Automating Security and Compliance for Hybrid Environments

Lucy Kerner

Senior Principal Security Global Technical Evangelist & Strategist

lkerner@redhat.com

Twitter: @LucyCloudBling

whoami

LUCY KERNER

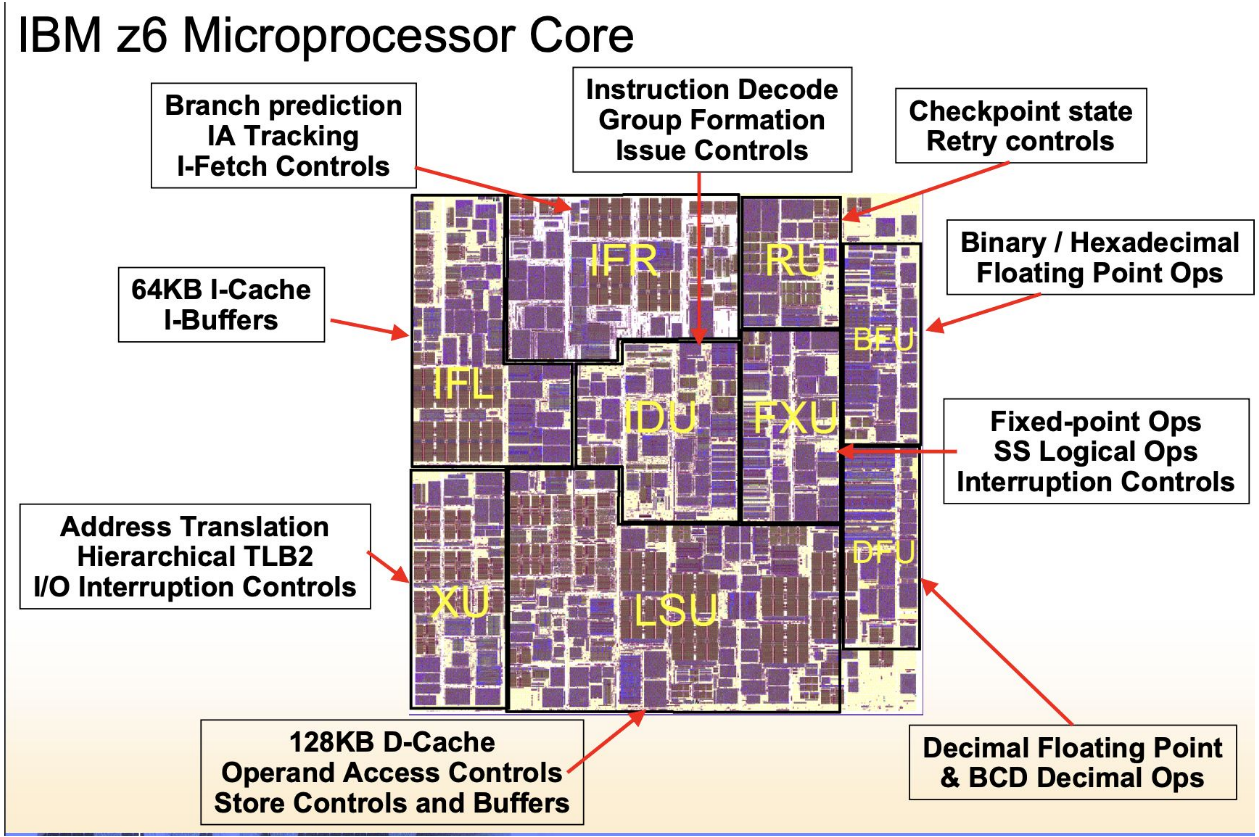
Security Global Technical Evangelist & Strategist

My first job was at my parent's restaurant

Carnegie Mellon University

Electrical & Computer ENGINEERING

whoami



IBM z6 Microprocessor Core

Branch prediction
IA Tracking
I-Fetch Controls

Instruction Decode
Group Formation
Issue Controls

Checkpoint state
Retry controls

64KB I-Cache
I-Buffers

Binary / Hexadecimal
Floating Point Ops

Fixed-point Ops
SS Logical Ops
Interruption Controls

Address Translation
Hierarchical TLB2
I/O Interruption Controls

128KB D-Cache
Operand Access Controls
Store Controls and Buffers

Decimal Floating Point
& BCD Decimal Ops

CYBERSECURITY ATTACKS ARE CONTINUOUSLY CHANGING

Meltdown and Spectre

Vulnerabilities in modern processors leak passwords and sensitive data.

2018 speech by David Hogue, a National Security Agency official, who said the NSA had not responded to an intrusion that exploited a zero-day vulnerability in over two years.

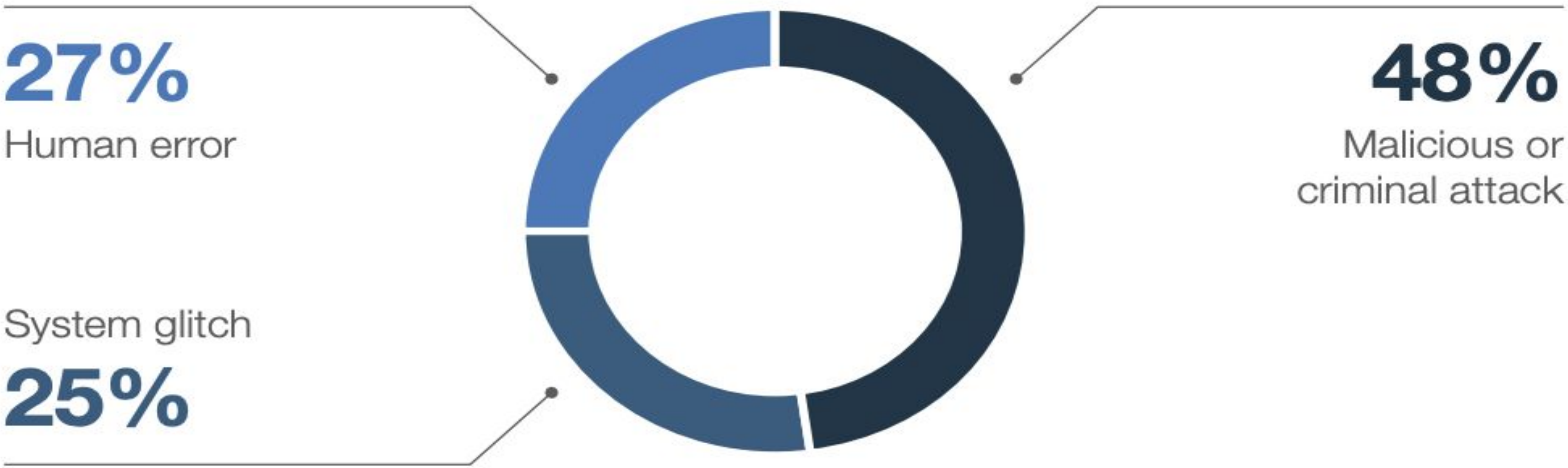
99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident[3]

81% of hacking-related breaches leveraged either stolen and/or weak passwords[1]

68% of breaches took months or longer to discover[2]

[1] 2017 Verizon Data Breach Investigations Report
[2] 2018 Verizon Data Breach Investigations Report
[3] Gartner, "Focus on the Biggest Security Threats, Not the Most Publicized," November, 2017

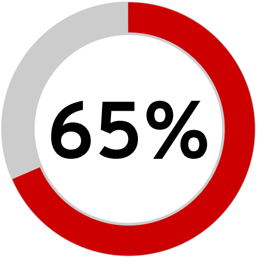
Distribution of the benchmark sample by root cause of the data breach



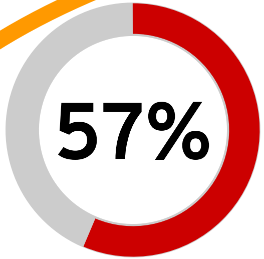
“77% of firms surveyed lack proper security incident response plans”

The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)

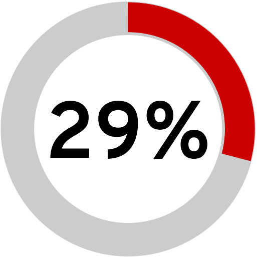
The Cyber Security Challenge is Not Getting Easier



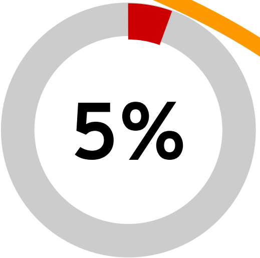
Reported increased severity of attacks [1]



Said the time to resolve an incident has grown [1]



Have their ideal security-skilled staffing level, making it the #2 barrier to cyber resilience [1]



Portion of alerts coming in that the average security team examines every day [2]

[1] The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)

[2] https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/

SECURITY PRACTICES, POLICIES, AND TOOLS HAVEN'T FULLY CAUGHT UP WITH CLOUD TECHNOLOGIES

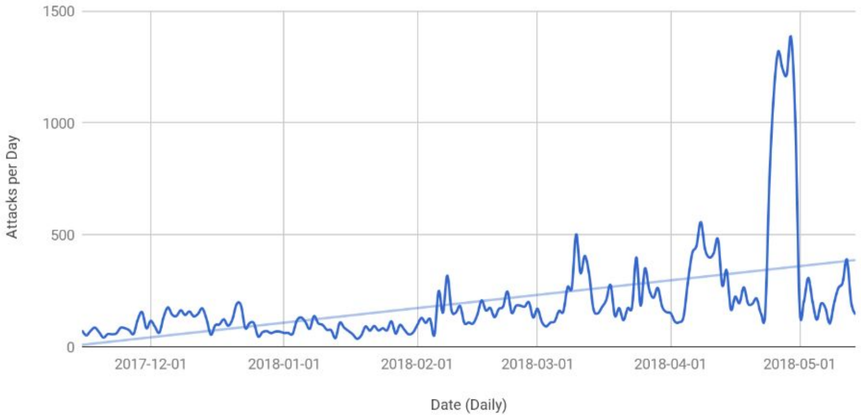
> *"According to analyst firm McKinsey, a full 78 percent of more than 100 firms recently surveyed are NOT reconfiguring their security tools when migrating to the cloud"*

Source: B. Cameron Gain for thenewstack.io, *Microservices Security: Probably Not What You Think It Is*, Mar 2018
https://thenewstack.io/microservices-security-probably-not-what-you-think-it-is/

DEVELOPERS AREN'T SECURITY EXPERTS

L7 ATTACKS ON THE RISE

"In the last 6 months we have seen a large upward trend of Layer 7 based DDoS attacks… On average seeing around 160 attacks a day, with some days spiking up to over 1000 attacks."



blog.cloudflare.com/rate-limiting-delivering-more-rules-and-greater-control/

MICROSERVICES

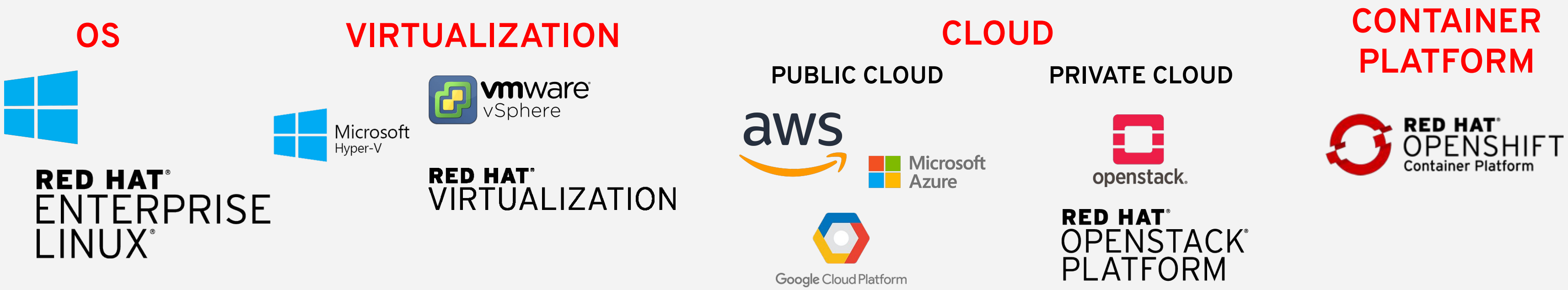
A BLESSING AND A CURSE FOR SECURITY

"The softest target in most organizations is the app layer and attackers know this. Microservices thus both make this problem harder and easier for the defenders"

Many separate APIs and ports per app == numerous doors for attackers

Source: B. Cameron Gain for thenewstack.io, *Microservices Security: Probably Not What You Think It Is*, Mar 2018
https://thenewstack.io/microservices-security-probably-not-what-you-think-it-is/

Security, Compliance and Governance Challenges in Hybrid Environments



OS

VIRTUALIZATION

CLOUD

PUBLIC CLOUD

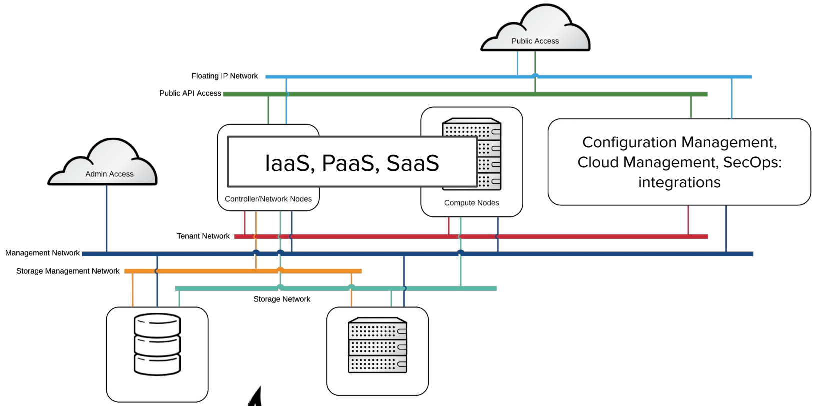
PRIVATE CLOUD

CONTAINER PLATFORM

- Increasing complexity introduces risk
- Decreased visibility and control

- Inconsistent configurations and patching
- Manually monitoring & managing systems for security and compliance becomes ***impossible***

Dealing with Compliance Adds More Complexity



ANSSI
Agence Nationale de la Sécurité des Systèmes d'Information
PCI Security Standards Council
DISA
AICPA SOC
ETSI
FedRAMP
HIPAA
COBIT 5
NIAP
Common Criteria
cloud security alliance CSA
NIST
ISO 27001
International Organization for Standardization
GSA

Compliance and Security Artifacts

System Security Plans, Gap Analysis Reports
Audit and Remediation Baselines, General Security Documentation

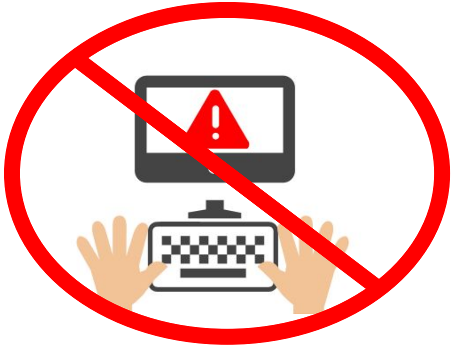
“The Bad Guys use Automation - Fight Fire with Fire” [1]

[1] Reduce Risk and Improve Security Through Infrastructure Automation (Forrester, June 2018)

“We cannot be left behind. China, Russia, and North Korea are already massively implementing Automation and DevSecOps.” [1]

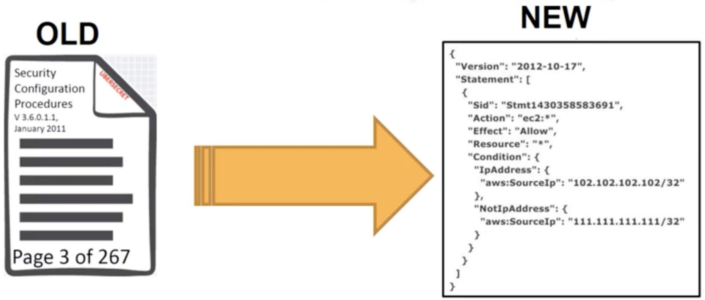
[1] Quote from Nicolas Chaillan, US DoD Special Advisor for Cloud Security and DevSecOps

Automation for Increased Security and Compliance



Continuous Monitoring & Controlled Remediations for Security + Compliance

Bake Security into Dev & Ops

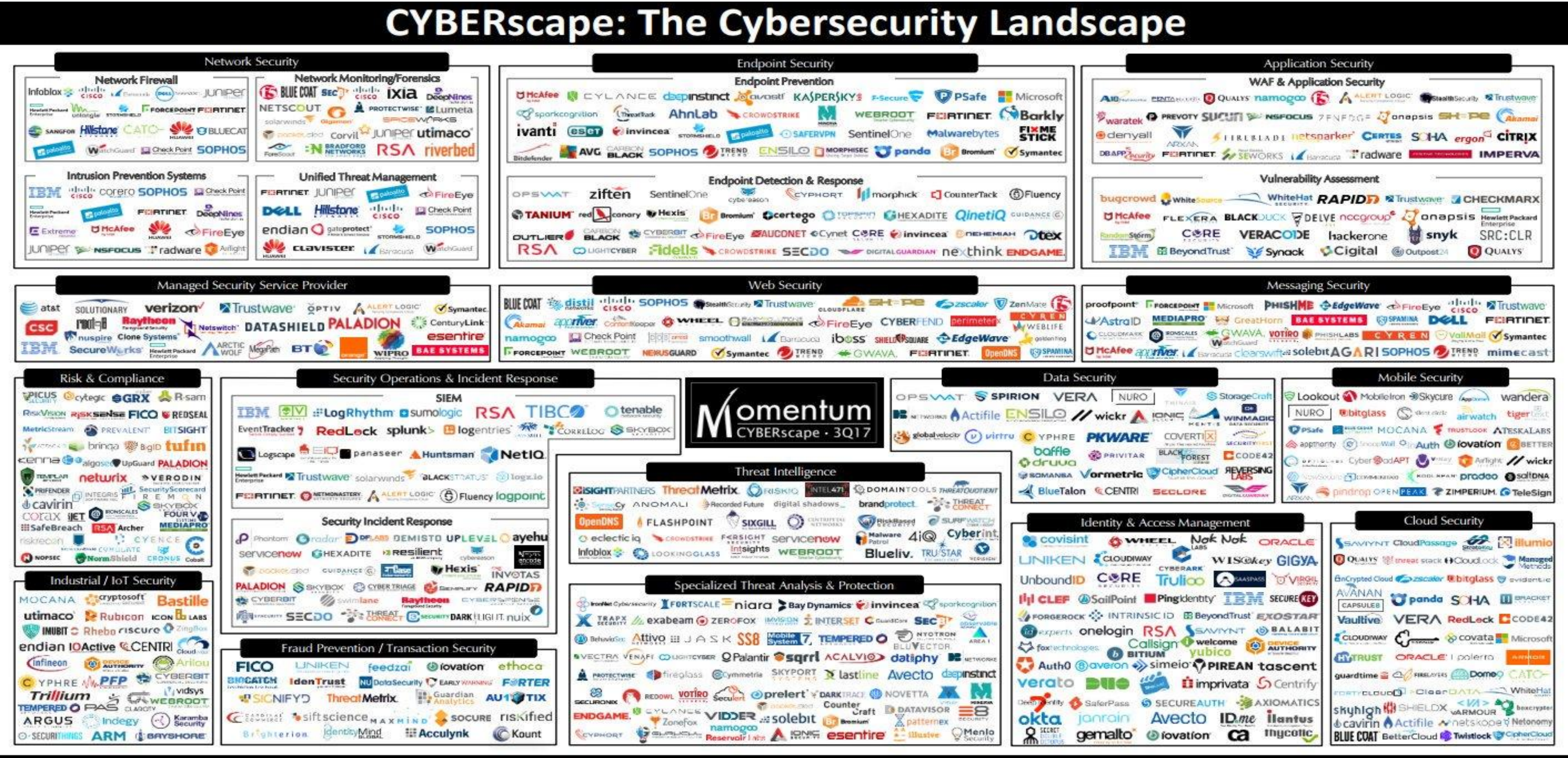


```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "Stmt1430358583691",
   "Action": "ec2:*",
   "Effect": "Allow",
   "Resource": "*",
   "Condition": {
    "IpAddress": {
     "aws:SourceIp": "102.102.102.102/32"
    },
    "NotIpAddress": {
     "aws:SourceIp": "111.111.111.111/32"
    }
   }
  }
 ]
}
```

Infrastructure, Security, and Compliance as Code ==
Repeatable, Shareable, Verifiable

How can Red Hat help?

Welcome to the Vast World of Cybersecurity Tools


CYBERscape: The Cybersecurity Landscape
Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Web Security
Messaging Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum CYBERscape · 3Q17
Threat Intelligence
Specialized Threat Analysis & Protection
Data Security
Mobile Security
Identity & Access Management
Cloud Security
Industrial / IoT Security
Fraud Prevention / Transaction Security

Source: Momentum Partners

Let's not forget the growing # of open source security tools...

GRR
RAPID RESPONSE

osquery

Moloch

NMAP.ORG

{php}IPAM
Open-source IP address management

The Bro Network Security Monitor

VeraCrypt

WIRESHARK

NIKTO - WEB SCANNER

SNORT®

KALI
BY OFFENSIVE SECURITY

Security Onion
Peel Back the Layers of Your Network

LibreNMS

OpenVAS
Open Vulnerability Assessment System

graylog

SSH...
OpenSSH
KEEPING YOUR COMMUNIQUÉS SECRET
TOP SECRET

RAPID7
metasploit®

OSSEC

mhn
Modern Honey Network

NOT Zero Sum

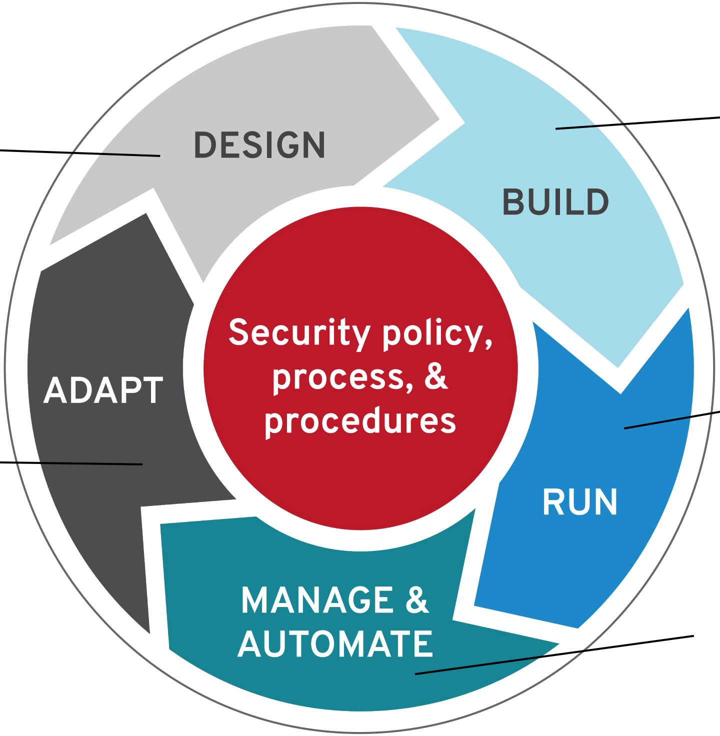
“Security is a process, NOT a product.”

– Bruce Schneier

(American cryptographer, security blogger, and author)

SECURITY MUST BE CONTINUOUS + HOLISTIC

AND INTEGRATED THROUGHOUT THE I.T. LIFE CYCLE



Identify security requirements & governance models

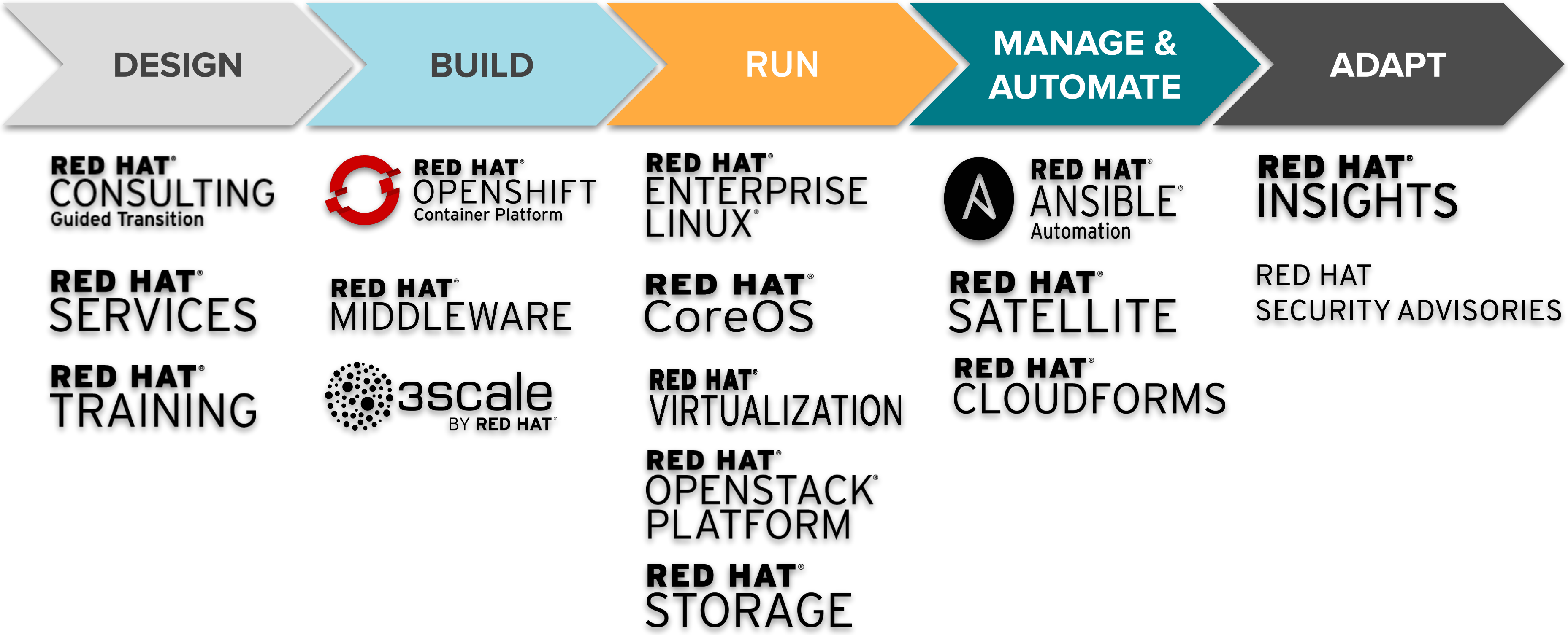
Built-in from the start; not bolted-on

Deploy to trusted platforms with enhanced security capabilities

Automate systems for security & compliance

Revise, update, remediate as the landscape changes

SECURITY THROUGHOUT THE STACK + LIFECYCLE



DESIGN

RED HAT® CONSULTING Guided Transition

RED HAT® SERVICES

RED HAT® TRAINING

BUILD

RED HAT® OPENSHIFT Container Platform

RED HAT® MIDDLEWARE

3scale BY RED HAT®

RUN

RED HAT® ENTERPRISE LINUX®

RED HAT® CoreOS

RED HAT® VIRTUALIZATION

RED HAT® OPENSTACK® PLATFORM

RED HAT® STORAGE

MANAGE & AUTOMATE

RED HAT® ANSIBLE® Automation

RED HAT® SATELLITE

RED HAT® CLOUDFORMS

ADAPT

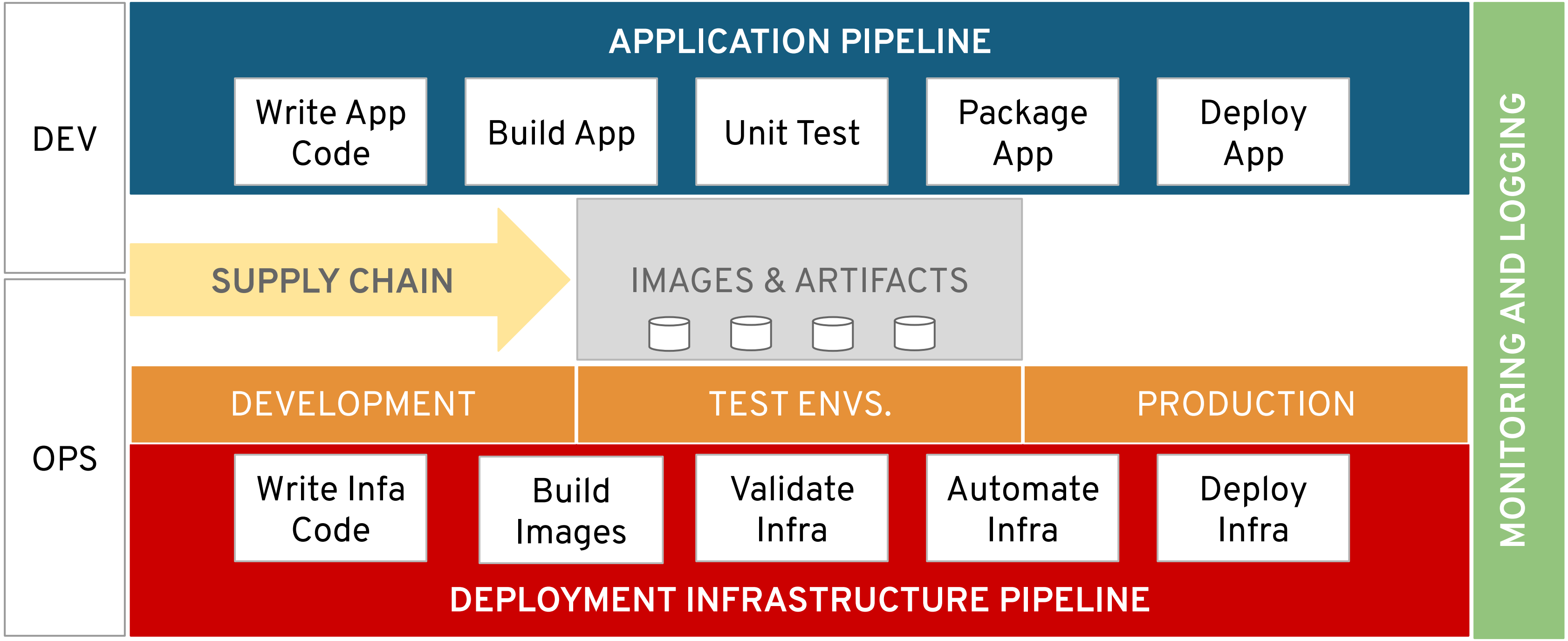
RED HAT® INSIGHTS

RED HAT SECURITY ADVISORIES

TESTED, CERTIFIED, STABLE, AND SUPPORTED OPEN SOURCE SOFTWARE

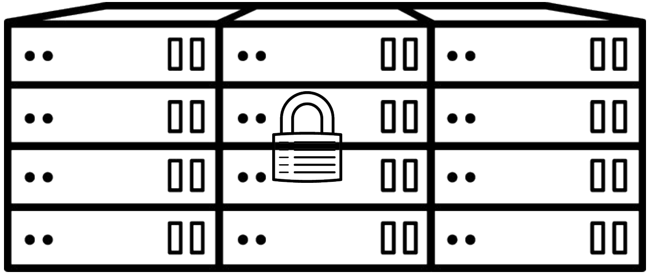
Holistic DevSecOps with Red Hat

It’s not just about the application CI/CD pipeline!



Automated Security and Compliance with Red Hat

Applications



Infrastructure and Operations

Security Operations Center
(SOC)

Automated Security and Compliance with Red Hat

DevSecOps and Building Security into the Application

Applications

Enabling Faster & Scalable DevSecOps with Red Hat OpenShift Container Platform

AUTOMATED BUILDS

CI/CD using Jenkins

Tekton

Source-2-Image

Buildah

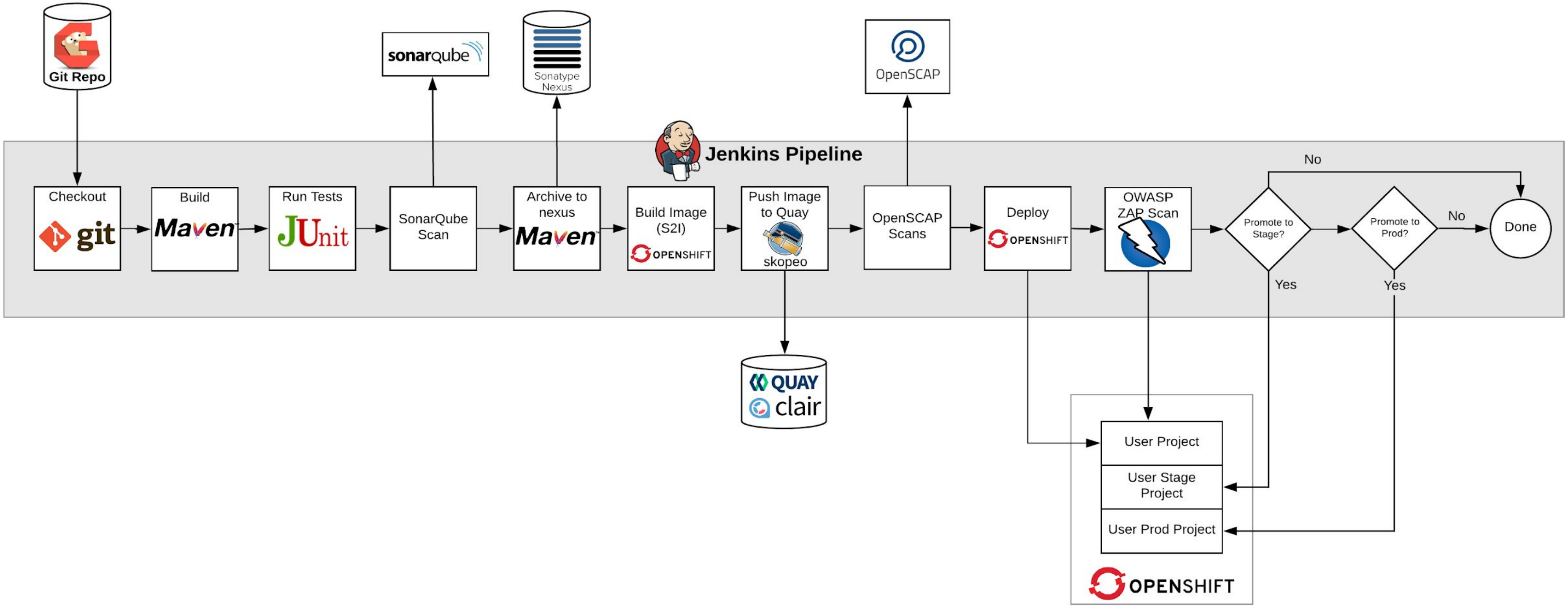
CONTINUOUS BUILT-IN SECURITY

Automated analysis with SonarQube, OWASP Dependency Check, NPM Audit, OWASP Zed Attack Proxy, OpenSCAP, etc...

AUTOMATED OPERATIONS

OpenShift Operators to monitor and respond to changing needs, load, threats, etc..

DevSecOps and Building Security into the Application with an Automated 'Software Factory'

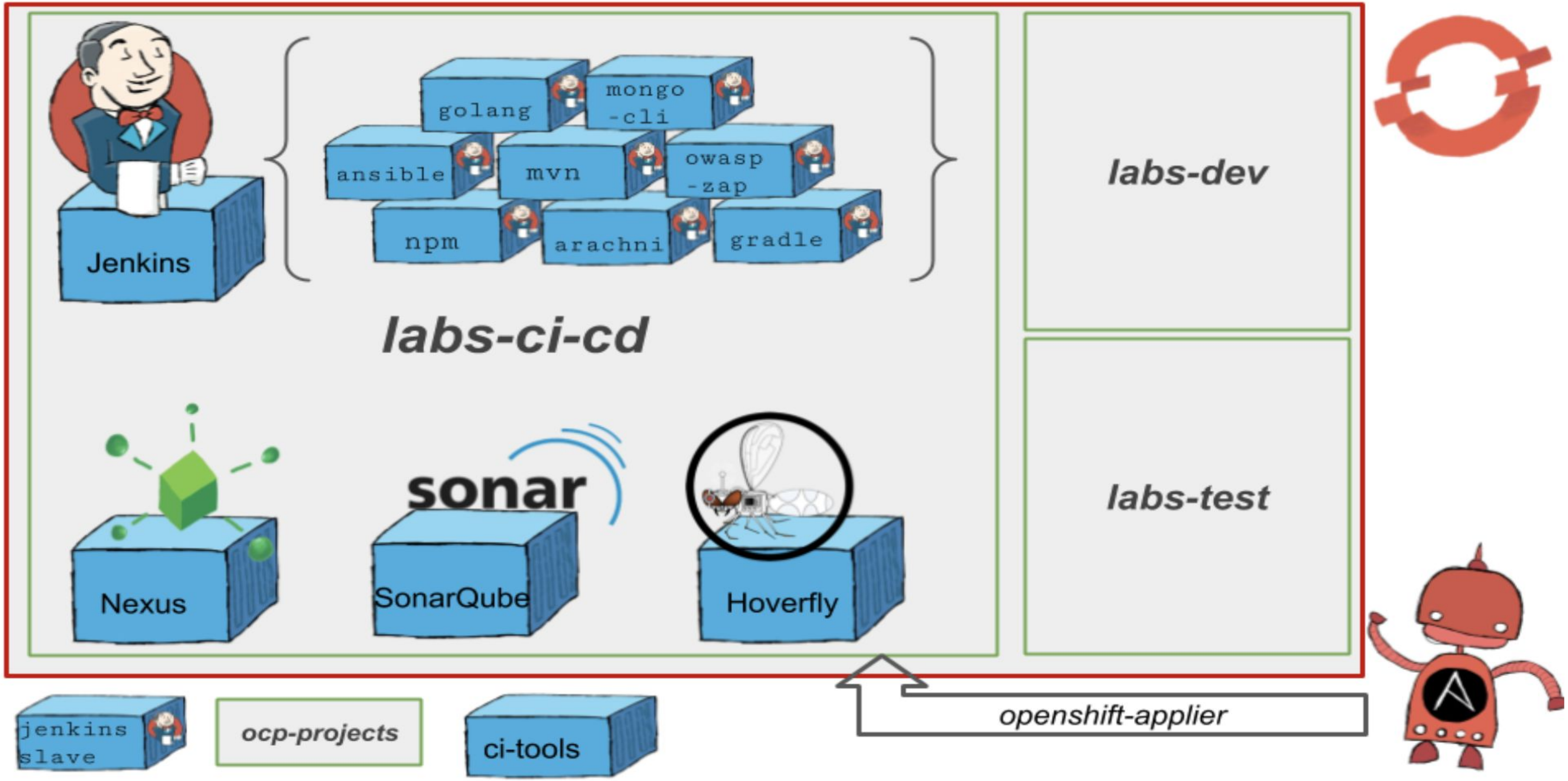


2019 Red Hat Summit Security Hands-On Labs

https://red.ht/securitylabs

The DevSecOps pipeline from the previous slide was implemented in the 'Proactive Security' lab that my team and I created. See link above for more details. You'll also find all 3 Security hands-on labs that we created for Red Hat Summit 2019.

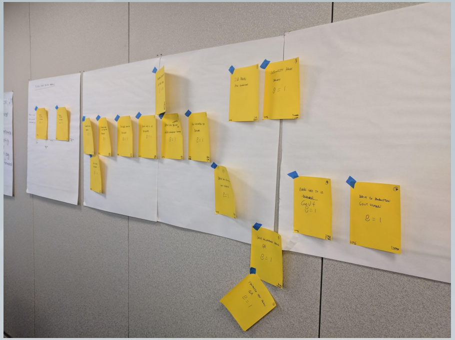
Red Hat Innovation Labs Provides You the Easy Button to Accelerate Your DevSecOps!

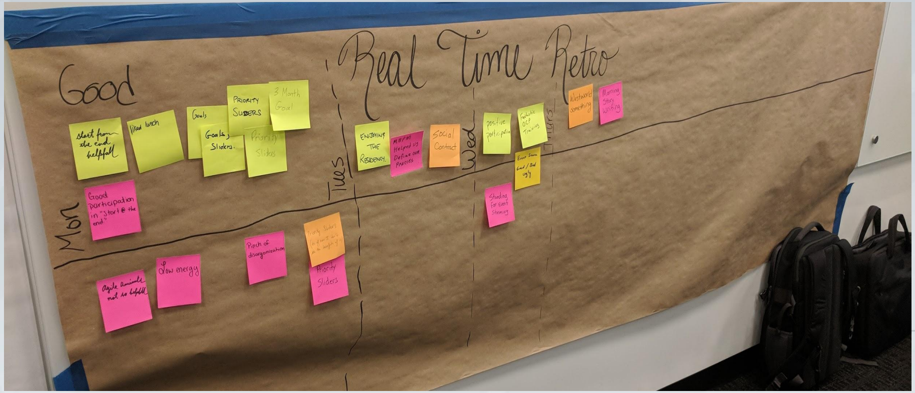


Red Hat Provides You the Easy Button to Accelerate Your DevSecOps!

- **Red Hat Innovation Labs “easy button” Ansible playbook to deploy CI/CD environment onto OpenShift**
  - Deploys these tools:
    - SonarQube and associated PostgreSQL database
    - Sonatype Nexus as an artifact repository
    - Jenkins
    - Hoverfly - create isolated test environments by simulating test dependencies.
    - Selenium Grid- parallel tests
  - Example pipelines which use this tooling: https://github.com/redhat-cop/container-pipelines
  - We can help you jump-start your journey with our Open Source tools like CASL-Ansible, infra-ansible, openshift-applier, labs-ci-cd

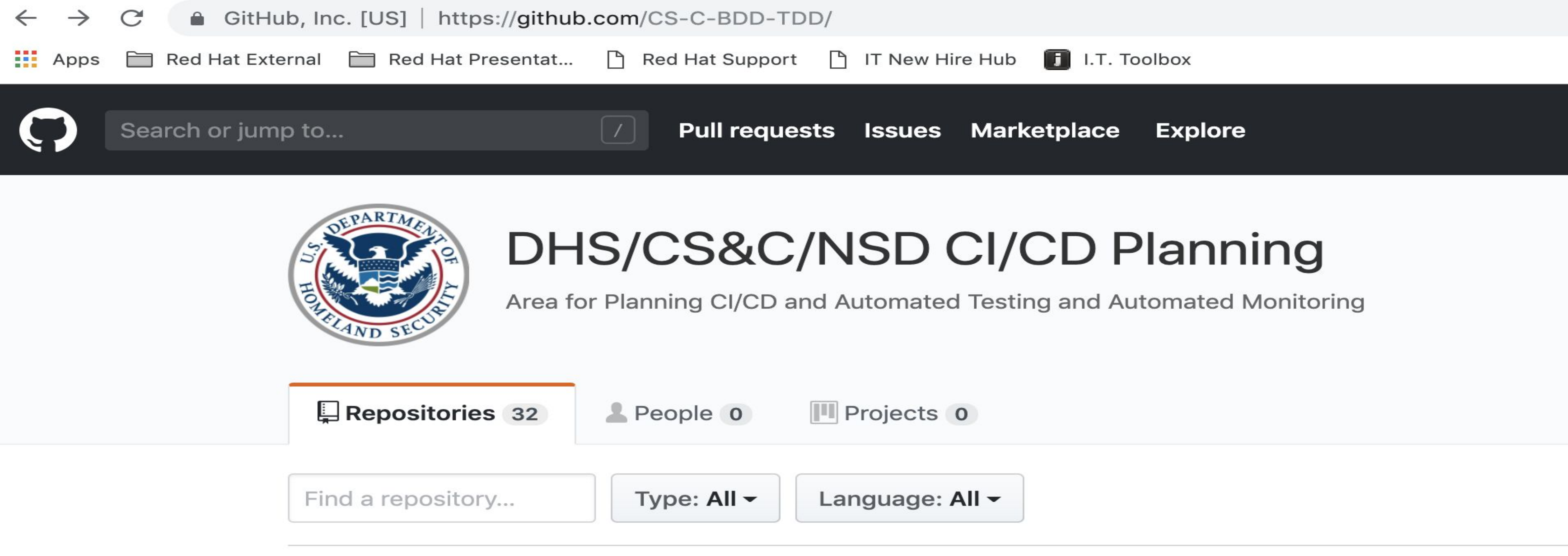
Accelerating DevSecOps with Red Hat Open Innovation Labs





DHS documented their entire Red Hat Innovation Labs & DevSecOps journey on Github:

- Quote from DHS: “Successful adoption of DevSecOps Best Practices through Red Hat Labs Residency”



GitHub, Inc. [US] | https://github.com/CS-C-BDD-TDD/

Apps | Red Hat External | Red Hat Presentat... | Red Hat Support | IT New Hire Hub | I.T. Toolbox

Search or jump to... | Pull requests | Issues | Marketplace | Explore

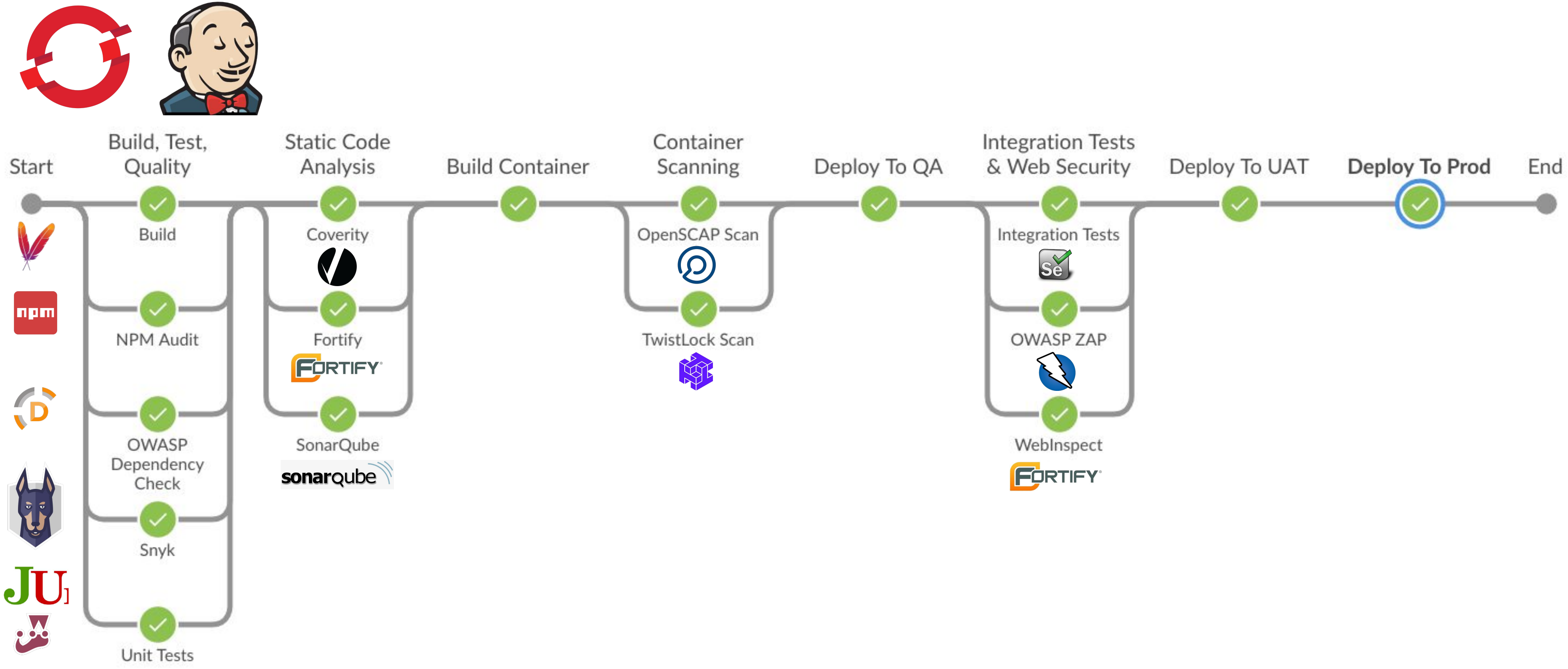
DHS/CS&C/NSD CI/CD Planning

Area for Planning CI/CD and Automated Testing and Automated Monitoring

Repositories 32 | People 0 | Projects 0

Find a repository... | Type: All | Language: All

Security Enabled Pipeline at DHS



Start

Build, Test, Quality
- Build
- NPM Audit
- OWASP Dependency Check
- Snyk
- Unit Tests

Static Code Analysis
- Coverity
- Fortify
- SonarQube

Build Container

Container Scanning
- OpenSCAP Scan
- TwistLock Scan

Deploy To QA

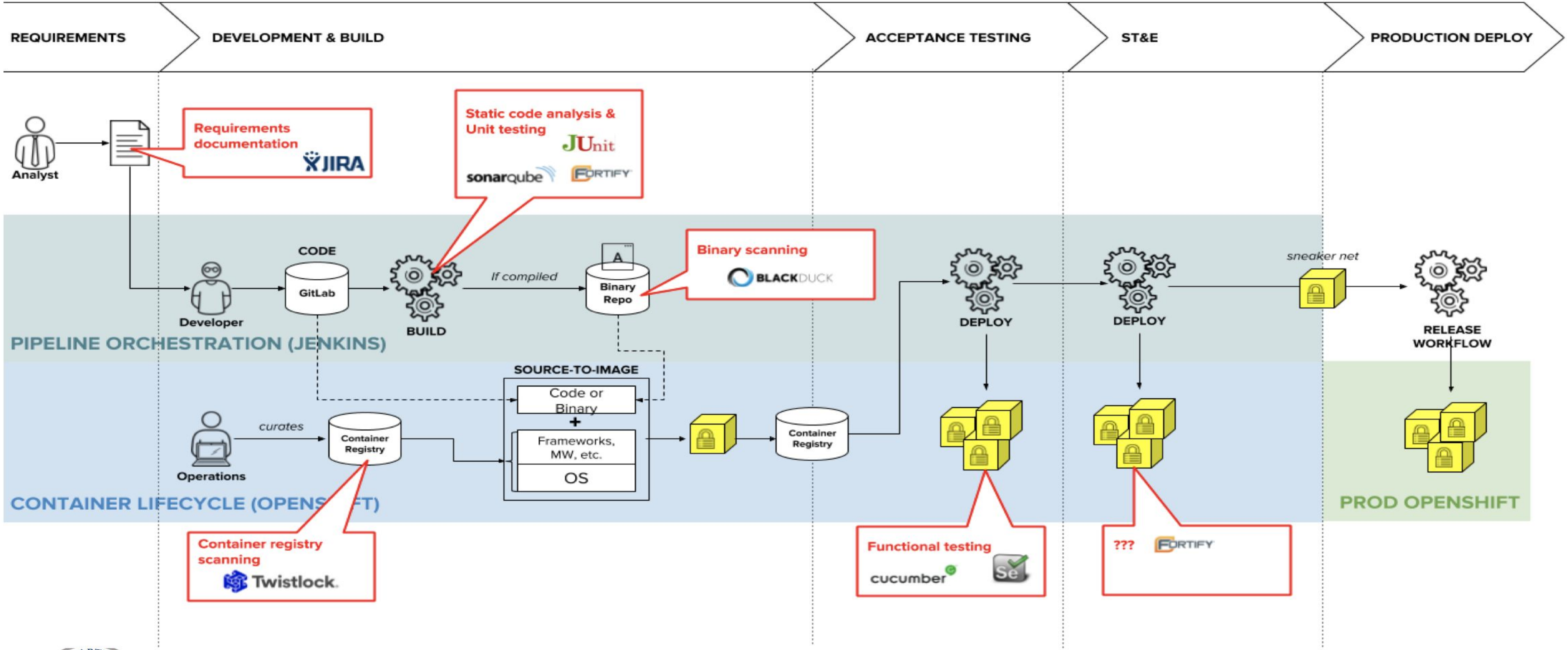
Integration Tests & Web Security
- Integration Tests
- OWASP ZAP
- WebInspect

Deploy To UAT

Deploy To Prod

End

We are leveraging CI/CD as a key practice in the enablement of DevSecOps to automate manual processes and inefficiencies in the current process.

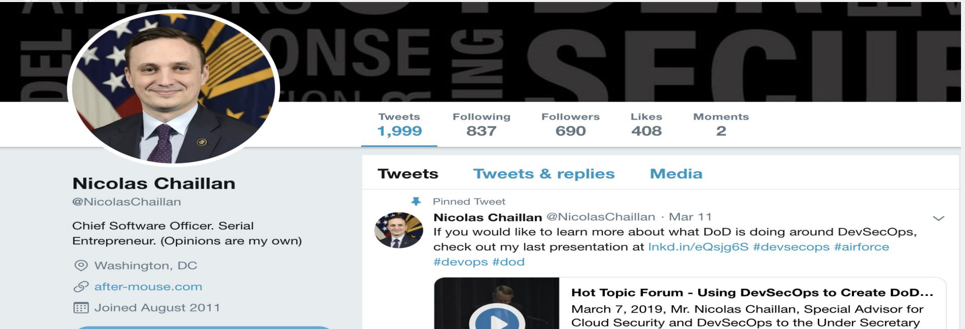


Evaluation of DevSecOps tools

- Key tools leveraged so far: Jenkins, SonarQube, Selenium, Jest, Junit, Serenity, Cucumber, Nexus, OWASP Dependency Checker, Twistlock, Ansible, Github, Jira, Confluence and Slack.
- Leveraging Red Hat OpenShift for gaining experience in working with containers in a managed environment.
- Will be utilizing VMC as a tool for testing the pipeline across air-gapped environments.
- Still to integrate OWASP ZAP, BlackDuck and Fortify into the pipeline.
- Provide feedback to stakeholders for decision-making.

DevSecOps at the US Department of Defense

https://twitter.com/nicolaschaillan



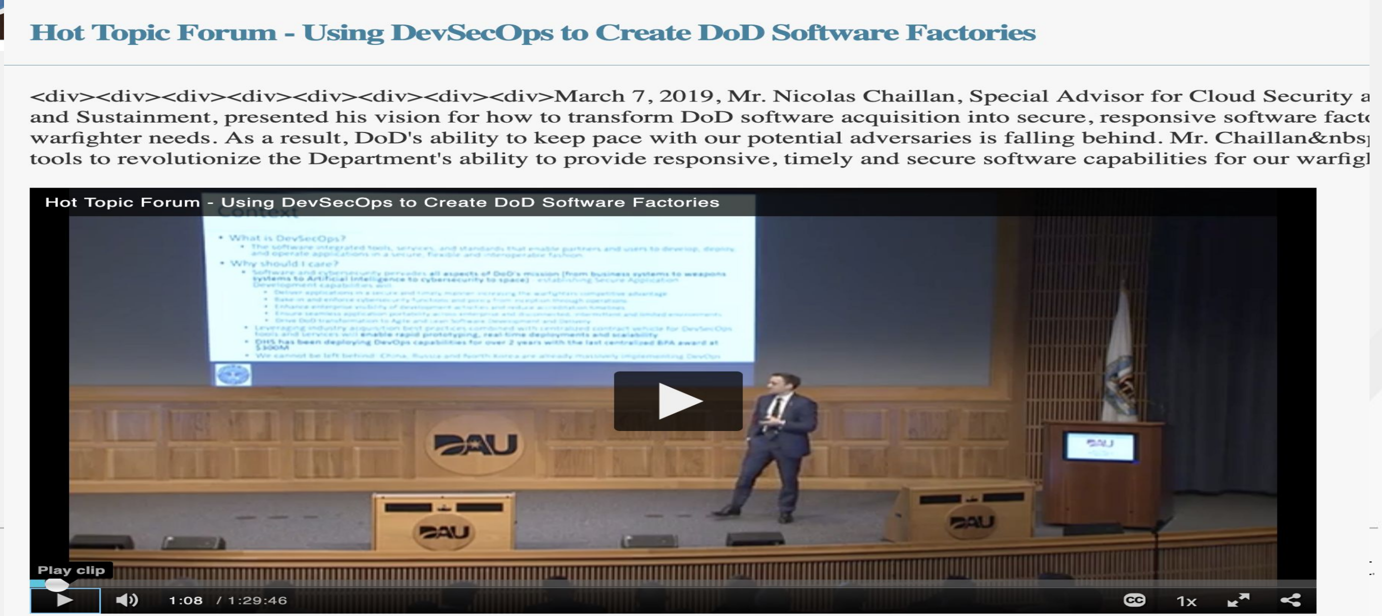
Nicolas Chaillan
@NicolasChaillan

Chief Software Officer. Serial Entrepreneur. (Opinions are my own)

Washington, DC
after-mouse.com
Joined August 2011

Pinned Tweet
Nicolas Chaillan @NicolasChaillan · Mar 11
If you would like to learn more about what DoD is doing around DevSecOps, check out my last presentation at lnkd.in/eQsjg6S #devsecops #airforce #devops #dod

Hot Topic Forum - Using DevSecOps to Create DoD...
March 7, 2019, Mr. Nicolas Chaillan, Special Advisor for Cloud Security and DevSecOps to the Under Secretary



Hot Topic Forum - Using DevSecOps to Create DoD Software Factories

<div><div><div><div><div><div><div><div>March 7, 2019, Mr. Nicolas Chaillan, Special Advisor for Cloud Security a
and Sustainment, presented his vision for how to transform DoD software acquisition into secure, responsive software facto
warfighter needs. As a result, DoD's ability to keep pace with our potential adversaries is falling behind. Mr. Chaillan&nbs
tools to revolutionize the Department's ability to provide responsive, timely and secure software capabilities for our warfig

Hot Topic Forum - Using DevSecOps to Create DoD Software Factories

Journey to DevSecOps Panel

“In Security, consistency and repeatability is key. Adopting containers in a container platform will ***improve*** *your security.”*

US Courts
US Citizen and Immigration Services
Oak Ridge National Laboratory
Internal Revenue Service

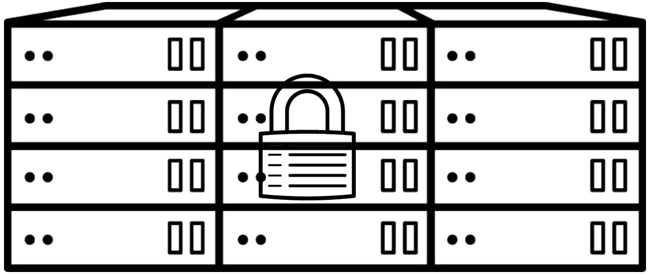
[US Government Panel, Openshift Commons Briefing]()

[Journey of DevSecOps - US Department Homeland Security]()

[Book by USCIS CIO: A Seat at the Table: IT Leadership in the Age of Agility]()

.Gov on OpenShift Panel - US Courts, USCIS/DHS, and Oak Ridge National Laboratory

Automated Security and Compliance with Red Hat



Infrastructure and Operations

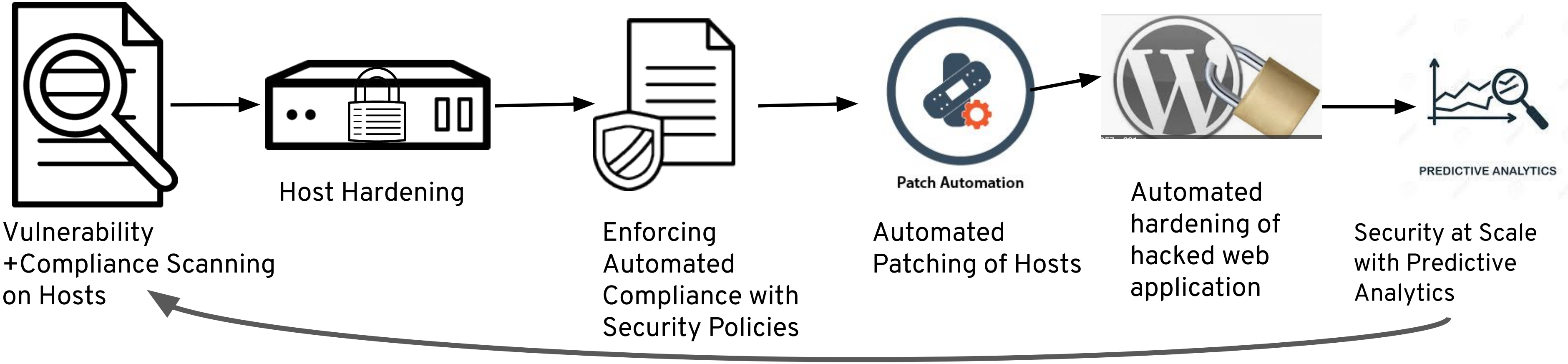
2019 Red Hat Summit Security Hands-On Labs

https://red.ht/securitylabs

(Everything you are about to see in the slides in this section has been implemented in the 'Proactive Security' lab that my teammates and I created. See the link above for more details.)

Automated Security and Compliance for Infrastructure & Operations

Infrastructure and Application Hardening Improvements with Automation



Vulnerability +Compliance Scanning on Hosts

Host Hardening

Enforcing Automated Compliance with Security Policies

Automated Patching of Hosts

Automated hardening of hacked web application

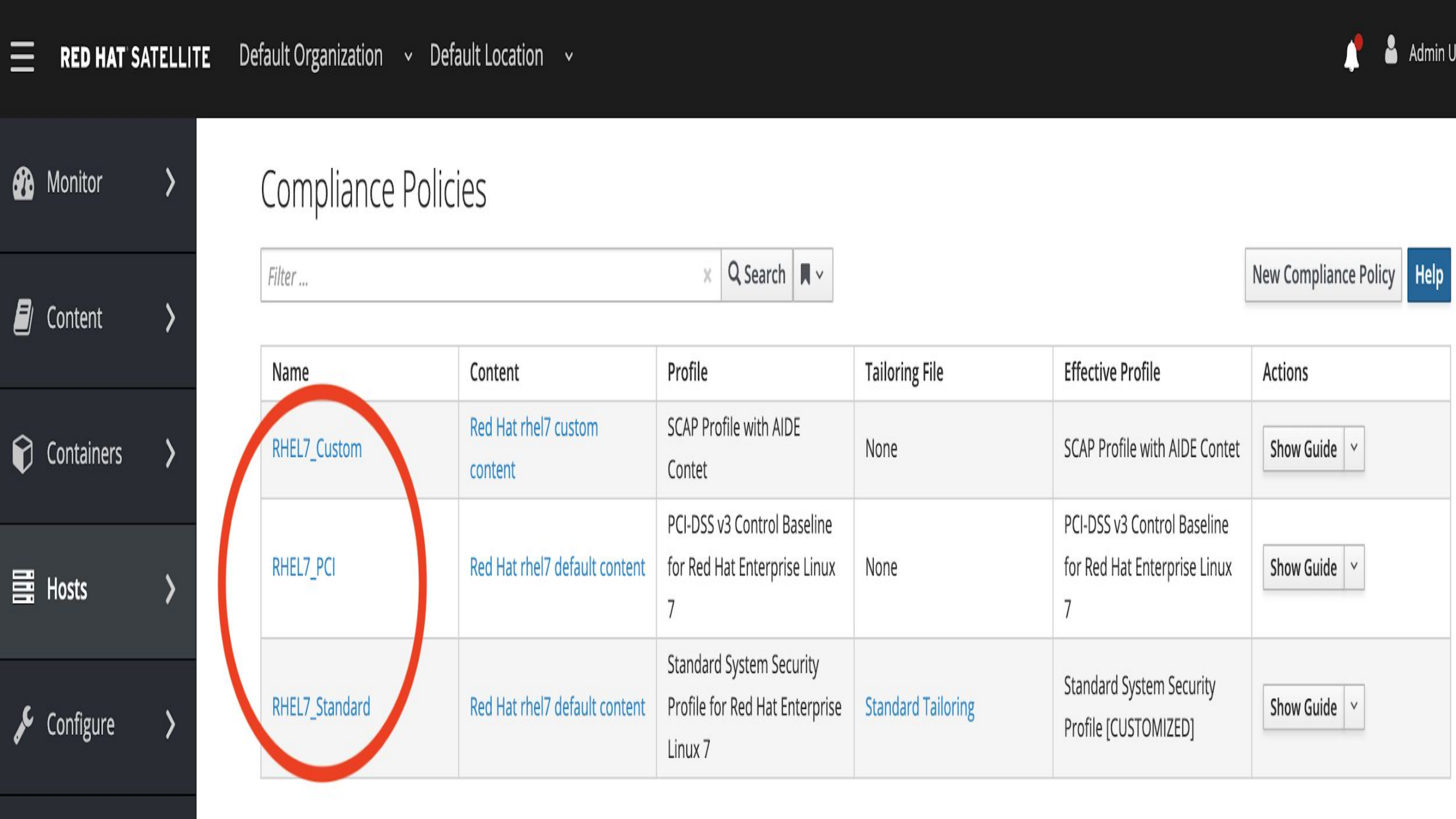
Security at Scale with Predictive Analytics

AUTOMATION IS KEY

Introduce more automation in small incremental improvements to improve security & reduce risk wherever you are on the DevSecOps journey

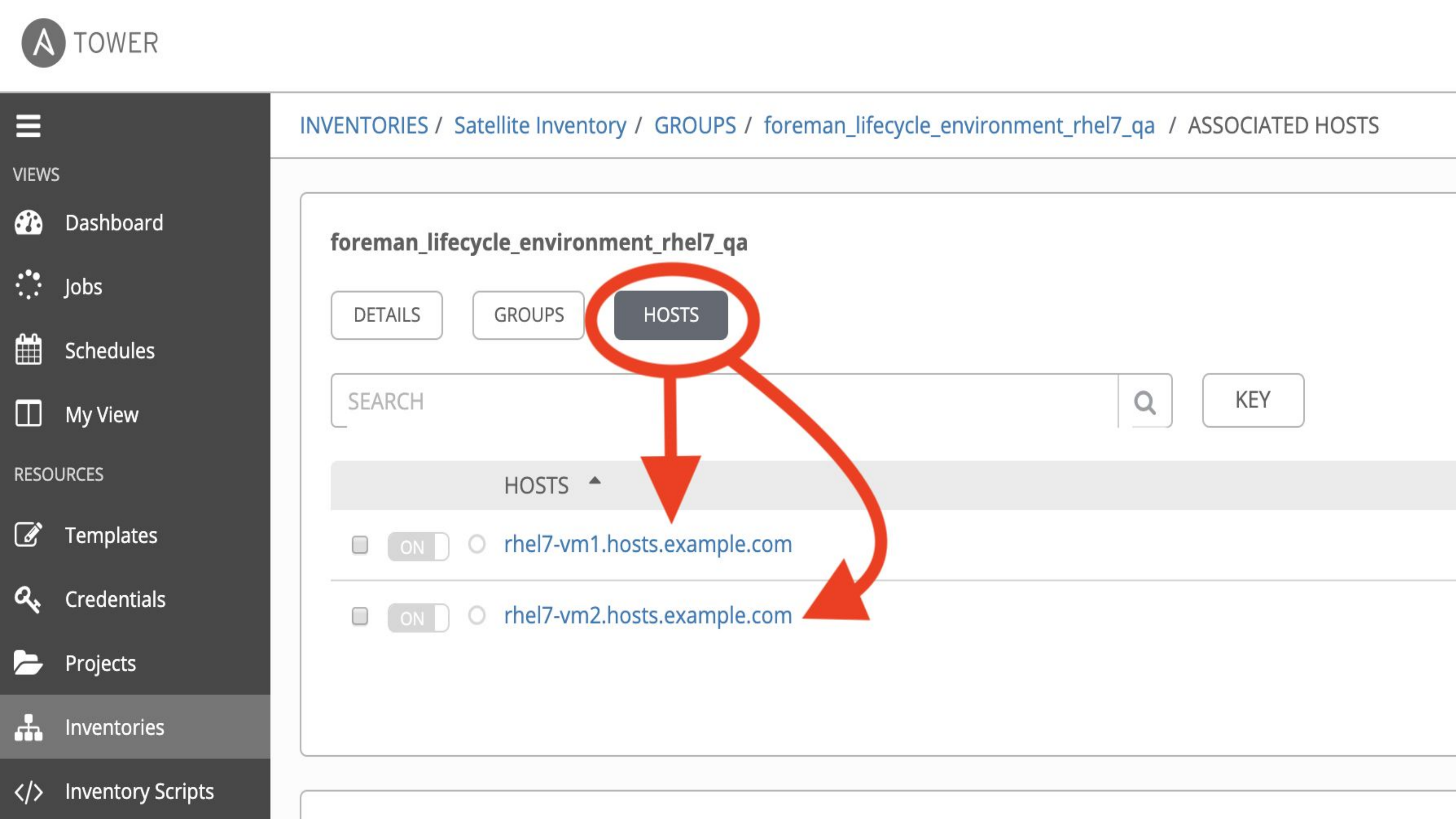
Red Hat

Vulnerability & Compliance Scanning on Hosts at Scale with Red Hat Ansible Tower + Satellite



Compliance Policies

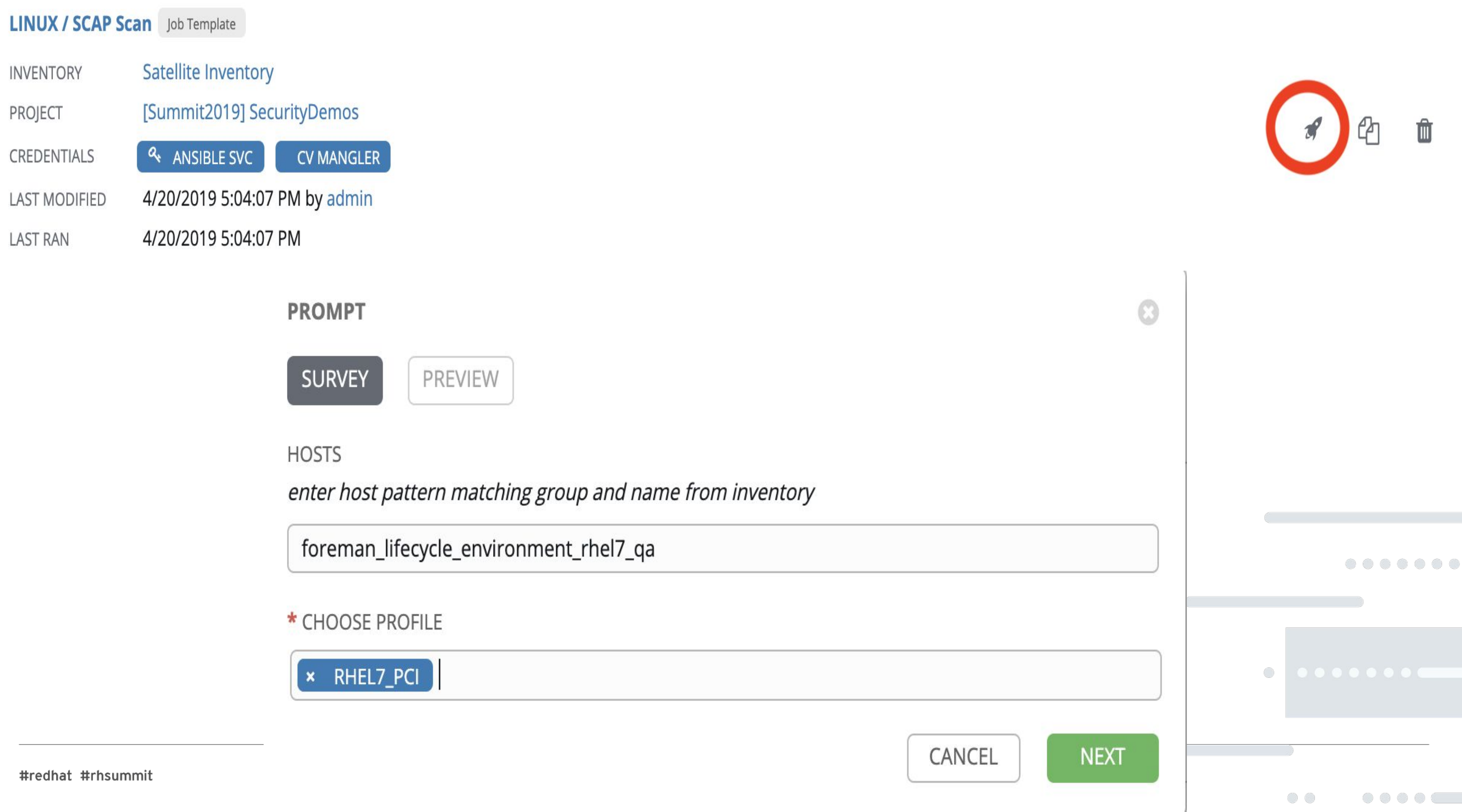
Name	Content	Profile	Tailoring File	Effective Profile	Actions
RHEL7_Custom	Red Hat rhel7 custom content	SCAP Profile with AIDE Contet	None	SCAP Profile with AIDE Contet	Show Guide
RHEL7_PCI	Red Hat rhel7 default content	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	None	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	Show Guide
RHEL7_Standard	Red Hat rhel7 default content	Standard System Security Profile for Red Hat Enterprise Linux 7	Standard Tailoring	Standard System Security Profile [CUSTOMIZED]	Show Guide



INVENTORIES / Satellite Inventory / GROUPS / foreman_lifecycle_environment_rhel7_qa / ASSOCIATED HOSTS

foreman_lifecycle_environment_rhel7_qa

			HOSTS ▲
□	ON	○	rhel7-vm1.hosts.example.com
□	ON	○	rhel7-vm2.hosts.example.com



LINUX / SCAP Scan Job Template

INVENTORY Satellite Inventory

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC CV MANGLER

LAST MODIFIED 4/20/2019 5:04:07 PM by admin

LAST RAN 4/20/2019 5:04:07 PM

PROMPT

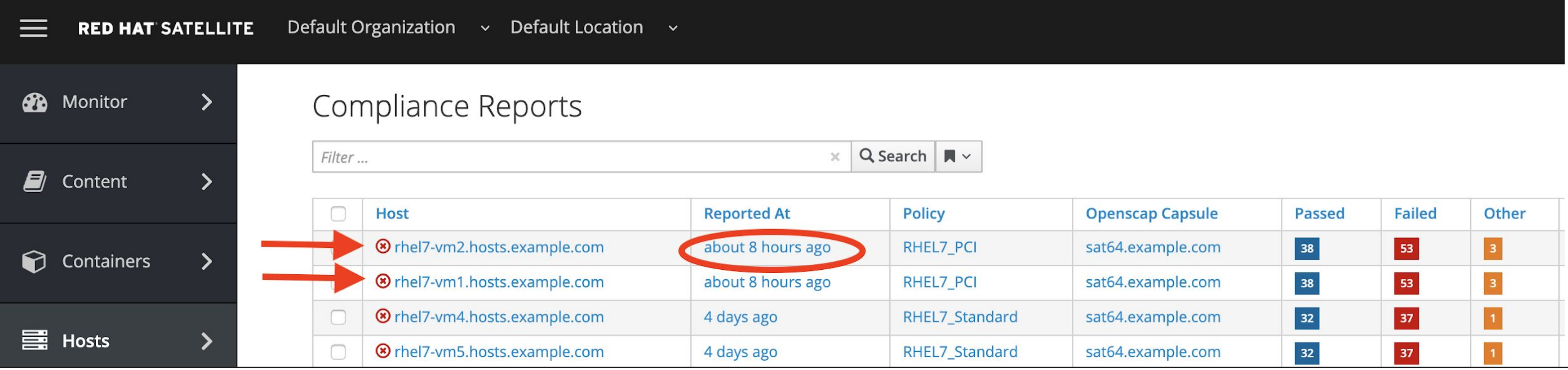
HOSTS

enter host pattern matching group and name from inventory

foreman_lifecycle_environment_rhel7_qa

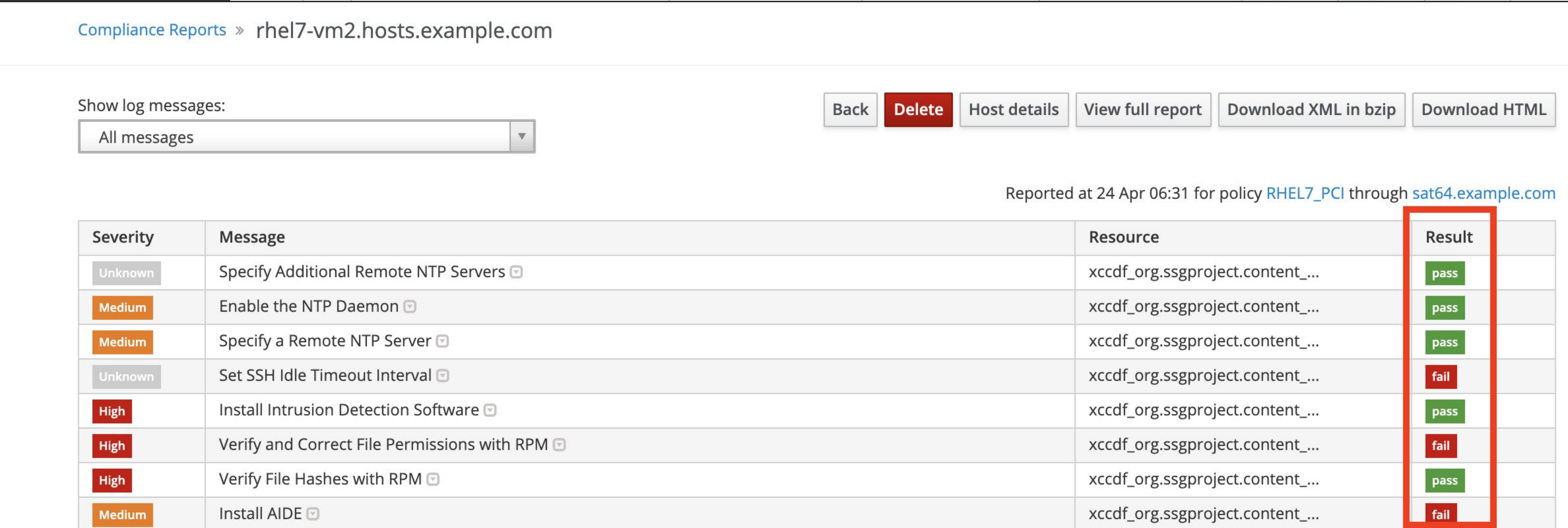
* CHOOSE PROFILE

× RHEL7_PCI



Compliance Reports

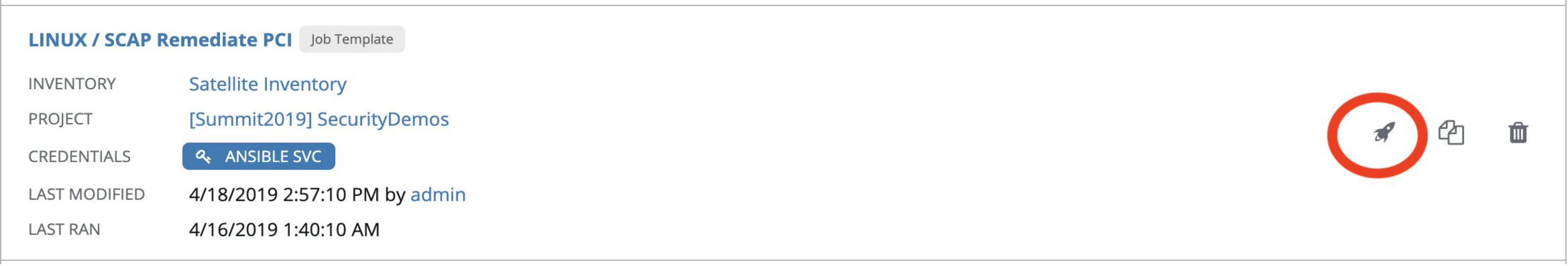
☐	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other
☐	rhel7-vm2.hosts.example.com	about 8 hours ago	RHEL7_PCI	sat64.example.com	38	53	3
☐	rhel7-vm1.hosts.example.com	about 8 hours ago	RHEL7_PCI	sat64.example.com	38	53	3
☐	rhel7-vm4.hosts.example.com	4 days ago	RHEL7_Standard	sat64.example.com	32	37	1
☐	rhel7-vm5.hosts.example.com	4 days ago	RHEL7_Standard	sat64.example.com	32	37	1



Show log messages: All messages

Reported at 24 Apr 06:31 for policy RHEL7_PCI through sat64.example.com

Severity	Message	Resource	Result
Unknown	Specify Additional Remote NTP Servers	xccdf_org.ssgproject.content_...	pass
Medium	Enable the NTP Daemon	xccdf_org.ssgproject.content_...	pass
Medium	Specify a Remote NTP Server	xccdf_org.ssgproject.content_...	pass
Unknown	Set SSH Idle Timeout Interval	xccdf_org.ssgproject.content_...	fail
High	Install Intrusion Detection Software	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
Medium	Install AIDE	xccdf_org.ssgproject.content_...	fail



LINUX / SCAP Remediate PCI

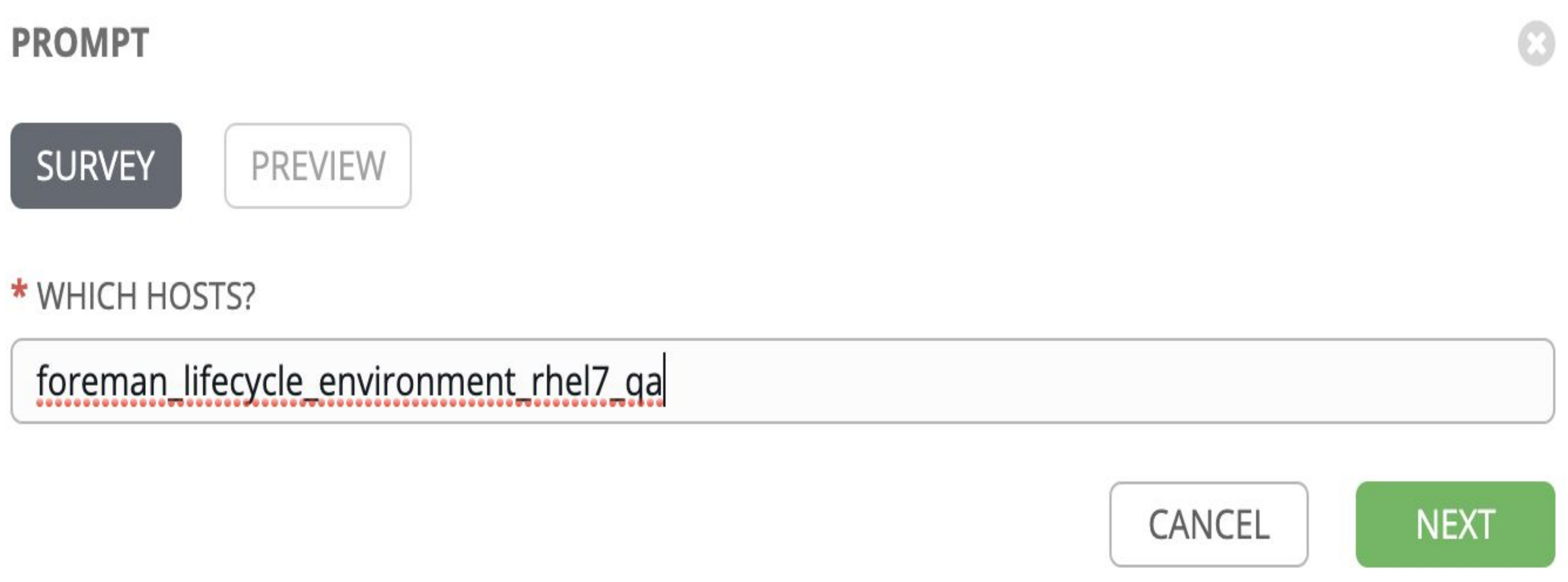
INVENTORY: Satellite Inventory

PROJECT: [Summit2019] SecurityDemos

CREDENTIALS: ANSIBLE SVC

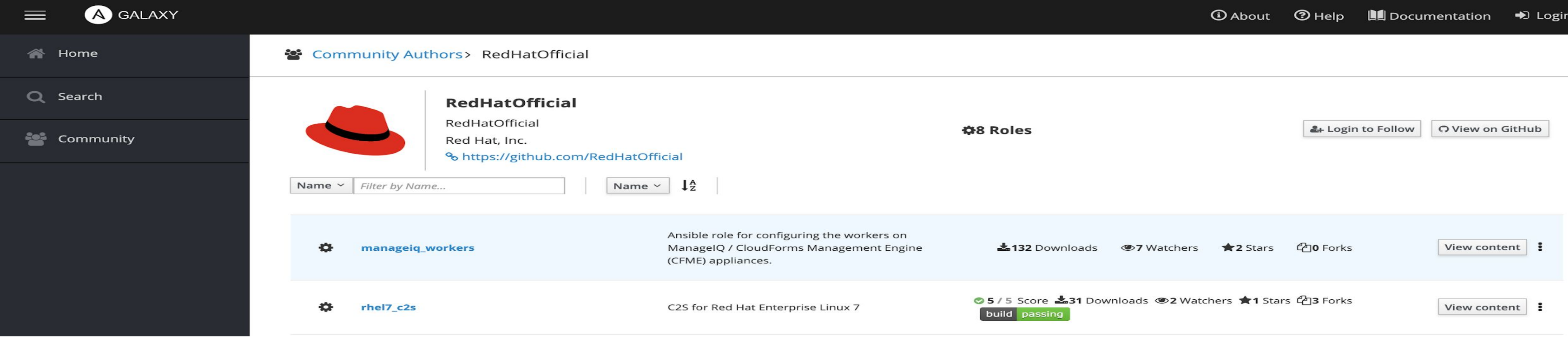
LAST MODIFIED: 4/18/2019 2:57:10 PM by admin

LAST RAN: 4/16/2019 1:40:10 AM



PROMPT

* WHICH HOSTS?: foreman_lifecycle_environment_rhel7_qa



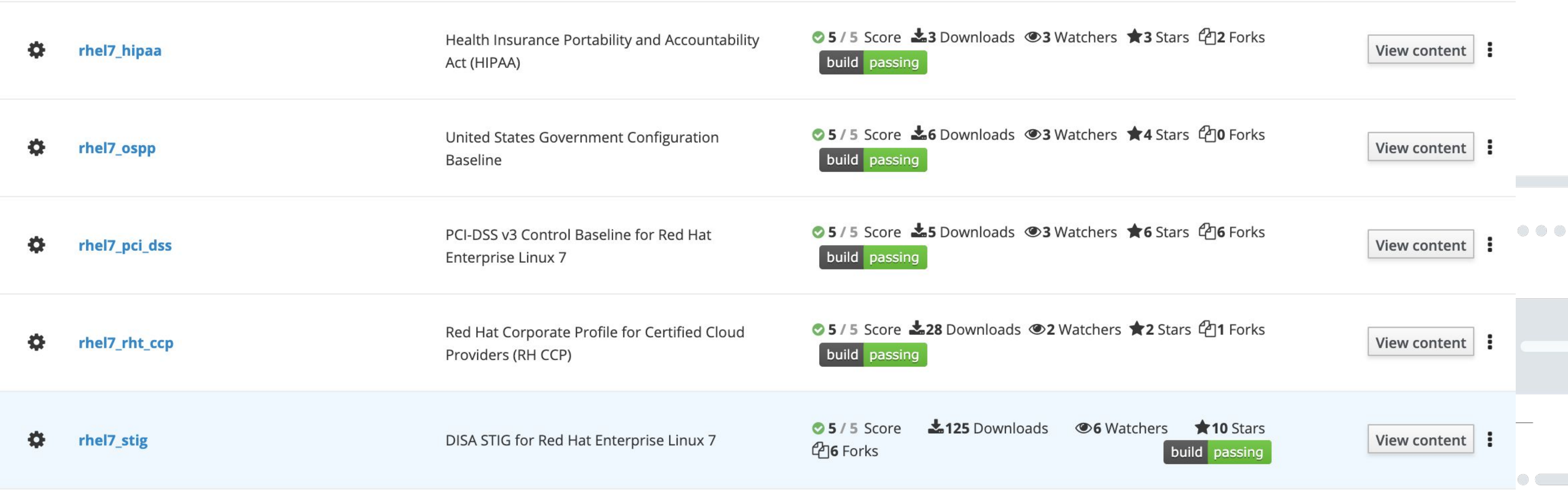
Community Authors > RedHatOfficial

RedHatOfficial

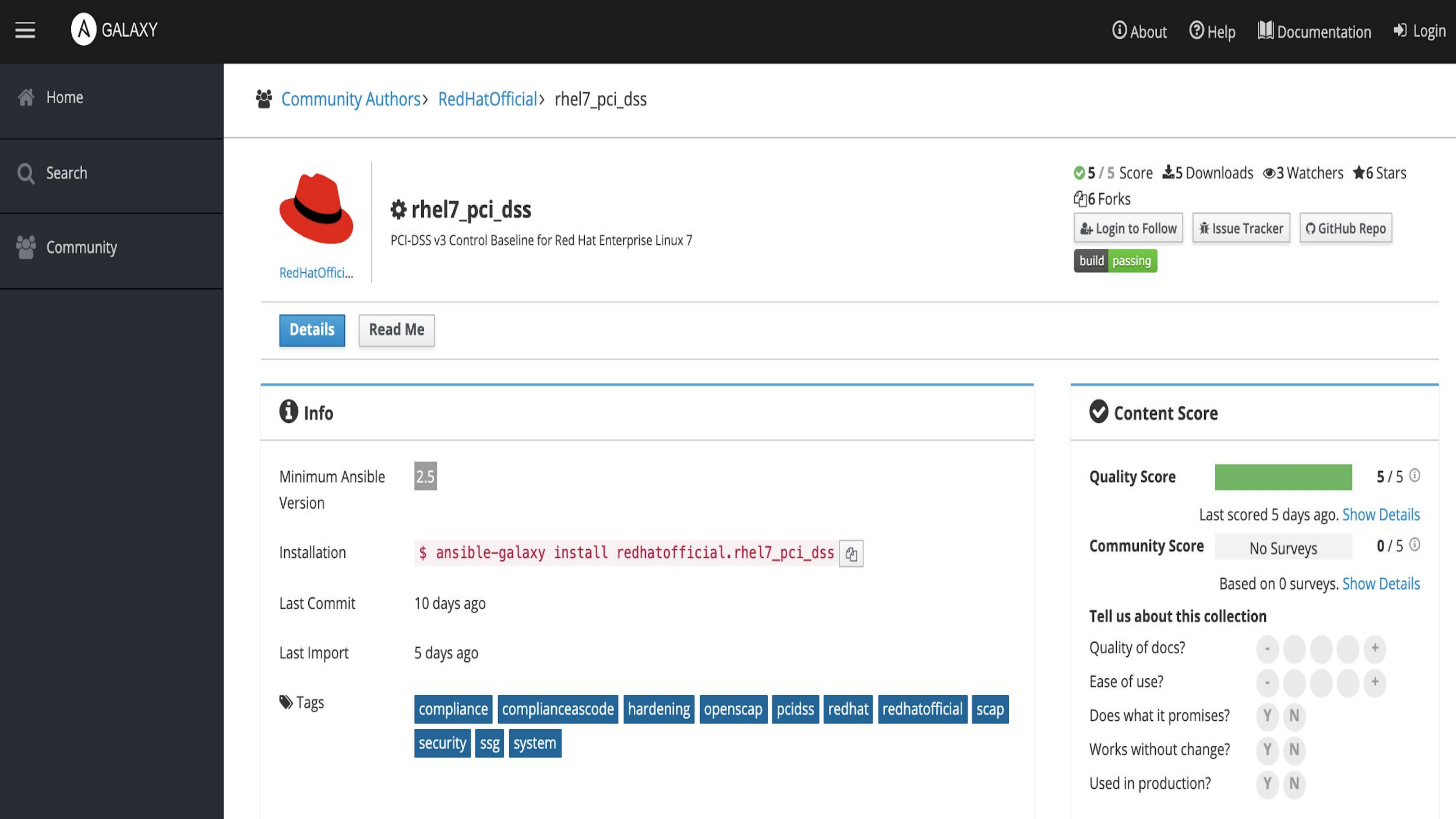
RedHatOfficial
Red Hat, Inc.
https://github.com/RedHatOfficial

8 Roles

manageiq_workers	Ansible role for configuring the workers on ManageIQ / CloudForms Management Engine (CFME) appliances.	132 Downloads 7 Watchers 2 Stars 0 Forks
rhel7_c2s	C2S for Red Hat Enterprise Linux 7	5 / 5 Score 31 Downloads 2 Watchers 1 Stars 3 Forks build passing



rhel7_hipaa	Health Insurance Portability and Accountability Act (HIPAA)	5 / 5 Score 3 Downloads 3 Watchers 3 Stars 2 Forks build passing
rhel7_ospp	United States Government Configuration Baseline	5 / 5 Score 6 Downloads 3 Watchers 4 Stars 0 Forks build passing
rhel7_pci_dss	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	5 / 5 Score 5 Downloads 3 Watchers 6 Stars 6 Forks build passing
rhel7_rht_ccp	Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	5 / 5 Score 28 Downloads 2 Watchers 2 Stars 1 Forks build passing
rhel7_stig	DISA STIG for Red Hat Enterprise Linux 7	5 / 5 Score 125 Downloads 6 Watchers 10 Stars 6 Forks build passing



rhel7_pci_dss

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

5 / 5 Score 5 Downloads 3 Watchers 6 Stars 6 Forks

Info

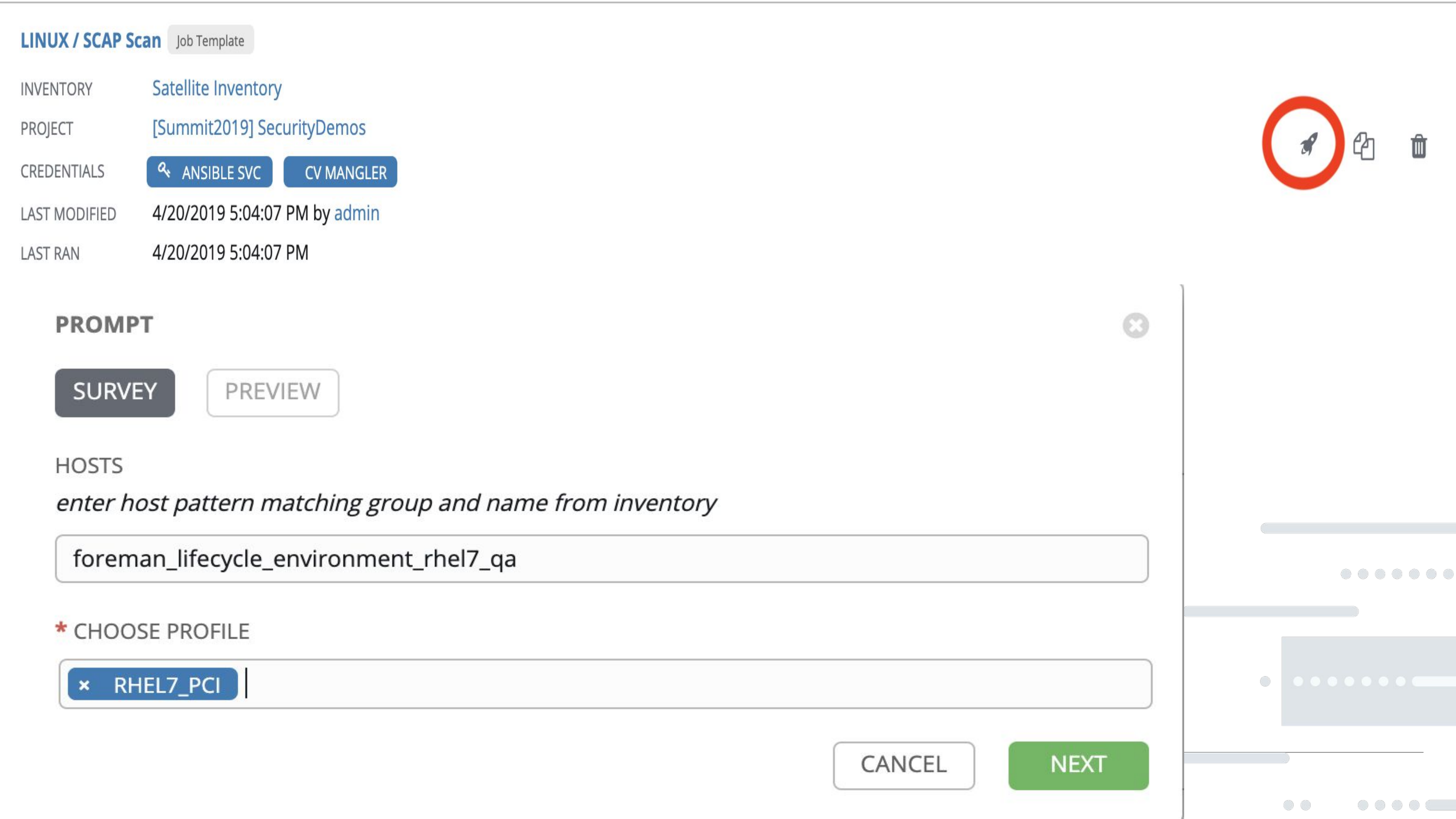
Minimum Ansible Version	2.5
Installation	`$ ansible-galaxy install redhatofficial.rhel7_pci_dss`
Last Commit	10 days ago
Last Import	5 days ago
Tags	compliance complianceascode hardening openscap pcidss redhat redhatofficial scap security ssg system

Content Score

Quality Score	🟩	5 / 5
	Last scored 5 days ago. Show Details	
Community Score	No Surveys	0 / 5
	Based on 0 surveys. Show Details	

Tell us about this collection

Quality of docs?	- ○ ○ ○ +
Ease of use?	- ○ ○ ○ +
Does what it promises?	Y N
Works without change?	Y N
Used in production?	Y N



LINUX / SCAP Scan Job Template

INVENTORY Satellite Inventory

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC CV MANGLER

LAST MODIFIED 4/20/2019 5:04:07 PM by admin

LAST RAN 4/20/2019 5:04:07 PM

PROMPT

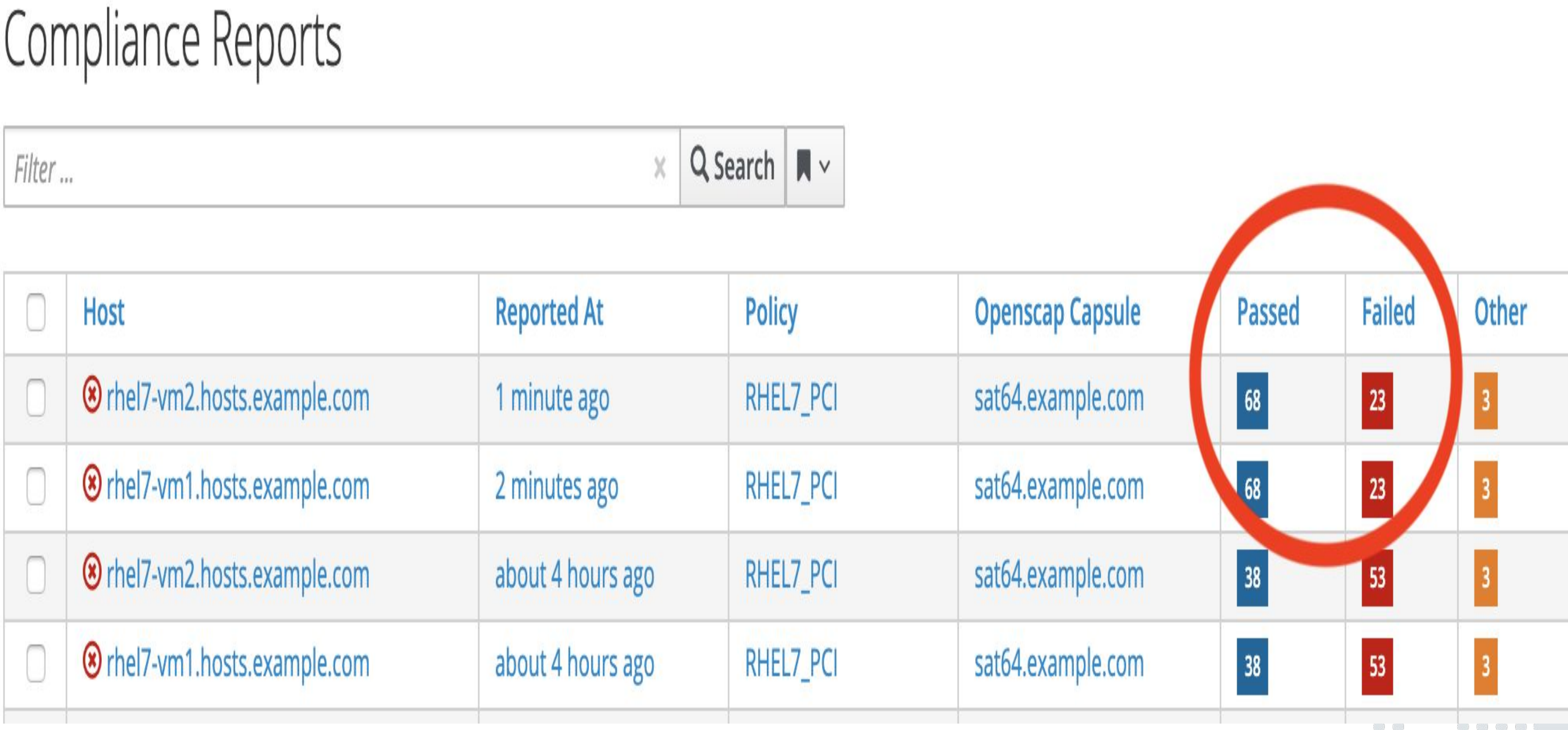
HOSTS

enter host pattern matching group and name from inventory

foreman_lifecycle_environment_rhel7_qa

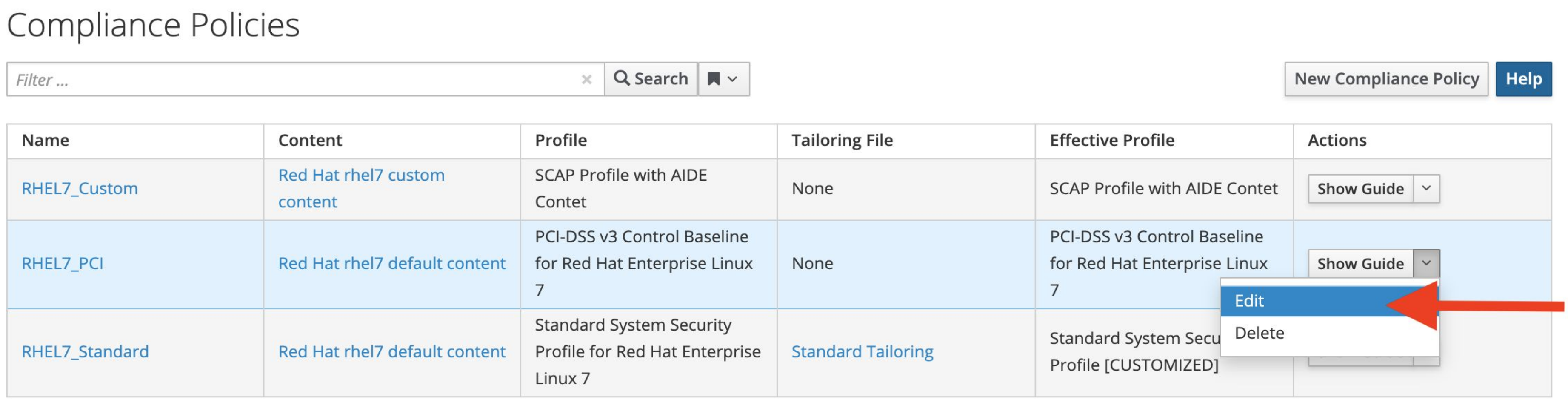
* CHOOSE PROFILE

RHEL7_PCI



Compliance Reports

□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other
□	⊗ rhel7-vm2.hosts.example.com	1 minute ago	RHEL7_PCI	sat64.example.com	68	23	3
□	⊗ rhel7-vm1.hosts.example.com	2 minutes ago	RHEL7_PCI	sat64.example.com	68	23	3
□	⊗ rhel7-vm2.hosts.example.com	about 4 hours ago	RHEL7_PCI	sat64.example.com	38	53	3
□	⊗ rhel7-vm1.hosts.example.com	about 4 hours ago	RHEL7_PCI	sat64.example.com	38	53	3

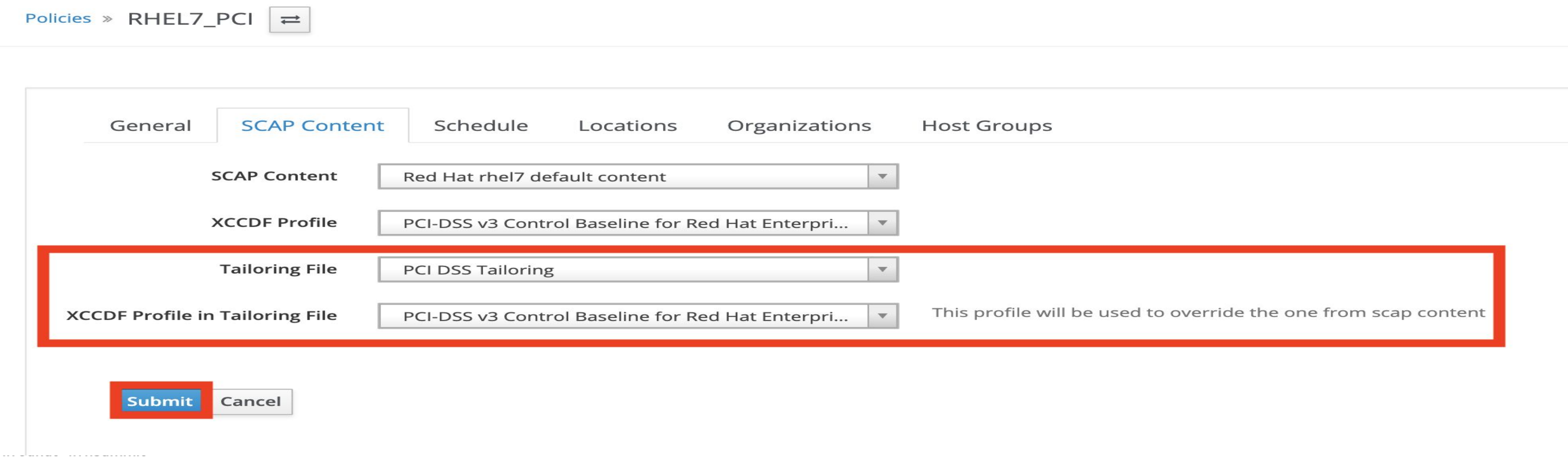


Compliance Policies

Filter ... × Search

New Compliance Policy Help

Name	Content	Profile	Tailoring File	Effective Profile	Actions
RHEL7_Custom	Red Hat rhel7 custom content	SCAP Profile with AIDE Contet	None	SCAP Profile with AIDE Contet	Show Guide
RHEL7_PCI	Red Hat rhel7 default content	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	None	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	Show Guide Edit Delete
RHEL7_Standard	Red Hat rhel7 default content	Standard System Security Profile for Red Hat Enterprise Linux 7	Standard Tailoring	Standard System Secu Profile [CUSTOMIZED]	



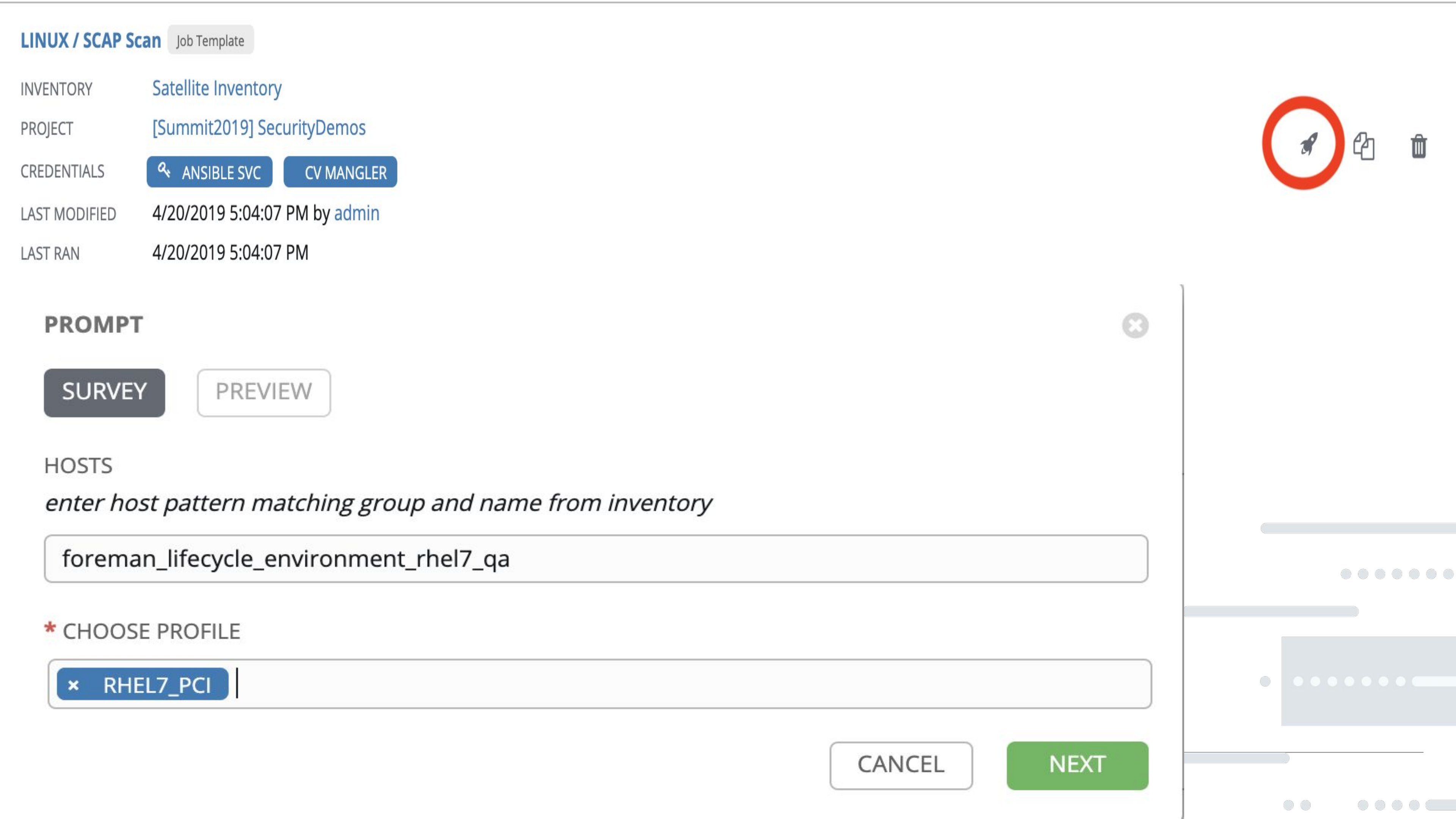
Policies » RHEL7_PCI

SCAP Content: Red Hat rhel7 default content

XCCDF Profile: PCI-DSS v3 Control Baseline for Red Hat Enterpri...

Tailoring File: PCI DSS Tailoring

XCCDF Profile in Tailoring File: PCI-DSS v3 Control Baseline for Red Hat Enterpri... This profile will be used to override the one from scap content



LINUX / SCAP Scan Job Template

INVENTORY Satellite Inventory

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC CV MANGLER

LAST MODIFIED 4/20/2019 5:04:07 PM by admin

LAST RAN 4/20/2019 5:04:07 PM

PROMPT

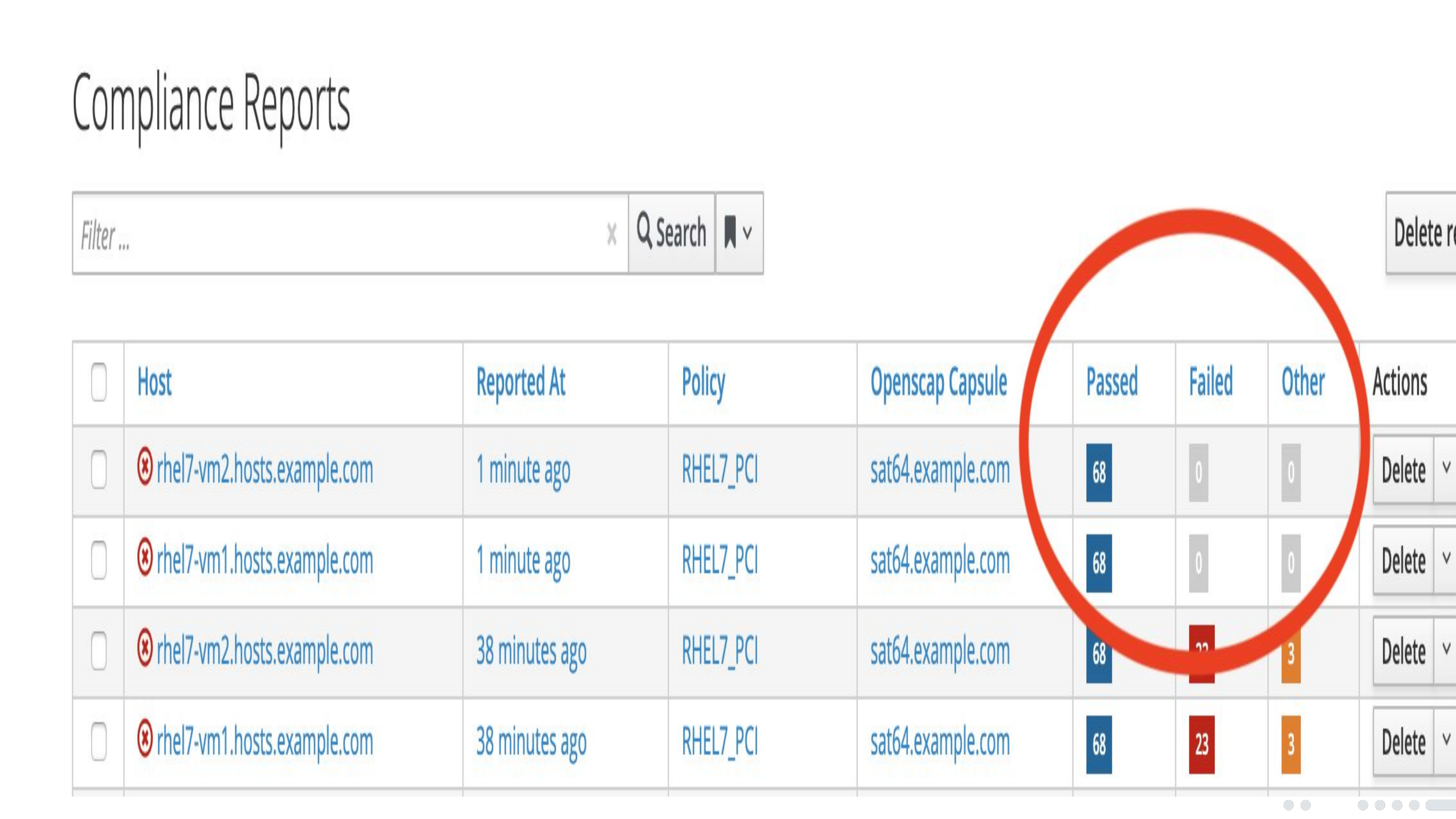
HOSTS

enter host pattern matching group and name from inventory

foreman_lifecycle_environment_rhel7_qa

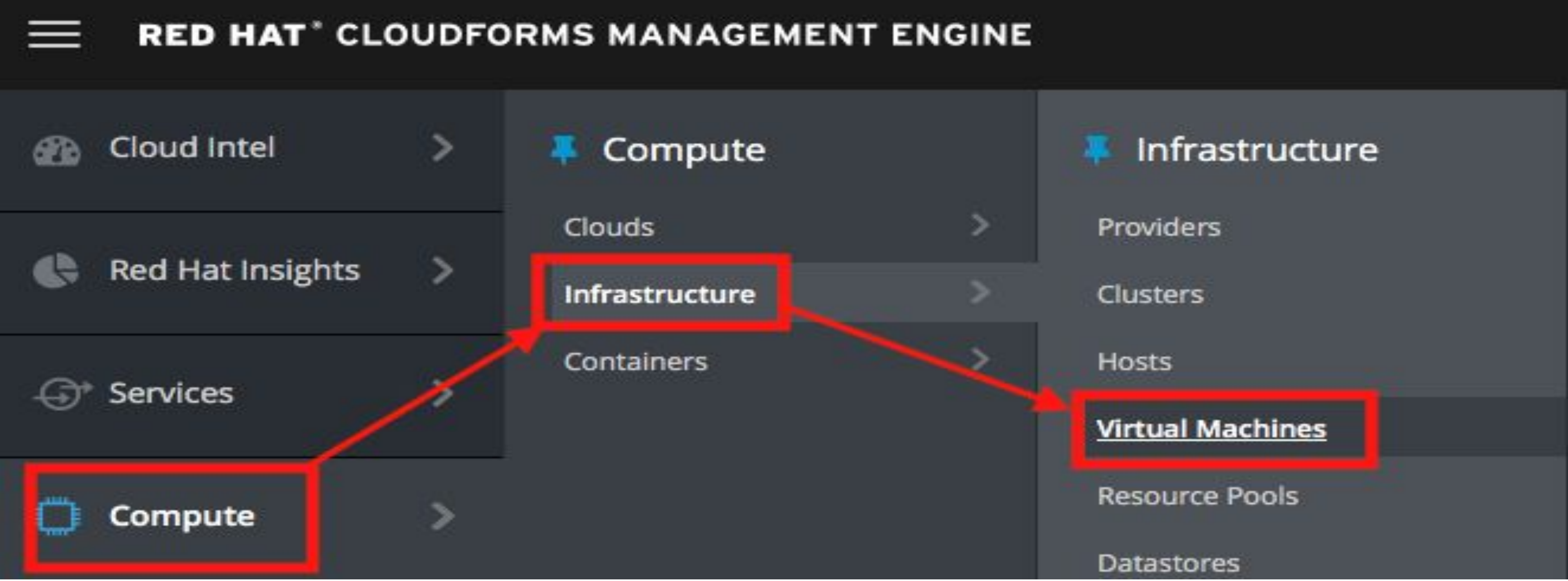
* CHOOSE PROFILE

× RHEL7_PCI

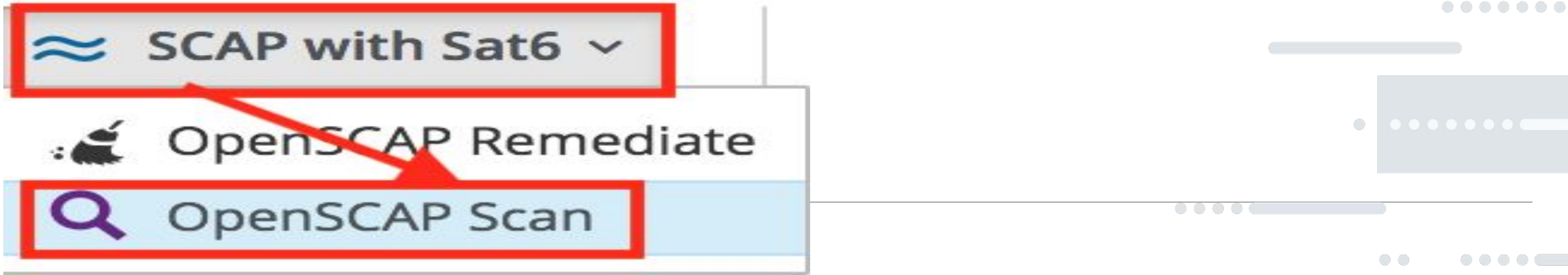


Compliance Reports

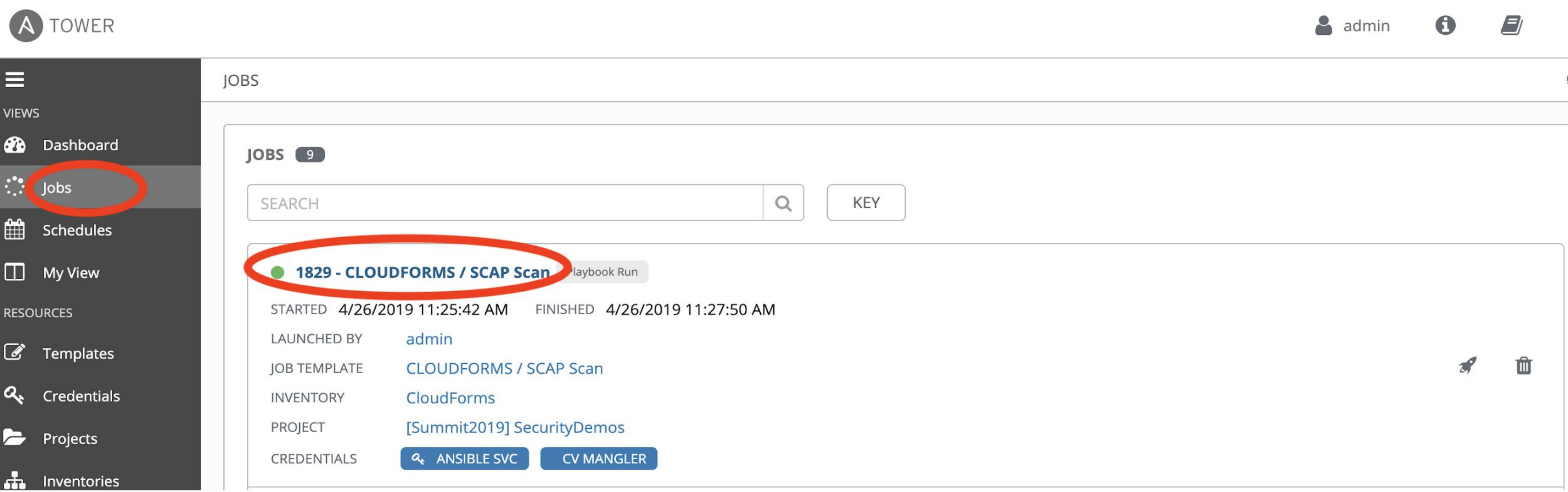
☐	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other	Actions
☐	⊗ rhel7-vm2.hosts.example.com	1 minute ago	RHEL7_PCI	sat64.example.com	68	0	0	Delete ˅
☐	⊗ rhel7-vm1.hosts.example.com	1 minute ago	RHEL7_PCI	sat64.example.com	68	0	0	Delete ˅
☐	⊗ rhel7-vm2.hosts.example.com	38 minutes ago	RHEL7_PCI	sat64.example.com	68	23	3	Delete ˅
☐	⊗ rhel7-vm1.hosts.example.com	38 minutes ago	RHEL7_PCI	sat64.example.com	68	23	3	Delete ˅



RED HAT® CLOUDFORMS MANAGEMENT ENGINE
Cloud Intel
Red Hat Insights
Services
Compute
Compute
Clouds
Infrastructure
Containers
Infrastructure
Providers
Clusters
Hosts
Virtual Machines
Resource Pools
Datastores



SCAP with Sat6
OpenSCAP Remediate
OpenSCAP Scan



JOBS

JOBS 9

1829 - CLOUDFORMS / SCAP Scan

STARTED 4/26/2019 11:25:42 AM FINISHED 4/26/2019 11:27:50 AM

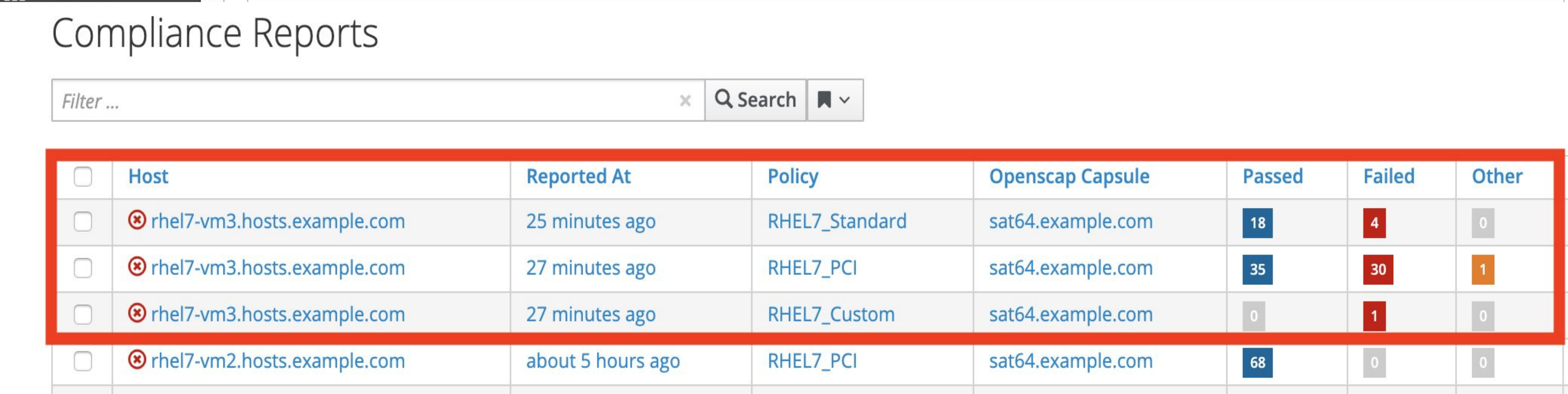
LAUNCHED BY admin

JOB TEMPLATE CLOUDFORMS / SCAP Scan

INVENTORY CloudForms

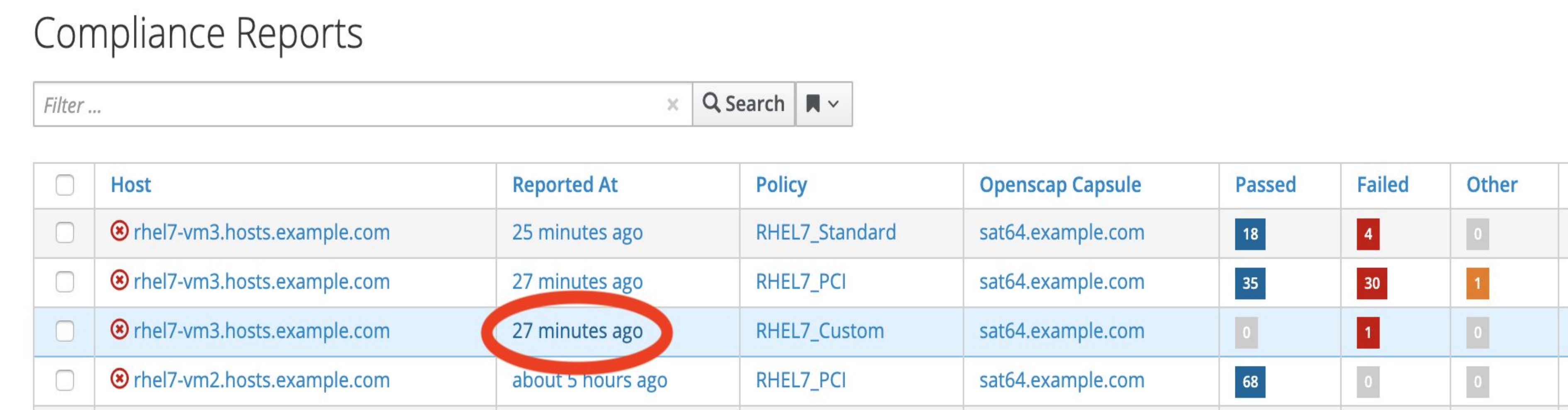
PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC CV MANGLER



Compliance Reports

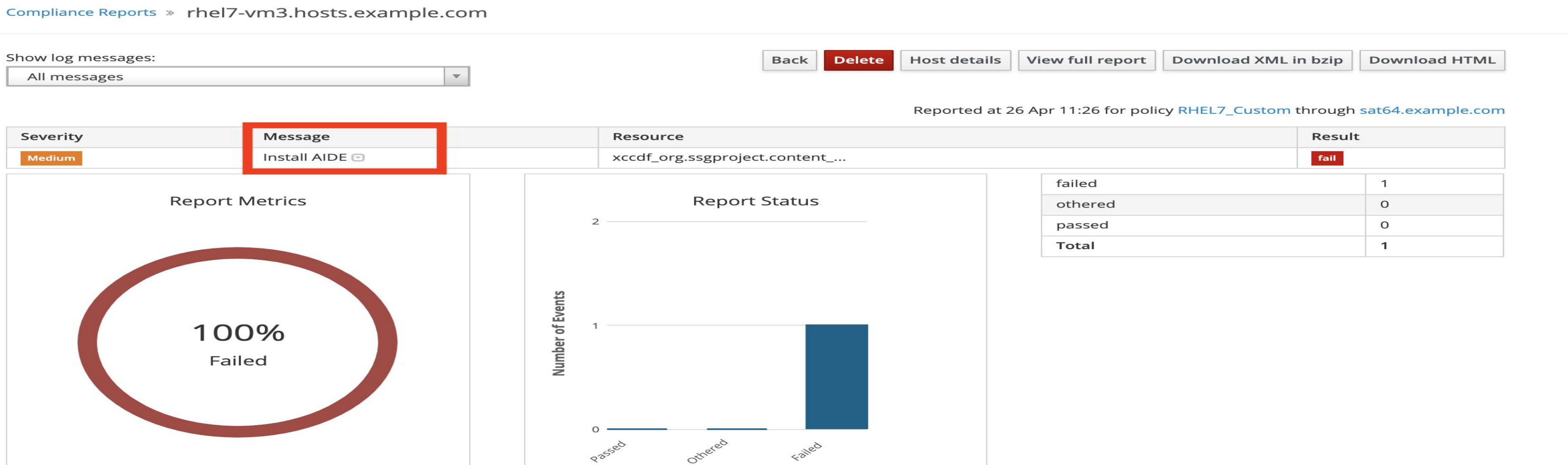
□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other
□	rhel7-vm3.hosts.example.com	25 minutes ago	RHEL7_Standard	sat64.example.com	18	4	0
□	rhel7-vm3.hosts.example.com	27 minutes ago	RHEL7_PCI	sat64.example.com	35	30	1
□	rhel7-vm3.hosts.example.com	27 minutes ago	RHEL7_Custom	sat64.example.com	0	1	0
□	rhel7-vm2.hosts.example.com	about 5 hours ago	RHEL7_PCI	sat64.example.com	68	0	0



Compliance Reports

Filter ...

□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other
□	⊗ rhel7-vm3.hosts.example.com	25 minutes ago	RHEL7_Standard	sat64.example.com	18	4	0
□	⊗ rhel7-vm3.hosts.example.com	27 minutes ago	RHEL7_PCI	sat64.example.com	35	30	1
□	⊗ rhel7-vm3.hosts.example.com	27 minutes ago	RHEL7_Custom	sat64.example.com	0	1	0
□	⊗ rhel7-vm2.hosts.example.com	about 5 hours ago	RHEL7_PCI	sat64.example.com	68	0	0



Compliance Reports » rhel7-vm3.hosts.example.com

Show log messages: All messages

Reported at 26 Apr 11:26 for policy RHEL7_Custom through sat64.example.com

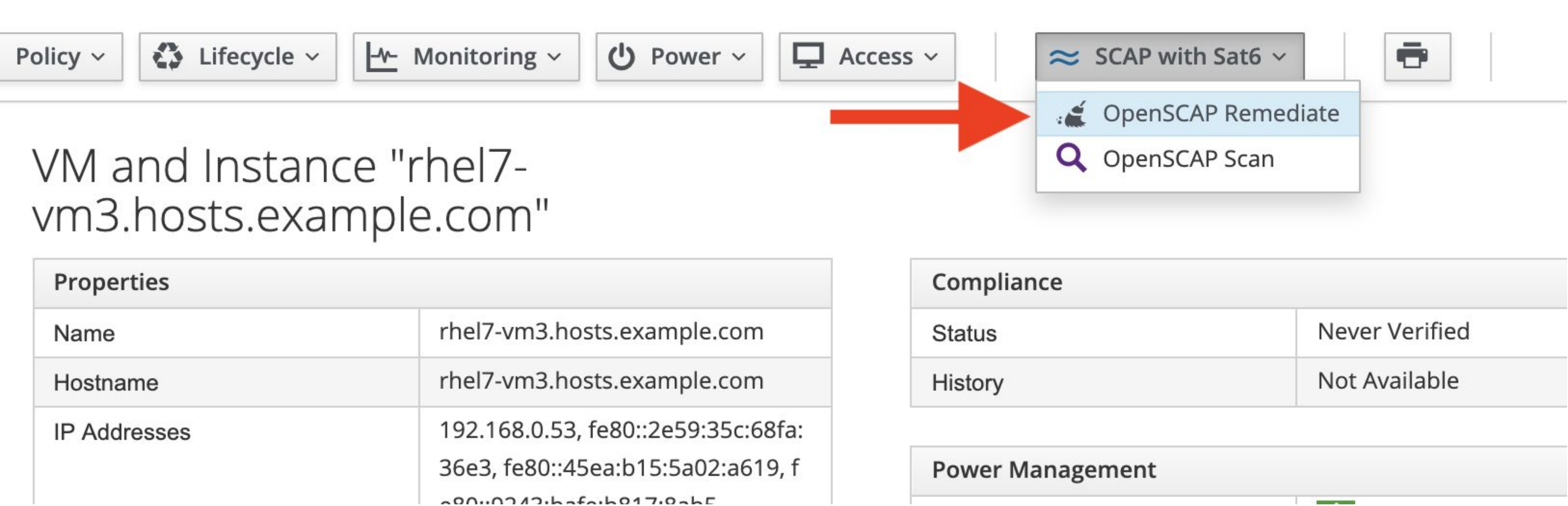
Severity	Message	Resource	Result
Medium	Install AIDE	xccdf_org.ssgproject.content_...	fail

Report Metrics

100% Failed

Report Status

failed	1
othered	0
passed	0
Total	1

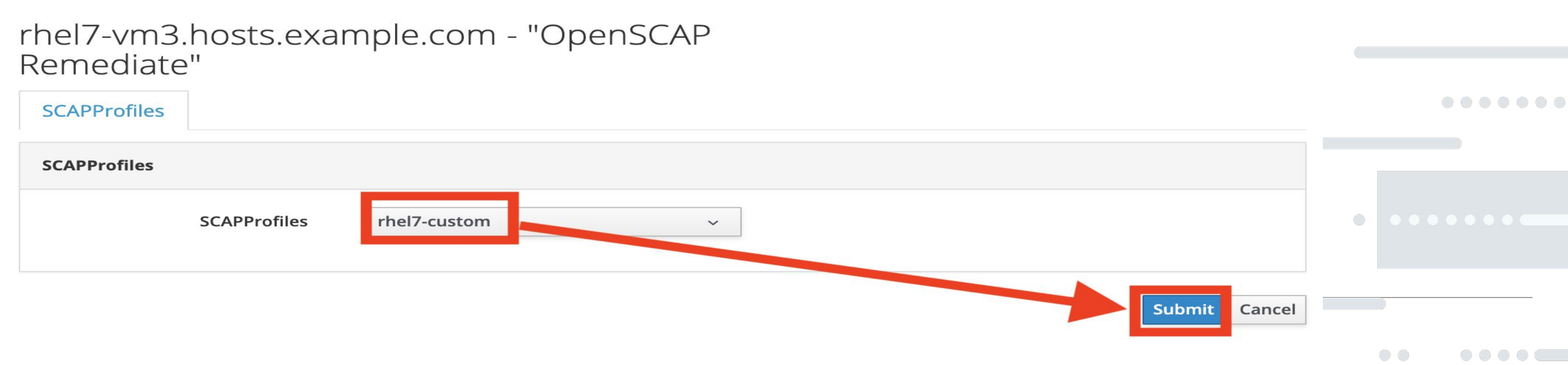


VM and Instance "rhel7-vm3.hosts.example.com"

Properties	
Name	rhel7-vm3.hosts.example.com
Hostname	rhel7-vm3.hosts.example.com
IP Addresses	192.168.0.53, fe80::2e59:35c:68fa:36e3, fe80::45ea:b15:5a02:a619, fe80::0242:bafe:b817:8ab5

Compliance	
Status	Never Verified
History	Not Available

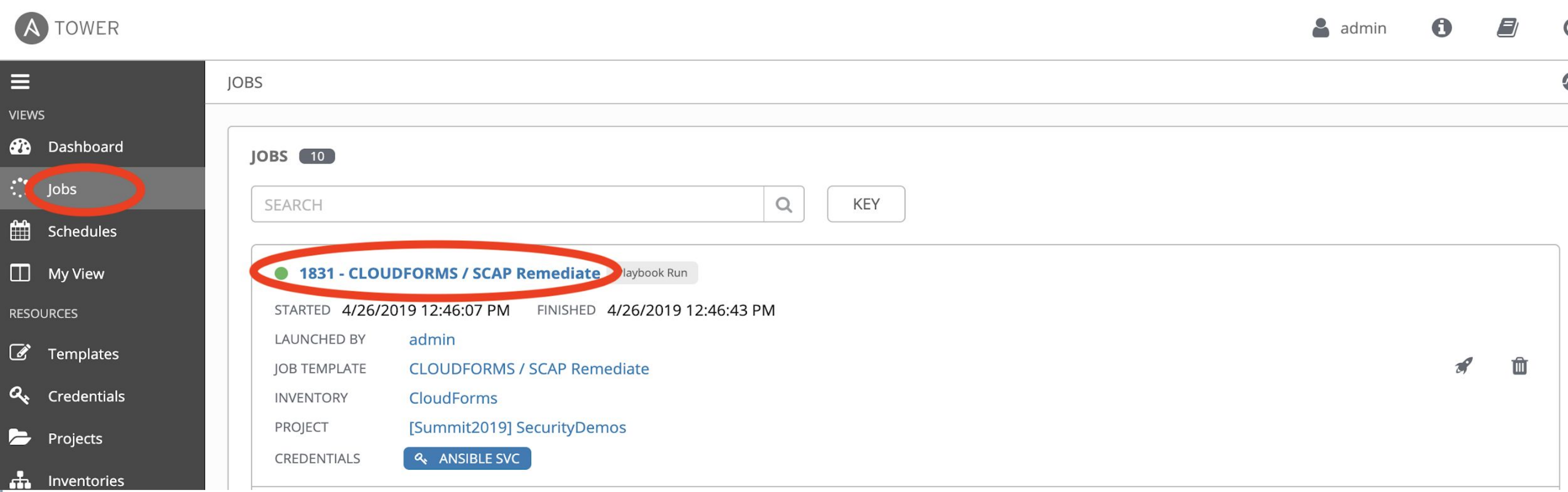
Power Management



rhel7-vm3.hosts.example.com - "OpenSCAP Remediate"

SCAPProfiles

SCAPProfiles: rhel7-custom



JOBS 10

1831 - CLOUDFORMS / SCAP Remediate Playbook Run

STARTED 4/26/2019 12:46:07 PM FINISHED 4/26/2019 12:46:43 PM

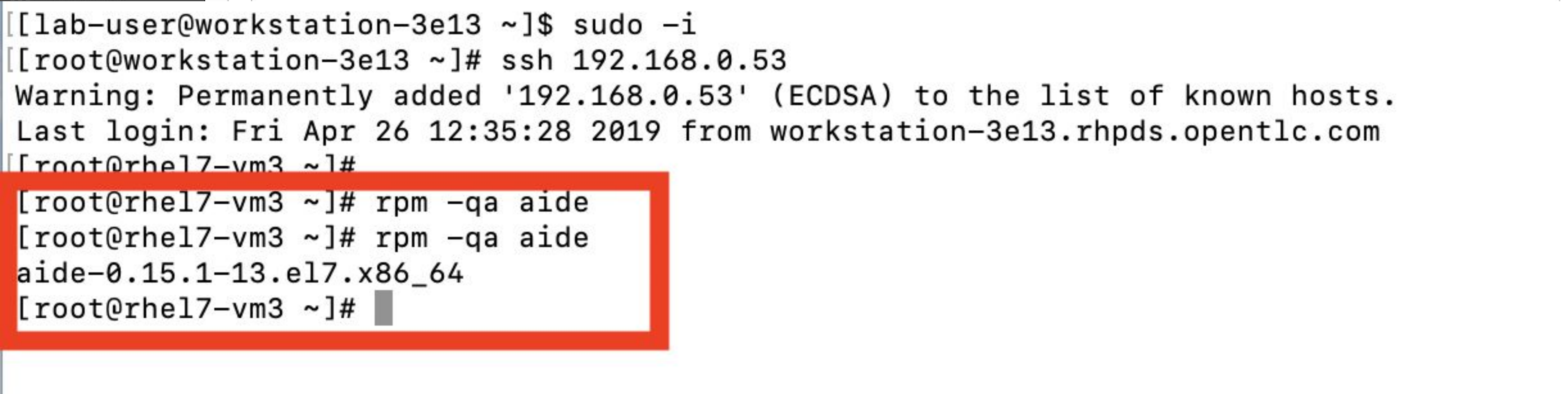
LAUNCHED BY admin

JOB TEMPLATE CLOUDFORMS / SCAP Remediate

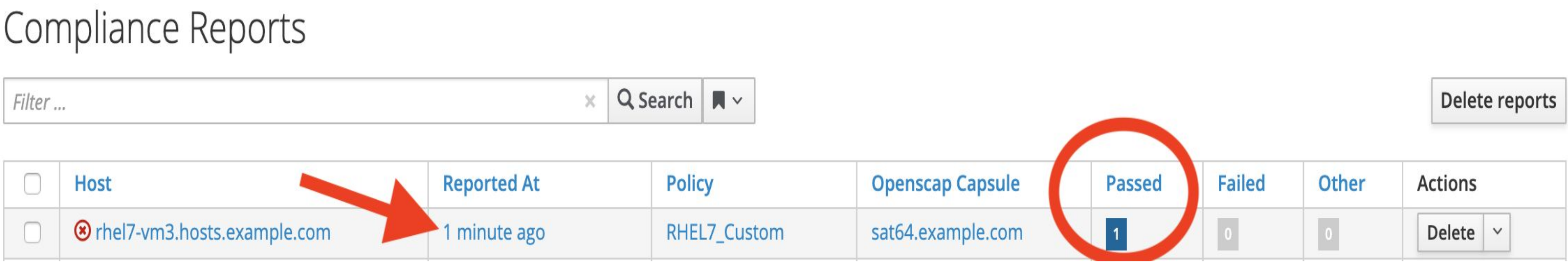
INVENTORY CloudForms

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC

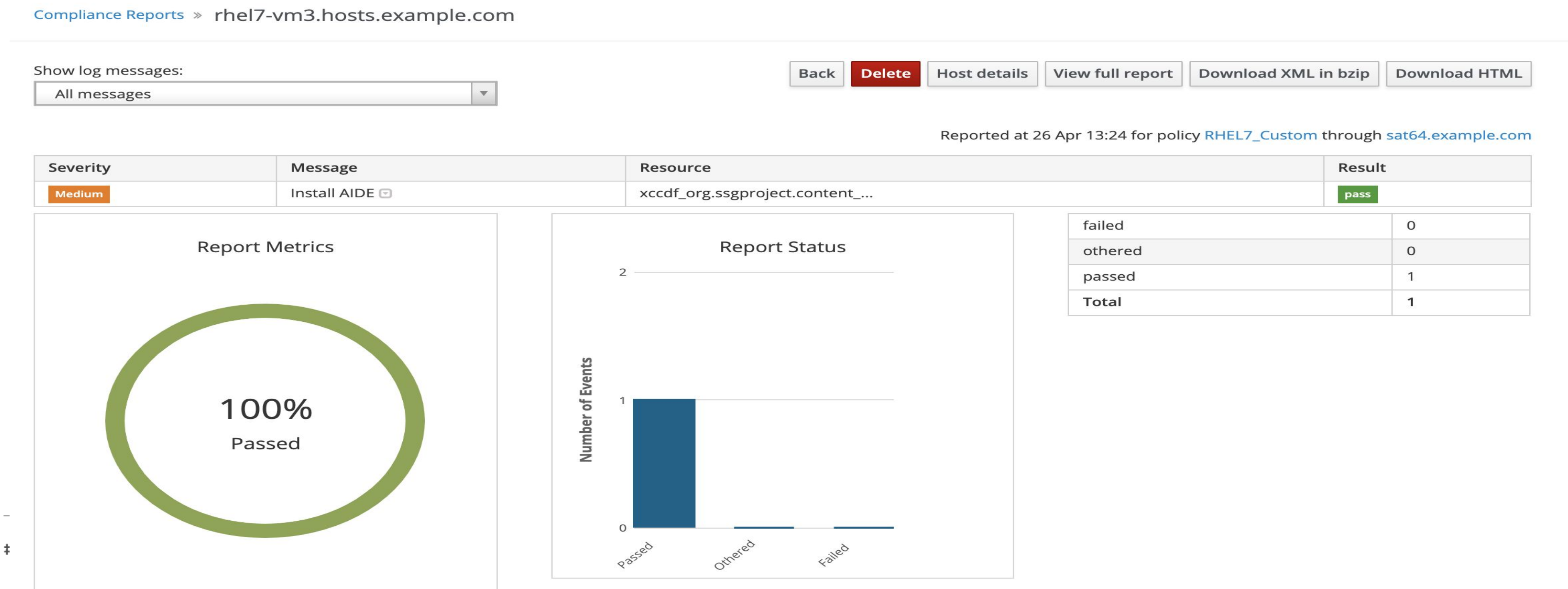


```
[lab-user@workstation-3e13 ~]$ sudo -i
[root@workstation-3e13 ~]# ssh 192.168.0.53
Warning: Permanently added '192.168.0.53' (ECDSA) to the list of known hosts.
Last login: Fri Apr 26 12:35:28 2019 from workstation-3e13.rhpds.opentlc.com
[root@rhel7-vm3 ~]#
[root@rhel7-vm3 ~]# rpm -qa aide
[root@rhel7-vm3 ~]# rpm -qa aide
aide-0.15.1-13.el7.x86_64
[root@rhel7-vm3 ~]#
```



Compliance Reports

□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other	Actions
□	⊗ rhel7-vm3.hosts.example.com	1 minute ago	RHEL7_Custom	sat64.example.com	1	0	0	Delete



Compliance Reports » rhel7-vm3.hosts.example.com

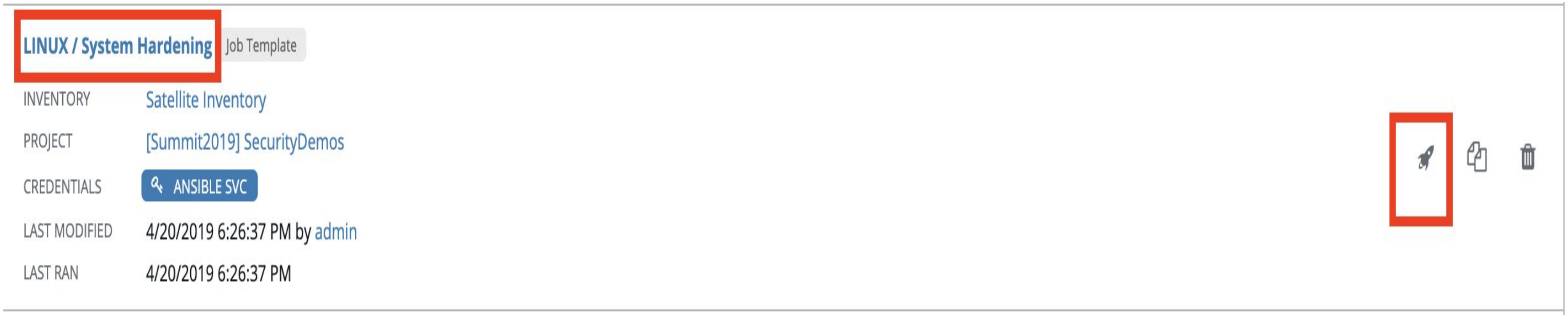
Show log messages: All messages

Reported at 26 Apr 13:24 for policy RHEL7_Custom through sat64.example.com

Severity	Message	Resource	Result
Medium	Install AIDE	xccdf_org.ssgproject.content_...	pass

failed	0
othered	0
passed	1
Total	**1**

Additional Automated Security Hardening on Hosts



LINUX / System Hardening Job Template

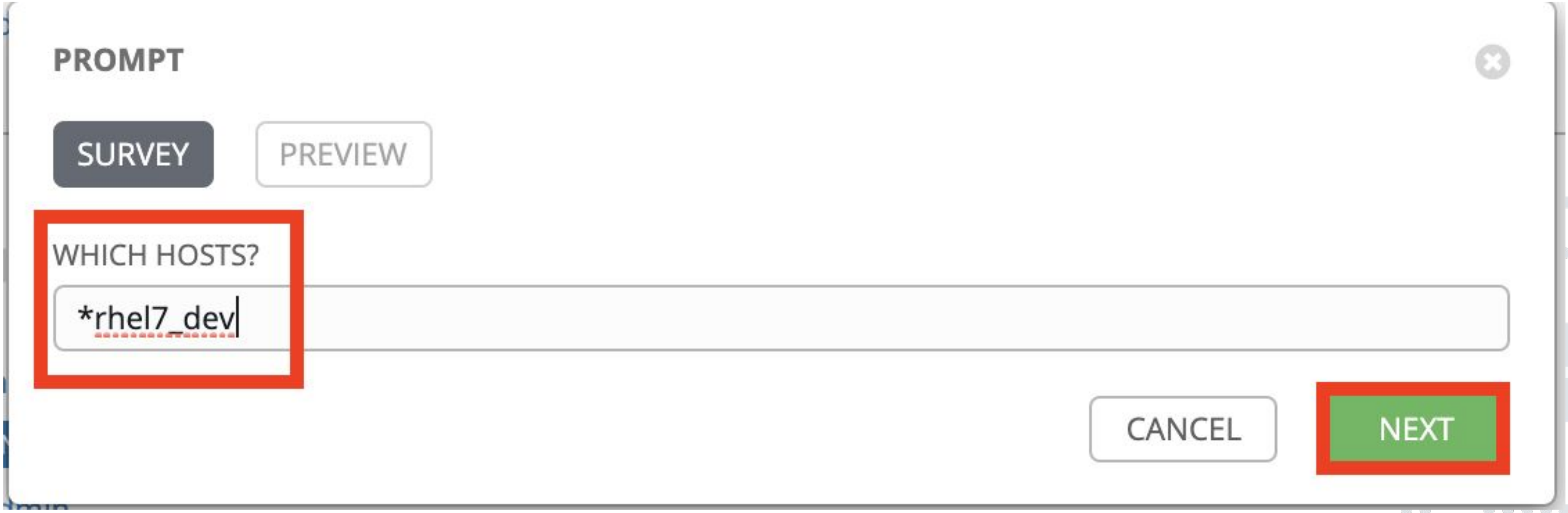
INVENTORY Satellite Inventory

PROJECT [Summit2019] SecurityDemos

CREDENTIALS ANSIBLE SVC

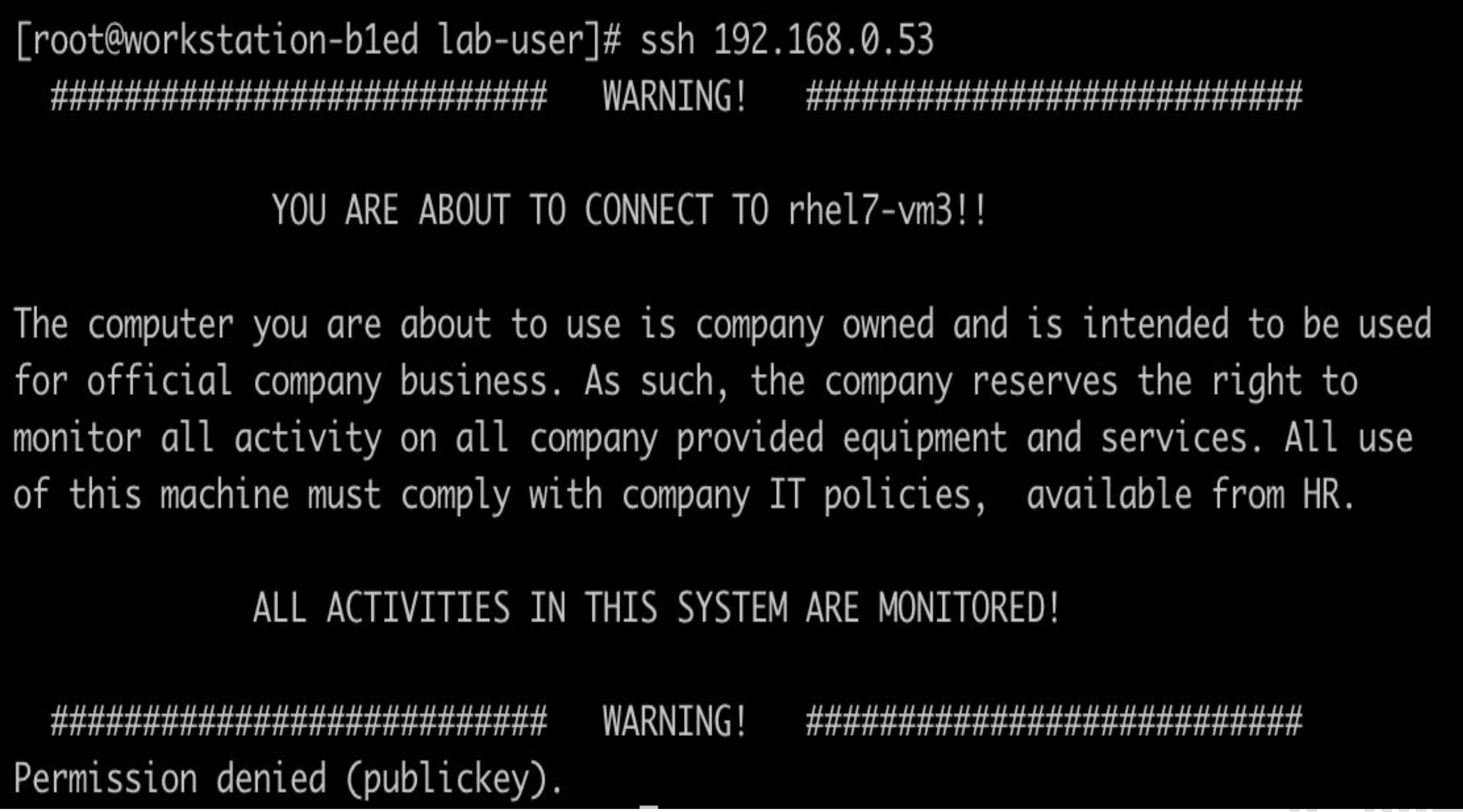
LAST MODIFIED 4/20/2019 6:26:37 PM by admin

LAST RAN 4/20/2019 6:26:37 PM



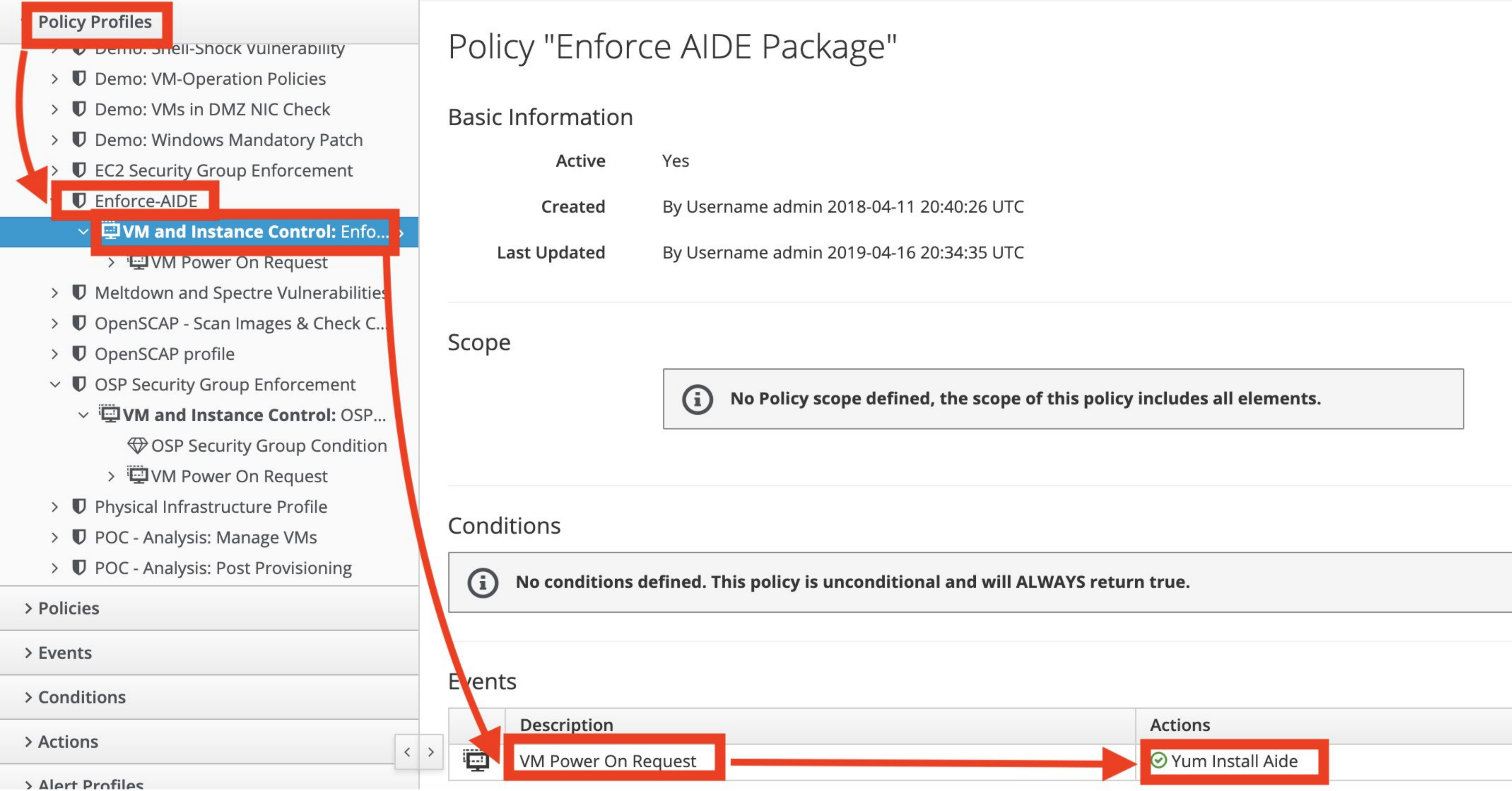
PROMPT

WHICH HOSTS? *rhel7_dev



```
[root@workstation-b1ed lab-user]# ssh 192.168.0.53
  ###########################   WARNING!   ###########################

              YOU ARE ABOUT TO CONNECT TO rhel7-vm3!!

The computer you are about to use is company owned and is intended to be used
for official company business. As such, the company reserves the right to
monitor all activity on all company provided equipment and services. All use
of this machine must comply with company IT policies,  available from HR.

             ALL ACTIVITIES IN THIS SYSTEM ARE MONITORED!

  ###########################   WARNING!   ###########################
Permission denied (publickey).
```

Enforcing Automated Compliance with Security Policies


Policy Profiles
Demo: Shell-Shock Vulnerability
Demo: VM-Operation Policies
Demo: VMs in DMZ NIC Check
Demo: Windows Mandatory Patch
EC2 Security Group Enforcement
Enforce-AIDE
VM and Instance Control: Enfo...
VM Power On Request
Meltdown and Spectre Vulnerabilities
OpenSCAP - Scan Images & Check C...
OpenSCAP profile
OSP Security Group Enforcement
VM and Instance Control: OSP...
OSP Security Group Condition
VM Power On Request
Physical Infrastructure Profile
POC - Analysis: Manage VMs
POC - Analysis: Post Provisioning
Policies
Events
Conditions
Actions
Alert Profiles

Policy "Enforce AIDE Package"

Basic Information

Active	Yes
Created	By Username admin 2018-04-11 20:40:26 UTC
Last Updated	By Username admin 2019-04-16 20:34:35 UTC

Scope

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

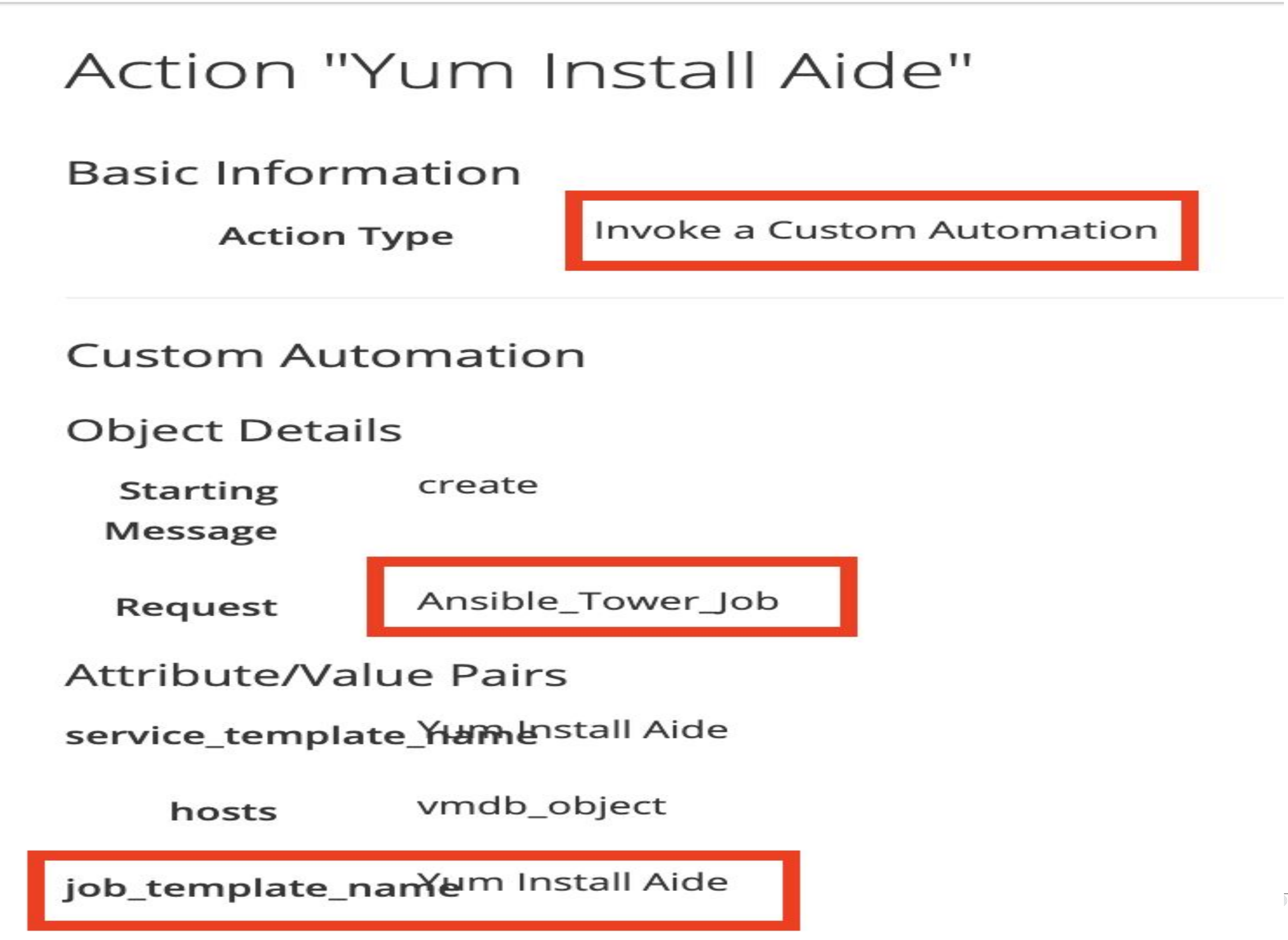
Conditions

No conditions defined. This policy is unconditional and will ALWAYS return true.

Events

Description	Actions
VM Power On Request	✓ Yum Install Aide

#redhat #rhsummit



Action "Yum Install Aide"

Basic Information

Action Type	Invoke a Custom Automation

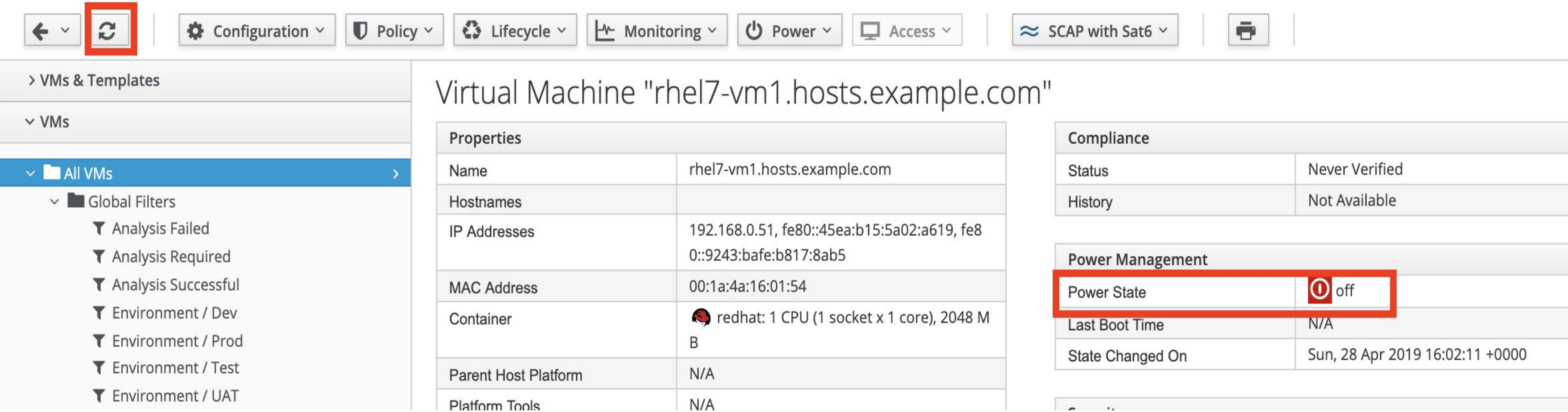
Custom Automation

Object Details

Starting Message	create
Request	Ansible_Tower_Job

Attribute/Value Pairs

service_template_name	Yum Install Aide
hosts	vmdb_object
job_template_name	Yum Install Aide

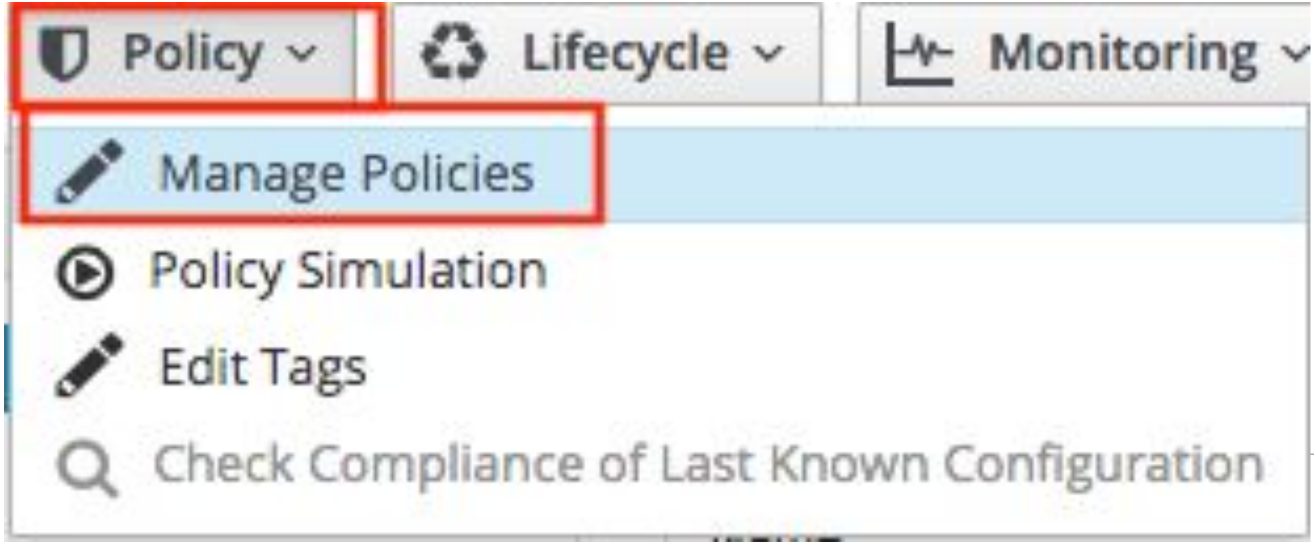


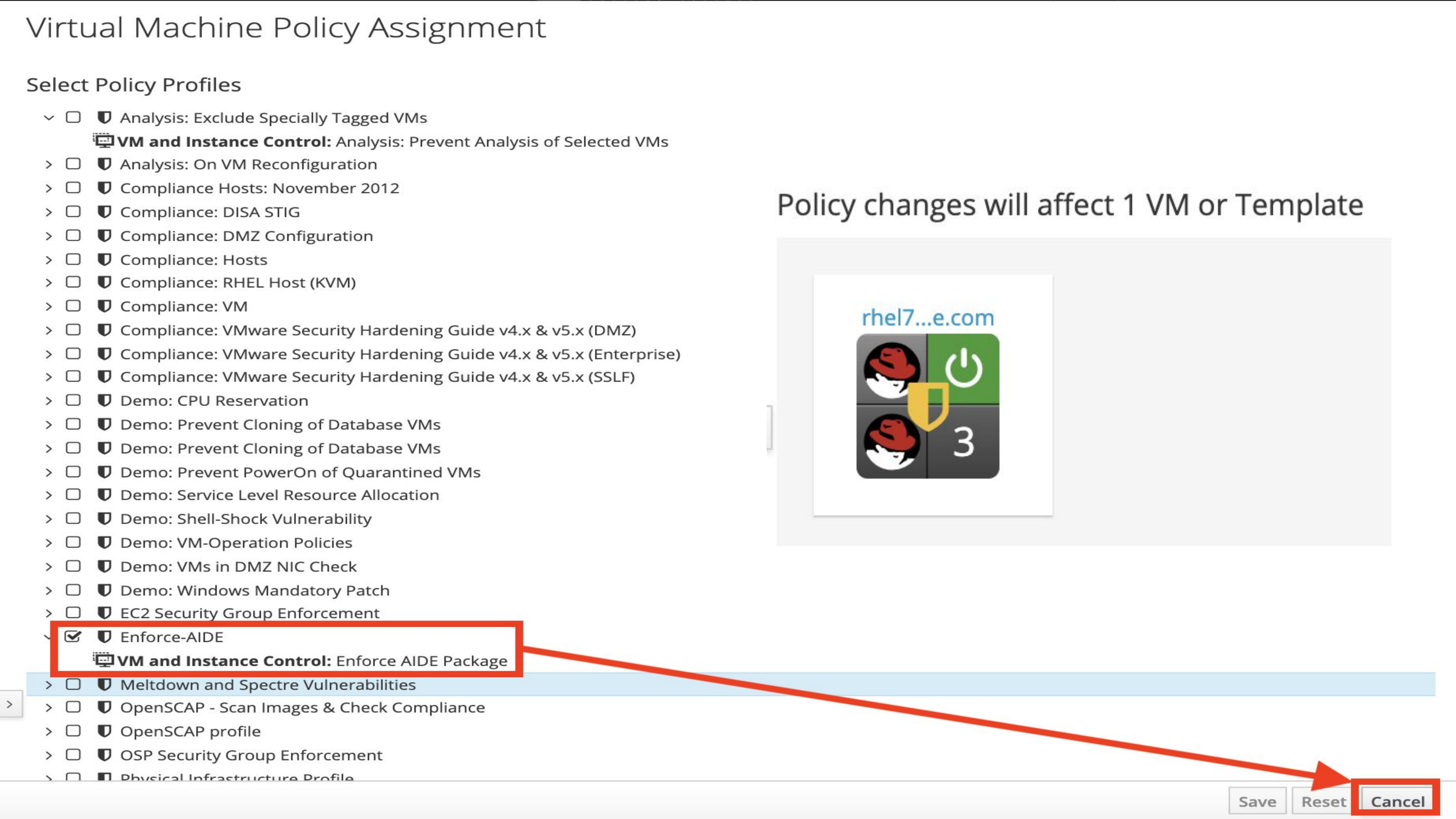
Virtual Machine "rhel7-vm1.hosts.example.com"

Properties	
Name	rhel7-vm1.hosts.example.com
Hostnames	
IP Addresses	192.168.0.51, fe80::45ea:b15:5a02:a619, fe80::9243:bafe:b817:8ab5
MAC Address	00:1a:4a:16:01:54
Container	redhat: 1 CPU (1 socket x 1 core), 2048 MB
Parent Host Platform	N/A
Platform Tools	N/A

Compliance	
Status	Never Verified
History	Not Available

Power Management	
Power State	off
Last Boot Time	N/A
State Changed On	Sun, 28 Apr 2019 16:02:11 +0000



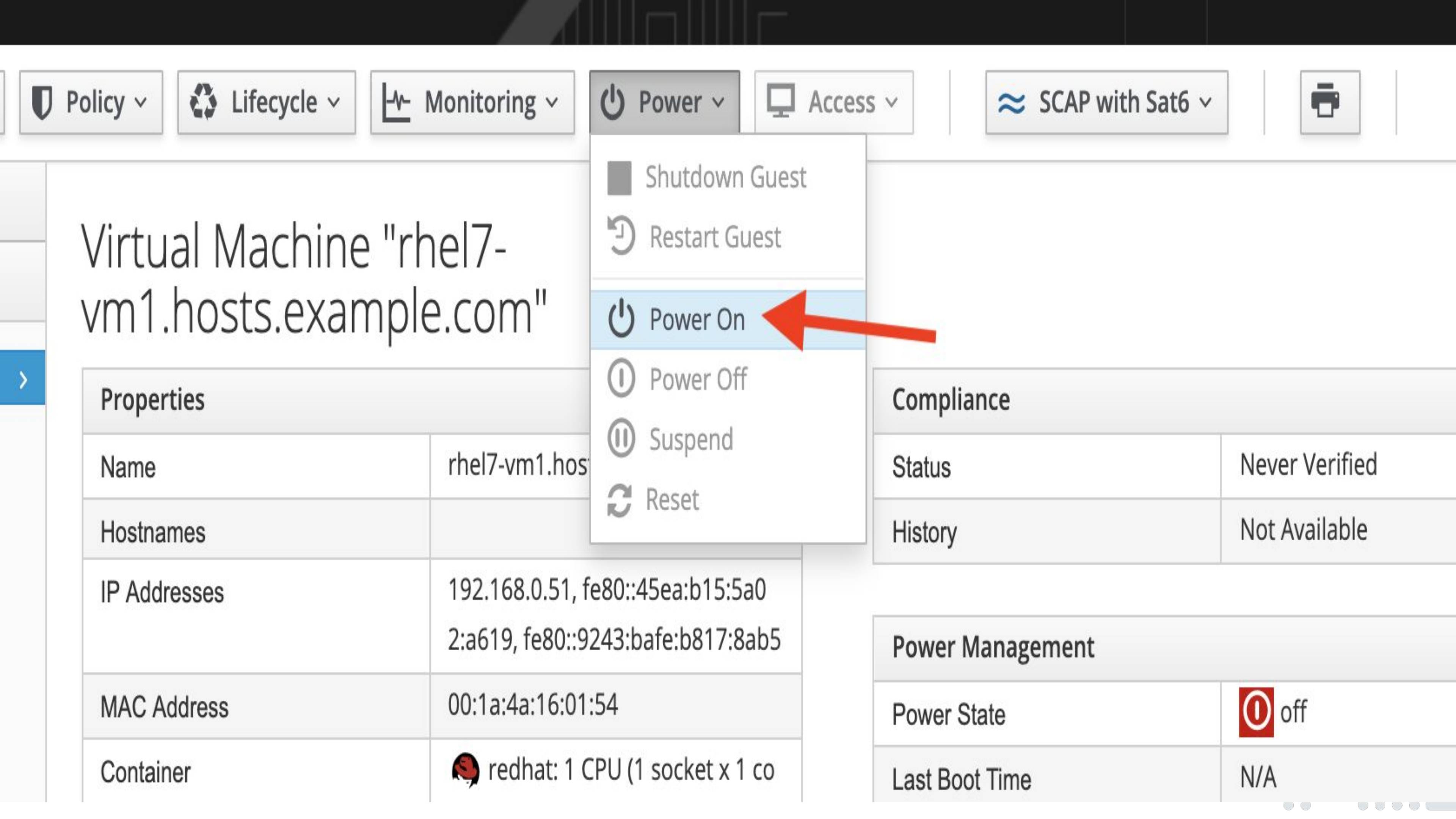


Virtual Machine Policy Assignment

Select Policy Profiles

- □ Analysis: Exclude Specially Tagged VMs
  - **VM and Instance Control:** Analysis: Prevent Analysis of Selected 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
- □ EC2 Security Group Enforcement
- ☑ Enforce-AIDE
  - **VM and Instance Control:** Enforce AIDE Package
- □ Meltdown and Spectre Vulnerabilities
- □ OpenSCAP - Scan Images & Check Compliance
- □ OpenSCAP profile
- □ OSP Security Group Enforcement
- □ Physical Infrastructure Profile

Policy changes will affect 1 VM or Template

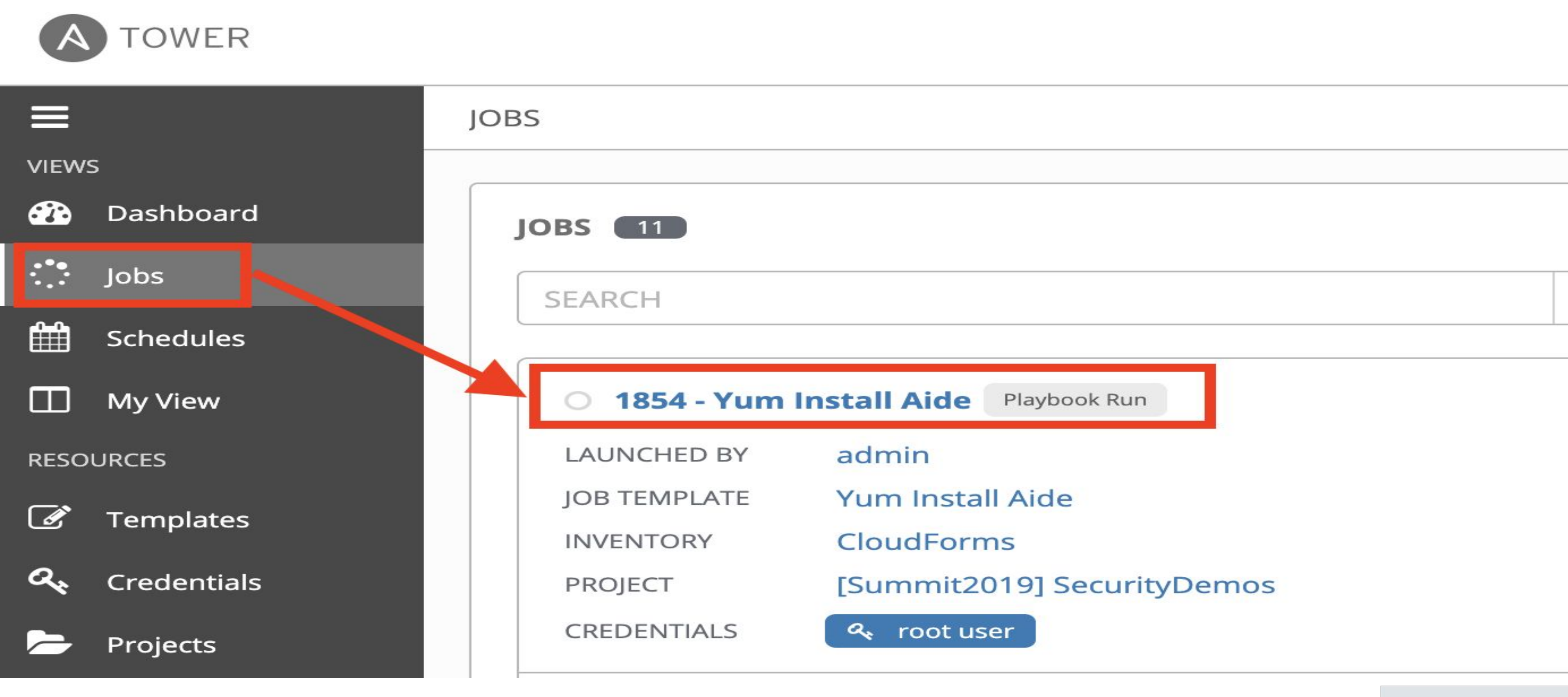


Virtual Machine "rhel7-vm1.hosts.example.com"

Properties	
Name	rhel7-vm1.hos
Hostnames	
IP Addresses	192.168.0.51, fe80::45ea:b15:5a0 2:a619, fe80::9243:bafe:b817:8ab5
MAC Address	00:1a:4a:16:01:54
Container	redhat: 1 CPU (1 socket x 1 co

Compliance	
Status	Never Verified
History	Not Available

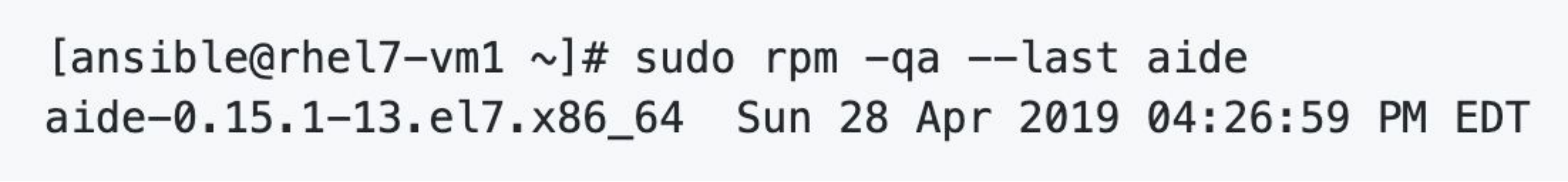
Power Management	
Power State	off
Last Boot Time	N/A



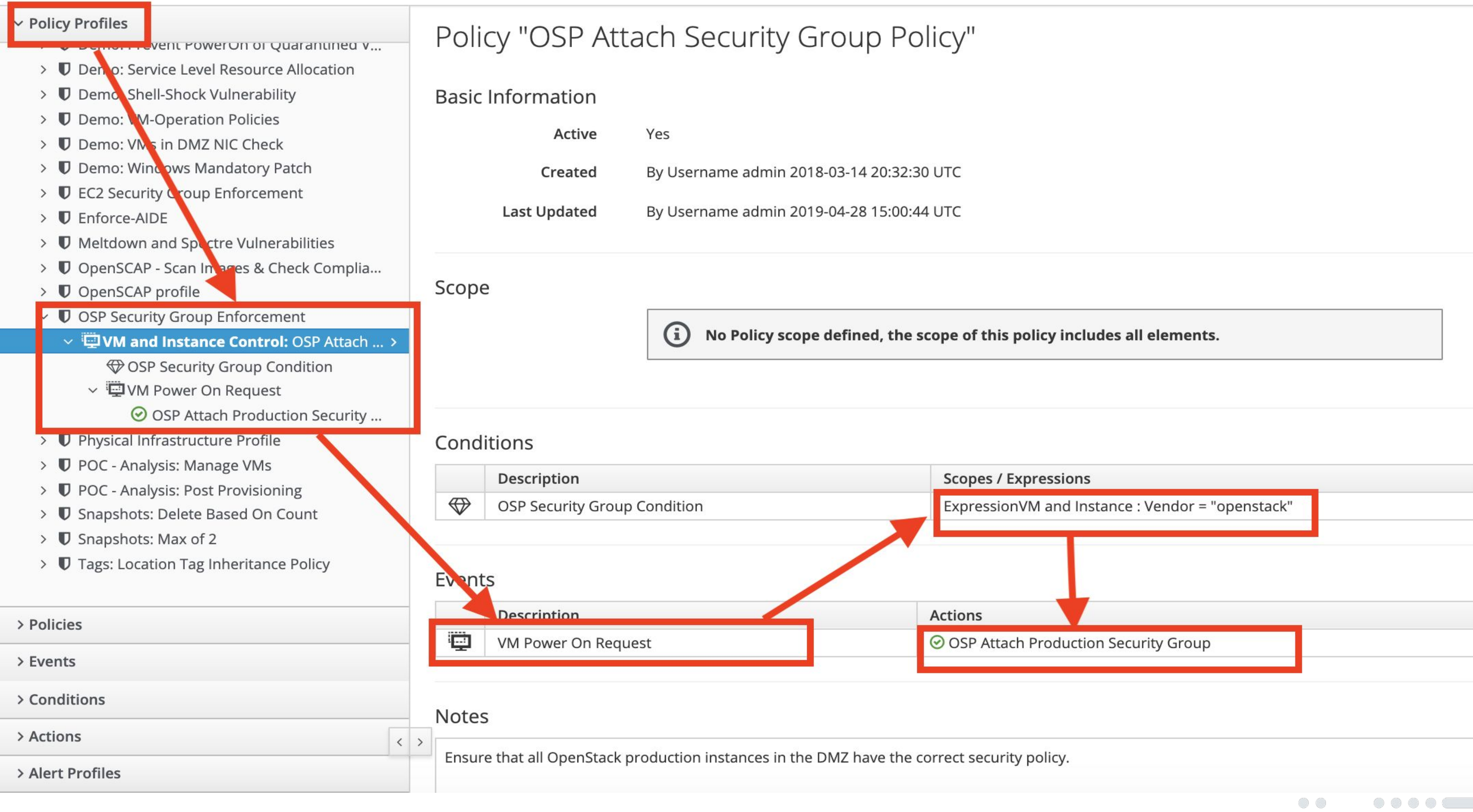
JOBS 11

1854 - Yum Install Aide Playbook Run

LAUNCHED BY admin
JOB TEMPLATE Yum Install Aide
INVENTORY CloudForms
PROJECT [Summit2019] SecurityDemos
CREDENTIALS root user



```
[ansible@rhel7-vm1 ~]# sudo rpm -qa --last aide
aide-0.15.1-13.el7.x86_64  Sun 28 Apr 2019 04:26:59 PM EDT
```



Policy Profiles
Demo: Prevent PowerOn of Quarantined V...
Demo: Service Level Resource Allocation
Demo: Shell-Shock Vulnerability
Demo: VM-Operation Policies
Demo: VMs in DMZ NIC Check
Demo: Windows Mandatory Patch
EC2 Security Group Enforcement
Enforce-AIDE
Meltdown and Spectre Vulnerabilities
OpenSCAP - Scan Images & Check Complia...
OpenSCAP profile
OSP Security Group Enforcement
VM and Instance Control: OSP Attach ...
OSP Security Group Condition
VM Power On Request
OSP Attach Production Security ...
Physical Infrastructure Profile
POC - Analysis: Manage VMs
POC - Analysis: Post Provisioning
Snapshots: Delete Based On Count
Snapshots: Max of 2
Tags: Location Tag Inheritance Policy
Policies
Events
Conditions
Actions
Alert Profiles

Policy "OSP Attach Security Group Policy"

Basic Information

Active	Yes
Created	By Username admin 2018-03-14 20:32:30 UTC
Last Updated	By Username admin 2019-04-28 15:00:44 UTC

Scope

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

Conditions

	Description	Scopes / Expressions
	OSP Security Group Condition	ExpressionVM and Instance : Vendor = "openstack"

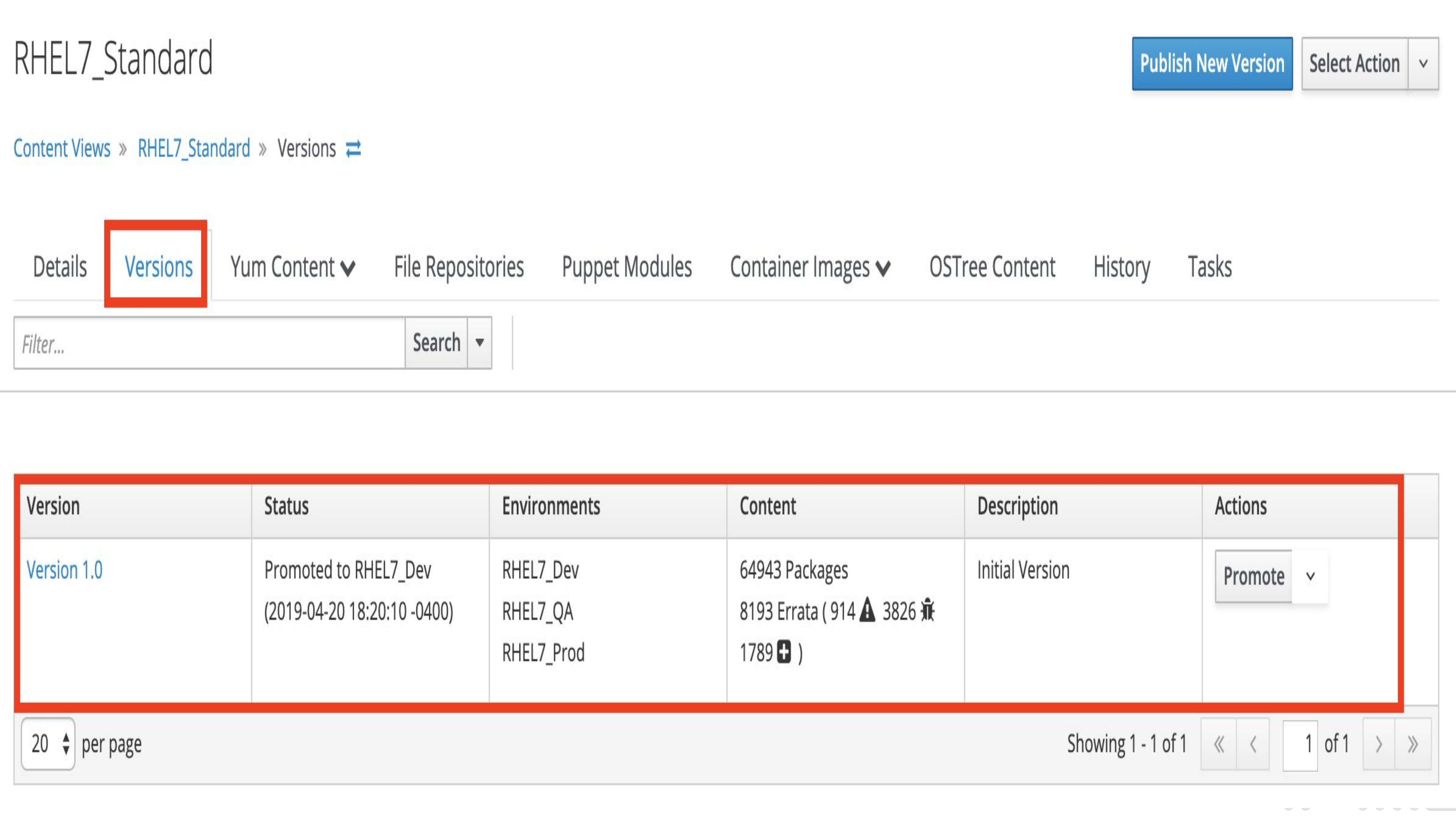
Events

	Description	Actions
	VM Power On Request	✓ OSP Attach Production Security Group

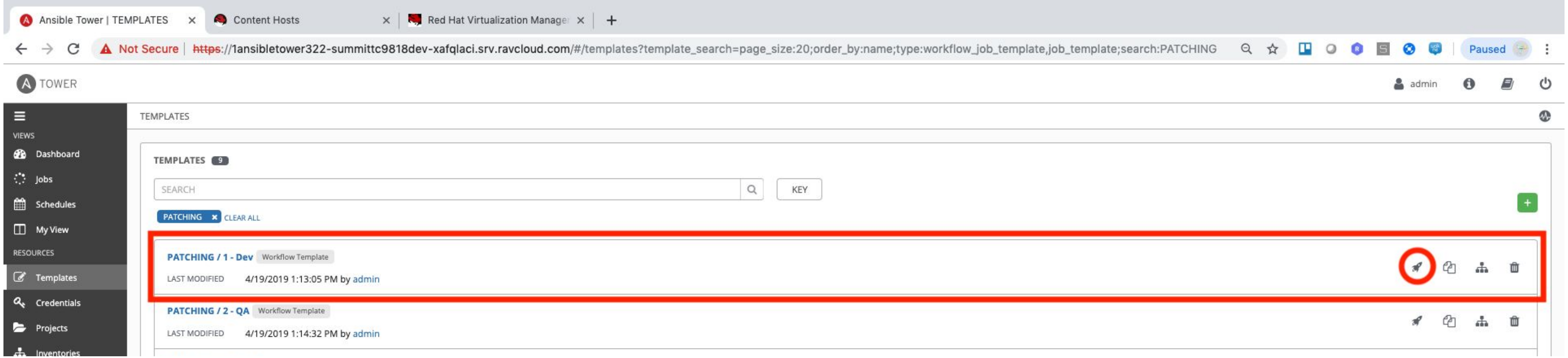
Notes

Ensure that all OpenStack production instances in the DMZ have the correct security policy.

Automated Patching of Host Systems at Scale



Version	Status	Environments	Content	Description	Actions
Version 1.0	Promoted to RHEL7_Dev (2019-04-20 18:20:10 -0400)	RHEL7_Dev RHEL7_QA RHEL7_Prod	64943 Packages 8193 Errata (914 ⚠ 3826 🐞 1789 ⊞)	Initial Version	Promote



Ansible Tower | TEMPLATES
Content Hosts
Red Hat Virtualization Manage
Not Secure
https://1ansibletower322-summittc9818dev-xafqlaci.srv.ravcloud.com/#/templates?template_search=page_size:20;order_by:name;type:workflow_job_template,job_template;search:PATCHING
Paused
TOWER
admin
VIEWS
Dashboard
Jobs
Schedules
My View
RESOURCES
Templates
Credentials
Projects
Inventories

TEMPLATES

TEMPLATES 9

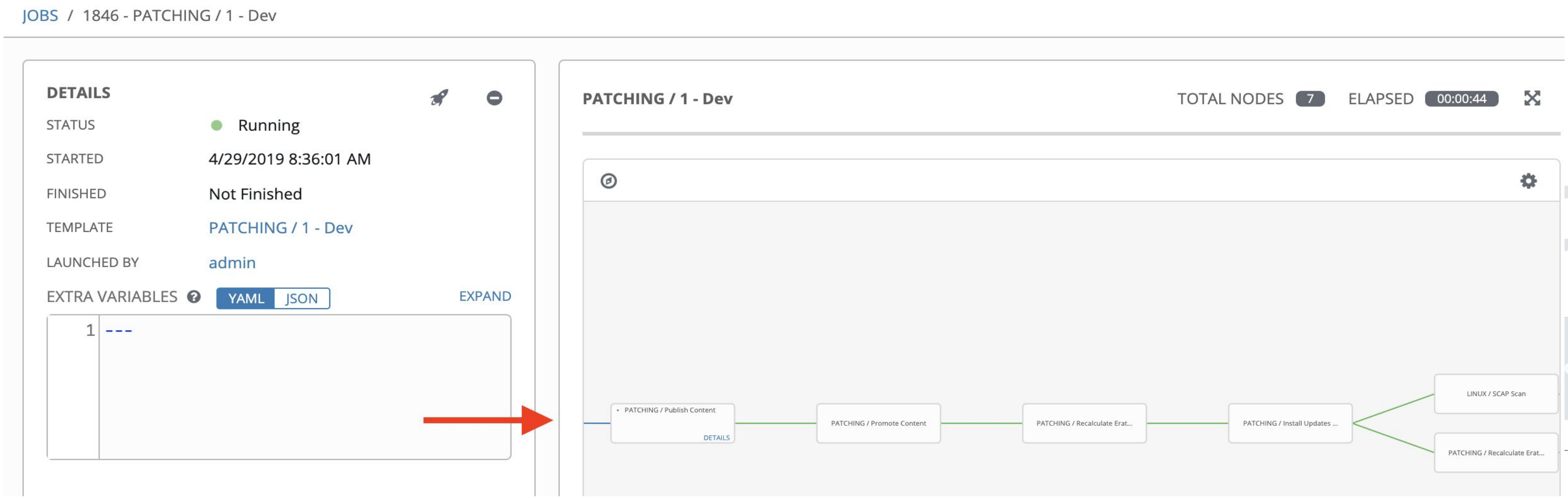
SEARCH

KEY

PATCHING CLEAR ALL

PATCHING / 1 - Dev Workflow Template
LAST MODIFIED 4/19/2019 1:13:05 PM by admin

PATCHING / 2 - QA Workflow Template
LAST MODIFIED 4/19/2019 1:14:32 PM by admin



JOBS / 1846 - PATCHING / 1 - Dev

DETAILS

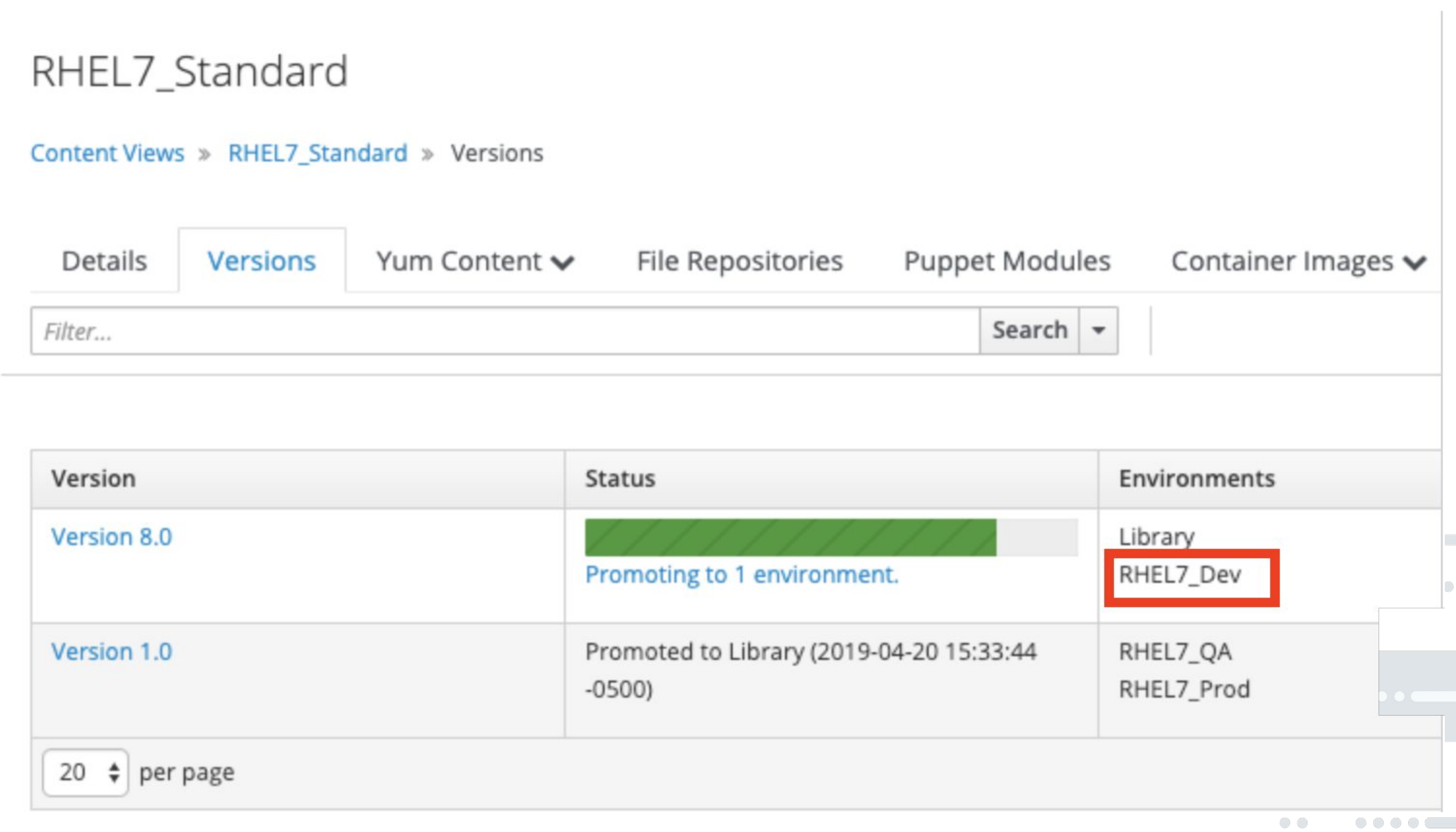
STATUS	● Running
STARTED	4/29/2019 8:36:01 AM
FINISHED	Not Finished
TEMPLATE	PATCHING / 1 - Dev
LAUNCHED BY	admin

EXTRA VARIABLES YAML JSON EXPAND

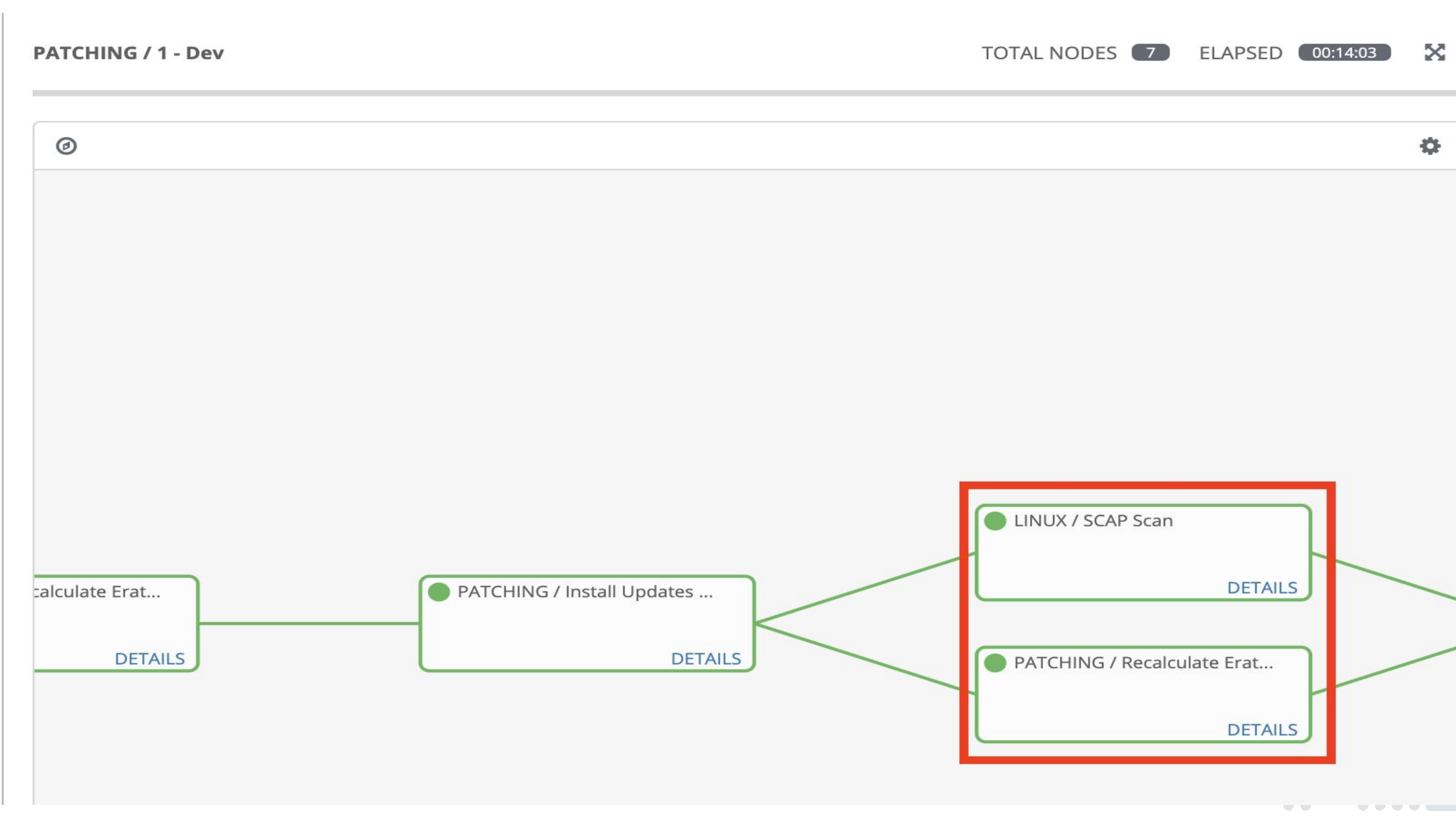
```
---
```

PATCHING / 1 - Dev TOTAL NODES 7 ELAPSED 00:00:44

PATCHING / Publish Content
DETAILS
PATCHING / Promote Content
PATCHING / Recalculate Erat...
PATCHING / Install Updates ...
LINUX / SCAP Scan
PATCHING / Recalculate Erat...



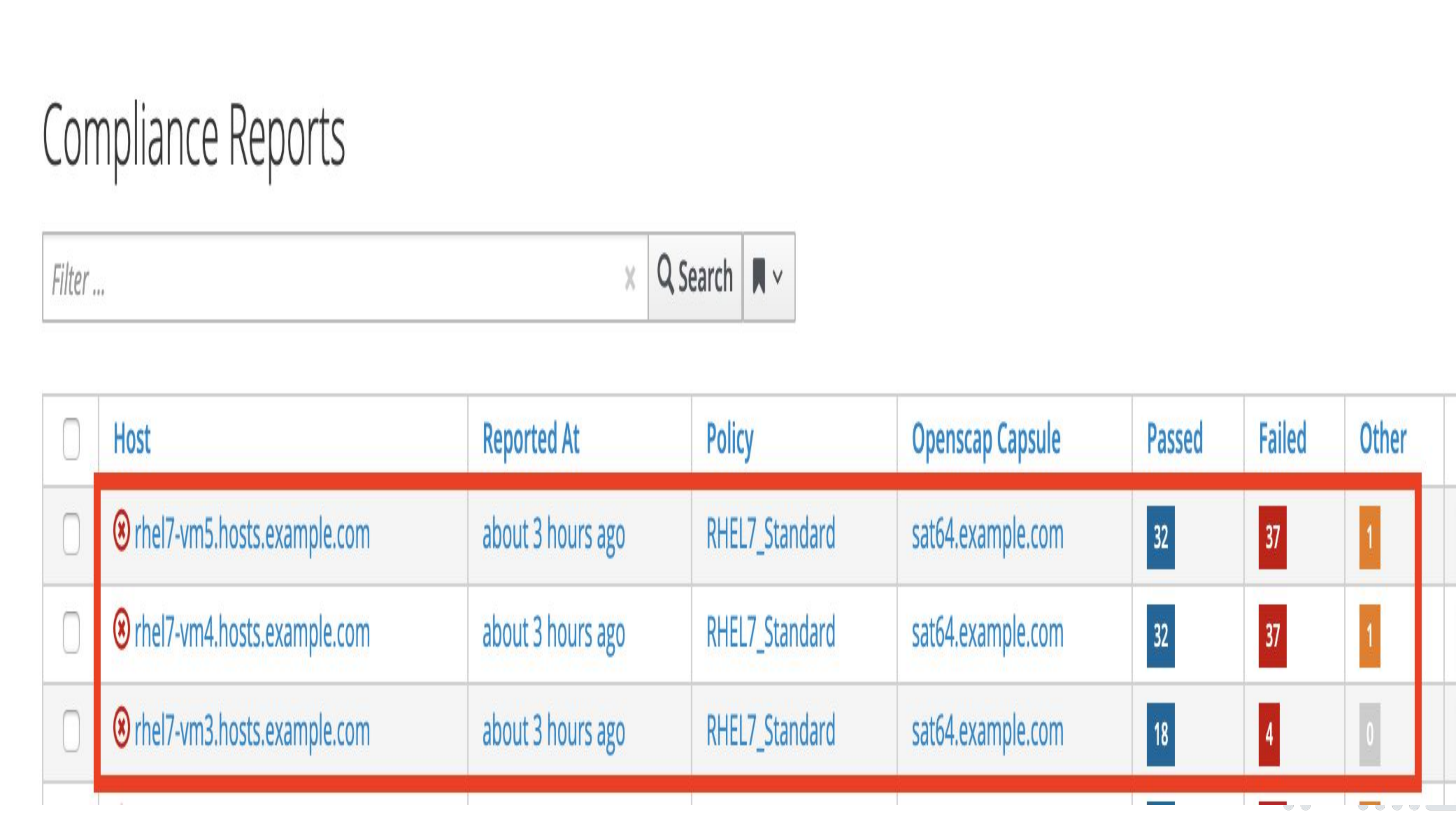
Version	Status	Environments
Version 8.0	Promoting to 1 environment.	Library RHEL7_Dev
Version 1.0	Promoted to Library (2019-04-20 15:33:44 -0500)	RHEL7_QA RHEL7_Prod



PATCHING / 1 - Dev

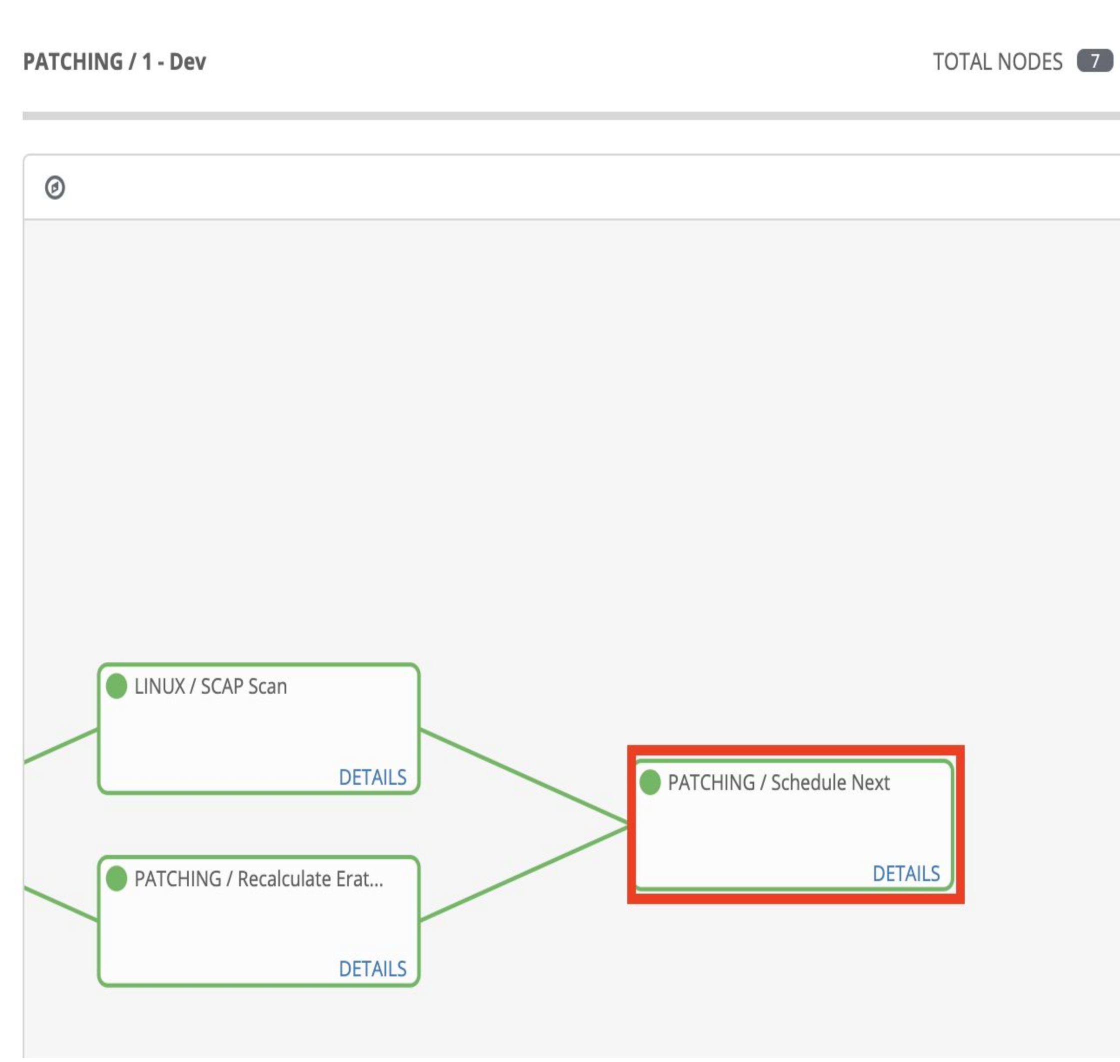
TOTAL NODES 7

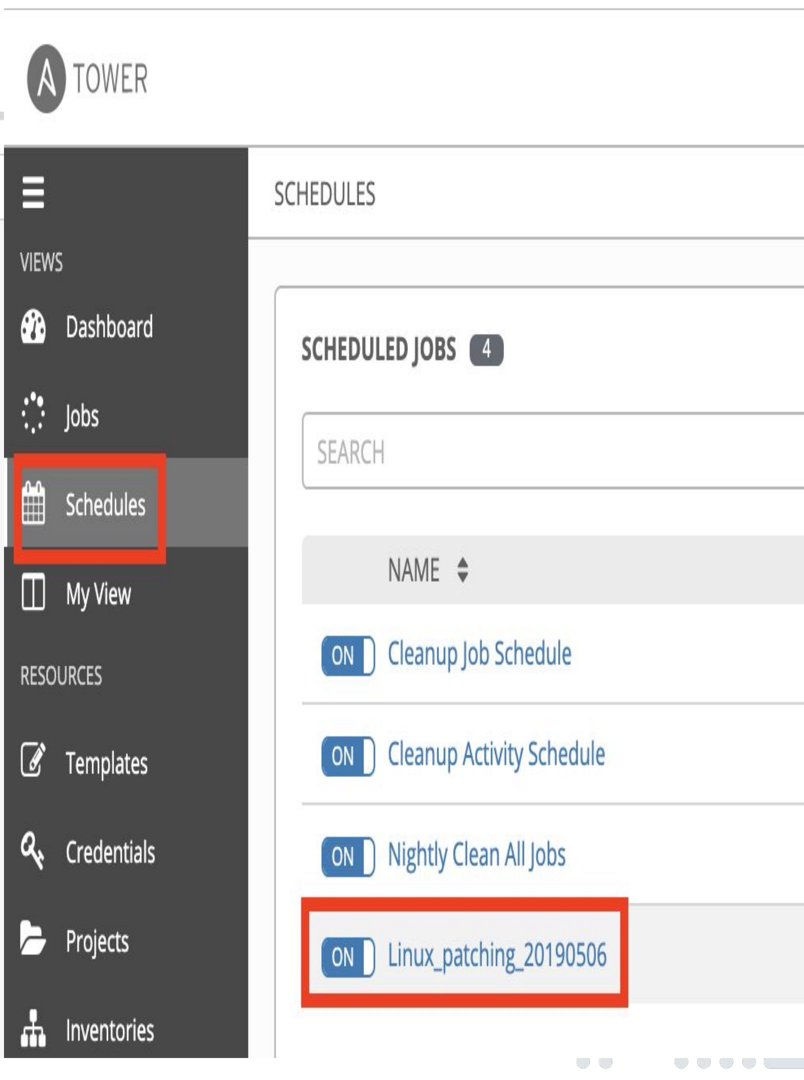
ELAPSED 00:14:03



Compliance Reports

□	Host	Reported At	Policy	Openscap Capsule	Passed	Failed	Other
□	⊗ rhel7-vm5.hosts.example.com	about 3 hours ago	RHEL7_Standard	sat64.example.com	32	37	1
□	⊗ rhel7-vm4.hosts.example.com	about 3 hours ago	RHEL7_Standard	sat64.example.com	32	37	1
□	⊗ rhel7-vm3.hosts.example.com	about 3 hours ago	RHEL7_Standard	sat64.example.com	18	4	0



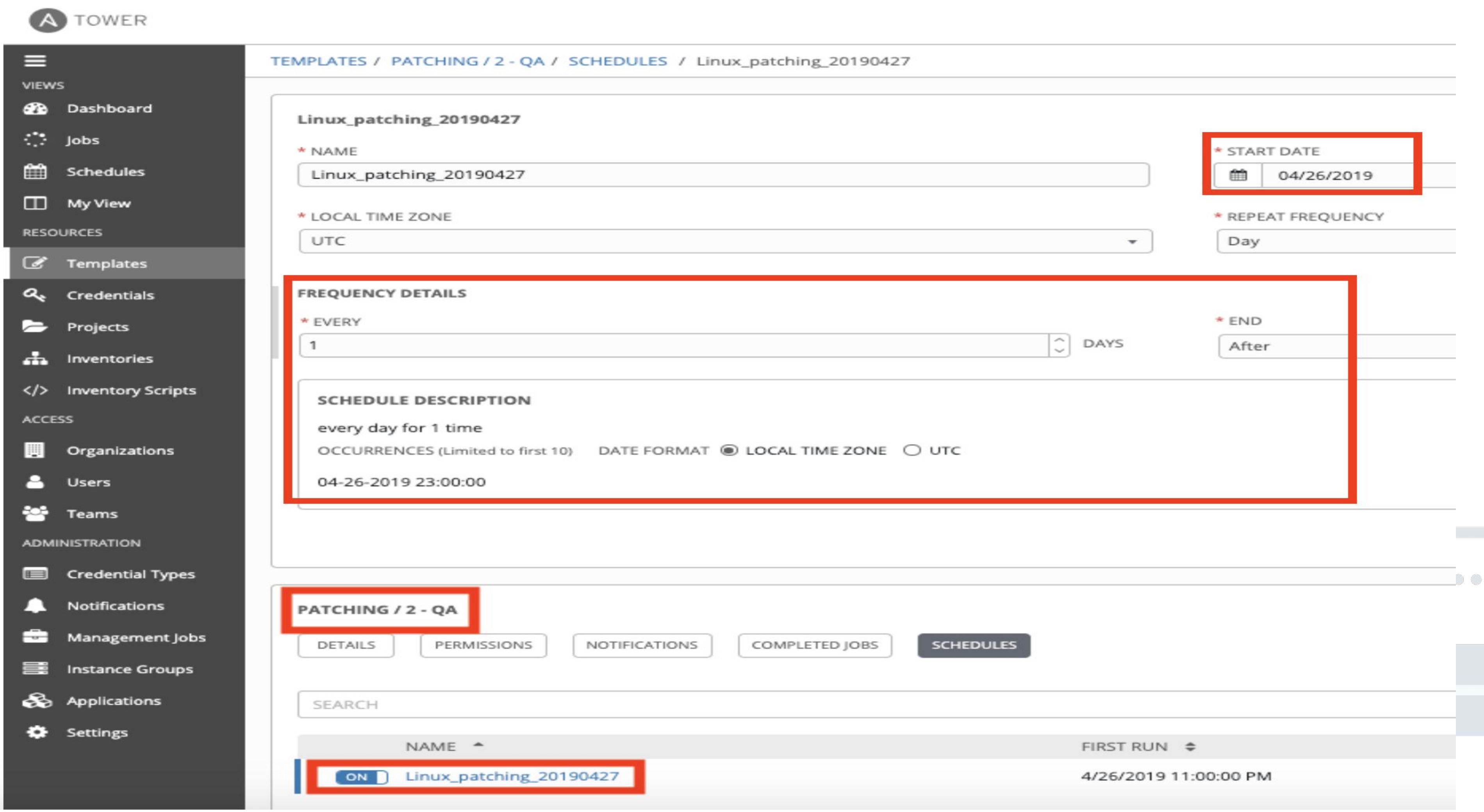


ON Cleanup Job Schedule

ON Cleanup Activity Schedule

ON Nightly Clean All Jobs

ON Linux_patching_20190506



TEMPLATES / PATCHING / 2 - QA / SCHEDULES / Linux_patching_20190427

Linux_patching_20190427

* NAME: Linux_patching_20190427

* START DATE: 04/26/2019

* LOCAL TIME ZONE: UTC

* REPEAT FREQUENCY: Day

FREQUENCY DETAILS

* EVERY: 1 DAYS

* END: After

SCHEDULE DESCRIPTION

every day for 1 time

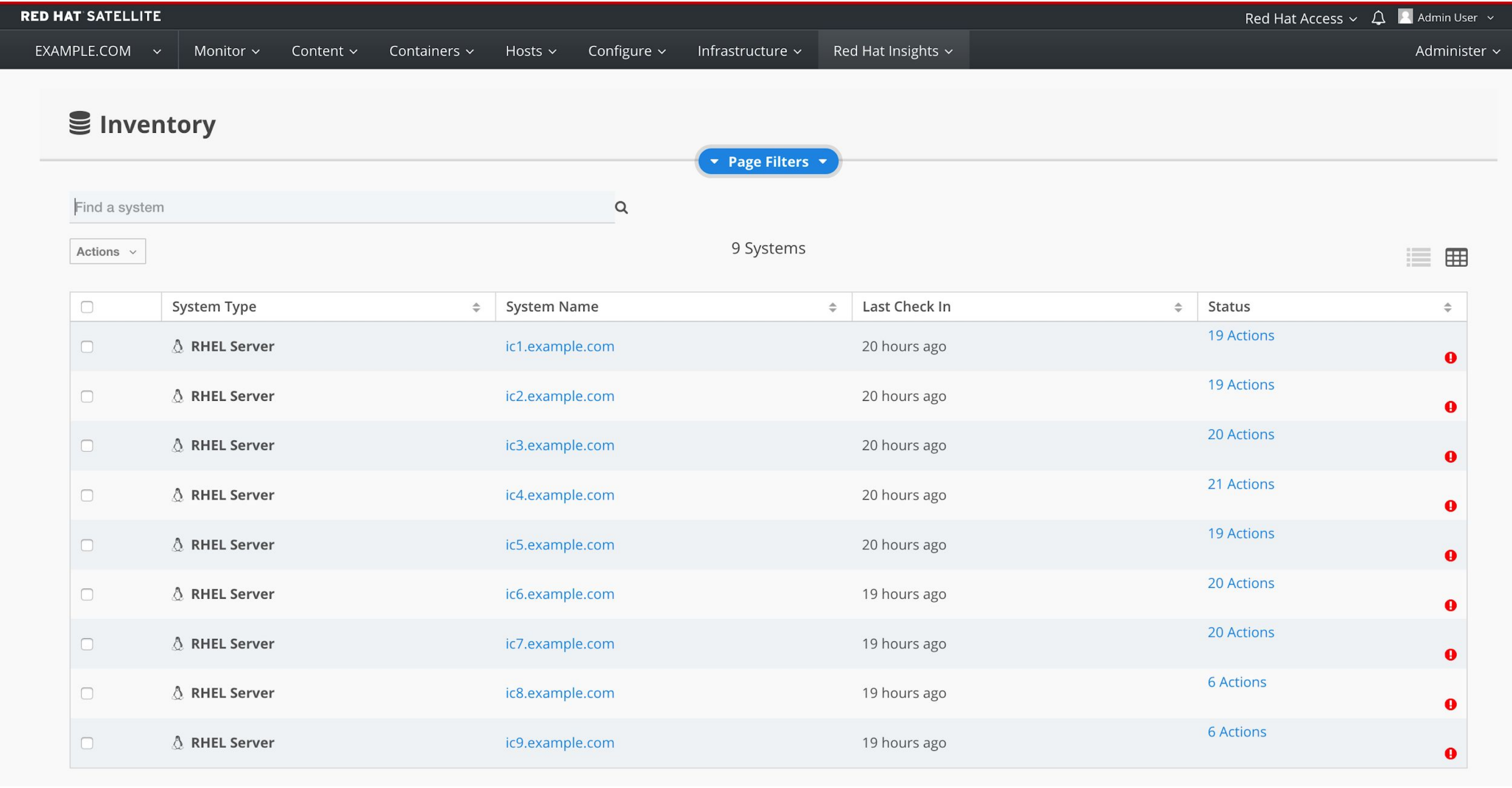
OCCURRENCES (Limited to first 10) DATE FORMAT ● LOCAL TIME ZONE ○ UTC

04-26-2019 23:00:00

PATCHING / 2 - QA

NAME	FIRST RUN
ON Linux_patching_20190427	4/26/2019 11:00:00 PM

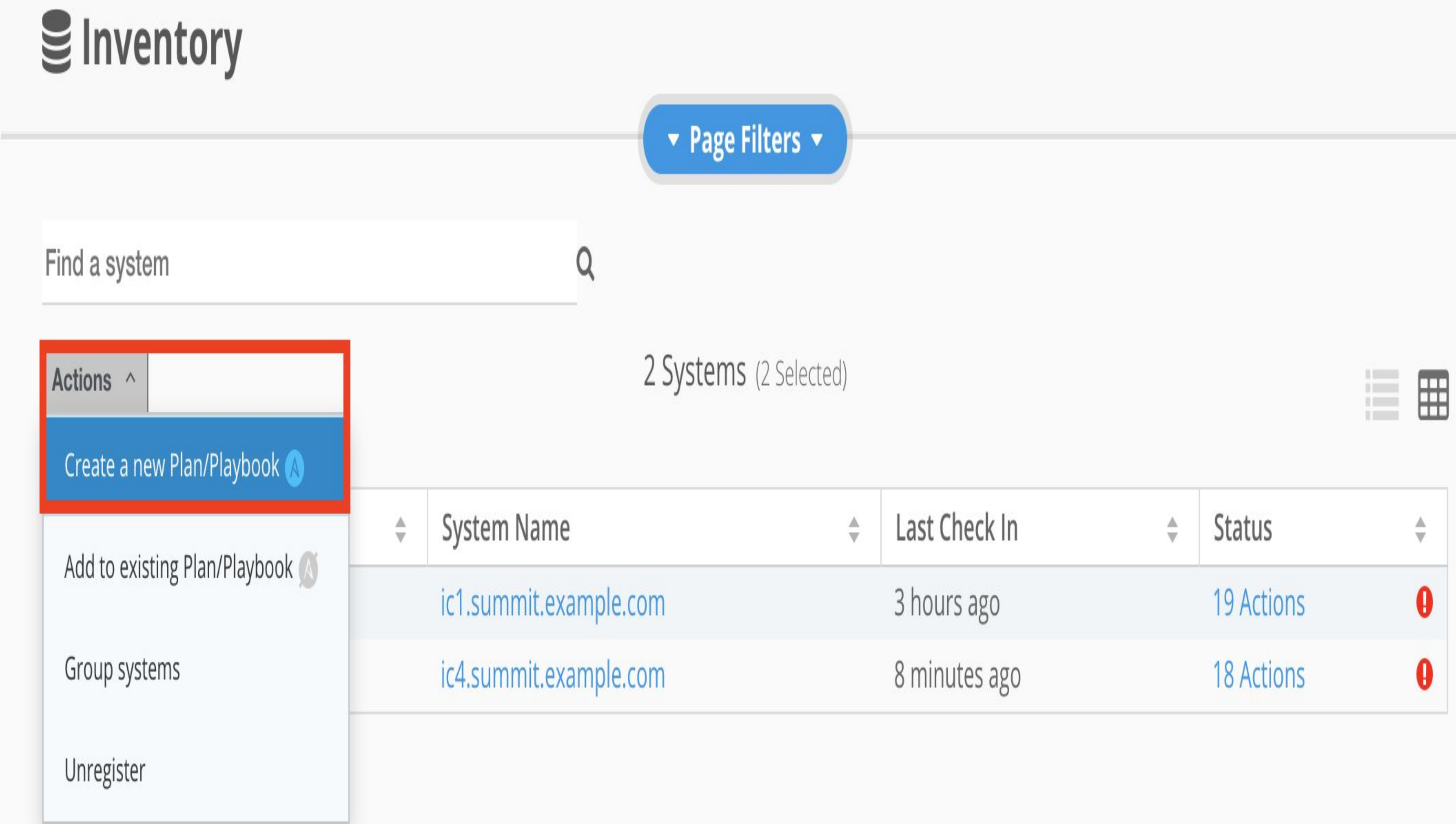
Proactive Security and Automated Risk Management with Predictive Analytics



Inventory

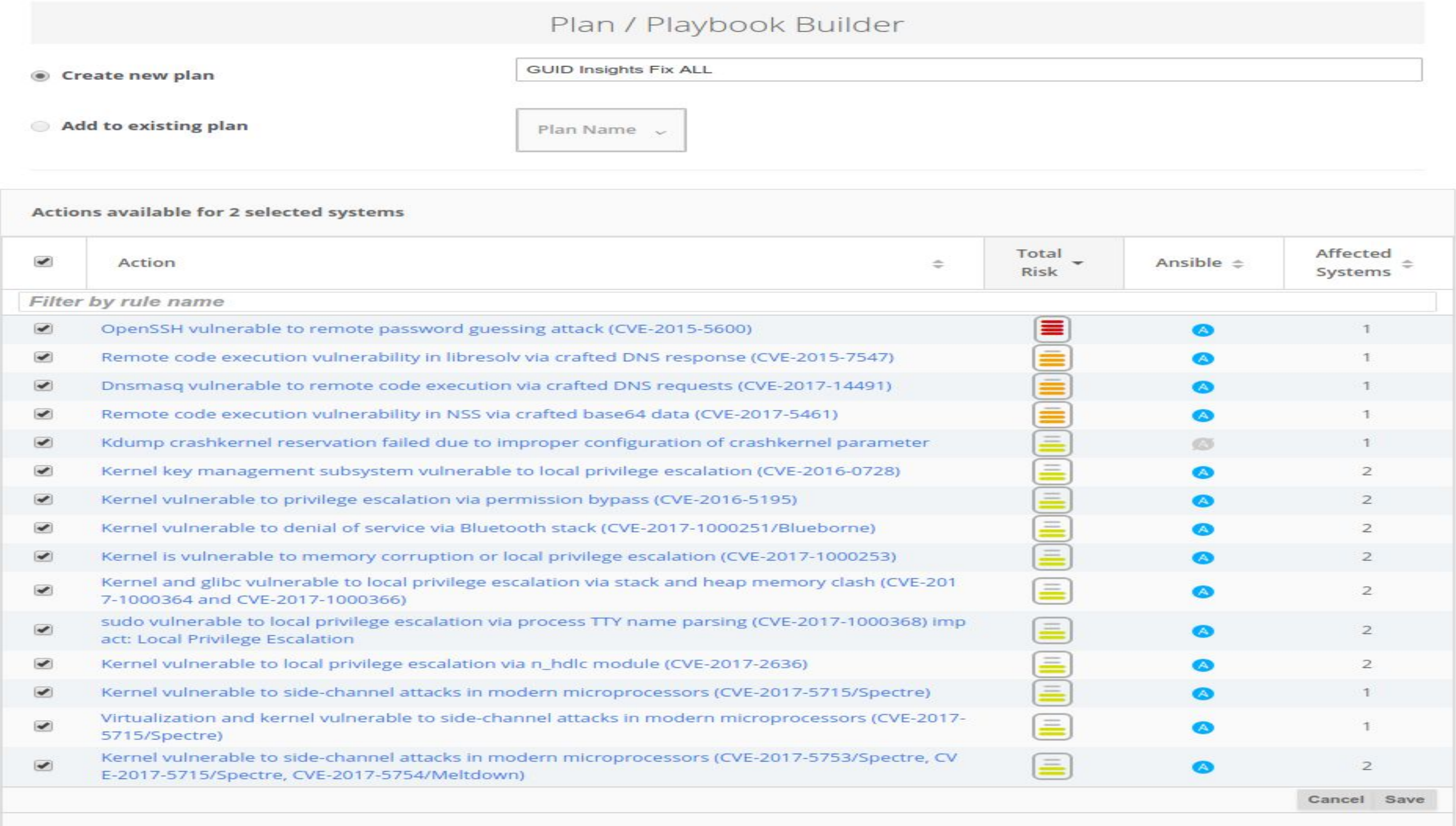
9 Systems

□	System Type	System Name	Last Check In	Status
□	RHEL Server	ic1.example.com	20 hours ago	19 Actions
□	RHEL Server	ic2.example.com	20 hours ago	19 Actions
□	RHEL Server	ic3.example.com	20 hours ago	20 Actions
□	RHEL Server	ic4.example.com	20 hours ago	21 Actions
□	RHEL Server	ic5.example.com	20 hours ago	19 Actions
□	RHEL Server	ic6.example.com	19 hours ago	20 Actions
□	RHEL Server	ic7.example.com	19 hours ago	20 Actions
□	RHEL Server	ic8.example.com	19 hours ago	6 Actions
□	RHEL Server	ic9.example.com	19 hours ago	6 Actions



2 Systems (2 Selected)

System Name	Last Check In	Status	
ic1.summit.example.com	3 hours ago	19 Actions	!
ic4.summit.example.com	8 minutes ago	18 Actions	!



Plan / Playbook Builder

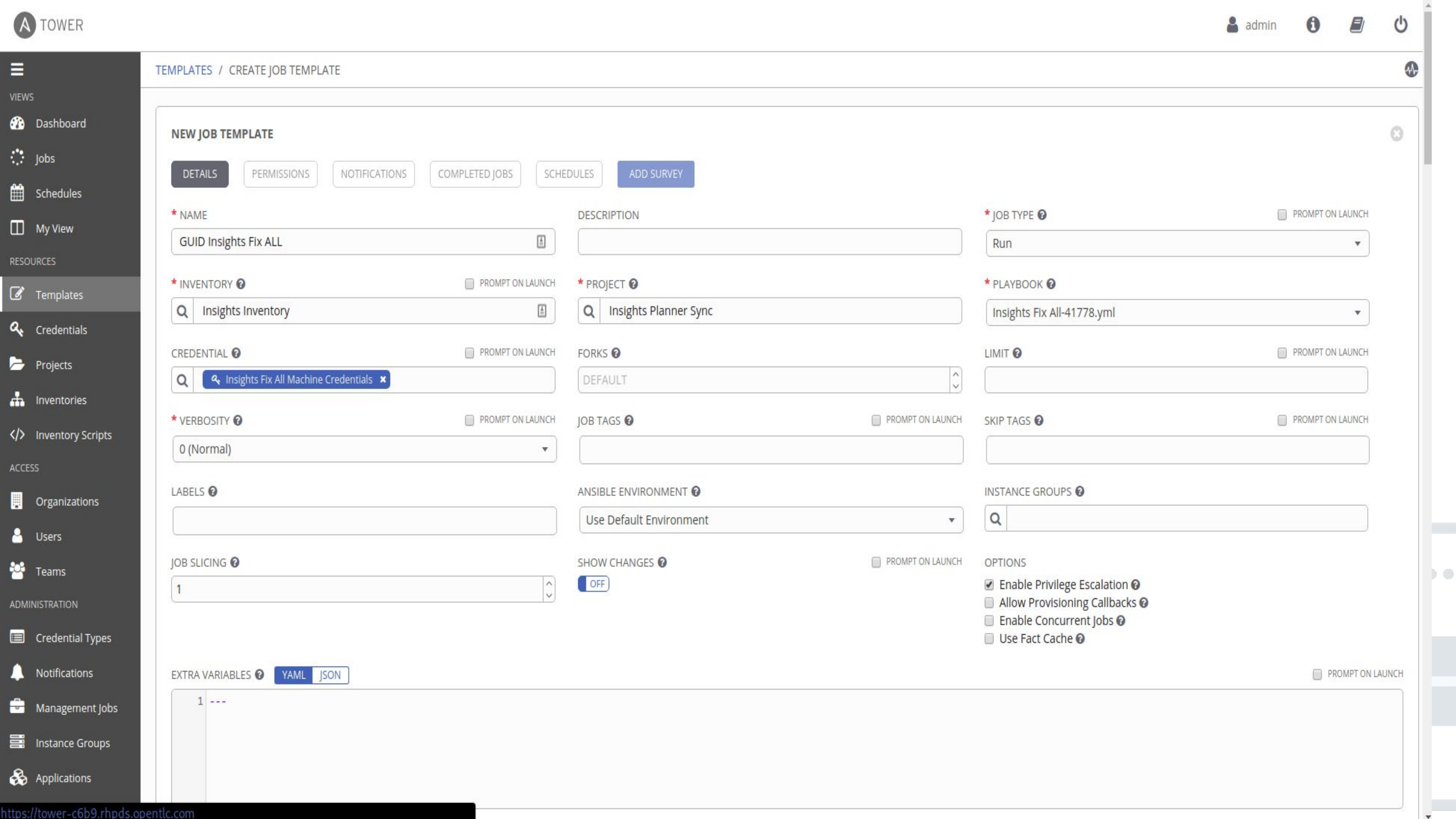
● Create new plan — GUID Insights Fix ALL

○ Add to existing plan — Plan Name ⌄

Actions available for 2 selected systems

Filter by rule name

☑	Action	Total Risk	Ansible	Affected Systems
☑	OpenSSH vulnerable to remote password guessing attack (CVE-2015-5600)	🟥	Ⓐ	1
☑	Remote code execution vulnerability in libresolv via crafted DNS response (CVE-2015-7547)	🟧	Ⓐ	1
☑	Dnsmasq vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)	🟧	Ⓐ	1
☑	Remote code execution vulnerability in NSS via crafted base64 data (CVE-2017-5461)	🟧	Ⓐ	1
☑	Kdump crashkernel reservation failed due to improper configuration of crashkernel parameter	🟨	Ⓐ	1
☑	Kernel key management subsystem vulnerable to local privilege escalation (CVE-2016-0728)	🟨	Ⓐ	2
☑	Kernel vulnerable to privilege escalation via permission bypass (CVE-2016-5195)	🟨	Ⓐ	2
☑	Kernel vulnerable to denial of service via Bluetooth stack (CVE-2017-1000251/Blueborne)	🟨	Ⓐ	2
☑	Kernel is vulnerable to memory corruption or local privilege escalation (CVE-2017-1000253)	🟨	Ⓐ	2
☑	Kernel and glibc vulnerable to local privilege escalation via stack and heap memory clash (CVE-2017-1000364 and CVE-2017-1000366)	🟨	Ⓐ	2
☑	sudo vulnerable to local privilege escalation via process TTY name parsing (CVE-2017-1000368) impact: Local Privilege Escalation	🟨	Ⓐ	2
☑	Kernel vulnerable to local privilege escalation via n_hdlc module (CVE-2017-2636)	🟨	Ⓐ	2
☑	Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre)	🟨	Ⓐ	1
☑	Virtualization and kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre)	🟨	Ⓐ	1
☑	Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5753/Spectre, CVE-2017-5715/Spectre, CVE-2017-5754/Meltdown)	🟨	Ⓐ	2



NEW JOB TEMPLATE

* NAME: GUID Insights Fix ALL

DESCRIPTION:

* JOB TYPE: Run — □ PROMPT ON LAUNCH

* INVENTORY: Insights Inventory — □ PROMPT ON LAUNCH

* PROJECT: Insights Planner Sync

* PLAYBOOK: Insights Fix All-41778.yml

CREDENTIAL: Insights Fix All Machine Credentials — □ PROMPT ON LAUNCH

FORKS: DEFAULT

LIMIT: — □ PROMPT ON LAUNCH

* VERBOSITY: 0 (Normal) — □ PROMPT ON LAUNCH

JOB TAGS: — □ PROMPT ON LAUNCH

SKIP TAGS: — □ PROMPT ON LAUNCH

LABELS:

ANSIBLE ENVIRONMENT: Use Default Environment

INSTANCE GROUPS:

JOB SLICING: 1

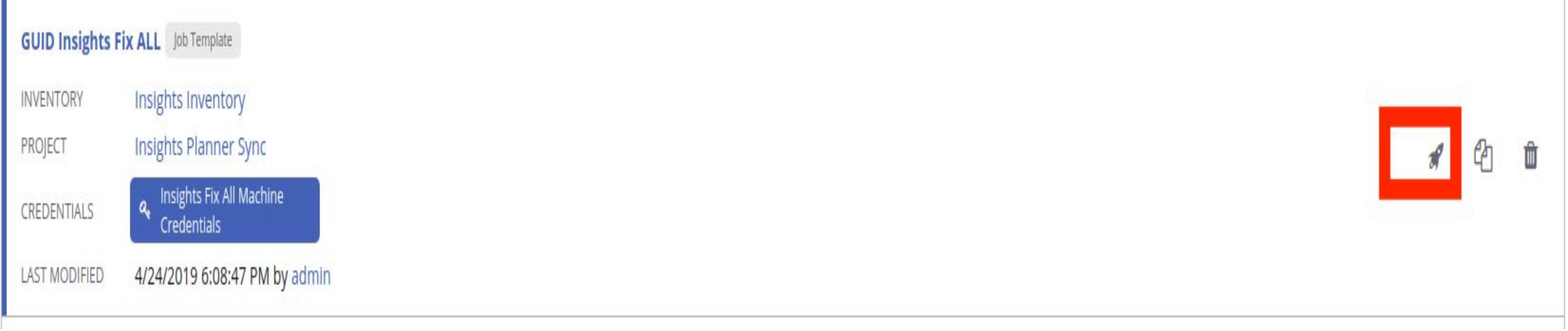
SHOW CHANGES: OFF — □ PROMPT ON LAUNCH

OPTIONS

- ☑ Enable Privilege Escalation
- □ Allow Provisioning Callbacks
- □ Enable Concurrent Jobs
- □ Use Fact Cache

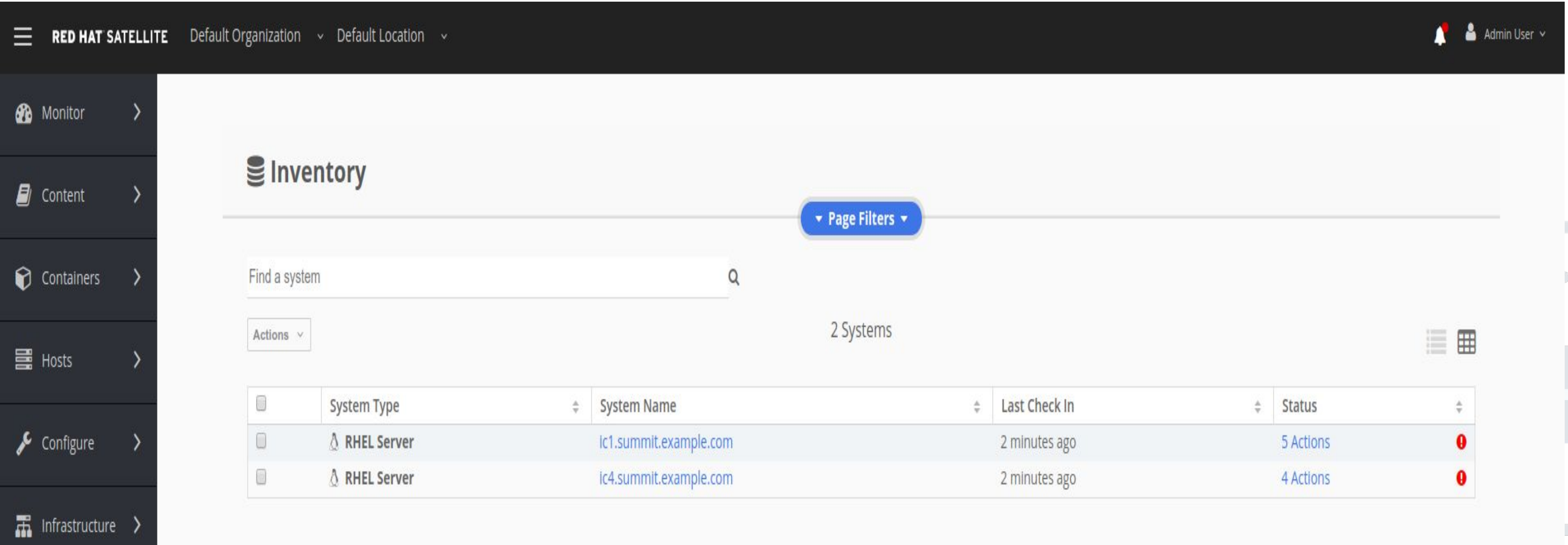
EXTRA VARIABLES: YAML JSON — □ PROMPT ON LAUNCH

```
---
```



GUID Insights Fix ALL

INVENTORY	Insights Inventory
PROJECT	Insights Planner Sync
CREDENTIALS	Insights Fix All Machine Credentials
LAST MODIFIED	4/24/2019 6:08:47 PM by admin



Inventory

2 Systems

□	System Type	System Name	Last Check In	Status
□	RHEL Server	ic1.summit.example.com	2 minutes ago	5 Actions !
□	RHEL Server	ic4.summit.example.com	2 minutes ago	4 Actions !

Red Hat Insights Rules for Red Hat OpenShift Container Platform

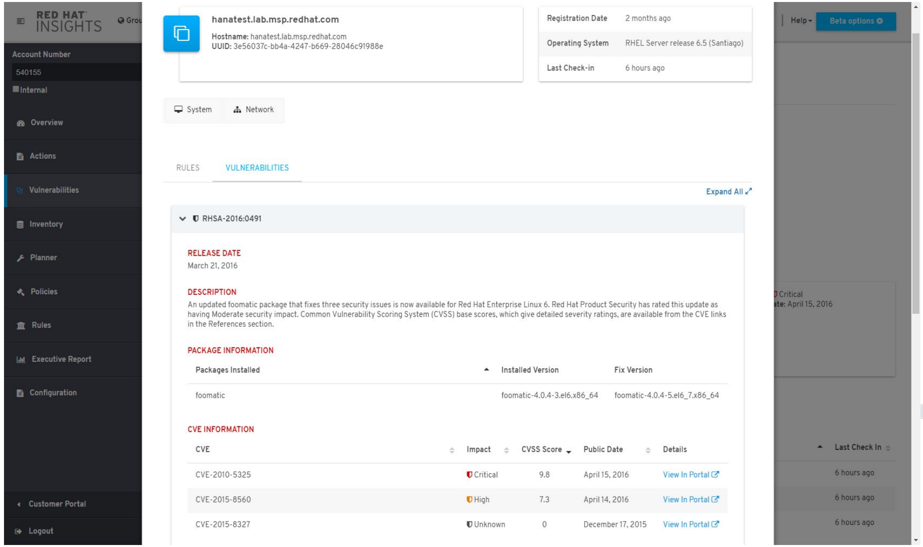
- Communication fails between components when certificates have expired in Openshift
- Image build failure when creating a large number of concurrent builds
- Containers allow non-privileged user to modify filesystem inside containers when created with cri-o
- Docker registry pod restarts occasionally when liveness and readiness probes collide
- Failed api connection between docker and OpenShift when version of docker and openshift are incompatible
- Insufficient space available when image garbage collection fails to run in OpenShift
- GlusterFS storage disconnects from pods when restarting atomic-openshift-node server
- Master controller fails to start when changes are made to the SDN plugin if there are headless services in the cluster
- Failure to connect to service when configured IP is in use by another service
- Pod creation fails when is under high load due to iptables-restore process
- Excessive load time for new routes when a large number of routes exist
- Router does not work when deleting route with host set to "localhost"

Vulnerability Management (SaaS offering)

PURPOSE

Eeep security CVE analysis like that found in Satellite.

Provide CVE scanning of registered assets, including RHEL and RHEL-based images and provide these capabilities in a SaaS deployment.



hanatest.lab.msp.redhat.com

Hostname: hanatest.lab.msp.redhat.com
UUID: 3e56037c-bb4a-4247-b669-28046c91988e

Registration Date	2 months ago
Operating System	RHEL Server release 6.5 (Santiago)
Last Check-in	6 hours ago

RHSA-2016:0491

RELEASE DATE
March 21, 2016

DESCRIPTION
An updated foomatic package that fixes three security issues is now available for Red Hat Enterprise Linux 6. Red Hat Product Security has rated this update as having Moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available from the CVE links in the References section.

PACKAGE INFORMATION

Packages Installed	Installed Version	Fix Version
foomatic	foomatic-4.0.4-3.el6.x86_64	foomatic-4.0.4-5.el6_7.x86_64

CVE INFORMATION

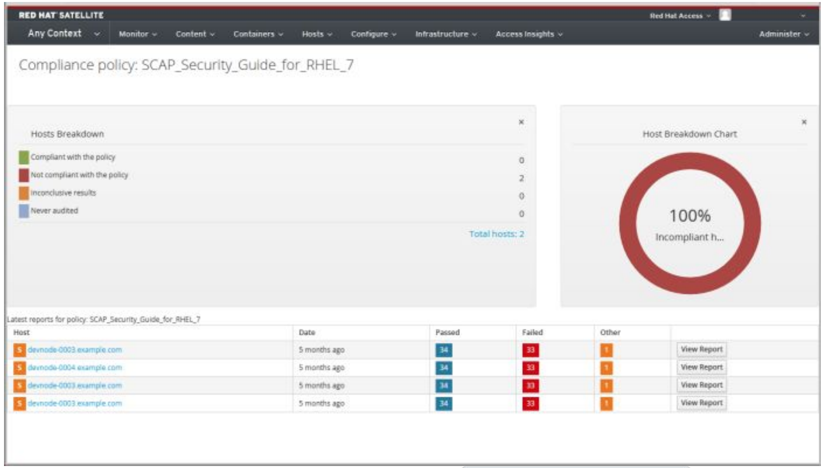
CVE	Impact	CVSS Score	Public Date	Details
CVE-2010-5325	Critical	9.8	April 15, 2016	View In Portal
CVE-2015-8560	High	7.3	April 14, 2016	View In Portal
CVE-2015-8327	Unknown	0	December 17, 2015	View In Portal

Compliance Management(SaaS offering)

PURPOSE

Leverage OpenSCAP

Provide a unified view to identify the current health of their Red Hat estate in a SaaS deployment.



Compliance policy: SCAP_Security_Guide_for_RHEL_7

Hosts Breakdown

🟩 Compliant with the policy	0
🟥 Not compliant with the policy	2
🟧 Inconclusive results	0
🟦 Never audited	0

Total hosts: 2

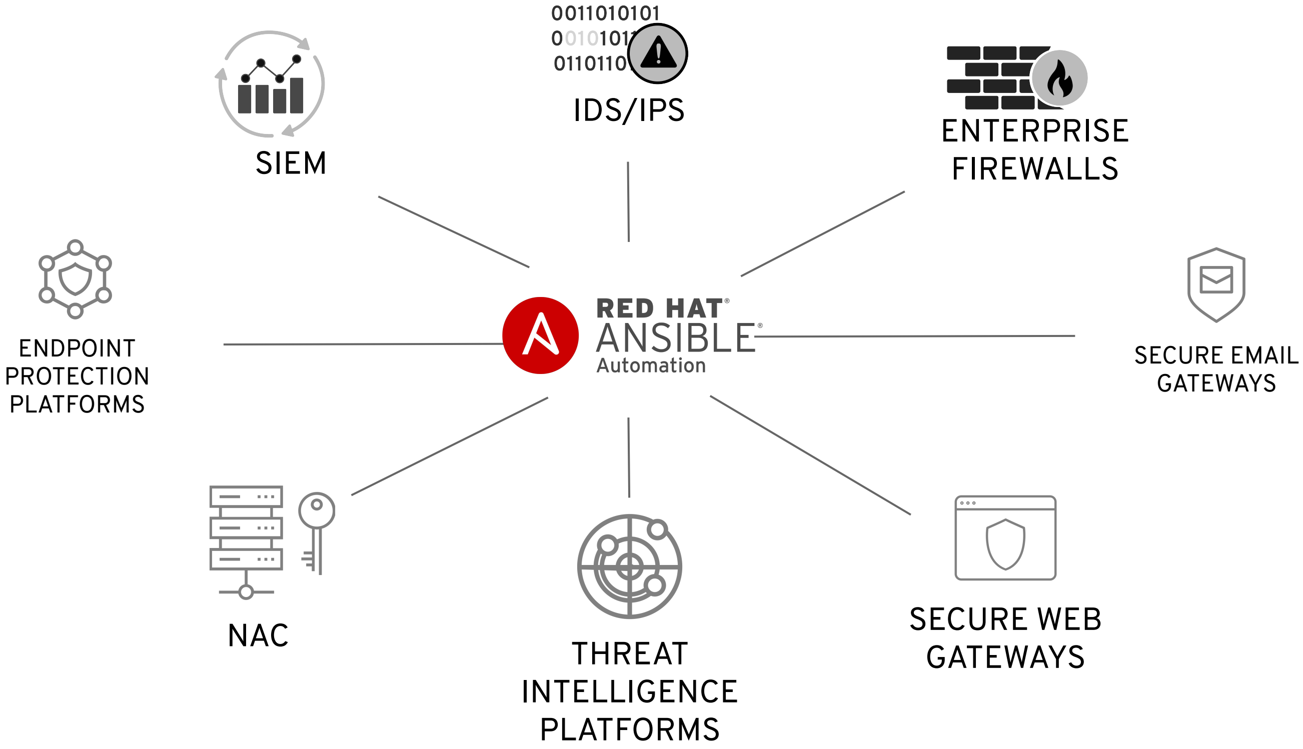
Host Breakdown Chart

Latest reports for policy: SCAP_Security_Guide_for_RHEL_7

Host	Date	Passed	Failed	Other	
S devnode-0003.example.com	5 months ago	34	33	1	View Report
S devnode-0004.example.com	5 months ago	34	33	1	View Report
S devnode-0003.example.com	5 months ago	34	33	1	View Report
S devnode-0003.example.com	5 months ago	34	33	1	View Report

Automated Security and Compliance with Red Hat

Security Operations Center
(SOC)



RED HAT® ANSIBLE® Automation

SIEM

IDS/IPS

ENTERPRISE FIREWALLS

ENDPOINT PROTECTION PLATFORMS

SECURE EMAIL GATEWAYS

NAC

THREAT INTELLIGENCE PLATFORMS

SECURE WEB GATEWAYS

Who Are We Working With?

Enterprise Firewalls

Check Point
SOFTWARE TECHNOLOGIES LTD

paloalto
NETWORKS

Intrusion Detection & Prevention Systems

SNORT

cisco

Security Information & Events Management

splunk>

IBM

What Does It Do?

Triage Of Suspicious Activities

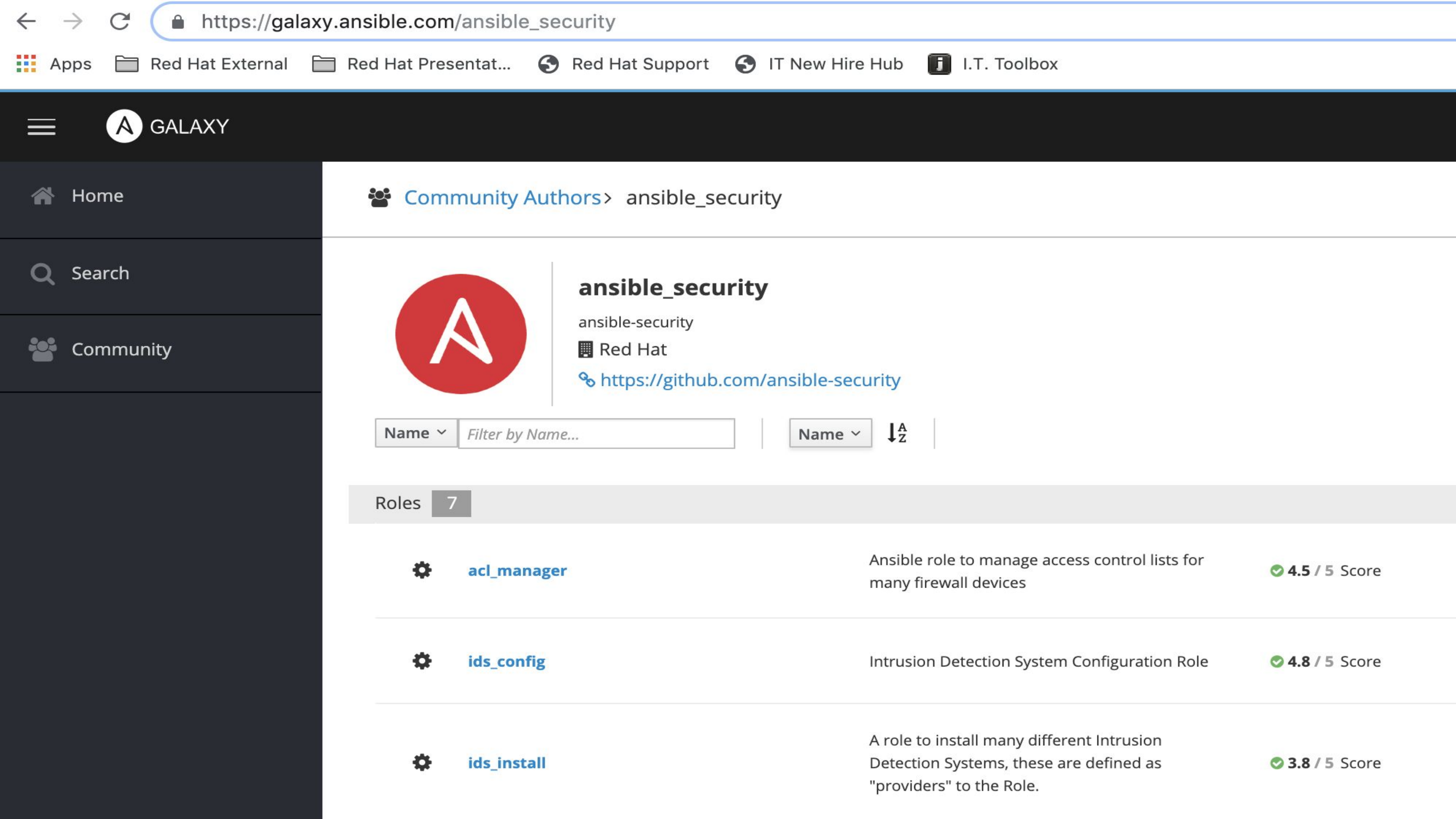
Enabling programmatic access to log configurations such as destination, verbosity, etc.

Threat Hunting

Automating alerts, correlation searches and signature manipulation

Incident Response

Creating new security policies to whitelist, blacklist or quarantine a machine



Community Authors > ansible_security

ansible_security

ansible-security

Red Hat

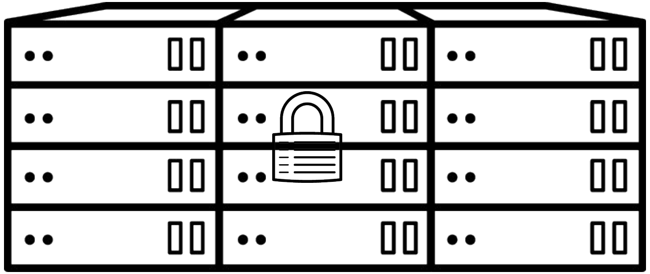
https://github.com/ansible-security

Roles 7

acl_manager	Ansible role to manage access control lists for many firewall devices	✓ 4.5 / 5 Score
ids_config	Intrusion Detection System Configuration Role	✓ 4.8 / 5 Score
ids_install	A role to install many different Intrusion Detection Systems, these are defined as "providers" to the Role.	✓ 3.8 / 5 Score

Automated Security and Compliance with Red Hat

Applications



Infrastructure and Operations

Security Operations Center
(SOC)

TAKEAWAYS

1. Identify your **risk tolerance**. There's no such thing as 100% security.

2. Security is **everyone's** job. Take a **holistic, continuous, defense-in-depth** approach to security.

3. **Prevention, Detection, Response**. Implement security hygiene practices (regular patches, etc).

4. Leverage the security technologies that **you already have** (OS, Middleware, etc)

5. Identify **focus areas for automation** , **take baby steps,** and learn from **examples**
(Keep in Mind: There's **no such thing as one size fits all** for automation or DevSecOps)

6. Security is not *just* about technology - the **human factor** can be your weakest link!
(social engineering breaches, insider threats, lack of skills, bad processes in place, etc)

Red Hat Training Offerings

1. D0500: DevOps Culture and Practice Enablement
2. D0700: Container Adoption Boot Camp
3. D0426: Securing Containers and OpenShift (with exam)

   <Also free OpenShift hands-on training on : http://learn.openshift.com/>
4. RH415: Red Hat Security: Linux in Physical, Virtual, Cloud (with exam)
5. RH413: Red Hat Security and Server Hardening (with exam)

Red Hat Security Related Links

- Solution Brief: Increase Security and Compliance with Advanced Automation
  - https://www.redhat.com/en/resources/automate-security-compliance-solution-brief
- Whitepaper: Red Hat Automated Security and Compliance
  - https://www.redhat.com/en/resources/red-hat-automated-security-and-compliance
- Red Hat Consulting Services Datasheet: Automate Security and Reliability Workflows
  - https://www.redhat.com/en/resources/services-consulting-automate-security-reliability-datasheet
- Red Hat provided and supported Ansible security hardening Ansible playbooks in Ansible Galaxy
  - https://galaxy.ansible.com/RedHatOfficial
- Red Hat Security Hands-on Labs
  - https://red.ht/securitylabs

Red Hat Security Related Links (cont..)

- Guide to continuous security
    - https://www.redhat.com/en/technologies/guide/it-security
- Understanding IT Security
    - https://www.redhat.com/en/topics/security
- Container Security
    - https://www.redhat.com/en/topics/security/container-security
- Red Hat Product Security
    - https://access.redhat.com/security/overview

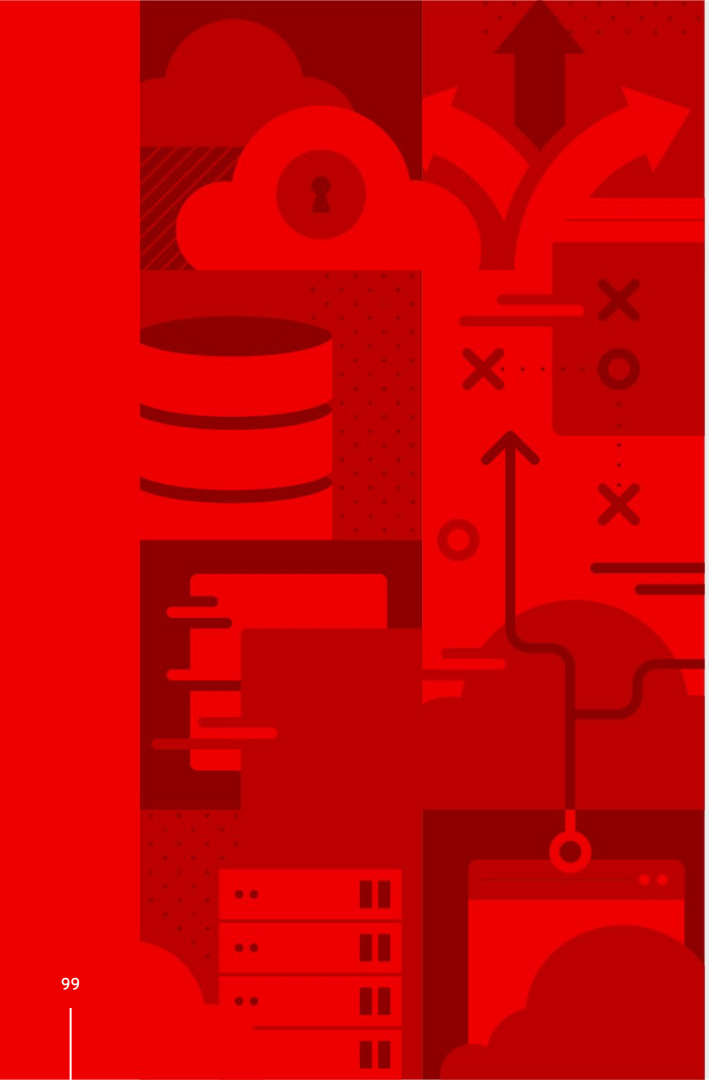
Next Steps

- Speak with a Red Hat expert here at Security Symposium
- Look for the slides in a “Thank You” email from us in the next few days
- Stay up to date with Red Hat at redhat.com/security
- Visit redhat.com/events to find out about workshops and other events like this one coming to your area

Thank you for coming.

Feedback or questions?

infrastructure@redhat.com



Questions?

lkerner@redhat.com

Thank you

Red Hat is the world's leading provider of

enterprise open source software solutions.

Award-winning support, training, and consulting

services make

Red Hat a trusted adviser to the Fortune 500.

in linkedin.com/company/red-hat

▶ youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat

Thank you to our partner