bitwarden | ヘルプセンターの記事

SELF-HOSTING › インストール＆デプロイガイド ›

OpenShiftデプロイメント

OpenShiftデプロイメント

この記事では、OpenShiftの特定の提供に基づいて、あなたがどのようにBitwarden自己ホスト型Helm Chartのデプロイメントを変更するかについて深く掘り下げています。

OpenShiftのルート

この例では、デフォルトのイングレスコントローラーの代わりにOpenShift Routesを示します。

デフォルトのイングレスを無効にする

1. アクセス `my-values.yaml`。

2. デフォルトのイングレスを無効にするには、`ingress.enabled: false`を指定します:

```
Bash

general:
  domain: "replaceme.com"
  ingress:
    enabled: false
```

残りのingress値は変更を必要としません。なぜなら、`ingress.enabled: false`を設定すると、チャートはそれらを無視するように促されます。

ルートのための生のマニフェストを追加します

`rawManifests`セクションを`my-values.yaml`で見つけてください。このセクションは、OpenShift Routeマニフェストが割り当てられる場所です。

OpenShift Routesを使用する`rawManifests`セクションの例ファイルは、⭳ タイプ: アセット-ハイパーリンク id: 33Or6BrWsFLL9FLZbPSLIcからダウンロードできます。

> **ⓘ Note**
>
> 上記の例では、`destinationCACertificate`は空の文字列に設定されています。これはOpenShiftのデフォルトの証明書設定を使用します。あるいは、ここに証明書の名前を指定するか、このガイドに従ってLet's Encryptを使用することもできます。もしそうするなら、各ルートの注釈に`kubernetes.io/tls-acme: "true"`を追加する必要があります。

共有ストレージクラス

ほとんどのOpenShiftデプロイメントには共有ストレージクラスが必要です。`ReadWriteMany`ストレージを有効にする必要があります。これはあなたの選択した方法で行うことができます、一つの選択肢はNFSサブディレクトリ外部プロビジョナーを使用することです。

シークレット

`oc`コマンドは、シークレットをデプロイするために使用できます。有効なインストールIDとキーは、bitwarden.com/host/から取得できます。詳細については、インストールIDとインストールキーは何に使われますか？をご覧ください。

次のコマンドは例です：

> ⚠ Warning
> この例では、シェルの履歴にコマンドを記録します。他の方法も秘密を安全に設定するために考慮されるかもしれません。

```bash
oc create secret generic custom-secret -n bitwarden \
    --from-literal=globalSettings__installation__id="REPLACE" \
    --from-literal=globalSettings__installation__key="REPLACE" \
    --from-literal=globalSettings__mail__smtp__username="REPLACE" \
    --from-literal=globalSettings__mail__smtp__password="REPLACE" \
    --from-literal=globalSettings__yubico__clientId="REPLACE" \
    --from-literal=globalSettings__yubico__key="REPLACE" \
    --from-literal=globalSettings__hibpApiKey="REPLACE" \
    --from-literal=SA_PASSWORD="REPLACE" # If using SQL pod
    # --from-literal=globalSettings__sqlServer__connectionString="REPLACE" # If using your own SQL
server
```

サービスアカウントを作成

OpenShiftでは、各コンテナが起動時に昇格コマンドを実行する必要があるため、サービスアカウントが必要です。
これらのコマンドはOpenShiftの制限付きSCCによってブロックされています。私たちはサービスアカウントを作成し、それを`anyuid` SCCに割り当てる必要があります。

1. 次のコマンドを`oc`コマンドラインツールで実行してください：

   ```bash
   oc create sa bitwarden-sa
   oc adm policy add-scc-to-user anyuid -z bitwarden-sa
   ```

2. 次に、新しいサービスアカウントを使用するように`my-values.yaml` を更新してください。
   次のキーを前のステップで作成されたサービスアカウント`bitwarden-sa`の名前に設定します:

```Bash
component.admin.podServiceAccount
component.api.podServiceAccount
component.attachments.podServiceAccount
component.events.podServiceAccount
component.icons.podServiceAccount
component.identity.podServiceAccount
component.notifications.podServiceAccount
component.scim.podServiceAccount
component.sso.podServiceAccount
component.web.podServiceAccount
database.podServiceAccount
```

これは`my-values.yaml`ファイルの例です:

```Bash
component:
  # The Admin component
  admin:
    # Additional deployment labels
    labels: {}
    # Image name, tag, and pull policy
    image:
      name: bitwarden/admin
    resources:
      requests:
        memory: "64Mi"
        cpu: "50m"
      limits:
        memory: "128Mi"
        cpu: "100m"
    securityContext:
    podServiceAccount: bitwarden-sa
```

Note

これらのポッドのセキュリティを微調整するために、自分自身のSCCを作成することができます。「OpenShift での SCC の管理」では、すぐに使える SSC と、必要に応じて独自の SSC を作成する方法について説明します。