Red Hat build of Cryostat 2

使用 Cryostat Operator 配置 Cryostat

指南

Last Updated: 2023-02-23

Red Hat build of Cryostat 2 使用 Cryostat Operator 配置 Cryostat

指南

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

红帽构建的 Cryostat 是 OpenShift Container Platform 上的红帽产品。使用 Cryostat Operator 配置 Cryostat 以了解如何使用 Cryostat Operator 配置 Cryostat。

目录

前言

Red Hat build of Cryostat 是 JDK Flight Recorder (JFR)的一个容器原生实现，可用于安全地监控在 OpenShift Container Platform 集群上运行的工作负载中的 Java 虚拟机(JVM)性能。您可以使用 Cryostat 2.2 使用 Web 控制台或 HTTP API 启动、停止、检索、存档、导入和导出 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存储和分析您的记录，或者您可以将记录导出到外部监控应用程序，以对记录的数据执行更加深入的分析。

重要

红帽构建的 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。

对红帽文档提供反馈

我们感谢您对我们文档的反馈。要提供反馈，您可以突出显示文档中的文本并添加注释。按照以下步骤，了解如何向红帽文档提交反馈。

前提条件

- 登录红帽客户门户。
- 在红帽客户门户网站中，以 多页 HTML 格式查看文档。

流程

1. 点击 **反馈** 按钮查看现有的读者注释。

注意

反馈功能仅在多页 HTML 格式中启用。

2. 高亮标记您要提供反馈的文档中的部分。
3. 在您选择的文本旁边的提示菜单中，单击 **Add feedback**。
   文本框将在页面右侧的"反馈"部分中打开。
4. 在文本框中输入您的反馈，然后点 **Submit**。
   您已创建了文档问题。
5. 要查看问题，请单击反馈视图中的问题跟踪器链接。

第 1 章 CRYOSTAT OPERATOR

您可以使用 Cryostat Operator 管理和配置 Cryostat 实例。Cryostat Operator 在 OpenShift Container Platform (OCP)上提供。

1.1. CRYOSTAT OPERATOR 概述

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

在 Cryostat 2.2 中，Cryostat Operator 的 Operator Capability Level 设置为 Operator Lifecycle Manager 框架上的 **Level 2 Seamless Upgrades**。升级 Cryostat Operator 后，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、规则和其他存储组件。

您可以使用 Cryostat Operator 在 OpenShift 上创建持久性卷声明(PVC)，以便您的 Cryostat 应用程序可以在云存储磁盘上存储存档的记录。

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

- 配置由 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。
- 将您的 Cryostat 应用程序配置为信任特定应用程序的 TLS 证书。
- 将 Cryostat 部署为最小部署，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。
- 安装位于 ConfigMap 中的自定义事件模板文件，指向您的 Cryostat 实例，因此您可以在 Cryostat 启动时使用模板来创建记录。

Cryostat 2.2 版本为 Cryostat Operator 包括以下配置选项：

- 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 Cryostat Operator 创建的服务。
- sidecar 报告选项，C Cryostat Operator 可用于为您的 Cryostat 应用程序置备一个或多个报告生成器。

在配置Cryostat Operator 前，请确保满足以下先决条件：

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

其他资源

- 请参阅 Operator Capability Levels (Operator SDK)
- 请参阅使用 操作器在 OpenShift 上安装 Cryostat （以 Cryostat 开始）

1.2. 排除支持容器

您可以选择排除支持性应用程序使用 Cryostat 应用程序进行部署。支持的应用程序是您的 Cryostat pod 中列出的支持容器。当排除支持容器时，部署 Cryostat 应用程序需要较少的系统资源。

默认情况下，C Cryostat 将项目的 Cryostat Operator YAML 配置文件中的 **minimal** 属性设置为 **false**。使用这个配置，C Cryostat Operator 使用所有标准支持的应用程序（如 **jfr-datasource** 和 Grafana 仪表板）部署您的 Cryostat 应用程序，它们包含在与 Cryostat 应用程序相同的 pod 中。这些支持的应用程序可以与您的 Cryostat 数据交互，并为您提供与这个数据交互的额外功能。

Cryostat Operator 默认使用以下配置：

- 部署预先配置的 Grafana 应用程序。
- 部署 **jfr-datasource** 应用，以将 JDK Flight Recorder (JFR)数据转换为 JSON，这是 Grafana 的可读取格式。
- 在部署 Cryostat 时，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 Cryostat Operator 会自动重启 Cryostat 实例作为最小部署。这意味着，Operator 只部署在 Cryostat 容器中列出的应用程序，并忽略任何标准的支持性应用程序，如 **jfr-datasource** 和 Grafana 仪表板，它们包含在与 Cryostat 应用程序相同的 pod 中。

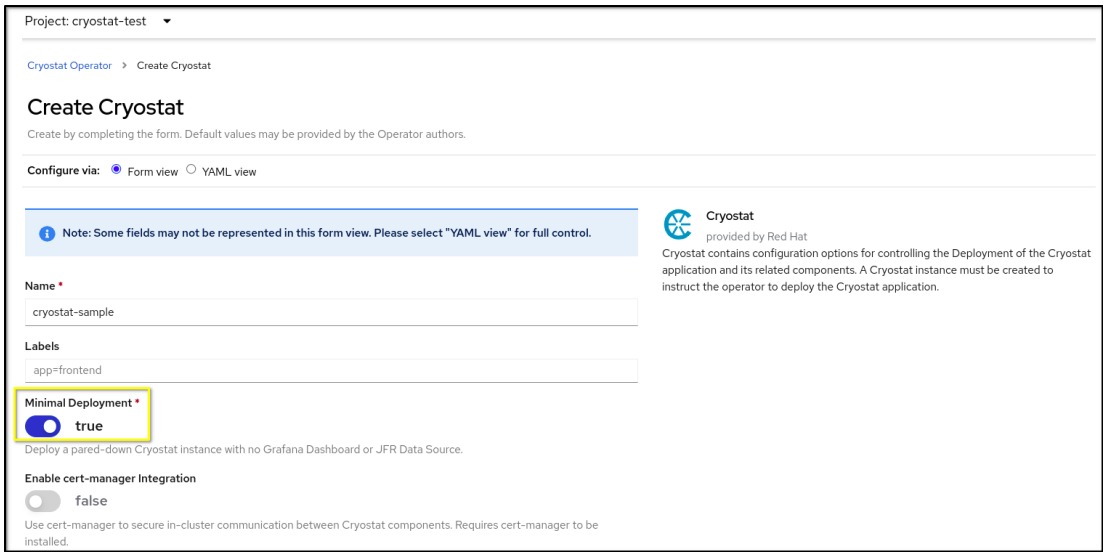
前提条件

- 使用 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 操作器在 OpenShift 上安装 Cryostat （使用 Cryostat 开始）。

流程

1. 在 OpenShift Web 控制台中，点 **Operators > Installed Operators**。
2. 从可用 operator 列表中选择 **Cryostat Operator**。
3. 点 **Provided APIs** 菜单下的 **Create instance**。
4. 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 开关切换为 true



ii. 点 **Create**。您的 Cryostat 实例会在 **Operator** 详情页面的 **Cryostat** 标签页中打开。

b. 点击 **YAML 视图** 单选按钮。

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

配置 minimal 属性示例

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

ii. 点 **Save** 按钮。

验证

1. 在 OpenShift Web 控制台中，选择您的 Cryostat 实例。
2. 选择 **Resources** 选项卡。
3. 从部署列表中，选择与 Cryostat 实例名称匹配的部署。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 Cryostat Operator 已部署您的 Cryostat 应用程序作为最小部署。

其他资源

- 如需有关 OpenShift CLI 的更多信息，请参阅 OpenShift CLI 入门 (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 Cryostat Operator 的 **enableCertManager** 属性来禁用 cert-manager 功能。

默认情况下，C Cryostat Operator 的 **enableCertManager** 属性被设置为 **true**。这意味着 Cryostat Operator 使用 cert-manager **CA** 签发者为您的 Cryostat 组件生成自签名证书。Cryostat Operator 使用这些证书在集群中运行的 Cryostat 组件间启用 HTTPS 通讯。

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

重要

如果将 **enableCertManager** 属性设为 **false**，您可能会引入从未加密内部流量到包含运行的 Cryostat 应用程序的集群的潜在安全隐患。

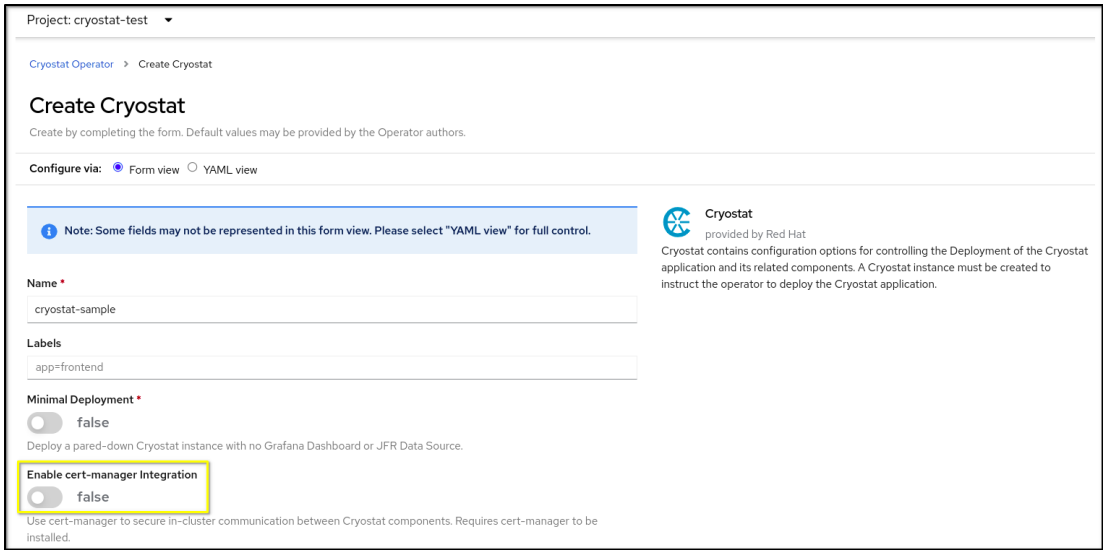
前提条件

- 使用 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 操作器在 OpenShift 上安装 Cryostat （使用 Cryostat 开始）。

流程

1. **在 OpenShift Web 控制台中进入 Operators > Installed Operators。**
2. 从可用 operator 列表中选择 **Cryostat Operator**。
3. 在 **Provided APIs** 菜单中点 **Create instance**。
4. 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** switch 设为 **false**，然后在 **Name** 字段中输入值。

图 1.2. 将 Enable cert-manager Integration 开关切换为 false



      ii. 点 **Create**。您的 Cryostat 实例会在 **Operator** 详情页面的 **Cryostat** 标签页中打开。

b. 点击 **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 文件中配置 spec: key 的示例

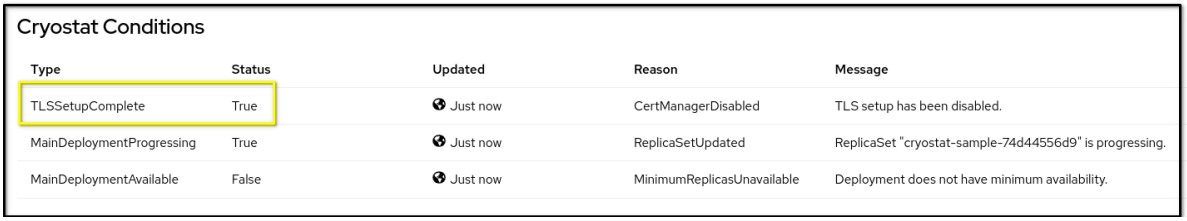
```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  enableCertManager: false
--
```

ii. 点 **Save** 按钮。
Cryostat Operator 会自动重启 Cryostat 应用程序，可让应用程序使用更新的 **enableCertManager** 属性配置运行。

验证

1. 从 **Operator** 详情页面的 **Cryostat** 选项卡中选择您的 Cryostat 实例。
2. 导航到 **Cryostat Conditions** 表。
3. 验证 **TLSSetupComplete** 条件已设置为 **true**，并且此条件的 **Reason** 列已设置为 **CertManagerDisabled**。这表示您已将 **enableCertManager** 属性设置为 **false**。

图 1.3. 显示将 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 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。您可以通过其关联的事件模板配置 JFR。

默认情况下，C Cryostat Operator 包含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 Cryostat Operator 为 Cryostat 实例生成自定义事件模板，并将这些模板存储在 ConfigMap 中以方便检索。您可以使用以下方法生成自定义事件模板：

- 使用 OpenShift Web 控制台将事件模板上传到自定义资源中。

- 在 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一个新的 Cryostat 实例。然后，您可以将自定义事件模板与 JFR 一起使用，以监控 Java 应用程序以满足您的需要。

前提条件

- 使用 OpenShift Web 控制台登录到 OpenShift Container Platform。
- 在项目中创建 Cryostat 实例。
- 登录到您的 Cryostat web 控制台。

流程

1. 要下载默认事件模板，请导航到 Cryostat Web 控制台和 **Events** 菜单，点 **Downloads**。

注意

事件模板采用 XML 格式，文件名扩展名为 **.jfc**。

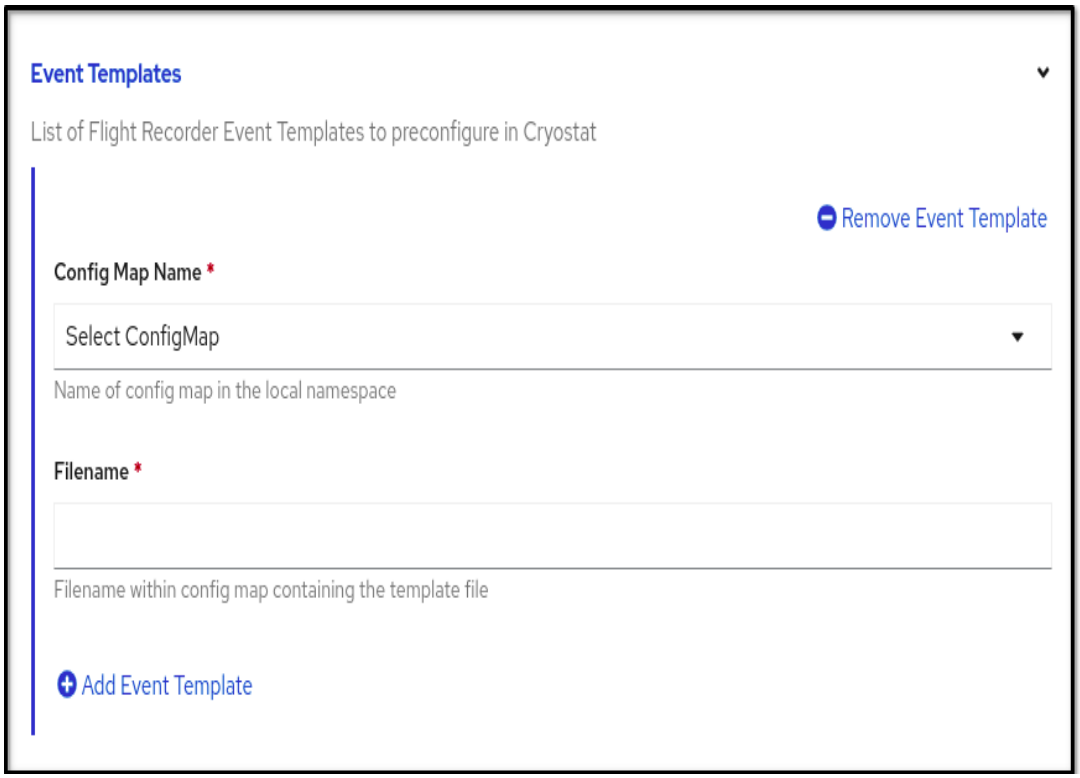
2. *可选：* 如果您希望自定义事件模板，使用文本编辑器或 XML 编辑器编辑下载的默认事件模板，以配置模板以满足您的需要。
3. 在 CLI 中输入 **oc login** 命令，登录到您的 OpenShift Web 控制台。
4. 在 CLI 中输入以下命令，从事件模板创建 **ConfigMap** 资源。您必须在要部署 Cryostat 应用程序的路径中发出 命令。您可以使用此资源存储运行 Cryostat 实例的集群中的事件模板文件。

使用 CLI 创建 ConfigMap 资源示例

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

5. 在 OpenShift Web 控制台中，点 **Operators > Installed Operators**。
6. 从可用 operator 列表中选择 **Cryostat Operator**。
7. 点 **Provided APIs** 菜单下的 **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 实例的 **Event Templates** 部分。
      ii. 在 **Event Templates** 菜单中点 **Add Event Template**。在 OpenShift 控制台中打开 **Event Templates** 部分。
      iii. 从 **Config Map Name** 下拉列表中，选择包含事件模板的 ConfigMap 资源。

图 1.4. Cryostat 实例的事件模板选项



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

v. 点 **Create** 按钮生成带有自定义事件模板的 Cryostat 实例。

b. 点击 **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 Cryostat Operator 指向 ConfigMap，以便 Cryostat Operator 可以读取事件模板。

为 eventTemplates 属性指定自定义事件模板示例

```
--
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

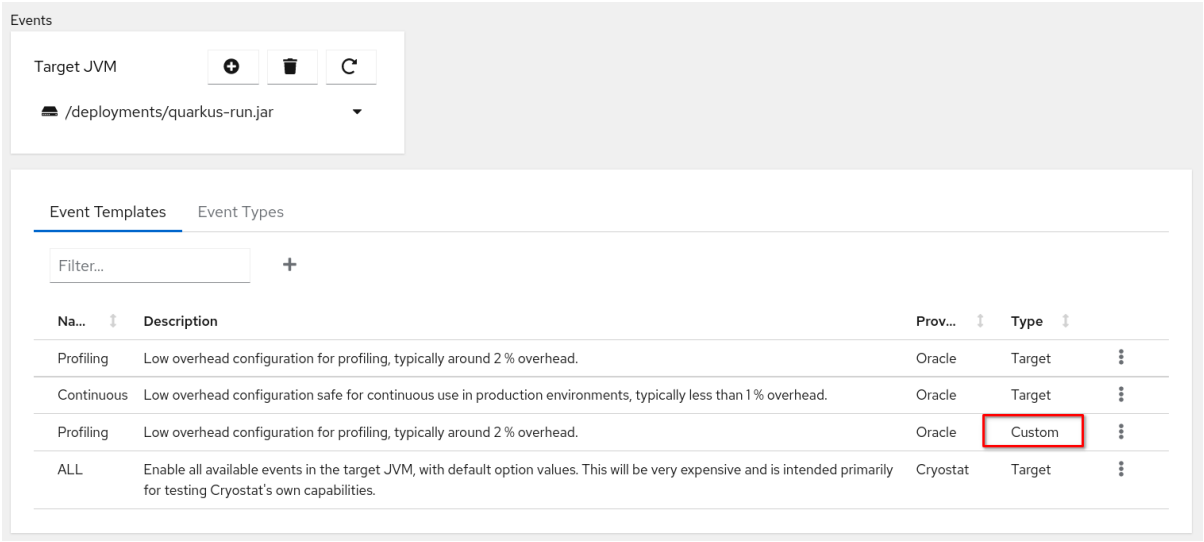
您必须从 **configMapName** 下拉列表中选择与 Cryostat 实例关联的 ConfigMap 名称。另外，您必须在 **filename** 字段中指定一个与 ConfigMap 关联的键。

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在 Cryostat web 控制台中与默认事件模板一起打开。

验证

1. 在 Cryostat Web 控制台中，从菜单中点击 **Events**。如果 web 控制台中打开 **Authentication Required** 窗口，请输入您的凭证并点 **Save**。
2. 在 **Event Templates** 选项卡中，检查您的自定义事件模板是否显示在可用事件模板列表中。

图 1.5. 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 （以 Cryostat 开始）
- 请参阅使用 Web 控制台访问 Cryostat（通过 Cryostat 开始）
- 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 Cryostat Operator 来配置 Cryostat 以信任特定应用程序的 TLS 证书。

Cryostat 尝试打开使用 TLS 证书的目标 JVM 的 JMX 连接。对于成功的 JMX 连接，Cryostat 必须在目标 JVM 证书上传递其所有身份验证检查。

您可以在 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** 属性中指定与 Cryostat 应用程序相同的 secret。 **certificateKey** 属性默认为 **tls.crt**，但您可以将值改为 X.509 证书文件名称。

重要

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

前提条件

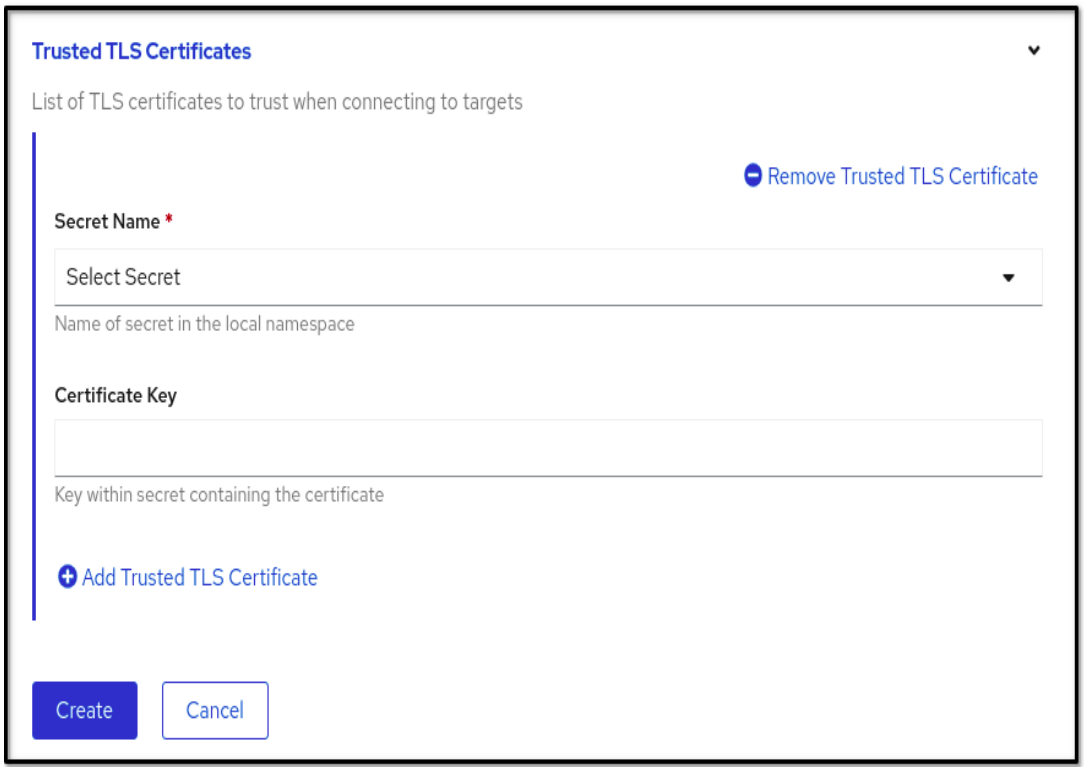
- 使用 OpenShift Web 控制台登录到 OpenShift Container Platform。

- 在项目中创建 Cryostat 实例。
- 登录到您的 Cryostat web 控制台。

流程

1. 在 OpenShift Web 控制台中，点 **Operators > Installed Operators**。
2. 从可用 operator 列表中选择 **Cryostat Operator**。
3. 要配置 TLS 证书，请选择以下选项之一：
   a. 在 **Operator** 详情页面的 **Details** 标签页中创建一个 Cryostat 实例。
      i. 在 **Provided APIs** 菜单下，点 **Create instance**。
      ii. 在 **Name** 字段中输入值。
      iii. 展开 **Trusted TLS Certificates** 选项，然后单击 **Add Trusted TLS 证书**。OpenShift Web 控制台中显示选项列表。

      图 1.6. Trusted TLS Certificates 选项



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

      注意

      您可以点 **Remove Trusted TLS 证书 来删除 TLS 证书**。

      v. 点 **Create**。您的 Cryostat 实例会在 **Operator** 详情页面的 **Cryostat** 标签页中打开。

   b. 导航到 **Operator Details** 页面中的 **YAML** 选项卡。您的 Cryostat Operator 的 YAML 文件在您的 OpenShift Container Platform Web 控制台中打开。
      i. 在 **trustedCertSecrets** 数组的 **secretName** 属性中指定您的 secret，它和您的 Crvostat

i. 在 trustedCertSecrets 数组中 secretName 属性值指定 secret，它和 Cryostat 应用程序位于同一个命名空间中。

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** 属性值更改为应用程序的 X.509 证书文件名称。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 **Save** 按钮。
Cryostat Operator 会自动重启带有配置的安全设置的 Cryostat 实例。

验证

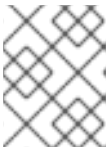
1. 在 CLI 中发出以下命令，确定所有应用程序 pod 是否都存在于与 Cryostat pod 相同的 OpenShift 集群命名空间中：

```
$ oc get pods
```

2. 登录到您的 Cryostat 实例的 web 控制台。

3. 在 Cryostat 实例的 **Dashboard** 菜单中，从下拉列表中选择 **Target JVM**。

4. 从 Cryostat Web 控制台的左侧面板中选择 **Recordings**。在 **Authentication Required 对话框窗口中** 输入您的 secret 的凭据，然后选择 **Save**，将凭证提供给目标 JVM。



注意

如果所选目标启用了 JMX 连接的密码身份验证，在提示输入连接时必须为目标 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 记录 和事件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 操作器在 OpenShift 上安装 Cryostat（以 Cryostat 开始）
- 请参阅使用 Web 控制台访问 Cryostat（通过 Cryostat 开始）

1.6. 更改存储卷选项

您可以使用 Cryostat Operator 为 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，C Cryostat Operator 为您的 Cryostat 实例创建一个 PVC，它使用分配 500MB 字节(MiB)的默认 StorageClass 资源。

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

- 在 Form view 窗口中导航到 Storage Options > PVC > Spec，然后通过完成相关字段自定义 PVC。
- 导航到 YAML 视图 窗口，然后编辑 spec: key set 中的 storageOptions 数组，以满足您的需要。

注意

如需了解更多有关创建自定义 PVC 的信息，可以使用 *Cryostat Operator 更改存储卷选项来配置 Cryostat* 指南。

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

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

前提条件

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

流程

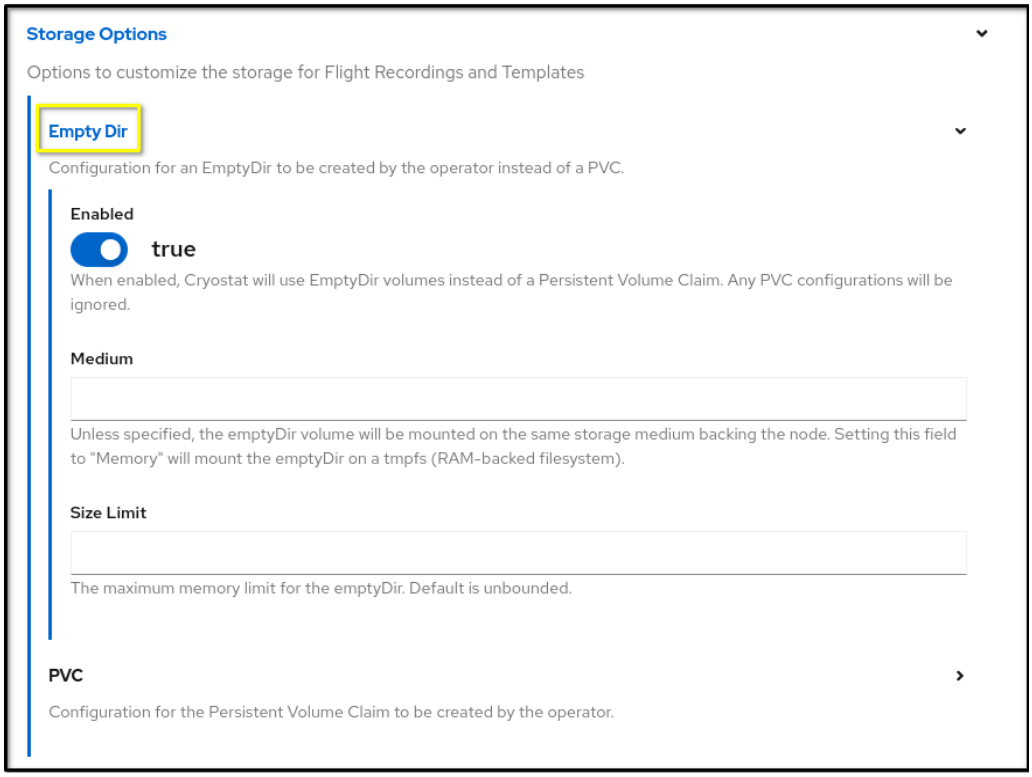
1. 在 OpenShift Web 控制台中，点 Operators > Installed Operators。
2. 从可用 operator 列表中选择 Cryostat Operator。
3. 点 Provided APIs 菜单下的 Create instance。
4. 选择以下选项之一来更改 Cryostat 应用程序的存储设置：
    a. 点 Form view 单选按钮。

i. 导航到 Storage Options 部分，然后在 Name 字段中输入一个值。

ii. 展开 Storage Options，再单击 Empty Dir。在 OpenShift Web 控制台中打开展开的选项选择。

iii. 将 Enabled 开关设置为 true。

图 1.7. 显示 Empty Dir switch 设为true的示例



iv. 点 Create。您的 Cryostat 实例在 Operator 详情页面上的 Cryostat 标签页下打开。

b. 点击 YAML 视图 单选按钮。

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

显示 emptyDir 属性设置为 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。Cryostat Operator 为存储创建一个 EmptyDir 卷，而不是为您的 Cryostat 实例创建一个 PVC。

1.7. CRYOSTAT 的调度选项

在 OpenShift Web 控制台中，您可以使用 Cryostat Operator 定义调度 Cryostat 应用程序及其生成的报告到节点的策略。

您可以在 OpenShift 上 Cryostat 自定义资源(CR)的 YAML 配置文件中定义 Node Selector、Affinities 和 Tolerations 定义。您必须在 Cryostat 应用程序的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 应用程序及其报告会生成 sidecar pod。这些 pod 可以调度到匹配的节点上。

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

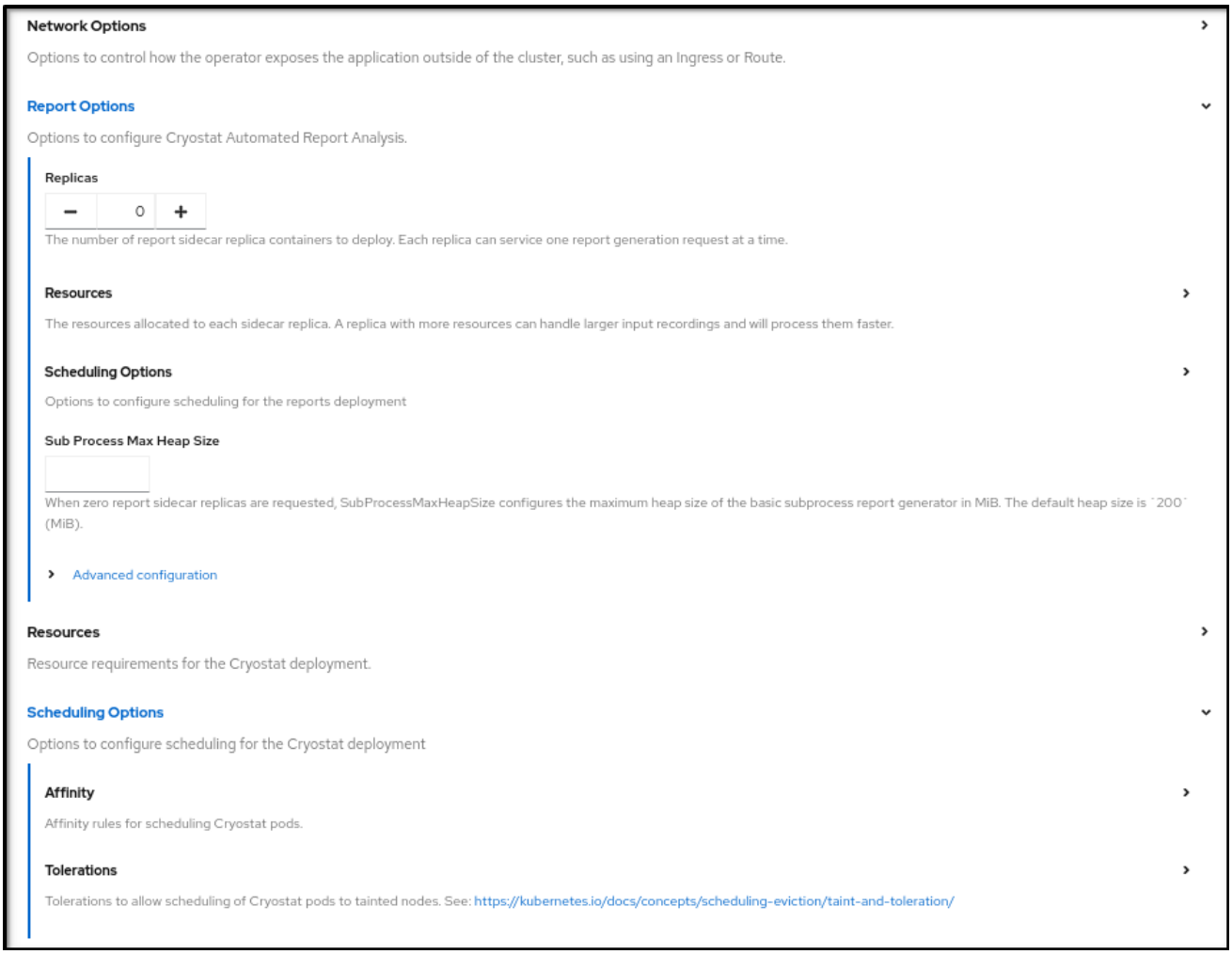
显示定义调度选项的 Cryostat CR 的 YAML 配置

```
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
```

或者，您可以打开 OpenShift Web 控制台，创建一个 Cryostat 实例，然后为该 Cryostat 实例定义 SchedulingOptions 和 reportOptions.SchedulingOptions 选项中的 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

OpenShift 使用 Pod Security Admission (PSA)为同一 OpenShift 集群中的应用容器集应用一组安全规则。在 Cryostat 上下文中，这些应用程序 pod 包括一个 Cryostat pod 和 Report sidecar pod。您可选择在自定义资源(CR)上启用 Report sidecar pod。如果应用不符合策略标准，则应用无法在 OpenShift 集群中运行。

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

- 包含一个内置控制器，可以为应用容器集强制执行 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 OpenShift 上，您可以使用带有安全性上下文约束(SCC)的 PSA 为 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 的安全上下文符合 **restricted-v2** SCC，这意味着 OpenShift 可以接受实施 **Privileged** Pod 安全标准的命名空间中的 pod。

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

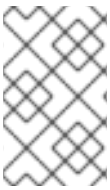
- 将 **runAsNonRoot** 设置为 **true**
- 将 **seccompProfile** 设置为 **RuntimeDefault**

另外，Cryostat Operator 在 Cryostat 应用 Pod 的 Pod 安全上下文中定义 **fsGroup**，因此 Cryostat 可以读取和写入 OpenShift 上持久性存储卷中的文件。

如果您在满足限制的 Pod 安全标准之外还有额外的要求，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 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** （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，这些设置将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容器集中存在的应用。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 OpenShift 集群对 Pod 强制实施严格的权限，如 Pod 可以执行或 Pod 可以访问的资源等。

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

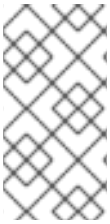
SCC 在 OpenShift 集群级别和命名空间级别强制实施更改，以便此集群内运行的任何容器集都可以接收策略标准。相反，安全上下文对 pod 是唯一的。

默认情况下，Cryostat Operator 符合 Cryostat Pod 的 restricted-v2 SCC 策略。

默认情况下，Cryostat Operator 创建一个服务帐户，用于指定对 Cryostat 组件的访问，如 jfr-datasource、grafana 和其他组件。

要让此服务帐户使用自定义 SCC，请执行以下步骤：

- 创建一个 角色绑定，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 OpenShift 系统命名空间中使用 Label Syncer 组件，它们通常带有 openshift- tag 前缀。

重要

在配置安全上下文以将特定权限应用到应用容器集之前，请考虑 OpenShift 中可能会引入的安全风险。PSA 提供三级策略级别，它们通常满足大多数要求。红帽对与 OpenShift pod 安全标准不一致的安全上下文更改不承担任何责任。

前提条件

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

- 在 OpenShift 上的项目中安装了 Cryostat Operator。请参阅使用 Cryostat Operator （通过 Cryostat 开始）在 OpenShift 上安装 Cryostat。

- 在 OCP 上创建服务帐户。请参阅 了解并创建服务帐户 (OpenShift Container Platform)。

- *可选：* 读取新的 PSA 和新 SCC 策略。请参阅管理安全性上下文约束 (OpenShift Container Platform)。

- *可选：* 将项目配置为使用 PSA 提供的三个策略之一。

  - 如果要使用自定义 SCC 为 Pod 强制执行特定策略，您可能需要配置 SCC，以允许服务帐户访问您的 Pod。

流程

1. 在 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。默认情况下，Cryostat Operator 为您的 Cryostat pod 创建一个服务帐户，并为您启用的任何 Report sidecar pod 创建一个服务帐户。

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。

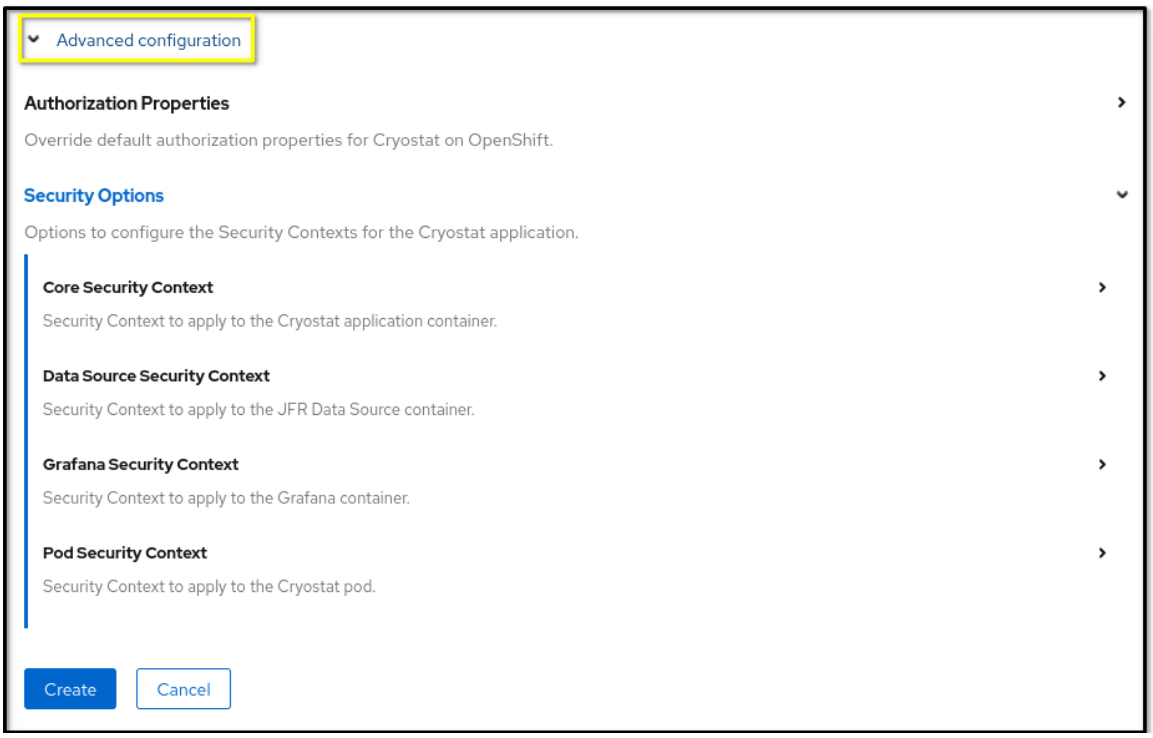
   安全上下文配置示例

```
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 Configurations，以在 OpenShift Web 控制台中打开附加选项。**

图 2.1. 高级配置菜单选项



展开 Core 安全上下文。在可用选项列表中，为您的安全上下文定义设置。

5. 点 Create。

6. 根据需要，为 数据源安全上下文、Grafana 安全上下文 和 Pod 安全上下文重复一个到 五个。

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 报告选项 中，展开 Advanced Configuration。

   b. 展开 Security Options。根据情况定义 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 安全策略

Pod Security Admission (PSA)包含三个策略，它们涵盖与 pod 安全标准相关的安全级别。下表解释每个策略：

配置集	描述
privileged	为您的 Cryostat pod 提供大量权限的不受限制的策略。如果您需要向 pod 提供已知的特权升级，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	为 Cryostat pod 提供低级权限的 **Restricted** 策略。此策略设置控制，每个控制定义 restricted 字段和允许的值。

第 3 章 RBAC 映射配置

在 OpenShift Container Platform (OCP)上，Cryostat 使用权限配置将 OCP 资源映射到 Cryostat 管理的资源。权限配置为 Cryostat 提供了一个框架，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 JVM 应用的 SSL 证书。
凭证	为启用了 JMX 的身份验证的目标存储凭证。
记录	为 JVM 应用程序创建的记录。
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，以非交互方式使用 Cryostat。
TARGET	要监控的 JVM 应用。
模板	配置记录的事件模板。

权限配置定义等同于之前列出的资源定义的 OCP 资源列表。API 请求指定将 Cryostat 管理的资源权限转换为 OCP 资源的资源操作。Cryostat 检查每个 API 请求，然后处理 API 请求。

Cryostat 为每个端点分配资源验证对。这些动词是自定义的，特定于 Cryostat。在权限检查过程中，Cryostat 将自定义动词转换为 RBAC 动词。

您可以在这些 Cryostat-managed 资源上实施以下操作动词：

- **CREATE ：create**
- **DELETE: delete**

- READ: get
- UPDATE: patch

以下示例显示了将 Cryostat-managed 资源链接到 OpenShift 资源列表的映射配置：

```
TARGET=pods,services
```

要创建输出发现的 JVM 目标列表的 API 请求，例如，从 Recordings 页面的 Target JVM 窗格中，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 和服务的访问权限。

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。上例不会列出所有 Cryostat-managed 资源。如果 ConfigMap 中缺少 Cryostat 管理的资源，Cryostat 会在处理 API 请求期间跳过权限检查。

Cryostat Operator 将提供的 ConfigMap API 对象中的这些设置项目到 OpenShift 上的 Cryostat 容器集。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 功能的权限。然后，您可以在 CR 中定义 ClusterRole，为这些映射的 OpenShift 资源提供特定权限。

显示了一个在 spec 字段中定义的 ConfigMap、ClusterRole 和 filename 字段的 Cryostat CR

```
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 （使用 Cryostat 开始）。

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 OpenShift 帐户。当您要为在同一 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。

前提条件

- 使用 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 操作器在 OpenShift 上安装 Cryostat （使用 Cryostat 开始）。

流程

1. 在 ConfigMap 对象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 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 OpenShift Web 控制台中输入凭据后，OAuth 服务器将使用您的凭据和指定范围来生成 API 令牌。

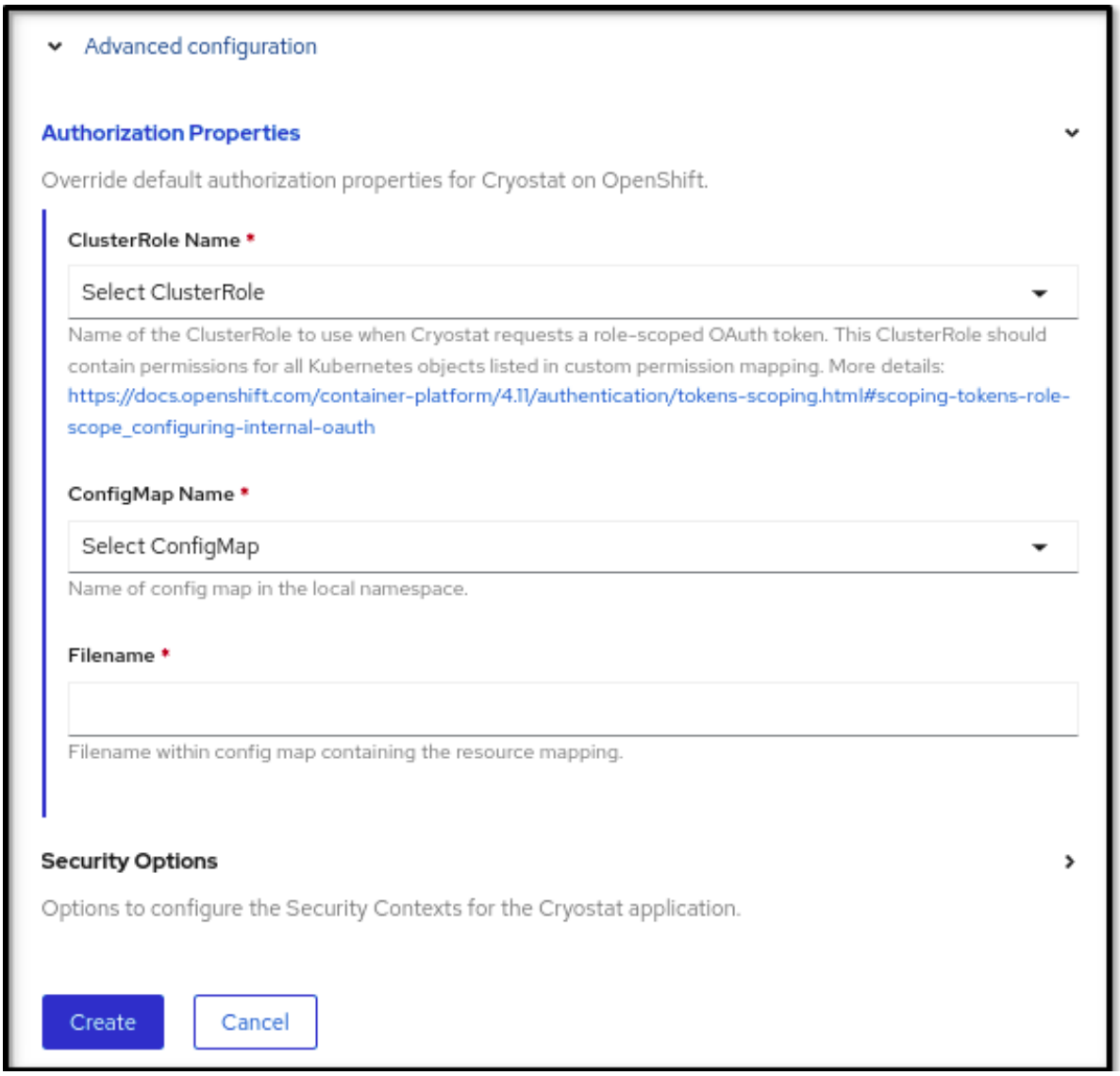
2. 在 Cryostat 自定义资源(CR)中提供 authProperties spec，以引用包含映射内容的 ConfigMap 和 ClusterRole，为映射的 OpenShift 资源定义 RBAC 访问权限。

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
```

或者，您可以打开 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 部分中访问它们。

图 3.1. OpenShift Web 控制台中的高级配置部分



验证

1. **在 Installed Operators 菜单中，选择您的 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。**

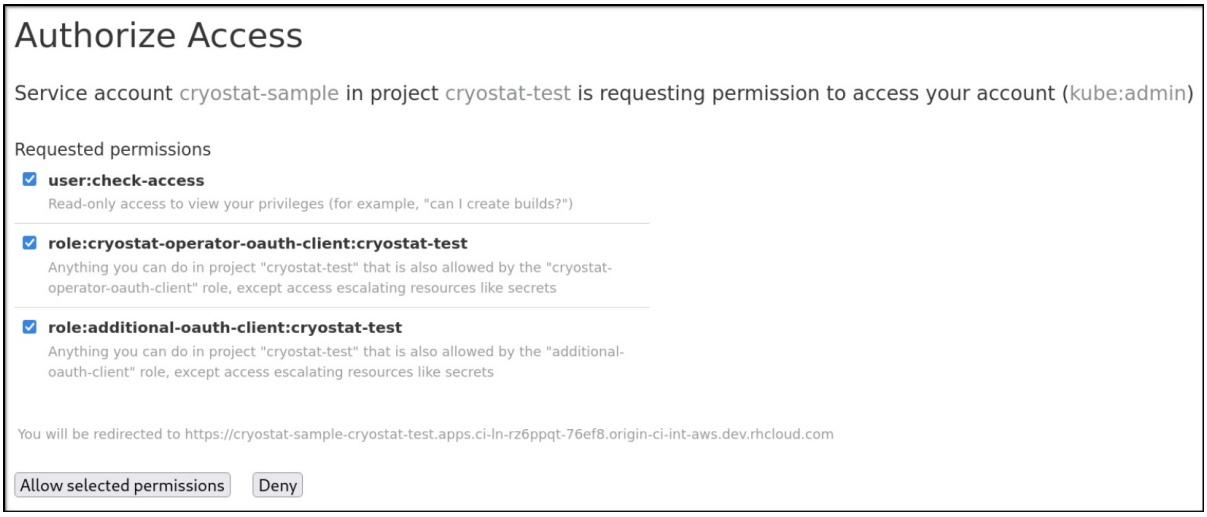
3. **输入您的凭证详情，然后点 Login。第一次通过 OAuth 服务器登录时，网页浏览器上打开一个 Authorize Access 页面。**

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。为了获得最佳 Cryostat 性能，请选中所有复选框。

图 3.2. Authorize Access 窗口列出了三个权限



Authorize Access 窗口列出以下权限：

- user:check-access，这是检查内部 Cryostat 应用请求的权限。权限为用户提供了查看其特权的只读权限。
- role:cryostat-operator-oauth-client:<namespace >，这是检查内部 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。*权限可让用户访问完成 cryostat-operator-oauth-client 角色指定的任何操作，但访问升级资源（如 secret）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。权限可让用户访问完成 additional-oauth-client 角色 指定的任何操作，除了升级对资源（如 secret）的访问外。*

6. *选择以下选项之一：*

   a. *如果要接受所选请求的权限，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 Cryostat Operator （通过 Cryostat 开始）在 OpenShift 上安装 Cryostat。*

修订于 2022-12-17 19:28:32 +1000