Red Hat Insights 2020-10

Assessing and Monitoring Security Policy Compliance of RHEL Systems

Understanding the Security Compliance Status of your Infrastructure

Last Updated: 2021-03-04

Red Hat Insights 2020-10 Assessing and Monitoring Security Policy Compliance of RHEL Systems

Understanding the Security Compliance Status of your 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. 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 AND ASSESSMENT 3
1.1. REQUIREMENTS AND PREREQUISITES 3
1.2. SUPPORTED CONFIGURATIONS 3
1.3. BEST PRACTICES 5

CHAPTER 2. MANAGING SCAP SECURITY POLICIES IN THE COMPLIANCE SERVICE 6
2.1. CREATING NEW SCAP POLICIES 6
2.2. EDITING EXISTING POLICIES 7

CHAPTER 3. UNDERSTANDING YOUR COMPLIANCE SERVICE REPORTING 9
3.1. SCAP POLICIES 9
3.2. SYSTEMS 9
3.3. SEARCHING 9
3.4. FILTERING 9
3.5. SORTING YOUR DATA 10

CHAPTER 4. REFERENCE MATERIALS 11

CHAPTER 1. COMPLIANCE SERVICE REPORTING AND ASSESSMENT

The Red Hat Insights 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 administrators understand Compliance service reporting, manage issues, and get re-mediatingue from Compliance 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 Red Hat Insights, 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 Red Hat Insights and the Compliance service.

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

- **Install and register the Insights client.** If your RHEL system does not already have the Insights client installed and operational, follow the Red Hat Insights, Get Started instructions to install and register the client on each system you want to monitor.
- **Set up OpenSCAP.** OpenSCAP has been set up for your organization, with SCAP security guides (SSGs) and datastreams, and can 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.

1.2. SUPPORTED CONFIGURATIONS

Use the supported version of SCAP Security Guide (SSG) for the RHEL minor version

Accurate reporting requires that you use the correct, Red Hat-supported version of the SCAP Security Guide (SSG) for the **RHEL minor version** installed on the system. Officially supported versions of the SCAP Security Guide are versions provided in the related minor release of RHEL or in the related batch update of RHEL. If a policy includes one or more systems with an unsupported SSG version installed, an **unsupported** notification, preceded by the number of affected systems, is visible in Compliance service > Reports.

You can still see failed rules on the system with an unsupported version of SSG installed but results may not be considered accurate for compliance reporting purposes. 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.
- Results from systems with an unsupported version of SSG installed are not included in the overall compliance assessment for the policy.
- Remediations are unavailable for rules on systems with an unsupported version of SSG installed.

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 6.9	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
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

1.3. BEST PRACTICES

To benefit from the best user experience and receive the most accurate information in the Compliance service, Red Hat Insights recommends that you follow a few best practices.

Ensure that your RHEL systems are registered with the Insights client

The Insights client must be installed and registered on the system from which you wish to see Compliance reporting. Enter the insights-client command with the --register option to register your RHEL system with Red Hat Insights:

```
[root@insights]# insights-client --register
```

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

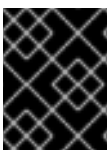
The Insights client allows users to redact certain data, including RHEL OS minor version, from the data payload uploaded to Red Hat Insights. If the Compliance service cannot see your RHEL OS minor version, then the supported SCAP Security Guide version cannot be validated and your reporting may not be accurate.

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

Define security policies within the Compliance service

As of November 2020, you must create and define your organization's security policies within the Compliance service. Policies created externally are no longer supported and results for those policies will no longer be included in your results.

Creating policies within the Compliance service enables you to get the most feature-rich user experience and reliable reporting. Associate multiple systems with a policy; be assured of using the Red Hat-supported SSG for your RHEL version; edit which rules are included in the policy, based on your organization's specific requirements.

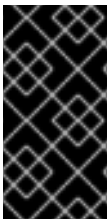


IMPORTANT

The Compliance service will no longer support any externally sourced and uploaded policies after November 2020.

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. Edit existing policies as your requirements change.



IMPORTANT

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

2.1. CREATING NEW SCAP POLICIES

To use the Compliance service, you must associate SCAP security policies with your Insights-registered RHEL systems. A policy is defined for a single major release such as RHEL 7 but can span multiple minor versions. If your RHEL servers span across multiple major releases of RHEL, you will need to create one policy per major release. Compliance service users must create their policies within the Compliance service.

To create a new policy using the Compliance service, complete the following steps:

Procedure

1. Navigate to the Compliance service > SCAP Policies page and log in if necessary.
2. Click the blue, **Create new policy** button to open the **Create SCAP policy wizard**
3. On the **Create SCAP policy** page of the wizard, make the following selections:
   a. Select the correct RHEL **operating system** version on the systems you want to monitor.

NOTE

SCAP policies are RHEL-version specific. If you want to use the DISA STIG policy type, for example, for systems running RHEL 7 and for systems running RHEL 8, you must create two policies, one for each major version of RHEL.

   b. Select a **Policy type**.

NOTE

The profile options are predetermined by the latest available 'scap-security-guide' for the OS version you chose in the previous step.

NOTE

If the policy is already being use for that RHEL version, you can add new systems to it.

c. Click **Next**.

4. On the **Policy details** page, review the prepopulated information in each field or change as needed to suit your requirements:

   a. Provide a descriptive **Policy name**.

   b. The **Reference ID** cannot be changed.

   c. The **Description** is prepopulated with the policy description from OpenSCAP but you can add more detail.

   d. Specify a **Compliance threshold** for the systems associated with this policy. In cases where 100% compliance is unrealistic, you can specify an acceptable level of compliance here.

   e. Click **Next**.

5. On the **Rules** page, search or scroll through the list of rules and tailor the policy to your requirements by clearing unneeded rules, then click **Next**.

NOTE

At this time, you can only modify the rule set when the policy is created. Changing rules in existing policies is not currently available.

6. On the **Systems** page, check the box next to each system you want to associate with this policy, then click **Next**.

NOTE

Enter a system name in the Search box, or filter by Status or Source to see a subset of your systems.

7. On the **Review** page, ensure that the policy information is correct, then click **Finish**.

8. On the Compliance service > Reports page, click on your policy and verify that details, including systems, are correct.

2.2. EDITING EXISTING POLICIES

Use the following procedure to edit existing policies in the Compliance service to change policy details, business objective, compliance threshold, and included systems.

NOTE

The ability to edit existing policies is an evolving feature set; additional capabilities are coming soon, including the ability to add or remove the rules included in an existing policy.

Procedure

1. Log in to cloud.redhat.com and navigate to the Compliance > SCAP Policies page.

2. Use the search or filtering functionality to locate the policy to edit.

3. On the far-right side of the policy row, click the more-actions icon and select Edit policy.
4. In the Edit <Policy name> card, click each tab to edit the following information:
    a. In **Details**, edit *Policy description*, *Business objective*, and *Compliance threshold*.
    b. **Rule** editing is coming soon.
    c. In the **Systems** tab, select systems to add to the policy, or, using search and filters, find and clear systems that you no longer wish to include.
5. Navigate to the SCAP Policies page and locate the edited policy.
6. Click on the policy and verify that the details and included systems 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 system. View summary results for each policy in Red Hat Insights Compliance > Reports .

For a deeper understanding of compliance status per system, and to reduce the "noise" of many systems reporting data, you can 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 Search function 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 versions.
- **Rules.** View and filter the rules included in the specific SSG version of the policy by name and severity, then sort 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.
- Break systems into smaller groups by
  - **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 RHEL 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.

3.5. SORTING YOUR DATA

You can order your results by sorting columns in the Compliance service Systems list and the Rules list for a policy. The following columns are sortable on each list:

- **Compliance service Systems list**
  - System name (Alphabetical)
  - Policy name (Alphabetical)
  - Compliance score (Percentage of rules passed on a system)
  - Last scan (Time elapsed since last scan)
- **Rules list for a policy**
  - Rule name (Alphabetical)
  - Severity (Low, Medium, High, Critical)
  - Ansible support (Playbook available or not available)

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*
- Red Hat Insights Documentation
- Red Hat Insights Product Support page