Red Hat Insights 2023

Assessing and Monitoring Security Policy Compliance of RHEL Systems

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

Last Updated: 2023-03-24

Red Hat Insights 2023 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. 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 .

Table of Contents

CHAPTER 1. INSIGHTS FOR RED HAT ENTERPRISE LINUX COMPLIANCE SERVICE OVERVIEW

The Red Hat Insights for Red Hat Enterprise Linux compliance service enables IT security and compliance administrators to assess, monitor, and report on the security-policy compliance of RHEL systems.

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, IT security 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 Service Reports*

1.1. REQUIREMENTS AND PREREQUISITES

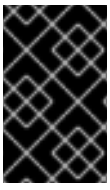
The compliance service is part of Red Hat Insights for Red Hat Enterprise Linux, which is included with your Red Hat Enterprise Linux (RHEL) subscription and can be used with all versions of RHEL currently supported by Red Hat. You do not need additional Red Hat subscriptions to use Insights for Red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

1.2. USER ACCESS FOR COMPLIANCE SERVICE USERS

Before you can access certain features in the Insights for RHEL application, you must have the correct permissions. These permissions are granted in Red Hat Hybrid Cloud Console > User Access > Groups . An Organization Administrator or User Access administrator must add you as a member to a User Access group with the required roles.

By default, User Access on the Red Hat Hybrid Cloud Console has preconfigured **Compliance administrator** (all access) and **Compliance viewer** (read-only access) roles. If your organization determines that the predefined roles provide insufficient access, a User Access administrator can configure a custom role to provide the specific permissions that your users require.

The following sections in this chapter describe each of the predefined roles for compliance service users.



IMPORTANT

Changes to User Access must be performed by an Organization Administrator on your Red Hat account, or by an account user who is a member of a User Access group with the User Access administrator role.

Additional resources

User Access https://access.redhat.com/documentation/en-us/red_hat_hybrid_cloud_console/2023/html/user_access_configuration_guide_for_role-based_access_control_rbac/index

1.2.1. Compliance administrator role

The **Compliance administrator** role is a predefined role in the **Default admin access group**. All Insights for Red Hat Enterprise Linux users on your account are members of the **Default access** group. In its default configuration, members of a group with the **Compliance administrator** role have access to all compliance service resources.

Your organization might decide that the predefined role is too limited or too permissive. To limit access to some features, or to add additional permissions, a **User Access administrator** can customize the role and configure it with whatever permissions are required. Customizing the preconfigured role replaces the **Default access group** with the customized role.

1.2.2. Compliance viewer role

In its default configuration, the **Compliance viewer** role is included in the **Default access group** and can read any compliance service resource. The **Compliance viewer** role includes the following permissions:

- View data in systems section Red Hat Enterprise Linux > Compliance > Systems .
- View SCAP policies Red Hat Enterprise Linux > Compliance > SCAP policies .
- View, download and export reports (incuding PDFs) in compliance service reports *Generating Compliance Service Reports*].

If your organization determines that the default configuration of the Compliance viewer role is inadequate, a User Access administrator can create a custom role with the specific permissions required.

1.3. SUPPORTED CONFIGURATIONS

Red Hat supports specific versions of the SCAP Security Guide (SSG) for each minor version of Red Hat Enterprise Linux (RHEL). The rules and policies in an SSG version are only accurate for one RHEL minor version. In order to receive accurate compliance reporting, the system must have the supported SSG version installed.

Red Hat Enterprise Linux minor versions ship and upgrade with the supported SSG version included. However, 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.

NOTE

For more information about which versions of the SCAP Security Guide are supported in RHEL, refer to Insights Compliance - Supported configurations .

Example of a compliance policy with a system running an unsupported version of SSG

1.3.1. Frequently asked questions about the compliance service

How do I interpret the SSG package name?

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.

What if Red Hat supports more than 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.

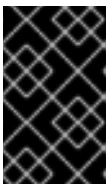
Why is my old policy no longer supported by SSG?

As RHEL minor versions get older, fewer SCAP profiles are supported. To view which SCAP profiles are supported, refer to Insights Compliance - Supported configurations .

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.

1.4. 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 Red Hat 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. GETTING STARTED USING THE COMPLIANCE SERVICE

The following procedure describes how to configure your RHEL systems to report compliance data to the Insights for RHEL application. This installs necessary additional components such as the SCAP Security Guide (SSG), which is used to perform the compliance scan.

Prerequisites

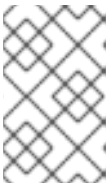
- The Insights client is deployed on the system.
- You must have root privileges on the system.

Procedure

1. Check the version of RHEL on the system:

```
[user@insights]$ cat /etc/redhat-release
```

2. Review the Insights Compliance – Supported configurations article and make note of the supported SSG version for the RHEL minor version on the system.



NOTE

Some minor versions of RHEL support more than one version of SSG. The Insights compliance service will always show results for the latest supported version.

3. Check if the supported version of the SSG package is installed on the system:
Example – for RHEL 8.4 run:

```
[root@insights]# dnf info scap-security-guide-0.1.57-3.el8_4
```

4. If it isn't already installed, install the supported version of SSG on the system.
Example – for RHEL 8.4 run:

```
[root@insights]# dnf install scap-security-guide-0.1.57-3.el8_4
```

5. In the compliance service UI, Red Hat Enterprise Linux > Compliance > SCAP policies , add the system to a policy.
   a. Click **Create new policy** to add the system to a new security policy.
   b. Or, select an existing policy and click **Edit policy** to add the system to it.
6. After adding each system to the desired security policy, return to the system and run the compliance scan using:

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

NOTE

The scan can take 1-5 minutes to complete.

7. Navigate to *Generating Compliance Service Reports* to view results.
8. Optionally, schedule the compliance jobs to run with cron .

Additional Resources

To learn which versions of the SCAP Security Guide are supported for Red Hat Enterprise Linux minor versions, see Insights Compliance - Supported configurations .

CHAPTER 3. MANAGING SCAP SECURITY POLICIES IN THE INSIGHTS FOR RHEL COMPLIANCE SERVICE

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

IMPORTANT

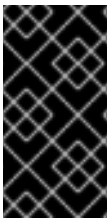
Unlike most other Red Hat Insights for Red Hat Enterprise Linux services, the compliance service does not run automatically on a default schedule. In order to upload OpenSCAP data to the Insights for Red Hat Enterprise Linux application, you must run **insights-client --compliance**, either on-demand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

Additional resources

How do I set up recurring uploads for Insights services?

3.1. CREATING NEW SCAP POLICIES

You must add each Insights for Red Hat Enterprise Linux-registered system to one or more security policies before you can perform a scn or see results for that scan in the compliance service UI. To create a new policy, and include specific systems and rules, complete the following steps:

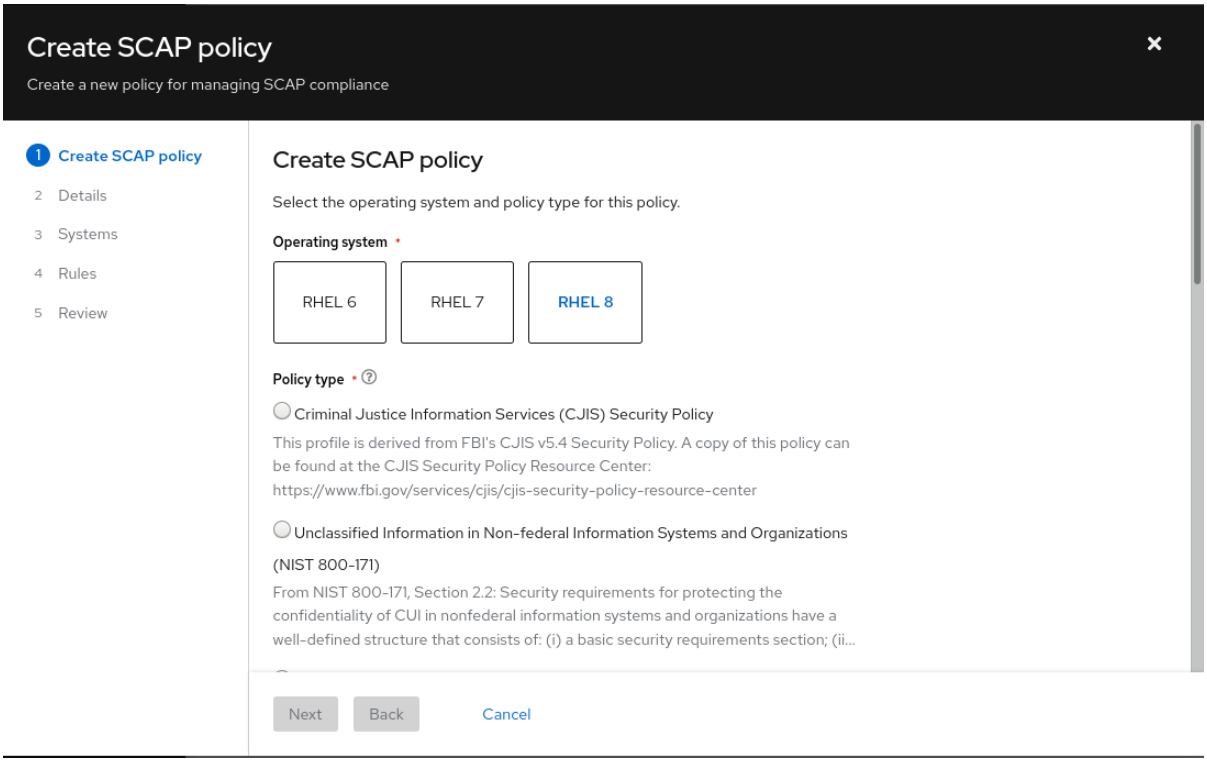


IMPORTANT

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.

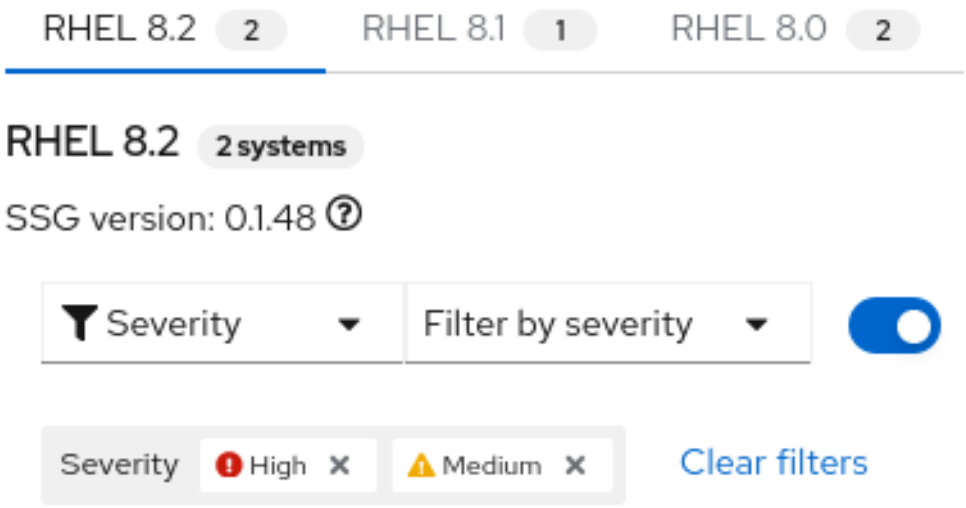
6. Optionally, add a **Business objective** to give context, for example, "CISO mandate."

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.

NOTE

You have to go to the system and run the compliance scan before results will be shown in the compliance service UI.

3.2. 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

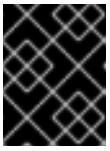
1. Log in to Red Hat Hybrid Cloud Console and navigate to the Red Hat Enterprise Linux > Compliance > SCAP policies page.

2. Locate the policy to edit.

3. On the right side of the policy row, click the More Actions icon, , 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.

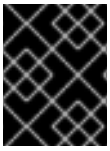
2. Click on the policy and verify that the included rules are consistent with the edits you made.

CHAPTER 4. ANALYZING AND TRIAGING YOUR COMPLIANCE REPORTS

The compliance service displays data for each policy and system registered (and reporting data) to the service. This can be a lot of data, most of which might not be relevant to your immediate goals.

The following sections discuss ways to refine the bulk of compliance service data—in Reports, SCAP policies, and Systems—to focus on the systems or policies that matter the most to you.

The compliance service enables users to set filters on lists of systems, rules, and policies. Like other Insights for Red Hat Enterprise Linux services, the compliance service also enables filtering by system-group tags. However, because compliance-registered systems use a different reporting mechanism, the tag filters must be set directly in lists of systems in the compliance UI views, rather than from the global, **Filter by status** dropdown used elsewhere in the Insights application.



IMPORTANT

To see accurate data for your systems, always run **insights-client --compliance** on each system prior to viewing the results in the UI.

4.1. REPORTS

Red Hat Enterprise Linux > Compliance > Reports

From the Reports page, use the following primary and secondary filters to focus on a specific or narrow set of reports:

- **Policy name.** Search for a policy by name.
- **Policy type.** Select from the policy types configured for your infrastructure in the compliance service.
- **Operating system.** Select one or more RHEL OS major versions.
- **Systems meeting compliance.** Show policies for which a percentage (range) of included systems are compliant.

4.2. SCAP POLICIES

Red Hat Enterprise Linux > Compliance > 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.

4.3. SYSTEMS

Red Hat Enterprise Linux > Compliance > Systems

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

- **Tags.** Search by system group or tag 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.

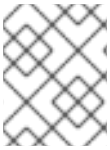
4.4. SEARCHING

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.

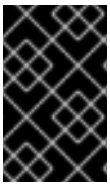
CHAPTER 5. SYSTEM TAGS AND GROUPS

Red Hat Insights for Red Hat Enterprise Linux enables administrators to filter groups of systems in inventory and in individual services using group tags. Groups are identified by the method of system data ingestion to Insights for Red Hat Enterprise Linux. Insights for Red Hat Enterprise Linux enables filtering groups of systems by those running SAP workloads, by Satellite host group, by Microsoft SQL Server workload, and by custom tags that are defined by system administrators with root access to configure the Insights client on the system.



NOTE

As of Spring 2022, inventory, advisor, compliance, vulnerability, patch, drift, and policies enable filtering by groups and tags. Other services will follow.



IMPORTANT

Unlike the other services that enable tagging, the compliance service sets tags within lists of systems in the compliance service UI. For more information, see Group and tag filters in the compliance service.

Use the global, **Filter results** box to filter by SAP workloads, Satellite host groups, MS SQL Server workloads, or by custom tags added to the Insights client configuration file.

Prerequisites

The following prerequisites and conditions must be met to use the tagging features in Red Hat Insights for Red Hat Enterprise Linux:

- The Red Hat Insights client is installed and registered on each system.
- You must have root permissions, or their equivalent, to create custom tags or change the **/etc/insights-client/tags.yaml** file.

5.1. SAP WORKLOADS

As Linux becomes the mandatory operating system for SAP ERP workloads in 2025, Red Hat Enterprise Linux and Red Hat Insights for Red Hat Enterprise Linux are working to make Insights for Red Hat Enterprise Linux the management tool of choice for SAP administrators.

As part of this ongoing effort, Insights for Red Hat Enterprise Linux automatically tags systems running SAP workloads and by SAP ID (SID), without any customization needed by administrators. Users can easily filter those workloads throughout the Insights for Red Hat Enterprise Linux application by using the global **Filter by tags** drop-down menu.

5.2. SATELLITE HOST GROUPS

Satellite host groups are configured in Satellite and recognized automatically by Insights for Red Hat Enterprise Linux.

5.3. MICROSOFT SQL SERVER WORKLOADS

Using the global **Filter by tags** feature, Red Hat Insights for Red Hat Enterprise Linux users can select groups of systems running Microsoft SQL Server workloads.

In May of 2019, the Red Hat Insights team introduced a new set of Insights for Red Hat Enterprise Linux recommendations for Microsoft SQL Server running on Red Hat Enterprise Linux (RHEL). These rules alert administrators to operating system level configurations that do not conform to the documented recommendations from Microsoft and Red Hat.

A limitation of these rules was that they primarily analyzed the operating system and not the database itself. The latest release of Insights for Red Hat Enterprise Linux and RHEL 8.5, introduces Microsoft SQL Assessment API. The SQL Assessment API provides a mechanism to evaluate the database configuration of MS SQL Server for best practices. The API is delivered with a rule set containing best practice rules suggested by the Microsoft SQL Server Team. While this rule set is enhanced with the release of new versions, the API is built with the intent to give a highly customizable and extensible solution, which enables users to tune the default rules and create their own.

The SQL Assessment API is supported by PowerShell for Linux (available from Microsoft), and Microsoft has developed a PowerShell script that can be used to call the API and store its results as a JSON formatted file. With RHEL 8.5, the Insights client now uploads this JSON file and presents the results in an easy-to-understand format in the Insights for Red Hat Enterprise Linux UI.

For more information about SQL Server assessment in Insights for Red Hat Enterprise Linux, see SQL Server database best practices now available through Red Hat Insights.

5.3.1. Setting up SQL Server assessments

To configure the Microsoft SQL Assessment API to provide information to Red Hat Insights, the database administrator needs to take the following steps.

Procedure

1. In the database you wish to assess, create a login for SQL Server assessments using SQL Authentication. The following Transact-SQL creates a login. Replace **<*PASSWORD*>** with a strong password:

```
USE [master]
GO
CREATE LOGIN [assessmentLogin] with PASSWORD= N'<*PASSWORD*>'
ALTER SERVER ROLE [sysadmin] ADD MEMBER [assessmentLogin]
GO
```

2. Store the credentials for login on the system as follows, again replacing <*PASSWORD*> with the password you used in step 1.

```
# echo "assessmentLogin" > /var/opt/mssql/secrets/assessment
# echo "<*PASSWORD*>" >> /var/opt/mssql/secrets/assessment
```

3. Secure the credentials used by the assessment tool by ensuring that only the mssql user can access the credentials.

```
# chmod 0600 /var/opt/mssql/secrets/assessment
# chown mssql:mssql /var/opt/mssql/secrets/assessment
```

4. Download PowerShell from the microsoft-tools repository. This is the same repository you configured when you installed the **mssql-tools** and **mssqlodbc17** packages as part of SQL Server installation.

```
# yum -y  install powershell
```

5. Install the SQLServer module for PowerShell. This module includes the assessment API.

```
# su mssql -c "/usr/bin/pwsh -Command Install-Module SqlServer"
```

6. Download the runassessment script from the Microsoft examples GitHub repository. Ensure it is owned and executable by mssql.

```
# /bin/curl -LJ0 -o /opt/mssql/bin/runassessment.ps1
https://raw.githubusercontent.com/microsoft/sql-server-samples/master/samples/manage/sql-assessment-api/RHEL/runassessment.ps1
# chown mssql:mssql /opt/mssql/bin/runassessment.ps1
# chmod 0700 /opt/mssql/bin/runassessment.ps1
```

7. Create the directory that will store the log file used by Red Hat Insights. Again, make sure it is owned and executable by mssql.

```
# mkdir /var/opt/mssql/log/assessments/
# chown mssql:mssql /var/opt/mssql/log/assessments/
# chmod 0700 /var/opt/mssql/log/assessments/
```

8. You can now create your first assessment, but be sure to do so as the user mssql so that subsequent assessments can be run automatically via cron or systemd more securely as the mssql user.

```
# su mssql -c "pwsh -File /opt/mssql/bin/runassessment.ps1"
```

9. Insights for Red Hat Enterprise Linux will automatically include the assessment next time it runs, or you can initiate Insights client by running this command:

```
# insights-client
```

5.3.1.1. Setting up the SQL Assessment on a timer

Because SQL Server Assessments can take 10 minutes or more to complete, it may or may not make sense for you to run the assessment process automatically every day. If you would like to run them automatically, the Red Hat SQL Server community has created systemd service and timer files to use with the assessment tool.

Procedure

1. Download the following files from Red Hat public SQL Server Community of Practice GitHub site.
   - **mssql-runassessment.service**
   - **mssql-runassessment.timer**
2. Install both files in the directory /**etc**/**systemd**/**system**/:

```
# cp mssql-runassessment.service /etc/systemd/system/
# cp mssql-runassessment.timer /etc/systemd/system/
# chmod 644 /etc/systemd/system/
```

3. Enable the timer with:

```
# systemctl enable --now mssql-runassessment.timer
```

5.4. CUSTOM SYSTEM TAGGING

By applying custom grouping and tagging to your systems, you can add contextual markers to individual systems, filter by those tags in the Insights for Red Hat Enterprise Linux application, and more easily focus on related systems. This functionality can be especially valuable when deploying Insights for Red Hat Enterprise Linux at scale, with many hundreds or thousands of systems under management.

In addition to the ability to add custom tags to several Insights for Red Hat Enterprise Linux services, you can add predefined tags. The advisor service can use those tags to create targeted recommendations for your systems that might require more attention, such as those systems that require a higher level of security.

NOTE

To create custom and predefined tags, you must have root permissions, or their equivalent, to add to, or change the **/etc/insights-client/tags.yaml** file.

5.4.1. Tag structure

Tags use a **namespace/key=value** paired structure.

- **Namespace.** The namespace is the name of the ingestion point, *insights-client*, and cannot be changed. The **tags.yaml** file is abstracted from the namespace, which is injected by the Insights client before upload.
- **Key.** The key can be a user-chosen key or a predefined key from the system. You can use a mix of capitalization, letters, numbers, symbols and whitespace.
- **Value.** Define your own descriptive string value. You can use a mix of capitalization, letters, numbers, symbols and whitespace.

NOTE

The advisor service includes Red Hat-supported predefined tags.

5.4.2. Creating a tags.yaml file and adding a custom group

Create and add tags to **/etc/insights-client/tags.yaml** simply by using **insights-client --group=<name-you-choose>**, which performs the following actions:

- Creates the **etc/insights-client/tags.yaml** file
- Adds the **group=** key and **<name-you-choose>** value to **tags.yaml**
- Uploads a fresh archive from the system to the Insights for Red Hat Enterprise Linux application so the new tag is immediately visible along with your latest results

After creating the initial **group** tag, add additional tags as needed by editing the **/etc/insights-client/tags.yaml** file.

The following procedure shows how to create the **/etc/insights-client/tags.yaml** file and the initial group, then verify the tag exists in the Insights for Red Hat Enterprise Linux inventory.

Procedure to create new group

1. Run the following command as root, adding your custom group name after **--group=**:

```
[root@server ~]# insights-client --group=<name-you-choose>
```

Example of tags.yaml format

The following example of a **tags.yaml** file shows an example of file format and additional tags added for the new group:

```
# tags
---
group: eastern-sap
name: Jane Example
contact: jexample@corporate.com
Zone: eastern time zone
Location:
- gray_rack
- basement
Application: SAP
```

Procedure to verify your custom group was created

1. Navigate to Red Hat Enterprise Linux > Inventory and log in if necessary.
2. Click the **Filter results** dropdown menu.
3. Scroll through the list or use the search function to locate the tag.
4. Click the tag to filter by it.
5. Verify that your system is among the results on the advisor systems list.
6. Procedure to verify the system is tagged
7. Navigate to Red Hat Enterprise Linux > Inventory and log in if necessary.
8. Activate the **Name** filter and begin typing the system name until you see your system, then select it.
9. Verify that, next to the system name, the tag symbol is darkened and shows a number representing the correct number of tags applied.

5.4.3. Editing tags.yaml to add or change tags

After creating the group filter, edit the contents of **/etc/insights-client/tags.yaml** as needed to add or modify tags.

Procedure

Procedure

1. Using the command line, open the tag configuration file for editing.
   [root@server ~]# vi /etc/insights-client/tags.yaml

2. Edit content or add additional values as needed. The following example shows how you can organize **tags.yaml** when adding multiple tags to a system.

```
# tags
---
group: eastern-sap
location: Boston
description:
- RHEL8
- SAP
key 4: value
```

NOTE

Add as many key=value pairs as you need. Use a mix of capitalization, letters, numbers, symbols, and whitespace.

3. Save your changes and close the editor.

4. Optionally, generate an upload to Insights for Red Hat Enterprise Linux.

```
# insights-client
```

5.4.4. Using predefined system tags to get more accurate Red Hat Insights advisor service recommendations and enhanced security

Red Hat Insights advisor service recommendations treat every system equally. However, some systems may require a higher level of security than others, or require different networking performance levels. In addition to the ability to add custom tags, Red Hat Insights for Red Hat Enterprise Linux provides predefined tags which can be used by the advisor service to create targeted recommendations for your systems that might require more attention.

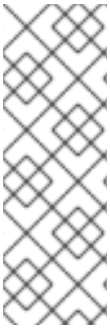
To opt in and get the extended security hardening and enhanced detection and remediation capabilities offered by predefined tags, you need to configure the tags. After configuration, the advisor service provides recommendations based on tailored severity levels, and preferred network performance that apply to your systems.

To configure the tags, use the **/etc/insights-client/tags.yaml** file to tag systems with predefined tags in a similar way that you might use it to tag systems in the inventory service. The predefined tags are configured using the same **key=value** structure used to create custom tags. Details about the Red Hat-predefined tags are in the following table.

Table 5.1. List of Supported Predefined Tags

Key	Value	Note

Key	Value	Note
security	**normal** (default) / **strict**	With **default**, the advisor service compares the system's risk profile to a baseline derived from the default configuration of the latest version of RHEL and from frequently-used usage patterns, keeping recommendations focused, actionable, and low in numbers. With the **strict**, value, the advisor service considers the system to be security-sensitive, causing specific recommendations to use a stricter baseline, potentially showing recommendations even on fresh up-to-date RHEL installations.
network_performance`	**null** (default) / **latency** / **throughput**	The preferred network performance (either latency or throughput according to your business requirement) would affect the severity of an advisor service recommendation to a system.



NOTE

The predefined tag keys names are reserved. If you already use the key **security**, with a value that differs from one of the predefined values, you will not see a change in your recommendations. You will only see a change in recommendations if your existing **key=value** is the same as one of the predefined keys. For example, if you have a **key=value** of **security: high**, your recommendations will not change because of the Red Hat-predefined tags. If you currently have a **key=value** pair of **security: strict**, you will see a change in the recommendations for your systems.

Additional resources

- Using system tags to enable extended security hardening recommendations
- Leverage tags to make Red Hat Insights Advisor recommendations understand your environment better
- Custom system tagging

5.4.5. Configuring predefined tags

You can use the Red Hat Insights for Red Hat Enterprise Linux advisor service's predefined tags to adjust the behavior of recommendations for your systems to gain extended security hardening and enhanced detection and remediation capabilities. This section describes how to configure the predefined tags.

Prerequisites

- You have root-level access to your system
- You have Insights client installed
- You have systems registered within the Insights client
- You have already created the **tags.yaml** file. See Creating a tags.yaml file and adding a custom group

Procedure

- Using the command line, open the **tags.yaml** configuration file located in **/etc/insights-client/** using your preferred editor. (The following example uses Vim.)

```
[root@server ~]# vi /etc/insights-client/tags.yaml
```

- Edit the **/etc/insights-client/tags.yaml** file to add the predefined **key=value** pair for the tags. This example shows how to add **security: strict** and **network_performance: latency** tags.

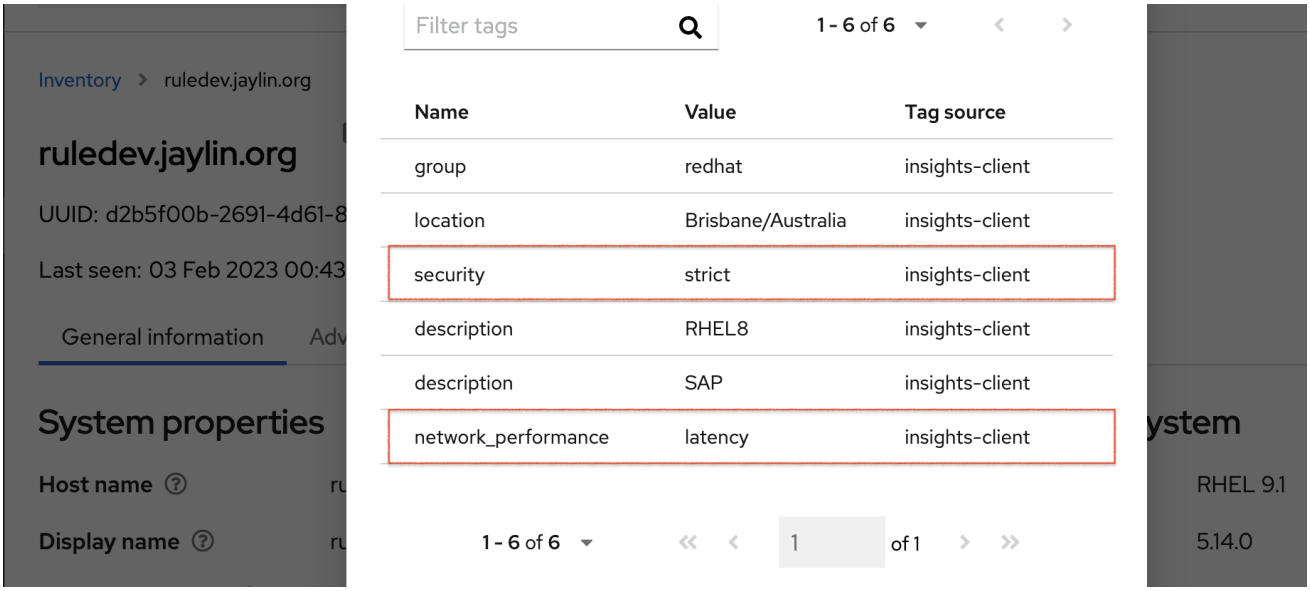
```
# cat /etc/insights-client/tags.yaml
group: redhat
location: Brisbane/Australia
description:
- RHEL8
- SAP
security: strict
network_performance: latency
```

- Save your changes.
- Close the editor.
- **Optional:** Run the **insights-client** command to generate an upload to Red Hat Insights for Red Hat Enterprise Linux, or wait until the next scheduled Red Hat Insights upload.

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

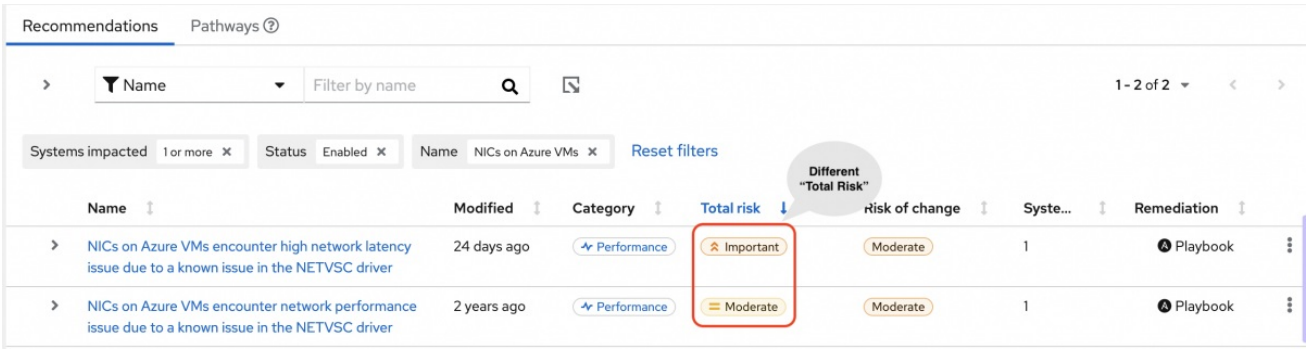
Confirming that predefined tags are in your production area

After generating an upload to Red Hat Insights (or waiting for the next scheduled Insights upload), you can check whether the tags are in the production environment by accessing Red Hat Enterprise Linux > Inventory. Find your system and look for the new tags. You should see something similar to what is shown in the following image.



Example of recommendations after applying a predefined tag

In the following image, the advisor service shows a system with the **network_performance: latency** tag configured.



The system shows a recommendation with a higher Total Risk that is categorized as Important. The system without the **network_performance: latency** tag is categorized with a Total Risk of Moderate. You can make decisions about prioritizing the system with the higher Total Risk.

CHAPTER 6. REFERENCE MATERIALS

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

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

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.