Red Hat build of Cryostat 2

使用 Red Hat build of Cryostat Operator 配置 Cryostat

Last Updated: 2024-02-01

Red Hat build of Cryostat 2 使用 Red Hat build of Cryostat Operator 配置 Cryostat

法律通告

摘要

Red Hat build of Cryostat 是 OpenShift Container Platform 上的红帽产品。使用 Red Hat build of Cryostat Operator 配置 Cryostat，了解如何使用 Red Hat build of Cryostat Operator 配置 Cryostat。

目录

前言

Red Hat build of Cryostat 是 JDK Flight Recorder (JFR)的容器原生虚拟化实现，可用于安全地监控 OpenShift Container Platform 集群上运行的工作负载的 Java 虚拟机(JVM)性能。您可以使用 Cryostat 2.4 使用 web 控制台或 HTTP API 启动、停止、检索、存档、导入和导出容器化应用程序中 JVM 的 JFR 数据。

根据您的用例，您可以使用 Cryostat 提供的内置工具直接在 Red Hat OpenShift 集群上存储和分析记录，或者您可以将记录导出到外部监控应用程序，以对记录的数据进行更深入的分析。

重要

Red Hat build of Cryostat 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。

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 的信息。

第 1 章 RED HAT BUILD OF CRYOSTAT OPERATOR

您可以使用 Red Hat build of Cryostat Operator 管理并配置 Cryostat 实例。Red Hat build of Cryostat Operator 在 OpenShift Container Platform (OCP)上提供。

1.1. RED HAT BUILD OF CRYOSTAT OPERATOR 概述

在 OpenShift Container Platform 上创建或更新 Cryostat 应用程序后，Red Hat build of Cryostat Operator 会创建和管理 Cryostat 应用程序。

Operator 级别 2 无缝升级

从 Cryostat 2.2 开始，Red Hat build of Cryostat Operator 的 Operator Capability Level 设置为 Operator Lifecycle Manager 框架中的 **Level 2 Seamless Upgrades**。升级 Red Hat build of Cryostat Operator 后，Red Hat build of Cryostat Operator 会自动升级 Cryostat 及其相关组件。自动升级操作不会从 Cryostat 实例中删除任何 JFR 记录、模板、规则和其他存储的组件。

注意

自动升级操作只适用于次版本或补丁更新版本。对于主版本，您可能需要重新安装 Red Hat build of Cryostat Operator。

持久性卷声明 (PVC)

您可以使用 Red Hat build of Cryostat Operator 在 Red Hat OpenShift 上创建持久性卷声明(PVC)，以便 Cryostat 应用程序可以将存档记录存储在云存储磁盘上。

Operator 配置设置

另外，您可以对 Red Hat build of Cryostat Operator 的默认配置设置进行以下更改：

- 配置由 Red Hat build of Cryostat Operator 创建的 PVC，以便您的 Cryostat 应用程序可以在云存储磁盘上存储存档记录。
- 配置 Cryostat 应用程序以信任来自特定应用程序的 TLS 证书。
- 将 Cryostat 作为最小部署部署，以便 Operator 需要较少的资源来部署 Cryostat 应用程序。
- 禁用 cert-manager，以便 Operator 不需要为 Cryostat 组件生成自签名证书。
- 将自定义事件模板文件（位于 ConfigMaps 中）安装到 Cryostat 实例，以便您可以使用模板在 Cryostat 启动时创建记录。

从 Cryostat 2.2 中，包括 Red Hat build of Cryostat Operator 的以下配置选项：

- 资源要求，可用于为核心、**数据源** 或 **grafana** 容器指定资源请求或限制。
- **服务自定义，以便您可以控制 Red Hat build of Cryostat Operator 所创建的服务。**
- **sidecar 报告选项，Red Hat build of Cryostat Operator 可用于为 Cryostat 应用程序置备一个或多个报告生成器。**

单命名空间或多命名空间 Cryostat 实例

Red Hat build of Cryostat Operator 提供了 Cryostat API 和 Cluster Cryostat API。您可以使用 Cryostat API 创建在单个命名空间中工作的 Cryostat 实例。您可以使用 Cluster Cryostat API 创建在多个命名空间间工作的 Cryostat 实例。您可以使用可从 Red Hat OpenShift Web 控制台访问的 GUI 控制这些 Cryostat 实例。

可以访问 multi-namespace Cryostat 实例的用户，可以访问该 Cryostat 实例可见的任意命名空间中的所有目标应用程序。因此，当部署多命名空间 Cryostat 实例时，您必须考虑选择哪个命名空间进行监控，哪些命名空间要安装到哪个命名空间，以及用户可以具有访问权限。

配置 Red Hat build of Cryostat Operator 的先决条件

在配置 Red Hat build of Cryostat Operator 前，请确保满足以下先决条件：

- 在 Red Hat OpenShift 上的项目中安装了 Red Hat build of Cryostat Operator。
- 使用 Red Hat build of Cryostat Operator 创建 Cryostat 实例。

其他资源

- 请参阅 Operator Capability Levels (Operator SDK)
- 请参阅使用 Operator 在 Red Hat OpenShift 上安装 Cryostat （安装 Cryostat）

1.2. 除了支持容器外

您可以选择排除使用 Cryostat 应用程序部署的支持应用程序。支持应用程序是您的 Cryostat pod 中列出的支持性容器。当您排除了支持容器时，部署 Cryostat 应用程序需要较少的系统资源。

默认情况下，Cryostat 将项目的 Red Hat build of Cryostat Operator YAML 配置文件中的 minimal 属性设为 false。使用这个配置，Red Hat build of Cryostat Operator 会使用所有标准支持应用程序（如 jfr-datasource 和 Grafana 仪表板）部署 Cryostat 应用程序，这些应用程序包含在与 Cryostat 应用程序相同的 pod 中。这些支持性应用程序可以与 Cryostat 数据交互，并为您提供与这个数据交互的额外功能。

Red Hat build of Cryostat Operator 默认为以下配置：

- 部署预先配置的 Grafana 应用程序。
- 部署一个 jfr-datasource 应用程序，用于将 JDK Flight Recorder (JFR)数据转换为 JSON，这是 Grafana 的可读格式。
- 在部署 Cryostat 时，包括一个在 Grafana 中预先配置的 Dashboard JSON 文件。

您可以将 minimal 属性设置为 true，以便 Red Hat build of Cryostat Operator 会自动重启 Cryostat 实例作为最小部署。这意味着，Operator 只部署 Cryostat 容器中列出的应用程序，并忽略任何标准支持应用程序，如 jfr-datasource 和 Grafana 仪表板，它们包含与 Cryostat 应用程序相同的 pod 中。

先决条件

- 使用 Red Hat OpenShift Web 控制台登录到 OpenShift Container Platform。

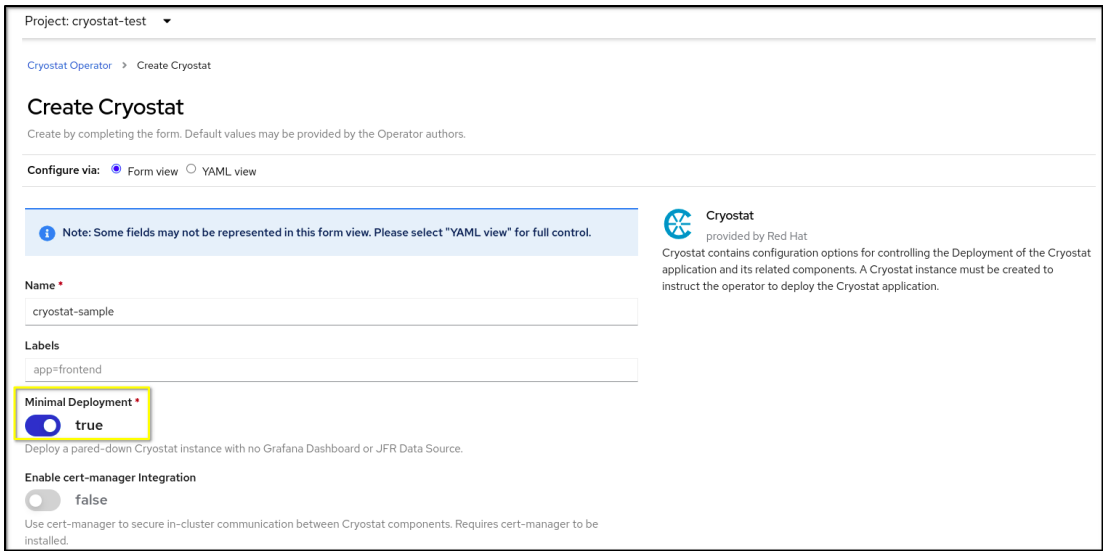
流程

1. 在 Red Hat OpenShift web 控制台中，点 Operators > Installed Operators。
2. 从可用 operator 列表中，选择 Red Hat build of Cryostat。
3. 点 Details 标签页。
4. 在 Provided APIs 部分中，提供 Cryostat 和 Cluster Cryostat 自定义资源(CR)。选择以下选项之一：
   - 要创建单命名空间 Cryostat 实例，请选择 Cryostat，然后单击 Create instance。
   - 要创建 Cryostat 的多命名空间实例，请选择 Cluster Cryostat，然后点 Create instance。
5. 要配置 minimal 属性，请选择以下选项之一：

a. 点 Form view 单选按钮。

i. 将 Minimal Deployment 开关设置为 true。您还必须在 Name 字段中输入值。

图 1.1. 将 Minimal Deployment 开关切换到 true



ii. 点 Create。根据您创建的实例类型，实例会在以下标签页之一下打开：

- 如果您创建了单命名空间 Cryostat 实例，则实例位于 Operator 详情页面的 Cryostat 选项卡下。
- 如果您创建了 Cluster Cryostat 实例，则实例位于 Operator 详情页面的 Cluster Cryostat 选项卡下。

b. 点 YAML 视图 单选按钮。

i. 在 spec: 键集中，将 minimal 属性的值更改为 true。

配置 minimal 属性的示例

```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
```

```
  name: cryostat-sample
spec:
  minimal: true
--
```

ii. 点击 **Save**。

验证

1. 在 Red Hat OpenShift Web 控制台中，选择创建 Cryostat 实例的项目，或选择的项目作为 Cluster Cryostat 实例的 Install Namespace。

2. 导航到 **Workloads** → **Deployments**。

3. 从部署列表中，选择与 Cryostat 或 Cluster Cryostat 实例的名称匹配的部署。在 Web 控制台中打开 Deployment 详情页面。

4. 导航到 Containers 部分。单个列出的容器表示红帽构建的 Cryostat Operator 已作为最小部署部署了 Cryostat 应用程序。

其他资源

- 如需有关 OpenShift CLI 的更多信息，请参阅 OpenShift CLI 入门 (Red Hat OpenShift 文档)

- 请参阅创建 JDK Flight Recorder (JFR)记录 （使用 Cryostat 创建 JFR 记录）

1.3. 禁用 CERT-MANAGER

您可以通过配置 Red Hat build of Cryostat Operator 的 enableCertManager 属性来禁用 cert-manager 功能。

默认情况下，Red Hat build of Cryostat Operator 的 enableCertManager 属性被设置为 true。这意味着 Red Hat build of Cryostat Operator 使用 cert-manager CA 签发者为您的 Cryostat 组件生成自签

名证书。Red Hat build of Cryostat Operator 使用这些证书在集群中运行的 Cryostat 组件中启用 HTTPS 通信。

您可以将 enableCertManager 属性设置为 false，以便 Red Hat build of Cryostat Operator 不需要为 Cryostat 组件生成自签名证书。

重要

如果将 enableCertManager 属性设置为 false，则可能会向包含运行中 Cryostat 应用程序的集群引入未加密内部流量的潜在安全影响。

先决条件

- 使用 Red Hat OpenShift Web 控制台登录到 OpenShift Container Platform。

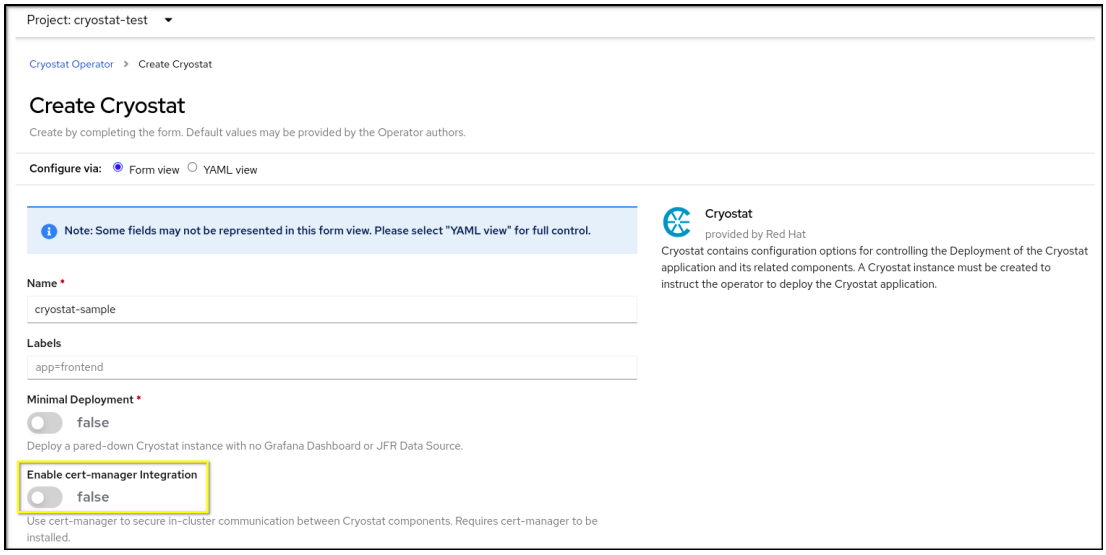
流程

1. 在 OpenShift web 控制台中进入到 Operators > Installed Operators。
2. 从可用 operator 列表中，选择 Red Hat build of Cryostat。
3. 点 Details 标签页。
4. 在 Provided APIs 部分中，提供 Cryostat 和 Cluster Cryostat 自定义资源(CR)。选择以下选项之一：
   - 要创建单命名空间 Cryostat 实例，请选择 Cryostat，然后单击 Create instance。
   - 要创建 Cryostat 的多命名空间实例，请选择 Cluster Cryostat，然后点 Create instance。
5. 要配置 enableCertManager 属性，请选择以下选项之一：

a. 点 Form view 单选按钮。

i. 将 Enable cert-manager Integration 开关设置为 false，然后在 Name 字段中输入值。

图 1.2. 将 Enable cert-manager Integration 切换到 false



ii. 点 Create。根据您创建的实例类型，实例会在以下标签页之一下打开：

- 如果您创建了单命名空间 Cryostat 实例，则实例位于 Operator 详情页面的 Cryostat 选项卡下。
- 如果您创建了 Cluster Cryostat 实例，则实例位于 Operator 详情页面的 Cluster Cryostat 选项卡下。

b. 点 YAML 视图 单选按钮。

i. 在 YAML 文件的 spec: 键集中，将 enableCertManager 属性更改为 false。

在 YAML 文件中设置 spec: key 的示例

```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
```

```
metadata:
  name: cryostat-sample
spec:
  enableCertManager: false
--
```

ii. 点 Save 按钮。

Red Hat build of Cryostat Operator 会自动重启 Cryostat 应用程序，使应用程序可以使用更新的 enableCertManager 属性配置运行。

验证

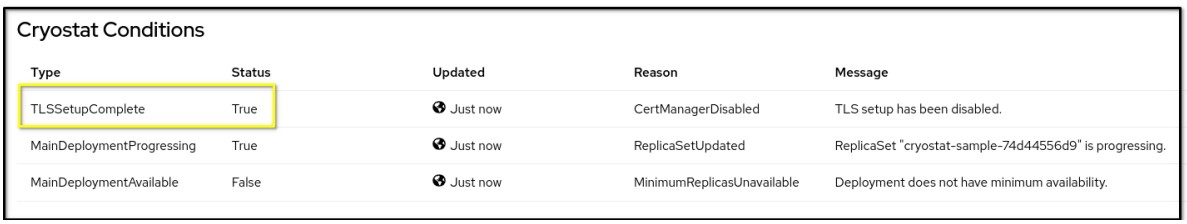
1. 选择 Cryostat 或 Cluster Cryostat 实例：

- 如果您创建了 Cryostat 实例，请从 Operator 详情页面的 Cryostat 选项卡中选择 Cryostat 实例。
- 如果您创建了 Cluster Cryostat 实例，请从 Operator 详情页面上的 Cluster Cryostat 选项卡中选择 Cluster Cryostat 实例。

2. 进入到 Cryostat Conditions 表。

3. 验证 TLSSetupComplete 条件是否已设置为 true，并且此条件的 Reason 列是否已设置为 CertManagerDisabled。这表示您已将 enableCertManager 属性设置为 false。

图 1.3. 显示 TLSSetupComplete 条件设置为 true 的示例



其他资源

- 请参阅 cert-manager 文档

- 请参阅创建 JDK Flight Recorder (JFR)记录 （使用 Cryostat 创建 JFR 记录）

1.4. 自定义事件模板

在 Cryostat 2 中，您可以配置 Red Hat build of Cryostat Operator YAML 配置文件的 eventTemplates 属性，使其包含多个自定义模板。事件模板概述了 JDK Flight Recording (JFR)的事件记录标准。您可以通过关联的事件模板配置 JFR。

默认情况下，Red Hat build of Cryostat Operator 包括一些预先配置的事件模板。这些预先配置的事件模板可能无法满足您的需要，因此您可以使用 Red Hat build of Cryostat Operator 为 Cryostat 实例生成自定义事件模板，并将这些模板存储在 ConfigMaps 中以便更轻松地检索。您可以使用以下方法生成自定义事件模板：

- 使用 Red Hat OpenShift Web 控制台将事件模板上传到自定义资源中。

- 在 Red Hat OpenShift web 控制台中编辑 Cryostat 自定义资源的 YAML 文件。

在 ConfigMap 中存储自定义事件模板后，您可以使用此自定义事件模板部署新的 Cryostat 实例。然后，您可以使用带有 JFR 的自定义事件模板来监控 Java 应用程序以满足您的需要。

先决条件

- 使用 Red Hat OpenShift Web 控制台登录到 OpenShift Container Platform。

- 登录到 Cryostat web 控制台。

流程

1. 要下载默认事件模板，请导航到 Cryostat web 控制台并从 Events 菜单中点 Downloads。

注意

事件模板采用 XML 格式，文件扩展名为 .jfc。

2. *可选：* **如果要自定义事件模板，请使用文本编辑器或 XML 编辑器编辑下载的默认事件模板，以配置模板以满足您的需要。**

3. **通过在 CLI 中输入 oc login 命令登录到您的 Red Hat OpenShift Web 控制台。**

4. **在 CLI 中输入以下命令来从事件模板创建 ConfigMap 资源。您必须在要部署 Cryostat 应用程序的路径中发出该命令。您可以使用此资源存储运行 Cryostat 实例的集群中的事件模板文件。**

   使用 CLI 创建 ConfigMap 资源的示例

   ```
   $ oc create configmap <template_name> --from-file=<path_to_custom_event_template>
   ```

5. **在 Red Hat OpenShift web 控制台中，点 Operators > Installed Operators。**

6. **从可用 operator 列表中，选择 Red Hat build of Cryostat。**

7. **在 Operator 详情页面的 Details 选项卡下，创建一个 Cryostat 或 Cluster Cryostat 实例。**

   a. **在 Provided APIs 部分中，提供 Cryostat 和 Cluster Cryostat 自定义资源(CR)。选择以下选项之一：**

   - **要创建单命名空间 Cryostat 实例，请选择 Cryostat，然后单击 Create instance。**
   - **要创建 Cryostat 的多命名空间实例，请选择 Cluster Cryostat，然后点 Create instance。**

8. 选择以下选项之一将 XML 格式的事件模板上传到资源中：

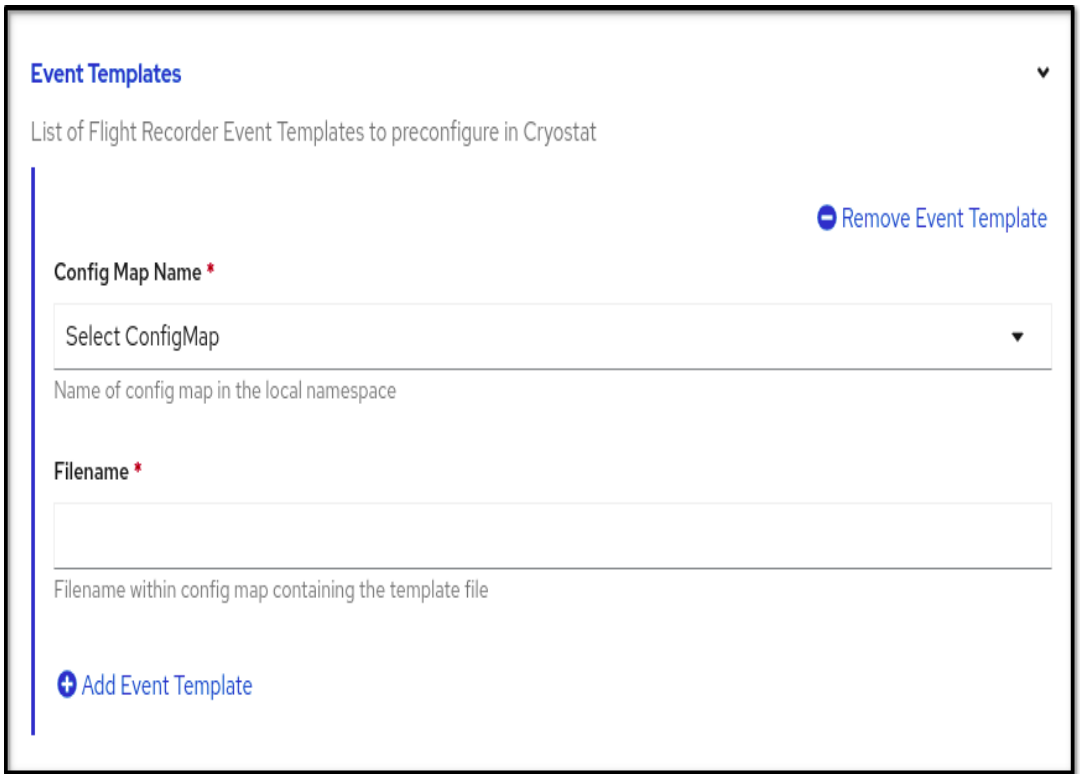
a. 点 Form view 单选按钮。

i. 导航到 Cryostat 或 Cluster Cryostat 实例的 Event Templates 部分。

ii. 在 Event Templates 菜单中点 Add Event Template。在 Red Hat OpenShift 控制台中打开一个 Event Templates 部分。

iii. 在 Config Map Name 下拉列表中选择包含您的事件模板的 ConfigMap 资源。

图 1.4. Cryostat 实例的 event Templates 选项



iv. 在 Filename 字段中，输入 ConfigMap 中包含的 .jfc 文件的名称。

v. 要使用自定义事件模板生成 Cryostat 或 Cluster Cryostat 实例，请点 Create。

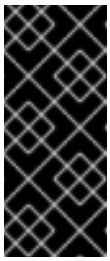
b. 点 YAML 视图 单选按钮。

i.

为 **eventTemplates** 属性指定任何自定义事件模板。此属性将 **Red Hat build of Cryostat Operator** 指向 **ConfigMap**，以便 **Red Hat build of Cryostat Operator** 可以读取事件模板。

为 **eventTemplates** 属性指定自定义事件模板的示例

```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  eventTemplates:
  - configMapName: custom-template1
    filename: my-template1.jfc
  - configMapName: custom-template2
    filename: my-template2.jfc
--
```



重要

您必须从 **configMapName** 下拉列表中选择与 **Cryostat** 或 **Cluster Cryostat** 实例关联的 **ConfigMap** 名称。另外，您必须在 **filename** 字段中指定与 **ConfigMap** 关联的键。

Red Hat build of Cryostat Operator 现在可将自定义事件模板作为 **XML** 文件提供给您的 **Cryostat** 应用程序。您的自定义事件模板会与 **Cryostat web** 控制台中的默认事件模板一起打开。

验证

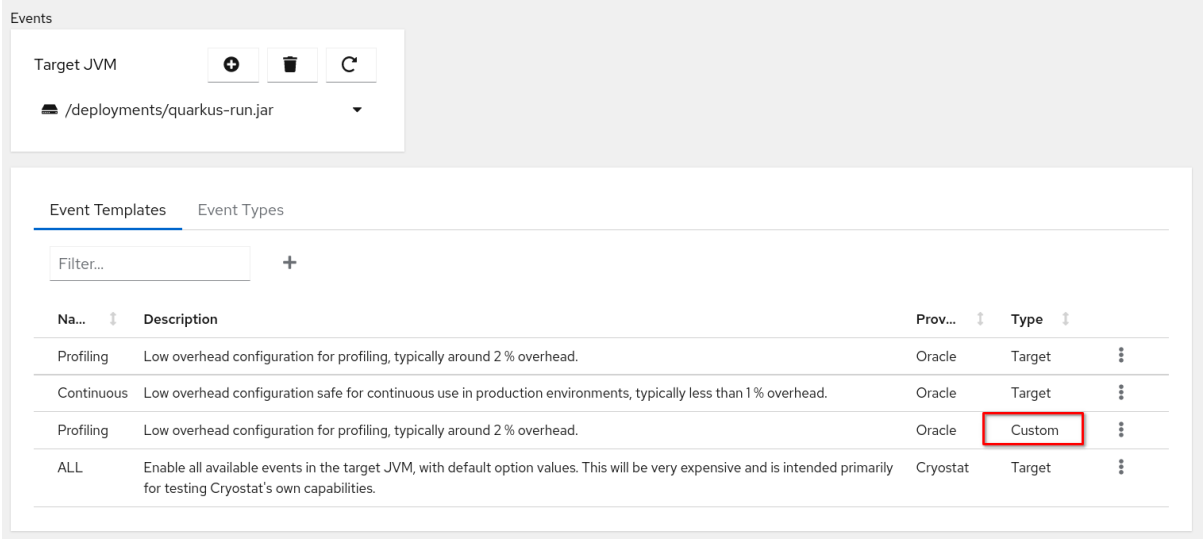
1.

在 **Cryostat web** 控制台中，点菜单中的 **Events**。如果在 **web** 控制台中打开了一个 **Authentication Required** 窗口，请输入您的凭证并点 **Save**。

2.

在 **Event Templates** 选项卡下，检查您的自定义事件模板是否在可用事件模板列表中显示。

图 1.5. 在 Event Templates 选项卡下列出的自定义事件模板示例



其他资源

- 请参阅使用 操作器在 OpenShift 上安装 Cryostat (Installing Cryostat)
- 请参阅使用 Web 控制台访问 Cryostat(Installing Cryostat)
- 请参阅使用自定义事件模板 （使用 Cryostat 管理 JFR 记录）

1.5. 配置 TLS 证书

您可以指定 Red Hat build of Cryostat Operator，将 Cryostat 配置为信任来自特定应用程序的 TLS 证书。

Cryostat 尝试打开到使用 TLS 证书的目标 JVM 的 JMX 连接。对于成功 JMX 连接，Cryostat 必须传递目标 JVM 证书上的所有身份验证检查。

您可以在 Red Hat build of Cryostat Operator YAML 配置文件的 trustedCertSecrets 数组中指定多个 TLS secret。您必须在数组的 secretName 属性中指定位于与 Cryostat 应用程序相同的命名空间中的 secret。certificateKey 属性默认为 tls.crt，但您可以将值改为 X.509 证书文件名。

重要

只有在使用 **com.sun.management.jmxremote.registry.ssl=true** 属性为远程 **JMX** 连接启用了 **TLS** 的应用程序才需要配置 **TLS** 证书。

先决条件

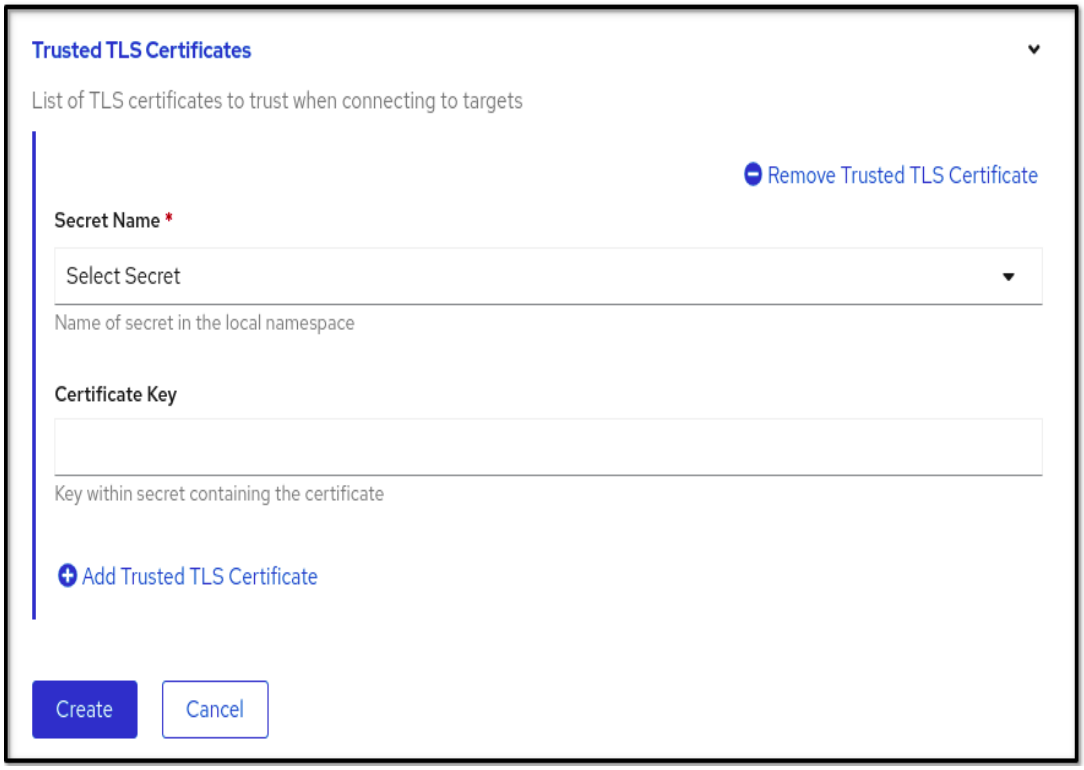
- 使用 **OpenShift Web** 控制台登录到 **OpenShift Container Platform**。
- 登录到 **Cryostat web** 控制台。

流程

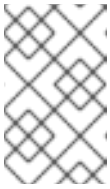
1. 在 **Red Hat OpenShift web** 控制台中，点 **Operators > Installed Operators**。
2. 从可用 **operator** 列表中，选择 **Red Hat build of Cryostat**。
3. 在 **Operator** 详情页面中，点 **Details** 选项卡。
4. 在 **Provided APIs** 部分中，提供 **Cryostat** 和 **Cluster Cryostat** 自定义资源(CR)。选择以下选项之一：
   a. 要创建单命名空间 **Cryostat** 实例，请选择 **Cryostat**，然后单击 **Create instance**。
   b. 要创建 **Cryostat** 的多命名空间实例，请选择 **Cluster Cryostat**，然后点 **Create instance**。
5. 要配置 **TLS** 证书，请选择以下选项之一：
   a. 点 **Form view** 单选按钮。
      i. 在 **Name** 字段中，为您要创建的 **Cryostat** 实例指定一个名称。

ii. 展开 **Trusted TLS Certificates** 选项，然后单击 **Add Trusted TLS Certificate**。在 Red Hat OpenShift Web 控制台中显示选项列表。

图 1.6. Trusted TLS Certificates 选项



iii. 从 **Secret Name** 列表中选择 **TLS secret**。**Certificate Key** 字段是可选的。



注意

您可以通过单击 **Remove Trusted TLS** 证书来删除 **TLS** 证书。

iv. 点 **Create**。根据您创建的实例类型，实例会在以下标签页之一下打开：

- 如果您创建了单命名空间 **Cryostat** 实例，则实例位于 **Operator** 详情页面的 **Cryostat** 选项卡下。
- 如果您创建了 **Cluster Cryostat** 实例，则实例位于 **Operator** 详情页面的 **Cluster Cryostat** 选项卡下。

b. 点 **YAML** 视图 单选按钮。

i. 在 trustedCertSecrets 数组的 secretName 属性中指定您的 secret （位于与 Cryostat 应用程序相同的命名空间中）。

在 trustedCertSecrets 阵列中指定 secret 的示例

```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  trustedCertSecrets:
  - secretName: my-tls-secret
--
```

ii. *可选：* 将 certificateKey 属性值改为应用程序的 X.509 证书文件名。如果没有更改值，则 certificateKey 属性默认为 tls.crt。

更改 certificateKey 属性的值示例

```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  trustedCertSecrets:
  - secretName: my-tls-secret
    certificateKey: ca.crt
--
```

iii. 点击 Save。

Red Hat build of Cryostat Operator 会自动使用配置的安全设置重启 Cryostat 实例。

验证

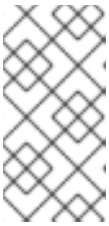
1. 通过在 CLI 中运行以下命令来确定所有应用程序 pod 是否都与 Cryostat pod 位于同一个 OpenShift 集群命名空间中：

```
$ oc get pods
```

2. 登录到 Cryostat 实例的 web 控制台。

3. 在 Cryostat 实例的 Dashboard 菜单中，从 Target 列表中选择一个目标 JVM。

4. 在 Cryostat web 控制台的导航菜单中选择 Recordings。在 Authentication Required 对话框中，输入您的 secret 的凭证，然后选择 Save 以将您的凭据提供给目标 JVM。



注意

如果所选目标为 JMX 连接启用了密码身份验证，则系统提示连接时必须为目标 JVM 提供 JMX 凭据。

Cryostat 通过经过身份验证的 JMX 连接连接到您的应用程序。现在，您可以使用 Recordings 和 Events 功能来监控应用程序的 JFR 数据。

其他资源

- 请参阅创建 JDK Flight Recorder (JFR)记录 （使用 Cryostat 创建 JFR 记录）
- 请参阅使用 Operator 在 Red Hat OpenShift 上安装 Cryostat（安装 Cryostat）
- 请参阅使用 Web 控制台访问 Cryostat(Installing Cryostat)

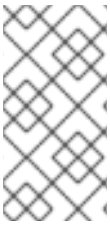
1.6. 更改存储卷选项

您可以使用 Red Hat build of Cryostat Operator 为 Cryostat 或 Cluster Cryostat 实例配置存储卷。Cryostat 支持持久性卷声明(PVC)和 emptyDir 存储卷类型。

默认情况下，Red Hat build of Cryostat Operator 为 Cryostat 或 Cluster Cryostat 实例创建一个 PVC，它使用分配的存储的默认 StorageClass 资源(MiB)。

您可以通过选择以下选项之一在 OpenShift Container Platform 上为 Cryostat 应用程序创建自定义 PVC：

- 进入 Form view 窗口中的 Storage Options > PVC > Spec，然后通过完成相关字段来自定义 PVC。
- 导航到 YAML 视图 窗口，然后编辑 spec: 键 集中的 storageOptions 数组以满足您的需要。



注意

如需了解更多有关使用 *Red Hat build of Cryostat Operator 配置 Cryostat* 指南中的更改存储卷选项的信息。

您可以通过选择以下选项之一在 OpenShift Container Platform 上为 Cryostat 应用程序配置 emptyDir 存储卷：

- 在 Form view 窗口中的 Storage Options 中启用 Empty Dir 设置。
- 在 YAML 视图 窗口中，将 spec.storageOptions.emptyDir.enabled 设置为 true。

先决条件

- 使用 Red Hat OpenShift Web 控制台登录到 OpenShift Container Platform。

流程

1. 在 Red Hat OpenShift web 控制台中，点 Operators > Installed Operators。
2. 从可用 operator 列表中，选择 Red Hat build of Cryostat。

a. 点 Details 标签页。

3. 在 Provided APIs 部分中，提供 Cryostat 和 Cluster Cryostat 自定义资源(CR)。选择以下选项之一：

- 要创建单命名空间 Cryostat 实例，请选择 Cryostat，然后单击 Create instance。
- 要创建 Cryostat 的多命名空间实例，请选择 Cluster Cryostat，然后点 Create instance。

4. 要更改 Cryostat 应用程序的存储设置，请选择以下选项之一：

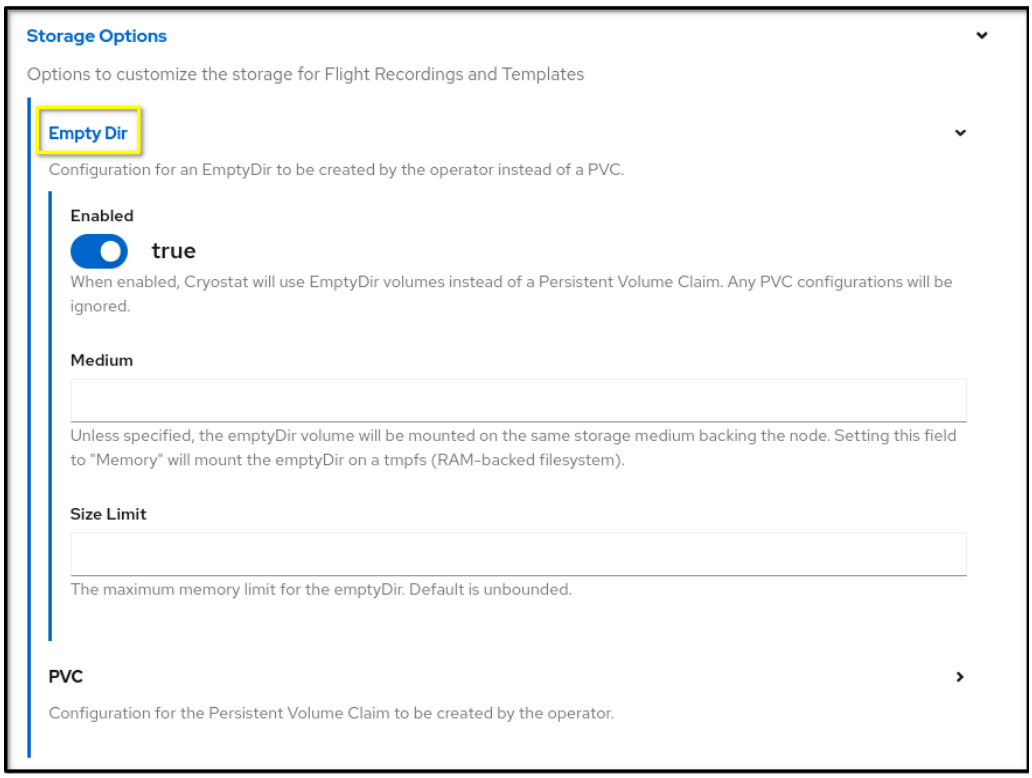
a. 点 Form view 单选按钮。

i. 导航到 Storage Options 部分，然后在 Name 字段中输入值。

ii. 展开 Storage Options，再点 Empty Dir。在 Red Hat OpenShift Web 控制台中打开展开的选择选项。

iii. 将 Enabled 开关设置为 true。

图 1.7. 显示 Empty Dir 交换机设置为 true的示例



iv. 点 Create。根据您创建的实例类型，实例会在以下标签页之一下打开：

- 如果您创建了单命名空间 Cryostat 实例，则实例位于 Operator 详情页面的 Cryostat 选项卡下。
- 如果您创建了 Cluster Cryostat 实例，则实例位于 Operator 详情页面的 Cluster Cryostat 选项卡下。

b. 点 YAML 视图 单选按钮。

i. 在 YAML 文件的 spec: 键集中，添加 storageOptions 定义，并将 emptyDir 属性设置为 true。

显示 emptyDir 属性设为 true的示例

```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
```

```
spec:
  storageOptions:
    emptyDir:
      enabled: true
      medium: "Memory"
      sizeLimit: 1Gi
--
```

ii. *可选：*为 **medium** 和 **sizeLimit** 属性设置值。

iii. 点 **Save** 按钮。**Red Hat build of Cryostat Operator** 为存储创建一个 **EmptyDir** 卷，而不是为您的 **Cryostat** 实例创建 **PVC**。

1.7. CRYOSTAT 的调度选项

在 **Red Hat OpenShift Web** 控制台中，您可以使用 **Red Hat build of Cryostat Operator** 定义用于调度 **Cryostat** 应用程序及其生成的报告到节点的策略。

您可以在 **Red Hat OpenShift** 的 **YAML** 配置文件中定义 **Node Selector**、**Affinities**、**Affinities** 和 **Tolerations** 定义。您必须在 **Cryostat** 应用的 **spec.SchedulingOptions** 属性和报告生成器 **sidecar** 的 **spec.ReportOptions.SchedulingOptions** 属性下定义这些定义。通过指定 **SchedulingOptions** 属性，**Cryostat** 应用程序及其报告生成器 **sidecar pod** 将调度到满足调度条件的节点。

目标节点应用程序可以从 **Cryostat** 实例接收 **sidecar** 报告更新。

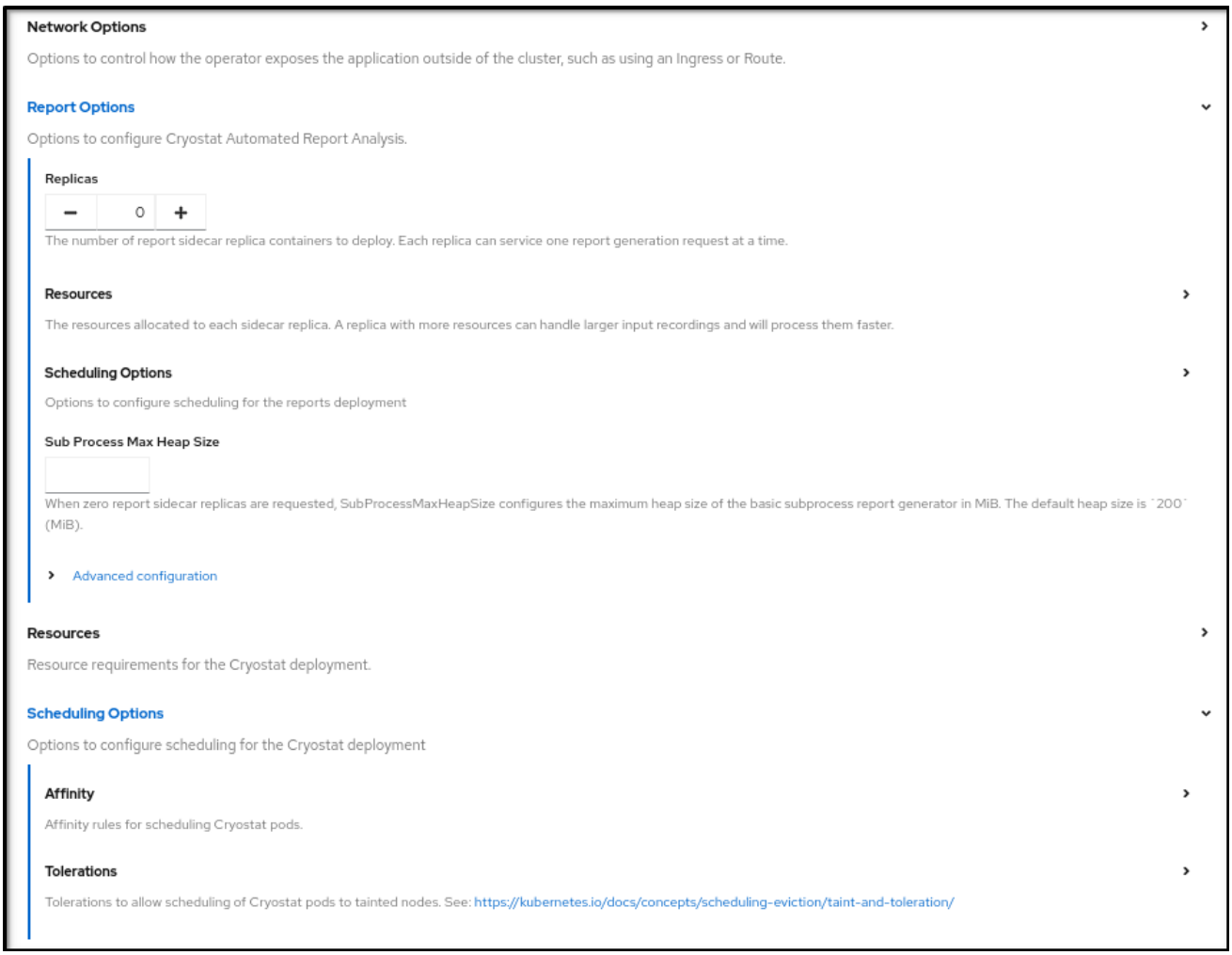
显示定义调度选项的 **Cryostat CR** 的 **YAML** 配置示例

```
kind: Cryostat
apiVersion: operator.cryostat.io/v1beta1
metadata:
  name: cryostat
spec:
  schedulingOptions:
    nodeSelector:
      node: good
    affinity:
      nodeAffinity:
        requiredDuringSchedulingIgnoredDuringExecution:
          nodeSelectorTerms:
```

```
        - matchExpressions:
          - key: node
            operator: In
            values:
            - good
            - better
      podAffinity:
        requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchLabels:
              pod: good
          topologyKey: topology.kubernetes.io/zone
      podAntiAffinity:
        requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchLabels:
              pod: bad
          topologyKey: topology.kubernetes.io/zone
    tolerations:
    - key: node
      operator: Equal
      value: ok
      effect: NoExecute
  reportOptions:
    replicas: 1
    schedulingOptions:
      nodeSelector:
        node: good
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
            - matchExpressions:
              - key: node
                operator: In
                values:
                - good
                - better
        podAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
          - labelSelector:
              matchLabels:
                pod: good
            topologyKey: topology.kubernetes.io/zone
        podAntiAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
          - labelSelector:
              matchLabels:
                pod: bad
            topologyKey: topology.kubernetes.io/zone
      tolerations:
      - key: node
        operator: Equal
        value: ok
        effect: NoExecute
```

另外，您可以打开 Red Hat OpenShift Web 控制台，创建一个 Cryostat 实例，然后在该 Cryostat 实例的 SchedulingOptions 和 reportOptions. SchedulingOptions 选项中定义 Affinities 和 Tolerations 定义。

图 1.8. OpenShift Web 控制台中的 Report Options 和 Scheduling Options 面板



第 2 章 POD SECURITY ADMISSION

Red Hat OpenShift 使用 Pod Security Admission (PSA)为同一 Red Hat OpenShift 集群中的应用程序 pod 应用一组安全规则。在 Cryostat 上下文中，这些应用程序 pod 包含 Cryostat pod 和一个 Report sidecar pod。另外，您可以在 Cryostat 自定义资源(CR)上启用 Report sidecar pod。如果应用程序不符合策略标准，则应用程序无法在 Red Hat OpenShift 集群中运行。

Red Hat OpenShift 4.8 弃用 PodSecurityPolicy API，并使用 PSA。PSA 提供以下优点：

- 包括一个内置控制器，可为应用程序 pod 强制执行 pod 安全标准。
- 包括一组定义三种不同策略的 pod 安全标准：Privileged、Baseline 和 Restricted。

在 Red Hat OpenShift 上，您可以使用 PSA 及安全性上下文约束(SCC)为 Red Hat OpenShift 集群定义策略。默认情况下，restricted-v2 SCC 与 Restricted pod 安全标准一致。

注意

默认情况下，Cryostat pod 的安全上下文符合 restricted-v2 SCC，这意味着 Red Hat OpenShift 可以接受强制限制 pod 安全标准的命名空间中 pod。

Restricted 策略要求 Red Hat build of Cryostat Operator 配置容器安全上下文，如下所示：

- 丢弃所有 功能
- 将 allowPrivilegeEscaltion 设置为 false

Restricted 策略要求 Red Hat build of Cryostat Operator 配置 pod 安全上下文，如下所示：

- 将 runAsNonRoot 设置为 true

- 将 seccompProfile 设置为 RuntimeDefault

另外，Red Hat build of Cryostat Operator 在 Cryostat 应用程序 pod 的 pod 安全上下文中定义 fsGroup，以便 Cryostat 可以在 Red Hat OpenShift 上的持久性存储卷中读取和写入文件。

如果您在符合 Restricted pod 安全标准外还有额外的要求，您可以覆盖 Cryostat 使用的默认安全上下文。

2.1. 配置安全上下文

您可以在 Red Hat OpenShift 上的 Cryostat 自定义资源(CR)中指定 pod 和容器安全上下文。安全上下文对 Cryostat pod、Report sidecar pod （在使用时）和每个 pod 的容器应用权限。

注意

如果您更改了 CR 的设置，这些设置会覆盖默认的安全上下文设置。

安全上下文将特定权限应用到 pod 中存在的应用程序。安全上下文无法更改 SCC 策略的条件。您可以创建自定义 SCC 来指示 Red Hat OpenShift 集群对 pod 强制执行严格的权限，如 Pod 可以执行的操作或 Pod 可以访问的资源。

要创建自定义 SCC，您必须具有集群管理权限。您还必须为在集群中运行的任何 pod 创建安全上下文，以便这些 pod 满足自定义 SCC 要求。

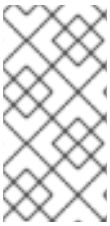
SCC 在 Red Hat OpenShift 集群级别和命名空间级别强制实施更改，以便此集群中运行的任何 pod 都接收策略标准。相反，安全性上下文对 pod 是唯一的。

默认情况下，Red Hat build of Cryostat Operator 遵循 Cryostat pod 的 restricted-v2 SCC 策略。

默认情况下，Red Hat build of Cryostat Operator 为 Cryostat 及其组件创建一个服务帐户，如 jfr-datasource 和 grafana。

要使此服务帐户使用自定义 SCC，请执行以下步骤之一：

- 创建一个 Role Binding，将 Cryostat 服务帐户绑定到使用自定义 SCC 的角色。
- 使用 Label Syncer 组件指示项目的命名空间遵循 PSA 策略。



注意

Label Syncer 组件超出了本文档的范围。您不能在 Red Hat OpenShift 系统命名空间中使用 Label Syncer 组件，它们通常以 openshift- 标签作为前缀。

重要

在将安全上下文配置为对应用程序 pod 应用特定权限前，请考虑 Red Hat OpenShift 上可能会引入的安全风险。PSA 提供三个通常满足大多数要求的逐步策略级别。红帽不承担与 Red Hat OpenShift pod 安全标准一致的安全上下文更改。

先决条件

- 使用 Red Hat OpenShift Web 控制台登录到 OpenShift Container Platform。
- 在 Red Hat OpenShift 上的项目中安装了 Red Hat build of Cryostat Operator。请参阅使用 Red Hat build of Cryostat Operator (Installing Cryostat)在 Red Hat OpenShift 上安装 Cryostat。
- *可选：* 阅读新的 PSA 和新的 SCC 策略。请参阅管理安全性上下文约束 (OpenShift Container Platform)。
- *可选：* 将您的项目配置为使用 PSA 提供的三种策略之一。
  - 如果要使用自定义 SCC 为 Pod 强制执行特定的策略，您必须配置 SCC 以启用 Pod 的服务帐户来访问它。

流程

1. 在 Red Hat OpenShift web 控制台中点 Operators > Installed Operators。

2. **从可用 operator 列表中，选择 Red Hat build of Cryostat。**

3. **点 Provided APIs > Create。Red Hat build of Cryostat Operator 不会为 Report sidecar pod 创建服务帐户。相反，这些 pod 在自己的命名空间中使用默认服务帐户。**

4. **要配置安全上下文，请完成以下选项之一：**

   a. **点 YAML 视图。在 spec: 元素中，编辑 securityOptions 和 reportOptions 属性以匹配您的安全要求。**

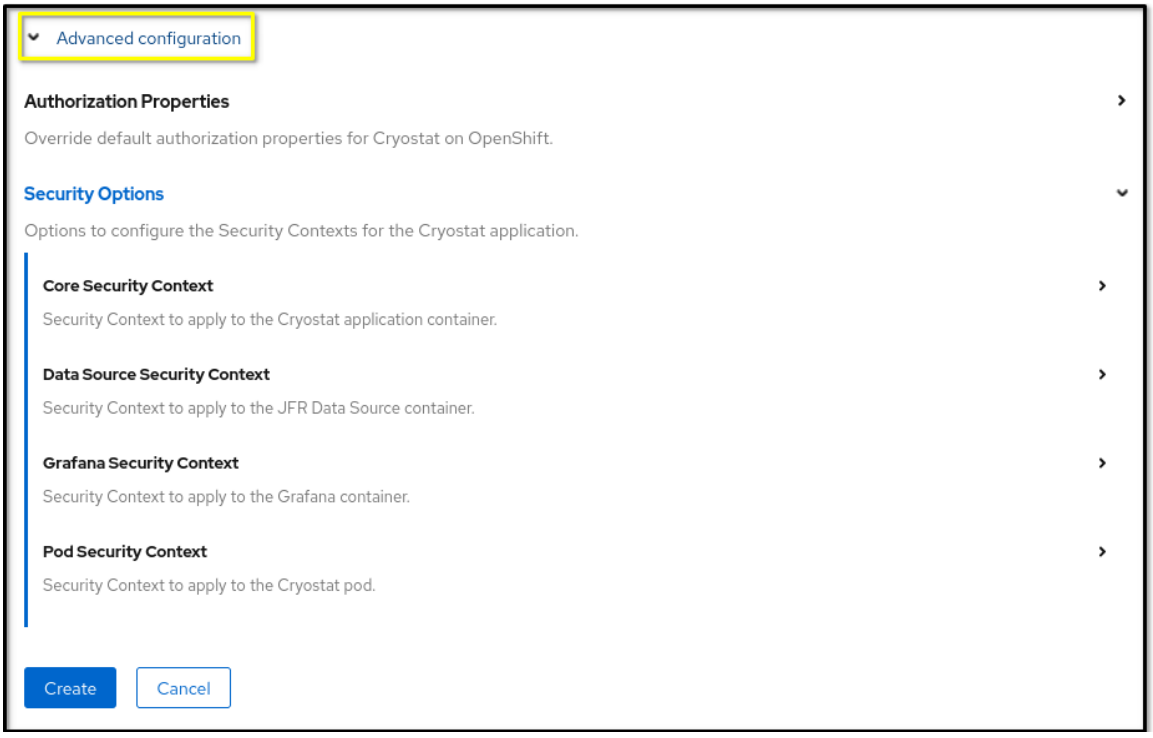
   安全上下文配置示例

```
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  securityOptions:
    podSecurityContext:
      runAsNonRoot: true
      seccompProfile:
        type: RuntimeDefault
    coreSecurityContext:
      allowPrivilegeEscalation: false
      capabilities:
        drop:
          - ALL
      runAsUser: 1001
    dataSourceSecurityContext:
      allowPrivilegeEscalation: false
      capabilities:
        drop:
          - ALL
    grafanaSecurityContext:
      allowPrivilegeEscalation: false
      capabilities:
        drop:
          - ALL
  reportOptions:
    replicas: 1
    podSecurityContext:
      runAsNonRoot: true
      seccompProfile:
        type: RuntimeDefault
    reportsSecurityContext:
      allowPrivilegeEscalation: false
```

```
    capabilities:
      drop:
        - ALL
    runAsUser: 1001
```

b. **展开 Advanced Configuration 以打开 Red Hat OpenShift Web 控制台中的附加选项。**

图 2.1. 高级配置菜单选项



c. **展开 Core Security Context。在可用选项列表中，为您的安全上下文定义设置。**

5. **点 Create。**

6. **根据情况，对数据源 安全上下文、Grafana 安全上下文 和 Pod 安全上下文 重复步骤一到五。**

7. ***可选：*** **如果您使用 Report Generator 服务，您也可以为此服务配置安全上下文，如下所示：**

a. 在 Report Options 中，展开 高级配置。

b. 展开 Security Options。根据需要定义 报告安全上下文 和 Pod 安全上下文。

其他资源

- Pod 安全标准策略.

2.2. POD 安全标准策略

Pod Security Admission (PSA)包括三个策略，它们涵盖了与 pod 安全标准相关的安全级别。下表解释每个策略：

profile	描述
Privileged	为您的 Cryostat pod 提供了广泛权限的不受限制策略。如果您需要向 pod 提供已知特权升级，请考虑设置此策略。
Baseline	限制已知特权升级的默认策略。**Baseline** 策略设置控制每个控制定义受限字段和允许值的位置。
Restricted	**Restricted** 策略，为您的 Cryostat pod 提供低级别权限。此策略为每个控制定义受限字段和允许的值设置控制。

第 3 章 RBAC 映射配置

在 OpenShift Container Platform (OCP)上，Cryostat 使用一个权限配置，它将 OCP 资源映射到 Cryostat 管理的资源。权限配置提供 Cryostat 框架，用于授权用户执行某些操作，如创建 JFR 记录或查看发现的目标。

下表概述了代表 Cryostat 管理的资源的定义：

资源	描述
CERTIFICATE	通过启用加密连接到 Java 虚拟机(JVM)应用的 SSL 证书。
凭证	存储的目标 JVM 应用凭据。
记录	为 JVM 应用创建的记录。
报告	报告从记录生成的内容。
规则	自动规则在匹配目标上开始记录，当它们对 Cryostat 可用时，以非交互方式进行记录。
TARGET	用于监控的 JVM 应用。
模板	配置记录的事件模板。

权限配置定义与前面列出的资源定义等效的 OCP 资源列表。API 请求指定资源操作，以将 Cryostat 管理的资源权限转换为 OCP 资源。Cryostat 检查这个操作的每个 API 请求，然后处理 API 请求。

Cryostat 为每个端点分配 resource-verb 对。这些动词是自定义的，特定于 Cryostat。在权限检查过程中，Cryostat 会将自定义动词转换为 RBAC 动词。

您可以在这些 Cryostat 管理的资源上实现以下动词：

- **CREATE** ：创建
- **DELETE** ：删除

- READ: get
- UPDATE: patch

以下示例显示了将 Cryostat 管理的资源链接到 Red Hat OpenShift 资源列表的映射配置：

```
TARGET=pods,services
```

要创建输出已发现 JVM 目标列表的 API 请求，例如从 Recordings 页面上的 Target JVM 窗格，您必须具有 READ 权限才能查看可发现的 TARGET。在 RBAC 系统中，READ 权限提供对读取 pod 和服务的访问。

默认情况下，Cryostat 使用以下 RBAC 映射配置。

```
auth.properties:
  TARGET=pods,services
  RECORDING=pods,pods/exec,cryostats.operator.cryostat.io
  CERTIFICATE=pods,cryostats.operator.cryostat.io
  CREDENTIALS=pods,cryostats.operator.cryostat.io
```

注意

ConfigMap 定义映射内容。前面的例子不会列出所有 Cryostat 管理的资源。如果 ConfigMap 中没有 Cryostat 管理的资源，Cryostat 会在处理 API 请求的过程中跳过权限检查。

Red Hat build of Cryostat Operator 将提供的 ConfigMap API 对象中的这些设置项目到 Red Hat OpenShift 上的 Cryostat pod 中。您的 Cryostat pod 可以随时访问这些设置，以确认用户可以访问的 Cryostat 功能。然后，您可以在自定义资源(CR)中定义 ClusterRole，为这些映射的 Red Hat OpenShift 资源提供特定权限。

显示 Cryostat CR 示例，其中包含 spec 字段中定义的 ConfigMap、ClusterRole 和 filename 字段

```
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
```

```
authProperties:
  configMapName: auth-properties
  filename: auth.properties
  clusterRoleName: oauth-cluster-role
```

其他资源

- 请参阅 RBAC 权限 (Installing Cryostat)。

3.1. 配置 RBAC 映射

您可以使用特定于 Cryostat 的 RBAC 权限创建自定义角色，然后将此角色绑定到用户的 Red Hat OpenShift 帐户。当您想为在同一 Cryostat 命名空间中运行的每个用户设置特定权限时，此功能很有用。

先决条件

- 使用 Red Hat OpenShift Web 控制台登录到 OpenShift Container Platform。
- 在项目中创建 Cryostat 实例。请参阅使用 operator (Installing Cryostat)在 Red Hat OpenShift 上安装 Cryostat。

流程

1. 在 ConfigMap 中定义自定义权限映射。

包含权限映射的 ConfigMap 示例

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: auth-properties
data:
  auth.properties: |
    TARGET=pods,deployments.apps
    RECORDING=pods,pods/exec
    CERTIFICATE=deployments.apps,pods,cryostats.operator.cryostat.io
    CREDENTIALS=cryostats.operator.cryostat.io
```

要使用自定义权限映射，ClusterRole 必须存在，并包含自定义权限映射中列出的所有 Red Hat OpenShift 对象的权限。

包含必要规则的 ClusterRole 示例

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: additional-oauth-client
rules:
- apiGroups:
  - operator.cryostat.io
  resources:
  - cryostats
  verbs:
  - create
  - patch
  - delete
  - get
- apiGroups:
  - ""
  resources:
  - pods
  - pods/exec
  verbs:
  - create
  - patch
  - delete
  - get
- apiGroups:
  - apps
  resources:
  - deployments
  verbs:
  - create
  - patch
  - delete
  - get
```

在 Red Hat OpenShift Web 控制台中输入凭证后，OAuth 服务器使用您的凭证和指定的范围来生成 API 令牌。

2.

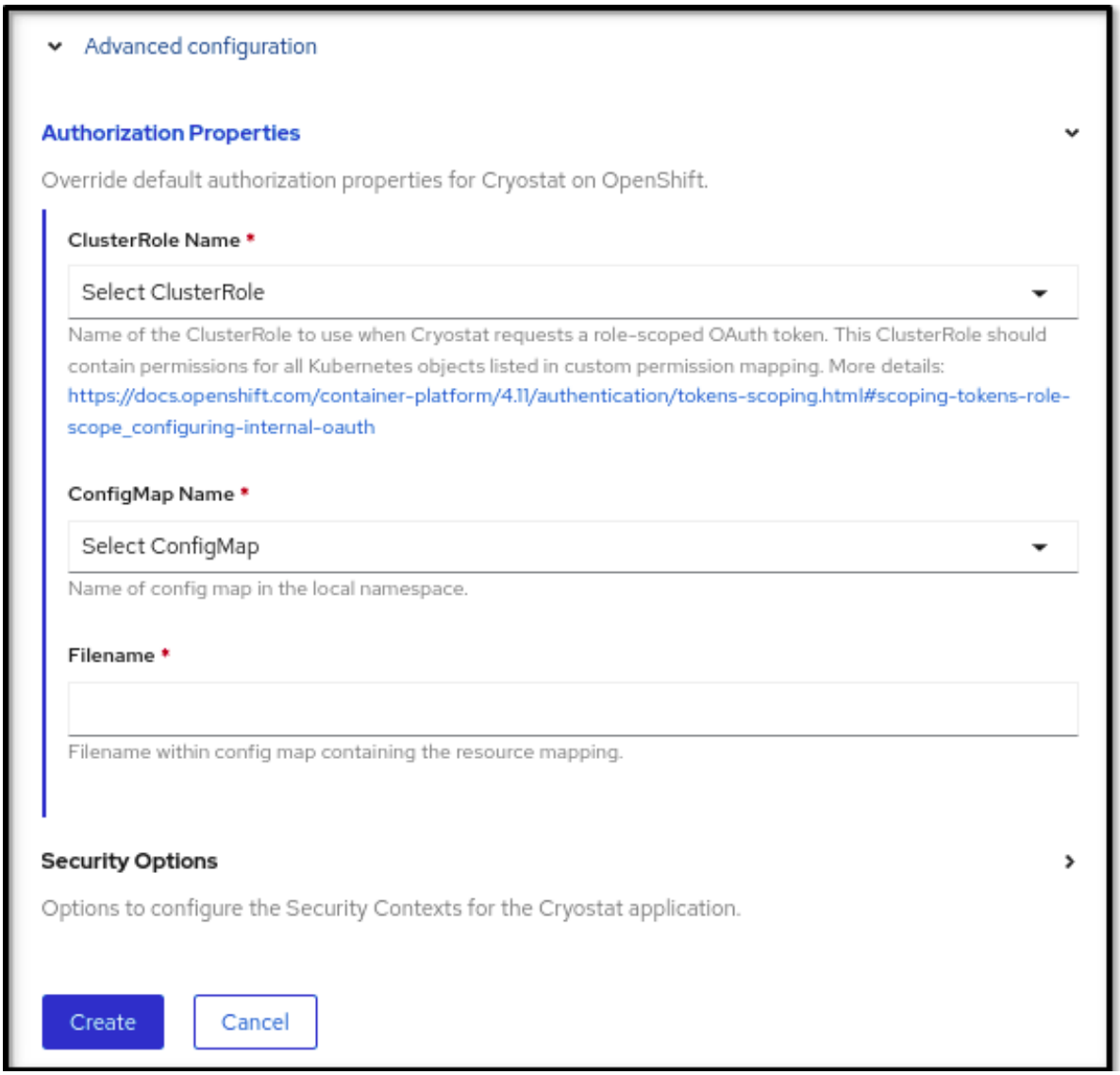
在 Cryostat 自定义资源(CR)中提供 authProperties spec，以引用包含映射内容的 ConfigMap，以及为这些映射的 Red Hat OpenShift 资源定义 RBAC 访问的 ClusterRole。

带有定义自定义权限映射的 authProperties 的 Cryostat CR 示例

```
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  authProperties:
 configMapName: auth-properties
 filename: auth.properties
 clusterRoleName: oauth-cluster-role
```

另外，您可以打开 Red Hat OpenShift Web 控制台，创建一个 Cryostat 实例，并在 Authorization Properties 选项中定义 ClusterRole Name、ConfigMap Name 和 Filename 属性，您可以在 Advanced configuration 部分中访问它。

图 3.1. OpenShift Web 控制台的高级配置部分



验证

1. 在 Installed Operators 菜单中，选择 Cryostat 实例。

2. 单击 Application URL 部分中的链接，以访问登录屏幕。OAuth 服务器将您重定向到 OpenShift Container Platform 登录页面。

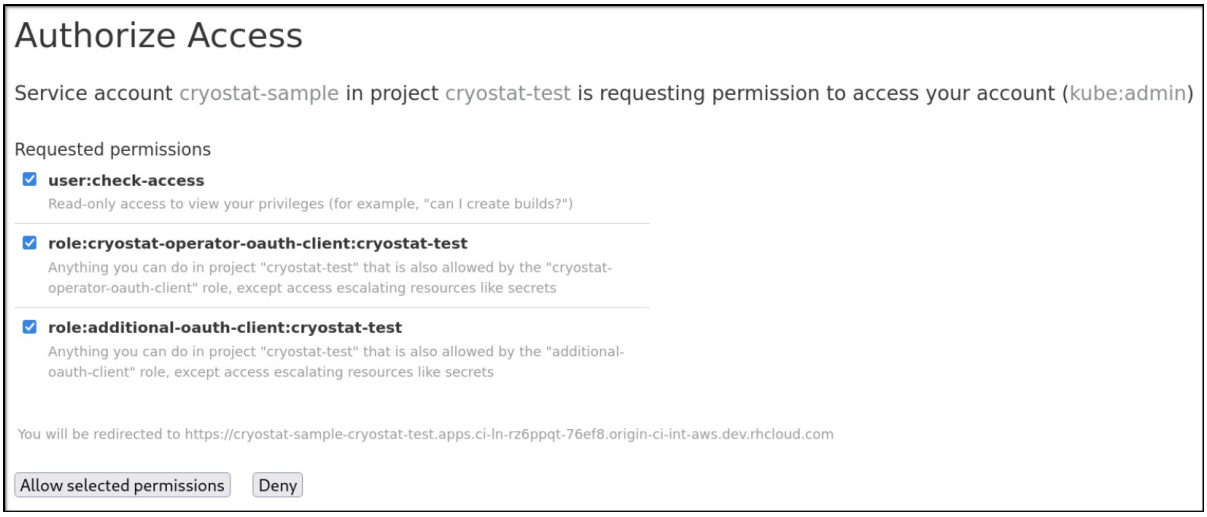
3. 输入您的凭证详情，然后点 Login。对于您第一次通过 OAuth 服务器登录时，您的 Web 浏览器上会打开一个 Authorize Access 页面。

4. 在 Requested Permissions 选项中，确认集群角色名称与您在 Cryostat CR 中指定的名称匹配。

5.

在 Authorize Access 窗口中，您可以选择所需的复选框。要获得最佳 Cryostat 性能，请选择所有复选框。

图 3.2. 列出三个权限的 Authorize Access 窗口



Authorize Access 窗口列出了以下权限：

- user:check-access，这是检查内部 Cryostat 应用程序请求的权限。权限为用户提供了查看其特权的只读访问权限。
- role:cryostat-operator-oauth-client:<namespace >，它是内部 Cryostat 应用程序请求的权限检查。通过 CLI 将 < *namespace* > 替换为项目名称或命名空间的名称。权限允许用户完成 cryostat-operator-oauth-client 角色指定的操作，但升级资源（如 secret）的权限除外。
- role:<user-define-clusterrole-name>:<namespace > : 您在 Cryostat CR spec 中定义的 clusterrole。通过 CLI 将 < *namespace* > 替换为项目名称或命名空间的名称。权限允许用户完成 additional-oauth-client 角色 指定的任何操作的访问权限，但升级对资源（如 secret）的访问。

6. 选择以下选项之一：

   a. 如果要接受所选请求权限，请点击 Allow selected permissions。

   b. 如果要拒绝所有请求的权限选项，请单击 Deny 按钮。

   您的 Web 浏览器会将您重定向到 Cryostat web 控制台，您可以在其中监控 Java 虚拟

机(JVM)中运行的 Java 应用程序。

其他资源

- 请参阅使用 Red Hat build of Cryostat Operator (Installing Cryostat)在 Red Hat OpenShift 上安装 Cryostat。

更新于 2023-12-13