Red Hat Insights 2021

Assessing and Monitoring Security Policy Compliance of RHEL Systems

Understanding the Security Compliance Status of your Red Hat Enterprise Linux Infrastructure

Last Updated: 2021-09-13

Red Hat Insights 2021 Assessing and Monitoring Security Policy Compliance of RHEL Systems

Understanding the Security Compliance Status of your Red Hat Enterprise Linux Infrastructure

Legal Notice

Abstract

Assess and track the security-policy compliance status of your RHEL environment to determine compliance level and plan a course of action to resolve compliance issues.

Table of Contents

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 HYBRID CLOUD CONSOLE DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so, create a Bugzilla ticket:

1. Go to the Bugzilla website.
2. As the Component, use **Documentation**.
3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
4. Click **Submit Bug**.

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL COMPLIANCE SERVICE SECURITY POLICY COMPLIANCE ASSESSMENT AND MONITORING

The Insights for Red Hat Enterprise Linux compliance service enables you to assess and monitor the compliance of your Red Hat Enterprise Linux (RHEL) systems with SCAP security policies.

The compliance service provides a simple but powerful user interface, enabling the creation, configuration, and management of SCAP security policies. With the filtering and context-adding features built in, administrators can easily identify and manage security compliance issues in the RHEL infrastructure.

This documentation describes some of the functionality of the compliance service, to help users understand reporting, manage issues, and get the maximum value from the service.

You can also create Ansible Playbooks to resolve security compliance issues and share reports with stakeholders to communicate compliance status.

Additional Resources

- *Remediating Security-Policy Compliance issues using Ansible Playbooks*
- *Generating Compliance Reports*

1.1. REQUIREMENTS AND PREREQUISITES

The compliance service is part of Insights for Red Hat Enterprise Linux, which is included with your Red Hat Enterprise Linux (RHEL) subscription and can be used with all versions of RHEL currently supported by Red Hat. You do not need additional Red Hat subscriptions to use Insights for RHEL and the compliance service.

Verify the following conditions are met before using the compliance service:

- **Register the system with Insights for Red Hat Enterprise Linux.** Register systems with Insights for RHEL from the Insights for RHEL application.
- **Set up OpenSCAP.** Set up OpenSCAP with the ability to report data to the compliance service. Policies can then be added and modified using the compliance service. If you are unfamiliar with OpenSCAP, see Getting Started with OpenSCAP.
- **Create security policies in the compliance service.** In the compliance service, you have to assign each Insights for RHEL-registered system to one or more security policies in order to see results for your systems.

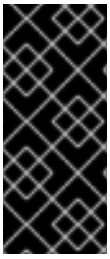
1.2. SUPPORTED CONFIGURATIONS

Accurate compliance reporting requires that the Red Hat-approved version of SCAP Security Guide (SSG) is installed on the system. Red Hat Enterprise Linux minor versions ship and upgrade with the approved SSG version included; although, some organizations may decide to continue using an earlier version temporarily, prior to upgrading.

If a policy includes systems using unsupported SSG versions, an **unsupported** warning, preceded by the number of affected systems, is visible next to the policy in Red Hat Enterprise Linux > Compliance > Reports.

DISA STIG for Red Hat Enterprise Linux 7
DISA STIG for Red Hat Enterprise Linux 7
RHEL 7
0%
0 of 0 systems
1 unsupported

The following table lists the supported SSG version(s) for each minor version of RHEL.



IMPORTANT

The following table lists the supported SSG version for each minor version of RHEL. Packages names look like this: **scap-security-guide-0.1.43-13.el7**. The SSG version in this case is 0.1.43; the release is 13 and architecture is el7. The release number can differ from the version number shown in the table; however, the version number must match as indicated below for it to be a supported configuration.

Table 1.1. Supported versions of the SCAP Security Guide in RHEL

Red Hat Enterprise Linux version	SCAP Security Guide version
RHEL 6.6	scap-security-guide-0.1.18-3.el6
RHEL 6.7	scap-security-guide-0.1.21-3.el6
RHEL 6.8	scap-security-guide-0.1.28-2.el6
RHEL 6.9	scap-security-guide-0.1.28-3.el6
RHEL 6.10	scap-security-guide-0.1.28-4.el6
RHEL 7.2 AUS	scap-security-guide-0.1.25-3.el7
RHEL 7.3 AUS	scap-security-guide-0.1.30-5.el7_3
RHEL 7.4 AUS, E4S	scap-security-guide-0.1.33-6.el7_4
RHEL 7.5 (batch update)	scap-security-guide-0.1.36-10.el7_5
RHEL 7.6 EUS	scap-security-guide-0.1.40-13.el7_6
RHEL 7.7 EUS	scap-security-guide-0.1.43-13.el7
RHEL 7.8 (batch update)	scap-security-guide-0.1.46-11.el7
RHEL 7.9	scap-security-guide-0.1.49-13.el7 scap-security-guide-0.1.52-2.el7_9 scap-security-guide-0.1.54-3.el7_9
RHEL 8.0 SAP	scap-security-guide-0.1.42-11.el8

Red Hat Enterprise Linux version	SCAP Security Guide version
RHEL 8.1 EUS	scap-security-guide-0.1.46-1.el8 scap-security-guide-0.1.47-8.el8_1
RHEL 8.2 (batch update)	scap-security-guide-0.1.48-7.el8
RHEL 8.3	scap-security-guide-0.1.50-14.el8
RHEL 8.4	scap-security-guide-0.1.54-5.el8

What if Red Hat supports more that one SSG for my RHEL minor version?

When more than one SSG version is supported for a RHELminor version, as is the case with RHEL 7.9 and RHEL 8.1, the compliance service will use the latest available version.

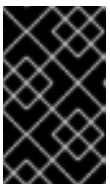
Why is my old policy no longer supported by SSG?

As RHEL minor versions get older, fewer SCAP profiles are supported. To view which SCAP profiles are supported, see tables in SCAP Security Guide profiles supported in RHEL 7 and SCAP Security Guide profiles supported in RHEL 8.

More about limitations of unsupported configurations

The following conditions apply to the results for unsupported configurations:

- These results are a "best-guess" effort because using any SSG version other than what is supported by Red Hat can lead to inaccurate results.



IMPORTANT

Although you can still see results for a system with an unsupported version of SSG installed, those results may be considered inaccurate for compliance reporting purposes.

- Results for systems using an unsupported version of SSG *are not included* in the overall compliance assessment for the policy.
- Remediations are not available for rules on systems with an unsupported version of SSG installed.

1.3. BEST PRACTICES

To benefit from the best user experience and receive the most accurate results in the compliance service, Red Hat recommends that you follow some best practices.

Ensure that the RHEL OS system minor version is visible to the Insights client

If the compliance service cannot see your RHEL OS minor version, then the supported SCAP Security Guide version cannot be validated and your reporting may not be accurate. The Insights client allows users to redact certain data, including Red Hat Enterprise Linux OS minor version, from the data payload that is uploaded to Insights for Red Hat Enterprise Linux. This will prohibit accurate compliance service reporting.

To learn more about data redaction, see the following documentation: Configuring Red Hat Insights client redaction.

Create security policies within the compliance service

Creating your organization's security policies within the compliance service allows you to associate multiple systems with the policy, be assured of using the supported SCAP Security Guide for your RHEL minor version, and edit which rules are included, based on your organization's requirements.

CHAPTER 2. MANAGING SCAP SECURITY POLICIES IN THE COMPLIANCE SERVICE

Create and manage your SCAP security policies entirely within the compliance service. Define new policies and select the rules and systems you want to associate with them, and edit existing policies as your requirements change.

IMPORTANT

Unlike other Insights for Red Hat Enterprise Linux services, the compliance service does not run automatically on a default schedule. In order to upload OpenSCAP data to the Insights for RHEL application, you must run **insights-client --compliance**, either on-demand or on a scheduled job that you set.

2.1. CREATING NEW SCAP POLICIES

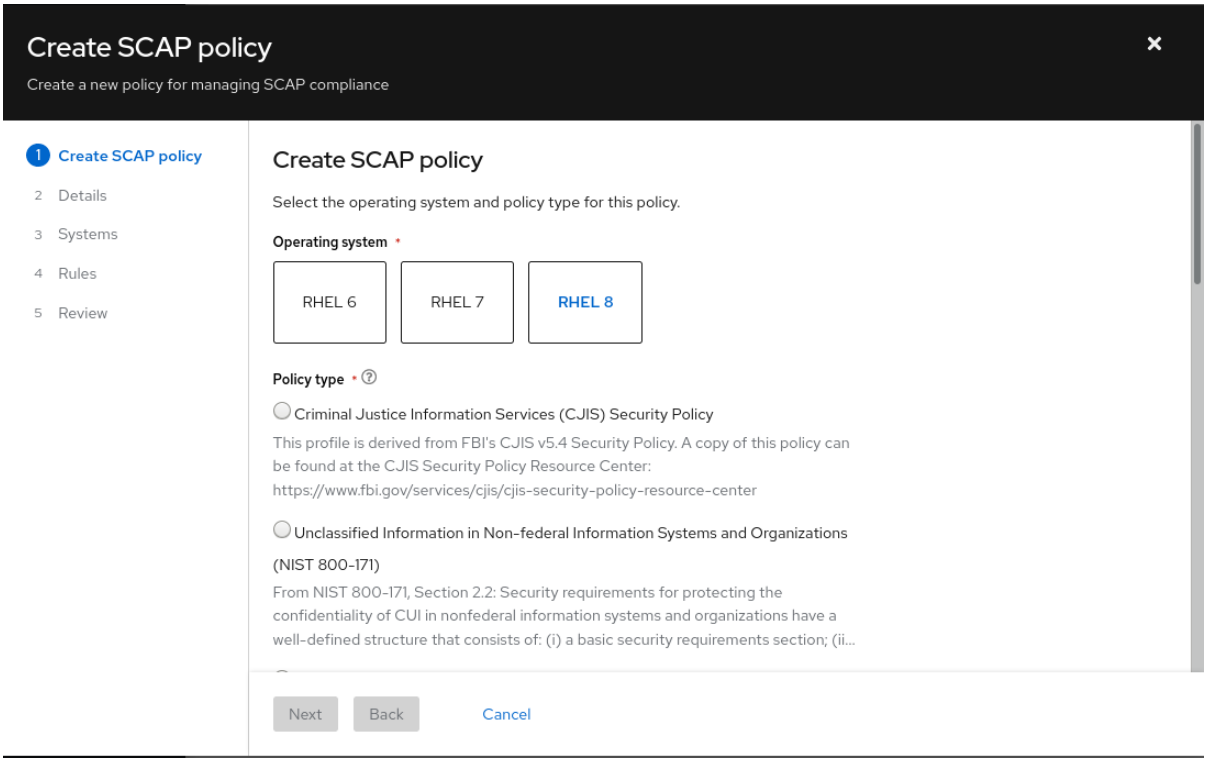
You must add each Insights for RHEL-registered system to a security policy before you will see results for it in the compliance service. To create a new policy, and include specific systems and rules, complete the following steps:

IMPORTANT

If your RHEL servers span across multiple major releases of RHEL, you must create a separate policy for each major release. For example, all of your RHEL 7 servers would be on one *Standard System Security Profile for RHEL* policy and all of your RHEL 8 servers will be on another.

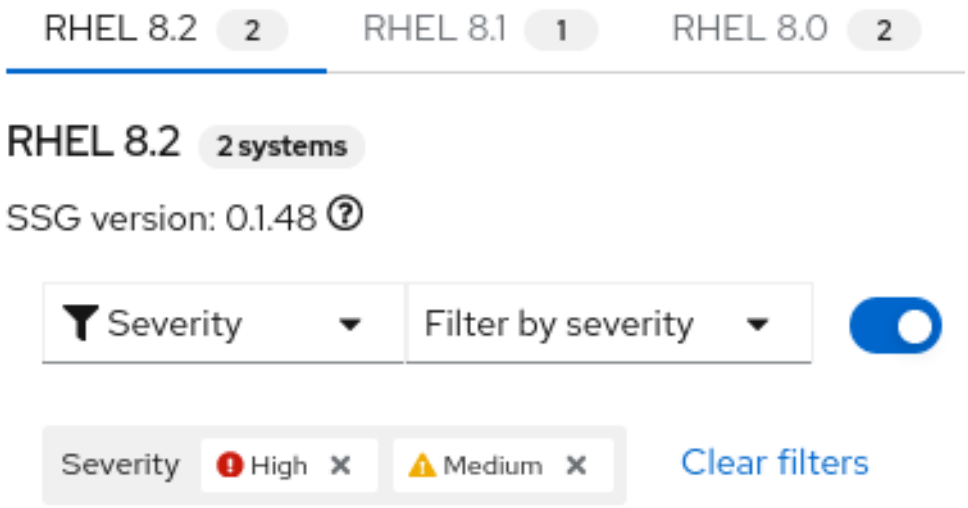
Procedure

1. Log in to Red Hat Hybrid Cloud Console and navigate to the Red Hat Enterprise Linux > Compliance > SCAP policies page.
2. Click the **Create new policy** button.
3. On the **Create SCAP policy** page of the wizard, select the **RHEL major version** of the systems you will include in the policy.



4. Select one of the **policy types** available for that RHEL major version, then click **Next**.
5. On the **Details** page, accept the name and description already provided or provide your own more meaningful entries.
6. Optionally, add a **Business objective** to give context, for example, "CISO mandate."
7. Define a **compliance threshold** acceptable for your requirements and click **Next**.
8. Select the **Systems** to include on this policy and click **Next**. Your selection of a RHEL major version in the first step automatically determines which systems can be added to this policy.
9. Select which **Rules** to include with each policy. Because each minor version of RHEL supports the use of a specific SCAP Security Guide (SSG) version (sometimes more than one, in which case we use the latest), the rule set for each RHEL minor version is slightly different and must be selected separately.

   a. Optionally, use the filtering and search capabilities to refine the list of rules.
   For example, to show only the highest severity rules, click the primary filter dropdown and select **Severity**. In the secondary filter, check the boxes for **High** and **Medium**.



b. The rules shown by default are those designated for that policy type and that version of SSG. By default, the **Selected only** toggle next to the filter boxes is enabled. You may remove this toggle if so desired.

c. Repeat this process as needed **for *each* RHEL minor version tab**.

d. After you select rules for each Red Hat Enterprise Linux minor version SSG, click **Next**.

10. On the **Review** page, verify that the information shown is correct, then click **Finish**.

11. Give the app a minute to create the policy, then click the **Return to application** button to view your new policy located at the bottom of the SCAP policies.

2.2. EDITING EXISTING POLICIES

You may decide after creating a security policy that you want to change which rules (or systems) are included because they may no longer apply to your requirements. Use the following procedure to edit an existing policy to add or remove specific rules.

Procedure

1. Log in to Red Hat Hybrid Cloud Console and navigate to the Red Hat Enterprise Linux > Compliance > SCAP policies page.

2. Locate the policy to edit.

3. On the right side of the policy row, click the more-actions icon, **three vertical dots**, and click **Edit policy**.

4. In the **Edit <Policy name>** card, click the **Rules** tab.

   a. Use the filter or search functions to locate the rules to remove.

IMPORTANT

By default, the **Selected only** toggle to the right of the search box is enabled. You may remove the toggle as needed.

b. Uncheck the box next to any rule you want to remove.

c. Repeat this process as needed for each RHEL minor version SSG tab.

5. Click **Save**.

Verification

1. Navigate to the Red Hat Enterprise Linux > Compliance > SCAP policies page and locate the edited policy.
2. Click on the policy and verify that the included rules are consistent with the edits you made.

CHAPTER 3. UNDERSTANDING YOUR COMPLIANCE SERVICE REPORTING

The compliance service displays the latest available OpenSCAP results for each policy and the associated systems. View summary results for each policy in Red Hat Enterprise Linux > Compliance > Reports.

For a deeper understanding of compliance status per system, filter and sort your data to see which rules have passed and failed.

The following sections describe ways to refine your data, depending on your location in the compliance service, to focus on your most important issues.

3.1. SCAP POLICIES

Use the **Filter by name** search box to locate a specific policy by name. Then click on the policy name to see the policy card, which includes the following information:

- **Details.** View details such as compliance threshold, business objective, OS, and SSG version.
- **Rules.** View and filter the rules included in the specific SSG version of the policy by Name, Severity and Remediation available. Then sort the results by Rule name, Severity or Ansible Playbook support.
- **Systems.** Search by system name to locate a specific system associated with the policy then click the system name to see more information about that system and issues that may affect it.

3.2. SYSTEMS

The default functionality on this page is to search by system name.

- **Name.** Search by system name.
- **Policy.** Search by policy name and see the systems included in that policy.
- **Operating system.** Search by RHEL OS major versions to see only RHEL 7 or RHEL 8 systems.

3.3. SEARCHING

The search function in the compliance service works in the context of the page you are viewing.

- **SCAP Policies.** Search for a specific policy by name.
- **Systems.** Search by system name, policy, or Red Hat Enterprise Linux operating system major version.
- **Rules list (single system).** The rules list search function allows you to search by the rule name or identifier. Identifiers are shown directly below the rule name.

3.4. FILTERING

Filtering is available from multiple views in the compliance service and filtering options are unique to the page view. The **Filters** icon is located on the left side of the **Search field**. Click the down arrow and check the boxes to set filters.

- **Systems list.** Filter by Name, Status, and Source.
- **Single system rules list.** Filter rules that have passed or not passed, or by rule severity.

CHAPTER 4. REFERENCE MATERIALS

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

- *Remediating Security-Policy Compliance issues using Ansible Playbooks*
- *Generating Compliance Reports*
- Insights for Red Hat Enterprise Linux Documentation
- Insights for Red Hat Enterprise Linux Product Support page