

Red Hat Insights

Mitigate Risk & Proactively Manage Your Infrastructure

William Nix

Technical Product Marketing Manager
Red Hat Management Business Unit

Will Nix @ Red Hat



Public Sector Information Systems Management

- Reduce complexity in hybrid secure environments
- Automate workflow and streamline management

Red Hat Strategic Customer Engagement

- Work closely with customers like you
- Design and implement proactive solutions for some of the largest deployments in the world

Red Hat Insights

- Develop service used for predictive and prescriptive analytics on infrastructure

Insights Lab Hench-helpers

The team will be assisting you during this lab. If you need assistance, grab our attention by raising your hand or calling us out by name.

Chris Henderson, Insights Rules Product Manager

Rex White, Insights Senior Software Engineer

Summit Labs made possible by Red Hat Training

Check out Red Hat's online and classroom based labs and exams!

LAB OBJECTIVES

1. Register SERVERA, SERVERB, SERVERC, SERVERD to Insights.
2. Login to Satellite and use Insights interface
3. USE Lab Manual PDF on Desktop for instructions or if you get lost.
4. Ask Will, Rex, or Chris for help by raising hand.
5. After registering and identifying risks in demo environment, resolve all issues leading to ZERO actions for your POD.

ANALYZING INFRASTRUCTURE RISK

RESPONSE - Are you confident that you can quickly respond when vulnerabilities strike?

TOOLS - Are you comfortable that your tooling and processes will scale as your environment scales?

COMPLIANCE - Are you certain that your systems are compliant with various audit requirements such as PCI, HIPAA, SOX, DISA STIG, etc?

WHY WE BUILT A NEW PRODUCT

COMPLEXITY IS RISK

80%

Carnegie
Mellon
University

Commercial application
outages are caused by
software failure and
operational complexity.

COMPLEXITY IS RISK

80%

Carnegie
Mellon
University

Commercial application outages are caused by software failure and operational complexity.

336^{k/hr}

Gartner®

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

COMPLEXITY IS RISK

80%

Carnegie
Mellon
University

Commercial application outages are caused by software failure and operational complexity.

336^{k/hr}

Gartner®

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

65%

CompTIA®

Customers thought they were behind in training and capabilities needed to manage their next gen infrastructure.

**DO NOT
BECOME
A STATISTIC**

WE CANNOT
JUST THROW PEOPLE AT THE PROBLEM,
WE NEED
TECHNOLOGY

THIS LAB WILL FOCUS ON:

Risk Analysis and Response Methodology with Insights

Registering Insights Client to a Demonstration Only Lab Environment:

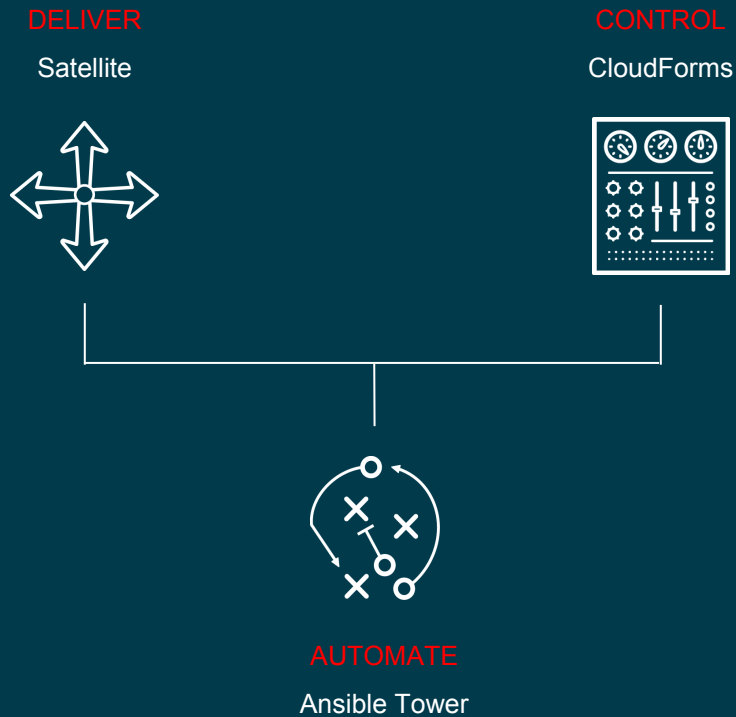
Satellite 6, RHEL 6 & 7, Custom Red Hat Insights Service

Understanding how the Insights Service is able to provide information

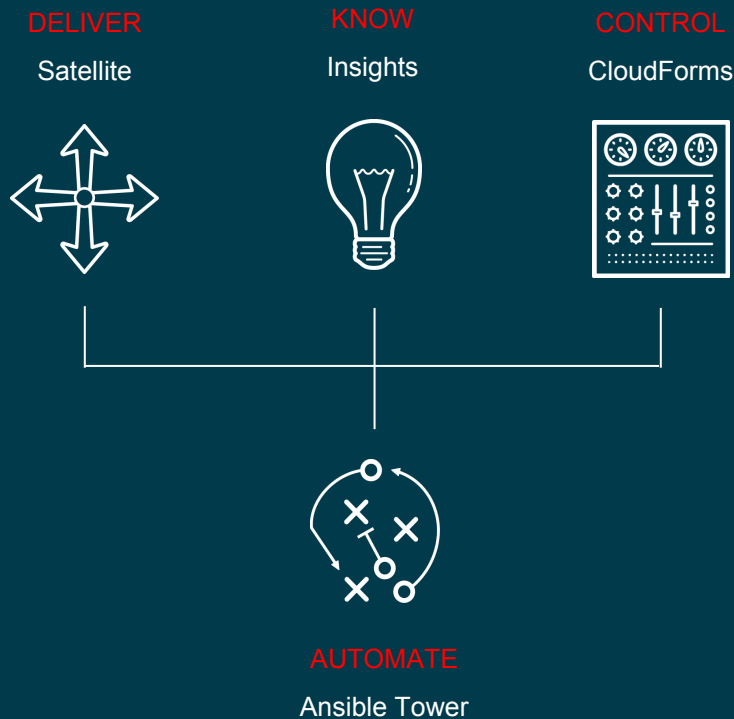
Using the Insights Service to proactively identify risk

& Reactive situations

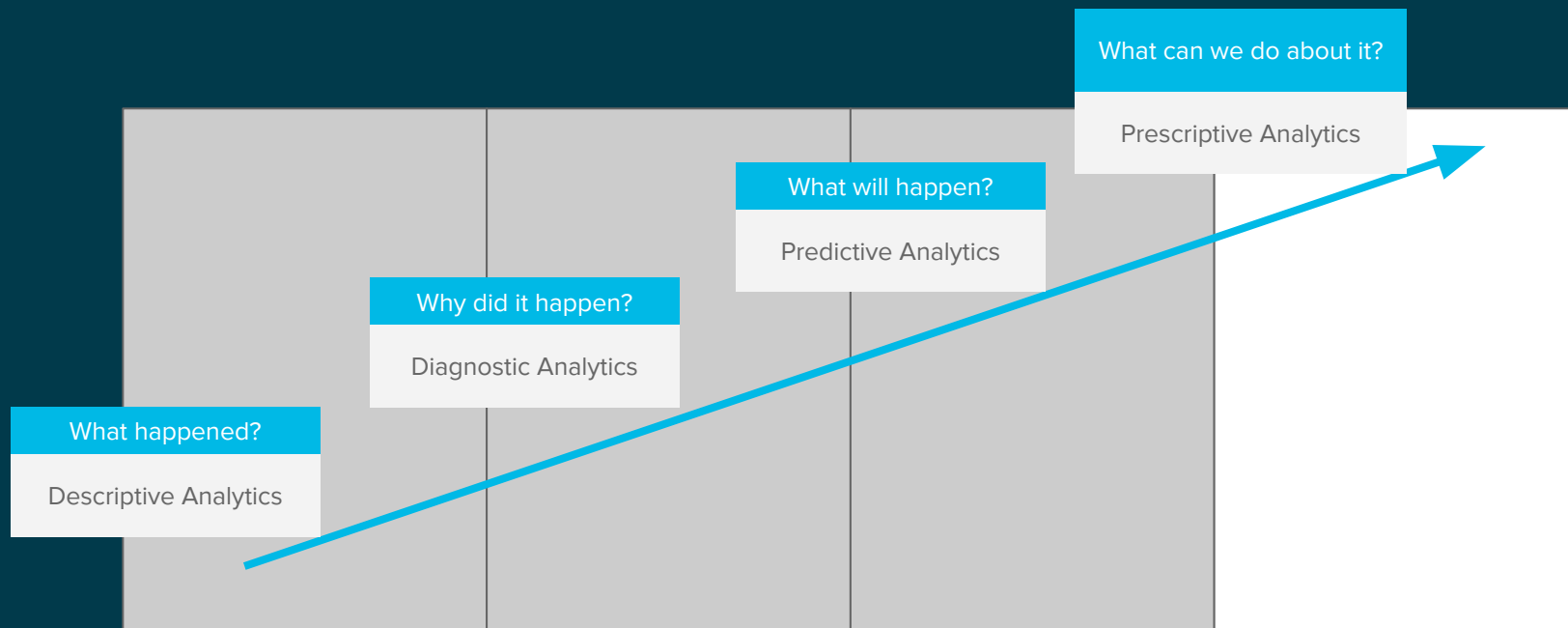
THE OPEN MANAGEMENT PLATFORM



INSIGHTS LETS YOU **KNOW** FASTER SO YOU CAN *FIX THINGS FASTER*

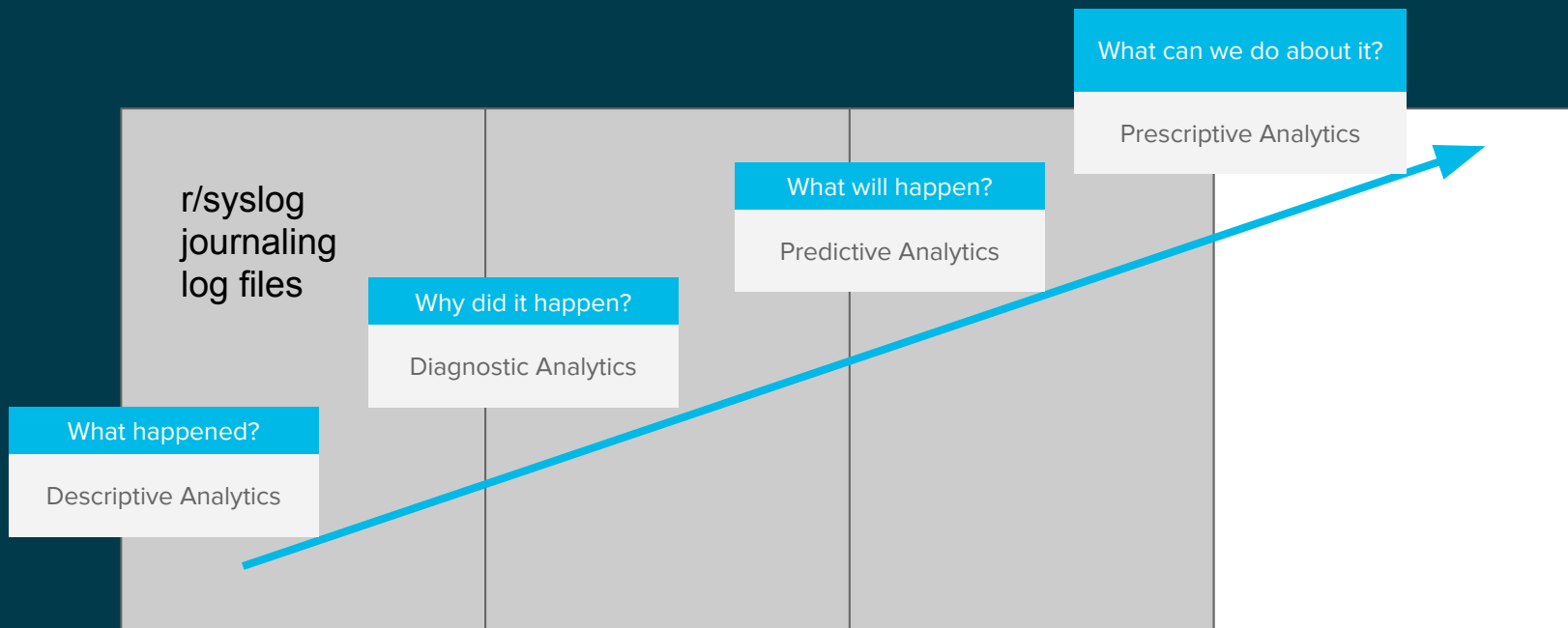


IT OPERATIONAL ANALYTICS



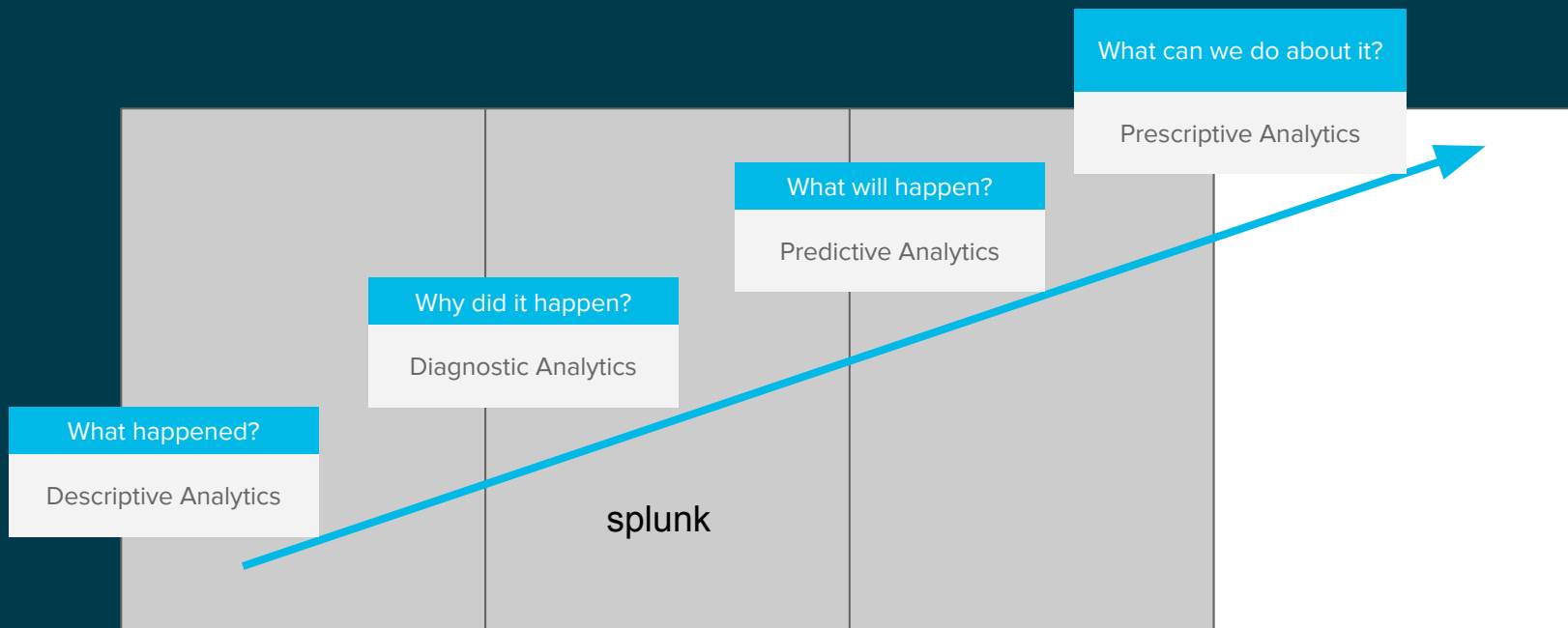
Gartner®

IT OPERATIONAL ANALYTICS



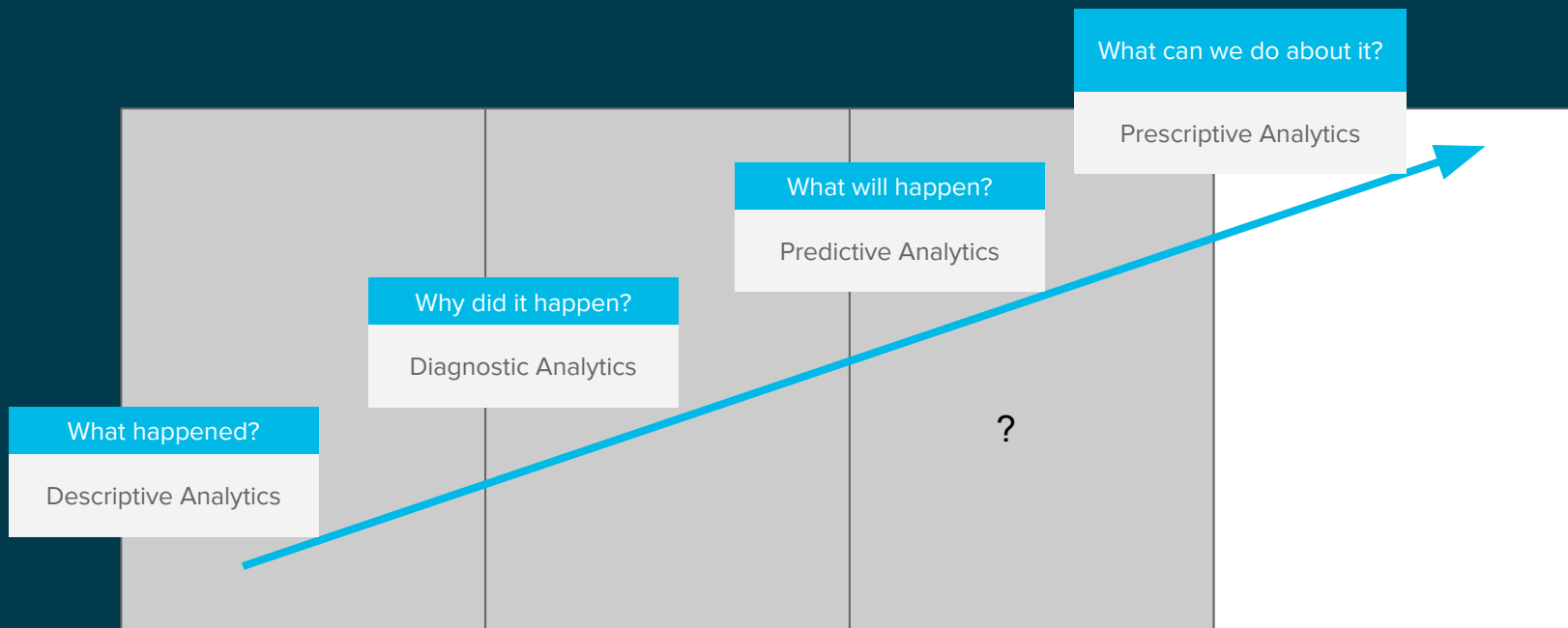
Gartner®

IT OPERATIONAL ANALYTICS



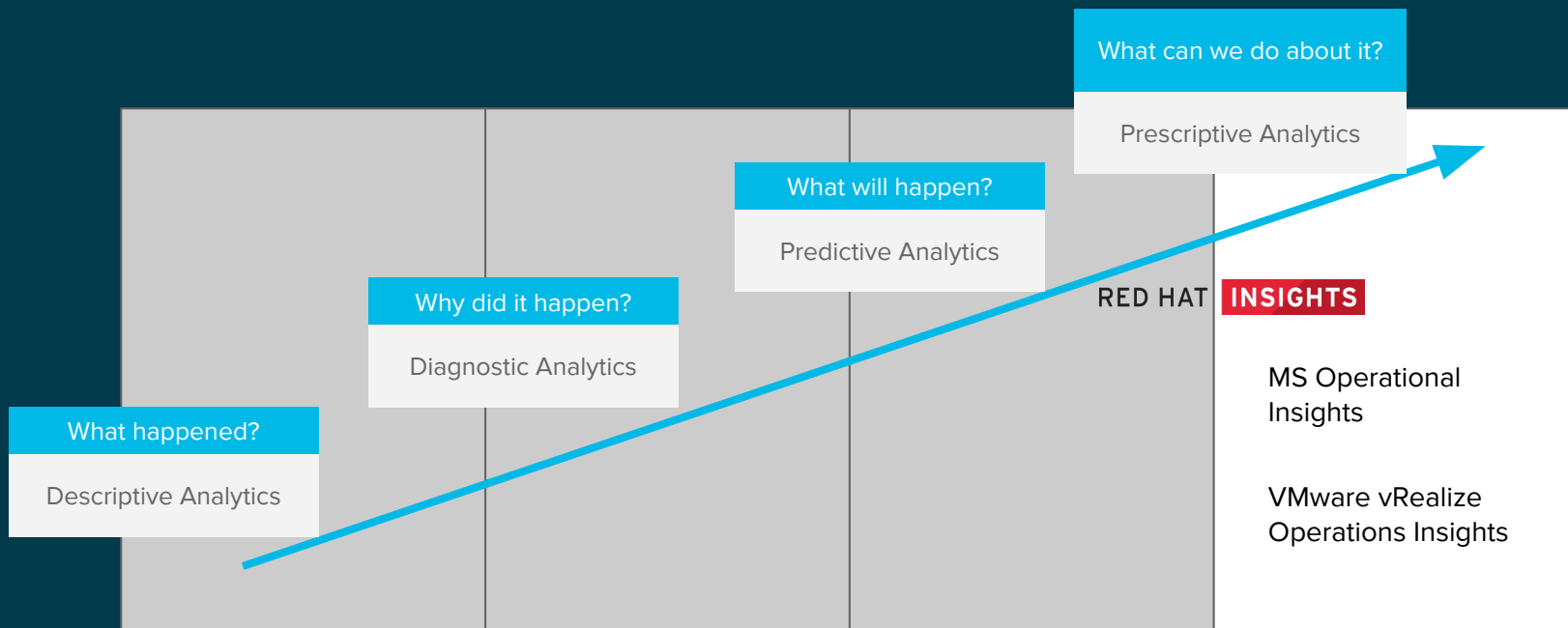
Gartner®

IT OPERATIONAL ANALYTICS



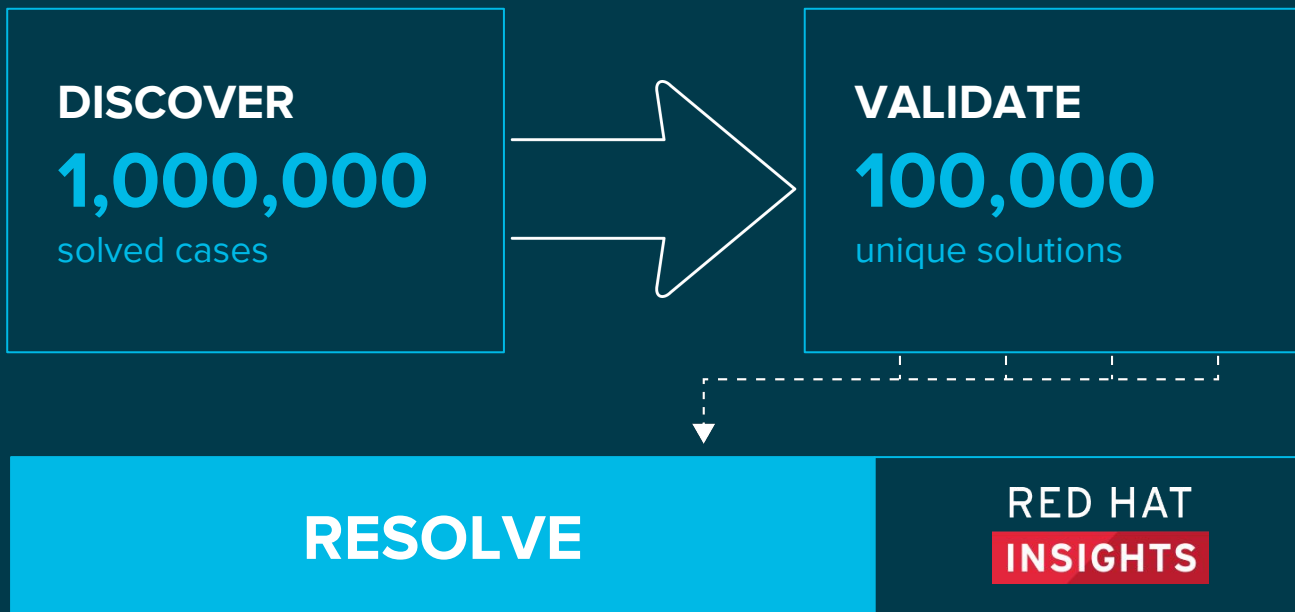
Gartner®

IT OPERATIONAL ANALYTICS

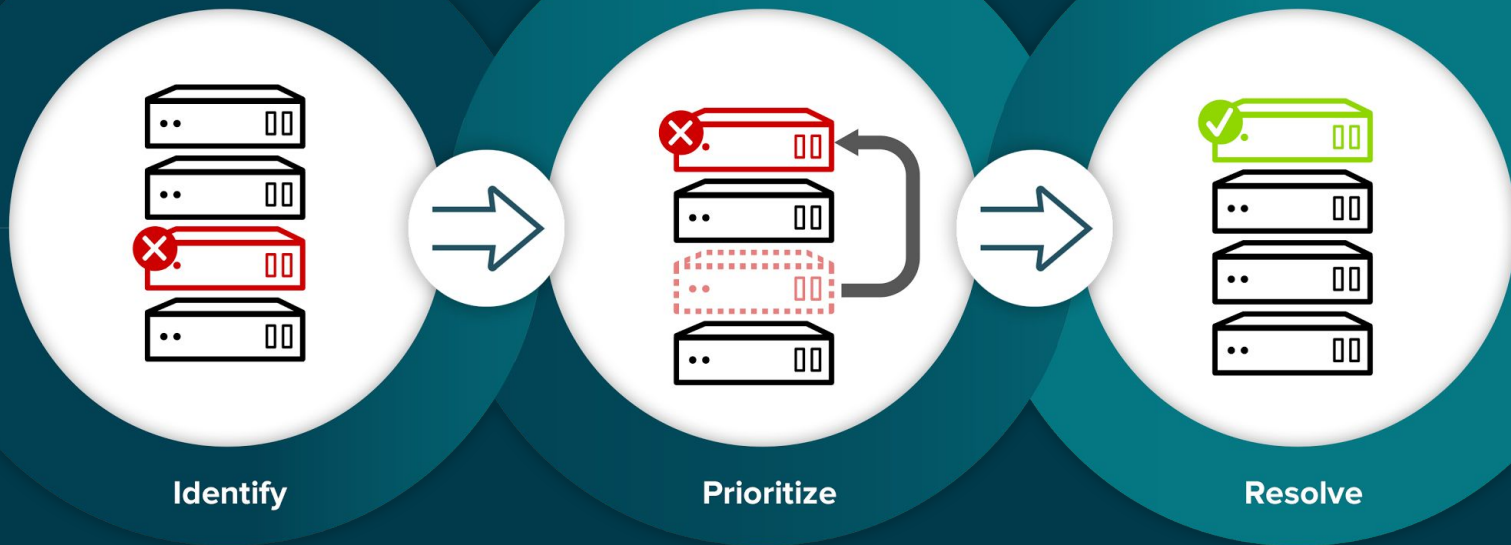


Gartner®

UNIQUE ENTERPRISE EXPERTISE



MANAGING INFRASTRUCTURE RISK



VERIFIED RESOLUTION STEPS AND SUPPORT RESOURCES

to help you respond to immediate issues and prevent future issues



Stability > MCE kernel panic

DETECTED ISSUE

- ---
- ---
- ---

STEPS TO RESOLVE



Related Knowledgebase articles

HOW INSIGHTS WORKS

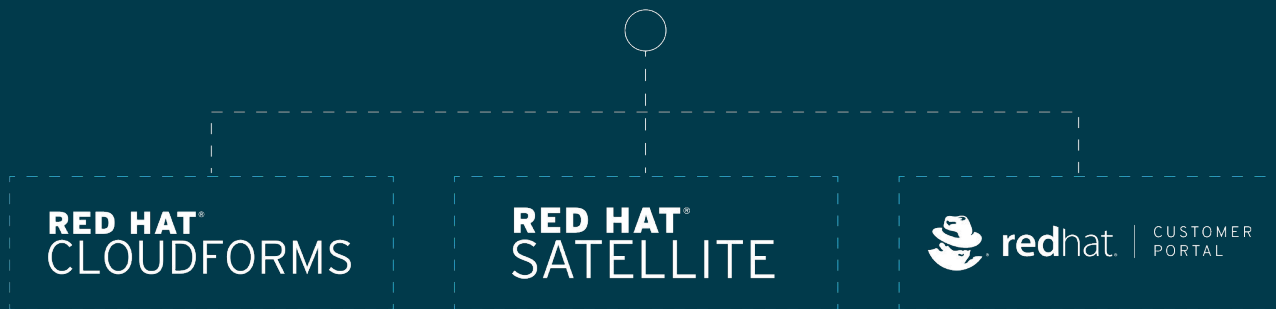
MODERN SYSTEMS MANAGEMENT

Red Hat Insights (RHI) is based on four main concepts:

- Proactive Systems Management
- Insights Powered By Red Hat
- Lightweight Data Collection
- Clear, Tailored, and Actionable Intelligence

INTEGRATED INTO TOOLS YOU ALREADY USE

RED HAT **INSIGHTS**



FULL STACK ANALYSIS



splunk>

Chelsio
Communications
Accelerate

lenovo

intel

AMD

FUJITSU

ORACLE

QUALCOMM

SOLARFLARE

hp

BROADCOM

IBM

EMULEX
An Avago Technologies Company

DELL



Microsoft

NEC

vmware

EMC²

HITACHI
Inspire the Next

Mellanox
TECHNOLOGIES

CISCO

DEMO



REAL WORLD RESULTS

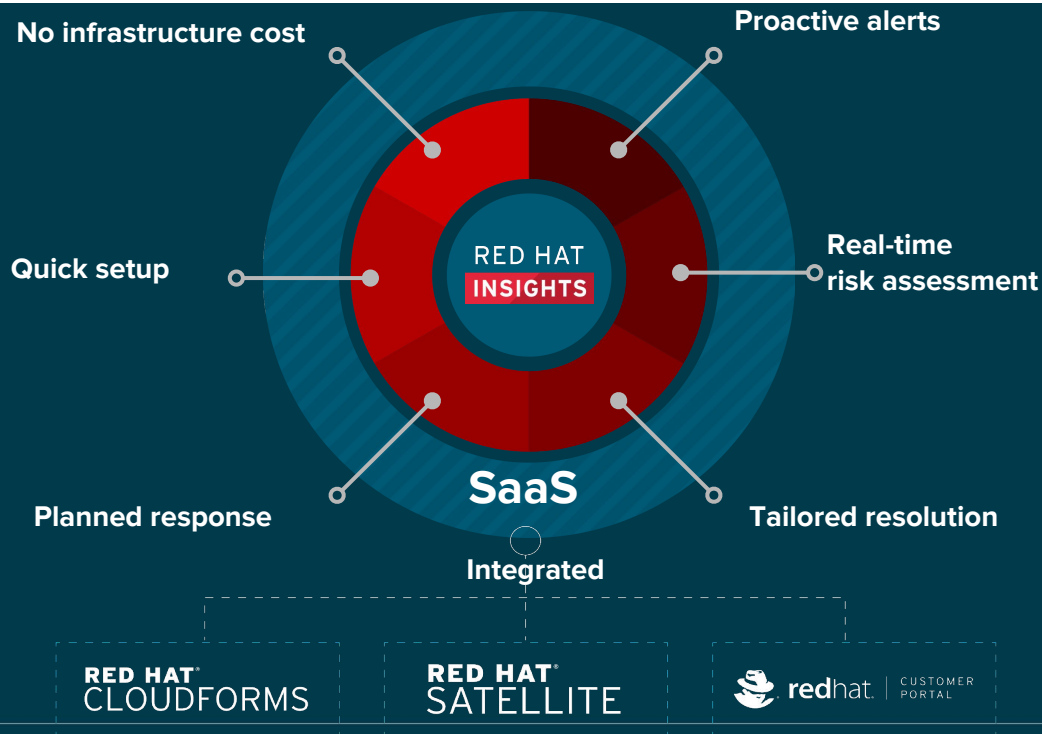
“Insights helps our teams be more proactive at resolving critical issues before they occur. The reliability of Insights saves us time and labor intensive tasks.

We no longer have to look at individual systems because we have one system with insight into our entire infrastructure.”

-- Jason Cornell, AutoTrader / Cox Automotive

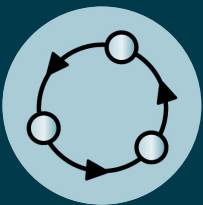
RED HAT® INSIGHTS

Operational analytics from Red Hat empowers you to prevent downtime and avoid firefighting while responding faster to new risks.

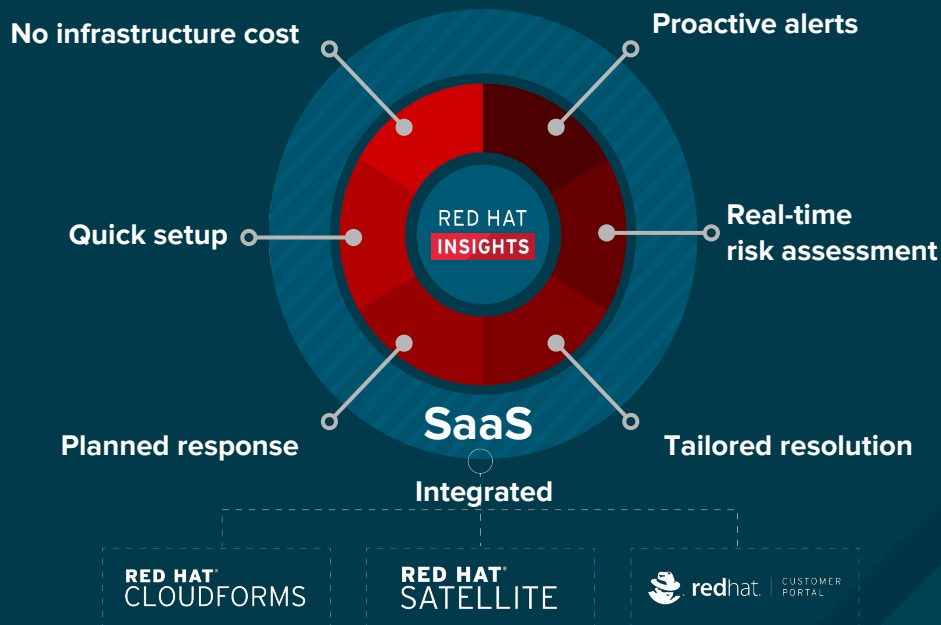


RED HAT® INSIGHTS

Operational analytics from Red Hat empowers you to prevent downtime and avoid firefighting while responding faster to new risks.

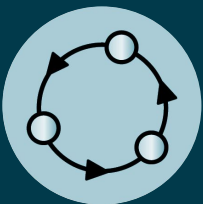


**MOVES YOU FROM REACTIVE
TO PROACTIVE SYSTEMS
MANAGEMENT**

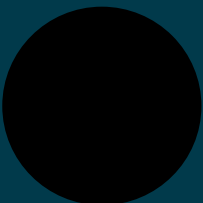


RED HAT® INSIGHTS

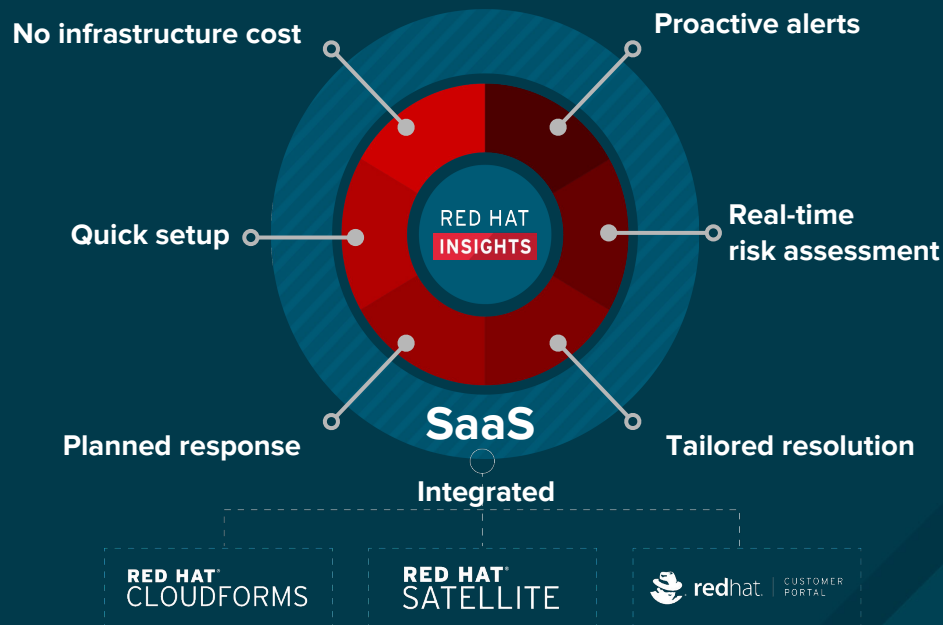
Operational analytics from Red Hat empowers you to prevent downtime and avoid firefighting while responding faster to new risks.



**MOVES YOU FROM REACTIVE
TO PROACTIVE SYSTEMS
MANAGEMENT**

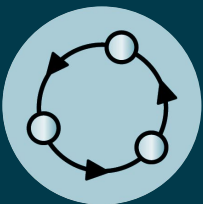


**DELIVERS ACTIONABLE INTELLIGENCE
FROM THE OPEN SOURCE LEADER**

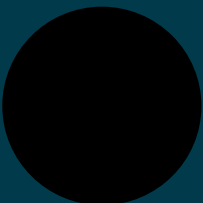


RED HAT® INSIGHTS

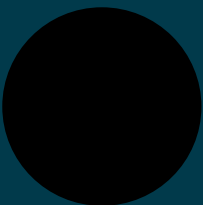
Operational analytics from Red Hat empowers you to prevent downtime and avoid firefighting while responding faster to new risks.



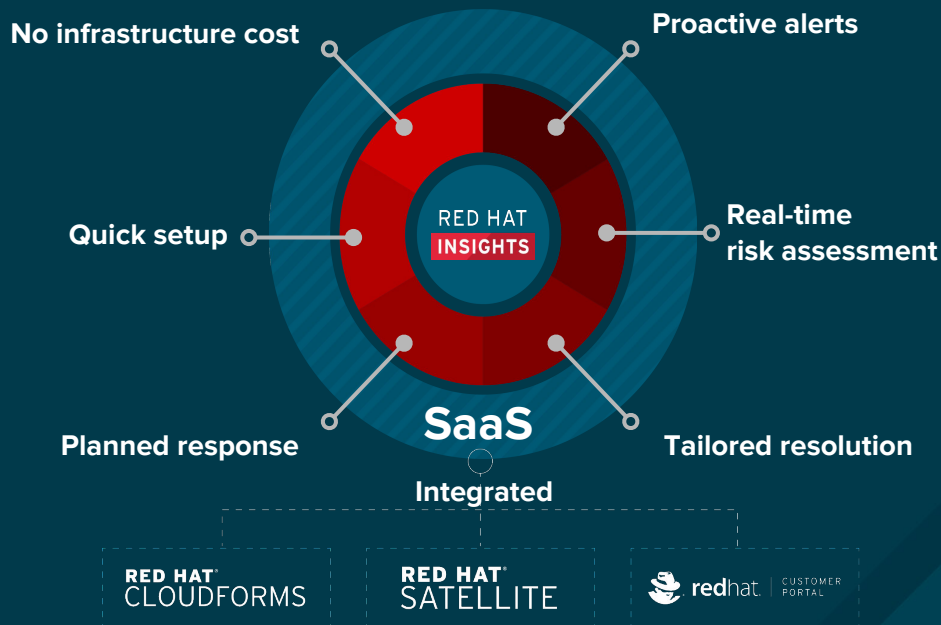
**MOVES YOU FROM REACTIVE
TO PROACTIVE SYSTEMS
MANAGEMENT**



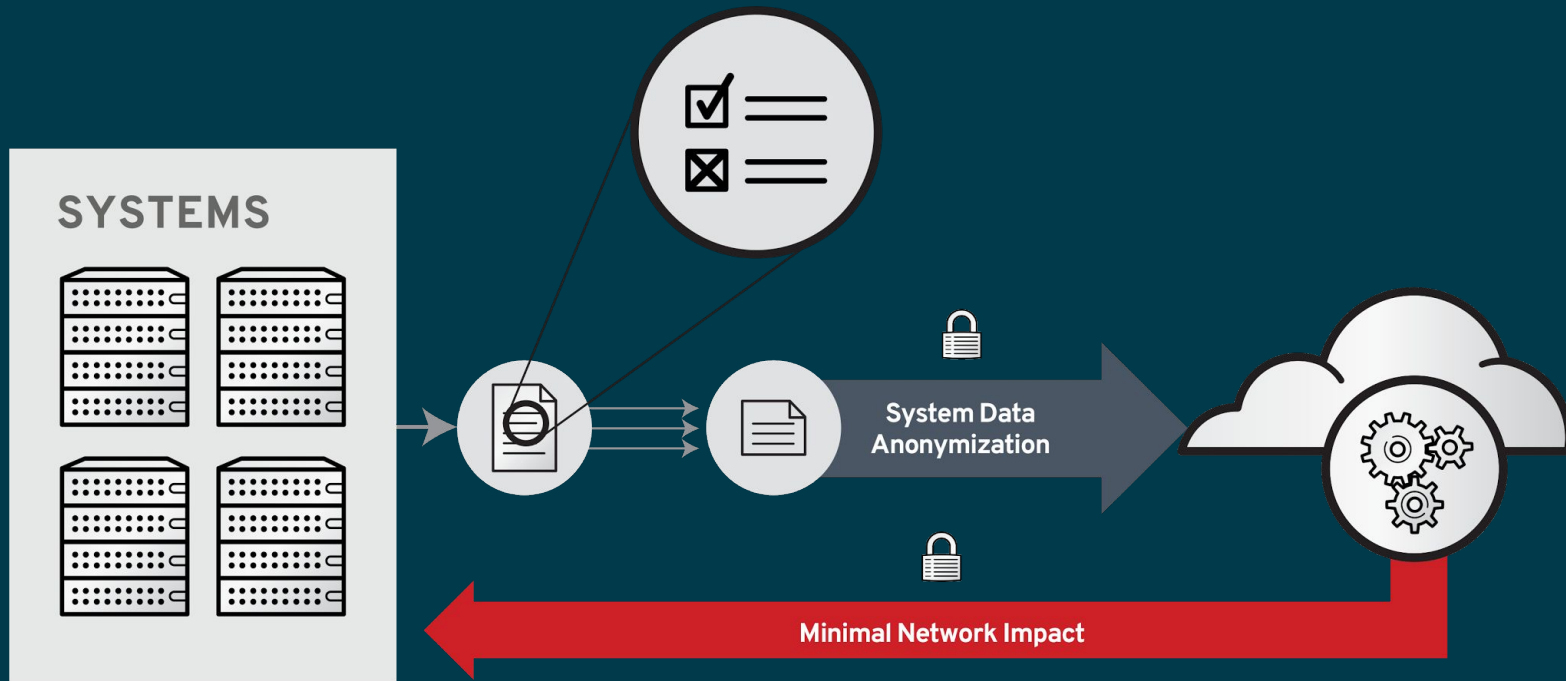
**DELIVERS ACTIONABLE INTELLIGENCE
FROM THE OPEN SOURCE LEADER**



**INCREASES VISIBILITY
OF INFRASTRUCTURE RISKS
AND THE LATEST SECURITY THREATS**



NO NEW INFRASTRUCTURE TO MANAGE



BECAUSE WE ARE A SERVICE

- The ability to quickly alert on new problems arising across the board
- Adapt to many changing infrastructure configurations
- We're able to provide real-time risk assessment in Red Hat infrastructure
- Iterate quickly and add new features and functionality based on feedback

WHAT'S NEW

Released at Summit

Container analysis

Identify risks in container platforms, images, and containers

Continuous stream of updated checks

Simple remediations steps and guidance with awareness of state of container lifecycles

OpenStack and RHEV support

Analysis of individual nodes, cluster manager, and overall cluster state

Data collection and communication via OSP Director and RHEV-Manager

Action plans

Identify, prioritize, and share maintenance plans to better bridge the gap between assessment and action

Insights recommended action plans, when new critical issues hit

Early Access Mode

Test out and provide feedback on new features while still in development

Switch seamlessly between stable and early access mode without re-registering systems

WHAT'S COMING

Next 12 month roadmap

Site-guidance

Track site-wide trends in security response, technical debt, and deployment agility

Get site-wide recommendations based on statistically validated industry trends

Configuration anomalies

Identify configuration and usage anomalies relative to typical enterprise usage patterns

Visualize most common configurations to suggested adjustments

Hybrid-Cloud enhancements

Awareness of application topologies for key orchestration tools and compound analysis of risks

Increased awareness of cloud-specific topologies and configuration

Analytics-driven automation

Accelerate and simplify critical issues through generated response automation

Deeper integration in common automation and deployment platforms

THANK YOU

<https://access.redhat.com/insights>



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos

ServerA,B,C,D logon credentials:

The root user on each server has a password that's the same as the server name, i.e. "servera", all work in this lab will be performed as 'root'.

If you should need them, the laptop credentials are username: kiosk password: redhat - but they automatically login and you shouldn't need them!

Please note your POD #.

You can find your pod number by clicking "Applications" in the top left corner of your desktop and going to "Utilities" and opening "Terminal". Once the terminal is opened type the command
`hostname`.

Your POD# is the number after the word "foundation" in the output of the hostname command on your desktop lab system.

Ex. *foundation67.ilt.redhat.com*

Ex server. *servera.pod67.example.com*

Note the difference in the hostnames, but the pod in this example is 67.

You can access the console of each server machine by double clicking the hostname of the server on your POD's desktop. If you click into a server console and you lose control of your mouse or keyboard, simultaneously press the left CTRL and left ALT keys on your keyboard to release the input devices from the virtual machine back to your laptop.

Satellite Credentials - Use the link on your desktop or <https://insightsat.example.com> to open Satellite. Click Red Hat Insights in the top right of the interface to inspect systems.

Use these to login with your pod number.

User: user_X (X = POD number)

Password: user_X (X = POD number)

Open VirtViewer console for each server by double-clicking the icon on the desktop.

See Step 1 Register all servers to Satellite

See Step 1 Yum install client on all

See Step 2 Register insights on all

See Step 3 Break serverd

ServerX:

User: root

Password: serverX

All console commands in this lab will be run as the 'root' user.

GETTING STARTED

Step 1 Register servera and serverb to the Demo Satellite Org "Example_Dot_Com" with the activation key "rhel_7"

```
# subscription-manager register --org="Example_Dot_Com" --activationkey="rhel_7"
```

Install the Red Hat Insights client

```
# yum install redhat-access-insights
```

Register serverc and serverd to the Demo Satellite Org "Example_Dot_Com" with the activation key "rhel_6":

```
# subscription-manager register --org="Example_Dot_Com" --activationkey="rhel_6"
```

Install the Red Hat Insights client

```
# yum install redhat-access-insights
```

Step 2:

Register servera, serverb, serverc, and serverd to the Demo Insights service.

Login to each server and run (as root): redhat-access-insights --register

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

<should have output indicating a successful Insights registration>

Step 3:

Run break-me script on serverd

Open serverd's console by double clicking on its icon on the desktop. Log in as root, and run the following

```
# /usr/bin/break-me
```

Or just type 'break-me' and hit enter, the command is in the path.

Log out of serverd by typing exit - or close the console.

Once all systems are registered, and serverd is broken, log back into the Satellite console and see all the affected systems in the Red Hat Insights console by clicking Red Hat Insights -> Overview in the top right of the Satellite interface.

Click on an category and down into an action to get information on which systems are affected.

Filter on systems in your POD by typing "podX" where X is your pod number into the filter field. You will repeat this every time you need to filter only on the systems you're responsible for.

Go back to Satellite, click Red Hat Insights -> Overview and filter on the systems in your POD, continuing to fix any problems on your systems with the resolution instructions.

Notice once you have 0 actions found the lab is complete.

Step-by-step Instructions

Here are step-by-step instructions if you're stuck and need a little extra help.

servera - rhel 7.2 base

Start the server if it isn't running

- login as root (pw: servera)
- register server with satellite
`#subscription-manager register --org="Example_Dot_Com" --activationkey="rhel_7"`
- install insights client
`#yum install redhat-access-insights`
- register server with insights
`#redhat-access-insights --register`
- Go look at insights in satellite. Your new system should show up (as servera.podx.example.com) with 2 security actions: DROWN and kernel keychain vulnerability.
- Reading the description for DROWN we see that openssl needs updating so we:
`#yum update openssl`
- Rerun the insights client and verify the problem is resolved
`#redhat-access-insights`
- The kernel keychain vulnerability description indicates that we need to update the kernel, so:
`#yum update kernel`
- Rerun the insights client and check the results:
`#redhat-access-insights`
- Oh no, it's still lists it as a problem... Reading more closely we see that the we need to reboot the box. Reboot and check again...
`#reboot`
`#redhat-access-insights`
- All problems resolved: Yay!

serverb - rhel 7.1 base with apache and a full filesystem (both space and i-nodes)

- Start the server if it isn't running
- login as root (pw: serverb)
- register server with satellite
`#subscription-manager register --org="Example_Dot_Com" --activationkey="rhel_7"`
- install insights client
`#yum install redhat-access-insights`
- register server with insights
`#redhat-access-insights --register`
- Go look at insights in satellite. Your new system should show up (as serverb.podx.example.com) with 4 actions:
 - DROWN
 - kernel keychain vulnerability
 - filesystem at or near capacity
 - i-node usage greater than 90%.
- Fix the two security issues just like servera above, then:
- determine which filesystem is out of space:
`#df`
The output shows /var/www is 100% used. Poking around a bit we see that /var/www/data has a BUNCH of files in it. Also, the output of
`#df -i`
show the same filesystem is also almost out of i-nodes.
`#rm -f /var/www/data/*`
- rerun insights and check the results:
`#redhat-access-insights`
- All problems resolved: Yay!

- Start the server if it isn't running
- login as root (pw: serverc)
- register server with satellite
`#subscription-manager register --org="Example_Dot_Com" --activationkey="rhel_6"`
- install insights client
`#yum install redhat-access-insights`
- register server with insights
`#redhat-access-insights --register`
- Go look at insights in satellite. Your new system should show up (as serverc.podx.example.com) with 5 security actions:
 - Special DROWN
 - Badlock
 - Heartbleed
 - Shellshock
 - Insecure SSH ciphers

and 2 performance actions:

- Memory overcommit
- swappiness.

Resolve the issues as follows:

- DROWN `#yum update openssl`
- Badlock `#yum update samba`
- Heartbleed also `#yum update openssl`
- Shellshock `#yum update bash`
- SSH Ciphers `#vi /etc/ssh/sshd_config` (remove line with bad ciphers - the last line of file)
- Memory overcommit `#vi /etc/sysctl.conf` (make `vm.overcommit_memory = 0`)
- Swappiness `#vi /etc/sysctl.conf` (make `vm.swappiness = 1`)
- Reboot and run insights client to verify:
`#reboot`
`#redhat-access-insights`
- All problems resolved: Yay!

- Start the server if it isn't running
- login as root (pw: serverd)
- register server with satellite
`#subscription-manager register --org="Example_Dot_Com" --activationkey="rhel_6"`
- install insights client
`#yum install redhat-access-insights`
- register server with insights
`#redhat-access-insights --register`
- Go look at insights in satellite. Your new system should show up (as serverd.podx.example.com) with 4 security actions
 - Special DROWN
 - Badlock
 - Heartbleed
 - Shellshock.

Resolve the issues as follows:

- DROWN
`#yum update openssl`
- Badlock
`#yum update samba*`
- Heartbleed
also `#yum update openssl`
- Shellshock
`#yum update bash`
- Reboot and run insights client to verify:
`#reboot`
`#redhat-access-insights`
- All problems resolved: Yay! But wait, there's more...

-
- Run break-me script:
`#break-me`

This will break the system (rendering it unbootable), run insights to update the system info and leave some hints about how to fix the server.

- Looking at Insights we see that we now have three new problems
 - Missing kernel
 - Device name contains extra whitespace
 - bad LVM filter
- Resolve the issues as follows (WARNING: if you reboot the system before fixing these issues it may not come back up easily)
 - Missing kernel: Fix grub.conf
`#vi /boot/grub/grub.conf` (remove __FIXME__ from kernel line)
 - Fix device name problem:
`#vi /etc/sysconfig/network-scripts/ifcfg-eth0` (remove quotes from DEVICE name)
 - Bad LVM filter: Fix the entry in /etc/lvm/lvm.conf
`#vi /etc/lvm/lvm.conf` (remove obviously bad filter line -- look for comment)
- Reboot and rerun insights
`#reboot` (you might have to do this twice for the networking to resolve itself)
`#redhat-access-insights`
- All problems resolved: Yay!