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.”

ZDNET TOLD ME OUR SERVERS HAVE POODLES

I'LL NEED YOU TO PATCH ALL THE BASHES

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

https://nvd.nist.gov/scappproducts.cfm
METHOD #1: Create a Security Compliant host at Provisioning time with: Red Hat Satellite 6 + OpenSCAP
Kickstarting SCAP
SECURITY POLICY

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
ccontent-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 = 240f2f18222f98856c3b4fc50c4195
%end

%addon org_fedora_oscap
content-type = scap-security-guide
profile = pci-dss
%end
### New Host Group

<table>
<thead>
<tr>
<th>Host Group</th>
<th>Puppet Classes</th>
<th>Network</th>
<th>Operating System</th>
<th>Parameters</th>
<th>Locations</th>
<th>Organizations</th>
<th>Activation Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent</td>
<td>RHEL 7 Base</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>PCI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifecycle Environment</td>
<td>DEV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content View</td>
<td>RHEL7 Base</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Puppet Environment</td>
<td>KT_DLT_Solutions_development_rhel7_base_2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Capsule Settings**

- **Content Source**: sats-local.lab.dlt.com
- **Puppet CA**: sats-local.lab.dlt.com
- **Puppet Master**: sats-local.lab.dlt.com

**Included Classes**

- forman_scap_client

**Available Classes**

- access_insights_client
- forman_scap_client
- forman_scap_client::params
- selinux
Create new Scan policy
### Upload new SCAP content file

<table>
<thead>
<tr>
<th>File Upload</th>
<th>Locations</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>SSG-RHEL7-DS</td>
<td></td>
</tr>
<tr>
<td><strong>Scap file</strong></td>
<td><a href="ssg-rhel7-ds.xml">Browse...</a></td>
<td>Upload SCAP DataStream file</td>
</tr>
</tbody>
</table>

### Options
- **Cancel**
- **Submit**
New Compliance Policy

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

Name
SSG-RHEL7

Description

Red Hat Satellite

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.
New Compliance Policy

Organizations

- All Items
- Filter

Selected Items

DLT Solutions

Hostgroups

- All Items
- Filter

Selected Items

RHEL 7 Base

RHEL 7 Base/PCI
Update scan host group
## Index of /pub

<table>
<thead>
<tr>
<th>[ICO]</th>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PARENTDIR]</td>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[]</td>
<td>katello-ca-consumer-latest.noarch.rpm</td>
<td>2016-03-08 15:44</td>
<td>8.2K</td>
<td></td>
</tr>
<tr>
<td>[]</td>
<td>katello-ca-consumer-sat6-local.lab.dlt.com-1.6.1.noarch.rpm</td>
<td>2016-03-08 15:44</td>
<td>8.2K</td>
<td></td>
</tr>
<tr>
<td>[]</td>
<td>katello-ca-consumer-sat6-local.lab.dlt.com-1.6.1.src.rpm</td>
<td>2016-03-08 15:44</td>
<td>8.6K</td>
<td></td>
</tr>
<tr>
<td>[]</td>
<td>katello-server-ca.crt</td>
<td>2016-03-08 15:44</td>
<td>5.3K</td>
<td></td>
</tr>
<tr>
<td>[]</td>
<td>ssg-rhel7-ds.xml</td>
<td>2016-03-09 12:55</td>
<td>2.4M</td>
<td></td>
</tr>
</tbody>
</table>
## Puppet Classes Parameters

<table>
<thead>
<tr>
<th>Puppet class</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>foreman,scap_client</strong></td>
<td>policies</td>
<td><code>&lt;%e16:0c:0e:0c:0e:0e:0e:0e:0e:0e:0e:0e:0e:0e:0e:0e%&gt;</code></td>
</tr>
<tr>
<td></td>
<td>port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server</td>
<td></td>
</tr>
</tbody>
</table>

**Loading parameters...**

---

### Host Group Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>scap_download_path</code></td>
<td><code>/path/to/download</code></td>
</tr>
</tbody>
</table>
Create Kickstart templates
```
if @host.policies_enc != '[]' then
  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
end
```

# Provisioning Template

**Name**: oscap_anaconda_addon

*Note: Useful template functions and macros*

---

**Partition Tables**

**Name**: PCI-SCAP

**Layout**:

- # Create particular logical volumes (optional)
  - `lvol1`:
    - `/dev/mapper/pci-0030-0000-00`:
      - `/dev/pci-0030-0000-00-00`:
        - Name: `/dev/pci-0030-0000-00-00`
        - Flags: `+rw` (read-write)
  - `lvol2`:
    - `/dev/mapper/pci-0030-0000-01`:
      - `/dev/pci-0030-0000-01-00`:
        - Name: `/dev/pci-0030-0000-01-00`
        - Flags: `+rw` (read-write)

---

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

Provisioning Template | Type | Association | History | Locations | Organizations
--- | --- | --- | --- | --- | ---
Name * | Redhat with SCAP | can't be blank

Note: Useful template functions and macros

Template editor

```yaml
# Code
```

---

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 Hosts.

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

+ Add combination
Put it together in a new host
### New Host

<table>
<thead>
<tr>
<th>Host</th>
<th>Puppet Classes</th>
<th>Network</th>
<th>Operating System</th>
<th>Parameters</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture *</td>
<td>x86_64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system *</td>
<td>RedHat 7.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build mode</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media *</td>
<td>DLT_SolutionsLibraryRed_Hat_ServerRed_Hat_Enterprise_Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partition table *</td>
<td>PCI SCAP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**

Display the templates that will be used to provision this host.

---

### New Host

<table>
<thead>
<tr>
<th>Host</th>
<th>Puppet Classes</th>
<th>Network</th>
<th>Operating System</th>
<th>Parameters</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Puppet class Parameters**

<table>
<thead>
<tr>
<th>Puppet class</th>
<th>Name</th>
<th>Value</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policies</td>
<td>^%{ host.policies_enc %}</td>
<td>Additional info</td>
</tr>
<tr>
<td></td>
<td>Foreman_scap_client</td>
<td>port</td>
<td>^{5000}</td>
</tr>
<tr>
<td></td>
<td>Foreman_scap_client</td>
<td>server</td>
<td>^{snl3-local.lab.redhat.com}</td>
</tr>
</tbody>
</table>

**Included Parameters via Inheritance**

<table>
<thead>
<tr>
<th>Scope</th>
<th>Name</th>
<th>Value</th>
<th>Use Puppet default</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>ke_credential_keys</td>
<td>^{RHET_Baseline}</td>
<td></td>
<td>Additional info</td>
</tr>
<tr>
<td></td>
<td>scap_download_path</td>
<td>^{/pub/sg-rhel7-ds.xml}</td>
<td></td>
<td>Additional info</td>
</tr>
</tbody>
</table>

---

# redhat #rhsummit
network --bootproto dhcp --hostname pci-test.mylab.dlt.com --device=52:54:00:00:00:20
rootpass --isrtyk0d skH0YwheZeHvD12J3Y9ye4ST2K6yH0X3
firewall --service=ssh
authconfig --useshadow --passalgo=sha256 --kickstart
timezone --utc UTC

bootloader --location=mbr --append="neth 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
# -nlabel initialize the disk label to the default based on the underlying architecture
clearpart --all --nolabel
#autopart --type=lv

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

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

# Create particular logical volumes (optional)


text
reboot

%packages --ignoremissing
yum
dhcclient
ntp
wpe
@Core
%end

%addon org.fedoraproject.
content-type = osscap
content-url = http://set6-local.lab.dlt.com/pub/oss.rhel7.ds.xml
profile = xccdf.org.sspproject.content_profile_pci-dss
%end
Compliance Reports

Filter:

<table>
<thead>
<tr>
<th>Host</th>
<th>Date</th>
<th>Passed</th>
<th>Failed</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>postest.mylab.dlt.com</td>
<td>about 20 hours ago</td>
<td>61</td>
<td>11</td>
<td>2</td>
</tr>
</tbody>
</table>

Displaying 1 entry

Compliance and Scoring

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

Rule results

61 passed
41 failed

Severity of failed rules

32 low
9 medium

Score

<table>
<thead>
<tr>
<th>Scoring system</th>
<th>Score</th>
<th>Maximum</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>um:scoring:default</td>
<td>60.734955</td>
<td>100.00000</td>
<td>60.73%</td>
</tr>
</tbody>
</table>

Rule Overview

Check:
- pass
- fixed
- informational

Failed:
- fail
- error
- notselected
- notapplicable

Title

Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Search through XCCDF rules
METHOD #2:
Create a Security Compliant host at Provisioning time with:
Red Hat CloudForms + Red Hat Satellite + Ansible Tower
WHAT IS CLOUDFORMS?

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

Lauch the CloudForms Provisioning State Machine

Post Provisioning Steps

ANSIBLE PLAYBOOK

ANSIBLE TOWER by Red Hat®

RED HAT® SATELLITE


CIS Security Benchmarks

Lauch the CloudForms Provisioning State Machine

Post Provisioning Steps

ANSIBLE PLAYBOOK

ANSIBLE TOWER by Red Hat®

RED HAT® SATELLITE


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

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

Create a Report based on scap_compliant and scap_noncompliant tags
Security remediations with Ansible Tower using Red Hat CloudForms
DEMO
The Power and Flexibility of the Red Hat CloudForms Control/Policy Engine
Managing Shell Shock compliance with Red Hat CloudForms Control

Policy "Shell-Shock Vulnerability"

Basic Information

Active: Yes
Created: By Username admin on 06/29/16 at 06:13:38 EDT

Scope

VM and Instance OS Name INCLUDES "inux"

Conditions

| Description | Regression
|-------------|------------|
| Vulnerable bash Package (Shellshock) | Expensive (VM and Instance Guest Applications: Name CONTAINS "bash" AND FIND VM and Instance Guest Applications: Version = "4.1.2" CHECK ALL Releases REGULAR EXPRESSION MATCHES "105", "on x86_64" ("x64", "x86", "x86_64", "i686", "x86_64")"

Events

<table>
<thead>
<tr>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Compliance Check</td>
<td>Send Email to Security Team, Mark as Non-Compliant, Generate log message</td>
</tr>
</tbody>
</table>

Notes

This policy is based on https://access.redhat.com/articles/120023:
Red Hat Enterprise Linux 4
bash-4.1.2-19.8.el5
bash-4.1.2-19.8.el6.5
bash-4.1.2-19.8.el7.2
bash-4.1.2-19.8.el8.2

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

- **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 a kernel panic to protect against data corruption.
    - The messages detected in your log file for this host are:
      - May 13 29:52:03 spade12 kernel: Machine check exception logged ZOMG GGGG 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-2016-6800)**

- **Security > Backoff: 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 template 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
LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.