Red Hat Hybrid Cloud Console 1-latest

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

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

Red Hat Hybrid Cloud Console 1-latest Integrating the Red Hat Hybrid Cloud Console with third-party applications

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

Legal Notice

Abstract

You can configure Red Hat Hybrid Cloud Console 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

PREFACE

You can integrate the Red Hat Hybrid Cloud Console with Splunk, ServiceNow, Slack, Event-Driven Ansible, Microsoft Teams, and Google Chat to route event-triggered notifications to those third-party applications. Integrating third-party applications expands the scope of notifications beyond emails and messages, so that you can view and manage Hybrid Cloud Console events from your preferred platform dashboard.

To learn more about notifications, see *Configuring notifications on the Red Hat Hybrid Cloud Console* .

Prerequisites

- You have Organization Administrator or Notifications administrator permissions for the Hybrid Cloud Console.

- You have the required configuration permissions for each third-party application that you want to integrate with the Hybrid Cloud Console.

CHAPTER 1. INSTALLING AND CONFIGURING THE RED HAT INSIGHTS APPLICATION FOR SPLUNK

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

Contacting support

If you have any issues with the Red Hat Insights application for Splunk, 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**.

Splunk will not provide troubleshooting. The Red Hat Insights application for Splunk is fully supported by Red Hat.

Prerequisites

- You have Splunk login credentials:

    - On Splunk Cloud Platform, you must have the Splunk Cloud Administrator **sc-admin** role.

    - On Splunk Enterprise, you must have the **admin** role. For more information about creating the **admin** role, see Create secure administration credentials in the Splunk documentation.

- You have Organization Administrator permissions for the Hybrid Cloud Console.

1.1. INSTALLING THE RED HAT INSIGHTS APPLICATION FOR SPLUNK

Install and configure the Red Hat Insights application for Splunk to integrate Splunk with the Hybrid Cloud Console so that Splunk can receive event notifications from the Hybrid Cloud Console. The setup automation performs the following tasks:

- Creates a user group with the 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 Hybrid Cloud Console 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 Hybrid Cloud Console services. This forwards the events from all services to Splunk. Currently, the behavior group forwards events from the Advisor, Policies, Drift, Compliance, Malware Detection, Patch, and Vulnerability services.

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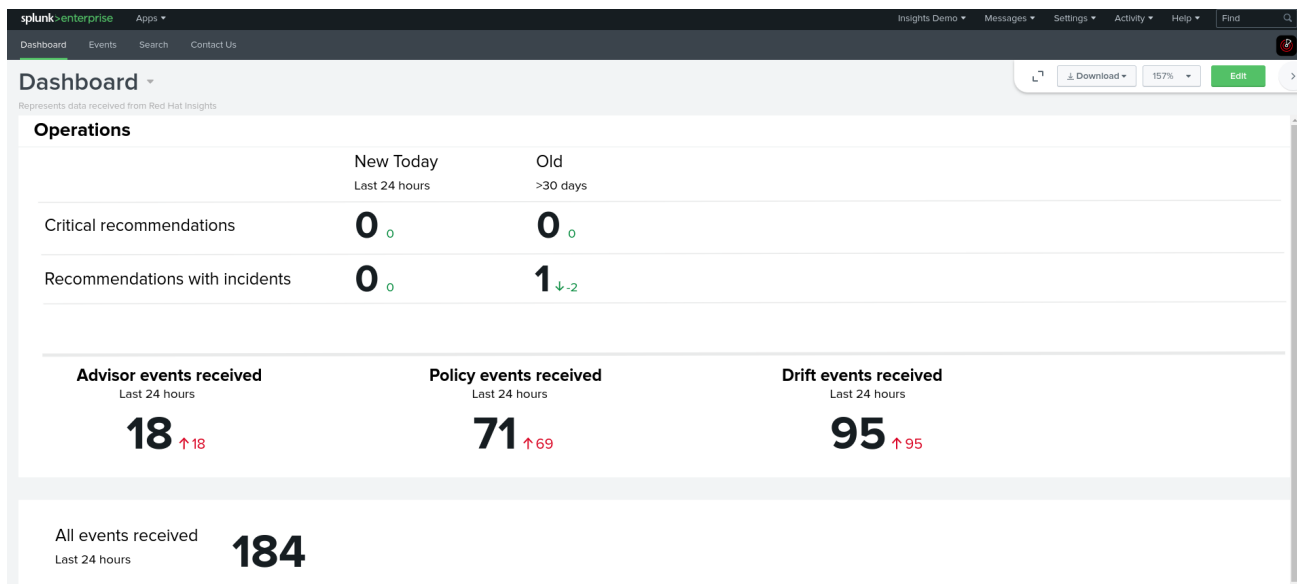
Prerequisites

- You have Organization Administrator permissions for the Hybrid Cloud Console.

- You have Splunk login credentials:

  - To install applications on Splunk Cloud Platform, you must have the Splunk Cloud Administrator **sc-admin** role.

  - To install applications on Splunk Enterprise, you must have the **admin** role. 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. Install the Red Hat Insights Application for Splunk:

   a. Log in to Splunk.

   b. On the home page, search for **Red Hat Insights** in the filter box and select it.

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

   d. On the home page, click the Settings menu (gear icon). The **Apps** page opens.

   e. Enter **Red Hat Insights** in the **filter** box and then click the magnifying glass. The application appears in the search results.

   f. On the home page, click **Find more apps** under the **Apps** heading on the left of the screen. The **Browse More Apps** page opens.

   g. Enter **Red Hat Insights** in the filter box and then press the Enter key. **Red Hat Insights** appears in the search results.

   h. Select **Red Hat Insights**.

      i. Click **Install**.

      j. Confirm or enter your Splunk username and password and then click **Agree and Install**. When the installation process completes, the **Complete** dialog box opens.

2. Set up the Red Hat Insights Application for Splunk:

    a. In the **Complete** dialog box, click **Open the App**. The **App configuration** page opens.

    b. Click **Continue to app setup page** The **Set up integration with Red Hat Insights** page opens. The page includes the HTTP Event Collector (HEC) name and default index fields.
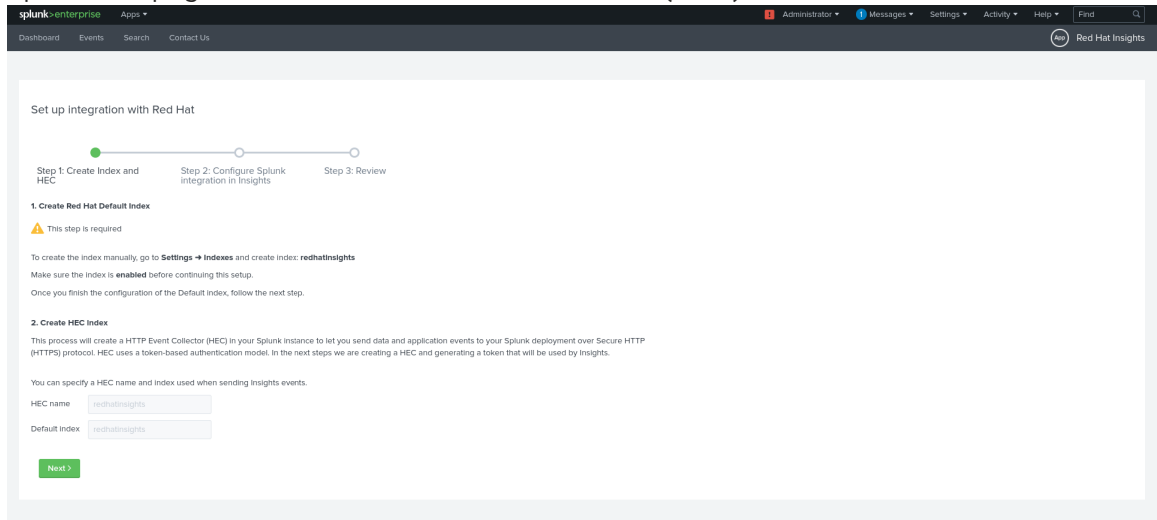
    c. Under **Create Red Hat Default Index**, click **Settings > Index**. The **Indexes** page opens in a new tab.

    d. On the **Indexes** page, click **New Index**.

    e. Type a name for the index in the **Name** field (for example, **redhatinsights**).

    f. Enter values in the **Max raw data size** and **Searchable retention (days)** field.

    g. Click **Save**. The index you created appears in the **Indexes** list. It is enabled by default.

    h. On the first Splunk screen, on the **Set up integration with Red Hat** page, type the name for the HEC in the HEC name field (for example, **redhatinsights**).

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

    j. Click **Next**.

    k. Click **Review** and then click **Submit**. The HEC name that you created appears in the **HEC Name** field.

    l. Click **Next** to create the HEC URL and HEC Token.
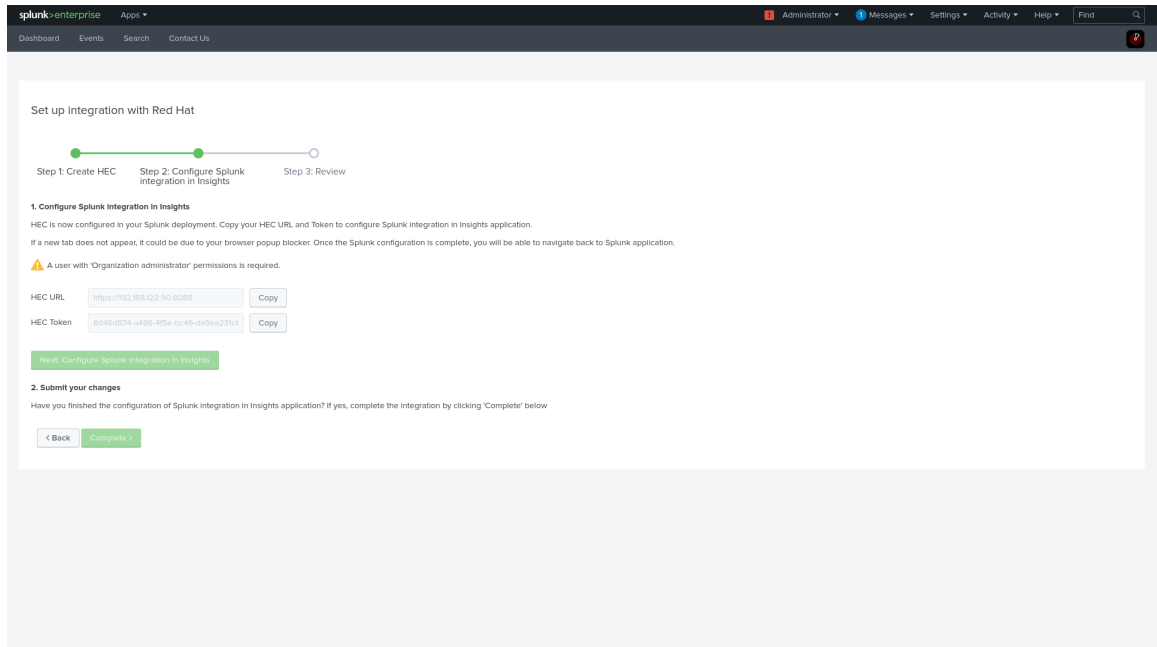
3. Configure Splunk integration in Insights:

   a. Click **Copy** to copy the HEC URL value in Splunk Enterprise.

   b. Click **Next: Configure Splunk integration in Insights** The Hybrid Cloud Console opens in a new browser tab.

      > **NOTE**
      >
      > This button is disabled until you click the **Copy** button for either the HEC URL or HEC token.

   c. In the Hybrid Cloud Console, navigate to **Settings** > **Integrations**.

   a. Paste the HEC URL value into the **Splunk HEC URL** field.

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

   b. 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.
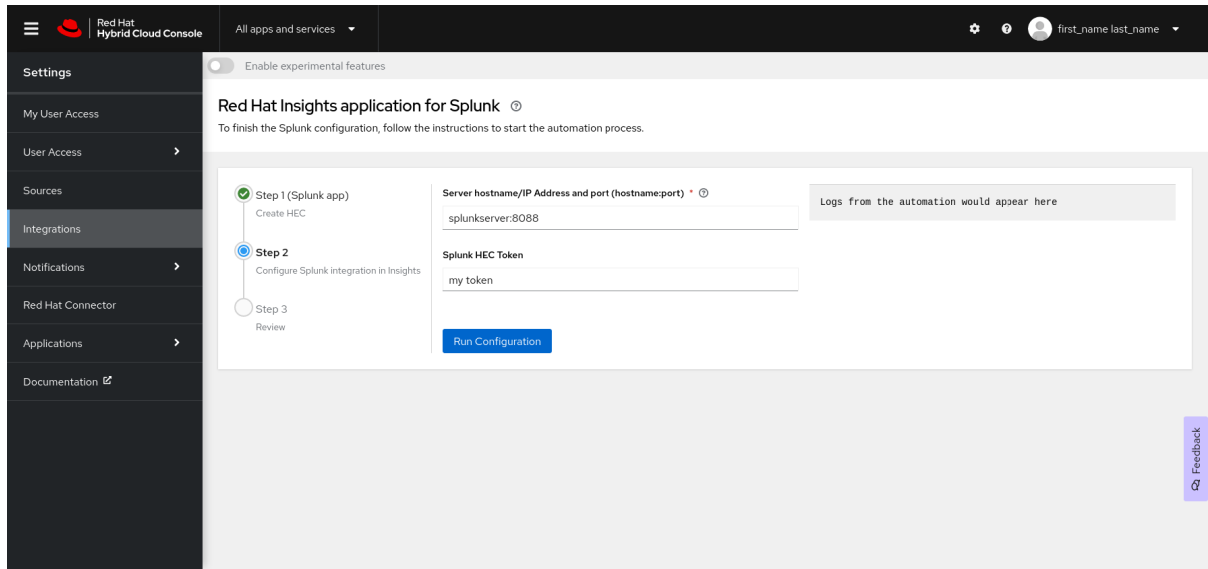
c. Optional: If you are using Splunk Cloud, edit the HEC URL that you pasted into the **Splunk HEC URL** field on the **Integrations** page to match the Splunk Cloud format:

- Use the following format for Splunk Cloud Platform on all clouds except Google Cloud Platform (GCP):

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

- Use the following format for Splunk Cloud Platform on Google Cloud Platform (GCP):

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

  Replace the following placeholders:

- **protocol**: Either **http** or **https**.

- **host**: The 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 that you want to use. In many cases, you use the /**services**/**collector**/**event** endpoint for JSON-formatted events, or the **services**/**collector**/**raw** endpoint for raw events.
  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:

  https://http-inputs-otherhost.splunkcloud.com:443/services/collector/raw

  1. Complete the setup process:

d. Copy the **HEC Token** value in Splunk and paste it into the **Splunk HEC Token** field in on the Hybrid Cloud Console **Integrations** page.

e. In the Hybrid Cloud Console, click **Run configuration**. The Hybrid Cloud Console sets up the integration, creates the behavior group, and associates Hybrid Cloud Console events to the behavior group. The status message section on the right side of the page shows the status of each of these actions.
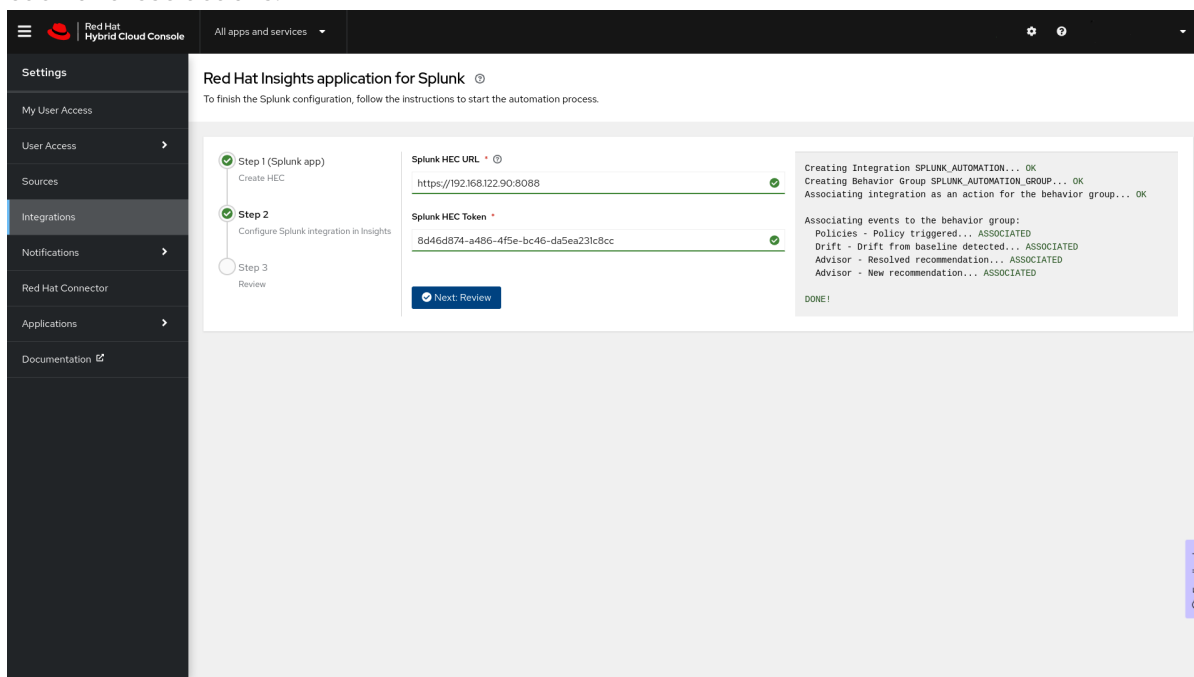
f. When the setup completes successfully, click **Next: Review**. The application returns the message **Splunk integration in Insights completed**.
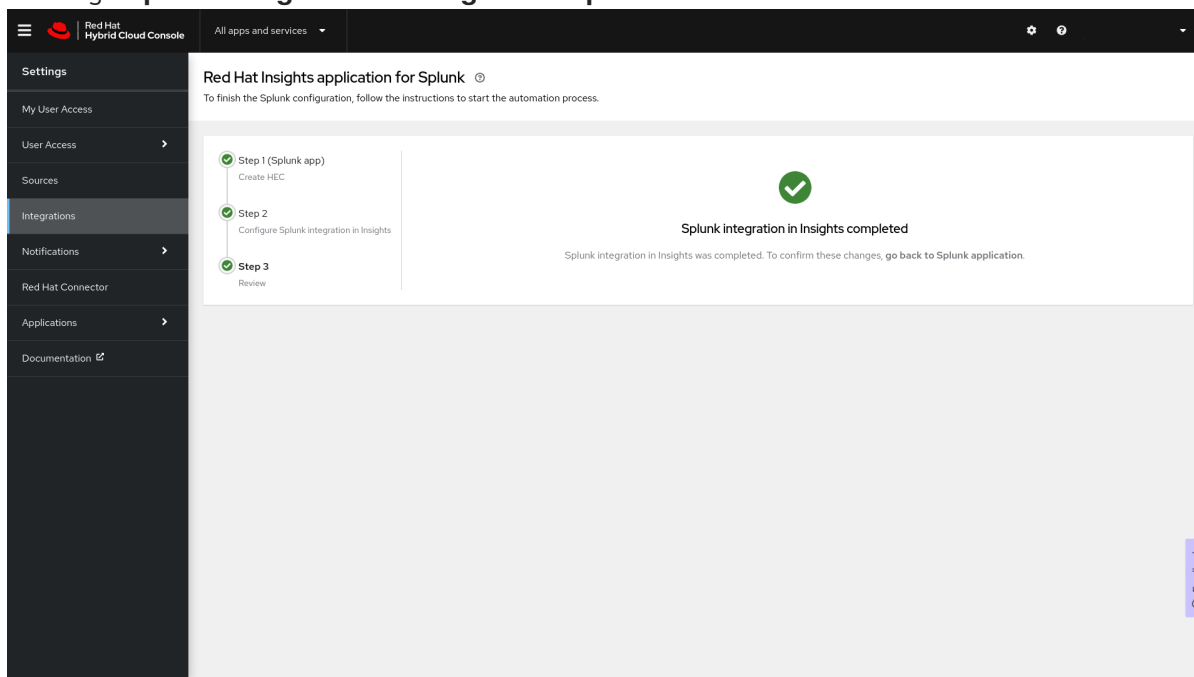
g. Click **Go back to the Splunk application** This redirects you to the Set up integration with Red Hat screen in Splunk.

h. Click **Finish set up** to complete the setup in Splunk.
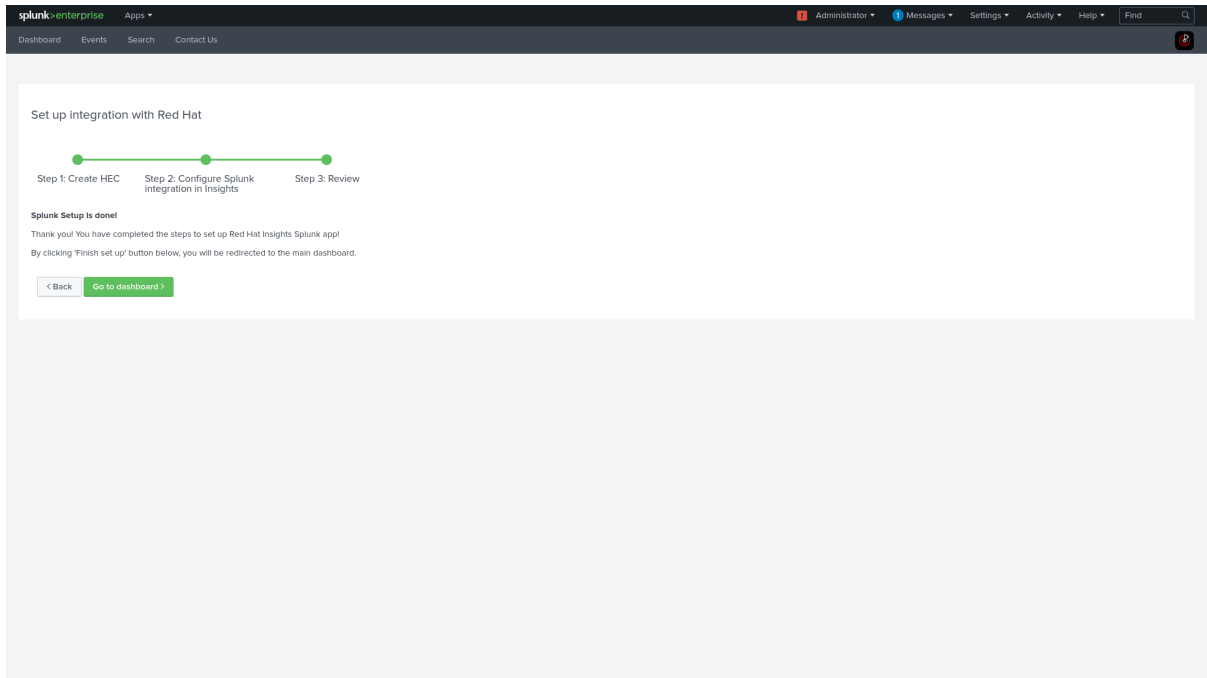
i. Click **Go to dashboard** to be redirected to your Splunk dashboard.
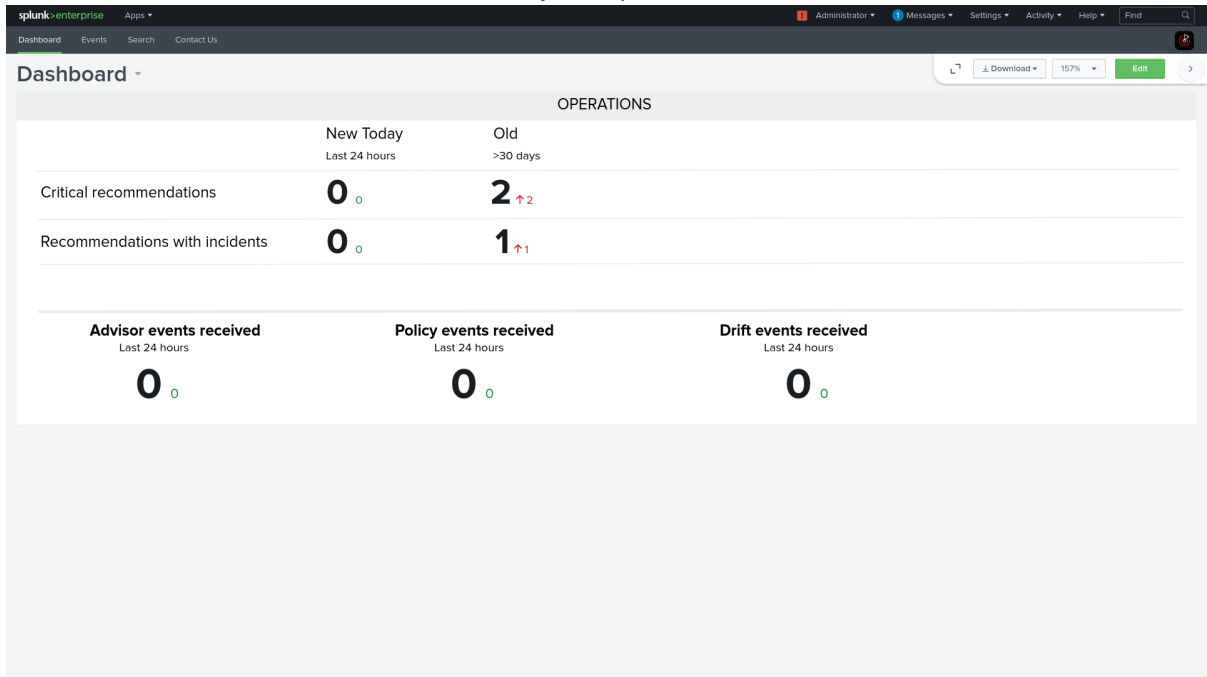
NOTE

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

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

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 Hybrid Cloud Console account

1.2. ENABLING THE HEC TOKEN

Before Splunk can receive Hybrid Cloud Console events, you must enable the HEC token.

Prerequisites

- You have Organization Administrator permissions for the Hybrid Cloud Console.

- You have Splunk login credentials:

  - On Splunk Cloud Platform, you must have the Splunk Cloud Administrator **sc-admin** role.

  - On Splunk Enterprise, you must have the **admin** role. For more information about creating the **admin** role, see Create secure administration credentials in the Splunk documentation.

Procedure

1. From the Splunk home 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.
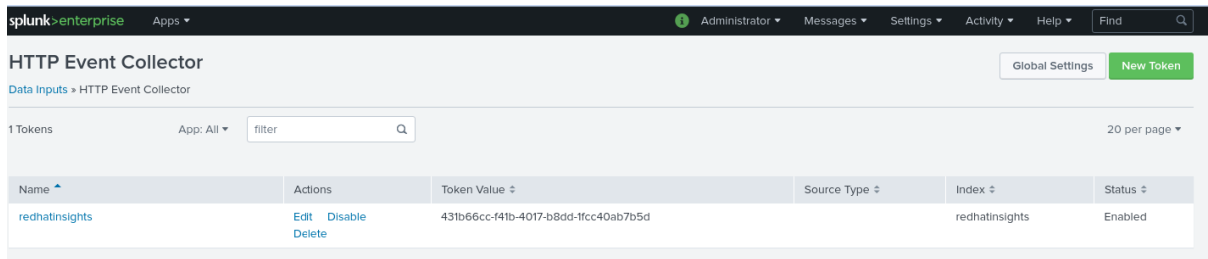
3. Click **Global Settings** in the upper right corner of the page. The Edit Global Settings dialog box displays.

4. Select **Enabled**. This enables the HEC token that was automatically created during the setup process.
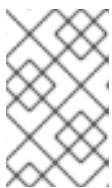
> **NOTE**
>
> The HEC token uses a default HTTP port number of 8088. If you are using a different port (such as port 443 for Splunk Cloud), you must update your Hybrid Cloud Console Splunk Integration to match.

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.

1.3. MANUALLY CONFIGURING A NOTIFICATIONS ADMINISTRATOR GROUP IN YOUR HYBRID CLOUD CONSOLE ACCOUNT

The Red Hat Insights application for Splunk automated installation and setup process automatically configures a Notifications administrator role and group in your Hybrid Cloud Console account. However, you can create the Notifications administrator manually.

Prerequisites

- You are logged in to the Hybrid Cloud Console with the Organization Administrator role.

Procedure

1. Click **Settings** > **Identity & Access Management**

2. Under **Identity & Access Management**, expand **User Access** if necessary, and select **Groups**.

3. Click **Create group**. The **Name and description** page appears.

4. Enter a name for the group (for example, **splunknotifgroup**), enter a description, and click **Next**. The **Add roles** page opens.

5. To add the Notifications administrator role, enter **notif** in the search box.

6. Select **Notifications administrator** from the search results list, and click **Next**. The **Add Members** page opens.

7. Select the users to add to this group. You can use the search box to search for specific names.

8. Click **Next**. The **Review Details** page opens.

9. Review the information, and click **Submit** to create the group.

10. Click **Exit**. The **Groups** page opens.

Verification

1. Enter the new group name in the search box.

2. Click the group name. The page for the group opens.

3. On the **Roles** tab, verify that the group has the **Notifications administrator** role.

4. Click the **Members** tab and verify that the group includes the correct members.

1.4. MANUALLY CONFIGURING A SPLUNK INTEGRATION

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

Prerequisites

- You have an HTTP Event Collector (HEC) URL from Splunk Cloud or Splunk Enterprise.

- You have the HEC token value from Splunk Cloud or Splunk Enterprise.

- You are logged in to the Hybrid Cloud Console with the Notifications administrator role.

Procedure

1. In the Hybrid Cloud Console, navigate to **Settings** > **Integrations**.

2. Select the **Reporting & Automation** tab.

3. Click **Add integration**.

4. Select **Splunk** as the integration type, and click **Next**.

5. Enter a name for your new integration in the **Integration name** field (for example, **redhat_splunk**).

6. 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 .

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

   The following 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**

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

8. Click **Next**.

9. Review the integration details and click **Submit**.

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.

1.5. TROUBLESHOOTING THE SPLUNK INTEGRATION WITH THE HYBRID CLOUD CONSOLE

Review the following issues if your Hybrid Cloud Console console integration with Splunk is not working as expected:

Splunk does not receive event notifications from the Hybrid Cloud Console

Configuration errors in the Splunk environment can result in Splunk not receiving event notifications from the Hybrid Cloud Console.

- In Splunk, make sure that the HTTP Event Collector (HEC) is enabled under **Global Settings**. See Section 1.2, "Enabling the HEC token".

- Make sure that the default index is **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 might need. For more information, refer to Splunk Phantom ports and endpoints.

For more information about configuring Splunk HEC ports, see Splunk Phantom ports and endpoints.

Cannot click links in the Events table in Splunk when using real-time search

In Splunk, 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.

1.6. ADDITIONAL RESOURCES

- For more information about Splunk, see the Splunk website.

- For more information about Splunkbase, see the Splunkbase website.

CHAPTER 2. INTEGRATING SERVICENOW WITH THE RED HAT HYBRID CLOUD CONSOLE

The ServiceNow 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 Hybrid Cloud Console events to ServiceNow. The Flow Templates for Red Hat Insights application seamlessly integrates with the Hybrid Cloud Console so that you can focus on handling the data on the ServiceNow application side in the same way you manage other sources of data.

You can use the Flow Templates for Red Hat Insights application to handle events from the following Hybrid Cloud Console services:

- Advisor

- Vulnerability

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

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

Contacting support

If you have any issues with the Red Hat Insights application for ServiceNow, 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**.

ServiceNow will not provide troubleshooting. The Red Hat Insights application for ServiceNow is fully supported by Red Hat.

2.1. INSTALLING AND CONFIGURING THE SERVICENOW FLOW TEMPLATES FOR RED HAT INSIGHTS APPLICATION

You can use the Flow Templates for Red Hat Insights application to integrate ServiceNow with the Hybrid Cloud Console to create ServiceNow flows from triggered events in the Hybrid Cloud Console. To integrate ServiceNow with Red Hat Hybrid Cloud Console, you must install the ServiceNow IntegrationHub Enterprise Pack Installer plugin. After the plugin and the application are configured, event data flows from the Hybrid Cloud Console to your ServiceNow instance. A ServiceNow REST API asynchronous trigger receiver is used within the application flow.

Prerequisites

- You have Organization Administrator permissions for the Hybrid Cloud Console.

- Notifications administrator permissions are configured in User Access.

- You have a Red Hat subscription and 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.

- You have access to the following ServiceNow roles:

  - **admin**

  - **x_rhtpp_rh_webhook.rest**

  - **sn_appclient.app_client_company_installer** (can only install applications that match the instance company), or **sn_appclient.app_client_user**.

- In ServiceNow you have 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 and install or update the Flow Templates:

   - Install the Flow Templates for Red Hat Insights application from the ServiceNow Store (or as an Update Set).

     a. Create a new user with User ID **rh_insights_integration**.

     b. Check **Internal Integration User** for the user you just created.

     c. Ensure that the user is Active.

     d. Assign role **x_rhtpp_rh_webhook.rest** to the user.

     e. Generate a password for the user. Copy this information for use during the setup process.

3. Open the Hybrid Cloud Console in a new browser window or tab.

4. Navigate to **Settings** > **Integrations**, select the **Reporting & Automation** tab, and complete the following steps:

   a. Click **Add integration**.

   b. Select **ServiceNow** as the integration type, and click **Next**.

   c. Enter a name for the integration, such as *ServiceNow integration*.

   d. Provide the **Endpoint URL** and replace **<instance.servicenow.com>** with your ServiceNow instance:
      https://<instance.servicenow.com>/api/x_rhtpp_rh_webhook/flow_templates_for_red_hat_insights

   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.

   g. Click **Next**.

h. Review the integration details and click **Submit**.

5. Navigate to Hybrid Cloud Console > Settings > Notifications and complete the following steps:

   a. Under **Notifications**, select **Configure Events**.

   b. Select the application bundle tab you want to configure event notification behavior for: **Red Hat Enterprise Linux**, **Console**, or **OpenShift**.

   c. Click the **Behavior Groups** tab.

   d. Click **Create new group** to open the **Create behavior group** wizard.

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

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

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

6. Click **Next**. The **Associate event types** window opens.

7. 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

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

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

- For information about designing ServiceNow flows, see the ServiceNow Flow Designer.

- To download ServiceNow applications, see the ServiceNow Store.

- For information about installing an application that you purchased from the ServiceNow Store to make it available on your instance, see Install a ServiceNow Store Application .

- For information about configuring notifications after you have integrated ServiceNow with the Hybrid Cloud Console, see *Configuring notifications on the Red Hat Hybrid Cloud Console* .

2.2. TROUBLESHOOTING INTEGRATION WITH SERVICENOW

If ServiceNow is not receiving events from the Red Hat Hybrid Cloud Console, verify the configuration:

- 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 **https://<instance.servicenow.com>/api/x_rhtpp_rh_webhook/flow_templates_for_red_hat _insights**.

- Ensure that the **x_rhtpp_rh_webhook.rest** user role is defined in ServiceNow. Otherwise, notifications from the Hybrid Cloud Console 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

- For more troubleshooting information, see Troubleshooting notification failures with the event log and integration settings.

2.3. ADDITIONAL RESOURCES

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

- For more information about ServiceNow, see ServiceNow.

CHAPTER 3. INTEGRATING SLACK WITH THE HYBRID CLOUD CONSOLE

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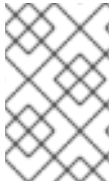
> **NOTE**
>
> The Slack integration in this example is configured for Red Hat Enterprise Linux. The integration also works with other Red Hat OpenShift, Application Services, and Red Hat Hybrid Cloud Console events.

The Slack integration uses incoming webhooks to receive event data. For more information about webhooks, see Sending messages using Incoming Webhooks in the Slack API documentation.

Contacting support

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

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

3.1. CONFIGURING SLACK FOR INTEGRATION WITH INCOMING WEBHOOKS

To prepare Slack for integration with the Hybrid Cloud Console, you must configure incoming webhooks in Slack.
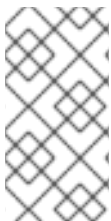
> **NOTE**
>
> The preferred method to integrate Slack with third-party products is to build your own custom workflow as shown in the Slack help center. However, you cannot use custom workflows to integrate Slack with the Hybrid Cloud Console. This is because custom workflows in Slack do not yet support nested JSON structures as workflow variables.

Prerequisites

- You have owner or admin permissions to the Slack instance where you want to add incoming webhooks.

- You have App Manager permissions to add Slack apps to a channel.

- You have a Slack channel or user to receive 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 window. The configuration window opens.

3. Select **Integrations** and then click **Add Apps**. The **Add apps to <channel name>** window opens, where **<channel name>** is the name of the channel.

4. Search for **Incoming Webhooks**, and then select it from the search results.

5. Click **Add to Slack** to add the Hybrid Cloud Console integration to the channel. The **Post to Channel** box opens.

6. Perform one of the following tasks:

   a. To select an existing channel, click the **Choose a Channel** drop-down menu or type the user or channel name in the field.

   b. To create a new channel, click or create a new channel, type the name of the new channel and an optional description, and click **Create**.

   > **NOTE**
   >
   > If you do not enter a channel name in the **Name** field, 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 opens in the Slack app directory.

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 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

- For more information about incoming webhooks for Slack, see the Slack Help Center.

- For information about workflows, see Create more advanced workflows using webhooks .

- For information about managing app approvals, see Managing app approvals in Enterprise Grid workspaces.

- For information about admin apps in Slack, see Managing app approvals in Enterprise Grid workspaces.

- For general help with Slack, see the Slack Help Center.

3.2. CONFIGURING SLACK INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE

If you have configured a Slack channel for incoming webhooks, you can configure the Hybrid Cloud Console to send event notifications to that Slack channel.

Prerequisites

- You have Organization Administrator or Notifications administrator permissions for the Red Hat Hybrid Cloud Console.

- You have the name of a Slack channel that you configured to receive incoming webhooks. See Section 3.1, "Configuring Slack for integration with incoming webhooks" for information about configuring a Slack channel for integration.

- You copied the Slack webhook URL for the Slack channel that you configured for incoming webhooks. See Section 3.1, "Configuring Slack for integration with incoming webhooks" for information about the Slack webhook URL.

Procedure

1. In the Hybrid Cloud Console, navigate to **Settings** > **Integrations**.

2. Select the **Communications** tab.

3. Click **Add integration**.

4. Select **Slack** as the integration type, and click **Next**.

5. Enter a name for the integration (for example, **SLACK_INTEGRATION**).

6. Paste the Slack webhook URL that you copied from the Webhook URL field in Slack into the **Workspace URL** field.

7. Add the name of the Slack channel that you configured during Slack setup to the **Channel** field.

8. Click **Next**.

9. Review the integration details and click **Submit** to enable the integration.

10. Navigate to **Notifications** > **Configure Events**.

11. Select the application bundle tab you want to configure event notification behavior for: **Red Hat Enterprise Linux**, **Console**, or **OpenShift**.

12. Click the **Behavior Groups** tab 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 .

13. Click **Edit Behavior Group**.

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

15. The list of configured Slack integrations shows in the **Recipient** drop-down list. Select the integration name that you previously created.

16. Click **Next**. The **Associate event types** window opens.

17. Select the event types for which you want notifications, and click **Next**. The Review window opens.

18. Review the settings for the behavior group, and click **Finish**.

> **NOTE**
>
> You can create and edit multiple behavior groups to include any additional platforms that the notifications service supports.

19. Select **Settings > Integrations**, and click the **Communications** tab. 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**.

Verification

1. Navigate to **Settings** > **Notifications** > **Event Log**. **Integration: Slack** is listed in the **Actions** column for the event. If the notification was successful, the integration label is green.

2. Hover over the integration to verify that an event was sent.

Additional resources

- For more information about behavior groups, see Configuring Hybrid Cloud Console notification behavior groups.

CHAPTER 4. INTEGRATING EVENT-DRIVEN ANSIBLE WITH THE RED HAT HYBRID CLOUD CONSOLE

You can use Event-Driven Ansible to take advantage of Hybrid Cloud Console capabilities such as Red Hat Insights to continuously analyze your inventory for potential issues and recommendations. Event-Driven Ansible connects sources of events with corresponding actions through rules.

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

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**.

4.1. CONFIGURING EVENT-DRIVEN ANSIBLE FOR INTEGRATION WITH THE RED HAT HYBRID CLOUD CONSOLE

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

Prerequisites

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

- You have Organization Administrator or Notifications administrator permissions for the Hybrid Cloud Console.

Procedure

1. Connect your environment to the Red Hat Ansible Automation Hub:

   a. In the Hybrid Cloud Console, navigate to Ansible Automation Platform > Connect to Hub .

   b. Under **Offline token**, copy the string under **The token will expire after 30 days of inactivity. Run the command below periodically to prevent your token from expiring**.

   c. In a terminal window, paste the string that you copied in the previous step.

2. Enter the following command to install the Red Hat Insights collection for Event-Driven Ansible:

   ```
   $ ansible-galaxy collection install redhat.insights_eda
   ```

3. To install the Red Hat Insights requirements, enter the following command as the **root** user:

   ```
   # pip3 install -r ~/.ansible/collections/ansible_collections/redhat/insights_eda/requirements.txt
   ```

4. Enter the following command and verify that **redhat.insights_eda** is included in the output:

   ```
   $ ansible-galaxy collection list
   ```

   Sample output for this command:

```
# /home/username/.ansible/collections/ansible_collections
Collection          Version
----------------- -------
ansible.eda         1.3.8
community.general   7.0.1
redhat.insights_eda 1.0.0
```

5. Use a text editor to create a YAML file that contains a simple Ansible rulebook that uses the Red Hat Insights collection. For example, create a file called **simple-rulebook.yaml** with the following content:

```
---
- name: Listen for events from Red Hat Insights
  hosts: all
  sources:
    - redhat.insights_eda.insights:
  rules:
    - name: Handle Red Hat Insights payload
      condition: event.payload is defined
      action:
        debug:
          msg: "Received: {{ event.payload }}"
```

This simple playbook uses the **redhat.insights_eda.insights** collection as the source. If an event with **payload** is defined, the contents of **event.payload** are displayed as output.

The rulebook exposes an endpoint that is used to receive events and communicate with the Hybrid Cloud Console. See the Event-Driven Ansible for Red Hat Insights documentation in Ansible Automation Hub for more advanced examples for the Red Hat Insights Advisor, Compliance, and Vulnerability services.

6. Create a YAML file that contains an associated playbook. For example, create a file called **inventory.yaml** that contains a simple inventory:

```
all:
```

7. Run the **ansible-rulebook** command to start your Event-Driven Ansible listener to listen for new events. In the following example, this command exposes your **localhost** on the default port 5000:

```
$ ansible-rulebook --verbose --rulebook simple-rulebook.yml -i inventory.yml
```

8. Run the **curl** command in a separate terminal window to verify that your Event-Driven Ansible listener is configured correctly, for example:

```
$ curl -H 'Content-Type: application/json' -d "{\"payload\": \"Test incoming event\"}" localhost:5000/endpoint
```

In this example, if the configuration is correct, a new message appears in the EDA listener window with the content of the event:

```
Received: {'payload': 'Test incoming event'}
```

9. In the Hybrid Cloud Console, navigate to **Settings** > **Integrations**.

10. Select the **Reporting & Automation** tab.

11. Click **Add integration**.

12. Select **Event-Driven Ansible** as the integration type, and then click **Next**.

13. In the **Integration name** field, enter a name for your integration (for example, *My EDA Integration*).

14. Enter the URL that you configured in your Ansible rulebook into the **Endpoint URL** field. This is the endpoint that points to the Event-Driven Ansible listener.

> **NOTE**
>
> The **Endpoint URL** must include **http://** or **https://**, for example **https://<eda_hostname>:5000/endpoint**.
>
> If necessary, ask the security administrator for your organization to configure access to the Red Hat Hybrid Cloud Console.

15. Optional: Enter 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.

16. Click **Next**.

17. Review the integration details, and then click **Submit** to enable the integration.

Your Event-Driven Ansible integration is now listed on the **Integrations** > **Reporting & Automation** page. Under **Last connection attempt**, the status is **Ready** to show the connection can accept notifications from the console.

Verification

Create a test notification to confirm you have correctly connected Event-Driven Ansible to the Hybrid Cloud Console:

1. Next to your Event-Driven Ansible integration on the **Integrations** > **Reporting & Automation** page, click the options icon (⋮) and click **Test**.

2. In the **Integration Test** screen, enter a message and click **Send**. If you leave the field empty, the Hybrid Cloud Console sends a default message.

3. In the Event-Driven Ansible listener terminal, check for the message sent from the Hybrid Cloud Console.

4. In the Hybrid Cloud Console, go to **Notifications** > **Event Log** and check that the **Integration: Event-Driven Ansible** event is listed with a green label.

Additional resources

- For more information about setting up Notifications administrator permissions, see Configure User Access to manage notifications in **Configuring notifications on the Red Hat Hybrid Cloud Console**.

- For more Event-Driven Ansible configuration information and examples of Red Hat Insights rulebooks, see the **Documentation** tab in the **insights_eda** collection available from the Ansible Automation Hub Collections page.

4.2. 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 with the Hybrid Cloud Console is configured. See Section 4.1, "Configuring Event-Driven Ansible for integration with the Red Hat Hybrid Cloud Console" for information about configuring Event-Driven Ansible integration.

Procedure

1. In the Hybrid Cloud Console, navigate to Settings > Notifications.

2. Under **Notifications**, select **Configure Events**.

3. Select the application bundle tab you want to configure event notification behavior for: **Red Hat Enterprise Linux**, **Console**, or **OpenShift**.

4. Click the **Behavior Groups** tab.

5. Click **Create new group** to open the **Create behavior group** wizard.

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

7. In the **Actions and Recipients** step, select **Integration: Event-Driven Ansible** from the **Actions** drop-down list.

8. From the **Recipient** drop-down list, select the name of the integration you created (for example, *My EDA Listener*) and click **Next**.

9. In the **Associate event types** step, select one or more events for which you want to send notifications (for example, **Advisor: New recommendation**), and click **Next**.

10. 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. See the Ansible Automation Hub page for an example.

2. To test that the Hybrid Cloud Console integration was successful, in the Hybrid Cloud Console, go to **Settings** > **Notifications** > **Event Log** and check for an event that shows the label **Integration: Event-Driven Ansible**.

Event	Application	Actions ⑦	Date ... ↓
Detected Malware	Malware - Red Hat Enterprise Linux	✅ Integration: Event-Driven Ansible ✅ Integration: ServiceNow ✅ Integration: Splunk ✅ Email ✅ Integration: Webhook Show Less	3 minutes ago

- If the label is green, the notification succeeded.

- If the label is red, verify that the webhook has been properly created and exposed in Event-Driven Ansible, and that the correct webhook URL is configured in the Hybrid Cloud Console integration configuration.

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

4.3. ADDITIONAL RESOURCES

- For more information about Event-Driven Ansible, see the Getting Started with Event-Driven Ansible Guide.

- For information about how to configure and use the Event-Driven Ansible controller, see Event-Driven Ansible controller user guide.

- For more information about behavior groups, see Configuring Hybrid Cloud Console notification behavior groups.

- For configuration examples, see Red Hat Insights Collection for Event-Driven Ansible and Using Red Hat Insights as a source of events for Event-Driven Ansible automation in the Red Hat Ansible blog.

CHAPTER 5. INTEGRATING MICROSOFT TEAMS WITH THE HYBRID CLOUD CONSOLE

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.

Contacting support

If you have any issues with integrating the Hybrid Cloud Console with Microsoft Teams, 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**.

Microsoft will not provide troubleshooting. The Hybrid Cloud Console integration with Microsoft Teams is fully supported by Red Hat.

5.1. CONFIGURING MICROSOFT TEAMS FOR INTEGRATION WITH THE HYBRID CLOUD CONSOLE

You can use incoming webhooks to configure Microsoft Teams to receive event notifications from the Red Hat Hybrid Cloud Console or a third-party application.

Prerequisites

- You have admin permissions for Microsoft Teams.

- You have Organization Administrator or Notification administrator permissions for the Hybrid Cloud Console.

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.

10. In the Hybrid Cloud Console, navigate to **Settings** > **Integrations**.

11. Click the **Communications** tab.

12. Click **Add integration**.

13. Select **Microsoft Office Teams** as the integration type, and click **Next**.

14. In the **Integration name** field, enter a name for your integration (for example, *console-teams*).

15. Paste the incoming webhook URL that you copied from Microsoft Teams into the **Endpoint URL** field.

16. Click **Next**.

17. Review the integration details and click **Submit** to enable the integration.

Your Microsoft Teams integration is now listed on the **Integrations** > **Communications** page. Under **Last connection attempt**, the status is **Ready** to show the connection can accept notifications from the console.

Verification

Create a test notification to confirm you have correctly connected Microsoft Teams to the Hybrid Cloud Console:

1. Next to your Microsoft Teams integration on the **Integrations** > **Communications** page, click the options icon (⋮) and click **Test**.

2. In the **Integration Test** screen, enter a message and click **Send**. If you leave the field empty, the Hybrid Cloud Console sends a default message.

3. Open your Microsoft Teams channel and check for the message sent from the Hybrid Cloud Console.

4. In the Hybrid Cloud Console, go to **Notifications** > **Event Log** and check that the **Integration: Microsoft Teams** event is listed with a green label.

Additional resources

- For more information about setting up Notifications administrator permissions, see Configure User Access to manage notifications in the notifications documentation.

5.2. 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. For more information about behavior groups, see Configuring Hybrid Cloud Console notification behavior groups .

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. For information about configuring Microsoft Teams integration, see Section 5.1, "Configuring Microsoft Teams for integration with the Hybrid Cloud Console".

Procedure

1. In the Hybrid Cloud Console, navigate to Settings > Notifications.

2. Under **Notifications**, select **Configure Events**.

3. Select the application bundle tab you want to configure event notification behavior for: **Red Hat Enterprise Linux**, **Console**, or **OpenShift**.

4. Click the **Behavior Groups** tab.

5. Click **Create new group** to open the **Create behavior group** wizard.

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

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

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

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

10. 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 that you configured from the left menu. If the setup process succeeded, the page displays a notification from the Hybrid Cloud Console. 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** > **Event Log** and check for an event that shows the label **Integration: Microsoft Teams**.

   - If the label is green, the notification succeeded.

   - If the label is red, 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 Troubleshooting notification failures with the event log and integration settings in the notifications documentation for more details.

5.3. ADDITIONAL RESOURCES

- For more information about webhooks, see Create an Incoming Webhook and Webhooks and Connectors in the Microsoft Teams documentation.

CHAPTER 6. INTEGRATING GOOGLE CHAT WITH THE RED HAT HYBRID CLOUD CONSOLE

You can configure the Red Hat Hybrid Cloud Console to send event notifications to a new or existing Google space in Google Chat. The Google Chat integration supports events from all Hybrid Cloud Console services.

The integration with the Hybrid Cloud Console notifications service uses incoming webhooks to receive event data. Each Red Hat account configures how and who can receive these events, with the ability to perform actions depending on the event type.

Contacting Support

If you have any issues with the Hybrid Cloud Console integration with Google Chat, contact Red Hat for support. You can open a Red Hat support case directly from the Hybrid Cloud Console by clicking **Help** > **Open a support case**, or view more options from **Help** > **Support options**.

Google will not provide troubleshooting. The Hybrid Cloud Console integration with Google Chat is fully supported by Red Hat.

6.1. CONFIGURING INCOMING WEBHOOKS IN GOOGLE CHAT

In Google spaces, create a new webhook to connect with the Hybrid Cloud Console.

Prerequisites

- You have a new or existing Google space in Google Chat.

Procedure

1. In your Google space, click the arrow on the space name to open the dropdown menu:

   a. Select **Apps & Integrations**.

   b. Click **Webhooks**.

2. Enter the following information in the **Incoming webhooks** dialog:

   a. Enter a name for the integration (for example, *Engineering Google Chat*).

   b. Optional: To add an avatar for the notifications, enter a URL to an image.

   c. Click **Save** to generate the webhook URL.

   d. Copy the webhook URL to use for configuration in the Hybrid Cloud Console.

Additional resources

- See Send messages to Google Chat with incoming webhooks in the Google Chat documentation for more detailed information about Google Chat configuration.

6.2. CONFIGURING THE GOOGLE CHAT INTEGRATION IN THE RED HAT HYBRID CLOUD CONSOLE

Create a new integration in the Hybrid Cloud Console using the webhook URL from Google Chat.

Prerequisites

- You are logged in to the Hybrid Cloud Console as an Organization Administrator or as a user with Notifications administrator permissions.

- You have a Google Chat incoming webhook.

Procedure

1. In the Hybrid Cloud Console, navigate to **Settings** > **Integrations**.

2. Select the **Communications** tab.

3. Click **Add integration**.

4. Select **Google Chat** as the integration type, and click **Next**.

5. In the **Integration name** field, enter a name for your integration (for example, *console-gchat*).

6. Paste the incoming webhook URL that you copied from your Google space into the **Endpoint URL** field, and click **Next**.

7. Review the integration details and click **Submit** to enable the integration.

Your Google Chat integration is now listed on the **Integrations** > **Communications** page. Under **Last connection attempt**, the status is **Ready** to show the connection can accept notifications from the console.

Verification

Create a test notification to confirm you have successfully connected Google Chat to the Hybrid Cloud Console:

1. Next to your Google Chat integration on the **Integrations** > **Communications** page, click the options icon (⋮) and click **Test**.

2. In the **Integration Test** screen, enter a message and click **Send**. If you leave the field empty, the Hybrid Cloud Console sends a default message.

3. Open your Google space and check for the message sent from the Hybrid Cloud Console.

4. In the Hybrid Cloud Console, go to **Notifications** > **Event Log** and check that the **Integration: Google Chat** event is listed with a green label.

Additional resources

- For more information about setting up Notifications administrator permissions, see Configure User Access to manage notifications in the notifications documentation.

6.3. CREATING THE BEHAVIOR GROUP FOR THE GOOGLE CHAT INTEGRATION

A behavior group defines which notifications will be sent to external services such as Google Chat 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.

- You have configured the Google Chat integration.

Procedure

1. In the Hybrid Cloud Console, navigate to Settings > Notifications.

2. Under **Notifications**, select **Configure Events**.

3. Select the application bundle tab you want to configure event notification behavior for: **Red Hat Enterprise Linux**, **Console**, or **OpenShift**.

4. Click the **Behavior Groups** tab.

5. Click **Create new group** to open the **Create behavior group** wizard.

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

7. In the **Actions and Recipients** step, select **Integration: Google Chat** from the **Actions** drop-down list.

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

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

10. Review your behavior group settings, and click **Finish**. The new behavior group is listed 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 Google Chat.

3. In your Google Space, check for notifications from the Hybrid Cloud Console.

4. In the Hybrid Cloud Console, go to **Settings** > **Notifications** > **Event Log** and check for an event that shows the label **Integration: Google Chat**.

   - If the label is green, the notification succeeded.

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

5. If the integration is not working as expected, verify that the incoming webhook connector was properly created in Google Chat, and that the correct incoming webhook URL is added in the Hybrid Cloud Console integration configuration.
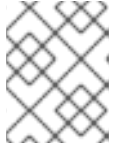
NOTE

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

6.4. ADDITIONAL RESOURCES

- See the Google Chat documentation about incoming webhooks for more detailed information about Google Chat configuration.

- For more information about behavior groups, see Configuring Hybrid Cloud Console notification behavior groups.

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Provide as much detail as possible so that your request can be addressed.

Prerequisites

- You have a Red Hat account.

- You are logged in to your Red Hat account.

Procedure

1. To provide your feedback, 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. If your Red Hat user name does not automatically appear in the **Reporter** text box, enter it.

5. Scroll to the bottom of the page and then click the **Create** button. A documentation issue is created and routed to the appropriate documentation team.

Thank you for taking the time to provide feedback.