Red Hat build of Cryostat 3

使用 Red Hat build of Cryostat Operator 配置 Cryostat

Last Updated: 2024-07-03

法律通告

摘要

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

目录

前言

Red Hat build of Cryostat 是 JDK Flight Recorder (JFR)的容器原生虚拟化，可用于安全监控在 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 3.0 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中的 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 Red Hat OpenShift 集群上的记录，或者您可以将记录导出到外部监控应用程序，以对记录数据进行更深入分析。

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

红帽致力于替换我们的代码、文档和 Web 属性中有问题的语言。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 来管理并配置 Cryostat 实例。OpenShift Container Platform (OCP)上提供了 Red Hat build of Cryostat Operator。

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

Red Hat build of Cryostat Operator 的 Operator Capability Level 设置为 Operator Lifecycle Manager 框架上的 **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

自动升级操作仅适用于 Cryostat 的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 应用程序可以将存档记录存储在云存储磁盘上。
- 将您的 Cryostat 应用程序配置为信任来自特定应用程序的 TLS 证书。
- 禁用 cert-manager，以便 Operator 不需要为 Cryostat 组件生成自签名证书。
- 将位于 ConfigMap 中的自定义事件模板文件安装到 Cryostat 实例，以便您可以使用模板在 Cryostat 启动时创建记录。

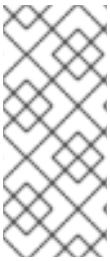
包括 Red Hat build of Cryostat Operator 的以下配置选项：

- 资源要求，可用于为核心 ,**数据源**,**grafana**,**存储**,**db**, 或 **auth-proxy** 容器指定资源请求或限值。
- **服务自定义，以便您可以控制 Red Hat build of Cryostat Operator 创建的服务。**
- **sidecar 报告选项，红帽构建的 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。**

单命名空间或多命名空间 Cryostat 实例

Red Hat build of Cryostat Operator 提供了一个 Cryostat API，您可以使用它来创建在单一命名空间

或多个命名空间中工作的 Cryostat 实例。您可以使用可从 Red Hat OpenShift Web 控制台访问的 GUI 来控制这些 Cryostat 实例。



注意

从 Cryostat 3.0 中，Cryostat API 支持创建单命名空间和多命名空间实例。在 Cryostat 2.x 版本中用于创建多命名空间实例的 Cluster Cryostat API 已被弃用，并由 Cryostat 3.x 中的 Cryostat API 替换。

可以访问多命名空间 Cryostat 实例的用户可以访问该 Cryostat 实例可见的任何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，您必须考虑为监控选择哪些命名空间、要安装 Cryostat 的命名空间，以及哪些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 能力级别 (Operator SDK)
- 请参阅使用 Operator 在 Red Hat OpenShift 上安装 Cryostat （安装 Cryostat）

1.2. 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 属性被设为 true。这意味着 Red Hat build of Cryostat Operator 使用 cert-manager CA issuer 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 组件之间启用 HTTPS 通信。

您可以将 enableCertManager 属性设置为 false，因此 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，您可以引入从未加密内部流量到包含正在运行的 Cryostat 应用程序的集群的潜在安全影响。

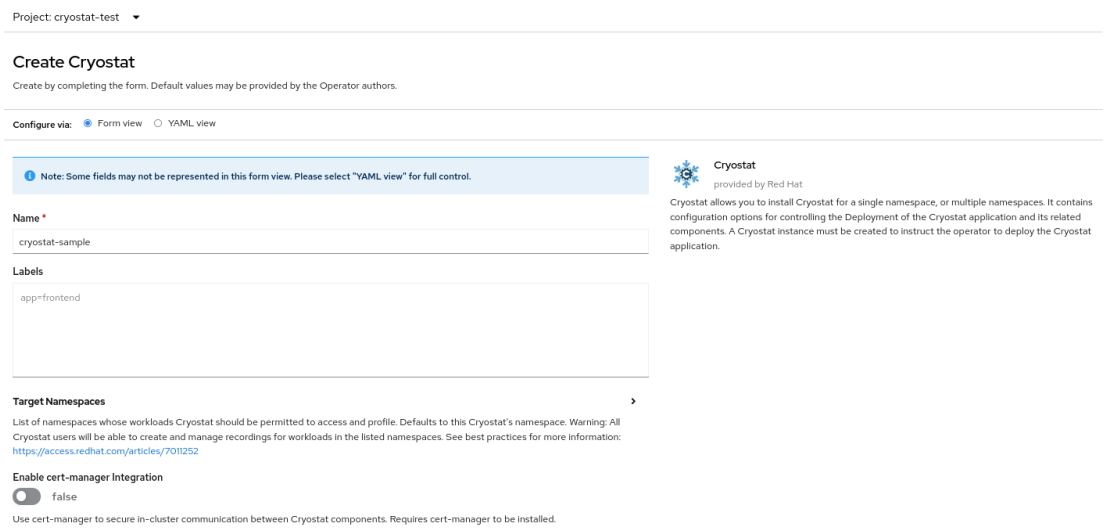
先决条件

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

流程

1. 如果要开始创建 Cryostat 实例，请执行以下步骤：
   a. 在 Red Hat OpenShift web 控制台中，点 Operators > Installed Operators。
   b. 从可用 Operator 列表中，选择 Red Hat build of Cryostat。
   c. 在 Operator 详情页中，点 Details 选项卡。
   d. 在 Provided APIs 部分中，选择 Cryostat，然后单击 Create instance。
2. 在 Create Cryostat 面板上，要配置 enableCertManager 属性，请选择以下选项之一：
   a. 如果要使用 Form 视图：
      i. 点 Form view 单选按钮。
      ii. 将 Enable cert-manager Integration 开关设置为 false，然后在 Name 字段中输入值。

图 1.1. 将 Enable cert-manager Integration 开关切换为 false



b. **如果要使用 YAML 视图：**

i. **点 YAML 视图 单选按钮。**

ii. **在 YAML 文件的 spec: 键集合中，将 enableCertManager 属性更改为 false。**

在 YAML 文件中配置的 spec: 键示例

```
--
apiVersion: operator.cryostat.io/v1beta2
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  enableCertManager: false
--
```

3. **如果要为这个 Cryostat 实例配置自定义资源(CR)中的其他属性，请参阅本文档的其它部分来了解有关这些属性的更多信息。**

4. **如果要完成创建此 Cryostat 实例，请点击 Create。**

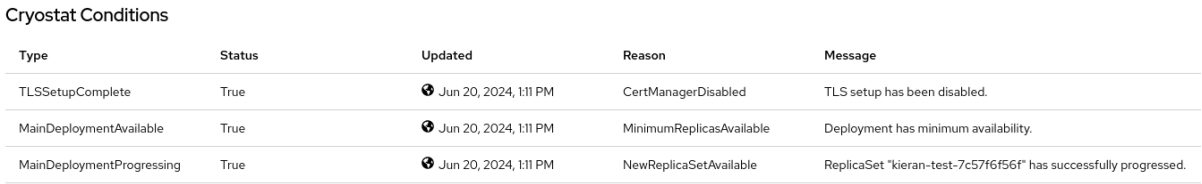
当您点 Create 时，Operator 详情页中的 Cryostat 选项卡下提供了此 Cryostat 实例。然后，您可以通过点 Operator 详情页面上的实例名称来编辑 Cryostat 实例的 CR 属性，然后从 Actions 下拉菜单中选择 Edit Cryostat。

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. 从 Operator 详情页面的 Cryostat 选项卡中选择您的 Cryostat 实例。
2. 进入 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 1.2. 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）

1.3. 自定义事件模板

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。您可以通过其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不满足您的需要，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 ConfigMap 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，您可以使用这个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，再从 Events 菜单点击 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，请使用文本编辑器或 XML 编辑器编辑下载的默认事件模板，来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. 通过在 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 资源示例

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

5. **如果要开始创建 Cryostat 实例，请执行以下步骤：**

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

   b. **从可用 Operator 列表中，选择 Red Hat build of Cryostat。**

   c. **在 Operator 详情页中，点 Details 选项卡。**

   d. **在 Provided APIs 部分中，选择 Cryostat，然后单击 Create instance。**

6. **在 Create Cryostat 面板中，要将 XML 格式的事件模板上传到资源中，请选择以下选项之一：**

   a. **如果要使用 Form 视图：**

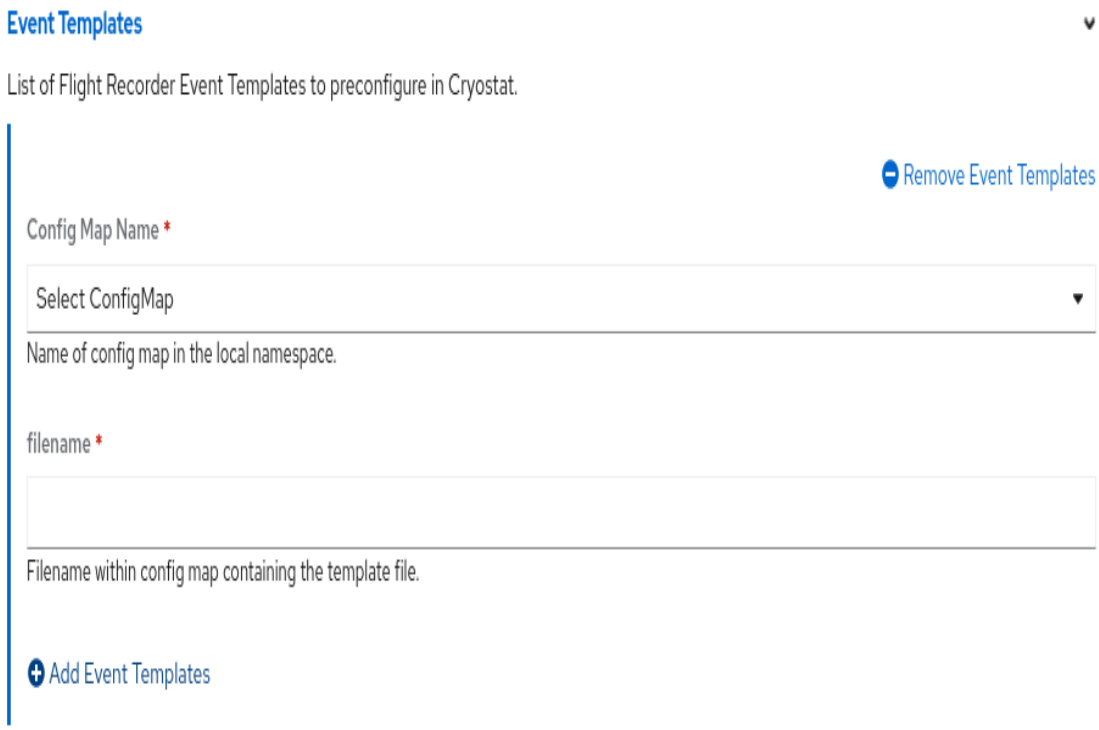
      i. **点 Form view 单选按钮。**

      ii. **导航到 Cryostat 实例的 Event Templates 部分。**

      iii. **在 Event Templates 菜单中点 Add Event Template。在 Red Hat OpenShift 控制台中打开 Event Templates 部分。**

      iv. **从 Config Map Name 下拉列表中选择包含事件模板的 ConfigMap 资源。**

图 1.3. Cryostat 实例的事件模板选项



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

b. 如果要使用 YAML 视图：

i. 点 YAML 视图 单选按钮。

ii. 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 指向您的 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示例

```
--
apiVersion: operator.cryostat.io/v1beta2
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 关联的密钥。

7. 如果要为这个 Cryostat 实例配置自定义资源(CR)中的其他属性，请参阅本文档的其它部分来了解有关这些属性的更多信息。

8. 如果要完成创建此 Cryostat 实例，请点击 Create。

当您点 Create 时，Operator 详情页中的 Cryostat 选项卡下提供了此 Cryostat 实例。然后，您可以通过点 Operator 详情页面上的实例名称来编辑 Cryostat 实例的 CR 属性，然后从 Actions 下拉菜单中选择 Edit Cryostat。

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，点菜单中的 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 选项卡下，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 1.4. Event Templates 选项卡下列出的自定义事件模板示例

Na...	Description	Prov...	Type	
Profiling	Low overhead configuration for profiling, typically around 2 % overhead.	Oracle	Target	⋮
Continuous	Low overhead configuration safe for continuous use in production environments, typically less than 1 % overhead.	Oracle	Target	⋮
Profiling	Low overhead configuration for profiling, typically around 2 % overhead.	Oracle	Custom	⋮
ALL	Enable all available events in the target JVM, with default option values. This will be very expensive and is intended primarily for testing Cryostat's own capabilities.	Cryostat	Target	⋮

其他资源

- 请参阅使用 operator 在 OpenShift 上安装 Cryostat （安装 Cryostat）
- 请参阅使用 Web 控制台（安装 Cryostat）访问Cryostat
- 请参阅使用自定义事件模板 （使用 Cryostat 管理 JFR 记录）

1.4. 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 尝试打开与使用 TLS 证书的目标 JVM 的 JMX 连接。对于成功的 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 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。
- 登录到您的 Cryostat web 控制台。

流程

1. 如果要开始创建 Cryostat 实例，请执行以下步骤：

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

b. 从可用 Operator 列表中，选择 Red Hat build of Cryostat。

c. 在 Operator 详情页中，点 Details 选项卡。

d. 在 Provided APIs 部分中，选择 Cryostat，然后单击 Create instance。

2. 在 Create Cryostat 面板上，要配置 TLS 证书，请选择以下选项之一：

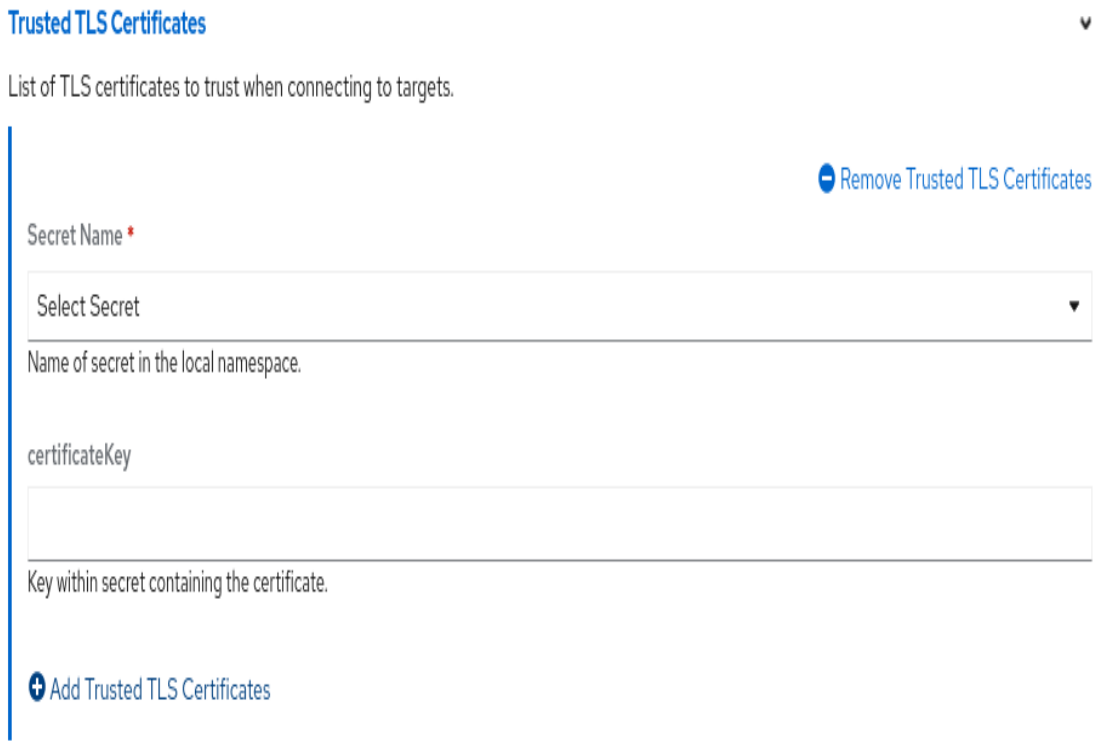
a. 如果要使用 Form 视图：

i. 点 Form view 单选按钮。

ii. 在 Name 字段中，为您要创建的 Cryostat 实例指定一个名称。

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

图 1.5. Trusted TLS 证书选项



iv. 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 Certificates 来删除 TLS 证书。

b. 如果要使用 YAML 视图：

i. 点 YAML 视图 单选按钮。

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

在 trustedCertSecrets 数组中指定 secret 的示例

```
--
apiVersion: operator.cryostat.io/v1beta2
kind: Cryostat
```

```
metadata:
  name: cryostat-sample
spec:
  trustedCertSecrets:
  - secretName: my-tls-secret
--
```

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

更改 certificateKey 属性值的示例

```
--
apiVersion: operator.cryostat.io/v1beta2
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  trustedCertSecrets:
  - secretName: my-tls-secret
    certificateKey: ca.crt
--
```

3. 如果要为这个 Cryostat 实例配置自定义资源(CR)中的其他属性，请参阅本文档的其它部分来了解有关这些属性的更多信息。

4. 如果要完成创建此 Cryostat 实例，请点击 Create。

当您点 Create 时，Operator 详情页中的 Cryostat 选项卡下提供了此 Cryostat 实例。然后，您可以通过点 Operator 详情页面上的实例名称来编辑 Cryostat 实例的 CR 属性，然后从 Actions 下拉菜单中选择 Edit Cryostat。

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，确定您的所有应用程序 pod 是否与 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 对话框窗口中，输入您的 secret 凭证，然后选择 Save 为目标 JVM 提供凭证。

注意

如果所选目标为 JMX 连接启用了密码身份验证，则当提示连接时，必须为目标 JVM 提供 JMX 凭证。

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（安装 Cryostat）访问Cryostat

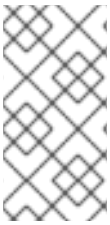
1.5. 更改存储卷选项

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 为您的 Cryostat 或 Cluster Cryostat 实例创建一个 PVC，它使用分配有 500 mebibytes (MiB)的默认 StorageClass 资源。

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：

- 在 Form view 窗口中导航到 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: key 设置中的 storageOptions 数组，以满足您的需要。



注意

您可以通过使用 *Red Hat build of Cryostat Operator* 中的更改存储卷选项 来了解更多有关创建自定义 PVC 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. 如果要开始创建 Cryostat 实例，请执行以下步骤：
   a. 在 Red Hat OpenShift web 控制台中，点 Operators > Installed Operators。

b. 从可用 Operator 列表中，选择 Red Hat build of Cryostat。

c. 在 Operator 详情页中，点 Details 选项卡。

d. 在 Provided APIs 部分中，选择 Cryostat，然后单击 Create instance。

2. 在 Create Cryostat 面板中，要更改 Cryostat 应用程序的存储设置，请选择以下选项之一：

a. 如果要使用 Form 视图：

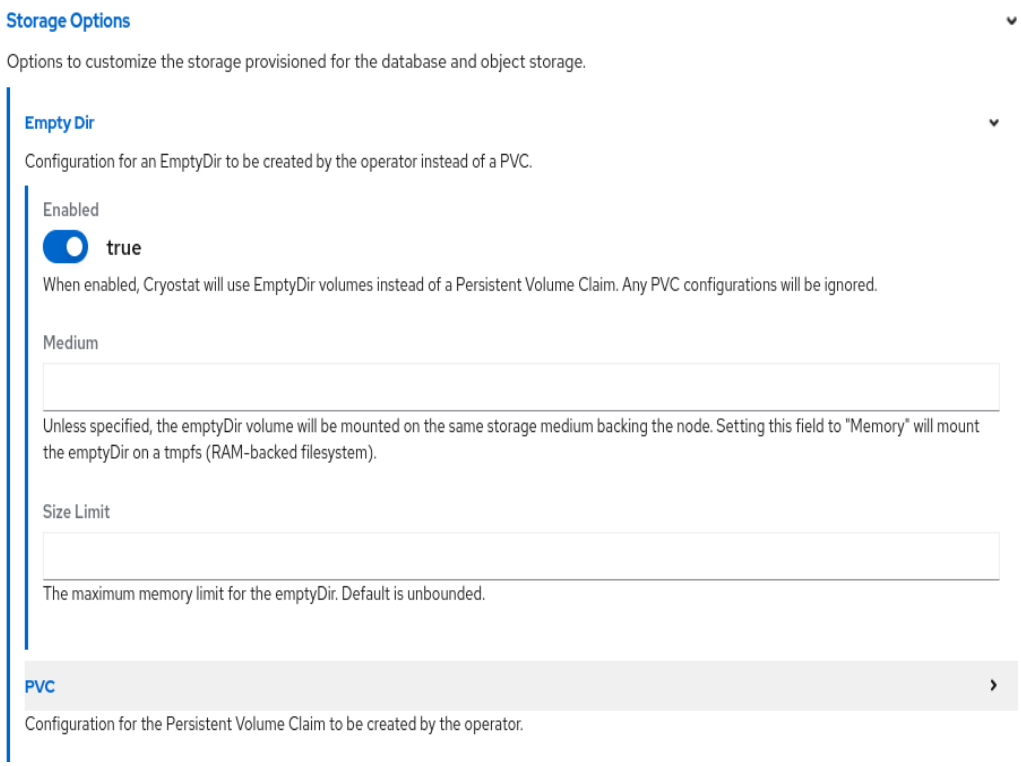
i. 点 Form view 单选按钮。

ii. 导航到 Storage Options 部分，并在 Name 字段中输入值。

iii. 展开 Storage Options，再单击 Empty Dir。在 Red Hat OpenShift Web 控制台中打开了扩展的选项选择。

iv. 将 Enabled 开关设置为 true。

图 1.6. 示例显示 Empty Dir 交换机设为 true



b. 如果要使用 YAML 视图：

i. 点 YAML 视图 单选按钮。

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

将 emptyDir 属性设置为 true的示例

```
--
apiVersion: operator.cryostat.io/v1beta2
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  storageOptions:
    emptyDir:
      enabled: true
      medium: "Memory"
      sizeLimit: 1Gi
--
```

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

3. 如果要为这个 **Cryostat** 实例配置自定义资源(CR)中的其他属性，请参阅本文档的其它部分来了解有关这些属性的更多信息。

4. 如果要完成创建此 **Cryostat** 实例，请点击 **Create**。

当您点 **Create** 时，**Operator** 详情页中的 **Cryostat** 选项卡下提供了此 **Cryostat** 实例。然后，您可以通过点 **Operator** 详情页面上的实例名称来编辑 **Cryostat** 实例的 **CR** 属性，然后从 **Actions** 下拉菜单中选择 **Edit Cryostat**。

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**。

1.6. 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** 上的 **Cryostat** 或 **Cluster 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** 属性下定义这些定义，以及报告生成器 **sidecar** 的 **spec.ReportOptions.SchedulingOptions** 属性。通过指定 **SchedulingOptions** 属性，**Cryostat** 应用程序及其报告生成器 **sidecar pod** 将调度到满足调度标准的节点。

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

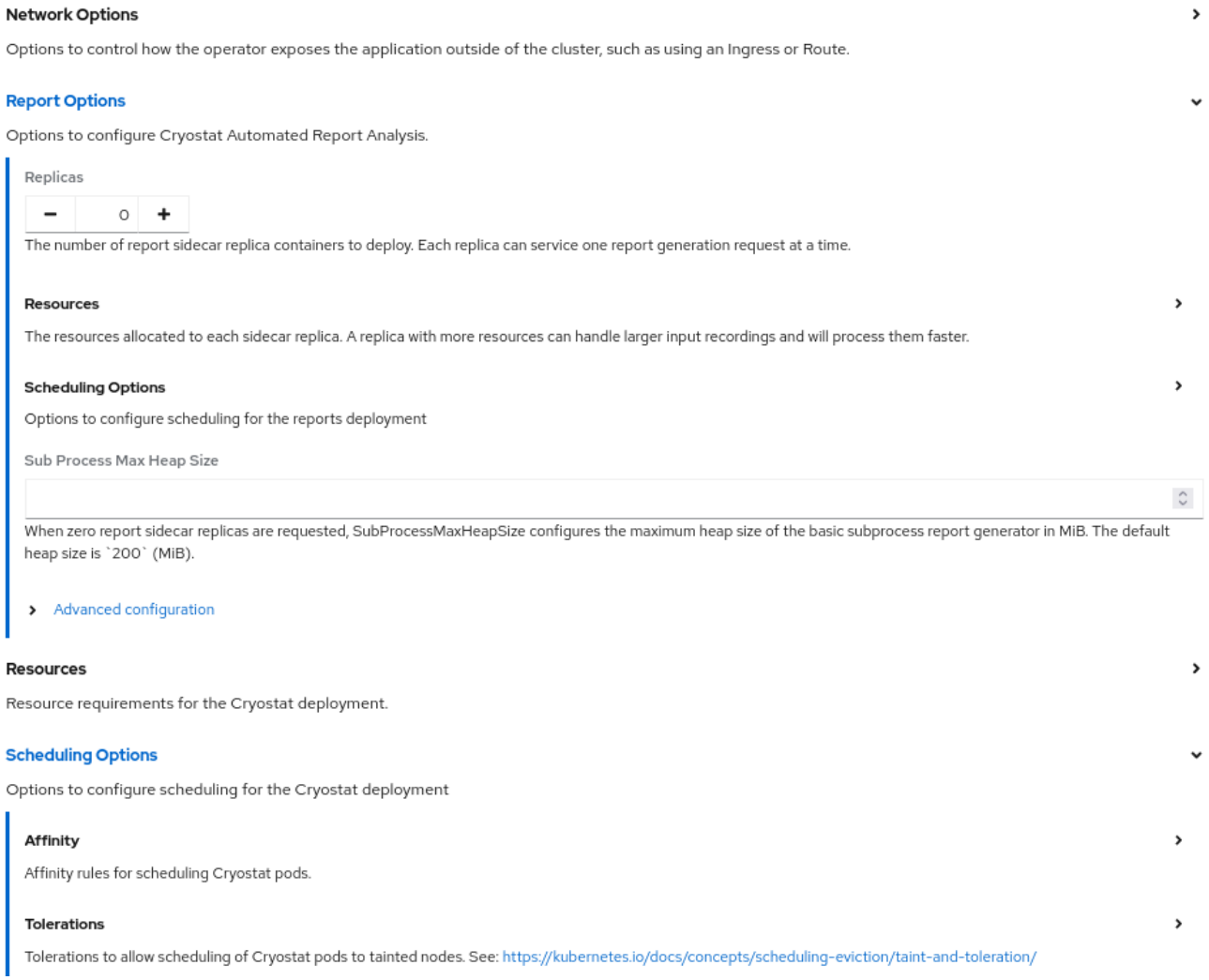
```
kind: Cryostat
apiVersion: operator.cryostat.io/v1beta2
metadata:
  name: cryostat
```

```
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 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 1.7. 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 的上下文中，这些应用程序 pod 包含一个 Cryostat pod 和 Report sidecar pod。另外，您还可以在 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 或更高版本不再支持 PodSecurityPolicy API，并使用 PSA。PSA 提供以下优点：

- 包含一个内置控制器，可为应用程序 Pod 实现 Pod 安全标准。
- 包含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，您可以使用带有安全性上下文约束(SCC)的 PSA 来为 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 可以在强制 Restricted pod 安全标准的命名空间中接受 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 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 Red Hat OpenShift 上的 Cryostat 自定义资源(CR)中指定 pod 和容器安全上下文。安全上下文将权限应用到 Cryostat pod、报告 sidecar pod （使用时）以及每个 pod 的容器。

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 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 可访问的资源。

要创建自定义 SCC，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，以便此集群内运行的任何 pod 都接收策略标准。相反，安全上下文对 pod 是唯一的。

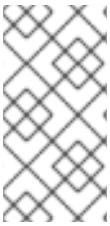
默认情况下，Red Hat build of Cryostat Operator 符合 Cryostat pod 的 restricted-v2 SCC 策略。

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、grafana、存储。数据库, 和 auth-proxy.

要启用此服务帐户使用自定义 SCC，请执行以下步骤之一：

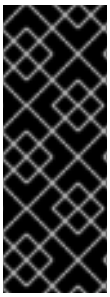
- 创建 Role Binding，将 Cryostat 服务帐户绑定到使用自定义 SCC 的角色。

- 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程序 pod 之前，请考虑以下在 Red Hat OpenShift 中可能引入的安全风险。PSA 提供三个通常满足大部分要求的 gradient 策略级别。红帽不承担与 Red Hat OpenShift pod 安全标准不匹配的安全上下文更改的任何责任。

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：* 读取新的 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 强制特定策略，您必须配置 SCC 以启用 Pod 的服务帐户来访问它。

流程

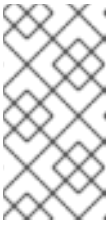
1. 如果要开始创建 Cryostat 实例，请执行以下步骤：

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

b. 从可用 Operator 列表中，选择 Red Hat build of Cryostat。

c. 在 Operator 详情页中，点 Details 选项卡。

d. 在 Provided APIs 部分中，选择 Cryostat，然后单击 Create instance。



注意

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。

2. 在 Create Cryostat 面板中，要配置安全上下文，请选择以下选项之一：

a. 如果要使用 YAML 视图：

i. 点 YAML 视图 单选按钮。

ii. 在 spec: 元素中，编辑 securityOptions 和 reportOptions 属性，以满足您的安全要求。

安全上下文配置示例

```
apiVersion: operator.cryostat.io/v1beta2
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  securityOptions:
    podSecurityContext:
      runAsNonRoot: true
      seccompProfile:
        type: RuntimeDefault
    coreSecurityContext:
```

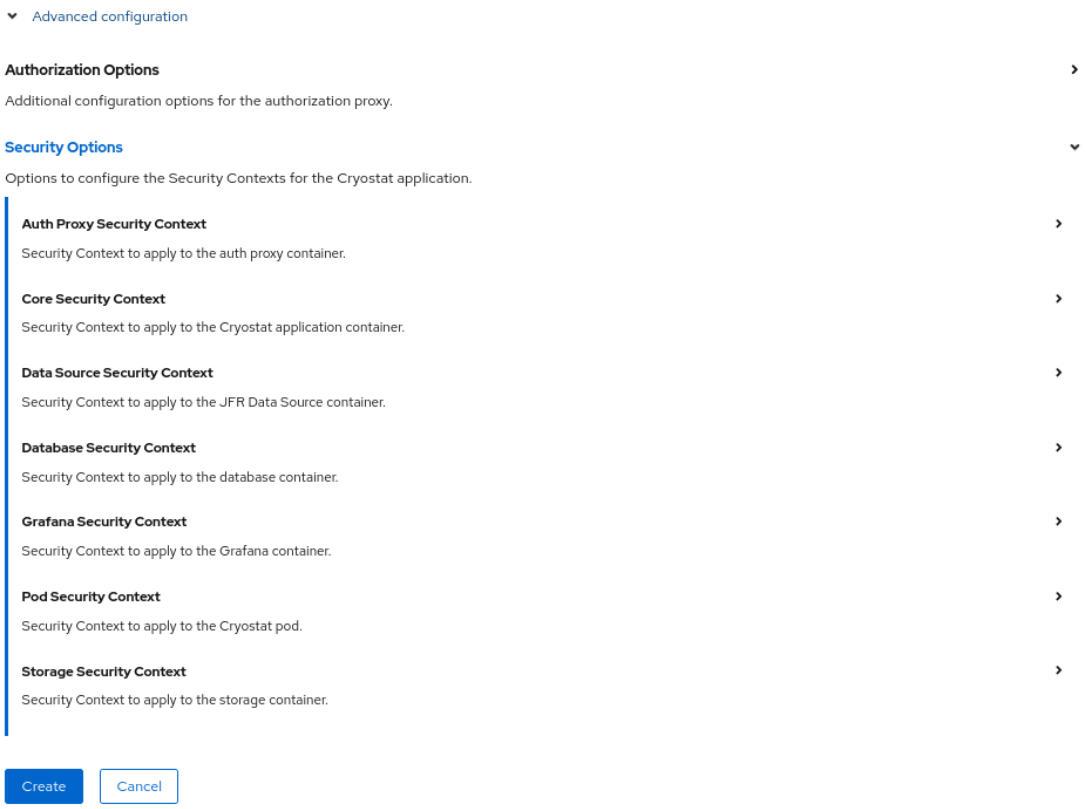
```
      allowPrivilegeEscalation: false
      capabilities:
        drop:
          - ALL
      runAsUser: 1001
    dataSourceSecurityContext:
      allowPrivilegeEscalation: false
      capabilities:
        drop:
          - ALL
    grafanaSecurityContext:
      allowPrivilegeEscalation: false
      capabilities:
        drop:
          - ALL
  reportOptions:
    replicas: 1
    podSecurityContext:
      runAsNonRoot: true
      seccompProfile:
        type: RuntimeDefault
    reportsSecurityContext:
      allowPrivilegeEscalation: false
      capabilities:
        drop:
          - ALL
      runAsUser: 1001
```

b. **如果要使用 Form 视图：**

i. **点 *Form view" 单选按钮。**

ii. **展开 Advanced configuration 以在 Red Hat OpenShift Web 控制台中打开附加选项。**

图 2.1. 高级配置菜单选项



iii. 展开 **Core Security Context**。从可用选项列表中，定义安全上下文的设置。

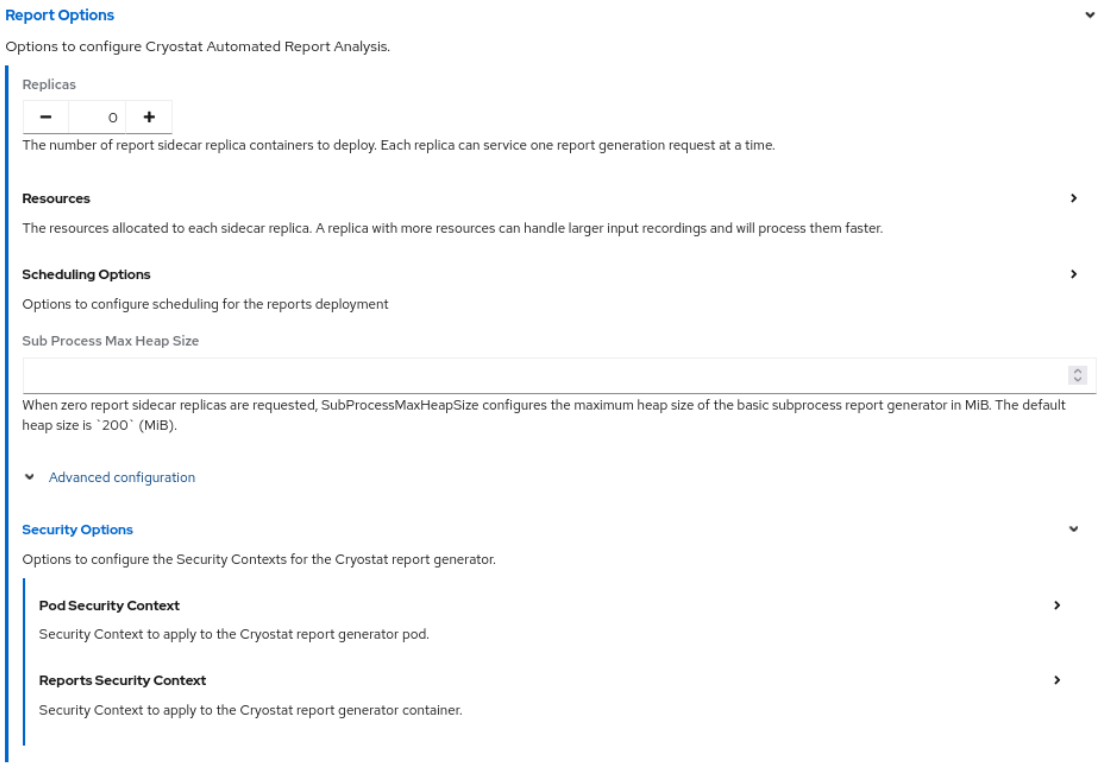
iv. 逐一扩展以下安全上下文，并根据情况定义设置：

- 身份验证代理安全上下文
- 数据源安全上下文
- 数据库安全上下文
- Grafana 安全上下文
- Pod 安全上下文
- 存储安全上下文

v.

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。在这种情况下，展开 Report Options > Advanced Configuration > Security Options。然后，根据情况扩展和定义 报告安全上下文 和 Pod 安全上下文设置。

图 2.2. 报告生成器安全上下文



3.

如果要为这个 Cryostat 实例配置自定义资源(CR)中的其他属性，请参阅本文档的其它部分来了解有关这些属性的更多信息。

4.

如果要完成创建此 Cryostat 实例，请点击 Create。

当您点 Create 时，Operator 详情页中的 Cryostat 选项卡下提供了此 Cryostat 实例。然后，您可以通过点 Operator 详情页面上的实例名称来编辑 Cryostat 实例的 CR 属性，然后从 Actions 下拉菜单中选择 Edit Cryostat。

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

了每个策略：

profile	描述
Privileged	为 Cryostat pod 提供大量权限的不受限制的策略。如果您需要向 pod 提供已知权限升级，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的值。
Restricted	为您的 Cryostat pod 提供低级权限的 **Restricted** 策略。此策略通过定义 restricted 字段和允许的值来设置控制。

第 3 章 配置 RBAC 设置

当使用 Cryostat Operator 或 Helm Chart 安装 Cryostat 3.0 时，Cryostat 在 pod 中包含反向代理 (openshift-oauth-proxy 或 oauth2_proxy)。所有对 Cryostat 的 API 请求以及 Cryostat Web 控制台或 Grafana 仪表板的所有用户都定向到此代理，该代理处理客户端会话来控制对应用程序的访问。当在 Red Hat OpenShift 上部署时，代理使用 Cryostat 安装命名空间通过与 Red Hat OpenShift 集群 SSO 供应商集成来执行对用户身份验证和授权的 RBAC 检查。

从 Cryostat 3.0 开始，Cryostat 会将相同的基于角色的访问控制(RBAC)权限检查应用到所有用户，以便允许或拒绝对产品的访问。默认情况下，Cryostat 应用程序的安装命名空间中的所需的 RBAC 角色是创建 pod/exec。任何分配了所需 RBAC 角色的 Red Hat OpenShift 用户帐户都可以完全访问 Cryostat web 控制台和所有 Cryostat 功能。如果 Red Hat OpenShift 帐户没有所需的 RBAC 角色，则此用户将阻止访问 Cryostat。

注意

您可以选择使用 htpasswd 文件配置 auth 代理，以启用基本身份验证。在 Red Hat OpenShift 中，您可以定义额外的用户帐户，这些用户帐户可以访问除 Red Hat OpenShift SSO RBAC 访问之外的 Cryostat。

当使用 Cryostat Operator 安装 Cryostat 实例时，您可以选择使用 Cryostat 自定义资源(CR)中的 .spec.authorizationOptions.openShiftSSO.accessReview 字段来自定义访问 Cryostat 所需的 Red Hat OpenShift SSO RBAC 权限。

先决条件

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

流程

1. 如果要开始创建 Cryostat 实例，请执行以下步骤：
   a. 在 Red Hat OpenShift web 控制台中，点 Operators > Installed Operators。
   b. 从可用 Operator 列表中，选择 Red Hat build of Cryostat。
   c. 在 Operator 详情页中，点 Details 选项卡。

d.

在 Provided APIs 部分中，选择 Cryostat，然后单击 Create instance。

2.

在 Create Cryostat 面板上，要自定义对 Cryostat 的所有客户端访问所需的 SubjectAccessReview 或 TokenAccessReview，请选择以下选项之一：

a.

如果使用 Form 视图：

i.

点 Form view 单选按钮。

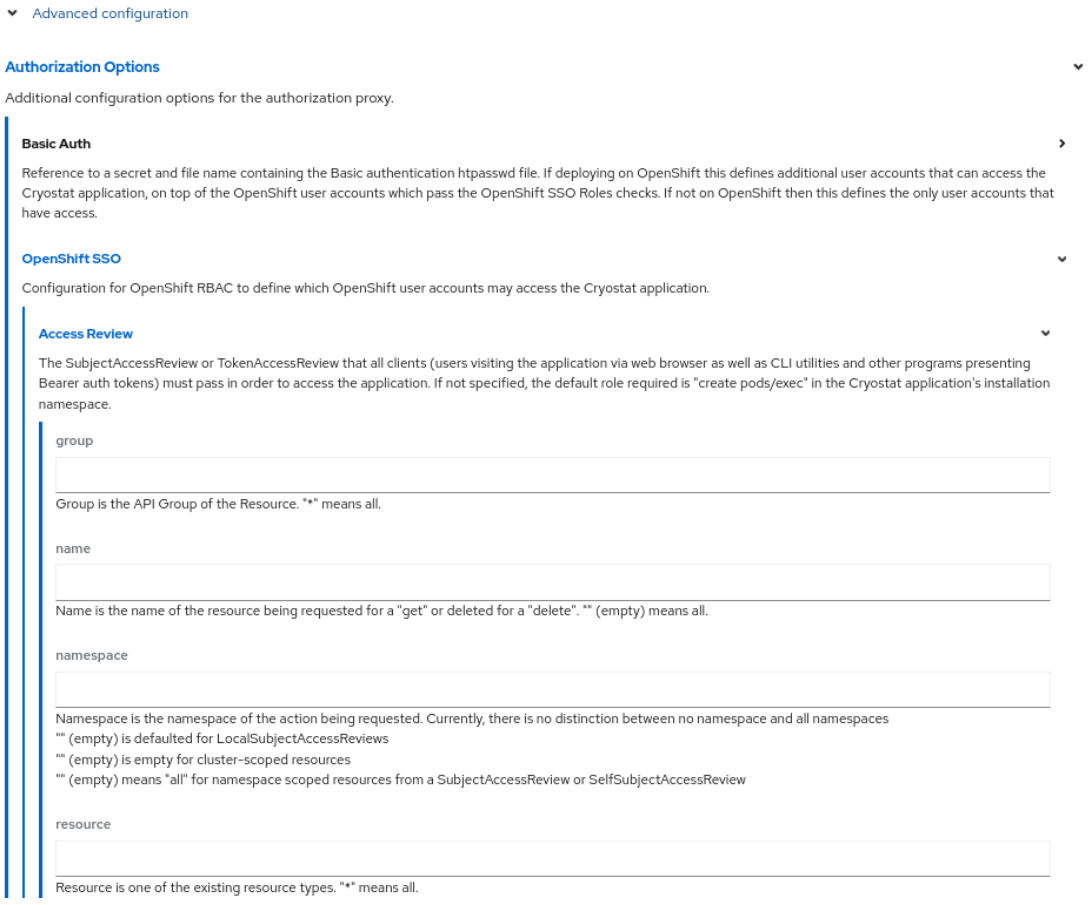
ii.

要打开附加选项，请展开 Advanced Configuration 以打开附加选项。

iii.

展开 Cryostat CR 的 Authorization Options > OpenShift SSO > Access Review 部分。

图 3.1. 访问 Cryostat 实例的查看属性



iv.

使用以下字段指定访问 Cryostat 所需的自定义 RBAC 设置：

字段	详情
group	资源的 API 组。 wilcard 星号(*)值表示所有组。
name	为 **get** 或删除请求的资源的名称，用于删除。 **空值表示所有名称。**
namespace	要请求的操作的命名空间。 目前，没有命名空间和所有命名空间之间没有区别。请考虑以下指南： ● 对于 LocalSubjectAccessReviews，默认为一个空值。 ● 空值代表没有集群范围的资源。 ● 空值代表来自 SubjectAccessReview 或 SelfSubjectAccessReview 的所有命名空间范围的资源。
resource	现有资源类型。 通配符星号(*)值表示所有资源类型。
subresource	现有资源类型。 空值代表没有资源类型。
verb	Kubernetes 资源 API 动词（例如：**get**,**list**,**watch**,**create**,**update**,**delete**,**proxy**）。 通配符星号(*)值表示所有操作动词。
version	资源的 API 版本。 通配符星号(*)值表示所有版本。

b. **如果使用 YAML 视图：**

i. **点 YAML 视图 单选按钮。**

ii. 在 spec: 元素中，编辑 authorizationOptions:OpenShiftSSO 属性以匹配您的 RBAC 权限要求。

RBAC 权限配置示例

```
apiVersion: operator.cryostat.io/v1beta2
kind: Cryostat
metadata:
  name: cryostat-sample
  namespace: cryostat-test
spec:
  ...
  authorizationOptions:
    openShiftSSO:
      accessReview:
        group: <API group of resource>
        name: <Name of resource being requested or deleted>
        namespace: <Namespace of action being requested>
        resource: <An existing resource type>
        subresource: <An existig resource type>
        verb: <A Kubernetes resource API verb>
        version: <API version of resource>
  ...
```

3. 如果要为这个 Cryostat 实例配置自定义资源(CR)中的其他属性，请参阅本文档的其它部分来了解有关这些属性的更多信息。

4. 如果要完成创建此 Cryostat 实例，请点击 Create。

当您点 Create 时，Operator 详情页中的 Cryostat 选项卡下提供了此 Cryostat 实例。然后，您可以通过点 Operator 详情页面上的实例名称来编辑 Cryostat 实例的 CR 属性，然后从 Actions 下拉菜单中选择 Edit Cryostat。

更新于 2024-07-02