

Available Classes

Filter classes

+ access_insights_client

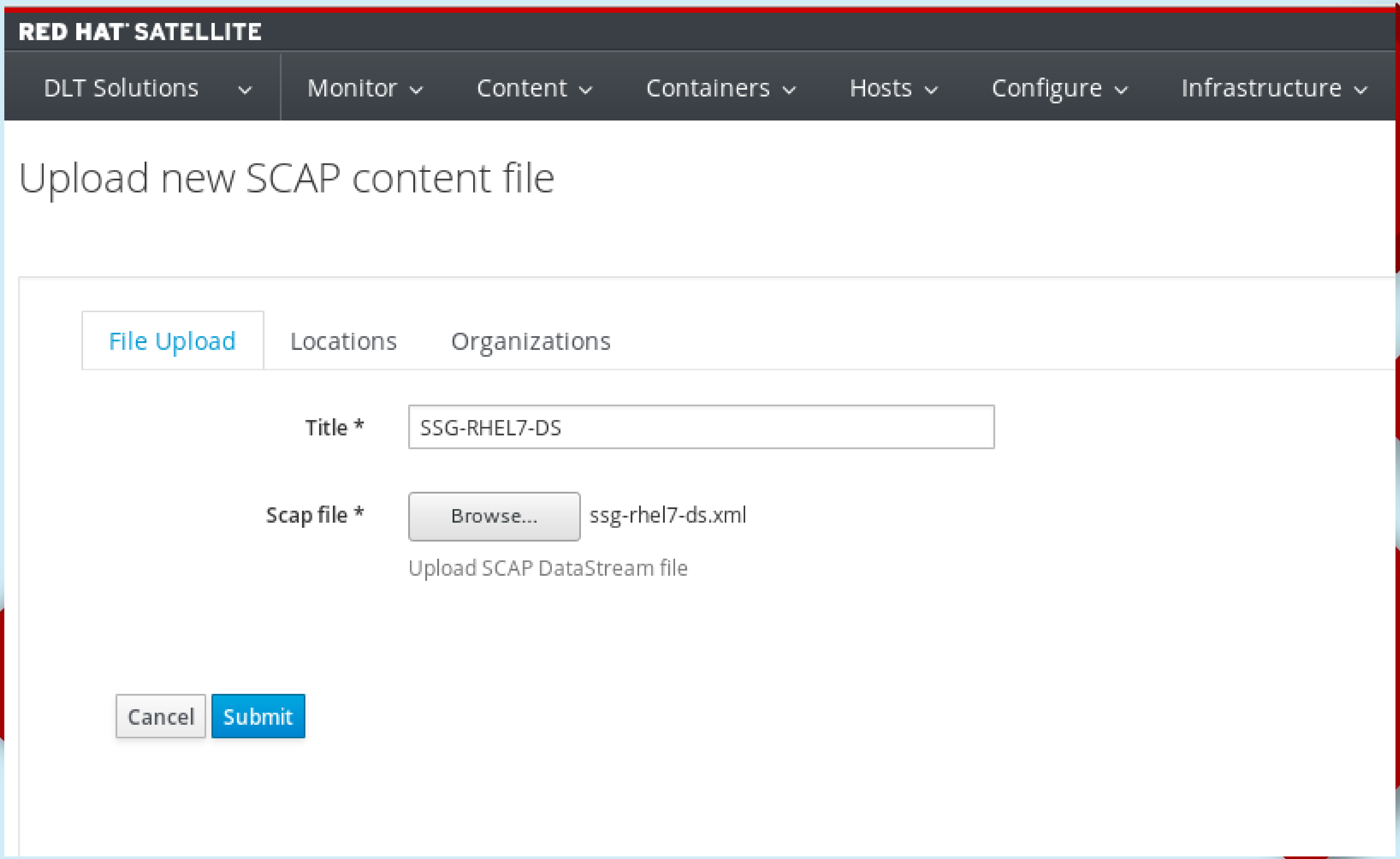
− foreman_scap_client

foreman_scap_client::params

+ stdlib

#redhat #rhsummit

Create new Scan policy



Upload new SCAP content file

Title * SSG-RHEL7-DS

Scap file * Browse... ssg-rhel7-ds.xml

Upload SCAP DataStream file

RED HAT SATELLITE
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights

New Compliance Policy

1 Create policy · 2 SCAP Content · 3 Schedule · 4 Locations · 5 Organizations · 6 Hostgroups

Name * SSG-PCI-RHEL7

Description

RED HAT SATELLITE
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights

New Compliance Policy

1 Create policy · 2 SCAP Content · 3 Schedule · 4 Locations · 5 Organizations · 6 Hostgroups

Scap content SSG-RHEL7-DS

XCCDF Profile PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7

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

RED HAT SATELLITE

DLT Solutions@HQ | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Red Hat Insights

New Compliance Policy

1 Create policy | 2 SCAP Content | 3 Schedule | 4 Locations | 5 Organizations | 6 Hostgroups

Period: Weekly

Weekday: Tuesday

RED HAT SATELLITE

DLT Solutions@HQ | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Red Hat Insights

New Compliance Policy

1 Create policy | 2 SCAP Content | 3 Schedule | 4 Locations | 5 Organizations | 6 Hostgroups

Locations

All items: Filter

Selected items: HQ

RED HAT SATELLITE
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights

New Compliance Policy

1 Create policy
2 SCAP Content
3 Schedule
4 Locations
5 Organizations
6 Hostgroups

Organizations

All items
Filter
Selected items

DLT Solutions

RED HAT SATELLITE
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights

New Compliance Policy

1 Create policy
2 SCAP Content
3 Schedule
4 Locations
5 Organizations
6 Hostgroups

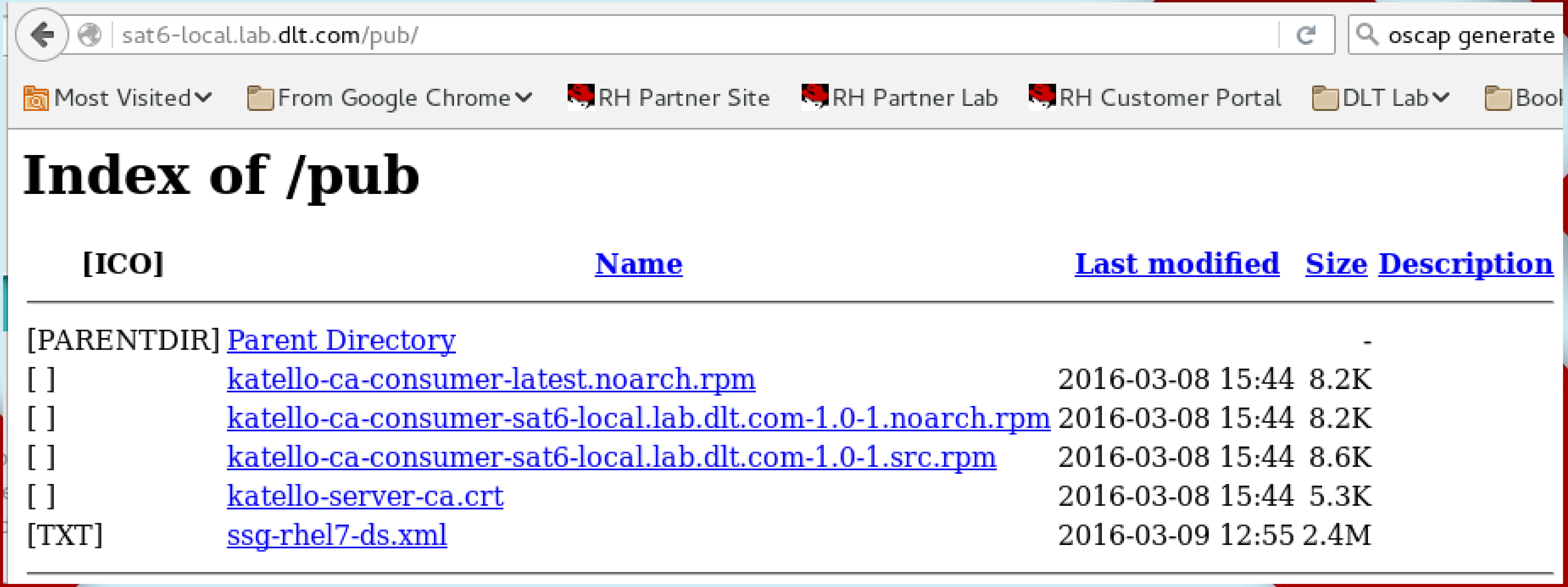
Hostgroups

All items
Filter
Selected items

RHEL 7 Base

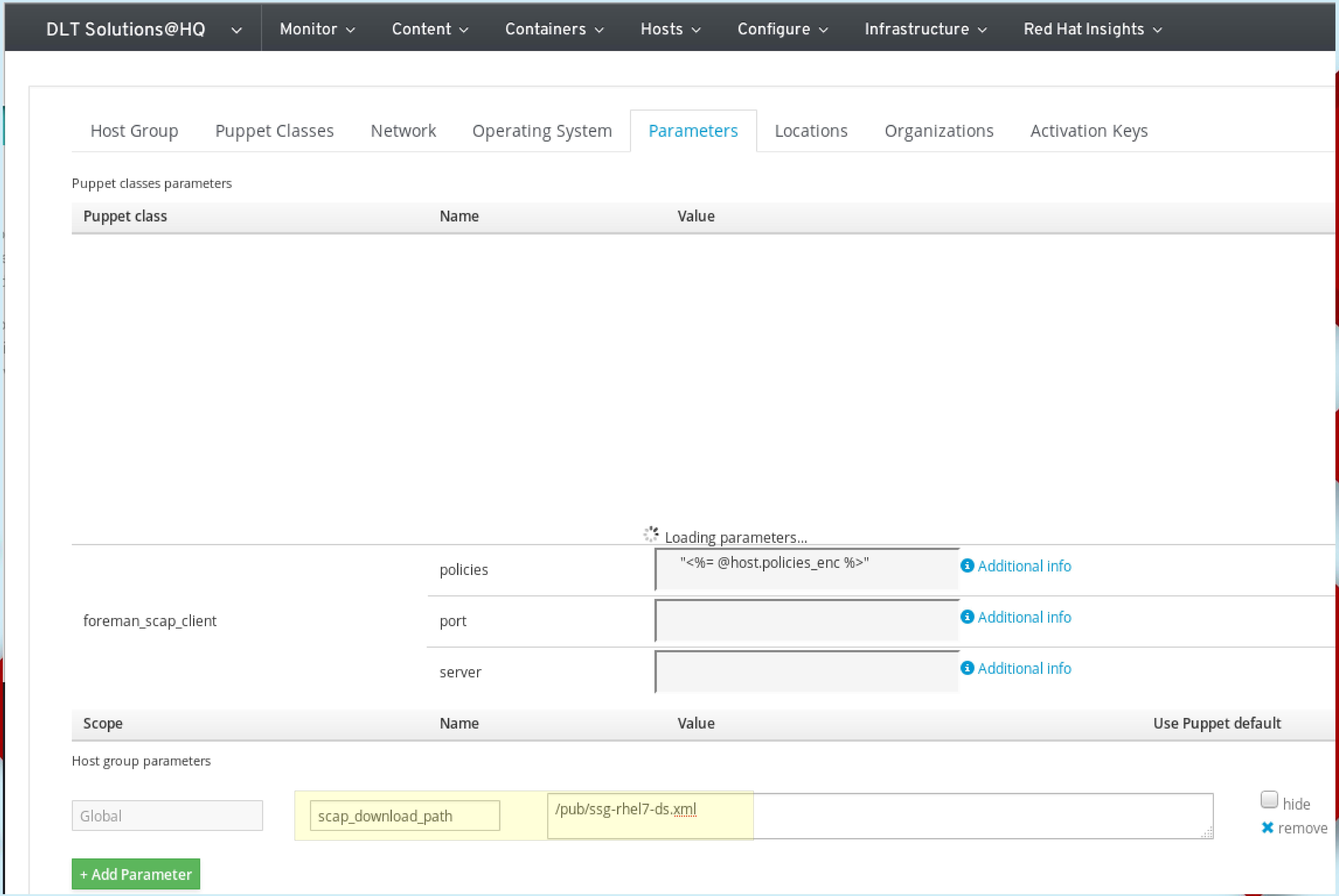
RHEL 7 Base/PCI

Update scan host group



Index of /pub

```
     [ICO]                        Name                              Last modified    Size Description
[PARENTDIR] Parent Directory                                                            -
[ ]         katello-ca-consumer-latest.noarch.rpm                   2016-03-08 15:44  8.2K
[ ]         katello-ca-consumer-sat6-local.lab.dlt.com-1.0-1.noarch.rpm 2016-03-08 15:44  8.2K
[ ]         katello-ca-consumer-sat6-local.lab.dlt.com-1.0-1.src.rpm    2016-03-08 15:44  8.6K
[ ]         katello-server-ca.crt                                   2016-03-08 15:44  5.3K
[TXT]       ssg-rhel7-ds.xml                                        2016-03-09 12:55 2.4M
```



Puppet classes parameters

Puppet class	Name	Value
foreman_scap_client	policies	"<%= @host.policies_enc %>"
	port	
	server	

Loading parameters...

Host group parameters

Scope	Name	Value	Use Puppet default
Global	scap_download_path	/pub/ssg-rhel7-ds.xml	□ hide ✖ remove

Create Kickstart templates

Provisioning Template
Type
Association
History
Locations
Organizations

Name * oscap_anaconda_addon

Note: Useful template functions and macros

Template editor

Code
Preview

```
<% if @host.policies_enc != '[]' %>
<%
  pol_array = @host.policies_enc.split(',')
  pol_hash = {}
  pol_array.each do |e|
    e.gsub! /"/, ''
    key_val = e.split(':')
    pol_hash[key_val[0]] = key_val[1]
  end
%>

%addon org_fedora_oscap
    content-type = datastream
    content-url = http://<%= @host.puppetmaster %><%= @host.params['scap_download_path'] %>
    profile = <%= pol_hash['profile_id'] %>
%end

<% end %>
```

Snippet ☑

Partition Tables

Name
AutoYaST entire SCSI disk
AutoYaST entire virtual disk
AutoYaST LVM
FreeBSD
Jumpstart default
Jumpstart mirrored
Junos default fake
Kickstart default
Preseed custom LVM
Preseed default

Name * PCI SCAP

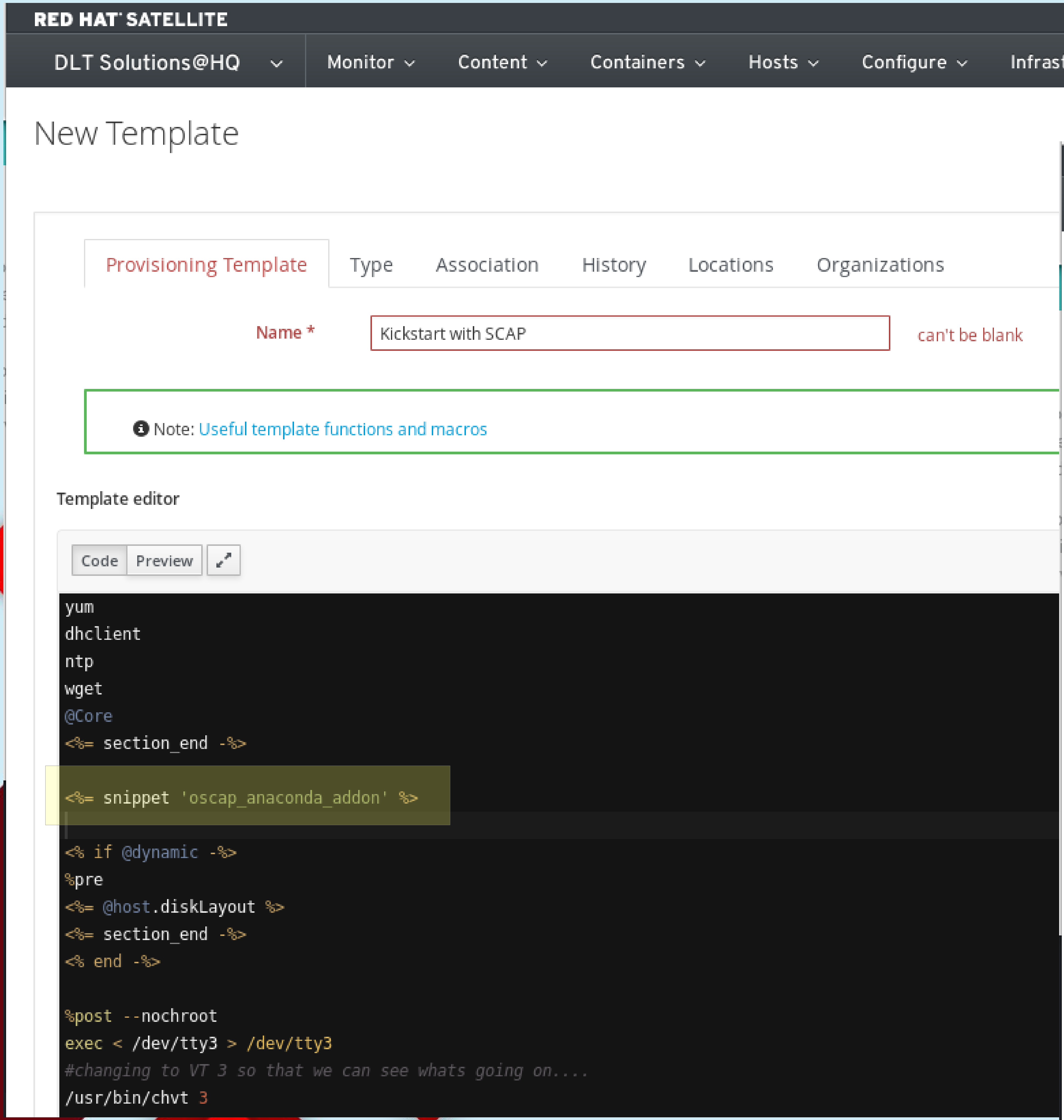
Layout *

```
# Create particular logical volumes (optional)
logvol / --fstype=xfs --name=LogVol06 --vgname=VolGroup --size=2048 --grow
# CCE-26557-9: Ensure /home Located On Separate Partition
logvol /home --fstype=xfs --name=LogVol02 --vgname=VolGroup --size=1024 --fsoptions="nodev"
# CCE-26435-8: Ensure /tmp Located On Separate Partition
logvol /tmp --fstype=xfs --name=LogVol01 --vgname=VolGroup --size=1024
--fsoptions="nodev,noexec,nosuid"
# CCE-26639-5: Ensure /var Located On Separate Partition
logvol /var --fstype=xfs --name=LogVol03 --vgname=VolGroup --size=1024 --fsoptions="nodev"
# CCE-26215-4: Ensure /var/log Located On Separate Partition
```

Notice you may use a script as well

Os family Red Hat

https://github.com/nzwulfin/rhsummit16-scap



New Template

Name * Kickstart with SCAP can't be blank

Note: Useful template functions and macros

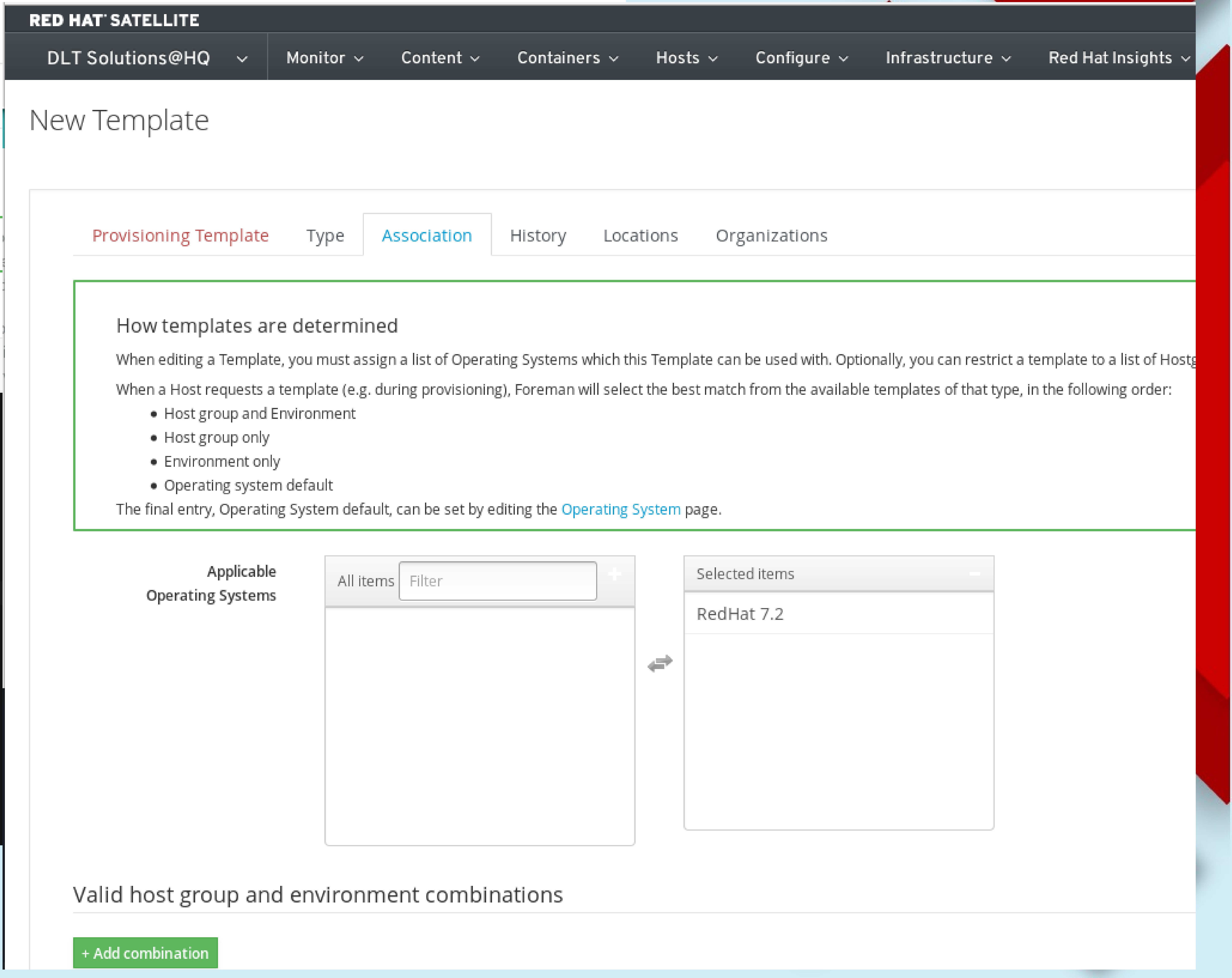
Template editor

```
yum
dhclient
ntp
wget
@Core
<%= section_end -%>

<%= snippet 'oscap_anaconda_addon' %>

<% if @dynamic -%>
%pre
<%= @host.diskLayout %>
<%= section_end -%>
<% end -%>

%post --nochroot
exec < /dev/tty3 > /dev/tty3
#changing to VT 3 so that we can see whats going on....
/usr/bin/chvt 3
```



New Template

How templates are determined

When editing a Template, you must assign a list of Operating Systems which this Template can be used with. Optionally, you can restrict a template to a list of Hostg

When a Host requests a template (e.g. during provisioning), Foreman will select the best match from the available templates of that type, in the following order:

- Host group and Environment
- Host group only
- Environment only
- Operating system default

The final entry, Operating System default, can be set by editing the Operating System page.

Applicable Operating Systems

RedHat 7.2

Valid host group and environment combinations

RED HAT SATELLITE
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights
Filter ...
Search
Title
Operating System
Partition table
Installation media
Templates
Parameters

Operating systems

RedHat 7.2

PXELinux * Kickstart default PXELinux

iPXE * Kickstart default iPXE

provision * Kickstart with SCAP

finish * Satellite Kickstart Default Finish

user_data * Satellite Kickstart Default User Data

RED HAT SATELLITE
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infra
Filter ...
Search
Title
Operating System
Partition table
Installation media

Operating systems

RedHat 7.2

Partition tables

☑ Select All

☑ Kickstart default

☑ PCI SCAP

Put it together in a new host

New Host

Host
Puppet Classes
Network
Operating System
Parameters
Additional Information

Name *	pci-test
Organization *	DLT Solutions
Location *	HQ
Host Group	RHEL 7 Base/PCI
Deploy on	Bare Metal
Lifecycle Environment	DEV
Content View	RHEL7_base
Puppet Environment *	KT_DLT_Solutions_development_rhel7_base_2

New Host

Host
Puppet Classes
Network
Operating System
Parameters
Additional Information

Included Classes

foreman_scap_client

Available Classes

Filter classes

+ access_insights_client
+ foreman_scap_client

#redhat #rhsummit

New Host

Host
Puppet Classes
Network
Operating System
Parameters
Additional Information

Architecture * x86_64

Operating system * RedHat 7.2

Build mode ☑

Enable this host for provisioning

Media * DLT_Solutions/Library/Red_Hat_Server/Red_Hat_Enterprise_Lint

Partition table * PCI SCAP

Custom partition table

What ever text(or ERB template) you use in here, would be used as you
delete all of the text from this field

Root password *

Provisioning templates

Resolve

Display the templates that will be used to provision this host

New Host

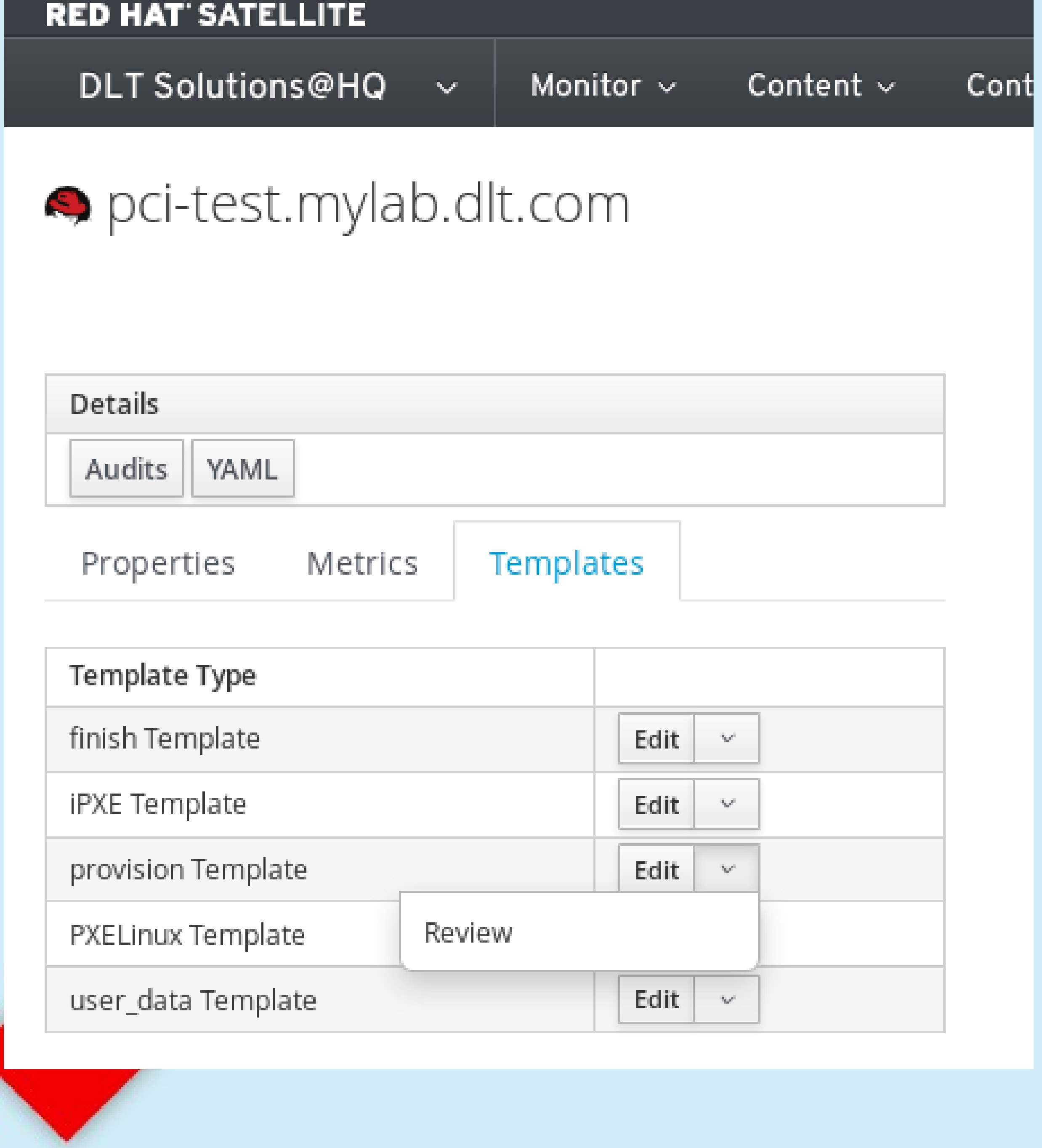
Puppet classes Parameters

Puppet class	Name	Value		Actions
foreman_scap_client	policies	"<%= @host.policies_enc %>"	Additional info	override
	port	9090	Additional info	override
	server	sat6-local.lab.dlt.com	Additional info	override

Included Parameters via inheritance

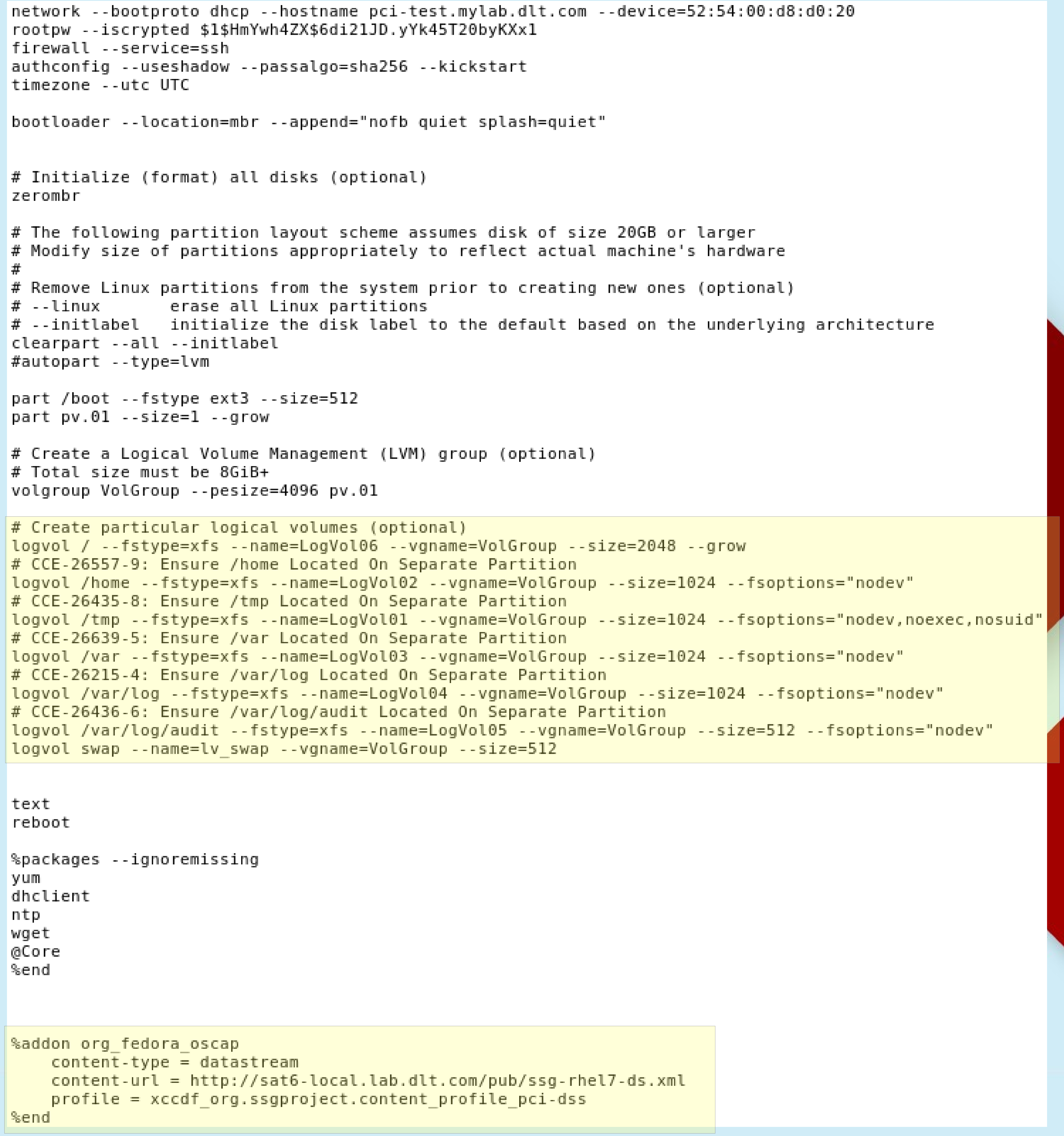
Scope	Name	Value		Use Puppet default	Actions
Global	kt_activation_keys	RHEL 7 Baseline	Additional info	override	
	scap_download_path	/pub/ssg-rhel7-ds.xml	Additional info	override	

Host Parameters



pci-test.mylab.dlt.com

Template Type	
finish Template	Edit
iPXE Template	Edit
provision Template	Edit
PXELinux Template	Review
user_data Template	Edit



```
network --bootproto dhcp --hostname pci-test.mylab.dlt.com --device=52:54:00:d8:d0:20
rootpw --iscrypted $1$HmYwh4ZX$6di21JD.yYk45T20byKXx1
firewall --service=ssh
authconfig --useshadow --passalgo=sha256 --kickstart
timezone --utc UTC

bootloader --location=mbr --append="nofb quiet splash=quiet"


# Initialize (format) all disks (optional)
zerombr

# The following partition layout scheme assumes disk of size 20GB or larger
# Modify size of partitions appropriately to reflect actual machine's hardware
#
# Remove Linux partitions from the system prior to creating new ones (optional)
# --linux       erase all Linux partitions
# --initlabel   initialize the disk label to the default based on the underlying architecture
clearpart --all --initlabel
#autopart --type=lvm

part /boot --fstype ext3 --size=512
part pv.01 --size=1 --grow

# Create a Logical Volume Management (LVM) group (optional)
# Total size must be 8GiB+
volgroup VolGroup --pesize=4096 pv.01

# Create particular logical volumes (optional)
logvol / --fstype=xfs --name=LogVol06 --vgname=VolGroup --size=2048 --grow
# CCE-26557-9: Ensure /home Located On Separate Partition
logvol /home --fstype=xfs --name=LogVol02 --vgname=VolGroup --size=1024 --fsoptions="nodev"
# CCE-26435-8: Ensure /tmp Located On Separate Partition
logvol /tmp --fstype=xfs --name=LogVol01 --vgname=VolGroup --size=1024 --fsoptions="nodev,noexec,nosuid"
# CCE-26639-5: Ensure /var Located On Separate Partition
logvol /var --fstype=xfs --name=LogVol03 --vgname=VolGroup --size=1024 --fsoptions="nodev"
# CCE-26215-4: Ensure /var/log Located On Separate Partition
logvol /var/log --fstype=xfs --name=LogVol04 --vgname=VolGroup --size=1024 --fsoptions="nodev"
# CCE-26436-6: Ensure /var/log/audit Located On Separate Partition
logvol /var/log/audit --fstype=xfs --name=LogVol05 --vgname=VolGroup --size=512 --fsoptions="nodev"
logvol swap --name=lv_swap --vgname=VolGroup --size=512


text
reboot

%packages --ignoremissing
yum
dhclient
ntp
wget
@Core
%end



%addon org_fedora_oscap
    content-type = datastream
    content-url = http://sat6-local.lab.dlt.com/pub/ssg-rhel7-ds.xml
    profile = xccdf_org.ssgproject.content_profile_pci-dss
%end
```

RED HAT SATELLITE
Red Hat Access
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights

Compliance Reports

Filter ...
Search

Host	Date	Passed	Failed	Other	
O pci-test.mylab.dlt.com	about 20 hours ago	51	41	2	View Report

Displaying **1** entry

RED HAT SATELLITE
Red Hat Access
Admin User
DLT Solutions@HQ
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Red Hat Insights
Administer

Compliance and Scoring

The target system did not satisfy the conditions of 41 rules! Please review rule results and consider applying remediation.

Rule results

51 passed | 41 failed | 2

Severity of failed rules

32 low | 9 medium

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	60.734955	100.000000	60.73%

Rule Overview

- ☑ pass
- ☑ fixed
- ☑ informational
- ☑ fail
- ☑ error
- ☑ unknown
- ☑ notchecked
- □ notselected
- ☑ notapplicable

Title	Severity	Result
▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 7 41x fail 2x notchecked		

METHOD #2:
Create a Security Compliant host at Provisioning time with:
Red Hat CloudForms + Red Hat Satellite + Ansible Tower

WHAT IS CLOUDFORMS?

RED HAT® CLOUDFORMS

Unified management

Complete self-service

Operational visibility

Compliance and governance

CONTAINERS

OpenShift by Red Hat | Kubernetes

VIRTUALIZATION

VMware

Microsoft Hyper-V

Red Hat Enterprise Virtualization

PRIVATE CLOUD

OpenStack

Red Hat Enterprise Linux OpenStack Platform

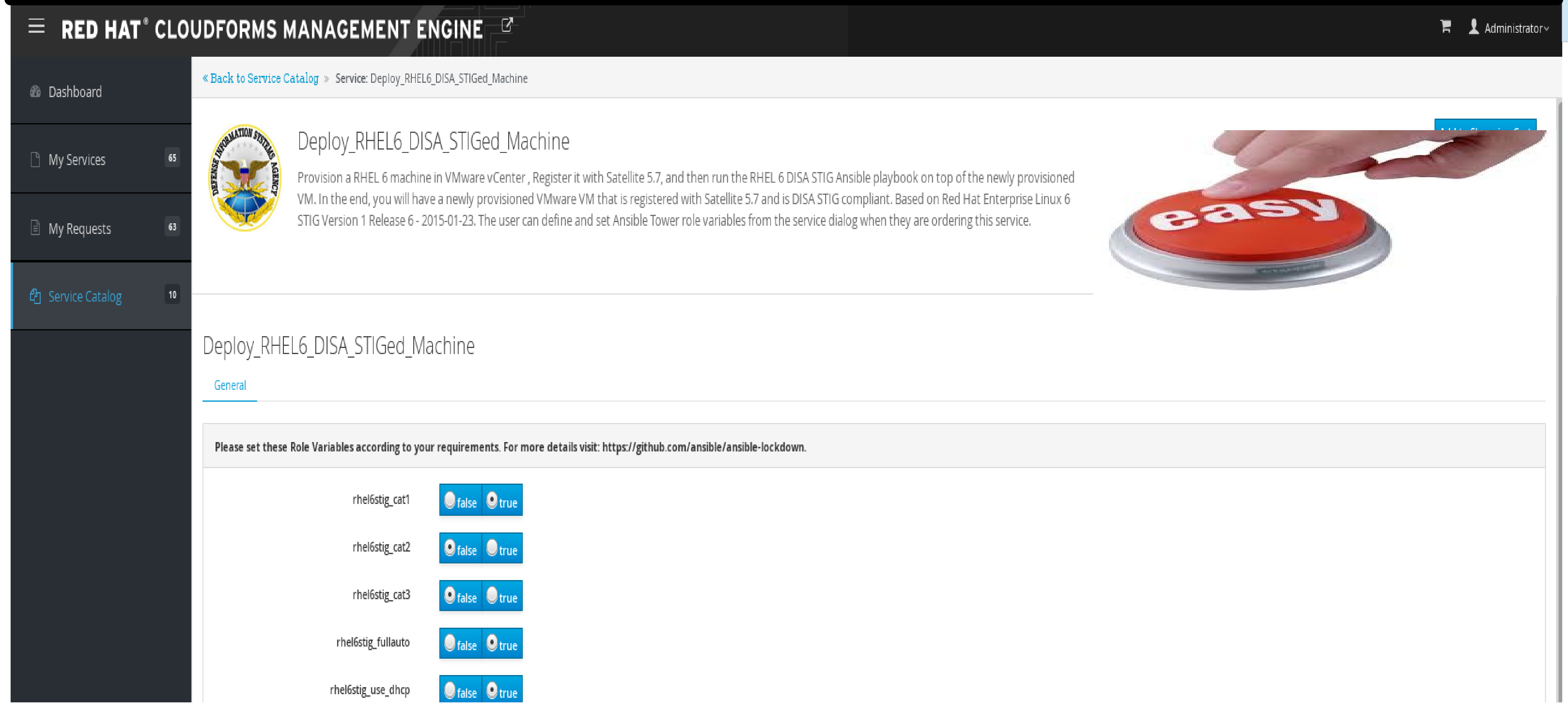
PUBLIC CLOUD

Amazon Web Services

Windows Azure

Creating a Security Compliant host at Provisioning time with:
Red Hat CloudForms + Red Hat Satellite + Ansible Tower

RED HAT® CLOUDFORMS



RED HAT® CLOUDFORMS MANAGEMENT ENGINE

Administrator

- Dashboard
- My Services 65
- My Requests 63
- Service Catalog 10

« Back to Service Catalog » Service: Deploy_RHEL6_DISA_STIGed_Machine

Deploy_RHEL6_DISA_STIGed_Machine

Provision a RHEL 6 machine in VMware vCenter , Register it with Satellite 5.7, and then run the RHEL 6 DISA STIG Ansible playbook on top of the newly provisioned VM. In the end, you will have a newly provisioned VMware VM that is registered with Satellite 5.7 and is DISA STIG compliant. Based on Red Hat Enterprise Linux 6 STIG Version 1 Release 6 - 2015-01-23. The user can define and set Ansible Tower role variables from the service dialog when they are ordering this service.

Deploy_RHEL6_DISA_STIGed_Machine

General

Please set these Role Variables according to your requirements. For more details visit: https://github.com/ansible/ansible-lockdown.

rhel6stig_cat1 ○ false ● true

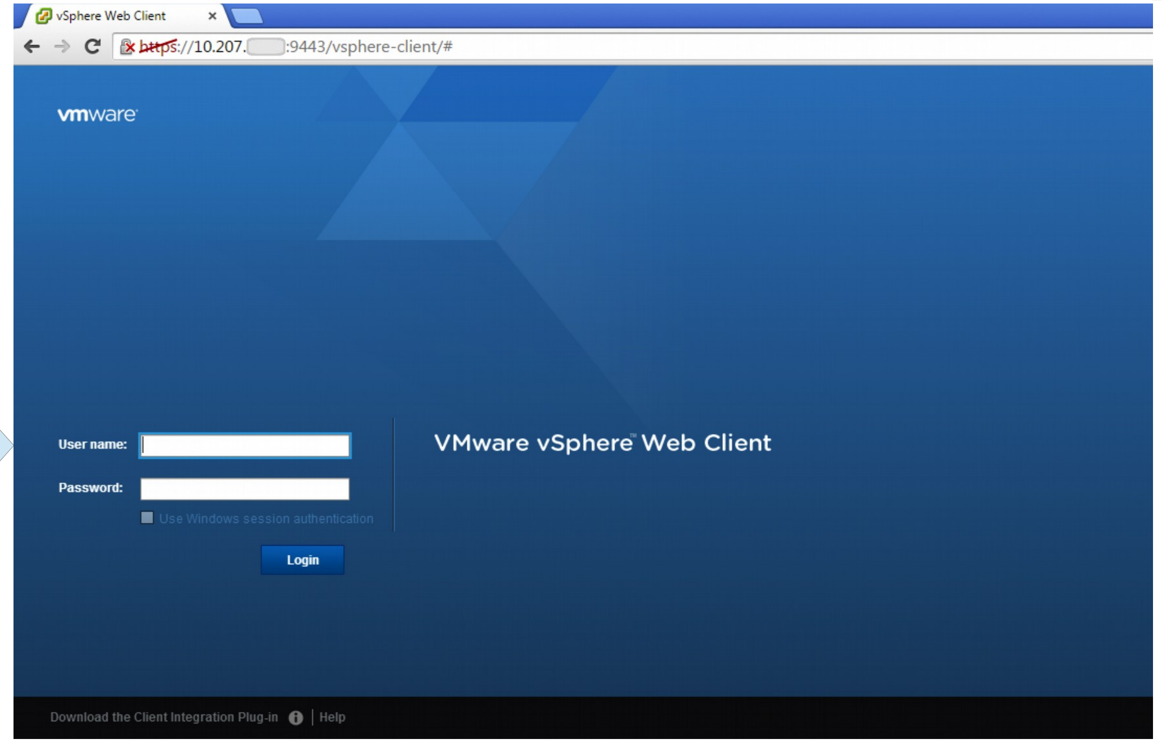
rhel6stig_cat2 ● false ○ true

rhel6stig_cat3 ● false ○ true

rhel6stig_fullauto ○ false ● true

rhel6stig_use_dhcp ○ false ● true

Lauch the CloudForms Provisioning State Machine



vSphere Web Client

~~https~~://10.207.[redacted]:9443/vsphere-client/#

vmware

User name:

Password:

□ Use Windows session authentication

Login

VMware vSphere™ Web Client

Download the Client Integration Plug-in | Help

Post Provisioning Steps

ANSIBLE TOWER by Red Hat®

ANSIBLE PLAYBOOK

RED HAT® SATELLITE

ANSIBLE PLAYBOOK

Defense Information Systems Agency Secure Technical Implementation Guide (DISA STIG)

Center for Internet Security®

CIS Security Benchmarks

DEMO

Automating ongoing Security Remediation and Compliance with:

Red Hat CloudForms + Red Hat Satellite + OpenSCAP

Red Hat CloudForms + Ansible Tower by Red Hat

Red Hat CloudForms Control/Policy Engine + Red Hat Insights

Automated security scanning and remediation with Red Hat Satellite 5.7 + OpenSCAP + Red Hat CloudForms

RED HAT® CLOUDFORMS
XML-RPC
RED HAT® SATELLITE
OpenSCAP
SCAN RESULTS: PASS/FAIL
REMEDIATE
IF SCAN FAILS
REST API
servicenow
E-MAIL
VM

XCCDF XML FILE with list of security checks by Profile id

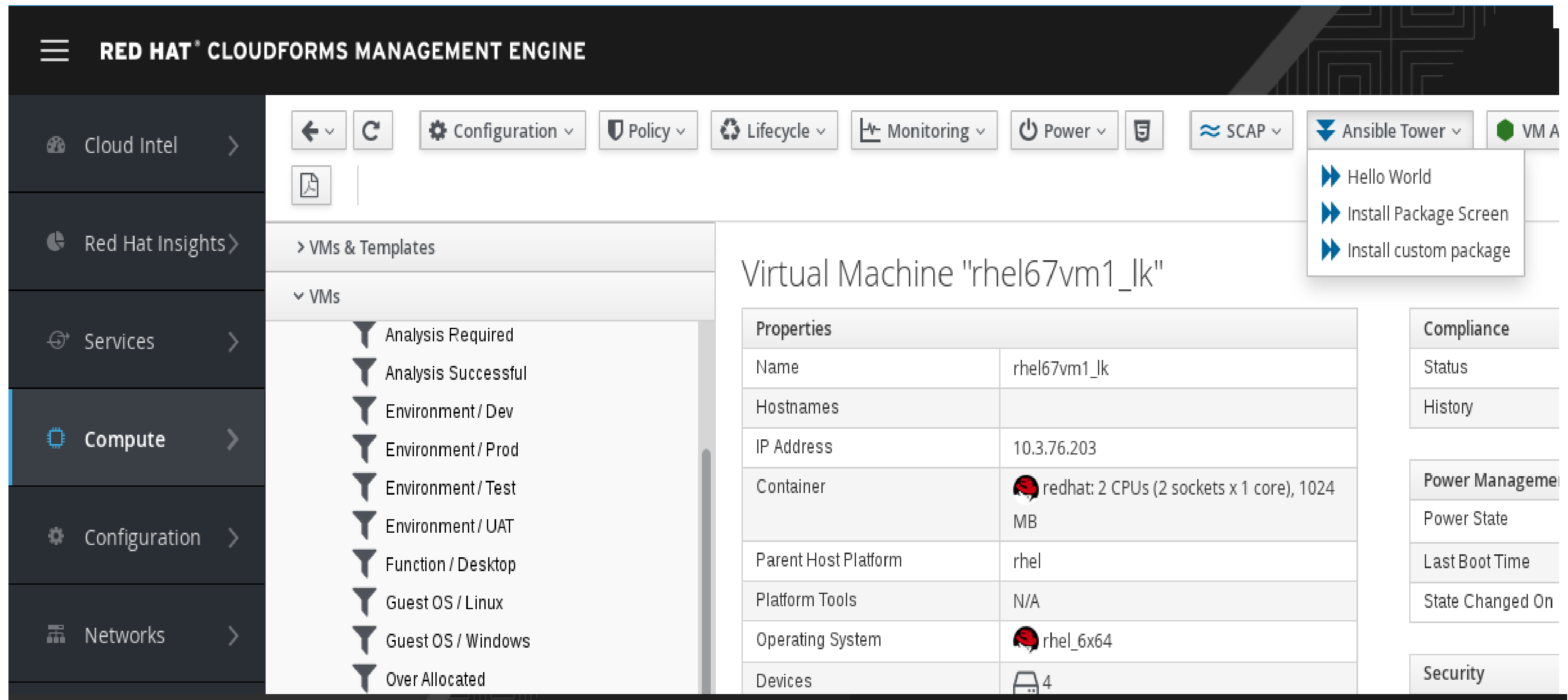
```
    </Profile>
    <Profile id="common">
      <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Common Profi
      <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">This p
n>
      <select idref="partition_for_tmp" selected="true"/>
      <select idref="partition_for_var" selected="true"/>
      <select idref="partition_for_var_log" selected="true"/>
      <select idref="partition_for_var_log_audit" selected="true"/>
      <select idref="partition_for_home" selected="true"/>
      <select idref="ensure_redhat_gpgkey_installed" selected="true"/>
      <select idref="service_rhnsd_disabled" selected="true"/>
      <select idref="security_patches_up_to_date" selected="true"/>
      <select idref="ensure_gpgcheck_globally_activated" selected="true"/>
      <select idref="ensure_gpgcheck_never_disabled" selected="true"/>
      <select idref="package_aide_installed" selected="true"/>
      <select idref="enable_selinux_bootloader" selected="true"/>
      <select idref="no_rsh_trust_files" selected="true"/>
      <select idref="selinux_state" selected="true"/>
      <select idref="selinux_policytype" selected="true"/>
      <select idref="selinux_all_devicefiles_labeled" selected="true"/>
      <select idref="securetty_root_login_console_only" selected="true"/>
      <select idref="restrict_serial_port_logins" selected="true"/>
      <select idref="no_shelllogin_for_systemaccounts" selected="true"/>
      <select idref="no_empty_passwords" selected="true"/>
      <select idref="accounts_password_all_shadowed" selected="true"/>
      <select idref="accounts_no_uid_except_zero" selected="true"/>
      <select idref="userowner_shadow_file" selected="true"/>
      <select idref="groupowner_shadow_file" selected="true"/>
      <select idref="file_permissions_etc_shadow" selected="true"/>
      <select idref="file_owner_etc_gshadow" selected="true"/>
      <select idref="file_groupowner_etc_gshadow" selected="true"/>
      <select idref="file_permissions_etc_gshadow" selected="true"/>
      <select idref="file_owner_etc_passwd" selected="true"/>
      <select idref="file_groupowner_etc_passwd" selected="true"/>
      <select idref="file_permissions_etc_passwd" selected="true"/>
      <select idref="file_owner_etc_group" selected="true"/>
      <select idref="file_groupowner_etc_group" selected="true"/>
      <select idref="file_permissions_etc_group" selected="true"/>
      <select idref="file_permissions_library_dirs" selected="true"/>
      <select idref="file_ownership_library_dirs" selected="true"/>
```

Tag VM
(example:
scap_compliant: core_base_os
scap_noncompliant: top_secret)

Create a Report based on scap_compliant and scap_non compliant tags

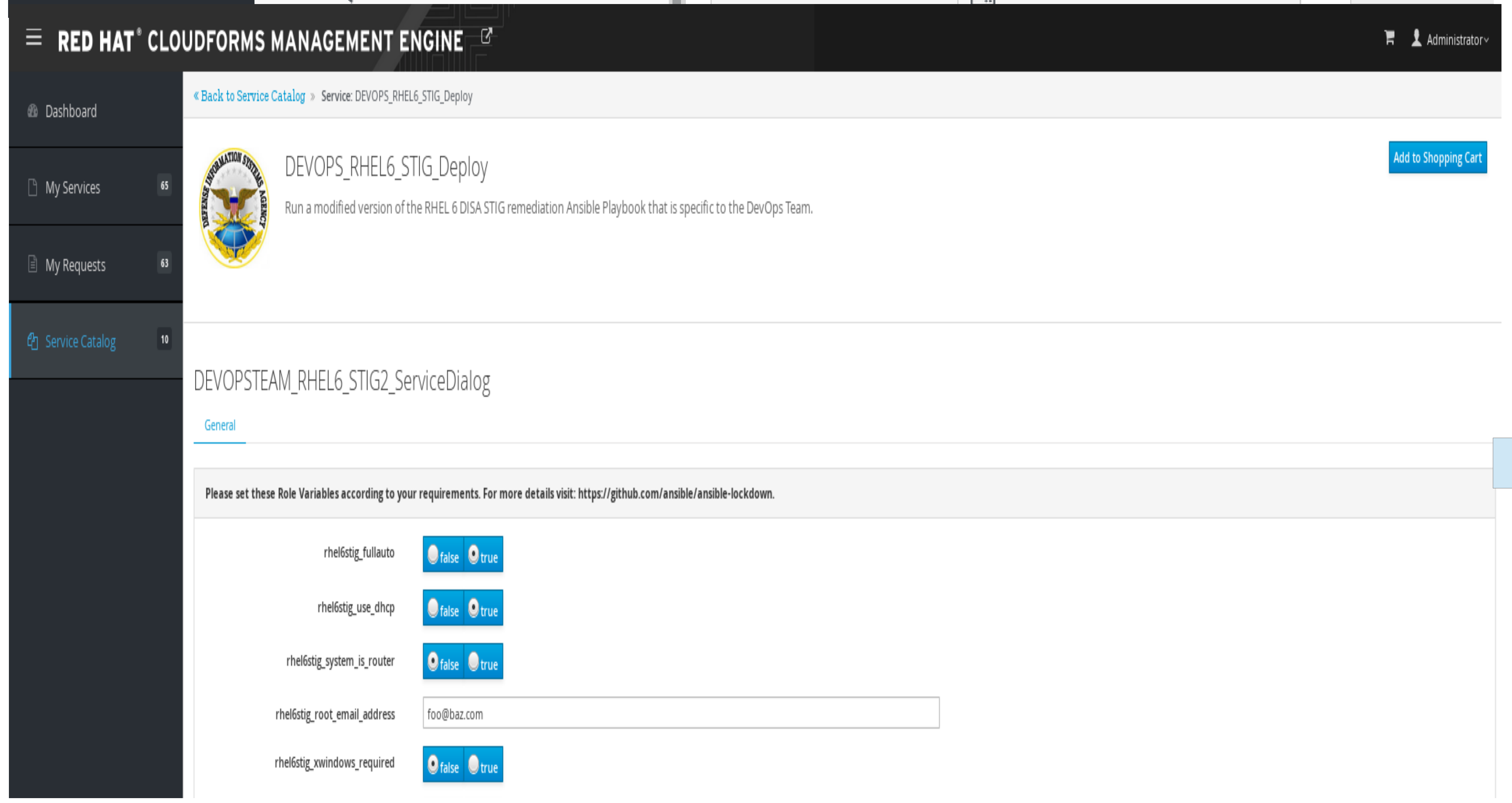
Security remediations with Ansible Tower using Red Hat CloudForms

RED HAT® CLOUDFORMS



Virtual Machine "rhel67vm1_lk"

Properties	
Name	rhel67vm1_lk
Hostnames	
IP Address	10.3.76.203
Container	redhat: 2 CPUs (2 sockets x 1 core), 1024 MB
Parent Host Platform	rhel
Platform Tools	N/A
Operating System	rhel_6x64
Devices	4



Service: DEVOPS_RHEL6_STIG_Deploy

DEVOPS_RHEL6_STIG_Deploy

Run a modified version of the RHEL 6 DISA STIG remediation Ansible Playbook that is specific to the DevOps Team.

DEVOPSTEAM_RHEL6_STIG2_ServiceDialog

Please set these Role Variables according to your requirements. For more details visit: https://github.com/ansible/ansible-lockdown.

rhel6stig_fullauto ○ false ● true

rhel6stig_use_dhcp ○ false ● true

rhel6stig_system_is_router ● false ○ true

rhel6stig_root_email_address foo@baz.com

rhel6stig_xwindows_required ● false ○ true

ANSIBLE TOWER by Red Hat®

DEMO

The Power and Flexibility of the Red Hat CloudForms Control/Policy Engine

Managing Shell Shock compliance with Red Hat CloudForms Control

RED HAT® CLOUDFORMS MANAGEMENT ENGINE
Administrator | EVM
Cloud Intel
Red Hat Insights
Services
Compute
Configuration
Networks
Control
Automate
Optimize
Settings
Configuration
Policy Profiles
Policies

- All Policy Profiles
  - Analysis: Exclude Specially Tagged VMs
  - Analysis: On VM Reconfiguration
  - Compliance Hosts: November 2012
  - Compliance: DISA STIG
  - Compliance: DMZ Configuration
  - Compliance: Hosts
  - Compliance: RHEL Host (KVM)
  - Compliance: VM
  - Compliance: VMware Security Hardening Guide v4.x & v5.x (DMZ)
  - Compliance: VMware Security Hardening Guide v4.x & v5.x (Enterprise)
  - Compliance: VMware Security Hardening Guide v4.x & v5.x (SSLF)
  - Demo: CPU Reservation
  - Demo: Power On/Off VMs
  - Demo: Prevent Cloning of Database VMs
  - Demo: Prevent Cloning of Database VMs
  - Demo: Prevent PowerOn of Quarantined VMs
  - Demo: Service Level Resource Allocation
  - Demo: Shell-Shock Vulnerability
    - **VM and Instance Compliance:** Shell-Shock Vulnerability
      - Vulnerable bash Package (ShellShock)
      - VM Compliance Check
        - Send Email to Security Team
        - Mark as Non-Compliant
        - Generate log message
  - Demo: VM-Operation Policies
  - Demo: VMs in DMZ NIC Check

Policy "Shell-Shock Vulnerability"

Basic Information

Active	Yes
Created	By Username admin on 05/25/16 at 06:13:38 EDT

Scope

VM and Instance : OS Name INCLUDES "linux"

Conditions

	Description	Scopes / Expressions	
◆	Vulnerable bash Package (ShellShock)	Expression	(VM and Instance.Guest Applications : Name CONTAINS "bash" AND FIND VM and Instance.Guest Applications : Version = "4.1.2" CHECK ALL Release REGULAR EXPRESSION MATCHES "1[5]\.(el6_5.2\b|el6_5.1.sjis.2(?!\.)|el6_4.2)")

Events

	Description	Actions
	VM Compliance Check	✕ Send Email to Security Team ✕ Mark as Non-Compliant ✕ Generate log message

Notes

This policy is based on https://access.redhat.com/articles/1200223.
Red Hat Enterprise Linux 6
bash-4.1.2-15.el6_5.2
bash-4.1.2-15.el6_5.1.sjis.2
bash-4.1.2-9.el6 2.2

http://cloudformsblog.redhat.com/2014/09/28/shell-shock-bash-code-injection-vulnerability-via-specially-crafted-environment-variables-cve-2014-6271-cve-2014-7169/#more-325

OpenSCAP compliance for Containers with Red Hat CloudForms Control

- OpenSCAP profile
  - **Image Compliance:** OpenSCAP
    - Has high severity OpenSCAP rule results
    - Container Image Compliance Check
      - Mark as Non-Compliant
  - **Image Control:** Analyse incoming container images
    - Container Image Discovered
      - Initiate SmartState Analysis for Container Image

Proactive Systems Management with Red Hat Insights

RED HAT® CLOUDFORMS MANAGEMENT ENGINE
Administrator | EVM
Cloud Intel
Red Hat Insights
Services
Compute
Configuration
Networks
Control
Automate
Optimize
Settings
Expand All

hostname:nelson.usersys.redhat.com

Stability > MCE kernel panic

Detected issue

A machine check exception (MCE) was detected in the */var/log /messages* file of this host. The MCE is an error that occurs when a computer's CPU detects a hardware problem. In this situation the impending hardware failure might cause kernel panics to protect against data corruption.

The messages detected in your log file for this host are:

- May 13 23:52:03 spebr012 kernel: Machine check events logged ZOMGGGG stuff

Steps to resolve

For further information and suggested resolutions for this issue see "Kernel panic - not syncing: Fatal Machine check" or Machine Check Exception (MCE) in /var/log/messages.

Security > Special DROWN: Cross-protocol attack on TLS using SSLv2 (CVE-2016-0800)

Security > Badlock: Samba protocol flaw affecting client

SUMMARY

- **Create a security compliant host at Provisioning time by 2 methods:**
  - Satellite 6 + OpenSCAP
  - CloudForms + Ansible Tower

- **Automate ongoing security remediation and compliance with:**
  - CloudForms + Satellite + OpenSCAP
  - CloudForms + Ansible Tower
  - CloudForms Control/Policy Engine and Red Hat Insights

QUESTIONS ?

Lucy Huh Kerner
Senior Cloud Solutions Architect
Red Hat U.S. Public Sector
lkerner@redhat.com
Twitter: @LucyCloudBling

Matt Micene
Solutions Architect
DLT Solutions
matt.micene@dlt.com
Twitter: @cleverbeard

APPENDIX

- **Example Satellite 6 provisioning templtae snippet and partition table**
  - https://github.com/nzwulfin/rhsummit16-scap

- **Ansible playbooks for RHEL 6 CIS Benchmarks**
  - **https://github.com/major/cis-rhel-ansible**

- **Ansible role for RHEL 6 DISA STIG from Ansible by Red Hat and MindPointGroup**
  - https://github.com/ansible/ansible-lockdown
  - https://github.com/MindPointGroup/RHEL6-STIG

RED HAT SUMMIT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.