



Red Hat Advanced Cluster Security for Kubernetes 4.4

备份和恢复

备份和恢复 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

描述如何备份系统并从备份中进行恢复。

目录

第 1 章 备份 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES	3
1.1. 使用 ROXCTL CLI 备份 CENTRAL 数据库	3
1.2. 备份 CENTRAL 部署	4
第 2 章 从备份中恢复	6
2.1. 使用 ROXCTL CLI 恢复 CENTRAL 数据库	6
2.2. 使用 ROXCTL CLI 恢复 CENTRAL 部署	7
2.3. 使用 RHACS OPERATOR 恢复 CENTRAL 部署	9
2.4. 使用 HELM 恢复 CENTRAL 部署	10
2.5. 将 CENTRAL 恢复到另一个集群或命名空间	10

第 1 章 备份 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES

您可以为 Red Hat Advanced Cluster Security for Kubernetes 执行数据备份，并在基础架构灾难或损坏数据时使用这些数据恢复。

您可以通过与 [Amazon S3](#) 或 [Google Cloud Storage](#) 集成来为 Central 数据库配置自动备份。您可以使用 **roxctl** CLI 对 Central 数据库执行按需备份。您还可以使用 RHACS Operator 或 Helm Chart 安装方法备份 Central 部署。

根据您的要求，您可以创建两种类型的备份：

1. Central 数据库的备份：它包含 RHACS 配置、资源、事件和证书。在不可预见的事件中，如数据库故障或数据损坏，您可以使用备份来恢复 Central 数据库并将其恢复到其早期功能状态。这样做可确保基本数据的可用性和完整性，允许您继续正常操作，而不会造成重大中断或重要信息丢失。
2. 所有自定义部署配置的备份：如果使用 Helm chart 或 RHACS Operator 安装 RHACS，您可以备份特定于安装的设置、参数和自定义。当 RHACS 安装被意外删除，或者您需要将它迁移到另一个集群或命名空间时，对部署配置进行备份可启用无缝恢复过程。另外，通过从备份中恢复自定义设置，您可以有效地重新恢复您的 Central 安装的唯一要求和配置，确保系统的一致性和准确的部署。

因为备份文件包含 secret 和证书，所以您必须安全地存储备份文件。

1.1. 使用 ROXCTL CLI 备份 CENTRAL 数据库

备份 Central 数据库对于确保数据完整性和系统可靠性至关重要。数据库的常规备份，包含必要的配置、资源、事件和证书，防止数据库故障、损坏和意外数据丢失。

您可以使用 **backup** 命令使用 **roxctl** CLI 进行备份。您需要 API 令牌或管理员密码来运行此命令。



注意

红帽支持通过与 [Amazon S3](#) 或 [Google Cloud Storage](#) 集成来备份 Central 数据库。

备份 Amazon S3 API 兼容存储可能可以正常工作。但是，红帽没有测试并支持 Amazon S3 API 兼容的存储来备份 RHACS。例如，请参阅 [MinIO 上的 RHACS 备份](#)。

1.1.1. 使用 API 令牌按需备份

您可以使用 API 令牌备份 RHACS 的整个数据库。

先决条件

- 您有一个带有 **Admin** 角色的 API 令牌。
- 已安装了 **roxctl** CLI。

流程

1. 运行以下命令，设置 **ROX_API_TOKEN** 和 **ROX_ENDPOINT** 环境变量：

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

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

2. 运行以下命令，为 Central 启动备份：

```
$ roxctl central backup 1
```

- 1** 您可以使用 **--output** 选项指定备份文件位置。

默认情况下，**roxctl** CLI 会将备份文件保存到运行命令的目录中。

其他资源

- [系统角色](#)

1.1.2. 使用管理员密码按需备份

您可以使用管理员密码备份 RHACS 的整个数据库。

先决条件

- 您有管理员密码。
- 已安装了 **roxctl** CLI。

流程

1. 运行以下命令设置 **ROX_ENDPOINT** 环境变量：

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

2. 运行以下命令，为 Central 启动备份：

```
$ roxctl -p <admin_password> central backup 1
```

- 1** 对于 **<admin_password>**，请指定管理员密码。

默认情况下，**roxctl** CLI 会将备份文件保存到您运行该命令的目录中。您可以使用 **--output** 选项指定备份文件位置。

1.2. 备份 CENTRAL 部署

您可以备份 Central 实例的部署。如果您要使用相同的配置值将 central 迁移到另一个命名空间或集群，这非常有用。



注意

红帽不支持使用 **roxctl** CLI 备份部署配置。您可以使用 **oc** 或 **kubectl** CLI 备份与 Central 实例相关的清单并恢复配置。

1.2.1. 使用 RHACS Operator 备份部署

当使用 RHACS Operator 来 instal RHACS 时，OpenShift Container Platform 会将 Central 部署的所有自定义配置存储在 Central 自定义资源中。您可以备份 Central 自定义资源、**central-tls** secret 和管理员密码。**central-tls** secret 包括用于使用安全集群和签名 API 令牌进行身份验证的证书。

流程

1. 运行以下命令，将 Central 自定义资源保存到 YAML 文件中：

```
$ oc get central -n _<central-namespace>_ _<central-name>_ -o yaml > central-cr.yaml
```

2. 运行以下命令，将 **central-tls** 保存到 JSON 文件中：

```
$ oc get secret -n _<central-namespace>_ central-tls -o json | jq  
'del(.metadata.ownerReferences)' > central-tls.json
```

3. 在 JSON 文件中的管理员密码中运行以下命令：

```
$ oc get secret -n _<central-namespace>_ central-htpasswd -o json | jq  
'del(.metadata.ownerReferences)' > central-htpasswd.json
```

1.2.2. 使用 Helm 备份部署

当使用 Helm Chart 安装 RHACS 时，您可以将 Central 部署的所有自定义配置存储在应用到 Helm Chart 的自定义值中。

您可以备份自定义值，并将其保存到 YAML 文件中。

流程

- 运行以下命令在 YAML 文件中备份自定义 Helm Chart 值：

```
$ helm get values --all -n _<central-namespace>_ _<central-helm-release>_ -o yaml >  
central-values-backup.yaml
```

第 2 章 从备份中恢复

您可以使用 **roxctl** 命令行界面(CLI)从现有备份中恢复 Red Hat Advanced Cluster Security for Kubernetes。

根据您的要求和您备份的数据，您可以从以下类型的备份中恢复：

1. **从 Central 数据库备份中恢复 Central 数据库**：使用此数据库从数据库故障或数据崩溃事件中恢复。它允许您将 Central 数据库恢复并恢复到其早期功能状态。
2. **从 Central 部署备份中恢复 Central**：如果您要将 Central 迁移到另一个集群或命名空间，请使用它。这个选项恢复中央安装的配置。

2.1. 使用 ROXCTL CLI 恢复 CENTRAL 数据库

您可以使用 **restore** 命令使用 **roxctl** CLI 恢复 Red Hat Advanced Cluster Security for Kubernetes。您需要 API 令牌或管理员密码来运行此命令。

2.1.1. 使用 API 令牌恢复

您可以使用 API 令牌恢复 RHACS 的整个数据库。

先决条件

- 您有一个 RHACS 备份文件。
- 您有一个带有管理员角色的 API 令牌。
- 已安装了 **roxctl** CLI。

流程

1. 运行以下命令，设置 **ROX_API_TOKEN** 和 **ROX_ENDPOINT** 环境变量：

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

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

2. 运行以下命令来恢复 Central 数据库：

```
$ roxctl central db restore <backup_file> 1
```

1 对于 **<backup_file>**，请指定您要恢复的备份文件的名称。

2.1.2. 使用管理员密码恢复

您可以使用管理员密码恢复 RHACS 的整个数据库。

先决条件

- 您有一个 RHACS 备份文件。

- 您有管理员密码。
- 已安装了 **roxctl** CLI。

流程

1. 运行以下命令设置 **ROX_ENDPOINT** 环境变量：

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

2. 运行以下命令来恢复 Central 数据库：

```
$ roxctl -p <admin_password> \ 1
  central db restore <backup_file> 2
```

- 1 对于 **<admin_password>**，请指定管理员密码。
- 2 对于 **<backup_file>**，请指定您要恢复的备份文件的名称。

2.1.3. 恢复操作

如果您的连接在恢复操作期间中断，或者您需要离线，您可以恢复恢复操作。

- 如果您无法访问运行恢复操作的机器，您可以使用 **roxctl central db restore status** 命令检查持续恢复操作的状态。
- 如果连接中断，**roxctl** CLI 会在连接再次可用时自动尝试恢复任务。自动连接重试取决于 **timeout** 选项指定的持续时间。
- 使用 **--timeout** 选项指定 **roxctl** CLI 停止尝试恢复恢复操作的时间（以秒为单位）。如果没有指定选项，则默认超时为 10 分钟。
- 如果恢复操作卡住或者您要取消它，请使用 **roxctl central db restore cancel** 命令来取消正在运行的恢复操作。
- 如果恢复操作卡住，您已取消了它，或者时间已过期，您可以通过再次运行原始命令来恢复之前的恢复。

重要

- 在中断期间，RHACS 会缓存持续恢复操作 24 小时。您可以通过再次执行原始恢复命令来恢复此操作。
- **--timeout** 选项只控制客户端侧连接重试，且不会对 24 小时的服务器端恢复缓存产生影响。
- 您无法在 Central pod 重启后恢复恢复。
- 如果恢复操作中断，您必须在 24 小时内重启它，并在重启 Central 前重启它，否则 RHACS 会取消恢复操作。

2.2. 使用 ROXCTL CLI 恢复 CENTRAL 部署

您可以使用您所做的备份将 Central 部署恢复到其原始配置。

您必须首先使用 **roxctl** CLI 恢复证书，然后运行 Central 安装脚本来恢复 Central 部署。

2.2.1. 使用 roxctl CLI 恢复证书

使用 **roxctl** CLI 生成 Kubernetes 清单，将 RHACS Central 组件安装到集群中。这样，您可以确保安全集群的验证证书，API 令牌对恢复的版本保持有效。如果备份了 RHACS Central 的另一个实例，您可以使用该备份中的证书文件。



注意

使用 **roxctl** CLI，您无法恢复整个 Central 部署。相反，您首先使用 **roxctl** CLI 使用中央数据备份中的证书生成新清单。之后，您可以使用这些清单安装 Central。

先决条件

- 您必须具有 Red Hat Advanced Cluster Security for Kubernetes 备份文件。
- 您必须已安装了 **roxctl** CLI。

流程

1. 运行交互式 **install** 命令：

```
$ roxctl central generate interactive
```

2. 对于以下提示，请输入 Red Hat Advanced Cluster Security for Kubernetes 备份文件的路径：

```
Enter path to the backup bundle from which to restore keys and certificates (optional):  
_<backup-file-path>_
```

3. 对于其他提示，按 **Enter** 键接受默认值，或者根据需要输入自定义值。

在完成时，交互式 **install** 命令会创建一个名为 **central-bundle** 的文件夹，其中包含部署 Central 所需的 YAML 清单和脚本。

2.2.2. 运行中央安装脚本

运行交互式安装程序后，您可以运行 **setup.sh** 脚本来安装 Central。

流程

1. 运行 **setup.sh** 脚本来配置镜像 registry 访问：

```
$ ./central-bundle/central/scripts/setup.sh
```

2. 创建所需资源：

```
$ oc create -R -f central-bundle/central
```

3. 检查部署进度：

```
$ oc get pod -n stackrox -w
```

- 在 Central 运行后，找到 RHACS 门户 IP 地址并在浏览器中打开。根据您在回答提示时选择的风险，请使用以下方法之一获取 IP 地址。

公开方法	命令	地址	Example
Route (路由)	<code>oc -n stackrox get route central</code>	在输出中 HOST/PORT 列下的地址	<code>https://central-stackrox.example.route</code>
节点端口	<code>oc get node -owide && oc -n stackrox get svc central-loadbalancer</code>	任何节点的 IP 或主机名，在服务显示的端口中	<code>https://198.51.100.0:31489</code>
Load Balancer	<code>oc -n stackrox get svc central-loadbalancer</code>	在端口 443 上为服务显示 EXTERNAL-IP 或主机名	<code>https://192.0.2.0</code>
无	<code>central-bundle/central/scripts/port-forward.sh 8443</code>	<code>https://localhost:8443</code>	<code>https://localhost:8443</code>



注意

如果您在互动安装过程中选择了自动生成的密码，您可以运行以下命令将其记录到 Central：

```
$ cat central-bundle/password
```

2.3. 使用 RHACS OPERATOR 恢复 CENTRAL 部署

您可以使用 RHACS Operator 将 Central 部署恢复到其原始配置。要成功恢复，您需要备份 Central 自定义资源、**central-tls** 和管理员密码。

先决条件

- 您必须具有 **central-tls** 备份文件。
- 您必须具有 Central 自定义资源备份文件。
- 您必须具有管理员密码备份文件。

流程

- 使用 **central-tls** 备份文件来创建资源：

```
$ oc apply -f central-tls.json
```

2. 使用 **central-htpasswd** 备份文件来创建 secret :

```
$ oc apply -f central-htpasswd.json
```

3. 使用 **central-cr.yaml** 文件来创建 Central 部署 :

```
$ oc apply -f central-cr.yaml
```

2.4. 使用 HELM 恢复 CENTRAL 部署

您可以使用 Helm 将 Central 部署恢复到其原始配置。要成功恢复，您需要备份 Central 自定义资源、**central-tls** secret 和管理员密码。

先决条件

- 您必须具有 Helm 值备份文件。
- 您必须具有 Red Hat Advanced Cluster Security for Kubernetes 备份文件。
- 您必须已安装了 **roxctl** CLI。

流程

1. 从 RHACS 数据库备份文件生成 **values-private.yaml** :

```
$ roxctl central generate k8s pvc --backup-bundle _<path-to-backup-file>_ --output-format "helm-values"
```

2. 运行 **helm install** 命令并指定您的备份文件 :

```
$ helm install -n stackrox --create-namespace stackrox-central-services rhacs/central-services -f central-values-backup.yaml -f central-bundle/values-private.yaml
```

2.5. 将 CENTRAL 恢复到另一个集群或命名空间

您可以使用 RHACS Central 数据库的备份和部署将 Central 恢复到另一个集群或命名空间。

以下列表提供了安装步骤的高级概述 :

1. 根据您的安装方法，您必须首先按照以下主题中的说明恢复 Central 部署 :



重要

- 确保使用备份的 Central 证书，以便旧 Central 实例发布的安全集群和 API 令牌保持有效。
- 如果要部署到另一个命名空间，您必须更改备份资源或命令中的命名空间。

- [使用 roxctl CLI 恢复 Central 部署](#)
- [使用 RHACS Operator 恢复 Central 部署](#)

- [使用 Helm 恢复 Central 部署](#)
2. 按照 [roxctl CLI 主题恢复 Central 数据库中的说明](#)，恢复 Central 数据库。
 3. 如果您有一个指向旧 RHACS Central 实例的外部 DNS 条目，则必须重新配置它以指向您创建的新的 RHACS Central 实例。