Monitoring and Reacting to Configuration Changes Using Policies

How to create policies to detect inventory configuration changes and send email notifications
Red Hat Insights 2023 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
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. 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. RED HAT INSIGHTS POLICIES SERVICE OVERVIEW ................................................. 3
  1.1. USER ACCESS CONSIDERATIONS ............................................................................ 3
    1.1.1. User Access roles for the Policies service .................................................... 4

CHAPTER 2. SETTING NOTIFICATIONS AND EMAIL PREFERENCES ........................................... 6
  2.1. ENABLING NOTIFICATIONS AND INTEGRATIONS FOR THE POLICIES SERVICE ..... 6
  2.2. SETTING USER PREFERENCES .............................................................................. 6

CHAPTER 3. CREATING POLICIES ............................................................................................... 8
  3.1. CREATING A POLICY TO ENSURE PUBLIC CLOUD PROVIDERS ARE NOT OVER PROVISIONED 8
  3.2. CREATING A POLICY TO DETECT IF SYSTEMS ARE RUNNING AN OUTDATED VERSION OF RHEL 9
  3.3. CREATING A POLICY TO DETECT A VULNERABLE PACKAGE VERSION BASED ON RECENT CVE 9

CHAPTER 4. REVIEWING AND MANAGING POLICIES ............................................................... 11

CHAPTER 5. APPENDIX ............................................................................................................. 12
  5.1. SYSTEM FACTS .................................................................................................. 12
  5.2. OPERATORS ....................................................................................................... 14

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION ....................................................... 16
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**

- 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

An Organization Administrator on your account configures settings in User Access to control access to Red Hat Insights for Red Hat Enterprise Linux features. All users on your account have access to most of the data in Insights for Red Hat Enterprise Linux. However, performing some actions requires users to have elevated access.

Access is granted in User Access in the Red Hat Hybrid Cloud Console. To grant or change access, an Organization Administrator or User Access administrator must add you to a User Access group with the required roles in Red Hat Hybrid Cloud Console > the Settings icon (⚙) > Identity & Access Management > User Access > Users.

**IMPORTANT**

In this documentation, prerequisites for procedures declare whether you need elevated access to perform the procedure.

Important predefined groups and roles relevant to understanding User Access are:

- Default access group
- Default admin access group
- Organization Administrator role
Brief overview about some 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.

- **Default admin access group.** All users on the account who are Organization Administrators are members of this group. Users cannot modify the roles in the Red Hat-managed Default admin access group. Members of the Default admin access group have read-write access, which allows you to view and perform other actions in Insights for Red Hat Enterprise Linux.

- **Organization Administrator role.** All users on the account who are Organization Administrators can create and modify User Access groups and grant access to other account users. To find out whether you are an Organization Administrator, click your name in the Red Hat Hybrid Cloud Console header, in the upper right of your screen, and see whether the words “Org. Administrator” show under your username.

**IMPORTANT**

**Requesting elevated access** If you do not have access to features that you need, you can:

- Contact Customer Service to get Organization Administrator details for your account.
  - Provide your account number when you send the request.
- Contact the Organization Administrator and ask for access, providing the following information:
  - The name of the role you need access to, for example, Remediations administrator
  - A link to full User Access documentation, to help inform the Organization Administrator about how to give you access.

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

- 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 and integrations on the Red Hat Hybrid Cloud Console.
- 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


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>
<thead>
<tr>
<th>Fact Name</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ansible</td>
<td>Category with a list of Ansible-related facts</td>
<td>controller_version with a value of 4.0.0</td>
</tr>
<tr>
<td>arch</td>
<td>System architecture</td>
<td>x86_64</td>
</tr>
<tr>
<td>bios_release_date</td>
<td>BIOS release date; typically MM/DD/YYYY</td>
<td>01/01/2011</td>
</tr>
<tr>
<td>bios_vendor</td>
<td>BIOS vendor name</td>
<td>LENOVO</td>
</tr>
<tr>
<td>bios_version</td>
<td>BIOS version</td>
<td>1.17.0</td>
</tr>
<tr>
<td>cloud_provider</td>
<td>Cloud vendor. Values are google, azure, aws, alibaba, or empty</td>
<td>google</td>
</tr>
<tr>
<td>cores_per_socket</td>
<td>Number of CPU cores per socket</td>
<td>2</td>
</tr>
<tr>
<td>cpu_flags</td>
<td>Category with a list of CPU flags. Each name is the CPU flag (ex: vmx), and the value is always enabled.</td>
<td>vmx, with a value of enabled.</td>
</tr>
<tr>
<td>enabled_services</td>
<td>Category with a list of enabled services. Each name in the category is the service name (ex: crond), and the value is always enabled.</td>
<td>crond, with a value of enabled.</td>
</tr>
<tr>
<td>fqdn</td>
<td>System Fully Qualified Domain Name</td>
<td>system1.example.com</td>
</tr>
<tr>
<td>infrastructure_type</td>
<td>System infrastructure; common values are virtual or physical</td>
<td>virtual</td>
</tr>
<tr>
<td>infrastructure_vendor</td>
<td>Infrastructure vendor; common values are kvm, vmware, baremetal, etc.</td>
<td>kvm</td>
</tr>
<tr>
<td>Fact Name</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>installed_packages</td>
<td>List of installed RPM packages. This is a category.</td>
<td>bash, with a value of 4.2.46-33.el7.x86_64.</td>
</tr>
<tr>
<td>installed_services</td>
<td>Category with a list of installed services. Each name in the category is the service name (ex: crond), and the value is always installed.</td>
<td>crond, with a value of installed.</td>
</tr>
<tr>
<td>kernel_modules</td>
<td>List of kernel modules. Each name in the category is the kernel module (ex: nfs), and the value is enabled.</td>
<td>nfs, with a value of enabled.</td>
</tr>
<tr>
<td>last_boot_time</td>
<td>The boot time in YYYY-MM-DDTHH:MM:SS format. Informational only; we do not compare boot times across systems.</td>
<td>2019-09-18T16:54:56</td>
</tr>
<tr>
<td>mssql</td>
<td>Category with a list of MSSQL-related facts</td>
<td>mssql_version with a value of 15.0.4153.1</td>
</tr>
<tr>
<td>network_interfaces</td>
<td>List of facts related to network interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>number_of_cpus</td>
<td>Total number of CPUs</td>
<td>1</td>
</tr>
<tr>
<td>number_of_sockets</td>
<td>Total number of sockets</td>
<td>1</td>
</tr>
<tr>
<td>os_kernel_version</td>
<td>Kernel version</td>
<td>4.18.0</td>
</tr>
<tr>
<td>Fact Name</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>os_release</strong></td>
<td>Kernel release</td>
<td>8.1</td>
</tr>
<tr>
<td><strong>running_processes</strong></td>
<td>List of running processes. The fact name is the name of the process, and the value is the instance count.</td>
<td><strong>crond</strong>, with a value of <strong>1</strong>.</td>
</tr>
<tr>
<td><strong>sap_instance_number</strong></td>
<td>SAP instance number</td>
<td>42</td>
</tr>
<tr>
<td><strong>sap_sids</strong></td>
<td>SAP system ID (SID)</td>
<td>A42</td>
</tr>
<tr>
<td><strong>sap_system</strong></td>
<td>Boolean field that indicates if SAP is installed on the system</td>
<td>True</td>
</tr>
<tr>
<td><strong>sap_version</strong></td>
<td>SAP version number</td>
<td>2.00.052.00.1599 235305</td>
</tr>
<tr>
<td><strong>satellite_managed</strong></td>
<td>Boolean field that indicates is a system is registered to a Satellite server.</td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>selinux_current_mode</strong></td>
<td>Current SELinux mode</td>
<td>enforcing</td>
</tr>
<tr>
<td><strong>selinux_config_file</strong></td>
<td>SELinux mode set in the config file</td>
<td>enforcing</td>
</tr>
<tr>
<td><strong>systemd</strong></td>
<td>The number of failures, number of current jobs queued, and current state of systemd</td>
<td>state with a value of degraded</td>
</tr>
<tr>
<td><strong>system_memory</strong></td>
<td>Total system memory in human-readable form</td>
<td>3.45 GiB</td>
</tr>
<tr>
<td><strong>tuned_profile</strong></td>
<td>Current profile resulting from the command <strong>tuned-adm active</strong></td>
<td>desktop</td>
</tr>
<tr>
<td><strong>yum_repos</strong></td>
<td>List of yum repositories. The repository name is added to the beginning of the fact. Each repository has the associated facts <strong>base_url</strong>, <strong>enabled</strong>, and <strong>gpgcheck</strong>.</td>
<td>Red Hat Enterprise Linux 7 Server (RPMs). <strong>base_url</strong> I would have the value <strong><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></strong></td>
</tr>
</tbody>
</table>

5.2. OPERATORS

Table 5.2. Available Operators in Conditions
<table>
<thead>
<tr>
<th>Operators</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Operators</strong></td>
<td>AND</td>
</tr>
<tr>
<td></td>
<td>OR</td>
</tr>
<tr>
<td><strong>Boolean Operators</strong></td>
<td>EQUAL</td>
</tr>
<tr>
<td></td>
<td>NOTEQUAL</td>
</tr>
<tr>
<td><strong>Numeric Compare Operators</strong></td>
<td>GT</td>
</tr>
<tr>
<td></td>
<td>GTE</td>
</tr>
<tr>
<td></td>
<td>LT</td>
</tr>
<tr>
<td></td>
<td>LTE</td>
</tr>
<tr>
<td><strong>String Compare Operator</strong></td>
<td>CONTAINS</td>
</tr>
<tr>
<td><strong>Array Operators</strong></td>
<td>IN</td>
</tr>
<tr>
<td></td>
<td>CONTAINS</td>
</tr>
<tr>
<td><strong>Parser Operators</strong></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>AND</td>
</tr>
<tr>
<td></td>
<td>NOT</td>
</tr>
<tr>
<td></td>
<td>EQUAL</td>
</tr>
<tr>
<td></td>
<td>NOTEQUAL</td>
</tr>
<tr>
<td></td>
<td>CONTAINS</td>
</tr>
<tr>
<td></td>
<td>NEG</td>
</tr>
</tbody>
</table>
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

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

Prerequisites

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

Procedure

To provide your 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 more details about the issue or enhancement in the Description text box.
4. You are automatically listed as the Reporter.
5. Click the Create button.

A documentation issue has been created and will be routed to the appropriate documentation team. Thank you for taking the time to provide feedback.