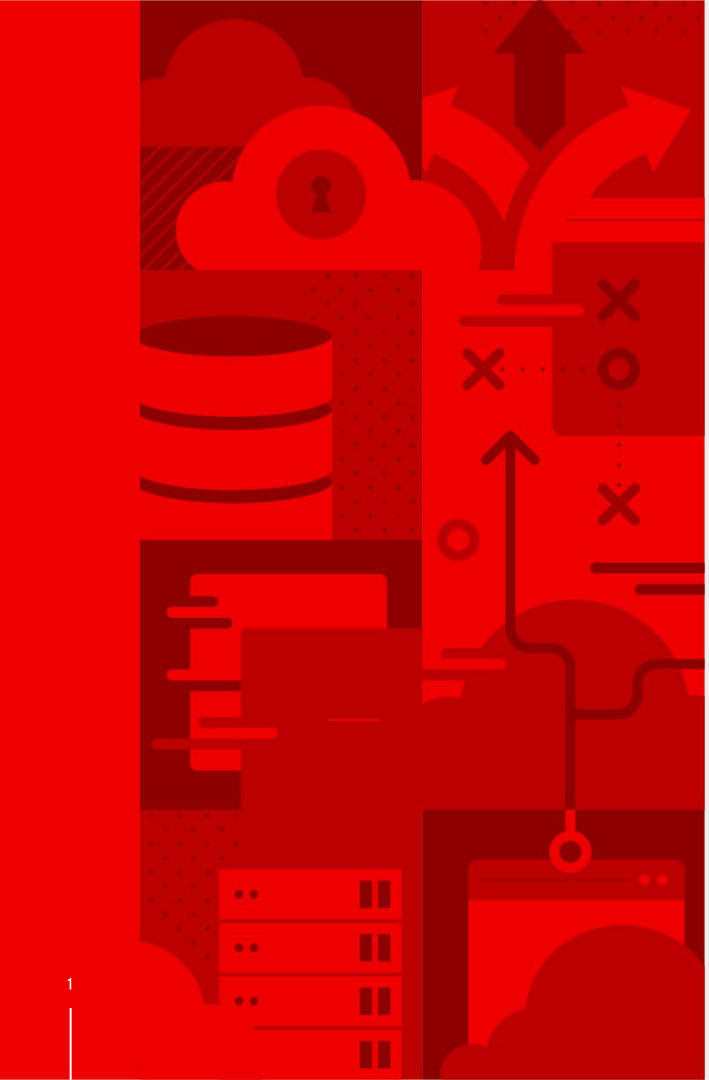


Red Hat Insights

Analyze, Secure and Automate your platform

Tim De Borger
Solution Architect Manager - BeLux

Red Hat

Disclaimer

The content set forth herein is Red Hat confidential information and does not constitute in any way a binding or legal agreement or impose any legal obligation or duty on Red Hat.

This information is provided for discussion purposes only and is subject to change for any or no reason.

Agenda

- Introduction
- cloud.redhat.com
- How Insights Helps you
- Insights Capabilities
- Insights Architecture
- Running Insights
- Automated Insights
- What do you do with my information?
- Demo

Introduction

Who Am I

- Tim De Borger
- Study
  - Systems Analyst/Programmer (Graduate)
- Career
  - KB (2.5)
  - Progress Software (20)
  - Red Hat (4)
- Areas
  - Technical Support (5 Years)
  - Programmer (3 Years)
  - Consultant (14 Years)
  - Solution Architect (6.5)

Why Am I Telling This?

- 5 Years in Support
  - 1995 - 2000
  - EMEA Based Center in Rotterdam
  - 40-45 people covering 15+ languages in one place
  - Era of dial-in/dial-back
- Support Optimizations
  - Character Based Application for Call Logging with primitive K-Base Interface
  - GUI Based Application with advance interface for K-Base
  - Online accessible K-Base for Customers
  - Online Call logging and access for Customers
- Internal Impact
  - Support Engineers not happy with GUI - Slower Reactions
  - Support Engineers happy with Faster Resolution
  - Support Engineers happy with less Calls logged
  - Management unhappy with less Calls logged
  - Customers Happy (most of the time) with the ‘Open System’

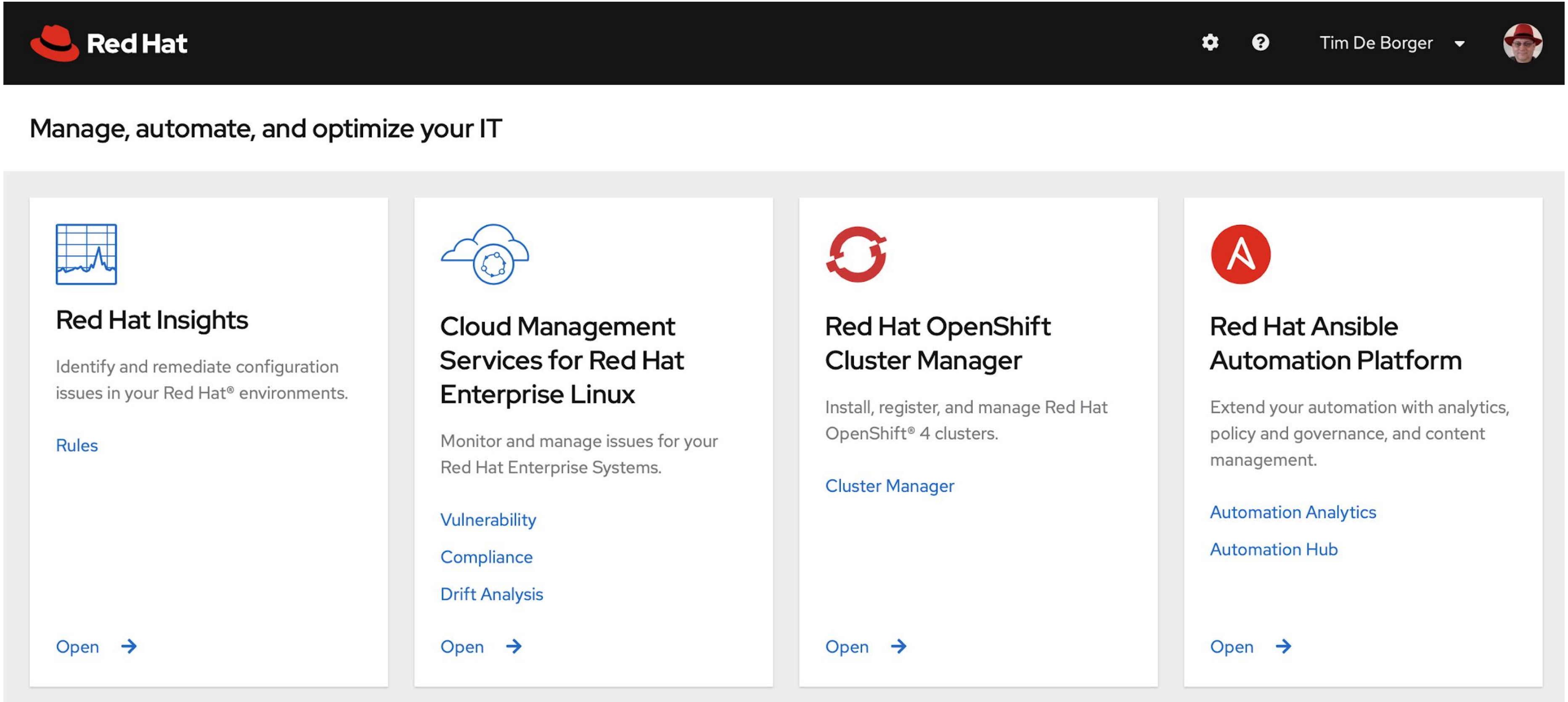
Next Level of Support

- What If:
  - Support understands more about the ‘base’ configuration @Customer
  - Support can correlate reoccurring issues with the ‘base’ configuration
  - Correlation based on knowledge from Engineering
  - With 0% Effort on the Customer Side
- Then there is an Automated Way to ...:
  - Notify Customers on possible issues in the systems and configurations
  - Provide the Solution in a simple and standard way
  - Improve Customers Platform Stability, Security and Performance
- How Is this done?
  - Stay for the next 30 minutes …
  - Can be seen as a sample of AI/ML

Red Hat Insights

cloud.redhat.com

Insights Portal Moved



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 →

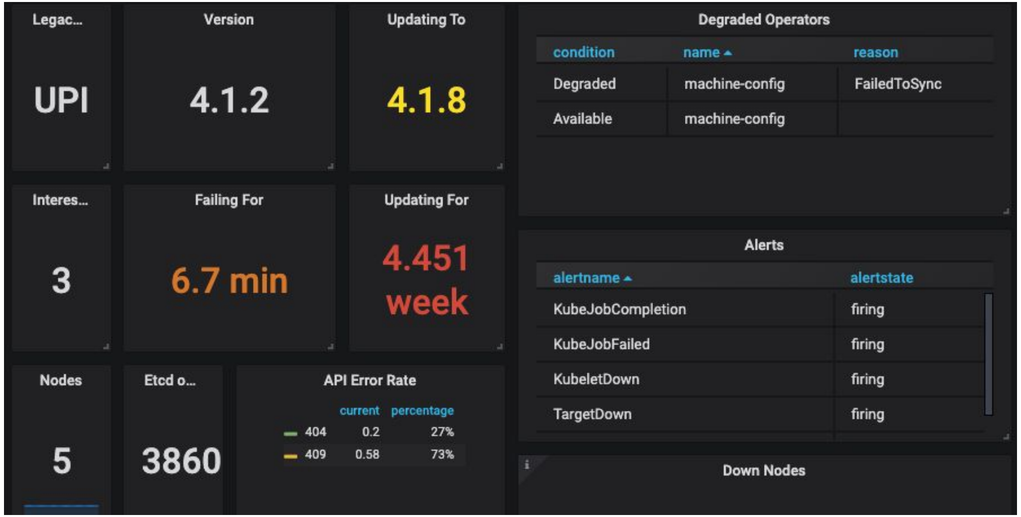
Connected Customer

Proactive support for customer issues

- Active upgrades
- Overall cluster health
- Firing alerts
- Node health

Driving a high quality product

- Monitor and improve upon the health of the customer base
- Prioritize engineering roadmap for platforms and prove they are improving over time
- Active monitoring of fast and stable channels



Legac... UPI

Version 4.1.2

Updating To 4.1.8

Interes... 3

Failing For 6.7 min

Updating For 4.451 week

Nodes 5

Etcd o... 3860

API Error Rate

	current	percentage
404	0.2	27%
409	0.58	73%

Degraded Operators

condition	name ▴	reason
Degraded	machine-config	FailedToSync
Available	machine-config	

Alerts

alertname ▴	alertstate
KubeJobCompletion	firing
KubeJobFailed	firing
KubeletDown	firing
TargetDown	firing

Down Nodes

How Insights Helps You

Complexity is risk

80%

Percentage of commercial application outages caused by software failure and operational complexity

Carnegie Mellon

$336k/hr

The median cost per hour of downtime for a production application for a large enterprise

Gartner®

$15m/yr

Mean annualized cost of cybercrime deference and remediation for large US-based corporations

Ponemon INSTITUTE

65% of CompTIA customers thought they were significantly behind in training and capabilities needed to manage their next generation infrastructure.

Red Hat Insights

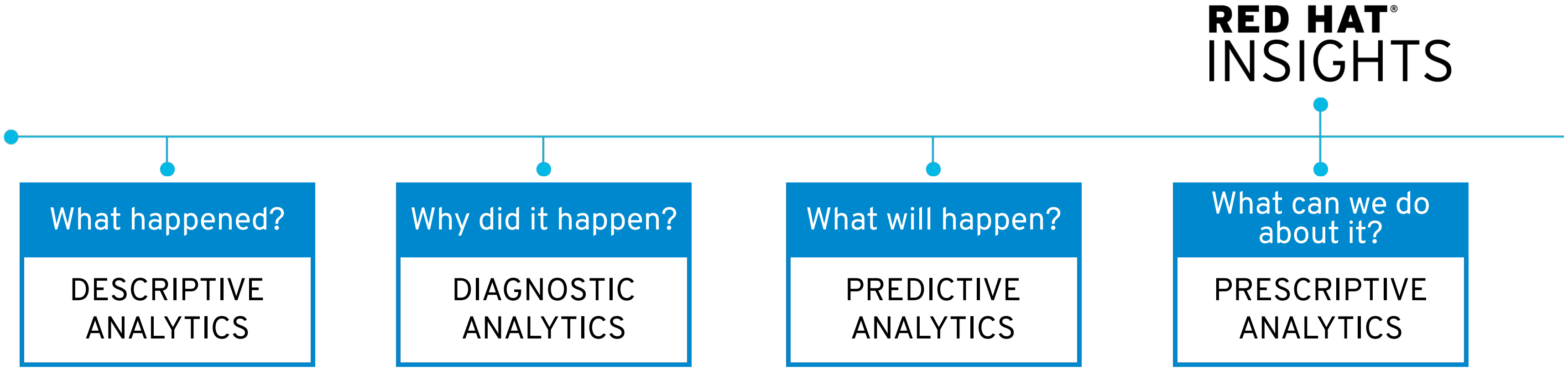
PREDICT RISK. GET GUIDANCE. STAY SECURE.

PREDICTIVE I.T. ANALYTICS

AUTOMATED EXPERT ASSESSMENT

SIMPLE REMEDIATION

I.T. OPERATIONAL ANALYTICS (ITOA)



RED HAT® INSIGHTS

What happened?

DESCRIPTIVE ANALYTICS

Why did it happen?

DIAGNOSTIC ANALYTICS

What will happen?

PREDICTIVE ANALYTICS

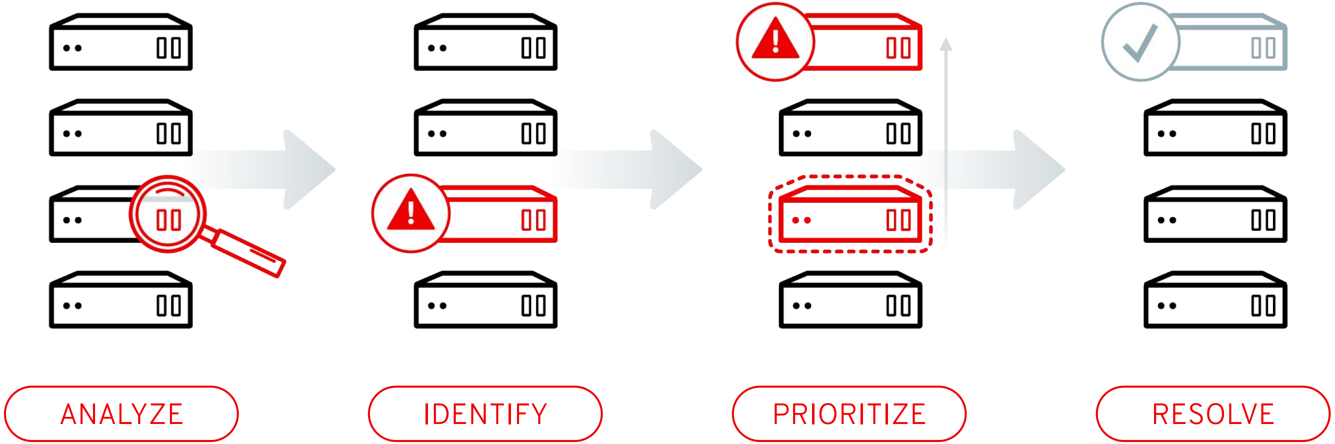
What can we do about it?

PRESCRIPTIVE ANALYTICS

Customer Stories

- Insights was able to immediately identify 10 issues on an Oracle RAC system that has been **plaguing a customer for 6 months.**
  - Oracle RAC systems are EXPENSIVE. Why not keep them running at **optimal** capacity?
- One customer swore their 2,000 servers were up-to-date.
  - A demonstration of Red Hat Insights showed them that **400 of their servers were not up-to-date**, and therefore at **risk**.

Managing infrastructure risk



Why Red Hat Insights?

ACTIONABLE INTELLIGENCE POWERED BY RED HAT

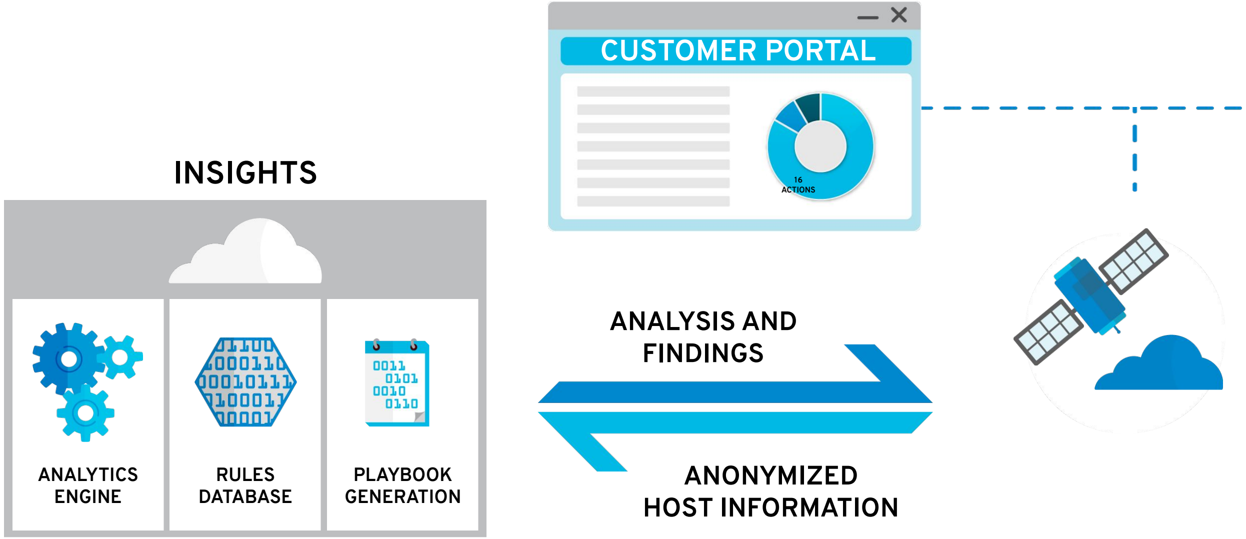
CONTINUOUS VULNERABILITY ALERTS

INCREASED VISIBILITY TO SECURITY RISKS

SIMPLE REMEDIATION

Automatic remediation available through Satellite or Tower

Red Hat Insights



View results and alerts from Insights in either the Customer Portal or through the Satellite user interface.

Red Hat Insights

Now included with all Red Hat Enterprise Linux subscriptions

Buy

Red Hat
Enterprise Linux

Get

Red Hat
Insights

Red Hat Insights Capabilities

Red Hat Insights

Included with your Red Hat Enterprise Linux subscription

Assesses

customer’s Red Hat environments

Remediates

findings with prescriptive remediation steps or an Ansible playbook

Insights

rule contributions directly from Red Hat subject matter experts

Identifying risks for Availability, performance, stability and security

Key risks discovered

Tailored resolution steps included for resolution

Performance issue

Network interface is not performing at maximum speed

Recommended action

Check cable, connections, and remote switch settings

Security risk detected

Privilege escalation

Recommended action

Apply mitigation and update the kernel

Availability

OpenShift operations fail if insufficient CPU or memory

Recommended action

Increase CPU and/or memory reservation

Stability

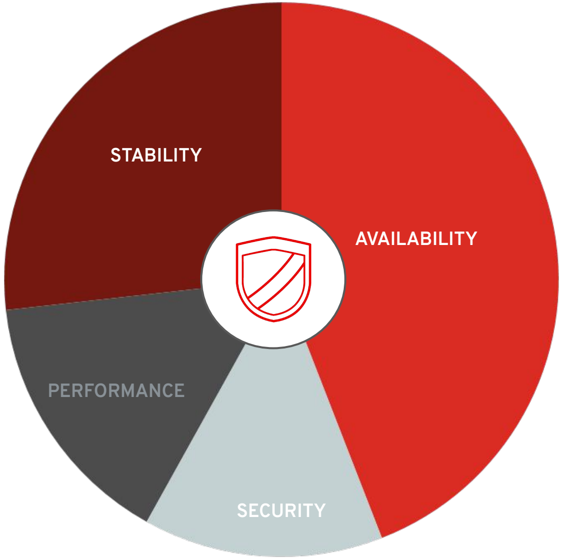
Filesystem has exceeded 95% capacity

Recommended action

Increase free space on the host.

More than just security

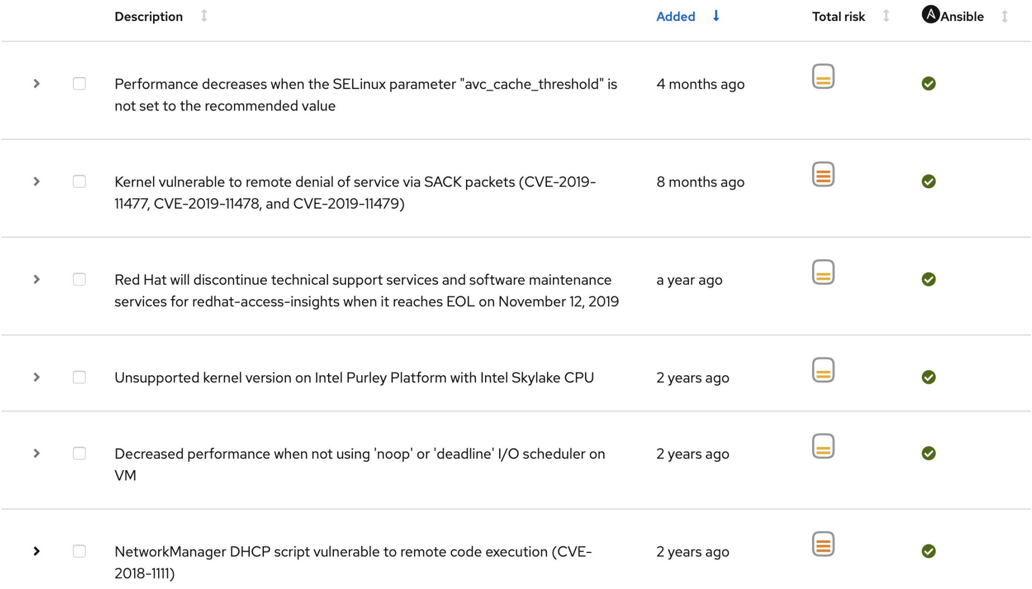
Red Hat Insights has more than 1000 rules—here is how they stack up across categories



- ● **Availability** 44%
- ● **Security** 15%
- ● **Stability** 27%
- ● **Performance** 14%

Get ahead of key security risks

Don’t wait for your security team to tap you on the shoulder



Description	Added	Total risk	Ansible
Performance decreases when the SELinux parameter "avc_cache_threshold" is not set to the recommended value	4 months ago	≡	✓
Kernel vulnerable to remote denial of service via SACK packets (CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479)	8 months ago	≡	✓
Red Hat will discontinue technical support services and software maintenance services for redhat-access-insights when it reaches EOL on November 12, 2019	a year ago	≡	✓
Unsupported kernel version on Intel Purley Platform with Intel Skylake CPU	2 years ago	≡	✓
Decreased performance when not using 'noop' or 'deadline' I/O scheduler on VM	2 years ago	≡	✓
NetworkManager DHCP script vulnerable to remote code execution (CVE-2018-1111)	2 years ago	≡	✓

- Prioritizes security response by analyzing runtime configuration and usage

- Automates security analysis, beyond just CVEs

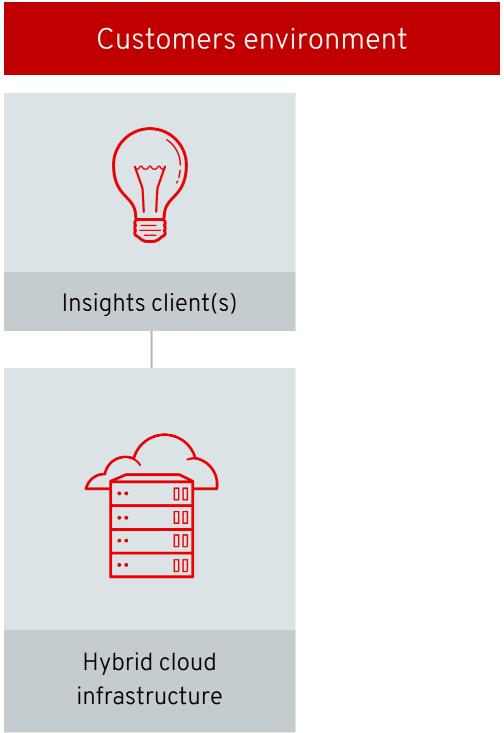
*“…when a vulnerability is released, it’s likely to be exploited within **40-60** days. However, it takes security teams between **100-120** days on average to remediate…”*

– KENNA SECURITY GROUP

Red Hat Insights

Architecture

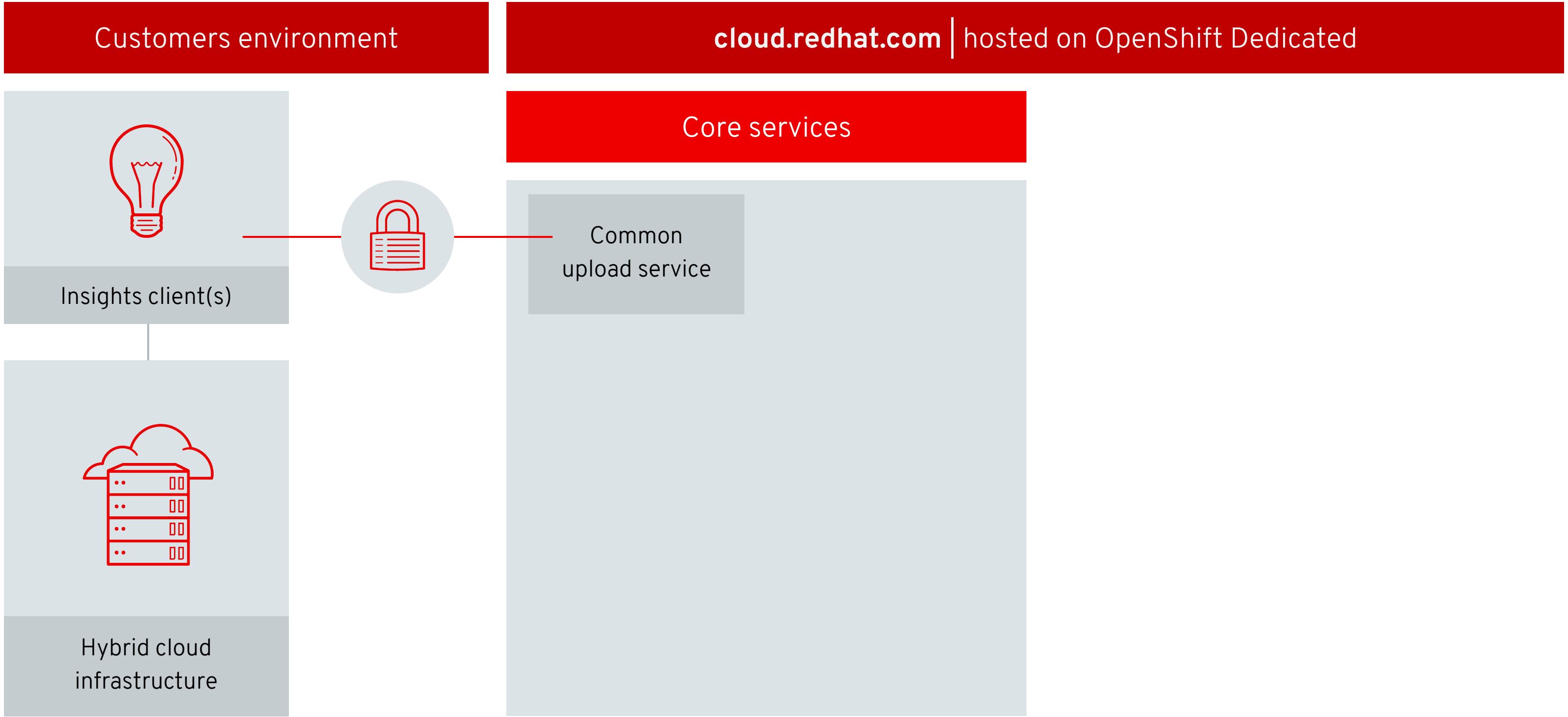
Red Hat Insights &
cloud management services for Red Hat Enterprise Linux

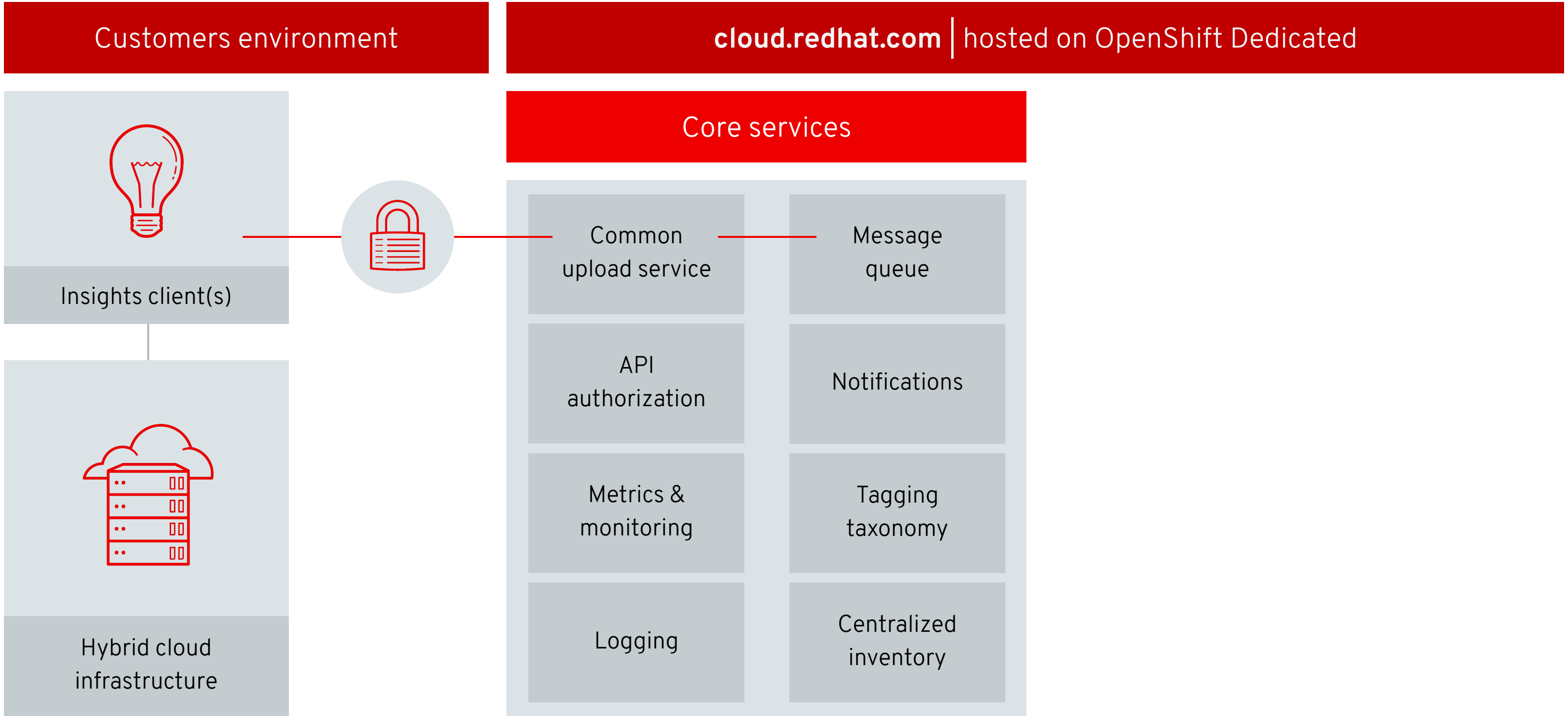


Customers environment

Insights client(s)

Hybrid cloud infrastructure


Customers environment
cloud.redhat.com | hosted on OpenShift Dedicated
Core services
Insights client(s)
Common upload service
Hybrid cloud infrastructure



Customers environment

cloud.redhat.com | hosted on OpenShift Dedicated

Insights client(s)

Hybrid cloud infrastructure

Core services

Common upload service

Message queue

API authorization

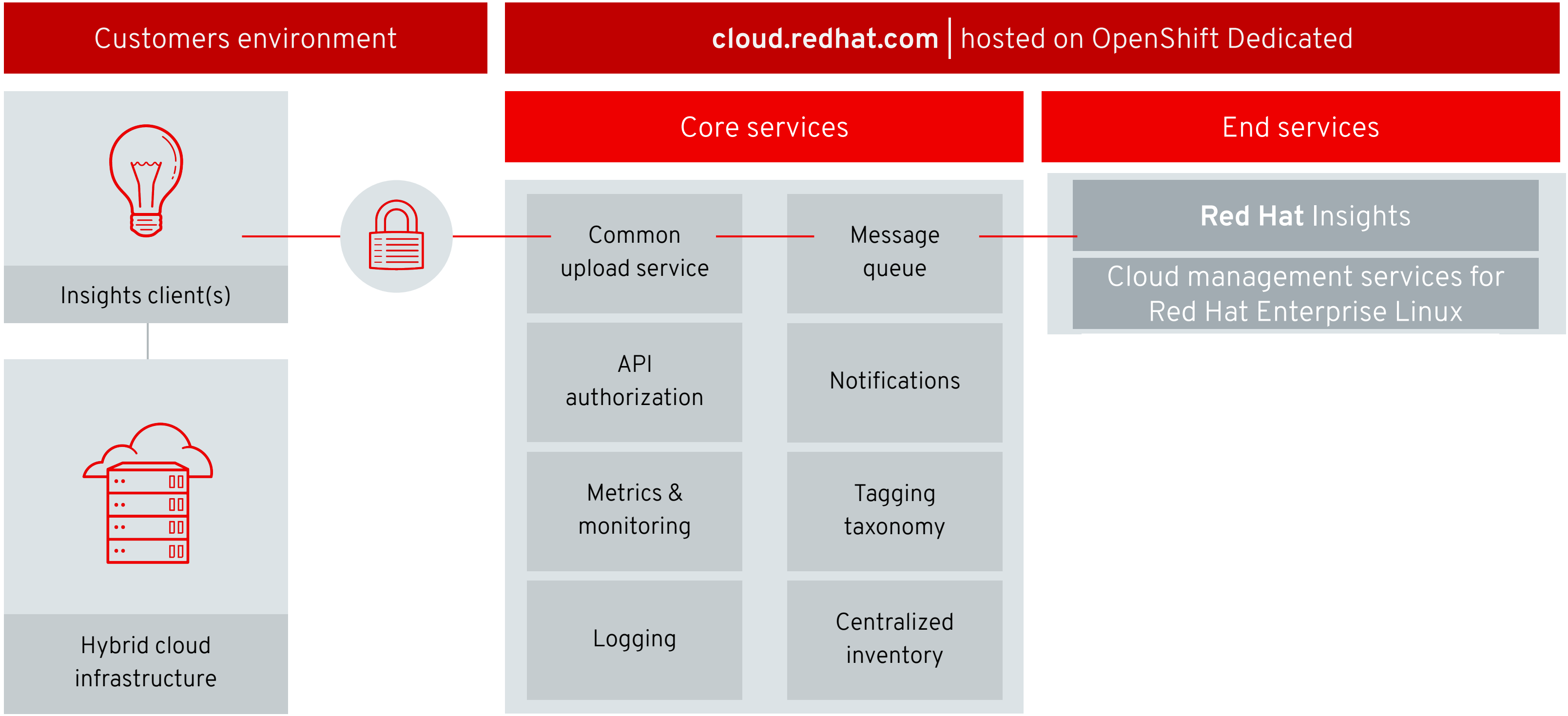
Notifications

Metrics & monitoring

Tagging taxonomy

Logging

Centralized inventory



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

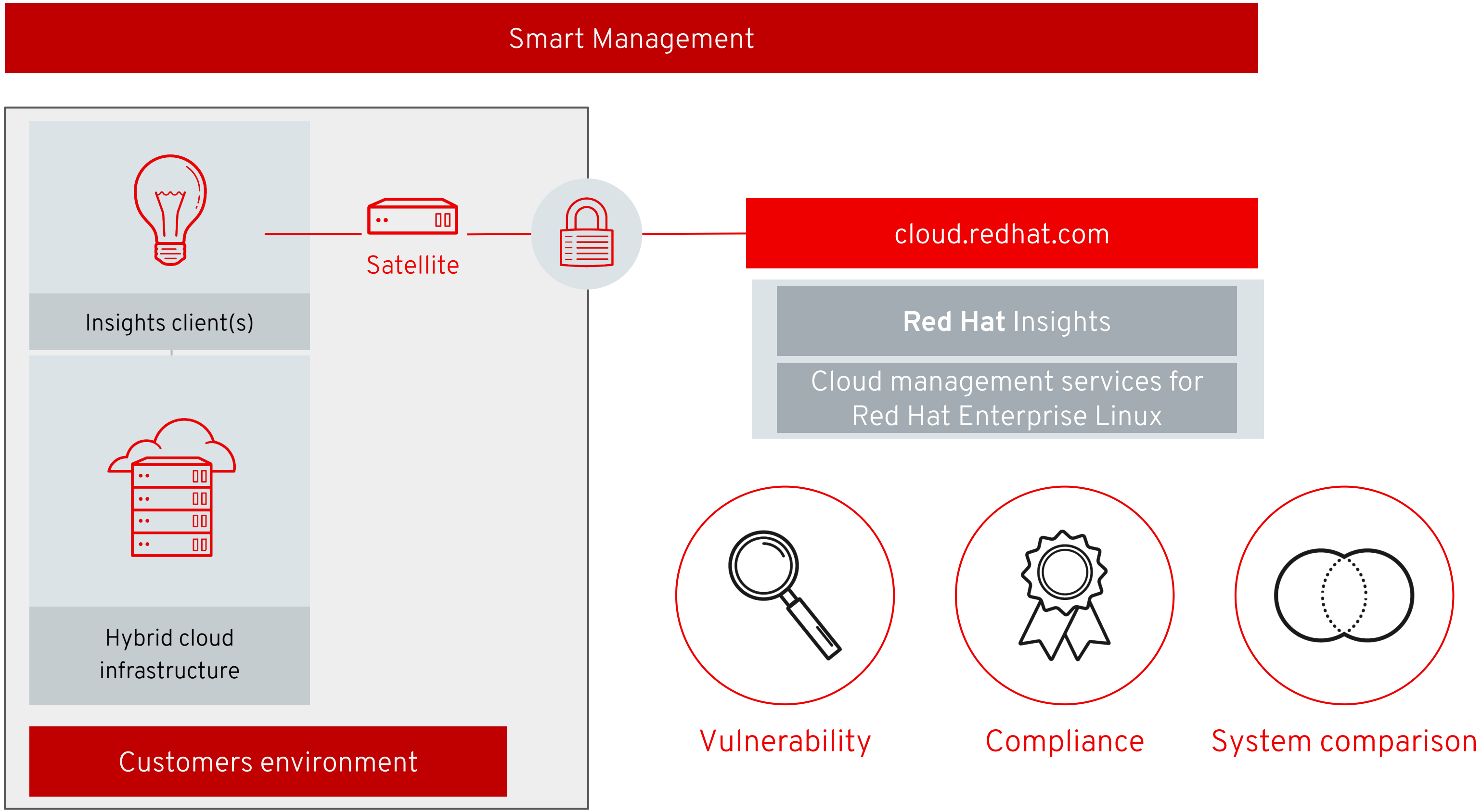
Logging

Centralized inventory

End services

Red Hat Insights

Cloud management services for Red Hat Enterprise Linux



Smart Management

Insights client(s)

Satellite

Hybrid cloud infrastructure

Customers environment

cloud.redhat.com

Red Hat Insights

Cloud management services for Red Hat Enterprise Linux

Vulnerability

Compliance

System comparison

Red Hat Insights

How to use Red Hat Insights

Installation and registration

Simple and Straightforward

Step #1: Run (as root) `# yum install insights-client`

- Red Hat Enterprise Linux 8 customers will not need to perform this step - the Insights client is pre-installed.

Step #2: Run (as root) `# insights-client --register`

More information including automation playbooks are available at:

- https://access.redhat.com/insights/getting-started

Man page available via $ man insights-client

Data collection

No sensitive data collected—only data needed for rule analysis

Example files

```
/etc/redhat-release
/proc/meminfo
/var/log/messages
/boot/grub/grub.conf
/boot/grub2/grub.cfg
/etc/modprobe.conf
```

Commands

```
/bin/rpm -qa
/bin/uname -a
/usr/sbin/dmidecode
/bin/netstat -i
/bin/ps auxcww
```

We do not collect log files, but we collect the lines that match a potential rule (e.g., page allocation failure.)

Four things you should know about data collection in Red Hat Insights

1 **Only portions of logs are collected.**

Bits of information about server configuration, rule match to the line of a log file.

2 **Data uploads are customizable.**

For example, you can delete server names or IP addresses. Collection schedules are also customizable.

3 **Information is encrypted.**

From the time it’s collected on the client server to transmission to the Insights service.

4 **Data remains for a short period of time.**

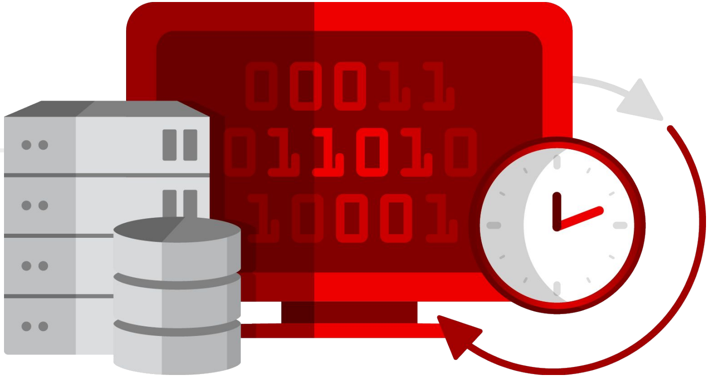
Daily replace of server upload? If upload is not sent, the current upload is deleted after 14 days.

How long does Red Hat store data?

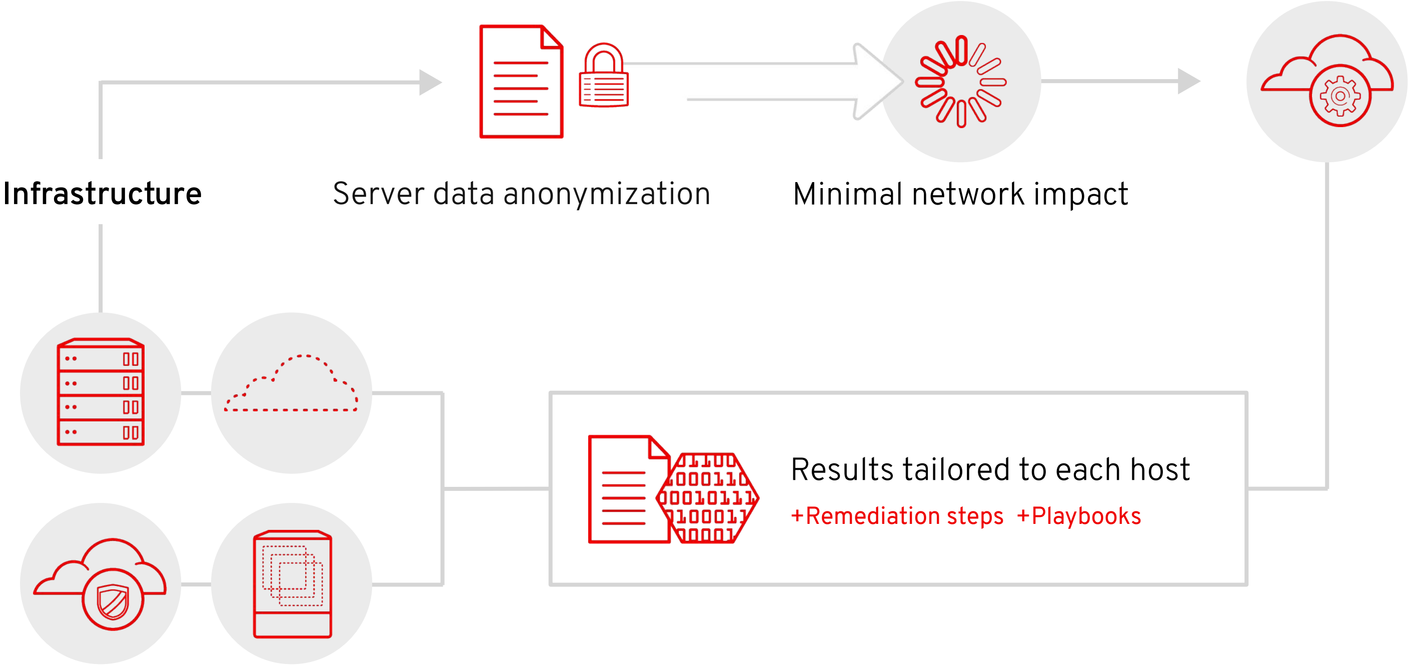
Typically 24 hours

2 weeks maximum

No permanent data storage



Architecture



Infrastructure

Server data anonymization

Minimal network impact

Results tailored to each host

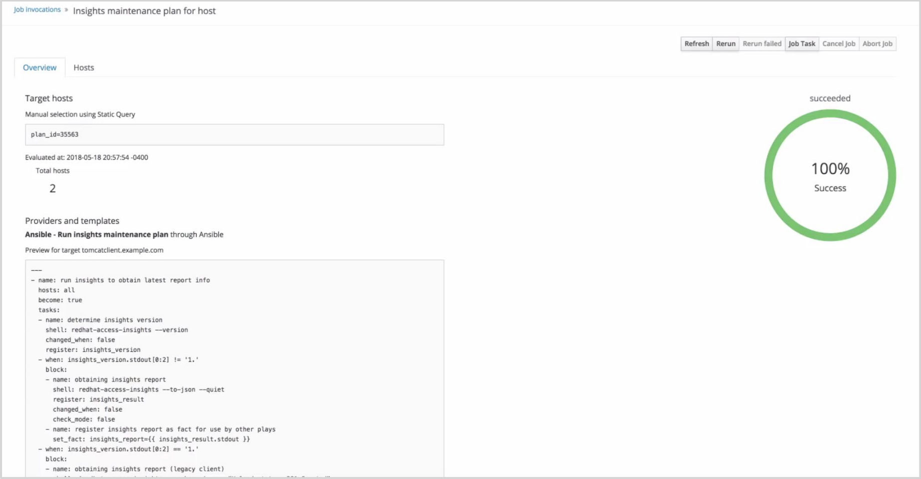
+Remediation steps +Playbooks

Red Hat Insights

Automatic remediation with Insights and Red Hat Management

Automatic remediation with Satellite 6.4+

Resolve issues with a click of a button



Insights maintenance plan for host

Target hosts

Manual selection using Static Query

```
plan_id=35563
```

Evaluated at: 2018-05-18 20:57:54 -0400

Total hosts

2

Providers and templates

Ansible - Run insights maintenance plan through Ansible

Preview for target tomcatclient.example.com

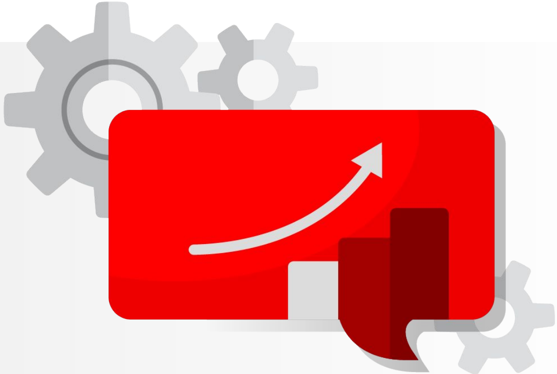
```
---
- name: run insights to obtain latest report info
  hosts: all
  become: true
  tasks:
  - name: determine insights version
    shell: redhat-access-insights --version
    changed_when: false
    register: insights_version
  - when: insights_version.stdout[0:2] != '1.'
    block:
    - name: obtaining insights report
      shell: redhat-access-insights --to-json --quiet
      register: insights_result
      changed_when: false
      check_mode: false
    - name: register insights report as fact for use by other plays
      set_fact: insights_report={{ insights_result.stdout }}
  - when: insights_version.stdout[0:2] == '1.'
    block:
    - name: obtaining insights report (legacy client)
```

Apply remediation plans with a click of a button–and track activity and progress on your machines.

Source: https://access.redhat.com/products/red-hat-insights#getstarted

Insights performance rules for Satellite

Customers can use Insights rules to recommend Satellite performance tunings, listed in the “Tuning Red Hat Satellite” guide.



Performance rules and tests include:

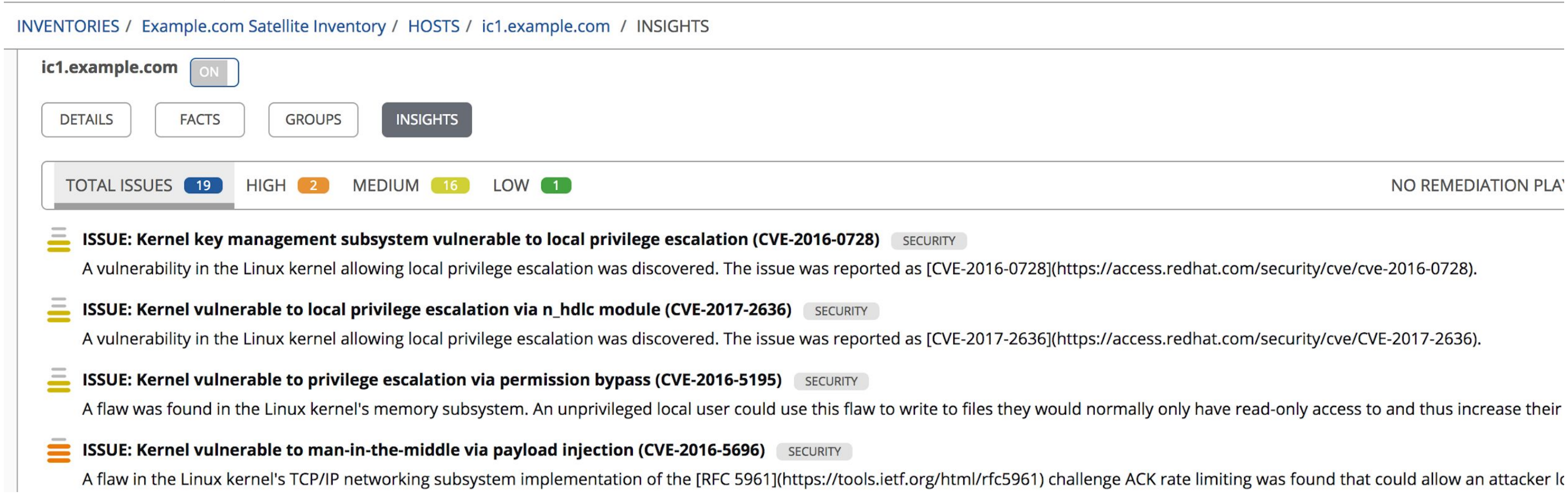
- MinInstance rule for Foreman.
- Passenger performance rule.
- Postgresql_frequent_checkpoints.py.
- Rule for pulp filetype to be of non-NFS type.
- Server limit rule for HTTPD access and error logs.
- Tests for pulp_ftype.
- Tests for serverLimit.
- Tests for postgresql_frequent_checkpoints.

Red Hat

Automatic reporting and remediation with Ansible Tower

Reporting and Remediation is also available on Red Hat Ansible Tower

- Reporting and Remediation, both manual and automatic (scheduling it)
    - Different look and feel, Tower approach



ISSUE: Kernel key management subsystem vulnerable to local privilege escalation (CVE-2016-0728) SECURITY

A vulnerability in the Linux kernel allowing local privilege escalation was discovered. The issue was reported as [CVE-2016-0728](https://access.redhat.com/security/cve/cve-2016-0728).

ISSUE: Kernel vulnerable to local privilege escalation via n_hdlc module (CVE-2017-2636) SECURITY

A vulnerability in the Linux kernel allowing local privilege escalation was discovered. The issue was reported as [CVE-2017-2636](https://access.redhat.com/security/cve/CVE-2017-2636).

ISSUE: Kernel vulnerable to privilege escalation via permission bypass (CVE-2016-5195) SECURITY

A flaw was found in the Linux kernel's memory subsystem. An unprivileged local user could use this flaw to write to files they would normally only have read-only access to and thus increase their

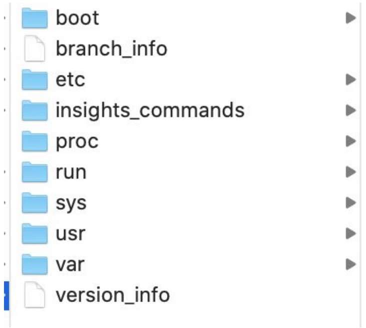
ISSUE: Kernel vulnerable to man-in-the-middle via payload injection (CVE-2016-5696) SECURITY

A flaw in the Linux kernel's TCP/IP networking subsystem implementation of the [RFC 5961](https://tools.ietf.org/html/rfc5961) challenge ACK rate limiting was found that could allow an attacker lo

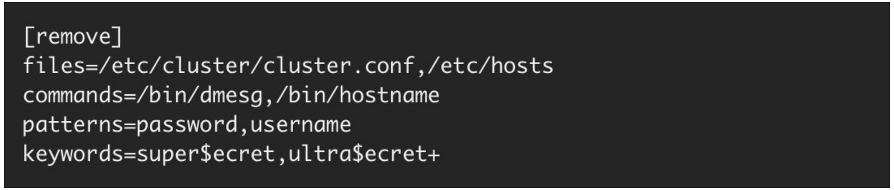
What do you do with my Information

Your Information

- All collected information is **non** GPDR
- All information can be checked:
  - insights-client --no-upload
    - Archive saved at /var/tmp/e7spk69h/insights-rhel81-20200123132507.tar.gz
- All information can be filtered:
  - `/etc/insights-client/remove.conf`
    - File Content
    - Specific Commands
    - String Patterns
    - Keywords
  - File can be validated
  - All can be Obfuscated
- Data-Collection can be Dynamic or … Based on RPM package install
- And …
  - What about SOS reports?



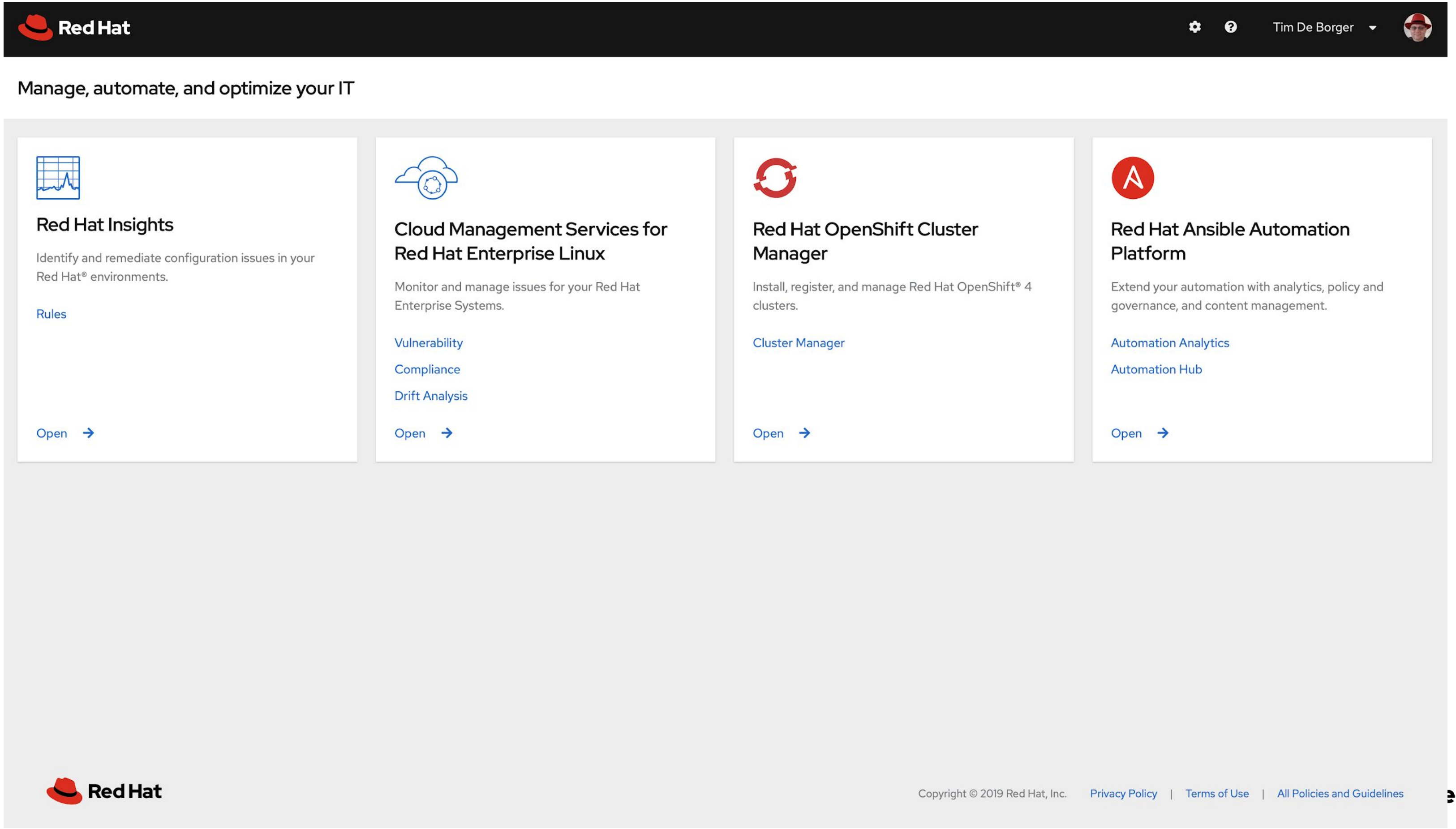
```
boot
branch_info
etc
insights_commands
proc
run
sys
usr
var
version_info
```



```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmesg,/bin/hostname
patterns=password,username
keywords=super$ecret,ultra$ecret+
```

Red Hat Insights

Demo



Manage, automate, and optimize your IT

Red Hat Insights

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

Cloud Management Services for Red Hat Enterprise Linux

Monitor and manage issues for your Red Hat Enterprise Systems.

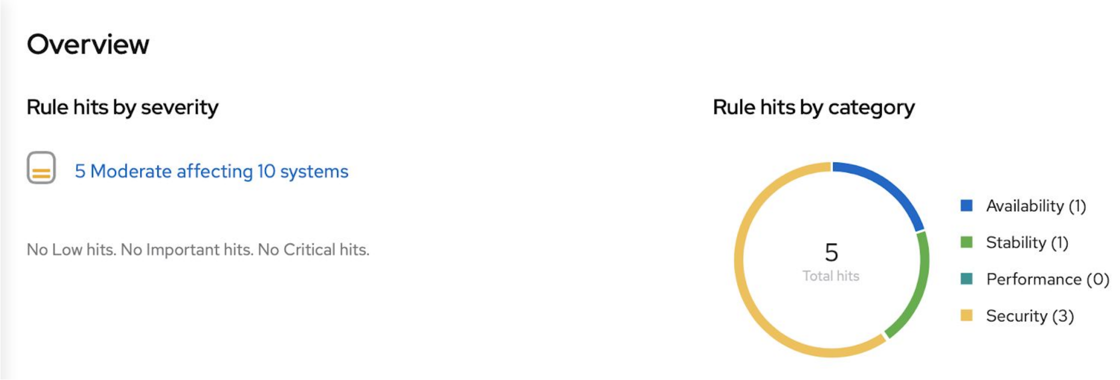
Red Hat OpenShift Cluster Manager

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

Red Hat Ansible Automation Platform

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

Demo



Overview

Rule hits by severity

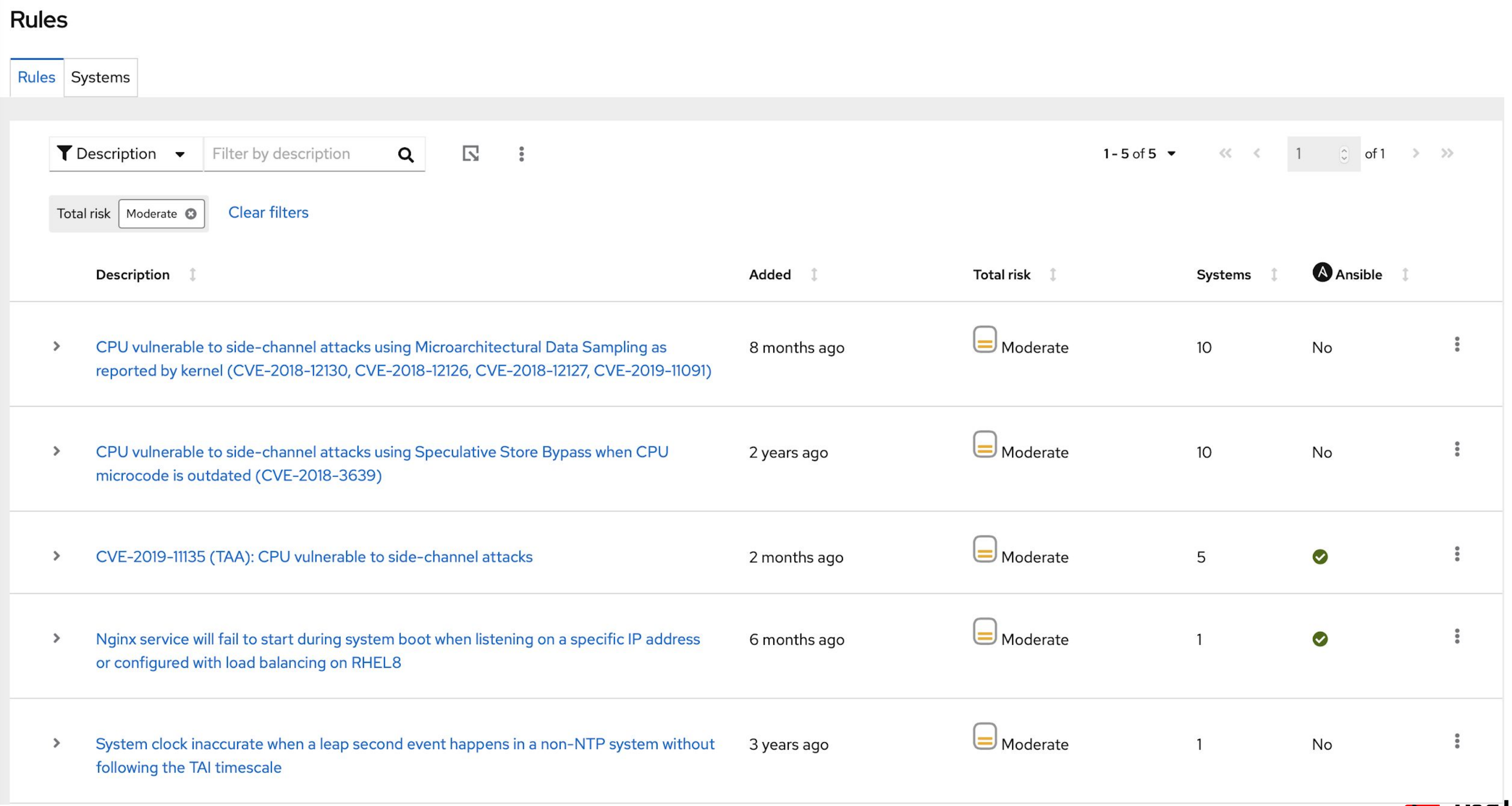
5 Moderate affecting 10 systems

No Low hits. No Important hits. No Critical hits.

Rule hits by category

5
Total hits

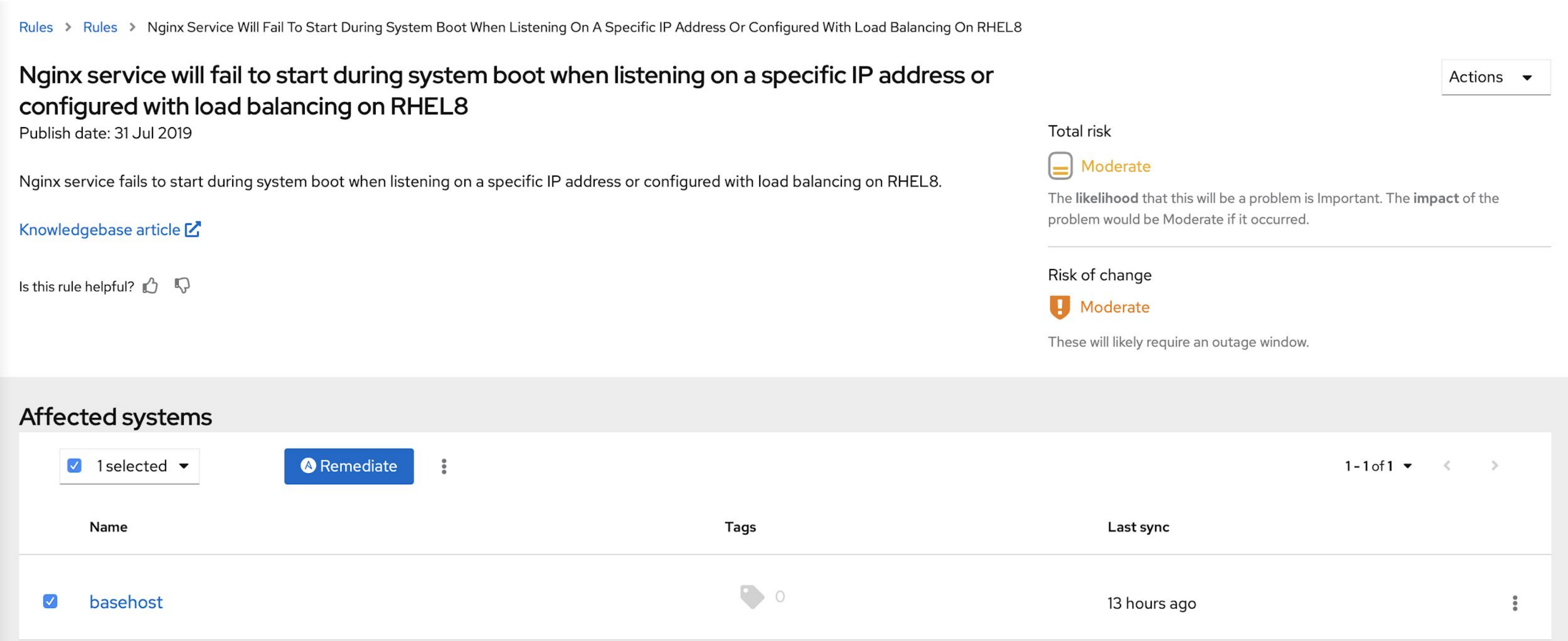
- Availability (1)
- Stability (1)
- Performance (0)
- Security (3)



Rules

Total risk: Moderate — Clear filters

	Description	Added	Total risk	Systems	Ansible
›	CPU vulnerable to side-channel attacks using Microarchitectural Data Sampling as reported by kernel (CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, CVE-2019-11091)	8 months ago	Moderate	10	No
›	CPU vulnerable to side-channel attacks using Speculative Store Bypass when CPU microcode is outdated (CVE-2018-3639)	2 years ago	Moderate	10	No
›	CVE-2019-11135 (TAA): CPU vulnerable to side-channel attacks	2 months ago	Moderate	5	✓
›	Nginx service will fail to start during system boot when listening on a specific IP address or configured with load balancing on RHEL8	6 months ago	Moderate	1	✓
›	System clock inaccurate when a leap second event happens in a non-NTP system without following the TAI timescale	3 years ago	Moderate	1	No



Rules › Rules › Nginx Service Will Fail To Start During System Boot When Listening On A Specific IP Address Or Configured With Load Balancing On RHEL8

Nginx service will fail to start during system boot when listening on a specific IP address or configured with load balancing on RHEL8

Publish date: 31 Jul 2019

Nginx service fails to start during system boot when listening on a specific IP address or configured with load balancing on RHEL8.

Knowledgebase article

Is this rule helpful?

Total risk

Moderate

The **likelihood** that this will be a problem is Important. The **impact** of the problem would be Moderate if it occurred.

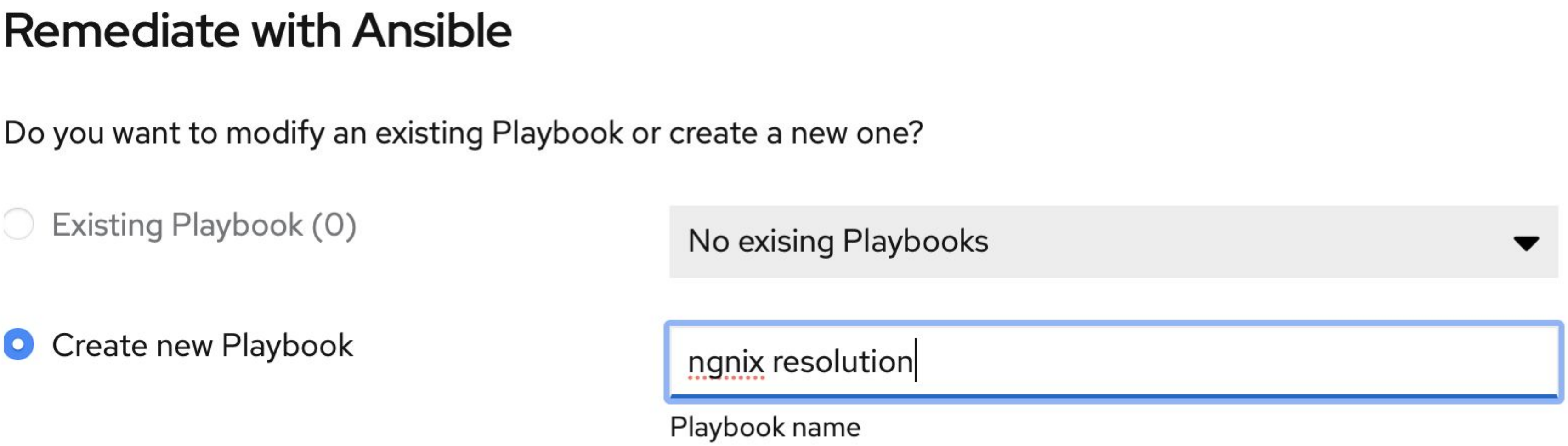
Risk of change

Moderate

These will likely require an outage window.

Affected systems

	Name	Tags	Last sync
☑	basehost	0	13 hours ago



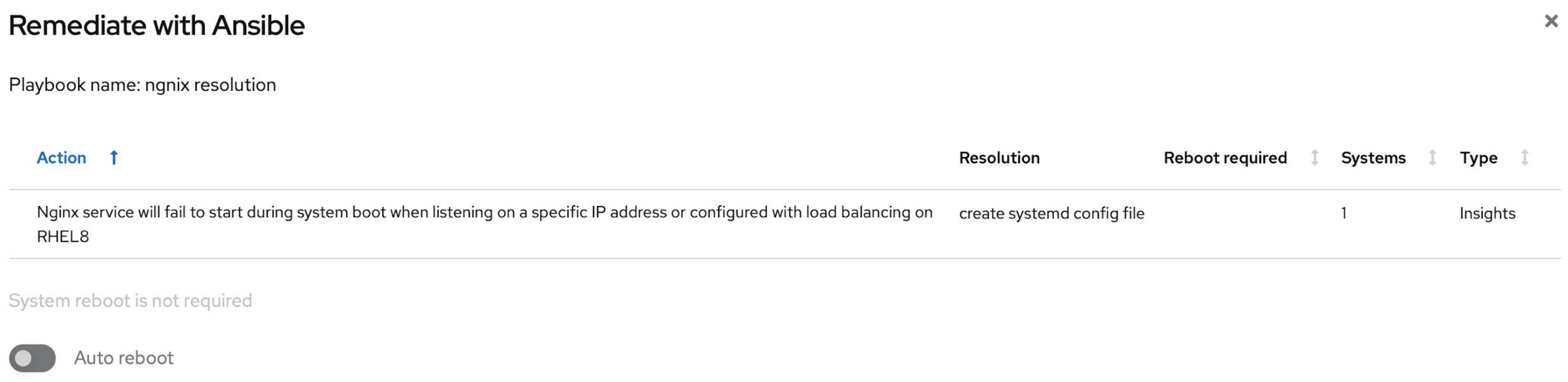
Remediate with Ansible

Do you want to modify an existing Playbook or create a new one?

○ Existing Playbook (0) — No exising Playbooks ▼

● Create new Playbook — ngnix resolution

Playbook name



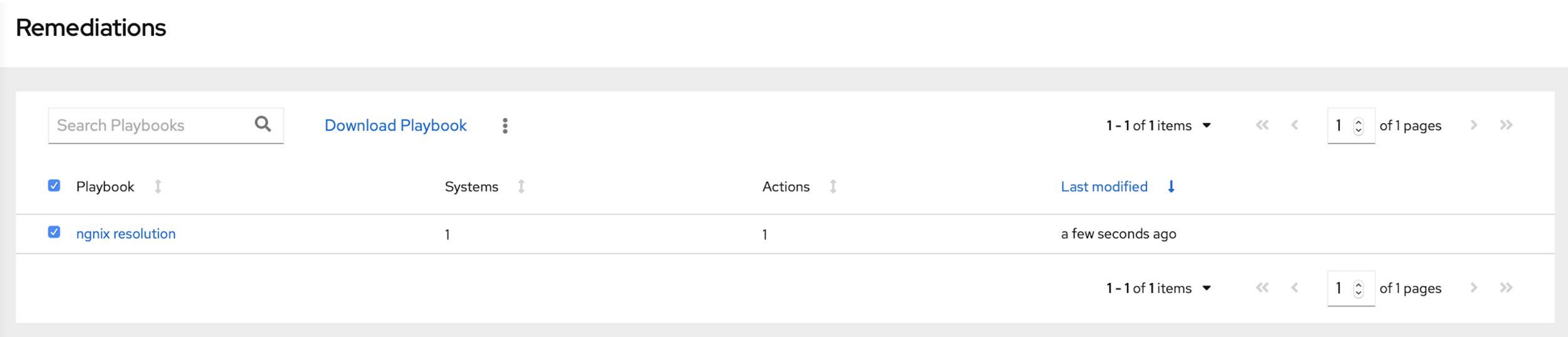
Remediate with Ansible

Playbook name: ngnix resolution

Action ↑	Resolution	Reboot required	Systems	Type
Nginx service will fail to start during system boot when listening on a specific IP address or configured with load balancing on RHEL8	create systemd config file		1	Insights

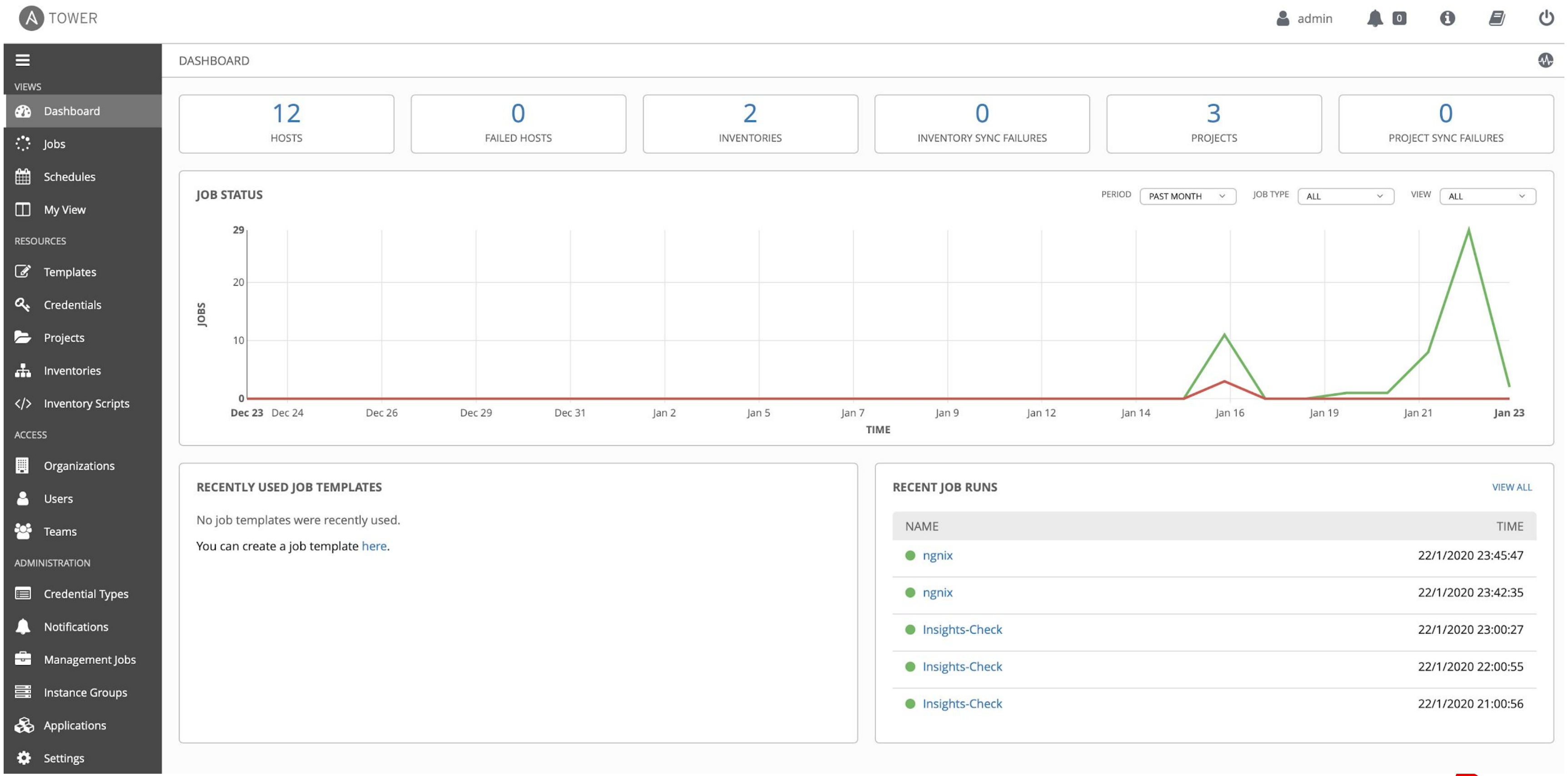
System reboot is not required

○ Auto reboot



Remediations

☑ Playbook	Systems	Actions	Last modified
☑ ngnix resolution	1	1	a few seconds ago



12	0	2	0	3	0
HOSTS	FAILED HOSTS	INVENTORIES	INVENTORY SYNC FAILURES	PROJECTS	PROJECT SYNC FAILURES

JOB STATUS

PERIOD PAST MONTH   JOB TYPE ALL   VIEW ALL

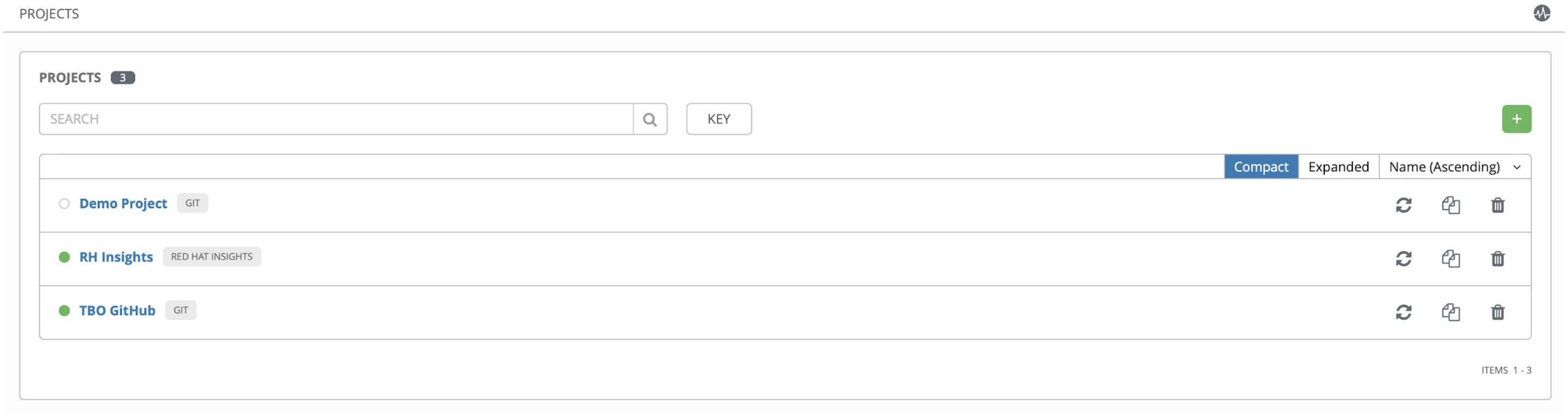
RECENTLY USED JOB TEMPLATES

No job templates were recently used.

You can create a job template here.

RECENT JOB RUNS

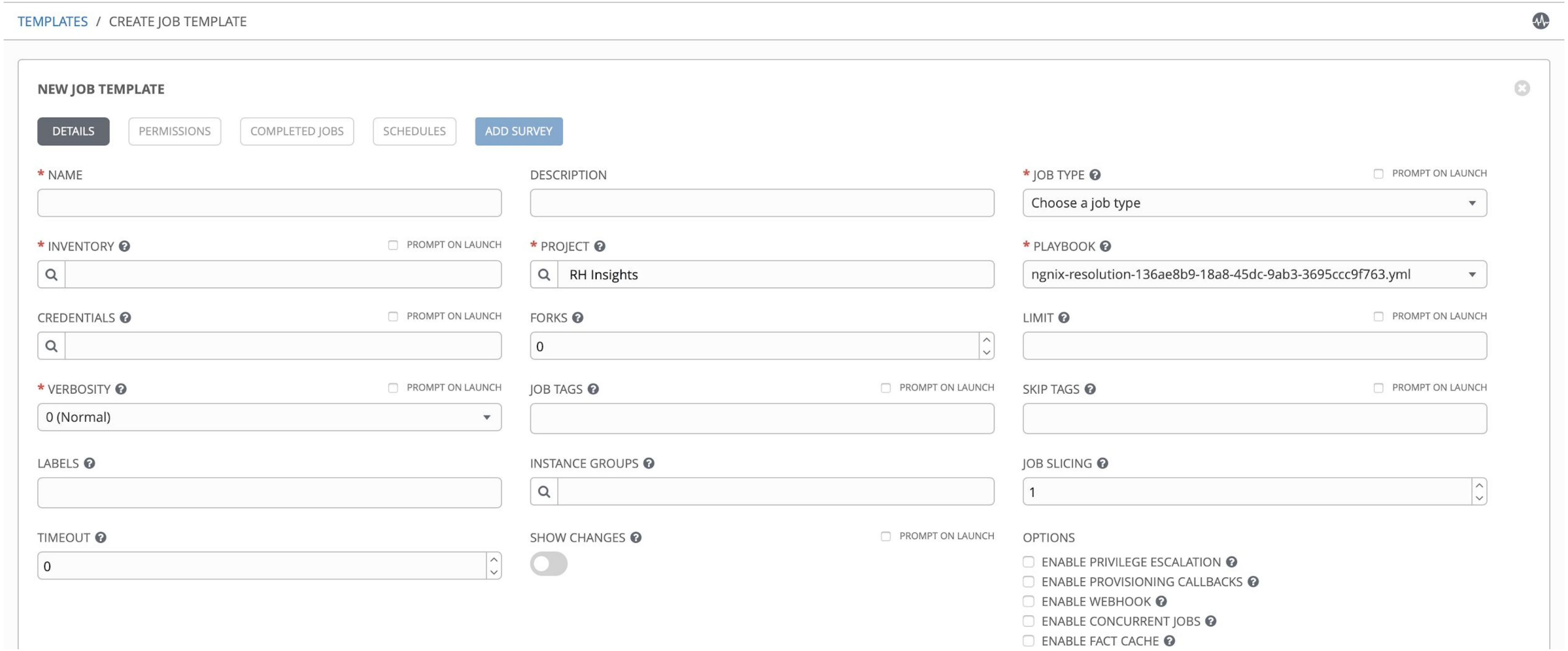
NAME	TIME
● ngnix	22/1/2020 23:45:47
● ngnix	22/1/2020 23:42:35
● Insights-Check	22/1/2020 23:00:27
● Insights-Check	22/1/2020 22:00:55
● Insights-Check	22/1/2020 21:00:56



PROJECTS 3

○	Demo Project	GIT
●	RH Insights	RED HAT INSIGHTS
●	TBO GitHub	GIT

ITEMS 1 - 3



TEMPLATES / CREATE JOB TEMPLATE

NEW JOB TEMPLATE

* NAME

DESCRIPTION

* JOB TYPE □ PROMPT ON LAUNCH
Choose a job type

* INVENTORY □ PROMPT ON LAUNCH

* PROJECT
RH Insights

* PLAYBOOK
ngnix-resolution-136ae8b9-18a8-45dc-9ab3-3695ccc9f763.yml

CREDENTIALS □ PROMPT ON LAUNCH

FORKS
0

LIMIT □ PROMPT ON LAUNCH

* VERBOSITY □ PROMPT ON LAUNCH
0 (Normal)

JOB TAGS □ PROMPT ON LAUNCH

SKIP TAGS □ PROMPT ON LAUNCH

LABELS

INSTANCE GROUPS

JOB SLICING
1

TIMEOUT
0

SHOW CHANGES □ PROMPT ON LAUNCH

OPTIONS
- □ ENABLE PRIVILEGE ESCALATION
- □ ENABLE PROVISIONING CALLBACKS
- □ ENABLE WEBHOOK
- □ ENABLE CONCURRENT JOBS
- □ ENABLE FACT CACHE

Red Hat Insights

Resources & Next Steps

Getting started with Red Hat Insights

ALREADY A RED HAT® ENTERPRISE LINUX® CUSTOMER?

You have Red Hat Insights at no additional cost:

https://access.redhat.com/insights/getting-started

WOULD YOU LIKE TO LEARN MORE ABOUT RED HAT INSIGHTS?

https://www.redhat.com/en/technologies/management/insights

For more info, visit: https://access.redhat.com/insights/info

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

Red Hat