Red Hat Insights 1.0

RELEASE NOTES

RELEASE NOTES FOR RED HAT INSIGHTS

Last Updated: 2018-01-09

Red Hat Insights 1.0 RELEASE NOTES

RELEASE NOTES FOR RED HAT INSIGHTS

Legal Notice

Abstract

These Release Notes provide high-level coverage of the improvements and additions to Red Hat Insights.

Table of Contents

CHAPTER 1. INTRODUCTION

1.1. INTRODUCTION TO RED HAT INSIGHTS

Red Hat Insights is a Software-as-a-Service (SaaS) offering that provides continuous, in-depth analysis of registered Red Hat-based systems to proactively identify threats to security, performance and stability across physical, virtual and cloud environments, and container deployments.

Red Hat Insights analyzes select files on a system, getting smarter with each additional piece of intelligence and data. Red Hat Insights can automatically discover relevant information, proactively recommend tailored next actions, and even automate tasks with Ansible Playbooks. Using Red Hat Insights, customers can benefit from the experience and technical knowledge of Red Hat Certified Engineers, making it easier to identify, prioritize, and resolve issues before business operations are affected.

As a SaaS offering, Red Hat Insights regularly updates and expands its knowledge base to reflect new IT challenges that can impact the stability of mission-critical systems.

1.2. REQUIRED ENTITLEMENTS

Red Hat Insights is an add-on SaaS offering and requires an additional subscription (standalone or bundled with RHCI/RHCS) or evaluation to begin use. Please reach out to your account team or Red Hat Sales for additional information.

CHAPTER 2. RELEASE INFORMATION

2.1. INSIGHTS RELEASE, JANUARY 2018

2.1.1. Release Notes

Features added with the current release include:

Red Hat Insights UI fullscreen - The team has given Red Hat Insights a new, full-screen layout, improving the usability and aesthetics of the UI while keeping the core Red Hat Insights functionality accessible.

Webhooks functionality - Red Hat Insights webhooks integrate with a user's own tooling to enable an event-driven monitoring strategy that alerts when a system changes. This can free administrators from having to routinely check-in to Red Hat Insights to get that information. To learn more, refer to the KCS article, Understanding Red Hat Insights - Webhooks Integration.

2.1.2. Enhancements

- **Recent rules widget and filters** - Stay informed of the latest rules we've added to our service with the Recent Rules widget located at the bottom of the Overview page.
  Additional filtering has been added to the rules page to highlight these new rules.
- **CI/CD example: Red Hat Insights with Jenkins** - Building on the CI/CD functionality of the September 2017 release, the Red Hat Insights team invites you to learn more about using Red Hat Insights with Jenkins in Continuous Integration with Insights Examples.
- **Webhooks example: Red Hat Insights with Slack** - This Slack bot tutorial builds a Red Hat Insights webhook with a Slack bot to get notifications of system events.

2.1.3. Rules Added

The following rules were added to Insights in this development period:

- Information disclosure vulnerability in BlueZ via crafted SDP requests (CVE-2017-1000250)
- Kernel with loaded modules vulnerable to remote code execution via Bluetooth stack (CVE-2017-1000251/Blueborne)
- Kernel with loaded modules vulnerable to denial of service via Bluetooth stack (CVE-2017-1000251/Blueborne)
- Kernel vulnerable to remote code execution via Bluetooth stack (CVE-2017-1000251/Blueborne)
- Kernel vulnerable to denial of service via Bluetooth stack (CVE-2017-1000251/Blueborne)
- Master controller fails to start when changes are made to the SDN plugin if there are headless services in the cluster
- Failure to start VDSM when network interfaces are misconfigured in RHV
- Kernel is vulnerable to memory corruption or local privilege escalation (CVE-2017-1000253)
- Dnsmasq vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)

- Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)
- System lockups possible when abnormal VPD data returned from HBA
- Failure to retrieve information from ESX hypervisors due to running unpatched virt-who on Satellite 6.
- OpenStack environment is down due to an infinite loop between Gnocchi and Swift
- Network performance degradation when networking parameters are not properly tuned
- Network connectivity loss for large TCP stream protocols when using affected bonding/teaming mode
- wpa_supplicant with active WiFi is vulnerable to man-in-the-middle attack via crafted WPA2 frames (CVE-2017-13077)
- Unexpected behavior in command-line tools and 3rd party software when user or group names are numeric
- System lockup occurs when using netconsole over a bonding interface with ALB/TLB mode
- Java applications will be unavailable when G1 GC is used due to native memory leak
- The httpd service will become unavailable when it exceeds the configured nproc limits
- Slow restarts for httpd when the StartServers parameter is set to a large value
- Live migration fails when security_driver is set to none on OSP compute nodes
- VM migration failure when incompatible filters are used in nova.conf as scheduler_default_filters
- DNS resolution fails within an OpenShift Pod when DNS server address is set incorrectly
- Samba authentication fails when krb5.keytab kvno version does not match secrets.tdb
- Disk space may be exceeded when soft deleted rows are not purged from Nova database
- Kickstart profile page inaccessible in the Satellite web UI due to incorrect configuration.
- Boot failure when root PV is filtered out
- Suboptimal performance when the start/end values of the net.ipv4.ip_local_port_range tunable have the same parity
- Kernel vulnerable to memory corruption via permission bypass (CVE-2017-1000405)
- Compromised system by Linux/Ebury 1.6 malware - modified library
- Compromised system by Linux/Ebury 1.6 malware - suspicious library location
- Remote code execution vulnerability in NSS via crafted base64 data (CVE-2017-5461)
- Satellite 5 does not work as expected when the database schema is not upgraded during system package update
- Startup failure for AWT java applications when invalid fonts are installed

- Filesystem corruption when using unsupported journal modes
- Failure of critical Satellite services when the available disk space of Satellite partitions is too low
- Performance degradation in httpd due to incorrect MaxClients/MaxRequestWorkers configurations
- The httpd service hangs when the maximum number of connections reaches the value of ServerLimit and the limit of cpu cores is exceeded
- Tomcat vulnerable to information disclosure when using VirtualDirContext (CVE-2017-12616)

CHAPTER 3. ADDITIONAL RESOURCES

3.1. MORE INFORMATION ABOUT RED HAT INSIGHTS

Learn more about Red Hat Insights:

- [Blogs](https://access.redhat.com/blogs/insights) from the Red Hat Insights team
- [Documentation](https://access.redhat.com/documentation/en/red-hat-insights/)
- [KCS articles and solutions](https://access.redhat.com/search/#/knowledgebase?q=&product=Red%20Hat%20Insights&language=en&documentKind=Solution,Article)

CHAPTER 4. PREVIOUS RELEASES

4.1. INSIGHTS RELEASE, SEPTEMBER 2017

4.1.1. Release Notes

The latest Red Hat Insights release adds the following features to the Customer Portal UI:

New Insights CI/CD Client [Technology Preview*] - The new Insights client can be integrated into your CI/CD pipeline, enabling the identification of risk in your infrastructure earlier in the development lifecycle. The new client is designed for flexibility and allows for integration within the existing tools you use, such as Jenkins or GitLab CI. Refer to Insights documentation to learn more.

Risk of Change [Insights Beta] - Rule remediations are evaluated for the impact that the change(s) could have on your environment. This assessment is visible in the Rule and system level views and can clarify whether the change is a quick fix or may require additional coordination. This feature will be migrated to production Insights soon.

*For more information about technology previews, see Technology Preview Features Support Scope.

4.1.2. Enhancements

With the current release, the Insights team has also added the following enhancements:

- **Improved Overall Score gauge** - [Executive Reporting] With several design improvements, the new Overall Score gauge enables a better understanding of your current score, color coded health of that score, and the overall range used.
- **Playbook plan summary** - [Planner] The Playbook summary provides clearer visibility of affected systems and resolution, as well as a reboot summary to identify reboot requirements for that playbook, if applicable.
- **Page filters** - [Inventory, Planner, and Rules] Add active filters to specific pages and collapse them when you’re done with them.

4.1.3. Rules Added

The following rules were added to Insights in this development period:

- Galera certificates will expire in 30 days in OpenStack
- Galera certificates will expire in 7 days in OpenStack
- Connectivity failure when Galera certificates have expired in OpenStack
- Compromised system by OutlawCountry malware
- Insecure updates from third-party yum repositories when GPG verification
- Insecure updates from Red Hat yum repositories when GPG verification
- Samba with externally listening process vulnerable to a denial of service via NetBIOS Session Service header (SMBLoris)
- Samba vulnerable to a denial of service via NetBIOS Session Service header (SMBLoris)

- 'Decreased security in system auditing (audit not running)'
- "Kernel and glibc vulnerable to local privilege escalation via stack and heap memory clash (CVE-2017-1000364 and CVE-2017-1000366)"
- Insufficient space available when image garbage collection fails to run
- Failed api connection between docker and OpenShift when version of docker
- Projects are unlisted when there is a rolebinding to a nonexistent role
- Failure to connect to service when configured IP is in use by another
- LUNs on iSCSI target inaccessible when deleting a pod using any LUN on
- Degraded performance when deleting dynamically provisioned persistent
- Denial of service caused by volume deletion requests exceeding API limits
- OpenShift functionality degraded when critical services are not running
- System resource restriction fails when pod eviction thresholds contain
- Packet loss when traffic is forwarded through an ipsec tunnel while using
- Kdump does not work due to XEN/AWS's limitation.
- Kernel panic occurs when running ipmitool command with specific kernels
- NFSv4 client hangs when trying to open files against NFSv4 server
- High CPU usage when extending Docker thin pool due to insufficient free space in Volume Group
- Running container fails when a race between device-mapper and docker daemon itself occurs (the issue may happen in the future)
- Running container fails when a race between device-mapper and docker daemon itself occurs (the issue has happened)
- Host entitlements not available to container due to bug in oci-systemd-hook

4.2. INSIGHTS RELEASE, JUNE 2017

4.2.1. Enhancements

With our latest release, Red Hat Insights has added capabilities to identify Incidents - critical issues that are actively impacting your environment at the time of Insights analysis. This additional level of detection provides another layer of analysis so Insights can both proactively prevent and actively detect issues or risks that require attention and remediation.

4.2.2. Release Notes

The latest Red Hat Insights release includes the following changes to the Customer Portal UI:

Incident Detection. The Insights engine has been expanded to detect Incidents: critical issues we know

are impacting your infrastructure at the time of analysis. We are highlighting these incidents uniquely within the UI to direct your attention to the them for immediate remediation to hopefully prevent impending or further disruption.

Global group filters. Enhanced filters enable a consistent, focused user experience. Group filters limit results to systems in a group that you specify. Global group filtering retains the filter on each page within Insights, until it is reset or another group is chosen. Additionally, the Inventory page enables filtering by System Status (Checking-In or Stale) and System Health (Affected or Healthy).

Analysis of Openshift Infrastructure. Insights now provides analysis of Red Hat Openshift, identifying potential security, stability, availability and performance risks within your Openshift infrastructure. This feature is currently available as a Tech Preview.

Red Hat Insights blog subscription. In an effort to keep users informed of the latest Red Hat Insights developments, users are now subscribed to the Red Hat Insights blog. New blog posts are posted as new rules or features are added to Insights. Users can manage their subscription to this blog.

Insights availability status. Users can view the current availability status of Red Hat Insights on the Customer Portal Status page (status.redhat.com). The Customer Portal Status page shows current information about outages, known availability issues, or upcoming maintenance windows for Red Hat Insights Stable, Beta, and API, and that of other Red Hat Customer Portal tools.

Automatic removal of stale systems. To help users focus on the most up-to-date, critical actions in their infrastructure, without the noise of older, stale systems, Insights automatically removes stale systems from visibility after one month. A system is considered stale when it no longer checks in daily with the Insights service, and is highlighted by red text. After one month has passed with stale status, the system is automatically removed from Insights views.

Executive reporting optimizations. Added in the April 2017 release of Red Hat Insights, executive reporting displays historical trends and snapshots of infrastructure health. In response to user feedback, we have added the following features:

- Reporting on the number of issues resolved over the past 30 days.
- The All Rule Hits tab displays rules that are currently impacting systems in an account's infrastructure, and the number of impacted systems for each rule.
- Export to PDF allows users to save and share their complete executive report.
- Overall Score improvements. Hover over the Overall Score to see additional information about the score and how it's calculated. Additionally, the score color changes based on health of systems.

4.2.3. Bugzillas Resolved

The following bugs were resolved for the current release:

- Export CSV results in JSON. BZ1450764
- Executive report issues since May 11th. BZ1453136
- Hostnames showing up as UUID by default. BZ1447352
- MISSED_GRUB_SYMLINK_ISSUE needs to handle UEFI locations of **`grub.conf`**. BZ1420155
- Weekly mail confusing. BZ1432417

- Hidden rules not hidden in summary. BZ1427584
- Incorrect info on https://access.redhat.com/products/red-hat-insights#satellite5. BZ1444071
- Rule - lacp-compliant hash algorithm not specified. BZ1397487
- SSH hardening rule needs updating. BZ1403962
- Drill down from actions shows an empty field in the "type" column. BZ1429669
- [RFE] Export list of systems in inventory (csv format). BZ1364531
- "Optimize Your Experience" says 5/10 in the graphic but also says "Congratulations! You have registered 10/10 available systems." BZ1420892

4.3. INSIGHTS RELEASE, APRIL 2017

4.3.1. Enhancements

With our latest release, Red Hat Insights brings the power of Ansible automation to the actionable intelligence platform. Aligned with Red Hat's vision to dramatically simplify IT management, Red Hat Insights now offers administrators the ability to automate the remediation of critical issues through the use of Ansible Playbooks.

4.3.2. Release Notes

The latest Red Hat Insights release includes:

Ansible Playbook creation. The Red Hat Insights console can now translate predictive intelligence into actions, enabling users to automatically remediate Insights findings - helping to more quickly and cost-effectively close infrastructure risks.

Integration with Ansible Tower by Red Hat. [Tech Preview] Ansible Tower 3.1 supports integration with Red Hat Insights, which allows Insights playbooks to be used as a Tower Project. This enables dynamically generated Ansible Playbooks to be more rapidly deployed in a highly scalable, more secure manner, allowing the extension of Insights into automation and self-service use cases.

Insights configuration playbook. Configuration of Insights as a playbook is designed to streamline large and small deployments of the Red Hat Insights client to reduce installation time and effort and provide Insights scalability as infrastructure needs grow.

Expanded executive reporting. The Executive Report allows administrators to view historical trends in addition to a snapshot of the current infrastructure health, enabling enterprises to more easily see their current risk assessment and what trends will most likely impact their IT estate.

Predictive risk assessments. Displayed per-rule, administrators can easily view Impact, Likelihood, and Total Risk to a system. Assessments are combined to produce a more meaningful total risk assessment, helping organizations to focus on the issues that can most impact risk reduction.

Enhanced user interface. The enhanced UI includes additional filtering based on type of issue, for a more simplified and streamlined look across the infrastructure.

Topic categorization. Designed for improved identification and remediation of issues, Insights findings can now be viewed by topics, such as SAP or Oracle, in addition to the level of risk.

Exporting Inventory to CSV. Accessible via the Inventory page, the CSV file provides an export of the registered system and related metadata of that system's registration.

Risk Summary. This assessment is visible on the Overview and Actions pages and reflects the percentage of Critical, High, Medium and Low risk actions-detected, enabling a better understanding of overall infrastructure health.

Simplified feedback. Above every page of the UI, a Provide Feedback link offers a conduit to provide helpful feedback and suggestions directly to Insights developers.

Revised on 2018-01-09 12:28:22 EST