Red Hat Insights 2022

Monitoring and Reacting to Configuration Changes Using Policies

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

Last Updated: 2022-06-16

Red Hat Insights 2022 Monitoring and Reacting to Configuration Changes Using Policies

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

Red Hat Customer Content Services

Legal Notice

Abstract

This document provides an overview of the Policies service and explains how to create a policy to detect system configuration changes and be notified by email.

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. RECEIVING AUTOMATIC NOTIFICATIONS FROM POLICIES ABOUT CHANGES IN YOUR INSIGHTS FOR RHEL INVENTORY

Policies service users can set notification preferences that notify the user of changes to systems or potential security issues.

1.1. POLICIES DETECTION AND NOTIFICATION OF INVENTORY CONFIGURATION CHANGES

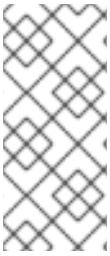
Policies you create are applicable to all systems in your Insights for RHEL inventory. You can create and manage policies using the Insights for RHEL user interface or via API.

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 Insights for Red Hat Enterprise Linux > Settings > User Access.
- See *User Access Configuration Guide for Role-based Access Control (RBAC)* for more information about this feature and example use cases.

1.2. ENABLING NOTIFICATIONS AND INTEGRATIONS FOR THE POLICIES SERVICE

You can enable the notifications service on 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 polcies 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 how to set up notifications for policies alerts, see Red Hat Insights Notifications.

CHAPTER 2. USER PREFERENCES

Update your information and set email preferences for Red Hat Hybrid Cloud Console services in your user preferences.

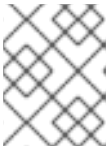
2.1. SETTING USER PREFERENCES

You can set or update your email preferences as follows.

Procedure

1. Click the user menu located on the upper-right side, then go to: User preferences > Notifications > Red Hat Enterprise Linux https://console.redhat.com/user-preferences/email. Check the appropriate boxes to define your policies notification preferences.

2. 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.



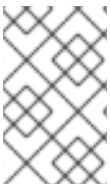
NOTE

Subscribing to instant notification can result in receiving many emails on large inventories, that is, one email per system checking in.

3. 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 preferences to receive email from your policies. See Chapter 2, User preferences, for information.

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

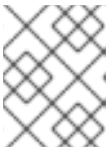
Procedure

1. In Red Hat Hybrid Cloud Console, go to Red Hat Enterprise Linux > 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 notificaitons 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 Red Hat Enterprise Linux > 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 Red Hat Enterprise Linux > 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

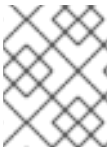
You can review and manage all created policies (enabled and disabled) by navigating to Red Hat Enterprise Linux > Policies.

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 preferences to receive email from your policies as described in Chapter 2, User preferences.

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

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

Fact Name	Description	Example Value
os_release	Kernel release	**8.1**
running_processes	List of running processes. The fact name is the name of the process, and the value is the instance count.	**crond**, with a value of **1**.
sap_instance_number	SAP instance number	**42**
sap_sids	SAP system ID (SID)	**A42**
sap_system	Boolean field that indicates if SAP is installed on the system	**True**
sap_version	SAP version number	**2.00.052.00.1599235305**
satellite_managed	Boolean field that indicates is a system is registered to a Satellite server.	**FALSE**
selinux_current_mode	Current SELinux mode	**enforcing**
selinux_config_file	SELinux mode set in the config file	**enforcing**
system_memory	Total system memory in human-readable form	**3.45 GiB**
tuned_profile	Current profile resulting from the command **tuned-adm active**	**desktop**
yum_repos	List of yum repositories. The repository name is added to the beginning of the fact. Each repository has the associated facts **base_url**,**enabled**, and **gpgcheck**.	**Red Hat Enterprise Linux 7 Server (RPMs).base_url** would have the value **https://cdn.redhat.com/content/dist/rhel/server/7/$releasever/$basearch/os**

5.2. OPERATORS

Table 5.2. Available Operators in Conditions

Operators	Value
Logical Operators	AND

Operators	Value
	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