Red Hat Insights 1.0

Assessing Red Hat Enterprise Linux (RHEL) Configuration Issues Using Red Hat Insights

Learn About the Conditions Impacting Your RHEL Systems

Last Updated: 2019-09-12

Red Hat Insights 1.0 Assessing Red Hat Enterprise Linux (RHEL) Configuration Issues Using Red Hat Insights

Learn About the Conditions Impacting Your RHEL Systems

Legal Notice

Abstract

Assess infrastructure exposure to configuration issues that can affect availability, stability, performance, and security of RHEL systems. Providing Feedback: If you have a suggestion for improving this documentation, or have found an error, please submit a Bugzilla report at http://bugzilla.redhat.com for the Cloud Software Services (cloud.redhat.com) product, and using the Documentation component.

Table of Contents

CHAPTER 1. ASSESSMENT WITH RED HAT INSIGHTS

Red Hat Insights helps you assess and monitor the health of your Red Hat Enterprise Linux (RHEL) infrastructure in order to understand your exposure and resolve configuration issues that can affect your systems.

The Insights client runs daily, by default, to check system metadata against a database of *rules*: sets of conditions that Red Hat knows to be potentially problematic with respect to the availability, stability, performance, or security of RHEL systems.

Your data is then uploaded to the Red Hat Insights console where you can

- See an overview of your infrastructure's risk exposure, by risk severity or category
- Learn more about individual rules, details about the risks they pose, and the steps to resolve them, tailored to your individual systems

CHAPTER 2. ASSESSMENT BY RULE SEVERITY

Each rule is given a severity rating that defines a level of the *total risk* that a rule poses to your infrastructure. Total risk is a combination of the *likelihood* that a rule will impact systems in your infrastructure, and the level of expected *impact* to the system if the identified risk occurs.

2.1. ASSESSING INFRASTRUCTURE EXPOSURE BY RULE SEVERITY

Use Red Hat Insights to view the most severe risks to your infrastructure and plan resolutions accordingly.

Procedure

1. From the Insights Overview, under **Rule hits by severity**, click on rules hits for a particular severity rating.
2. Modify your Rule-table view.
    a. Search by the rule name.
    b. Add filters or use the sorting function at the top of each column to show or group rules of particular interest.
    c. By default, the checkbox is selected to **Show Rules With Hits**. Unclick the box to see **all** the rules that Insights checks your systems against, including those that have no impact on your systems.
    d. Sort the columns of the Rule table to see, for example, which rules are impacting the greatest number of systems.
    e. Hide rules from view by disabling them.
        i. Click the Actions menu (three vertical dots).
        ii. Click **Disable Rule**.
3. Select a rule from the list.
    a. Click on the arrow next to the rule name to view the rule description, access knowledgebase documentation, if available, and view *risk of change*, an indicator of the likelihood that remediation of the rule on the system will result in system downtime.
    b. Click on the rule name to view the Affected Systems list.
4. Click on a system name to see system details and a list of rules affecting that system.

CHAPTER 3. ASSESSMENT BY RULE CATEGORY

The Insights team categorizes each rule based on the potential impact on one of the following areas of operation:

- **Availability.** The availability of a service can be compromised even if the service's host machine is up and running. Actions in the Availability category pertain to networking and/or service issues on a given machine. Review and resolve these availability issues to ensure that your vital services can be reached.

- **Stability.** Hardware issues, kernel panics, and memory corruption can lead to outages and data loss. Red Hat Insights detects stability issues in your environment that need to be addressed.

- **Performance.** File system, networking, and NUMA performance issues can cause unacceptable slow downs in your server environments. Whether it be hardware error or simple configuration, Red Hat Insights can find it. Reviewing, and resolving these actions will help you maintain your environment's performance.

- **Security.** Insights not only detects security issues, it also strives to let you know whether these issues leave you in a vulnerable state. SSL exploits, remote access, and local privilege escalation issues can lead to compromised data and data loss. Review and resolve these security issues to ensure your systems and data are kept safe.

3.1. ASSESSING INFRASTRUCTURE EXPOSURE BY RULE CATEGORY

Use Red Hat Insights to view rules by category of the type of risk they pose to your infrastructure.

Procedure

1. Go to the Red Hat Insights Overview and, under the **Rule hits by category** heading, click on a category name.

2. Modify your Rule table view.

    a. Search by the rule name.

    b. Apply Filters to include rules by risk type, category, and status (enabled or disabled) in your view.

    c. By default, the checkbox is selected to **Show Rules With Hits**. Unclick the box to see all the rules that Insights checks your systems against, including those that have no impact on your systems.

    d. Sort the various columns of the Rule table to see, for example, which rules are impacting the greatest number of systems.

    e. Hide rules from view by disabling them.

        i. Click the actions menu (three vertical dots).

        ii. Click **Disable Rule**.

3. Select a rule from the list.

a. Click on the right arrow to view the rule description, access knowledgebase documentation, if available, and view *risk of change*, an indicator of the likelihood that resolution of the rule on a system will result in system downtime.

b. Click on the rule name to view the Affected Systems list.

4. Click on a system name to see system details and a list of rules affecting that system.

CHAPTER 4. REFERENCE MATERIALS

To learn more about Red Hat Insights, the following resources might also be of interest:

Documentation

- *Remediating Configuration Issues Using Red Hat Insights and Ansible Playbooks*
- Documentation, Red Hat Insights
- Product Support Page, Red Hat Insights