Red Hat Insights 2020-04

Assessing and Monitoring Security Policy Compliance of RHEL Systems

Understanding the Compliance Status of your Infrastructure

Last Updated: 2020-09-21

Red Hat Insights 2020-04 Assessing and Monitoring Security Policy Compliance of RHEL Systems

Understanding the 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

The Compliance service enables you to assess and monitor the compliance of your RHEL systems with SCAP security policies.

The Compliance service provides a simple but powerful user interface, allowing you to create, configure, and manage your SCAP security policies directly within the Compliance service. With the filtering and context-adding features built into the Compliance service, you can easily identify and manage compliance issues.

This documentation describes some key features of the Compliance service and how to use them. The purpose of this document is to help you get maximum value from Compliance service, understand your Compliance service results, and manage issues.

You can also create Ansible playbooks to resolve these issues and share reports with stakeholders to communicate compliance status. For more information about remediations and reporting, see the following documentation:

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

1.1. REQUIREMENTS AND PREREQUISITES

The Compliance service is part of the Red Hat Insights application. Insights 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

Regardless of whether you define a policy within Compliance or upload reports for policies defined and managed outside of the Compliance service, the Compliance service will fully support only the version of SSG that ships with the minor version of RHEL installed on the system.

Because each version of SSG differs from the previous version, accurate reporting depends on using the set of rules included in the correct version of SSG for your RHEL version. Systems using unsupported SCAP versions are identified in the application.

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.

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
RHEL 8.0 SAP	scap-security-guide-0.1.42-11.el8
RHEL 8.1 EUS	scap-security-guide-0.1.46-1.el8
RHEL 8.2 (batch update)	scap-security-guide-0.1.48-7.el8

Any reports for systems using versions of SSG that are not supported by RHEL will be displayed by the Compliance service with the following conditions:

- These results will be a “best-guess” effort because using any other versions than what is outlined above can lead to inaccurate results.
- Reports for unsupported configuration will not be used to determine a compliance score for a policy.
- Remediations will not be available with such results.

1.3. BEST PRACTICES

To benefit from the best user experience and receive the most accurate information in the Compliance service, Red Hat 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 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

Red Hat recommends that you create and define your organization's security policies within the Compliance service to get the most feature-rich user experience and reliable reporting.

When you create a policy within the Compliance service, you can associate multiple systems with it, be assured of using the supported SSG for your RHEL version, and edit which rules are included, based on your organization's needs.

Reports for policies defined outside of the Compliance service will be visible within the Compliance service, but you will not be able to use many of the features available to internally defined policies.

IMPORTANT

The Compliance service will no longer support any externally sourced and uploaded policies after Summit 2021.

CHAPTER 2. MANAGING SCAP SECURITY POLICIES IN THE COMPLIANCE SERVICE

SCAP security can be created and managed within the Compliance service. You can define policies, and add systems to them, using the wizard in the Compliance service. You can then modify some parameters of policies as needed.

IMPORTANT

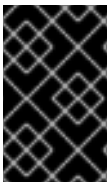
Unlike other Red Hat Insights services, the Compliance services do not run automatically on a default schedule. In order to upload OpenSCAP data to the compliance service, you must run the following command either on-demand on a scheduled job that you set.

2.1. CREATING NEW SCAP POLICIES

To use the Compliance service, you have to associate SCAP security policies with your RHEL systems. You can create new policies very easily using the wizard in the Compliance service. This involves the following actions:

- Specifying your host operating system
- Selecting a policy
- Editing the prepackaged rules
- Adding systems to the policy

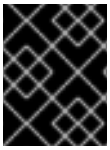
Red Hat recommends that users create their security policies directly within the Compliance service to get the most value and feature rich user experience.



IMPORTANT

Compliance reports uploaded from an external source, without a policy defined in the Compliance service, can no longer be edited to include a business objective and compliance threshold. This eliminates the ability to add important context to policies.

Reports in the Compliance service are grouped by SCAP Security Guide (SSG) version. If multiple versions of SSG are deployed on systems assigned to a single policy, users will see one report per version of SSG.



IMPORTANT

Red Hat recommends that users use the same SSG version for all the systems under a policy to have a consolidated and simplified view of your reports.

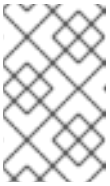
To create a new policy and associate systems with it using the Compliance service, complete the following steps:

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:

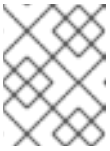
   a. Select the correct RHEL **operating system** version on the systems you want to monitor.

   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 version of RHEL.

   b. Select one **Policy type**.

   NOTE

   The available policy types are predetermined by the latest available SCAP Security Guide (SSG) for the OS version you chose in the previous step.

   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.

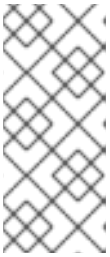
   

   NOTE

   In cases where 100% Compliance is unrealistic, you can specify an acceptable level of Compliance here.

   e. Click **Next**.

5. On the **Rules** page, edit your policy by clearing or adding rules and click **Next**.

   NOTE

   Each SCAP policy is prepackaged with a very large set of rules included. You can add or remove rules as needed based on your requirements. At this time, selecting specific rules to include in a policy is only available when a policy is newly created. However, the ability to edit rules included in an existing policy is coming soon.

6. On the **Systems** page, check the box next to each system you want to associate with this policy and 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, verify that the policy information is correct and click **Finish**.

Verification step

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

2.2. EDITING EXISTING POLICIES

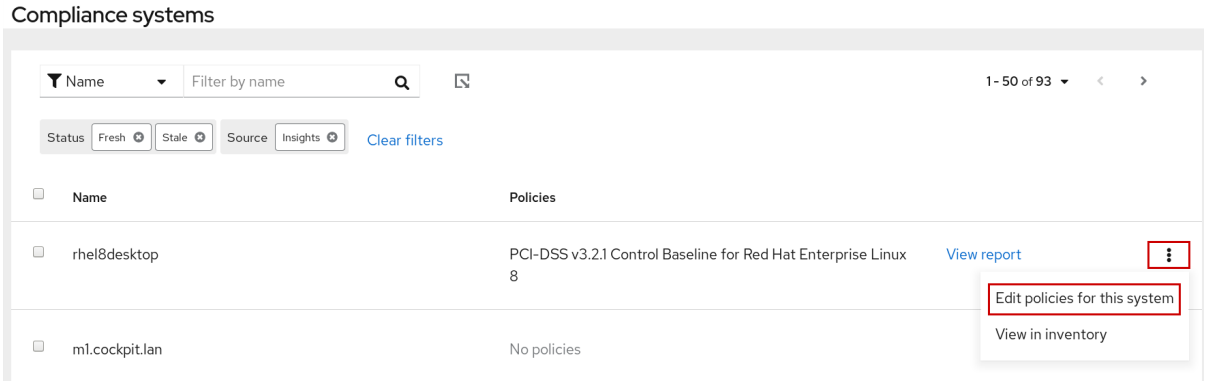
In addition to the multiple ways you can edit a policy at the time of creation, described in the previous section, you can also edit existing policies. The ability to edit existing policies is an evolving feature set; additional capabilities are coming soon, including the ability to add or remove the rules included in an existing policy.

2.2.1. Adding or removing policies associated with a system

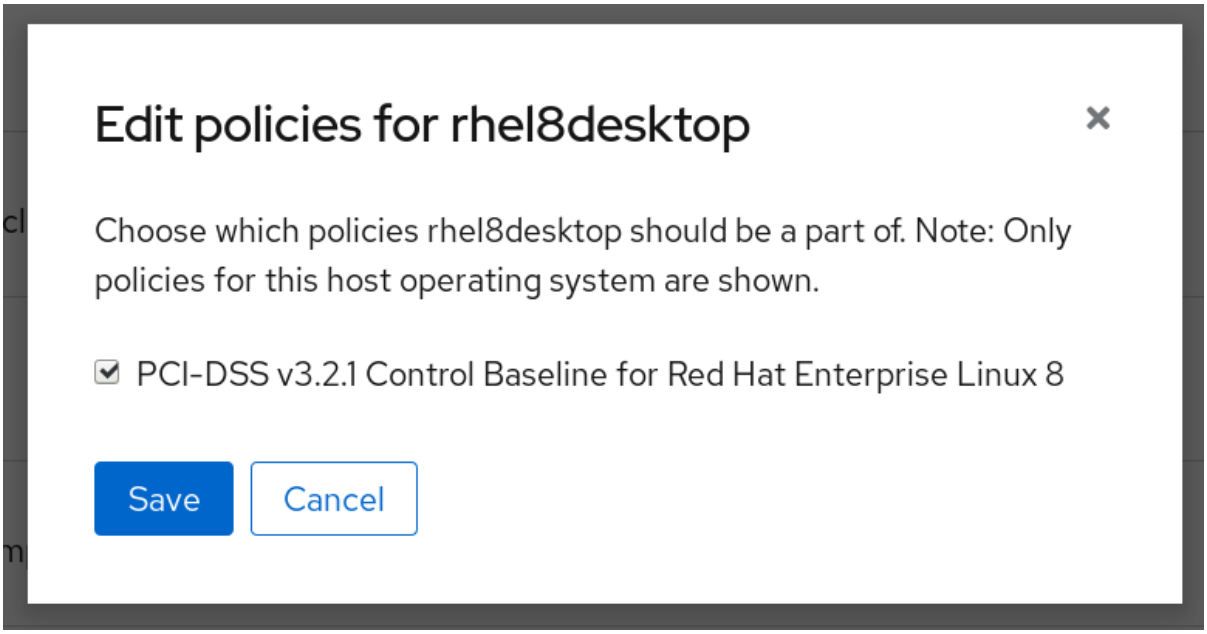
You can add to or remove policies from a system. Complete the following steps to add or remove a policy from a system using the Compliance service.

Procedure

1. Navigate to the Compliance service > Systems page and log in if necessary.
2. Locate the system you want to edit using the search or filtering functions.
3. Located on the far right side of the system row, click the more-actions icon (three vertical dots) and select **Edit policies for this system**



4. In the **Edit policies** card, select or clear checkboxes for the policy options presented and click **Save**. Only policies available for this system OS are shown.



Verification step

1. Returning to the **Systems list**, verify that you see the name of the new policy next to the system name.

2.2.2. Applying a business objective to a policy

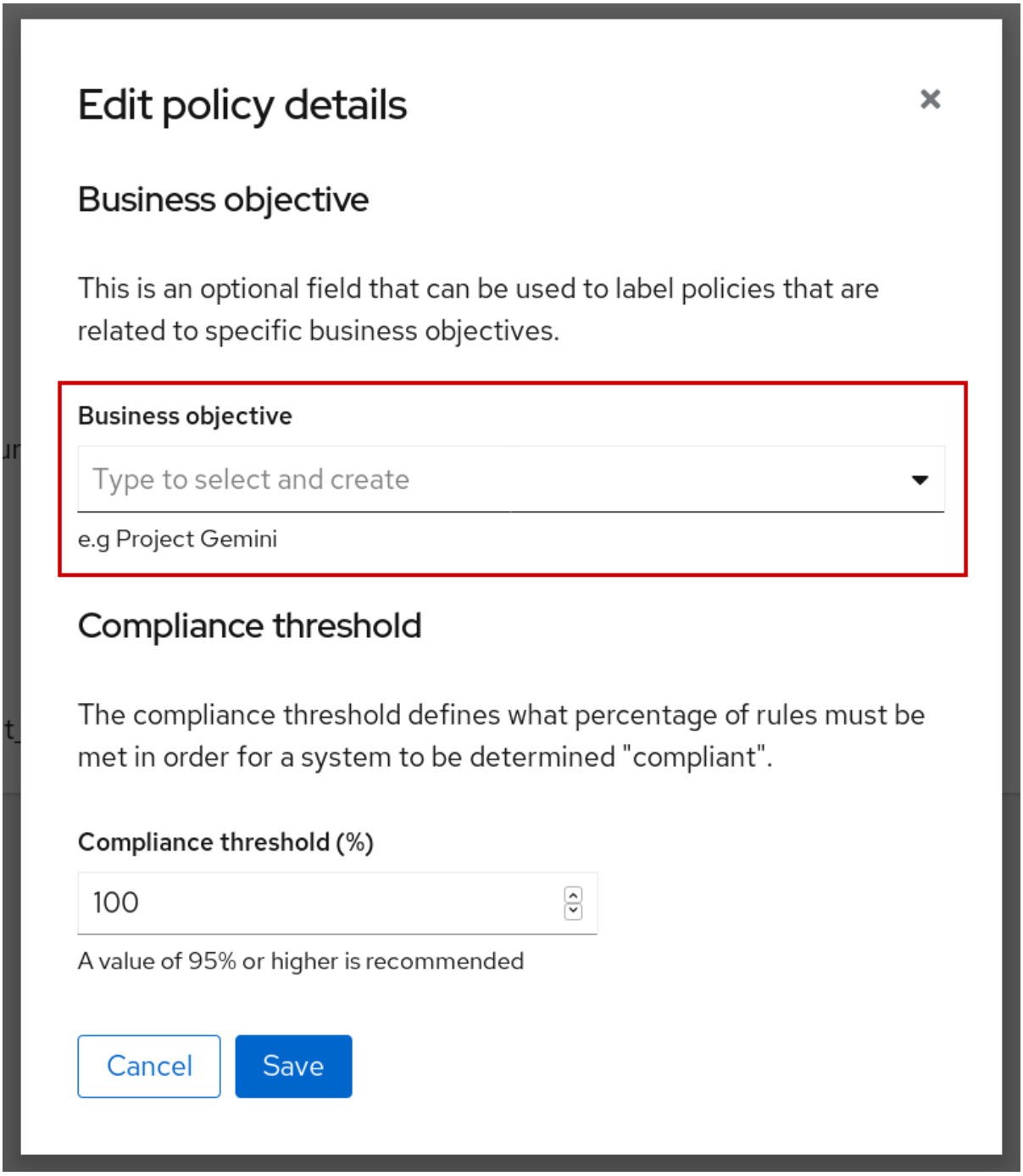
You can assign a business objective to a policy to associate the policy with a particular initiative or project, for example. When a business objective is added to a policy, it is visible in the **Business objective** column of the policies list and on the policy card in the Details tab.

Use the following procedure to apply or edit the business objective for a policy:

Procedure

1. Navigate to the Compliance service > SCAP Policies page and log in if necessary.
2. Click the policy to which you want to add a business objective.
3. On the policy card click **Edit policy**.

4. In the **Business objective** field, enter a relevant business objective or select an existing one from the list.



5. Click **Save**.

2.2.3. Specifying or changing compliance threshold

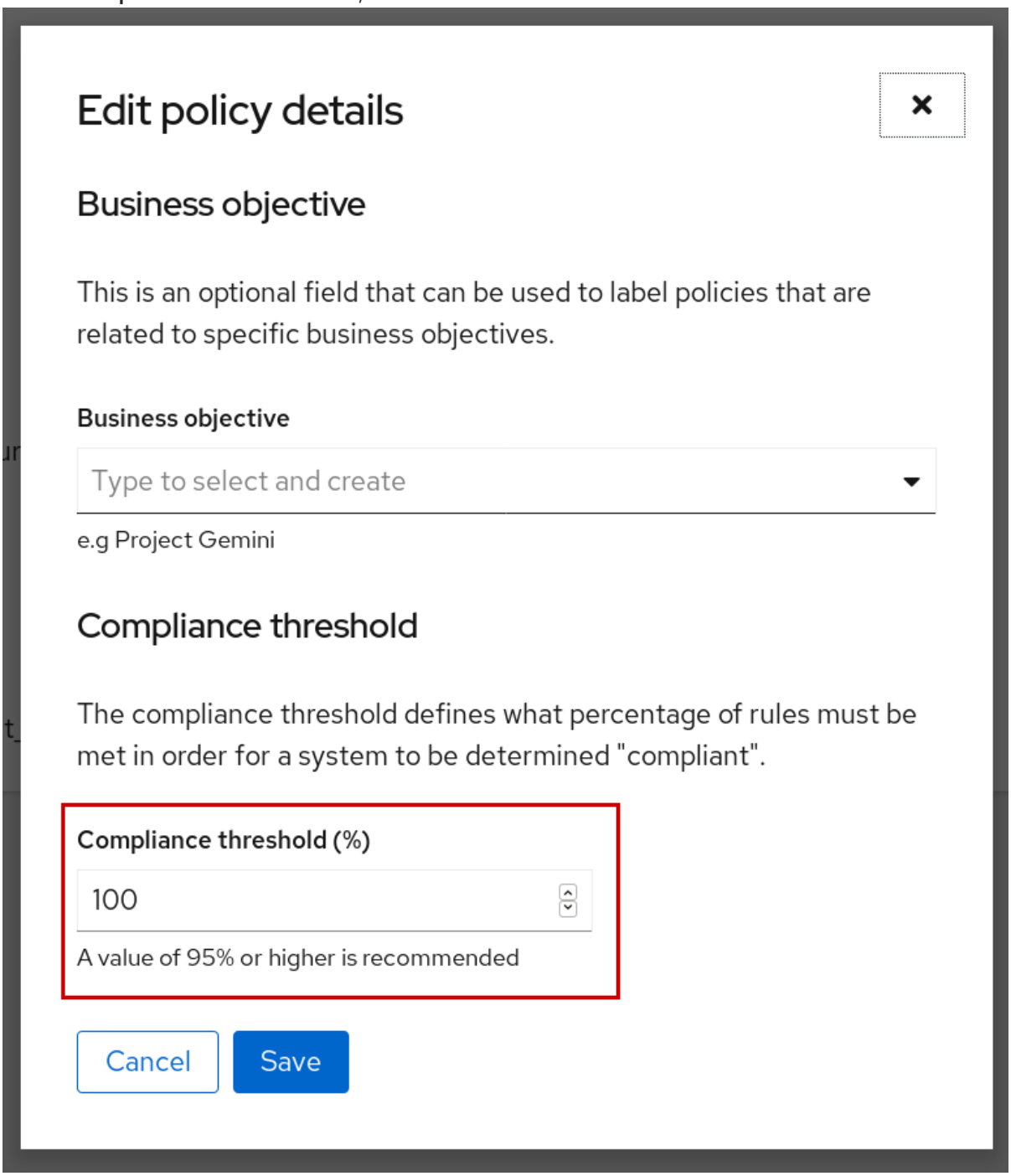
The compliance threshold defines what percentage of rules must be passed in order for a system to be compliant. The value can be changed from the default, 100%, when creating the policy. However, it can also be modified later on.

After you set a threshold, the threshold value will be visible in the policies list, next to the policy name, and on the policy card in the Details tab. Use the following procedure to set or modify a compliance threshold for a policy.

Procedure

1. Navigate to the Compliance service > SCAP Policies page and log in if necessary.

2. Select the policy for which to set a compliance threshold and click on the policy name.
3. On the policy card click **Edit policy**.
4. In the **Compliance threshold** field, enter a numeric value between 1-100.



5. Click **Save**.

CHAPTER 3. REFINING YOUR COMPLIANCE SERVICE RESULTS

After uploading your latest results to the Compliance service using **insights-client --compliance**, you can view the status of your RHEL infrastructure at Compliance service > Reports and drill into each policy for reports and per-system status. The following sections describe ways to refine or add context to your data to more easily focus on your most important issues.

IMPORTANT

Always run **insights-client --compliance** to ensure you are viewing the current results for your RHEL infrastructure.

3.1. SEARCHING

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

- **Systems tab.** System names can be searched in the Systems tab search box.
- **Rules list** (for a 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.

3.2. 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.
- **Policy rules list.** Filter by rule severity.
- **Single system rules list.** Filter rules that have passed or not passed, or by rule severity.

3.3. 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

CHAPTER 5. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS

The 2020-04 release of Red Hat Insights includes significant changes to the application features and services.

Changes to the Red Hat Insights application

The Red Hat Insights application now includes the services that were previously bundled with the Cloud Management Services for RHEL application, and were part of the Red Hat Smart Management bundle, along with Red Hat Satellite.

The former cloud management services, plus a couple of new services, are now included in the value that Insights brings to each Red Hat Enterprise Linux (RHEL) subscription.

Insights Advisor

The tools and capabilities that constituted Red Hat Insights prior to this release are now available as the **Advisor** service. The *rules* that have always been the currency of Insights are now called Advisor **Recommendations**.

Insights security rules have moved

The CVE security rules that were previously curated by the Insights rules team are now included with all other Red Hat CVEs in the Vulnerability service. Security rules are high profile CVEs, some of which have been through the Customer Security Awareness Program. They are identifiable in the Vulnerability service by a security rule icon. You can also filter security rules in the Vulnerability service.

Services included with Red Hat Insights

The services included with Red Hat Insights in the 2020-04 release are:

- **Advisor.** Identify and fix configuration issues that can negatively impact the availability, performance, stability, and security of RHEL systems.
- **Vulnerability.** Assess and monitor the exposure of your RHEL environment to CVEs and security rules.
- **Compliance.** Assess and monitor the compliance of your RHEL systems with SCAP security policies.
- **Patch.** Enable consistent patch workflows for RHEL systems across the open hybrid cloud.
- **Drift.** Compare system configurations of a system over time, or to other systems and baselines, to identify discrepancies in your environment and perform drift analysis.
- **Policies.** Evaluate and react to system configuration changes in your environment.

The integrated tools that work with each of the services above are:

- **Inventory.** Topological inventory of RHEL systems under Red Hat Insights management
- **Remediations.** Repository of Ansible Playbooks that you create and manage using Red Hat Insights
- **Subscription Watch.** Comprehensive, product-by-product, account-level subscription reporting service across hybrid cloud deployments

Resources

- Red Hat Insights Product Support page
- Red Hat Insights Documentation
- Red Hat Insights Release Notes
- Red Hat Insights blog channel