



Red Hat Insights 2022

Generating Compliance Service Reports

Communicate the compliance status of your RHEL infrastructure to security stakeholders

Red Hat Insights 2022 Generating Compliance Service Reports

Communicate the compliance status of your RHEL infrastructure to security stakeholders

Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Generate a variety of reports to communicate to enterprise security auditors the security-policy compliance status of your RHEL environment.

Table of Contents

| | |
|--|-----------|
| MAKING OPEN SOURCE MORE INCLUSIVE | 3 |
| PROVIDING FEEDBACK ON RED HAT DOCUMENTATION | 4 |
| CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL COMPLIANCE SERVICE REPORTS | 5 |
| CHAPTER 2. UPLOADING CURRENT OPENS CAP DATA FOR YOUR SYSTEM | 6 |
| CHAPTER 3. EXPORTING A COMPLIANCE REPORT FOR SELECTED SYSTEMS | 7 |
| 3.1. EXPORTING A REPORT FOR A SINGLE POLICY | 7 |
| 3.2. EXPORTING A REPORT FOR SELECTED SYSTEMS | 7 |
| CHAPTER 4. POLICY REPORTS | 8 |
| 4.1. CREATING A PDF REPORT FOR A POLICY | 8 |
| CHAPTER 5. ENABLING NOTIFICATIONS AND INTEGRATIONS | 9 |
| CHAPTER 6. REFERENCE MATERIALS | 10 |

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. To provide feedback, highlight text in a document and add comments.

Prerequisites

- You are logged in to the Red Hat Customer Portal.
- In the Red Hat Customer Portal, the document is in the **Multi-page HTML** viewing format.

Procedure

To provide your feedback, perform the following steps:

1. Click the **Feedback** button in the top-right corner of the document to see existing feedback.



NOTE

The feedback feature is enabled only in the **Multi-page HTML** format.

2. Highlight the section of the document where you want to provide feedback.
3. Click the **Add Feedback** pop-up that appears near the highlighted text.
A text box appears in the feedback section on the right side of the page.
4. Enter your feedback in the text box and click **Submit**.
A documentation issue is created.
5. To view the issue, click the issue link in the feedback view.

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL COMPLIANCE SERVICE REPORTS

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 OPENSAP 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 are 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, based on filtering in place at the time of export.

3.1. EXPORTING A REPORT FOR A SINGLE POLICY

Perform the following steps to export a compliance report for a single policy.

Procedure

1. Navigate to the [Red Hat Enterprise Linux > Compliance > Reports](#) tab and log in if necessary.
2. Click on the policy to view the report.
3. Apply filters as needed to refine results.
4. Click **View policy** for more detailed information such as compliance threshold and business objective.
5. At the top of the systems list, click the download icon to the right of the Remediate button and select **Export to CSV** or **Export to JSON**, based on your export preferences.
6. Choose to open or save the file. Then click **OK**.

3.2. EXPORTING A REPORT FOR SELECTED SYSTEMS

Perform the following steps to export a compliance report for selected systems.

Procedure

1. Navigate to [Red Hat Enterprise Linux > Compliance > 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 to CSV** or **Export to JSON**, based on your export preferences.
5. Choose to open or save the file. Then click **OK**.

CHAPTER 4. POLICY REPORTS

The Insights for RHELcompliance service enables you to create PDF reports for individual policies to share with stakeholders, such as your compliance team or auditors.

Reports include the following information:

- Policy details: policy type, operation system, compliance threshold, and business objective.
- Percentage of systems in compliance with the policy.
- Numbers of non-compliant and compliant systems.
- Non-compliant system information. You can select to include compliant systems when creating the report.
- List of top 10 failed rules: the most severe failed rules, along with the greatest number of failed systems for each rule, are ranked at the top.


4.1. CREATING A PDF REPORT FOR A POLICY

Perform the following steps to download a PDF report for a security policy.

Prerequisites

- You must be logged in to the Red Hat Hybrid Cloud Console.
- Policy reports are point-in-time reporting. Red Hat recommends uploading your latest system data to Insights for RHEL before creating a policy report in the compliance service.

Procedure

1. Optionally run **insights-client --compliance** on your systems to scan them and upload current data to the compliance service.
2. Navigate to [Red Hat Enterprise Linux > Compliance > Reports](#) .
3. Locate the policy for which to create the report.
4. Click the download icon  on the far right of the same row as the policy name.



NOTE

You can also click on the policy name and click **Download PDF** in the upper right of the page.

5. In the **Compliance report** modal dialog, make selections for system data to include.
6. Make selections for rule data to include.
7. Optionally, add user notes.
8. Click **Export report**.

CHAPTER 5. ENABLING NOTIFICATIONS AND INTEGRATIONS

You can enable the notifications service on Red Hat Hybrid Cloud Console to send notifications whenever a compliance policy is triggered. For example, you can configure the notifications service to automatically send an email message whenever a compliance policy falls below a certain threshold, or to send an email digest of all the compliance policy events that take place each day. Using the notifications service frees you from having to continually check the Red Hat Insights for RHEL dashboard for compliance event-triggered notifications.

Enabling the notifications service requires three main steps:

- First, an Organization Administrator creates a User access group with the Notifications administrator role, and then adds account members to the group.
- Next, a Notifications administrator sets up behavior groups for events in the notifications service. Behavior groups specify the delivery method for each notification. For example, a behavior group can specify whether email notifications are sent to all users, or just to Organization administrators.
- Finally, users who receive email notifications from events must set their user preferences so that they receive individual emails for each event or a daily digest of all compliance events.

In addition to sending email messages, you can configure the notifications service to send event data in other ways:

- Using an authenticated client to query Red Hat Insights APIs for event data
- Using webhooks to send events to third-party applications that accept inbound requests
- Integrating notifications with applications such as Splunk to route compliance events to the application dashboard

Additional resources

- For more information about how to set up notifications for compliance events, see [Configuring notifications and integrations on the Red Hat Hybrid Cloud Console](#).

CHAPTER 6. 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](#)
- [Insights for Red Hat Enterprise Linux Documentation](#)
- [Insights for Red Hat Enterprise Linux Product Support page](#)