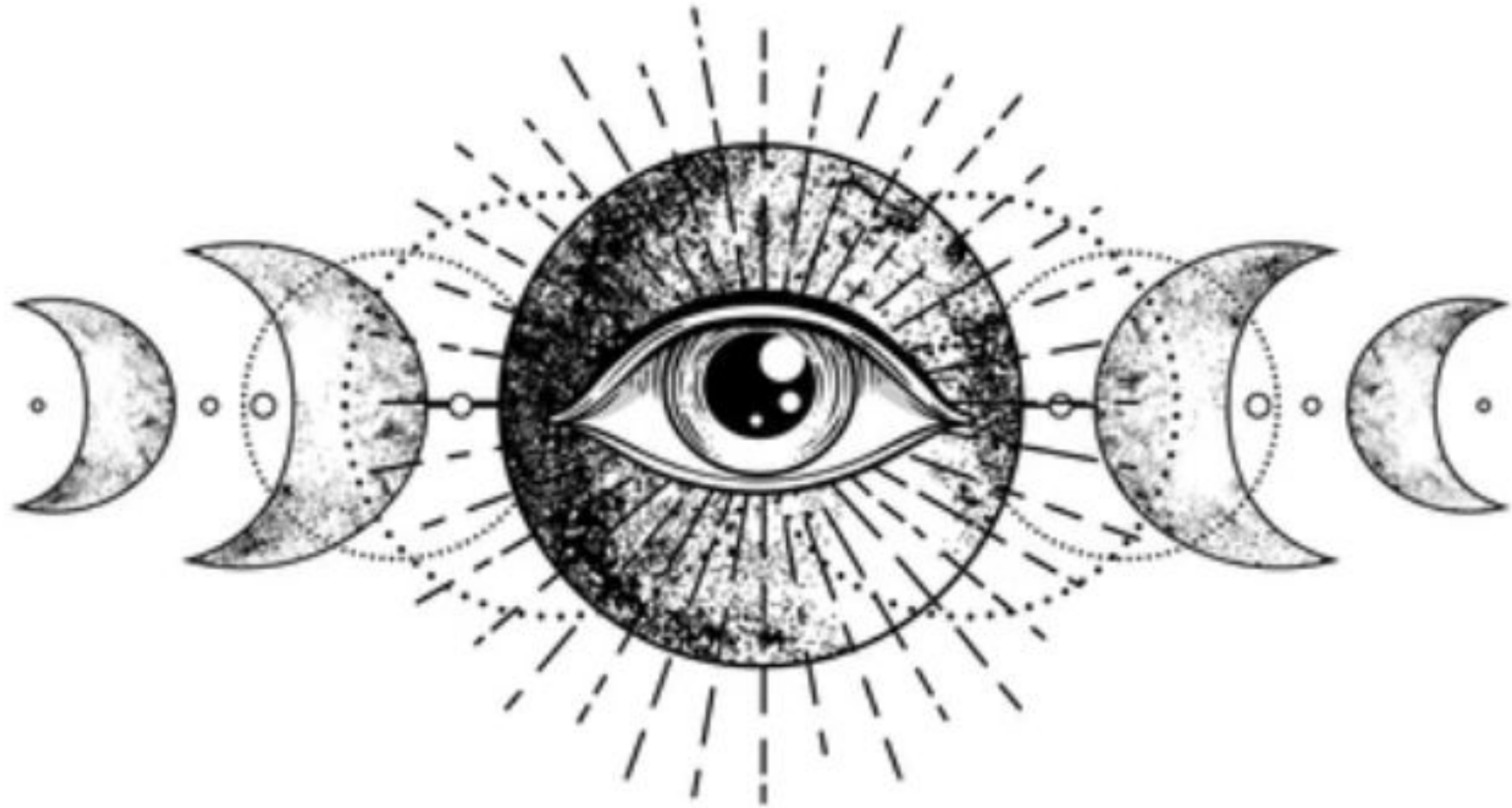**Red Hat Insights**

Red Hat Insights

for Red Hat Enterprise Linux
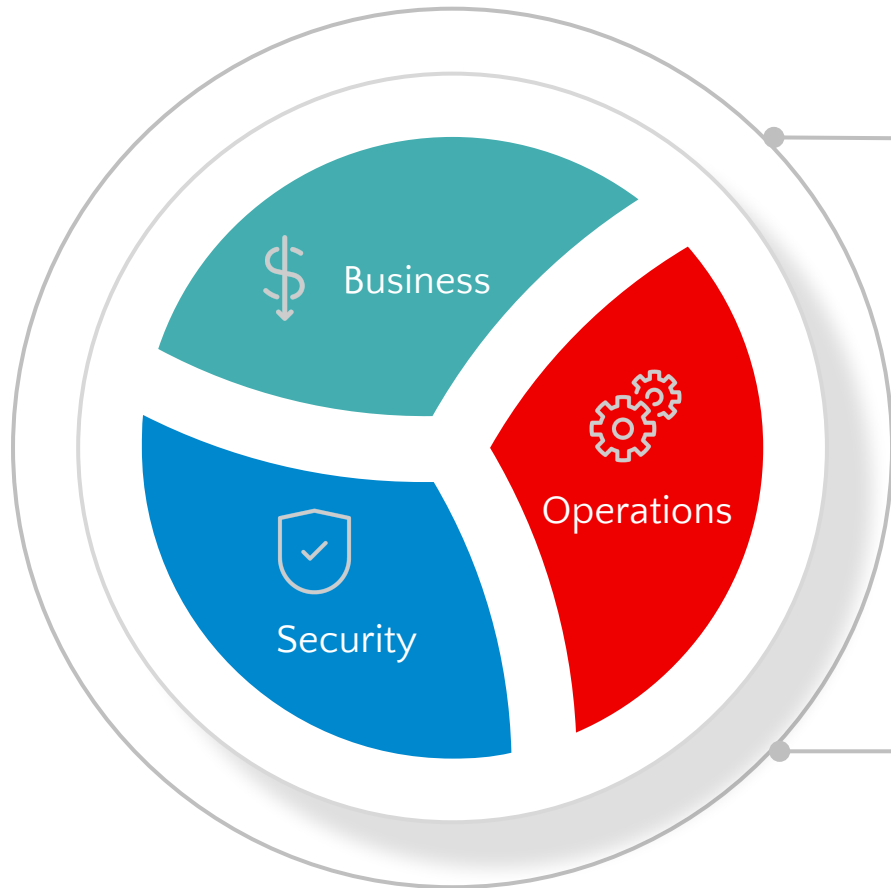
RHUG Edition

Alan Patrick
Solution Architect
alpatric@redhat.com

Red Hat
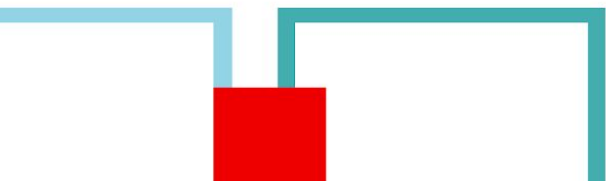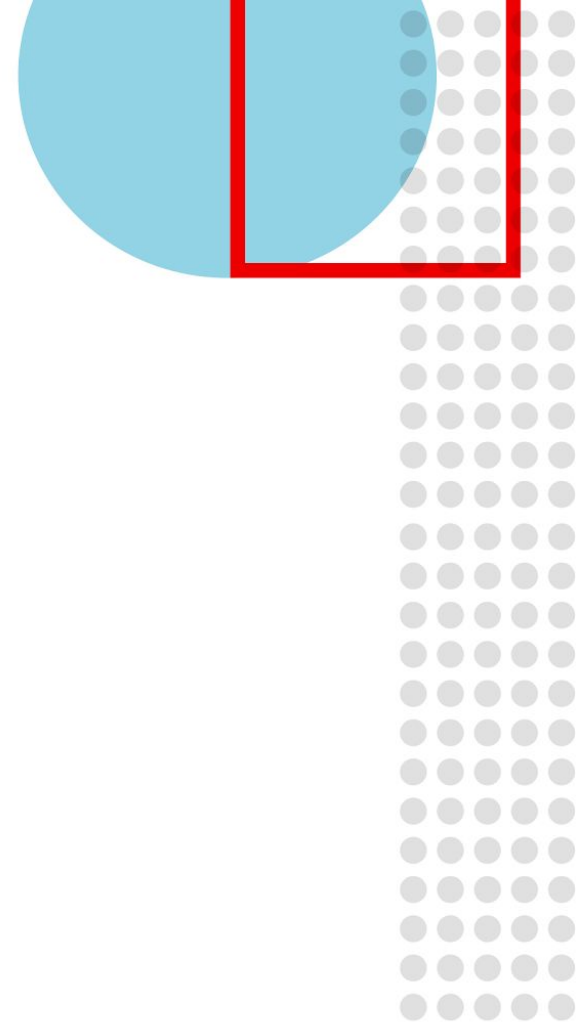
Red Hat
Insights

Business

Operations

Security

Track and optimize spend

Operations
Improve stability and performance

Security
Reduce vulnerability and compliance risks

Find and prioritize meaningful insights from your data so you can proactively take action.

Red Hat

How Insights Helps You

How much downtime can you afford?

What is the opportunity cost of your firefighting?
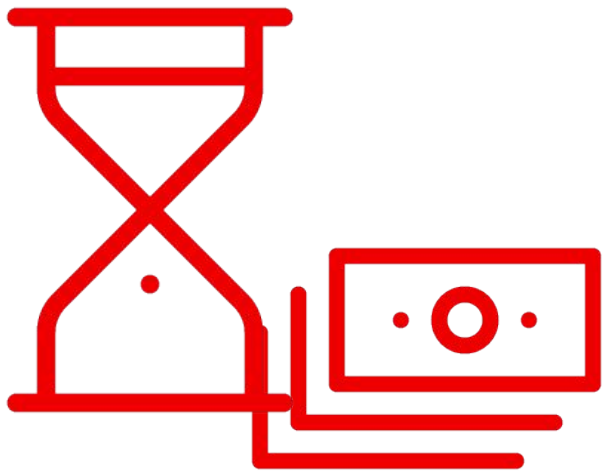
40% of enterprises say hourly downtime costs top $1 Million

98% of firms report costs of $100,000 per hour or more

Source: The Cost of IT Downtime and https://itic-corp.com/blog/2020/06/forty-percent-of-enterprises-say-hourly-downtime-costs-top-1million/

Red Hat

Why Red Hat Insights?

Operational Efficiency

Comprehensive analysis with Red Hat expertise

Continuous vulnerability alerts

Increased visibility to security risks

Simple remediation

Single, consistent management solution across on-premise, hybrid cloud, and public cloud.

Security Risk Management

Red Hat

Insights is included
with your Red Hat Enterprise Linux subscription.

Buy

Get

Red Hat
Enterprise Linux

Red Hat
Insights

for Red Hat Enterprise Linux

Add

Red Hat
Smart Management

Advanced management capabilities at scale available with optional subscription

Red Hat

Modernized management with analytics and automation

96% reduction in time to **detect** known risks to availability, performance, stability, and security

26% reduction in administrator steps to **detect** these known risks

88% less time to track **patch** status for all systems in environment, versus manual scripted workflow

1m 24s to **discover** vulnerabilities in a 100-VM environment, versus over 15m when performed manually

91% less task completion time to **address** a vulnerability

69% reduction in time to detect a **policy** violation

Three steps to advanced RHEL management

Register

Install client for Red Hat instances on-premises, virtual, cloud.

Get started steps
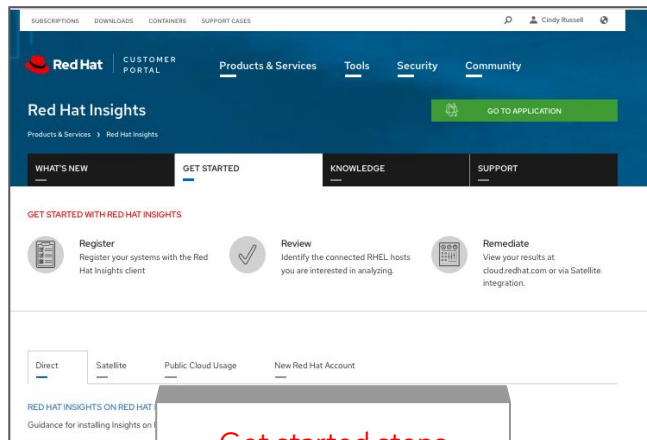
Review

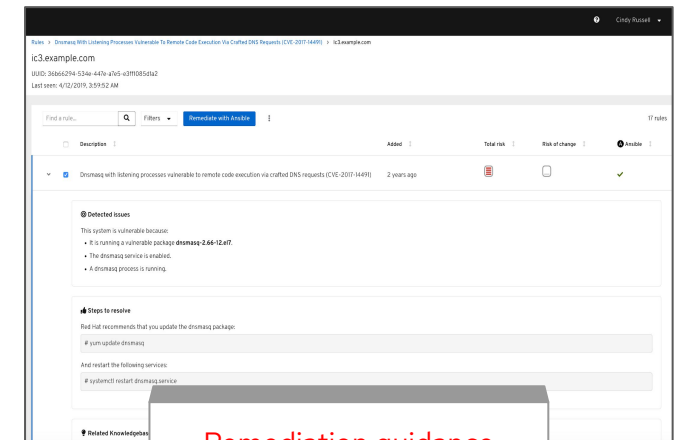Insights client runs and issues found are reported in the Insights dashboard at cloud.redhat.com

Browse results
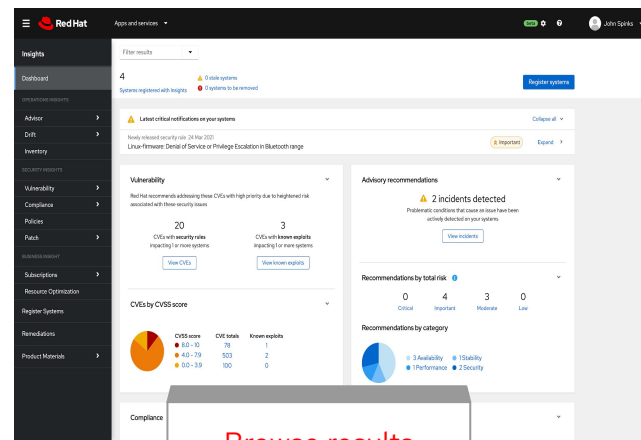
Remediate

Review issues and results in the dashboard and choose which you would like to remediate. Leverage guidance, and remediation options.

Remediation guidance

What kind of information will Insights for Red Hat Enterprise Linux give me?

Red Hat

☰

Apps and services ▾

Insights

Dashboard

OPERATIONS INSIGHTS

Advisor ❯

Drift ❯

Inventory

SECURITY INSIGHTS

Vulnerability ❯

Compliance ❯

Policies

Patch ❯

BUSINESS INSIGHT

Subscriptions ❯

Resource Optimization

Register Systems

Remediations

Product Materials ❯

Filter results ▾

4
Systems registered with Insights

⚠ 0 stale systems
🛑 0 systems to be removed

⚠ **Latest critical notifications on your systems**   Collapse all ▾

Newly released security rule 24 Mar 2021   ⚠ Important   Expand ❯
Linux-firmware: Denial of Service or Privilege Escalation in Bluetooth range

Vulnerability ▾

Red Hat recommends addressing these CVEs with high priority due to heightened risk
associated with these security issues

20   **3**
CVEs with **security rules**   CVEs with **known exploits**
impacting 1 or more systems   impacting 1 or more systems

View CVEs   View known exploits

CVEs by CVSS score ▾
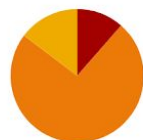
CVSS score	CVE totals	Known exploits
⬤ 8.0 – 10	78	1
⬤ 4.0 – 7.9	503	2
⬤ 0.0 – 3.9	100	0

Advisory recommendations ▾

⚠ **2 incidents detected**
Problematic conditions that cause an issue have been
actively detected on your systems

View incidents

Recommendations by total risk ⓘ ▾

0   **4**   **3**   **0**
Critical   Important   Moderate   Low

Recommendations by category

⬤ 3 Availability   ⬤ 1 Stability
⬤ 1 Performance   ⬤ 2 Security

Compliance ▾

No policies

Remediations ▾

Feedback

Red Hat

Apps and services ▾

- Helps you avoid unplanned downtime
- Recommendations to improve availability, performance, and stability issues that you may not be aware of.
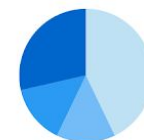- Gives you step-by-step resolution and Ansible playbooks

OPERATIONS INSIGHTS

Advisor ▾
- Recommendations
- Systems
- Topics

Drift ▸

Inventory

SECURITY INSIGHTS

Vulnerability ▸

Compliance ▸

Policies

Patch ▸

BUSINESS INSIGHT

Subscriptions ▸

Register Systems

Remediations

Product Materials ▸

Filter results ▾

Advisor recommendations

🔻 Name ▾ | Filter by name 🔍 | ⬈ | 1 – 10 of 116 ▾ ‹ ›

Systems impacted 1 or more ✕   Status Enabled ✕   Clear filters

Name ↕	Added ↓	Total risk ↕	Risk of ch... ↕	Systems ↕	Ⓐ Ansible ↕	
› System hangs on the boot when the problematic Intel CPU microcode is used by the Intel Skylake or Cascade Lake CPU	3 days ago	⌃ Important	Very Low	2	✅	⋮
› Yum and Subscription Manager commands will fail because the identity certificate has expired	24 days ago	⌃ Important	Very Low	1	No	⋮
› Incident The metadata of LVM will be out of sync with other members of the cluster when lvmetad is enabled or running with LVM resources configured and running on the other node	24 days ago	⌃ Important	Low	2	✅	⋮

Feedback

Red Hat

Apps and services ▾

- Simple to see what CVEs are impacting your hosts so you can prioritize what gets fixed
- Visibility into threat intelligence including publicly known exploits
- Helps you address CVEs with pre-built playbooks

Insights

Dashboard

OPERATIONS INSIGHTS

Advisor ›

Drift ›

Image Builder

Inventory

SECURITY INSIGHTS

Vulnerability ⌄

CVEs

Reports

Systems

Compliance ›

Policies

Patch ›

BUSINESS INSIGHT

Subscriptions ›

Register Systems

Filter results ▾

CVEs

☐ ▾ | 🗚 Known ex... ▾ | Filter by Known exp... ▾ | ↖ | ⋮ | 1 - 17 of 17 ▾ ‹ ›

Systems exposed 1 or more ✕   Known exploit Has a known exploit ✕   **Clear filters**

	CVE ID	Publish date ↓	Severity	CVSS base score	Systems exposed	Business risk	Status	
› ☐	CVE-2021-3156 Known exploit Security rule	26 Jan 2021	⚠ Important	7.8	118	Not defined	Not reviewed	⋮
› ☐	CVE-2020-9850 Known exploit	09 July 2020	⚠ Moderate	9.8	30	Not defined	Not reviewed	⋮
› ☐	CVE-2019-13272 Known exploit Security rule	15 July 2019	⚠ Important	7.8	4	Not defined	Not reviewed	⋮
› ☐	CVE-2019-9213 Known exploit	26 Feb 2019	⚠ Important	5.5	5	Not defined	Not reviewed	⋮
› ☐	CVE-2018-17456 Known exploit	04 Oct 2018	⚠ Important	8.8	1	Not defined	Not reviewed	⋮
› ☐	CVE-2018-16509 Known exploit	20 Aug 2018	⚠ Important	7.3	2	Not defined	Not reviewed	⋮
› ☐	CVE-2018-1111	15 May 2018	⚠ Critical	7.5	4	Not defined	Not reviewed	

Feedback

Red Hat Enterprise Linux

Monitor your Red Hat Enterprise Linux usage by physical, virtual,

Usage ▼   Filter by usage ▼

CPU socket usage

Daily ▼

April 5
- Physical RHEL   70
- Virtualized RHEL   9
- Public cloud   17
- Subscription threshold 144

■ Physical RHEL   ■ Virtualized RHEL   ■ Public cloud   ---- Subscription threshold

Current systems

Filter by name 🔍   1 - 27 of 27 ▼   ‹ ›

Name	Type	Subscribed sockets	Last seen
ip-172-17-0-120.auroracloud.com	Virtual	1	11 days ago
azure-2.example.com	Public cloud Azure	1	4 days ago

Left navigation:
- Advisor
- Drift
- Inventory

SECURITY INSIGHTS
- Vulnerability
- Compliance
- Policies
- Patch

BUSINESS INSIGHT
- Subscriptions ▼
  - All RHEL
  - ARM
  - IBM Power
  - IBM Z Systems
  - X86
  - OpenShift Subscriptions
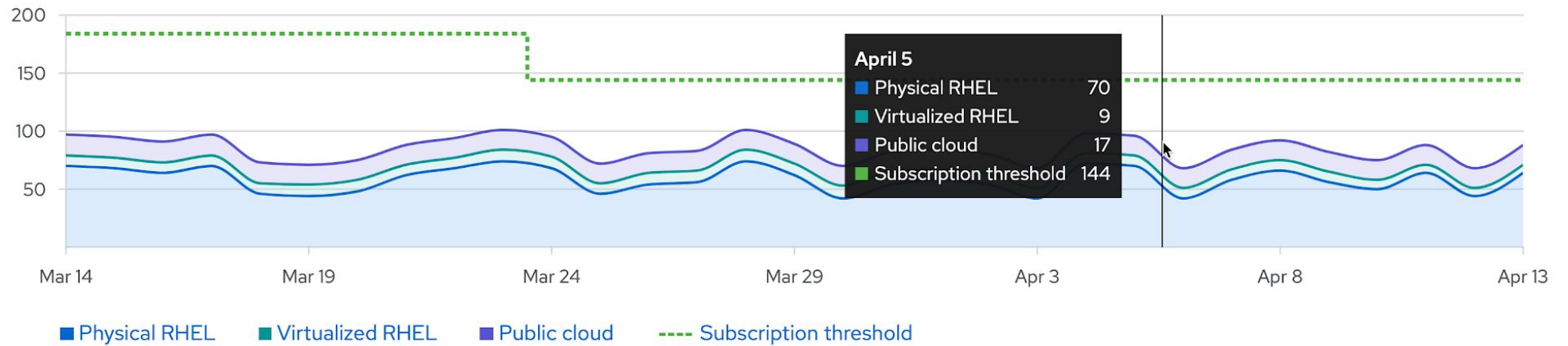 - Subscriptions Documentation ⧉
- Register Systems
- Remediations

Apps and services ▼

Feedback

Subscriptions [Business]

- Simple to see subscription utilization across your account
  - How much are you consuming?
  - Where are you consuming it?
  - Do you need to buy more?

3 ways to fix what Insights finds

With and without Red Hat Smart Management

How to fix what Insights finds

3 easy ways to remediate the issues that Insights detects

1. Insights only: Download playbooks and run with Ansible

2. Insights and Smart Management - Remediate via Cloud Connector with Red Hat connector

3. Insights and Smart Management - Remediate via Cloud Connector with Satellite

#1 – Insights standalone

Insights can create a playbook for many common issues that it finds.
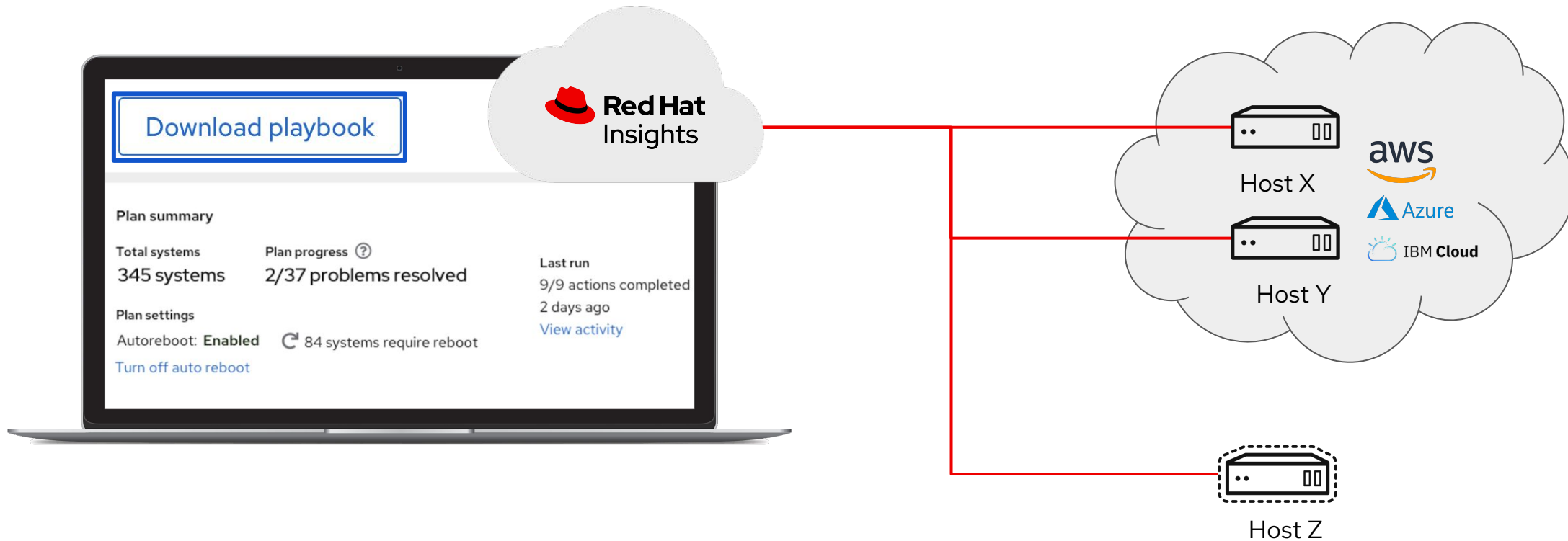
Insights

Dashboard

Advisor

Vulnerability

Compliance

Patch

Drift

Policies

Inventory

Remediations

Register Systems

Subscription Watch

Product Materials

John Spinks

Filter results

Remediations > SUDO_Fix

SUDO_Fix

Execute playbook   Download playbook

0/1
Issues resolved

Total systems

20 systems

Autoreboot

✓ Enabled   Turn off

ⓘ **Do more with your Find it Fix it capabilities**

Configure your systems with Cloud Connector to fix systems across all your Satellite instances.

Learn how to configure

✕

Actions   Activity
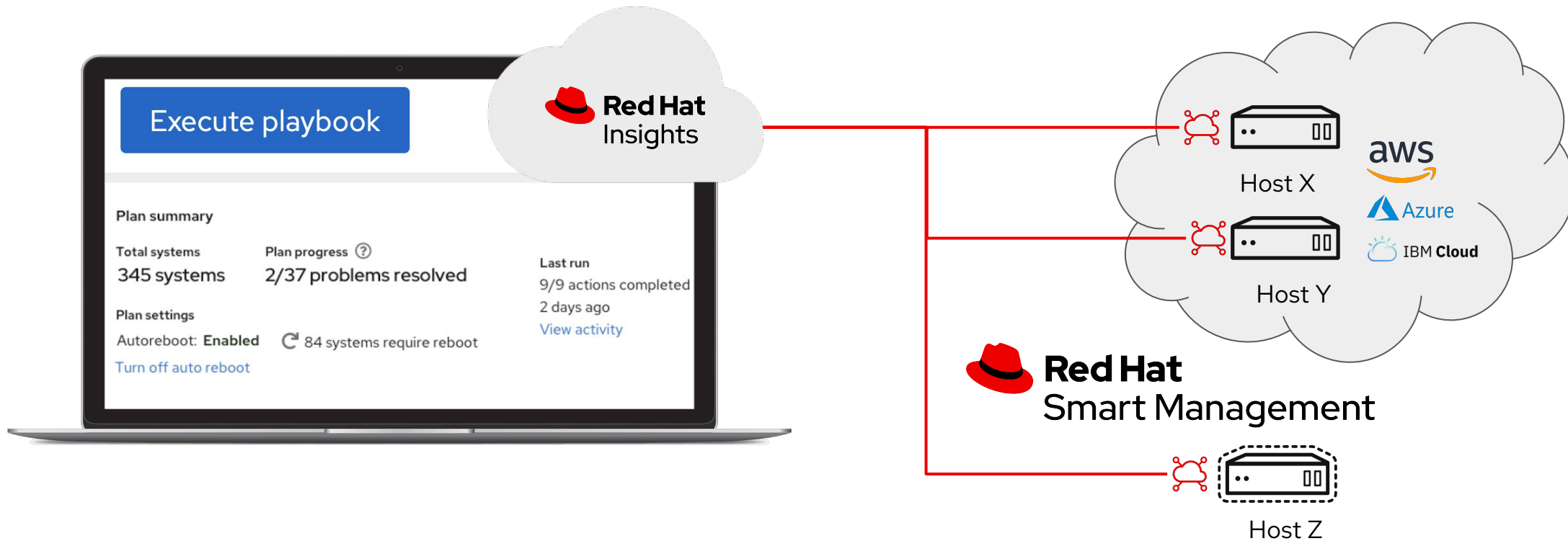
☐ ▼   Search 🔍   Remove action   1 - 1 of 1 ▼   ‹   ›

#2 - Insights and Smart Management

Enable Cloud Connector through Red Hat connector to fix issues that Insights finds*

*Requires use of Red Hat connector - Tech Preview in Red Hat Enterprise Linux 8.4

Red Hat

Dashboard

OPERATIONS INSIGHTS

Advisor

Drift

Image Builder

Inventory

SECURITY INSIGHTS

Vulnerability

Compliance

Policies

Patch

BUSINESS INSIGHT

Subscriptions

Register Systems

Remediations

Product Materials

Filter results

Remediations > SUDC

SUDO_Fix

te playbook   Download playbook

0/

Issues res

Actions   Activi

Execute playbook

Playbook contains **1 action** affecting **20 systems.**

Systems connected to a Satellite instance and configured with Cloud Connector can be automatically remediated. To remediate other systems, download the Ansible Playbook.

Connection status of systems

Connection type	Syste...	Connection status
opendemo.usersys.redha...	1	✔Ready
vm255-93.gsslab.pnq2.r...	1	✔Ready
wallsat67.usersys.redh...	1	✔Ready
Direct connection	9	Cannot remediate – Direct connection. Connect your systems to Satellite to automatically remediate. Learn how to connect

Search

Actions ↑

CVE_2021_315
Fix issues caus
Edit

1–1 of 1

Type   Status

Vulnerability   11/20 remediated

| Execute playbook on 3 systems | Download playbook |

Feedback

#3 - Red Hat Smart Management and Cloud Connectivity

Smart Management subscription enables push-button remediation of issues identified by Insights, with and without Satellite

Execute playbook

Plan summary

Total systems
345 systems

Plan progress ⓘ
2/37 problems resolved

Last run
9/9 actions completed
2 days ago
View activity

Plan settings
Autoreboot: **Enabled**   ↻ 84 systems require reboot
Turn off auto reboot

Red Hat Insights

Cloud Connector

Satellite

Capsule I

Capsule II

Host A

Host B

Host C

Host D

Host X

Host Y

aws

Azure

IBM **Cloud**

Red Hat
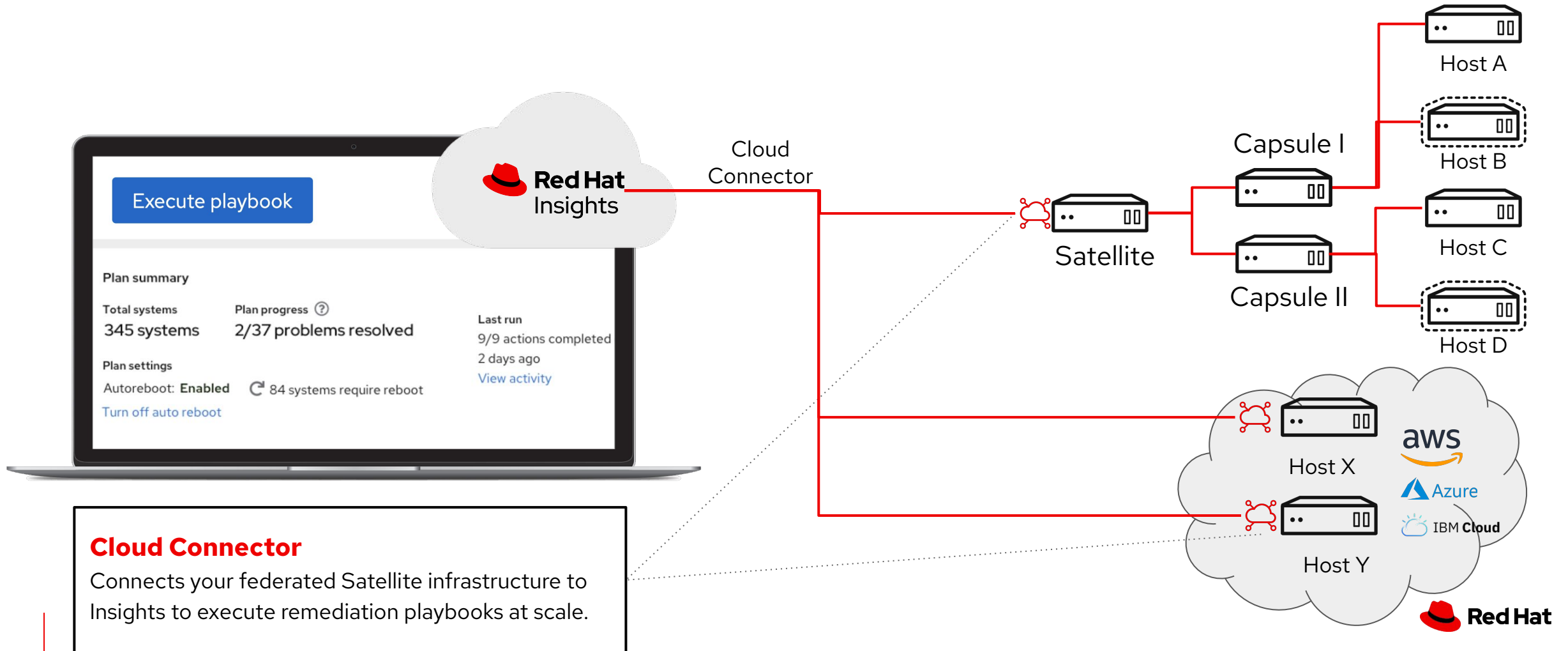
Cloud Connector
Connects your federated Satellite infrastructure to Insights to execute remediation playbooks at scale.

Dashboard

OPERATIONS INSIGHTS

Advisor

Drift

Image Builder

Inventory

SECURITY INSIGHTS

Vulnerability

Compliance

Policies

Patch

BUSINESS INSIGHT

Subscriptions

Register Systems

Remediations

Product Materials

Filter results

Remediations > SUDO_

SUDO_Fix

0/1

Issues res

Actions   Activit

Actions ↑

CVE_2021_315
Fix issues caus
Edit

Execute playbook ✕

Playbook contains **1 action** affecting **20 systems.**

Systems connected to a Satellite instance and configured with Cloud Connector can be automatically remediated. To remediate other systems, download the Ansible Playbook.

Connection status of systems

Connection type	Syste...	Connection status
opendemo.usersys.redha...	1	✅Ready
vm255-93.gsslab.pnq2.r...	1	✅Ready
wallsat67.usersys.redh...	1	✅Ready
Satellite 5fbc5298-199...	8	✅Ready
Direct connection	9	Cannot remediate – Direct connection. Connect your systems to Satellite to automatically remediate. Learn how to connect

Execute playbook on 11 systems   Download playbook

playbook   Download playbook

1–1 of 1

ulnerability   11/20 remediated

Status

You control the data

Red Hat

Four things you should know about data collection in Insights

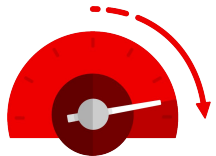**It's Granular - And Sortable**

**No PIN/PII
(GDPR in Mind!)**

No Raw Logs

**Encrypted from
Source to Service**

More information here: https://cloud.redhat.com/security/insights

Red Hat

Red Hat Insights Use Cases

Key use cases

Uptime and efficiency

- Frees time for admins to add value elsewhere
- Consolidate operations teams
- Always forward

Security

- Keep up with vulnerabilities
- Harden infrastructure proactively
- Proactively address CVEs

Insights combines with other tools to enhance the Red Hat Enterprise Linux investment.

Insights + technical account manager (TAM) encourages deeper customer conversations and delivers regular assessments.

Insights + Satellite identifies and prioritizes risks and patches so customers can resolve issues faster

How to configure Red Hat Insights
for Red Hat Enterprise Linux

Red Hat

Installation and registration

Simple and Straightforward

Step #1: Run # `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 # `insights-client --register`

Step #3 See results at cloud.redhat.com and Remediate.

More information including automation playbooks are available at:
- ○ https://access.redhat.com/insights/getting-started

Top 3 Insights Concerns

**I can't use
Software-as-a-Service (SaaS).**

Often we find that SaaS is already being used.
Services like Salesforce, ServiceNow, and New Relic are often deployed as SaaS.

Hostname / IP are sensitive, and we are concerned about sharing information about our systems.

All data is encrypted in transit AND at rest, and you can easily redact that further.

I am located in <LOCATION>, and can't use Insights.

Many regions have restrictions around citizen data storage, e.g., GDPR, but these types of laws are unrelated to the type of data Insights collects.

Red Hat

Top 3 Insights Data Collection Concerns

At a high level, what information does Insights collect?

Red Hat Insights Security Information article:

https://cloud.redhat.com/security/insights

How can my Security team review the actual Insights collection?

Generate a collection and inspect it in detail. Follow instructions in this article:

System Information Collected by Red Hat Insights

https://red.ht/2yPlWsH

How can I redact information from the Insights collection?

See article on Obfuscating IP Addresses and Host Names in Red Hat Insights

https://red.ht/2KebCgB

For more complicated redaction, refer to the: Use a YAML-style denylist Knowledgebase article:

https://red.ht/36lo6gB

Resources & Next Steps

Red Hat

Red Hat Insights:

Additional resources and next steps

Already a Red Hat Enterprise Linux user?

You have Red Hat Insights at no additional cost:

https://red.ht/insights_start

Would you like to learn more about Red Hat Insights?

https://redhat.com/insights

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

Refer to the Insights webinar library

Replays and upcoming webinars from this series

bit.ly/insights_webinarlibrary

▸ Watch the **intro video**.

▸ Read the **Insights blog**.

Red Hat

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

Red Hat

Agenda

- How Insights Helps You
- What kind of information will Insights for Red Hat Enterprise Linux give me?
- 3 ways to fix what Insights finds (with and without Smart Management)
- You control the data
- Insights Use Cases
- What's New in Red Hat Insights
- Insights Services
- Insights Customers
- How to Configure Red Hat Insights
- Common Questions
- Resource and Next Steps