



## Red Hat Insights 1-latest

# Monitoring and Reacting to Configuration Changes Using Policies with FedRAMP

How to create policies to detect inventory configuration changes and send email notifications



# Red Hat Insights 1-latest Monitoring and Reacting to Configuration Changes Using Policies with FedRAMP

---

How to create policies to detect inventory configuration changes and send email notifications

Red Hat Customer Content Services

## Legal Notice

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Abstract

This document provides an overview of the Policies service with FedRAMP<sup>®</sup> and explains how to create a policy to detect system configuration changes and be notified by email. 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

<b>CHAPTER 1. RED HAT INSIGHTS POLICIES SERVICE OVERVIEW</b> .....	<b>3</b>
1.1. USER ACCESS CONSIDERATIONS	3
1.1.1. User Access roles for the Policies service	3
<b>CHAPTER 2. SETTING NOTIFICATIONS AND EMAIL PREFERENCES</b> .....	<b>5</b>
2.1. ENABLING NOTIFICATIONS AND INTEGRATIONS FOR THE POLICIES SERVICE	5
2.2. SETTING USER PREFERENCES	5
<b>CHAPTER 3. CREATING POLICIES</b> .....	<b>7</b>
3.1. CREATING A POLICY TO ENSURE PUBLIC CLOUD PROVIDERS ARE NOT OVER PROVISIONED	7
3.2. CREATING A POLICY TO DETECT IF SYSTEMS ARE RUNNING AN OUTDATED VERSION OF RHEL	8
3.3. CREATING A POLICY TO DETECT A VULNERABLE PACKAGE VERSION BASED ON RECENT CVE	8
<b>CHAPTER 4. REVIEWING AND MANAGING POLICIES</b> .....	<b>10</b>
<b>CHAPTER 5. APPENDIX</b> .....	<b>11</b>
5.1. SYSTEM FACTS	11
5.2. OPERATORS	13
<b>PROVIDING FEEDBACK ON RED HAT DOCUMENTATION</b> .....	<b>15</b>



# CHAPTER 1. RED HAT INSIGHTS POLICIES SERVICE OVERVIEW

Policies evaluate system configurations in your environment, and can send notifications when changes occur. Policies you create are applicable to all systems in your Insights inventory. You can create and manage policies using the Red Hat Insights for Red Hat Enterprise Linux user interface in the Red Hat Hybrid Cloud Console, or using the Insights API.

Policies can assist you by managing tasks such as:

- Raising an alert when particular conditions occur in your system configuration.
- Emailing a team when security packages are out of date on a system.

Using policies to monitor configuration changes in your inventory and notifying by email requires:

- Setting user email preferences (if not already set).
- Creating a policy to detect configuration changes as a trigger and selecting email as the trigger action.



## NOTE

- Configure User Access in [Red Hat Hybrid Cloud Console](#) > the **Settings** icon (⚙️) > [Identity & Access Management](#) > [User Access](#) > [Users](#).
- See [User Access Configuration Guide for Role-based Access Control \(RBAC\)](#) for more information about this feature and example use cases.

## 1.1. USER ACCESS CONSIDERATIONS

All users on your account have access to most of the data in Insights for Red Hat Enterprise Linux.

### Brief overview about predefined groups and roles

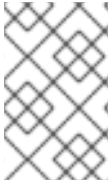
The following predefined groups and roles are relevant to access:

- **Default access group.** All users on the account are members of the Default access group. Members of the Default access group have read-only access, which allows you to view most information in Insights for Red Hat Enterprise Linux.

#### 1.1.1. User Access roles for the Policies service

The following predefined roles on the Red Hat Hybrid Cloud Console enable access to policies features in Insights for Red Hat Enterprise Linux:

- **Policies administrator role.** The Policies administrator role provides read and write access allowing these users to perform any available operation on policies resources. This predefined role is in the **Default admin access group**.
- **Policies viewer role.** The Policies viewer role provides read-only access. (If your organization determines that the default configuration of the Policies viewer role is inadequate, a **User Access administrator** can create a custom role with the specific permissions that you need.) This predefined role is in the **Default access group**.



## NOTE

If you configured groups before April 2023, any user who was not an Organization Administrator will have the Policies administrator role replaced with the Policies viewer role. Modifications made to the Default access group before April are not changed.

### Additional Resources

- [How to use User Access](#) in the User Access Configuration Guide for Role-based Access Control (RBAC).
- [Predefined User Access roles](#)



## CHAPTER 2. SETTING NOTIFICATIONS AND EMAIL PREFERENCES

By configuring notifications and user preferences settings in the Red Hat Hybrid Cloud Console, Red Hat Insights will notify you of policy changes to your Red Hat Enterprise Linux systems.

### 2.1. ENABLING NOTIFICATIONS AND INTEGRATIONS FOR THE POLICIES SERVICE

You can enable the notifications service on the Red Hat Hybrid Cloud Console to send notifications whenever the policy service detects an issue and generates an alert. Using the notifications service frees you from having to continually check the Red Hat Insights Dashboard for alerts.

For example, you can configure the notifications service to automatically send an email message whenever the policies service detects that a server's security software is out of date, or to send an email digest of all the alerts that the policies service generates each day.

In addition to sending email messages, you can configure the notifications service to send policies event data in other ways:

- Using an authenticated client to query Red Hat Insights APIs for event data
- Using webhooks to send events to third-party applications that accept inbound requests
- Integrating notifications with applications such as Splunk to route policies events to the application dashboard

Enabling the notifications service requires three main steps:

- First, an Organization Administrator creates a User access group with the Notifications administrator role, and then adds account members to the group.
- Next, a Notifications administrator sets up behavior groups for events in the notifications service. Behavior groups specify the delivery method for each notification. For example, a behavior group can specify whether email notifications are sent to all users, or just to Organization administrators.
- Finally, users who receive email notifications from events must set their user preferences so that they receive individual emails for each event.

#### Additional resources

- For more information about configuring Hybrid Cloud Console notifications to learn of identified events that have occurred and could impact your organization, see [Configuring notifications on the Red Hat Hybrid Cloud Console with FedRAMP](#).
- For more information about configuring Hybrid Cloud Console notifications to integrate with third-party applications, see [Integrating the Red Hat Hybrid Cloud Console with third-party applications](#).

### 2.2. SETTING USER PREFERENCES

To receive email notifications, you can set or update your email preferences using the following procedure.

## Procedure

1. Navigate to [Operations > Policies](#).
2. Click **Open user preferences** The My Notifications page appears.
3. Select **Red Hat Enterprise Linux > Policies** from the left menu.
4. Check the appropriate boxes to define your policies notification preferences.
5. Depending on your email notification preferences, you can subscribe to **Instant notification** emails for each system with triggered policies or a **Daily digest** summarizing triggered application events in a 24-hour time frame. To unsubscribe from all notifications, select **Unsubscribe from all**.



### NOTE

Subscribing to instant notifications can result in receiving many emails on large inventories. To reduce the volume of emails, consider selecting the Daily digest option.

6. Click **Submit**.

## CHAPTER 3. CREATING POLICIES

The following workflow examples explain how to create several types of policies that detect system configuration changes and send notification of the changes by email.



### NOTE

When creating a policy, if you see a warning message that you have not opted in for email alerts, set your User preferences to receive email from your policies.

### 3.1. CREATING A POLICY TO ENSURE PUBLIC CLOUD PROVIDERS ARE NOT OVER PROVISIONED

Create a policy using the following procedure.

#### Procedure

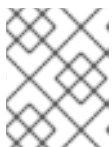
1. In [Red Hat Hybrid Cloud Console](#), go to [Operations > Policies](#).
2. Click **Create policy**.
3. On the Create a policy page, click **From scratch** or **As a copy of existing Policy** as required. Note that the **As a copy of existing Policy** option will prompt you to select a policy from the list of existing policies to use as a starting point.
4. Click **Next**.
5. Enter **Condition**. In this case, enter: `facts.cloud_provider in ['alibaba', 'aws', 'azure', 'google'] and (facts.number_of_cpus >= 8 or facts.number_of_sockets >=2)`. This condition will detect if an instance running on the specified public cloud providers are running with CPU hardware higher than the allowed limit.



### NOTE

You can expand **What condition can I define?** and/or **Review available system facts** to view an explanation of conditions you can use, and see the available system facts, respectively. In this section are examples of syntax you can use.

6. Click **Validate condition**.
7. Once the condition is validated, click **Next**.
8. On the Trigger actions page, click **Add trigger actions**. If notifications is greyed out, select **Notification settings** in the notifications box. Here you can customize notifications and their behaviors.
9. Click **Next**.



### NOTE

On the Trigger actions page, you can also enable email alerts as well as open email preferences.

10. On the Review and enable page, click the toggle switch to activate the policy and review its details.
11. Click **Finish**.

Your new policy is created. When the policy is evaluated on a system check-in, if the condition in the policy is met, Policies automatically sends an email to all users on the account with access to Policies, depending on their email preferences.

## 3.2. CREATING A POLICY TO DETECT IF SYSTEMS ARE RUNNING AN OUTDATED VERSION OF RHEL

You can create a policy that detects if systems are running outdated versions of RHEL and notifies you by email about what it finds.

### Procedure

1. In [Red Hat Hybrid Cloud Console](#), go to [Operations > Policies](#).
2. Click **Create policy**.
3. On the Create policy page, click **From scratch** or **As a copy of existing Policy** as required. Note that the **As a copy of existing Policy** option prompts you to select a policy from the list of existing policies to use as a starting point.
4. Click **Next**.
5. Enter a **Name** and **Description** for the policy.
6. Click **Next**.
7. Enter **Condition**. In this case, enter `facts.os_release < 8.1` This condition will detect if systems still run an outdated version of our operating system based on RHEL 8.1.
8. Click **Validate condition**, then click **Next**.
9. On the Trigger actions page, click **Add trigger actions** and select **Email**.
10. Click **Next**.
11. On the Review and activate page, click the toggle switch to activate the policy and review its details.
12. Click **Finish**.

Your new policy is created. When the policy is evaluated on a system check-in, if the condition in the policy is triggered, the policies service automatically sends an email to all users on the account with access to Policies, depending on their email preferences.

## 3.3. CREATING A POLICY TO DETECT A VULNERABLE PACKAGE VERSION BASED ON RECENT CVE

You can create a policy that detects vulnerable package versions based on recent CVE and notifies you by email about what it finds.

## Procedure

1. In [Red Hat Hybrid Cloud Console](#), go to [Operations > Policies](#).
2. Click **Create policy**.
3. On the Create Policy page, click **From scratch** or **As a copy of existing Policy** as required. Note that the **As a copy of existing Policy** option will prompt you to select a policy from the list of existing policies to use as a starting point.
4. Click **Next**.
5. Enter a **Name** and **Description** for the policy.
6. Click **Next**.
7. Enter **Condition**. In this case, enter `facts.installed_packages contains ['openssh-4.5']`. This condition will detect if systems still run a vulnerable version of an **openssh** package based on recent CVE.
8. Click **Validate condition**, then click **Next**.
9. On the Trigger actions page, click **Add trigger actions** and select **Email**.
10. Click **Next**.
11. On the Review and activate page, click the toggle switch to activate the policy and review its details.
12. Click **Finish**.


Your new policy is created. When the policy is evaluated on a system check-in, if the condition in the policy is met, Policies automatically sends an email to all users on the account with access to Policies, depending on their email preferences.

## CHAPTER 4. REVIEWING AND MANAGING POLICIES

You can review and manage all created policies (enabled and disabled) by navigating to [Operations > Policies](#).

You can filter the list of policies by name and by active state. You can click the options menu next to a policy to perform the following operations:

- Enable and disable
- Edit
- Duplicate
- Delete

Additionally, you can perform the following operations in bulk by selecting multiple policies from the list of policies and clicking the options menu  located next to the **Create policy** button at the top:

- Delete policies
- Enable policies
- Disable policies



### NOTE

If you see a warning message about email alerts not opted in, set your User preferences to receive email from your policies.

## CHAPTER 5. APPENDIX

This appendix contains the following reference materials:

- System Facts
- Operators

### 5.1. SYSTEM FACTS

The table below displays the system facts for use in system comparisons.

Table 5.1. System Facts and Their Functions

Fact Name	Description	Example Value
<b>Ansible</b>	Category with a list of Ansible-related facts	controller_version with a value of 4.0.0
<b>arch</b>	System architecture	<b>x86_64</b>
<b>bios_release_date</b>	BIOS release date; typically <b>MM/DD/YYYY</b>	01/01/2011
<b>bios_vendor</b>	BIOS vendor name	LENOVO
<b>bios_version</b>	BIOS version	1.17.0
<b>cloud_provider</b>	Cloud vendor. Values are <b>google, azure, aws, alibaba</b> , or empty	<b>google</b>
<b>cores_per_socket</b>	Number of CPU cores per socket	2
<b>cpu_flags</b>	Category with a list of CPU flags. Each name is the CPU flag (ex: <b>vmx</b> ), and the value is always <b>enabled</b> .	<b>vmx</b> , with a value of <b>enabled</b> .
<b>enabled_services</b>	Category with a list of enabled services. Each name in the category is the service name (ex: <b>crond</b> ), and the value is always <b>enabled</b> .	<b>crond</b> , with a value of <b>enabled</b> .
<b>fqdn</b>	System Fully Qualified Domain Name	system1.example.com
<b>infrastructure_type</b>	System infrastructure; common values are <b>virtual</b> or <b>physical</b>	<b>virtual</b>
<b>infrastructure_vendor</b>	Infrastructure vendor; common values are <b>kvm, vmware, baremetal</b> , etc.	<b>kvm</b>

Fact Name	Description	Example Value
<b>installed_packages</b>	List of installed RPM packages. This is a category.	<b>bash</b> , with a value of <b>4.2.46-33.el7.x86_64</b> .
<b>installed_services</b>	Category with a list of installed services. Each name in the category is the service name (ex: <b>crond</b> ), and the value is always <b>installed</b> .	<b>crond</b> , with a value of <b>installed</b> .
<b>kernel_modules</b>	List of kernel modules. Each name in the category is the kernel module (ex: <b>nfs</b> ), and the value is <b>enabled</b> .	<b>nfs</b> , with a value of <b>enabled</b> .
<b>last_boot_time</b>	The boot time in <b>YYYY-MM-DDTHH:MM:SS</b> format. Informational only; we do not compare boot times across systems.	<b>2019-09-18T16:54:56</b>
<b>mssql</b>	Category with a list of MSSQL-related facts	mssql_version with a value of 15.0.4153.1
<b>network_interfaces</b>	List of facts related to network interfaces.	
	There are six facts for each interface: <b>ipv6_addresses</b> , <b>ipv4_addresses</b> , <b>mac_address</b> , <b>mtu</b> , <b>state</b> and <b>type</b> . The two address fields are comma-separated lists of IP addresses. The <b>state</b> field is either <b>UP</b> or <b>DOWN</b> . The <b>type</b> field is the interface type (ex: <b>ether</b> , <b>loopback</b> , <b>bridge</b> , etc.).	
	Each interface (ex: <b>lo</b> , <b>em1</b> , etc) is prefixed to the fact name. For example, em1's mac address would be the fact named <b>em1.mac_address</b> .	
	Most network interface facts are compared to ensure they are equal across systems. However, <b>ipv4_addresses</b> , <b>ipv6_addresses</b> , and <b>mac_address</b> are checked to ensure they are different across systems. A subexception for <b>lo</b> should always have the same IP and mac address on all systems.	
<b>number_of_cpus</b>	Total number of CPUs	<b>1</b>
<b>number_of_sockets</b>	Total number of sockets	<b>1</b>
<b>os_kernel_version</b>	Kernel version	<b>4.18.0</b>



Fact Name	Description	Example Value
<b>os_release</b>	Kernel release	<b>8.1</b>
<b>running_processes</b>	List of running processes. The fact name is the name of the process, and the value is the instance count.	<b>crond</b> , with a value of <b>1</b> .
<b>sap_instance_number</b>	SAP instance number	<b>42</b>
<b>sap_sids</b>	SAP system ID (SID)	<b>A42</b>
<b>sap_system</b>	Boolean field that indicates if SAP is installed on the system	<b>True</b>
<b>sap_version</b>	SAP version number	<b>2.00.052.00.1599 235305</b>
<b>satellite_managed</b>	Boolean field that indicates is a system is registered to a Satellite server.	<b>FALSE</b>
<b>selinux_current_mode</b>	Current SELinux mode	<b>enforcing</b>
<b>selinux_config_file</b>	SELinux mode set in the config file	<b>enforcing</b>
<b>systemd</b>	The number of failures, number of current jobs queued, and current state of systemd	<b>state with a value of degraded</b>
<b>system_memory</b>	Total system memory in human-readable form	<b>3.45 GiB</b>
<b>tuned_profile</b>	Current profile resulting from the command <b>tuned-adm active</b>	<b>desktop</b>
<b>yum_repos</b>	List of yum repositories. The repository name is added to the beginning of the fact. Each repository has the associated facts <b>base_url,enabled</b> , and <b>gpgcheck</b> .	<b>Red Hat Enterprise Linux 7 Server (RPMs).base_ur</b> I would have the value <a href="https://cdn.redhat.com/content/dist/rhel/server/7/\$releasever/\$basearch/os">https://cdn.redhat.com/content/dist/rhel/server/7/\$releasever/\$basearch/os</a>

## 5.2. OPERATORS

Table 5.2. Available Operators in Conditions

Operators	Value
Logical Operators	AND
	OR
Boolean Operators	EQUAL
	NOTEQUAL
Numeric Compare Operators	GT
	GTE
	LT
	LTE
String Compare Operator	CONTAINS
Array Operators	IN
	CONTAINS
Parser Operators	OR
	AND
	NOT
	EQUAL
	NOTEQUAL
	CONTAINS
	NEG

# PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate and prioritize your feedback regarding our documentation. Provide as much detail as possible, so that your request can be quickly addressed.

## Prerequisites

- You are logged in to the Red Hat Customer Portal.

## Procedure

To provide feedback, perform the following steps:

1. Click the following link: [Create Issue](#)
2. Describe the issue or enhancement in the **Summary** text box.
3. Provide details about the issue or requested enhancement in the **Description** text box.
4. Type your name in the **Reporter** text box.
5. Click the **Create** button.

This action creates a documentation ticket and routes it to the appropriate documentation team. Thank you for taking the time to provide feedback.