Red Hat build of Cryostat 2

Red Hat build of Cryostat Operator を使用した Cryostat の設定

Last Updated: 2024-05-02

Red Hat build of Cryostat 2 Red Hat build of Cryostat Operator を使用した Cryostat の設定

法律上の通知

概要

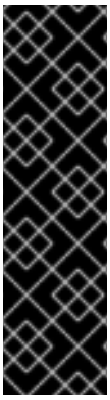
Red Hat build of Cryostat は、OpenShift Container Platform で提供される Red Hat 製品です。Red Hat build of Cryostat Operator を使用して Cryostat を設定する を使用して、Red Hat build of Cryostat Operator を使用して Cryostat を設定するを確認してください。

目次

はじめに

Red Hat build of Cryostat は、JDK Flight Recorder (JFR) のコンテナーネイティブ実装です。これを使用すると、OpenShift Container Platform クラスターで実行されるワークロードで Java 仮想マシン (JVM) のパフォーマンスを安全にモニターできます。Cryostat 2.4 を使用すると、Web コンソールまたは HTTP API を使用して、コンテナー化されたアプリケーション内の JVM の JFR データを起動、停止、取得、アーカイブ、インポート、およびエクスポートできます。

ユースケースに応じて、Cryostat が提供するビルトインツールを使用して、Red Hat OpenShift クラスターに直接レコーディングを保存して分析したり、外部のモニタリングアプリケーションにレコーディングをエクスポートして、レコーディングしたデータをより詳細に分析したりできます。



重要

Red Hat build of Cryostat は、テクノロジープレビュー機能のみです。テクノロジープレビュー機能は、Red Hat 製品のサービスレベルアグリーメント (SLA) の対象外であり、機能的に完全ではないことがあります。Red Hat は、実稼働環境でこれらを使用することを推奨していません。テクノロジープレビュー機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行いフィードバックを提供していただくことを目的としています。

Red Hat のテクノロジープレビュー機能のサポート範囲に関する詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

第1章 RED HAT BUILD OF CRYOSTAT OPERATOR

Red Hat build of Cryostat Operator を使用して、Cryostat インスタンスを管理および設定できます。Red Hat build of Cryostat Operator は OpenShift Container Platform (OCP) で利用できます。

1.1. RED HAT BUILD OF CRYOSTAT OPERATOR の概要

OpenShift Container Platform で Cryostat アプリケーションを作成または更新した後、Red Hat build of Cryostat Operator は Cryostat アプリケーションを作成および管理します。

Operator レベルの 2 つのシームレスアップグレード

Cryostat 2.2 以降、Red Hat build of Cryostat Operator の Operator Capability Level は、Operator Lifecycle Manager フレームワークで **Level 2 Seamless Upgrades** に設定されます。Red Hat build of Cryostat Operator をアップグレードすると、Red Hat build of Cryostat Operator は Cryostat とその関連コンポーネントを自動的にアップグレードします。自動アップグレード操作では、JFR 記録、テンプレート、ルール、およびその他の格納されたコンポーネントを Cryostat インスタンスから削除することはありません。

注記

自動アップグレード操作は、 Cryostat のマイナーリリースまたはパッチ更新リリースに対してのみ発生します。メジャーリリースの場合は、Red Hat build of Cryostat Operator を再インストールする必要がある場合があります。

永続ボリューム要求

Red Hat build of Cryostat Operator を使用して Red Hat OpenShift で永続ボリュームクレーム (PVC) を作成できるため、Cryostat アプリケーションはアーカイブされたレコーディングをクラウドストレージディスクに保存できます。

Operator 設定

さらに、Red Hat build of Cryostat Operator のデフォルト設定に次の変更を加えることができます。

- Red Hat build of Cryostat Operator によって作成された PVC を設定して、Cryostat アプリケーションがアーカイブされたレコーディングをクラウドストレージディスクに保存できるようにします。
- 特定のアプリケーションからの TLS 証明書を信頼するように Cryostat アプリケーションを設定します。
- Cryostat を最小限のデプロイメントとしてデプロイし、Operator が Cryostat アプリケーションをデプロイするために必要なリソースを少なくします。
- cert-manager を無効にして、Operator が Cryostat コンポーネントの自己署名証明書を生成する必要がないようにします。
- ConfigMaps にあるカスタムイベントテンプレートファイルを Cryostat インスタンスにインストールして、Cryostat の起動時にテンプレートを使用してレコーディングを作成できるようにします。

Cryostat 2.2 以降、Red Hat build of Cryostat Operator の次の設定オプションが含まれています。

- リソース要件。**core**、**datasource**、または **grafana** コンテナーのリソースリクエストまたは制限を指定するために使用できます。

- サービスのカスタマイズ。Cryostat Operator の Red Hat ビルドが作成するサービスを制御できます。
- サイドカーレポートオプション。Red Hat build of Cryostat Operator が Cryostat アプリケーション用に 1 つ以上のレポートジェネレーターをプロビジョニングするために使用できます。

シングル namespace またはマルチ namespace の Cryostat インスタンス

Red Hat build of Cryostat Operator は、**Cryostat** API と **Cluster Cryostat** API の両方を提供します。**Cryostat** API を使用して、単一の namespace で動作する Cryostat インスタンスを作成できます。**Cluster Cryostat** API を使用して、複数の namespace で機能する Cryostat インスタンスを作成できます。これらの Cryostat インスタンスは、Red Hat OpenShift Web コンソールからアクセスできる GUI を使用して制御できます。

マルチ namespace の Cryostat インスタンスにアクセスできるユーザーは、その Cryostat インスタンスに認識される namespace 内のすべてのターゲットアプリケーションにアクセスできます。したがって、マルチ namespace の Cryostat インスタンスをデプロイする場合は、監視対象にどの namespace を選択するか、Cryostat をどの namespace にインストールするか、およびどのユーザーにアクセスを許可するかを考慮する必要があります。

Red Hat build of Cryostat Operator を設定するための前提条件

Red Hat build of Cryostat Operator を設定する前に、以下の前提条件を満たしていることを確認してください。

- Red Hat build of Cryostat Operator を Red Hat OpenShift のプロジェクトにインストールしている。
- Red Hat build of Cryostat Operator を使用して Cryostat インスタンスを作成している。

関連情報

- Operator Capability Levels (Operator SDK) を参照してください。
- Operator を使用して Red Hat OpenShift に Cryostat をインストールする (Cryostat のインストール) を参照してください。

1.2. サポートコンテナーの除外

Cryostat アプリケーションでデプロイするサポートアプリケーションを除外できます。サポートアプリケーションは、Cryostat Pod にリストされているサポートコンテナーです。サポートするコンテナーを除外すると、Cryostat アプリケーションのデプロイに必要なシステムリソースが少なくなります。

デフォルトでは、Cryostat はプロジェクトの Red Hat build of Cryostat Operator YAML 設定ファイルの **minimal** プロパティーを **false** に設定します。この設定では、Red Hat build of Cryostat Operator は、Cryostat アプリケーションと同じ Pod に含まれている **jfr-datasource** や Grafana ダッシュボードなどのすべての標準サポートアプリケーションを使用して Cryostat アプリケーションをデプロイします。これらのサポートアプリケーションは、Cryostat データと対話し、このようなデータを操作するための機能を追加で提供します。

Red Hat build of Cryostat Operator はデフォルトで以下の設定になります。

- 事前設定された Grafana アプリケーションをデプロイします。
- JDK Flight Recorder (JFR) データを Grafana の読み取り可能な形式である JSON に変換するための **jfr-datasource** アプリケーションをデプロイします。

- Cryostat をデプロイするときに Grafana で事前設定されたダッシュボード JSON ファイルが含まれています。

minimal プロパティーを **true** に設定すると、Red Hat build of Cryostat Operator は、最小デプロイメントとして Cryostat インスタンスを自動的に再起動します。つまり、Operator は Cryostat コンテナーにリストされているアプリケーションのみをデプロイし、Cryostat アプリケーションと同じ Pod に含まれている **jfr-datasource** や Grafana ダッシュボードなどの標準のサポートアプリケーションを無視します。

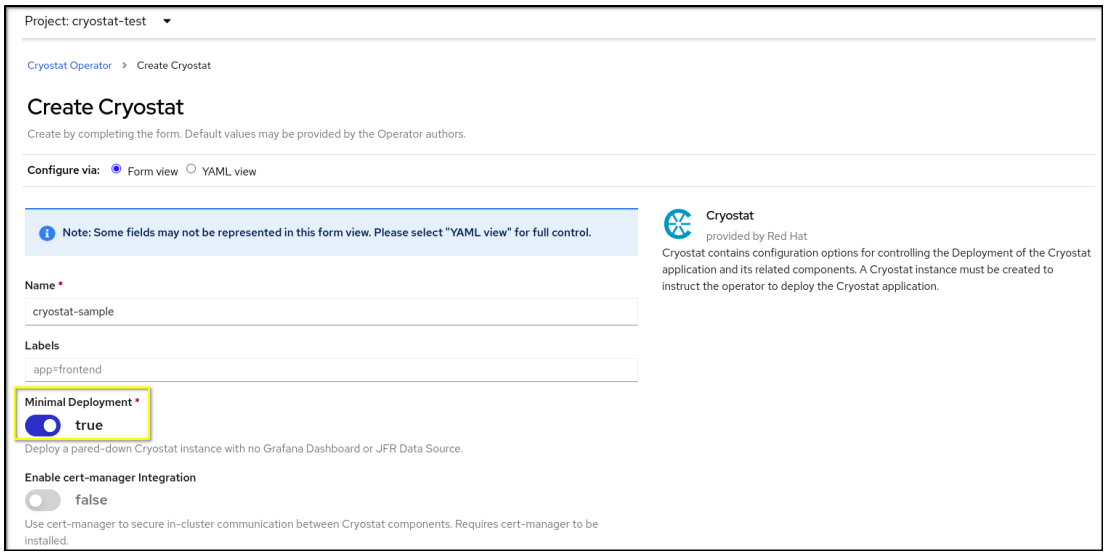
前提条件

- Red Hat OpenShift Web コンソールを使用して OpenShift Container Platform にログインしている。

手順

1. Red Hat OpenShift Web コンソールで、**Operators** > **Installed Operators**の順にクリックします。
2. 使用可能な Operator のリストから、Red Hat build of Cryostat を選択します。
3. **Details** タブをクリックします。
4. **Provided APIs** セクションで、**Cryostat** および **Cluster Cryostat** カスタムリソース (CR) が利用可能です。以下のオプションのいずれかを選択します。
   - 単一 namespace の Cryostat インスタンスを作成するには、Cryostat を選択してから **Create instance** をクリックします。
   - 複数 namespace の Cryostat インスタンスを作成するには、**Cluster Cryostat** を選択してから **Create instance** をクリックします。
5. **minimal** プロパティーを設定するには、次のいずれかのオプションを選択します。
   a. **Form view** ラジオボタンをクリックします。
      i. **Minimal Deployment** スイッチを **true** に設定します。**Name** フィールドにも値を入力する必要があります。

図1.1 Minimal Deployment スイッチを true に切り替える



ii. **Create** をクリックします。作成したインスタンスのタイプに応じて、インスタンスは以下のいずれかのタブで開きます。

- 単一 namespace の Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cryostat** タブで利用できます。
- Cluster Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cluster Cryostat** タブで利用できます。

b. **YAML view** のラジオボタンをクリックします。

i. **spec:** キーセットの **minimum** プロパティーの値を **true** に変更します。

最小プロパティーの設定例

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

ii. **Save** をクリックします。

検証

1. Red Hat OpenShift Web コンソールから、Cryostat インスタンスを作成したプロジェクト、または Cluster Cryostat インスタンスの **Install Namespace** として選択したプロジェクトを選択します。
2. **Workloads → Deployments** に移動します。
3. デプロイメントの一覧から、Cryostat または Cluster Cryostat インスタンスの名前に一致するデプロイメントを選択します。Web コンソールで **デプロイメントの詳細** ページが開きます。
4. **Containers** セクションに移動します。リストされている単一のコンテナーは、Red Hat build of Cryostat Operator が Cryostat アプリケーションを最小限のデプロイメントとしてデプロイしたことを示します。

関連情報

- OpenShift CLI の詳細は、OpenShift CLI の使用を開始する (Red Hat OpenShift ドキュメント) を参照してください。
- JDK Flight Recorder (JFR) レコーディングの作成 (Cryostat を使用した JFR レコーディングの作成) を参照してください。

1.3. CERT-MANAGER の無効化

Red Hat build of Cryostat Operator の **enableCertManager** プロパティーを設定することにより、cert-manager 機能を無効にできます。

デフォルトでは、Red Hat build of Cryostat Operatorの **enableCertManager** プロパティーは **true** に設

定されています。この設定では、Red Hat build of Cryostat Operator が cert-manager **CA** 発行者を使用して、Cryostat コンポーネントの自己署名証明書が生成されます。Red Hat build of Cryostat Operator は、これらの証明書を使用して、クラスターで動作する Cryostat コンポーネント間の HTTPS 通信を有効にします。

enableCertManager プロパティーを **false** に設定すると、Red Hat build of Cryostat Operator が Cryostat コンポーネントの自己署名証明書を生成する必要がなくなります。

重要

enableCertManager プロパティーを **false** に設定すると、暗号化されていない内部トラフィックから、実行中の Cryostat アプリケーションを含むクラスターに潜在的なセキュリティー上の影響が生じる可能性があります。

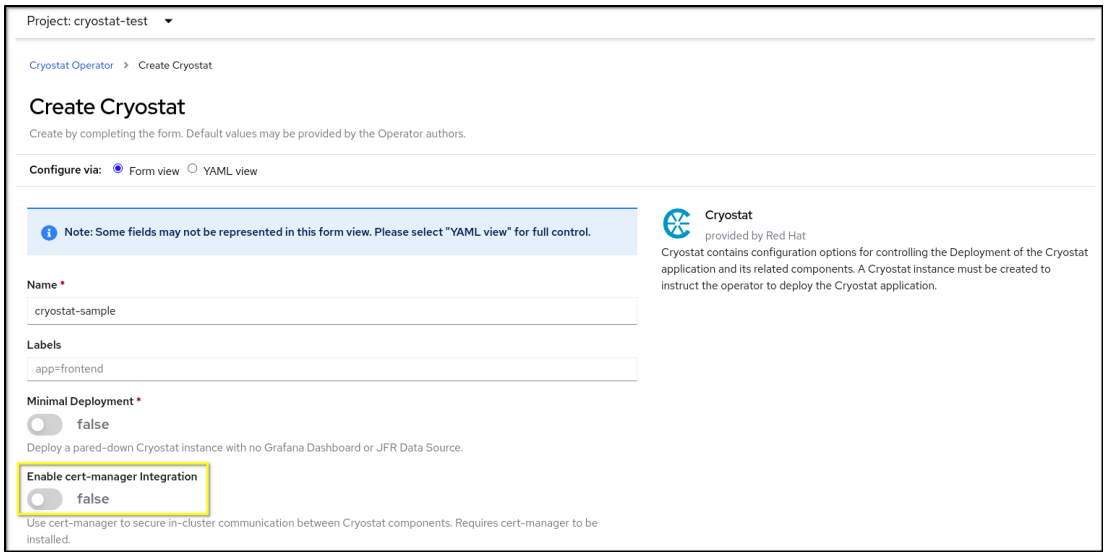
前提条件

- Red Hat OpenShift Web コンソールを使用して OpenShift Container Platform にログインしている。

手順

1. OpenShift Web コンソールで **Operators > Installed Operators** に移動します。
2. 使用可能な Operator のリストから、Red Hat build of Cryostat を選択します。
3. **Details** タブをクリックします。
4. **Provided APIs** セクションで、**Cryostat** および **Cluster Cryostat** カスタムリソース (CR) が利用可能です。以下のオプションのいずれかを選択します。
   - 単一 namespace の Cryostat インスタンスを作成するには、Cryostat を選択してから **Create instance** をクリックします。
   - 複数 namespace の Cryostat インスタンスを作成するには、**Cluster Cryostat** を選択してから **Create instance** をクリックします。
5. **enableCertManager** プロパティーを設定するには、次のいずれかのオプションを選択します。
   a. **Form view** ラジオボタンをクリックします。
      i. **Enable cert-manager Integration** を有効にするスイッチを **false** に設定し、**Name** フィールドに値を入力します。

図1.2 Enable cert-manager Integration スイッチを false に切り替える



ii. **Create** をクリックします。作成したインスタンスのタイプに応じて、インスタンスは以下のいずれかのタブで開きます。

- 単一 namespace の Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cryostat** タブで利用できます。
- Cluster Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cluster Cryostat** タブで利用できます。

b. **YAML view** のラジオボタンをクリックします。

i. YAML ファイルの **spec:** キーセットで、**enableCertManager** プロパティーを **false** に変更します。

YAML ファイルへの spec: キーセット設定例

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

ii. **Save** ボタンをクリックします。
Red Hat build of Cryostat Operator は、Cryostat アプリケーションを自動的に再起動し、更新された **enableCertManager** プロパティー設定でアプリケーションを実行できるようにします。

検証

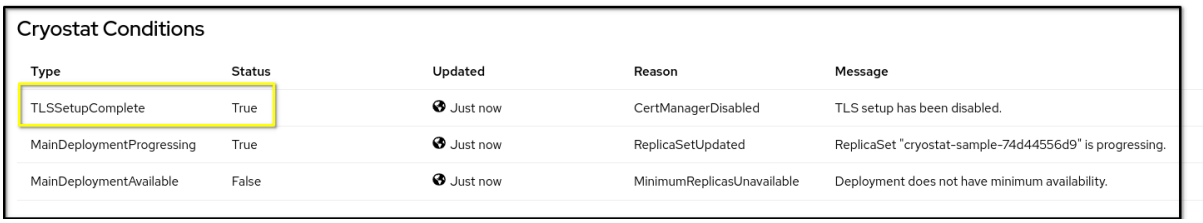
1. Cryostat または Cluster Cryostat インスタンスを選択します。

- Cryostat インスタンスを作成した場合は、**Operator details** ページの **Cryostat** タブから Cryostat インスタンスを選択します。

- Cluster Cryostat インスタンスを作成した場合は、**Operator details** ページの **Cluster Cryostat** タブからCluster Cryostat インスタンスを選択します。

2. **Cryostat Conditions** テーブルに移動します。
3. **TLSSetupComplete** 条件が **true** に設定されていること、およびこの条件の **Reason** 列が **CertManagerDisabled** に設定されていることを確認します。これは、**enableCertManager** プロパティーを **false** に設定したことを示します。

図1.3 TLSSetupComplete 条件が true に設定されていることを示す例



関連情報

- cert-manager ドキュメントを参照してください
- JDK Flight Recorder (JFR) レコーディングの作成 (Cryostat を使用した JFR レコーディングの作成) を参照してください。

1.4. イベントテンプレートのカスタマイズ

Cryostat 2 では、Red Hat build of Cryostat Operator YAML 設定ファイルの **eventTemplates** プロパティーを設定して、複数のカスタムテンプレートを含めることができます。イベントテンプレートは、JDK Flight Recording (JFR) のイベントレコーディング基準の概要を示しています。関連するイベントテンプレートを使用して JFR を設定できます。

デフォルトでは、Red Hat build of Cryostat Operator には事前設定されたイベントテンプレートが含まれています。これらの事前設定されたイベントテンプレートでは要件に対応しない可能性があるため、Red Hat build of Cryostat Operator を使用して Cryostat インスタンスのカスタムイベントテンプレートを生成し、これらのテンプレートを ConfigMaps に保存して簡単に取得できるようにします。次の方法でカスタムイベントテンプレートを生成できます。

- Red Hat OpenShift Web コンソールを使用して、イベントテンプレートをカスタムリソースにアップロードします。
- Red Hat OpenShift Web コンソールで Cryostat カスタムリソースの YAML ファイルを編集します。

カスタムイベントテンプレートを **ConfigMap** に保存した後、このカスタムイベントテンプレートを使用して新しい Cryostat インスタンスをデプロイできます。次に、JFR でカスタムイベントテンプレートを使用して、ニーズを満たすように Java アプリケーションを監視できます。

前提条件

- Red Hat OpenShift Web コンソールを使用して OpenShift Container Platform にログインしている。
- Cryostat Web コンソールにログインしている。

手順

1. デフォルトのイベントテンプレートをダウンロードするには、Cryostat Web コンソールに移動し、**Events** メニューから **Downloads** をクリックします。

注記

イベントテンプレートは XML 形式で、ファイル名拡張子は **.jfc** です。

2. **オプション:** カスタムイベントテンプレートが必要な場合は、テキストエディターまたは XML エディターを使用して、ダウンロードしたデフォルトのイベントテンプレートを編集し、ニーズに合わせてテンプレートを設定します。

3. CLI で **oc login** コマンドを入力して、Red Hat OpenShift Web コンソールにログインします。

4. CLI で次のコマンドを入力して、イベントテンプレートから **ConfigMap** リソースを作成します。Cryostat アプリケーションをデプロイするパスでコマンドを実行する必要があります。このリソースを使用して、Cryostat インスタンスを実行するクラスター内にあるイベントテンプレートファイルを保存できます。

CLI を使用して ConfigMap リソースを作成する例

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

5. Red Hat OpenShift Web コンソールで、**Operators** > **Installed Operators**の順にクリックします。

6. 使用可能な Operator のリストから、Red Hat build of Cryostat を選択します。

7. **Operator details** ページの **Details** タブで、Cryostat または Cluster Cryostat インスタンスを作成します。

   a. **Provided APIs** セクションで、**Cryostat** および **Cluster Cryostat** カスタムリソース (CR) が利用可能です。以下のオプションのいずれかを選択します。

      - 単一 namespace の Cryostat インスタンスを作成するには、Cryostat を選択してから **Create instance** をクリックします。

      - 複数 namespace の Cryostat インスタンスを作成するには、**Cluster Cryostat** を選択してから **Create instance** をクリックします。

8. 次のいずれかのオプションを選択して、XML 形式のイベントテンプレートをリソースにアップロードします。

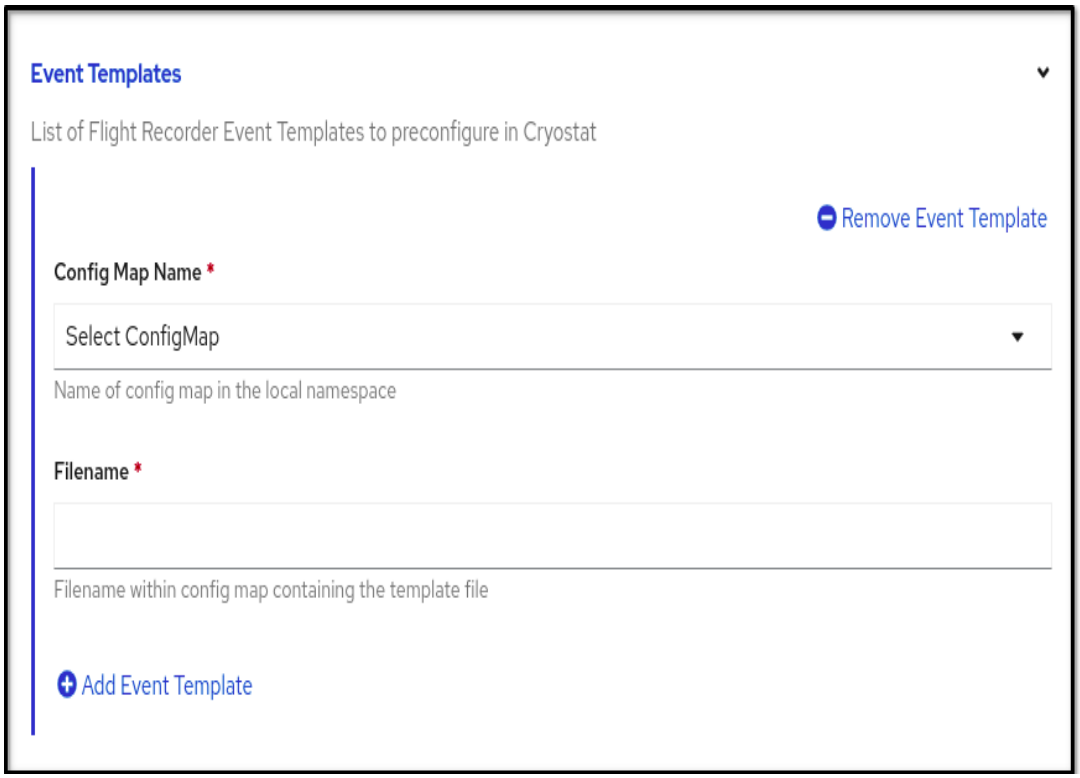
   a. **Form view** ラジオボタンをクリックします。

      i. Cryostat または Cluster Cryostat インスタンスの **Event Templates** セクションに移動します。

      ii. **Event Templates** メニューから、**Add Event Template** をクリックします。Red Hat OpenShift コンソールで **Event Templates** セクションが開きます。

      iii. **Config Map Name** ドロップダウンリストから、イベントテンプレートを含む ConfigMap リソースを選択します。

図1.4 Cryostat インスタンスのイベントテンプレートオプション



iv. **Filename** フィールドに、ConfigMap に含まれている **.jfc** ファイルの名前を入力します。

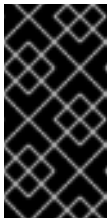
v. カスタムイベントテンプレートを使用して Cryostat または Cluster Cryostat インスタンスを生成するには、**Create** をクリックします。

b. **YAML view** のラジオボタンをクリックします。

i. **eventTemplates** プロパティーにカスタムイベントテンプレートを指定します。このプロパティーは、Red Hat build of Cryostat Operator が ConfigMap を指すようにし、Red Hat build of Cryostat Operator がイベントテンプレートを読み取れるようにします。

eventTemplates プロパティーにカスタムイベントテンプレートを指定する例

```
--
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

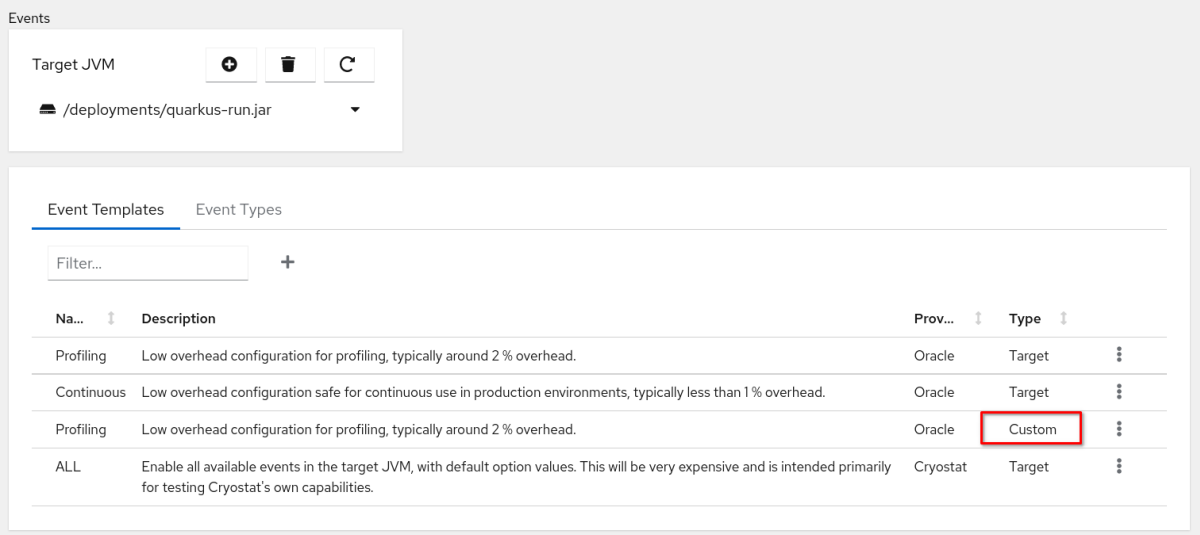
configMapName ドロップダウンリストから、Cryostat または Cluster Cryostat インスタンスに関連付けられている ConfigMap の名前を選択する必要があります。さらに、**filename** フィールドに ConfigMap に関連付けられたキーを指定する必要があります。

Red Hat build of Cryostat Operator は、カスタムイベントテンプレートを XML ファイルとして Cryostat アプリケーションに提供できるようになりました。Cryostat Web コンソールで、カスタムイベントテンプレートがデフォルトイベントテンプレートと一緒に開きます。

検証

1. Cryostat Web コンソールで、メニューから **Events** をクリックします。Web コンソールで **Authentication Required** ウィンドウが開いた場合は、認証情報を入力して **Save** をクリックします。
2. **Event Templates** タブで、使用可能なイベントテンプレートのリストにカスタムイベントテンプレートが表示されるかどうかを確認します。

図1.5 Event Templates タブにリストされているカスタムイベントテンプレートの例



関連情報

- Operator を使用して OpenShift に Cryostat をインストールする (Cryostat のインストール) を参照してください。
- Web コンソールを使用した Cryostat へのアクセス (Cryostat のインストール) を参照してください。
- カスタムイベントテンプレートの使用 (Cryostat を使用した JFR 記録の管理) を参照してください。

1.5. TLS 証明書の設定

Red Hat build of Cryostat Operator を指定して、特定のアプリケーションからの TLS 証明書を信頼するように Cryostat を設定できます。

Cryostat は、TLS 証明書を使用するターゲット JVM への JMX 接続を開くことを試みます。成功した JMX 接続では、Cryostat は、ターゲット JVM 証明書に認証チェックをすべて渡す必要があります。

Red Hat build of Cryostat Operator YAML 設定ファイルの **trustedCertSecrets** 配列で複数の TLS シークレットを指定できます。配列の **secretName** プロパティーで、Cryostat アプリケーションと同じ名前空間にあるシークレットを指定する必要があります。**certificateKey** プロパティーのデフォルトは **tls.crt** ですが、値を X.509 証明書ファイル名に変更できます。

重要

TLS 証明書の設定は、**com.sun.management.jmxremote.registry.ssl=true** 属性を使用してリモート JMX 接続に対して TLS を有効にしているアプリケーションにのみ必要です。

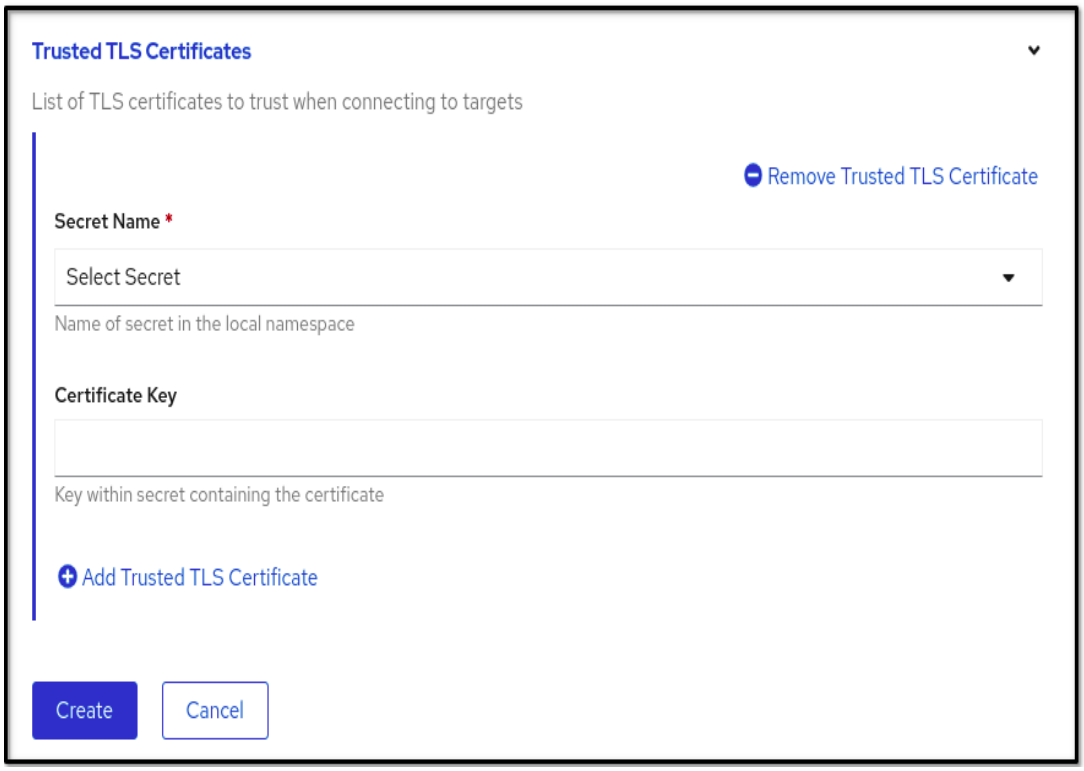
前提条件

- OpenShift Web コンソールを使用して OpenShift Container Platform にログインしている。
- Cryostat Web コンソールにログインしている。

手順

1. Red Hat OpenShift Web コンソールで、**Operators > Installed Operators**の順にクリックします。
2. 使用可能な Operator のリストから、Red Hat build of Cryostat を選択します。
3. **Operator details** ページで、**Details** タブをクリックします。
4. **Provided APIs** セクションで、**Cryostat** および **Cluster Cryostat** カスタムリソース (CR) が利用可能です。以下のオプションのいずれかを選択します。
    a. 単一 namespace の Cryostat インスタンスを作成するには、Cryostat を選択してから **Create instance** をクリックします。
    b. 複数 namespace の Cryostat インスタンスを作成するには、**Cluster Cryostat** を選択してから **Create instance** をクリックします。
5. TLS 証明書を設定するには、次のいずれかのオプションを選択します。
    a. **Form view** ラジオボタンをクリックします。
        i. **Name** フィールドに、作成する Cryostat のインスタンスの名前を指定します。
        ii. **Trusted TLS Certificates** オプションをデプロイメントし、**Add Trusted TLS Certificate** をクリックします。オプションのリストが Red Hat OpenShift Web コンソールに表示されます。

図1.6 信頼できる TLS 証明書オプション



iii. **Secret Name** リストから TLS シークレットを選択します。**Certificate Key** フィールドはオプションです。

注記

Remove Trusted TLS Certificate をクリックすると、TLS 証明書を削除できます。

iv. **Create** をクリックします。作成したインスタンスのタイプに応じて、インスタンスは以下のいずれかのタブで開きます。

- 単一 namespace の Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cryostat** タブで利用できます。
- Cluster Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cluster Cryostat** タブで利用できます。

b. **YAML view** のラジオボタンをクリックします。

i. **TrustedCertSecrets** 配列の **secretName** プロパティーで、Cryostat アプリケーションと同じ名前空間にあるシークレットを指定します。

trustedCertSecrets 配列でシークレットを指定する例

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

```
  trustedCertSecrets:
  - secretName: my-tls-secret
--
```

ii. **オプション: certificateKey** プロパティー値をアプリケーションの X.509 証明書ファイル名に変更します。値を変更しない場合、**certificateKey** プロパティーはデフォルトで **tls.crt** になります。

certificateKey プロパティーの値を変更する例

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

iii. **Save** をクリックします。
Red Hat build of Cryostat Operator は、設定されたセキュリティー設定を使用して Cryostat インスタンスを自動的に再起動します。

検証

1. CLI で次のコマンドを実行して、すべてのアプリケーション Pod が Cryostat Pod と同じ OpenShift クラスター名前空間に存在することを確認します。

```
$ oc get pods
```

2. Cryostat インスタンスの Web コンソールにログインします。

3. Cryostat インスタンスの **Dashboard** メニューで、**Target** リストから target JVM を選択します。

4. Cryostat Web コンソールのナビゲーションメニューで、**Recordings** を選択します。**Authentication Required dialog** ウィンドウで、シークレットの認証情報を入力し、**Save** を選択して、ターゲット JVM に認証情報を提供します。

注記

選択したターゲットで JMX 接続のパスワード認証が有効になっている場合は、接続のプロンプトが表示されたら、ターゲット JVM の JMX クレデンシャルを指定する必要があります。

Cryostat は、認証された JMX 接続を介してアプリケーションに接続します。これで、**Recordings** 機能および **Events** 機能を使用して、アプリケーションの JFR データを監視できます。

関連情報

- JDK Flight Recorder (JFR) レコーディングの作成 (Cryostat を使用した JFR レコーディングの作成) を参照してください。
- Operator を使用して Red Hat OpenShift に Cryostat をインストールする (Cryostat のインストール) を参照してください。
- Web コンソールを使用した Cryostat へのアクセス (Cryostat のインストール) を参照してください。

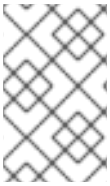
1.6. ストレージボリュームオプションの変更

Red Hat build of Cryostat Operator を使用して、Cryostat または Cluster Cryostat インスタンスのストレージボリュームを設定できます。Cryostat は、永続ボリュームクレーム (PVC) および **emptyDir** ストレージボリュームタイプをサポートします。

デフォルトでは、Red Hat build of Cryostat Operator は、500 メビバイト (MiB) の割り当てられたストレージを持つデフォルトの **StorageClass** リソースを使用する Cryostat または Cluster Cryostat インスタンス用の PVC を作成します。

以下のオプションのいずれかを選択することにより、OpenShift Container Platform で OpenShift Container Platform アプリケーション用のカスタム PVC を作成できます。

- **Form view** ウィンドウで **Storage Options > PVC > Spec**に移動し、関連するフィールドに入力して PVC をカスタマイズします。
- **YAML view** ウィンドウに移動し、必要に応じて **spec: key** セットの **storageOptions** 配列を編集します。



注記

Red Hat build of Cryostat Operator を使用して Cryostat を設定するガイドの ストレージボリュームオプションの変更 に移動することで、カスタム PVC の作成の詳細を確認できます。

以下のオプションのいずれかを選択することにより、OpenShift Container Platform で OpenShift Container Platform アプリケーションの **emptyDir** ストレージボリュームを設定できます。

- **Form view** ウィンドウの **Storage Options** で **Empty Dir** 設定を有効にします。
- **YAML view** ウィンドウで **spec.storageOptions.emptyDir.enabled** を **true** に設定します。

前提条件

- Red Hat OpenShift Web コンソールを使用して OpenShift Container Platform にログインしている。

手順

1. Red Hat OpenShift Web コンソールで、**Operators > Installed Operators**の順にクリックします。
2. 使用可能な Operator のリストから、Red Hat build of Cryostat を選択します。
   a. **Details** タブをクリックします。

3. **Provided APIs** セクションで、**Cryostat** および **Cluster Cryostat** カスタムリソース (CR) が利用可能です。以下のオプションのいずれかを選択します。

   - 単一 namespace の Cryostat インスタンスを作成するには、Cryostat を選択してから **Create instance** をクリックします。
   - 複数 namespace の Cryostat インスタンスを作成するには、**Cluster Cryostat** を選択してから **Create instance** をクリックします。

4. Cryostat アプリケーションのストレージ設定を変更するには、次のいずれかのオプションを選択してください。

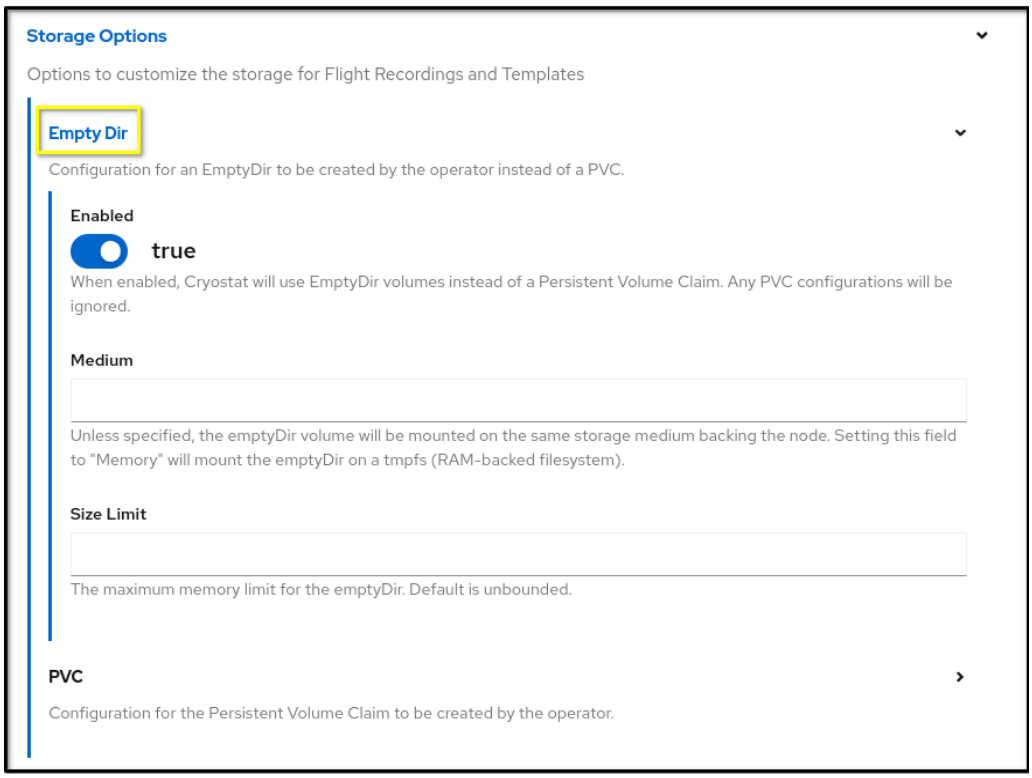
   a. **Form view** ラジオボタンをクリックします。

      i. **Storage Options** セクションに移動し、**Name** フィールドに値を入力します。

      ii. **Storage Options** をデプロイメントし、**Empty Dir** をクリックします。オプションの拡張された選択肢が Red Hat OpenShift Web コンソールで開きます。

      iii. **Enabled** スイッチを **true** に設定します。

      図1.7 EmptyDir スイッチを true に設定した例



      iv. **Create** をクリックします。作成したインスタンスのタイプに応じて、インスタンスは以下のいずれかのタブで開きます。

         - 単一 namespace の Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cryostat** タブで利用できます。
         - Cluster Cryostat インスタンスを作成した場合、インスタンスは **Operator details** ページの **Cluster Cryostat** タブで利用できます。

   b. **YAML view** のラジオボタンをクリックします。

      i. YAML ファイルの **spec:** キーセットで、**storageOptions** 定義を追加し、**emptyDir** プロパティーを **true** に設定します。

emptyDir プロパティーが true として設定されていることを示す例

```
--
apiVersion: operator.cryostat.io/v1beta1
kind: Cryostat
metadata:
  name: cryostat-sample
spec:
  storageOptions:
    emptyDir:
      enabled: true
      medium: "Memory"
      sizeLimit: 1Gi
--
```

ii. **オプション:medium** プロパティーと **sizeLimit** プロパティーの値を設定します。

iii. **Save** ボタンをクリックします。Red Hat build of Cryostat Operator は、Cryostat インスタンス用の PVC を作成する代わりに、ストレージ用の **EmptyDir** ボリュームを作成します。

1.7. CRYOSTAT のスケジューリングオプション

Red Hat OpenShift Web コンソールから、Red Hat build of Cryostat Operator を使用して、Cryostat アプリケーションおよびその生成されたレポートをノードにスケジュールするためのポリシーを定義できます。

Red Hat OpenShift 上の Cryostat または Cluster Cryostat カスタムリソース (CR) の YAML 設定ファイルで、**Node Selector**、**Affinities**、および **Tolerations** を定義できます。これらは、Cryostat アプリケーションの **spec.SchedulingOptions** プロパティーと、レポートジェネレーターサイドカーの **spec.ReportOptions.SchedulingOptions** プロパティーで定義する必要があります。**SchedulingOptions** プロパティーを指定すると、Cryostat アプリケーションとそのレポートジェネレーターサイドカー Pod が、スケジュール基準を満たすノード上でスケジュールされます。

ターゲットノードアプリケーションは、Cryostat インスタンスからサイドカーレポートの更新を受け取ることができます。

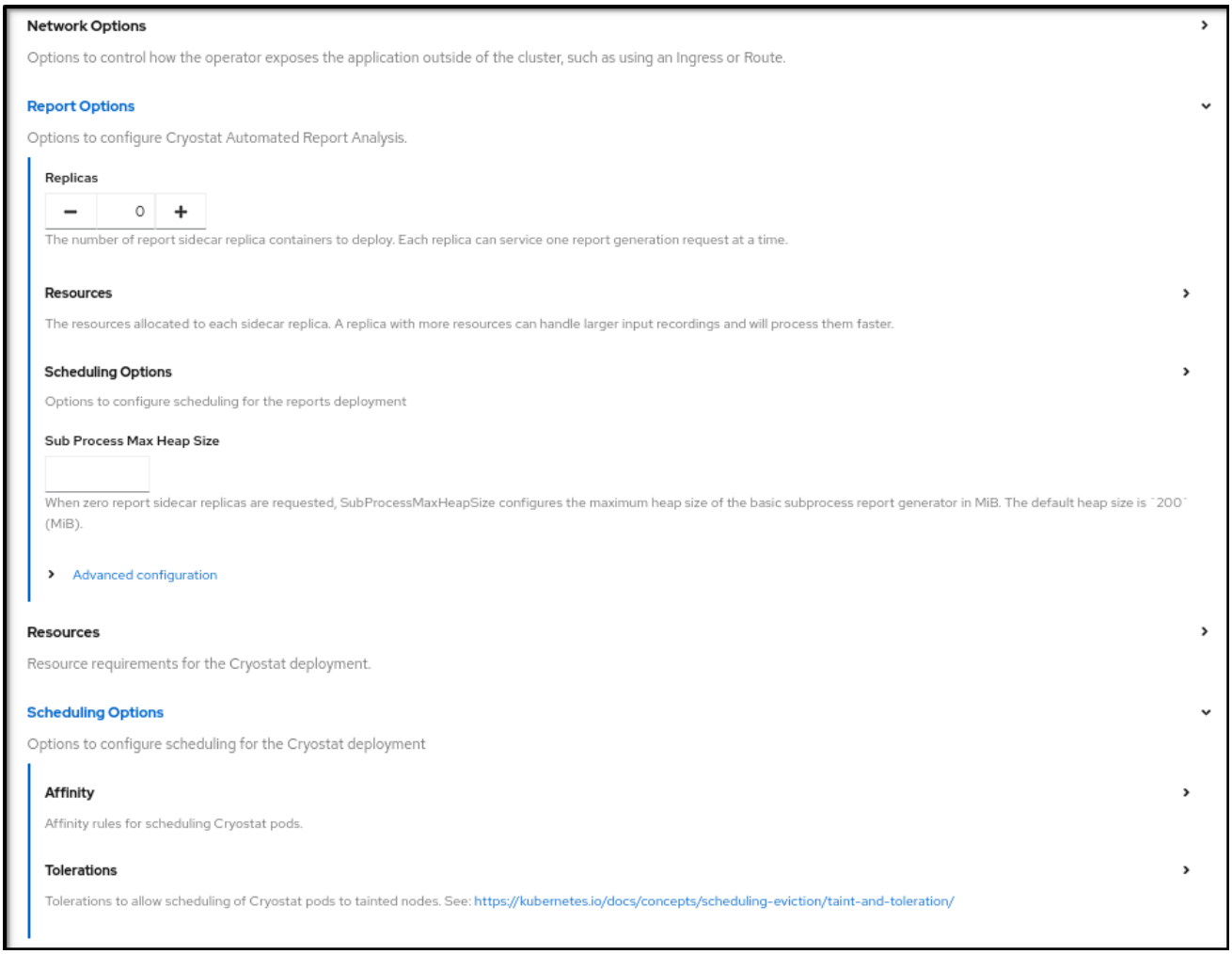
スケジュールオプションを定義する Cryostat CR の YAML 設定を示す例

```
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
```

または、Red Hat OpenShift Web コンソールを開いて Cryostat インスタンスを作成した後、その Cryostat インスタンスの **SchedulingOptions** と **reportOptions.SchedulingOptions** オプションで **Affinities**と **Tolerations** を定義することも可能です。

図1.8 OpenShift Web コンソールの Report Options および Scheduling Options パネル



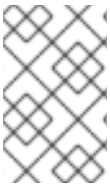
第2章 POD SECURITY ADMISSION (PSA)

Red Hat OpenShift は、Pod Security Admission (PSA) を使用して、同じ Red Hat OpenShift クラスター内にあるアプリケーション Pod に一連のセキュリティールールを適用します。Cryostat のコンテキストでは、これらのアプリケーション Pod には、Cryostat Pod と Report サイドカー Pod が含まれます。オプションで、Cryostat カスタムリソース (CR) で Report サイドカー Pod を有効にすることができます。アプリケーションがポリシー基準を満たしていない場合、そのアプリケーションを Red Hat OpenShift クラスターで実行することはできません。

Red Hat OpenShift 4.8 では **PodSecurityPolicy** API が非推奨となり、代わりに PSA が使用されます。PSA には以下のメリットがあります。

- アプリケーション Pod に Pod セキュリティー標準を適用できる組み込みコントローラーが含まれています。
- **Privileged**、**Baseline**、**Restricted** の 3 つの異なるポリシーを定義する Pod セキュリティー標準のセットが含まれています。

Red Hat OpenShift では、Security Context Constraints (SCC) で PSA を使用して、Red Hat OpenShift クラスターのポリシーを定義できます。デフォルトでは、**restricted-v2** SCC は **Restricted** Pod セキュリティー標準に準拠しています。



注記

デフォルトでは、Cryostat Pod のセキュリティーコンテキストは **restricted-v2** SCC に準拠します。つまり、Red Hat OpenShift は、**Restricted** Pod セキュリティー標準を強制する namespace で Pod を許可できます。

Restricted ポリシーでは、Red Hat build of Cryostat Operator がコンテナーセキュリティーコンテキストを次のように設定する必要があります。

- **ALL** 機能を停止します。
- **allowPrivilegeEscaltion** を **false** に設定します。

Restricted ポリシーでは、Red Hat build of Cryostat Operator が Pod セキュリティーコンテキストを次のように設定する必要があります。

- **runAsNonRoot** を **true** に設定します。
- **seccompProfile** を **RuntimeDefault** に設定します。

さらに、Red Hat build of Cryostat Operator は、Cryostat アプリケーション Pod の Pod セキュリティーコンテキストで **fsGroup** を定義し、Cryostat が Red Hat OpenShift の永続ストレージボリューム内のファイルを読み書きできるようにします。

Restricted Pod セキュリティー標準への準拠以外に追加の要件がある場合は、Cryostat が使用するデフォルトのセキュリティーコンテキストをオーバーライドできます。

2.1. セキュリティーコンテキストの設定

Red Hat OpenShift の Cryostat カスタムリソース (CR) で、Pod とコンテナーのセキュリティーコンテキストを指定できます。セキュリティーコンテキストは、Cryostat Pod、Report サイドカー Pod (使用中の場合)、および各 Pod のコンテナーにパーミッションを適用します。

注記

CR の設定を変更すると、これらの設定はデフォルトのセキュリティーコンテキスト設定をオーバーライドします。

セキュリティーコンテキストは、Pod 内に存在するアプリケーションに特定のパーミッションを適用します。セキュリティーコンテキストは、SCC ポリシーの基準を変更できません。カスタム SCC を作成して、Pod が実行できるアクションや Pod がアクセスできるリソースなど、厳密なパーミッションを Pod に適用するように Red Hat OpenShift クラスターに指示できます。

カスタム SCC を作成するには、クラスター管理パーミッションが必要です。また、クラスターで動作するすべての Pod のセキュリティーコンテキストを作成して、これらの Pod がカスタム SCC 要件を満たすようにする必要があります。

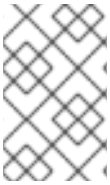
SCC は Red Hat OpenShift のクラスターレベルと namespace レベルで変更を強制的に適用するため、このクラスター内部で動作するすべての Pod がポリシー基準を受け取ります。これに対して、セキュリティーコンテキストは Pod 固有のものになります。

デフォルトでは、Red Hat build of Cryostat Operator は Cryostat Pod の **restricted-v2** SCC ポリシーに準拠しています。

デフォルトでは、Red Hat build of Cryostat Operator は、Cryostat とそのコンポーネント (**jfr-datasource** や **grafana** など) のサービスアカウントを作成します。

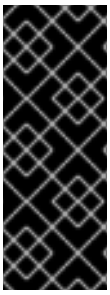
このサービスアカウントでカスタム SCC を使用できるようにするには、以下のいずれかの手順を実行します。

- カスタム SCC を **使用** するロールに Cryostat サービスアカウントをバインドする **Role Binding** を作成します。
- **Label Syncer** コンポーネントを使用して、プロジェクトの名前空間が PSA ポリシーに従うように指示します。



注記

Label Syncer コンポーネントは、このドキュメントの範囲外になります。通常、**openshift-** タグの接頭辞が付けられた Red Hat OpenShift システムの namespace で **Label Syncer** コンポーネントは使用できません。



重要

特定のパーミッションをアプリケーション Pod に適用するようにセキュリティーコンテキストを設定する前に、Red Hat OpenShift 上のクラスターにもたらされる可能性があるセキュリティーリスクを考慮してください。PSA では、通常、ほとんどの要件を満たす 3 つの段階的なポリシーレベルが用意されています。Red Hat は、Red Hat OpenShift Pod のセキュリティー標準に準拠しないセキュリティーコンテキストの変更について一切の責任を負いません。

前提条件

- Red Hat OpenShift Web コンソールを使用して OpenShift Container Platform にログインしている。

- Red Hat build of Cryostat Operator を Red Hat OpenShift のプロジェクトにインストールしている。Red Hat build of Cryostat Operator を使用した Red Hat OpenShift への Cryostat のインストール (Cryostat のインストール) を参照してください。
- **オプション:** PSA と SCC の新しいポリシーを参照している。セキュリティーコンテキスト制約の管理 (OpenShift Container Platform) を参照してください。
- **オプション:** PSA が提供する 3 つのポリシーのいずれかを使用するようにプロジェクトを設定している。
  - カスタム SCC を使用して Pod に特定のポリシーを適用する場合は、Pod のサービスアカウントがそれにアクセスできるように SCC を設定する必要があります。

手順

1. Red Hat OpenShift Web コンソールから、**Operators > Installed Operators**をクリックします。
2. 使用可能な Operator のリストから、Red Hat build of Cryostat を選択します。
3. **Provided APIs > Create**をクリックします。Red Hat build of Cryostat Operator は、Report サイドカー Pod のサービスアカウントを作成しません。代わりに、これらの Pod は独自の namespace でデフォルトのサービスアカウントを使用します。
4. セキュリティーコンテキストを設定するには、次のいずれかのオプションを完了します。
   a. **YAML view** をクリックします。**spec:** 要素から、セキュリティー要件に一致するように **securityOptions** プロパティーおよび **reportOptions** プロパティーを編集します。

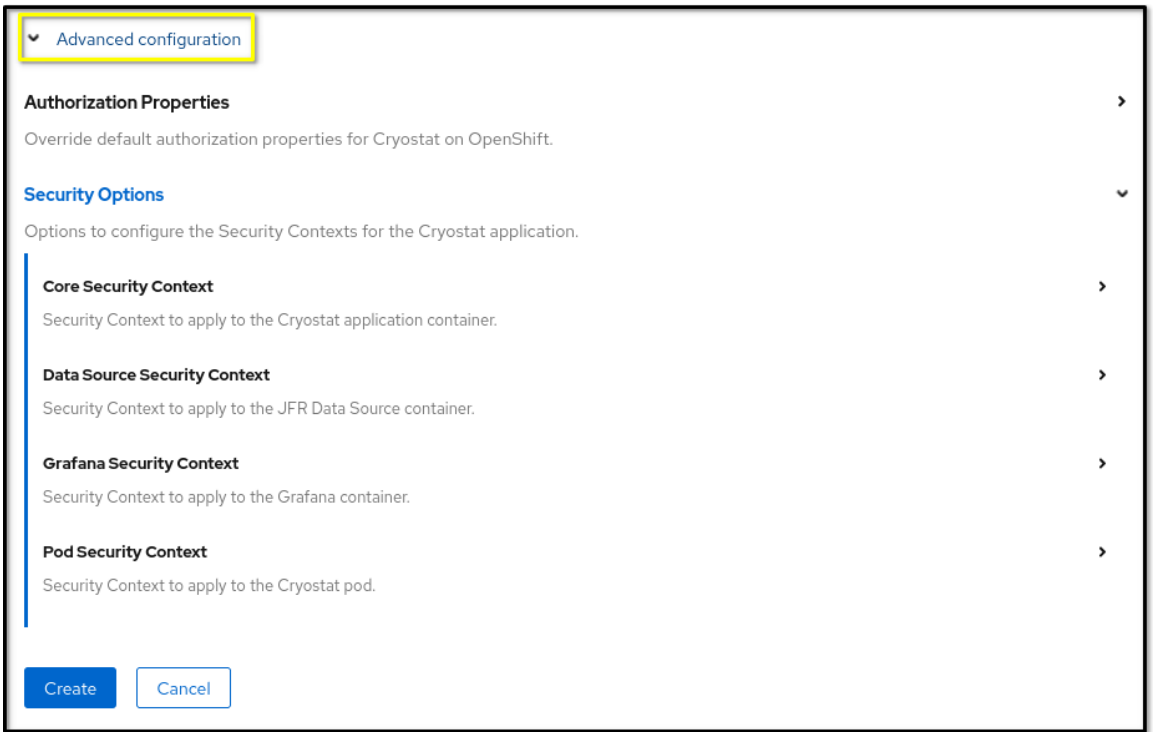
      セキュリティーコンテキストの設定例

```
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. **Advanced Configurations** を展開して、Red Hat OpenShift Web コンソールで追加のオプションを開きます。

図2.1詳細設定メニューオプション



c. **Core Security Context** を展開します。使用可能なオプションのリストから、セキュリティーコンテキストの設定を定義します。

5. **Create** をクリックします。

6. 必要に応じて、**Data Source Security Context**、**Grafana Security Context**、および **Pod Security Context** の手順 1 - 5 を繰り返します。

7. **オプション: Report Generator** サービスを使用している場合は、以下のように、このサービスのセキュリティーコンテキストを設定することもできます。

   a. **Report Options** から、**Advanced Configurations** を展開します。

   b. **Security Options** を展開します。必要に応じて、**Reports Security Context** および **Pod Security Context** を定義します。

関連情報

関連情報

- Pod セキュリティー標準ポリシー

2.2. POD セキュリティー標準ポリシー

Pod Security Admission (PSA) には、Pod セキュリティー標準に関連するセキュリティーレベルに対応する 3 つのポリシーが含まれています。各ポリシーについて、以下の表で説明します。

プロファイル	説明
Privileged	Cryostat Pod に幅広いレベルのパーミッションを提供する無制限のポリシー。Pod に既知の権限昇格を付与する必要がある場合は、このポリシーを設定することを検討してください。
Baseline	既知の権限昇格を制限するデフォルトのポリシー。**Baseline** ポリシーは、各コントロールが制限されたフィールドと許可された値を定義するコントロールを設定します。
Restricted	Cryostat Pod に低レベルのパーミッションを付与する **Restricted** ポリシー。このポリシーは、制限されたフィールドと許可された値を定義する各コントロールでコントロールを設定します。

第3章 RBAC マッピングの設定

OpenShift Container Platform (OCP)では、Cryostat は OCP リソースを Cryostat が管理するリソースにマップするパーミッション設定を使用します。パーミッション設定は、JFR レコーディングの作成や検出されたターゲットの表示など、特定のアクションを実行するようにユーザーを承認するためのフレームワークを Cryostat に提供します。

次の表は、Cryostat のマネージドリソースを表す定義の概要を示しています。

リソース	説明
CERTIFICATE	暗号化を有効にして Java 仮想マシン (JVM) アプリケーションに接続する SSL 証明書。
CREDENTIALS	ターゲット JVM アプリケーションの保存された認証情報。
RECORDING	JVM アプリケーション用に作成された記録。
REPORT	レコーディングから生成された報告の内容
RULE	一致するターゲットを非対話的に利用できるようになったときに、一致するターゲットのレコーディングを開始する自動化ルール。
TARGET	監視対象として検出された JVM アプリケーション。
TEMPLATE	レコーディングを設定するためのイベントテンプレート。

パーミッション設定は、前述のリソース定義と同等の OCP リソースのリストを定義します。API リクエストは、リソースアクションを指定して、Cryostat が管理するリソースパーミッションを OCP リソースに変換します。Cryostat は、このアクションの各 API 要求を確認してから、API 要求を送信します。

Cryostat はリソース検証ペアを各エンドポイントに割り当てます。これらの動詞はカスタムであり、Cryostat に固有のものです。パーミッションの確認時に、Cryostat はカスタム動詞を RBAC 動詞に変換します。

以下の動詞をこれらの Cryostat が管理するリソースに実装できます。

- **CREATE**: create
- **DELETE**: delete
- **READ**: get
- **UPDATE**: patch

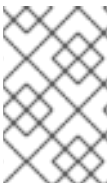
以下の例は、Cryostat が管理するリソースを Red Hat OpenShift リソースの一覧にリンクするマッピング設定を示しています。

```
TARGET=pods,services
```

Recordings ページの **Target JVM** ペインから検出された JVM ターゲットの一覧を出力する API 要求を作成するには、検出可能な **TARGET** を表示するには、**READ** パーミッションが必要です。RBAC システムでの **READ** パーミッションは Pod およびサービスの読み取りアクセスを割り当てます。

デフォルトでは、Cryostat は以下の RBAC マッピング設定を使用します。

```
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
```



注記

ConfigMap はマッピングの内容を定義します。上記の例では、Cryostat が管理するリソースがすべてリストされていません。Cryostat が管理するリソースが **ConfigMap** にない場合、Cryostat は API 要求の処理中のパーミッションチェックを省略します。

Red Hat build of Cryostat Operator は、提供された **ConfigMap** API オブジェクトから Red Hat OpenShift 上の Cryostat Pod にこれらの設定を適用します。Cryostat Pod はいつでもこれらの設定にアクセスし、ユーザーが Cryostat 機能にアクセスできるパーミッションを確認できます。次に、これらのマッピングされた Red Hat OpenShift リソースに特定の権限を提供するカスタムリソース (CR) で **ClusterRole** を定義できます。

spec フィールドで定義された ConfigMap、ClusterRole、および filename フィールドを持つ Cryostat CR を示す例

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

関連情報

- RBAC パーミッション (Cryostat のインストール) を参照してください。

3.1. RBAC マッピングの設定

Cryostat 固有の RBAC 権限を持つカスタムロールを作成し、このロールをユーザーの Red Hat OpenShift アカウントにバインドできます。この機能は、同じ Cryostat namespace 内で操作する各ユーザーに特定の権限を設定する場合に役立ちます。

前提条件

- Red Hat OpenShift Web コンソールを使用して OpenShift Container Platform にログインしている。

- プロジェクトに Cryostat インスタンスを作成している。Operator を使用して Red Hat OpenShift に Cryostat をインストールする (Cryostat のインストール) を参照してください。

手順

1. **ConfigMap** オブジェクトにカスタムパーミッションマッピングを定義します。

   パーミッションマッピングが含まれる ConfigMap の例

```
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
```

   カスタムパーミッションマッピングを使用するには、**ClusterRole** が存在し、カスタムパーミッションマッピングにリストされているすべての Red Hat OpenShift オブジェクトのパーミッションが含まれる必要があります。

   必要なルールが含まれる ClusterRole の例

```
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
```

Red Hat OpenShift Web コンソールで認証情報を入力すると、**OAuth** サーバーは認証情報と指定されたスコープを使用して API トークンを生成します。

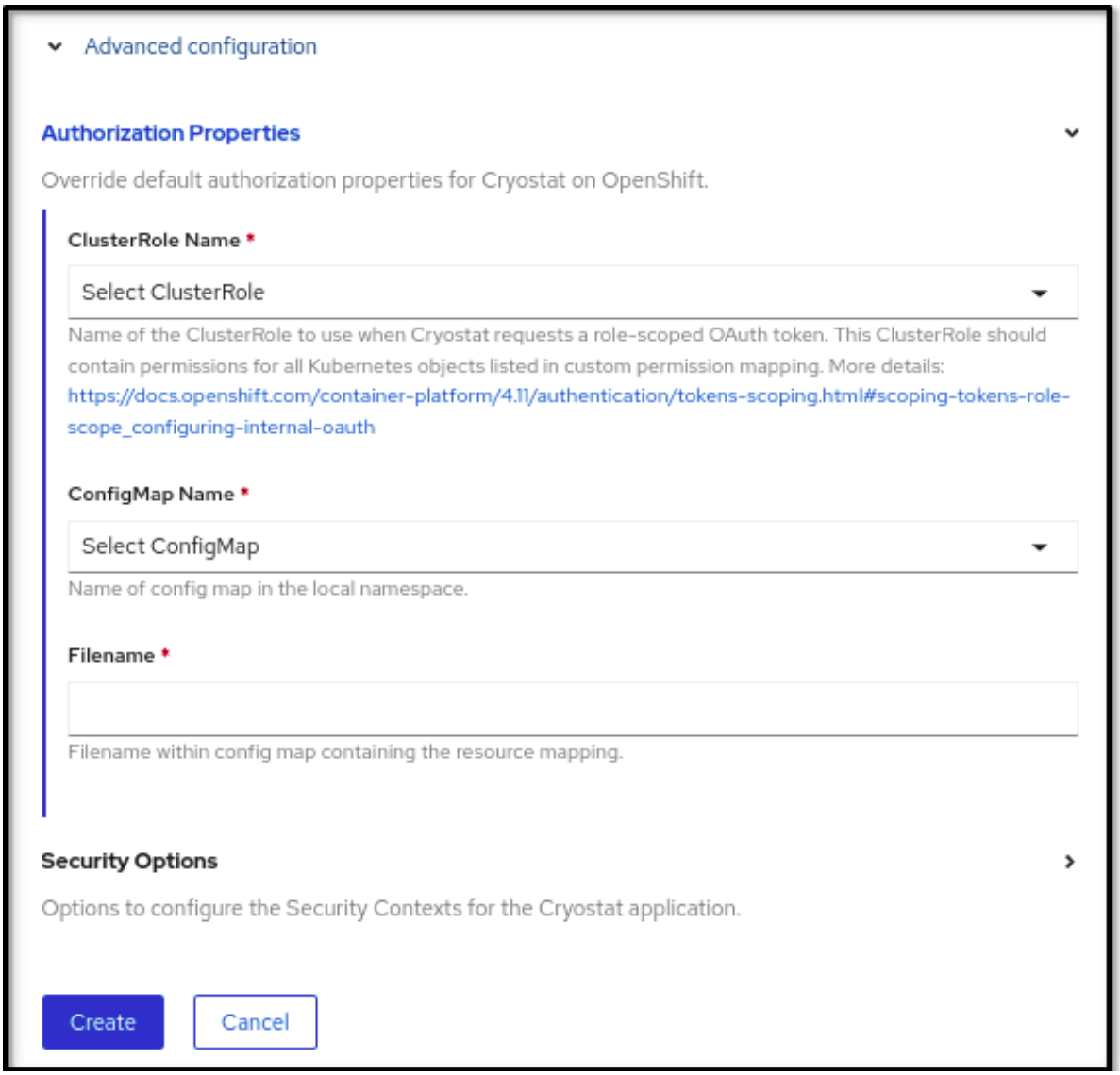
2. Cryostat カスタムリソース (CR) に **authProperties** 仕様を指定して、マッピングコンテンツを保持する **ConfigMap**、およびマップされた Red Hat OpenShift リソースの RBAC アクセスを定義する **ClusterRole** を参照します。

カスタムパーミッションマッピングを定義する authProperties のある Cryostat CR の例

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

または、Red Hat OpenShift Web コンソールを開き、Cryostat インスタンスを作成し、**Authorization Properties** オプションで **ClusterRole Name**、**ConfigMap Name**、および **Filename** プロパティーを定義できます。これは、**Advanced configuration** セクションでアクセスできます。

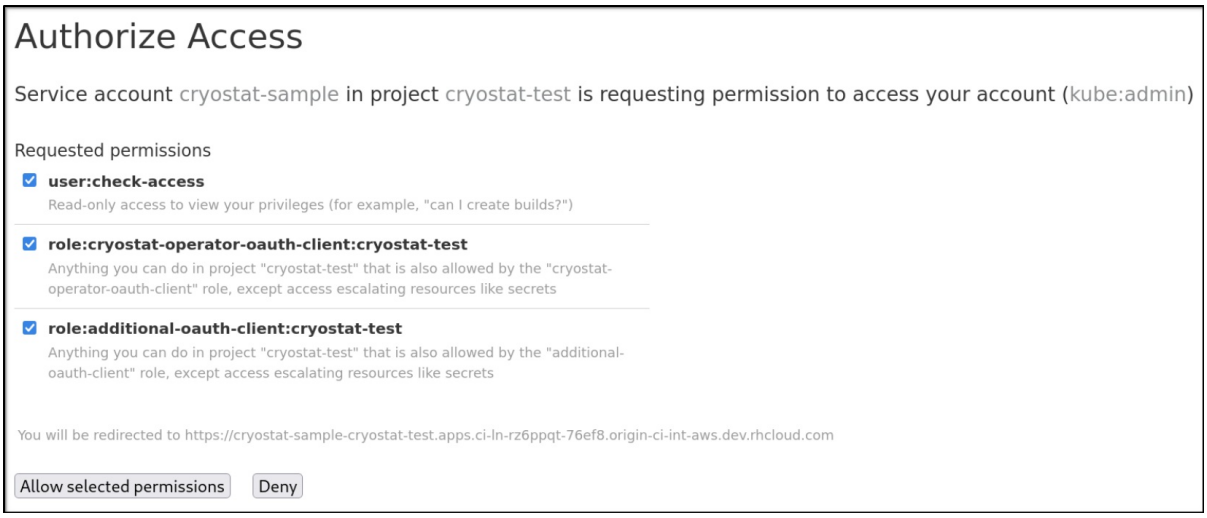
図3.1 OpenShift Web コンソールの Advanced configuration セクション



検証

1. **Installed Operators** メニューから、Cryostat インスタンスを選択します。
2. **Application URL** セクションのリンクをクリックして、ログイン画面にアクセスします。**OAuth** サーバーは、ユーザーを OpenShift Container Platform ログインページにリダイレクトします。
3. 認証情報の詳細を入力し、**ログイン** をクリックします。**OAuth** サーバーを介して初めてログインすると、Web ブラウザーに **Authorize Access** ページが開きます。
4. **Requested Permissions** オプションから、クラスターのロール名が Cryostat CR で指定した名前と一致することを確認します。
5. **Authorize Access** ウィンドウで、必要なチェックボックスを選択します。Cryostat のパフォーマンスを最適化するには、すべてのチェックボックスを選択します。

図3.2 3 つのパーミッションを一覧表示する Authorize Access ウィンドウ



Authorize Access ウィンドウには、以下のパーミッションが一覧表示されます。

- **user:check-access**: 内部 Cryostat アプリケーションリクエストを確認するパーミッションです。パーミッションは、権限を表示する読み取り専用権限を持つユーザーを提供します。

- **role:cryostat-operator-oauth-client:<namespace>** は、内部の Cryostat アプリケーション要求を確認するパーミッションです。**<namespace>** は、CLI からのプロジェクト名または namespace に置き換えます。パーミッションにより、シークレットなどのリソースのエスカレーションへのアクセスを除き、**cryostat-operator-oauth-client** ロールが指定する操作を完了するためのアクセスをユーザーに提供します。

- **role:<user-define-clusterrole-name>:<namespace>**: Cryostat CR 仕様で定義した **clusterrole**。**<namespace>** は、CLI からのプロジェクト名または namespace に置き換えます。パーミッション は、シークレットなどのリソースへのアクセスを昇格する場合を除き、**additional-oauth-client role** で指定する操作を実行するアクセス権をユーザーに割り当てます。

6. 以下のいずれかのオプションを選択します。

   a. 要求したパーミッションのうち、選択した内容で問題がなければ、**Allow selected permissions** をクリックします。

   b. 要求したパーミッションの選択内容をすべて拒否する場合は、**Deny** ボタンをクリックします。
   Web ブラウザーによって Cryostat Web コンソールにリダイレクトされます。このコンソールでは、Java 仮想マシン (JVM) で実行されている Java アプリケーションを監視できます。

関連情報

- Red Hat build of Cryostat Operator を使用した Red Hat OpenShift への Cryostat のインストール (Cryostat のインストール) を参照してください。

改訂日時: 2023-12-13