Integrating the Red Hat Hybrid Cloud Console with third-party applications

Configuring integrations between third-party tools and the Red Hat Hybrid Cloud Console
Integrating the Red Hat Hybrid Cloud Console with third-party applications

Configuring integrations between third-party tools and the Red Hat Hybrid Cloud Console
Abstract

You can configure Red Hat Insights notifications to integrate with third-party applications. 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

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CHAPTER 1. ABOUT INTEGRATIONS AND EVENTS IN THE RED HAT HYBRID CLOUD CONSOLE</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>CHAPTER 2. INSTALLING AND CONFIGURING RED HAT INSIGHTS APPLICATION FOR SPLUNK</strong></td>
<td>4</td>
</tr>
<tr>
<td>2.1. ABOUT THE RED HAT INSIGHTS APPLICATION FOR SPLUNK</td>
<td>4</td>
</tr>
<tr>
<td>2.2. CONTACTING SUPPORT</td>
<td>4</td>
</tr>
<tr>
<td>2.3. PREREQUISITES</td>
<td>4</td>
</tr>
<tr>
<td>2.4. INSTALLING THE RED HAT INSIGHTS APPLICATION FOR SPLUNK</td>
<td>4</td>
</tr>
<tr>
<td>2.4.1. Configuring the HEC URL in Splunk Cloud</td>
<td>7</td>
</tr>
<tr>
<td>2.5. COMPLETING THE SETUP PROCESS</td>
<td>7</td>
</tr>
<tr>
<td>2.6. ENABLING THE HEC TOKEN</td>
<td>11</td>
</tr>
<tr>
<td>2.7. MANUALLY CONFIGURING A NOTIFICATIONS ADMINISTRATOR GROUP IN YOUR INSIGHTS ACCOUNT</td>
<td>12</td>
</tr>
<tr>
<td>2.8. MANUALLY CONFIGURING A SPLUNK INTEGRATION</td>
<td>13</td>
</tr>
<tr>
<td>2.9. TROUBLESHOOTING INTEGRATION WITH SPLUNK</td>
<td>15</td>
</tr>
<tr>
<td>2.9.1. Events show as sent within Insights but do not appear in Splunk</td>
<td>15</td>
</tr>
<tr>
<td>2.9.2. Cannot click links in the Events table when using real-time search</td>
<td>16</td>
</tr>
<tr>
<td><strong>CHAPTER 3. INSTALLING AND CONFIGURING THE SERVICENOW FLOW TEMPLATES FOR RED HAT INSIGHTS</strong></td>
<td>17</td>
</tr>
<tr>
<td>3.1. CONTACTING SUPPORT</td>
<td>17</td>
</tr>
<tr>
<td>3.2. INSTALLING AND CONFIGURING THE SERVICENOW FLOW TEMPLATES</td>
<td>17</td>
</tr>
<tr>
<td>3.3. TROUBLESHOOTING INTEGRATION WITH SERVICENOW</td>
<td>19</td>
</tr>
<tr>
<td><strong>CHAPTER 4. CONFIGURING RED HAT INSIGHTS INTEGRATION WITH SLACK</strong></td>
<td>21</td>
</tr>
<tr>
<td>4.1. CONTACTING SUPPORT</td>
<td>21</td>
</tr>
<tr>
<td>4.2. CONFIGURING SLACK INTEGRATION</td>
<td>21</td>
</tr>
<tr>
<td>4.3. CONFIGURING THE SLACK INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE</td>
<td>24</td>
</tr>
<tr>
<td><strong>CHAPTER 5. CONFIGURING THE EVENT-DRIVEN ANSIBLE INTEGRATION WITH THE RED HAT HYBRID CLOUD CONSOLE</strong></td>
<td>28</td>
</tr>
<tr>
<td>5.1. CONTACTING SUPPORT</td>
<td>28</td>
</tr>
<tr>
<td>5.2. CONFIGURING INCOMING WEBHOOKS IN ANSIBLE</td>
<td>28</td>
</tr>
<tr>
<td>5.3. CONFIGURING THE EVENT-DRIVEN ANSIBLE INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE</td>
<td>29</td>
</tr>
<tr>
<td>5.4. CREATING THE BEHAVIOR GROUP FOR THE EVENT-DRIVEN ANSIBLE INTEGRATION</td>
<td>30</td>
</tr>
<tr>
<td><strong>CHAPTER 6. CONFIGURING RED HAT HYBRID CLOUD CONSOLE INTEGRATION WITH MICROSOFT TEAMS</strong></td>
<td>32</td>
</tr>
<tr>
<td>6.1. CONTACTING SUPPORT</td>
<td>32</td>
</tr>
<tr>
<td>6.2. CONFIGURING INCOMING WEBHOOKS IN MICROSOFT TEAMS</td>
<td>32</td>
</tr>
<tr>
<td>6.3. CONFIGURING THE MICROSOFT TEAMS INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE</td>
<td>33</td>
</tr>
<tr>
<td>6.4. CREATING THE BEHAVIOR GROUP FOR THE MICROSOFT TEAMS INTEGRATION</td>
<td>33</td>
</tr>
<tr>
<td><strong>PROVIDING FEEDBACK ON RED HAT DOCUMENTATION</strong></td>
<td>35</td>
</tr>
</tbody>
</table>
CHAPTER 1. ABOUT INTEGRATIONS AND EVENTS IN THE RED HAT HYBRID CLOUD CONSOLE

Integrations allow you to route event-triggered notifications to your preferred third-party tools and platforms, such as Splunk and ServiceNow. Using integrations expands the scope of notifications beyond emails and messages, so that you can view and manage Insights events from your preferred platform dashboard.

**IMPORTANT**

You must have Organization Administrator or Notifications Administrator privileges to configure notifications on Red Hat Insights. In addition, each third-party application requires specific permissions for the application to configure notifications.

To learn more about notifications, see Configuring notifications on the Red Hat Hybrid Cloud Console.
CHAPTER 2. INSTALLING AND CONFIGURING RED HAT INSIGHTS APPLICATION FOR SPLUNK

2.1. ABOUT THE RED HAT INSIGHTS APPLICATION FOR SPLUNK

The Red Hat Insights application for Splunk forwards selected Insights events to Splunk. The application seamlessly integrates with Red Hat Insights, so that you can focus on handling the data on the Splunk application side, in the same way you manage other sources of data. Once the integration has been configured, you can view and manage Insights notifications from the Splunk dashboard without having to open the Red Hat Hybrid Cloud Console.

Additional resources

- For more information about Splunk, see https://splunk.com.
- For more information about Splunkbase, the Splunk application marketplace, see https://splunkbase.splunk.com.

2.2. CONTACTING SUPPORT

If you have any issues with the Red Hat Insights application for Splunk, contact Red Hat for support at https://access.redhat.com. Splunk will not provide warm transfers or basic troubleshooting. The Red Hat Insights application for Splunk is fully supported by Red Hat.

2.3. PREREQUISITES

- **sc_admin** (Splunk Cloud Administrator) role to install apps on Splunk Cloud Platform.
- admin-level access to install apps in Splunk Enterprise.
- Organization Administrator-level login access to Red Hat Insights.

2.4. INSTALLING THE RED HAT INSIGHTS APPLICATION FOR SPLUNK

Prerequisites

- An Organization Administrator-level login to Red Hat Insights.
- The **sc_admin** (Splunk Cloud Administrator) role to install apps on Splunk Cloud Platform.
- The **admin** role to install apps on Splunk Enterprise. For more information about creating the admin role, see Create secure administration credentials in the Splunk documentation.
- Popup blockers are disabled in your browser.

Procedure

1. Navigate to the Splunk home page.
2. Click **Settings** (gear icon) in the left panel to manage apps. The Apps page opens.
3. Use the Search field to search for Red Hat Insights Application for Splunk. The application appears in the search results.

4. Select the application.

5. Click Install. When the installation process completes, the message Install successful displays.

6. Click Set up now. The Set up integration with Red Hat page displays. The page includes the HTTP Event Collector (HEC) name and Default index fields.

7. Open Splunk in a second browser window or tab.

8. In the second Splunk page, click the Settings drop-down menu in the upper right of the page.

9. Navigate to the Data section and select Indexes.

10. Click New Index.

11. Type a name for the index in the Name field (for example, redhatinsights). Leave the rest of the fields blank.

12. Click Save. The index you created appears in the Indexes list.

13. Click Enable next to the name of the new index to enable it.

14. Navigate back to the first Splunk screen with the Set up integration with Red Hat page.

15. Type the name for the HEC in the HEC name field (for example, redhatinsights).

16. Type the name of the index you just created in the Default index field (for example, redhatinsights).

17. Click Next.

18. Click Review.

19. Click Submit. The HEC name you created appears in the HEC Name field.

20. Click Next to create the HEC URL and HEC Token.
21. Click **Next: Configure Splunk integration in Insights** This button is disabled until you click on a **Copy** button for either the HEC URL or HEC token. This opens the console in a new browser tab.

**NOTE**

If the new tab for the console does not open, disable the popup blocker in your browser.

22. Click **Copy** to copy the HEC URL value in Splunk Enterprise, and then paste it into the **Splunk HEC URL** field on the Integrations page in **console.redhat.com**.

23. Add the port, if needed. The default port for Splunk Cloud Platform is 443. The default port for Splunk Enterprise and Splunk Cloud free trial is 8088.

**NOTE**

If you are using Splunk Cloud, configure the HEC URL to follow Splunk Cloud format. If you are using Splunk Enterprise, skip the following section.
2.4.1. Configuring the HEC URL in Splunk Cloud

The HEC URL in Splunk Cloud Platform takes the following standard form:

<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>

For Splunk Cloud Platform on Google Cloud Platform (GCP), the HEC URL standard form is slightly different:

<protocol>://http-inputs.<host>.splunkcloud.com:<port>/<endpoint>

- Edit the HEC URL you just pasted into the Splunk HEC URL field on the Integrations page. Substitute your values for the following:
  - **protocol**: either http or https
  - **host**: name of the Splunk Cloud Platform instance that runs the HEC, followed by the domain .splunkcloud.com.
  - **port**: the HEC port number (443 by default on Splunk Cloud Platform instances).
  - **endpoint**: the HEC endpoint you want to use. In many cases, you use the /services/collector/event endpoint for JavaScript Object Notation (JSON)-formatted events, or the services/collector/raw endpoint for raw events.

**NOTE**

The HEC URL for AWS has a slightly different format than the HEC URL on GCP.

- Add http-inputs- before the host on AWS.
- Add http-inputs. before the host on GCP.
- In both cases, add the domain .splunkcloud.com after the host value.

**Examples**

- Splunk Cloud Platform on GCP using JSON:
  
  https://http-inputs.myhost.splunkcloud.com:443/services/collector/event

- Splunk Cloud free trial on AWS using raw events:


2.5. COMPLETING THE SETUP PROCESS


2. In console.redhat.com, click Run configuration. Red Hat Insights sets up the integration, creates the behavior group, and associates Insights events to the behavior group. The status message section on the right side of the page shows the status of each of these actions.
3. When the setup completes successfully, click **Next: Review**. The application returns the message **Splunk integration in Insights completed**.

4. Click **Go back to the Splunk application** This redirects you to the Set up integration with Red Hat screen in Splunk.

5. Click **Finish set up** to complete the setup in Splunk.
6. Click Go to dashboard to be redirected to your Splunk dashboard.

NOTE
If the integration configuration fails during the Insights setup process, contact Red Hat support.

The setup automation performs the following tasks:

- Creates a user group with Notifications Administrator role using the Organization Administrator permissions. You can also create the user group manually. For more information about manual configuration, see Manually configuring a Notifications Administrator group in your Insights account.

- Uses the Splunk HEC URL and HEC token to create a new integration called SPLUNK_AUTOMATION, with the integration type Splunk.
- Creates a new Behavior Group called SPLUNK_AUTOMATION_GROUP on the RHEL bundle. The group includes an action to send notifications to the SPLUNK_AUTOMATION Splunk integration.

- Assigns the new Behavior Group SPLUNK_AUTOMATION_GROUP to all Insights services. This forwards the events from all services to Splunk. Currently, the Behavior Group forwards events from the Advisor, Policies, and Drift services.

When Splunk begins to receive notifications from Insights, the Red Hat Insights application for Splunk dashboard shows event activity. Each number contains a hyperlink to Insights.

To view a list of Insights events on the Splunk dashboard, click the Events tab. Each event is hyperlinked to Insights.

Additional Resources

- Splunk Enterprise
- Install apps on your Splunk Cloud deployment
- Configure HTTP Event Collector on Splunk Enterprise
- Configure HTTP Event Collector on Splunk Cloud Platform
- Configure user access
- Configure notifications on the Red Hat Hybrid Cloud Console
- Manually configuring a Notifications Administrator group in your Insights account

### 2.6. ENABLING THE HEC TOKEN

Before Splunk can receive Insights events, you must enable the HEC token.

**Prerequisites**

- An Organization Administrator-level login to Red Hat Insights.
- You must have the `admin` role in Splunk Enterprise, or the `sc_admin` role in Splunk Cloud.

**Procedure**

1. From the Splunk main page, navigate to **Settings**.

2. Select **Data Inputs**, and then select **HTTP Event Collector**. The HTTP Event Collector page shows the HEC, its Token value, the corresponding index that you selected during setup, and the status of the HEC.

3. Click **Global Settings** in the upper right corner of the page. The Edit Global Settings dialog box displays.
4. Select **Enabled**. This enables the HEC token that was automatically created during the setup process.

**NOTE**

The HEC token uses a default HTTP port number of 8088. If you are using a different port (such as port 443 for Splunk Cloud), you must update your Insights Splunk Integration to match.

Additional Resources

- For more information about the HEC token in Splunk Cloud, see [Configure HTTP Event Collector on Splunk Cloud Platform](#) in the Splunk documentation.
- For more information about setting up and using the HEC in Splunk Enterprise, see [Set up and use HTTP Event Collector on Splunk Enterprise](#) in the Splunk Enterprise documentation.

## 2.7. MANUALLY CONFIGURING A NOTIFICATIONS ADMINISTRATOR GROUP IN YOUR INSIGHTS ACCOUNT

**IMPORTANT**

The Red Hat Insights application for Splunk automated installation/setup process automatically configures a Notifications Administrator role and group in your Insights account. Use this procedure only if you want to manually create the Notifications Administrator role and group.

**Prerequisites**

- An Organization Administrator-level login to Red Hat Insights.

**Procedure**
1. Navigate to Settings, and then select My User Access from the drop-down menu.


3. Click Create Group. The Name and Description page appears.

4. Create a name for the group (for example, splunknotifgroup) and click Next. The Add Roles page appears.

5. To create the Notifications Administrator role, click in the Search field and type notif.

6. Select Notifications Administrator from the search results, and then click Next. The Add Members page appears.

7. Select the group members from the list who should have the Notifications Administrator role.

8. Click Next. The Review Details page appears.

9. Review the details: Group Name, Role, and Members, and then click Submit.

Insights verifies the details, and then the new group appears on the Groups page. The Success adding group message displays. Group members (for example, members of splunknotifgroup) can now configure notifications and integrations.

2.8. MANUALLY CONFIGURING A SPLUNK INTEGRATION

IMPORTANT

The Red Hat Insights application for Splunk automated installation/setup process automatically configures Splunk integration to your Insights account. Use this procedure only if you want to configure the integration manually.

Prerequisites

- HEC URL from Splunk Cloud or Splunk Enterprise
- HEC token value from Splunk Cloud or Splunk Enterprise
- Notifications Administrator access to Red Hat Insights

Procedure

1. Navigate to Settings, and select Integrations from the drop-down menu. The Integrations page appears.

2. Click Add Integration. The Add Integration dialog box appears.
3. Click **Type** from the drop-down menu and select **Splunk**.

4. Type a name for your new integration into the **Integration Name** field (for example, `redhat_splunk`).

5. In the **Endpoint URL** field, add your Splunk HEC endpoint URL.
   
   a. For Splunk Enterprise, Splunk uses port 8088 by default. For example: `https://<splunk-endpoint>:8088`
   
   b. For Splunk Cloud, Splunk uses port 443. For more information about Splunk Cloud on AWS or GCP, see [Send data to HTTP Event Collector](https://<splunk-endpoint>).
IMPORTANT

The service automatically adds `<endpoint>` (the http path). You do not need to include it in the form input for the Endpoint URL.

6. In the **Secret token** field, add the Splunk HEC token value.

7. **Optional.** Add any notes or other information about this integration to the **Extras** field.

8. Click **Save**.

These examples show endpoint URLs with the correct port numbers for Splunk platforms.

- **On premise (Splunk Enterprise):** https://splunk.company.com:8088
- **Splunk Cloud (on AWS):** https://http-inputs-mycompany.splunkcloud.com:443
- **Splunk Cloud (on GCP):** https://http-inputs.mycompany.splunkcloud.com:443

Additional resources

- For more information about the HEC token in Splunk Cloud, see Configure HTTP Event Collector on Splunk Cloud Platform in the Splunk documentation.
- For more information about configuring ports for Splunk Cloud, see Send data to HTTP Event Collector.
- For more information about setting up and using the HEC in Splunk Enterprise, see Set up and use HTTP Event Collector on Splunk Enterprise in the Splunk Enterprise documentation.

2.9. TROUBLESHOOTING INTEGRATION WITH SPLUNK

Here are some common configuration errors in the Splunk environment that could result in Splunk not receiving events from Red Hat Insights:

- Make sure the HEC is enabled (under Global Settings). See Enabling the HEC.
- Make sure that the default index has not changed for the HEC (it should be redhatinsights).
- Make sure the firewall allows for incoming requests on the configured Splunk HEC port (default for Splunk Enterprise is 8088, and default for Splunk Cloud is 443). If you are using AWS for your instance, allow any of the ports Splunk may need. For more information, refer to Splunk Phantom ports and endpoints.

2.9.1. Events show as sent within Insights but do not appear in Splunk

- Check your firewall for where your Splunk setup resides.
- Ensure that the Splunk port is allowed (port 8088 by default for Splunk Enterprise or port 443 by default for Splunk Cloud).

Additional resources

- For more information about configuring Splunk HEC ports, see Splunk Phantom ports and endpoints.
### 2.9.2. Cannot click links in the Events table when using real-time search

If you select a relative value from the Timestamp field in the Events table, you can then click any displayed event in the table to display a new tab with information about the affected system or policy.

However, if you select a real-time value from the Timestamp field, the displayed events do not respond when clicked. This is a limitation in Splunk. Splunk recommends that you avoid clicking real-time events to view event details.
CHAPTER 3. INSTALLING AND CONFIGURING THE SERVICENOW FLOW TEMPLATES FOR RED HAT INSIGHTS

The Flow Templates for Red Hat Insights application integrates with Insights for Red Hat Enterprise Linux services. The templates provide ServiceNow Flows for creating Incidents out of found vulnerabilities, performance, system configuration recommendation, and other risks. The application includes a sample flow that you can edit to customize it for your organization.

This application forwards selected Red Hat Insights events to ServiceNow. Flow Templates for Red Hat Insights seamlessly integrates with Red Hat Insights, so that you can focus on handling the data on the ServiceNow application side, in the same way you manage other sources of data.

Before data flow can take place, you must install the ServiceNow IntegrationHub Enterprise Pack Installer plugin. Once the plugin and the application are configured, event data flows from the Red Hat Hybrid Cloud Console to your ServiceNow instance. A ServiceNow REST API - Asynchronous trigger receiver is used within the application flow.

This version of the application supports handling events from the following Insights services:

- Advisor
- Vulnerability
- Any additional Red Hat Hybrid Cloud Console events that you might have configured

Install the Flow Templates for Red Hat Insights application from the ServiceNow Store.

Insights for RHEL is included as part of your Red Hat subscription, and is accessible through the Red Hat Hybrid Cloud Console.

3.1. CONTACTING SUPPORT

If you have any issues with the Red Hat Insights application for ServiceNow, contact Red Hat for support at access.redhat.com. ServiceNow will not provide troubleshooting. The Red Hat Insights application for ServiceNow is fully supported by Red Hat.

Additional resources

- For more information about the ServiceNow Store, see ServiceNow Store.
- For more information about ServiceNow, see ServiceNow.

3.2. INSTALLING AND CONFIGURING THE SERVICENOW FLOW TEMPLATES

Prerequisites

- You have an Organization Administrator-level login to Insights for Red Hat Enterprise Linux.
- Notifications Administrator-level permissions are configured in User Access.
- Ensure that you have a Red Hat Subscription, and that you can access the Red Hat Hybrid Cloud Console.
- Popup blockers are disabled in your browser.
- ServiceNow IntegrationHub Enterprise Pack Installer plugin is installed. If it is not installed, request the plugin from ServiceNow.
- ServiceNow Roles required for installation: admin, x_rhtpp_rh_webhook.rest, and sn_appclient.app_client_company_installer (can only install applications that match the instance company), or sn_appclient.app_client_user.
- ServiceNow: Incident (write) access for table permissions.
- You are using the San Diego or later release of ServiceNow.

### Procedure

1. Log in to your ServiceNow instance.

2. Navigate to the ServiceNow Store home page.
   a. Install the Flow Templates for Red Hat Insights from the ServiceNow Store (or as an Update Set).
   b. Create a new user with User ID rh_insights_integration.
   c. Check Internal Integration User for the user you just created.
   d. Ensure that the user is Active.
   e. Assign role x_rhtpp_rh_webhook.rest to the user.
   f. Generate a password for the user. Copy this information for use during the setup process.

3. Open console.redhat.com in a new browser window or tab.

4. Navigate to Red Hat Hybrid Cloud Console > Settings > Integrations. For more information about how to set up integrations, see Configuring integrations.
   a. Click Add integration.
   b. Create a name for the integration, such as ServiceNow integration.
   c. Select the ServiceNow integration type.
   d. Provide this Endpoint URL and replace `<instance.servicenow.com>` with your ServiceNow instance:
   e. The checkbox to Enable SSL is checked by default.
   f. In the Secret token field, paste the generated password of the rh_insights_integration user that you created in ServiceNow.


6. Select Notifications, and then select Red Hat Enterprise Linux.
7. Click **Create new group**. The Create new behavior group dialog box appears.

8. Type the name of the new behavior group in the Name field and click **Next**.

9. For Actions, select **Integration: ServiceNow** from the drop-down list.

10. For Recipient, select the integration for ServiceNow that you created earlier (for example, **ServiceNow integration**).

11. Click **Next**. The Associate event types screen appears.

12. Select the following event types from the list:
   - Advisor new recommendation
   - New vulnerability with CVSS >= 7.0
   - New vulnerability with Critical Severity
   - New vulnerability containing Security rule
   - Any vulnerability with known exploit

13. Click **Next**, and then click **Finish** to complete the setup process.

**Verification**

To confirm that the application has been configured successfully, view the Event Log on the Red Hat Hybrid Cloud Console, and view Flow Executions on your ServiceNow Instance (**Process Automation > Flow Administration > Today’s Executions**).

Note that events are generated on certain conditions (for example, when a system configured with Red Hat Insights checks in). If no events appear in ServiceNow, check the Event log to see whether any events matching the conditions have occurred.

**NOTE**

If the integration configuration fails during the Insights setup process, contact Red Hat support.

**Additional resources**

- ServiceNow Flow Designer
- ServiceNow Store
- Install a ServiceNow Store Application
- Configuring notifications on the Red Hat Hybrid Cloud Console

### 3.3. TROUBLESHOOTING INTEGRATION WITH SERVICENOW

If ServiceNow is not receiving events from Insights, check these configuration steps.

- Ensure that the integration in the Red Hat Hybrid Cloud Console is enabled and has type **ServiceNow**.
• Ensure that the integration in the Red Hat Hybrid Cloud Console has a correct URL. The URL should start with

• Ensure that the x_rhtpp_rh_webhook.rest user role is defined in ServiceNow. Otherwise, notifications from Insights will not work even if the application has been installed correctly.

• Ensure that the rh_insights_integration ServiceNow user exists, is active, and has the x_rhtpp_rh_webhook.rest role assigned.

• If necessary, reset the password for the rh_insights_integration ServiceNow user, and reset the user password in the integration on the Red Hat Hybrid Cloud Console.

Additional resources

• Troubleshoot notification failures with the event log and integration settings
CHAPTER 4. CONFIGURING RED HAT INSIGHTS INTEGRATION WITH SLACK

You can configure Red Hat Insights to send event notifications to a new or existing Slack channel. This enables you to send notifications to a selected user, or to all users on a channel. The Slack integration supports events from all Insights services.

NOTE
The Slack integration in this example is configured for Red Hat Enterprise Linux. The integration also works with other Red Hat OpenShift, Application Services, and Red Hat Hybrid Cloud Console events.

The Slack integration uses Incoming Webhooks to receive event data. For more information about webhooks, see https://api.slack.com/messaging/webhooks.

4.1. CONTACTING SUPPORT
If you have any issues with the Red Hat Insights integration with Slack, contact Red Hat for support at access.redhat.com. Slack will not provide troubleshooting. The Red Hat Insights integration with Slack is fully supported by Red Hat.

Additional resources
- https://api.slack.com/messaging/webhooks

4.2. CONFIGURING SLACK INTEGRATION

NOTE
Sending messages using Incoming Webhooks is a legacy application. The preferred method to integrate Slack is to build your own custom workflow as shown in the Slack help center at https://slack.com/help. However, integrating Red Hat Insights using this method is not yet available because custom workflows in Slack do not yet support nested JSON structures as workflow variables.

Prerequisites
- Owner or admin access to the Slack instance where you want to add Incoming Webhooks.
- App Manager permissions to add Slack apps to a channel.
- A Slack channel or user to receive the notifications.

Procedure
1. In the Slack application, navigate to the channel or user name to receive the notifications.
2. Click the channel name at the top of the screen. The configuration window appears.
3. Select Integrations, and then click Manage Apps. The Add apps to channel window appears.
4. Search for **Incoming Webhooks**, and then select it from the search results.

5. Click **Add to Slack** to add the Insights integration to the channel. The Post to Channel box appears.

6. Click the **Choose a Channel** drop-down menu to select an existing channel, or type the user or channel name in the field. To create a new channel, click or create a new channel, and then type the name of the new channel and an optional description. Click **Create**.

   **NOTE**

   The field requires a channel name. If you do not specify a channel, Slack integration uses **#general**.

   **NOTE**

   If you do not have App Manager permissions to add the app to the channel, click the **Request Configuration** button to send an add request to the App Manager for the channel.

7. Click **Add Incoming Webhooks Integration**. The Configuration page for the app appears in the Slack app directory.

   **slack** app directory

   ![Slack app directory](image)

   **Incoming Webhooks**

   **Setup Instructions**

   We'll guide you through the steps necessary to configure an Incoming Webhook so you can start sending data to Slack.

   **Message Attachments**

   Learn how to send richly-formatted messages to your Incoming Webhook.

   **Integration Settings**

   **Post to Channel**

   Messages that are sent to the incoming webhook will be posted here.
8. Scroll down to **Integration Settings**. The generated Webhook URL appears in the **Webhook URL** field.

9. Copy the URL displayed in the field. You will use it to set up the integration in the Red Hat Hybrid Cloud Console.

10. **Optional**: Add a name for the integration in the **Customize Name** field.

11. **Optional**: Upload an icon in the **Customize Icon** field.

12. Click **Save Settings**.

Additional resources

- https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack
- https://slack.com/help/articles/360041352714-Create-more-advanced-workflows-using-webhooks
- https://api.slack.com/admins/approvals
- https://api.slack.com/messaging/webhooks
- https://slack.com/help
4.3. CONFIGURING THE SLACK INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE

Prerequisites

- Organization administrator or Notifications administrator access to the Red Hat Hybrid Cloud Console.

Procedure

1. Navigate to the Red Hat Hybrid Cloud Console.

2. Click the gear icon to select Settings, and then select Integrations from the menu on the left side of the screen.

3. Click Add Integration.

4. Create a name for the integration (for example, SLACK_INTEGRATION).

5. Click the Type drop-down menu and select Slack.

6. Paste the URL that you copied from the Webhook URL field during Slack setup into the Endpoint URL field.

7. Add the name of the Slack channel configured during Slack setup to the Channel field.
8. Click **Save**. The Last Connection Attempt state takes a few minutes to process the change.

9. Navigate to **Notifications > Red Hat Enterprise Linux**

10. Navigate to **Behavior Groups** to add the new endpoint to an existing behavior group, or to create a new behavior group. For more information about creating behavior groups, see Configure notification behavior groups.

11. Click **Edit Behavior Group**.

12. Select **Integration: Slack** in the **Actions** column.

13. The list of configured Slack integrations shows in the **Recipient** drop-down list. Select the integration name that you previously created.
14. Click **Next**. The **Associate event types** screen appears.

15. Select the event types for which you want notifications.

16. When you have finished selecting event types, click **Next**. The Review screen appears.

17. Review the settings for the behavior group and then click **Finish**.

**NOTE**

You can create and edit multiple behavior groups to include any additional platforms that the Notifications service supports.

18. Return to **Settings > Integrations**. When the Slack integration is ready to send events to Slack, the **Last connection attempt** column shows **Ready**. If the notification reached Slack successfully, the **Last connection attempt** column shows **Success**.

When an event is triggered, Insights sends the notification to the Slack channel. The notification includes the name of the associated service, as well as that of the system that triggered the notification. To view more details, click on the hyperlinks.
Additional resources

- For more information about behavior groups, see Configure notification behavior groups.

Verification

To verify that events are being sent to the Slack channel, look in the Event Log. To view the Event Log, navigate to Settings > Notifications > Red Hat Enterprise Linux and click View event log.

Integration: Slack appears in the Actions column for the event. If the notification was successful, the integration shows green. Roll over the integration to verify that an event was sent.
CHAPTER 5. CONFIGURING THE EVENT-DRIVEN ANSIBLE INTEGRATION WITH THE RED HAT HYBRID CLOUD CONSOLE

You can configure Event-Driven Ansible to send event notifications from the Red Hat Hybrid Cloud Console or a third-party application.

The Event-Driven Ansible integration allows you to take advantage of Hybrid Cloud Console capabilities such as Red Hat Insights to continuously analyze your Ansible inventory for potential issues and recommendations. Event-Driven Ansible connects sources of events with corresponding actions via rules.

The integration with the Hybrid Cloud Console notifications service uses a webhook to trigger actions. Each account configures how and who can receive these events, with the ability to perform actions depending on the event type.

5.1. CONTACTING SUPPORT

If you have any issues with the Hybrid Cloud Console integration with Event-Driven Ansible, contact Red Hat for support.

You can open a Red Hat support case directly from the Hybrid Cloud Console by clicking Help (?) icon > Open a support case, or view more options from ? > Support options.

Additional resources

- Getting Started with Event-Driven Ansible Guide
- Event-Driven Ansible controller user guide

5.2. CONFIGURING INCOMING WEBHOOKS IN ANSIBLE

Prerequisites

- The ansible-rulebook CLI is installed. See Ansible rulebook installation for instructions.

Procedure

1. Install the Red Hat Insights collection for Event-Driven Ansible:

   ```
   $ ansible-galaxy collection install redhat.insights_eda servicenow.itsm
   $ pip3 install -r ~/.ansible/collections/ansible_collections/redhat/insights_eda/requirements.txt
   ```

2. Validate collection requirements:

   ```
   $ ansible-galaxy collection list
   # /home/username/.ansible/collections/ansible_collections/redhat/insights_eda
   Collection       Version
   ----------------------- -------
   ansible.eda      1.3.8
   community.general 7.0.1
   redhat.insights_eda 1.0.0
   servicenow.itsm  2.2.0
   ```
3. Create a simple Ansible rulebook using the Red Hat Insights collection. See the Event-Driven Ansible for Red Hat Insights documentation in Ansible Automation Hub for examples for the Red Hat Insights advisor, compliance, and vulnerability services.

4. Create an associated playbook based on the examples in the Ansible Automation Hub on the Hybrid Cloud Console.

Additional resources

- See the Event-Driven Ansible for Red Hat Insights documentation in Ansible Automation Hub for more detailed information about Event-Driven Ansible configuration.

5.3. CONFIGURING THE EVENT-DRIVEN ANSIBLE INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE

Prerequisites

- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator or as a user with Notifications Administrator permissions.
- The redhat.insights_eda collection is installed and configured.
- You have the webhook URL from Ansible.

Procedure

1. In the Hybrid Cloud Console, navigate to Settings (gear icon) > Integrations.
2. Click Add Integration.
3. In the Integration name field, enter a name for your integration (for example, ansible).
4. Select Event-Driven Ansible from the Type drop-down list.
5. Paste the URL that you copied from Ansible into the Endpoint URL field. This is the endpoint URL that points to the controller running the Event-Driven Ansible receiver.
6. The checkbox to Enable SSL verification is checked by default.

   **NOTE**

   SSL is essential for protecting the data sent to the integration endpoint. SSL should always be used when integrating the Hybrid Cloud Console with third-party applications.

7. Provide a Secret token if one is configured.

   **NOTE**

   A secret token is essential for protecting the data sent to the integration endpoint and should always be used when integrating the Hybrid Cloud Console with third-party applications.
8. To enable the notifications, click **Save**.

**Additional resources**

- For more information about setting up Notifications administrator permissions, see Configure user access in Configuring notifications on the Red Hat Hybrid Cloud Console.

### 5.4. CREATING THE BEHAVIOR GROUP FOR THE EVENT-DRIVEN ANSIBLE INTEGRATION

A behavior group defines which notifications will be sent to external services such as Event-Driven Ansible when a specific event is received by the notifications service. You can link events from any Red Hat Hybrid Cloud Console service to your behavior group.

**Prerequisites**

- You are logged in to the Hybrid Cloud Console as an Organization Administrator or as a user with Notifications Administrator permissions.
- The Event-Driven Ansible integration is configured.

**Procedure**

1. From the **Settings** menu in the console, click **Notifications > Red Hat Enterprise Linux**.
2. To open the **Create behavior group** wizard, click **Create new group**.
3. Type a name for the behavior group and click **Next**.
4. In the **Actions and Recipients** step, select **Integration: Event-Driven Ansible** from the **Actions** drop-down list.
5. From the **Recipient** drop-down list, select the name of the integration you created (for example, **console-teams**) and click **Next**.
6. In the **Associate event types** step, select one or more events for which you want to send notifications (for example, **Advisor: New recommendation**) and then click **Next**.
7. Review your behavior group settings, and click **Finish**. The new behavior group appears on the **Notifications** page.

**Verification**

1. Create an event that will trigger an Insights notification. See the Ansible Automation Hub page for an example.
2. To test the Hybrid Cloud Console integration is successful, in the Hybrid Cloud Console, go to **Settings > Notifications**.
3. Click the **View Event Log** button. The event shows the label **Integration: Event-Driven Ansible**.
If the label is green, the notification succeeded.

If the label is red, the integration might need to be adjusted.

- If the integration is not working as expected, verify that the webhook has been properly created in Event-Driven Ansible, and that the correct webhook URL is configured in the Hybrid Cloud Console integration configuration.

**NOTE**

See Troubleshoot notification failures with the event log and integration settings in the notifications documentation for more details.

**Additional resources**

- For more information about behavior groups, see Configure notification behavior groups.
CHAPTER 6. CONFIGURING RED HAT HYBRID CLOUD CONSOLE INTEGRATION WITH MICROSOFT TEAMS

You can configure the Red Hat Hybrid Cloud Console to send event notifications to all users on a new or existing channel in Microsoft Teams. The Microsoft Teams integration supports events from all services in the Hybrid Cloud Console.

The Microsoft Teams integration uses incoming webhooks to receive event data. For more information about webhooks, see Create an Incoming Webhook and Webhooks and Connectors in the Microsoft Teams documentation.

6.1. CONTACTING SUPPORT

If you have any issues with integrating the Hybrid Cloud Console with Microsoft Teams, contact Red Hat for support. Microsoft will not provide troubleshooting. The Hybrid Cloud Console integration with Microsoft Teams is fully supported by Red Hat.

You can open a Red Hat support case directly from the Hybrid Cloud Console by clicking Help ( icon) > Open a support case, or view more options from ? > Support options.

Additional resources

- Create an Incoming Webhook
- Webhooks and Connectors

6.2. CONFIGURING INCOMING WEBHOOKS IN MICROSOFT TEAMS

Prerequisites

- Admin-level access to Microsoft Teams

Procedure

1. Create a new channel in Microsoft Teams, or select an existing channel.
2. Navigate to Apps and search for the Incoming Webhook application.
3. Select the Incoming Webhook application and click Add to a team.
4. Select the team or channel name and click Set up a connector.
5. Enter a name for the incoming webhook (for example, Red Hat Notifications). This name appears on all notifications that the Microsoft Teams channel receives from the Red Hat Hybrid Cloud Console through this incoming webhook.
6. Optional: Upload an image to associate with the name of the incoming webhook. This image appears on all notifications that the Microsoft Teams channel receives from the Hybrid Cloud Console through this incoming webhook.
7. Click Create to complete creation and display the webhook URL.
8. Copy the URL to your clipboard. You need the URL to configure notifications in the Hybrid Cloud Console.
9. Click Done. The Microsoft Teams page displays the channel and the incoming webhook.

Additional resources

- For more information about incoming webhooks, see Webhooks and connectors in the Microsoft Teams documentation.

### 6.3. CONFIGURING THE MICROSOFT TEAMS INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE

**Prerequisites**

- You are logged in to the Hybrid Cloud Console as an Organization Administrator or as a user with Notifications Administrator permissions.
- You have the incoming webhook URL from Microsoft Teams.

**Procedure**

1. In the Red Hat Hybrid Cloud Console, navigate to Settings (gear icon) > Integrations.
2. Click Add Integration.
3. In the Integration name field, enter a name for your integration (for example, console-teams).
4. Select Microsoft Teams from the Type drop-down list.
5. Paste the incoming webhook URL that you copied from Microsoft Teams into the Endpoint URL field.
6. Click Save to enable the integration.

Additional resources

- For more information about setting up Notifications administrator permissions, see Configure user access in Configuring notifications on the Red Hat Hybrid Cloud Console.

### 6.4. CREATING THE BEHAVIOR GROUP FOR THE MICROSOFT TEAMS INTEGRATION

A behavior group defines which notifications will be sent to external services such as Microsoft Teams when a specific event is received by the notifications service. You can link events from any Red Hat Hybrid Cloud Console service to your behavior group.

**Prerequisites**

- You are logged in to the Hybrid Cloud Console as an Organization Administrator or as a user with Notifications Administrator permissions.
- The Microsoft Teams integration is configured.

**Procedure**
1. From the **Settings** menu in the Hybrid Cloud Console, click **Notifications > Red Hat Enterprise Linux**.

2. To open the **Create behavior group** wizard, click **Create new group**.

3. Type a name for the behavior group and click **Next**.

4. In the **Actions and Recipients** step, select **Integration: Microsoft Teams** from the **Actions** drop-down list.

5. From the **Recipient** drop-down list, select the name of the integration you created (for example, *console-teams*) and click **Next**.

6. In the **Associate event types** step, select one or more events for which you want to send notifications (for example, **Policies: Policy triggered**) and then click **Next**.

7. Review your behavior group settings and click **Finish**. The new behavior group appears on the **Notifications** page.

### Verification

1. Create an event that will trigger a Hybrid Cloud Console notification. For example, run `insights-client` on a system that will trigger a policy event.

2. Wait a few minutes, and then navigate to Microsoft Teams.

3. Select the channel you configured from the left menu. If the setup process succeeded, the page displays a notification from Insights. The notification contains the name of the host that triggered the event and a link to that host, as well as the number of events and a link that opens the corresponding Hybrid Cloud Console service.

4. In the Hybrid Cloud Console, go to **Settings > Notifications**.

5. Click the **View Event Log** button. The event shows the label **Integration:Microsoft Teams**.
   - If the label is green, the notification succeeded.
   - If the label is red, the integration might need to be adjusted.
     - If the integration is not working as expected, verify that the incoming webhook connector was properly created in Microsoft Teams, and that the correct incoming webhook URL is added in the Hybrid Cloud Console integration configuration.

### NOTE

See **Troubleshoot notification failures with the event log and integration settings** in the notifications documentation for more details.

### Additional resources

- For more information about behavior groups, see **Configure notification behavior groups**.
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.