Red Hat Advanced Cluster Security for Kubernetes 4.4

集成

集成 Red Hat Advanced Cluster Security for Kubernetes

Last Updated: 2024-06-28

Red Hat Advanced Cluster Security for Kubernetes 4.4 集成

集成 Red Hat Advanced Cluster Security for Kubernetes

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

本文档论述了如何在 Red Hat Advanced Cluster Security for Kubernetes 中配置通用集成，包括与镜像 registry、Slack、Pageruty、Dutyr、Duty、Dutt、JIRA、电子邮件和使用通用 Webhook 集成。

目录

第 1 章 与镜像 REGISTRY 集成

Red Hat Advanced Cluster Security for Kubernetes (RHACS)与各种镜像 registry 集成，以便您可以了解您的镜像并应用安全策略以供镜像使用。

与镜像 registry 集成时，您可以查看重要的镜像详情，如镜像创建日期和 Dockerfile 详情（包括镜像层）。

将 RHACS 与 registry 集成后，您可以扫描镜像、查看镜像组件，并在部署前或之后将安全策略应用到镜像。

注意

当您与镜像 registry 集成时，RHACS 不会扫描 registry 中的所有镜像。RHACS 仅在以下情况下扫描镜像：

- 在部署中使用镜像
- 使用 **roxctl** CLI 检查镜像
- 使用持续集成(CI)系统来强制执行安全策略

您可以将 RHACS 与主要镜像 registry 集成，包括：

- Amazon Elastic Container Registry (ECR)
- Docker Hub
- Google Container Registry (GCR)
- Google Artifact Registry
- IBM Cloud Container Registry (ICR)
- JFrog Artifactory
- Microsoft Azure Container Registry (ACR)
- Red Hat Quay
- 红帽容器 registry
- Sonatype Nexus
- 使用 Docker Registry HTTP API 的任何其他 registry

1.1. 自动配置

Red Hat Advanced Cluster Security for Kubernetes 包括与标准 registry 的默认集成，如 Docker Hub 和其他 registry。它还可以根据监控集群中发现的工件（如镜像 pull secret）自动配置集成。通常，您不需要手动配置 registry 集成。

重要

如果使用 GCR registry，Red Hat Advanced Cluster Security for Kubernetes 不会自动创建 registry 集成。

1.2. AMAZON ECR 集成

对于 Amazon ECR 集成，如果满足以下条件，Red Hat Advanced Cluster Security for Kubernetes 会自动生成 ECR registry 集成：

- 集群的云供应商是 AWS。
- 集群中的节点具有 Instance Identity and Access Management (IAM) 角色关联，且实例元数据服务在节点中可用。例如，当使用 Amazon Elastic Kubernetes Service (EKS) 来管理集群时，此角色被称为 EKS Node IAM 角色。
- Instance IAM 角色具有 IAM 策略，授予您要从中部署的 ECR registry 的访问权限。

如果满足列出的条件，Red Hat Advanced Cluster Security for Kubernetes 会监控从 ECR registry 拉取的部署，并为它们自动生成 ECR 集成。您可以在这些集成被自动生成后编辑它们。

1.3. 手动配置镜像 REGISTRY

如果使用 GCR，则必须手动创建镜像 registry 集成。

1.3.1. 手动配置 OpenShift Container Platform registry

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 OpenShift Container Platform 内置容器镜像 registry 集成。

前提条件

- 您需要一个用户名和密码才能通过 OpenShift Container Platform registry 进行身份验证。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Generic Docker Registry**。
3. 点 **New integration**。
4. 输入以下字段的详情：
   a. 集成名称 ：集成的名称。
   b. 端点 ：registry 的地址。
   c. 用户名和密码.。
5. 如果您在连接到 registry 时没有使用 TLS 证书，请选择 **Disable TLS 证书验证**（不安全）。
6. 选择 **Create integration without testing**来创建集成，而不测试到 registry 的连接。
7. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。

8. 选择 **Save**。

1.3.2. 手动配置 Amazon Elastic Container Registry

您可以使用 Red Hat Advanced Cluster Security for Kubernetes 手动创建和修改 Amazon Elastic Container Registry (ECR)集成。如果您要从 Amazon ECR 部署，则通常会自动生成 Amazon ECR registry 的集成。但是，您可能希望自行创建集成，以扫描部署外部的镜像。您还可以修改自动生成的集成的参数。例如，您可以更改自动生成的 Amazon ECR 集成使用的身份验证方法，以使用 AssumeRole 身份验证或其他授权模型。

重要

要擦除您对自动生成的 ECR 集成所做的更改，请删除集成和 Red Hat Advanced Cluster Security for Kubernetes，当您从 Amazon ECR 部署镜像时，使用自动生成的参数创建一个新的集成。

前提条件

- 您必须有一个 Amazon Identity and Access Management (IAM) 访问密钥 ID 和 secret 访问密钥。另外，您可以使用节点级别的 IAM 代理，如 **kiam** 或 **kube2iam**。
- 访问密钥必须具有 ECR 的读取访问权限。如需更多信息，请参阅如何创建 AWS 访问密钥？
- 如果您在 Amazon Elastic Kubernetes Service (EKS)中运行 Red Hat Advanced Cluster Security for Kubernetes，并希望与单独 Amazon 帐户的 ECR 集成，您必须首先在 ECR 中设置存储库策略声明。按照 设置存储库策略语句 和 **Actions** 中的说明，选择 Amazon ECR API 操作的以下范围：
  - ecr:BatchCheckLayerAvailability
  - ecr:BatchGetImage
  - ecr:DescribeImages
  - ecr:GetDownloadUrlForLayer
  - ecr:ListImages

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Amazon ECR**。
3. 点 **New integration**，或者点自动生成的集成之一打开它，然后点 **Edit**。
4. 输入或修改以下字段的详情：
   a. 更新存储的凭据 ：如果您在不更新密钥和密码等凭证的情况下修改集成，请清除此框。
   b. 集成名称 ：集成的名称。
   c. **Registry ID** ：registry 的 ID。
   d. 端点 ：registry 的地址。只有在为 Amazon ECR 使用私有虚拟私有云(VPC)端点时才需要这个值。选择 AssumeRole 选项时，不会启用此字段。

e. **Region**：registry 的区域，如 **us-west-1**。

5. 如果使用 IAM，请选择 **Use Container IAM role**。否则，清除 **Use Container IAM** 角色框并输入 **Access key ID** 和 **Secret access key**。

6. 如果使用 AssumeRole 身份验证，请选择 **Use AssumeRole** 并输入以下字段的详情：

   a. **AssumeRole ID** ：要假定的角色 ID。

   b. **AssumeRole External ID** （可选）：如果您使用带有 AssumeRole 的外部 ID，您可以在此处输入它。

7. 选择 **Create integration without testing** 来创建集成，而不测试到 registry 的连接。

8. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。

9. 选择 **Save**。

1.3.2.1. 将 assumerole 与 Amazon ECR 一起使用

您可以使用 AssumeRole 授予对 AWS 资源的访问权限，而无需手动配置每个用户的权限。取而代之，您可以定义具有所需权限的角色，以便授予用户访问权限来假定角色。**AssumeRole** 允许您授予、撤销或通常管理更精细的权限。

1.3.2.1.1. 使用容器 IAM 配置 AssumeRole

在 Red Hat Advanced Cluster Security for Kubernetes 中使用 AssumeRole 前，您必须首先配置它。

流程

1. 为您的 EKS 集群启用 IAM OIDC 供应商：

```
$ eksctl utils associate-iam-oidc-provider --cluster <cluster name> --approve
```

2. 为您的 EKS 集群创建一个 IAM 角色。

3. 将新创建的角色与服务帐户关联：

```
$ kubectl -n stackrox annotate sa central eks.amazonaws.com/role-
arn=arn:aws:iam::67890:role/<role-name>
```

4. 重启 Central 以应用更改。

```
$ kubectl -n stackrox delete pod -l app=central
```

5. 将角色分配给允许角色根据需要假设另一个角色的策略：

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "sts:AssumeRole",
         "Resource": "arn:aws:iam::<ecr-registry>:role/<assumerole-readonly>" (1)
```

```
        }
    ]
}
```

1 将 **<assumerole-readonly>** 替换为您要假定的角色。

6. 更新您要假设的角色的信任关系：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": [
     "arn:aws:iam::<ecr-registry>:role/<role-name>" 1
    ]
   },
   "Action": "sts:AssumeRole"
  }
 ]
}
```

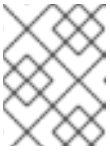
1 **<role-name>** 应该与之前创建的新角色匹配。

1.3.2.1.2. 在没有容器 IAM 的情况下配置 AssumeRole

要在没有容器 IAM 的情况下使用 AssumeRole，您必须使用访问和 secret 密钥以 AWS 用户身份进行身份验证，并具有编程访问。

流程

1. 根据 AssumeRole 用户与 ECR registry 位于同一个帐户中或在不同的帐户中，您必须：
   - 如果要假设角色的用户与 ECR registry 位于同一个帐户中，则创建带有所需权限的新角色。



注意

在创建角色时，您可以根据需要选择任何可信实体。但是，您必须在创建后修改它。

   - 或者，您必须提供访问 ECR registry 的权限，并在用户位于与 ECR registry 不同的帐户中时定义其信任关系：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ecr-registry>:role/<assumerole-readonly>" 1
```

```
        }
      ]
    }
```

1 将 **<assumerole-readonly>** 替换为您要假定的角色。

2. 通过在 **Principal** 字段中包含用户 ARN 来配置角色的信任关系：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<ecr-registry>:user/<role-name>"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

1.3.2.1.3. 在 RHACS 中配置 AssumeRole

在 ECR 中配置 AssumeRole 后，您可以使用 AssumeRole 将 Red Hat Advanced Cluster Security for Kubernetes 与 Amazon Elastic Container Registry (ECR)集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Amazon ECR**。
3. 单击 **New Integration**。
4. 输入以下字段的详情：
   a. 集成名称 ：集成的名称。
   b. **Registry ID** ：registry 的 ID。
   c. **Region**：registry 的区域，如 **us-west-1**。
5. 如果使用 IAM，请选择 **Use container IAM role**。否则，清除 **Use custom IAM** 角色框并输入 **Access key ID** 和 **Secret access key**。
6. 如果使用 AssumeRole，请选择 **Use AssumeRole**，并输入以下字段的详情：
   a. **AssumeRole ID** ：要假定的角色 ID。
   b. **AssumeRole External ID** （可选） ： 如果您使用带有 AssumeRole 的外部 ID，您可以在此处输入它。
7. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。

8. 选择 **Save**。

1.3.3. 手动配置 Google Container Registry

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 Google Container Registry (GCR)集成。

前提条件

- 您需要 工作负载身份 或服务帐户密钥进行身份验证。
- 关联的服务帐户必须有权访问 registry。有关授予用户和其他项目访问权限 GCR 的信息，请参阅配置访问控制。
- 如果使用 GCR Container Analysis，还必须将以下角色授予服务帐户：
  - 容器分析备注查看器
  - 容器分析 Occurrences Viewer
  - 存储对象查看器

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Google Container Registry**。
3. 点 **New integration**。
4. 输入以下字段的详情：
   a. **集成名称** ：集成的名称。
   b. **类型** ：选择 **Registry**。
   c. **注册表端点** ：registry 的地址。
   d. **项目** ：Google Cloud 项目名称。
   e. **使用工作负载身份** ：检查以使用工作负载身份进行身份验证。
   f. **服务帐户密钥(JSON)** ：用于身份验证的服务帐户密钥。
5. 选择 **Create integration without testing**来创建集成，而不测试到 registry 的连接。
6. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。
7. 选择 **Save**。

1.3.4. 手动配置 Google Artifact Registry

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 Google Artifact Registry 集成。

前提条件

- 您需要 工作负载身份 或服务帐户密钥进行身份验证。
- 关联的服务帐户必须具有 **Artifact Registry Reader** Identity and Access Management (IAM)角色 **roles/artifactregistry.reader**。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Google Artifact Registry**。
3. 点 **New integration**。
4. 输入以下字段的详情：
   a. **集成名称** ：集成的名称。
   b. **Registry 端点** ： registry 的地址。
   c. **项目** ：Google Cloud 项目名称。
   d. **使用工作负载身份** ：检查以使用工作负载身份进行身份验证。
   e. **服务帐户密钥(JSON)** ：用于身份验证的服务帐户密钥。
5. 选择 **Create integration without testing** 来创建集成，而不测试到 registry 的连接。
6. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。
7. 选择 **Save**。

1.3.5. 手动配置 Microsoft Azure Container Registry

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 Microsoft Azure Container Registry 集成。

前提条件

- 您必须有一个用户名和密码才能进行身份验证。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Microsoft Azure Container Registry**。
3. 点 **New integration**。
4. 输入以下字段的详情：
   a. **集成名称** ：集成的名称。
   b. **端点** ：registry 的地址。
   c. **用户名和密码**.。
5. 选择 **Create integration without testing** 来创建集成，而不测试到 registry 的连接。

6. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。
7. 选择 **Save**。

1.3.6. 手动配置 JFrog Artifactory

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 JFrog Artifactory 集成。

前提条件

- 您必须有一个使用 JFrog Artifactory 进行身份验证的用户名和密码。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **JFrog Artifactory**。
3. 点 **New integration**。
4. 输入以下字段的详情：
   a. 集成名称 ：集成的名称。
   b. 端点 ：registry 的地址。
   c. 用户名和密码.。
5. 如果您在连接到 registry 时没有使用 TLS 证书，请选择 **Disable TLS 证书验证**（不安全）。
6. 选择 **Create integration without testing**来创建集成，而不测试到 registry 的连接。
7. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。
8. 选择 **Save**。

1.3.7. 手动配置 Quay Container Registry

您可以将 Red Hat Advanced Cluster Security for Kubernetes (RHACS)与 Quay Container Registry 集成。您可以使用以下方法与 Quay 集成：

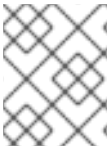
- 与 Quay 公共存储库(registry)集成：此方法不需要身份验证。
- 使用机器人帐户与 Quay 私有 registry 集成：此方法要求您创建机器人帐户以用于 Quay （推荐）。如需更多信息，请参阅 Quay 文档。
- 与 Quay 集成以使用 Quay 扫描程序而不是 RHACS 扫描程序：此方法使用 API，且需要 OAuth 令牌进行身份验证。请参阅"添加资源"部分中的"与 Quay Container Registry 集成以扫描镜像"。

前提条件

- 若要通过 Quay 私有注册表进行身份验证，您需要与机器人帐户或 OAuth 令牌关联的凭据（已弃用）。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Red Hat Quay.io**。
3. 点 **New integration**。
4. 输入集成名称。
5. 输入 **Endpoint**，或者输入 registry 的地址。
   a. 如果您要与 Quay 公共存储库集成，在 **Type** 下选择 **Registry**，然后进入下一步。
   b. 如果您要与 Quay 私有 registry 集成，在 **Type** 下选择 **Registry** 并在以下字段中输入信息：
      - **机器人 用户名** ：如果您使用 Quay 机器人帐户访问 registry，请输入用户名，格式为 ***<namespace>+<accountname>***。
      - **机器人 密码** ：如果您使用 Quay 机器人帐户访问 registry，请输入机器人帐户用户名的密码。
      - **OAuth 令牌** ：如果您使用 OAuth 令牌（已弃用）访问 registry，请在此字段中输入它。
6. 可选：如果您在连接到 registry 时没有使用 TLS 证书，请选择 **Disable TLS 证书验证**（不安全）。
7. 可选： 要在不测试的情况下创建集成，请选择 **Create integration without testing**。
8. 选择 **Save**。



注意

如果您要编辑 Quay 集成，但不想更新您的凭证，请验证没有选择 **Update stored credentials**。

1.4. 其他资源

- 与 Quay Container Registry 集成以扫描镜像

1.4.1. 手动配置 IBM Cloud Container Registry

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 IBM Cloud Container Registry 集成。

前提条件

- 您必须有一个 API 密钥用于使用 IBM Cloud Container Registry 进行身份验证。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **IBM Cloud Container Registry**。
3. 点 **New integration**。
4. 输入以下字段的详情：

a. 集成名称 ：集成的名称。

b. 端点 ：registry 的地址。

c. API 密钥.

5. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。
6. 选择 **Save**。

1.4.2. 手动配置 Red Hat Container Registry

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 Red Hat Container Registry 集成。

前提条件

- 您必须有一个用户名和密码才能通过 Red Hat Container Registry 进行身份验证。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integrations** 部分下，选择 **Red Hat Registry**。
3. 点 **New integration**。
4. 输入以下字段的详情：

a. 集成名称 ：集成的名称。

b. 端点 ：registry 的地址。

c. 用户名和密码.。

5. 选择 **Create integration without testing** 来创建集成，而不测试到 registry 的连接。
6. 选择 **Test** 来测试与所选 registry 的集成是否正常工作。
7. 选择 **Save**。

第 2 章 与 CI 系统集成

Red Hat Advanced Cluster Security for Kubernetes (RHACS)与各种持续集成(CI)产品集成。在部署镜像前，您可以使用 RHACS 将构建时间和部署时安全规则应用到您的镜像。

构建并推送到 registry 后，RHACS 集成到 CI 管道中。首先推送镜像可让开发人员在处理任何策略违反情况时继续测试其工件，同时处理任何其他 CI 测试失败、linter violations 或其他问题。

如果可能，将版本控制系统配置为阻止在构建阶段（包括 RHACS 检查）失败时的拉取或合并请求。

通过联系 RHACS 安装来与您的 CI 产品集成，以检查镜像是否符合您配置的构建时间策略。如果有策略违反情况，控制台日志中会显示一个详细的信息，包括策略描述、比例和补救说明。

每个策略都包括一个可选的强制设置。如果您为构建时间强制标记策略，则该策略失败会导致客户端以非零错误代码退出。

要将 Red Hat Advanced Cluster Security for Kubernetes 与 CI 系统集成，请按照以下步骤执行：

1. 配置构建策略。
2. 配置 registry 集成。
3. 配置对 RHACS 实例的访问。
4. 与 CI 管道集成。

2.1. 配置构建策略

您可以在构建期间检查 RHACS 策略。

流程

1. 配置适用于容器生命周期的构建时间的策略。
2. 与在构建期间推送到的 registry 集成。

其他资源

与镜像 registry 集成

2.1.1. 检查现有的构建时间策略

使用 RHACS 门户检查您在 Red Hat Advanced Cluster Security for Kubernetes 中配置的任何现有构建时间策略。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 使用全局搜索搜索 **Lifecycle Stage:Build**。

2.1.2. 创建新系统策略

除了使用默认策略外，您还可以在 Red Hat Advanced Cluster Security for Kubernetes 中创建自定义策略。

流程

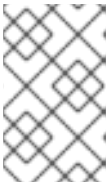
1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 单击 **+ New Policy**。
3. 输入策略的 **Name**。
4. 选择策略的严重性级别：Critical, High, Medium, 或 Low。
5. 选择适用于策略的生命周期阶段，**Build**, **Deploy**, 或 **Runtime**。您可以选择多个阶段。

注意

如果您为与 CI 系统创建新策略，请选择 **Build** 作为生命周期阶段。

- 构建时策略适用于镜像字段，如 CVE 和 Dockerfile 指令。
- Deployment-time 策略可以包含所有构建时策略标准。它们也可以具有来自集群配置的数据，如以特权模式运行或挂载 Docker 守护进程套接字。
- 运行时策略可以包含所有构建时间和部署时间策略标准，以及运行时期间进程执行的数据。

6. 在 **Description**,**Rationale**, 和 **Remediation** 字段中输入有关策略的信息。当 CI 验证构建时，将显示这些字段中的数据。因此，包含解释该策略的所有信息。
7. 从 **Categories** 下拉菜单中选择类别。
8. 从 通知下拉菜单中选择通知程序，该下拉菜单在出现违反此策略时接收警报通知。



注意

您必须将 RHACS 与通知供应商（如 Webhook、JIRA 或 PagerDuty）集成，才能接收警报通知。只有在您使用 RHACS 集成任何通知供应商时，才会显示通知程序。

9. 使用 **Restrict to Scope** 仅为特定集群、命名空间或标签启用此策略。您可以添加多个范围，还可在 RE2 语法中使用正则表达式进行命名空间和标签。
10. 使用 **Exclude by Scope** 来排除部署、集群、命名空间和标签。此字段表示策略不适用于您指定的实体。您可以添加多个范围，还可在 RE2 语法中使用正则表达式进行命名空间和标签。但是，您无法使用正则表达式来选择部署。
11. 对于 **Excluded Images** （仅限**Build Lifecycle**），请从您不想为其触发违反的列表中选择所有镜像。

注意

Excluded Images (Build Lifecycle only) 设置仅在检查持续集成系统中的镜像（构建生命周期阶段）时才适用。如果您使用此策略检查运行部署(Deploy 生命周期阶段)或运行时活动(Runtime 生命周期阶段)，则它无效。

12. 在 **Policy Criteria** 部分中，配置将触发该策略的属性。
13. 在面板标头中选择 **Next**。

14. 新策略面板显示在启用策略时触发的违反情况的预览。

15. 在面板标头中选择 **Next**。

16. 选择策略的强制行为。强制设置仅适用于您为 **Lifecycle Stages** 选项选择的阶段。选择 **ON** 强制执行策略并报告违反情况。选择 **OFF** 只报告违反情况。

注意

每个生命周期阶段的强制行为都有所不同。

- 对于 **Build** 阶段，当镜像与策略条件匹配时，RHACS 将无法进行 CI 构建。
- 对于 **Deploy** 阶段，如果 RHACS 准入控制器配置并运行，RHACS 会阻止创建和更新与策略条件匹配的部署。
    - 在带有准入控制器强制的集群中，Kubernetes 或 OpenShift Container Platform API 服务器会阻止所有不合规的部署。在其他集群中，RHACS 编辑不合规部署，以防止调度 pod。
    - 对于现有部署，策略更改仅在发生 Kubernetes 事件时在下次检测条件时导致强制。有关强制的更多信息，请参阅"部署阶段的安全策略强制"。
- 对于 **Runtime** 阶段，RHACS 会停止与策略条件匹配的所有 pod。

警告

策略实施可能会影响运行应用程序或开发流程。在启用强制选项前，请通知所有利益相关者，并计划如何响应自动强制操作。

2.1.2.1. 部署阶段的安全策略强制

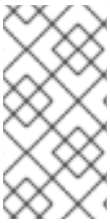
Red Hat Advanced Cluster Security for Kubernetes 支持两种类型的安全策略强制进行部署时间策略强制：通过准入控制器和 RHACS Sensor 的软强制进行硬强制。准入控制器会阻止创建或更新违反策略的部署。如果准入控制器被禁用或不可用，则 Sensor 可以通过将违反策略部署到 **0** 的部署来缩减副本来执行强制。

警告

策略实施可能会影响运行应用程序或开发流程。在启用强制选项前，请通知所有利益相关者，并计划如何响应自动强制操作。

2.1.2.1.1. 硬强制

硬强制由 RHACS 准入控制器执行。在带有准入控制器强制的集群中，Kubernetes 或 OpenShift Container Platform API 服务器会阻止所有不合规的部署。准入控制器会阻止 **CREATE** 和 **UPDATE** 操作。任何满足启用了 deploy-time 强制配置的策略的 pod 创建或更新请求都将失败。



注意

Kubernetes 准入 webhook 仅支持 **CREATE**、**UPDATE**、**DELETE** 或 **CONNECT** 操作。RHACS 准入控制器只支持 **CREATE** 和 **UPDATE** 操作。**kubectl patch**、**kubectl set** 和 **kubectl scale** 等操作是 PATCH 操作，而不是 UPDATE 操作。因为 Kubernetes 不支持 PATCH 操作，所以 RHACS 无法对 PATCH 操作执行强制。

要进行阻塞，您必须在 RHACS 中为集群启用以下设置：

- 在 **Object Creates** 上强制 ：此切换在 **Dynamic Configuration** 部分中，控制准入控制服务的行为。您必须在打开的 **Static Configuration** 部分中具有 **Configure Admission Controller Webhook** 来侦听 **Object Creates** 开关才能正常工作。
- 在对象更新上强制 ：此切换在 **Dynamic Configuration** 部分中，控制准入控制服务的行为。您必须在打开的 **Static Configuration** 部分中具有 **Configure Admission Controller Webhook** 来侦听 **Object Updates** 切换。

如果您对 **Static Configuration** 设置进行了更改，您必须重新部署安全集群才能使这些更改生效。

2.1.2.1.2. 软强制

软强制由 RHACS Sensor 执行。这个强制可防止启动操作。使用软强制时，Sensor 将副本扩展到 0，并阻止调度 pod。在这个强制中，集群中提供了非就绪的部署。

如果配置了软强制，且 Sensor 停机，则 RHACS 无法执行强制。

2.1.2.1.3. 命名空间排除

默认情况下，RHACS 从强制阻止中排除某些管理命名空间，如 **stackrox**、**kube-system** 和 **istio-system** 命名空间。这样做的原因是，必须部署这些命名空间中的一些项目才能使 RHACS 正常工作。

2.1.2.1.4. 对现有部署的强制

对于现有部署，策略更改仅在发生 Kubernetes 事件时在下次检测条件时导致强制。如果对策略进行更改，您必须通过选择 **Policy Management** 并点 **Reassess All** 来重新评估策略。此操作会在所有现有部署中应用部署策略，无论是否有新的传入的 Kubernetes 事件。如果违反了策略，则 RHACS 执行强制。

其他资源

- 使用准入控制器强制

2.2. 配置 REGISTRY 集成

要扫描镜像，您必须提供 Red Hat Advanced Cluster Security for Kubernetes，以访问您在构建管道中使用的镜像 registry。

2.2.1. 检查现有的 registry 集成

您可以使用 RHACS 门户检查是否已与 registry 集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **Image Integration** 部分下，查找突出显示的 **Registry** 标题。此标题还列出已为该标题配置的项目数量。

如果没有突出显示 Registry 标题，您必须首先与镜像 registry 集成。

2.2.1.1. 其他资源

- 与镜像 registry 集成

2.3. 配置访问

RHACS 提供 **roxctl** 命令行界面(CLI)，以便可以轻松地将 RHACS 策略集成到构建管道中。**roxctl** CLI 会输出有关问题的详细信息以及如何修复它们，以便开发人员可以在容器生命周期的早期阶段维护高标准。

要安全地对 Red Hat Advanced Cluster Security for Kubernetes API 服务器进行身份验证，您必须创建一个 API 令牌。

2.3.1. 导出并保存 API 令牌

流程

1. 生成身份验证令牌后，输入以下命令将其导出为 **ROX_API_TOKEN** 变量：

```
$ export ROX_API_TOKEN=<api_token>
```

2. （可选）：您还可以将令牌保存到文件中，并通过输入以下命令将其与 **--token-file** 选项一起使用：

```
$ roxctl central debug dump --token-file <token_file>
```

请注意以下信息：

- 您不能同时使用 **-password** (**-p**) 和 **--token-file** 选项。
- 如果您已经设置了 **ROX_API_TOKEN** 变量，并指定 **--token-file** 选项，**roxctl** CLI 会使用指定的令牌文件进行身份验证。
- 如果您已经设置了 **ROX_API_TOKEN** 变量，并指定 **--password** 选项，**roxctl** CLI 将使用指定的密码进行身份验证。

2.3.2. 通过下载二进制文件安装 roxctl CLI

您可以安装 **roxctl** CLI，以便使用命令行界面与 Red Hat Advanced Cluster Security for Kubernetes 交互。您可以在 Linux、Windows 或 macOS 上安装 **roxctl**。

2.3.2.1. 在 Linux 中安装 roxctl CLI

您可以按照以下流程在 Linux 上安装 **roxctl** CLI 二进制文件。

注意

用于 Linux 的 **roxctl** CLI 可用于 **amd64**、 **ppc64le** 和 **s390x** 架构。

流程

1. 确定目标操作系统的 **roxctl** 架构：

```
$ arch="$(uname -m | sed "s/x86_64//")"; arch="${arch:+-$arch}"
```

2. 下载 **roxctl** CLI：

```
$ curl -f -o roxctl "https://mirror.openshift.com/pub/rhacs/assets/4.4.3/bin/Linux/roxctl${arch}"
```

3. 使 **roxctl** 二进制文件可执行：

```
$ chmod +x roxctl
```

4. 将 **roxctl** 二进制文件放到 **PATH** 中的目录中：
要查看您的 **PATH**，请执行以下命令：

```
$ echo $PATH
```

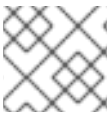
验证

- 验证您已安装的 **roxctl** 版本：

```
$ roxctl version
```

2.3.2.2. 在 macOS 上安装 roxctl CLI

您可以按照以下流程在 macOS 中安装 **roxctl** CLI 二进制文件。



注意

用于 macOS 的 **roxctl** CLI 可用于 **amd64** 架构。

流程

1. 下载 **roxctl** CLI：

```
$ curl -f -O https://mirror.openshift.com/pub/rhacs/assets/4.4.3/bin/Darwin/roxctl
```

2. 从二进制文件中删除所有扩展属性：

```
$ xattr -c roxctl
```

3. 使 **roxctl** 二进制文件可执行：

```
$ chmod +x roxctl
```

4. 将 **roxctl** 二进制文件放到 **PATH** 中的目录中：
要查看您的 **PATH**，请执行以下命令：

```
$ echo $PATH
```

验证

- 验证您已安装的 **roxctl** 版本：

```
$ roxctl version
```

2.3.2.3. 在 Windows 上安装 roxctl CLI

您可以按照以下流程在 Windows 上安装 **roxctl** CLI 二进制文件。

注意

amd64 架构提供了适用于 Windows 的 **roxctl** CLI。

流程

- 下载 **roxctl** CLI：

```
$ curl -f -O https://mirror.openshift.com/pub/rhacs/assets/4.4.3/bin/Windows/roxctl.exe
```

验证

- 验证您已安装的 **roxctl** 版本：

```
$ roxctl version
```

2.3.3. 从容器运行 roxctl CLI

roxctl 客户端是 RHACS **roxctl** 镜像的默认入口点。在容器镜像中运行 **roxctl** 客户端：

先决条件

- 您必须首先从 RHACS 门户生成身份验证令牌。

流程

1. 登录到 **registry.redhat.io** registry。

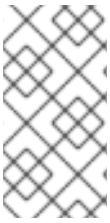
```
$ docker login registry.redhat.io
```

2. 为 **roxctl** CLI 拉取最新的容器镜像。

```
$ docker pull registry.redhat.io/advanced-cluster-security/rhacs-roxctl-rhel8:4.4.3
```

安装 CLI 后，您可以使用以下命令运行它：

```
$ docker run -e ROX_API_TOKEN=$ROX_API_TOKEN \
  -it registry.redhat.io/advanced-cluster-security/rhacs-roxctl-rhel8:4.4.3 \
  -e $ROX_CENTRAL_ADDRESS <command>
```



注意

在 Red Hat Advanced Cluster Security Cloud Service (RHACS Cloud Service)中，在使用需要 Central 地址的 **roxctl** 命令时，请使用 Red Hat Hybrid Cloud Console 的 **Instance Details** 部分显示的 **Central** 实例地址。例如，使用 **acs-ABCD12345.acs.rhcloud.com** 而不是 **acs-data-ABCD12345.acs.rhcloud.com**。

验证

- 验证您已安装的 **roxctl** 版本。

```
$ docker run -it registry.redhat.io/advanced-cluster-security/rhacs-roxctl-rhel8:4.4.3 version
```

2.4. 与 CI 管道集成

完成这些步骤后，下一步是与 CI 管道集成。

每个 CI 系统可能需要配置稍有不同。

2.4.1. 使用 Jenkins

使用 StackRox Container Image Scanner Jenkins 插件与 Jenkins 集成。您可以在 Jenkins 自由风格的项目和管道中使用此插件。

2.4.2. 使用 CircleCI

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 CircleCI 集成。

前提条件

- 您有对 **Image** 资源的 **read** 和 **write** 权限的令牌。
- 您有一个 Docker Hub 帐户的用户名和密码。

流程

1. 登录 CircleCI，再打开现有项目或创建新项目。
2. 单击 **Project Settings**。
3. 点 **环境变量**。
4. 点 **Add 变量** 并创建以下三个环境变量：
   - 名称 ：**STACKROX_CENTRAL_HOST** - Central 的 DNS 名称或 IP 地址。
   - 名称 ：**ROX_API_TOKEN** - 访问 Red Hat Advanced Cluster Security for Kubernetes 的 API 令牌。

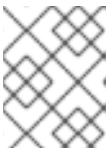
- 名称 ：**DOCKERHUB_PASSWORD** - Docker Hub 帐户的密码。
- 名称 ：**DOCKERHUB_USER** - Docker Hub 帐户的用户名。

5. 如果还没有 CircleCI 配置文件，请在您选择的项目的本地代码存储库的根目录中创建一个名为 **.circleci** 的目录。
6. 使用 **.circleci** 目录中的以下行创建 **config.yml** 配置文件：

```
version: 2
jobs:
  check-policy-compliance:
    docker:
      - image: 'circleci/node:latest'
        auth:
          username: $DOCKERHUB_USER
          password: $DOCKERHUB_PASSWORD
    steps:
      - checkout
      - run:
          name: Install roxctl
          command: |
            curl -H "Authorization: Bearer $ROX_API_TOKEN"
https://$STACKROX_CENTRAL_HOST:443/api/cli/download/roxctl-linux -o roxctl && chmod
+x ./roxctl
      - run:
          name: Scan images for policy deviations and vulnerabilities
          command: |
            ./roxctl image check --endpoint "$STACKROX_CENTRAL_HOST:443" --image "
<your_registry/repo/image_name>" 1
      - run:
          name: Scan deployment files for policy deviations
          command: |
            ./roxctl image check --endpoint "$STACKROX_CENTRAL_HOST:443" --image "
<your_deployment_file>" 2
            # Important note: This step assumes the YAML file you'd like to test is located in the
project.
workflows:
  version: 2
  build_and_test:
    jobs:
      - check-policy-compliance
```

1 将 **<your_registry/repo/image_name>** 替换为您的 registry 和镜像路径。

2 将 **<your_deployment_file>** 替换为部署文件的路径。



注意

如果您已在存储库中为 CircleCI 有一个 **config.yml** 文件，请在现有配置文件中添加一个带有指定详情的新 jobs 部分。

7. 将配置文件提交到存储库后，前往 CircleCI 仪表板中的 **Jobs** 队列，以验证构建策略强制。

第 3 章 与 PAGERDUTY 集成

如果使用 PagerDuty，您可以将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 PagerDuty。

以下步骤代表了将 Red Hat Advanced Cluster Security for Kubernetes 与 PagerDuty 集成的高级工作流：

1. 在 PagerDuty 中添加新的 API 服务并获取集成密钥。
2. 使用集成密钥在 Red Hat Advanced Cluster Security for Kubernetes 中设置通知。
3. 识别您要发送通知的策略，并更新这些策略的通知设置。

3.1. 配置 PAGERDUTY

通过创建新服务和获取集成密钥，开始与 PagerDuty 集成。

流程

1. 进入 **Configuration → Services**。
2. 选择 **Add Services**。
3. 在 **General Settings** 下，指定 **Name** 和 **Description**。
4. 在 **Integration Setting** 下，点 **Use our API Directly** 并为 **Integration Type** 下拉菜单选择 **Events v2 API**。
5. 在 **Incident Settings** 下，选择一个 **Escalation Policy**，并配置通知设置和事件超时。
6. 接受 **Incident Behavior** 和 **Alert Grouping** 的默认设置，或者根据需要进行配置。
7. 点 **Add Service**。
8. 在 **Service Details** 页面中，记录 **Integration Key**。

3.2. 为 KUBERNETES 配置 RED HAT ADVANCED CLUSTER SECURITY

使用集成密钥在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **PagerDuty**。
3. 点 **New Integration** (添加 图标)。
4. 输入 **Integration Name** 的名称。
5. 在 **PagerDuty** 集成键字段中，输入集成密钥。
6. 点 **Test** （**checkmark** 图标），以验证与 PagerDuty 的集成是否正常工作。

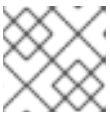
7. 点 **Create** (保存 图标)来创建配置。

3.3. 配置策略通知

为系统策略启用警报通知。

流程

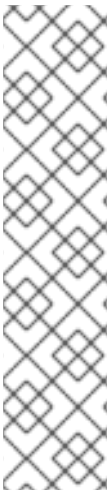
1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 PagerDuty notifier。



注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。



注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

第 4 章 与 SLACK 集成

如果使用 Slack，您可以将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 Slack。

以下步骤代表了将 Red Hat Advanced Cluster Security for Kubernetes 与 Slack 集成的高级工作流：

1. 创建新的 Slack 应用程序，启用传入的 Webhook，并获取 Webhook URL。
2. 使用 Webhook URL 将 Slack 与 Red Hat Advanced Cluster Security for Kubernetes 集成。
3. 识别您要发送通知的策略，并更新这些策略的通知设置。

4.1. 配置 SLACK

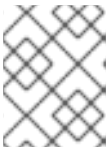
首先创建一个新的 Slack 应用程序，并获取 Webhook URL。

前提条件

1. 您需要管理员帐户或具有权限的用户帐户来创建 Webhook。

流程

1. 创建新的 Slack 应用程序：



注意

如果要使用现有的 Slack 应用程序，请访问 https://api.slack.com/apps 并选择应用程序。

   a. 转至 https://api.slack.com/apps/new。
   b. 输入 **App Name** 并选择 **Development Slack Workspace** 来安装应用程序。
   c. 点 **Create App**。

2. 在设置页面中的 **Basic Information** 部分，选择 **Incoming Webhooks**（在 **Add features and functionality** 下）。
3. 打开 **Activate Incoming Webhooks** 切换开关。
4. 选择 **Add New Webhook to Workspace**。
5. 选择一个应用程序将发布到的频道，然后选择 **Authorize**。页面会刷新，并返回到应用程序设置页面。
6. 复制位于您的 **Workspace** 部分的 **Webhook URL**。

如需更多信息，请参阅 Slack 文档，使用 Incoming Webhooks 开始。

4.1.1. 将警报发送到不同的 Slack 频道

您可以配置 Red Hat Advanced Cluster Security for Kubernetes 将通知发送到不同的 Slack 频道，以便直接进入正确的团队。

流程

1. 配置传入的 Webhook 后，在部署 YAML 文件中添加类似如下的注解：

```
example.com/slack-webhook:
https://hooks.slack.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX
```

2. 在配置 Red Hat Advanced Cluster Security for Kubernetes 时，在 **Label/Annotation Key for Slack Webhook** 字段中使用注解键 **example.com/slack-webhook**。

配置完成后，如果部署有您在 YAML 文件中配置的注解，Red Hat Advanced Cluster Security for Kubernetes 会将警报发送到您为该注解指定的 webhook URL。否则，它会将警报发送到默认的 Webhook URL。

4.2. 为 KUBERNETES 配置 RED HAT ADVANCED CLUSTER SECURITY

使用 webhook URL 在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Slack**。
3. 点 **New Integration** (添加 图标)。
4. 输入 **Integration Name** 的名称。
5. 在 **Default Slack Webhook** 字段中输入生成的 Webhook URL。
6. 选择 **Test** (勾选标记 图标)来测试与 Slack 的集成是否正常工作。
7. 选择 **Create** (**save** icon)来创建配置。

4.3. 配置策略通知

为系统策略启用警报通知。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 Slack notifier。

注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。

注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

第 5 章 使用通用 WEBHOOK 集成

使用 Red Hat Advanced Cluster Security for Kubernetes，您可以将警报通知作为 JSON 消息发送到任何 webhook 接收器。发生违反情况时，Red Hat Advanced Cluster Security for Kubernetes 在配置的 URL 上发出 HTTP POST 请求。POST 请求正文包含有关警报的 JSON 格式信息。

Webhook POST 请求的 JSON 数据包含 **v1.Alert** 对象和您配置的任何自定义字段，如下例所示：

```
{
  "alert": {
    "id": "<id>",
    "time": "<timestamp>",
    "policy": {
      "name": "<name>",
      ...
    },
    ...
  },
  "<custom_field_1>": "<custom_value_1>"
}
```

您可以创建多个 Webhook。例如，您可以创建一个 webhook 来接收所有审计日志，另一个 webhook 用于警报通知。

将 Red Hat Advanced Cluster Security for Kubernetes 的警报转发到任何 Webhook 接收器：

1. 设置用于接收警报的 webhook URL。
2. 使用 Webhook URL 在 Red Hat Advanced Cluster Security for Kubernetes 中设置通知。
3. 识别您要发送通知的策略，并更新这些策略的通知设置。

5.1. 使用 WEBHOOK 配置集成

使用 webhook URL 在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

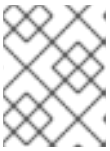
流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Generic Webhook**。
3. 点 **New integration**。
4. 输入 集成名称。
5. 在 **Endpoint** 字段中输入 Webhook URL。
6. 如果您的 webhook 接收器使用不可信证书，请在 **CA certificate** 字段中输入 CA 证书。否则，请将其留空。

注意

Webhook 接收器使用的服务器证书必须对端点 DNS 名称有效。您可以点 **跳过 TLS 验证** 来忽略这个验证。红帽不推荐关闭 TLS 验证。如果没有 TLS 验证，数据可以被意外的接收者拦截。

7. 可选：点 **Enable audit logging** 来接收有关 Red Hat Advanced Cluster Security for Kubernetes 中所有更改的警报。



注意

红帽建议将单独的 Webhook 用于警报和审计日志，以以不同的方式处理这些消息。

8. 要使用 webhook 接收器进行身份验证，请输入以下之一的详情：
   - 用于基本 HTTP 验证的用户名和密码
   - 自定义 **Header**，例如：**Authorization: Bearer <access_token>**
9. 使用 **Extra** 字段在 Red Hat Advanced Cluster Security for Kubernetes 发送的 JSON 对象中包含额外的键值对。例如，如果您的 webhook 接收器接受多个源的对象，您可以添加 **"source": "rhacs"** 作为额外字段，并过滤这个值来识别 Red Hat Advanced Cluster Security for Kubernetes 的所有警报。
10. 选择 **Test** 来发送测试消息，以验证与您的通用 Webhook 集成是否正常工作。
11. 选择 **Save** 以创建配置。

5.2. 配置策略通知

为系统策略启用警报通知。

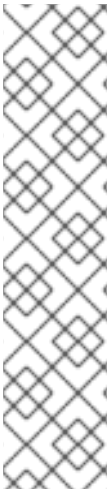
流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 Webhook 通知程序。

注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。



注意

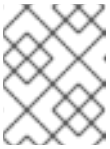
- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

第 6 章 与 QRADAR 集成

您可以通过在 RHACS 中配置通用 Webhook 集成，将 Red Hat Advanced Cluster Security for Kubernetes 配置为将事件发送到 QRadar。

以下步骤代表了将 RHACS 与 QRadar 集成的高级工作流：

1. 在 RHACS 中：
   a. 配置通用 Webhook。



注意

在 RHACS 中配置集成时，在 **Endpoint** 字段中使用以下示例作为指南：< **URL to QRadar Box>:<Port of Integration** >。

   b. 识别您要发送通知的策略，并更新这些策略的通知设置。

2. 如果 QRadar 没有自动检测日志源，请在 QRadar 控制台中添加 RHACS 日志源。有关配置 QRadar 和 RHACS 的更多信息，请参阅 Red Hat Advanced Cluster Security for Kubernetes IBM 资源。

6.1. 使用 WEBHOOK 配置集成

使用 webhook URL 在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

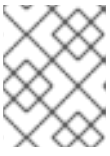
流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Generic Webhook**。
3. 点 **New integration**。
4. 输入 集成名称。
5. 在 **Endpoint** 字段中输入 Webhook URL。
6. 如果您的 webhook 接收器使用不可信证书，请在 **CA certificate** 字段中输入 CA 证书。否则，请将其留空。

注意

Webhook 接收器使用的服务器证书必须对端点 DNS 名称有效。您可以点 **跳过 TLS 验证** 来忽略这个验证。红帽不推荐关闭 TLS 验证。如果没有 TLS 验证，数据可以被意外的接收者拦截。

7. 可选：点 **Enable audit logging** 来接收有关 Red Hat Advanced Cluster Security for Kubernetes 中所有更改的警报。



注意

红帽建议将单独的 Webhook 用于警报和审计日志，以以不同的方式处理这些消息。

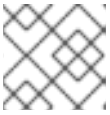
8. 要使用 webhook 接收器进行身份验证，请输入以下之一的详情：
   - 用于基本 HTTP 验证的用户名和密码
   - 自定义 **Header**，例如：**Authorization: Bearer <access_token>**
9. 使用 **Extra** 字段在 Red Hat Advanced Cluster Security for Kubernetes 发送的 JSON 对象中包含额外的键值对。例如，如果您的 webhook 接收器接受多个源的对象，您可以添加 **"source": "rhacs"** 作为额外字段，并过滤这个值来识别 Red Hat Advanced Cluster Security for Kubernetes 的所有警报。
10. 选择 **Test** 来发送测试消息，以验证与您的通用 Webhook 集成是否正常工作。
11. 选择 **Save** 以创建配置。

6.2. 配置策略通知

为系统策略启用警报通知。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 Webhook 通知程序。



注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。

注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

第 7 章 与 SERVICENOW 集成

您可以通过在 RHACS 中配置通用 Webhook 集成，将 Red Hat Advanced Cluster Security for Kubernetes 配置为将事件发送到 ServiceNow。

以下步骤代表了将 RHACS 与 ServiceNow 集成的高级工作流：

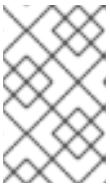
1. 在 ServiceNow 中，配置要在 RHACS 中使用的 REST API 端点。有关包含 ServiceNow 配置步骤的更多信息，请参阅 如何将 Red Hat Advanced Cluster Security for Kubernetes 与 ServiceNow 集成。
2. 在 RHACS 中：
   a. 配置通用 Webhook。
   b. 识别您要发送通知的策略，并更新这些策略的通知设置。

7.1. 使用 WEBHOOK 配置集成

使用 webhook URL 在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

流程

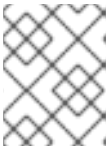
1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Generic Webhook**。
3. 点 **New integration**。
4. 输入 集成名称。
5. 在 **Endpoint** 字段中输入 Webhook URL。
6. 如果您的 webhook 接收器使用不可信证书，请在 **CA certificate** 字段中输入 CA 证书。否则，请将其留空。



注意

Webhook 接收器使用的服务器证书必须对端点 DNS 名称有效。您可以点 **跳过 TLS 验证** 来忽略这个验证。红帽不推荐关闭 TLS 验证。如果没有 TLS 验证，数据可以被意外的接收者拦截。

7. 可选：点 **Enable audit logging** 来接收有关 Red Hat Advanced Cluster Security for Kubernetes 中所有更改的警报。



注意

红帽建议将单独的 Webhook 用于警报和审计日志，以以不同的方式处理这些消息。

8. 要使用 webhook 接收器进行身份验证，请输入以下之一的详情：
   - 用于基本 HTTP 验证的用户名和密码
   - 自定义 **Header**，例如：**Authorization: Bearer <access_token>**

9. 使用 **Extra** 字段在 Red Hat Advanced Cluster Security for Kubernetes 发送的 JSON 对象中包含额外的键值对。例如，如果您的 webhook 接收器接受多个源的对象，您可以添加 **"source": "rhacs"** 作为额外字段，并过滤这个值来识别 Red Hat Advanced Cluster Security for Kubernetes 的所有警报。
10. 选择 **Test** 来发送测试消息，以验证与您的通用 Webhook 集成是否正常工作。
11. 选择 **Save** 以创建配置。

7.2. 配置策略通知

为系统策略启用警报通知。

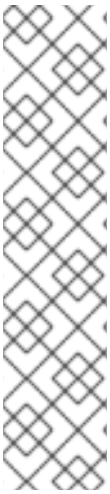
流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 Webhook 通知程序。

注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。



注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

第 8 章 与 SUMO 日志集成

如果使用 Sumo Logic，您可以将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 Sumo Logic。

以下步骤代表了将 Red Hat Advanced Cluster Security for Kubernetes 与 Sumo Logic 集成的高级工作流：

1. 在 Sumo Logic 中添加新的自定义应用程序，设置 HTTP 源，并获取 HTTP URL。
2. 使用 HTTP URL 将 Sumo Logic 与 Red Hat Advanced Cluster Security for Kubernetes 集成。
3. 识别您要发送通知的策略，并更新这些策略的通知设置。

8.1. 配置 SUMO 日志

使用 **Setup** 向导 设置 流数据 并获取 HTTP URL。

流程

1. 登录到您的 Sumo Logic Home 页面并选择 **Setup Wizard**。
2. 将光标移到 **Set Up Streaming Data** 并选择 **Get Started**。
3. 在 Select Data Type 页面中，选择您的自定义应用程序。
4. 在 Set Up Collection 页面中，选择 **HTTP Source**。
5. 输入 **Source Category** 的名称，例如 **rhacs**，然后单击 **Continue**。
6. 复制 生成的 URL。

8.2. 为 KUBERNETES 配置 RED HAT ADVANCED CLUSTER SECURITY

使用 HTTP URL 在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Sumo Logic**。
3. 点 **New Integration** (添加 图标)。
4. 输入 **Integration Name** 的名称。
5. 在 **HTTP Collector Source Address** 字段中输入生成的 HTTP URL。
6. 点 **Test** (**checkmark** 图标) 来测试与 Sumo Logic 的集成是否正常工作。
7. 点 **Create** (保存 图标)来创建配置。

8.3. 配置策略通知

为系统策略启用警报通知。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 Sumo Logic notifier。

注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。

注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

8.4. 在 SUMO LOGIC 中查看警报

您可以在 Sumo Logic 中查看 Red Hat Advanced Cluster Security for Kubernetes 中的警报。

1. 登录您的 Sumo Logic Home 页面，再单击 **Log Search**。
2. 在搜索框中，输入 **_sourceCategory=rhacs**。确保使用与您在配置 Sumo Logic 时输入的相同 **Source Category** 名称。
3. 选择时间，然后点 **Start**。

第 9 章 与 GOOGLE CLOUD STORAGE 集成

您可以与 Google Cloud Storage (GCS) 集成来启用数据备份。在出现基础架构灾难或出现被损坏的数据时，您可以使用这些备份进行数据恢复。与 GCS 集成后，您可以调度每天或每周备份，并进行按需备份。

备份包括 Red Hat Advanced Cluster Security for Kubernetes 整个数据库，其中包括所有配置、资源、事件和证书。确保备份安全存储。

注意

如果您使用 Red Hat Advanced Cluster Security for Kubernetes 版本 3.0.53 或更早版本，则备份不包括证书。

9.1. 为 KUBERNETES 配置 RED HAT ADVANCED CLUSTER SECURITY

要在 Google Cloud Storage (GCS)上配置数据备份，请在 Red Hat Advanced Cluster Security for Kubernetes 中创建集成。

前提条件

- 一个现有存储桶。要创建新存储桶，请参阅官方 Google Cloud Storage 文档中的 创建存储桶。
- 您要使用的存储桶中的 **Storage Object Admin** IAM 角色 的服务帐户。如需更多信息，请参阅使用云 IAM 权限。
- 服务帐户 的工作负载身份 或服务帐户密钥(JSON)。如需更多信息，请参阅创建服务帐户 和创建服务帐户密钥。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **External backups** 部分，然后选择 **Google Cloud Storage**。
3. 点 **New Integration** (添加 图标)。
4. 输入 **Integration Name** 的名称。
5. 在 **Backups To Retain** 框中输入要保留的备份数量。
6. 对于 **Schedule**，请选择备份频率（每天或每周）以及运行备份过程的时间。
7. 输入您要存储备份的 **Bucket** 名称。
8. 在使用工作负载身份时，请检查 **Use workload identity**。否则，在 **Service account key (JSON)** 字段中输入您的服务帐户密钥文件的内容。
9. 选择 **Test** （**checkmark** 图标）以确认与 GCS 的集成是否正常工作。
10. 选择 **Create** (**save** icon)来创建配置。

配置后，Red Hat Advanced Cluster Security for Kubernetes 根据指定的调度自动备份所有数据。

9.1.1. 在 Google Cloud Storage 上执行按需备份

使用 RHACS 门户在 Google Cloud Storage 上触发 Red Hat Advanced Cluster Security for Kubernetes 的手动备份。

前提条件

- 您必须已经将 Red Hat Advanced Cluster Security for Kubernetes 与 Google Cloud Storage 集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **External backups** 部分下，点 **Google Cloud Storage**。
3. 选择您要进行备份的 GCS 存储桶的集成名称。
4. 点 **Trigger Backup**。

注意

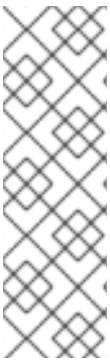
目前，当选择 **Trigger Backup** 选项时，没有通知。但是，Red Hat Advanced Cluster Security for Kubernetes 会在后台开始备份任务。

9.1.1.1. 其他资源

- 备份 Red Hat Advanced Cluster Security for Kubernetes
- 从备份中恢复

第 10 章 使用 SYSLOG 协议集成

Syslog 是一个事件日志协议，应用程序用来发送消息到中央位置，如 SIEM 或 syslog 收集器，用于数据保留和安全调查。使用 Red Hat Advanced Cluster Security for Kubernetes，您可以使用 syslog 协议发送警报和审计事件。



注意

- 使用 syslog 协议转发事件需要 Red Hat Advanced Cluster Security for Kubernetes 版本 3.0.52 或更新版本。
- 当使用 syslog 集成时，Red Hat Advanced Cluster Security for Kubernetes 会转发您配置和所有审计事件的违反警报。
- 目前，Red Hat Advanced Cluster Security for Kubernetes 只支持 **CEF** （通用事件格式）。

以下步骤代表了将 Red Hat Advanced Cluster Security for Kubernetes 与 syslog 事件接收器集成的高级别工作流：

1. 设置 syslog 事件接收器来接收警报。
2. 使用接收器的地址和端口号在 Red Hat Advanced Cluster Security for Kubernetes 中设置通知。

配置后，Red Hat Advanced Cluster Security for Kubernetes 会自动将所有违反和审计事件发送到配置的 syslog 接收器。

10.1. 配置与 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 的 SYSLOG 集成

在 Red Hat Advanced Cluster Security for Kubernetes (RHACS)中创建一个新的 syslog 集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Syslog**。
3. 点 **New Integration** （添加图标）。
4. 输入 **Integration Name** 的名称。
5. 在 **local0** 到 **local7** 中选择 **Logging Facility** 值。
6. 输入您的 **Receiver Host** address 和 **Receiver Port** number。
7. 如果使用 TLS，请打开 **Use TLS** 切换。
8. 如果您的 syslog 接收器使用不被信任的证书，请打开 **Disable TLS 证书验证(Insecure)** 切换。否则，请关闭此切换。
9. 点 **Add new extra** 字段添加额外的字段。例如，如果您的 syslog 接收器接受来自多个源的对象，在 **Key** 和 **Value** 字段中输入 **source** 和 **rhacs**。
   您可以使用 syslog 接收器中的自定义值过滤，以识别 RHACS 中的所有警报。

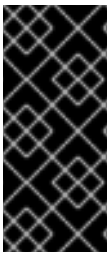
10. 选择 **Test** （**checkmark** 图标）来发送测试信息，以验证与您的通用 Webhook 集成是否正常工作。

11. 选择 **Create** (**save** icon)来创建配置。

第 11 章 与 AMAZON S3 集成

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 Amazon S3 集成，以启用数据备份。在出现基础架构灾难或损坏数据时，您可以使用这些备份进行数据恢复。与 Amazon S3 集成后，您可以调度每天或每周备份，并进行按需备份。

备份包括整个 Red Hat Advanced Cluster Security for Kubernetes 数据库，其中包括所有配置、资源、事件和证书。确保备份安全存储。



重要

- 如果您使用 Red Hat Advanced Cluster Security for Kubernetes 版本 3.0.53 或更早版本，则备份不包括证书。
- 如果您的 Amazon S3 是 air-gapped 环境的一部分，您必须将 AWS root CA 添加为 Red Hat Advanced Cluster Security for Kubernetes 中的 可信证书颁发机构。

11.1. 在 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 中配置 AMAZON S3 集成

要配置 Amazon S3 备份，请在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

前提条件

- 现有 S3 Bucket。要创建具有所需权限的新存储桶，请参阅 Amazon 文档创建存储桶。
- S3 存储桶的 **Read**, **write**, 和 **delete** 权限， **Access key ID**, 和 **Secret access key**。
- 如果您使用 **KIAM**、**kube2iam** 或另一个代理，则一个带有 **read**, **write**, 和 **delete** 权限的 **IAM** 角色。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration** → **Integrations**。
2. 向下滚动到 **External backups** 部分，再选择 **Amazon S3**。
3. 点 **New Integration** (添加 图标)。
4. 输入 **Integration Name** 的名称。
5. 在 **Backups To Retain** 框中输入要保留的备份数量。
6. 对于 **Schedule**，请选择每天或每周的备份频率，以及运行备份过程的时间。
7. 输入您要存储备份的 **Bucket** 名称。
8. （可选）如果要将备份保存在一个特定的文件夹结构中，输入对象前缀。如需更多信息，请参阅 Amazon 文档主题 使用对象元数据。
9. 如果使用非公共 S3 实例，请输入存储桶的端点，否则将其留空。
10. 输入存储桶的 **Region**。
11. 打开 **Use Container IAM Role** 切换，或者输入 **Access Key ID**，以及 **Secret Access Key**。

12. 选择 **Test** （**checkmark** 图标）以确认与 Amazon S3 的集成是否正常工作。
13. 选择 **Create** (**save** icon)来创建配置。

配置后，Red Hat Advanced Cluster Security for Kubernetes 根据指定的调度自动备份所有数据。

11.2. 在 AMAZON S3 上执行按需备份

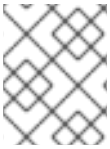
使用 RHACS 门户在 Amazon S3 上触发 Red Hat Advanced Cluster Security for Kubernetes 的手动备份。

前提条件

- 您必须已经将 Red Hat Advanced Cluster Security for Kubernetes 与 Amazon S3 集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 在 **External backups** 部分下，单击 **Amazon S3**。
3. 选择您要进行备份的 S3 存储桶的集成名称。
4. 点 **Trigger Backup**。



注意

目前，当选择 **Trigger Backup** 选项时，没有通知。但是，Red Hat Advanced Cluster Security for Kubernetes 会在后台开始备份任务。

11.3. 其他资源

- 备份 Red Hat Advanced Cluster Security for Kubernetes
- 从备份中恢复

第 12 章 与 GOOGLE CLOUD 安全命令中心集成

如果使用 Google Cloud Security Command Center（Cloud SCC），您可以将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 Cloud SCC。本指南说明了如何将 Red Hat Advanced Cluster Security for Kubernetes 与 Cloud SCC 集成。

以下步骤代表了将 Red Hat Advanced Cluster Security for Kubernetes 与 Cloud SCC 集成的高级工作流。

1. 使用 Google Cloud 注册新的安全源。
2. 为 Red Hat Advanced Cluster Security for Kubernetes 提供源 ID 和服务帐户密钥。
3. 识别您要发送通知的策略，并更新这些策略的通知设置。

12.1. CONFIGURING GOOGLE CLOUD SCC

首先，将 Red Hat Advanced Cluster Security for Kubernetes 添加为可信 Cloud SCC 源。

流程

1. 按照 Cloud Security Command Center 指南中的添加漏洞和威胁源，并添加 Red Hat Advanced Cluster Security for Kubernetes 作为可信 Cloud SCC 源。记录 Google Cloud 为 Red Hat Advanced Cluster Security for Kubernetes 集成创建的 **Source ID**。如果您在注册后没有看到源 ID，您可以在 Cloud SCC Security Sources 页面中找到 它。
2. 在上一步中为您创建的服务帐户或您所使用的现有帐户创建密钥。详情请参阅 Google Cloud 的指南中的创建和管理服务帐户密钥。

12.2. 配置 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 以与 GOOGLE CLOUD SCC 集成

您可以使用源 ID 和 Google 服务帐户在 Red Hat Advanced Cluster Security for Kubernetes 中创建新的 Google Cloud SCC 集成。

前提条件

- 在 机构级别带有 **Security Center Findings Editor** IAM 角色的服务帐户。如需更多信息，请参阅使用 IAM 的访问控制。
- 服务帐户 的工作负载身份 或服务帐户密钥(JSON)。如需更多信息，请参阅创建服务帐户 和创建服务帐户密钥。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration** → **Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Google Cloud SCC**。
3. 点 **New Integration** (添加 图标)。
4. 输入 **Integration Name** 的名称。
5. 输入 **Cloud SCC Source ID**。

6. 在使用工作负载身份时，请检查 **Use workload identity**。否则，在 **Service account key (JSON)** 字段中输入您的服务帐户密钥文件的内容。

7. 选择 **Create** (**save** icon)来创建配置。

12.3. 配置策略通知

为系统策略启用警报通知。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 Google Cloud SCC notifier。

注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。

注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

第 13 章 与 SPLUNK 集成

如果使用 Splunk，您可以将 Red Hat Advanced Cluster Security for Kubernetes 中的警报转发到 Splunk，并在 Splunk 中查看违反情况、漏洞检测和合规性数据。

重要

目前，IBM Power (**ppc64le**)和 IBM Z (**s390x**)不支持 Splunk 集成。

根据您的用例，您可以使用以下方法之一将 Red Hat Advanced Cluster Security for Kubernetes 与 Splunk 集成：

- 通过在 Splunk 中使用 HTTP 事件收集器 ：
  - 使用事件收集器选项转发警报和审计日志数据。
- 使用 Red Hat Advanced Cluster Security for Kubernetes 附加组件 ：
  - 使用附加组件将违反、漏洞检测和合规数据拉取到 Splunk 中。

您可以使用其中一个或两个集成选项将 Red Hat Advanced Cluster Security for Kubernetes 与 Splunk 集成。

13.1. 使用 HTTP 事件收集器

您可以使用 HTTP 事件收集器将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 Splunk。

要使用 HTTP 事件收集器将 Red Hat Advanced Cluster Security for Kubernetes 与 Splunk 集成，请按照以下步骤执行：

1. 在 Splunk 中添加新的 HTTP 事件收集器并获取令牌值。
2. 使用令牌值在 Red Hat Advanced Cluster Security for Kubernetes 中设置通知。
3. 识别您要发送通知的策略，并更新这些策略的通知设置。

13.1.1. 在 Splunk 中添加 HTTP 事件收集器

为您的 Splunk 实例添加新的 HTTP 事件收集器，并获取令牌。

流程

1. 在 Splunk 仪表板中，进入 **Settings → Add Data**。
2. 单击 **Monitor**。
3. 在 **Add Data** 页面上，单击 **HTTP Event Collector**。
4. 输入事件收集器的名称，然后点 **Next >**。
5. 接受默认的 **Input Settings** 并点 **Review >**。
6. 查看事件收集器属性并点 **Submit >**。

7. 复制事件 收集器的 **Token 值**。您需要此令牌值来配置与 Red Hat Advanced Cluster Security for Kubernetes 中的 Splunk 集成。

13.1.1.1. 启用 HTTP 事件收集器

您必须启用 HTTP 事件收集器令牌，然后才能接收事件。

流程

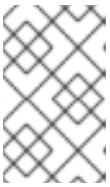
1. 在 Splunk 仪表板中，进入 **Settings → Data 输入**。
2. 单击 **HTTP Event Collector**。
3. 单击 **Global Settings**。
4. 在打开的对话框中，单击 **Enabled**，然后单击 **Save**。

13.1.2. 在 Red Hat Advanced Cluster Security for Kubernetes 中配置 Splunk 集成

使用令牌值在 Red Hat Advanced Cluster Security for Kubernetes 中创建一个新的 Splunk 集成。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 向下滚动到 **Notifier Integrations** 部分，然后选择 **Splunk**。
3. 点 **New Integration** (添加 图标)。
4. 输入 **Integration Name** 的名称。
5. 在 **HTTP Event Collector URL** 字段中输入您的 Splunk URL。如果对于 HTTPS 不是 **443**，对于 HTTP 不是 **80**，则需要指定一个端口号。您还必须在 URL 末尾添加 URL 路径 **/services/collector/event**。例如： **https://<mvapich-server-path>:8088/services/collector/event**。
6. 在 **HTTP Event Collector Token** 字段中输入您的令牌。



注意

如果您使用 Red Hat Advanced Cluster Security for Kubernetes 版本 3.0.57 或更新版本，您可以为 **Alert** 事件指定自定义 **Source Type**，为 审计事件指定 **Source Type**。

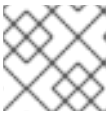
7. 选择 **Test** （**checkmark** 图标）来发送测试消息，以验证与 Splunk 的集成是否正常工作。
8. 选择 **Create** (**save** icon)来创建配置。

13.1.3. 配置策略通知

为系统策略启用警报通知。

流程

1. 在 RHACS 门户中，进入 **Platform Configuration → Policy Management**。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 **Bulk actions** 下，选择 **Enable notification**。
4. 在 **Enable notification** 窗口中，选择 Splunk notifier。



注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 **启用**。

注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

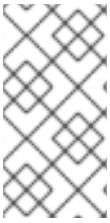
13.2. 使用 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 附加组件

您可以使用 Red Hat Advanced Cluster Security for Kubernetes 附加组件将漏洞检测和合规性相关数据从 Red Hat Advanced Cluster Security for Kubernetes 转发到 Splunk。

使用 Red Hat Advanced Cluster Security for Kubernetes 中所有资源 的读取权限 生成 API 令牌，然后使用该令牌安装和配置附加组件。

13.2.1. 安装和配置 Splunk 附加组件

您可以从 Splunk 实例安装 Red Hat Advanced Cluster Security for Kubernetes 附加组件。



注意

为了保持与 StackRox Kubernetes 安全平台附加组件的向后兼容性，配置的输入的 **source_type** 和 **input_type** 参数仍被称为 **stackrox_compliance**、**stackrox_violations**, 和 **stackrox_vulnerability_management**。

先决条件

- 您必须具有一个 API 令牌，其具有对 Red Hat Advanced Cluster Security for Kubernetes 的所有资源的 **read** 权限。您可以分配 **Analyst** 系统角色来授予此级别的访问权限。**Analyst** 角色具有所有资源的读取权限。

流程

1. 从 Splunkbase 下载 Red Hat Advanced Cluster Security for Kubernetes 附加组件。
2. 进入 Splunk 实例上的 Splunk 主页。
3. 进入 **Apps → Manage Apps**。
4. 选择 **Install app from file**。
5. 在 **Upload app** 弹出窗口中，选择 **Choose File** 并选择 Red Hat Advanced Cluster Security for Kubernetes 附加组件文件。
6. 点 **Upload**。
7. 点 **Restart Splunk**，并确认重启。
8. Splunk 重启后，从 **Apps** 菜单中选择 **Red Hat Advanced Cluster Security for Kubernetes**。
9. 进入 **Configuration**，然后点 **Add-on Settings**。
    a. 对于 **Central Endpoint**，输入 IP 地址或您的 Central 实例的名称。例如：**central.custom:443**。
    b. 输入您为附加组件生成的 **API** 令牌。
    c. 点击 **Save**。
10. 进入 **Inputs**。
11. 点 **Create New Input**，然后选择以下之一：
    - **ACS** 合规性数据。
    - **ACS Violations** 拉取违反数据。
    - **ACS Vulnerability Management** 拉取漏洞数据。
12. 输入输入 的名称。
13. 选择一个来自 Red Hat Advanced Cluster Security for Kubernetes 数据的间隔。例如，每 **14400** 秒。
14. 选择您要向其发送数据的 **Splunk Index**。
15. 对于 **Central Endpoint**，输入 **IP** 地址或您的 **Central** 实例的名称。
16. 输入您为附加组件生成的 **API** 令牌。
17. 点击 **Add**。

验证

- 要验证 **Red Hat Advanced Cluster Security for Kubernetes** 附加组件安装，请查询收到的数据。
    a. 在 **Splunk** 实例中，进入 **Search**，然后键入 **indexPROFILE sourcetype="stackrox ldapsearch"** 作为查询。

b. 按 Enter 键。

验证您配置的源是否在搜索结果中显示。

13.2.2. 更新 StackRox Kubernetes 安全平台附加组件

如果使用 StackRox Kubernetes Security Platform 附加组件，则必须升级到新的 Red Hat Advanced Cluster Security for Kubernetes 附加组件。

您可以在左侧的应用程序列表下看到 Splunk 主页上的更新通知。另外，您还可以进入 Apps → Manage apps 页面来查看更新通知。

先决条件

- 您必须具有一个 API 令牌，其具有对 Red Hat Advanced Cluster Security for Kubernetes 的所有资源的 **read** 权限。您可以分配 Analyst 系统角色来授予此级别的访问权限。Analyst 角色具有所有资源的读取权限。

流程

1. 在更新通知上点 Update。
2. 选中接受条款和条件的复选框，然后点 Accept and Continue 以安装更新。
3. 安装后，从 Apps 菜单中选择 Red Hat Advanced Cluster Security for Kubernetes。
4. 进入 Configuration，然后点 Add-on Settings。
   a. 输入您为附加组件生成的 API 令牌。
   b. 点击 Save。

13.2.3. 对 Splunk 附加组件进行故障排除

如果您停止从 Red Hat Advanced Cluster Security for Kubernetes 附加组件接收事件，请检查 Splunk 附加组件调试日志中的错误。

Splunk 为 **/opt/mvapich/var/log/mvapich** 目录中每个配置的输入创建一个调试日志文件。找到名为 **stackrox_<input>_<uid>.log** 的文件，例如 **stackrox_compliance_29a3e14798aa2363d.log** 并查找问题。

第 14 章 与镜像漏洞策略集成

Red Hat Advanced Cluster Security for Kubernetes (RHACS)与漏洞扫描程序集成，以便您导入容器镜像并将其监视是否有漏洞。

支持的容器镜像 registry

红帽支持以下容器镜像 registry：

- Amazon Elastic Container Registry (ECR)
- 通用 Docker registry （任何通用 Docker 或开放容器项目兼容镜像 registry，如 DockerHub、**gcr.io**、**mcr.microsoft.com**）
- Google Container Registry
- Google Artifact Registry
- IBM Cloud Container Registry
- JFrog Artifactory
- Microsoft Azure Container Registry (ACR)
- Red Hat Quay
- Red Hat registry (**registry.redhat.io**,**registry.access.redhat.com**)
- Sonatype Nexus

这种增强的支持为您提供了在首选 registry 中管理容器镜像的灵活性和选择。

支持的扫描器

您可以设置 RHACS 从以下商业容器镜像漏洞扫描程序中获取镜像漏洞数据：

RHACS 中包含的扫描程序

- 扫描程序 V4 （技术预览）：从 RHACS 版本 4.4 开始，引入了一个新的扫描程序，它基于 ClairCore 构建，同时还启用了 Clair 扫描程序。扫描程序 V4 支持扫描语言和特定于操作系统的镜像组件。您不必创建集成来使用此扫描程序，但您必须在安装过程中或安装后启用它。对于版本 4.4，如果启用此扫描程序，还必须启用 StackRox Scanner。有关 Scanner V4 的更多信息，包括安装文档的链接，请参阅关于 RHACS Scanner V4。

重要

扫描程序 V4 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

- stackrox Scanner：此扫描程序是 RHACS 中的默认扫描程序。它源自 Clair v2 开源扫描程序的分叉。如果启用了 Scanner V4，还必须启用此扫描程序来扫描 RHCOS 节点和平台漏洞，如 Red Hat OpenShift、Kubernetes 和 Istio。计划在以后的发行版本中对 Scanner V4 中的该功能的支持。

其他扫描程序

- Clair: 从版本 4.4 开始，您可以在 RHACS 中启用 Scanner V4，以提供 Clair V4 扫描程序提供的功能。但是，您可以通过配置集成将 Clair V4 配置为扫描程序。
- Google Container Analysis
- Red Hat Quay

重要

StackRox Scanner 与 Scanner V4 （可选）结合使用是与 RHACS 搭配使用的首选镜像漏洞扫描程序。有关使用 StackRox 扫描容器镜像和扫描器 V4 的更多信息，请参阅 扫描镜像。

如果您在 DevOps 工作流中使用这些替代扫描程序之一，您可以使用 RHACS 门户配置与漏洞扫描程序的集成。集成后，RHACS 门户会显示镜像漏洞，您可以轻松分类它们。

如果配置了多个扫描程序，RHACS 会尝试使用 non-StackRox/RHACS 和 Clair 扫描程序。如果这些扫描程序失败，RHACS 会尝试使用配置的 Clair 扫描程序。如果失败，RHACS 会尝试使用 Scanner V4 （如果已配置）。如果没有配置 Scanner V4，RHACS 会尝试使用 StackRox Scanner。

14.1. 与 CLAIR 集成

从版本 4.4 开始，Clair 扫描功能在新的 RHACS 扫描程序、Scanner V4 中提供，不需要单独集成。只有在使用 Clair V4 扫描程序时才需要本节中的说明。

重要

扫描程序 V4 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

请注意以下指导：

- 从 RHACS 3.74 开始，红帽弃用了以前的 CoreOS Clair 集成，并使用 Clair V4 集成。使用 Clair V4 Scanner 需要单独的集成。从版本 4.4 开始，如果您使用 Scanner V4，则不再需要此集成。
- 在下一个 RHACS 4.0 版本中，对 Clair V4 集成没有计划 支持基于 JWT 的身份验证选项。

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Integrations。
2. 在 Image Integrations 部分下，选择 Clair v4。
3. 点 New integration。
4. 输入以下字段的详情：
   a. 集成名称 ：集成的名称。
   b. 端点 ：扫描程序的地址。

5. （可选）如果您在连接到 registry 时没有使用 TLS 证书，请选择 Disable TLS 证书验证（不安全）。
6. （可选）点击 Test 来测试与所选 registry 的集成是否正常工作。
7. 点 Save。

14.2. 与 GOOGLE CONTAINER REGISTRY 集成

您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 Google Container Registry (GCR)集成，以进行容器分析和漏洞扫描。

前提条件

- 您必须具有 Google Container Registry 的服务帐户密钥。
- 关联的服务帐户可以访问 registry。有关授予用户和其他项目访问权限 GCR 的信息，请参阅配置访问控制。
- 如果使用 GCR Container Analysis，已将以下角色赋予服务帐户：
  - 容器分析备注查看器
  - 容器分析 Occurrences Viewer
  - 存储对象查看器

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Integrations。
2. 在 Image Integrations 部分下，选择 Google Container Registry。
   此时会打开 Configure image integration modal。
3. 单击 New Integration。
4. 输入以下字段的详情：
   a. 集成名称 ：集成的名称。
   b. 类型 ：选择 Scanner。
   c. 注册表端点 ：registry 的地址。
   d. 项目 ：Google Cloud 项目名称。
   e. 服务帐户密钥(JSON) 用于身份验证的服务帐户密钥。
5. 选择 Test （checkmark 图标）来测试与所选 registry 的集成是否正常工作。
6. 选择 Create (save icon)来创建配置。

14.3. 与 QUAY CONTAINER REGISTRY 集成以扫描镜像

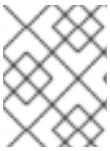
您可以将 Red Hat Advanced Cluster Security for Kubernetes 与 Quay Container Registry 集成来扫描镜像。

前提条件

- 您必须具有 OAuth 令牌才能通过 Quay Container Registry 进行身份验证才能扫描镜像。

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Integrations。
2. 在 Image Integrations 部分下，选择 Red Hat Quay.io。
3. 点 New integration。
4. 输入集成名称。
5. 在 Type 下，选择 Scanner。（如果您也与 registry 集成，请选择 Scanner + Registry。）在以下字段中输入信息：
   - 端点 ：输入 registry 的地址。
   - OAuth 令牌 ：输入 RHACS 使用 API 进行身份验证的 OAuth 令牌。
   - 可选： Robot username：如果要配置 Scanner + Registry 并使用 Quay 机器机器帐户访问 registry，以 Quay robot account, enter the user name in the format ***<namespace>+<accountname>*** 格式输入用户名。
   - 可选： Robot password ：如果您要配置 Scanner + Registry，并使用 Quay 机器机器帐户访问 registry，请输入机器人帐户用户名的密码。
6. 可选：如果您在连接到 registry 时没有使用 TLS 证书，请选择 Disable TLS 证书验证（不安全）。
7. 可选： 要在不测试的情况下创建集成，请选择 Create integration without testing。
8. 选择 Save。



注意

如果您要编辑 Quay 集成，但不想更新您的凭证，请验证没有选择 Update stored credentials。

第 15 章 与 JIRA 集成

如果使用 JIRA，您可以将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 JIRA。

以下步骤代表了将 Red Hat Advanced Cluster Security for Kubernetes 与 JIRA 集成的高级工作流：

1. 在 JIRA 中设置用户。
2. 使用 JIRA URL、用户名和密码将 JIRA 与 Red Hat Advanced Cluster Security for Kubernetes 集成。
3. 识别您要发送通知的策略，并更新这些策略的通知设置。

15.1. 配置 JIRA

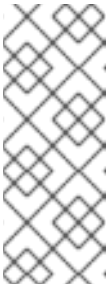
首先创建新用户，并分配适当的角色和权限。

前提条件

- 您需要一个带有权限的 Jira 帐户来创建和编辑您要集成的项目中的问题。

流程

- 在 JIRA 中创建一个用户，它有权访问您要为其创建问题的项目：
  - 要创建新用户，请参阅 JIRA 文档 创建、编辑或删除用户。
  - 要授予用户项目角色和应用程序的访问权限，请参阅 JIRA 文档主题将用户分配给组、项目角色和应用程序。



注意

如果使用 JIRA Software Cloud，在创建用户后，必须为该用户创建令牌：

1. 进入 https://id.atlassian.com/manage/api-tokens，以生成新的令牌。
2. 在配置 Red Hat Advanced Cluster Security for Kubernetes 时，使用令牌作为密码。

15.2. 为 KUBERNETES 配置 RED HAT ADVANCED CLUSTER SECURITY

使用 JIRA 服务器 URL 和用户凭证在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Integrations。
2. 向下滚动到 Notifier Integrations 部分，然后选择 JIRA Software。
3. 单击 New Integration。
4. 输入 Integration Name 的名称。
5. 在 Username 和 Password 或 API Token 框中输入用户凭证。

6. 对于 Issue Type，请输入有效的 JIRA Issue Type，如 Task、sub-task 或 Bug。
7. 在 JIRA URL 框中输入 JIRA 服务器 URL。
8. 在 Default Project 框中输入您要在其中创建问题的项目密钥。
9. 使用 注解键 For Project 在不同的 JIRA 项目中创建问题。
10. 如果您在 JIRA 项目中使用自定义优先级，请使用 Priority Mapping 切换来配置自定义优先级。
11. 如果您在 JIRA 项目中使用强制自定义字段，请在 Default Fields JSON (Necessary If Required Fields) 框中输入它们作为 JSON 值。例如：

```
{
  "customfield_10004": 3,
  "customfield_20005": "Alerts",
}
```

12. 选择 Test (勾选标记 图标)来测试与 JIRA 的集成是否正常工作。
13. 选择 Create (save icon)来创建配置。

15.2.1. 在不同的 JIRA 项目中创建问题

您可以配置 Red Hat Advanced Cluster Security for Kubernetes 在不同的 JIRA 项目中造成问题，以便直接进入正确的团队。

前提条件

- 您必须有一个有权访问将警报发送到的每个项目的帐户。

流程

1. 在部署 YAML 文件中添加类似如下的注解：

```
jira/project-key: <jira_project_key>
```

2. 在配置 Red Hat Advanced Cluster Security for Kubernetes 时，在 Annotation Key For Project 字段中使用注解键 **jira/project-key**。

配置完成后，如果部署在 YAML 文件中有一个注解，Red Hat Advanced Cluster Security for Kubernetes 会将警报发送到为该注解指定的项目。否则，警报将发送到 default 项目。

15.2.2. 在 JIRA 中配置自定义优先级

如果您在 JIRA 项目中使用自定义优先级，您可以在 Red Hat Advanced Cluster Security for Kubernetes 中配置它们。

流程

1. 在 Red Hat Advanced Cluster Security for Kubernetes 中配置 JIRA 集成时，打开 优先级映射切换。Red Hat Advanced Cluster Security for Kubernetes 获取 JIRA 项目模式，并自动填写 CRITICAL_SEVERITY、HIGH_SEVERITY、MEDIUM_SEVERITY 和 LOW_SEVERITY 字段的值。

2. 根据您的 JIRA 项目配置验证或更新优先级值。
3. 选择 Test (勾选标记 图标)来测试与 JIRA 的集成是否正常工作。
4. 选择 Create (**save** icon)来创建配置。

注意

如果出现错误，请按照 故障排除 JIRA 集成 部分中的说明进行操作。

15.3. 配置策略通知

为系统策略启用警报通知。

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Policy Management。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 Bulk actions 下，选择 Enable notification。
4. 在 Enable notification 窗口中，选择 JIRA notifier。

注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 启用。

注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

15.4. JIRA 集成故障排除

如果您在 JIRA 项目中使用自定义优先级或强制自定义字段，在尝试将 Red Hat Advanced Cluster Security for Kubernetes 与 JIRA Software 集成时可能会出现错误。此错误可能是因为严重性和优先级字段值不匹配造成的。

如果您不知道 JIRA 项目中的自定义优先级值，请使用 **roxctl** CLI 为 JIRA 集成启用调试日志。

流程

1. 要从 JIRA 项目获取自定义优先级值，请运行以下命令为 JIRA 集成打开 debug 日志记录：

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" central debug log --level Debug --modules notifiers/jira
```

2. 按照说明配置 Red Hat Advanced Cluster Security for Kubernetes for Jira 集成。当您测试集成时，即使集成测试失败，生成的日志也会包含 JIRA 项目模式和自定义优先级。

3. 要将调试信息保存为压缩的 **.zip** 文件，请运行以下命令：

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" central debug dump
```

4. 解压 **.zip** 文件，以检索 JIRA 项目中使用的自定义优先级值。

5. 要关闭调试日志，请运行以下命令：

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" central debug log --level Info
```

6. 再次为 JIRA 集成配置 Red Hat Advanced Cluster Security for Kubernetes，并使用优先级值来配置自定义优先级。

第 16 章 与电子邮件集成

配置 Red Hat Advanced Cluster Security for Kubernetes (RHACS)，将有关策略违反的警报发送到标准电子邮件供应商。

您可以通过将警报从 RHACS 转发到标准电子邮件供应商来将电子邮件用作通知方法。要将 RHACS 平台的警报转发到电子邮件地址，您可以使用 **Default Recipient** 字段将电子邮件发送到标准和集中式团队，或使用部署注解来指定通知的受众。

使用注解键，您可以定义一个 audience 来通知与部署或命名空间关联的策略违反情况。如果部署具有注解，则注解的值会覆盖默认值。如果命名空间具有注解，则命名空间的值会覆盖默认值。

- 如果部署具有注解密钥和定义的受众，则会发送电子邮件到由密钥定义的受众。
- 如果部署没有注解键，则会检查命名空间是否有注解键，并将电子邮件发送到定义的受众。
- 如果没有注解键，则会发送电子邮件到集成中定义的默认接收者。

16.1. 配置电子邮件插件

RHACS 通知程序可将电子邮件发送到集成中指定的接收方，也可以使用注解来确定接收者。

使用注解动态确定电子邮件接收者：

1. 在部署 YAML 文件中添加类似以下示例的注解，其中 **email** 是您在电子邮件集成中指定的 注解键。

```
annotations:
  email: <email_address>
```

2. 在配置 RHACS 时，在 Annotation 键用于接收者 字段中使用注解键 电子邮件。

注意

您可以为部署或命名空间创建注解。

如果您使用注解配置了部署或命名空间，RHACS 平台会将警报发送到注解中指定的电子邮件。否则，它会将警报发送到默认接收者。

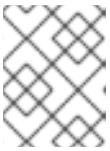
流程

1. 进入 Platform Configuration → Integrations。
2. 在 Notifier Integrations 部分下，选择 Email。
3. 选择 New Integration。
4. 在 Integration name 字段中，输入您的电子邮件集成的名称。
5. 在 Email server 字段中，输入您的电子邮件服务器的地址。电子邮件服务器地址包括完全限定域名(FQDN)和端口号；例如 **smtp.example.com:465**。
6. 可选：如果您使用未经身份验证的 SMTP，请选择 Enable unauthenticated SMTP。这是不安全且不推荐的，但有些集成可能是必需的。例如，如果您使用内部服务器进行不需要身份验证的通知，您可能需要启用这个选项。

注意

您无法更改使用身份验证来启用未经身份验证的 SMTP 的现有电子邮件集成。您必须删除现有集成，并创建一个选择 Enable unauthenticated SMTP 的新集成。

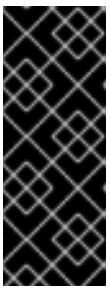
7. 输入用于身份验证的服务帐户的用户名和密码。
8. 可选：在 From 字段中输入您要出现在电子邮件通知的 **FROM** 标头中的名称，例如 **Security Alerts**。
9. 在 Sender 字段中指定您要出现在电子邮件通知的 **SENDER** 标头中的电子邮件地址。
10. 在 Default 接收者 字段中指定将接收通知的电子邮件地址。
11. 可选： 为接收者在注解键中输入注解键。如果您提供注解，部署或命名空间具有这个值的密钥，则通知将发送到注解中的电子邮件地址。否则，通知将发送到 Default Recipient 字段中指定的电子邮件。
12. 可选： 选择 Disable TLS 证书验证（不安全） 在没有 TLS 的情况下发送电子邮件。除非使用 StartTLS，否则不应禁用 TLS。



注意

使用 TLS 进行电子邮件通知。如果没有 TLS，则所有电子邮件都会被未加密的发送。

13. 可选： 要使用 StartTLS，请从 Use STARTTLS （需要禁用 TLS） 下拉菜单中选择 Login 或 Plain。



重要

使用 StartTLS 时，凭证在建立会话加密前以纯文本传递给电子邮件服务器。

- 使用 Login 参数的 STARTTLS 在 **base64** 编码字符串中发送身份验证凭据。
- 使用 Plain 参数的 STARTTLS 以纯文本形式将身份验证凭据发送到您的邮件中继。

16.2. 配置策略通知

为系统策略启用警报通知。

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Policy Management。
2. 选择您要为其发送警报的一个或多个策略。
3. 在 Bulk actions 下，选择 Enable notification。
4. 在 Enable notification 窗口中，选择电子邮件通知。

注意

如果您还没有配置任何其他集成，系统会显示一条没有配置通知程序的消息。

5. 单击 启用。

注意

- Red Hat Advanced Cluster Security for Kubernetes 根据选择发送通知。要接收通知，您必须首先为策略分配一个通知程序。
- 通知仅针对给定警报发送一次。如果您为策略分配了通知程序，则不会收到通知，除非违反了新警报。
- Red Hat Advanced Cluster Security for Kubernetes 为以下情况创建新警报：
  - 部署中第一次发生策略违反。
  - 在解决该部署中策略的以前的运行时警报后，运行时策略违反会在部署中发生。

第 17 章 与云管理平台集成

您可以将 Red Hat Advanced Cluster Security for Kubernetes (RHACS)与不同的云管理平台集成，以发现潜在的集群安全。集群发现旨在获取已或尚未由 RHACS 保护的集群资产的详细概述。

从云管理平台发现的集群可从 Platform Configuration → Clusters → Discovered cluster 页面访问。

RHACS 将发现的集群与已保护的集群匹配。根据匹配的结果，发现的集群具有以下状态之一：

- 安全 ：集群由 RHACS 保护。
- unsecured ：集群不受 RHACS 保护。
- 未确定的 ：从安全集群收集的元数据不足以达到唯一匹配项。集群受保护或不受保护。

要成功进行集群匹配，请确保满足以下条件：

- 在安全集群中运行的传感器已更新至最新版本。
- 为在 AWS 上运行的安全集群授予 通过元数据服务访问实例标签。传感器需要访问 AWS EC2 实例标签来确定集群状态。

您可以将 RHACS 与以下云管理平台集成：

- Paladin Cloud
- OpenShift Cluster Manager

17.1. 配置 PALADIN 云集成

要从 Paladin Cloud 发现集群资产，请在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

前提条件

- Paladin Cloud 帐户。
- Paladin Cloud API 令牌。

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Integrations。
2. 向下滚动到 Cloud source integrations 部分，然后选择 Paladin Cloud。
3. 点 New integration。
4. 输入 集成名称。
5. 为 Paladin Cloud 端点输入 Paladin Cloud API 端点。默认值为 **https://api.paladincloud.io**。
6. 为 Paladin Cloud 令牌输入 Paladin Cloud API 令牌。
7. 选择 Test 以确认身份验证是否正常工作。
8. 选择 Create 来创建配置。

配置后，Red Hat Advanced Cluster Security for Kubernetes 从连接的 Paladin Cloud 帐户中发现集群资产。

17.2. 配置 RED HAT OPENSHIFT CLUSTER MANAGER 集成

要从 Red Hat OpenShift Cluster Manager 发现集群资产，请在 Red Hat Advanced Cluster Security for Kubernetes 中创建新集成。

前提条件

- 红帽帐户。
- Red Hat OpenShift Cluster Manager API 令牌。

流程

1. 在 RHACS 门户中，进入 Platform Configuration → Integrations。
2. 向下滚动到 Cloud source integrations 部分，然后选择 Red Hat OpenShift Cluster Manager。
3. 点 New integration。
4. 输入 集成名称。
5. 为 Endpoint 输入 Red Hat OpenShift Cluster Manager API 端点。默认值为 **https://api.openshift.com**。
6. 为 API 令牌输入 Red Hat OpenShift Cluster Manager API 令牌。
7. 选择 Test 以确认身份验证是否正常工作。
8. 选择 Create 来创建配置。

配置后，Red Hat Advanced Cluster Security for Kubernetes 从您连接的红帽帐户发现集群资产。

第 18 章 使用简短令牌集成 RHACS

使用 Red Hat Advanced Cluster Security for Kubernetes (RHACS)，您可以使用简短的令牌对所选云供应商 API 进行身份验证。RHACS 支持以下云供应商集成：

- 使用安全令牌服务(STS)的 Amazon Web Services (AWS)
- 使用工作负载身份联邦的 Google Cloud Platform (GCP)

RHACS 仅在以下平台上安装 RHACS 时支持短期令牌集成：

- AWS 上的 Elastic Kubernetes Service (EKS)
- GCP 上的 Google Kubernetes Engine (GKE)
- OpenShift Container Platform

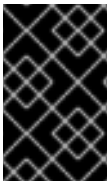
要激活短期身份验证，您必须在 Kubernetes 或 OpenShift Container Platform 集群和云供应商之间建立信任。对于 EKS 和 GKE 集群，请使用云供应商元数据服务。对于 OpenShift Container Platform 集群，需要一个包括 OpenShift Container Platform 服务帐户 signer 密钥的公开可用的 OpenID Connect (OIDC)供应商存储桶。

注意

您必须为每个使用短期令牌集成的 Central 集群建立对云供应商的信任。但是，如果您将委托扫描与短实时令牌镜像集成结合使用，还必须为 Sensor 集群建立信任。

18.1. 配置 AWS 安全令牌服务

RHACS 集成可以使用 安全令牌服务 对 Amazon Web Services 进行身份验证。在集成中启用Use container IAM role 选项前，您必须使用 RHACS 配置**AssumeRole**。



重要

验证与 RHACS pod 关联的 AWS 角色必须具有集成所需的 IAM 权限。例如，若要设置与 Elastic Container Registry 集成的容器角色，请启用对 registry 的完整读取访问权限。如需有关 AWS IAM 角色的更多信息，请参阅 IAM 角色。

18.1.1. 配置 Elastic Kubernetes Service (EKS)

当在 EKS 上运行 Red Hat Advanced Cluster Security for Kubernetes (RHACS)时，您可以通过 Amazon Secure Token Service 配置简短的令牌。

流程

1. 运行以下命令，为您的 EKS 集群启用 IAM OpenID Connect (OIDC)供应商：

```
$ eksctl utils associate-iam-oidc-provider --cluster <cluster_name> --approve
```

2. 为您的 EKS 集群创建一个 IAM 角色。
3. 编辑角色的权限策略，并授予集成所需的权限。例如：

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
          "ecr:BatchCheckLayerAvailability",
          "ecr:BatchGetImage",
          "ecr:DescribeImages",
          "ecr:DescribeRepositories",
          "ecr:GetAuthorizationToken",
          "ecr:GetDownloadUrlForLayer",
          "ecr:ListImages"
        ],
        "Resource": "arn:aws:iam::<ecr_registry>:role/<role_name>"
      }
    ]
}
```

4. 更新您要假设的角色的信任关系：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<ecr-registry>:role/<role_name>" (1)
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

(1) & lt;role_name > 应该与您在前面的步骤中创建的新角色匹配。

5. 输入以下命令将新创建的角色与服务帐户关联：

```
$ oc -n stackrox annotate sa central eks.amazonaws.com/role-
arn=arn:aws:iam::67890:role/<role_name> (1)
```

(1) 如果使用 Kubernetes，请输入 **kubectl** 而不是 **oc**。

6. 输入以下命令重启 Central pod 并应用更改：

```
$ oc -n stackrox delete pod -l "app in (central,sensor)" (1)
```

(1) 如果使用 Kubernetes，请输入 **kubectl** 而不是 **oc**。

18.1.2. 配置 OpenShift Container Platform

在 OpenShift Container Platform 上运行 Red Hat Advanced Cluster Security for Kubernetes (RHACS)时，您可以通过 Amazon Secure Token Service 配置简短的令牌。

前提条件

- 您必须使用 OpenShift Container Platform 服务帐户 signer 密钥有一个公共 OpenID Connect (OIDC)配置存储桶。要获取 OpenShift Container Platform 集群的 OIDC 配置，红帽建议 以手动模式为短期凭证使用 Cloud Credential Operator 的说明。
- 您必须有权访问 AWS IAM 和创建和更改角色的权限。

流程

1. 按照 创建 OpenID Connect (OIDC)身份提供程序 中的说明，创建 OpenShift Container Platform 集群的 Web 身份。使用 **openshift** 作为 Audience 的值。
2. 为 OpenShift Container Platform 集群的 Web 身份 创建一个 IAM 角色。
3. 编辑角色的权限策略，并授予集成所需的权限。例如：

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "ecr:BatchCheckLayerAvailability",
            "ecr:BatchGetImage",
            "ecr:DescribeImages",
            "ecr:DescribeRepositories",
            "ecr:GetAuthorizationToken",
            "ecr:GetDownloadUrlForLayer",
            "ecr:ListImages"
         ],
         "Resource": "arn:aws:iam::<ecr_registry>:role/<role_name>"
      }
   ]
}
```

4. 更新您要假设的角色的信任关系：

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Federated": "<oidc_provider_arn>"
         },
         "Action": "sts:AssumeRoleWithWebIdentity",
         "Condition": {
            "StringEquals": {
```

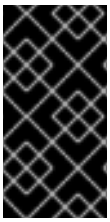
```
                "<oidc_provider_name>:aud": "openshift"
            }
        }
    }
  ]
}
```

5. 在 Central 或 Sensor 部署中设置以下 RHACS 环境变量：

```
AWS_ROLE_ARN=<role_arn>
AWS_WEB_IDENTITY_TOKEN_FILE=/var/run/secrets/openshift/serviceaccount/token
```

18.2. 配置 GOOGLE 工作负载身份联邦

RHACS 集成可以使用 工作负载身份 对 Google Cloud Platform 进行身份验证。选择Use workload identity 选项，以便在 Google Cloud 集成中启用工作负载身份身份验证。



重要

通过工作负载身份与 RHACS pod 关联的 Google 服务帐户必须具有集成所需的 IAM 权限。例如，若要设置与 Google Artifact Registry 集成的工作负载身份，请将服务帐户与 roles/artifactregistry.reader 角色连接。有关 Google IAM 角色的更多信息，请参阅配置角色和权限。

18.2.1. 配置 Google Kubernetes Engine (GKE)

在 GKE 上运行 Red Hat Advanced Cluster Security for Kubernetes (RHACS)时，您可以通过 Google 工作负载身份配置简短的令牌。

前提条件

- 您必须有权访问包含集群和集成资源的 Google Cloud 项目。

流程

1. 按照 Google Cloud Platform 文档中的说明，为 GKE 使用工作负载身份联邦。
2. 运行以下命令来注解 RHACS 服务帐户：

```
$ oc annotate serviceaccount \ 1
  central \ 2
  --namespace stackrox \
  iam.gke.io/gcp-service-account=
<GSA_NAME>@<GSA_PROJECT>.iam.gserviceaccount.com
```

1. 如果使用 Kubernetes，请输入 **kubectl** 而不是 **oc**。
2. 在设置委派的扫描时，请使用 传感器 而不是 中央。

18.2.2. 配置 OpenShift Container Platform

在 OpenShift Container Platform 上运行 Red Hat Advanced Cluster Security for Kubernetes (RHACS)时，您可以通过 Google 工作负载身份配置简短的令牌。

前提条件

- 您必须使用 OpenShift Container Platform 服务帐户 signer 密钥有一个公共 OIDC 配置存储桶。获取 OpenShift Container Platform 集群的 OIDC 配置的建议方法是以手动模式使用 Cloud Credential Operator 进行短期凭证 说明。
- 使用 roles/iam.workloadIdentityPoolAdmin 角色访问 Google Cloud 项目。

流程

1. 按照 管理工作负载身份池中 的说明，创建工作负载身份池。例如：

```
$ gcloud iam workload-identity-pools create rhacs-pool \
    --location="global" \
    --display-name="RHACS workload pool"
```

2. 按照 管理工作负载身份提供程序中的说明，创建工作负载身份提供程序。例如：

```
$ gcloud iam workload-identity-pools providers create-oidc rhacs-provider \
    --location="global" \
    --workload-identity-pool="rhacs-pool" \
    --display-name="RHACS provider" \
    --attribute-mapping="google.subject=assertion.sub" \
    --issuer-uri="https://<oidc_configuration_url>" \
    --allowed-audiences=openshift
```

3. 将 Google 服务帐户连接到工作负载身份池。例如：

```
$ gcloud iam service-accounts add-iam-policy-binding
<GSA_NAME>@<GSA_PROJECT>.iam.gserviceaccount.com \
    --role roles/iam.workloadIdentityUser \
    --
member="principal://iam.googleapis.com/projects/<GSA_PROJECT_NUMBER>/locatio
ns/global/workloadIdentityPools/rhacs-
provider/subject/system:serviceaccount:stackrox:central" (1)
```

(1) 对于委派的扫描，请将主题设置为 system:serviceaccount:stackrox:sensor。

4. 创建包含安全令牌服务(STS)配置的服务帐户 JSON。例如：

```
{
  "type": "external_account",
  "audience":
"//iam.googleapis.com/projects/<GSA_PROJECT_ID>/locations/global/workloadIdentit
yPools/rhacs-pool/providers/rhacs-provider",
  "subject_token_type": "urn:ietf:params:oauth:token-type:jwt",
  "token_url": "https://sts.googleapis.com/v1/token",
  "service_account_impersonation_url":
"https://iamcredentials.googleapis.com/v1/projects/-
/serviceAccounts/<GSA_NAME>@<GSA_PROJECT>.iam.gserviceaccount.com:genera
teAccessToken",
```

```
  "credential_source": {
    "file": "/var/run/secrets/openshift/serviceaccount/token",
    "format": {
      "type": "text"
    }
  }
}
```

5. 使用服务帐户 JSON 作为 RHACS 命名空间的 secret：

```
apiVersion: v1
kind: Secret
metadata:
  name: gcp-cloud-credentials
  namespace: stackrox
data:
  credentials: <base64_encoded_json>
```