Red Hat Advanced Cluster Security for Kubernetes 4.4

支持

获取对 Red Hat Advanced Cluster Security for Kubernetes 的支持

Last Updated: 2024-06-28

Red Hat Advanced Cluster Security for Kubernetes 4.4 支持

获取对 Red Hat Advanced Cluster Security for Kubernetes 的支持

法律通告

摘要

本文档提供了有关从 Red Hat for Red Hat for Red Hat for Kubernetes 获取支持的信息，并包括了如何生成诊断捆绑包的说明。

目录

第 1 章 获取对 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 的支持

本主题提供有关 Red Hat Advanced Cluster Security for Kubernetes 的技术支持的信息。

如果您在执行本文档所述的某个流程或 Red Hat Advanced Cluster Security for Kubernetes 时遇到问题，请访问 红帽客户门户网站。通过红帽客户门户网站：

- 搜索或浏览红帽知识库，了解与红帽产品相关的文章和解决方案。
- 向红帽支持提交支持问题单。
- 访问其他产品文档。

如果您对文档有任何改进建议，或发现了错误，请针对 **Red Hat Advanced Cluster Security for Kubernetes** 产品为 **Documentation** 组件创建一个 JIRA 问题。确保包含具体详情，如部分名称和 Red Hat Advanced Cluster Security for Kubernetes 的版本，以便我们有效地管理您的反馈。

1.1. 关于红帽知识库

红帽知识库 提供丰富的内容以帮助您充分利用红帽产品和技术。红帽知识库包括文章、产品文档和视频，概述了安装、配置和使用红帽产品的最佳实践。另外，您还可以搜索已知问题的解决方案，其提供简洁的根原因描述和补救措施。

1.2. 搜索红帽知识库

如果出现 Red Hat Advanced Cluster Security for Kubernetes 问题，您可以执行初始搜索来确定红帽知识库中是否已存在解决方案。

先决条件

- 您有一个红帽客户门户网站帐户。

流程

1. 登录红帽客户门户。
2. 在主红帽客户门户网站搜索字段中，输入与问题相关的关键字和字符串，包括：
   - Red Hat Advanced Cluster Security for Kubernetes 组件（如 **etcd**）
   - 相关步骤（比如 **安装**）
   - 警告、错误消息和其他与输出与特定的问题相关
3. 点 **Search**。
4. 选择 **Red Hat Advanced Cluster Security for Kubernetes**产品过滤器。
5. 在内容类型过滤中选择 **Knowledgebase**。

1.3. 生成诊断捆绑包

您可以生成诊断捆绑包并发送这些数据，以便支持团队能够深入了解 Red Hat Advanced Cluster Security for Kubernetes 组件的状态和健康状况。

注意

诊断捆绑包是未加密的，具体取决于您环境中的集群数量，捆绑包大小介于 100 KB 到 1 MB 之间。

1.3.1. 使用 RHACS 门户生成诊断捆绑包

您可以使用 RHACS 门户中的系统健康仪表板生成诊断捆绑包。

先决条件

- 要生成诊断捆绑包，您需要 **DebugLogs** 资源的 **read** 权限。

流程

1. 在 RHACS 门户中，选择 **Platform Configuration → System Health**。
2. 在 **System Health** view 标头上，点 **Generate Diagnostic Bundle**。
3. 对于 **Filter by clusters** 下拉菜单，选择要为其生成诊断数据的集群。
4. 对于 **Filter by starting time**，指定您要包含诊断数据的日期和时间（以 UTC 格式）。
5. 点 **Download Diagnostic Bundle**。

1.3.2. 使用 roxctl CLI 生成诊断捆绑包

您可以使用 **roxctl** CLI 使用 Red Hat Advanced Cluster Security for Kubernetes (RHACS)管理员密码或 API 令牌和中央地址生成诊断捆绑包。

先决条件

- 要生成诊断捆绑包，您需要对 **Administration** 资源具有读权限。这是比版本 3.73.0 更早的 **DebugLogs** 资源版本所必需的。
- 您必须已配置了 RHACS 管理员密码或 API 令牌和中央地址。

流程

- 要使用 RHACS 管理员密码生成诊断捆绑包，请执行以下步骤：
  1. 运行以下命令来配置 **ROX_PASSWORD** 和 **ROX_CENTRAL_ADDRESS** 环境变量：

     ```
     $ export ROX_PASSWORD=<rox_password> && export
     ROX_CENTRAL_ADDRESS=<address>:<port_number>
     ```
     (1)

     (1) 对于 **<rox_password>**，请指定 RHACS 管理员密码。

  2. 运行以下命令，以使用 RHACS 管理员密码生成诊断捆绑包：

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" -p "$ROX_PASSWORD" central debug
download-diagnostics
```

- 要使用 API 令牌生成诊断捆绑包，请执行以下步骤：

  1. 运行以下命令来配置 **ROX_API_TOKEN** 环境变量：

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

  2. 运行以下命令，以使用 API 令牌生成诊断捆绑包：

     ```
     $ roxctl -e "$ROX_CENTRAL_ADDRESS" central debug download-diagnostics
     ```

1.4. 提交支持问题单

先决条件

- 您可以访问集群。
- 您有一个红帽客户门户网站帐户。
- 您有一个 Red Hat OpenShift Platform Plus 订阅。

流程

1. 登录到红帽客户门户网站 并选择 **SUPPORT CASES → Open a case**。
2. 为您的问题选择适当的类别（如 **Defect / Bug**）、产品(**Red Hat Advanced Cluster Security for Kubernetes**)和产品版本（如果还没有自动填充则为**4.4** ）。
3. 查看推荐的红帽知识库解决方案列表，以便与正在报告的问题匹配。如果建议的文章没有解决这个问题，请点 **Continue**。
4. 输入一个简洁但描述性的问题概述，以及问题症状的详细信息，以及您预期的结果。
5. 查看更新的推荐红帽知识库解决方案列表，以便与正在报告的问题匹配。这个列表的范围会缩小，因为您在创建问题单的过程中提供了更多信息。如果建议的文章没有解决这个问题，请点 **Continue**。
6. 请确保提供的帐户信息是正确的，如果需要，请相应调整。
7. 上传生成的诊断捆绑包，然后点 **Continue**。
8. 输入相关问题单管理详情，点 **Continue**。
9. 预览问题单详情，点 **Submit**。