

L105190: Proactive Security Compliance Automation with CloudForms, Satellite, OpenSCAP, Insights, and Ansible Tower

Lead Presenter:

Lucy Kerner, Principal Technical Marketing Manager - Security, Red Hat

Co-Presenters:

Patrick Rutledge, Principal Solutions Architect - GPTE, Red Hat

Nate Stephany, Senior Cloud Specialist Solutions Architect, Red Hat

Kevin Morey, Principal Cloud Specialist Solutions Architect, Red Hat

Will Nix, Principal Technical Marketing Manager - Red Hat Insights, Red Hat

Abstract:

In this hands-on lab, you will learn how to automate security compliance using a combination of Red Hat CloudForms, Red Hat Satellite, OpenSCAP, and Ansible Tower by Red Hat. Specifically, you will go through a series of exercises that will show you: how to use Red Hat CloudForms to create control policies, how to automate security scans and remediations using the OpenSCAP integration in Red Hat Satellite, how to utilize the data provided by Red Hat Insights for proactive security and automated risk management, how to use Ansible Tower by Red Hat for automated security remediations, and how to use Red Hat CloudForms as a central place for security compliance automation.

Overview and Prerequisites:

The goal of this lab is to introduce you to a variety of Red Hat products that can help you with proactive security compliance automation. We will demonstrate the power and flexibility of using either one or a combination of Red Hat products, such as Red Hat Satellite, Ansible Tower by Red Hat, Red Hat Insights, and Red Hat CloudForms, to help you with security compliance and automation.

This lab is geared towards systems administrators, cloud administrators and operators, architects, and others working on infrastructure operations management who are interested in learning how to automate security compliance across their heterogeneous infrastructure using one or more Red Hat Products. The prerequisite for this lab include basic Linux skills gained from Red Hat Certified System Administrator (RHCSA) or equivalent system administration skills. Knowledge of virtualization and basic linux scripting would also be helpful, but not required.

Attendees, during this session, will learn :

- What Security Content Automation Protocol (SCAP) is and how you can use it to automate compliance with security policies
- How to use Red Hat Satellite and Red Hat CloudForms to automatically apply and enforce security policies on bare metal and virtual machines
- How to use OpenSCAP, Red Hat Satellite and Red Hat CloudForms to audit bare metal and virtual machines for security compliance
- How to use OpenSCAP, Red Hat CloudForms and Ansible Tower by Red Hat to automatically remediate systems that are out of compliance
- How to create and view reports showing compliant and non-compliant VMs in Red Hat CloudForms after running OpenSCAP security compliance scans on these VMs
- How to prevent Red Hat Openshift container images with severity high vulnerabilities from running in Red Hat Openshift using Red Hat CloudForms
- How to provision a security compliant host, at the push of a button, using Red Hat CloudForms and Ansible Tower by Red Hat
- How to use Red Hat Insights for pro-active security and automated risk management

Lab Environment :

Your entire lab environment is hosted online and includes Red Hat Virtualization, Red Hat Satellite 5.7 and Satellite 6.2, Red Hat CloudForms, Ansible Tower by Red Hat, Red Hat Insights, Red Hat Openshift Container Platform, and a workstation node which will have a public IP you can SSH into. You can get to all the listed Red Hat products and all your VMs(one RHEL 6 and two RHEL 7 VMs) from the workstation node.

You will each be given your own unique GUID, which you will use to access your own instance of these Red Hat products for your lab exercises.

[Lab 0: Setup steps](#)

[Starting your VMs](#)

[Logging into all the other Red Hat Products](#)

[Lab 1: How to utilize the integrated security scanning and auditing tool, OpenSCAP, in Satellite 6](#)

[Goal of Lab 1](#)

[Introduction](#)

[Introduction to SCAP content provided in Satellite 6](#)

[Creating a SCAP compliance policy for a host](#)

[Executing the compliance policy on a host](#)

[View the SCAP scan results report in Satellite 6](#)

[Fix a specific SCAP scan failure, re-run the SCAP scan, and view the resulting scan report in Satellite 6](#)

[Viewing the global status indicator in Satellite 6](#)

[Lab 2: How to use the control policy engine in Red Hat CloudForms and Ansible Tower to enforce compliance with security policies](#)

[Goal of Lab 2](#)

[Introduction](#)

[Using the Red Hat CloudForms control engine and Ansible Tower by Red Hat to execute the Shellshock control policy and do remediation](#)

[Lab 3: Managing the security of Red Hat Openshift container images from Red Hat CloudForms](#)

[Goal of Lab 3](#)

[Introduction](#)

[Preventing Red Hat Openshift container images with high severity vulnerabilities from running in Red Hat Openshift using Red Hat CloudForms](#)

[Lab 4: OpenSCAP security scans and remediations at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Satellite 5.7](#)

[Goal of Lab 4](#)

[Introduction](#)

[OpenSCAP security scan on a VM at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Red Hat Satellite 5.7](#)

[OpenSCAP security remediation on a VM at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Red Hat Satellite 5.7](#)

[Lab 5 : OpenSCAP security scans and remediations at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Satellite 6.2](#)

[Goal of Lab 5](#)

[Introduction](#)

[OpenSCAP security scan on a VM at the push of a button in Red Hat CloudForms utilizing Satellite 6's built-in OpenSCAP scanning capabilities](#)

[OpenSCAP security remediation on a VM at the push of a button in Red Hat CloudForms utilizing Satellite 6's built-in OpenSCAP remediation capabilities](#)

[Lab 6 : Viewing SCAP compliant and non-compliant VMs from a report in Red Hat CloudForms](#)

[Goal of Lab 6](#)

[Introduction](#)

[View SCAP compliant and non-compliant VM reports](#)

[Lab 7 : Ordering a custom service using Red Hat CloudForms and Ansible Tower by Red Hat for security compliance automation](#)

[Goal of Lab 7](#)

[Introduction](#)

[Using the Red Hat CloudForms service catalog to order a service to execute an Ansible playbook against your entire Ansible Tower inventory](#)

[Understanding how to use the Red Hat CloudForms service catalog to provision a security compliant host at the push of a button](#)

[Lab 8: Proactive Security and Automated Risk Management with Red Hat Insights](#)

[Goal of Lab 8](#)

[Introduction](#)

[Fixing the payload injection security issue in your system using Red Hat Insights](#)

[Lab 9: Viewing Red Hat Insights security findings from Red Hat CloudForms](#)

[Goal of Lab 9](#)

[Introduction](#)

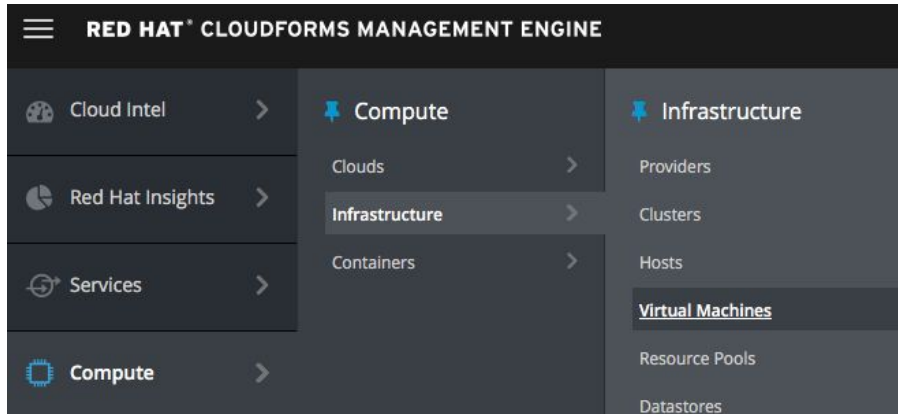
[View Red Hat Insights security findings from Red Hat CloudForms](#)

Lab 0: Setup steps

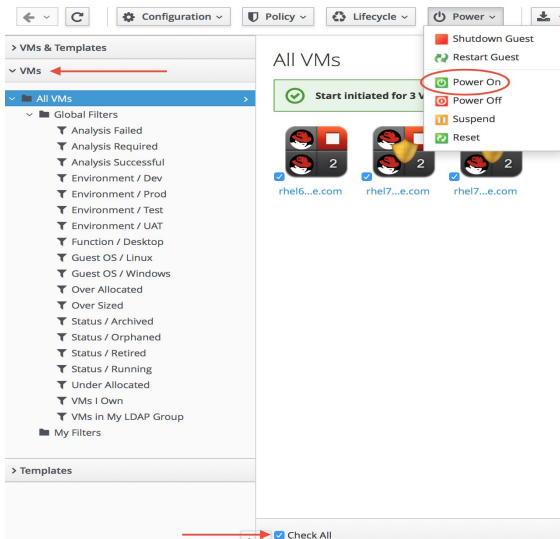
Starting your VMs

1. Before starting the lab steps, you will need to turn on your VMs. Open up your Firefox web browser and log into **https://cfme-*<GUID>*.rhpds.opentlc.com**. The *<GUID>* portion is a 4 character random string that will be assigned to you.
2. Accept the SSL warnings.
3. Login as **admin** with password **r3dh@t2017**.

- On the left menus, navigate to **Compute -> Infrastructure -> Virtual Machines**.



- Click the **VMs** accordion on the left.
- At the bottom, click **Check All**.
- At the top click **Power -> Power On**.



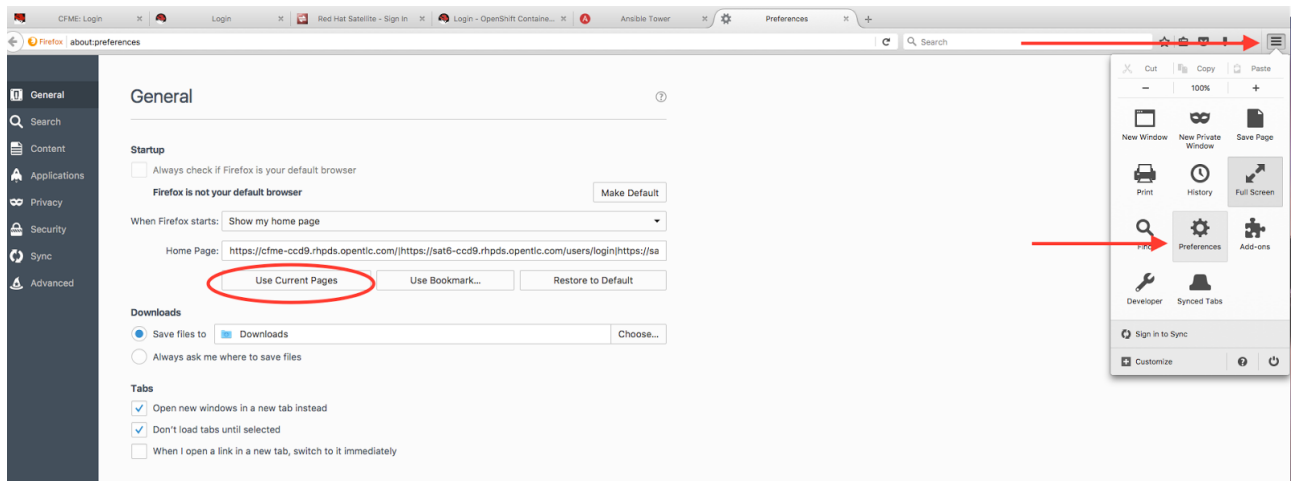
- Click **OK**.
- Do not close your CloudForms UI since you will be using it in future lab exercises.

Logging into all the other Red Hat Products

Now, let's login to the rest of the Red Hat Products so they are ready for us to use in the rest of the labs. The table below lists the web pages of the Red Hat Products you need to be logged into for the lab exercises in this lab. Open a new tab on your Firefox web browser for each of the Red Hat Products listed below. Log in with the credentials listed below and accept any warnings regarding the SSL certificate. Note that the **<GUID>** portion is a 4 character random string that will be assigned to you.

Name of Red Hat Product	URL	Username	Password
Satellite 6.2	<a href="https://sat6-<GUID>.rhpds.opentlc.com">https://sat6-<GUID>.rhpds.opentlc.com	admin	r3dh@t2017
Satellite 5.7	<a href="https://sat5-<GUID>.rhpds.opentlc.com">https://sat5-<GUID>.rhpds.opentlc.com	admin	r3dh@t2017
Ansible Tower	<a href="https://tower-<GUID>.rhpds.opentlc.com">https://tower-<GUID>.rhpds.opentlc.com	admin	r3dh@t2017
Openshift	<a href="https://ocp-<GUID>.rhpds.opentlc.com:8443/console">https://ocp-<GUID>.rhpds.opentlc.com:8443/console	summit17	r3dh@t2017

10. Now, let's save the URLs on these tabs that we just opened as the startup pages of the web browser. In your Firefox web browser, open up **Preferences** and Click on **Use Current Pages**. Then, close the **Preferences** tab.



Lab 1: How to utilize the integrated security scanning and auditing tool, OpenSCAP, in Satellite 6

Goal of Lab 1

The goal of this lab is to introduce you to the integrated security scanning and auditing tool, OpenSCAP, in Satellite 6.

Introduction

Security compliance management is the ongoing process of defining security policies, auditing for compliance with those policies and resolving instances of non-compliance. Once a security policy is defined, an audit is conducted to verify compliance with the policy. Any non-compliance is managed according to the organization's configuration management policies. Security policies vary in their scope, from being host-specific to industry-wide, so there is a need for flexibility in their definition.

The Security Content Automation Protocol (SCAP) enables the definition of security configuration policies. For example, a security policy might specify that for hosts running Red Hat Enterprise Linux, login via SSH is not permitted for the root account.

In Satellite 6, tools provided by the *OpenSCAP* project are used to implement security compliance auditing. For more information about OpenSCAP see the [Red Hat Enterprise Linux 7 Security Guide](#). The Satellite web UI enables scheduled compliance auditing and reporting on all hosts under management by Red Hat Satellite.

Introduction to SCAP content provided in Satellite 6

Before creating a SCAP compliance policy for a host, you need SCAP content.

SCAP content is a datastream format containing the configuration and security baseline against which hosts are checked. Checklists are described in the *extensible checklist configuration description format* (XCCDF) and vulnerabilities in the *open vulnerability and assessment language* (OVAL). Checklist items, also known as *rules* express the desired configuration of a system item. For example, you may specify that no one can log in to a host over SSH using the root user account. Rules can be grouped into one or more *profiles*, allowing multiple profiles to share a rule. SCAP content consists of both rules and profiles.

You can either create SCAP content or obtain it from a vendor. Supported profiles are provided for Red Hat Enterprise Linux in the `scap-security-guide` package. The creation of SCAP content is outside the scope of this lab, but see the [Red Hat Enterprise Linux 7 Security Guide](#) or [Red Hat Enterprise Linux 6 Security Guide](#) for information on how to download, deploy, modify, and create your own content. The SCAP content provided with Red Hat Enterprise Linux is compliant with SCAP specification 1.2.

The default SCAP content provided with the OpenSCAP components of Satellite 6 depends on the version of Red Hat Enterprise Linux:

- On Red Hat Enterprise Linux 6, content for Red Hat Enterprise Linux 6 is installed.
- On Red Hat Enterprise Linux 7, content for both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 is installed.

When you install the SCAP components in Satellite as defined in the [Host Configuration Guide](#), all of the Red Hat default content will show up in Satellite so no extra steps are necessary to add the SCAP content to Satellite. But if you had customized content that you wrote yourself or if you have a modified policy and you wanted to upload that modified version, you can do that in the Satellite UI under Hosts → SCAP contents.

1. Take a look at the default SCAP content provided with the OpenSCAP components of Satellite 6 by navigating to **Hosts** → **SCAP contents**.

The screenshot shows the Red Hat Satellite web interface. The top navigation bar includes 'RED HAT SATELLITE', 'Default Organization', 'Monitor', 'Content', 'Containers', 'Hosts', 'Configure', 'Infrastructure', 'Red Hat Insights', 'Red Hat Access', 'Admin User', and 'Administer'. The 'Hosts' dropdown menu is open, showing options like 'All hosts', 'Discovered hosts', 'Content Hosts', 'Host Collections', 'New host', 'PROVISIONING SETUP', 'Architectures', 'Hardware models', 'Installation media', 'Operating systems', 'TEMPLATES', 'Partition tables', 'Provisioning templates', 'Job templates', 'COMPLIANCE', 'Policies', 'SCAP contents', and 'Reports'. A red arrow points to the 'SCAP contents' option. The main content area shows a table of SCAP contents with columns for 'Title', 'Created', and 'Edit'. The table lists four default contents: 'Red Hat firefox default content', 'Red Hat jre default content', 'Red Hat rhel6 default content', and 'Red Hat rhel7 default content', all created 'about 1 month ago'.

Creating a SCAP compliance policy for a host

Now that you have SCAP content defined in Satellite, you can create a SCAP compliance policy for a host.

2. Navigate to **Hosts** → **Policies** and click on **New Compliance Policy** at the top right.

RED HAT SATELLITE

Default Organization | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Red Hat Insights | Red Hat Access | Admin User | Administrator

Compliance Policies

Filter ...

Name	Content
rhel7-base	Red Hat rhel7 default content
RHEL7_Common	Red Hat rhel7 default content
RHEL7_PC_DSS	Red Hat rhel7 default content
RHEL7_Standard	Red Hat rhel7 default content

Hosts dropdown menu:

- All hosts
- Discovered hosts
- Content Hosts
- Host Collections
- New host
- PROVISIONING SETUP
 - Architectures
 - Hardware models
 - Installation media
 - Operating systems
- TEMPLATES
 - Partition tables
 - Provisioning templates
 - Job templates
- COMPLIANCE
 - Policies**
 - SCAP contents
 - Reports

Buttons: [New Compliance Policy](#) [Help](#)

3. In the **Create Policy** tab,
 - a. For the compliance policy **Name**, type **RHEL7_Standard**.
 - b. For the **Description**, type **RHEL7 Standard System Compliance Policy**.
 - c. Click **Next**.

RED HAT SATELLITE

Default Organization | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Red Hat Insights | Red Hat Access | Admin User | Administrator

New Compliance Policy

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

Name *

Description

[Cancel](#) [Next](#)

4. In the **SCAP Content** tab,
 - a. For **SCAP Content**, choose the **Red Hat rhel7 default content**.
 - b. For **XCCDF Profile**, choose **Standard System Security Profile**.
 - c. Click **Next**.

RED HAT SATELLITE

Default Organization | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Red Hat Insights | Red Hat Access | Admin User | Administrator

New Compliance Policy

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

SCAP Content

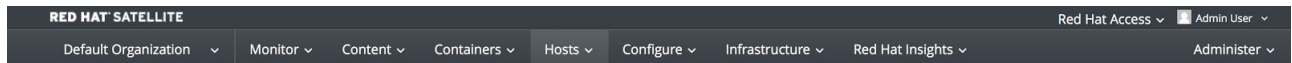
XCCDF Profile

[Cancel](#) [Next](#)

5. In the **Schedule** tab,
 - a. For **Period**, choose **Weekly**.
 - b. For **Weekday** choose **Thursday**.

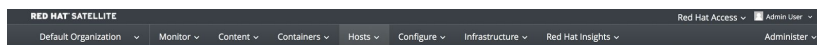
Note: Whatever is defined here as a schedule is executed as a cron job on the client. For Period, if you selected Custom, you can define normal cron syntax to define when the schedule is going to run.

- c. Click **Next**.



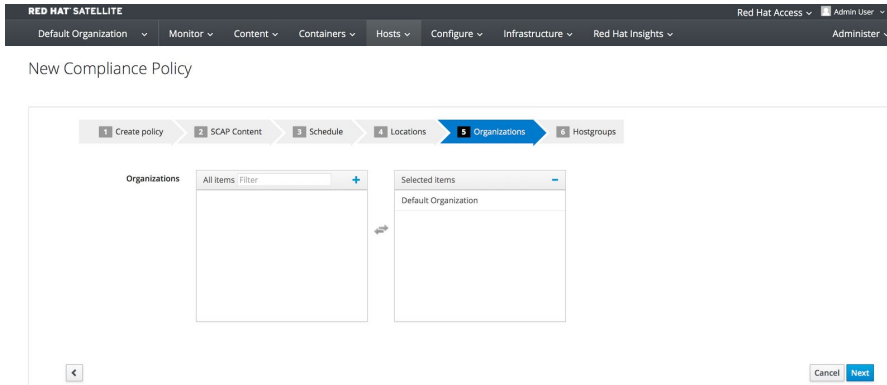
New Compliance Policy

6. In the **Locations** tab,
 - a. Click the **Default Location** to move it over to the **Selected items** box. This will associate the compliance policy with this **Location**.
 - b. Click **Next**.



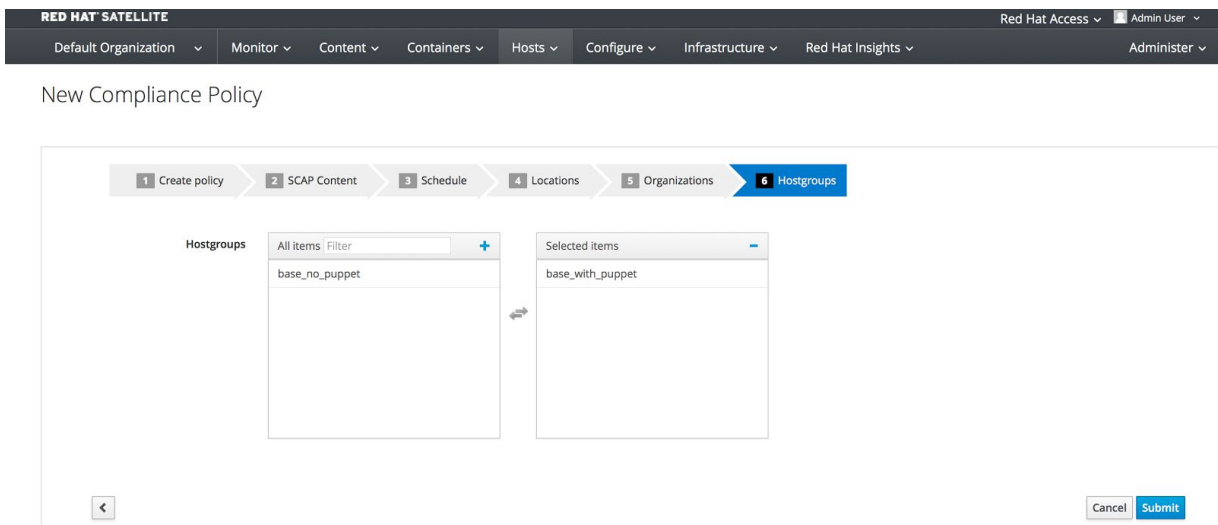
New Compliance Policy

7. In the **Organizations** tab,
 - a. (If not already on the right) Click the **Default Organization** to move it over to the **Selected items** box. This will associate the compliance policy with this **Organization**.
 - b. Click **Next**.



8. In the **Hostgroups** tab,
 - a. Click **base_with_puppet** to move it over to the **Selected items** box.
The compliance policy will apply to this selected **Hostgroup**.

9. Click **Submit**.



Executing the compliance policy on a host

10. After you have defined the SCAP compliance policy in Satellite, SSH into your workstation host at workstation-*<GUID>*.rhpds.opentlc.com as the summit17 user. An ssh key is already in the home directory of your laptop, which should allow you to login without a password. Should a password be required, use r3dh@t2017 as your password.

```
$ ssh summit17@workstation-<GUID>.rhpds.opentlc.com
```

11. Now that you are in the **workstation** host, SSH into your **RHEL 7 VM 1** host. This host has already been registered to both Red Hat Satellite 6 and Red Hat Insights for you.

```
$ ssh rhel7vm1.summit.example.com
```

12. As root, run the puppet agent:

```
$ sudo -i
```

```
# puppet agent --test
```

Note: Ignore the Warning that appears regarding the “Local environment”

This will set up all the SCAP components, which are delivered via the puppet agent. Satellite provides a puppet module and a means for the puppet module to set up all the SCAP components. Normally, in production, the puppet agent run automatically occurs within 30 mins so the puppet agent --test is not necessary. We are just doing this in the lab to avoid waiting 30 mins for the puppet agent to run.

13. Now that the SCAP components are installed and configured on the client, take a look at the SCAP configuration on the client which is stored in `/etc/foreman_scap_client/config.yaml`

```
# less /etc/foreman_scap_client/config.yaml
```

Note: In this yaml file, you will see some basic information such as what server will your reports be uploaded to which is defined by your Hostgroup, certification information such as what certificates were used to authenticate, and towards the bottom, you'll see your policy ID(s) which are the SCAP policies which you associated in the Satellite UI to its Hostgroup.

14. In the above `/etc/foreman_scap_client/config.yaml` file, take note of the **highest** numbered Policy ID which should be the **RHEL7_Standard** compliance policy we created earlier. In the example `/etc/foreman_scap_client/config.yaml` file below, notice that the highest Policy ID is 4. However, your Policy ID may be different.

```

lkerner — summit17@rhel7vm1:/etc/foreman_scap_client — ssh summit17@workstation-ccd9.rhpd.opentlc.com — 133
# Or (recommended for client reporting to Katello) consumer certificate (e.g., '/etc/pki/consumer/cert.pem')
:host_certificate: '/etc/pki/consumer/cert.pem'
# Client private key
# It could be Puppet agent private key (e.g., '/var/lib/puppet/ssl/private_keys/myhost.example.com.pem')
# Or (recommended for client reporting to Katello) consumer private key (e.g., '/etc/pki/consumer/key.pem')
:host_private_key: '/etc/pki/consumer/key.pem'

# policy (key is id as in Foreman)

1:
profile: ''
content_path: '/var/lib/openscap/content/96c2a9d5278d5da905221bbb2dc61d0ace7ee3d97f021fccac994d26296d986d.xml'
Download path
# A path to download SCAP content from proxy
download_path: '/compliance/policies/1/content'

3:
profile: 'xccdf_org.ssgproject.content_profile_common'
content_path: '/var/lib/openscap/content/96c2a9d5278d5da905221bbb2dc61d0ace7ee3d97f021fccac994d26296d986d.xml'
Download path
# A path to download SCAP content from proxy
download_path: '/compliance/policies/3/content'

4:
profile: 'xccdf_org.ssgproject.content_profile_standard'
content_path: '/var/lib/openscap/content/96c2a9d5278d5da905221bbb2dc61d0ace7ee3d97f021fccac994d26296d986d.xml'
Download path
# A path to download SCAP content from proxy
download_path: '/compliance/policies/4/content'

2:
profile: 'xccdf_org.ssgproject.content_profile_pci-dss'
content_path: '/var/lib/openscap/content/96c2a9d5278d5da905221bbb2dc61d0ace7ee3d97f021fccac994d26296d986d.xml'
# Download path
# A path to download SCAP content from proxy
download_path: '/compliance/policies/2/content'

```

Take Note of the highest
Profile ID!

15. Type **q** to exit **less**.

16. Execute the **RHEL7_Standard** compliance policy on the **RHEL 7 VM 1** host using the **Policy ID** number found in the previous step (where **X** is the Policy ID found earlier):

```
# foreman_scap_client X
```

This will run the scap scan, bzip the scan results, and upload the results to Satellite. Wait for the command to complete before continuing.

View the SCAP scan results report in Satellite 6

17. Go back to your Satellite UI and view your SCAP scan results report for your RHEL7_Standard compliance policy by navigating to:

Hosts → Reports.

The screenshot shows the Red Hat Satellite interface. At the top, there is a navigation bar with the following items: Default Organization, Monitor, Content, Containers, Hosts, and Configure. The 'Hosts' menu is open, showing a list of options: All hosts, Discovered hosts, Content Hosts, Host Collections, New host, PROVISIONING SETUP (Architectures, Hardware models, Installation media, Operating systems), TEMPLATES (Partition tables, Provisioning templates, Job templates), COMPLIANCE (Policies, SCAP contents), and Reports. The 'Reports' option is highlighted with a blue background and a red arrow points to it from the table below.

The main content area is titled 'Compliance Reports' and has a 'Filter ...' input field. Below it is a table with the following columns: Host, Reported At, Passed, and Failed. The table contains 14 rows of data for the host 'rhel7vm1.summit.example.com'. The first row is highlighted in grey and has a red arrow pointing to the 'Reports' link in the 'Reported At' column.

Host	Reported At	Passed	Failed
<input type="checkbox"/> rhel7vm1.summit.example.com	less than a minute ago	9	1
<input type="checkbox"/> rhel7vm1.summit.example.com	about 21 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 22 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 23 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	1 day ago	0	0

18. Click on the report you just created by clicking on the **most recent** report for **rhel7vm1.summit.example.com** by clicking the link in the second **Reported At** column (do not click the host link).

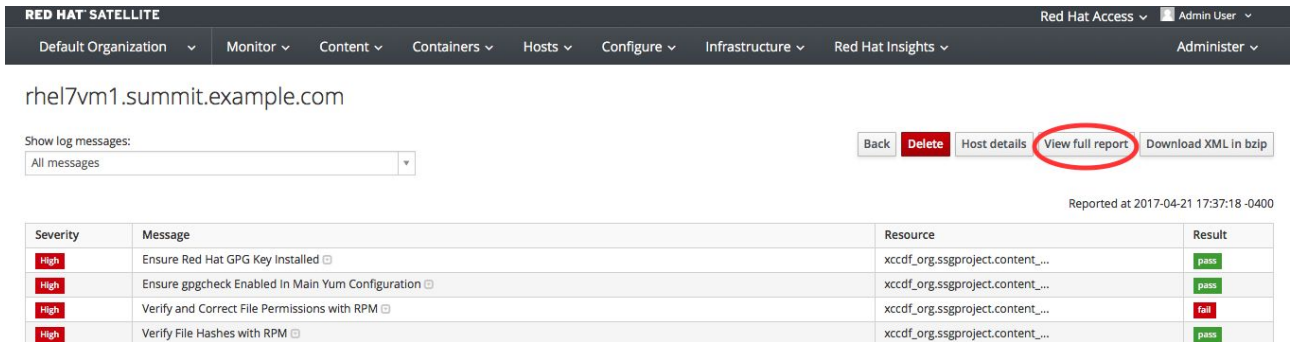
Compliance Reports

The screenshot shows the 'Compliance Reports' table with a search bar at the top. The table has the following columns: Host, Reported At, Passed, and Failed. The first row is highlighted in grey and has a red arrow pointing to the 'less than a minute ago' link in the 'Reported At' column.

Host	Reported At	Passed	Failed
<input type="checkbox"/> rhel7vm1.summit.example.com	less than a minute ago	9	1
<input type="checkbox"/> rhel7vm1.summit.example.com	about 21 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 22 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 23 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	1 day ago	0	0

In this report, you can see the security rules that have passed and failed at a high level which allows you to see the security posture of a system based upon an assigned audit policy.

19. To see the detailed full report, click on **View full report** at the top right.



RED HAT SATELLITE

Default Organization Monitor Content Containers Hosts Configure Infrastructure Red Hat Insights Administer

rhel7vm1.summit.example.com

Show log messages: All messages

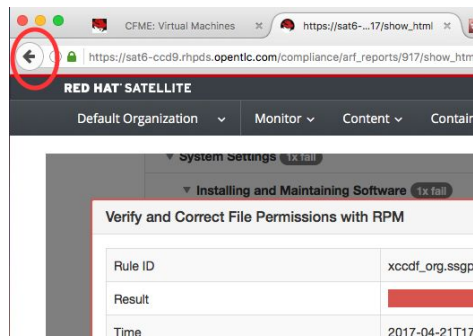
Back Delete Host details **View full report** Download XML in bzip

Reported at 2017-04-21 17:37:18 -0400

Severity	Message	Resource	Result
High	Ensure Red Hat GPG Key Installed	xccdf_org.ssgproject.content_...	pass
High	Ensure gpgcheck Enabled In Main Yum Configuration	xccdf_org.ssgproject.content_...	pass
High	Verify and Correct File Permissions with RPM	xccdf_org.ssgproject.content_...	fail
High	Verify File Hashes with RPM	xccdf_org.ssgproject.content_...	pass

20. Glance through this report to see what rules passed/failed, severity of the rules, etc. Notice that you can click on each rule for a deeper drill down.

21. Click the **back arrow** on your web browser to go back to the previous report summary page.



CFME: Virtual Machines

https://sat6-...17/show_html

https://sat6-ccd9.rhpd5.opentlc.com/compliance/arf_reports/917/show_html

RED HAT SATELLITE

Default Organization Monitor Content Contain

System Settings (1x fail)

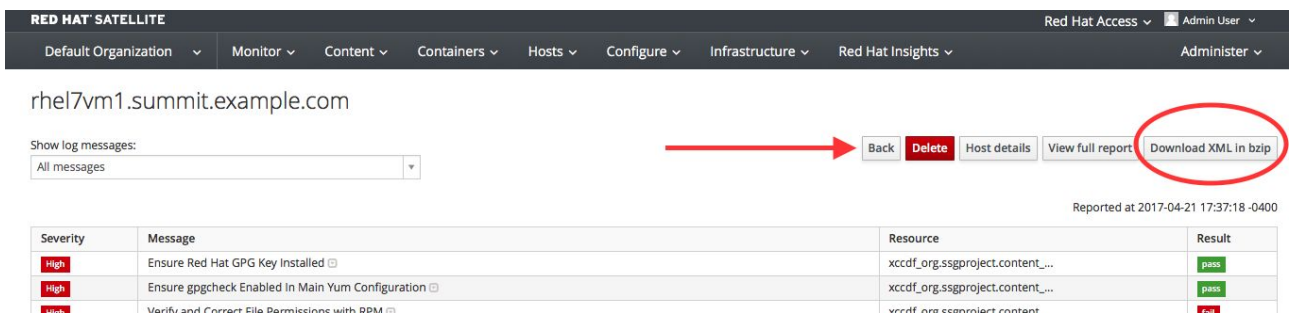
Installing and Maintaining Software (1x fail)

Verify and Correct File Permissions with RPM

Rule ID	xccdf_org.ssgp
Result	fail
Time	2017-04-21T17

22. Take a look at the top right buttons in the Satellite UI. Notice also that you can Download the XML of the report in bzip as well.

Click the **Back** button from the top right of the Satellite UI.



RED HAT SATELLITE

Default Organization Monitor Content Containers Hosts Configure Infrastructure Red Hat Insights Administer

rhel7vm1.summit.example.com

Show log messages: All messages

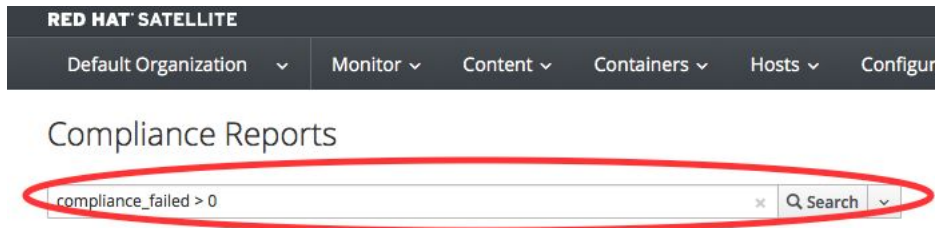
Back Delete Host details View full report **Download XML in bzip**

Reported at 2017-04-21 17:37:18 -0400

Severity	Message	Resource	Result
High	Ensure Red Hat GPG Key Installed	xccdf_org.ssgproject.content_...	pass
High	Ensure gpgcheck Enabled In Main Yum Configuration	xccdf_org.ssgproject.content_...	pass
High	Verify and Correct File Permissions with RPM	verrifi are ssonmriact content	fail

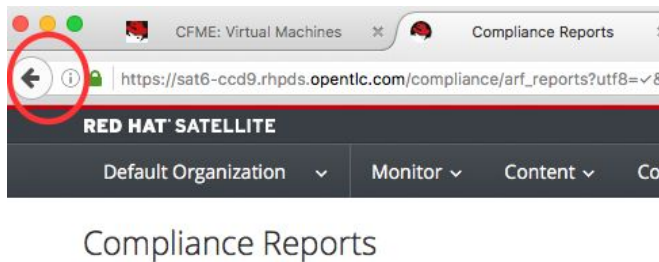
23. Notice the search bar at the top of the Satellite UI. Here, you can filter the compliance reports search with various filters.

Type `compliance_failed > 0` and press Search.



This will find any compliance report that have greater than 0 compliance failures.

24. Click the **back arrow** on your web browser to go back to your full list of compliance reports.



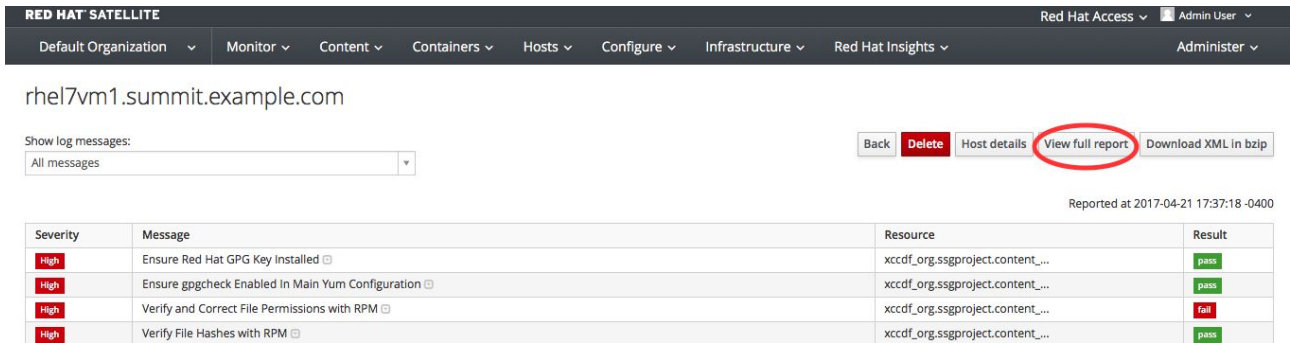
25. Click on the report you just created again by clicking on the **most recent** report for **rhel7vm1.summit.example.com** by clicking the link in the second **Reported At** column (again do not click the host link).

Compliance Reports

Filter ... Search

Host	Reported At	Passed	Failed
<input type="checkbox"/> rhel7vm1.summit.example.com	less than a minute ago	0	1
<input type="checkbox"/> rhel7vm1.summit.example.com	about 21 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 22 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 23 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	1 day ago	0	0

26. Click on **View full report** at the top right again.



RED HAT SATELLITE Red Hat Access ▼ Admin User ▼

Default Organization ▼ Monitor ▼ Content ▼ Containers ▼ Hosts ▼ Configure ▼ Infrastructure ▼ Red Hat Insights ▼ Administer ▼

rhel7vm1.summit.example.com

Show log messages: Back Delete Host details **View full report** Download XML in bzip

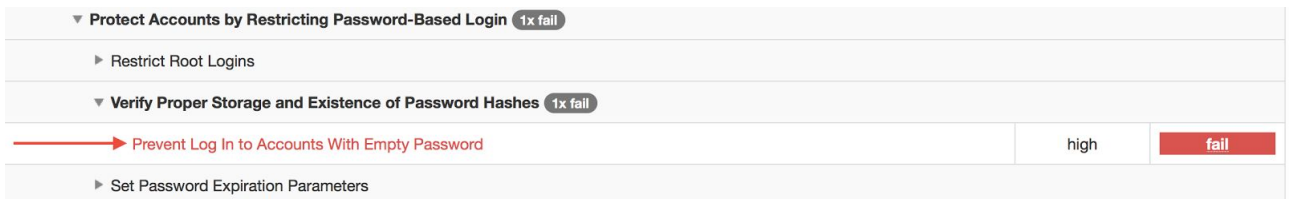
Reported at 2017-04-21 17:37:18 -0400

Severity	Message	Resource	Result
High	Ensure Red Hat GPG Key Installed 🔍	xccdf_org.ssgproject.content_...	pass
High	Ensure gpgcheck Enabled In Main Yum Configuration 🔍	xccdf_org.ssgproject.content_...	pass
High	Verify and Correct File Permissions with RPM 🔍	xccdf_org.ssgproject.content_...	fail
High	Verify File Hashes with RPM 🔍	xccdf_org.ssgproject.content_...	pass

Fix a specific SCAP scan failure, re-run the SCAP scan, and view the resulting scan report in Satellite 6

27. From the full report, Search for “**Prevent Log In to Accounts With Empty Password**” and notice that this “**Prevent Log In to Accounts With Empty Password**” rule fails with severity **high**.

28. Click on “**Prevent Log In to Accounts With Empty Password**”.



▼ Protect Accounts by Restricting Password-Based Login 1x fail

- ▶ Restrict Root Logins

▼ Verify Proper Storage and Existence of Password Hashes 1x fail

- ▶ **Prevent Log In to Accounts With Empty Password** high fail
- ▶ Set Password Expiration Parameters

29. You can see in the **Remediation script** section that you can fix this with the command:

Remediation script:

```
sed -i 's/^\<nullok\>//g' /etc/pam.d/system-auth
```

30. Go ahead and execute this command on the **RHEL 7 VM 1** host as **root**.

```
# sed -i 's/^\<nullok\>//g' /etc/pam.d/system-auth
```

31. Re-run the RHEL7_Standard compliance policy on this host with the Policy ID you found earlier in the `/etc/foreman/scap_client/config.yaml` file:

```
# foreman_scap_client X (where X is your Policy ID)
```

This will run the scap scan again, bzip the scan results, and upload the results to Satellite. Wait for the command to complete before continuing.

32. Go back to your Satellite UI and view your SCAP scan results report for your RHEL7_Standard compliance policy by navigating to **Hosts** → **Reports**.

The screenshot shows the Red Hat Satellite web interface. At the top, there is a navigation bar with the following items: Default Organization, Monitor, Content, Containers, Hosts, and Configure. The 'Hosts' menu is open, showing a list of options: All hosts, Discovered hosts, Content Hosts, Host Collections, New host, PROVISIONING SETUP (Architectures, Hardware models, Installation media, Operating systems), TEMPLATES (Partition tables, Provisioning templates, Job templates), and COMPLIANCE (Policies, SCAP contents, Reports). A red arrow points from the 'Reports' option in the 'COMPLIANCE' section to the 'Reports' link in the main content area.

33. Click on the report you just created by clicking on the **most recent** report for **rhel7vm1.summit.example.com** by clicking the link in the **Reported At** column (do not click the host link).

Compliance Reports

Host	Reported At	Passed	Failed
<input type="checkbox"/> rhel7vm1.summit.example.com	less than a minute ago	9	1
<input type="checkbox"/> rhel7vm1.summit.example.com	about 21 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 22 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	about 23 hours ago	0	0
<input type="checkbox"/> rhel7vm1.summit.example.com	1 day ago	0	0

34. Search for “**Prevent Log In to Accounts With Empty Password**” and notice now that this rule **passes** since the problem has been remediated.

Severity	Message	Resource	Result
High	Ensure Red Hat GPG Key Installed	xccdf_org.ssgproject.content_...	pass
High	Ensure gpgcheck Enabled In Main Yum Configuration	xccdf_org.ssgproject.content_...	pass
High	Verify and Correct File Permissions with RPM	xccdf_org.ssgproject.content_...	fail
High	Verify File Hashes with RPM	xccdf_org.ssgproject.content_...	pass
Low	Verify that All World-Writable Directories Have Sticky Bits Set	xccdf_org.ssgproject.content_...	pass
Medium	Ensure No World-Writable Files Exist	xccdf_org.ssgproject.content_...	pass
Low	Ensure All SGID Executables Are Authorized	xccdf_org.ssgproject.content_...	pass
Low	Ensure All SUID Executables Are Authorized	xccdf_org.ssgproject.content_...	pass
High	Prevent Log In to Accounts With Empty Password	xccdf_org.ssgproject.content_...	pass

35. Please do not attempt to remediate any other issues at this time.

Viewing the global status indicator in Satellite 6

Compliance status is one of the items that affect the global status of a system. In Satellite 6.2 (which you are using in this lab), we have the global status indicator, which is an aggregate of all the compliance states on the system. Specifically, in order to determine the global status, Satellite checks the status of: compliance with SCAP policies, configuration, errata, and subscription. Whichever is the worst status is what governs the overall status of the system. This is important to note since if you have a system that fails a SCAP policy finding, you’ll be able to see this quickly in the Satellite UI.

36. Take a look at the global status indicator by navigating to:

- Hosts** → **All Hosts** and then click on your client/host, which is **rhel7vm1.summit.example.com**.

The screenshot shows the Red Hat Satellite interface. The top navigation bar includes 'RED HAT SATELLITE', 'Default Organization', 'Monitor', 'Content', 'Containers', 'Hosts', 'Configure', 'Infrastructure', 'Red Hat Insights', and 'Administer'. The 'Hosts' dropdown menu is open, with 'All hosts' circled in red. Below the menu, a table lists hosts with columns for Name, Operating system, Model, Host group, Last report, and Actions. A red arrow points to the host 'rhel7vm1.summit.example.com' in the table.

Name	Operating system	Model	Host group	Last report	Actions
<input type="checkbox"/> cfme.summit.example.com	RedHat 7.3	Bochs			<input type="button" value="Edit"/>
<input type="checkbox"/> rhel7vm1.summit.example.com	RedHat 7.0	RHEV Hypervisor	base_with_puppet	15 minutes ago	<input type="button" value="Edit"/>
<input type="checkbox"/> rhel7vm2.summit.example.com	RedHat 7.0	RHEV Hypervisor			<input type="button" value="Edit"/>
<input type="checkbox"/> sat6.summit.example.com	RedHat 7.3	Bochs		18 minutes ago	<input type="button" value="Edit"/>

37. In the **Properties** box on the left of the Satellite UI, notice that the global **Status** indicator says Error due to failing the SCAP scan.

Properties	
Status	⊗ Error ←
Compliance	⊗ Incompliant
Configuration	☑ Active
Errata	⊗ Security errata applicable
Subscription	☑ Fully entitled

Lab 2: How to use the control policy engine in Red Hat CloudForms and Ansible Tower to enforce compliance with security policies

Goal of Lab 2

The goal of this lab is to introduce you to the power and flexibility of Red Hat CloudForms and Ansible Tower by Red Hat to enforce your security policies.

Specifically, using a combination of Red Hat CloudForms and Ansible Tower by Red Hat, you will identify and fix the Shellshock vulnerability in your system in an automated fashion.

The Shellshock vulnerability is the bash remote code execution vulnerability ([CVE-2014-6271](#)), which allows an attacker to gain control over a targeted computer if exploited successfully. Specifically, an attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Certain services and applications allow remote unauthenticated attackers to provide environment variables, allowing them to exploit this issue. If your system is vulnerable, you can fix these issues by updating to the most recent version of the Bash package available from Red Hat for Red Hat Enterprise Linux 5, 6, and 7.

Introduction

Red Hat CloudForms provides unified hybrid cloud management across your entire heterogeneous environment, including virtual, private cloud, public cloud, and container environments. Other supported technologies include software defined networking, middleware, and in the future storage management.

Red Hat CloudForms is an agentless solution, delivered as a virtual appliance, that is highly scalable and provides deep continuous visibility and discovery of your entire infrastructure. The Red Hat CloudForms control and policy engine provides compliance and governance capabilities right in the GUI of CloudForms. The Red Hat CloudForms automate engine can be utilized to execute free-form automation using either ruby or Ansible playbooks. Red Hat CloudForms is able to communicate directly to your Ansible Tower instance to execute your Ansible playbooks.

Ansible is a simple, powerful, and agentless IT automation technology that can help improve your current processes, migrate applications for better optimization, and provide a single language for DevOps practices across your organization including Developers, Operations, and the Security Team.

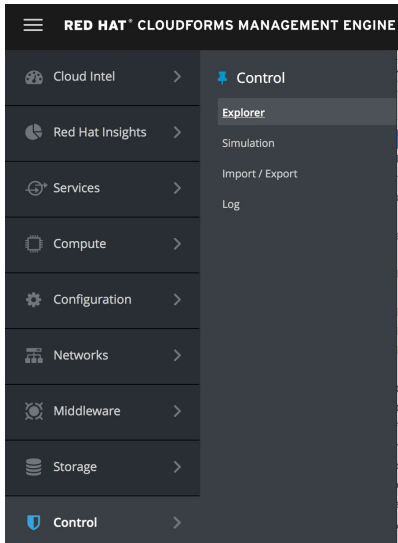
Ansible Tower by Red Hat provides a graphical user interface for Ansible with a visual dashboard, a centralized API for your Ansible automation, role-based access control for increased security, job scheduling, graphical inventory management, and real-time job status updates thus providing you all the IT automation features you need to support your enterprise.

Ansible is great for security automation because it is agentless, only requires SSH/WinRM, supports desired state, is extensible and modular, has a push-based architecture, and provides easy targeting based on facts.

Using the Red Hat CloudForms control engine and Ansible Tower by Red Hat to execute the Shellshock control policy and do remediation

1. If you have to log back in, go to your Firefox web browser and click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

2. In the Red Hat CloudForms UI, in the left pane, navigate to **Control** → **Explorer**.



3. In the **Policy Profiles** accordion, click **Demo: Shell-Shock Vulnerability**

Note: This policy profile has been created for you using the data collected by Red Hat CloudForms, such as the details of the installed packages. Also notice that this policy profile includes one VM and Instance Compliance policy named "Shell-Shock Vulnerability".

Policy Profiles

- > Compliance Hosts: November 2012
- > Compliance: DISA STIG
- > Compliance: DMZ Configuration
- > Compliance: Hosts
- > Compliance: RHEL Host (KVM)
- > Compliance: VM
- > Compliance: VMware Security Hard...
- > Compliance: VMware Security Hard...
- > Compliance: VMware Security Hard...
- > Demo: CPU Reservation
- > Demo: Prevent Cloning of Database ...
- > Demo: Prevent Cloning of Database ...
- > Demo: Prevent PowerOn of Quarant...
- > Demo: Service Level Resource Alloc...
- ▼ Demo: Shell-Shock Vulnerability >
 - ▼ VM and Instance Compliance: ...
 - ◆ Vulnerable bash Package (Sh...
 - > VM Compliance Check

Policy Profile "Demo: Shell-Shock Vulnerability"

Policies

- VM and Instance Compliance: Shell-Shock Vulnerability

Notes

No notes have been entered.

4. Click on this control policy by clicking on **VM and Instance Compliance: Shell-Shock Vulnerability**. You can expand the Policy Profiles accordion by clicking on the > button at the bottom.

The screenshot shows the 'Policy Profiles' sidebar on the left, with 'VM and Instance Compliance: Shell-Shock Vulnerability' selected and highlighted by a red circle. The main content area displays the details for this policy:

Policy "Shell-Shock Vulnerability"

Basic Information

- Active: Yes
- Created: By Username admin 2017-03-17 16:06:05 UTC

Scope

VM and Instance : OS Name INCLUDES "linux"

Conditions

Description	Scopes / Expressions
Vulnerable bash Package (ShellShock)	Exp[VM and Instance.Guest Applications : Name CONTAINS "bash" AND (FIND VM and res Instance.Guest Applications : Version = "4.1.2" CHECK ALL Release REGULAR EXPRESSION MATCHES "1[5][e]6_5.2[b e]6_5.1.sj[s:2(?)]e6_4.2" OR FIND VM and Instance.Guest Applications : Version = "4.2.46" CHECK ALL Release = "21.e17_3")]

Events

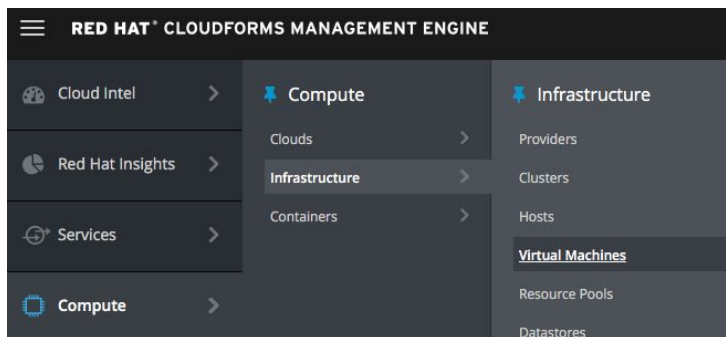
Description	Actions
VM Compliance Check	✗ Mark as Non-Compliant

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

Note: In this control policy, you are checking to see if the VM that this policy is assigned to has a particular package (in this case bash) with a particular version and release number installed. If this is found, this control policy will mark the VM as non-compliant.

5. Navigate to **Compute** → **Infrastructure** → **Virtual Machines**.

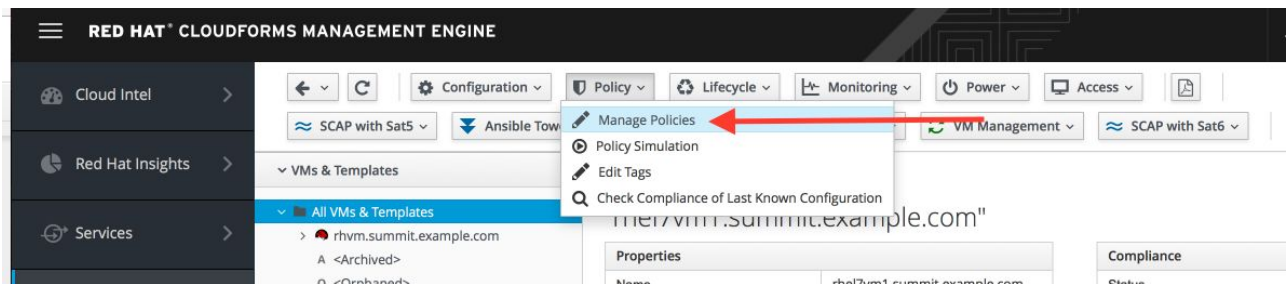


6. Navigate to your RHEL 7 VM 1 VM by **typing rhel7vm1.summit.example.com** in the search bar at the top right and then pressing the search icon. **Click on the rhel7vm1.summit.example.com VM.**

Note: You could have also hovered the VM icons to see their full name. Notice that the `rhel7vm1.summit.example.com` VM has a yellow shield on it. This means that a control policy is applied to this VM.



7. Take a look at the assigned control policies by navigating to **Policy** → **Manage Policies** at the top of the page.



8. Notice that there is a check box next to the **Demo: Shell-Shock Vulnerability** control policy profile. This means that this policy profile is assigned to this VM. Do not make any changes, click **Cancel**.

Virtual Machine Policy Assignment

Select 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: 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 ←
- > Demo: VM-Operation Policies
- > Demo: VMs in DMZ NIC Check
- > Demo: Windows Mandatory Patch
- > OpenSCAP profile
- > POC - Analysis: Manage VMs
- > POC - Analysis: Post Provisioning
- > Snapshots: Delete Based On Count
- > Snapshots: Max of 2
- > Tags: Location Tag Inheritance Policy

Save Reset Cancel

- Back in the VM summary page (which you should now be in), notice that in the top right there is a **Compliance** box and the **status** is shown is “**Non-Compliant as of...**”. Click on the **Status** field.

VM and Instance

"rhel7vm1.summit.example.com"

✔ Edit policy assignments was cancelled by the user
✕

Properties		Compliance	
Name	rhel7vm1.summit.example.com	Status	✕ Non-Compliant as of 9 Days Ago
Hostname	rhel7vm1.summit.example.com	History	↺ Available
IP Address	192.168.200.101	Power Management	
Container	🔥 redhat: 2 CPUs (2 sockets x 1 core), 1024 MB	Power State	🟢 on
Parent Host Platform	rhel	Last Boot Time	Sat, 22 Apr 2017 20:21:20 +0000
Platform Tools	N/A	State Changed On	Sat, 22 Apr 2017 20:23:03 +0000
Operating System	🔥 Red Hat Enterprise Linux Serv		

- Expand “**Compliance Check on:...**” → **Policy: Shell-Shock Vulnerability**

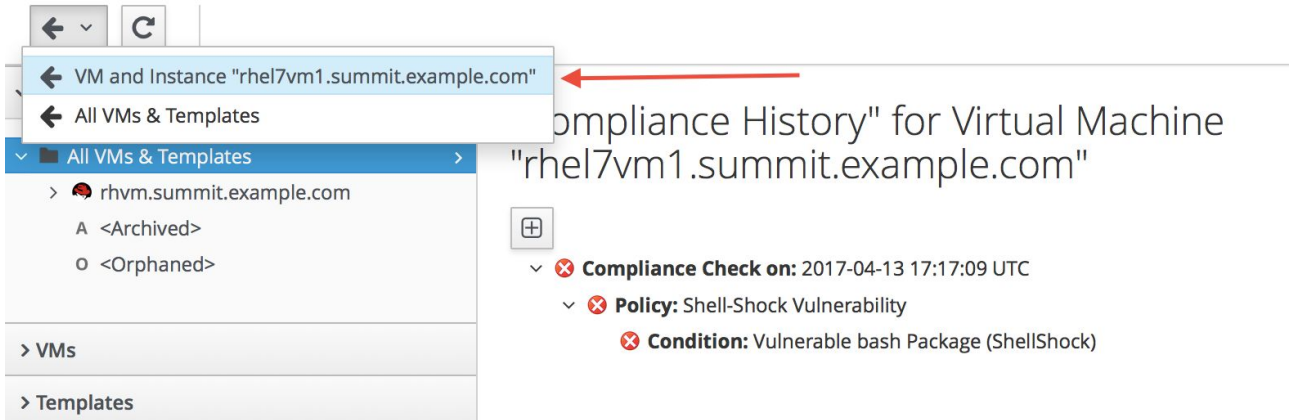
*Note: You can see that the **Shell-Shock Vulnerability** control policy has failed.*

"Compliance History" for Virtual Machine "rhel7vm1.summit.example.com"

+

- ✕ **Compliance Check on:** 2017-04-13 17:17:09 UTC
- ✕ **Policy:** Shell-Shock Vulnerability
- ✕ **Condition:** Vulnerable bash Package (ShellShock)

11. Go back to your VM by clicking the top back arrow button in the CloudForms UI (not the web browser) then Click on **VM and Instance "rhel7vm1.summit.example.com"**



12. In the VM summary page (which you should now be in), on the right side of the screen, take a look at the **Configuration** box. Notice that you can see the number of **Packages**, **Init Processes**, and **Files** installed on this VM.

VM and Instance
"rhel7vm1.summit.example.com"

Properties	
Name	rhel7vm1.summit.example.com
Hostname	rhel7vm1.summit.example.com
IP Address	192.168.200.101
Container	redhat: 2 CPUs (2 sockets x 1 core), 1024 MB
Parent Host Platform	rhel
Platform Tools	N/A
Operating System	Red Hat Enterprise Linux Server release 7.0 (Maipo)
Devices	4
CPU Affinity	
Snapshots	2
Advanced Settings	0
Resources	Available
Management Engine GUID	a3bf085c-206b-11e7-8ca9-2cc2603c6ac9

Compliance	
Status	Non-Compliant as of 9 Days Ago
History	Available

Power Management	
Power State	on
Last Boot Time	Sat, 22 Apr 2017 20:21:20 +0000
State Changed On	Sat, 22 Apr 2017 20:23:03 +0000

Security	
Users	28
Groups	47

Configuration	
Packages	368
Init Processes	152
Files	34

Lifecycle	
Discovered	Thu, 13 Apr 2017 17:07:13 +0000
Last Analyzed	Fri, 14 Apr 2017 01:06:52 +0000
Retirement Date	Never

Datastore Allocation Summary	
Number of Disks	1
Disks Aligned	Unknown
Thin Provisioning Used	True

Note: Using the SmartState Analysis functionality, Red Hat CloudForms has the ability to collect this deep OS level information, without using agents, by looking into the VM's disk image. The VM doesn't even need to be powered on to be analyzed.

13. Click on **Packages** in the **Configuration** box.

Note: Here, you can see a list of all the installed packages with version and release numbers of these packages. This is how Red Hat CloudForms knows whether or not you are vulnerable to Shellshock since it can easily see all this detailed information about what's installed in the VM's OS, including the version and release number for the bash package.

VM and Instance

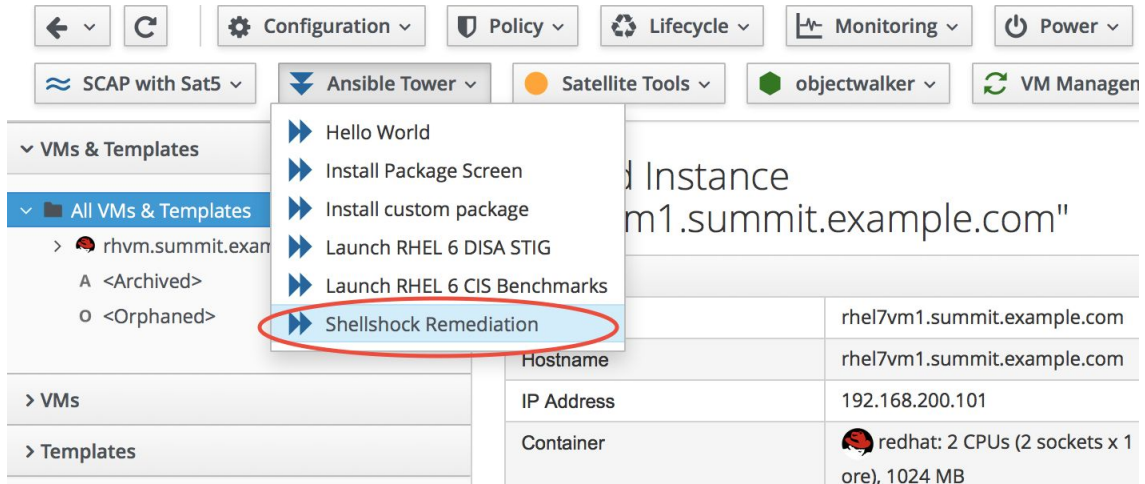
"rhel7vm1.summit.example.com"

Properties		Compliance	
Name	rhel7vm1.summit.example.com	Status	✘ Non-Compliant as of 9 Days Ago
Hostname	rhel7vm1.summit.example.com	History	✔ Available
IP Address	192.168.200.101	Power Management	
Container	redhat: 2 CPUs (2 sockets x 1 core), 1024 MB	Power State	▶ on
Parent Host Platform	rhel	Last Boot Time	Sat, 22 Apr 2017 20:21:20 +0000
Platform Tools	N/A	State Changed On	Sat, 22 Apr 2017 20:23:03 +0000
Operating System	Red Hat Enterprise Linux Server release 7.0 (Maipo)	Security	
Devices	4	Users	28
CPU Affinity		Groups	47
Snapshots	2	Configuration	
Advanced Settings	0	Packages	368 ←
Resources	Available	Init Processes	152
Management Engine GUID	a3bf085c-206b-11e7-8ca9-2cc2603c6ac9	Files	34

Note: We will now fix the Shellshock vulnerability for this VM by executing the Ansible playbook for Shellshock Remediation, directly from Red Hat CloudForms. Note that this playbook has already been pre-created for you. The Ansible Tower job template, which calls this playbook, has already been set up for you in Ansible Tower as well.

14. At the top of the Red Hat CloudForms UI, click on **Ansible Tower -> Shellshock Remediation**.

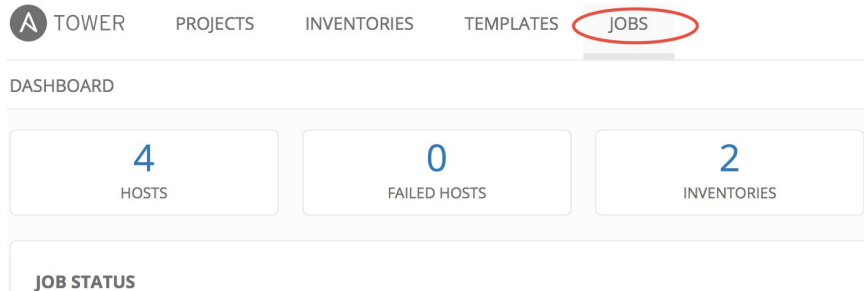
Note: This custom button will make Red Hat CloudForms schedule a job on Ansible Tower to execute the Ansible playbook for Shellshock remediation on this VM. This playbook simply updates the bash package by executing yum update bash on your system.



Now, let's take a look at Ansible Tower to see the status of the Shellshock remediation job we just executed.

15. In your Firefox web browser, click on the tab you have opened to your Ansible Tower UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

16. In the Ansible Tower UI, Click on **Jobs** at the top of the UI.



17. You should (eventually) see that your **Shellshock** Ansible playbook is being run.

JOBS

JOBS SCHEDULES

Search

ID	NAME	TYPE	FINISHED
461	Shellshock	Playbook Run	

18. Click the latest **Shellshock** job to see the progress and wait for the **STATUS** to show **Successful**

Note: Notice that this Shellshock Ansible playbook ran successfully on the `rhel7vm1.summit.example.com` VM.

TOWER PROJECTS INVENTORIES TEMPLATES JOBS admin

JOBS / 457 - SHELLSHOCK

DETAILS

STATUS: Successful

STARTED: 4/23/2017 9:55:06 PM

FINISHED: 4/23/2017 9:56:00 PM

TEMPLATE: Shellshock

JOB TYPE: Run

LAUNCHED BY: admin

INVENTORY: CloudForms

PROJECT: Red Hat Security Demos

REVISION: d85710555acf90c234398bc4ab38161d99916cf5

PLAYBOOK: ikerner/shellshock.yml

MACHINE CREDENTIAL: VMCredentials

FORKS: 0

LIMIT: rhel7vm1.summit.example.com

VERBOSITY: 0 (Normal)

EXTRA VARIABLES

```
1 ---
```

SHELLSHOCK PLAYS 1 TASKS 2 HOSTS 1 ELAPSED 00:00:54

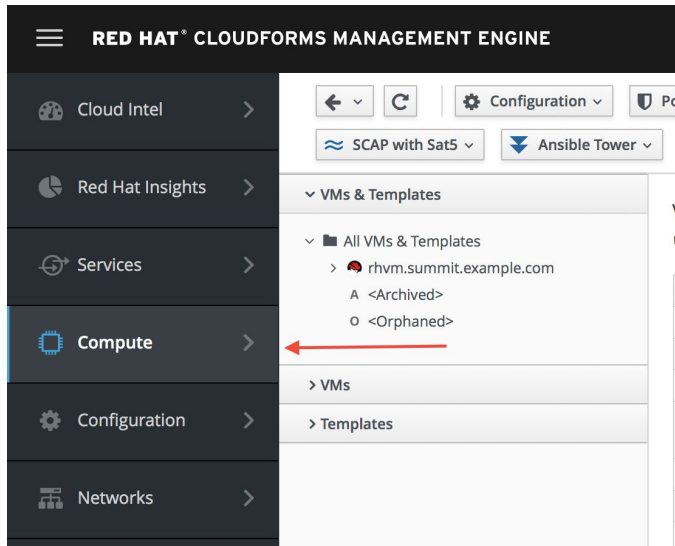
SEARCH KEY

```

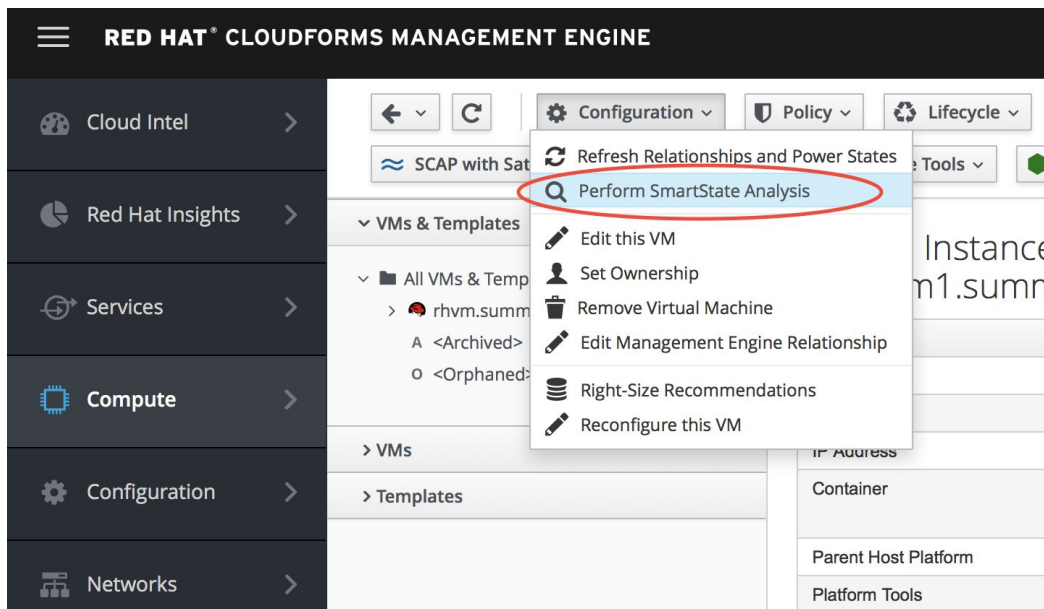
1 Identity added: /tmp/ansible_tower_nxE8vi/credential (/tmp/ansible_tower_nxE8vi/credential)
2 SSH password:
3
4 PLAY [Test and fix shellshock] ***** 21:55:27
5
6 TASK [setup] ***** 21:55:27
7 ok: [rhel7vm1.summit.example.com]
8
9 TASK [Update bash] ***** 21:55:39
10 changed: [rhel7vm1.summit.example.com]
11
12 PLAY RECAP ***** 21:55:58
13 rhel7vm1.summit.example.com : ok=2 changed=1 unreachable=0 failed=0
14
```

Now, let's go back to Red Hat CloudForms and confirm that your VM is remediated against the Shellshock vulnerability.

19. In the Red Hat CloudForms UI navigate to your **rhel7vm1.summit.example.com** VM (Clicking on **Compute** on the left side is a shortcut).

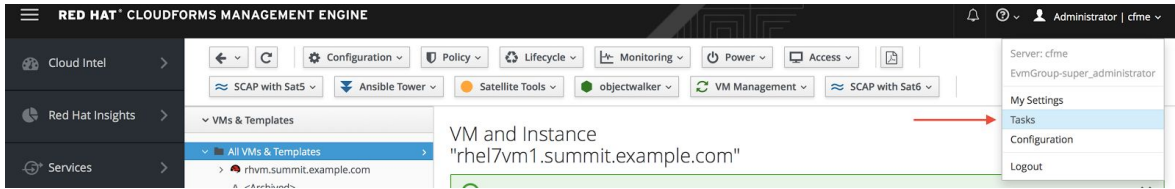


20. Re-scan the VM by clicking on **Configuration** → **Perform SmartState Analysis**.

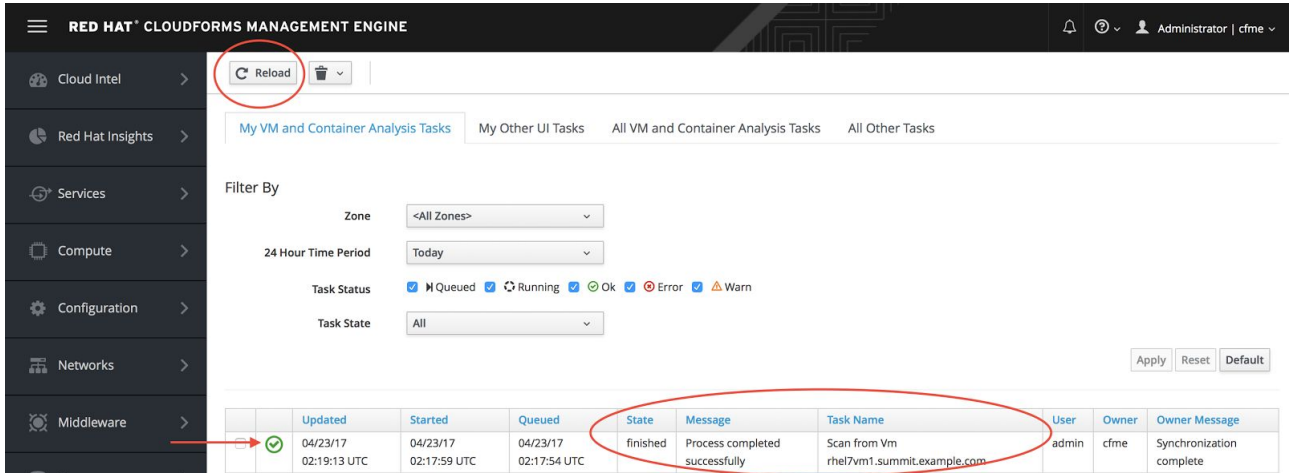


21. Click **OK**.

22. Click **Administrator | cfme** at the top right then click **Tasks**.

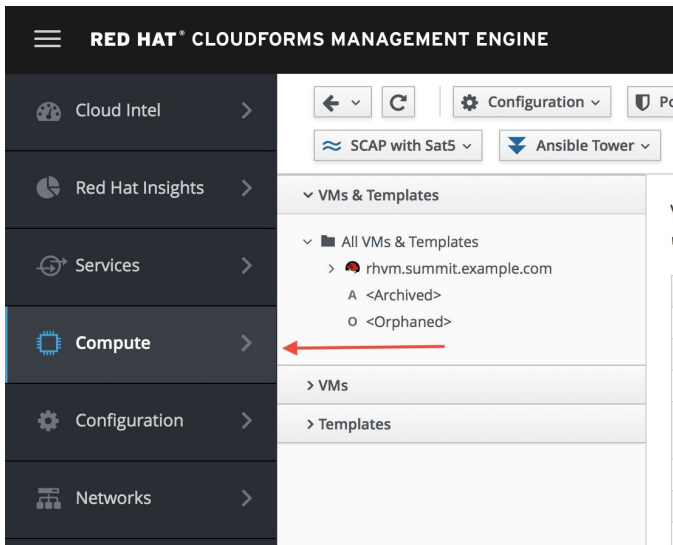


23. Click the circular **Reload** arrow in the Red Hat CloudForms UI (not the browser) until the **State** for the latest scanning job shows **finished** and you see a **green checkbox** icon on the left of the line. This will take a few minutes to complete.

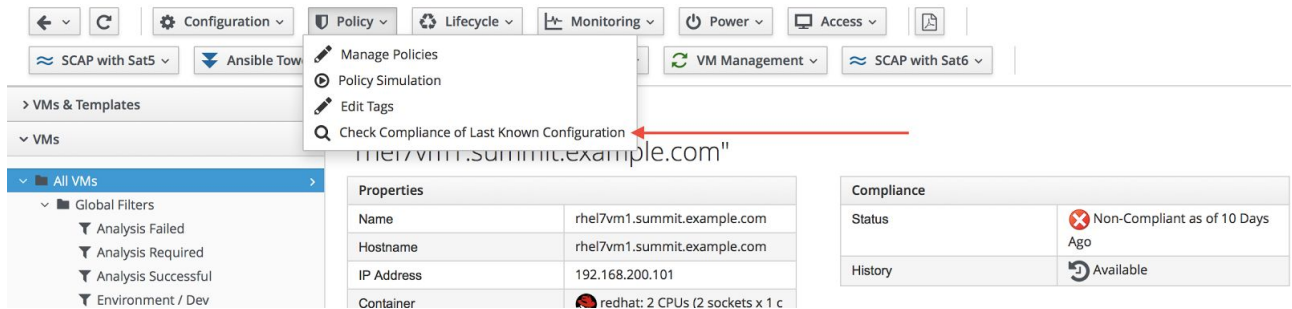


Now Red Hat CloudForms knows about the updated **bash** package.

24. In the Red Hat CloudForms UI navigate to your **rhel7vm1.summit.example.com** VM again (Clicking on **Compute** on the left side is a shortcut).



25. Click on **Policy** → **Check Compliance of Last Known Configuration**.

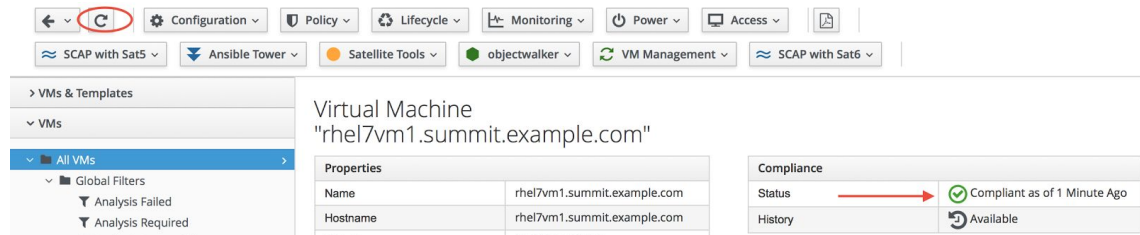


26. Click **OK**.

27. Click the **circular arrow** refresh button at the top left of the Red Hat CloudForms UI (not the browser) until the **Compliance** box -> **Status** line shows **Compliant**.

The **Status** should now come back as **Compliant** with a green check box for the Shellshock control policy.

Click on the **Status** field.



28. Expand "**Compliance Check on:...**" → **Policy: Shell-Shock Vulnerability**

*Note: You can see that the **Shell-Shock Vulnerability** control policy has now passed.*

"Compliance History" for Virtual Machine
"rhel7vm1.summit.example.com"



- ✓ **Compliance Check on:** 2017-04-23 11:19:28 UTC
 - ✓ **Policy:** Shell-Shock Vulnerability
 - ✓ **Condition:** Vulnerable bash Package (ShellShock)
- > ✗ **Compliance Check on:** 2017-04-13 17:17:09 UTC

Your VM is now remediated against the Shellshock vulnerability!

Lab 3: Managing the security of Red Hat Openshift container images from Red Hat CloudForms

Goal of Lab 3

The goal of this lab is demonstrate how you can use Red Hat CloudForms to manage the security of Red Hat Openshift container images. Specifically, we will see how you can use the Red Hat CloudForms control engine to prevent Red Hat Openshift container images with high severity vulnerabilities from running in Red Hat Openshift.

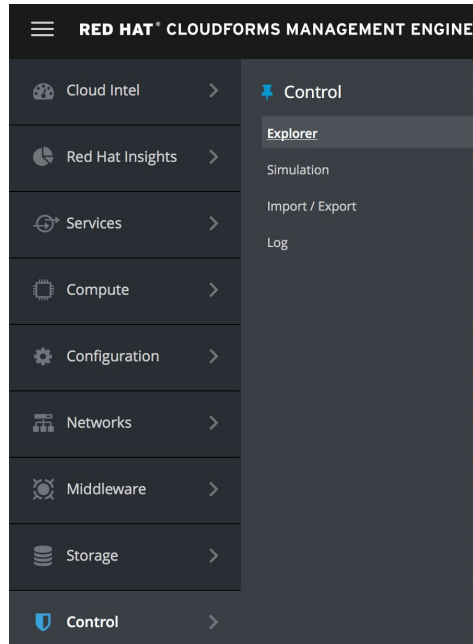
Introduction

Red Hat CloudForms has a container scanning feature that allows Red Hat CloudForms to flag images in the container registry in which it has found vulnerabilities. Specifically, Red Hat CloudForms can apply an annotation to an image in the OpenShift container registry when it finds high severity vulnerabilities after doing a scan on it. Then, Red Hat Openshift will prevent new containers from running this image with the high severity vulnerabilities.

Red Hat CloudForms has multiple ways a container image scan can be initiated: scheduled scan of the registry, scan based on a newly discovered image in the registry, or a manual execution of the scan via smart state analysis. Having this scanning feature with native integration in Red Hat Openshift allows for near real time monitoring of your images within the Red Hat Openshift environment. Once Red Hat CloudForms flags an image in the registry, the next time someone tries to start the vulnerable image, Red Hat Openshift will alert the user that the image execution was blocked based on the policy annotation set by Red Hat CloudForms.

Preventing Red Hat Openshift container images with high severity vulnerabilities from running in Red Hat Openshift using Red Hat CloudForms

1. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. If you are not already logged in, log back in with **admin** as the username and **r3dh@t2017** as your password.
2. In the Red Hat CloudForms UI, in the left pane, navigate to **Control** → **Explorer**.



3. Then in the left pane, click on **Policy Profiles** → **OpenSCAP profile** to see the **OpenSCAP profile** control policy profile.

Note: Notice that this control policy profile has 3 control policies in it.:

- *Container Image Compliance: OpenSCAP*
- *Container Image Control: Analyse incoming container images*
- *Container Image Control: Schedule compliance after smart state analysis.*

Policy Profile "OpenSCAP profile"

Policies

- Container Image Compliance: OpenSCAP
- Container Image Control: Analyse incoming container images
- Container Image Control: Schedule compliance after smart state analysis

Notes

No notes have been entered.

Next, you can Optionally take a look at these 3 control policies in the 3 next steps.

4. (Optional) Click on **Container Image Compliance: OpenSCAP**.

Note: Notice that during a compliance check, this control policy checks to see if the OpenSCAP rule results include any severity high failures. If so, Red Hat CloudForms marks this container image as non-compliant and prevents this container image from running in Red Hat OpenShift ever again.

Policy "OpenSCAP"

Basic Information

Active: Yes

Created: By Username admin 2017-03-11 05:36:17 UTC

Scope

No Policy scope defined, the scope of this policy includes all elements.

Conditions

Description	Scopes / Expressions
Has high severity OpenSCAP rule results	Express FIND Container Image.Openscap Rule Results : Result = "fail" Condition ECK ANY Severity = "High"

Events

Description	Actions
Container Image Compliance Check	<ul style="list-style-type: none"> Mark as Non-Compliant Prevent container image from running on OpenShift

5. (Optional) Now click on **Container Image Control: Analyse incoming container images**.

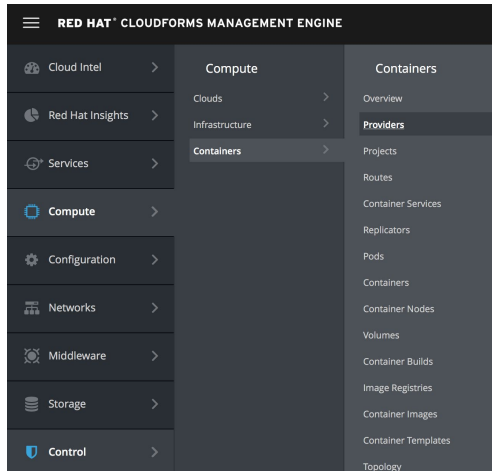
Note: In this control policy, whenever a new container image is discovered, a smart state analysis scan is done on the new container image. This way, Red Hat CloudForms knows exactly what is in the newly discovered container image.

The screenshot shows the Red Hat CloudForms Policy Profiles interface. On the left, a tree view lists various policy profiles. A red arrow points to the profile 'Container Image Control: Analyse incoming container images', which is highlighted in blue. On the right, the configuration details for this policy are shown. The title 'Policy "Analyse incoming container images"' is circled in red. The 'Basic Information' section shows the policy is 'Active' and was 'Created' by 'Username admin' on '2017-03-11 05:36:17 UTC'. The 'Scope' section indicates 'No Policy scope defined, the scope of this policy includes all elements.' The 'Conditions' section shows a single condition: 'Don't scan image-inspector's image' with the expression 'Container Image : Name ENDS WITH "/>

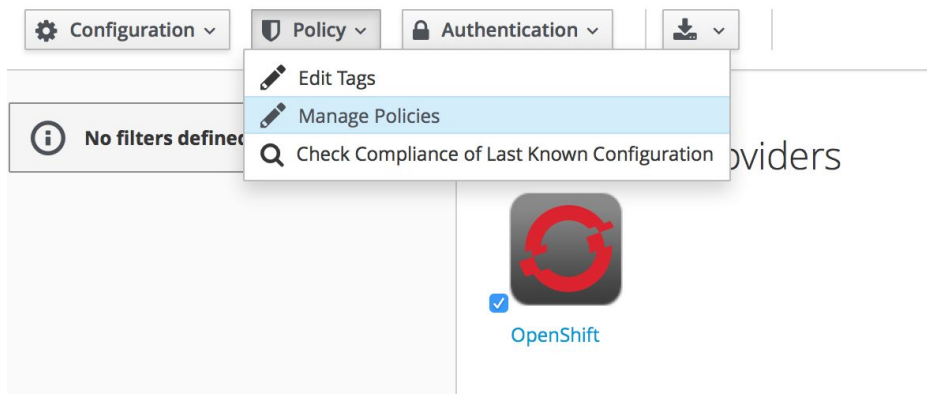
6. (Optional) When the container image smart state analysis is complete, the Host or VM compliance is then checked as you can see from the last control policy, **Container Image Control: Schedule compliance after smart state analysis.**

The screenshot shows the Red Hat CloudForms Policy Profiles interface. On the left, a tree view lists various policy profiles. A red arrow points to the profile 'Container Image Control: Schedule compliance after smart state a...', which is highlighted in blue. On the right, the configuration details for this policy are shown. The title 'Policy "Schedule compliance after smart state analysis"' is circled in red. The 'Basic Information' section shows the policy is 'Active' and was 'Created' by 'Username admin' on '2017-03-11 05:36:18 UTC'. The 'Scope' section indicates 'No Policy scope defined, the scope of this policy includes all elements.' The 'Conditions' section shows 'No conditions defined. This policy is unconditional and will ALWAYS return true.' The 'Events' section shows a single event: 'Container Image Analysis Complete' with the action 'Check Host or VM Compliance'.

7. Now, in the Red Hat CloudForms UI, in the left pane, navigate to **Compute** → **Containers** → **Providers**.



8. Check the box next to the OpenShift Container Provider and click on **Policy** → **Manage Policies**.



*Note: After clicking on **Policy** → **Manage Policies**, notice that there is a checkbox next to the **OpenSCAP profile** policy profile . This means that the **OpenSCAP profile** policy profile is assigned to this Red Hat OpenShift provider, which means that all container images in this OpenShift container provider will have this policy profile applied.*

9. At the bottom right, Click **Cancel**.

- > Demo: Windows Mandatory Patch
- > OpenSCAP profile
- > POC - Analysis: Manage VMs
- > POC - Analysis: Post Provisioning
- > Snapshots: Delete Based On Count
- > Snapshots: Max of 2
- > Tags: Location Tag Inheritance Policy

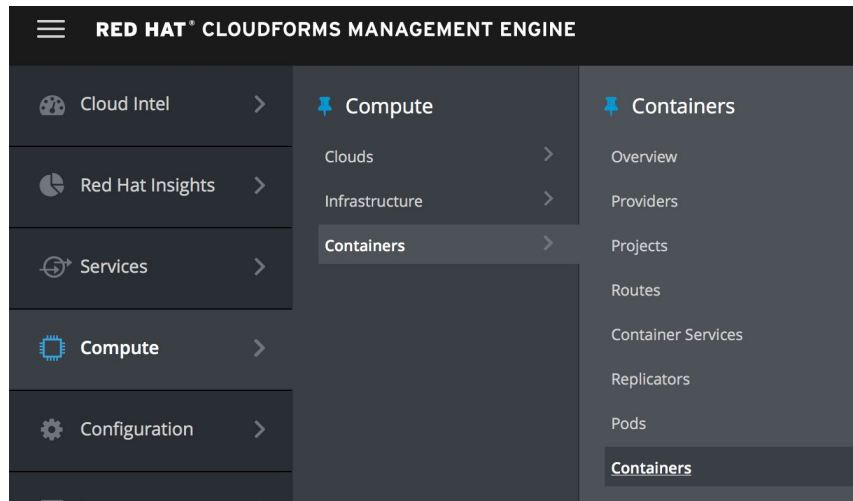
Save **Cancel**

Policy changes will affect 1 Containers Provider

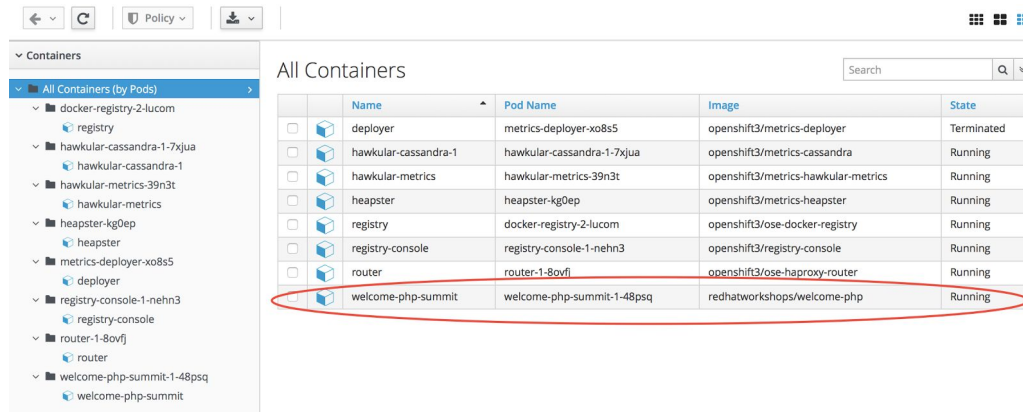


OpenShift

10. Next, in the Red Hat CloudForms UI, in the left pane, navigate to **Compute** → **Containers** → **Containers**.



11. Click on the **welcome-php-summit** container.



12. In the **Relationships** box, click on Container Image **redhatworkshops/welcome-php**

Container "welcome-php-summit" (Summary)

Properties		Relationships	
Name	welcome-php-summit	Containers Provider	OpenShift
State	running	Project	summit-demo
Last State	terminated	Replicator	welcome-php-summit-1
Restart count	12	Pod	welcome-php-summit-1-48psq
Backing Ref (Container ID)	docker://de1284cb12a67e4523906d227988606f545d6064788b403c99f7e22558b2cc85	Node	ocp.summit.example.com
Drop Capabilities	KILL,MKNOD,SETGID,SETUID,SYS_CHROOT	Container Image	redhatworkshops/welcome-php
Privileged	false	Smart Management	
Run As User	1000060000	Red Hat Summit Tags	No Red Hat Summit Tags have been assigned
SELinux Level	s0:c8,c2		

- In the **Configuration** box, notice that you can see the **Packages** and **OpenSCAP** results. Click on **OpenSCAP** results.

Note: Notice that there are several severity high security rule failures.

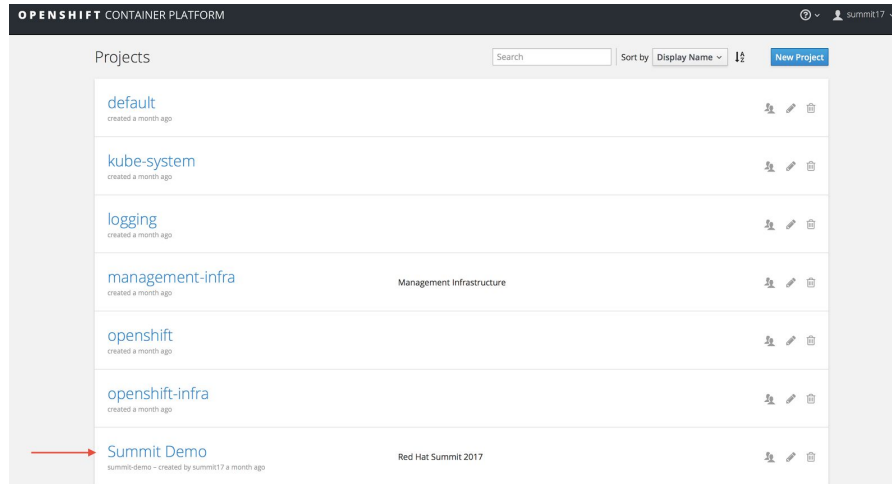
Containers > redhatworkshops/welcome-php (Summary)

redhatworkshops/welcome-php (Summary)

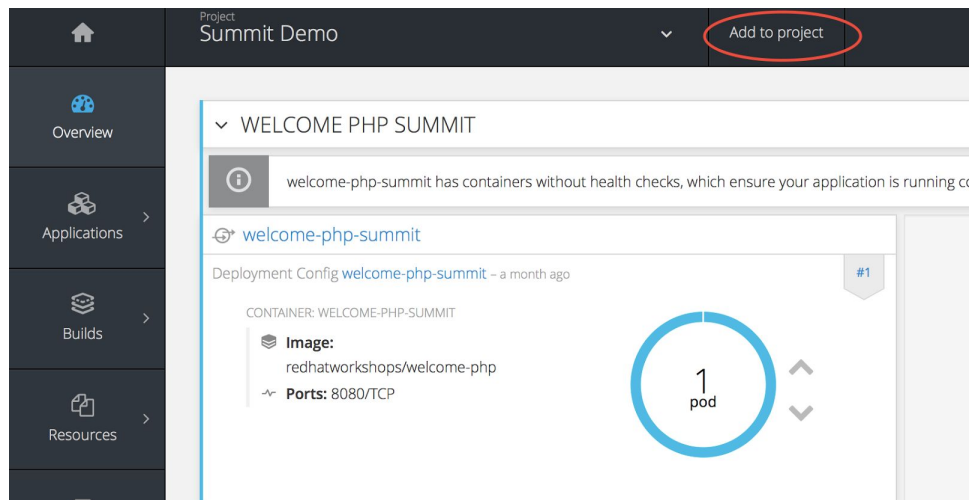
Properties		Relationships	
Name	redhatworkshops/welcome-php	Containers Provider	OpenShift
Image Id	docker-pullable://docker.io/redhatworkshops/welcome-php@sha256:d5e66730d05c332503abf9a1f5ce7b6d9c49373f098342fcc9d3249be308bc2b	Image Registry	Unknown image source
Full Name	redhatworkshops/welcome-php@sha256:d5e66730d05c332503abf9a1f5ce7b6d9c49373f098342fcc9d3249be308bc2b	Projects	1
Operating System Distribution	redhat	Pods	1
Product Type	Linux	Containers	1
Product Name	Red Hat Enterprise Linux Server release 7.3 (Maipo)	Nodes	1
Architecture		Smart Management	
Author		Red Hat Summit Tags	No Red Hat Summit Tags have been assigned
Command		Configuration	
Endpoint		Packages	313
		OpenSCAP Results	431
		OpenSCAP HTML	Available
		Last scan	Thu, 23 Mar 2017 23:28:07 +0000

- Now , in your Firefox web browser, click on the tab you have opened to your Red Hat Openshift UI. Log back in with **summit17** (NOT admin) as the username and **r3dh@t2017** as your password.

- Click on the **Summit Demo** Project.



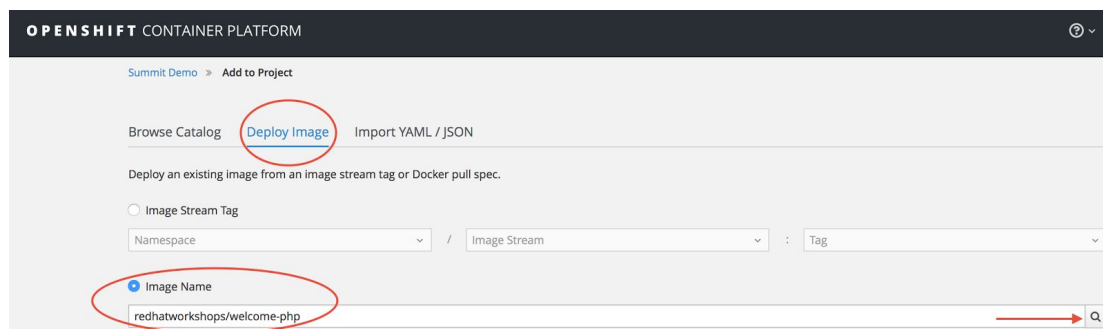
16. At the top of the Red Hat Openshift UI, click on **Add to Project**.



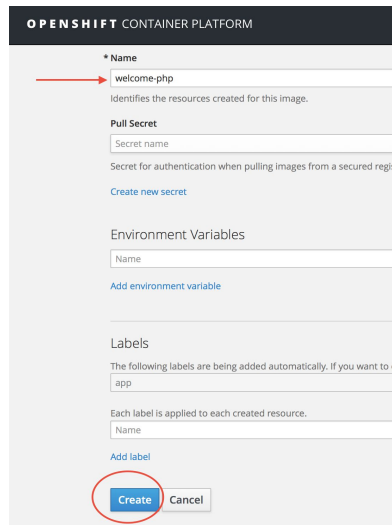
17. Click on **Deploy Image**, which is the middle tab at the top of the UI.

18. Select **Image Name** and type redhatworkshops/welcome-php and hit enter or search glass.

Note: This will search and pull back metadata for the image.



19. For the **Name**, type **welcome-php**. Then at the bottom, click **Create**.



OPENSIFT CONTAINER PLATFORM

* Name
welcome-php
Identifies the resources created for this image.

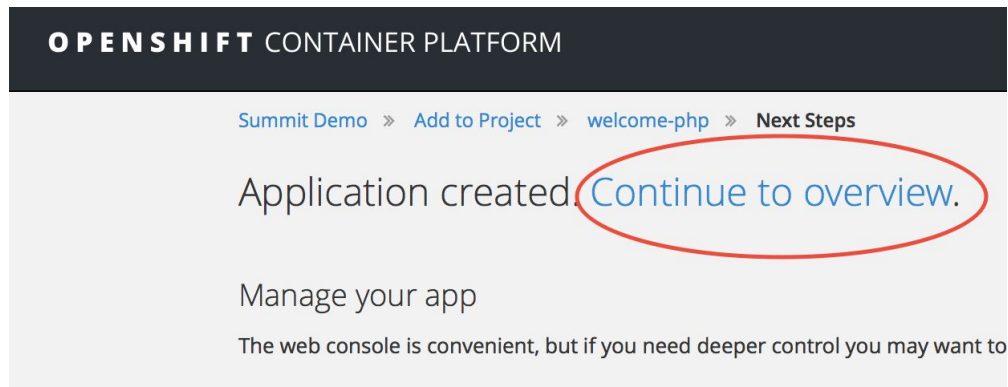
Pull Secret
Secret name
Secret for authentication when pulling images from a secured registry
[Create new secret](#)

Environment Variables
Name
[Add environment variable](#)

Labels
The following labels are being added automatically. If you want to customize, click [Add label](#).
app
Each label is applied to each created resource.
Name
[Add label](#)

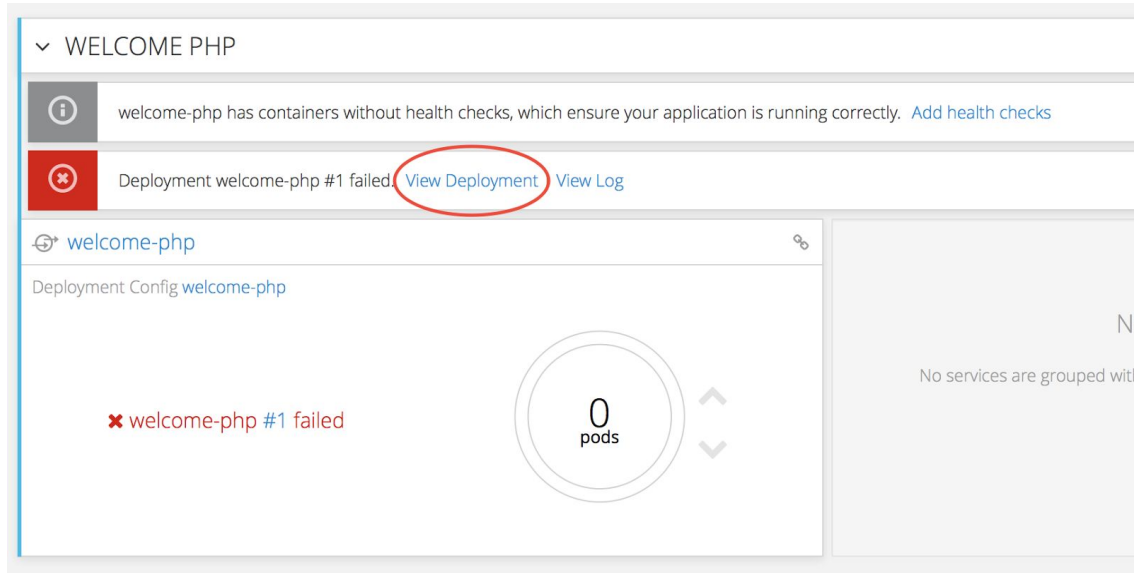
[Create](#) [Cancel](#)

20. Click on **Continue to overview**. Wait a few mins for the deployment to finish.



Note: Red Hat OpenShift will try to spin up the app, but ultimately the deployment will fail.

21. To see this, from the Overview page (which you should now be on), click on **View Deployment**.



22. Then, click on the **Events** tab.

[Deployments](#) » [welcome-php](#) » #1

welcome-php-1 created 5 minutes ago

[app](#) [welcome-php](#) [openshift.io/deployment-config.name](#) [welcome-php](#)

[Details](#) [Environment](#) [Metrics](#) [Logs](#) [Events](#)

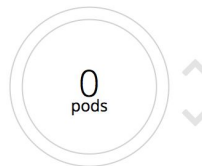
Status: × Failed

Deployment config: [welcome-php](#)

Status reason: image change

Selectors: app=welcome-php
deployment=welcome-php-1
deploymentconfig=welcome-php

Replicas: 0 current / 0 desired



Template

23. After clicking the **Events** tab, you will see “**Failed create**” as the Reason and “**Error creating: Pod "" is invalid: spec.containers[0].image: Forbidden: this image is prohibited by policy**” as the Message.

Note: Since Red Hat CloudForms flagged this image in the registry due to the high severity vulnerabilities in this image, when you try to start a container with this vulnerable image, Red Hat OpenShift is alerting you that this image execution is being blocked based on the policy annotation set by Red Hat CloudForms.

Deployments > welcome-php > #1

welcome-php-1 created 8 minutes ago

app welcome-php openshift.io/deployment-config.name welcome-php

Details Environment Metrics Logs **Events**

Filter by keyword Sort by Time ↓

Time	Reason	Message
8:45:10 AM	⚠ Failed create	Error creating: Pod "" is invalid: spec.containers[0].image: Forbidden: this image is prohibited by policy 16 times in the last 7 minutes

Lab 4: OpenSCAP security scans and remediations at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Satellite 5.7

Goal of Lab 4

The goal of this lab is to show the ability to execute OpenSCAP security scans and remediations at the push of a button in Red Hat CloudForms with the custom integration of Red Hat CloudForms and Red Hat Satellite 5.7.

Introduction

Red Hat CloudForms has a powerful and flexible automate engine , which can be used to integrate Red Hat CloudForms with any 3rd party software product that has a web service API , such as REST. In this lab, you will see how integrating Red Hat CloudForms with Red Hat Satellite 5.7,using the Satellite 5.7 OpenSCAP APIs, allows you to execute OpenSCAP scans and remediations at the push of a button on a particular VM using Red Hat CloudForms.

Executing the OpenSCAP scan on a VM from a custom button in Red Hat CloudForms will cause Red Hat CloudForms to communicate with Red Hat Satellite 5.7 via the OpenSCAP API in Satellite 5.7. As a result, Satellite 5.7 will execute the OpenSCAP scan commands and send the scan results back to Red Hat CloudForms. Then, Red Hat CloudForms can take any specific actions based on the scan results. For example, in this lab, when a scan of a chosen SCAP profile fails even one rule in the profile, Red Hat CloudForms will tag the scanned VM as SCAP non-compliant with the name of the profile and automatically open an incident ticket in ServiceNow. However,

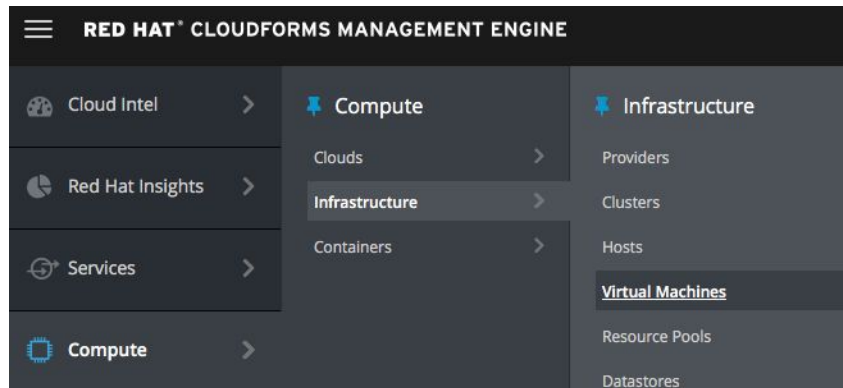
when a scan of a given SCAP profile passes all the rules in the profile, Red Hat CloudForms will simply tag the scanned VM as SCAP compliant with the name of the profile.

Similarly, executing the OpenSCAP remediation of a chosen profile on a VM from a custom button in Red Hat CloudForms will cause Red Hat CloudForms to ssh into the client VM to execute the OpenSCAP command for remediation.

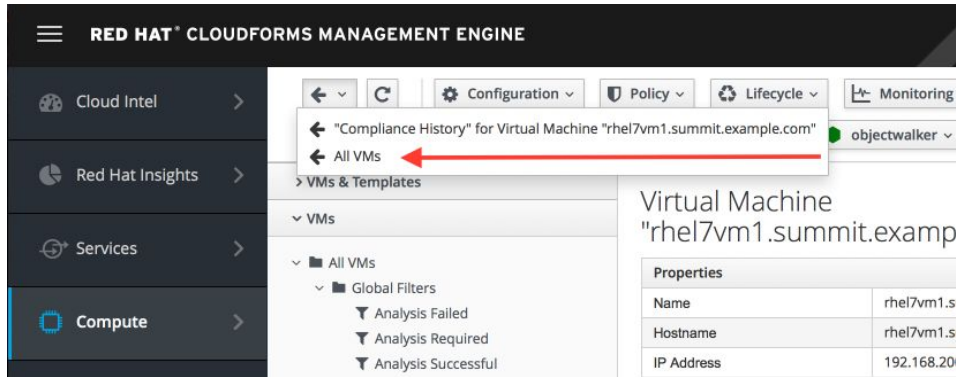
This integration between Red Hat CloudForms and Red Hat Satellite allows you to have a central and automated way to do point in time security compliance scans and remediations on a per-vm basis.

OpenSCAP security scan on a VM at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Red Hat Satellite 5.7

1. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
2. In the Red Hat CloudForms UI, in the left pane, navigate to **Compute** → **Infrastructure** → **Virtual Machines**.



3. If you end up in a VM summary page, click the back arrow button in the Red Hat CloudForms UI and click on **All VMs**.



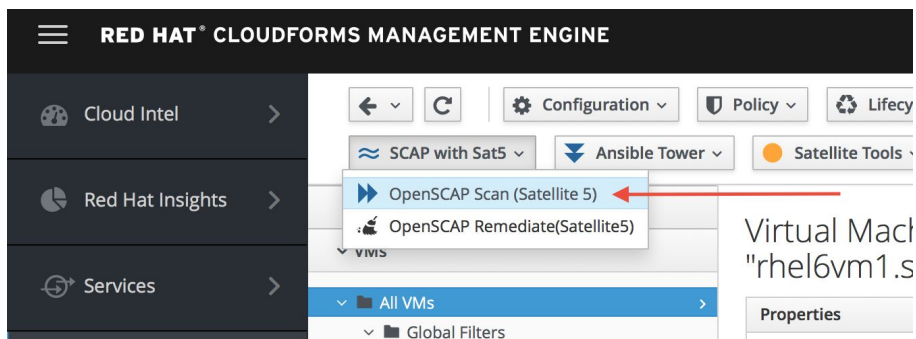
4. Navigate to your RHEL 6 VM 1 VM by **typing rhel6vm1.summit.example.com** in the search bar at the top right and then pressing the search icon. **Click on the rhel6vm1.summit.example.com VM.**

Note: You could have also hovered the VM icons to see their full name.

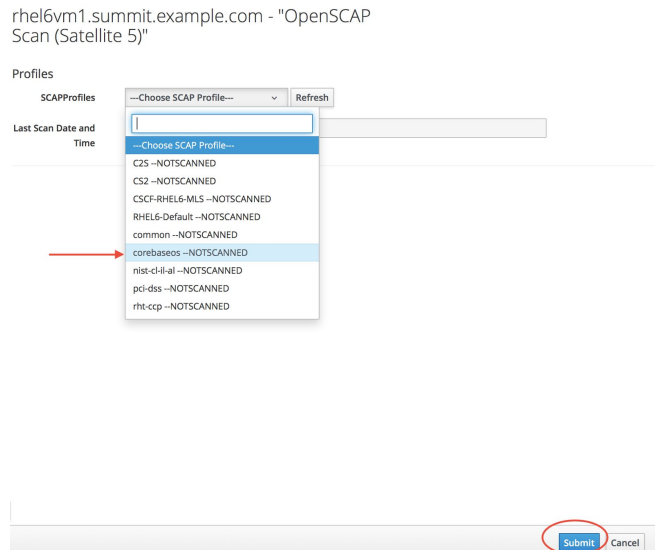
All VMs (Names with "rhel6vm1.summit.example.com")



5. Now, at the top, Click on the **SCAP with Sat5** button and Click on **OpenSCAP Scan (Satellite 5)**.

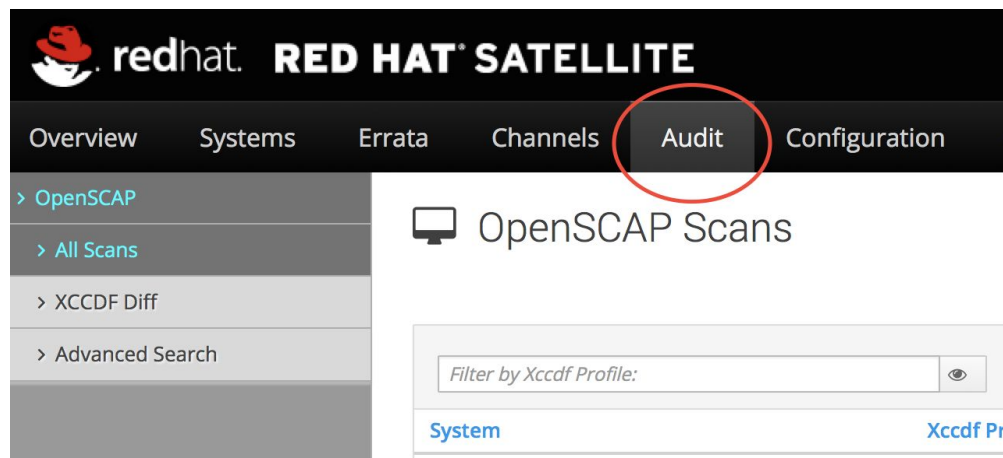


- Next, in the dialog window, for **SCAPProfiles**, choose the **corebaseos** profile. After choosing the **corebaseos** profile, press **Submit**.

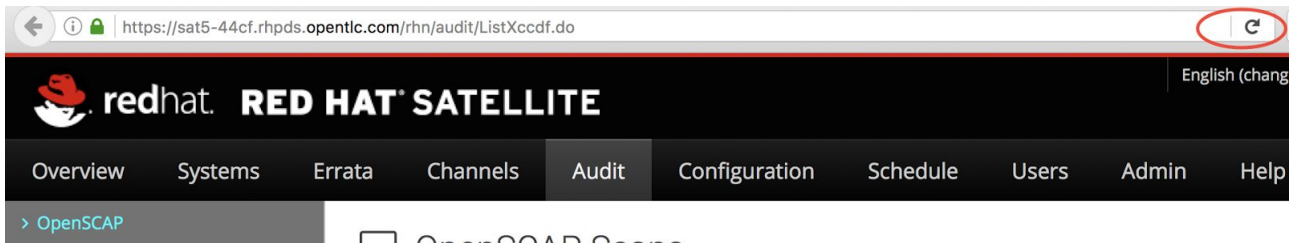


*Note: This is a simple profile that checks just one rule: The aide package must be installed. Also, notice that next to each profile name, you can see the status of its last scan (pass, failed, or not scanned). Also, notice that you can also see the **Last Scan Date and Time**. This shows you when this VM was last scanned.*

- Now, let's see if this profile fails or passes. In your Firefox web browser, click on the tab you have opened to your Red Hat Satellite 5.7 UI. Log back in with **admin** as the user name and **r3dh@t2017** as your password.
- In the Red Hat Satellite 5.7 UI, navigate to the top "**Audit**" tab.



- After a few minutes, you should see your completed OpenSCAP scan in the completed scan list. Press the refresh button on your web browser.



10. In the second Xccdf Profile column, Click on the **corebaseos** profile from the top of the list with today' date and current time, as indicated in the third Completed column.

OpenSCAP Scans

System	Xccdf Profile	Completed	Satisfied	Dissatisfied
rhel6vm1.summit.example.com	corebaseos	Sun Apr 23 09:28:48 EDT 2017	0	1

Details of XCCDF Scan

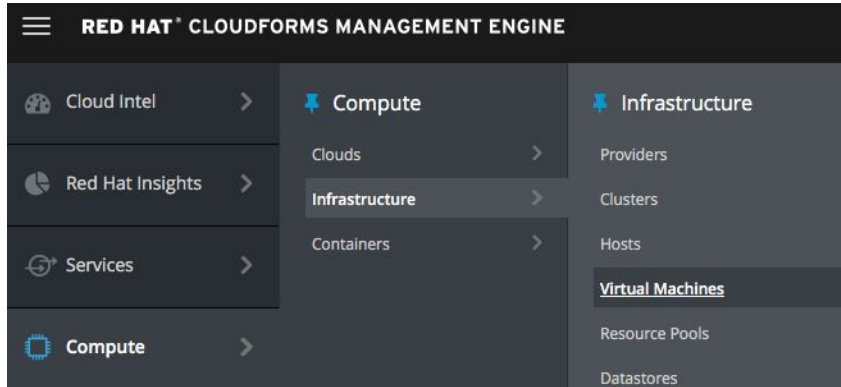
Scan ID (xid):	23
File System Path:	/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
Command-line Arguments:	--profile corebaseos
Scheduled By:	admin
Benchmark Identifier:	RHEL-6
Benchmark Version:	0.1.28
Profile Identifier:	corebaseos
Profile Title:	Common Profile for General-Purpose Systems
Started:	2017-04-23 09:28:30.0
Completed:	2017-04-23 09:28:32.0
Scan's Error output:	WARNING: Skipping http://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml file which is referenced from XCCDF c xccdf_eval: oscap tool returned 2

XCCDF Rule Results

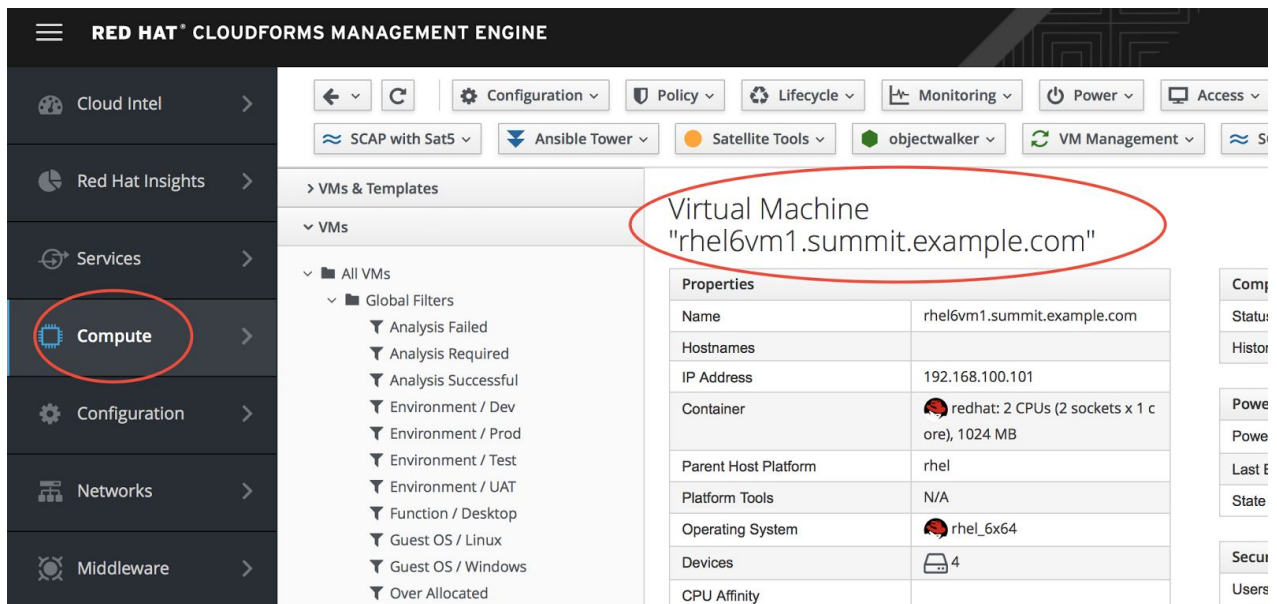
XCCDF Rule Identifier	XCCDF Ident Tags	Result
package_aide_installed	CCE-27024-9, DISA FSO RHEL-06-000016	fail

*Note: As stated earlier, this corebaseos profile just checks to see if the aide package is installed. As you can see, the result is **fail**, which means that the aide package is not installed on this VM.*

11. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
12. Then, navigate to **Compute** → **Infrastructure** → **Virtual Machines**.



13. You should be at the VM summary page for the **rhel6vm1.summit.example.com** VM.



14. At the VM summary page, take a look at the bottom right of the VM summary page in the **Smart Management** box. Notice that in the Red Hat Summit Tags, you have a tag named **scap_noncompliant: corebaseos**. If you don't see this tag yet, Click the circular **Reload** arrow In the Red Hat CloudForms UI (not the browser).

The screenshot displays the Red Hat CloudForms Management Engine interface. The left sidebar shows navigation options: Cloud Intel, Red Hat Insights, Services, Compute, Configuration, Networks, and Middleware. The main content area is divided into several sections:

- VMs & Templates:** A tree view showing 'All VMs' and 'Global Filters' with sub-items like 'Analysis Failed', 'Analysis Required', etc.
- Relationships:** A table listing various relationships for the VM, such as Infrastructure Provider (rhvm.summit.example.com), Cluster (Default), Host (kvm.summit.example.com), Resource Pool (Default for Cluster Default), Datastores (vmstore), Service (None), Genealogy (Show parent and child VMs), Drift History (None), and Analysis History (None).
- VMsafe:** A table with 'Enable' set to 'false'.
- Smart Management:** A table with 'Red Hat Summit Tags' and a value 'scap_noncompliant: corebaseos' circled in red.

Note: Upon failure of the corebaseos profile OpenSCAP scan , Red Hat CloudForms will auto-tag the VM with a SCAP non-compliant tag with the name of the failed corebaseos profile. In this integration, Red Hat CloudForms also automatically opens up an incident ticket in ServiceNow. This way, you can automatically keep track of which VMs are failing OpenSCAP scans by profile name.

- Refresh the VM summary page of your **rhel6vm1.summit.example.com** VM. Notice that at the bottom of this page, in the **Custom Attributes** box, a ServiceNow incident ticket number has been assigned in the custom attributes of this VM.

Custom Attributes	
servicenow_incident_sysid	fbe81af34fc6320091938ab18110c78b
servicenow_incident_number	INC0010033
lastendscancime	2017-04-23 09:28:32 UTC

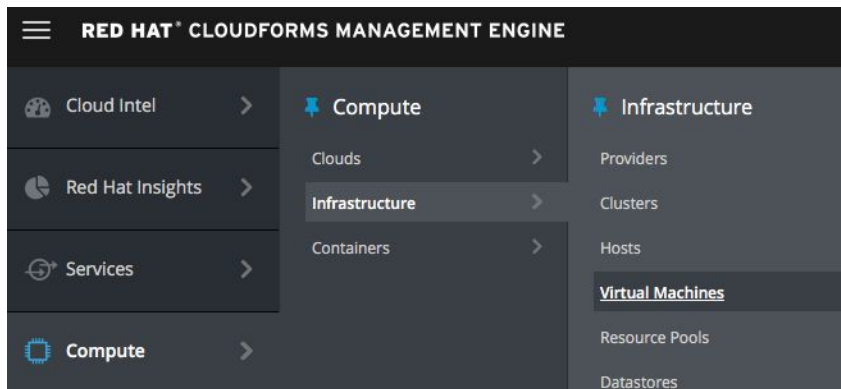
Note: Red Hat CloudForms has automatically opened up an incident ticket for you in ServiceNow, with this ticket number, and has passed to ServiceNow all the relevant details about this VM, such as the VM's IP address, how the VM was sized, etc.

16. To verify that the aide package is not installed on this VM, simply SSH into the rhel6vm1.summit.example.com and check. To login to your client VM, first SSH into your workstation node at workstation-<GUID>.rhpds.opentlc.com as the summit17 user. The summit17 user has sudo privileges. An ssh key is already in the home directory of your laptop, which should allow you to login without a password. Should a password be required, use r3dh@t2017 as your password.
\$ ssh summit17@workstation-<GUID>.rhpds.opentlc.com
17. Next, now that you are in the workstation node, SSH into your RHEL 6 client/host. This host has already been registered to both Red Hat Satellite 6 and Red Hat Insights for you.
\$ ssh summit17@rhel6vm1.summit.example.com
18. Now, see if the aide package is installed:
\$ rpm -qa aide
Note: Notice that the aide package is not installed.
19. Keep your terminal window open so that you remain logged into the rhel6vm1.summit.example.com VM.

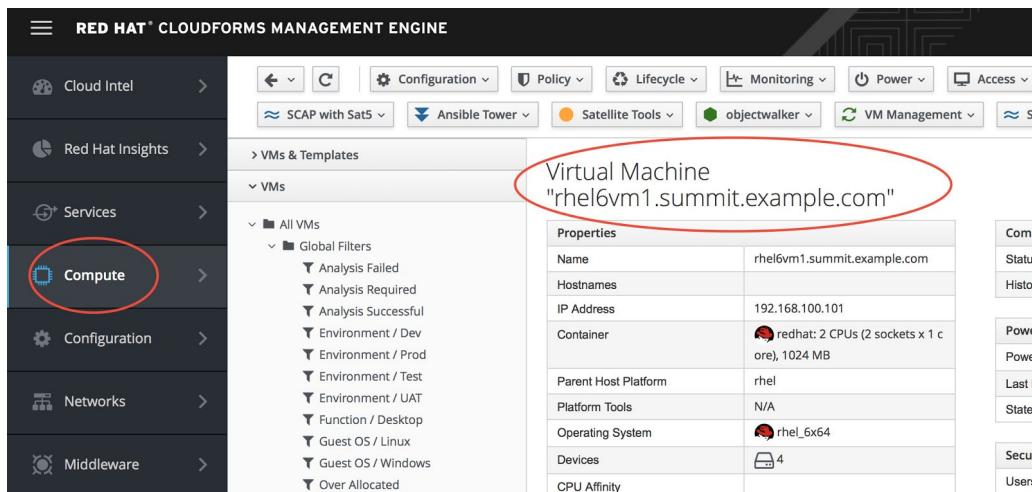
OpenSCAP security remediation on a VM at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Red Hat Satellite 5.7

20. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

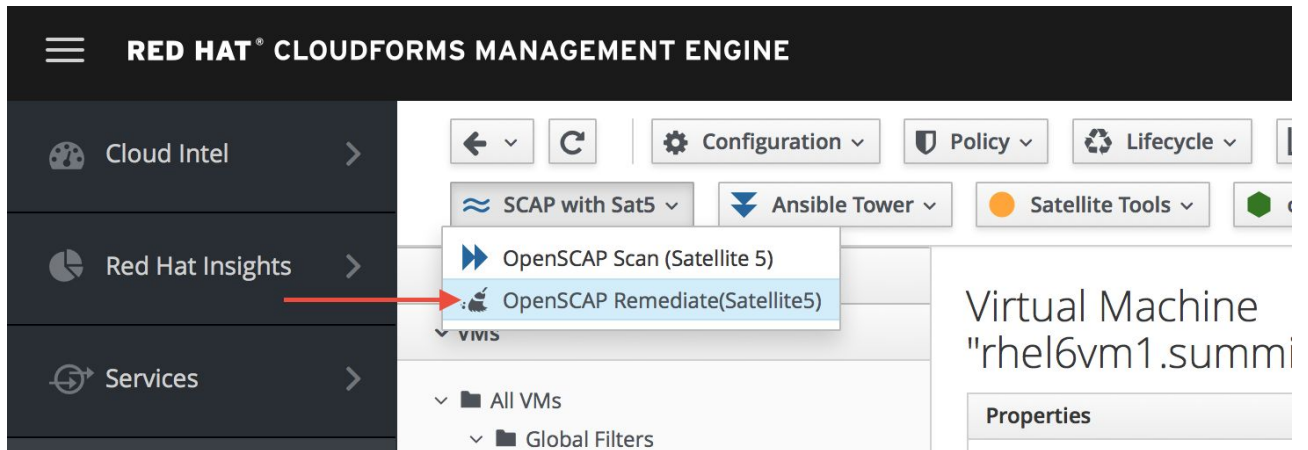
21. Then, navigate to **Compute** → **Infrastructure** → **Virtual Machines**



22. You should be at the VM summary page for the **rhel6vm1.summit.example.com** VM.

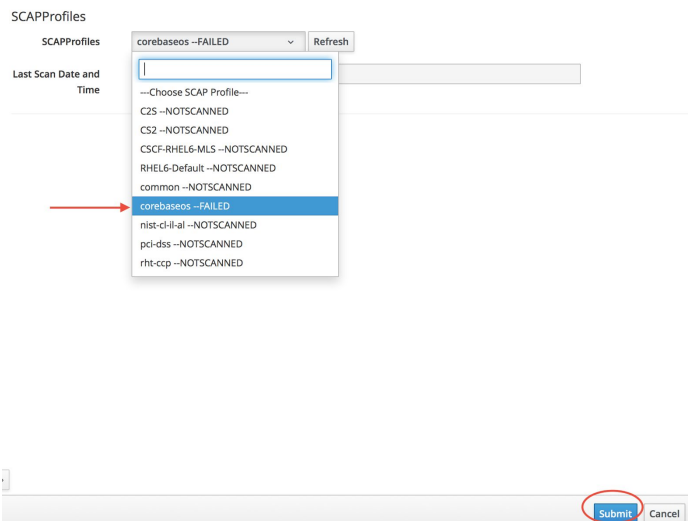


23. Now, at the top click on the **SCAP with Sat5** button and click on **OpenSCAP Remediate (Satellite 5)**.



24. Next, in the dialog window, for **SCAPProfiles**, choose the **corebaseos** profile. Press **Submit**.

rhel6vm1.summit.example.com - "OpenSCAP Remediate(Satellite5)"



Note: Notice that in the dropdown, next to the corebaseos profile name, you now see FAILED since the last scan you just did failed this policy. Remember that this profile is just checking to see if the aide package is installed. By choosing this profile during this remediation step, Red Hat CloudForms will give the command to execute the remediation on this VM (which in this case will install the aide package on this VM).

25. Go back to the terminal window open where you are logged into the rhel6vm1.summit.example.com VM.

```
lkernel — summit17@rhel6vm1:~ — ssh summit17@workstation-44cf.rhpd.s.op...
[summit17@rhel6vm1 ~]$
```

26. Now, see if the aide package is installed (it may take a minute for the package to show up):

\$ rpm -qa aide

```
lkernel — summit17@rhel6vm1:~ — ssh s
[summit17@rhel6vm1 ~]$ rpm -qa aide
aide-0.14-8.el6.x86_64
[summit17@rhel6vm1 ~]$
```

Note: Notice that now the aide package has been installed.

27. First, if you're not already there, navigate back to the **rhel6vm1.summit.example.com** by clicking on **Compute** in the left pane of Red Hat CloudForms.

The screenshot shows the Red Hat CloudForms Management Engine interface. The left navigation pane has 'Compute' selected. The main content area shows a list of Virtual Machines under 'All VMs'. One VM, 'rhel6vm1.summit.example.com', is highlighted. The properties table for this VM is shown on the right:

Properties	
Name	rhel6vm1.summit.example.com
Hostnames	
IP Address	192.168.100.101
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
CPU Affinity	

28. Now, let's re-run the SCAP scan for the **corebaseos** profile. At the top, click on the **SCAP with Sat5** button and click on **OpenSCAP Scan (Satellite 5)**.

The screenshot shows the Red Hat CloudForms Management Engine interface. The top navigation bar has 'SCAP with Sat5' selected. A dropdown menu is open, showing 'OpenSCAP Scan (Satellite 5)' as the selected option. The main content area shows a list of Virtual Machines under 'All VMs'. One VM, 'rhel6vm1.summit.example.com', is highlighted. The properties table for this VM is shown on the right:

Properties	
Name	rhel6vm1.summit.example.com
Hostnames	
IP Address	192.168.100.101
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
CPU Affinity	

29. Next, in the dialog window, for **SCAPPProfiles**, choose the **corebaseos** profile. Notice that next to the profile name it says **FAILED** since this profile did fail its last scan. Press **Submit**.

rhel6vm1.summit.example.com - "OpenSCAP Scan (Satellite 5)"

Profiles

SCAPPProfiles corebaseos --FAILED Refresh

Last Scan Date and Time

--Choose SCAP Profile--

- C2S --NOTSCANNED
- CS2 --NOTSCANNED
- CSCF-RHEL6-MLS --NOTSCANNED
- RHEL6-Default --NOTSCANNED
- common --NOTSCANNED
- corebaseos --FAILED
- nist-cl-ii-ai --NOTSCANNED
- pcl-dss --NOTSCANNED
- rht-ccp --NOTSCANNED

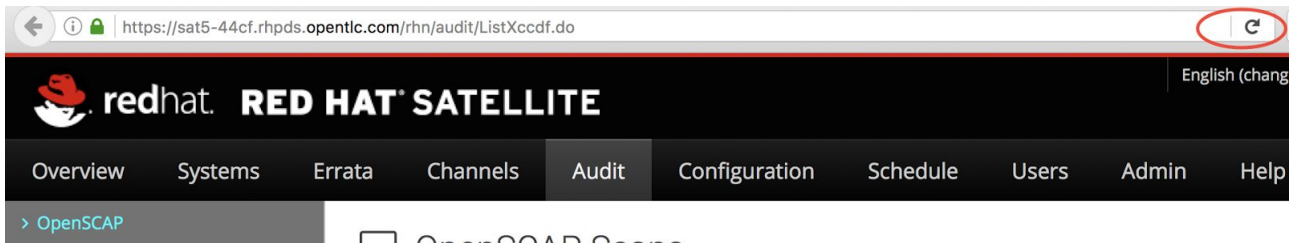
Submit Cancel

30. Now, let's see if this profile fails or passes. In your Firefox web browser, click on the tab you have opened to your Red Hat Satellite 5.7 UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

31. In the Red Hat Satellite 5.7 UI, navigate to the top "Audit" tab.

The screenshot shows the Red Hat Satellite 5.7 UI. The top navigation bar includes the Red Hat logo and the text "RED HAT SATELLITE". Below the navigation bar, there are several tabs: Overview, Systems, Errata, Channels, Audit, and Configuration. The "Audit" tab is highlighted with a red circle. On the left side, there is a sidebar menu with options: OpenSCAP, All Scans, XCCDF Diff, and Advanced Search. The main content area displays "OpenSCAP Scans" with a search filter "Filter by Xccdf Profile:" and a table with columns "System" and "Xccdf Pr".

32. After a few minutes, you should see your completed OpenSCAP scan in the completed scan list. Press the refresh button on your web browser.



33. In the second Xccdf Profile column, Click on the **corebaseos** profile from the top of the list with today' date and current time, as indicated in the third Completed column.

OpenSCAP Scans

System	Xccdf Profile	Completed	Satisfied	Dissatisfied
rhel6vm1.summit.example.com	corebaseos	Sun Apr 23 10:42:05 EDT 2017	1	0

Details of XCCDF Scan

Scan ID (xid): 23
File System Path: /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
Command-line Arguments: --profile corebaseos
Scheduled By: admin
Benchmark Identifier: RHEL-6
Benchmark Version: 0.1.28
Profile Identifier: corebaseos
Profile Title: Common Profile for General-Purpose Systems
Started: 2017-04-23 09:28:30.0
Completed: 2017-04-23 09:28:32.0

Scan's Error output:

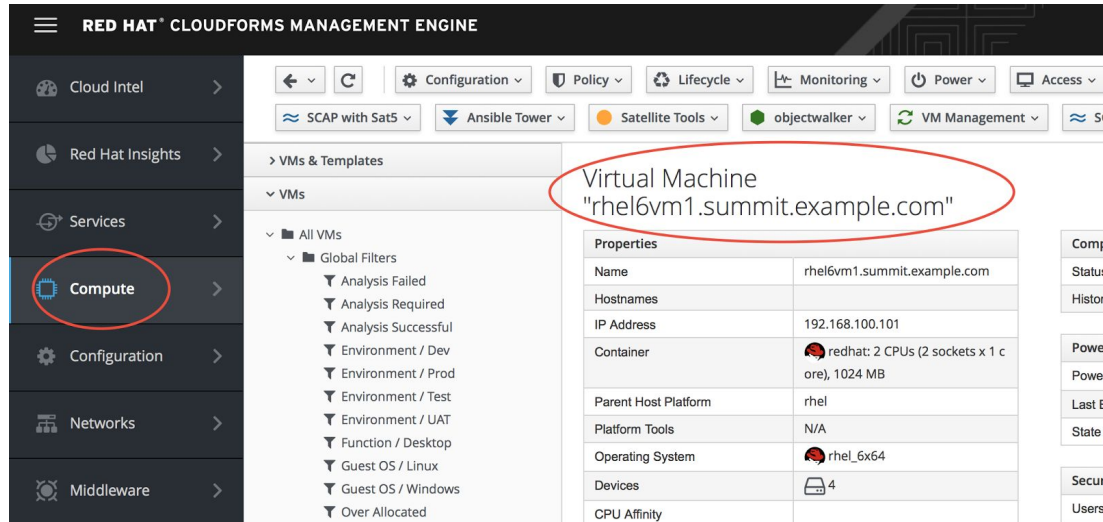
WARNING: Skipping http://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml file which is referenced from XCCDF c
 xccdf_eval: oscap tool returned 2

XCCDF Rule Results

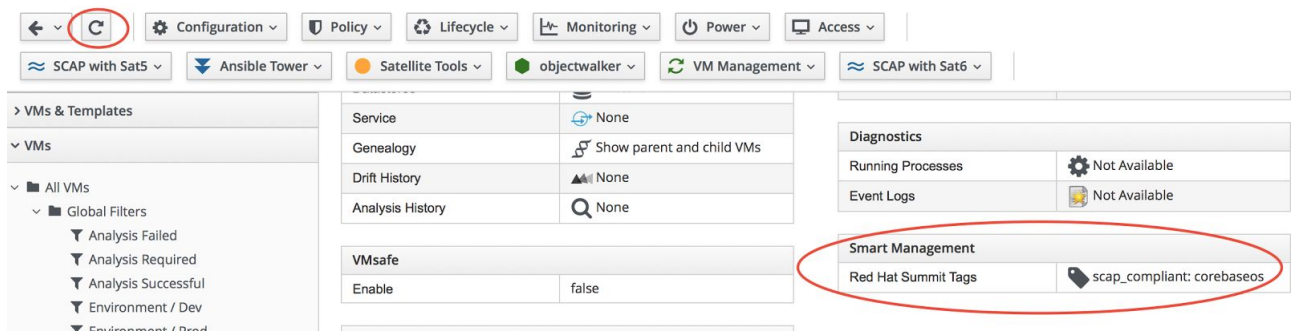
XCCDF Rule Identifier	XCCDF Ident Tags	Result
package_aide_installed	CCE-27024-9, DISA FSO RHEL-06-000016	fail

*Note: As stated earlier, this corebaseos profile just checks to see if the aide package is installed. As you can see, the result is **pass**, which means that the aide package is now installed on this VM.*

34. Go back to **Red Hat CloudForms** and click on **Compute** in the left pane to go back to your **rhel6vm1.summit.example.com** VM (if you're not already there).



35. At the VM summary page of your **rhel6vm1.summit.example.com** VM, take a look at the bottom right of the VM summary page in the Smart Management box. Notice that in the Red Hat Summit Tags, your tag for the corebaseos profile has now changed to **scap_compliant: corebaseos** since your VM is now compliant to the corebaseos profile. If you don't see this tag yet, Click the circular **Reload** arrow In the Red Hat CloudForms UI (not the browser).



Lab 5 : OpenSCAP security scans and remediations at the push of a button in Red Hat CloudForms with the integration of Red Hat CloudForms and Satellite 6.2

Goal of Lab 5

The goal of this lab is to show the ability to execute OpenSCAP security scans and remediations at the push of a button in Red Hat CloudForms with the custom integration of Red Hat CloudForms with Red Hat Satellite 6.2.

Introduction

In this lab, you will see how you can leverage Red Hat Satellite 6's built-in OpenSCAP scanning and remediation capabilities from Red Hat CloudForms.

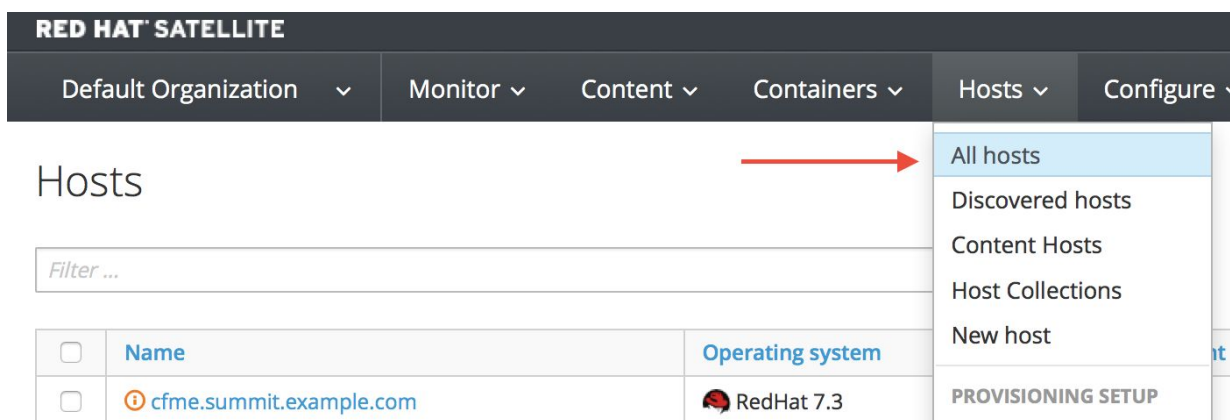
Red Hat CloudForms provides out-of-the-box integration to Ansible Tower by Red Hat. This integration provides visibility in Red Hat CloudForms of the Ansible Tower inventory, including hosts and job templates. As a result, with this integration, you can launch Ansible Tower job templates from Red Hat CloudForms automate. For example, from Red Hat CloudForms, the Ansible Tower job templates can be executed as part of the provisioning or retirement state machines, from a button on a host/vm , or as an action on a control policy. You can also launch Ansible Tower job templates from the Red Hat CloudForms service catalog as a service item or as part of a service bundle.

In this lab, you will launch the OpenSCAP scan and OpenSCAP remediate Ansible job templates by pressing custom buttons on a VM in Red Hat CloudForms.

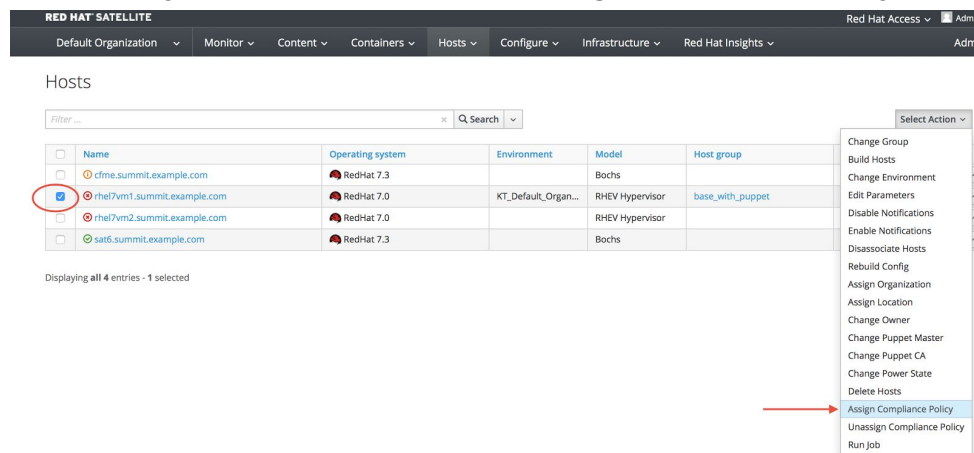
This integration between Red Hat CloudForms and Red Hat Satellite allows you to have a central and automated way to do point in time security scans and remediations on a per-vm basis.

OpenSCAP security scan on a VM at the push of a button in Red Hat CloudForms utilizing Satellite 6's built-in OpenSCAP scanning capabilities

1. In your Firefox web browser, click on the tab you have opened to your Red Hat Satellite 6.2 UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
2. From your Satellite UI, click on **Hosts** → **All Hosts**.



3. Then put a checkmark next to the **rhel7vm1.summit.example.com** VM and at the button on the top right, press **Select Action** → **Assign Compliance Policy**



4. Select the **RHEL7_Common** compliance policy from the dropdown. This will assign this RHEL7_Common policy to this client VM. Press **Submit**.

Assign Compliance Policy - The following hosts are about to be changed x

Name	Host group	Environment	Location	Organization
rhel7vm1.summit.example.com	base_with_puppet	KT_Default_Organization_Library_rhel7_soe_with_puppet_4	Default Location	Default Organization

Keep selected hosts for a future action

RHEL7_Common
 Select Compliance Policy
 rhel7-base
RHEL7_Common
 RHEL7_PCI_DSS
 RHEL7_Standard

←

5. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
6. Go back to **Red Hat CloudForms** and click on the **top back arrow button** in the CloudForms UI (not the browser) then click on **All VMs**.
7. Navigate to your RHEL 7 VM 1 VM by **typing rhel7vm1.summit.example.com** in the search bar at the top right and then pressing the search icon. **Click on the rhel7vm1.summit.example.com VM**.

Note: Notice that the rhel7vm1.summit.example.com VM has a yellow shield on it. This means that a control policy is applied to this VM.

VMs & Templates

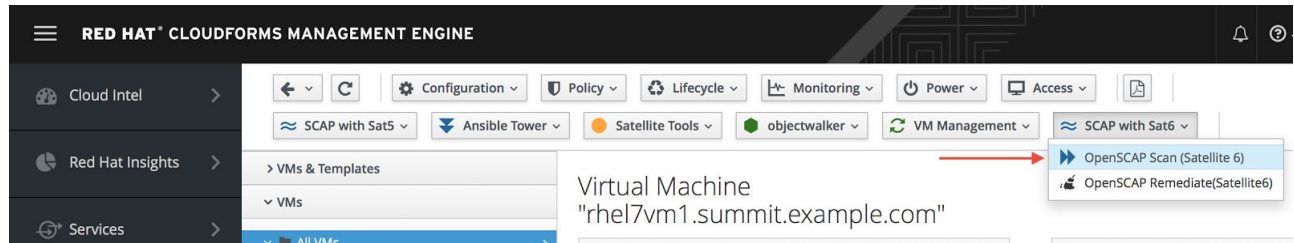
- ▼ All VMs & Templates >
 - rhvm.summit.example.com
 - A <Archived>
 - o <Orphaned>
- > VMs
- > Templates

All VMs & Templates (Names with "rhel7vm1.summit.example.com")

rhel7...e.com

rhel7vm1.summit.exami x

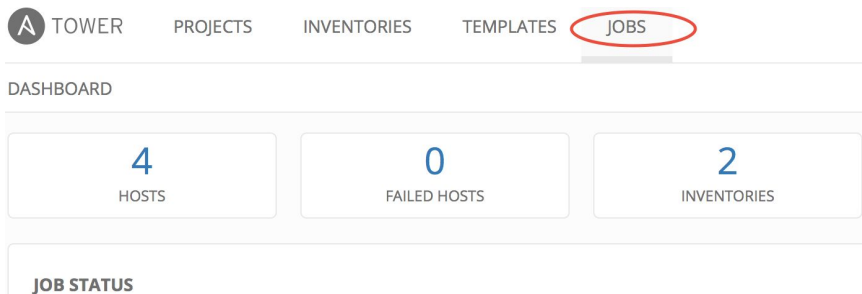
8. Now, at the top click on the **SCAP with Sat6** button and click on **OpenSCAP Scan (Satellite 6)** (**Satellite 6**).



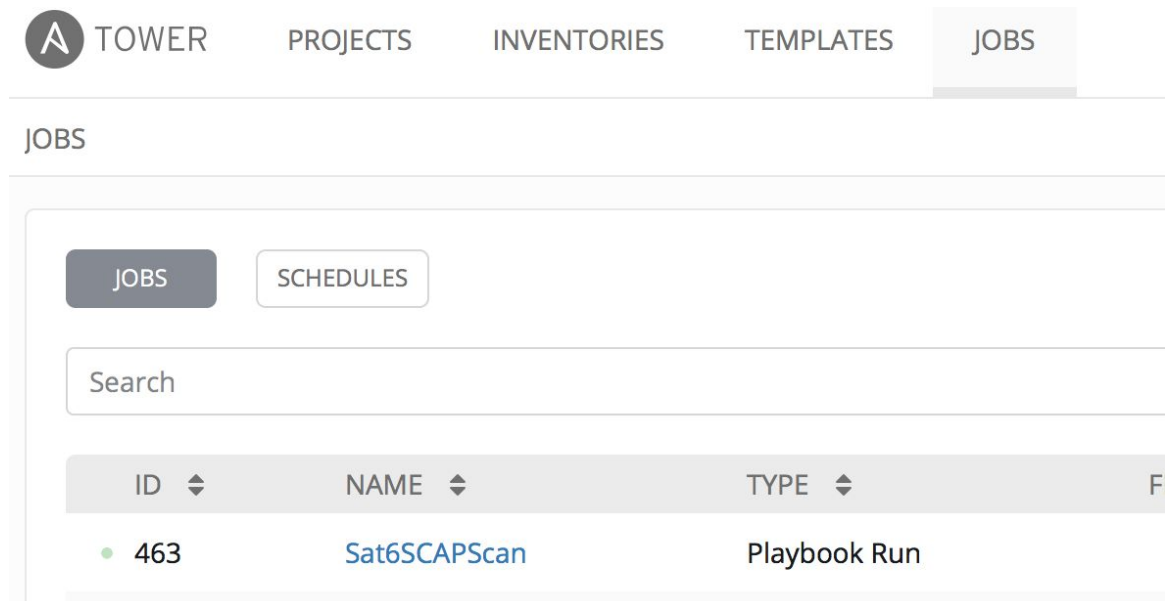
Note: This will leverage Satellite 6's built-in OpenSCAP scanning capability by launching the OpenSCAP scan Ansible playbook on the rhel7vm1.summit.example.com.

9. Now, let's log into Ansible Tower to see the status of the OpenSCAP scan job we just ran on this VM. In your Firefox web browser, click on the tab you have opened to your Ansible Tower UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

10. In the Ansible Tower UI, Click on **Jobs** at the top of the UI.



11. You should (eventually) see that your Sat6SCAPScan Ansible playbook is being run.



12. Click the latest **Sat6SCAPScan** job to see the progress and wait for the **STATUS** to show **Successful**

The screenshot displays the Red Hat Ansible Tower interface for a job named 'SAT6SCAPSCAN'. The job status is 'Successful', indicated by a green dot and a red arrow pointing to the 'Successful' text. The job was started on 4/23/2017 at 11:18:13 AM and finished at 11:20:18 AM. The template used is 'Sat6SCAPScan', and the job type is 'Run'. The job was launched by 'admin' and is associated with the 'Red Hat Security Demos' project. The limit is 'rhel7vm1.summit.example.com', which is circled in red. The job log shows the execution of the 'OpenScap scan' task on the specified host, with the output 'changed: [rhel7vm1.summit.example.com]' circled in red.

DETAILS	VALUE
STATUS	Successful
STARTED	4/23/2017 11:18:13 AM
FINISHED	4/23/2017 11:20:18 AM
TEMPLATE	Sat6SCAPScan
JOB TYPE	Run
LAUNCHED BY	admin
INVENTORY	CloudForms
PROJECT	Red Hat Security Demos
REVISION	d85710555acF90c234398bc4ab38161d99916cf5
PLAYBOOK	cf-ans-sat-scap/cf-ans-sat-scan.yml
MACHINE CREDENTIAL	RHEL 7 VM Key
FORKS	0
LIMIT	rhel7vm1.summit.example.com
VERBOSITY	0 (Normal)
EXTRA VARIABLES	1 policy_id: '3'

```

1 Identity added: /tmp/ansible_tower_AdYHa2/credential (/tmp/credential)
2
3 PLAY [all] *****
4
5 TASK [setup] *****
6 ok: [rhel7vm1.summit.example.com]
7
8 TASK [[Configure puppet client] *****
9 changed: [rhel7vm1.summit.example.com]
10
11 TASK [[OpenScap scan] *****
12 changed: [rhel7vm1.summit.example.com]
13
14 PLAY RECAP *****

```

Note: Notice that this Sat6SCAPScan Ansible playbook ran successfully on the rhel7vm1.summit.example.com VM. This means that the OpenSCAP scan was successfully completed on the rhel7vm1.summit.example.com VM.

13. In your Firefox web browser, click on the tab you have opened to your Red Hat Satellite 6.2 UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

14. From your Satellite 6.2 UI, click on **Hosts**→**Reports**

The screenshot shows the Red Hat Satellite 6.2 UI. The top navigation bar includes 'Default Organization', 'Monitor', 'Content', 'Containers', 'Hosts', and 'Configure'. The 'Hosts' dropdown menu is open, showing options like 'All hosts', 'Discovered hosts', 'Content Hosts', 'Host Collections', 'New host', 'PROVISIONING SETUP', 'Architectures', 'Hardware models', 'Installation media', 'Operating systems', 'TEMPLATES', 'Partition tables', 'Provisioning templates', 'Job templates', 'COMPLIANCE', 'Policies', 'SCAP contents', and 'Reports'. A red arrow points to the 'Reports' option.

15. Click on the report you just created by clicking on the **most recent** report for **rhel7vm1.summit.example.com** by clicking the link in the **Reported At** column (do not click the host link).

The screenshot shows the Red Hat Satellite 6.2 UI. The top navigation bar includes 'Default Organization', 'Monitor', 'Content', 'Containers', 'Hosts', 'Configure', 'Infrastructure', and 'Red Hat Insights'. The 'Compliance Reports' section is visible, showing a table with columns for 'Host', 'Reported At', 'Passed', and 'Failed'. The 'Reported At' column for the most recent report for 'rhel7vm1.summit.example.com' is circled in red.

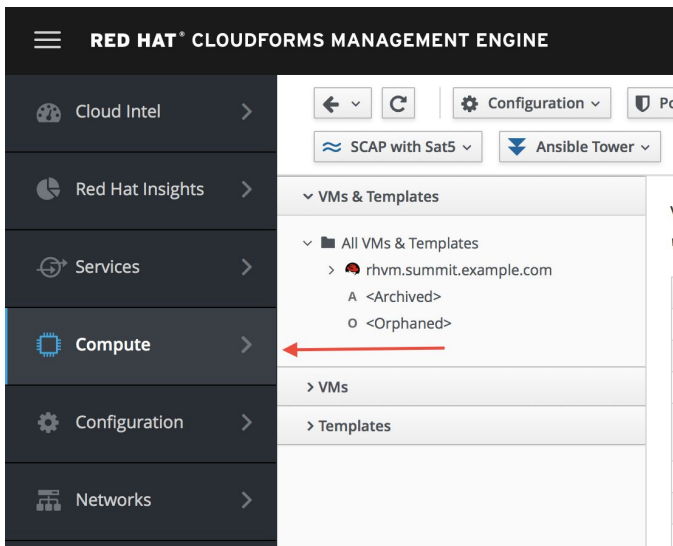
Host	Reported At	Passed	Failed
rhel7vm1.summit.example.com	9 minutes ago	9	29

Note: In the scan results for this VM, notice that you have 9 rules that Passed and 29 that Failed.

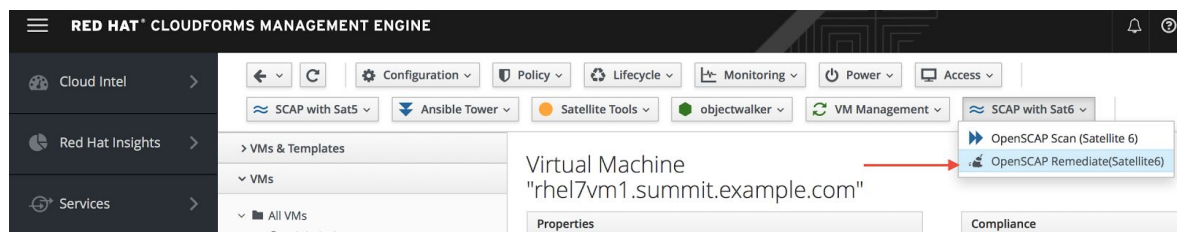
OpenSCAP security remediation on a VM at the push of a button in Red Hat CloudForms utilizing Satellite 6's built-in OpenSCAP remediation capabilities

16. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

17. In the Red Hat CloudForms UI, if you're not already there, navigate to your **rhel7vm1.summit.example.com** VM. Clicking on **Compute** on the left side is a shortcut.



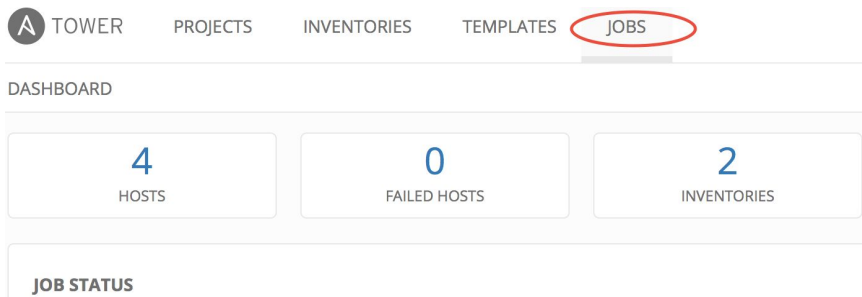
18. Now, at the top, click on the **SCAP with Sat6** button and click on **OpenSCAP Remediate (Satellite 6)**.



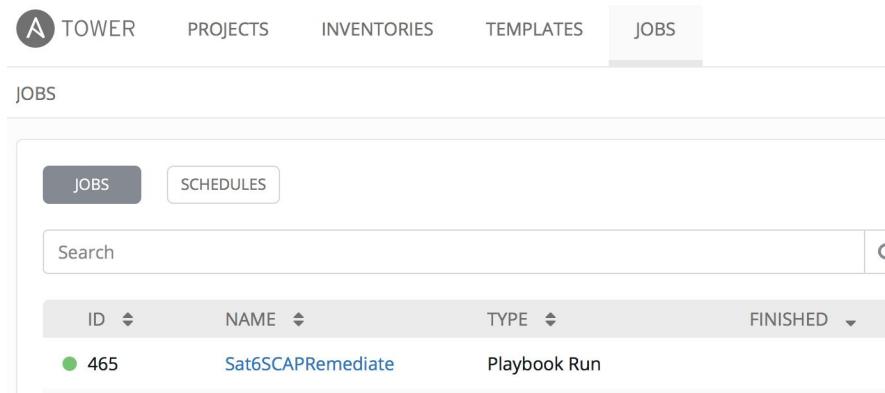
Note: This will leverage Satellite 6's built-in OpenSCAP remediation capability by launching the OpenSCAP scan Ansible playbook on the rhel7vm1.summit.example.com. This remediate playbook will also run the OpenSCAP scan report at the end.

19. Now, let's log into Ansible Tower to see the status of the OpenSCAP scan job we just ran on this VM. In your Firefox web browser, click on the tab you have opened to your Ansible Tower UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

20. In the Ansible Tower UI, Click on **Jobs** at the top of the UI.



21. You should (eventually) see that your **Sat6SCAPRemediate** Ansible playbook is being run.



22. Click the latest **Sat6SCAPRemediate** job to see the progress and wait for the **STATUS** to show **Successful**

The screenshot shows the details of a job named 'SAT6SCAPREMIATE'. The job is in a 'Successful' state, which is circled in red. The job was started on 4/23/2017 at 11:51:53 AM and finished at 11:55:02 AM. The template used is 'Sat6SCAPRemediate'. The job type is 'Run', and it was launched by 'admin'. The inventory is 'CloudForms', and the project is 'Red Hat Security Demos'. The revision is 'd85710555acf90c234398bc4ab38161d99916cf5'. The playbook is 'cf-ans-sat-scrap/cf-ans-sat-fix.yml'. The machine is 'RHEL 7 VM Key'. The job has 0 forks and a limit of 'rhel7vm1.summit.example.com', which is also circled in red. The verbosity is set to 0 (Normal). The extra variables are 'policy_id: '3'' and 'sat_server: 'https://sat6.summit.example.com''. The job log shows the following tasks:

```

1 Identity added: /tmp/ansible_tower_rdrXc4/credential (/tmp/ansible_t...
2
3 PLAY [all] *****
4
5 TASK [setup] *****
6 ok: [rhel7vm1.summit.example.com]
7
8 TASK [Puppet run to get foreman_scrap_client config] *****
9 changed: [rhel7vm1.summit.example.com]
10
11 TASK [get profile] *****
12 changed: [rhel7vm1.summit.example.com]
13
14

```

23. In your Firefox web browser, click on the tab you have opened to your Red Hat Satellite 6.2 UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

24. From your Satellite 6.2 UI, click on **Hosts**→**Reports**

The screenshot shows the Red Hat Satellite 6.2 UI. The top navigation bar includes 'Default Organization', 'Monitor', 'Content', 'Containers', 'Hosts', and 'Configure'. The 'Hosts' menu is open, showing options like 'All hosts', 'Discovered hosts', 'Content Hosts', 'Host Collections', 'New host', 'PROVISIONING SETUP', 'Architectures', 'Hardware models', 'Installation media', 'Operating systems', 'TEMPLATES', 'Partition tables', 'Provisioning templates', 'Job templates', 'COMPLIANCE', 'Policies', 'SCAP contents', and 'Reports'. The 'Reports' option is highlighted with a red arrow. The 'Compliance Reports' page is visible in the background, showing a list of hosts with checkboxes and a filter input.

25. Click on the report you just created by clicking on the **most recent** report for **rhel7vm1.summit.example.com** by clicking the link in the **Reported At** column (do not click the host link).

RED HAT SATELLITE

Default Organization ▾ Monitor ▾ Content ▾ Containers ▾ Hosts ▾ Configure ▾ Infrastructure ▾ Red Hat Insights ▾

Compliance Reports

Filter ... x Q Search ▾

Host	Reported At	Passed	Failed
<input type="checkbox"/> rhel7vm1.summit.example.com	7 minutes ago	36	2

RED HAT SATELLITE

Default Organization ▾ Monitor ▾ Content ▾ Containers ▾ Hosts ▾ Configure ▾ Infrastructure ▾ Red Hat Insights ▾

Red Hat Access ▾ Admin User ▾

rhel7vm1.summit.example.com

Administrator ▾

Show log messages: All messages ▾

Back Delete Host details View full report Download XML in bzip

Reported at 2017-04-23 11:54:56 -0400

Severity	Message	Resource	Result
Low	Ensure /var/log Located On Separate Partition <input type="checkbox"/>	xccdf_org.ssgproject.content_...	fail
Low	Ensure /var/log/audit Located On Separate Partition <input type="checkbox"/>	xccdf_org.ssgproject.content_...	fail

*Note: Notice that all the rules that have passed now for this assigned **Common** profile except 2 rules: the rules for ensuring /var/log and /var/log/audit being located on separate partitions. These rules are easier to fix manually. We will not worry about fixing these in this lab.*

Lab 6 : Viewing SCAP compliant and non-compliant VMs from a report in Red Hat CloudForms

Goal of Lab 6

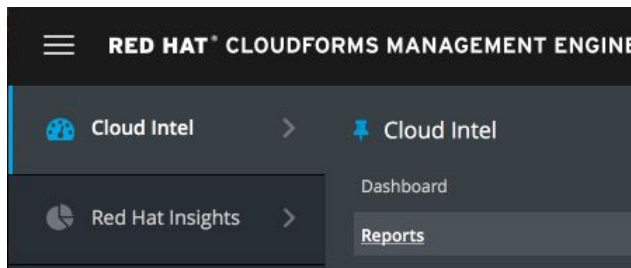
The goal of this lab is to view reports in Red Hat CloudForms showing SCAP non-compliant and compliant VMs based on compliance profiles.

Introduction

Red Hat CloudForms has a robust reporting engine built into the product that allows you to create reports using any of the introspective data collected from your heterogeneous infrastructure. This data is stored either in an internal or external PostgreSQL database. You can use this collected data when creating reports , in control policies , or in automation workflows in Red Hat CloudForms.

View SCAP compliant and non-compliant VM reports

1. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
2. In the left pane of the Red Hat CloudForms UI, navigate to **Cloud Intel** → **Reports**



3. Then Click on **Saved Reports** → **All Saved Reports** → **SCAP Compliant VMs (corebaseos profile)**. Then click on the → to view the saved report.

Name	IP Addresses	Date Created
rhel6vm1.summit.example.com	192.168.100.101	04/03/17 19:59:47 UTC

*Note: This is a report showing you all the VMs that are compliant to the corebaseos profile. In addition to showing you the name of the VM, you can see the IP address and date the VM was created. Notice that in this report, you can see that the **rhel6vm1.summit.example.com** VM with IP address 192.168.100.101 was created on 04/03/17 at 19:59:47 UTC and is compliant to the corebaseos SCAP profile. Red Hat CloudForms knows that this VM is compliant to the corebaseos SCAP profile since it has the `scap_compliant: corebaseos` tag on it.*

4. Now, to view the report showing you the SCAP Non-Compliant VMs based on a particular profile, click on **Saved Reports** → **All Saved Reports** → **SCAP Non-Compliant VMs (pci_dss profile)**. Then click on the → to view the saved report.

Configuration

▼ Saved Reports

- ▼ All Saved Reports
 - SCAP Compliant VMs (corebaseos profile)
 - 2017-04-14 01:59:38 UTC
 - SCAP Non-Compliant VMs(pci_dss profile)
 - 2017-04-14 02:03:07 UTC

Saved Report "SCAP Non-Compliant VMs(pci_dss profile) - Fri, 14 Apr 2017 02:03:05 +0000"

Name	IP Addresses	Date Created
rhel6vm1.summit.example.com	192.168.100.101	04/03/17 19:59:47 UTC

*Note: This is a report showing you all the VMs that are non-compliant to the pci_dss profile. In addition to showing you the name of the VM, you can see the IP address, and the date the VM was created. Notice that in this report, you can see that the **rhel6vm1.summit.example.com** VM with IP address 192.168.100.101 was created on 04/03/17 at 19:59:47 UTC and is non-compliant to the pci_dss SCAP profile.*

Lab 7 : Ordering a custom service using Red Hat CloudForms and Ansible Tower by Red Hat for security compliance automation

Goal of Lab 7

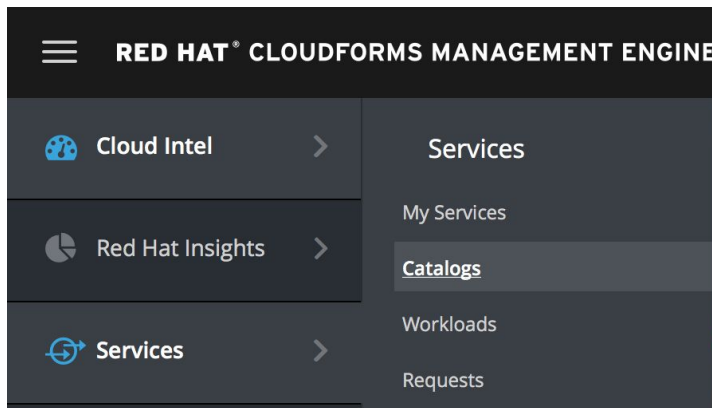
The goal of this lab is to show the ability for a user to click an order button in the service catalog of Red Hat CloudForms to execute specific custom defined services. Specifically, in this lab, a Red Hat CloudForms service will execute a specific Ansible Tower job template for your entire Ansible Tower inventory. You will also use the Red Hat CloudForms service catalog to see how you can create a security compliant host at provisioning time. This lab is another example of how you can automate security compliance at the push of a button.

Introduction

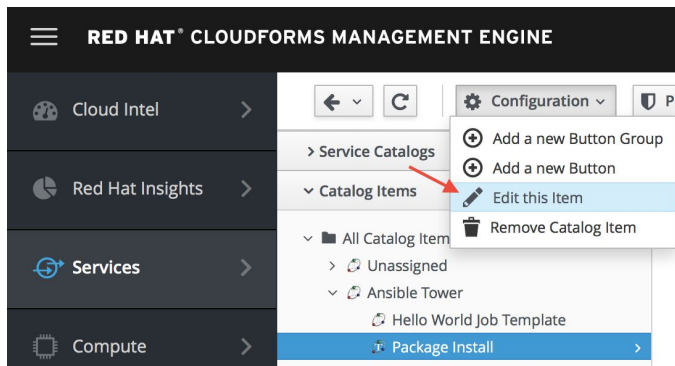
Red Hat CloudForms provides users the ability to create self-service catalogs. Through the use of catalogs, Red Hat CloudForms provides support for executing free form automation as a service and also allow for multi-tier service provisioning to deploy layered workloads across hybrid environments. You can create customized dialogs that will give consumers of the services the ability to input just a few parameters and provision the entire service. In addition to using the native ruby language, free form automation workflows using the service catalog of Red Hat CloudForms can call Ansible Tower job templates as part of your automation workflow as well. All of this allows you to automate security compliance at the push of a button using Red Hat CloudForms and Ansible Tower.

Using the Red Hat CloudForms service catalog to order a service to execute an Ansible playbook against your entire Ansible Tower inventory

1. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
2. In the Red Hat CloudForms UI, in the left pane, navigate to **Services** → **Catalogs**.



3. Let's take a look at the Package Install service catalog item by navigating to **Catalog Items** → **All Catalog Items** → **Ansible Tower** → **Package Install**. Then go to the **Configuration** button at the top left of the UI and click on **Edit this item**.



Editing Service Catalog Item "Package Install "

Basic Info Details

Name / Description: Package Install Package Install Display in Catalog

Catalog: Ansible Tower

Dialog: CustomInstallPackageforService

Provider: Ansible Tower Provider Configur.

Ansible Tower Job Template: InstallPackage

Provisioning Entry Point: Demo Job Template
HelloWorld

Reconfigure Entry Point: InstallPackage
NIST 800-53
RHEL6 STIG

Retirement Entry Point: RHEL7 STIG
RegisterToSatellite6
RegisterToSatellite5
Sat6SCAPRemediate

Save Reset **Cancel**

Note: Notice that here we have defined what Ansible Job Template we want to use for this service in addition to what custom dialog we want to present to the users who order this service from Red Hat CloudForms.

4. Click **Cancel** at the bottom right.
5. Now, **Click** on the **Service Catalogs** accordion on the left. Press **Order** next to the Service named **"Package Install"**.

Service Catalogs

- All Services
 - Ansible Tower
 - Provision VM
- Catalog Items
- Orchestration Templates
- Catalogs

All Services

Name	Description	Tenant	
Hello World Job Template	Hello World Job Template	Red Hat Summit	Order
Package Install	Package Install	Red Hat Summit	Order
Provision RHEL 7 VM (Bundle)		Red Hat Summit	Order
RHEL6_DISA_STIGed	RHEL6_DISA_STIGed	Red Hat Summit	Order
RHEL 7		Red Hat Summit	Order

6. For Package Name, type **screen**. Press **Submit**.

Order Service "Package Install "

General

Package Name

Note: Red Hat CloudForms will now tell Ansible Tower to execute its Package Install job template which will install the screen package for all the systems in your Ansible Tower inventory.

7. Now, let's log into Ansible Tower to see the status of the InstallPackage scan job we just ran on this VM. In your Firefox web browser, click on the tab you have opened to your Ansible Tower UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

8. In the Ansible Tower UI, Click on **Jobs** at the top of the UI.

TOWER PROJECTS INVENTORIES TEMPLATES **JOBS**

DASHBOARD

4 HOSTS	0 FAILED HOSTS	2 INVENTORIES
------------	-------------------	------------------

JOB STATUS

9. You should (eventually) see that your InstallPackage Ansible playbook is being run.

The screenshot shows the Ansible Tower interface. At the top, there are navigation tabs: TOWER, PROJECTS, INVENTORIES, TEMPLATES, and JOBS. The JOBS tab is active. Below the navigation, there is a sub-navigation bar with buttons for JOBS and SCHEDULES. A search bar is located below the sub-navigation. Underneath the search bar is a table with the following columns: ID, NAME, and TYPE. The table contains one entry: ID 467, NAME InstallPackage, and TYPE Playbook Run.

10. Click the latest **InstallPackage** job to see the progress and wait for the **STATUS** to show **Successful**

The screenshot displays the details of an Ansible Tower job named 'INSTALLPACKAGE'. On the left, the 'DETAILS' sidebar shows the following information: STATUS is 'Successful', STARTED at 4/23/2017 4:14:48 PM, FINISHED at 4/23/2017 4:17:10 PM, TEMPLATE is 'InstallPackage', JOB TYPE is 'Run', LAUNCHED BY is 'admin', INVENTORY is 'CloudForms', PROJECT is 'Red Hat Security Demos', REVISION is 'd85710555acf90e234398bo4ab38161d99916cf5', PLAYBOOK is 'lkernel/installpackage/installrpm.yml', MACHINE CREDENTIAL is 'VMCredentials', FORKS is '0', and VERBOSITY is '0 (Normal)'. The EXTRA VARIABLES section shows '1 package_name: screen'. The main content area shows the job output with a search bar and a list of tasks. The output shows 'TASK [install package]' followed by 'changed:' for three hosts: [rhel7vm1.summit.example.com], [rhel7vm2.summit.example.com], and [rhel6vm1.summit.example.com]. The output ends with 'PLAY RECAP' and a summary of results for each host.

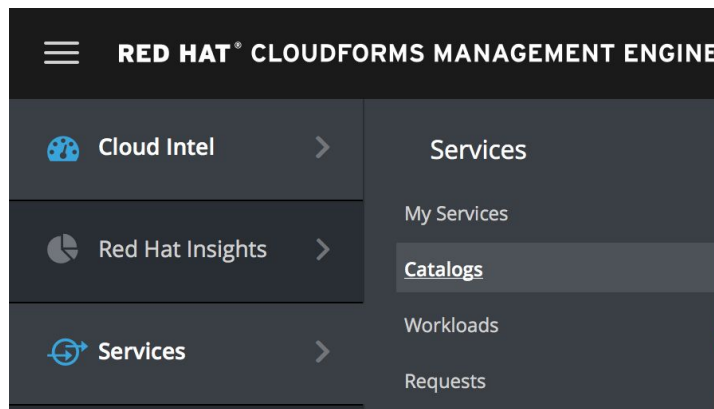
Note: Notice that this InstallPackage Ansible Tower job template ran successfully on all 3 VM's in the Ansible Tower inventory (rhel6vm1.summit.example.com, rhel7vm1.summit.example.com, and rhel7vm2.summit.example.com). Also even though we only executed 1 Ansible Tower job template in this lab exercise via the Red Hat CloudForms service catalog, you can create a service catalog bundle that can execute

multiple different Ansible Tower job templates, in the order that you specify, for your entire Ansible Tower inventory.

Understanding how to use the Red Hat CloudForms service catalog to provision a security compliant host at the push of a button

Using the service catalog of Red Hat CloudForms, you can also create a custom provisioning service.

11. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
12. In the Red Hat CloudForms UI, in the left pane, navigate to **Services** → **Catalogs**.



13. Press **Order** for the **RHEL6_DISA_STIGed** service. **Do not press Submit.**

The screenshot shows the 'All Services' page in Red Hat CloudForms. The left sidebar shows 'Service Catalogs' with 'All Services' expanded to show 'Ansible Tower' and 'Provision VM'. The main content area displays a table of services. A green notification banner at the top indicates 'Service Order was cancelled by the user'. The table lists several services, with 'RHEL6_DISA_STIGed' highlighted and its 'Order' button pointed to by a red arrow.

Name	Description	Tenant	
Hello World Job Template	Hello World Job Template	Red Hat Summit	Order
Package Install	Package Install	Red Hat Summit	Order
Provision RHEL 7 VM (Bundle)		Red Hat Summit	Order
RHEL6_DISA_STIGed	RHEL6_DISA_STIGed	Red Hat Summit	Order
RHEL 7		Red Hat Summit	Order

Note: This service provisions a RHEL 6 machine in Red Hat Virtualization, registers it to Satellite, and then runs the RHEL 6 DISA STIG Ansible playbook on top of the newly provisioned VM. Note that DISA STIG stands for Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). At the end of the provisioning workflow, a VM is provisioned in Red Hat Virtualization, registered with Satellite and is DISA STIG compliant. The user can define and set Ansible Tower role variables from the

service dialog when ordering this service. Specifically, in this dialog, the user is able to select how much they want to lock down their system (cat3 being the most locked down).

14. We will not order this service in this lab. Press **Cancel**.

Order Service "RHEL6_DISA_STIGed"

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

rhel6stg_cat1 false true

rhel6stg_cat2 false true

rhel6stg_cat3 false true

Submit Cancel

Lab 8: Proactive Security and Automated Risk Management with Red Hat Insights

Goal of Lab 8

The goal of this lab is to introduce you to the proactive security capabilities of Red Hat Insights.

Introduction

Red Hat Insights was designed to proactively evaluate the security, performance, and stability of your Red Hat platforms by providing prescriptive analytics of your systems. Red Hat Insights helps move you from reactive to proactive systems management, delivers actionable intelligence, and increases visibility of infrastructure risks and the latest security threats. Operational analytics from Red Hat Insights empowers you to prevent downtime and avoid firefighting while responding faster to new risks.

In this lab, we will focus only on the specific security features of Red Hat Insights.

Red Hat Insights recommendations are tailored for the individual system where risk is detected. This allows you to be certain that actions identified by Insights are validated and have a verified resolution for each detected risk, reducing false positives you may experience from critical risks identified by third-party security scanners. Red Hat Insights provides predictive analysis of security risk in your infrastructure based on a constantly evolving threat feed from Red Hat.

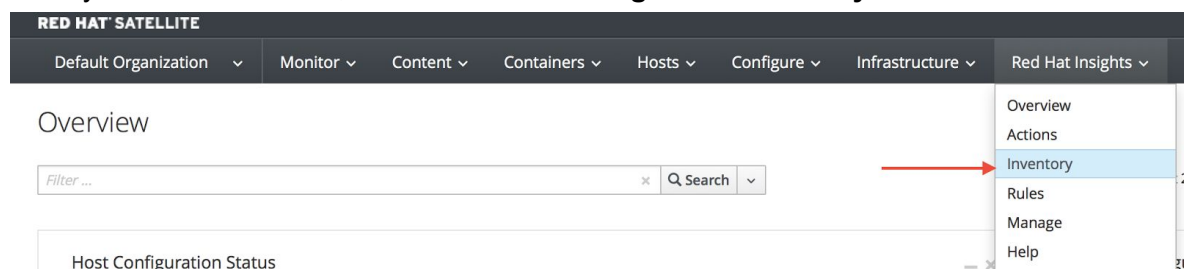
Through analysis of Red Hat Insights metadata and curated knowledge based on over fifteen years of enterprise customer support, Red Hat is able to identify critical security vulnerabilities, statistically frequented risks, and known bad configurations. We scale this knowledge to our customers with Red Hat Insights reporting and alerts, allowing prediction of what will happen on a monitored system, why it will happen, and how to fix a problem before it can occur.

Red Hat Insights functionality is integrated into Red Hat's Customer Portal, Red Hat Satellite, Red Hat CloudForms, and Ansible Tower by Red Hat. Recommendations from Red Hat Insights are human-readable and in most cases can simply be copy and pasted into the terminal to resolve the issue. You may also automate remediation of hosts in your infrastructure with Red Hat Insights generated Ansible playbooks or Ansible Tower by Red Hat integration.

Fixing the payload injection security issue in your system using Red Hat Insights

In this lab, we will fix the specific payload injection problem on your client VM without causing downtime.

1. In your Firefox web browser, click on the tab you have opened to your Red Hat Satellite 6.2 UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.
2. From your Satellite 6.2 UI, click on **Red Hat Insights** → **Inventory**.



3. Click on your client VM, which is **rhel7vm1.summit.example.com**.

Red Hat Insights

The screenshot displays the Red Hat Insights interface. At the top, there is a search bar with the placeholder text "Search...". To the right of the search bar are a "Filter" button and a "Hostname" dropdown menu. Below the search bar, the text "Actions: With or Without" and "Group: All" is visible. A "Unregister" button is located on the left side of the system list. The system list shows three entries, each with a "RHEL Server" icon, a hostname, and a "7 Actions", "8 Actions", or "2 Actions" button. The first system, "rhel7vm1.summit.example.com", is highlighted with a red arrow pointing to its hostname. The second system is "rhel7vm2.summit.example.com" and the third is "sat6.summit.example.com".

4. Notice that your system shows up with multiple security vulnerabilities.

Note: Our objective is to fix the payload injection problem without causing downtime, and see that it no longer appears as a vulnerability in Red Hat Insights. Specifically, this payload injection problem causes the kernel to be vulnerable to man-in-the-middle via payload injection. A flaw was found in the implementation of the Linux kernel's handling of networking challenge ack ([RFC 5961](#)) where an attacker is able to determine the shared counter. This flaw allows an attacker located on different subnet to inject or take over a TCP connection between a server and client without needing to use a traditional man-in-the-middle (MITM) attack.

5. Use your browser's search function to search for "payload injection".

Security > Kernel vulnerable to man-in-the-middle via **payload injection**

Detected issue

A flaw was found in the implementation of the Linux kernel's handling of networking challenge ack (RFC 5961) where an attacker is able to determine the shared counter. This flaw allows an attacker located on different subnet to inject or take over a TCP connection between a server and client without needing to use a traditional man-in-the-middle (MITM) attack.

This host is affected because it is running kernel 3.10.0-123.el7.

Your currently loaded kernel configuration contains this setting:

```
net.ipv4.tcp_challenge_ack_limit = 100
```

Your currently stored kernel configuration is:

```
net.ipv4.tcp_challenge_ack_limit = 100 # Implicit default
```

There is currently no mitigation applied and your system is vulnerable.

Steps to resolve

Red Hat recommends that you update the **kernel** package and restart the system:

```
# yum update kernel
# reboot
```

or

Alternatively, this issue can be addressed by applying the following mitigations until the machine is restarted with the updated kernel package.

Edit `/etc/sysctl.conf` file as root, add the mitigation configuration, and reload the kernel configuration:

```
# echo "net.ipv4.tcp_challenge_ack_limit = 2147483647" >>
/etc/sysctl.conf
# sysctl -p
```

[Show more info](#)

*Note: Reading the description for the vulnerability shows that the **sysctl** variable is set to a level that allows being exploited. We want to do the active mitigation by changing the **sysctl** variable and making it permanent on reboot. In this case, we do not want to update the kernel or reboot since we don't want downtime.*

6. If not already there, SSH to the client VM and perform the recommended active mitigation. To login to your client VM, first SSH into your workstation node at workstation-`<GUID>`.rhpds.opentlc.com as the summit17 user. An ssh key is already in the home directory of your laptop, which should allow you to login without a password. Should a password be required, use r3dh@t2017 as your password.

\$ ssh summit17@workstation-`<GUID>`.rhpds.opentlc.com

7. Now that you are in the workstation node, SSH into your RHEL7 client/host. This host has already been registered to both Red Hat Satellite 6 and Red Hat Insights for you.

\$ ssh rhel7vm1.summit.example.com

8. Now, as **root**, perform the recommended active mitigation. Edit the `/etc/sysctl.conf` file to add the mitigation configuration, and reload the kernel configuration:

\$ sudo -i

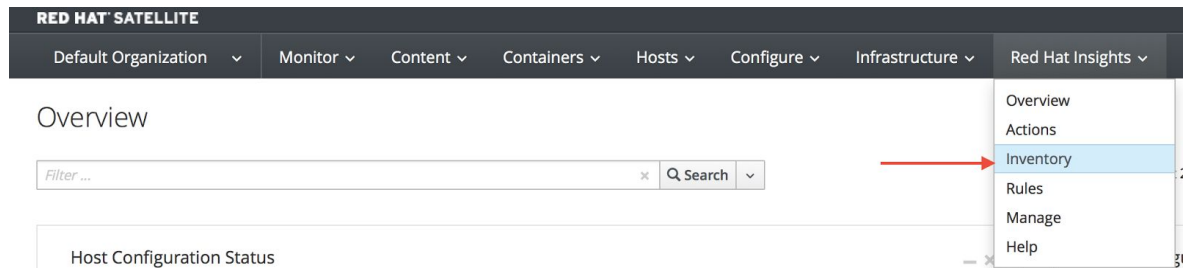
```
# echo "net.ipv4.tcp_challenge_ack_limit = 2147483647" >> /etc/sysctl.conf
# sysctl -p
```

9. After applying the active mitigation, we want to have the system report any changes, run the following command as root on `rhel7vm1.summit.example.com`:

```
# redhat-access-insights
```

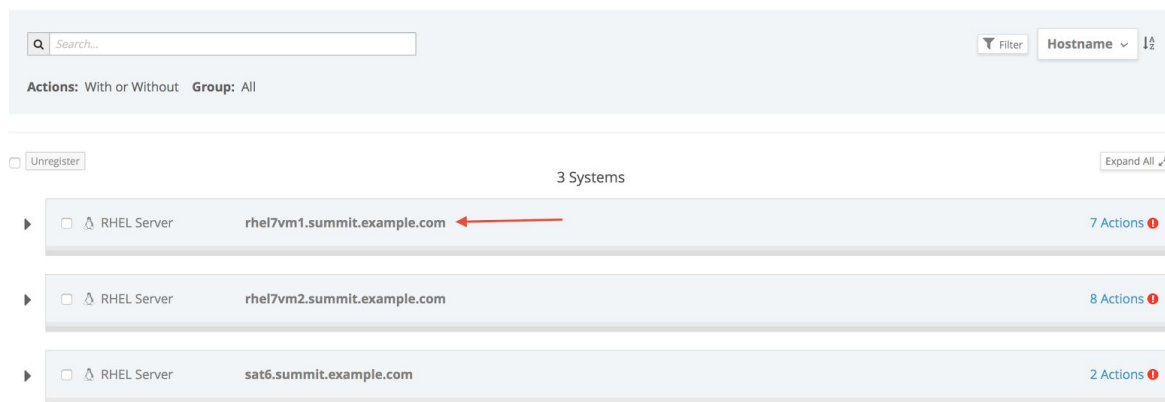
Wait until this step completes before moving to the next step.

10. From your Satellite 6.2 UI, click on **Red Hat Insights** → **Inventory**.



11. Click on your client VM, which is `rhel7vm1.summit.example.com`.

Red Hat Insights



12. Use your browser's search function to search for "**payload injection**". You will notice that this payload injection issue is no longer listed due to fixing the vulnerability.

hostname:
rhel7vm1.summit.example.com
UUID: f20ef3dd-ccaa-41c4-88c3-3195a26b28e6

OS	Red Hat Enterprise Linux Server release 7.0 (Maipo)	BIOS Version	SeaBIOS seabios
Registration Date	10 days ago	BIOS Release Date	
Last Check In	2 minutes ago		

Security > OpenSSL vulnerable to very efficient session decryption (CVE-2016-0800/Special DROWN)

Detected issue
This host is vulnerable because it has vulnerable package `openssl-libs-1.0.1e-34.el7` installed.

This package does not have a patch for **CVE-2015-0293** applied, which makes the system especially vulnerable. This is known as **Special DROWN**. An attacker can use this flaw to perform active man-in-the-middle (MITM) attacks and impersonate a TLS server to connecting TLS client in a matter of minutes.

Fortunately, it does not seem to run any processes that use OpenSSL libraries.

Steps to resolve
Red Hat recommends the following steps to resolve the affected system:

```
# yum update openssl
# reboot
```

Alternatively, you can re-link the openssl libraries to the IP addresses.

payload injection | Highlight All | Match Case | Phrase not found

Congratulations, you're no longer vulnerable to the payload injection vulnerability!

Lab 9: Viewing Red Hat Insights security findings from Red Hat CloudForms

Goal of Lab 9

The goal of this lab is to show the ability to view Red Hat Insights security findings on a particular VM right from the GUI of Red Hat CloudForms.

Introduction

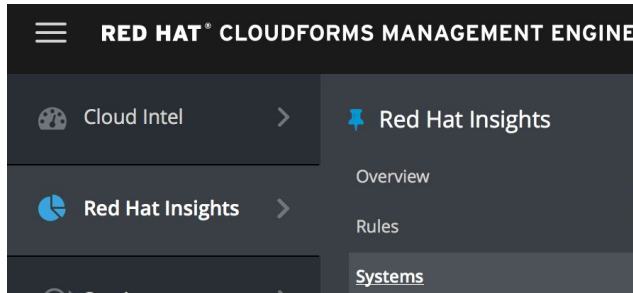
In addition to being able to view Red Hat Insights results from the customer portal and Red Hat Satellite 6, you can also view the Red Hat Insights findings from Red Hat CloudForms.

This allows you to use Red Hat CloudForms as the central management tool to view and control your entire heterogeneous infrastructure from a single place.

View Red Hat Insights security findings from Red Hat CloudForms

1. In your Firefox web browser, click on the tab you have opened to your Red Hat CloudForms UI. Log back in with **admin** as the username and **r3dh@t2017** as your password.

2. In the Red Hat CloudForms UI, in the left pane, navigate to **Red Hat Insights** → **Systems**.



3. Notice that the **rhel7vm1.summit.example.com** is listed. **Click on this VM.**

Systems

🚫 1 System with actions ✅ 0 Systems with no actions

Filter by System Actions

ALL SYSTEMS 🚫 WITH ACTIONS ✅ WITHOUT ACTIONS

<input type="checkbox"/>	Hostname
	Filter
<input type="checkbox"/>	rhel7vm1.summit.example.com ←

4. Now take a look at all the security issues detected by Red Hat Insights and recommended steps to resolve the issues. Use your browser's search function to search for "**payload injection**" here as well. You will notice that this payload injection issue doesn't show up in this view as well due to fixing the vulnerability earlier.

RED HAT CLOUDFORMS MANAGEMENT ENGINE

Cloud Intel >

Red Hat Insights >

Services >

Compute >

Configuration >

Networks >

Middleware >

Storage >

Control >

Automate >

Optimize >

hostname:rhel7vm1.summit.example.com

Security > OpenSSL vulnerable to very efficient session decryption (CVE-2016-0800/Special DROWN)

Detected issue

This host is vulnerable because it has vulnerable package `openssl-libs-1.0.1e-34.el7` installed.

This package does not have a patch for [CVE-2015-0293](#) applied, which makes the system especially vulnerable. This is known as **Special DROWN**. An attacker can use this flaw to perform active man-in-the-middle (MITM) attacks and impersonate a TLS server to connecting TLS client in a matter of minutes.

Fortunately, it does not seem to run any processes that use OpenSSL libraries.

A new cross-protocol attack against a vulnerability in the SSLv2 protocol has been found. It can be used to passively decrypt collected TLS/SSL sessions from any connection that

Steps to resolve

Red Hat recommends that you update `openssl` and rest

```
# yum update openssl
# reboot
```

Alternatively, you can restart all affected services (that is, especially those listening on public IP addresses.

payload injection

Highlight All Match Case Phrase not found

5. Click the x at the top right when you are done glancing through the security issues. We will not be fixing any other Red Hat Insights security findings.

RED HAT CLOUDFORMS MANAGEMENT ENGINE

Cloud Intel >

Red Hat Insights >

Services >

Compute >

hostname:rhel7vm1.summit.example.com

Security > OpenSSL vulnerable to very efficient session decryption (CVE-2016-0800/Special DROWN)

Close (x)

Collapse All