



Red Hat Hybrid Cloud Console 1-latest

将 Red Hat Hybrid Cloud 控制台与第三方应用程序集成

配置第三方工具和 Red Hat Hybrid Cloud Console 之间的集成

Red Hat Hybrid Cloud Console 1-latest 将 Red Hat Hybrid Cloud 控制台与第三方应用程序集成

配置第三方工具和 Red Hat Hybrid Cloud Console 之间的集成

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

您可以配置 Red Hat Hybrid Cloud Console 通知，以与第三方应用程序集成。红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 信息。

目录

前言	3
第 1 章 为 SPLUNK 安装和配置 RED HAT INSIGHTS 应用程序	4
1.1. 为 SPLUNK 安装 RED HAT INSIGHTS 应用程序	4
1.2. 启用 HEC 令牌	11
1.3. 在 HYBRID CLOUD CONSOLE 帐户中手动配置管理员组	12
1.4. 手动配置 SPLUNK 集成	13
1.5. 其他资源	14
第 2 章 将 SERVICENOW 与 RED HAT HYBRID CLOUD CONSOLE 集成	15
2.1. 为 RED HAT INSIGHTS 应用程序安装和配置 SERVICENOW FLOW TEMPLATES	15
2.2. 其他资源	17
第 3 章 将 SLACK 与混合云控制台集成	18
3.1. 在 SLACK 中配置传入的 WEBHOOK	18
3.2. 在 RED HAT HYBRID CLOUD 控制台中配置 SLACK 集成	19
3.3. 为 SLACK 集成创建行为组	20
3.4. 其他资源	22
第 4 章 将 EVENT-DRIVEN ANSIBLE 与 RED HAT HYBRID CLOUD CONSOLE 集成	23
4.1. 配置 EVENT-DRIVEN ANSIBLE 以与红帽混合云控制台集成	23
4.2. 为 EVENT-DRIVEN ANSIBLE 集成创建行为组	25
4.3. 其他资源	26
第 5 章 将 MICROSOFT 团队与混合云控制台集成	28
5.1. 配置 MICROSOFT 团队以与混合云控制台集成	28
5.2. 为 MICROSOFT 团队集成创建行为组	29
5.3. 其他资源	30
第 6 章 将 GOOGLE CHAT 与 RED HAT HYBRID CLOUD CONSOLE 集成	31
6.1. 在 GOOGLE CHAT 中配置传入的 WEBHOOK	31
6.2. 在 RED HAT HYBRID CLOUD CONSOLE 中配置 GOOGLE CHAT 集成	31
6.3. 为 GOOGLE CHAT 集成创建行为组	32
6.4. 其他资源	33
附录 A. 混合云控制台集成故障排除	34
A.1. 对第三方集成和 RED HAT INSIGHTS 之间的连接问题进行故障排除	34
A.2. 混合云控制台与 SPLUNK 的集成故障排除	34
A.3. 混合云控制台与 SERVICENOW 的集成故障排除	34
A.4. 其他资源	35
对红帽文档提供反馈	36

前言

您可以将 Red Hat Hybrid Cloud Console 与 Splunk、ServiceNow、Slack、Slack、EventDriven Ansible、Microsoft Teams 和 Google Chat 集成，将事件触发的通知路由到这些第三方应用程序。集成第三方应用程序会扩展电子邮件和消息之外的通知范围，以便您可以从您首选的平台仪表板中查看和管理混合云控制台事件。

要了解更多有关通知的信息，请参阅 [Red Hat Hybrid Cloud Console 上配置通知](#)。

先决条件

- 您有机构管理员或通知混合云控制台的管理员权限。
- 您有要与混合云控制台集成的每个第三方应用程序所需的配置权限。

第 1 章 为 SPLUNK 安装和配置 RED HAT INSIGHTS 应用程序

用于 Splunk 的 Red Hat Insights 应用程序将所选混合云控制台事件转发到 Splunk。应用程序与混合云控制台无缝集成，以便您可以集中精力处理 Splunk 应用程序端的数据，与管理其他数据源的方式相同。配置了集成后，您可以从 Splunk 仪表板查看和管理混合云控制台通知，而无需打开 Red Hat Hybrid Cloud Console。

联系支持

如果您在 Red Hat Insights 应用程序 for Splunk 时遇到问题，请联系红帽获得支持。您可以通过点 Help (? icon) > **Open a case**, 或从 ? > **Support options** 查看更多选项，直接从混合云控制台打开红帽支持问题单。

Splunk 不提供故障排除。红帽完全支持用于 Splunk 的 Red Hat Insights 应用程序。

先决条件

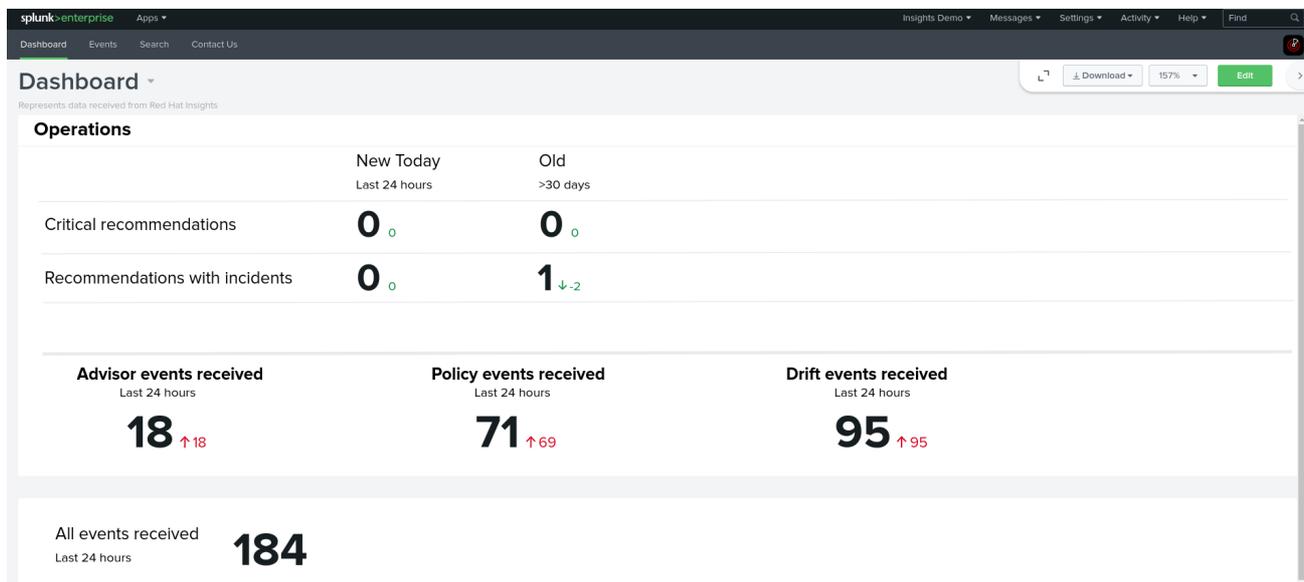
- 您有 Splunk 登录凭证：
 - 在 Splunk Cloud Platform 上，您必须具有 Splunk Cloud Administrator **sc-admin** 角色。
 - 在 Splunk Enterprise 上，您必须具有 **admin** 角色。有关创建 **admin** 角色的更多信息，请参阅 [Splunk 文档中的创建安全管理凭证](#)。
- 具有混合云控制台的机构管理员权限。

1.1. 为 SPLUNK 安装 RED HAT INSIGHTS 应用程序

安装和配置 Splunk 的 Red Hat Insights 应用程序，以便将 Splunk 与混合云控制台集成，以便 Splunk 可以从 Hybrid Cloud Console 接收事件通知。设置自动化执行以下任务：

- 使用机构管理员权限创建具有通知管理员角色的用户组。您还可以手动创建用户组。有关手动配置的更多信息，请参阅 [混合云控制台帐户 中手动配置管理员组](#)。
- 使用 Splunk HEC URL 和 HEC 令牌创建名为 SPLUNK_AUTOMATION 的新集成，集成类型 Splunk。
- 在 RHEL 捆绑包上创建一个名为 SPLUNK_AUTOMATION_GROUP 的新行为组。组包含向 SPLUNK_AUTOMATION Splunk 集成发送通知的操作。
- 将新行为组 SPLUNK_AUTOMATION_GROUP 分配给所有混合云控制台服务。这会将事件从所有服务转发到 Splunk。目前，行为组转发来自 Advisor, Policies, Drift, Compliance, Malware Detection, Patch, 和 Vulnerability 服务的事件。

当 Splunk 开始从 Hybrid Cloud Console 接收通知时，Sununk 仪表板的 Red Hat Insights 应用程序会显示事件活动。每个数字都包含到混合云控制台的超链接。



先决条件

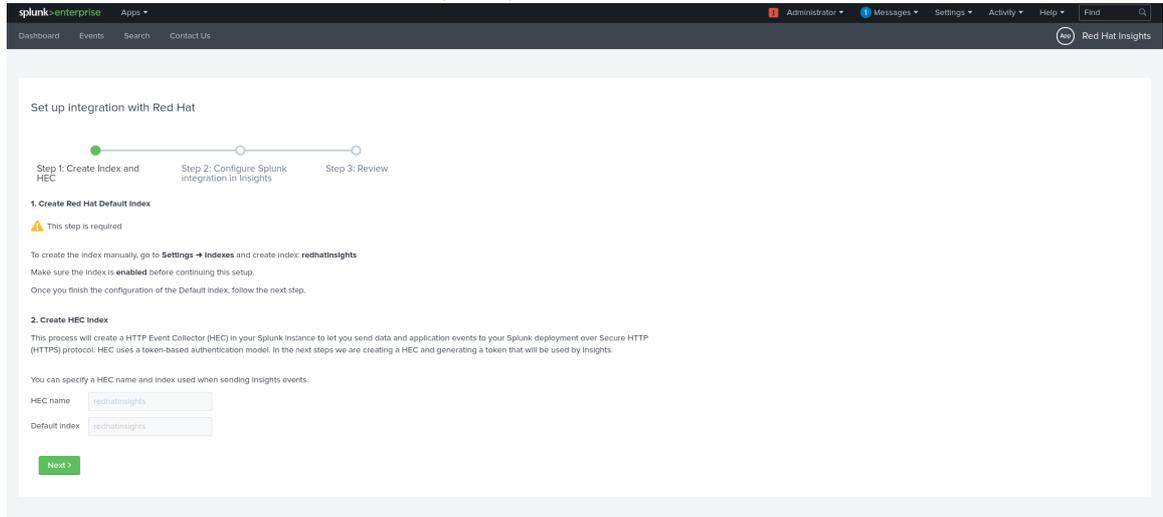
- 具有混合云控制台的机构管理员权限。
- 您有 Splunk 登录凭证：
 - 要在 Splunk Cloud Platform 上安装应用程序，您必须具有 Splunk Cloud Administrator **sc-admin** 角色。
 - 要在 Splunk Enterprise 上安装应用程序，您必须具有 **admin** 角色。有关创建 **admin** 角色的更多信息，请参阅 [Splunk 文档中的创建安全管理凭证](#)。
- 您的浏览器中禁用了弹出窗口块程序。

流程

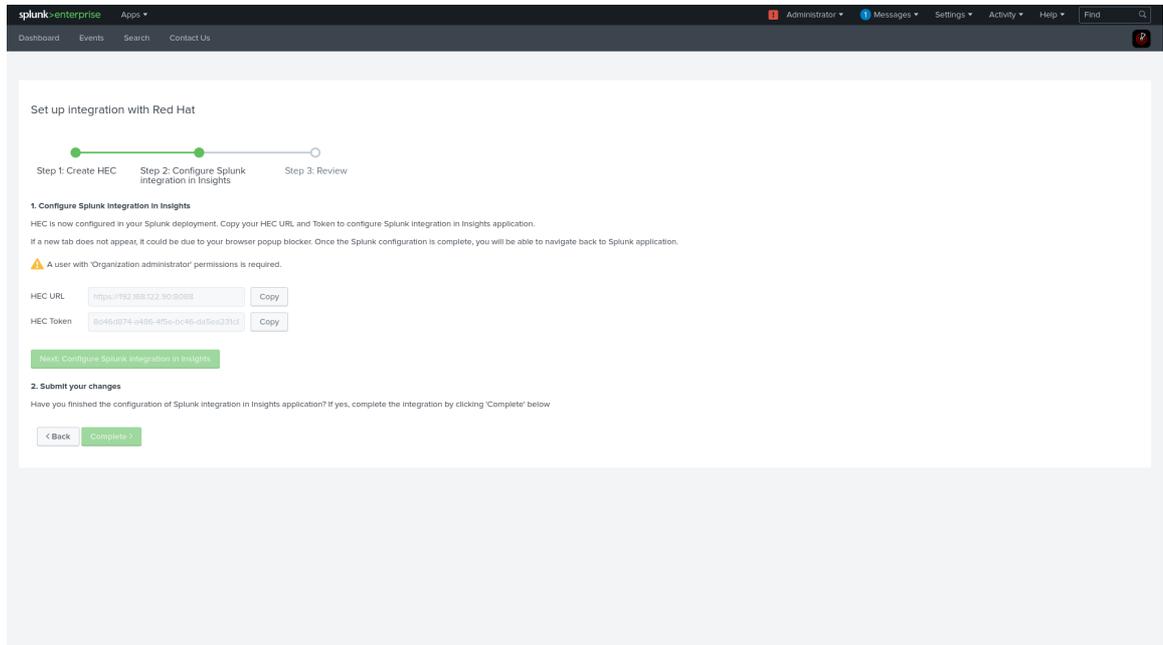
1. 为 Splunk 安装 Red Hat Insights 应用程序：
 - a. 登录到 Splunk。
 - b. 在主页上，在过滤器框中搜索 **Red Hat Insights** 并选择它。
 - c. 点 **Install**。安装过程完成后，会显示 **Install successful** 消息。
 - d. 在主页上，单击 **Settings** 菜单(gear 图标)。**Apps** 页面将打开。
 - e. 在过滤器框中输入 **Red Hat Insights**，然后单击放大镜。应用程序会出现在搜索结果中。
 - f. 在主页上，单击屏幕左侧的 **Apps** 标题下的 **Find more apps**。此时会打开 **Browse More Apps** 页面。
 - g. 在过滤器框中输入 **Red Hat Insights**，然后按 **Enter** 键。**Red Hat Insights** 会出现在搜索结果中。
 - h. 选择 **Red Hat Insights**。
 - i. 点 **Install**。
 - j. 确认或输入 Splunk 用户名和密码，然后单击 **Agree** 和 **Install**。安装过程完成后，会打开 **Complete** 对话框。

2. 为 Splunk 设置 Red Hat Insights 应用程序：

- a. 在 Complete 对话框中，单击 Open the App。此时会打开 App configuration 页面。
- b. 单击 Continue to app setup 页面。此时会打开 Set up integration with Red Hat Insights 页面。该页面包括 HTTP 事件收集器(HEC)名称和默认索引字段。

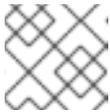


- c. 在 Create Red Hat Default Index 下，点 Settings > Indexes。Indexes 页面会在一个新标签页中打开。
- d. 在 Indexes 页面上，点 New Index。
- e. 在 Name 字段中输入索引名称（例如，redhatinsights）。
- f. 在 Max raw data size 和 Searchable retention（天）字段中输入值。
- g. 点击 Save。您创建的索引会出现在 Indexes 列表中。它会被默认启用。
- h. 在第一个 Splunk 屏幕中，在 Set up integration with Red Hat 页面中，在 HEC name 字段中输入 HEC 的名称（例如 redhatinsights）。
 - i. 在 Default index 字段输入您刚才创建的索引名称（例如，redhatinsights）。
 - j. 点击 Next。
 - k. 点 Review，然后点 Submit。您创建的 HEC 名称会出现在 HEC Name 字段中。
 - l. 点 Next 创建 HEC URL 和 HEC Token。



3. 在 Insights 中配置 Splunk 集成：

- a. 点 Copy 复制 Splunk Enterprise 中的 HEC URL 值。
- b. 点 Next: Configure Splunk integration in Insights。Hybrid Cloud Console 在新的浏览器标签页中打开。



注意

此按钮将被禁用，直到您点击 HEC URL 或 HEC 令牌的 Copy 按钮。

- c. 在 Hybrid Cloud Console 中，进入到 Settings > Integrations。

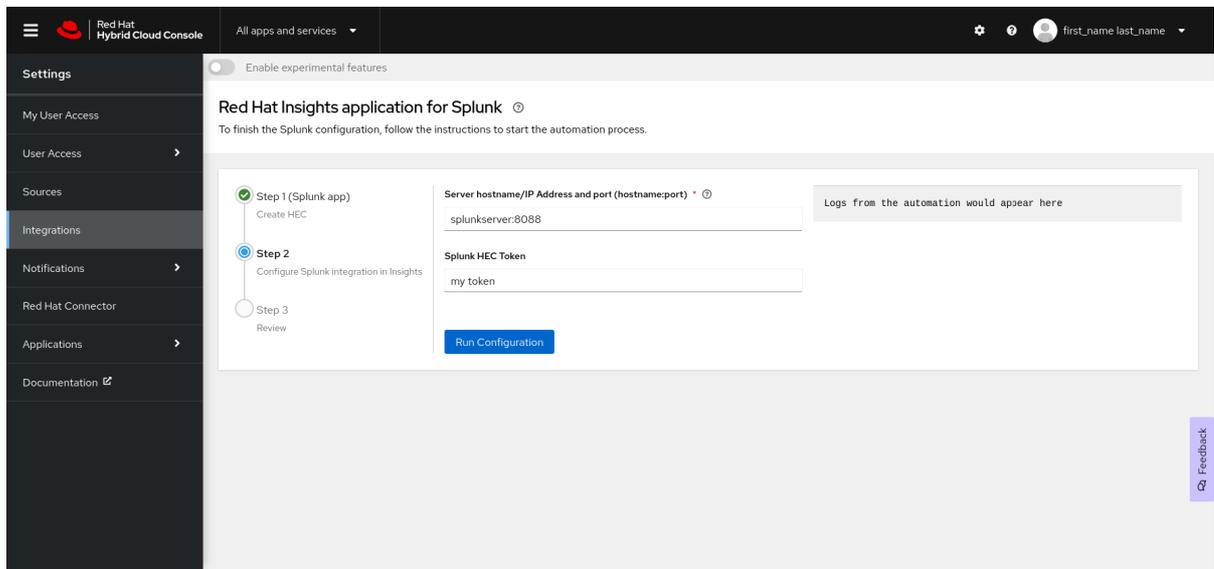
- a. 将 HEC URL 值粘贴到 Splunk HEC URL 字段中。



注意

如果控制台的新标签页没有打开，请在浏览器中禁用弹出窗口块程序。

- b. 如果需要，添加端口。Splunk Cloud Platform 的默认端口为 443。Splunk Enterprise 和 Splunk 云免费试用的默认端口为 8088。



- c. 可选：如果您使用 Splunk Cloud，请编辑要粘贴到 Integrations 页面中的 Splunk HEC URL 字段的 HEC URL，以匹配 Splunk Cloud 格式：

- 在 Google Cloud Platform (GCP) 以外的所有云上使用 Splunk Cloud Platform 的以下格式：

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

- 在 Google Cloud Platform (GCP) 上为 Splunk Cloud Platform 使用以下格式：

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

替换以下占位符：

- 协议：**http** 或 **https**。
- Host**：运行 HEC 的 Splunk Cloud Platform 实例的名称，后跟域 **mvapichcloud.com**。
- 端口**：HEC 端口号（在 Splunk Cloud Platform 实例中默认为 443）。
- 端点**：您要使用的 HEC 端点。在很多情况下，您将 **/services/collector/event** 端点用于 JSON 格式的事件，或原始事件的 **services/collector/raw** 端点。

示例：

- 使用 JSON 在 GCP 上的 Splunk 云平台：

```
https://http-inputs.myhost.splunkcloud.com:443/services/collector/event
```

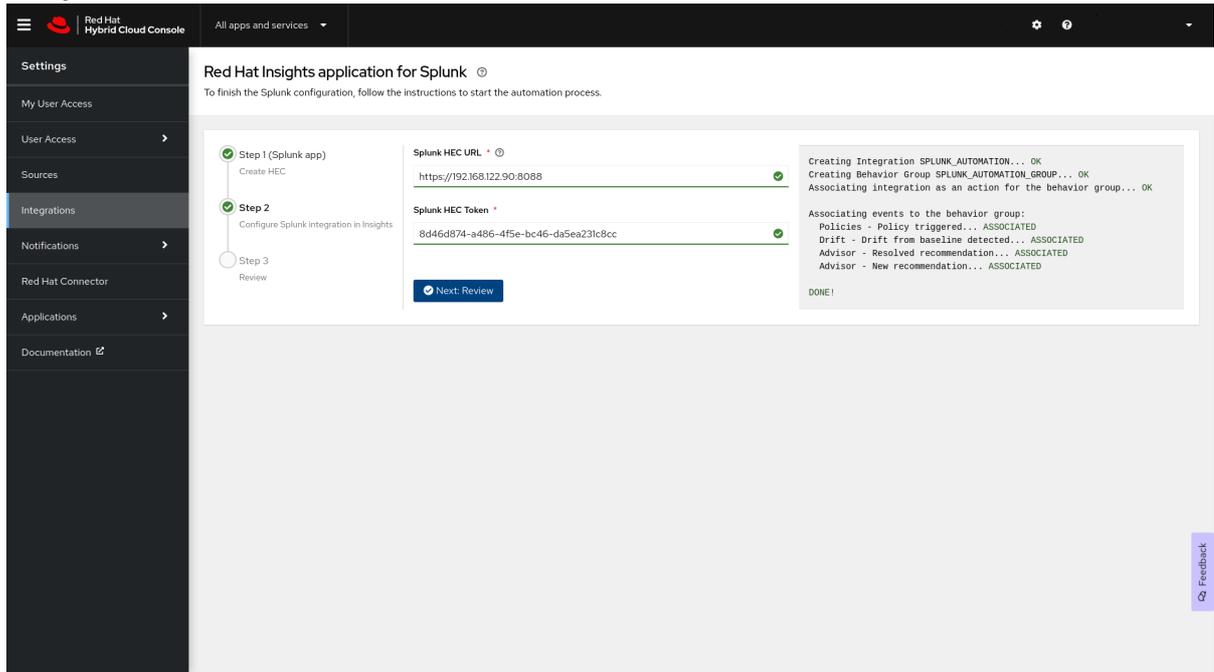
- Splunk Cloud free trial on AWS 使用原始事件：

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

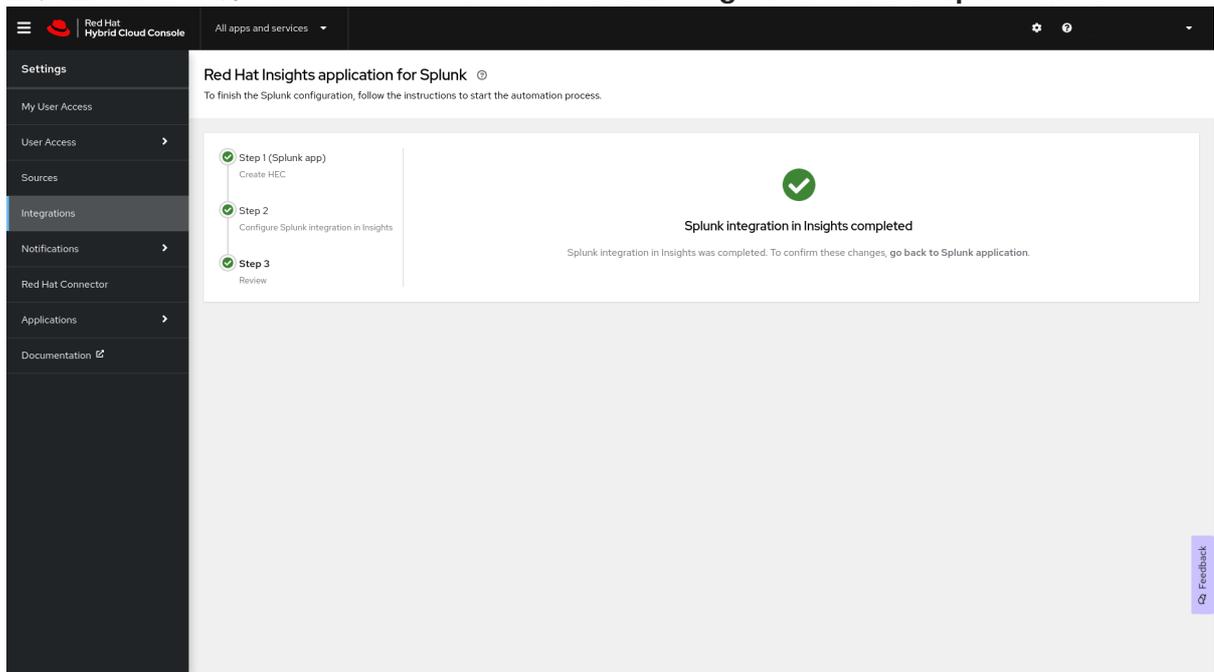
- 完成设置过程：

- d. 复制 Splunk 中的 HEC Token 值，并将它粘贴到 Hybrid Cloud Console Integrations 页面上的 Splunk HEC Token 字段。

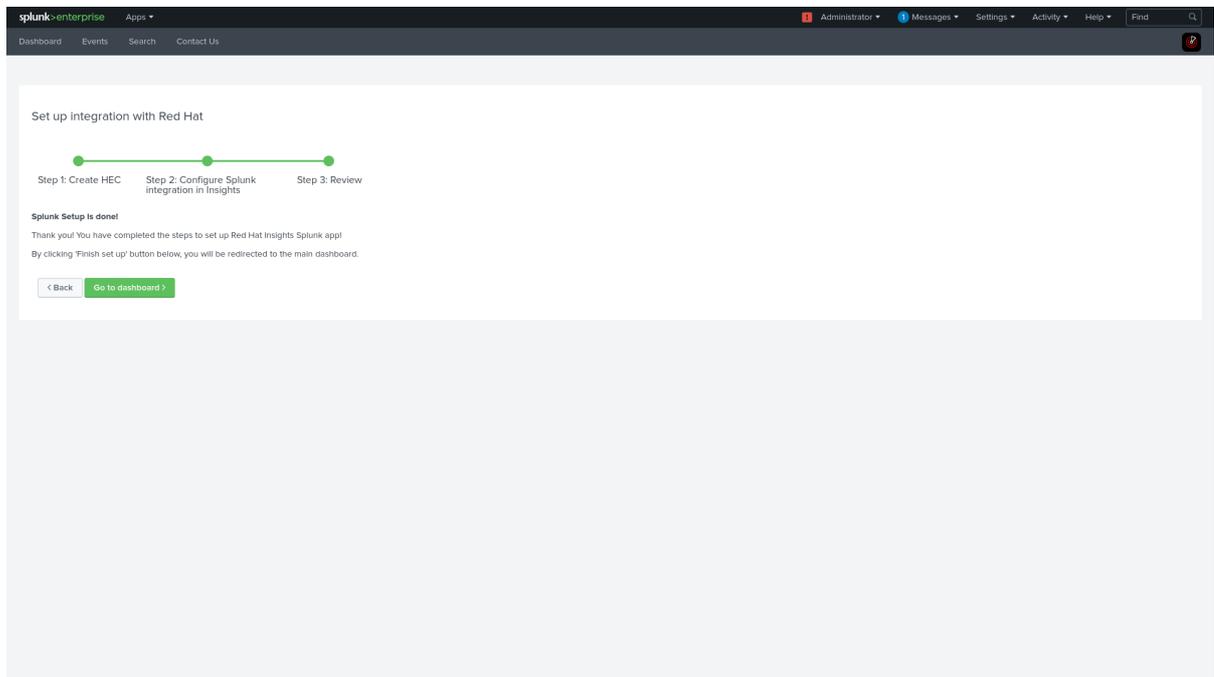
- e. 在 Hybrid Cloud Console 中，点 Run configuration。混合云控制台设置集成，创建行为组，并将 Hybrid Cloud Console 事件与行为组相关联。页面右侧的状态消息部分显示这些操作的状态。



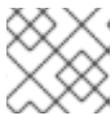
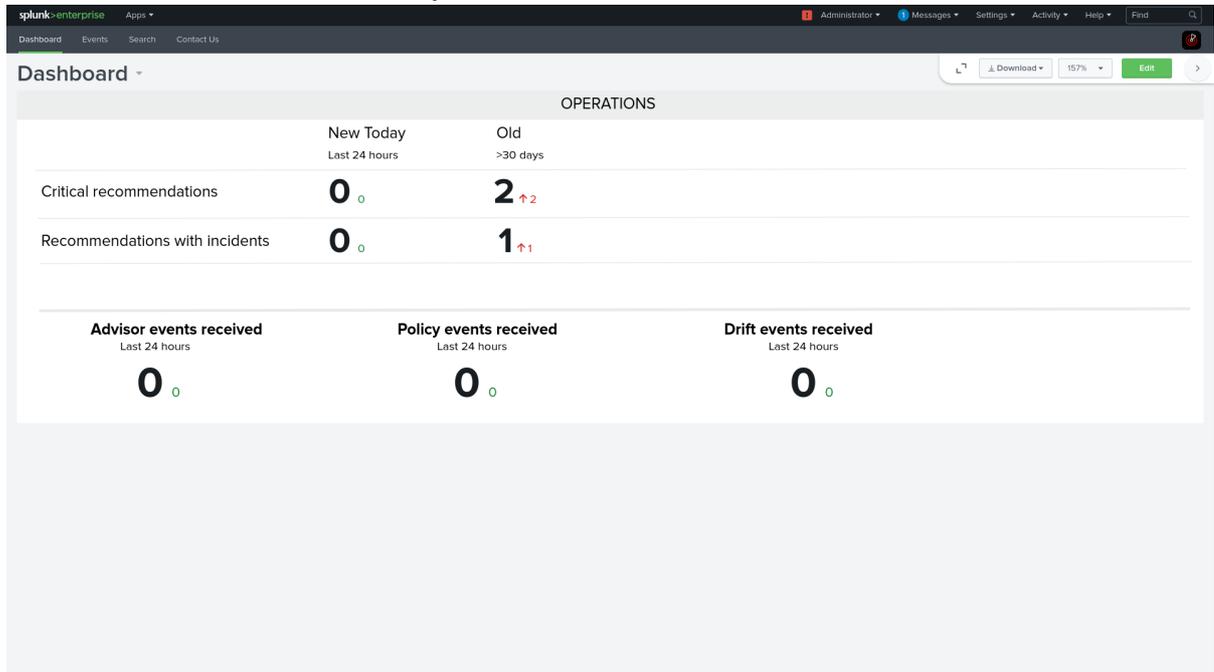
- f. 当设置成功完成时，点 Next: Review。应用程序返回 Insights 完成的消息 Splunk 集成。



- g. 点 Go back to the Splunk 应用程序 这会将您重定向到 Splunk 中的 Set up integration with Red Hat 屏幕。
- h. 点 Finish set up 以完成 Splunk 中的设置。



i. 点 **Go to dashboard** 来重定向到 Splunk 仪表板。



注意

如果在 Insights 设置过程中的集成配置失败，请联系红帽支持。

1. 要在 Splunk 仪表板上查看 Hybrid Cloud Console 事件列表，请点 **Events** 选项卡。每个事件都超链接至混合云控制台。

Timestamp	Account	Application	System	Description
2022-05-02 15:50:09	5685364	Policies	rhe18scontroller	Second test new policy policy triggered
2022-05-02 15:50:09	5685364	Policies	rhe18scontroller	Test new policy policy triggered
2022-05-02 15:50:09	5685364	Drift	rhe18scontroller	Drift detected from baseline (arch) baseline
2022-05-02 15:50:09	5685364	Drift	rhe18scontroller	Drift detected from Baseline (kernel) baseline
2022-05-02 15:50:09	5685364	Drift	rhe18scontroller	Drift detected from Test other facts baseline
2022-05-02 15:50:07	5685364	Drift	rhe18skvm	Drift detected from Baseline (arch) baseline
2022-05-02 15:50:07	5685364	Drift	rhe18skvm	Drift detected from Baseline (kernel) baseline
2022-05-02 15:50:07	5685364	Drift	rhe18skvm	Drift detected from Test other facts baseline
2022-05-02 15:50:05	5685364	Drift	rhe18mssql	Drift detected from Baseline (arch) baseline
2022-05-02 15:50:05	5685364	Drift	rhe18mssql	Drift detected from Baseline (kernel) baseline
2022-05-02 15:50:05	5685364	Drift	rhe18mssql	Drift detected from Test other facts baseline
2022-05-02 15:50:01	5685364	Policies	rhe18mssql	Second test new policy policy triggered
2022-05-02 15:50:01	5685364	Policies	rhe18mssql	Test new policy policy triggered
2022-05-02 15:50:01	5685364	Policies	rhe18skvm	Second test new policy policy triggered
2022-05-02 15:50:01	5685364	Policies	rhe18skvm	Test new policy policy triggered
2022-05-02 15:49:59	5685364	Policies	rhe18laptop	Second test new policy policy triggered
2022-05-02 15:49:59	5685364	Policies	rhe18laptop	Test new policy policy triggered
2022-05-02 15:49:58	5685364	Drift	rhe18laptop	Drift detected from Baseline (arch) baseline
2022-05-02 15:49:58	5685364	Drift	rhe18laptop	Drift detected from Baseline (kernel) baseline
2022-05-02 15:49:58	5685364	Drift	rhe18laptop	Drift detected from Test other facts baseline

其它资源

- [Splunk Enterprise](#)
- [在 Splunk 云部署上安装应用程序](#)
- [在 Splunk Enterprise 上配置 HTTP 事件收集器](#)
- [在 Splunk Cloud Platform 上配置 HTTP 事件收集器](#)
- [配置用户访问](#)
- [在 Red Hat Hybrid Cloud Console 中配置通知](#)
- [在混合云控制台帐户中手动配置管理员组](#)

1.2. 启用 HEC 令牌

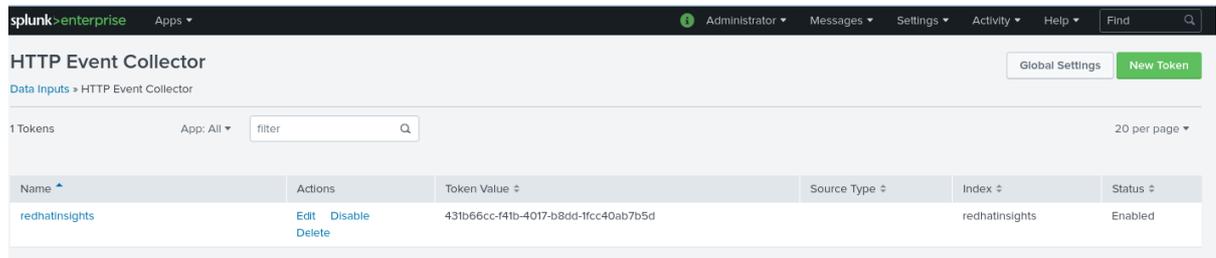
在 Splunk 可以接收混合云控制台事件前，您必须启用 HEC 令牌。

先决条件

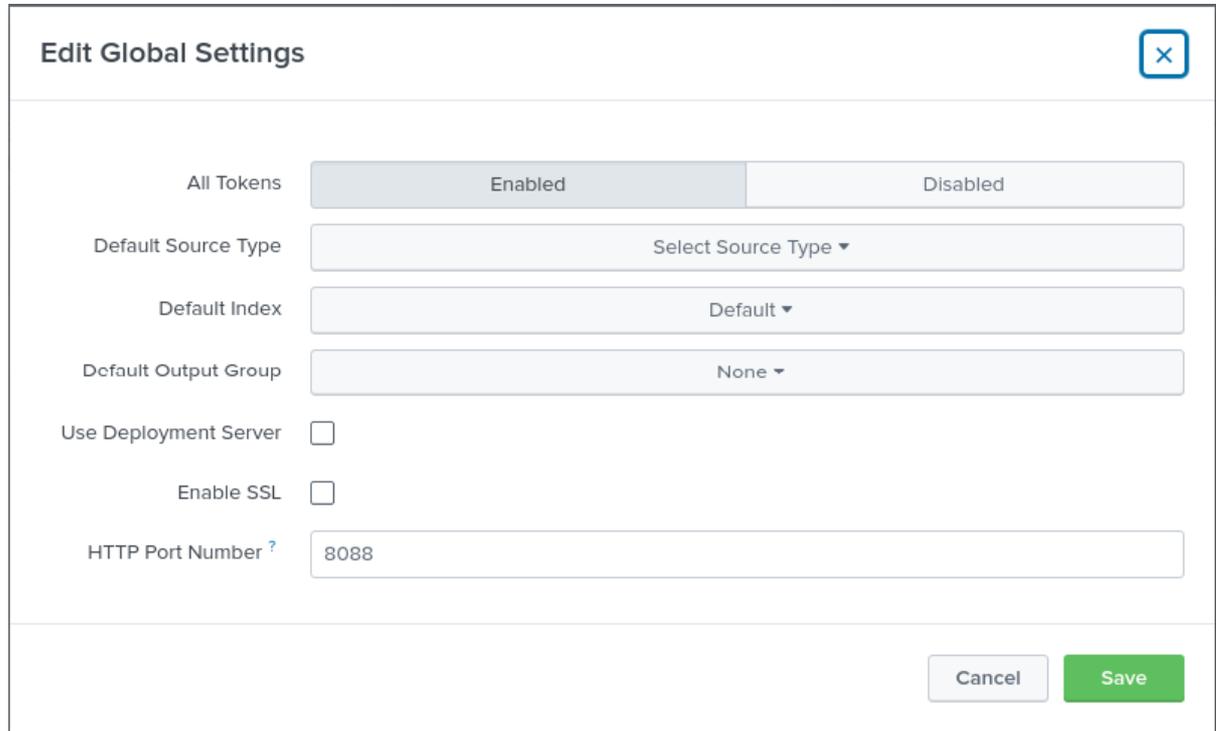
- 具有混合云控制台的机构管理员权限。
- 您有 Splunk 登录凭证：
 - 在 Splunk Cloud Platform 上，您必须具有 Splunk Cloud Administrator `sc-admin` 角色。
 - 在 Splunk Enterprise 上，您必须具有 `admin` 角色。有关创建 `admin` 角色的更多信息，请参阅 [Splunk 文档中的创建安全管理凭证](#)。

流程

1. 在 Splunk 主页中，导航到 **Settings**。
2. 选择 **Data Inputs**，然后选择 **HTTP Event Collector**。HTTP 事件收集器页面显示 HEC、其 Token 值、您在设置过程中选择的对应索引以及 HEC 的状态。



3. 点页面右上角的 Global Settings。此时将显示 Edit Global Settings 对话框。



4. 选择 Enabled。这可启用设置过程中自动创建的 HEC 令牌。



注意

HEC 令牌使用默认 HTTP 端口号 8088。如果您使用不同的端口（如 Splunk 云的端口 443），您必须更新 Hybrid Cloud Console Splunk Integration 以匹配。

其它资源

- 有关 Splunk 云中的 HEC 令牌的更多信息，请参阅 Splunk 文档中的在 [Splunk Cloud Platform 上配置 HTTP 事件收集器](#)。
- 有关在 Splunk Enterprise 中设置和使用 HEC 的更多信息，请参阅 Splunk Enterprise 文档中的 [设置和使用 Splunk Enterprise 上的 HTTP 事件收集器](#)。

1.3. 在 HYBRID CLOUD CONSOLE 帐户中手动配置管理员组

用于 Splunk 自动安装和设置流程的 Red Hat Insights 应用程序会在 Hybrid Cloud Console 帐户中自动配置一个通知管理员角色和组。但是，您可以手动创建通知管理员。

先决条件

- 使用 Organization Administrator 角色登录到 Hybrid Cloud Console。

流程

1. 点 Settings > Identity & Access Management
2. 在 Identity & Access Management 下，根据需要展开 User Access，然后选择 Groups。
3. 点 Create group。此时会出现 Name 和 description 页面。
4. 输入组的名称（例如：mvapich notifgroup），输入描述，然后单击 Next。此时会打开 Add roles 页面。
5. 要添加 Notifications 管理员角色，请在搜索框中输入 notif。
6. 从搜索结果列表中选择 Notifications 管理员，然后单击 Next。此时会打开 Add Members 页面。
7. 选择要添加到此组的用户。您可以使用搜索框搜索特定名称。
8. 单击 Next。Review Details 页面将打开。
9. 检查信息，然后单击 Submit 以创建该组。
10. 单击 退出。Groups 页面将打开。

验证

1. 在搜索框中输入新组名称。
2. 点组名称。该组的页面将打开。
3. 在 Roles 选项卡上，验证组是否具有 Notifications 管理员角色。
4. 单击 Members 选项卡，再验证组是否包含正确的成员。

1.4. 手动配置 SPLUNK 集成

用于 Splunk 自动安装和设置流程的 Red Hat Insights 应用程序会自动配置 Splunk 集成到您的混合云控制台帐户。如果要手动配置集成，请使用这个步骤。

先决条件

- 您有一个来自 Splunk Cloud 或 Splunk Enterprise 的 HTTP 事件收集器(HEC) URL。
- 您有 Splunk Cloud 或 Splunk Enterprise 中的 HEC 令牌值。
- 使用通知管理员角色登录到 Hybrid Cloud Console。

流程

1. 在 Hybrid Cloud Console 中，进入到 Settings > Integrations。
2. 选择 Reporting & Automation 选项卡。
3. 点 Add integration。
4. 选择 Splunk 作为集成类型，然后单击 Next。

5. 在 Integration name 字段中输入新集成的名称（例如，redhat_mvapich）。
6. 在 Endpoint URL 字段中，添加您的 Splunk HEC 端点 URL：
 - a. 对于 Splunk Enterprise，Splunk 默认使用端口 8088。例如：`https://<mvapich-endpoint>:8088`
 - b. 对于 Splunk 云，Splunk 使用端口 443。有关 AWS 或 GCP 上的 Splunk 云的更多信息，请参阅 [将数据发送到 HTTP 事件收集器](#)。



注意

该服务会自动添加 `<endpoint>` (http 路径)。您不需要在 Endpoint URL 的表单中包括它。

以下示例显示了带有 Splunk 平台的正确端口号的端点 URL。

- 内部(Splunk Enterprise)：`https://splunk.company.com:8088`
 - Splunk Cloud（在 AWS 上）：`https://http-inputs-mycompany.splunkcloud.com:443`
 - Splunk Cloud（在 GCP 上）：`https://http-inputs.mycompany.splunkcloud.com:443`
7. 在 Secret token 字段中，添加 Splunk HEC 令牌值。
 8. 点击 Next。
 9. 检查集成详情并点 Submit。

其他资源

- 有关 Splunk 云中的 HEC 令牌的更多信息，请参阅 Splunk 文档中的在 [Splunk Cloud Platform 上配置 HTTP 事件收集器](#)。
- 有关为 Splunk 云配置端口的更多信息，请参阅 [将数据发送到 HTTP 事件收集器](#)。
- 有关在 Splunk Enterprise 中设置和使用 HEC 的更多信息，请参阅 Splunk Enterprise 文档中的 [设置和使用 Splunk Enterprise 上的 HTTP 事件收集器](#)。

1.5. 其他资源

- 有关 Splunk 的更多信息，请参阅 [Splunk 网站](#)。
- 有关 Splunkbase 的更多信息，请参阅 [Splunkbase 网站](#)。
- 有关 Splunk 集成故障排除的详情，请参考 [对混合云控制台集成 进行故障排除](#)。

第 2 章 将 SERVICENOW 与 RED HAT HYBRID CLOUD CONSOLE 集成

Red Hat Insights 应用程序的 ServiceNow Flow Templates 与 Insights for Red Hat Enterprise Linux 服务集成。模板提供 ServiceNow 流，用于创建发现的漏洞、性能、系统配置建议和其他风险中的事件。应用程序包含一个示例流，您可以编辑它来为您的机构自定义它。

此应用程序将所选的 Hybrid Cloud Console 事件转发到 ServiceNow。Red Hat Insights 应用程序的流模板与混合云控制台无缝集成，以便您可以像管理其他数据源一样专注于处理 ServiceNow 应用程序端的数据。

您可以使用 Red Hat Insights 应用程序的 Flow Templates 处理以下混合云控制台服务中的事件：

- Advisor
- 漏洞
- 您可能已经配置的任何其他 Red Hat Hybrid Cloud Console 事件

Insights for RHEL 作为红帽订阅的一部分提供，可通过 [Red Hat Hybrid Cloud Console](#) 访问。

联系支持

如果您在 Red Hat Insights 应用程序 for ServiceNow 时遇到问题，请联系红帽获得支持。您可以通过点 Help (? icon) > Open a case, 或从 ? > Support options 查看更多选项，直接从混合云控制台打开红帽支持问题单。

ServiceNow 将不提供故障排除。红帽完全支持 ServiceNow 的 Red Hat Insights 应用程序。

2.1. 为 RED HAT INSIGHTS 应用程序安装和配置 SERVICENOW FLOW TEMPLATES

您可以使用 Red Hat Insights 应用程序的 Flow Templates 将 ServiceNow 与混合云控制台集成，从混合云控制台中触发的事件创建 ServiceNow 流。要将 ServiceNow 与 Red Hat Hybrid Cloud Console 集成，您必须安装 ServiceNow IntegrationHub Enterprise Pack Installer 插件。配置插件和应用程序后，从混合云控制台的事件数据流到 ServiceNow 实例。在应用流中使用 ServiceNow REST API 异步触发器接收器。

先决条件

- 具有混合云控制台的机构管理员权限。
- 通知管理员权限在 User Access 中配置。
- 您有一个红帽订阅，您可以访问 Red Hat Hybrid Cloud Console。
- 您的浏览器中禁用了弹出窗口块程序。
- 已安装 ServiceNow IntegrationHub Enterprise Pack Installer 插件。如果没有安装，请从 ServiceNow 请求插件。
- 您可以访问以下 ServiceNow 角色：
 - admin
 - x_rhttp_rh_webhook.rest

- `sn_appclient.app_client_company_installer`（只能安装与实例公司匹配的应用程序）或 `sn_appclient.app_client_user`。
- 在 ServiceNow 中，您有表权限的事件（写入）访问权限。
- 您使用 San Diego 或更高的 ServiceNow 版本。

流程

1. 登录您的 ServiceNow 实例。
2. 进入 [ServiceNow Store 主页](#) 并安装或更新 Flow Templates：
 - 从 ServiceNow Store（或作为 [更新集](#)）安装 Red Hat Insights 应用程序的流模板。
 - a. [创建一个新用户](#)，用户 ID 为 `rh_insights_integration`。
 - b. 检查 Internal Integration User 以了解您刚才创建的用户。
 - c. 确保该用户为 Active。
 - d. 将角色 `x_rhttp_rh_webhook.rest` 分配给用户。
 - e. 为用户生成密码。复制在设置过程中使用的信息。
3. 在新的浏览器窗口或标签页中打开 [Hybrid Cloud Console](#)。
4. 导航到 Settings > Integrations，选择 Reporting & Automation 选项卡，然后完成以下步骤：
 - a. 点 Add integration。
 - b. 选择 ServiceNow 作为集成类型，然后单击 Next。
 - c. 输入集成的名称，如 *ServiceNow 集成*。
 - d. 提供 Endpoint URL，将 `<instance.servicenow.com>` 替换为您的 ServiceNow 实例：
`https://<instance.servicenow.com>/api/x_rhttp_rh_webhook/flow_templates_for_red_hat_insights`
 - e. 启用 SSL 的复选框会默认启用。
 - f. 在 Secret token 字段中，粘贴您在 ServiceNow 中创建的 `rh_insights_integration` 用户生成的密码。
 - g. 单击 Next。
 - h. 检查集成详情并点 Submit。
5. 进入 [Hybrid Cloud Console > Settings > Notifications](#) 并完成以下步骤：
 - a. 在通知下，选择 Configure Events。
 - b. 选择您要为其配置事件通知行为的应用程序捆绑包选项卡：Red Hat Enterprise Linux、Console 或 OpenShift。
 - c. 点 Behavior Groups 选项卡。

- d. 点 Create new group 打开 Create behavior group 向导。
 - e. 在 Name 字段中输入新行为组的名称，然后点 Next。
 - f. 对于 Actions，从下拉列表中选择 Integration: ServiceNow。
 - g. 对于 Recipient，请选择您之前创建的 ServiceNow 集成（例如，ServiceNow 集成）。
6. 点击 Next。此时会打开 Associate 事件类型 窗口。
 7. 从列表中选择以下事件类型：
 - Advisor 新建议
 - 带有 CVSS >= 7.0 的新漏洞
 - 严重(Critical)严重性的安全漏洞
 - 包含安全规则的新漏洞
 - 任何带有已知漏洞的漏洞
 8. 单击 Next，然后单击 Finish 以完成设置过程。

请注意，事件在特定条件上生成（例如，当系统配置了 Red Hat Insights 检查时）。如果 ServiceNow 中没有显示事件，请检查 Event 日志，以查看是否有与条件匹配的事件。



注意

如果在 Insights 设置过程中的集成配置失败，请联系红帽支持。

2.2. 其他资源

其他资源

- 有关设计 ServiceNow 流的详情，请参考 [ServiceNow Flow Designer](#)。
- 要下载 ServiceNow 应用程序，请参阅 [ServiceNow Store](#)。
- 有关安装从 ServiceNow Store 购买的应用程序使其在实例上可用的详情，请参阅安装 [ServiceNow Store 应用程序](#)。
- 有关在将 ServiceNow 与混合云控制台集成后配置通知的详情，请参考在 [Red Hat Hybrid Cloud Console 中配置通知](#)。
- 有关对 ServiceNow 集成进行故障排除的详情，请参考 [对混合云控制台集成进行故障排除](#)。
- 有关 ServiceNow Store 的更多信息，请参阅 [ServiceNow Store](#)。
- 有关 ServiceNow 的更多信息，请参阅 [ServiceNow](#)。

第 3 章 将 SLACK 与混合云控制台集成

您可以配置 Hybrid Cloud Console，将事件通知发送到 Slack 频道或直接向用户发送。Slack 集成支持所有混合云控制台服务的事件。



注意

本例中为 Red Hat Enterprise Linux 配置 Slack 集成。集成也适用于 Red Hat OpenShift 和 Hybrid Cloud Console 事件。

Slack 集成使用传入的 Webhook 接收事件数据。如需有关 Webhook 的更多信息，请参阅 [Slack API 文档中的使用传入 Webhook 发送信息](#)。

联系支持

如果您在与 Slack 的混合云控制台集成时遇到问题，请联系红帽获得支持。Slack 将不提供故障排除。红帽完全支持混合云控制台与 Slack 集成。

您可以通过点 Help > Open a case，或者从 Help > Support 选项中查看更多选项，直接从 Hybrid Cloud Console 打开 Red Hat 支持问题单。

3.1. 在 SLACK 中配置传入的 WEBHOOK

要准备 Slack 以便与混合云控制台集成，您必须在 Slack 中配置传入的 Webhook。

先决条件

- 对于您要添加传入 Webhook 的 Slack 实例具有所有者或 admin 权限。
- 您有 App Manager 权限才能将 Slack 应用程序添加到频道。
- 您有一个 Slack 频道或用户来接收通知。

流程

1. 创建 Slack 应用程序：

- a. 进入 [Slack API](#) 网页并点 Create your Slack app 按钮。这将打开 Create a app 对话框。
- b. 从头开始使用 Slack 配置 UI 来创建应用程序。
- c. 输入应用程序的名称并选择您要接收通知的工作区。



注意

如果您看到需要管理员批准的消息，您可以在下一步中请求批准。

- d. 点 Create App 以完成 Slack 应用程序的创建。

2. 启用传入的 Webhook：

- a. 在左侧导航的 Features 标题下，单击 Incoming Webhooks。
- b. 将 Activate Incoming Webhooks 切换为 On。

- c. 点 Request to Add New Webhook 按钮。如果需要，请为您的管理员输入一条消息，以授予应用程序的访问权限，然后单击 Submit Request。成功消息将确认您已经正确配置了这一点。
3. 创建传入的 Webhook：
 - a. 在左侧导航中的 Settings 下，单击 Basic Information。
 - b. 在 Install your app 部分中，点 Install to Workspace 按钮。
 - c. 选择您要 Slack 应用程序发布通知的频道，或者选择要发送通知的用户作为直接消息。
 - d. 点 Allow 以保存更改。
 4. 可选：配置您的 Hybrid Cloud Console 通知如何在 Slack 中出现：
 - a. 向下滚动到 显示信息。
 - b. 根据需要配置应用程序描述、图标和背景颜色。
 5. 复制 Webhook URL：
 - a. 在 Features 下，单击 Incoming Webhooks。
 - b. 点 Webhook URL 旁边的 Copy 按钮。您将使用 URL 在混合云控制台中设置集成第 3.2 节“在 Red Hat Hybrid Cloud 控制台中配置 Slack 集成”。

验证

- 打开您在配置过程中选择的 Slack 频道或用户，并检查您添加了集成的消息。

其他资源

- 有关 Slack 中 Webhook 的详情，请参考[使用传入的 webhook 发送信息](#)。
- 有关工作流的详情，请参阅[构建工作流：创建在 Slack 外启动的工作流](#)。
- 有关管理应用程序批准的详情，请参考在[Enterprise Grid 工作区 中管理应用程序批准](#)。
- 有关 Slack 的一般帮助，请查看[Slack 帮助中心](#)。

3.2. 在 RED HAT HYBRID CLOUD 控制台中配置 SLACK 集成

在 Slack 中配置了传入的 webhook 后，您可以将 Hybrid Cloud Console 配置为将事件通知发送到您配置的 Slack 频道或用户。

先决条件

- 您有机构管理员或通知 Red Hat Hybrid Cloud 控制台的管理员权限。

流程

1. 如有必要，进入[Slack API 网页](#)并复制您配置的 Webhook URL。



注意

有关创建 Slack Webhook URL 的步骤，请参阅 [第 3.1 节“在 Slack 中配置传入的 Webhook”](#)。

2. 在 Hybrid Cloud Console 中，进入到 Settings > Integrations。
3. 选择 Communications 选项卡。
4. 点 Add integration。
5. 选择 Slack 作为集成类型，然后单击下一步。
6. 为集成输入一个名称（例如，*My Slack notification*）。
7. 将您从 Slack 复制的 Slack Webhook URL 粘贴到 Workspace URL 字段，然后单击 Next。
8. 要启用集成，请查看集成详情，然后点 Submit。
9. 刷新集成页面，以显示列表中的 Slack 集成。您的 Slack 集成现在列在 Integrations > Communications 页面中。在 Last connection attempt 下，状态为 Ready 以显示连接可以从 Hybrid Cloud Console 接受通知。

验证

创建一个测试通知，以确认您已成功将 Slack 连接到混合云控制台：

1. 在 Integrations > Communications 页面上的 Slack 集成旁边，点选项图标(&&)并点 Test。
2. 在 Integration Test 屏幕中，输入消息并点 Send。如果字段留空，则 Hybrid Cloud Console 会发送默认消息。
3. 打开您配置的 Slack 频道，并检查从 Hybrid Cloud Console 发送的消息。
4. 在 Hybrid Cloud Console 中，进入 Notifications > Event Log，检查 Integration: Slack 事件是否列出了带有绿色标签。

其他资源

- 有关设置通知管理员权限的更多信息，请参阅通知文档中的 [配置用户访问来管理通知](#)。

3.3. 为 SLACK 集成创建行为组

行为组定义了当通知服务收到特定事件时，哪些通知将发送到外部服务，如 Slack。您可以将任何红帽混合云控制台服务中的事件链接到您的行为组。

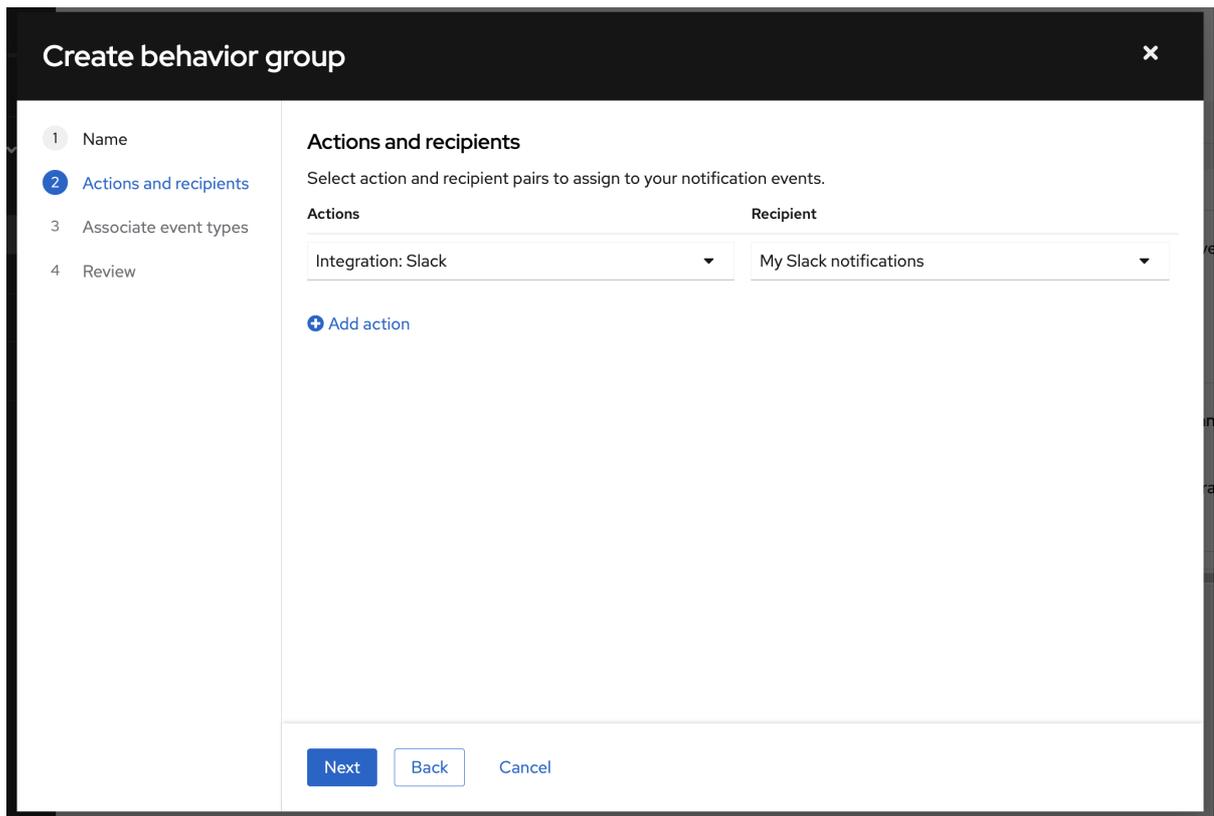
先决条件

- 以机构管理员或具有通知管理员权限的用户身份登录到 Hybrid Cloud Console。
- 您已配置了 Slack 集成。

流程

1. 在 Hybrid Cloud Console 中，进入到 [Settings > Notifications](#)。

2. 在通知下，选择 Configure Events。
3. 选择您要为其配置事件通知行为的应用程序捆绑包选项卡：Red Hat Enterprise Linux Console 或 OpenShift。
4. 点 Behavior Groups 选项卡。
5. 点 Create new group 打开 Create behavior group 向导。
6. 输入行为组的名称，然后点 Next。
7. 在 Actions 和 Recipients 步骤中，从 Actions 下拉列表中选择 Integration: Slack。
8. 从 Recipient 下拉列表中选择您创建的集成的名称（如 *My Slack notifications*），然后单击 Next。



9. 在 关联事件类型 步骤中，选择要发送通知的一个或多个事件（如 Policies: Policy triggered），然后单击 Next。
10. 查看您的行为组设置并点 完成。新行为组在 Notifications 页面中列出。



注意

您可以创建并编辑多个行为组，使其包含通知服务支持的任何其他平台。

11. 选择 Settings > Integrations 并点 Communications 选项卡。当 Slack 集成准备好将事件发送到 Slack 时，Last connection attempt 列会显示 Ready。如果通知成功到达 Slack，则 Last connection attempt 列会显示 Success。

Name	Type	Last connection...	Enabled
> My Google Chat notifications	Google Chat	Success	Enabled
> My Slack notifications	Slack	Success	Enabled

验证

1. 创建将触发混合云控制台通知的事件。例如，在将触发策略事件的系统中运行 `insights-client`。
2. 等待几分钟，然后进入 Slack。
3. 在 Slack 频道中，检查来自 Hybrid Cloud 控制台的通知。
4. 在 Hybrid Cloud Console 中，进入 Settings > Notifications > Event Log，并检查显示标签 Integration: Slack 的事件。
 - 如果标签为绿色，则通知成功。
 - 如果标签为红色，则可能需要调整集成。
5. 如果集成无法正常工作，请验证在 Slack 中已正确创建了传入的 Webhook 连接器，并在 Hybrid Cloud Console 集成配置中添加了正确的传入的 Webhook URL。



注意

如需了解更多详细信息，请参阅通知文档中的[对事件日志和集成设置进行故障排除](#)。

3.4. 其他资源

- 有关 Slack 配置的详情，请参考 Slack [文档中的使用传入 Webhook 发送信息](#)。
- 有关行为组的更多信息，请参阅[配置混合云控制台通知行为组](#)。
- 有关对 Slack 集成进行故障排除的信息，请参阅[混合云控制台集成故障排除](#)。

第 4 章 将 EVENT-DRIVEN ANSIBLE 与 RED HAT HYBRID CLOUD CONSOLE 集成

您可以使用 Event-Driven Ansible 利用 Red Hat Insights 等混合云控制台功能，以持续分析您的清单以了解潜在问题和^{建议}。event-Driven Ansible 通过规则将事件源与相应的操作连接。

与混合云控制台通知服务集成使用 Event-Driven Ansible 来触发操作。每个帐户配置接收这些事件的方式以及谁，可以根据事件类型执行操作。

联系支持

如果您有与 Event-Driven Ansible 集成的混合云控制台的问题，请联系红帽获得支持。您可以通过点 Help (? icon) > Open a case, 或从 ? > Support options 查看更多选项，直接从混合云控制台打开红帽支持问题单。

4.1. 配置 EVENT-DRIVEN ANSIBLE 以与红帽混合云控制台集成

您可以配置 Event-Driven Ansible，以接收来自 Red Hat Hybrid Cloud Console 或第三方应用程序的事件通知。

先决条件

- **ansible-rulebook CLI 已安装。** 具体步骤请参阅 [Ansible 规则手册安装](#)。
- 您有机构管理员或通知混合云控制台的管理员权限。

流程

1. 将您的环境连接到 Red Hat Ansible Automation Hub :

- 在 Hybrid Cloud Console 中，进入到 [Ansible Automation Platform > Connect to Hub](#)
- 在离线令牌下，在下复制字符串将在 30 天不活跃后过期。定期运行以下命令防止您的令牌过期。
- 在终端窗口中，粘贴您在上一步中复制的字符串。

2. 输入以下命令为 Event-Driven Ansible 安装 Red Hat Insights 集合 :

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

3. 要安装 Red Hat Insights 要求，请以 root 用户身份输入以下命令 :

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

4. 输入以下命令并验证输出中是否包含 **redhat.insights_eda** :

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

这个命令的输出示例 :

```
# /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. 使用文本编辑器创建一个 YAML 文件，其中包含使用 Red Hat Insights 集合的简单 Ansible 规则手册。例如，使用以下内容创建一个名为 `simple-rulebook.yaml` 的文件：

```
---
- 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 }}"
```

这个简单 `playbook` 使用 `redhat.insights_eda.insights` 集合作为源。如果定义了带有 `payload` 的事件，则 `event.payload` 的内容将显示为输出。

规则手册公开了用于接收事件并与混合云控制台通信的端点。有关 Red Hat Insights Advisor、Compliance 和 Vulnerability 服务的更多高级示例，请参阅 [Ansible Automation Hub](#) 中的 [Event-Driven Ansible for Red Hat Insights](#) 文档。

6. 创建包含关联 `playbook` 的 YAML 文件。例如，创建一个名为 `inventory.yaml` 的文件，其中包含一个简单的清单：

```
all:
```

7. 运行 `ansible-rulebook` 命令，以启动 Event-Driven Ansible 侦听器来侦听新事件。在以下示例中，这个命令会在默认端口 5000 上公开您的 `localhost`：

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

8. 在一个单独的终端窗口中运行 `curl` 命令，以验证您的 Event-Driven Ansible 侦听程序是否已正确配置，例如：

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

在本例中，如果配置正确，则 EDA 侦听器窗口中会出现一个新信息，其内容如下：

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

9. 在 Hybrid Cloud Console 中，进入到 `Settings > Integrations`。
10. 选择 `Reporting & Automation` 选项卡。
11. 点 `Add integration`。
12. 选择 `Event-Driven Ansible` 作为集成类型，然后单击 `Next`。

- 在 Integration name 字段中，输入您的集成名称（如 *My EDA Integration*）。
- 在 Endpoint URL 字段中输入您在 Ansible rulebook 中配置的 URL。这是指向 Event-Driven Ansible 侦听器的端点。



注意

Endpoint URL 必须包含 `http://` 或 `https://`，如 `https://<eda_hostname>:5000/endpoint`。

如有必要，请要求您的组织的安全管理员配置红帽混合云控制台的访问权限。

- 可选：如果配置了 Secret 令牌。



注意

secret 令牌对于保护发送到集成端点的数据至关重要，在将 Hybrid Cloud Console 与第三方应用程序集成时应始终使用。

- 点击 Next。
- 检查集成详情，然后点 Submit 以启用集成。

您的 Event-Driven Ansible 集成现在在 Integrations > Reporting & Automation 页面中列出。在 Last connection attempt 下，状态为 Ready 以显示连接可以接受控制台的通知。

验证

创建一个测试通知，以确认您已将 Event-Driven Ansible 连接到混合云控制台：

- 在 Integrations > Reporting & Automation 页面上的 Event-Driven Ansible 集成旁边，点选项图标(HBAC)并点 Test。
- 在 Integration Test 屏幕中，输入消息并点 Send。如果字段留空，则 Hybrid Cloud Console 会发送默认消息。
- 在 Event-Driven Ansible 侦听器终端中，检查从 Hybrid Cloud Console 发送的消息。
- 在 Hybrid Cloud Console 中，进入 Notifications > Event Log 并检查 Integration: Event-Driven Ansible 事件是否列出了绿色标签。

其他资源

- 有关设置通知管理员权限的更多信息，请参阅配置用户访问 [以在 Red Hat Hybrid Cloud Console 中配置通知 中的 配置 用户访问权限](#)。
- 如需了解更多 Event-Driven Ansible 配置信息和 Red Hat Insights 规则手册示例，请参阅 [Ansible Automation Hub Collections](#) 页中的 insights_eda 集合中的 Documentation 选项卡。

4.2. 为 EVENT-DRIVEN ANSIBLE 集成创建行为组

当通知服务收到特定事件时，行为组定义哪些通知将发送到外部服务，如 Event-Driven Ansible。您可以将任何红帽混合云控制台服务中的事件链接到您的行为组。

先决条件

- 以机构管理员或具有通知管理员权限的用户身份登录到 Hybrid Cloud Console。
- 配置 Event-Driven Ansible 与混合云控制台的集成。有关配置 Event-Driven Ansible 集成的信息，请参阅第 4.1 节“配置 Event-Driven Ansible 以与红帽混合云控制台集成”。

流程

1. 在 Hybrid Cloud Console 中，进入到 [Settings > Notifications](#)。
2. 在通知下，选择 Configure Events。
3. 选择您要为其配置事件通知行为的应用程序捆绑包选项卡：Red Hat Enterprise Linux Console 或 OpenShift。
4. 点 Behavior Groups 选项卡。
5. 点 Create new group 打开 Create behavior group 向导。
6. 输入行为组的名称，然后点 Next。
7. 在 Actions 和 Recipients 步骤中，从 Actions 下拉列表中选择 Integration: Event-Driven Ansible。
8. 从 Recipient 下拉列表中，选择您创建的集成的名称（例如，My EDA Listener），然后单击 Next。
9. 在 关联事件类型 步骤中，选择要发送通知的一个或多个事件（例如：Advisor: New recommendations），然后点 Next。
10. 查看您的行为组设置，然后点 Finish。新行为组会出现在 Notifications 页面中。

验证

1. 创建将触发混合云控制台通知的事件。如需示例，请参阅 [Ansible Automation Hub 页面](#)。
2. 要测试混合云控制台集成是否成功，在 Hybrid Cloud Console 中进入 Settings > Notifications > Event Log，并检查显示标签 Integration: Event-Driven Ansible 的事件。

Event	Application	Actions 	Date ... 
Detected Malware	Malware - Red Hat Enterprise Linux	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid green; border-radius: 5px; padding: 2px 5px; display: inline-block;">Integration: Event-Driven Ansible</div> <div style="border: 1px solid green; border-radius: 5px; padding: 2px 5px; display: inline-block;">Integration: ServiceNow</div> <div style="border: 1px solid green; border-radius: 5px; padding: 2px 5px; display: inline-block;">Integration: Splunk</div> <div style="border: 1px solid green; border-radius: 5px; padding: 2px 5px; display: inline-block;">Email</div> <div style="border: 1px solid green; border-radius: 5px; padding: 2px 5px; display: inline-block;">Integration: Webhook</div> <div style="color: blue; font-size: small;">Show Less</div> </div>	3 minutes ago

- 如果标签为绿色，则通知成功。
- 如果标签是 red，请验证 webhook 是否已正确创建并公开在 Event-Driven Ansible 中，并在 Hybrid Cloud Console 集成配置中配置了正确的 Webhook URL。



注意

如需了解更多详细信息，请参阅通知文档中的[对事件日志和集成设置进行故障排除](#)。

4.3. 其他资源

- 有关 Event-Driven Ansible 的更多信息，请参阅 [Event-Driven Ansible 指南](#)。
- 有关如何配置和使用 Event-Driven Ansible 控制器的详情，请参考 [Event-Driven Ansible 控制器用户指南](#)。
- 有关行为组的更多信息，请参阅[配置混合云控制台通知行为组](#)。
- 如需配置示例，请参阅 Red Hat Ansible 博客中的 [Red Hat Insights Collection for Event-Driven Ansible](#) 和 [使用 Red Hat Insights 作为 Event-Driven Ansible 自动化的事件源](#)。
- 有关对 Event-Driven Ansible 集成进行故障排除的信息，请参阅 [混合云控制台集成故障排除](#)。

第 5 章 将 MICROSOFT 团队与混合云控制台集成

您可以配置 Red Hat Hybrid Cloud Console，将事件通知发送到 Microsoft 团队中新或现有频道上的所有用户。Microsoft Teams 集成支持来自混合云控制台中所有服务的事件。Microsoft Teams 集成使用传入的 Webhook 接收事件数据。

联系支持

如果您在将混合云控制台与 Microsoft 团队集成有疑问，请联系红帽支持。您可以通过点 Help (? icon) > Open a case, 或从 ? > Support options 查看更多选项，直接从混合云控制台打开红帽支持问题单。

Microsoft 将不提供故障排除。红帽完全支持混合云控制台与 Microsoft 团队的集成。

5.1. 配置 MICROSOFT 团队以与混合云控制台集成

您可以使用传入的 Webhook 来配置 Microsoft 团队，以接收来自 Red Hat Hybrid Cloud Console 或第三方应用程序的事件通知。

先决条件

- 您有 Microsoft Teams 的 admin 权限。
- 具有混合云控制台的机构管理员或通知管理员权限。

流程

1. 在 Microsoft Teams 中创建新频道或选择现有频道。
2. 导航到 Apps 并搜索 Incoming Webhook 应用程序。
3. 选择 Incoming Webhook 应用程序，再单击 Add to a team。
4. 选择团队或频道名称并点 Set up a connector。
5. 输入传入 Webhook 的名称（例如，*红帽通知*）。此名称会出现在 Microsoft Teams 频道通过这个传入 webhook 从 Red Hat Hybrid Cloud Console 接收的所有通知中。
6. 可选：上传与传入 Webhook 名称关联的镜像。此镜像会出现在 Microsoft Teams 频道通过此传入 Webhook 从混合云控制台接收的所有通知中。
7. 点 Create 以完成创建并显示 Webhook URL。
8. 将 URL 复制到您的剪贴板。您需要 URL 在混合云控制台中配置通知。
9. 点 Done。Microsoft Teams 页面显示频道和传入的 Webhook。
10. 在 Hybrid Cloud Console 中，进入到 Settings > Integrations。
11. 点 Communications 选项卡。
12. 点 Add integration。
13. 选择 Microsoft Office Teams 作为集成类型，然后单击下一步。
14. 在 Integration name 字段中，输入您的集成名称（如 *console-teams*）。

15. 将您从 Microsoft Teams 复制的传入 Webhook URL 粘贴到 Endpoint URL 字段中。
16. 点击 Next。
17. 检查集成详情并点 Submit 来启用集成。

您的 Microsoft Teams 集成现在在 Integrations > Communications 页面中列出。在 Last connection attempt 下，状态为 Ready 以显示连接可以接受控制台的通知。

验证

创建一个测试通知，以确认您已将 Microsoft 团队正确连接到混合云控制台：

1. 在 Integrations > Communications 页面上的 Microsoft Teams 集成旁边，点选项图标（需要）并点 Test。
2. 在 Integration Test 屏幕中，输入消息并点 Send。如果字段留空，则 Hybrid Cloud Console 会发送默认消息。
3. 打开 Microsoft Teams 频道，并检查从混合云控制台发送的消息。
4. 在 Hybrid Cloud Console 中，进入 Notifications > Event Log 并检查 Integration: Microsoft Teams 事件是否列出了绿色标签。

其他资源

- 有关设置通知管理员权限的更多信息，请参阅通知文档中的 [配置用户访问来管理通知](#)。

5.2. 为 MICROSOFT 团队集成创建行为组

当通知服务收到特定事件时，行为组定义哪些通知将发送到外部服务，如 Microsoft 团队。您可以将任何红帽混合云控制台服务中的事件链接到您的行为组。有关行为组的更多信息，[请参阅配置混合云控制台通知行为组](#)。

先决条件

- 以机构管理员或具有通知管理员权限的用户身份登录到 Hybrid Cloud Console。
- Microsoft Teams 集成已配置。有关配置 Microsoft 团队集成的详情，请参考 [第 5.1 节“配置 Microsoft 团队以与混合云控制台集成”](#)。

流程

1. 在 Hybrid Cloud Console 中，进入到 [Settings > Notifications](#)。
2. 在 通知 下，选择 Configure Events。
3. 选择您要为其配置事件通知行为的应用程序捆绑包选项卡：Red Hat Enterprise Linux、Console 或 OpenShift。
4. 点 Behavior Groups 选项卡。
5. 点 Create new group 打开 Create behavior group 向导。
6. 输入行为组的名称，然后点 Next。

7. 在 Actions 和 Recipients 步骤中，从 Actions 下拉列表中选择 Integration: Microsoft Teams。
8. 在 Recipient 下拉列表中选择您创建的集成名称（如 `console-teams`），然后点 Next。
9. 在 关联事件类型 步骤中，选择要发送通知的一个或多个事件（例如，策略：Policy 触发），然后单击 Next。
10. 查看您的行为组设置，然后点 Finish。新行为组会出现在 Notifications 页面中。

验证

1. 创建将触发混合云控制台通知的事件。例如，在将触发策略事件的系统中运行 `insights-client`。
2. 等待几分钟，然后导航到 Microsoft Teams。
3. 从左侧菜单中选择您配置的频道。如果设置过程成功，页面会显示来自 Hybrid Cloud Console 的通知。通知包含触发事件的主机的名称，以及打开相应混合云控制台服务的事件数和链接。
4. 在 Hybrid Cloud Console 中，进入 Settings > Notifications > Event Log 并检查一个显示标签 Integration: Microsoft Teams 的事件。
 - 如果标签为绿色，则通知成功。
 - 如果标签是 red，请验证 Microsoft 团队中已正确创建了传入的 Webhook 连接器，并在 Hybrid Cloud Console 集成配置中添加了正确的传入的 Webhook URL。



注意

如需了解更多详细信息，请参阅[通知文档中的对事件日志和集成设置进行故障排除](#)。

5.3. 其他资源

- 有关对 Microsoft 团队集成进行故障排除的信息，请参阅[混合云控制台集成故障排除](#)。
- 如需有关 Webhook 的更多信息，请参阅 Microsoft 团队文档中的[Incoming Webhook](#)和[Webhooks](#)和[Connectors](#)。

第 6 章 将 GOOGLE CHAT 与 RED HAT HYBRID CLOUD CONSOLE 集成

您可以配置 Red Hat Hybrid Cloud Console，将事件通知发送到 Google Chat 中的新或现有 Google 空间。Google Chat 集成支持所有混合云控制台服务的事件。

与混合云控制台通知服务集成使用传入的 Webhook 来接收事件数据。每个红帽帐户都配置如何和谁接收这些事件，并根据事件类型执行操作。

联系支持

如果您对 Hybrid Cloud Console 与 Google Chat 集成的问题，请联系红帽获得支持。您可以通过点 Help > Open a case，或者从 Help > Support 选项中查看更多选项，直接从 Hybrid Cloud Console 打开 Red Hat 支持问题单。

Google 不提供故障排除。红帽完全支持 Hybrid Cloud Console 与 Google Chat。

6.1. 在 GOOGLE CHAT 中配置传入的 WEBHOOK

在 Google 空间中，创建一个新的 webhook 来与混合云控制台连接。

先决条件

- 在 Google Chat 中已有新的或现有的 Google 空间。

流程

1. 在 Google 空间中，点空格名称上的箭头打开下拉菜单：
 - a. 选择 Apps & Integrations。
 - b. 单击 Webhooks。
2. 在 Incoming webhook 对话框中输入以下信息：
 - a. 输入集成的名称（例如，工程师 *Google Chat*）。
 - b. 可选：要为通知添加 avatar，请输入镜像的 URL。
 - c. 点 Save 生成 Webhook URL。
 - d. 复制用于在混合云控制台中配置的 Webhook URL。

其他资源

- 如需了解更多与 [Google Chat 配置](#) 相关的信息，请参阅 [Google Chat 文档](#) 中的向带有传入 Webhook 的 Google Chat 发送消息。

6.2. 在 RED HAT HYBRID CLOUD CONSOLE 中配置 GOOGLE CHAT 集成

使用 Google Chat 中的 Webhook URL 在混合云控制台中创建一个新的集成。

先决条件

- 以机构管理员或具有通知管理员权限的用户身份登录到 Hybrid Cloud Console。

- 您有一个 Google Chat incoming Webhook。

流程

1. 在 Hybrid Cloud Console 中，进入到 Settings > Integrations。
2. 选择 Communications 选项卡。
3. 点 Add integration。
4. 选择 Google Chat 作为集成类型，然后单击 Next。
5. 在 Integration name 字段中，输入您的集成名称（如 *console-gchat*）。
6. 将从 Google 空间复制的传入 webhook URL 粘贴到 Endpoint URL 字段中，然后点 Next。
7. 检查集成详情并点 Submit 来启用集成。

您的 Google Chat 集成现在在 Integrations > Communications 页面中列出。在 Last connection attempt 下，状态为 Ready 以显示连接可以接受控制台的通知。

验证

创建一个测试通知，以确认您已将 Google Chat 连接到混合云控制台：

1. 在 Integrations > Communications 页面上的 Google Chat integration 旁边，点选项图标 (HBAC) 并点 Test。
2. 在 Integration Test 屏幕中，输入消息并点 Send。如果字段留空，则 Hybrid Cloud Console 会发送默认消息。
3. 打开 Google 空间，并检查从 Hybrid Cloud Console 发送的消息。
4. 在 Hybrid Cloud Console 中，进入 Notifications > Event Log 并检查 Integration: Google Chat 事件是否列出了绿色标签。

其他资源

- 有关设置通知管理员权限的更多信息，请参阅通知文档中的 [配置用户访问来管理通知](#)。

6.3. 为 GOOGLE CHAT 集成创建行为组

当通知服务收到特定事件时，行为组定义哪些通知将发送到外部服务，如 Google Chat。您可以将任何红帽混合云控制台服务中的事件链接到您的行为组。

先决条件

- 以机构管理员或具有通知管理员权限的用户身份登录到 Hybrid Cloud Console。
- 您已配置了 Google Chat 集成。

流程

1. 在 Hybrid Cloud Console 中，进入到 [Settings > Notifications](#)。
2. 在 通知 下，选择 Configure Events。

3. 选择您要为其配置事件通知行为的应用程序捆绑包选项卡：Red Hat Enterprise Linux、Console 或 OpenShift。
4. 点 Behavior Groups 选项卡。
5. 点 Create new group 打开 Create behavior group 向导。
6. 输入行为组的名称并点 Next。
7. 在 Actions 和 Recipients 步骤中，从 Actions 下拉列表中选择 Integration: Google Chat。
8. 在 Recipient 下拉列表中选择您创建的集成名称（如 `console-gchat`），然后点 Next。
9. 在 关联事件类型 步骤中，选择要发送通知的一个或多个事件（例如，策略：Policy 触发），然后单击 Next。
10. 查看您的行为组设置，然后点 Finish。新行为组在 Notifications 页面中列出。

验证

1. 创建将触发混合云控制台通知的事件。例如，在将触发策略事件的系统中运行 `insights-client`。
2. 等待几分钟，然后进入到 Google Chat。
3. 在 Google Space 中，从 Hybrid Cloud Console 检查通知。
4. 在 Hybrid Cloud Console 中，进入 Settings > Notifications > Event Log，并检查一个显示标签 Integration: Google Chat 的事件。
 - 如果标签为绿色，则通知成功。
 - 如果标签为红色，则可能需要调整集成。
5. 如果集成没有按预期工作，请验证在 Google Chat 中已正确创建了传入的 Webhook 连接器，并在 Hybrid Cloud Console 集成配置中添加了正确的传入的 Webhook URL。



注意

如需了解更多详细信息，请参阅通知文档中的[对事件日志和集成设置进行故障排除](#)。

6.4. 其他资源

- 有关对 Google Chat 集成进行故障排除的详情，请参考[对混合云控制台集成进行故障排除](#)。
- 有关 Google Chat 配置的详情，请查看[Google Chat 文档中的传入 Webhook 文档](#)。
- 有关行为组的更多信息，请参阅[配置混合云控制台通知行为组](#)。

附录 A. 混合云控制台集成故障排除

如果您在将第三方应用程序与混合云控制台集成时遇到问题，请查看以下故障排除解决方案。

A.1. 对第三方集成和 RED HAT INSIGHTS 之间的连接问题进行故障排除

如果您在第三方应用程序和 Red Hat Insights 间遇到连接问题，请确保您的第三方应用程序接受来自以下红帽 IP 地址的传入请求：

- 23.20.194.86
- 23.22.242.238
- 54.147.218.140

其他资源

- 有关最新 IP 地址列表，请参阅 [用于访问 Red Hat Insights / Hybrid Cloud Console Integrations 和 Notifications 的防火墙配置](#)。

A.2. 混合云控制台与 SPLUNK 的集成故障排除

如果您的 Hybrid Cloud Console 与 Splunk 集成无法正常工作，请查看以下问题：

Splunk 不会从混合云控制台接收事件通知

Splunk 环境中的配置错误可能会导致 Splunk 无法从混合云控制台接收事件通知。

- 在 Splunk 中，确保全局设置下启用了 HTTP 事件收集器(HEC)。请参阅[启用 HEC 令牌](#)。
- 确保默认索引为 `redhatinsights`。
- 确保防火墙允许配置的 Splunk HEC 端口上的传入请求(Splunk Enterprise 的默认是 8088)，并且 Splunk 云的默认请求为 443。如果您的实例使用了 AWS，则允许任何端口 Splunk 可能需要。如需更多信息，请参阅 [Splunk Phantom 端口和端点](#)。

有关配置 Splunk HEC 端口的更多信息，请参阅 [Splunk Phantom 端口和端点](#)。

使用实时搜索时，无法点 Splunk 中的 Events 表中的链接

在 Splunk 中，如果您从 Events 表中的 Timestamp 字段中选择一个相对值，则您可以点击表中的任何显示的事件来显示包含受影响系统或策略信息的新标签页。

但是，如果您从 Timestamp 字段中选择一个实时值，则显示的事件在点击时不会响应。这是 Splunk 的一个限制。Splunk 建议避免点击实时事件来查看事件详情。

A.3. 混合云控制台与 SERVICENOW 的集成故障排除

如果 ServiceNow 没有从 Red Hat Hybrid Cloud Console 接收事件，请验证配置：

- 确保启用了 [Red Hat Hybrid Cloud Console](#) 中的集成，且类型为 `ServiceNow`。
- 确保 Red Hat Hybrid Cloud Console 中的集成具有正确的 URL。URL 应该以 `https://<instance.servicenow.com>/api/x_rhttp_rh_webhook/flow_templates_for_red_hat_insights` 开头。

- 确保在 ServiceNow 中定义了 `x_rhttp_rh_webhook.rest` 用户角色。否则，即使应用程序已正确安装，来自混合云控制台的通知将无法正常工作。
- 确保 `rh_insights_integration` ServiceNow 用户存在，并且已分配了 `x_rhttp_rh_webhook.rest` 角色。
- 如有必要，重置 `rh_insights_integration` ServiceNow 用户的密码，并重置 [Red Hat Hybrid Cloud Console](#) 集成中的用户密码。

其他资源

- 如需更多信息，请参阅链接：[使用事件日志和集成设置故障排除通知失败](#)。

A.4. 其他资源

- 如需更多信息，请参阅链接：[使用事件日志和集成设置故障排除通知失败](#)。

对红帽文档提供反馈

我们感谢您对我们文档的反馈。尽可能提供详细信息，以便可以解决您的请求。

先决条件

- 您有红帽帐户。
- 您已登录到您的红帽帐户。

流程

1. 要提供反馈，请点击以下链接：[Create Issue](#)
2. 在 Summary 文本框中描述问题或功能增强。
3. 在 Description 文本框中提供有关问题或功能增强的更多详细信息。
4. 如果您的红帽用户名没有自动显示在 Reporter 文本框中，请输入它。
5. 滚动到页面底部，然后单击 Create 按钮。创建文档问题并路由到适当的文档团队。

感谢您花时间来提供反馈。