Red Hat
Smart Management

Some Assembly Required: Smart/Cloud Management

2/4/2020

Josh Swanson
Solution Architect

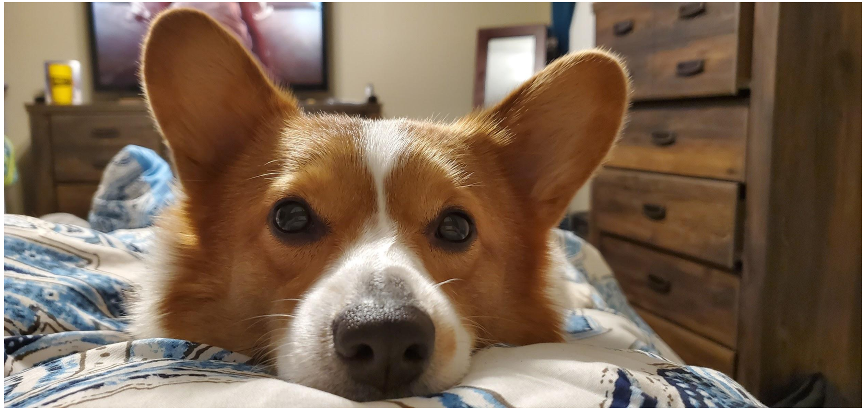
Mohit Goyal
Sr. Principal Product Manager

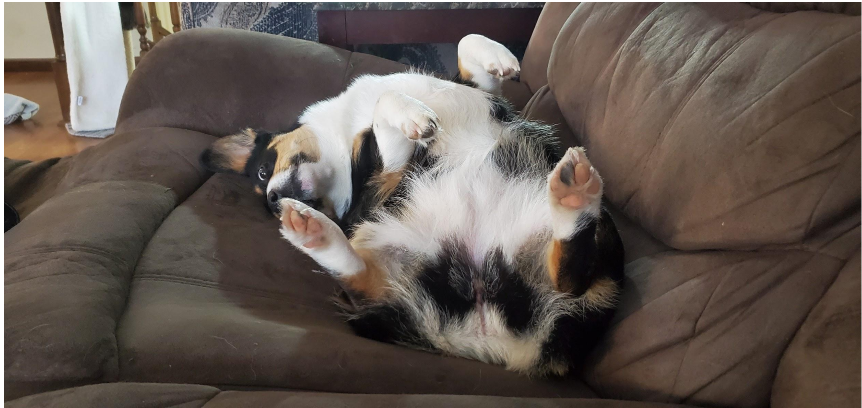
Red Hat

who am I?

Josh Swanson

jswanson@redhat.com





Housekeeping

Ansible Meetup

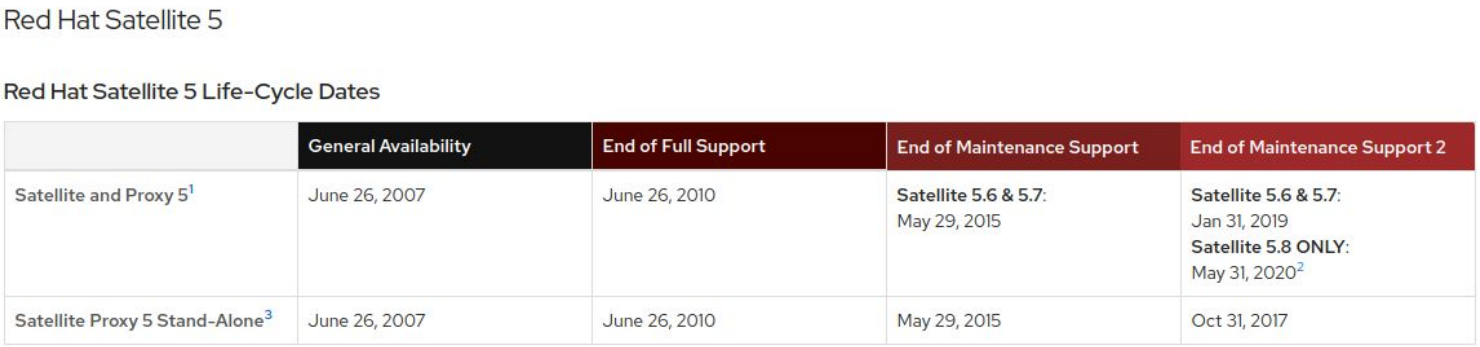
Thursday, February 20, 2020 - 6:30 PM to 9:30 PM

https://www.meetup.com/Ansible-Minneapolis/

Want to be a speaker? Let’s talk!

Red Hat Satellite 5.8 End of Life

There will NOT be ELS for satellite 5.8

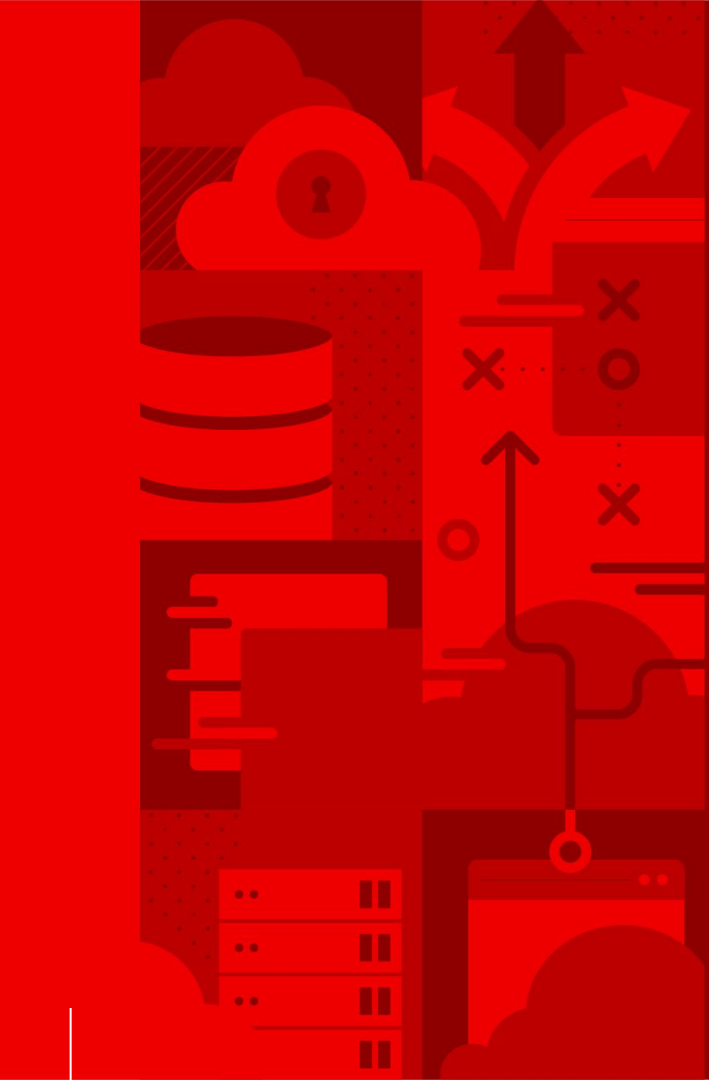


Red Hat Satellite 5

Red Hat Satellite 5 Life-Cycle Dates

	General Availability	End of Full Support	End of Maintenance Support	End of Maintenance Support 2
Satellite and Proxy 5[1]	June 26, 2007	June 26, 2010	**Satellite 5.6 & 5.7**: May 29, 2015	**Satellite 5.6 & 5.7**: Jan 31, 2019 **Satellite 5.8 ONLY**: May 31, 2020[2]
Satellite Proxy 5 Stand-Alone[3]	June 26, 2007	June 26, 2010	May 29, 2015	Oct 31, 2017

https://access.redhat.com/support/policy/updates/satellite/



Where Are We Going?

- Tracer (Tech Preview)
- Insights Deployment
- Smart/Cloud Management
- (Hopefully) Demos

CONFIDENTIAL Designator

Some Assembly Required: A Brief History of Tracer

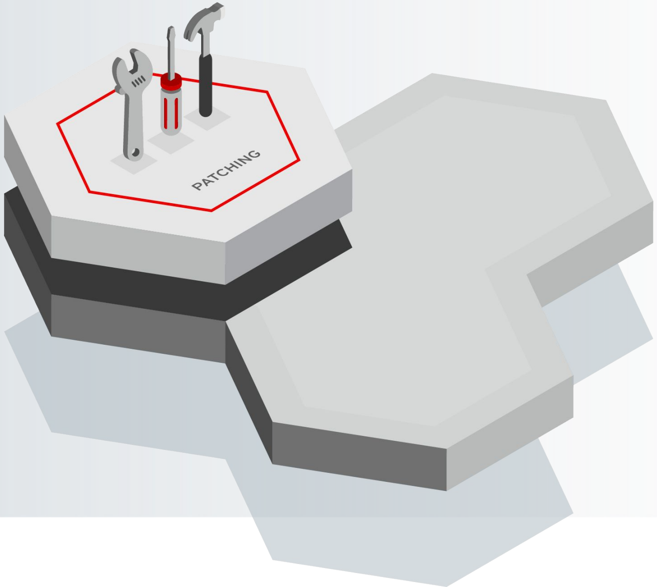
Tracer (Tech Preview) in Satellite 6.3 and later

Scott C. Danielson
Sr. Solution Architect

Josh Swanson
Solution Architect

Tracer (Tech Preview)

Post Patch Intelligence



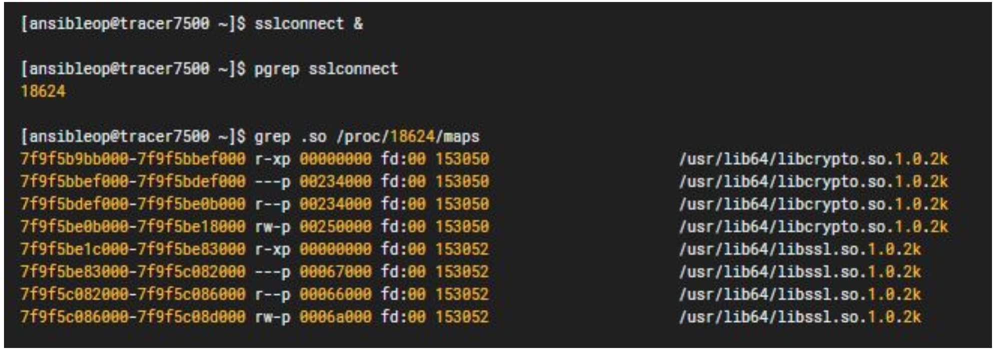
⚠ **Report** on services or processes that require restart or system that require a reboot post patching. (Tracer!)

Process dependencies on shared libraries

Example program is dynamically linked with dependencies on OpenSSL

We can see this by finding the PID of the sslconnect process, then looking at the `/proc/<PID>/maps` file to see if there are any references to deleted files:

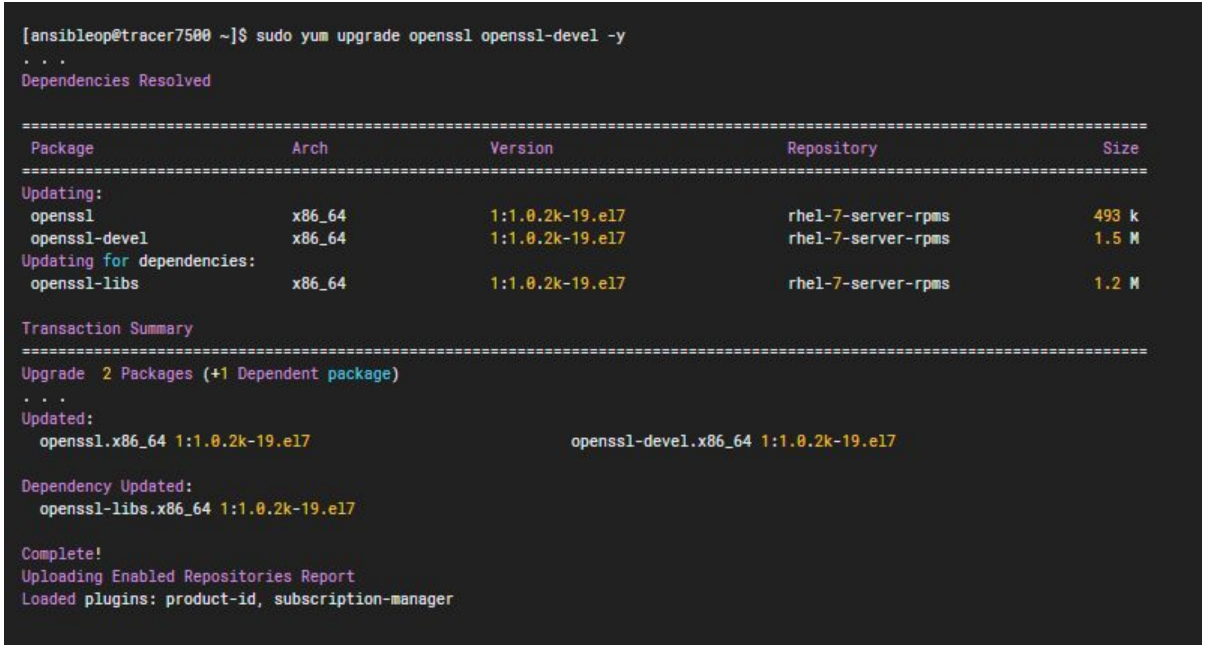
In our example, the PID is 18624.



```
[ansibleop@tracer7500 ~]$ sslconnect &

[ansibleop@tracer7500 ~]$ pgrep sslconnect
18624

[ansibleop@tracer7500 ~]$ grep .so /proc/18624/maps
7f9f5b9bb000-7f9f5bbef000 r-xp 00000000 fd:00 153050                    /usr/lib64/libcrypto.so.1.0.2k
7f9f5bbef000-7f9f5bdef000 ---p 00234000 fd:00 153050                    /usr/lib64/libcrypto.so.1.0.2k
7f9f5bdef000-7f9f5be0b000 r--p 00234000 fd:00 153050                    /usr/lib64/libcrypto.so.1.0.2k
7f9f5be0b000-7f9f5be18000 rw-p 00250000 fd:00 153050                    /usr/lib64/libcrypto.so.1.0.2k
7f9f5be1c000-7f9f5be83000 r-xp 00000000 fd:00 153052                    /usr/lib64/libssl.so.1.0.2k
7f9f5be83000-7f9f5c082000 ---p 00067000 fd:00 153052                    /usr/lib64/libssl.so.1.0.2k
7f9f5c082000-7f9f5c086000 r--p 00066000 fd:00 153052                    /usr/lib64/libssl.so.1.0.2k
7f9f5c086000-7f9f5c08d000 rw-p 0006a000 fd:00 153052                    /usr/lib64/libssl.so.1.0.2k
```

Patching can upgrade dependent libraries

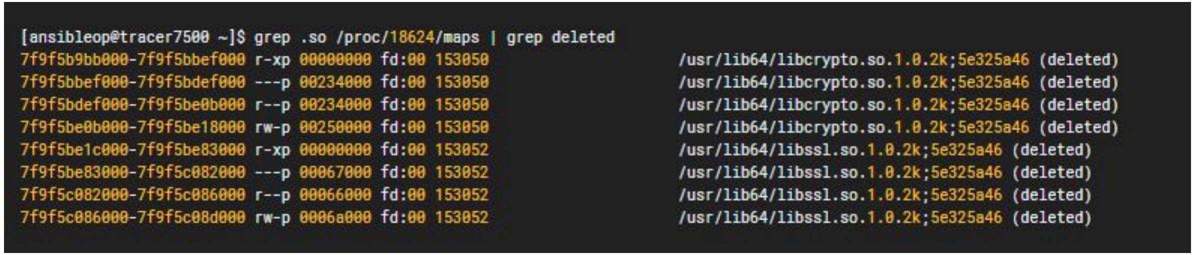
Now, we update the openssl packages and let’s see what we see in the maps file for our sslconnect process (pid = 18624)



```
[ansibleop@tracer7500 ~]$ sudo yum upgrade openssl openssl-devel -y
. . .
Dependencies Resolved

=============================================================================================================================
 Package                      Arch                  Version                          Repository                         Size
=============================================================================================================================
Updating:
 openssl                      x86_64                1:1.0.2k-19.el7                  rhel-7-server-rpms               493 k
 openssl-devel                x86_64                1:1.0.2k-19.el7                  rhel-7-server-rpms               1.5 M
Updating for dependencies:
 openssl-libs                 x86_64                1:1.0.2k-19.el7                  rhel-7-server-rpms               1.2 M

Transaction Summary
=============================================================================================================================
Upgrade  2 Packages (+1 Dependent package)
. . .
Updated:
  openssl.x86_64 1:1.0.2k-19.el7                             openssl-devel.x86_64 1:1.0.2k-19.el7

Dependency Updated:
  openssl-libs.x86_64 1:1.0.2k-19.el7

Complete!
Uploading Enabled Repositories Report
Loaded plugins: product-id, subscription-manager
```

Patching can upgrade dependent libraries

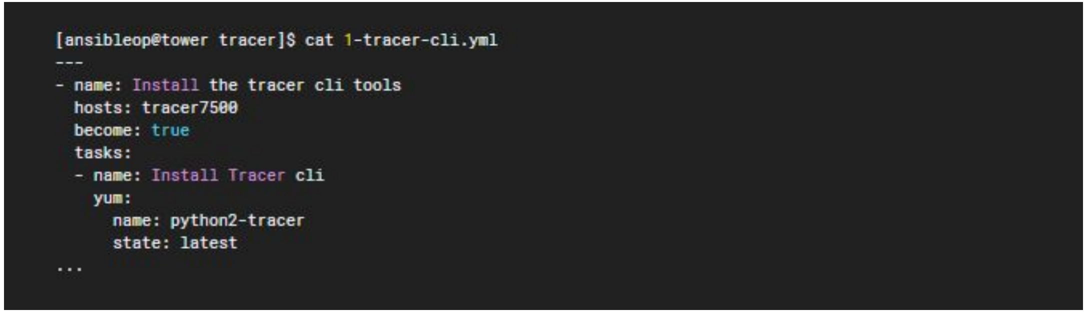
After patching, look at the memory map again (filter by searching for “deleted”)



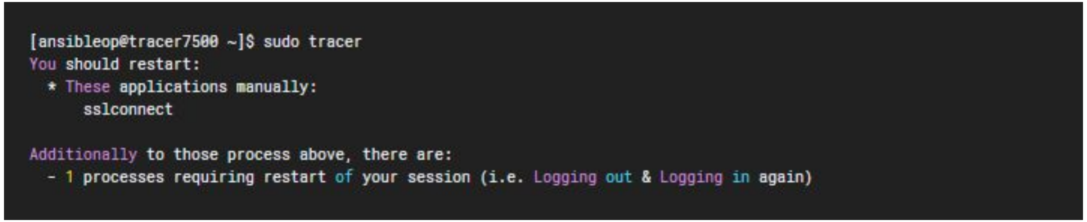
```
[ansibleop@tracer7500 ~]$ grep .so /proc/18624/maps | grep deleted
7f9f5b9bb000-7f9f5bbef000 r-xp 00000000 fd:00 153050                     /usr/lib64/libcrypto.so.1.0.2k;5e325a46 (deleted)
7f9f5bbef000-7f9f5bdef000 ---p 00234000 fd:00 153050                     /usr/lib64/libcrypto.so.1.0.2k;5e325a46 (deleted)
7f9f5bdef000-7f9f5be0b000 r--p 00234000 fd:00 153050                     /usr/lib64/libcrypto.so.1.0.2k;5e325a46 (deleted)
7f9f5be0b000-7f9f5be18000 rw-p 00250000 fd:00 153050                     /usr/lib64/libcrypto.so.1.0.2k;5e325a46 (deleted)
7f9f5be1c000-7f9f5be83000 r-xp 00000000 fd:00 153052                     /usr/lib64/libssl.so.1.0.2k;5e325a46 (deleted)
7f9f5be83000-7f9f5c082000 ---p 00067000 fd:00 153052                     /usr/lib64/libssl.so.1.0.2k;5e325a46 (deleted)
7f9f5c082000-7f9f5c086000 r--p 00066000 fd:00 153052                     /usr/lib64/libssl.so.1.0.2k;5e325a46 (deleted)
7f9f5c086000-7f9f5c08d000 rw-p 0006a000 fd:00 153052                     /usr/lib64/libssl.so.1.0.2k;5e325a46 (deleted)
```

Tracer to the rescue!

- Tracer does the hard work for you.
- Install the *python2-tracer* RPM from the Satellite Tools repo and run tracer.

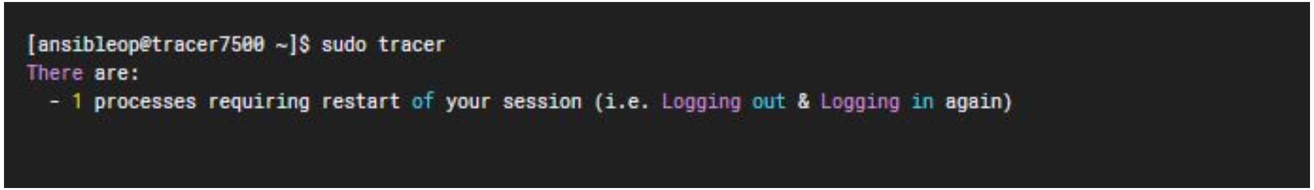


```
[ansibleop@tower tracer]$ cat 1-tracer-cli.yml
---
- name: Install the tracer cli tools
  hosts: tracer7500
  become: true
  tasks:
  - name: Install Tracer cli
    yum:
      name: python2-tracer
      state: latest
...
```



```
[ansibleop@tracer7500 ~]$ sudo tracer
You should restart:
  * These applications manually:
      sslconnect

Additionally to those process above, there are:
  - 1 processes requiring restart of your session (i.e. Logging out & Logging in again)
```

Restart our test program and test again.



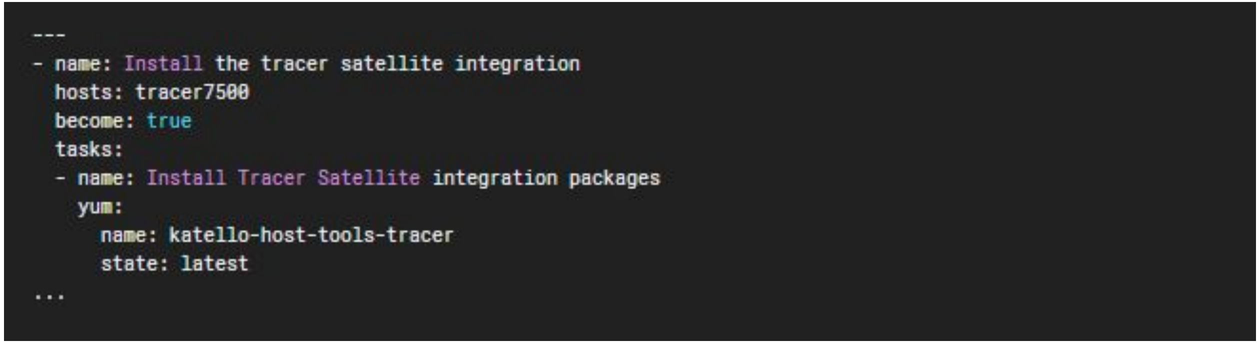
```
[ansibleop@tracer7500 ~]$ sudo tracer
There are:
  - 1 processes requiring restart of your session (i.e. Logging out & Logging in again)
```

- Tracer is examining *all* processes on the system, and not just looking at our test application.

Tracer and Satellite

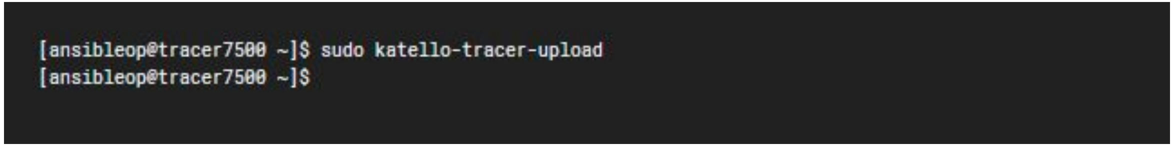
Tracer Integration with Satellite

- Tracer has been Tech Preview since Satellite 6.3
- No changes necessary to the Satellite server. Simply install the *katello-host-tools-tracer* RPM on each host (which can be done during provisioning)
- Tracer reports will automatically be run after using yum for install/update operations
- Can also be run manually using the *katello-tracer-upload* CLI tool
- Here is a playbook that installs the package:



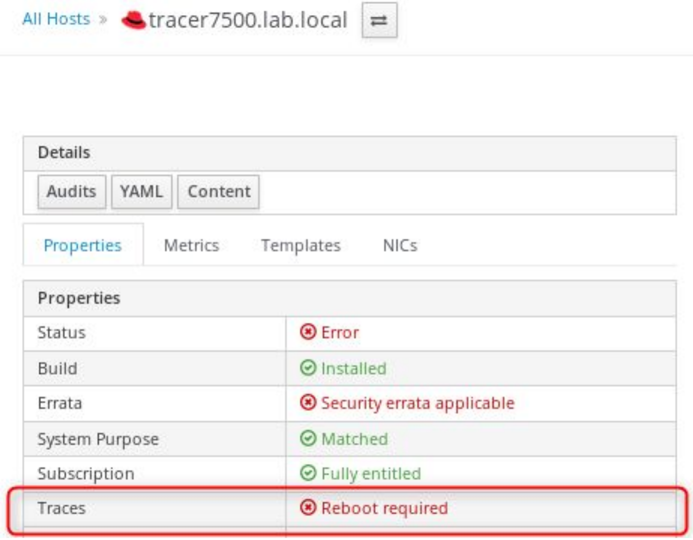
```
---
- name: Install the tracer satellite integration
  hosts: tracer7500
  become: true
  tasks:
  - name: Install Tracer Satellite integration packages
    yum:
      name: katello-host-tools-tracer
      state: latest
...
```

Run the CLI tool and view the results in Satellite



```
[ansibleop@tracer7500 ~]$ sudo katello-tracer-upload
[ansibleop@tracer7500 ~]$
```

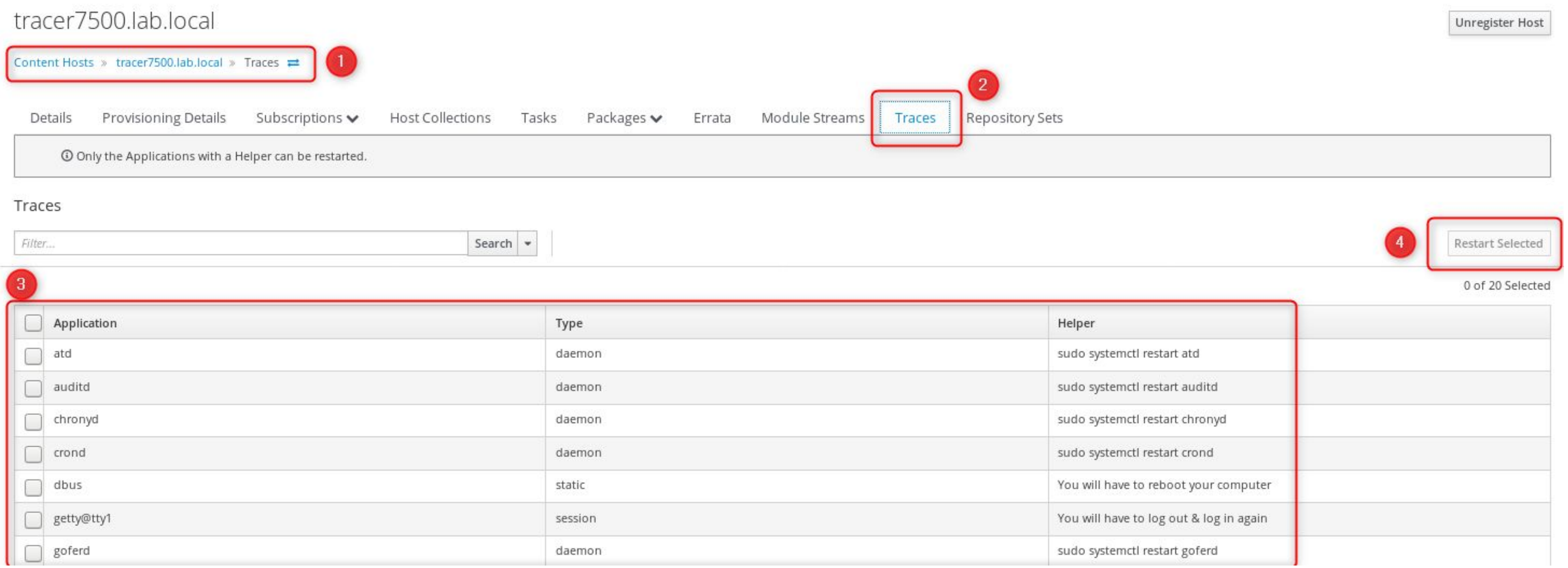
- Look for the Traces property from the Hosts -> All Hosts view of a system



Properties	
Status	☒ Error
Build	✓ Installed
Errata	☒ Security errata applicable
System Purpose	✓ Matched
Subscription	✓ Fully entitled
Traces	☒ Reboot required

Tracer is calling for a restart! Let’s have a look at the details.

Detailed View of Tracer Results from the Content Hosts Menu



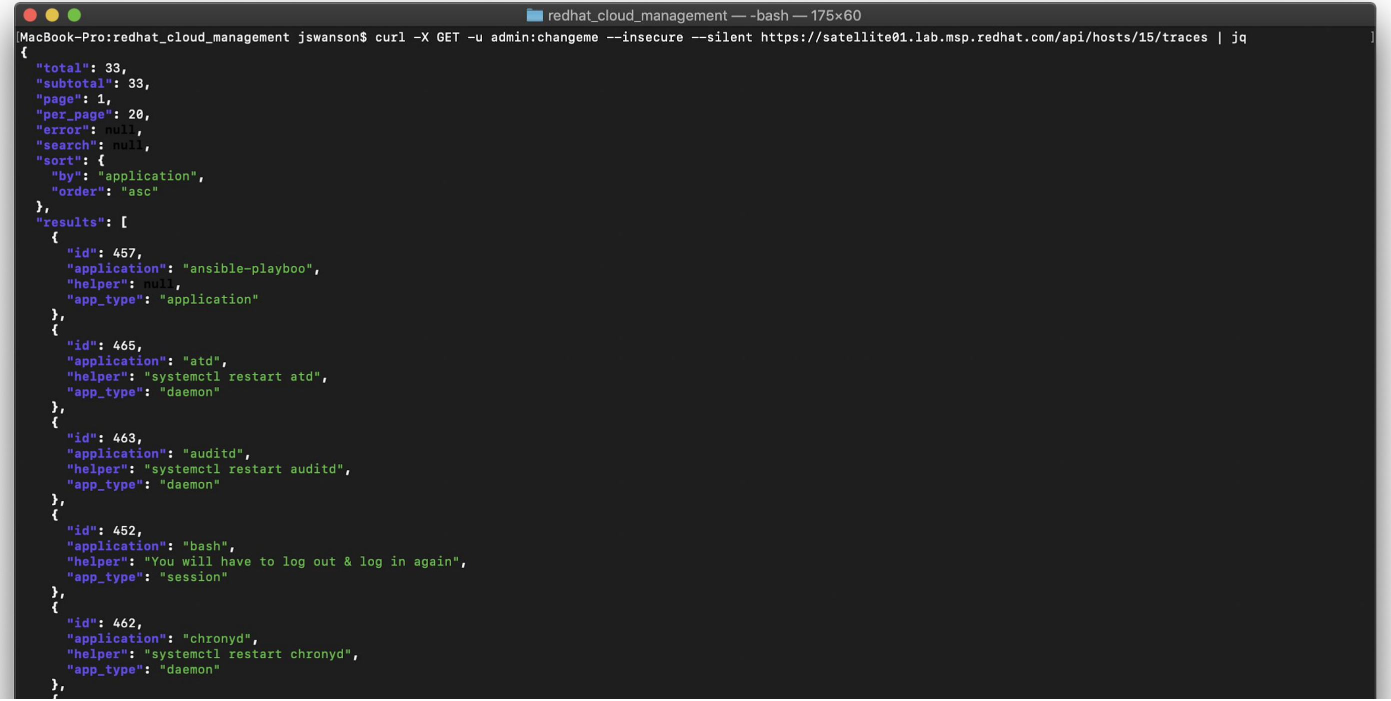
ⓘ Only the Applications with a Helper can be restarted.

Traces

0 of 20 Selected

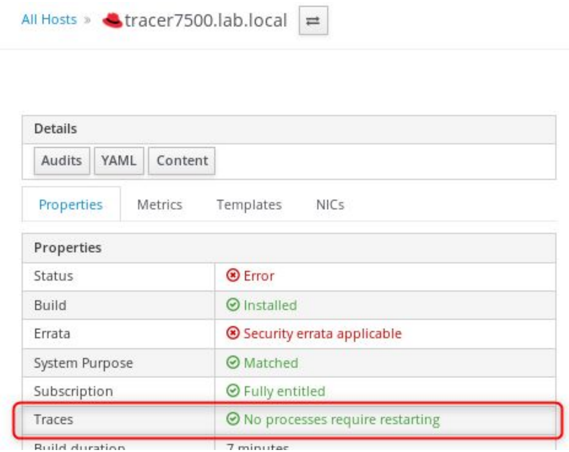
□	Application	Type	Helper
□	atd	daemon	sudo systemctl restart atd
□	auditd	daemon	sudo systemctl restart auditd
□	chronyd	daemon	sudo systemctl restart chronyd
□	crond	daemon	sudo systemctl restart crond
□	dbus	static	You will have to reboot your computer
□	getty@tty1	session	You will have to log out & log in again
□	goferd	daemon	sudo systemctl restart goferd

Tracer Info is Available for the Satellite API



```
[MacBook-Pro:redhat_cloud_management jswanson$ curl -X GET -u admin:changeme --insecure --silent https://satellite01.lab.msp.redhat.com/api/hosts/15/traces | jq
{
  "total": 33,
  "subtotal": 33,
  "page": 1,
  "per_page": 20,
  "error": null,
  "search": null,
  "sort": {
    "by": "application",
    "order": "asc"
  },
  "results": [
    {
      "id": 457,
      "application": "ansible-playboo",
      "helper": null,
      "app_type": "application"
    },
    {
      "id": 465,
      "application": "atd",
      "helper": "systemctl restart atd",
      "app_type": "daemon"
    },
    {
      "id": 463,
      "application": "auditd",
      "helper": "systemctl restart auditd",
      "app_type": "daemon"
    },
    {
      "id": 452,
      "application": "bash",
      "helper": "You will have to log out & log in again",
      "app_type": "session"
    },
    {
      "id": 462,
      "application": "chronyd",
      "helper": "systemctl restart chronyd",
      "app_type": "daemon"
    },
    {
```

Reboot and Review the Traces Status Again



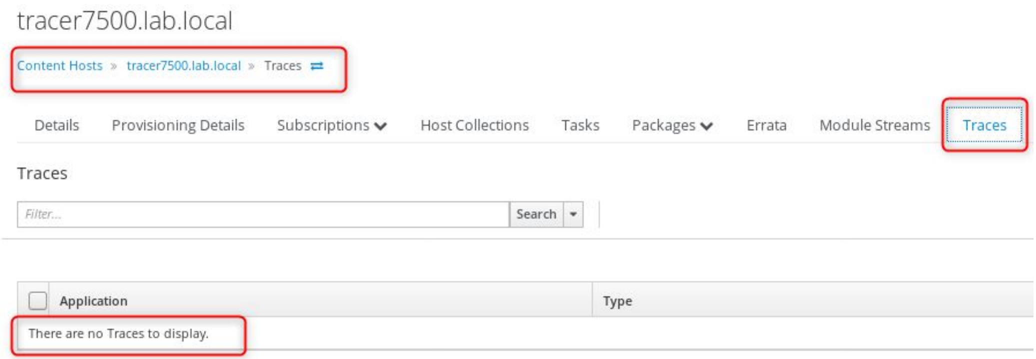
All Hosts » tracer7500.lab.local ⇄

Details

Audits | YAML | Content

Properties | Metrics | Templates | NICs

Properties	
Status	⊗ Error
Build	✓ Installed
Errata	⊗ Security errata applicable
System Purpose	✓ Matched
Subscription	✓ Fully entitled
Traces	✓ No processes require restarting
Build duration	7 minutes



tracer7500.lab.local

Content Hosts » tracer7500.lab.local » Traces ⇄

Details | Provisioning Details | Subscriptions | Host Collections | Tasks | Packages | Errata | Module Streams | Traces

Traces

Filter... | Search

□ Application	Type
There are no Traces to display.	

- After the reboot, we have a clean Tracer report!

Red Hat Insights

Red Hat Insights

Now included with all Red Hat Enterprise Linux subscriptions

Buy

Red Hat
Enterprise Linux

Get

Red Hat
Insights

Red Hat Insights

ansible-galaxy install redhatinsights.insights-client

```
roles/requirements.yml
---
- src: redhatinsights.insights-client

rhel_standards.insights.yml
---
- name: deploy redhat insights
  hosts:
    - all
  roles:
    - redhatinsights.insights-client
```

cloud management services for Red Hat Enterprise Linux

Demo: Deploying Red Hat Insights

Insights Inventory

Click Here!

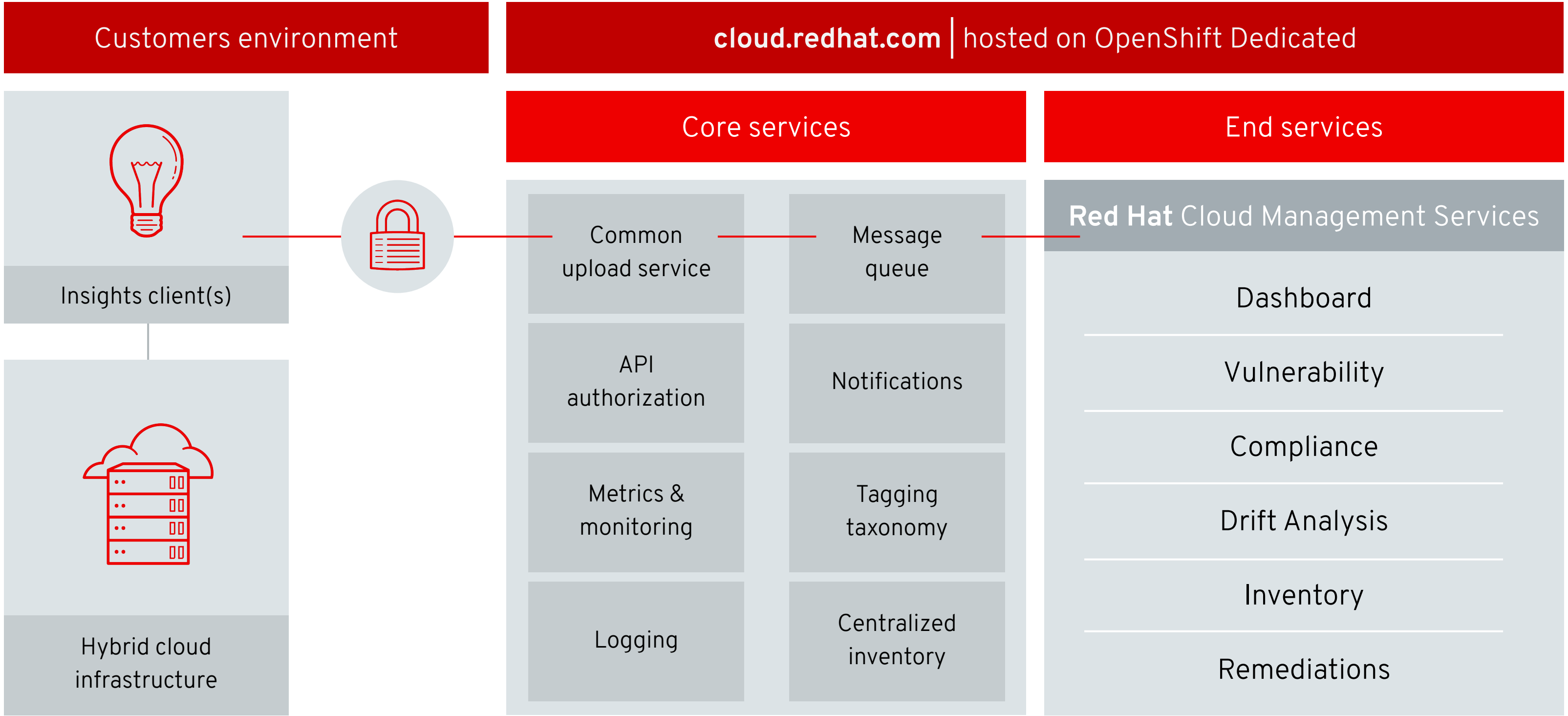
cloud management services for Red Hat Enterprise Linux

Red Hat Smart/Cloud Management Overview

Cloud Management Services for RHEL

We are here.

Cloud Management Services for RHEL



Customers environment

Insights client(s)

Hybrid cloud infrastructure

cloud.redhat.com | hosted on OpenShift Dedicated

Core services

Common upload service

Message queue

API authorization

Notifications

Metrics & monitoring

Tagging taxonomy

Logging

Centralized inventory

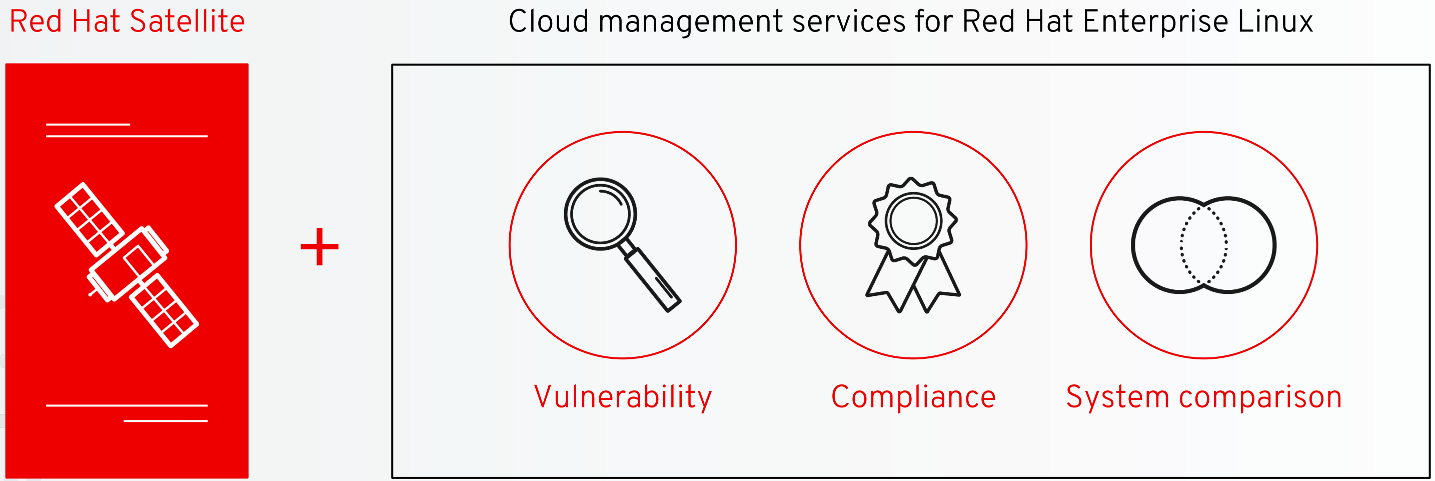
End services

Red Hat Cloud Management Services

- Dashboard
- Vulnerability
- Compliance
- Drift Analysis
- Inventory
- Remediations

Red Hat

Red Hat Smart Management



Red Hat Satellite

+

Cloud management services for Red Hat Enterprise Linux

Vulnerability

Compliance

System comparison

Management Flexibility

Offering Red Hat Management on-premises or in the cloud

Red Hat Satellite

Requirements for resource set up and configuration

Addresses on-prem or disconnected environment

Limited to viewing hosts registered to the individual Satellite servers

Use cases:

Content management, patching, configuration, subscription management, provisioning

Cloud Management Services

No requirements for resource set up and maintenance

Adopt new features faster with a software-as-a-service preference

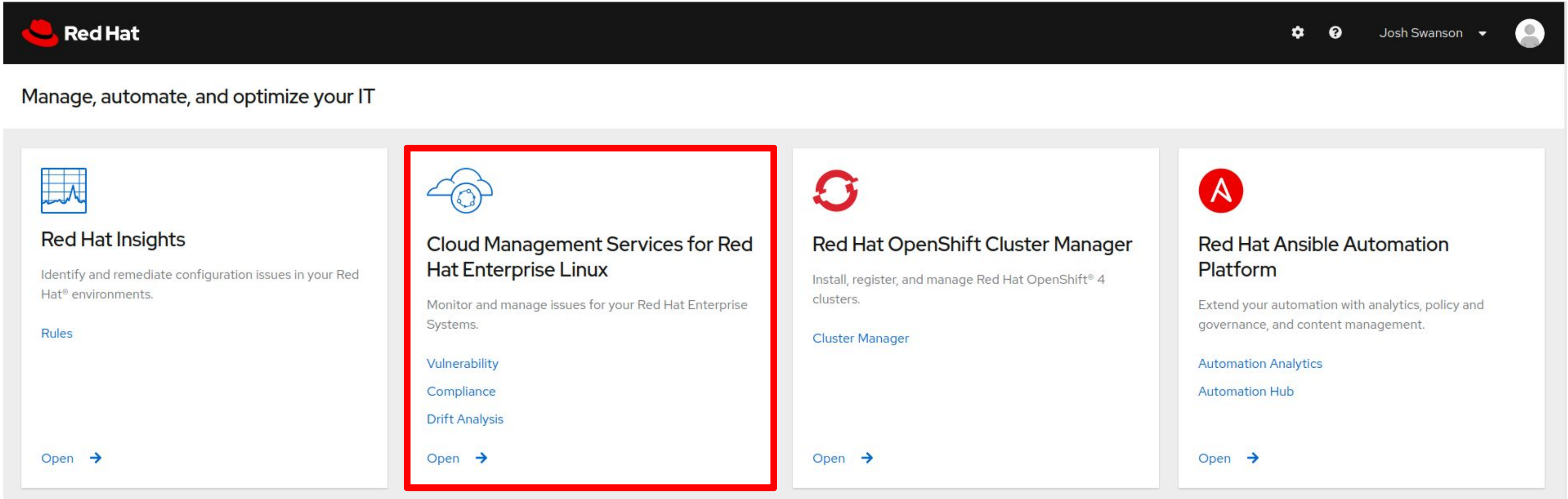
Single view of all hosts across your RH infrastructure

Use cases:

Vulnerability, Compliance, System Comparison

Smart Management Packaging gives access to both Satellite AND cloud management services

cloud.redhat.com



Red Hat

Josh Swanson

Manage, automate, and optimize your IT

Red Hat Insights

Identify and remediate configuration issues in your Red Hat® environments.

Rules

Open →

Cloud Management Services for Red Hat Enterprise Linux

Monitor and manage issues for your Red Hat Enterprise Systems.

Vulnerability

Compliance

Drift Analysis

Open →

Red Hat OpenShift Cluster Manager

Install, register, and manage Red Hat OpenShift® 4 clusters.

Cluster Manager

Open →

Red Hat Ansible Automation Platform

Extend your automation with analytics, policy and governance, and content management.

Automation Analytics

Automation Hub

Open →

cloud management services for Red Hat Enterprise Linux

Vulnerability

Vulnerability

Remediate all Common Vulnerabilities and Exposures (CVEs)

Vulnerability offers

Assess and monitor the risk of vulnerabilities that impact Red Hat products with operational ease

Remediate known Common Vulnerabilities and Exposures (CVEs)

Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

Why CVE, why not Errata?

CVE

Security focused

Product agnostic

Limited to one vulnerability/exposure per CVE (May cover multiple versions of a piece of software)

Stakeholders:
Security teams, researchers, the public

Errata

Bugfix, enhancement, and security

Specific to Red Hat products

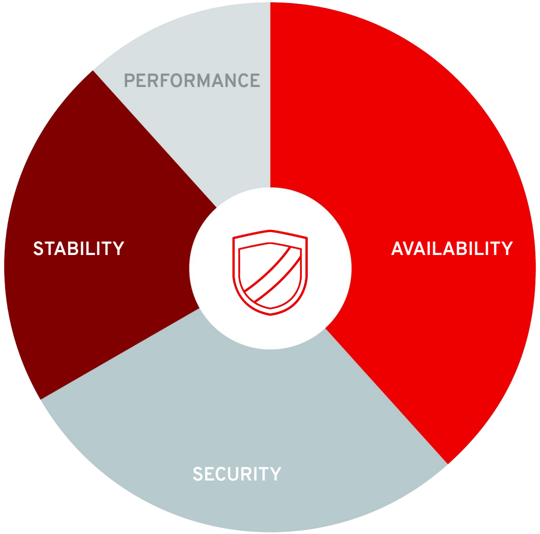
May resolve multiple CVEs/bugs/RFEs within one errata.

May contain multiple packages

Stakeholders:
Content managers for Red Hat products

More than just security

Red Hat Insights has more than 1,000+ rules—here is how they stack up across categories

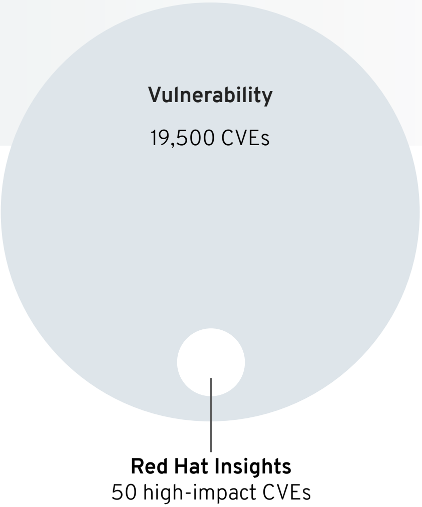


- ● **Availability** 38.6%
- ● **Security** 28.1%
- ● **Stability** 21.7%
- ● **Performance** 11.6%

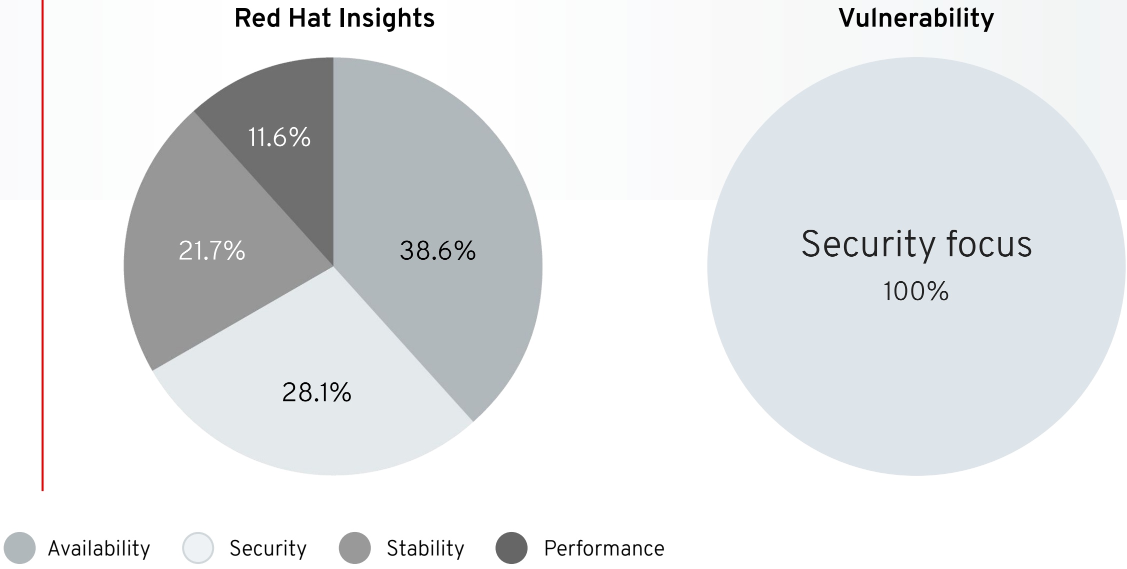
Insights does this already, right?

Vulnerability is security-focused–all CVEs with errata

CVEs covered



Areas / Rules covered



Vulnerability - Use Cases

Summit 2019

- View and triage vulnerabilities by:
  - CVEs
  - ystems
- Triaging vulnerabilities via
  - CVSS base score
  - Impact
  - Publish date
- Ansible Automation
- Reporting
  - JSON
  - CSV
- Set Status for CVE+System

Oct 2019

- Improved UI navigation
- CVSS v3 metrics on details page
- Customization: Business Risk
- Set Status for a CVE as a whole
- Better triaging of vulnerabilities
  - Excluded system from Vulnerability Analysis
  - Business risk
  - Status

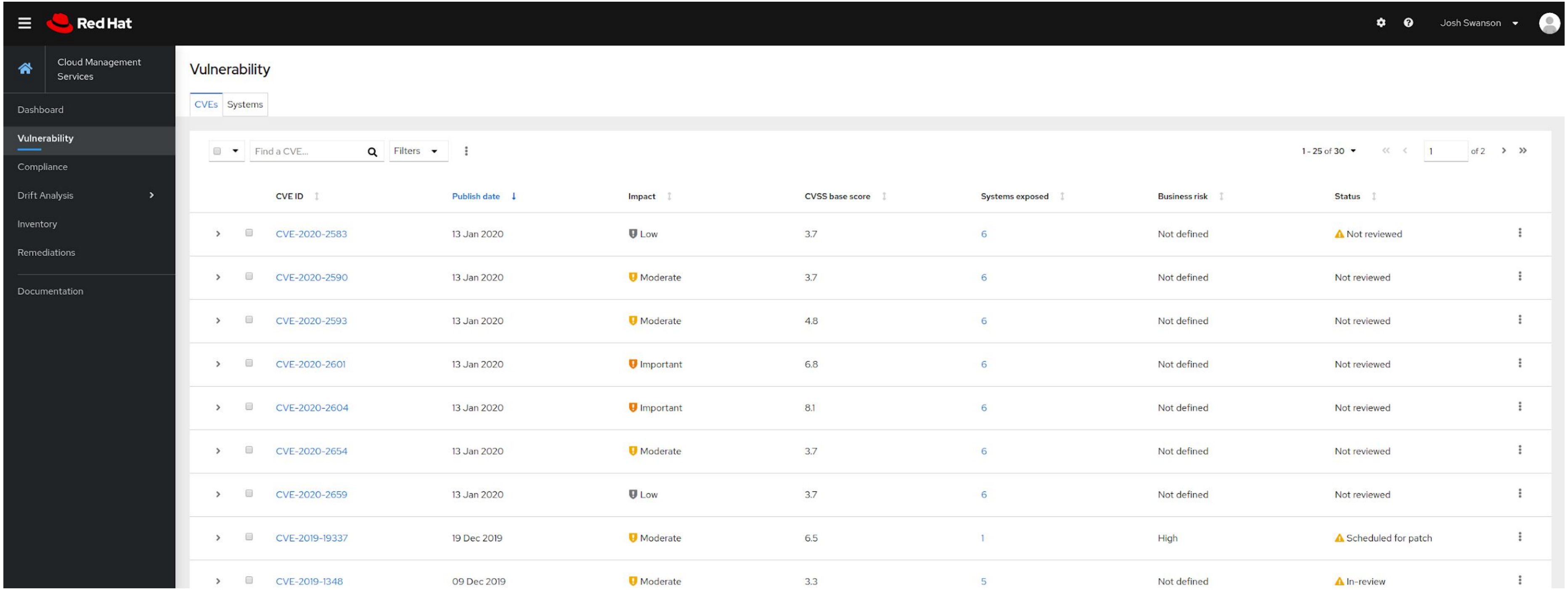
Backlog

- Search by Host Name
- Tagging/Tag Filtering*
- Integration to status.redhat.com*
- Well-documented APIs
- Executive Report (PDF)
- Alerting & Notification*
- RBAC Enabled (light)*
- RBAC Enabled (heavy)*
- Reporting
  - CVE w/out Errata Report
  - Vulnerability Risk Report

* Dependency on the Platform

Vulnerability

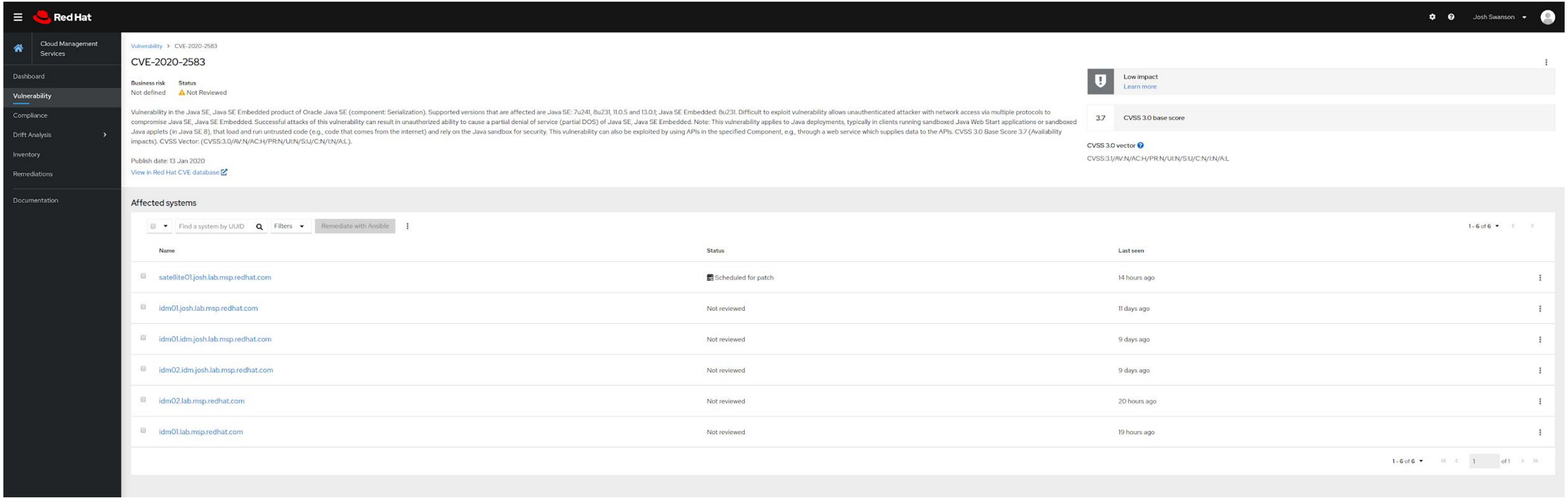
CVE Listing



CVE ID	Publish date	Impact	CVSS base score	Systems exposed	Business risk	Status
CVE-2020-2583	13 Jan 2020	Low	3.7	6	Not defined	⚠ Not reviewed
CVE-2020-2590	13 Jan 2020	Moderate	3.7	6	Not defined	Not reviewed
CVE-2020-2593	13 Jan 2020	Moderate	4.8	6	Not defined	Not reviewed
CVE-2020-2601	13 Jan 2020	Important	6.8	6	Not defined	Not reviewed
CVE-2020-2604	13 Jan 2020	Important	8.1	6	Not defined	Not reviewed
CVE-2020-2654	13 Jan 2020	Moderate	3.7	6	Not defined	Not reviewed
CVE-2020-2659	13 Jan 2020	Low	3.7	6	Not defined	Not reviewed
CVE-2019-19337	19 Dec 2019	Moderate	6.5	1	High	⚠ Scheduled for patch
CVE-2019-1348	09 Dec 2019	Moderate	3.3	5	Not defined	⚠ In-review

Vulnerability

CVE Details



CVE-2020-2583

Business risk: Not defined
Status: ⚠ Not Reviewed

Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).

Publish date: 13 Jan 2020
View in Red Hat CVE database

Low impact
Learn more

3.7 CVSS 3.0 base score

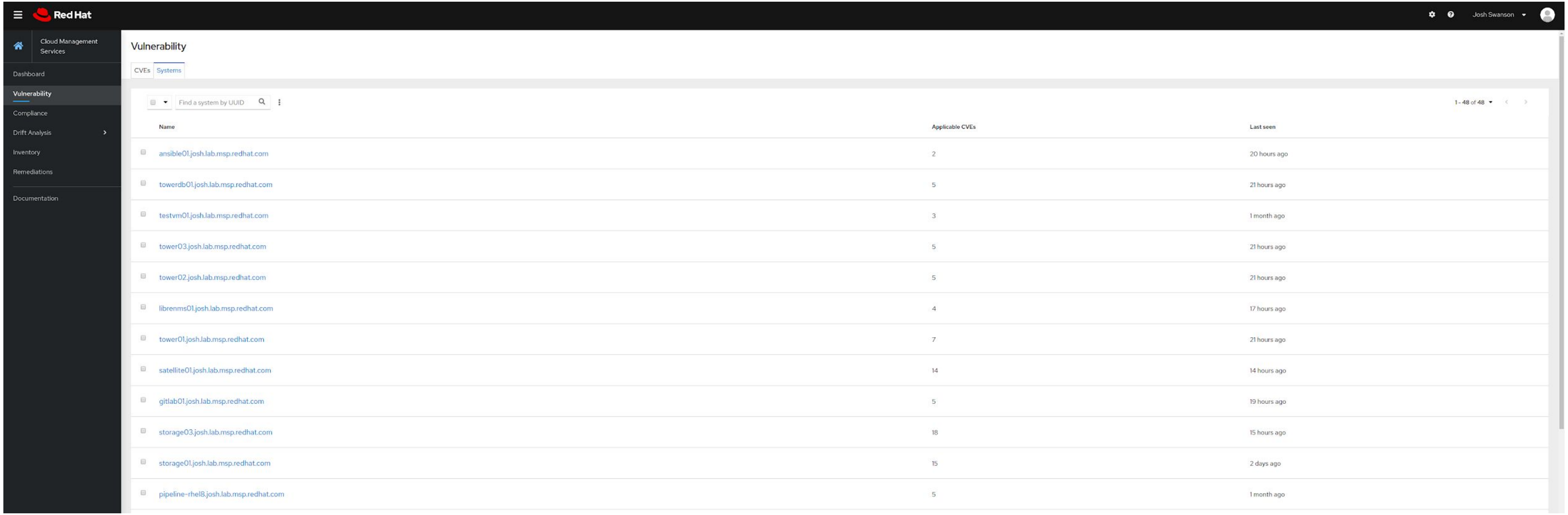
CVSS 3.0 vector
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

Affected systems

	Name	Status	Last seen
□	satellite01.josh.lab.msp.redhat.com	Scheduled for patch	14 hours ago
□	idm01.josh.lab.msp.redhat.com	Not reviewed	11 days ago
□	idm01.idm.josh.lab.msp.redhat.com	Not reviewed	9 days ago
□	idm02.idm.josh.lab.msp.redhat.com	Not reviewed	9 days ago
□	idm02.lab.msp.redhat.com	Not reviewed	20 hours ago
□	idm01.lab.msp.redhat.com	Not reviewed	19 hours ago

Vulnerability

Systems overview

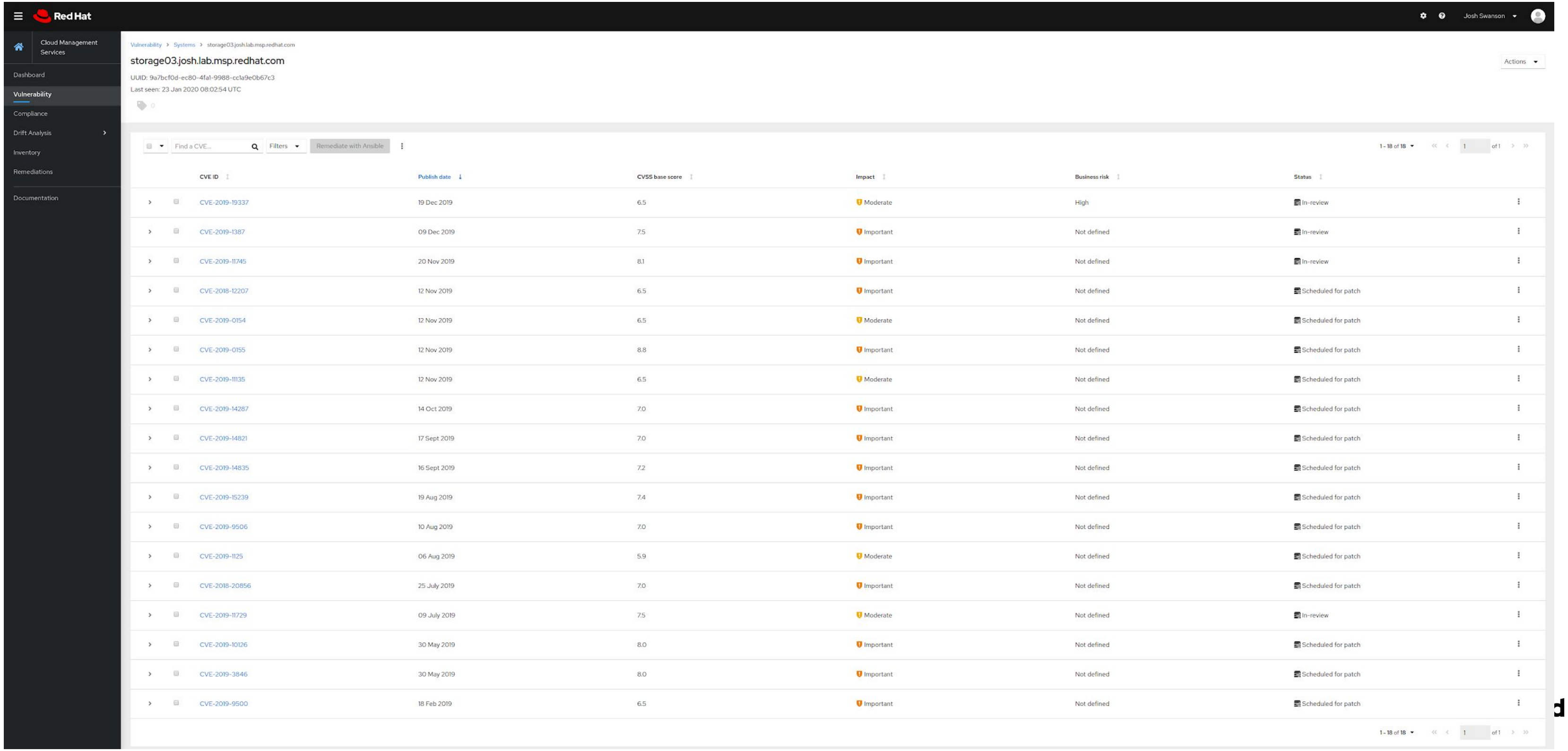


Vulnerability

Name	Applicable CVEs	Last seen
ansible01.josh.lab.msp.redhat.com	2	20 hours ago
towerdb01.josh.lab.msp.redhat.com	5	21 hours ago
testvm01.josh.lab.msp.redhat.com	3	1 month ago
tower03.josh.lab.msp.redhat.com	5	21 hours ago
tower02.josh.lab.msp.redhat.com	5	21 hours ago
librenms01.josh.lab.msp.redhat.com	4	17 hours ago
tower01.josh.lab.msp.redhat.com	7	21 hours ago
satellite01.josh.lab.msp.redhat.com	14	14 hours ago
gitlab01.josh.lab.msp.redhat.com	5	19 hours ago
storage03.josh.lab.msp.redhat.com	18	15 hours ago
storage01.josh.lab.msp.redhat.com	15	2 days ago
pipeline-rhel8.josh.lab.msp.redhat.com	5	1 month ago

Vulnerability

Vulnerabilities for a Host



storage03.josh.lab.msp.redhat.com

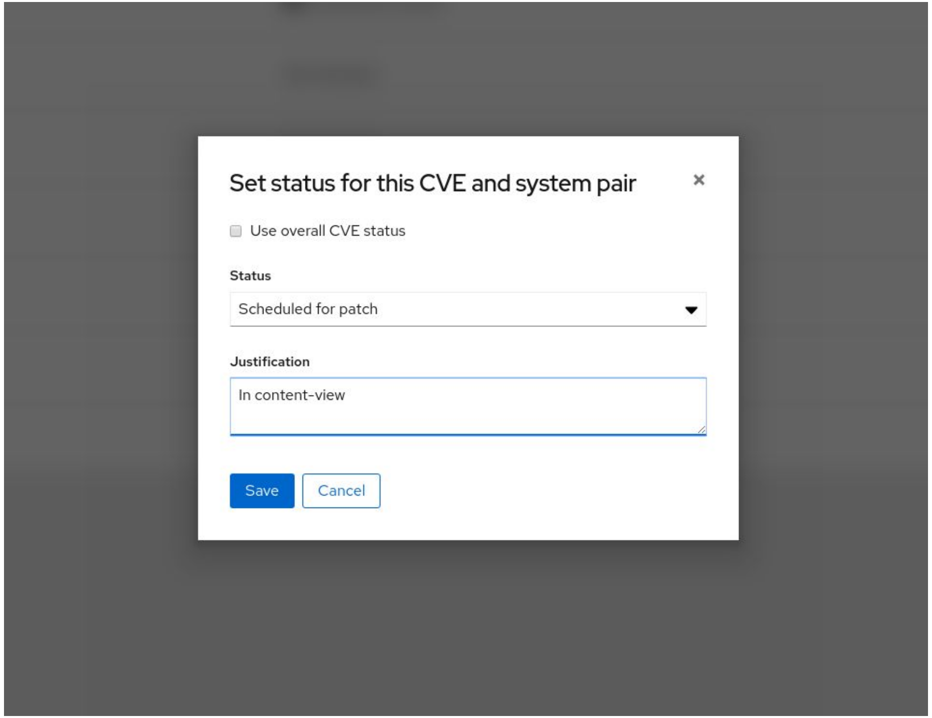
UUID: 9a7bcf0d-ec80-4fa1-9988-cc1a9e0b67c3

Last seen: 23 Jan 2020 08:02:54 UTC

CVE ID	Publish date	CVSS base score	Impact	Business risk	Status
CVE-2019-19337	19 Dec 2019	6.5	Moderate	High	In-review
CVE-2019-1387	09 Dec 2019	7.5	Important	Not defined	In-review
CVE-2019-11745	20 Nov 2019	8.1	Important	Not defined	In-review
CVE-2018-12207	12 Nov 2019	6.5	Important	Not defined	Scheduled for patch
CVE-2019-0154	12 Nov 2019	6.5	Moderate	Not defined	Scheduled for patch
CVE-2019-0155	12 Nov 2019	8.8	Important	Not defined	Scheduled for patch
CVE-2019-11135	12 Nov 2019	6.5	Moderate	Not defined	Scheduled for patch
CVE-2019-14287	14 Oct 2019	7.0	Important	Not defined	Scheduled for patch
CVE-2019-14821	17 Sept 2019	7.0	Important	Not defined	Scheduled for patch
CVE-2019-14835	16 Sept 2019	7.2	Important	Not defined	Scheduled for patch
CVE-2019-15239	19 Aug 2019	7.4	Important	Not defined	Scheduled for patch
CVE-2019-9506	10 Aug 2019	7.0	Important	Not defined	Scheduled for patch
CVE-2019-1125	06 Aug 2019	5.9	Moderate	Not defined	Scheduled for patch
CVE-2018-20856	25 July 2019	7.0	Important	Not defined	Scheduled for patch
CVE-2019-11729	09 July 2019	7.5	Moderate	Not defined	In-review
CVE-2019-10126	30 May 2019	8.0	Important	Not defined	Scheduled for patch
CVE-2019-3846	30 May 2019	8.0	Important	Not defined	Scheduled for patch
CVE-2019-9500	18 Feb 2019	6.5	Important	Not defined	Scheduled for patch

Vulnerability

Status can be set for all hosts vulnerable to a CVE or on a CVE/system pair basis



Set status for this CVE and system pair

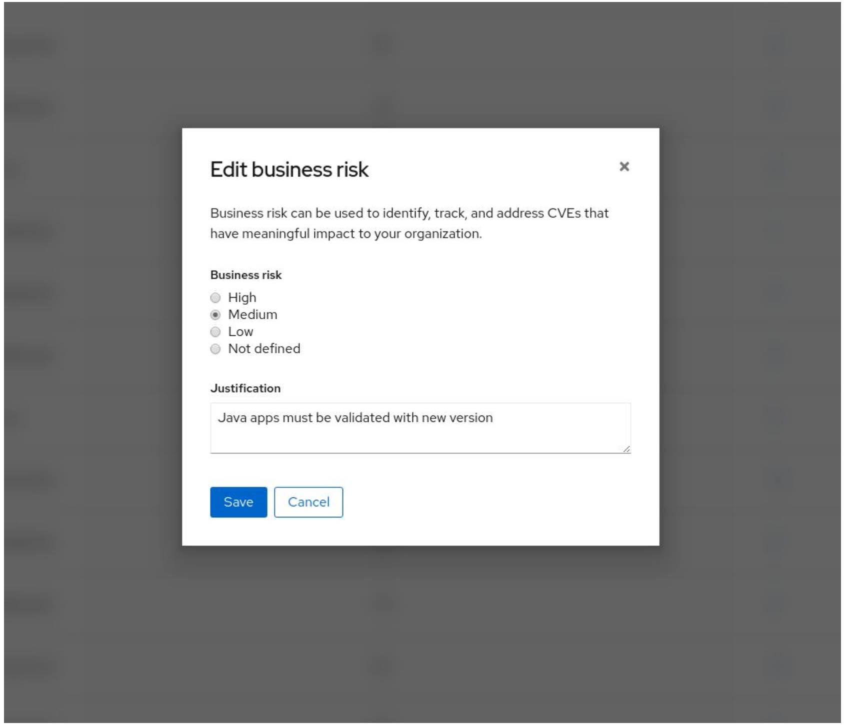
□ Use overall CVE status

Status: Scheduled for patch

Justification: In content-view

Vulnerability

Business risk to better communicate impact/importance



Edit business risk

Business risk can be used to identify, track, and address CVEs that have meaningful impact to your organization.

Business risk

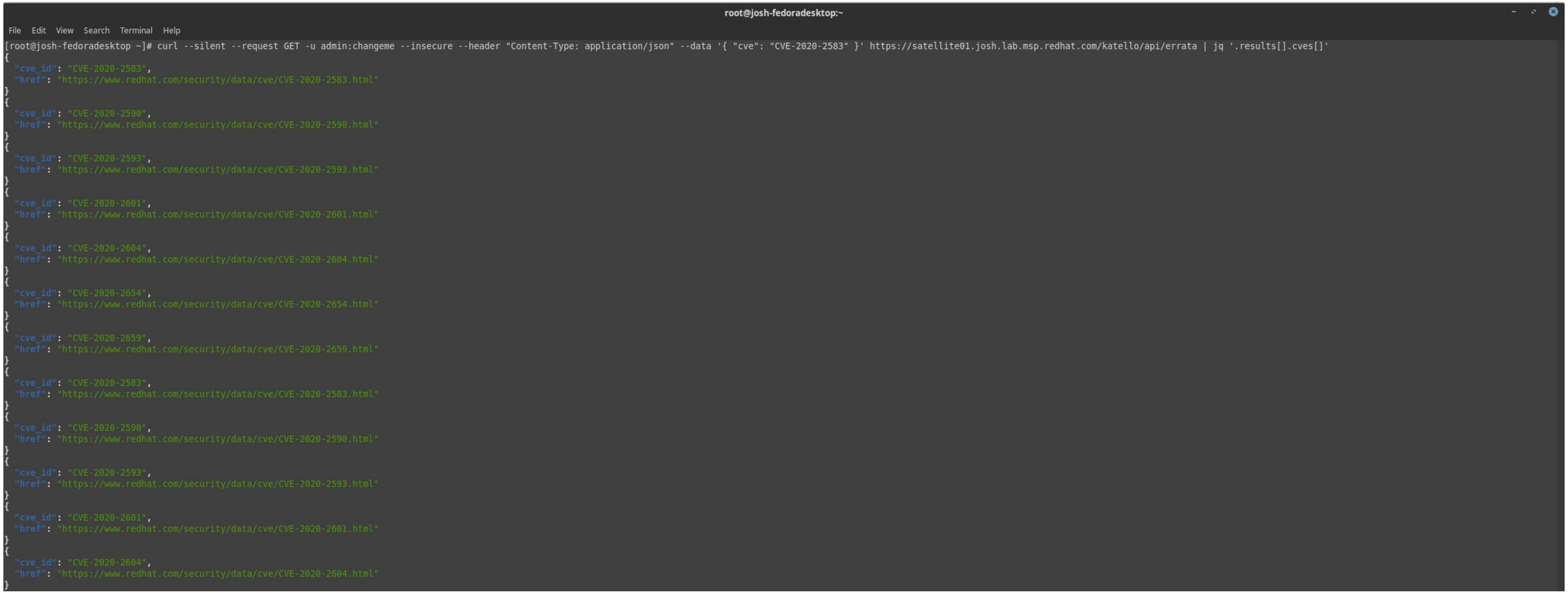
○ High
● Medium
○ Low
○ Not defined

Justification

Java apps must be validated with new version

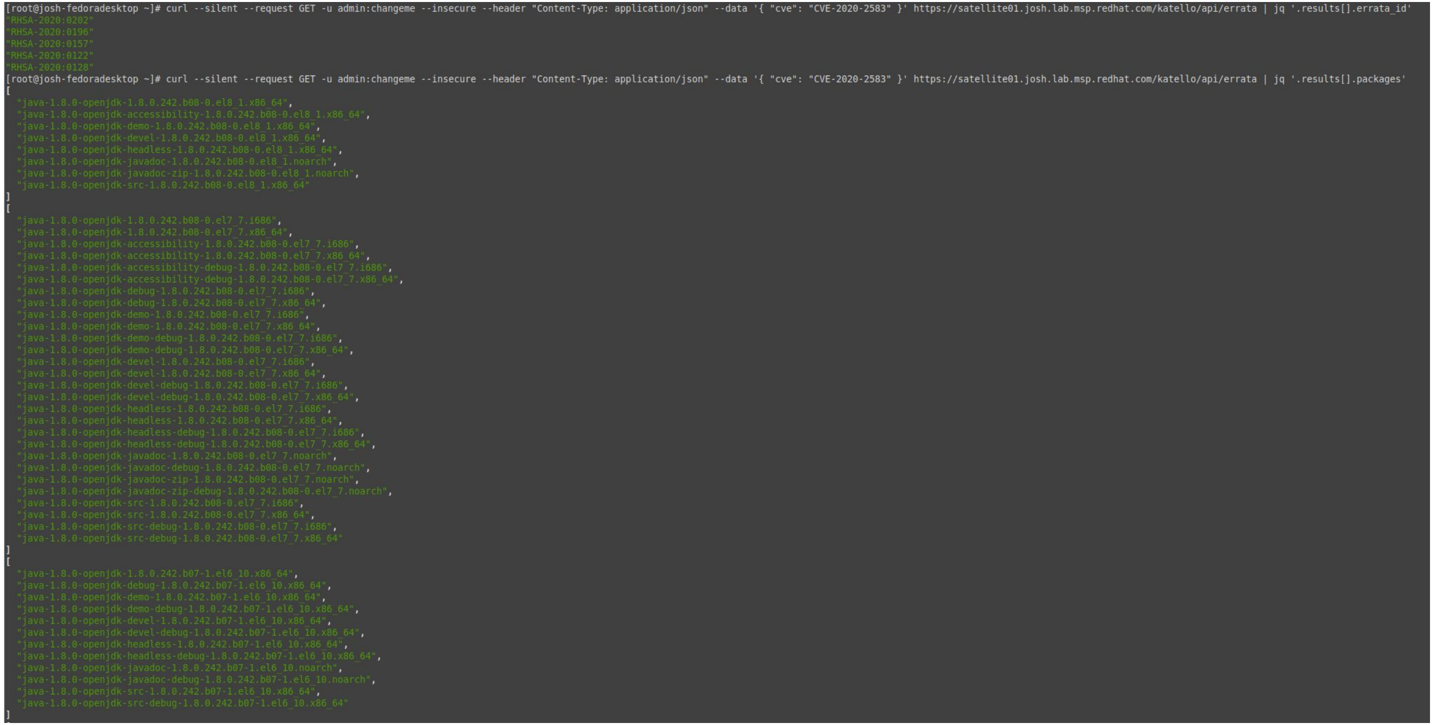
What About Satellite?

Satellite knows about CVEs



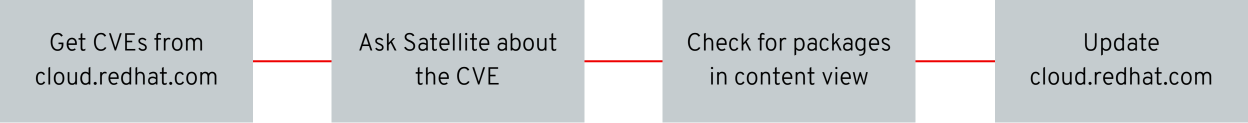
```
[root@josh-fedoradesktop ~]# curl --silent --request GET -u admin:changeme --insecure --header "Content-Type: application/json" --data '{ "cve": "CVE-2020-2583" }' https://satellite01.josh.lab.msp.redhat.com/katello/api/errata | jq '.results[].cves[]'
{
  "cve_id": "CVE-2020-2583",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2583.html"
}
{
  "cve_id": "CVE-2020-2590",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2590.html"
}
{
  "cve_id": "CVE-2020-2593",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2593.html"
}
{
  "cve_id": "CVE-2020-2601",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2601.html"
}
{
  "cve_id": "CVE-2020-2604",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2604.html"
}
{
  "cve_id": "CVE-2020-2654",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2654.html"
}
{
  "cve_id": "CVE-2020-2659",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2659.html"
}
{
  "cve_id": "CVE-2020-2583",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2583.html"
}
{
  "cve_id": "CVE-2020-2590",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2590.html"
}
{
  "cve_id": "CVE-2020-2593",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2593.html"
}
{
  "cve_id": "CVE-2020-2601",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2601.html"
}
{
  "cve_id": "CVE-2020-2604",
  "href": "https://www.redhat.com/security/data/cve/CVE-2020-2604.html"
}
```

Satellite Knows CVEs



```
[root@josh-fedoradesktop ~]# curl --silent --request GET -u admin:changeme --insecure --header "Content-Type: application/json" --data '{ "cve": "CVE-2020-2583" }' https://satellite01.josh.lab.msp.redhat.com/katello/api/errata | jq '.results[].errata_id'
"RHSA-2020:0202"
"RHSA-2020:0196"
"RHSA-2020:0157"
"RHSA-2020:0122"
"RHSA-2020:0128"
[root@josh-fedoradesktop ~]# curl --silent --request GET -u admin:changeme --insecure --header "Content-Type: application/json" --data '{ "cve": "CVE-2020-2583" }' https://satellite01.josh.lab.msp.redhat.com/katello/api/errata | jq '.results[].packages'
[
  "java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64",
  "java-1.8.0-openjdk-accessibility-1.8.0.242.b08-0.el8_1.x86_64",
  "java-1.8.0-openjdk-demo-1.8.0.242.b08-0.el8_1.x86_64",
  "java-1.8.0-openjdk-devel-1.8.0.242.b08-0.el8_1.x86_64",
  "java-1.8.0-openjdk-headless-1.8.0.242.b08-0.el8_1.x86_64",
  "java-1.8.0-openjdk-javadoc-1.8.0.242.b08-0.el8_1.noarch",
  "java-1.8.0-openjdk-javadoc-zip-1.8.0.242.b08-0.el8_1.noarch",
  "java-1.8.0-openjdk-src-1.8.0.242.b08-0.el8_1.x86_64"
]
[

  "java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-accessibility-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-accessibility-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-accessibility-debug-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-accessibility-debug-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-debug-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-debug-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-demo-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-demo-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-demo-debug-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-demo-debug-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-devel-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-devel-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-devel-debug-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-devel-debug-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-headless-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-headless-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-headless-debug-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-headless-debug-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-javadoc-1.8.0.242.b08-0.el7_7.noarch",
  "java-1.8.0-openjdk-javadoc-debug-1.8.0.242.b08-0.el7_7.noarch",
  "java-1.8.0-openjdk-javadoc-zip-1.8.0.242.b08-0.el7_7.noarch",
  "java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.242.b08-0.el7_7.noarch",
  "java-1.8.0-openjdk-src-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-src-1.8.0.242.b08-0.el7_7.x86_64",
  "java-1.8.0-openjdk-src-debug-1.8.0.242.b08-0.el7_7.i686",
  "java-1.8.0-openjdk-src-debug-1.8.0.242.b08-0.el7_7.x86_64"
]
[

  "java-1.8.0-openjdk-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-debug-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-demo-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-demo-debug-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-devel-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-devel-debug-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-headless-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-headless-debug-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-javadoc-1.8.0.242.b07-1.el6_10.noarch",
  "java-1.8.0-openjdk-javadoc-debug-1.8.0.242.b07-1.el6_10.noarch",
  "java-1.8.0-openjdk-src-1.8.0.242.b07-1.el6_10.x86_64",
  "java-1.8.0-openjdk-src-debug-1.8.0.242.b07-1.el6_10.x86_64"
]
```

Demo: Aligning Satellite and Cloud Management



Get CVEs from cloud.redhat.com

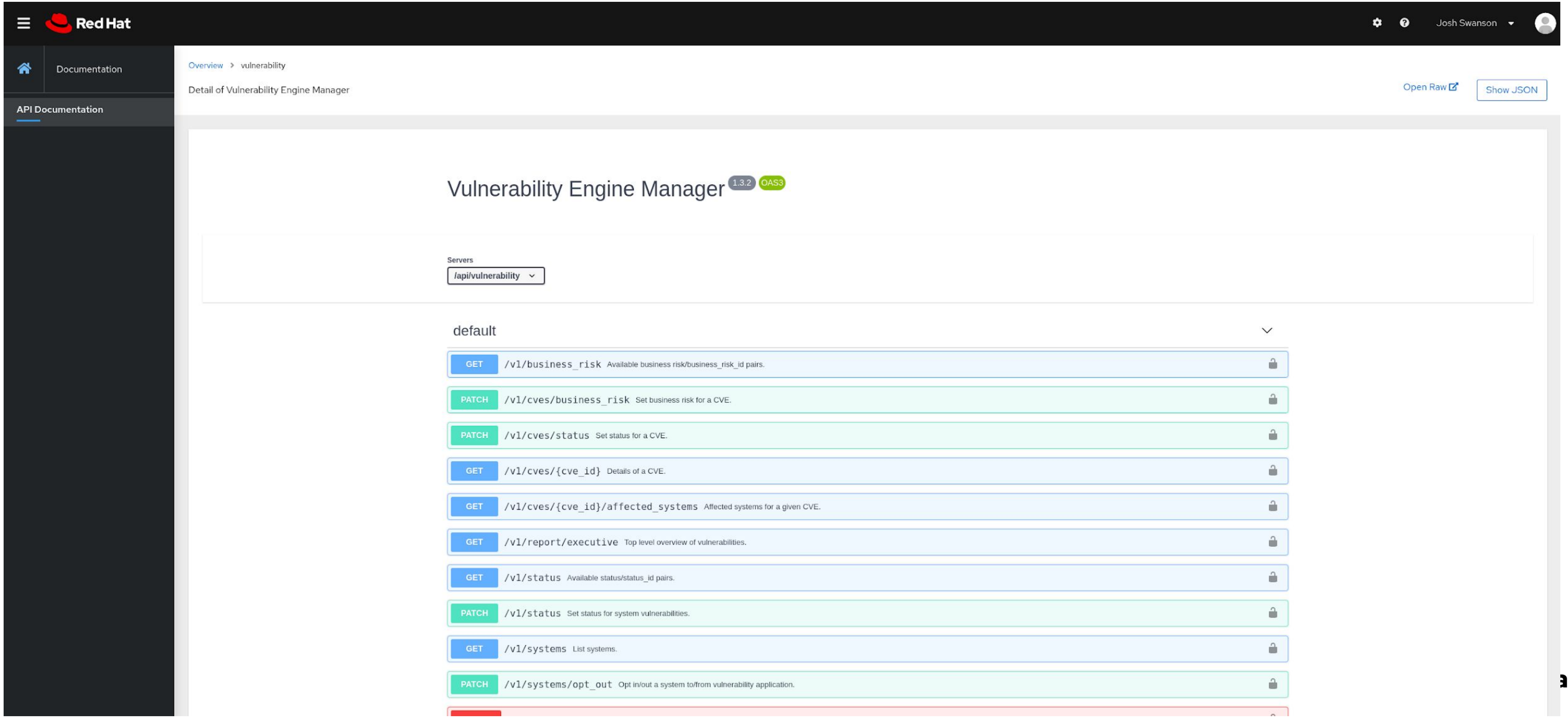
Ask Satellite about the CVE

Check for packages in content view

Update cloud.redhat.com

Cloud Management API

https://cloud.redhat.com/docs/api/vulnerability



Detail of Vulnerability Engine Manager

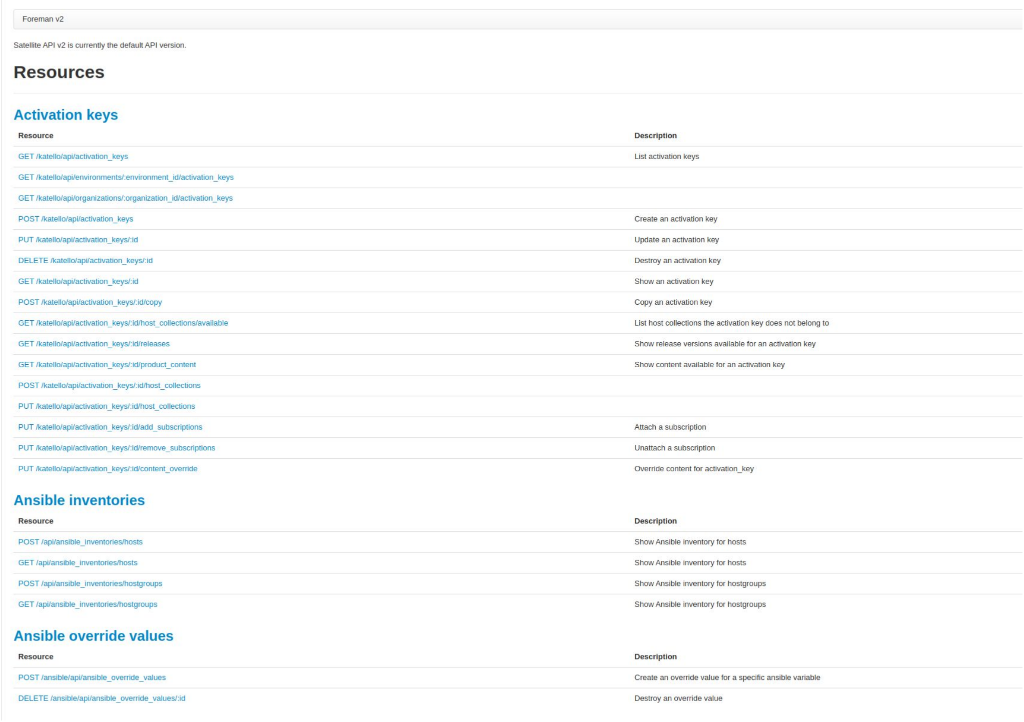
Vulnerability Engine Manager

default

- GET `/v1/business_risk` Available business risk/business_risk_id pairs.
- PATCH `/v1/cves/business_risk` Set business risk for a CVE.
- PATCH `/v1/cves/status` Set status for a CVE.
- GET `/v1/cves/{cve_id}` Details of a CVE.
- GET `/v1/cves/{cve_id}/affected_systems` Affected systems for a given CVE.
- GET `/v1/report/executive` Top level overview of vulnerabilities.
- GET `/v1/status` Available status/status_id pairs.
- PATCH `/v1/status` Set status for system vulnerabilities.
- GET `/v1/systems` List systems.
- PATCH `/v1/systems/opt_out` Opt in/out a system to/from vulnerability application.

Satellite API

https://satellite.example.com/apidoc/v2.html



Foreman v2

Satellite API v2 is currently the default API version.

Resources

Activation keys

Resource	Description
GET /katello/api/activation_keys	List activation keys
GET /katello/api/environments/:environment_id/activation_keys	
GET /katello/api/organizations/:organization_id/activation_keys	
POST /katello/api/activation_keys	Create an activation key
PUT /katello/api/activation_keys/:id	Update an activation key
DELETE /katello/api/activation_keys/:id	Destroy an activation key
GET /katello/api/activation_keys/:id	Show an activation key
POST /katello/api/activation_keys/:id/copy	Copy an activation key
GET /katello/api/activation_keys/:id/host_collections/available	List host collections the activation key does not belong to
GET /katello/api/activation_keys/:id/releases	Show release versions available for an activation key
GET /katello/api/activation_keys/:id/product_content	Show content available for an activation key
POST /katello/api/activation_keys/:id/host_collections	
PUT /katello/api/activation_keys/:id/host_collections	
PUT /katello/api/activation_keys/:id/add_subscriptions	Attach a subscription
PUT /katello/api/activation_keys/:id/remove_subscriptions	Unattach a subscription
PUT /katello/api/activation_keys/:id/content_override	Override content for activation_key

Ansible inventories

Resource	Description
POST /api/ansible_inventories/hosts	Show Ansible inventory for hosts
GET /api/ansible_inventories/hosts	Show Ansible inventory for hosts
POST /api/ansible_inventories/hostgroups	Show Ansible inventory for hostgroups
GET /api/ansible_inventories/hostgroups	Show Ansible inventory for hostgroups

Ansible override values

Resource	Description
POST /ansible/api/ansible_override_values	Create an override value for a specific ansible variable
DELETE /ansible/api/ansible_override_values/:id	Destroy an override value

Demo

Please please please work.

cloud management services for Red Hat Enterprise Linux

Compliance

Compliance

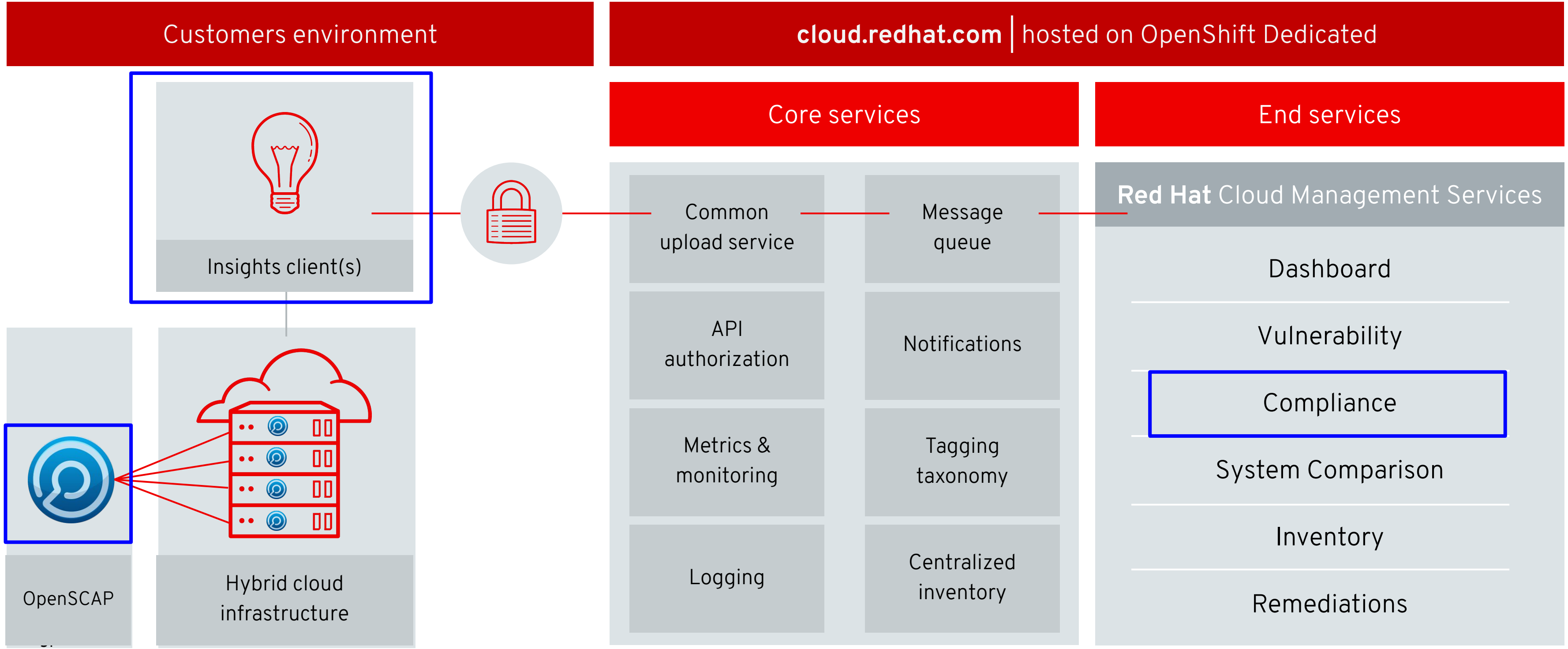
Built on OpenSCAP reporting

Compliance offers

Assess and monitor the degree/level of compliance to a policy for Red Hat products with operational ease

Remediate known issues of non-compliance in the Red Hat environment via Ansible playbooks based on business risk & relevance

Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed



Customers environment

Insights client(s)

OpenSCAP

Hybrid cloud infrastructure

cloud.redhat.com | hosted on OpenShift Dedicated

Core services

Common upload service

Message queue

API authorization

Notifications

Metrics & monitoring

Tagging taxonomy

Logging

Centralized inventory

End services

Red Hat Cloud Management Services

Dashboard

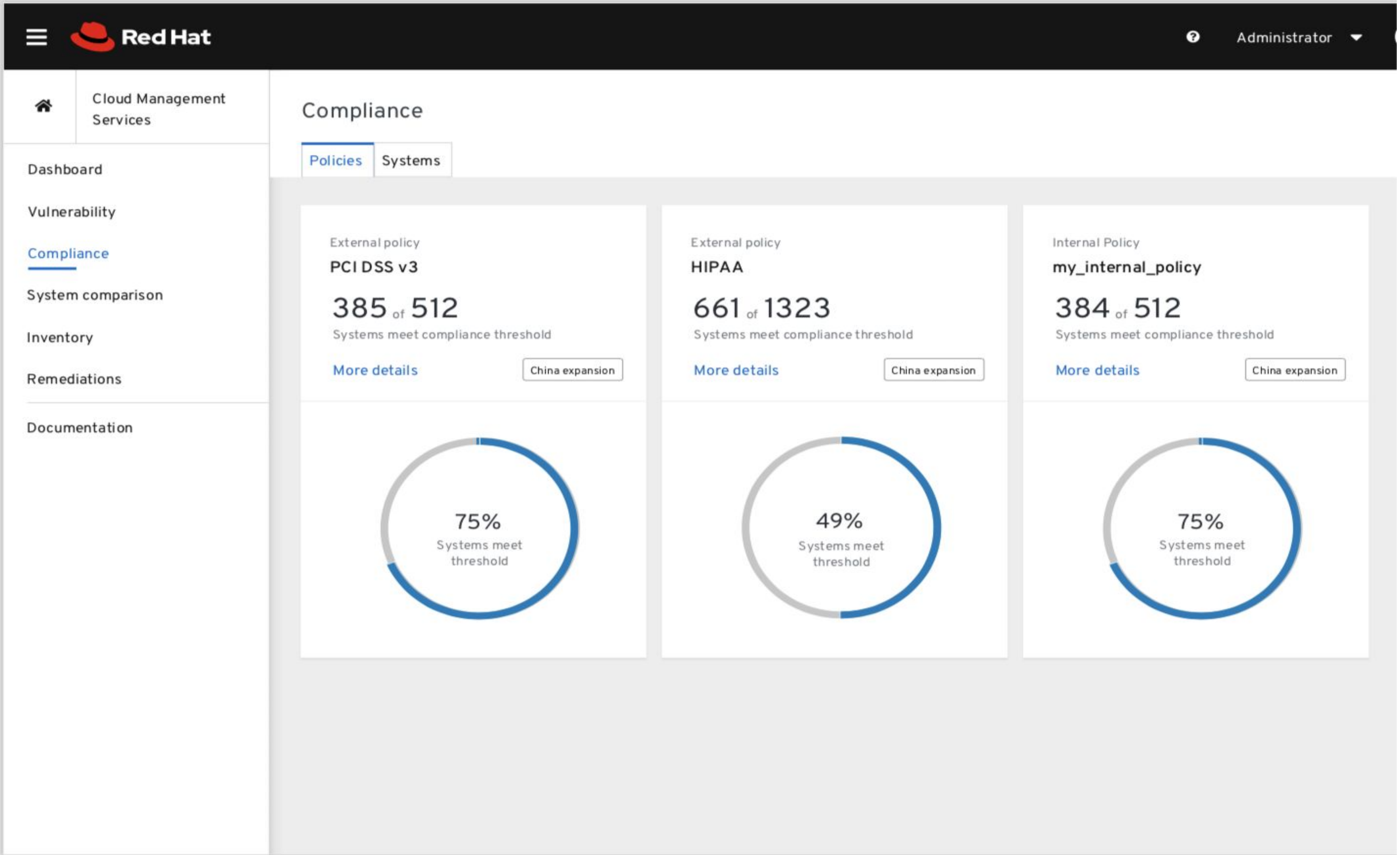
Vulnerability

Compliance

System Comparison

Inventory

Remediations



Compliance

External policy

PCI DSS v3

385 of 512

Systems meet compliance threshold

More details

China expansion

75% Systems meet threshold

External policy

HIPAA

661 of 1323

Systems meet compliance threshold

More details

China expansion

49% Systems meet threshold

Internal Policy

my_internal_policy

384 of 512

Systems meet compliance threshold

More details

China expansion

75% Systems meet threshold

Compliance - Use Cases

Summit 2019

- Ingest & view reports from OpenSCAP
  - By Policy
  - By Systems
- Triaging reports via
  - Failed rules
  - Severity
- Ansible Automation
- Reporting
  - JSON
  - CSV
- Set Compliance Threshold

Oct 2019

- Improved UI navigation
- Customization: Tie “Business Objective” to a policy
- Better triaging of rules
  - Filter rules when system has multiple policies
  - By Identifiers

Backlog

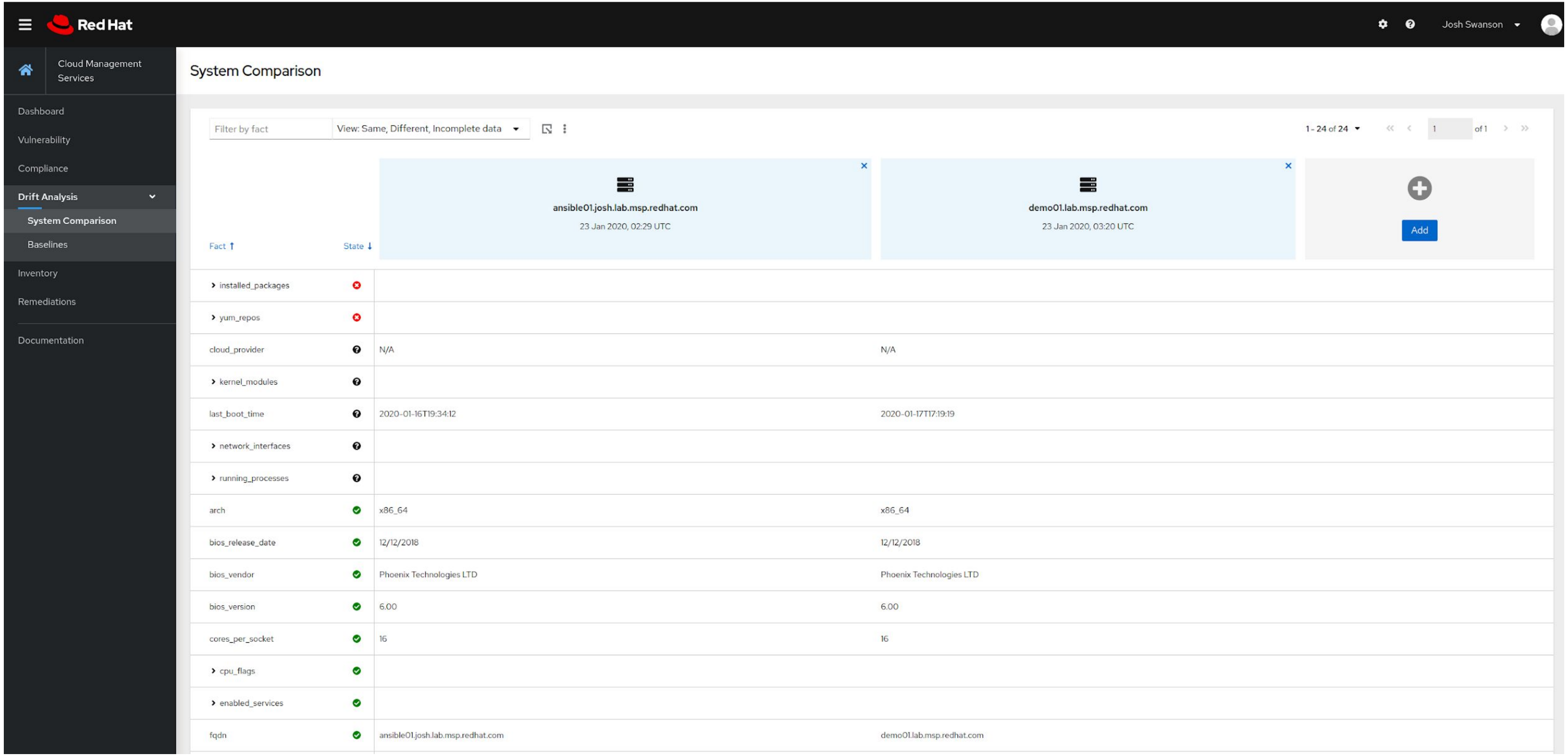
- Create a new SCAP Policy
- Tailor/modify rules
- Tagging/Tag Filtering*
- Integration to status.redhat.com*
- RBAC Enabled (light)*
- Search by References
- Delete a Report
- Well-documented APIs
- RBAC Enabled (heavy)*
- Alerting & Notification*
- Reporting
  - Executive Report (PDF)
  - Report by Policy (PDF)
- Fail policy if “high severity” rules fail
- Exempt host from a report for a temporary duration

* Dependency on the Platform

cloud management services for Red Hat Enterprise Linux

System Comparison

System Comparison



System Comparison

Fact ↑	State ↓	ansible01.josh.lab.msp.redhat.com 23 Jan 2020, 02:29 UTC	demo01.lab.msp.redhat.com 23 Jan 2020, 03:20 UTC
› installed_packages	✕		
› yum_repos	✕		
cloud_provider	?	N/A	N/A
› kernel_modules	?		
last_boot_time	?	2020-01-16T19:34:12	2020-01-17T17:19:19
› network_interfaces	?		
› running_processes	?		
arch	✓	x86_64	x86_64
bios_release_date	✓	12/12/2018	12/12/2018
bios_vendor	✓	Phoenix Technologies LTD	Phoenix Technologies LTD
bios_version	✓	6.00	6.00
cores_per_socket	✓	16	16
› cpu_flags	✓		
› enabled_services	✓		
fqdn	✓	ansible01.josh.lab.msp.redhat.com	demo01.lab.msp.redhat.com

cloud management services for Red Hat Enterprise Linux

Call to Action

Cloud Management Is a Journey

We need your feedback

Are there specific use-cases cloud management can help with?

What can we do to make this a bigger part of your system management strategy?

How does this fit into your system management landscape?

Are there any barriers to entry we can eliminate?

The BU is excited for feedback. Let’s talk!
jswanson@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.

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat

Toss a coin to your solution architect.