Red Hat Insights 2020-04

Configuring and Using Hooks Notifications For Policies

How to configure and use hooks to notify on third-party applications

Last Updated: 2020-08-18

Red Hat Insights 2020-04 Configuring and Using Hooks Notifications For Policies

How to configure and use hooks to notify on third-party applications

Red Hat Customer Content Services

Legal Notice

Abstract

This document demonstrates how to configure and use hooks in Policies to notify on third-party applications. Providing Feedback: If you have a suggestion to improve this document or find an error, submit a Bugzilla report at http://bugzilla.redhat.com against Cloud Software Services (cloud.redhat.com) for the Policies component.

Table of Contents

CHAPTER 1. OVERVIEW

IMPORTANT

Hooks integration on cloud.redhat.com is currently only available as Beta.

Webhooks, or simply hooks, enables Red Hat Insights to send event-driven notifications to a customer's own hooks-compatible tooling, as those events happen. This frees administrators from having to routinely check into the Insights user interface, enabling a more event-driven monitoring strategy.

Policies integrate with Insights webhooks for their actions. Webhooks are responsible for sending POST messages as notifications to third-party applications that support incoming webhooks integration, such as instant messaging platforms, external ticketing systems among others. This provides users with the ability to integrate cloud.redhat.com to their own operational workflow.

NOTE

- Use the Role Based Access Control (RBAC) capability in https://cloud.redhat.com (Settings  > User access) to control user access for Policies.
- See Role Based Access Control for Red Hat Insights and cloud management services for Red Hat Enterprise Linux for more information about this feature and example use cases.

CHAPTER 2. USING HOOKS TO NOTIFY ON THIRD-PARTY APPLICATIONS

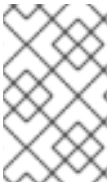
To assist operational management, you can use webhooks to notify on third-party applications that support incoming webhooks as an action for event-driven notification in policies, say, when system resources are configured above threshold, for example. Many commonly-used applications that are part of your daily workflow allow hooks integration.

Using hooks to notify on third-party applications requires:

1. Configuring an incoming webhook in the third-party application.
2. Adding a new hook via Red Hat Insights settings.
3. Creating a new policy with **Send to hook** as the trigger action.

CHAPTER 3. USING HOOKS TO NOTIFY ON WEBHOOK.SITE

This workflow example describes how to configure a hook and use it as an action in Policies to notify on Webhook.site. Webhook.site allows you to test, inspect, forward and create custom actions for any incoming HTTP request or e-mail.



NOTE

Webhook.site instantly generates a unique, random URL that you can use to test and debug Webhooks and HTTP requests, as well as to create your own workflows. So, no configuration is required to obtain an incoming webhook URL on Webhook.site.

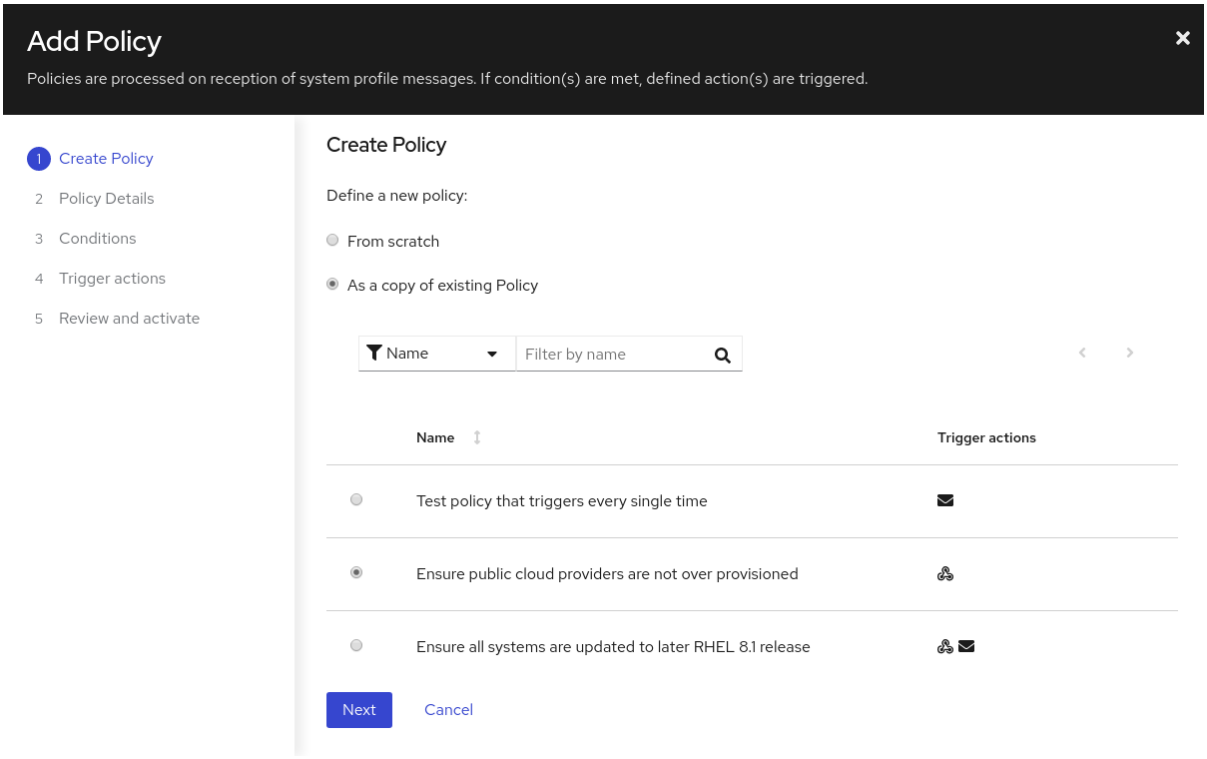
3.1. ADDING A NEW HOOK VIA SETTINGS

1. In the cloud.redhat.com beta platform, click Policies under Red Hat Insights.
2. Click Settings  , then select **Hooks** on the left-side menu.
3. Click **New hook**.
4. Enter a **Name** for the new hook.
5. Enter the **URL** for the service you want to push notifications to. In this case, enter the randomly generated URL obtained on Webhook.site.
6. Under Triggers, select **Policies**, **Triggered policies** and **All** policies.
7. Use the toggle switch located on the upper-right to activate the hook.
8. Click **Submit**.

Your new hook is now added and listed on the Hooks page. Click the options menu  next to the hook and click **Test**. This will send a message to the endpoint URL as a test event. If the test event is successful, the status for the new hook you added will show **Success** with a green check mark. You can now create a new policy with the trigger action.

3.2. CREATING A NEW POLICY WITH SEND TO HOOK AS THE TRIGGER ACTION

1. In the cloud.redhat.com beta platform, click Policies under Red Hat Insights.
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.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 said public cloud providers are running with CPU hardware higher than the allowed limit.
8. Click **Validate condition**, then click **Next**.
9. On the Trigger actions page, click **Add trigger actions** and select **Send to hook**
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**.

When the policy is evaluated on a system check-in, and if the condition in the policy is met, a notification will be sent to the configured hook using the endpoint URL, and hook settings added in Red Hat Insights. You will see the POST request logged instantly in Webhook.site with additional request details and the raw message content. Webhook.site offers Custom Action that allows additional processing and action on your requests.