Abstract

These release notes highlight the latest features and improvements implemented in the Red Hat Insights application and services. Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.
# Table of Contents

**CHAPTER 1. INTRODUCTION TO RED HAT INSIGHTS** ............................................. 3  
  1.1. REQUIRED ENTITLEMENTS  ................................................................. 3  

**CHAPTER 2. APRIL 2020** ............................................................................. 4  
  2.1. RED HAT INSIGHTS  .............................................................................. 4  
  2.2. ADVISOR  ............................................................................................. 4  
  2.3. COMPLIANCE  ...................................................................................... 5  
  2.4. VULNERABILITY  .................................................................................. 5  
  2.5. DRIFT  ................................................................................................ 6  
  2.6. POLICIES (NEW SERVICE)  ................................................................. 6  
  2.7. PATCH (NEW SERVICE)  ..................................................................... 6  

**CHAPTER 3. MORE INFORMATION ABOUT RED HAT INSIGHTS** .......... 7
CHAPTER 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.

1.1. REQUIRED ENTITLEMENTS

As of May 2019, Red Hat Insights is free, offered as part of the value of your Red Hat Enterprise Linux subscription. No additional entitlements are required to use Insights.
CHAPTER 2. APRIL 2020

2.1. RED HAT INSIGHTS

In order to more effectively manage risks to Red Hat Enterprise Linux (RHEL) systems, the Red Hat Insights application now includes the Advisor, Compliance, Vulnerability, Drift, Patch, and Policies services. The configuration assessment and reporting features that previously constituted Red Hat Insights are now available within the Advisor service.

This release includes the following enhancements:

User-specific-settings: Individual users can begin to personalize their own interaction with the Insights services, and related behaviors on the cloud.redhat.com platform. For example, setting options are now available for Advisor service notifications.

Account settings: Org admins can configure and modify certain features (like User Access and Application Settings) that affect application behaviors at the Account/Org level. For example, Insights has an application setting that provides the option to show Satellite-managed hosts for your account.

User access: Role-based access control (RBAC) enables org admins to configure and manage user access across many of the applications on cloud.redhat.com. For example, org admins can elect to disable access to Drift and enable access to Compliance for one or more account users.

System tagging: Insights now allows users to add descriptive tags to systems, either from the Insights client or from Satellite 6.x and later, allowing them to filter by those tags in Inventory and the Advisor service. Filtering by tags will be enabled in other services soon.

Find it fix it remediations: Users can create and execute Ansible Playbooks on systems across one or more Red Hat Satellite instances, directly from the Insights application.

Stale system dentification and management: The Insights Inventory now marks systems as "stale" when they stop checking in. Eventually stale systems will automatically be removed from your inventory.

2.2. ADVISOR

This release includes the following enhancements:

Weekly email report: The Advisor service Weekly Email report provides a quick view of the health of your infrastructure. Subscribing to the email is optional and requires that you opt in using the application settings in the Advisor service. The email is informative yet unobtrusive; all of the included information can be consumed at a glance.

Filtering by groups of systems: Leveraging the Insights tagging capability, Advisor service Recommendations and Systems views can be filtered by tags added to the Insights client, allowing users to focus on specific groups of impacted systems.

Granular controls for disabling recommendations: Users have additional controls around completely disabling recommendations for selected hosts.

Executive report download: You can download a high-level, PDF report summarizing the status of your infrastructure and designed for an executive audience. The Advisor executive report summarizes recommendations based on severity, category, and the top three recommendations in your infrastructure based on greatest risk and greatest number of impacted systems.
Advisor service recommendations now highlighted in Red Hat KCS articles and solutions: When viewing a KCS article or solution in the customer portal, Advisor support for the issue will be highlighted, if a recommendation is available.

**Important change to CVE security recommendations:** CVE security recommendations have moved to the Vulnerability service. All CVE security rules previously provided within the Advisor service have been transitioned over to the Vulnerability service for more robust and comprehensive security vulnerability detection.

**2.3. COMPLIANCE**

This release includes the following enhancements:

**Ability to search rules by reference ID:** SCAP policy rules are often referenced by a reference ID rather than a name. The ability to search for compliance policy rules by the reference ID is now available.

**Ability to create and edit policies with the Compliance service:** You can now create and edit SCAP security policies in the Compliance service. This makes it easier to add new policies, edit the included rules, and add and remove systems to which they are applied.

**Important changes and recommendations to Compliance service users:**

- The Compliance service team recommends that users create their security policies directly within the Compliance service to enjoy the full functionality of the service. Compliance reports uploaded from an external source, without a policy defined in the Compliance service, can no longer be edited to include a business objective and compliance threshold.

- At this time, selecting specific rules to include in a policy is only available when a policy is newly created. However, the ability to edit rules included in an existing policy is coming soon.

- Reports in the Compliance service will be grouped by SCAP Security Guide (SSG) version. If multiple versions of SSG are deployed on systems assigned to a single policy, users will see one report per version of SSG. We recommend that users use the same SSG version for all the systems under a policy to have a consolidated and simplified view of your reports.

**2.4. VULNERABILITY**

This release includes the following enhancements:

**Executive report download:** You can download a high-level report summarizing the security status of your infrastructure and designed for an executive audience. The PDF report summarizes CVEs impacting your RHEL infrastructure, broken down by severity, and identifies the top CVEs impacting the most systems.

**CVE security rules previously shown in Advisor have moved to Vulnerability:** The CVE security rules that were previously curated by the Insights rules team are now included with all other Red Hat CVEs in the Vulnerability service. Security rules are high profile CVEs, some of which have been through the Customer Security Awareness Program. CVE security rules are identifiable in the Vulnerability service by a security rule icon. You can also filter security rules in the Vulnerability service. Remediation of security rules impacting your systems should be given the highest priority.
IMPORTANT

For the CVE-based security rules that have moved from Advisor to the Vulnerability service, the ability for users to select and use Ansible playbooks that are different than those associated with the errata during the remediations step is not yet available. This is a known gap and will be addressed in the near future.

Ability to search systems by system name: Users can now search for systems in the Vulnerability service by system name, eliminating the need to remember the system’s UUID.

2.5. DRIFT

This release includes the following enhancements:

Visual revamp: Drift was updated for a better user experience with enhancements covering additional real estate for comparison, updated toolbar, color scheme change, and improved visibility of applied filter and search elements.

Historical system profiles: Changes to RHEL system configuration are now stored in Insights over time. Users can use the Drift service to access previous configurations and compare them with the current configuration, other systems, and/or baselines. Historical system profiles are stored and available for seven days.

Reference comparison and highlights: A new feature was added to specify a reference for your comparison. When a system or a baseline is selected as a reference, specific differences in all other compared systems or baselines are highlighted. If no reference is selected, the entire row is highlighted (as previously) if at least one of the values differ.

2.6. POLICIES (NEW SERVICE)

The Policies service is a new offering and includes the following functionalities:

Policies: Create and manage policies on RHEL system configuration. Evaluate your systems configuration and trigger actions when conditions are met.

Email notifications: Get alerted when system configuration differs from what is expected. Send instant notifications and/or daily summaries of policies triggered in your inventory.

Integration to hooks (Beta): The Hooks integration functionality used by the Policies service is currently available as a Beta feature. Integrate with your organization’s operational processes. Send POST requests to configured hooks every time conditions are met on your inventory.

2.7. PATCH (NEW SERVICE)

The Patch service is a new offering and includes the following functionalities:

Red Hat errata applicability: Discover which of your systems may be impacted by Red Hat security, bugfix, and enhancement advisories.

Create Ansible Playbooks to Patch Your Systems: Remediate security, bugfix, and enhancement advisory exposure by creating Ansible Playbooks to patch your systems with a set of Red Hat advisories.
CHAPTER 3. MORE INFORMATION ABOUT RED HAT INSIGHTS

Learn more about Red Hat Insights from the following resources:

- Red Hat Insights blog
- Product page
- Get Started with Red Hat Insights
- Product documentation

Revised on 2020-05-28 17:57:37 UTC