# Red Hat Advanced Cluster Security for Kubernetes 4.4

## roxctl CLI

roxctl CLI

Last Updated: 2024-06-28

# Red Hat Advanced Cluster Security for Kubernetes 4.4 roxctl CLI

roxctl CLI

## 法律通告



## 摘要

本文档论述了如何安装和使用 roxctl 命令行界面，包括 roxctl 语法和操作。它提供了一些常见的命令示例。

# 目录

# 第 1 章 安装 ROXCTL CLI

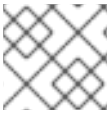
**roxctl** 是一个命令行界面(CLI)，用于在 Red Hat Advanced Cluster Security for Kubernetes (RHACS)上运行命令。您可以通过下载二进制文件或从容器镜像运行 **roxctl** CLI 来安装 **roxctl** CLI。

## 1.1. 通过下载二进制文件安装 ROXCTL CLI

您可以安装 **roxctl** CLI，以便从命令行界面与 RHACS 进行交互。您可以在 Linux、Windows 或 macOS 上安装 **roxctl**。

### 1.1.1. 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
```

### 1.1.2. 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
```

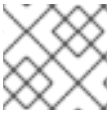
**验证**

- 验证您已安装的 **roxctl** 版本：

```
$ roxctl version
```

### 1.1.3. 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
```

## 1.2. 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
```

# 第 2 章 使用 ROXCTL CLI

## 2.1. 先决条件

- 您已使用以下命令配置了 **ROX_ENDPOINT** 环境变量：

```
$ export ROX_ENDPOINT=<host:port> 1
```

1 存储在 **ROX_ENDPOINT** 环境变量中的主机和端口信息。

## 2.2. 获取身份验证信息

以下流程描述了如何使用 **roxctl central whoami** 命令检索有关 Central 中身份验证状态和用户配置集的信息。示例输出演示了您可以看到的数据，包括用户角色、访问权限和各种管理功能。此步骤允许您在 Central 中查看访问和角色。

**流程**

- 运行以下命令，在 Central 中获取有关当前验证状态和用户信息的信息：

```
$ roxctl central whoami
```

**输出示例**

```
UserID:
    <redacted>
User name:
    <redacted>
Roles:
 APIToken creator, Admin, Analyst, Continuous Integration, Network Graph Viewer, None,
Sensor Creator, Vulnerability Management Approver, Vulnerability Management Requester,
Vulnerability Manager, Vulnerability Report Creator
Access:
  rw Access
  rw Administration
  rw Alert
  rw CVE
  rw Cluster
  rw Compliance
  rw Deployment
  rw DeploymentExtension
  rw Detection
  rw Image
  rw Integration
  rw K8sRole
  rw K8sRoleBinding
  rw K8sSubject
  rw Namespace
  rw NetworkGraph
  rw NetworkPolicy
  rw Node
  rw Secret
```

```
rw ServiceAccount
rw VulnerabilityManagementApprovals
rw VulnerabilityManagementRequests
rw WatchedImage
rw WorkflowAdministration
```

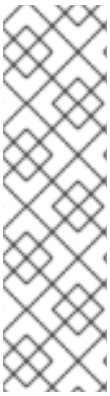
检查输出，以确保身份验证和用户详情如预期。

## 2.3. 使用 ROXCTL CLI 进行身份验证

要进行身份验证，您可以使用 API 令牌、管理员密码或 **roxctl central login** 命令。

遵循以下准则来有效地使用 API 令牌：

- 在生产环境中使用 API 令牌以及持续集成 (CI)。每个令牌都被分配特定的访问权限，提供对它可以执行的操作的控制。此外，API 令牌不需要以交互的形式进行（例如通过浏览器进行登录），使其成为自动化流程的理想选择。这些令牌具有 1 年的生存时间 (TTL) 值，为无缝集成和操作效率提供更长的有效期。
- 仅使用管理员密码用于测试目的。不要在生产环境中使用它。
- **roxctl central login** 命令仅适用于交互式的本地使用。



**注意**

- 为防止特权升级，在创建新令牌时，您的权限将限制您可以分配给该令牌的权限。例如，如果您只有 Integration 资源的 **read** 权限，则无法创建 **具有写入权限** 的令牌。
- 如果您希望自定义角色为其他用户创建令牌，则必须为该自定义角色分配所需的权限。
- 将短期令牌用于机器到机器的通信，如 CI/CD 管道、脚本和其他自动化。另外，使用 **roxctl central login** 命令进行人工到机器通信，如 **roxctl** CLI 或 API 访问。

**其他资源**

- 配置 API 令牌
- 配置短期访问

### 2.3.1. 创建 API 令牌

**流程**

1. 在 RHACS 门户中，进入 **Platform Configuration → Integrations**。
2. 滚动到 **Authentication Tokens** 类别，然后点 **API Token**。
3. 点 **Generate Token**。
4. 输入令牌的名称并选择提供所需访问级别的角色（例如： **Continuous Integration** 或 **Sensor Creator**）。
5. 点 **Generate**。

**重要**

复制生成的令牌并安全地存储它。您将无法再次查看它。

### 2.3.2. 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。

### 2.3.3. 使用身份验证供应商与 roxctl 进行身份验证

您可以在 Central 中配置身份验证供应商，并使用 **roxctl** CLI 启动登录过程。设置 **ROX_ENDPOINT** 变量，使用 **roxctl central login** 命令启动登录过程，在浏览器窗口中选择身份验证供应商，并从 **roxctl** CLI 检索令牌信息，如以下步骤所述。

**前提条件**

- 选择一个身份验证供应商，如带有片段或查询模式的 OpenID Connect (OIDC)。

**流程**

1. 运行以下命令，将 **ROX_ENDPOINT** 变量设置为 Central 主机名和端口：

```
export ROX_ENDPOINT=<central_hostname:port>
```

2. 运行以下命令，将登录过程启动到 Central：

```
$ roxctl central login
```

3. 在 **roxctl** CLI 中，URL 包括在输出中，您会被重定向到一个浏览器窗口，您可以在其中选择您要使用的身份验证供应商。
4. 使用您的身份验证供应商登录。
   成功登录后，浏览器窗口表示身份验证成功，您可以关闭浏览器窗口。

5. **roxctl** CLI 会显示您的令牌信息，包括访问令牌、访问令牌的过期时间、刷新令牌（如果已发布），并通知这些值存储在本地。

**输出示例**

```
Please complete the authorization flow in the browser with an auth provider of your choice.
If no browser window opens, please click on the following URL:
      http://127.0.0.1:xxxxx/login

INFO: Received the following after the authorization flow from Central:
INFO: Access token: <redacted> 1
INFO: Access token expiration: 2023-04-19 13:58:43 +0000 UTC 2
INFO: Refresh token: <redacted> 3
INFO: Storing these values under $HOME/.roxctl/login… 4
```

1. 访问令牌。
2. 访问令牌的过期时间。
3. 刷新令牌。
4. 用于本地存储访问令牌的值、访问令牌过期时间以及刷新令牌的目录。

**重要**

确保将环境设置为确定存储配置的目录。默认情况下，配置存储在 **$HOME/.roxctl/roxctl-config** 目录中。

- 如果您设置了 **$ROX_CONFIG_DIR** 环境变量，则配置存储在 **$ROX_CONFIG_DIR/roxctl-config** 目录中。这个选项具有最高优先级。
- 如果您设置了 **$XDG_RUNTIME_DIR** 环境变量，并且未设置 **$ROX_CONFIG_DIR** 变量，则配置存储在 **$XDG_RUNTIME_DIR /roxctl-config** 目录中。
- 如果您没有设置 **$ROX_CONFIG_DIR** 或 **$XDG_RUNTIME_DIR** 环境变量，则配置存储在 **$HOME/.roxctl/roxctl-config** 目录中。

## 2.4. 在 RHACS 云服务中配置和使用 ROXCTL CLI

**流程**

- 运行以下命令导出 **ROX_API_TOKEN** ：

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

- 运行以下命令来导出 **ROX_ENDPOINT** ：

```
$ export ROX_ENDPOINT=<address>:<port_number>
```

- 您可以使用 **--help** 选项获取有关命令的更多信息。

- 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**。

# 第 3 章 管理安全集群

要保护 Kubernetes 或 OpenShift Container Platform 集群，您必须将 Red Hat Advanced Cluster Security for Kubernetes (RHACS)服务部署到集群中。您可以通过进入到 **Platform Configuration → Clusters** 视图在 RHACS 门户中生成部署文件，也可以使用 **roxctl** CLI。

## 3.1. 先决条件

- 您已使用以下命令配置了 **ROX_ENDPOINT** 环境变量：

```
$ export ROX_ENDPOINT=<host:port> 1
```

1 存储在 **ROX_ENDPOINT** 环境变量中的主机和端口信息。

## 3.2. 生成 SENSOR 部署文件

### 为 Kubernetes 系统生成文件

#### 流程

- 运行以下命令，为您的 Kubernetes 集群生成所需的传感器配置，并将其与您的 Central 实例关联：

```
$ roxctl sensor generate k8s --name <cluster_name> --central "$ROX_ENDPOINT"
```

### 为 OpenShift Container Platform 系统生成文件

#### 流程

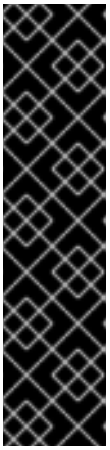
- 运行以下命令，为 OpenShift Container Platform 集群生成所需的传感器配置，并将其与您的 Central 实例关联：

```
$ roxctl sensor generate openshift --openshift-version <ocp_version> --name
<cluster_name> --central "$ROX_ENDPOINT" 1
```

1 对于 **--openshift-version** 选项，请指定集群的主 OpenShift Container Platform 版本号。例如，为 OpenShift Container Platform 版本 **3.x** 指定 **3**，为 OpenShift Container Platform 版本 **4.x** 指定 **4**。

阅读 **--help** 输出以查看您可能需要使用的其他选项，具体取决于您的系统架构。

验证您为 **--central** 提供的端点是否可以从部署 Red Hat Advanced Cluster Security for Kubernetes 服务的集群中访问。



**重要**

如果您使用支持非 gRPC 的负载均衡器，如 HAProxy、AWS Application Load Balancer (ALB) 或 AWS Elastic Load Balancing (ELB)，请按照以下步骤操作：

- 使用 WebSocket Secure (**ws**) 协议。要使用 **wss**，使用 **ws://** 为地址添加前缀，并
- 在地址后添加端口号，例如：

```
$ roxctl sensor generate k8s --central wss://stackrox-central.example.com:443
```

## 3.3. 使用 SENSOR.SH 脚本安装 SENSOR

当您生成 Sensor 部署文件时，**roxctl** 会在工作目录中创建一个名为 **sensor-<cluster_name>** 的目录。安装 Sensor 的脚本位于这个目录中。

**流程**

- 运行传感器安装脚本来安装 Sensor：

```
$ ./sensor-<cluster_name>/sensor.sh
```

如果您收到没有安装 Sensor 所需的权限的警告，请按照屏幕说明操作，或者联系集群管理员寻求帮助。

## 3.4. 为现有集群下载 SENSOR 捆绑包

**流程**

- 运行以下命令，通过指定 **集群名称**或 **ID** 为现有集群下载 Sensor 捆绑包：

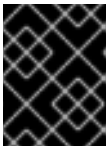
```
$ roxctl sensor get-bundle <cluster_name_or_id>
```

## 3.5. 删除集群集成

**流程**

- 在删除集群前，请确定您有要从 Central 中删除的正确集群名称：

```
$ roxctl cluster delete --name=<cluster_name>
```



**重要**

删除集群集成不会删除集群中运行的 RHACS 服务，具体取决于安装方法。您可以从 Sensor 安装捆绑包中运行 **delete-sensor.sh** 脚本来删除服务。

# 第 4 章 检查策略合规性

您可以使用 **roxctl** CLI 检查部署 YAML 文件和镜像是否合规。

## 4.1. 先决条件

- 您已使用以下命令配置了 **ROX_ENDPOINT** 环境变量：

```
$ export ROX_ENDPOINT=<host:port> 1
```

1 存储在 **ROX_ENDPOINT** 环境变量中的主机和端口信息。

## 4.2. 配置输出格式

当您使用 **roxctl deployment check** 或 **roxctl image check** 命令检查策略时，您可以使用命令的 **-o** 选项指定输出格式，并将格式指定为 **json**、**table**、**csv** 或 **junit**。此选项决定了如何在终端中显示命令的输出。

例如，以下命令检查部署，然后以 **csv** 格式显示结果：

```
$ roxctl deployment check --file =<yaml_filename> -o csv
```

**注意**

当您没有为输出格式指定 **-o** 选项时，会使用以下默认行为：

- **deployment check** 和 **image check** 命令的格式是 **table**。
- **image scan** 命令的默认输出格式是 **json**。这是与 CLI 旧版本兼容的旧 JSON 格式输出。若要以新的 JSON 格式获取输出，使用格式选项，如 **-o json**。在收集数据以进行故障排除时，请使用旧的 JSON 格式输出。

可以不同的选项用于配置输出。下表列出了选项及其可用格式。

| 选项 | 描述 | 格式 |
| --- | --- | --- |
| **--compact-output** | 使用此选项以紧凑格式显示 JSON 输出。 | **json** |
| **--headers** | 使用这个选项指定自定义标头。 | **table** 和 **csv** |
| **--no-header** | 使用这个选项省略输出中的标头行。 | **table** 和 **csv** |

| 选项 | 描述 | 格式 |
| --- | --- | --- |
| **--row-jsonpath-expressions** | 使用这个选项指定 GJSON 路径，以选择输出中的特定项目。例如，若要获取部署检查的**策略名称**和**严重性**，请使用以下命令：<br><br>$ roxctl deployment check --file=<*yaml_filename*> \<br>-o table --headers POLICY-NAME,SEVERITY \<br>--row-jsonpath-expressions="{results..violatedPolicies..name,results..violatedPolicies..severity}" | **table** 和 **csv** |
| **--merge-output** | 使用此选项合并具有相同值的表单元。 | **table** |
| **headers-as-comment** | 使用这个选项在输出中将标头行包含为注释。 | **csv** |
| **--junit-suite-name** | 使用此选项指定 JUnit 测试套件的名称。 | **junit** |

## 4.3. 检查部署 YAML 文件

**流程**

- 以下命令检查 YAML 部署文件中的安全策略的构建时间和部署时间违反情况：

```
$ roxctl deployment check --file=<yaml_filename> \ 1
--namespace=<cluster_namespace> \ 2
--cluster=<cluster_name_or_id> \ 3
--verbose 4
```

1. 对于 & **lt;yaml_filename** >，请指定要发送到 Central 的一个或多个部署的 YAML 文件，以进行策略评估。您还可以使用 --file 标志指定多个 YAML 文件来发送到 Central 以进行策略评估，如 **--file =<yaml_filename** 1>、**--file=<yaml_filename2&** gt; 等等。

2. 对于 **<cluster_namespace** >，指定一个命名空间来增强带有上下文信息（如网络策略、基于角色的访问控制(RBAC)和服务）的部署，以便在规格中没有命名空间的部署。规范中定义的命名空间不会改变。默认值为 **default**。

3. 对于 **<cluster_name_or_id** >，请指定您要用作评估上下文的集群名称或 ID，以使用特定于集群的信息启用扩展部署。

4. 通过启用 **--verbose** 标志，您可以在策略检查过程中收到每个部署的附加信息。扩展的信息包括 RBAC 权限级别和应用的网络策略的完整列表。

**注意**

您可以在 JSON 输出中查看每个部署的附加信息，无论是否启用 **--verbose** 标志。

格式在 API 引用中定义。要让 Red Hat Advanced Cluster Security for Kubernetes (RHACS)从关联的 registry 和扫描程序中重新拉取镜像元数据和镜像扫描结果，请添加 **--force** 选项。

**注意**

要检查特定的镜像扫描结果，您必须具有 **Image** 资源的 **read** 和 **write** 权限的令牌。默认的 **Continuous Integration** 系统角色已具有所需的权限。

此命令验证以下项目：

- YAML 文件中的配置选项，如资源限值或特权选项
- YAML 文件中使用的镜像的各个方面，如组件或漏洞

## 4.4. 检查镜像

**流程**

- 运行以下命令检查镜像中安全策略的构建时违反情况：

```
$ roxctl image check --image=<image_name>
```

格式在 API 引用中定义。要让 Red Hat Advanced Cluster Security for Kubernetes (RHACS)从关联的 registry 和扫描程序中重新拉取镜像元数据和镜像扫描结果，请添加 **--force** 选项。

**注意**

要检查特定的镜像扫描结果，您必须具有 **Image** 资源的 **read** 和 **write** 权限的令牌。默认的 **Continuous Integration** 系统角色已具有所需的权限。

**其他资源**

- roxctl 镜像

## 4.5. 检查镜像扫描结果

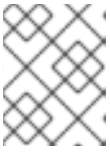
您还可以检查特定镜像的扫描结果。

**流程**

- 运行以下命令以以 JSON 格式返回镜像中发现的组件和漏洞：

```
$ roxctl image scan --image <image_name>
```

格式在 API 引用中定义。要让 Red Hat Advanced Cluster Security for Kubernetes (RHACS)从关联的 registry 和扫描程序中重新拉取镜像元数据和镜像扫描结果，请添加 **--force** 选项。



**注意**

要检查特定的镜像扫描结果，您必须具有 **Image** 资源的 **read** 和 **write** 权限的令牌。默认的 **Continuous Integration** 系统角色已具有所需的权限。

**其他资源**

- roxctl 镜像

# 第 5 章 调试问题

Central 将信息保存到其容器日志中。

## 5.1. 先决条件

- 您已使用以下命令配置了 **ROX_ENDPOINT** 环境变量：

```
$ export ROX_ENDPOINT=<host:port> 1
```

1 存储在 **ROX_ENDPOINT** 环境变量中的主机和端口信息。

## 5.2. 查看日志

您可以使用 **oc** 或 **kubectl** 命令查看 Central pod 的日志。

**流程**

- 要使用 **kubectl** 查看 Central pod 的日志，请运行以下命令：

```
$ kubectl logs -n stackrox <central_pod>
```

- 要使用 **oc** 查看 Central pod 的日志，请运行以下命令：

```
$ oc logs -n stackrox <central_pod>
```

## 5.3. 查看当前日志级别

您可以更改日志级别，以在 Central 日志中看到更多或较少的信息。

**流程**

- 运行以下命令来查看当前的日志级别：

```
$ roxctl central debug log
```

**其他资源**

- roxctl central debug

## 5.4. 更改日志级别

**流程**

- 运行以下命令来更改日志级别：

```
$ roxctl central debug log --level=<log_level> 1
```

1 **<log_level>** 可以接受的值是：**Panic**, **Fatal**, **Error**, **Warn**, **Info**, 和 **Debug**。

**其他资源**

- roxctl central debug

## 5.5. 检索调试信息

**流程**

- 运行以下命令来收集调查问题的调试信息：

```
$ roxctl central debug dump
```

- 要使用 RHACS 管理员密码或 API 令牌和中央地址生成诊断捆绑包，请按照使用 roxctl CLI 生成诊断捆绑包 的步骤进行操作。

**其他资源**

- roxctl central debug

# 第 6 章 生成构建时网络策略

build-time 网络策略生成器包含在 **roxctl** CLI 中。对于构建网络策略生成功能，**roxctl** CLI 不需要与 RHACS Central 通信，因此您可以在任何开发环境中使用它。

## 6.1. 使用构建时网络策略生成器

**先决条件**

1. build-time 网络策略生成器递归扫描您在运行命令时指定的目录。因此，在运行该命令前，您必须已具有服务清单、配置映射和工作负载清单，如 **Pod**、**Deployment**、**ReplicaSet**、**Job**、**DaemonSet** 和 **StatefulSet** 作为指定目录中的 YAML 文件。

2. 使用 **kubectl apply -f** 命令验证这些 YAML 文件是否按原样应用。build-time 网络策略生成器无法用于使用 Helm 样式模板的文件。

3. 验证服务网络地址没有硬编码。需要连接到服务的每个工作负载都必须将服务网络地址指定为变量。您可以使用工作负载的资源环境变量或配置映射来指定此变量。

   - 示例 1：使用环境变量
   - 示例 2：使用配置映射
   - 示例 3：使用配置映射

4. 服务网络地址必须与以下官方正则表达式模式匹配：

   ```
   (http(s)?://)?<svc>(.<ns>(.svc.cluster.local)?)?(:<portNum>)? 1
   ```

   1 在这种模式中，

   - <svc> 是服务名称。
   - <ns> 是定义该服务的命名空间。
   - <portNum> 是公开的服务端口号。

   以下是与模式匹配的一些示例：

   - **wordpress-mysql:3306**
   - **redis-follower.redis.svc.cluster.local:6379**
   - **redis-leader.redis**
   - **http://rating-service.**

**流程**

1. 运行 help 命令验证构建网络策略生成功能是否可用：

   ```
   $ roxctl netpol generate -h
   ```

2. 使用 **netpol generate** 命令生成策略：

```
$ roxctl netpol generate <folder-path> 1
```

1 指定具有 Kubernetes 清单的文件夹路径。

**roxctl netpol generate** 命令支持以下选项：

| 选项 | 描述 |
| --- | --- |
| **-h, --help** | 查看 **netpol** 命令的帮助文本。 |
| **-d, --output-dir <dir>** | 将生成的策略保存到目标文件夹中。每个策略有一个文件。 |
| **-f, --output-file <filename>** | 将生成的策略保存并合并到单个 YAML 文件中。 |
| **--fail** | 在第一次遇到的错误时失败。默认值为 **false**。 |
| **--remove** | 删除输出路径（如果已存在）。 |
| **--strict** | 将警告视为错误。默认值为 **false**。 |

# 第 7 章 使用 ROXCTL CLI 进行镜像扫描

您可以使用 **roxctl** CLI 扫描存储在镜像 registry 中的镜像，包括集群本地 registry，如 OpenShift Container Platform 集成的镜像 registry。

## 7.1. 使用远程集群扫描镜像

通过在委托扫描配置中指定适当的集群，或通过以下流程中描述的 cluster 参数指定适当的集群，您可以使用远程集群从集群本地 registry 中扫描镜像。

**重要**

有关如何配置委派的镜像扫描的更多信息，请参阅配置委派的镜像扫描。

**流程**

- 运行以下命令扫描远程集群中的指定镜像：

```
$ roxctl image scan \
  --image=<image_registry>/<image_name> \ 1
  --cluster=<cluster_detail> \ 2
  [flags] 3
```

1. 对于 **<image_registry** >，请指定镜像所在的 registry，例如 **image-registry.openshift-image-registry.svc:5000/**。对于 **<image_name** >，请指定您要扫描的镜像的名称，如 **default/image-stream:latest**。
2. 对于 **<cluster_detail** >，请指定远程集群的名称或 ID。例如，指定名称 **remote**。
3. 可选：对于 **[flags]**，您可以指定参数来修改命令的行为。

   有关可选参数的更多信息，请参阅 roxctl image scan 命令选项。

**输出示例**

```
{
  "Id":
"sha256:3f439d7d71adb0a0c8e05257c091236ab00c6343bc44388d091450ff58664bf9", 1
  "name": { 2
    "registry": "image-registry.openshift-image-registry.svc:5000", 3
    "remote": "default/image-stream", 4
    "tag": "latest", 5
    "fullName": "image-registry.openshift-image-registry.svc:5000/default/image-stream:latest"
6
  },
[...]
```

1. 用作镜像指纹的镜像的唯一标识符。它有助于确保镜像的完整性和真实性。
2. 包含镜像的具体详情。
3. 存储镜像 registry 的位置。

4. 到镜像的远程路径。
5. 与此镜像关联的版本或标签。
6. 镜像的完整名称，组合 registry、远程路径和标签。

## 7.2. ROXCTL IMAGE SCAN 命令选项

**roxctl image scan** 命令支持以下选项：

| 选项 | 描述 |
| --- | --- |
| **--cluster string** | 将镜像扫描委派给特定集群。 |
| **--compact-output** | 以紧凑格式显示 JSON 输出。默认值为 **false**。 |
| **-f,--force** | 忽略扫描的 Central 缓存，并强制从 Scanner 重新拉取。默认值为 **false**。 |
| **--headers string** | 以表格形式打印标头。默认值包括 **COMPONENT**、**VERSION**、**CVE**、SEE**R** ITY 和 **LINK**。 |
| **--headers-as-comments** | 在 CSV 标签页化输出中将标头显示为注释。默认值为 **false**。 |
| **-h, --help** | 查看 **roxctl image scan** 命令的帮助文本。 |
| **-i,--image string** | 指定镜像名称和您要扫描的引用。 |
| **-a, --include-snoozed** | 返回 snoozed 和 unsnoozed 通用漏洞和暴露(CVE)。默认值为 **false**。 |
| **--merge-output** | 在 tabular 输出中合并重复单元。默认值为 **true**。 |
| **--no-header** | 不要打印表格格式的标头。默认值为 **false**。 |
| **-o,--output string** | 指定输出格式。您可以选择自定义结果显示的格式。格式包括 **表**、**CSV**、**JSON** 和 **SARIF**。 |
| **-r,--retries int** | 在操作中止前设置重试次数，并显示错误。默认值为 **3**。 |
| **-d, --retry-delay int** | 设置重试之间等待的时间（以秒为单位）。默认值为 **3**。 |
| **--row-jsonpath-expressions string** | 使用 JSON 路径表达式从 JSON 对象创建行。如需了解更多详细信息，请运行 **roxctl image scan --help** 命令。 |

| 选项 | 描述 |
| --- | --- |

# 第 8 章 ROXCTL CLI 命令参考

## 8.1. ROXCTL

显示 **roxctl** CLI 的可用命令和可选参数。您必须具有具有管理员特权的帐户才能使用这些命令。

### 使用方法

```
$ roxctl [command] [flags]
```

**表 8.1. 可用命令**

| 命令 | 描述 |
|---|---|
| **Central** | 与 Central 服务相关的命令。 |
| **cluster** | 与集群相关的命令。 |
| **collector** | 与 Collector 服务相关的命令。 |
| **completion** | 生成 shell 补全脚本。 |
| **declarative-config** | 管理声明性配置。 |
| **部署** | 与部署相关的命令。 |
| **helm** | 与 Red Hat Advanced Cluster Security for Kubernetes (RHACS) Helm Charts 相关的命令。 |
| **image** | 您可以在特定镜像中运行的命令。 |
| **netpol** | 与网络策略相关的命令。 |
| **scanner** | 与 Scanner 服务相关的命令。 |
| **sensor** | 在安全集群中部署 RHACS 服务。 |
| **version** | 显示当前 roxctl 版本。 |

### 8.1.1. roxctl 命令选项

**roxctl** 命令支持以下选项：

| 选项 | 描述 |
|---|---|

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR** 环境变量设置为 **true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

## 8.2. ROXCTL CENTRAL

与 Central 服务相关的命令。

### 使用方法

```
$ roxctl central [command] [flags]
```

**表 8.2. 可用命令**

| 命令 | 描述 |
|---|---|
| **backup** | 创建 Red Hat Advanced Cluster Security for Kubernetes (RHACS)数据库和证书的备份。 |
| **cert** | 下载中央服务的证书链。 |
| **db** | 控制数据库操作。 |
| **debug** | 调试中央服务。 |
| **generate** | 生成所需的 YAML 配置文件，其中包含用于部署 Central 的编配器对象。 |
| **init-bundles** | 为 Central 初始化捆绑包。 |
| **login** | 登录 Central 实例以获取令牌。 |
| **userpki** | 管理用户证书授权提供程序。 |
| **whoami** | 显示有关当前用户及其身份验证方法的信息。 |

## 8.2.1. roxctl central 命令选项从父命令继承

**roxctl central** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
|---|---|
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e**, **--endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |

| 选项 | 描述 |
| --- | --- |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR** 环境变量设置为 **true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p**, **--password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s**, **--server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

**注意**

这些选项适用于 **roxctl central** 命令的所有子命令。

### 8.2.2. roxctl 中央备份

创建 RHACS 数据库和证书的备份。

**使用方法**

```
$ roxctl central backup [flags]
```

**表 8.3. 选项**

| 选项 | 描述 |
| --- | --- |
| **--certs-only** | 指定仅备份证书。在使用外部数据库时，这个选项用于生成带有证书的备份捆绑包。默认值为 **false**。 |
| **--output string** | 指定您要保存备份的位置。此行为取决于指定的路径：<br>● 如果路径是文件路径，则备份将写入文件，并在该文件已存在时覆盖该文件。目录必须存在。<br>● 如果路径是一个目录，则备份保存在服务器指定的文件名下。<br>● 如果省略此参数，则备份会保存在服务器指定的文件名下的当前工作目录中。 |
| **-t,--timeout 持续时间** | 指定 API 请求的超时时间。它代表请求的最长持续时间。默认值为 **1h0m0s**。 |

### 8.2.3. roxctl central cert

下载中央服务的证书链。

#### 使用方法

```
$ roxctl central cert [flags]
```

表 8.4. 选项

| 选项 | 描述 |
| --- | --- |
| **--output string** | 指定要保存 PEM 证书的文件名。您可以使用 **-** 生成标准输出。默认值为 **-**。 |
| **--retry-timeout duration** | 指定重试 API 请求超时。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1m0s**。 |

### 8.2.4. roxctl central login

登录 Central 实例以获取令牌。

#### 使用方法

```
$ roxctl central login [flags]
```

表 8.5. 选项

| 选项 | 描述 |
| --- | --- |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **5m0s**。 |

### 8.2.5. roxctl central whoami

显示有关当前用户及其身份验证方法的信息。

#### 使用方法

```
$ roxctl central whoami [flags]
```

表 8.6. 选项

| 选项 | 描述 |
| --- | --- |
| **--retry-timeout duration** | 指定重试 API 请求超时。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1m0s**。 |

### 8.2.6. roxctl central db

控制数据库操作。

#### 使用方法

```
$ roxctl central db [flags]
```

表 8.7. 选项

| 选项 | 描述 |
| --- | --- |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1h0m0s**。 |

#### 8.2.6.1. roxctl central db restore

从以前的备份中恢复 RHACS 数据库。

#### 使用方法

```
$ roxctl central db restore <file> [flags] 1
```

1 对于 **<file >**，请指定您要恢复的数据库备份文件。

表 8.8. 选项

| 选项 | 描述 |
| --- | --- |
| **-f,--force** | 如果设置为 **true**，则在没有确认的情况下执行恢复。默认值为 **false**。 |
| **--interrupt** | 如果设置为 **true**，它将中断正在运行的恢复过程，以允许它继续。默认值为 **false**。 |

#### 8.2.6.2. roxctl central db generate

生成 Central 数据库捆绑包。

**使用方法**

```
$ roxctl central db generate [flags]
```

表 8.9. 选项

| 选项 | 描述 |
| --- | --- |
| **--debug** | 如果设置为 **true**，则会从本地文件系统读取模板。默认值为 **false**。 |
| **--debug-path string** | 指定本地文件系统中的 Helm 模板路径。如需了解更多详细信息，请运行 **roxctl central db generate** 命令。 |
| **--enable-pod-security-policies** | 如果设置为 **true**，则会创建**PodSecurityPolicy** 资源。默认值为 **true**。 |

#### 8.2.6.3. roxctl central db generate k8s

生成用于部署 Central 数据库组件的 Kubernetes YAML 文件。

**使用方法**

```
$ roxctl central db generate k8s [flags]
```

表 8.10. 选项

| 选项 | 描述 |
| --- | --- |
| **--central-db-image string** | 指定您要使用的 Central 数据库镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |

| 选项 | 描述 |
| --- | --- |
| **--image-defaults string** | 指定容器镜像的默认设置。它控制从中下载镜像的存储库、镜像名称和标签格式。默认值为 **development_build**。 |
| **--output-dir 输出目录** | 指定要保存部署捆绑包的目录。默认值为 **central-db-bundle**。 |

### 8.2.6.4. roxctl central db restore cancel

取消持续的 Central 数据库恢复过程。

#### 使用方法

```
$ roxctl central db restore cancel [flags]
```

**表 8.11. 选项**

| 选项 | 描述 |
| --- | --- |
| **f**, **--force** | 如果设置为 **true**，请在不确认的情况下继续取消。默认值为 **false**。 |

### 8.2.6.5. roxctl central db restore status

显示有关持续数据库恢复过程的信息。

#### 使用方法

```
$ roxctl central db restore status [flags]
```

### 8.2.6.6. roxctl central db generate k8s pvc

为 Central 中的持久性卷声明(PVC)生成 Kubernetes YAML 文件。

#### 使用方法

```
$ roxctl central db generate k8s pvc [flags]
```

**表 8.12. 选项**

| 选项 | 描述 |
| --- | --- |
| **--name string** | 指定 Central 数据库的外部卷名称。默认值为 **central-db**。 |
| **--size uint32** | 为 Central 数据库指定外部卷大小（以 GB 为单位）。默认值为 **100**。 |

| 选项 | 描述 |
| --- | --- |
| **--storage-class string** | 指定 Central 数据库的存储类名称。如果您配置了默认存储类，则这是可选的。 |

### 8.2.6.7. roxctl central db generate openshift

生成 OpenShift YAML 清单，用于在 Red Hat OpenShift 集群上部署中央数据库实例。

#### 使用方法

```
$ roxctl central db generate openshift [flags]
```

表 8.13. 选项

| 选项 | 描述 |
| --- | --- |
| **--central-db-image string** | 指定您要使用的 Central 数据库镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |
| **--image-defaults string** | 指定容器镜像的默认设置。它控制从中下载镜像的存储库、镜像名称和标签格式。默认值为 **development_build**。 |
| **--openshift-version int** | 为部署指定 Red Hat OpenShift 主版本 3 或 4。默认值为 **3**。 |
| **--output-dir output-directory** | 指定要保存部署捆绑包的目录。默认值为 **central-db-bundle**。 |

### 8.2.6.8. roxctl central db generate k8s hostpath

为在 Central 中带有 hostpath 卷类型的数据库部署生成 Kubernetes YAML 清单。

#### 使用方法

```
$ roxctl central db generate k8s hostpath [flags]
```

表 8.14. 选项

| 选项 | 描述 |
| --- | --- |
| **--hostpath string** | 指定主机上的路径。默认值为 **/var/lib/stackrox-central-db**。 |
| **--node-selector-key 字符串** | 指定节点选择器键。有效值包括 **kubernetes.io** 和 **hostname**。 |

| 选项 | 描述 |
| --- | --- |
| **--node-selector-value string** | 指定节点选择器值。 |

### 8.2.6.9. roxctl central db generate openshift pvc

使用 Central 中的持久性卷声明(PVC)为数据库部署生成 OpenShift YAML 清单。

#### 使用方法

```
$ roxctl central db generate openshift pvc [flags]
```

表 8.15. 选项

| 选项 | 描述 |
| --- | --- |
| --name string | 指定 Central 数据库的外部卷名称。默认值为 **central-db**。 |
| --size uint32 | 为 Central 数据库指定外部卷大小（以 GB 为单位）。默认值为 **100**。 |
| --storage-class string | 指定 Central 数据库的存储类名称。如果您配置了默认存储类，则这是可选的。 |

### 8.2.6.10. roxctl central db generate openshift hostpath

将 hostpath 外部卷添加到 Central 数据库。

#### 使用方法

```
$ roxctl central db generate openshift hostpath [flags]
```

表 8.16. 选项

| 选项 | 描述 |
| --- | --- |
| **--hostpath string** | 指定主机上的路径。默认值为 **/var/lib/stackrox-central-db**。 |
| **--node-selector-key 字符串** | 指定节点选择器键。有效值包括 **kubernetes.io** 和 **hostname**。 |
| **--node-selector-value string** | 指定节点选择器值。 |

## 8.2.7. roxctl central debug

调试中央服务。

**使用方法**

```
$ roxctl central debug [flags]
```

#### 8.2.7.1. roxctl central debug db

控制数据库的调试。

**使用方法**

```
$ roxctl central debug db [flags]
```

**表 8.17. 选项**

| 选项 | 描述 |
| --- | --- |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1m0s**。 |

#### 8.2.7.2. roxctl central debug log

检索当前的日志级别。

**使用方法**

```
$ roxctl central debug log [flags]
```

**表 8.18. 选项**

| 选项 | 描述 |
| --- | --- |
| **-l, --level string** | 指定要设置模块的日志级别。有效值包括 **Debug**,**Info**,**Warn**,**Error**,**Panic**, 和 **Fatal**。 |
| **-m,--modules 字符串** | 指定要应用命令的模块。 |
| **--retry-timeout duration** | 指定重试 API 请求超时。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 指定 API 请求的超时时间，这是请求的最长持续时间。默认值为 **1m0s**。 |

#### 8.2.7.3. roxctl central debug dump

下载包含 Central 的调试信息的捆绑包。

**使用方法**

```
$ roxctl central debug dump [flags]
```

表 8.19. 选项

| 选项 | 描述 |
| --- | --- |
| **--logs** | 如果设置为 **true**，则日志会包含在 Central 转储中。默认值为 **false**。 |
| **--output-dir string** | 指定捆绑包内容的输出目录。默认值是当前目录中自动生成的目录名称。 |
| **-t,--timeout 持续时间** | 指定 API 请求的超时时间，这是请求的最长持续时间。默认值为 **5m0s**。 |

### 8.2.7.4. roxctl central debug db stats

控制 Central 数据库的统计信息。

**使用方法**

```
$ roxctl central debug db stats [flags]
```

### 8.2.7.5. roxctl central debug authz-trace

在 Central 中启用或禁用授权追踪以进行调试。

**使用方法**

```
$ roxctl central debug authz-trace [flags]
```

表 8.20. 选项

| 选项 | 描述 |
| --- | --- |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **20m0s**。 |

### 8.2.7.6. roxctl central debug db stats reset

重置 Central 数据库的统计信息。

**使用方法**

```
$ roxctl central debug db stats reset [flags]
```

### 8.2.7.7. roxctl central debug download-diagnostics

下载包含平台诊断信息的快照的捆绑包。

**使用方法**

```
$ roxctl central debug download-diagnostics [flags]
```

表 8.21. 选项

| 选项 | 描述 |
| --- | --- |
| **--clusters string** | 指定您要从中收集日志的 Sensor 集群的逗号分隔列表。 |
| **--output-dir string** | 指定要保存诊断捆绑包的输出目录。 |
| **--since string** | 指定您要从 Sensor 集群收集日志的时间戳。 |
| **-t,--timeout 持续时间** | 指定 API 请求的超时时间，指定请求的最长持续时间。默认值为 **5m0s**。 |

### 8.2.8. roxctl central generate

生成所需的 YAML 配置文件，其中包含用于部署 Central 的编配器对象。

#### 使用方法

```
$ roxctl central generate [flags]
```

表 8.22. 选项

| 选项 | 描述 |
| --- | --- |
| **--backup-bundle string** | 指定要恢复密钥和证书的备份捆绑包的路径。 |
| **--debug** | 如果设置为 **true**，则会从本地文件系统读取模板。默认值为 **false**。 |
| **--debug-path string** | 指定本地文件系统中的 Helm 模板路径。如需了解更多详细信息，请运行 **roxctl central generate --help** 命令。 |
| **--default-tls-certfile** | 指定您要用作默认值的 PEM 证书捆绑包文件。 |
| **--default-tls-keyfile** | 指定您要用作默认值的 PEM 私钥文件。 |
| **--enable-pod-security-policies** | 如果设置为 **true**，则会创建**PodSecurityPolicy** 资源。默认值为 **true**。 |
| **-p, --password string** | 指定管理员密码。默认值会自动生成。 |
| **--plaintext-endpoints string** | 指定您要用于未加密的暴露的端口或端点，作为逗号分隔的列表。 |

#### 8.2.8.1. roxctl central generate k8s

生成所需的 YAML 配置文件，以将 Central 部署到 Kubernetes 集群中。

**使用方法**

```
$ roxctl central generate k8s [flags]
```

表 8.23. 选项

| 选项 | 描述 |
| --- | --- |
| **--central-db-image string** | 指定您要使用的 Central 数据库镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |
| **--declarative-config-config-maps strings** | 指定您要添加为 Central 中的声明性配置挂载的配置映射列表。 |
| **--declarative-config-secrets strings** | 指定您要作为声明性配置挂载添加到 Central 中的 secret 列表。 |
| **--enable-telemetry** | 指定是否要启用遥测。默认值为 **false**。 |
| **--image-defaults string** | 指定容器镜像的默认设置。指定设置控制从中下载镜像的存储库、镜像名称和标签格式。默认值为 **development_build**。 |
| **--istio-support version** | 生成支持指定 Istio 版本的部署文件。有效值包括 1.0,**1.1 , 1.2**,**1.3**,**1.4**,**1.5**,**1.6**, 和 **1.7**。 |
| **--lb-type 负载均衡器类型** | 指定要暂停 Central 的方法。有效值包括 **lb**、**np** 和 **none**。默认值为 **none**。 |
| **-i,--main-image string** | 指定您要使用的主镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |
| **--offline** | 指定是否要以离线模式运行 RHACS，避免连接到互联网。默认值为 **false**。 |
| **--output-dir 输出目录** | 指定要保存部署捆绑包的目录。默认值为 **central-bundle**。 |

| 选项 | 描述 |
| --- | --- |
| **--output-format 输出格式** | 指定您要使用的部署工具。有效值包括 **kubectl**、**helm** 和 **helm-values**。默认值为 **kubectl**。 |
| **--scanner-db-image string** | 指定您要使用的 Scanner 数据库镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |
| **--scanner-image string** | 指定您要使用的 Scanner 镜像。如果没有指定，则使用与 '--image-defaults" 对应的默认值。 |

#### 8.2.8.2. roxctl central generate k8s pvc

为 Central 中的持久性卷声明(PVC)生成 Kubernetes YAML 文件。

**使用方法**

```
$ roxctl central generate k8s pvc [flags]
```

表 8.24. 选项

| 选项 | 描述 |
| --- | --- |
| **--db-name string** | 指定 Central 数据库的外部卷名称。默认值为 **central-db**。 |
| **--db-size uint32** | 为 Central 数据库指定外部卷大小（以 GB 为单位）。默认值为 **100**。 |
| **--db-storage-class string** | 指定 Central 数据库的存储类名称。如果您配置了默认存储类，则这是可选的。 |
| **--name string** | 指定 Central 的外部卷名称。默认值为 **stackrox-db**。 |
| **--size uint32** | 为 Central 指定外部卷大小（以 GB 为单位）。默认值为 **100**。 |
| **--storage-class string** | 指定 Central 的存储类名称。如果您配置了默认存储类，则这是可选的。 |

#### 8.2.8.3. roxctl central generate openshift

生成所需的 YAML 配置文件以在 Red Hat OpenShift 集群中部署 Central。

**使用方法**

-

```
$ roxctl central generate openshift [flags]
```

表 8.25. 选项

| 选项 | 描述 |
| --- | --- |
| **--central-db-image string** | 指定您要使用的 Central 数据库镜像。如果没有指定，则会创建一个与 **--image-defaults** 对应的默认值。 |
| **--declarative-config-config-maps strings** | 指定您要添加为 Central 中的声明性配置挂载的配置映射列表。 |
| **--declarative-config-secrets strings** | 指定您要作为声明性配置挂载添加到 Central 中的 secret 列表。 |
| **--enable-telemetry** | 指定是否要启用遥测。默认值为 **false**。 |
| **--image-defaults string** | 指定容器镜像的默认设置。它控制从中下载镜像的存储库、镜像名称和标签格式。默认值为 **development_build**。 |
| **--istio-support version** | 生成支持指定 Istio 版本的部署文件。有效值包括 1.0,**1.1 , 1.2**,**1.3**,**1.4**,**1.5**,**1.6**, 和 **1.7**。 |
| **--lb-type 负载均衡器类型** | 指定公开 Central 的方法。有效值包括 **route**、**lb**、**np** 和 **none**。默认值为 **none**。 |
| **-i,--main-image string** | 指定您要使用的主镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |
| **--offline** | 指定是否要以离线模式运行 RHACS，避免连接到互联网。默认值为 **false**。 |
| **--openshift-monitoring false\|true\|auto[=true]** | 指定与 Red Hat OpenShift 4 监控的集成。默认值为 **auto**。 |
| **--openshift-version int** | 为部署指定 Red Hat OpenShift 主版本 3 或 4。 |
| **--output-dir 输出目录** | 指定要保存部署捆绑包的目录。默认值为 **central-bundle**。 |

| 选项 | 描述 |
| --- | --- |
| **--output-format 输出格式** | 指定您要使用的部署工具。有效值包括 **kubectl**、**helm** 和 **helm-values**。默认值为 **kubectl**。 |
| **--scanner-db-image string** | 指定您要使用的 Scanner 数据库镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |
| **--scanner-image string** | 指定您要使用的 Scanner 镜像。如果没有指定，则使用与 **--image-defaults** 对应的默认值。 |

#### 8.2.8.4. roxctl central generate interactive

在 Central 中生成交互式资源。

**使用方法**

```
$ roxctl central generate interactive [flags]
```

#### 8.2.8.5. roxctl central generate k8s hostpath

使用 hostpath 卷类型，生成 Kubernetes YAML 清单以部署 Central 实例。

**使用方法**

```
$ roxctl central generate k8s hostpath [flags]
```

表 8.26. 选项

| 选项 | 描述 |
| --- | --- |
| **--db-hostpath string** | 指定中央数据库主机上的路径。默认值为 **/var/lib/stackrox-central**。 |
| **--db-node-selector-key string** | 指定 Central 数据库的节点选择器键。有效值包括 **kubernetes.io** 和 **hostname**。 |
| **--db-node-selector-value string** | 指定 Central 数据库的节点选择器值。 |
| **--hostpath string** | 指定主机上的路径。默认值为 **/var/lib/stackrox**。 |

| 选项 | 描述 |
| --- | --- |
| **--node-selector-key 字符串** | 指定节点选择器键。有效值包括 **kubernetes.io** 和 **hostname**。 |
| **--node-selector-value string** | 指定节点选择器值。 |

### 8.2.8.6. roxctl central generate openshift pvc

生成 OpenShift YAML 清单，以在 Central 中部署持久性卷声明(PVC)。

#### 使用方法

```
$ roxctl central generate openshift pvc [flags]
```

表 8.27. 选项

| 选项 | 描述 |
| --- | --- |
| **--db-name string** | 指定 Central 数据库的外部卷名称。默认值为 **central-db**。 |
| **--db-size uint32** | 为 Central 数据库指定外部卷大小（以 GB 为单位）。默认值为 **100**。 |
| **--db-storage-class string** | 指定 Central 数据库的存储类名称。如果您配置了默认存储类，则这是可选的。 |
| **--name string** | 指定 Central 的外部卷名称。默认值为 **stackrox-db**。 |
| **--size uint32** | 为 Central 指定外部卷大小（以 GB 为单位）。默认值为 **100**。 |
| **--storage-class string** | 指定 Central 的存储类名称。如果您配置了默认存储类，则这是可选的。 |

### 8.2.8.7. roxctl central generate openshift hostpath

将 hostpath 外部卷添加到 Red Hat OpenShift 中的部署定义中。

#### 使用方法

```
$ roxctl central generate openshift hostpath [flags]
```

表 8.28. 选项

| 选项 | 描述 |
| --- | --- |
| **--db-hostpath string** | 指定中央数据库主机上的路径。默认值为 **/var/lib/stackrox-central**。 |
| **--db-node-selector-key string** | 指定节点选择器键。有效值包括 Central 数据库的 **kubernetes.io** 和 **hostname**。 |
| **--db-node-selector-value string** | 指定 Central 数据库的节点选择器值。 |
| **--hostpath string** | 指定主机上的路径。默认值为 **/var/lib/stackrox**。 |
| **--node-selector-key 字符串** | 指定节点选择器键。有效值包括 **kubernetes.io** 和 **hostname**。 |
| **--node-selector-value string** | 指定节点选择器值。 |

### 8.2.9. roxctl central init-bundles

在 Central 中初始化捆绑包。

#### 使用方法

```
$ roxctl central init-bundles [flag]
```

表 8.29. 选项

| 选项 | 描述 |
| --- | --- |
| **--retry-timeout duration** | 指定重试 API 请求超时。值 **0 表示** 在不重试的情况下等待整个请求持续时间。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1m0s**。 |

#### 8.2.9.1. roxctl central init-bundles list

列出 Central 中的可用初始化捆绑包。

#### 使用方法

```
$ roxctl central init-bundles list [flags]
```

#### 8.2.9.2. roxctl central init-bundles revoke

在 Central 中撤销一个或多个集群初始化捆绑包。

**使用方法**

```
$ roxctl central init-bundles revoke <init_bundle_ID or name> [<init_bundle_ID or name> ...] [flags]
```
1

1 对于 **<init_bundle_ID 或 name >**，请指定您要撤销的初始化捆绑包的 ID 或名称。您可以使用空格提供多个 ID 或名称。

### 8.2.9.3. roxctl central init-bundles fetch-ca

从 Central 获取证书颁发机构(CA)捆绑包。

**使用方法**

```
$ roxctl central init-bundles fetch-ca [flags]
```

表 8.30. 选项

| 选项 | 描述 |
| --- | --- |
| **--output string** | 指定您要用来存储 CA 配置的文件。 |

### 8.2.9.4. roxctl central init-bundles generate

生成新的集群初始化捆绑包。

**使用方法**

```
$ roxctl central init-bundles generate <init_bundle_name> [flags]
```
1

1 对于 **<init_bundle_name >**，请指定您要生成的初始化捆绑包的名称。

表 8.31. 选项

| 选项 | 描述 |
| --- | --- |
| **--output string** | 指定您要用来以 Helm 配置的形式存储新生成的初始化捆绑包的文件。您可以使用 **-** 生成标准输出。 |
| **--output-secrets 字符串** | 指定您要用来以 Kubernetes secret 格式存储新生成的初始化捆绑包的文件。您可以使用 **-** 生成标准。 |

## 8.2.10. roxctl central userpki

管理用户证书授权提供程序。

**使用方法**

```
$ roxctl central userpki [flags]
```

#### 8.2.10.1. roxctl central userpki list

显示所有用户证书身份验证提供程序。

**使用方法**

```
$ roxctl central userpki list [flags]
```

表 8.32. 选项

| 选项 | 描述 |
|---|---|
| **-j, --json** | 启用 JSON 输出。默认值为 **false**。 |
| **--retry-timeout duration** | 指定重试 API 请求超时。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1m0s**。 |

#### 8.2.10.2. roxctl central userpki create

创建新用户证书身份验证提供程序。

**使用方法**

```
$ roxctl central userpki create name [flags]
```

表 8.33. 选项

| 选项 | 描述 |
|---|---|
| **-c, --cert strings** | 指定 root CA 证书的 PEM 文件。您可以指定几个证书文件。 |
| **--retry-timeout duration** | 指定重试 API 请求超时。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-r, --role string** | 指定此提供程序用户的最小访问角色。 |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1m0s**。 |

#### 8.2.10.3. roxctl central userpki delete

删除用户证书身份验证提供程序。

### 使用方法

```
$ roxctl central userpki delete id|name [flags]
```

表 8.34. 选项

| 选项 | 描述 |
| --- | --- |
| **-f,--force** | 如果设置为 **true**，请在不确认的情况下继续删除。默认值为 **false**。 |
| **--retry-timeout duration** | 指定重试 API 请求超时。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 指定代表请求最长持续时间的 API 请求超时。默认值为 **1m0s**。 |

## 8.3. ROXCTL CLUSTER

与集群相关的命令。

### 使用方法

```
$ roxctl cluster [command] [flags]
```

表 8.35. 可用命令

| 命令 | 描述 |
| --- | --- |
| **delete** | 从 Central 中删除 Sensor。 |

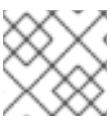
表 8.36. 选项

| 选项 | 描述 |
| --- | --- |
| **--retry-timeout duration** | 为 API 请求设置重试超时。值为零表示完整请求持续时间在无需重试的情况下被等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **1m0s**。 |

### 8.3.1. roxctl cluster 命令选项从父命令继承

**roxctl cluster** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e**, **--endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR** 环境变量设置为 **true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p**, **--password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s**, **--server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |



**注意**

这些选项适用于 **roxctl cluster** 命令的所有子命令。

### 8.3.2. roxctl cluster delete

从 Central 中删除 Sensor。

#### 使用方法

```
$ roxctl cluster delete [flags]
```

表 8.37. 选项

| 选项 | 描述 |
| --- | --- |
| **--name string** | 指定要删除的集群名称。 |

## 8.4. ROXCTL 收集器

与 Collector 服务相关的命令。

#### 使用方法

```
$ roxctl collector [command] [flags]
```

表 8.38. 可用命令

| 命令 | 描述 |
| --- | --- |
| **support-packages** | 上传 Collector 的支持软件包。 |

### 8.4.1. roxctl collector 命令选项从父命令继承

**roxctl collector** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR** 环境变量设置为 **true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

**注意**

这些选项适用于 **roxctl collector** 命令的所有子命令。

### 8.4.2. roxctl 收集器 support-packages

上传 Collector 的支持软件包。

**使用方法**

```
$ roxctl collector support-packages [flags]
```

#### 8.4.2.1. roxctl 收集器支持软件包上传

将文件从 Collector 支持软件包上传到 Central。

**使用方法**

```
$ roxctl collector support-packages upload [flags]
```

表 8.39. 选项

| 选项 | 描述 |
| --- | --- |
| **--overwrite** | 指定是否要覆盖现有的文件，但要覆盖不同的文件。默认值为 **false**。 |
| **--retry-timeout duration** | 设置 API 请求被重试的超时时间。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 设置 API 请求的超时时间。这个选项代表请求的最长持续时间。默认值为 **1m0s**。 |

## 8.5. ROXCTL COMPLETION

生成 shell 补全脚本。

### 使用方法

```
$ roxctl completion [bash|zsh|fish|powershell]
```

表 8.40. 支持的 shell 类型

| shell 类型 | 描述 |
| --- | --- |
| **bash** | 为 Bash shell 生成完成脚本。 |
| **zsh** | 为 Zsh shell 生成完成脚本。 |
| **fish** | 为 Fish shell 生成完成脚本。 |
| **PowerShell** | 为 PowerShell shell 生成完成脚本。 |

### 8.5.1. roxctl completion 命令选项从父命令继承

**roxctl completion** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR** 环境变量设置为 **true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

## 8.6. ROXCTL DECLARATIVE-CONFIG

管理声明性配置。

### 使用方法

```
$ roxctl declarative-config [command] [flags]
```

**表 8.41. 可用命令**

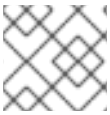
| 命令 | 描述 |
| --- | --- |
| **create** | 创建声明性配置。 |
| **lint** | lint 现有的声明性配置 YAML 文件。 |

### 8.6.1. roxctl declarative-config 命令选项从父命令继承

**roxctl declarative-config** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR 环境变量设置为 true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |



**注意**

这些选项适用于 **roxctl declarative-config** 命令的所有子命令。

### 8.6.2. roxctl declarative-config lint

lint 现有的声明性配置 YAML 文件。

**使用方法**

```
$ roxctl declarative-config lint [flags]
```

**表 8.42. 选项**

| 选项 | 描述 |
| --- | --- |
| **--config-map string** | 从 **--config-map 字符串** 中读取声明性配置。如果没有指定，则使用 **--file** 标志从指定的 YAML 文件中读取配置。 |
| **-f, --file string** | 包含 YAML 格式的声明性配置的文件。 |
| **--namespace string** | 从配置映射的 **--namespace 字符串** 读取声明性配置。如果没有指定，则使用当前 Kubernetes 配置上下文中指定的命名空间。 |
| **--secret string** | 从指定的 **--secret 字符串** 中读取声明性配置。如果没有指定，则使用 **--file** 标志从指定的 YAML 文件中读取配置。 |

### 8.6.3. roxctl declarative-config create

创建声明性配置。

**使用方法**

```
$ roxctl declarative-config create [flags]
```

**表 8.43. 选项**

| 选项 | 描述 |
| --- | --- |
| **--config-map string** | 在配置映射中编写声明性配置 YAML。如果没有指定，并且未指定 **--secret** 标志，则生成的 YAML 将以标准输出格式打印。 |
| **--namespace string** | 如果要将声明性配置 YAML 写入配置映射或 secret，则需要此项。如果没有指定，则使用当前 Kubernetes 配置中的 default 命名空间。 |
| **--secret string** | 在 Secret 中编写声明性配置 YAML。您必须使用 secret 进行敏感数据。如果没有指定，并且没有指定 **--config-map** 标志，则生成的 YAML 将以标准输出格式打印。 |

#### 8.6.3.1. roxctl declarative-config create role

为角色创建声明性配置。

**使用方法**

```
$ roxctl declarative-config create role [flags]
```

表 8.44. 选项

| 选项 | 描述 |
| --- | --- |
| **--access-scope string** | 通过提供名称，您可以指定引用的访问范围。 |
| **--description string** | 设置角色的描述。 |
| **--name string** | 指定角色的名称。 |
| **--permission-set string** | 通过提供名称，您可以指定引用的权限集。 |

#### 8.6.3.2. roxctl declarative-config create notifier

为通知程序创建声明性配置。

**使用方法**

```
$ roxctl declarative-config create notifier [flags]
```

表 8.45. 选项

| 选项 | 描述 |
| --- | --- |
| **--name string** | 指定通知程序的名称。 |

### 8.6.3.3. roxctl declarative-config create access-scope

为访问范围创建声明性配置。

#### 使用方法

```
$ roxctl declarative-config create access-scope [flags]
```

表 8.46. 选项

| 选项 | 描述 |
| --- | --- |
| **--cluster-label-selector 要求** | 指定根据集群标签创建标签选择器的条件。键值对代表要求，您可以多次使用此标志来创建要求组合。默认值为 **[ [ ] ]**。如需了解更多详细信息，请运行 **roxctl declarative-config create access-scope --help** 命令。 |
| **--description string** | 设置访问范围的描述。 |
| **--included included-object** | 指定访问范围中包含的集群及其命名空间列表。默认值为 **[null]**。 |
| **--name string** | 指定访问范围的名称。 |
| **--namespace-label-selector requirement** | 指定基于命名空间标签创建标签选择器的条件。与 cluster-label-selector 类似，您可以多次使用此标志来满足要求的组合。如需了解更多详细信息，请运行 **roxctl declarative-config create access-scope --help** 命令。 |

### 8.6.3.4. roxctl declarative-config create auth-provider

为身份验证提供程序创建声明性配置。

#### 使用方法

```
$ roxctl declarative-config create auth-provider [flags]
```

表 8.47. 选项

| 选项 | 描述 |
| --- | --- |
| **--extra-ui-endpoints strings** | 指定使用身份验证提供程序的其他用户界面(UI)端点。预期格式为 **<endpoint>:<port>**。 |

| 选项 | 描述 |
| --- | --- |
| **--groups-key string** | 设置要在身份验证供应商中添加的组的密钥。key、value 和 role 的元组应该具有相同的长度。如需了解更多详细信息，请运行 **roxctl declarative-config create auth-provider --help** 命令。 |
| **--groups-role string** | 设置要在身份验证供应商中添加的组的角色。key、value 和 role 的元组应该具有相同的长度。如需了解更多详细信息，请运行 **roxctl declarative-config create auth-provider --help** 命令。 |
| **--groups-value strings** | 设置要在身份验证供应商中添加的组值。key、value 和 role 的元组应该具有相同的长度。如需了解更多详细信息，请运行 **roxctl declarative-config create auth-provider --help** 命令。 |
| **--minimum-access-role string** | 设置身份验证提供程序的最小访问角色。如果您不想使用声明性配置配置最小访问角色，您可以将此字段留空。 |
| **--name string** | 指定身份验证供应商的名称。 |
| **--required-attributes stringToString** | 设置身份验证提供程序必须在身份验证过程中返回的属性列表。默认值为 **[]**。 |
| **--ui-endpoint string** | 设置使用身份验证供应商的 UI 端点。这通常是提供 RHACS 的公共端点。预期格式为 **<endpoint>:<port>**。 |

### 8.6.3.5. roxctl declarative-config create permission-set

为权限集创建声明性配置。

#### 使用方法

```
$ roxctl declarative-config create permission-set [flags]
```

**表 8.48. 选项**

| 选项 | 描述 |
| --- | --- |
| **--description string** | 设置权限集的描述。 |
| **--name string** | 指定权限集的名称。 |
| **--resource-with-access stringToString** | 设置具有相应访问级别的资源列表。默认值为 **[]**。如需了解更多详细信息，请运行 **roxctl declarative-config create permission-set --help** 命令。 |

### 8.6.3.6. roxctl declarative-config create notifier mvapich

为 zFCP 通知程序创建声明性配置。

**使用方法**

```
$ roxctl declarative-config create notifier splunk [flags]
```

**表 8.49. 选项**

| 选项 | 描述 |
| --- | --- |
| **--audit-logging** | 启用审计日志记录。默认值为 **false**。 |
| **--source-types stringToString** | 将 Splunk 源类型指定为用逗号分开的 **key=value** 对。默认值为 **[]**。 |
| **--splunk-endpoint string** | 指定 Splunk HTTP 端点。这是强制选项。 |
| **--splunk-skip-tls-verify** | 使用到 Splunk 的不安全连接。默认值为 **false**。 |
| **--splunk-token string** | 指定 Splunk HTTP 令牌。这是强制选项。 |
| **--truncate int** | 指定 Splunk truncate 限制。默认值为 **10000**。 |

### 8.6.3.7. roxctl declarative-config create notifier generic

为通用通知程序创建声明性配置。

**使用方法**

```
$ roxctl declarative-config create notifier generic [flags]
```

**表 8.50. 选项**

| 选项 | 描述 |
| --- | --- |
| **--audit-logging** | 启用审计日志记录。默认值为 **false**。 |
| **--extra-fields stringToString** | 将其他字段指定为用逗号分开的 **key=value** 对。默认值为 **[]**。 |
| **--headers stringToString** | 将标头指定为用逗号分开的 **key=value** 对。默认值为 **[]**。 |
| **--webhook-cacert-file string** | 以 PEM 格式指定端点 CA 证书的文件名。 |
| **--webhook-endpoint string** | 指定 webhook 端点的 URL。 |
| **--webhook-password string** | 指定 webhook 端点基本身份验证的密码。如果没有指定身份验证。需要 **--webhook-username**。 |
| **--webhook-skip-tls-verify** | 跳过 Webhook TLS 验证。默认值为 **false**。 |
| **--webhook-username string** | 指定 webhook 端点基本身份验证的用户名。如果没有指定身份验证，则不会进行身份验证。需要 **--webhook-password**。 |

### 8.6.3.8. roxctl declarative-config create auth-provider iap

使用身份感知代理(IAP)标识符为身份验证供应商创建声明配置。

#### 使用方法

```
$ roxctl declarative-config create auth-provider iap [flags]
```

表 8.51. 选项

| 选项 | 描述 |
| --- | --- |
| **--audience 字符串** | 指定您要验证的目标组。 |

### 8.6.3.9. roxctl declarative-config create auth-provider oidc

为 OpenID Connect (OIDC)身份验证供应商创建声明性配置。

#### 使用方法

```
$ roxctl declarative-config create auth-provider oidc [flags]
```

表 8.52. 选项

| 选项 | 描述 |
| --- | --- |
| **--claim-mappings stringToString** | 指定您要包含在身份验证提供程序规则中的身份提供程序(IdP)令牌中的非标准声明列表。默认值为 **[]**。 |
| **--client-id string** | 指定 OIDC 客户端的客户端 ID。 |
| **--client-secret string** | 指定 OIDC 客户端的客户端 secret。 |
| **--disable-offline-access** | 从 OIDC IdP 禁用 offline_access 的请求。如果 OIDC IdP 使用 **offline_access** 范围限制了会话数量，则需要使用这个选项。默认值为 **false**。 |
| **--issuer 字符串** | 指定 OIDC 客户端的签发者。 |
| **--mode string** | 指定您要使用的回调模式。有效值包括 **auto**、**post**、**query** 和 **fragment**。默认值为 **auto**。 |

### 8.6.3.10. roxctl declarative-config create auth-provider saml

为 SAML 身份验证供应商创建声明性配置。

#### 使用方法

```
$ roxctl declarative-config create auth-provider saml [flags]
```

表 8.53. 选项

| 选项 | 描述 |
| --- | --- |
| **--idp-cert string** | 以 PEM 格式指定包含 SAML 身份提供程序(IdP)证书的文件。 |
| **--idp-issuer string** | 指定 IdP 的签发者。 |
| **--metadata-url string** | 指定服务提供商的元数据 URL。 |
| **--name-id-format string** | 指定名称 ID 的格式。 |
| **--SP-issuer 字符串** | 指定服务提供商的签发者。 |
| **--sso-url string** | 为单点登录(SSO)指定 IdP 的 URL。 |

#### 8.6.3.11. roxctl declarative-config create auth-provider userpki

为用户 PKI 身份验证提供程序创建声明配置。

**使用方法**

```
$ roxctl declarative-config create auth-provider userpki [flags]
```

**表 8.54. 选项**

| 选项 | 描述 |
| --- | --- |
| **--ca-file string** | 以 PEM 格式指定包含证书颁发机构的文件。 |

#### 8.6.3.12. roxctl declarative-config create auth-provider openshift-auth

为 OpenShift Container Platform OAuth 身份验证供应商创建声明性配置。

**使用方法**

```
$ roxctl declarative-config create auth-provider openshift-auth [flags]
```

## 8.7. ROXCTL 部署

与部署相关的命令。

**使用方法**

```
$ roxctl deployment [command] [flags]
```

**表 8.55. 可用命令**

| 命令 | 描述 |
| --- | --- |
| **check** | 检查部署是否有部署时间策略。 |

**表 8.56. 选项**

| 选项 | 描述 |
| --- | --- |
| **-t,--timeout 持续时间** | 设置 API 请求的超时时间。这个选项代表请求的最长持续时间。默认值为 **10m0s**。 |

### 8.7.1. roxctl 部署命令选项从父命令继承

**roxctl 部署命令** 支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR 环境变量设置为 true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

**注意**

这些选项适用于 **roxctl 部署命令** 的所有子命令。

### 8.7.2. roxctl 部署检查

检查部署是否有部署时间策略。

#### 使用方法

```
$ roxctl deployment check [flags]
```

表 8.57. 选项

| 选项 | 描述 |
| --- | --- |
| **-c, --categories strings** | 定义您要执行的策略类别。默认情况下执行所有策略类别。 |
| **--cluster string** | 设置您要用作评估上下文的集群名称或 ID，以使用特定于集群的信息启用扩展部署。 |
| **--compact-output** | 以紧凑的形式打印 JSON 输出。默认值为 **false**。 |
| **-f, --file stringArray** | 指定要发送到 Central 进行策略评估的 YAML 文件。 |
| **--force** | 绕过镜像的 Central 缓存，并强制从 Scanner 进行新的拉取。默认值为 **false**。 |
| **--headers string** | 定义要在表格化输出中打印的标头。默认值包括 **POLICY**,**SEVERITY**,**BREAKS DEPLOY**,**DEPLOYMENT**,**DESCRIPTION**,**VIOLATION**, 和 **REMEDIATION**。 |
| **--headers-as-comments** | 在 CSV 标签页化输出中将标头打印为注释。默认值为 **false**。 |
| **--junit-suite-name string** | 设置 JUnit 测试套件的名称。默认值为 **deployment-check**。 |
| **--merge-output** | 在 tabular 输出中合并重复单元。默认值为 **false**。 |
| **-n,--namespace string** | 指定命名空间，以使用上下文信息（如网络策略、RBAC 和服务）来增强部署，以便在规格中没有命名空间。规范中定义的命名空间不会改变。默认值为 **default**。 |
| **--no-header** | 不要打印表格输出的标头。默认值为 **false**。 |
| **-o,--output string** | 选择输出格式。输出格式包括 **json**、**junit**、**sarif**、**table**、**csv** 和 csv。默认值为 **table**。 |
| **-r,--retries int** | 设置退出作为错误前的重试次数。默认值为 **3**。 |

| 选项 | 描述 |
| --- | --- |
| **-d**, **--retry-delay int** | 设置重试之间等待的时间（以秒为单位）。默认值为 **3**。 |
| **--row-jsonpath-expressions string** | 定义从 JSON 对象创建行的 JSON 路径表达式。如需了解更多详细信息，请运行 **roxctl deployment check --help** 命令。 |

## 8.8. ROXCTL HELM

与 Red Hat Advanced Cluster Security for Kubernetes (RHACS) Helm Charts 相关的命令。

### 使用方法

```
$ roxctl helm [command] [flags]
```

**表 8.58. 可用命令**

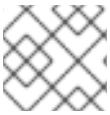
| 命令 | 描述 |
| --- | --- |
| **derive-local-values** | 从集群配置中获取本地 Helm 值。 |
| **output** | 输出 Helm Chart。 |

### 8.8.1. roxctl helm 命令选项从父命令继承

**roxctl helm** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e**, **--endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR** 环境变量设置为 **true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |



**注意**

这些选项适用于 **roxctl helm** 命令的所有子命令。

### 8.8.2. roxctl helm output

输出 Helm Chart。

#### 使用方法

```
$ roxctl helm output <central_services or secured_cluster_services> [flags]
```
1

1 对于 **<central_services 或 secured_cluster_services >**，请指定中央服务的路径或安全集群服务来生成 Helm Chart 输出。

**表 8.59. 选项**

| 选项 | 描述 |
| --- | --- |
| **--debug** | 从本地文件系统读取模板。默认值为 **false**。 |
| **--debug-path string** | 指定本地文件系统上的 Helm 模板的路径。如需了解更多详细信息，请运行 **roxctl helm output --help** 命令。 |
| **--image-defaults string** | 设置默认容器镜像设置。镜像设置包括 **development_build**、**stackrox.io**、**rhacs** 和 **opensource**。它会影响镜像下载、镜像名称和标签格式的存储库。默认值为 **development_build**。 |
| **--output-dir string** | 定义 Helm Chart 的输出目录的路径。默认路径为 **./stackrox-<chart name>-chart**。 |
| **--remove** | 删除输出目录（如果已存在）。默认值为 **false**。 |

### 8.8.3. roxctl helm derived-local-values

从集群配置中获取本地 Helm 值。

#### 使用方法

```
$ roxctl helm derive-local-values --output <path> \ 1
<central_services> [flags] 2
```

1 对于 <path>，请指定您要保存生成的本地值文件的路径。

2 对于 <central_services>，指定中央服务配置文件的路径。

表 8.60. 选项

| 选项 | 描述 |
| --- | --- |
| **--input string** | 指定包含 YAML 输入的文件或目录的路径。 |
| **--output string** | 定义输出文件的路径。 |
| **--output-dir string** | 定义输出目录的路径。 |
| **--retry-timeout duration** | 设置 API 请求被重试的超时时间。超时值表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **1m0s**。 |

## 8.9. ROXCTL 镜像

您可以在特定镜像中运行的命令。

### 使用方法

```
$ roxctl image [command] [flags]
```

**表 8.61. 可用命令**

| 命令 | 描述 |
| --- | --- |
| **check** | 检查镜像是否有构建时间策略违反情况，并报告它们。 |
| **扫描** | 扫描指定的镜像，并返回扫描结果。 |

表 8.62. 选项

| **-t,--timeout 持续时间** | **为代表请求最长持续时间的 API 请求设置超时。默认值为 10m0s。** |
| --- | --- |

### 8.9.1. roxctl image 命令选项从父命令继承

**roxctl image** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR 环境变量设置为 true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

**注意**

这些选项适用于 **roxctl image** 命令的所有子命令。

### 8.9.2. roxctl 镜像扫描

扫描指定的镜像，并返回扫描结果。

**使用方法**

```
$ roxctl image scan [flags]
```

表 8.63. 选项

| 选项 | 描述 |
| --- | --- |
| **--cluster string** | 指定要将镜像扫描委派给的集群名称或 ID。 |
| **--compact-output** | 以紧凑格式显示 JSON 输出。默认值为 **false**。 |
| **-f,--force** | 忽略 Central 的缓存，并强制从 Scanner 中重新拉取。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **--headers string** | 指定要在表格化输出中打印的标头。默认值包括 **COMPONENT**、**VERSION**、**CVE**、SEE**RITY** 和 **LINK**。 |
| **--headers-as-comments** | 在 CSV 标签页化输出中将标头打印为注释。默认值为 **false**。 |
| **-i,--image string** | 指定镜像名称并引用扫描。例如，**nginx:latest** 或 **nginx@sha256:...**。 |
| **-a, --include-snoozed** | 在扫描结果中包含 snoozed 和 unsnoozed CVE。默认值为 **false**。 |
| **--merge-output** | 在 tabular 输出中合并重复单元。默认值为 **true**。 |
| **--no-header** | 不要打印表格输出的标头。默认值为 **false**。 |
| **-o,--output string** | 指定输出格式。输出格式包括 **表**、**csv**、**json** 和 **sarif**。 |
| **-r,--retries int** | 指定在退出作为错误前的重试次数。默认值为 **3**。 |
| **-d, --retry-delay int** | 设置重试之间等待的时间（以秒为单位）。默认值为 **3**。 |
| **--row-jsonpath-expressions string** | 指定从 JSON 对象创建行的 JSON 路径表达式。如需了解更多详细信息，请运行 **roxctl image scan --help** 命令。 |
| **--severity 字符串** | 输出中要包含的严重性列表。使用它来过滤特定严重性。默认值包括 **LOW**、**MODERATE**、**IMPORTANT** 和 **CRITICAL**。 |

### 8.9.3. roxctl image check

检查镜像是否有构建时间策略违反情况，并报告它们。

#### 使用方法

```
$ roxctl image check [flags]
```

表 8.64. 选项

| 选项 | 描述 |
| --- | --- |
| **-c**, **--categories strings** | 您要执行的策略类别列表。默认情况下使用所有策略类别。 |
| **--cluster string** | 定义您要用作评估上下文的集群名称或 ID。 |
| **--compact-output** | 以紧凑格式显示 JSON 输出。默认值为 **false**。 |
| **-f**,**--force** | 绕过镜像的 Central 缓存，并强制从 Scanner 中进行新的拉取。默认值为 **false**。 |
| **--headers string** | 定义要在表格化输出中打印的标头。默认值包括 **POLICY**,**SEVERITY**,**BREAKS BUILD**,**DESCRIPTION**,**VIOLATION**, 和 **REMEDIATION**。 |
| **--headers-as-comments** | 在 CSV 标签页化输出中将标头打印为注释。默认值为 **false**。 |
| **-i**,**--image string** | 指定镜像名称和引用。例如，**nginx:latest** 或 **nginx@sha256:...**）。 |
| **--junit-suite-name string** | 设置 JUnit 测试套件的名称。默认值为 **image-check**。 |
| **--merge-output** | 在 tabular 输出中合并重复单元。默认值为 **false**。 |
| **--no-header** | 不要打印表格输出的标头。默认值为 **false**。 |
| **-o**,**--output string** | 选择输出格式。输出格式包括 **junit**、**sarif**、**table**、**csv** 和 **json**。默认值为 **table**。 |
| **-r**,**--retries int** | 设置退出作为错误前的重试次数。默认值为 **3**。 |
| **-d**, **--retry-delay int** | 设置重试之间等待的时间（以秒为单位）。默认值为 **3**。 |
| **--row-jsonpath-expressions string** | 使用 JSON 路径表达式从 JSON 对象创建行。如需了解更多详细信息，请运行 **roxctl image check --help** 命令。 |
| **--send-notifications** | 定义是否在出现违反情况时发送通知。默认值为 **false**。 |

## 8.10. ROXCTL NETPOL

与网络策略相关的命令。

### 使用方法

```
$ roxctl netpol [command] [flags]
```

**表 8.65. 可用命令**

| 命令 | 描述 |
| --- | --- |
| **连接性** | 网络策略资源的连接分析。 |
| **generate** | 根据部署信息推荐网络策略。 |

### 8.10.1. roxctl netpol 命令选项从父命令继承

**roxctl netpol** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR 环境变量设置为 true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

**注意**

这些选项适用于 **roxctl netpol** 命令的所有子命令。

### 8.10.2. roxctl netpol generate

根据部署信息推荐网络策略。

#### 使用方法

```
$ roxctl netpol generate <folder_path> [flags] 1
```

1 对于 **<folder_path >**，请指定包含 Kubernetes 部署和服务配置文件的目录的路径。

表 8.66. 选项

| 选项 | 描述 |
| --- | --- |
| **--fail** | 在第一次遇到的错误时失败。默认值为 **false**。 |
| **-d, --output-dir string** | 将生成的策略保存到目标文件夹中。 |
| **-f,--output-file string** | 将生成的策略保存并合并到单个 YAML 文件中。 |
| **--remove** | 删除输出路径（如果已存在）。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **--strict** | 将警告视为错误。默认值为 **false**。 |

### 8.10.3. roxctl netpol 连接

与网络策略资源连接分析相关的命令。

#### 使用方法

```
$ roxctl netpol connectivity [flags]
```

#### 8.10.3.1. roxctl netpol 连接映射

根据网络策略和其他资源分析连接。

#### 使用方法

```
$ roxctl netpol connectivity map <folder_path> [flags] 1
```

1 对于 **<folder_path >**，请指定包含 Kubernetes 部署和服务配置文件的目录的路径。

表 8.67. 选项

| 选项 | 描述 |
| --- | --- |
| **--fail** | 在第一次遇到的错误时失败。默认值为 **false**。 |
| **--focus-workload string** | 专注于输出中指定工作负载名称的连接。 |
| **-f,--output-file string** | 将连接列表输出保存到特定文件中。 |
| **-o,--output-format string** | 以特定格式配置连接列表。支持的格式包括 **txt**、**json**、**md**、**点** 和 **csv**。默认值为 **txt**。 |
| **--remove** | 删除输出路径（如果已存在）。默认值为 **false**。 |
| **--save-to-file** | 定义是否要在默认文件中保存连接列表的输出。默认值为 **false**。 |
| **--strict** | 将警告视为错误。默认值为 **false**。 |

#### 8.10.3.2. roxctl netpol 连接 diff

根据两个网络策略目录和带有工作负载资源的 YAML 清单报告连接差异。

#### 使用方法

-

```
$ roxctl netpol connectivity diff [flags]
```

表 8.68. 选项

| 选项 | 描述 |
|---|---|
| **--dir1 string** | 指定输入资源的第一个目录路径。这个值是必需的。 |
| **--dir2 string** | 指定您要与第一个目录路径进行比较的输入资源的第二个目录路径。这个值是必需的。 |
| **--fail** | 在第一次遇到时失败。默认值为 **false**。 |
| **-f,--output-file string** | 将 connectivity difference 命令的输出保存到特定的文件中。 |
| **-o,--output-format string** | 以特定格式配置 connectivity difference 命令的输出。支持的格式包括 **txt**、**md**、**csv**。默认值为 **txt**。 |
| **--remove** | 删除输出路径（如果已存在）。默认值为 **false**。 |
| **--save-to-file** | 定义是否在默认文件中存储连接差异的输出。默认值为 **false**。 |
| **--strict** | 将警告视为错误。默认值为 **false**。 |

## 8.11. ROXCTL SCANNER

与 StackRox Scanner 和 Scanner V4 服务相关的命令。

**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。

### 使用方法

```
$ roxctl scanner [command] [flags]
```

表 8.69. 可用命令

| 命令 | 描述 |
|---|---|
| **download-db** | 下载 StackRox Scanner 和 Scanner V4 的离线漏洞数据库。 |

| 命令 | 描述 |
| --- | --- |
| **generate** | 生成所需的 YAML 配置文件来部署 StackRox Scanner 和 Scanner V4。 |
| **upload-db** | 上传 StackRox Scanner 和 Scanner V4 的漏洞数据库。 |

### 8.11.1. roxctl scanner 命令选项从父命令继承

**roxctl scanner** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR 环境变量设置为 true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |

| 选项 | 描述 |
| --- | --- |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

**注意**

这些选项适用于 **roxctl scanner** 命令的所有子命令。

### 8.11.2. roxctl scanner generate

生成所需的 YAML 配置文件来部署 Scanner。

#### 使用方法

```
$ roxctl scanner generate [flags]
```

表 8.70. 选项

| 选项 | 描述 |
| --- | --- |
| **--cluster-type 集群类型** | 指定您要在其上运行 Scanner 的集群类型。集群类型包括 **k8s** 和 **openshift**。默认值为 **k8s**。 |
| **--enable-pod-security-policies** | 创建 **PodSecurityPolicy** 资源。默认值为 **true**。 |
| **--istio-support string** | 生成支持指定 Istio 版本的部署文件。有效版本包括 **1.0, 1.1**,**1.2**,**1.3**,**1.4**,**1.5**,**1.6**, 和 **1.7**。 |
| **--output-dir string** | 指定 Scanner 捆绑包的输出目录。留空以使用默认值。 |
| **--retry-timeout duration** | 设置 API 请求被重试的超时时间。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |
| **--scanner-image string** | 指定您要使用的 Scanner 镜像。留空，以使用服务器默认值。 |

| 选项 | 描述 |
| --- | --- |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **1m0s**。 |

### 8.11.3. roxctl scanner upload-db

为 Scanner 上传漏洞数据库。

#### 使用方法

```
$ roxctl scanner upload-db [flags]
```

表 8.71. 选项

| 选项 | 描述 |
| --- | --- |
| **--scanner-db-file string** | 指定包含转储的 Scanner 定义 DB 的文件。 |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **10m0s**。 |

### 8.11.4. roxctl scanner download-db

下载 StackRox Scanner 或 Scanner V4 的离线漏洞数据库。

**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。

此命令下载特定于版本的离线漏洞捆绑包。系统联系 Central 以确定未指定版本。如果通信失败，则下载默认为 **roxctl** 中嵌入的版本。

默认情况下，它将尝试下载确定的版本和更具体的变体的数据库。例如，如果指定了 **4.4.1-extra** 版本，则会对以下版本变体尝试下载：

- 4.4.1-extra
- 4.4.1
- 4.4

#### 使用方法

```
$ roxctl scanner download-db [flags]
```

表 8.72. 选项

| 选项 | 描述 |
| --- | --- |
| **--force** | 强制覆盖输出文件（如果已存在）。默认值为 **false**。 |
| **--scanner-db-file string** | 输出文件，将漏洞数据库保存到。默认值为下载的远程文件的名称和路径。 |
| **--skip-central** | 在检测版本时不要联系 Central。默认值为 **false**。 |
| **--skip-variants** | 不要尝试处理确定版本的变体。默认值为 **false**。 |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **10m0s**。 |
| **--version string** | 下载漏洞数据库的特定版本或版本变体。默认情况下会自动检测到版本。 |

## 8.12. ROXCTL SENSOR

在安全集群中部署 Red Hat Advanced Cluster Security for Kubernetes (RHACS)服务。

### 使用方法

```
$ roxctl sensor [command] [flags]
```

表 8.73. 可用命令

| 命令 | 描述 |
| --- | --- |
| **generate** | 生成文件以在安全集群中部署 RHACS 服务。 |
| **generate-certs** | 使用 Sensor、Collector 和 Admission 控制器更新的证书下载 YAML 文件。 |
| **get-bundle** | 下载带有文件的捆绑包，以在集群中部署 RHACS 服务。 |

表 8.74. 选项

| 选项 | 描述 |
| --- | --- |
| **--retry-timeout duration** | 设置 API 请求被重试的超时时间。值为零表示整个请求持续时间都在不重试的情况下等待。默认值为 **20s**。 |

| 选项 | 描述 |
| --- | --- |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **1m0s**。 |

### 8.12.1. roxctl sensor 命令选项从父命令继承

**roxctl sensor** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e, --endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR 环境变量设置为 true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p, --password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |

| 选项 | 描述 |
| --- | --- |
| **-s, --server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |

**注意**

这些选项适用于 **roxctl sensor** 命令的所有子命令。

### 8.12.2. roxctl sensor generate

生成文件以在安全集群中部署 RHACS 服务。

#### 使用方法

```
$ roxctl sensor generate [flags]
```

表 8.75. 选项

| 选项 | 描述 |
| --- | --- |
| **--admission-controller-disable-bypass** | 为准入控制器禁用绕过注解。默认值为 **false**。 |
| **--admission-controller-enforce-on-creates** | 动态启用，用于在准入控制器中创建对象时强制进行强制。默认值为 **false**。 |
| **--admission-controller-enforce-on-updates** | 在准入控制器中启用对对象更新的动态强制。默认值为 **false**。 |
| **--admission-controller-listen-on-creates** | 配置准入控制器 Webhook 以侦听部署创建。默认值为 **false**。 |
| **--admission-controller-listen-on-updates** | 配置准入控制器 Webhook 以侦听部署更新。默认值为 **false**。 |
| **--admission-controller-scan-inline** | 使用准入控制器时，获取内联扫描。默认值为 **false**。 |
| **--admission-controller-timeout int32** | 为准入控制器设置超时（以秒为单位）。默认值为 **3**。 |
| **--central string** | 设置要连接 Sensor 的端点。默认值为 **central.stackrox:443**。 |

| 选项 | 描述 |
| --- | --- |
| **--collection-method collection 方法** | 指定您要用于运行时支持的集合方法。集合方法 **没有**,**默认**,**ebpf** 和 **core_bpf**。默认值为 **default**。 |
| **--collector-image-repository string** | 设置您要用来部署 Collector 的镜像存储库。如果没有指定，则会派生与有效 **--main-image 存储库** 值对应的默认值。 |
| **--continue-if-exists** | 继续下载传感器捆绑包，即使集群已存在。默认值为 **false**。 |
| **--create-upgrader-sa** | 决定是否创建带有 **cluster-admin** 权限的 upgrader 服务帐户，以便于自动传感器升级。默认值为 **true**。 |
| **--disable-tolerations** | 禁用污点节点的容限。默认值为 **false**。 |
| **--enable-pod-security-policies** | 创建 **PodSecurityPolicy** 资源。默认值为 **true**。 |
| **--istio-support string** | 生成支持指定 Istio 版本的部署文件。有效版本包括 1.0,**1.1**,**1.2**,**1.3**,**1.4**,**1.5**,**1.6**,**1.7**。 |
| **--main-image-repository string** | 指定您要用来部署 Sensor 的镜像存储库。如果没有指定，则使用默认值。 |
| **--name string** | 设置集群名称来标识集群。 |
| **--output-dir string** | 设置捆绑包内容的输出目录。默认值是当前目录中自动生成的目录名称。 |
| **--slim-collector string[="true"]** | 在部署捆绑包中使用 Collector-slim。有效值包括 **auto**、**true** 和 **false**。默认值为 **auto**。 |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **5m0s**。 |

#### 8.12.2.1. roxctl sensor generate k8s

生成所需的文件以在 Kubernetes 集群中部署 RHACS 服务。

**使用方法**

```
$ roxctl sensor generate k8s [flags]
```

表 8.76. 选项

| 选项 | 描述 |
| --- | --- |
| **--admission-controller-listen-on-events** | 启用准入控制器 Webhook 以侦听 Kubernetes 事件。默认值为 **true**。 |

#### 8.12.2.2. roxctl sensor generate openshift

生成所需的文件以在 Red Hat OpenShift 集群中部署 RHACS 服务。

**使用方法**

```
$ roxctl sensor generate openshift [flags]
```

表 8.77. 选项

| 选项 | 描述 |
| --- | --- |
| `--admission-controller-listen-on-events false | true |
| auto[=true]` | **启用或禁用准入控制器 Webhook 以侦听 Kubernetes 事件**。默认值为 **auto**。 |
| `--disable-audit-logs false | true |
| auto[=true]` | 为运行时检测启用或禁用审计日志收集。默认值为 **auto**。 |
| **--openshift-version int** | 指定您要为其生成部署文件的 Red Hat OpenShift 主版本。 |

### 8.12.3. roxctl sensor get-bundle

下载带有文件的捆绑包，将 RHACS 服务部署到集群中。

**使用方法**

```
$ roxctl sensor get-bundle <cluster_details> [flags] 1
```

1 对于 **<cluster_details >**，请指定集群名称或 ID。

表 8.78. 选项

| 选项 | 描述 |
| --- | --- |
| **--create-upgrader-sa** | 指定是否为自动 Sensor 升级使用 **cluster-admin** 权限创建 upgrader 服务帐户。默认值为 **true**。 |
| **--istio-support string** | 生成支持指定 Istio 版本的部署文件。有效版本包括 **1.0, 1.1**,**1.2**,**1.3**,**1.4**,**1.5**,**1.6**, 和 **1.7**。 |
| **--output-dir string** | 指定捆绑包内容的输出目录。默认值是当前目录中自动生成的目录名称。 |
| **--slim-collector string[="true"]** | 在部署捆绑包中使用 Collector-slim。有效值包括 **auto**,**true** 和 **false**。默认值为 **auto**。 |
| **-t,--timeout 持续时间** | 为代表请求最长持续时间的 API 请求设置超时。默认值为 **5m0s**。 |

### 8.12.4. roxctl sensor generate-certs

使用 Sensor、Collector 和 Admission 控制器更新的证书下载 YAML 文件。

#### 使用方法

```
$ roxctl sensor generate-certs <cluster_details> [flags] 1
```

1 对于 **<cluster_details >**，请指定集群名称或 ID。

表 8.79. 选项

| 选项 | 描述 |
| --- | --- |
| **--output-dir string** | 指定 YAML 文件的输出目录。默认值为 **。** |

## 8.13. ROXCTL 版本

显示当前 roxctl 版本。

#### 使用方法

```
$ roxctl version [flags]
```

### 8.13.1. roxctl version 命令选项

**roxctl version** 命令支持以下选项：

| 选项 | 描述 |
| --- | --- |
| **--json** | 以 JSON 的形式显示扩展版本信息。默认值为 **false**。 |

### 8.13.2. roxctl version 命令选项从父命令继承

**roxctl version** 命令支持从父 **roxctl** 命令继承的以下选项：

| 选项 | 描述 |
| --- | --- |
| **--ca string** | 为安全连接指定自定义 CA 证书文件路径。或者，您可以使用 **ROX_CA_CERT_FILE** 环境变量指定文件路径。 |
| **--direct-grpc** | 设置 **--direct-grpc** 以改进连接性能。或者，通过将 **ROX_DIRECT_GRPC_CLIENT** 环境变量设置为 **true**，您可以启用直接 gRPC。默认值为 **false**。 |
| **-e**, **--endpoint string** | 将服务的端点设置为 contact。或者，您可以使用 **ROX_ENDPOINT** 环境变量设置端点。默认值为 **localhost:8443**。 |
| **--force-http1** | 强制将 HTTP/1 用于所有连接。或者，通过将 **ROX_CLIENT_FORCE_HTTP1** 环境变量设置为 **true**，您可以强制使用 HTTP/1。默认值为 **false**。 |
| **--insecure** | 启用不安全的连接选项。或者，通过将 **ROX_INSECURE_CLIENT** 环境变量设置为 **true**，您可以启用不安全的连接选项。默认值为 **false**。 |
| **--insecure-skip-tls-verify** | 跳过 TLS 证书验证。或者，通过将 **ROX_INSECURE_CLIENT_SKIP_TLS_VERIFY** 环境变量设置为 **true**，您可以跳过 TLS 证书验证。默认值为 **false**。 |
| **--no-color** | 禁用颜色输出。或者，通过将 **ROX_NO_COLOR** 环境变量设置为 **true**，您可以禁用颜色输出。默认值为 **false**。 |
| **-p**, **--password string** | 指定基本身份验证的密码。或者，您可以使用 **ROX_ADMIN_PASSWORD** 环境变量设置密码。 |

| 选项 | 描述 |
| --- | --- |
| **--plaintext** | 使用未加密的连接。或者，通过将 **ROX_PLAINTEXT** 环境变量设置为 **true**，您可以启用未加密的连接。默认值为 **false**。 |
| **-s**, **--server-name string** | 设置用于 SNI 的 TLS 服务器名称。或者，您可以使用 **ROX_SERVER_NAME** 环境变量设置服务器名称。 |
| **--token-file string** | 使用指定文件中提供的 API 令牌进行身份验证。另外，您可以使用 **ROX_API_TOKEN** 环境变量设置令牌。 |