Red Hat Insights 2022

Assessing and Monitoring Security Policy Compliance of RHEL Systems

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

Last Updated: 2022-06-16

Red Hat Insights 2022 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 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. INSIGHTS FOR RHEL COMPLIANCE SERVICE OVERVIEW

The 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

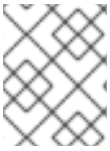
The compliance service is part of Insights for Red Hat Enterprise Linux, which is included with your Red Hat Enterprise Linux (RHEL) subscription and can be used with all versions of RHEL currently supported by Red Hat. You do not need additional Red Hat subscriptions to use Insights for RHEL and the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

1.2. 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

1.2.1. 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.

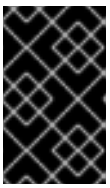
Why is my old policy no longer supported by SSG?

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.

1.3. 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. 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

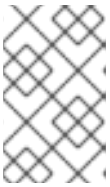
- The Insights client is deployed on the system.
- You must have root privileges on the system.

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 .

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.

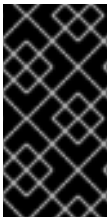
IMPORTANT

Unlike most other 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.

1. Additional resources For more information about scheduling compliance scans, see *How do I setup recurring uploads for Insights services?*.

3.1. CREATING NEW SCAP POLICIES

You must add each Insights for RHEL-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:

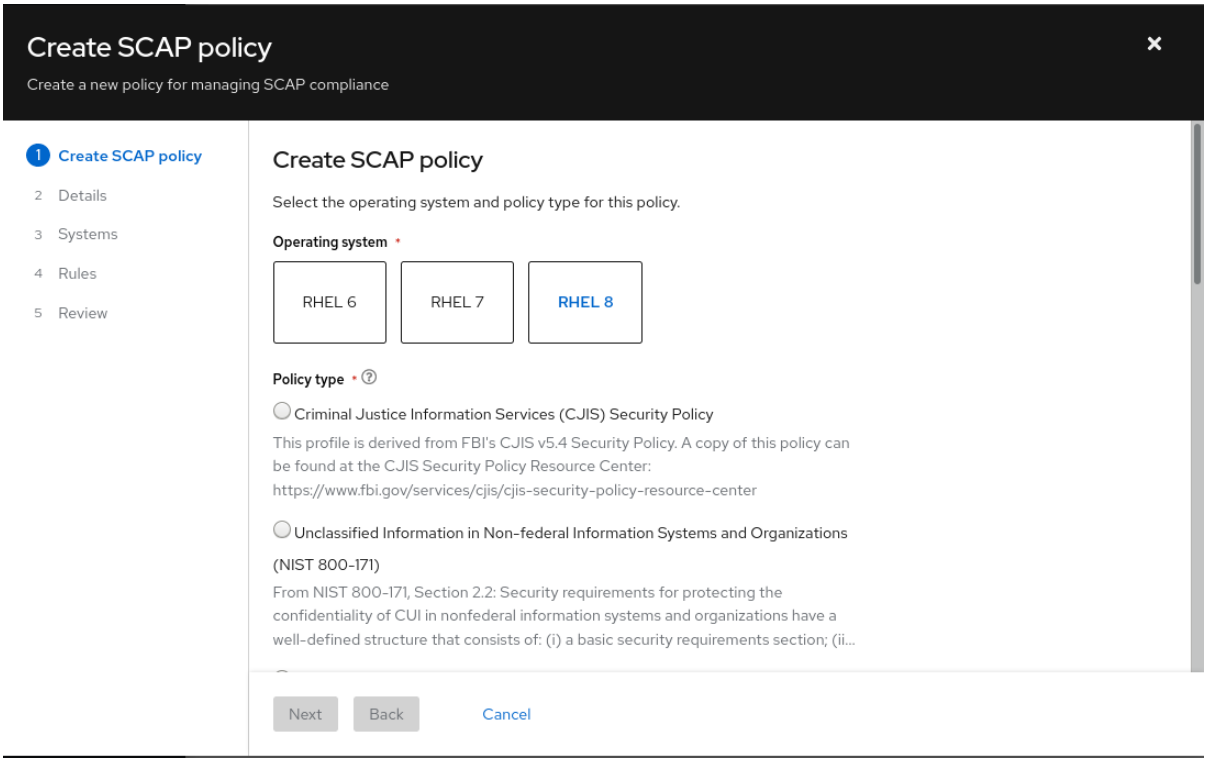


IMPORTANT

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.

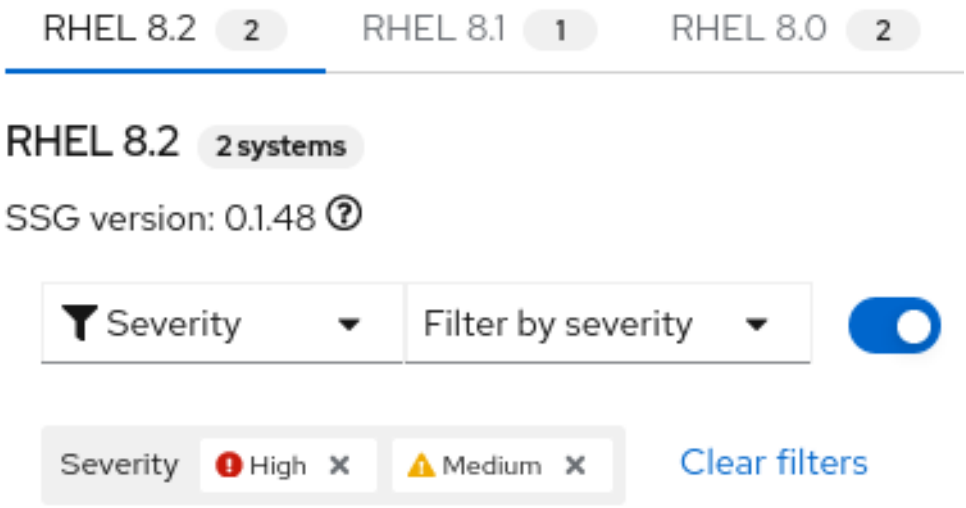
Procedure

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 RHEL 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.

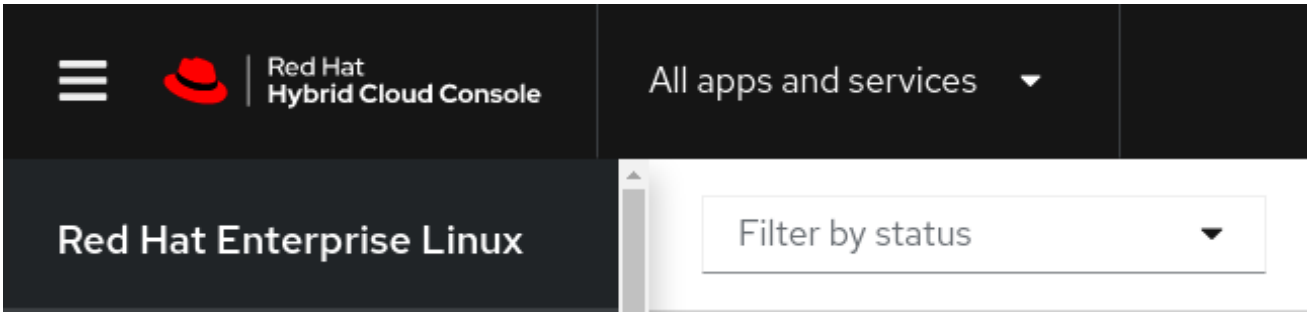
- **SCAP Policies.** Search for a specific policy by name.
- **Systems.** Search by system name, policy, or Red Hat Enterprise Linux operating system major version.
- **Rules list (single system).** The rules list search function allows you to search by the rule name or identifier. Identifiers are shown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

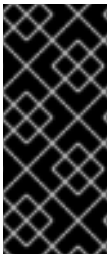
4.5. SYSTEM GROUPS AND TAGS IN INSIGHTS FOR RHEL

The Insights for RHEL application enables users to filter data to only show selected groups of systems. When one or more groups are selected using the **Filter by status** dropdown, that group filtering remains in place in each service throughout the UI, with the exception of systems lists in the compliance service.

The ability to filter by groups of systems can aid users who want to focus on results, and create reports, for those systems, no matter which service they are viewing.

Insights for RHEL global group and tag filters





IMPORTANT

In the compliance service UI, group and tag filters are set specifically for systems reporting compliance data. Tag and group filters set using **Filter by status** are not applied to systems lists in the compliance service UI. Instead, users set the **Tags** primary filter above lists of systems, then select specific groups or tags in the secondary filter. See section *Group and tag filters in the compliance service* , below, for more information.

How systems are tagged or assigned to groups

Systems are added to groups in two ways:

- **Automatically, by Insights data-ingestion method.** With no action required by administrators, the Insights client automatically tags systems running SAP workloads by SAP ID, and systems belonging to Satellite host groups by host collection name.

- **Configuring custom tags.** Users with root access can configure custom tags for specific systems in /etc/insights-client/tags.yaml. Users can then filter by custom group tag in the Insights for RHEL UI and see only those systems configured with that tag.

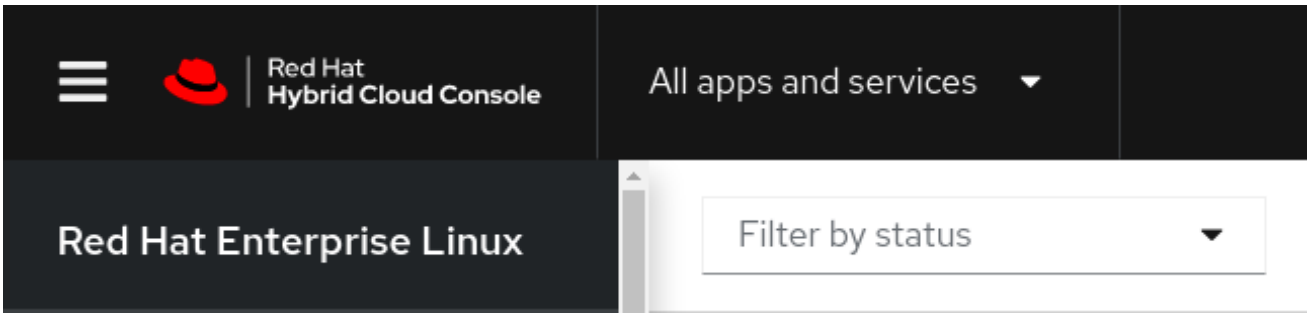
To learn more about groups and tags, including how to add system tags to the Insights client, refer to Chapter 8. System filtering and groups in Insights for RHEL advisor service documentation.

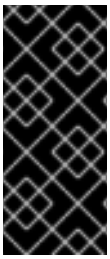
4.6. SYSTEM GROUPS AND TAGS IN INSIGHTS FOR RHEL

The Insights for RHEL application enables users to filter data to only show selected groups of systems. When one or more groups are selected using the **Filter by status** dropdown, that group filtering remains in place in each service throughout the UI, with the exception of systems lists in the compliance service.

The ability to filter by groups of systems can aid users who want to focus on results, and create reports, for those systems, no matter which service they are viewing.

Insights for RHEL global group and tag filters





IMPORTANT

In the compliance service UI, group and tag filters are set specifically for systems reporting compliance data. Tag and group filters set using **Filter by status** are not applied to systems lists in the compliance service UI. Instead, users set the **Tags** primary filter above lists of systems, then select specific groups or tags in the secondary filter. See section *Group and tag filters in the compliance service* , below, for more information.

How systems are tagged or assigned to groups

Systems are added to groups in two ways:

- **Automatically, by Insights data-ingestion method.** With no action required by administrators, the Insights client automatically tags systems running SAP workloads by SAP ID, and systems belonging to Satellite host groups by host collection name.

- **Configuring custom tags.** Users with root access can configure custom tags for specific systems in /etc/insights-client/tags.yaml. Users can then filter by custom group tag in the Insights for RHEL UI and see only those systems configured with that tag.

To learn more about groups and tags, including how to add system tags to the Insights client, refer to Chapter 8. System filtering and groups in Insights for RHEL advisor service documentation.

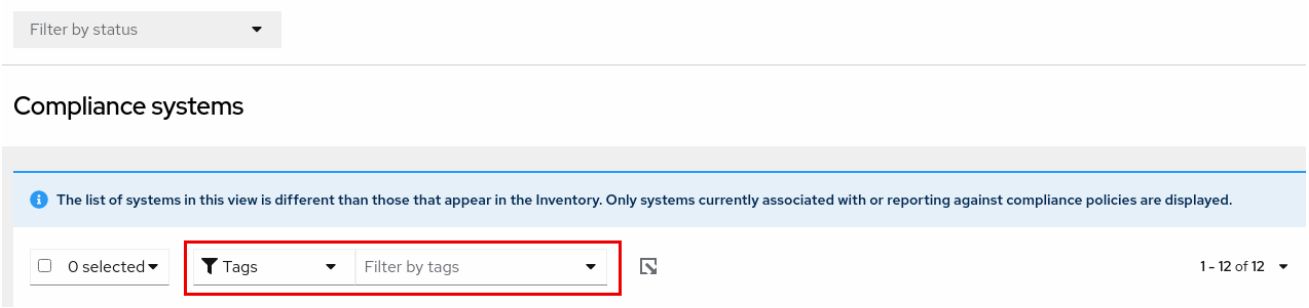
4.6.1. Group and tag filters in the compliance service

The compliance service enables users to apply tag and group filters to systems reporting compliance data; however, they are not set using the **Filter by status** dropdown. Unlike most of the other services in the Insights for RHEL application, the compliance service only shows data for systems under the following conditions:

- The system is associated with a compliance service security policy.
- The system is reporting compliance data to insights using the **insights-client --compliance** command.

Because of those conditions, compliance-service users have to set tag and group filters using the primary and secondary filters located above lists of systems in the compliance service UI.

Tag and group filters above systems list in the compliance service



4.6.2. Filtering compliance service systems lists by group or tag

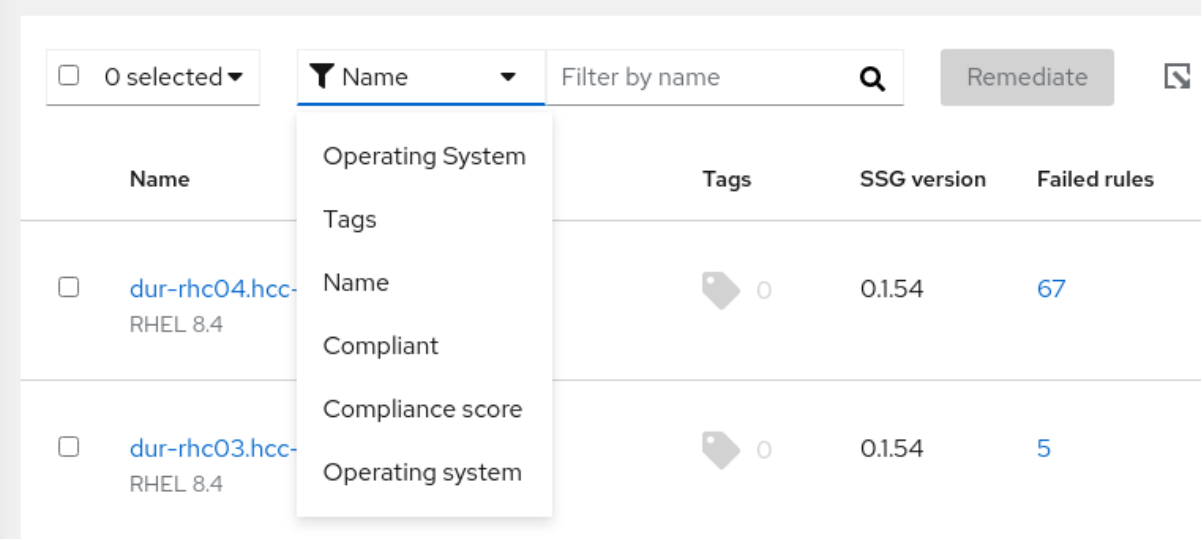
Use the following procedure to set filters for specific groups of systems in the compliance service. This procedure demonstrates one path to setting a group filter; however, once set, the filter is persistent on systems lists throughout the compliance service UI.

Prerequisites

- User is logged into the Red Hat Hybrid Cloud Console.

Procedure

1. Navigate to Red Hat Enterprise Linux > Compliance > Reports .
2. Click on a report name.
3. Above the systems list, click on the primary filter dropdown and select **Tags**.



4. In the secondary filter, enter the name of the group or tag, or scroll through the list to make multiple selections.

5. View systems from the selected group(s) in the systems list.

CHAPTER 5. 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*
- Insights for Red Hat Enterprise Linux Documentation
- Insights for Red Hat Enterprise Linux Product Support page