Red Hat Insights 2020-04

Generating Compliance Service Reports

Communicate the Level of Compliance of RHEL Environment with Security Policies

Last Updated: 2020-09-11

Red Hat Insights 2020-04 Generating Compliance Service Reports

Communicate the Level of Compliance of RHEL Environment with Security Policies

Legal Notice

Abstract

Generate a variety of reports to communicate to enterprise security auditors the security-policy compliance status of a RHEL environment. 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. COMPLIANCE SERVICE REPORTING OVERVIEW

The Compliance service enables users to export granular data based on filters in place at the time of export. Exporting a Compliance report requires the following actions:

- Uploading current OpenSCAP results
- Filtering your view in the Compliance service
- Exporting to CSV or JSON file and saving your download

CHAPTER 2. UPLOADING CURRENT OPENSCAP DATA FOR YOUR SYSTEM

The Compliance service presents data from OpenSCAP scans. Whether you are using the Compliance service to view system compliance status, remediate issues, or report on results, ensure that you're seeing current data by uploading the latest system data from OpenSCAP *before* continuing with other procedures.

Procedure

1. Run the following command to upload current data from OpenSCAP:

```
[root@server ~]# insights-client --compliance
```

CHAPTER 3. EXPORTING A COMPLIANCE REPORT FOR SELECTED SYSTEMS

Perform the following steps to export a Compliance report showing CVEs impacting your systems, and based on filtering in place at the time of export:

Procedure to export a report for a single policy

1. Navigate to the Compliance service > Reports tab and log in if necessary.
2. Locate the policy and click **View report**.
3. Apply filters as needed to refine results.
4. Select the systems you want to see in the report.
5. At the top of the systems list, click the download icon and select **Export CSV** or **Export JSON**, based on your export preferences.
6. Select a download location and click **Save**.

Procedure to export a report for selected systems

1. Navigate to Compliance service > Systems and log in if necessary.
2. Apply filters as needed to refine results.
3. Select the systems you want to see in the report by checking the box next to each system name.
4. At the top of the systems list, click the download icon and select **Export CSV** or **Export JSON**, based on your export preferences.
5. Select a download location and click **Save**.

CHAPTER 4. REFERENCE MATERIALS

To learn more about the Compliance service, see the following resources:

- *Assessing and Monitoring Security Policy Compliance of RHEL Systems*
- *Remediating Security-Policy Compliance issues using Ansible Playbooks*
- Red Hat Insights Documentation
- Red Hat Insights Product Support page

CHAPTER 5. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS

The 2020-04 release of Red Hat Insights includes significant changes to the application features and services.

Changes to the Red Hat Insights application

The Red Hat Insights application now includes the services that were previously bundled with the Cloud Management Services for RHEL application, and were part of the Red Hat Smart Management bundle, along with Red Hat Satellite.

The former cloud management services, plus a couple of new services, are now included in the value that Insights brings to each Red Hat Enterprise Linux (RHEL) subscription.

Insights Advisor

The tools and capabilities that constituted Red Hat Insights prior to this release are now available as the **Advisor** service. The *rules* that have always been the currency of Insights are now called Advisor **Recommendations**.

Insights security rules have moved

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. They are identifiable in the Vulnerability service by a security rule icon. You can also filter security rules in the Vulnerability service.

Services included with Red Hat Insights

The services included with Red Hat Insights in the 2020-04 release are:

- **Advisor.** Identify and fix configuration issues that can negatively impact the availability, performance, stability, and security of RHEL systems.
- **Vulnerability.** Assess and monitor the exposure of your RHEL environment to CVEs and security rules.
- **Compliance.** Assess and monitor the compliance of your RHEL systems with SCAP security policies.
- **Patch.** Enable consistent patch workflows for RHEL systems across the open hybrid cloud.
- **Drift.** Compare system configurations of a system over time, or to other systems and baselines, to identify discrepancies in your environment and perform drift analysis.
- **Policies.** Evaluate and react to system configuration changes in your environment.

The integrated tools that work with each of the services above are:

- **Inventory.** Topological inventory of RHEL systems under Red Hat Insights management
- **Remediations.** Repository of Ansible Playbooks that you create and manage using Red Hat Insights
- **Subscription Watch.** Comprehensive, product-by-product, account-level subscription reporting service across hybrid cloud deployments

Resources

- Red Hat Insights Product Support page
- Red Hat Insights Documentation
- Red Hat Insights Release Notes
- Red Hat Insights blog channel