Red Hat 3scale API Management 2.8

3scale のインストール

3scale API Management のインストールおよび設定

Last Updated: 2023-03-04

Red Hat 3scale API Management 2.8 3scale のインストール

3scale API Management のインストールおよび設定

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.

法律上の通知

概要

本ガイドは、3scale API Management のインストールおよび設定に関する情報を提供します。

目次

はじめに

本ガイドは、3scale のインストールおよび設定に役立ちます。

第1章 OPENSHIFT への 3SCALE のインストール

本セクションでは、OpenShift に Red Hat 3scale API Management 2.8 をデプロイする一連の手順を説明します。

オンプレミスデプロイメントの Red Hat 3scale API Management ソリューションは、以下の要素で設定されています。

- 2 つの API ゲートウェイ: Embedded APIcast
- 1 つの 3scale 管理ポータルおよび永続ストレージを持つデベロッパーポータル

3scale ソリューションをデプロイする方法は 2 つあります。

- 「テンプレートを使用した OpenShift への 3scale のデプロイ」
- 「operator を使用した 3scale のデプロイ」

注記

3scale のデプロイに operator とテンプレートのどちらを使用するかにかかわらず、まず Red Hat コンテナーレジストリーへのレジストリー認証を設定する必要があります。コンテナーイメージの registry.redhat.io を使用した認証 を参照してください。

前提条件

- 3scale サーバーを UTC (協定世界時) に設定する必要があります。

OpenShift に 3scale をインストールするには、以下のセクションに概略を示す手順を実施します。

- 「OpenShift に 3scale をインストールするためのシステム要件」
- 「ノードおよびエンタイトルメントの設定」
- 「テンプレートを使用した OpenShift への 3scale のデプロイ」
- 「3scale テンプレートのパラメーター」
- 「OpenShift 上での 3scale と APIcast の使用」
- 「operator を使用した 3scale のデプロイ」
- 「典型的な 3scale インストールの問題のトラブルシューティング」

1.1. OPENSHIFT に 3SCALE をインストールするためのシステム要件

本セクションでは、3scale - OpenShift テンプレートの要件を示します。

1.1.1. 環境要件

Red Hat 3scale API Management には、Red Hat 3scale API Management のサポート対象設定 に指定されている環境が必要です。

1.1.1.1. ローカルファイルシステムストレージの使用

永続ボリューム

- Redis および MySQL の永続用の 3 つの RWO (ReadWriteOnce) 永続ボリューム
- デベロッパーポータルコンテンツおよび System-app Assets 用の 1 つの RWX (ReadWriteMany) 永続ボリューム

RWX 永続ボリュームは、グループによる書き込みができるように設定します。必要なアクセスモードをサポートする永続ボリュームタイプのリストは、OpenShift のドキュメント を参照してください。

1.1.1.2. Amazon Simple Storage Service (Amazon S3) ストレージの使用

永続ボリューム

- Redis および MySQL の永続用の 3 つの RWO (ReadWriteOnce) 永続ボリューム

ストレージ:

- 1 x Amazon S3 バケット

1.1.2. ハードウェア要件

ハードウェア要件は、用途のニーズによって異なります。Red Hat は、テストを行い個々の要件を満たすように環境を設定することを推奨します。OpenShift 上に 3scale の環境を設定する場合、以下が推奨されます。

- クラウド環境へのデプロイメントには、コンピュートタスクに最適化したノードを使用する (AWS c4.2xlarge または Azure Standard_F8)。
- メモリーの要件が現在のノードで使用できる RAM よりも大きい場合、非常に大きなインストールでは、Redis に別のノードが必要になることがある (AWS M4 シリーズまたは Azure Av2 シリーズ)。
- ルーティングタスクとコンピュートタスクには別のノードを使用する。
- 3scale 固有のタスクには専用のコンピュートノードを使用する。
- バックエンドリスナーの **PUMA_WORKERS** 変数をコンピュートノードのコア数に設定します。

1.2. ノードおよびエンタイトルメントの設定

3scale を OpenShift にデプロイする前に、環境が Red Hat コンテナーレジストリー からイメージを取得するのに必要なノードおよびエンタイトルメントを設定する必要があります。ノードとエンタイトルメントを設定するには、以下の手順を実施します。

手順

1. 各ノードに Red Hat Enterprise Linux (RHEL) をインストールします 。
2. インターフェイス または コマンドライン で Red Hat Subscription Manager (RHSM) を使用し、Red Hat にノードを登録します。
3. RHSM を使用して ノードを 3scale サブスクリプションに割り当てます。
4. 以下の要件に準拠して、ノードに OpenShift をインストールします。

- サポート対象バージョンの OpenShift を使用する。
- 複数書き込みをサポートするファイルシステムで 永続ストレージ を設定する。

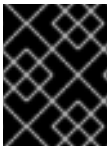
5. OpenShift コマンドラインインターフェイス をインストールします。
6. Subscription Manager を使用して、**rhel-7-server-3scale-amp-2-rpms** リポジトリーへのアクセスを有効にします。

```
sudo subscription-manager repos --enable=rhel-7-server-3scale-amp-2-rpms
```

7. 3scale テンプレート **3scale-amp-template** をインストールします。このテンプレートは **/opt/amp/templates** に保存されます。

```
sudo yum install 3scale-amp-template
```

1.2.1. Amazon Simple Storage Service の設定



重要

ローカルファイルシステムストレージで 3scale をデプロイする場合は、本セクションを飛ばして次に進んでください。

Amazon Simple Storage Service (Amazon S3) バケットをストレージとして使用する場合には、3scale を OpenShift にデプロイする前にバケットを設定する必要があります。

3scale 用の Amazon S3 バケットを設定するには、以下の手順を実施します。

1. 以下の最低限のパーミッションで Identity and Access Management (IAM) ポリシーを作成します。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "s3:ListAllMyBuckets",
         "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::targetBucketName",
            "arn:aws:s3:::targetBucketName/*"
         ]
      }
   ]
}
```

2. 以下のルールで CORS 設定を作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
<CORSRule>
  <AllowedOrigin>https://*</AllowedOrigin>
  <AllowedMethod>GET</AllowedMethod>
</CORSRule>
</CORSConfiguration>
```

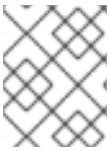
1.3. テンプレートを使用した OPENSHIFT への 3SCALE のデプロイ

注記

OpenShift Container Platform (OCP) 4.x は、operator を使用した 3scale のデプロイメントのみをサポートしています。operator を使用した 3scale のデプロイ を参照してください。

前提条件

- ノードおよびエンタイトルメントの設定 セクションで指定されたとおりに設定された OpenShift クラスター
- OpenShift クラスターに対して解決する ドメイン
- Red Hat コンテナーカタログ へのアクセス
- コンテンツ管理システム (CMS) ストレージに Amazon Simple Storage Service (Amazon S3) バケットを使用している場合は、以下を実行します。
- (オプション) PostgreSQL を使用したデプロイメント。
  - これは Openshift のデフォルトデプロイメントと同じですが、PostgreSQL を内部システムデータベースとして使用します。
- (オプション) 稼働中の電子メール機能用 SMTP サーバー



注記

テンプレートを使用した OpenShift への 3scale のデプロイは、OpenShift Container Platform 3.11 がベースとなります。

以下の手順に従い、**.yml** テンプレートを使用して 3scale を OpenShift にインストールします。

- コンテナーレジストリー認証の設定
- レジストリーサービスアカウントの作成
- レジストリーサービスアカウントの変更
- 3scale テンプレートのインポート
- 管理ポータルの URL の取得
- Amazon Simple Storage Service を使用した 3scale のデプロイ
- PostgreSQL を使用した 3scale のデプロイ
- SMTP 変数の設定

1.4. コンテナーレジストリー認証の設定

3scale 管理者は、3scale コンテナーイメージを OpenShift にデプロイする前に、**registry.redhat.io** との認証を設定します。

前提条件

- OpenShift Container Platform クラスターへアクセスできるクラスター管理者権限。
- OpenShift **oc** クライアントツールがインストール済みであること。詳細は、OpenShift CLI のドキュメント を参照してください。

手順

1. 管理者として OpenShift クラスターにログインします。

```
$ oc login -u system:admin
```

2. 3scale をデプロイするプロジェクトを開きます。

```
$ oc project myproject
```

3. Red Hat カスタマーポータルアカウントを使用して **docker-registry** シークレットを作成します。**threescale-registry-auth** は作成するシークレットに置き換えます。

```
$ oc create secret docker-registry threescale-registry-auth \
  --docker-server=registry.redhat.io \
  --docker-username=CUSTOMER_PORTAL_USERNAME \
  --docker-password=CUSTOMER_PORTAL_PASSWORD \
  --docker-email=EMAIL_ADDRESS
```

以下の出力が表示されるはずです。

```
secret/threescale-registry-auth created
```

4. シークレットをサービスアカウントにリンクして、シークレットをイメージをプルするために使用します。サービスアカウント名は、OpenShift Pod が使用する名前と一致する必要があります。以下は、**default** サービスアカウントを使用する例になります。

```
$ oc secrets link default threescale-registry-auth --for=pull
```

5. シークレットを **builder** サービスアカウントにリンクし、ビルドイメージをプッシュおよびプルするためにシークレットを使用します。

```
$ oc secrets link builder threescale-registry-auth
```

関連情報

コンテナーイメージに対する Red Hat の認証に関する詳細は、以下を参照してください。

- Red Hat コンテナーレジストリーの認証
- Red Hat registry service accounts

1.4.1. レジストリーサービスアカウントの作成

OpenShift 上にデプロイされた 3scale 2.8 と共に共有環境で **registry.redhat.io** からのコンテナーイメージを使用するには、個々のユーザーの **カスタマーポータル** のクレデンシャルではなく、**レジストリーサービスアカウント** を使用する必要があります。

注記

テンプレートまたは operator のどちらを使用して 3scale 2.8 を OpenShift にデプロイする場合でも、その前に以下に概略を示す手順に従う必要があります。両オプションともレジストリーの認証を使用するためです。

手順

1. Registry Service Accounts のページに移動し、ログインします。
2. **New Service Account** をクリックします。
3. **Create a New Registry Service Account**のページに表示されるフォームに入力します。
   a. **サービスアカウント** の名前を追加します。
   注記: フォームのフィールドの前に、決められた桁数のランダムに生成された数字の文字列が表示されます。
4. **Description** を入力します。
5. **Create** をクリックします。
6. **Registry Service Accounts**のページに戻ります。
7. 作成した **サービスアカウント** をクリックします。
8. 接頭辞の文字列を含めたユーザー名 (例: **12345678|username**) およびパスワードを書き留めます。
   a. このユーザー名およびパスワードは、**registry.redhat.io** へのログインに使用されます。

注記

Token Information のページには、認証トークンの使用方法を説明したタブがあります。たとえば、**Token Information** タブには、**12345678|username** フォーマットのユーザー名およびその下にパスワードの文字列が表示されます。

1.4.2. レジストリーサービスアカウントの変更

サービスアカウントを変更または削除することができます。**Registry Service Account** ページの表中の各認証トークン右側のポップアップメニューを使用して、その操作を行うことができます。

警告

トークンを再生成したり **サービスアカウント** を削除したりすると、そのトークンを用いて認証および **registry.redhat.io** からコンテンツを取得しているシステムに影響を及ぼします。

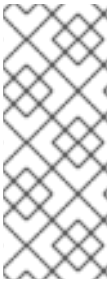
各機能の説明は以下のとおりです。

- **Regenerate Token:** 許可されたユーザーは、**サービスアカウント** に関連付けられたパスワードをリセットすることができます。
  注記: サービスアカウント のユーザー名を変更することはできません。
- **Update Description:** 許可されたユーザーは、**サービスアカウント** の説明を更新することができます。
- **Delete Account:** 許可されたユーザーは、**サービスアカウント** を削除することができます。

関連情報

- Red Hat コンテナーレジストリーの認証
- Authentication enabled Red Hat registry

1.4.3. 3scale テンプレートのインポート



注記

- ワイルドカードルートは、3scale 2.6 の時点で 廃止されています。
  - この機能は、バックグラウンドで Zync により処理されます。
- API プロバイダーが作成、更新、または削除されると、これらの変更が自動的にルートに反映されます。

3scale テンプレートを OpenShift クラスターにインポートするには、以下の手順を実施します。

手順

1. ターミナルセッションから、OpenShift にクラスター管理者としてログインします。

```
oc login
```

2. プロジェクトを選択するか新しいプロジェクトを作成します。

```
oc project <project_name>
```

```
oc new-project <project_name>
```

3. **oc new-app** コマンドを入力します。

a. **--file** オプションを使用して、ノードおよびエンタイトルメントの設定 でダウンロードした **amp.yml** ファイルへのパスを指定します。

b. **--param** オプションを使用して、**WILDCARD_DOMAIN** パラメーターに OpenShift クラスターのドメインを設定します。

```
oc new-app --file /opt/amp/templates/amp.yml --param WILDCARD_DOMAIN=
<WILDCARD_DOMAIN>
```

ターミナルには、マスターおよびテナント URL と、新たに作成された 3scale 管理ポータルのクレデンシャルが表示されます。この出力には以下の情報が含まれます。

- マスター管理者のユーザー名
- マスターのパスワード
- マスターのトークン情報
- テナントのユーザー名
- テナントのパスワード
- テナントのトークン情報

4. https://user-admin.3scale-project.example.com に admin/xXxXyz123 としてログインします。

```
* With parameters:

 * ADMIN_PASSWORD=xXxXyz123 # generated
 * ADMIN_USERNAME=admin
 * TENANT_NAME=user

 * MASTER_NAME=master
 * MASTER_USER=master
 * MASTER_PASSWORD=xXxXyz123 # generated

--> Success
Access your application via route 'user-admin.3scale-project.example.com'
Access your application via route 'master-admin.3scale-project.example.com'
Access your application via route 'backend-user.3scale-project.example.com'
Access your application via route 'user.3scale-project.example.com'
Access your application via route 'api-user-apicast-staging.3scale-project.example.com'
Access your application via route 'api-user-apicast-production.3scale-project.example.com'
```

5. 後で確認できるようにするため、詳細を書き留めておきます。

6. 以下のコマンドが返されると、OpenShift での 3scale デプロイメントが成功しています。

```
oc wait --for=condition=available --timeout=-1s $(oc get dc --output=name)
```

注記

OpenShift への 3scale のデプロイメントに成功すると、ログインクレデンシャルが機能します。

1.4.4. 管理ポータルの URL の取得

テンプレートを使用して 3scale をデプロイすると、固定 URL (**3scale-admin.${wildcardDomain}**) のデフォルトテナントが作成されます。

3scale の Dashboard には、テナントの新しいポータル URL が表示されます。たとえば、**<wildCardDomain>** が **3scale-project.example.com** の場合、管理ポータル URL は **https://3scale-admin.3scale-project.example.com** となります。

wildcardDomain は、インストール中に指定した **<wildCardDomain>** パラメーターです。以下のコマンドを使用し、ブラウザーでこの一意の URL を開きます。

```
xdg-open https://3scale-admin.3scale-project.example.com
```

オプションとして、**マスターポータル URL** (master.${wildcardDomain}) に新しいテナントを作成できます。

1.4.5. Amazon Simple Storage Service を使用した 3scale のデプロイ

Amazon Simple Storage Service (Amazon S3) を使用した 3scale のデプロイは任意の手順です。以下の手順を使用して、Amazon S3 で 3scale をデプロイします。

手順

1. amp-s3.yml ダウンロードします。
2. ターミナルセッションから OpenShift にログインします。

```
oc login
```

3. プロジェクトを選択するか新しいプロジェクトを作成します。

```
oc project <project_name>
```

または

```
oc new-project <project_name>
```

1. oc new-app コマンドを入力します。
   - **--file** オプションを使用して、**amp-s3.yml** ファイルへのパスを指定します。
   - **--param** オプションを以下の値を指定します。
   - **WILDCARD_DOMAIN**: パラメーターは OpenShift クラスターのドメインに設定されます。
   - **AWS_BUCKET**: ターゲットバケット名に置き換えます。
   - **AWS_ACCESS_KEY_ID**: AWS 認証情報 ID に置き換えます。
   - **AWS_SECRET_ACCESS_KEY**: AWS 認証情報 KEY に置き換えます。
   - **AWS_REGION: with the AWS**: リージョンに置き換えます。

- **AWS_HOSTNAME**: Amazon エンドポイント: AWS S3 と互換性のあるプロバイダーエンドポイントのホスト名。
- **AWS_PROTOCOL**: デフォルト: HTTPS - AWS S3 と互換性のあるプロバイダーエンドポイントプロトコル。
- **AWS_PATH_STYLE**: デフォルト: **false** - **true** に設定すると、バケット名は常にリクエスト URI に残り、サブドメインとしてホストに移動されません。
- 管理ポータルでカスタム名を設定するには **--param** オプションを指定して **TENANT_NAME** パラメーターを指定します。省略した場合、デフォルトは 3scale に設定されます。

```
oc new-app --file /path/to/amp-s3.yml \
 --param WILDCARD_DOMAIN=<a-domain-that-resolves-to-your-ocp-cluster.com> \
 --param TENANT_NAME=3scale \
 --param AWS_ACCESS_KEY_ID=<your-aws-access-key-id> \
 --param AWS_SECRET_ACCESS_KEY=<your-aws-access-key-secret> \
 --param AWS_BUCKET=<your-target-bucket-name> \
 --param AWS_REGION=<your-aws-bucket-region> \
 --param FILE_UPLOAD_STORAGE=s3
```

ターミナルには、マスターおよびテナント URL と、新たに作成された 3scale 管理ポータルの認証情報が表示されます。この出力には以下の情報が含まれます。

- マスター管理者のユーザー名
- マスターのパスワード
- マスターのトークン情報
- テナントのユーザー名
- テナントのパスワード
- テナントのトークン情報

2. https://user-admin.3scale-project.example.com に admin/xXxXyz123 としてログインします。

```
...

* With parameters:
 * ADMIN_PASSWORD=xXxXyz123 # generated
 * ADMIN_USERNAME=admin
 * TENANT_NAME=user
 ...

 * MASTER_NAME=master
 * MASTER_USER=master
 * MASTER_PASSWORD=xXxXyz123 # generated
 ...

--> Success
Access your application via route 'user-admin.3scale-project.example.com'
Access your application via route 'master-admin.3scale-project.example.com'
Access your application via route 'backend-user.3scale-project.example.com'
Access your application via route 'user.3scale-project.example.com'
```

```
Access your application via route 'api-user-apicast-staging.3scale-project.example.com'
Access your application via route 'api-user-apicast-production.3scale-project.example.com'
Access your application via route 'apicast-wildcard.3scale-project.example.com'

...
```

3. 後で確認できるようにするため、詳細を書き留めておきます。
4. 以下のコマンドが返されると、OpenShift での 3scale デプロイメントが成功しています。

```
oc wait --for=condition=available --timeout=-1s $(oc get dc --output=name)
```

注記

OpenShift への 3scale のデプロイメントに成功すると、ログインクレデンシャルが機能します。

1.4.6. PostgreSQL を使用した 3scale のデプロイ

PostgreSQL を使用した 3scale のデプロイは、任意の手順です。以下の手順を使用して、PostgreSQL で 3scale をデプロイします。

手順

1. amp-postgresql.yml をダウンロードします。
2. ターミナルセッションから OpenShift にログインします。

```
oc login
```

3. プロジェクトを選択するか新しいプロジェクトを作成します。

```
oc project <project_name>
```

または

```
oc new-project <project_name>
```

1. oc new-app コマンドを入力します。
   - **--file** オプションを使用して、**amp-postgresql.yml** ファイルへのパスを指定します。
   - **--param** オプションを以下の値を指定します。
   - **WILDCARD_DOMAIN**: パラメーターは OpenShift クラスターのドメインに設定されます。
   - 管理ポータルでカスタム名を設定するには **--param** オプションを指定して **TENANT_NAME** パラメーターを指定します。省略した場合、デフォルトは 3scale に設定されます。

```
oc new-app --file /path/to/amp-postgresql.yml \
 --param WILDCARD_DOMAIN=<a-domain-that-resolves-to-your-ocp-cluster.com> \
 --param TENANT_NAME=3scale \
```

ターミナルには、マスターおよびテナント URL と、新たに作成された 3scale 管理ポータルの認証情報が表示されます。この出力には以下の情報が含まれます。

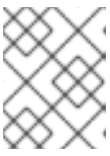
- マスター管理者のユーザー名
- マスターのパスワード
- マスターのトークン情報
- テナントのユーザー名
- テナントのパスワード
- テナントのトークン情報

2. https://user-admin.3scale-project.example.com に admin/xXxXyz123 としてログインします。

```
...

* With parameters:
 * ADMIN_PASSWORD=xXxXyz123 # generated
 * ADMIN_USERNAME=admin
 * TENANT_NAME=user
 ...

 * MASTER_NAME=master
 * MASTER_USER=master
 * MASTER_PASSWORD=xXxXyz123 # generated
 ...

--> Success
Access your application via route 'user-admin.3scale-project.example.com'
Access your application via route 'master-admin.3scale-project.example.com'
Access your application via route 'backend-user.3scale-project.example.com'
Access your application via route 'user.3scale-project.example.com'
Access your application via route 'api-user-apicast-staging.3scale-project.example.com'
Access your application via route 'api-user-apicast-production.3scale-project.example.com'
Access your application via route 'apicast-wildcard.3scale-project.example.com'

...
```

3. 後で確認できるようにするため、詳細を書き留めておきます。
4. 以下のコマンドが返されると、OpenShift での 3scale デプロイメントが成功しています。

```
oc wait --for=condition=available --timeout=-1s $(oc get dc --output=name)
```



注記

OpenShift への 3scale のデプロイメントに成功すると、ログインとクレデンシャルが機能します。

1.4.7. SMTP 変数の設定 (任意)

OpenShift は 通知の送信 および 新規ユーザーの招待 に電子メールを使用します。この機能を使用する場合は、独自の SMTP サーバーを提供し、**system-smtp** シークレットで SMTP 変数を設定する必要があります。

system-smtp シークレットで SMTP 変数を設定するには、以下の手順を実行します。

手順

1. OpenShift にログインしていない場合はログインします。

```
oc login
```

   a. **oc patch** コマンドを使用して **secret** タイプを指定し (**system-smtp** はシークレット名)、続いて **-p** オプションを指定し、以下の変数に対して JSON 形式で新しい値を指定します。

変数	説明
address	リモートメールサーバーをリレーとして指定できます。
username	メールサーバーのユーザー名を指定します。
password	メールサーバーのパスワードを指定します。
domain	HELO ドメインを指定します。
port	メールサーバーが新しい接続をリッスンするポートを指定します。
authentication	メールサーバーの認証タイプを指定します。指定できる値は **plain** (パスワードをクリアテキストで送信)、**login** (パスワードを Base64 エンコードで送信)、または **cram_md5** (ハッシュ関数に Message Digest 5 アルゴリズムを使用し認証情報を交換) です。
openssl.verify.mode	TLS の使用時に OpenSSL が証明書をチェックする方法を指定します。使用できる値は **none** または **peer** です。

例

```
oc patch secret system-smtp -p '{"stringData":{"address":"<your_address>"}}'
oc patch secret system-smtp -p '{"stringData":{"username":"<your_username>"}}'
oc patch secret system-smtp -p '{"stringData":{"password":"<your_password>"}}'
```

2. secret 変数を設定した後、**system-app** および **system-sidekiq** Pod を再デプロイします。

```
oc rollout latest dc/system-app
oc rollout latest dc/system-sidekiq
```

3. ロールアウトのステータスを表示し、読み込みが完了したことを確認します。

```
oc rollout status dc/system-app
oc rollout status dc/system-sidekiq
```

1.5. 3SCALE テンプレートのパラメーター

テンプレートパラメーターにより、デプロイメント中およびデプロイメント後の 3scale **amp.yml** テンプレートの環境変数を設定します。

名前	説明	デフォルト値	必須/任意
APP_LABEL	オブジェクトアプリのラベルに使用されます。	**3scale-api-management**	必須
ZYNC_DATABASE_PASSWORD	PostgreSQL 接続ユーザーのパスワード。指定のない場合は無作為に生成されます。	該当なし	必須
ZYNC_SECRET_KEY_BASE	Zync の秘密鍵ベース。指定のない場合は無作為に生成されます。	該当なし	必須
ZYNC_AUTHENTICATION_TOKEN	Zync の認証トークン。指定のない場合は無作為に生成されます。	該当なし	必須
AMP_RELEASE	3scale リリースタグ	**2.8.0**	必須
ADMIN_PASSWORD	無作為に生成される 3scale 管理者アカウントのパスワード	該当なし	必須
ADMIN_USERNAME	3scale 管理者アカウントのユーザー名	**admin**	必須
APICAST_ACCESS_TOKEN	APIcast が設定のダウンロードに使用する読み取り専用アクセストークン	該当なし	必須
ADMIN_ACCESS_TOKEN	すべての API をスコープとし、書き込みアクセス権限が設定された管理者アクセストークン	該当なし	任意

名前	説明	デフォルト値	必須/任意
WILDCARD_DOMAIN	ワイルドカードルートのルートドメイン。たとえば、ルートドメイン **example.com** は **3scale-admin.example.com** を生成します。	該当なし	必須
TENANT_NAME	ルート下のテナント名。-admin 接尾辞を付けて管理ポータルにアクセスすることができます。	**3scale**	必須
MYSQL_USER	データベースのアクセスに使用される MySQL ユーザーのユーザー名	**mysql**	必須
MYSQL_PASSWORD	MySQL ユーザーのパスワード	該当なし	必須
MYSQL_DATABASE	アクセスされた MySQL データベースの名前	**system**	必須
MYSQL_ROOT_PASSWORD	Root ユーザーのパスワード	該当なし	必須
SYSTEM_BACKEND_USERNAME	内部 3scale api auth の内部 3scale API ユーザー名	**3scale_api_user**	必須
SYSTEM_BACKEND_PASSWORD	内部 3scale api auth の内部 3scale API パスワード	該当なし	必須
REDIS_IMAGE	使用する Redis イメージ	**registry.redhat.io/rhscl/redis-5-rhel7:5.0**	必須
MYSQL_IMAGE	使用する Mysql イメージ	**registry.redhat.io/rhscl/mysql-57-rhel7:5.7**	必須
MEMCACHED_IMAGE	使用する Memcached イメージ	**registry.redhat.io/3scale-amp2/memcached-rhel7:3scale2.8**	必須
POSTGRESQL_IMAGE	使用する Postgresql イメージ	**registry.redhat.io/rhscl/postgresql-10-rhel7**	必須

名前	説明	デフォルト値	必須/任意
AMP_SYSTEM_IMAGE	使用する 3scale システムイメージ	**registry.redhat.io/3scale-amp2/system-rhel7:3scale2.8**	必須
AMP_BACKEND_IMAGE	使用する 3scale バックエンドイメージ	**registry.redhat.io/3scale-amp2/backend-rhel7:3scale2.8**	必須
AMP_APICAST_IMAGE	使用する 3scale APIcast イメージ	**registry.redhat.io/3scale-amp2/apicast-gateway-rhel8:3scale2.8**	必須
AMP_ZYNC_IMAGE	使用する 3scale Zync イメージ	**registry.redhat.io/3scale-amp2/zync-rhel7:3scale2.8**	必須
SYSTEM_BACKEND_SHARED_SECRET	バックエンドからシステムにイベントをインポートするための共有シークレット	該当なし	必須
SYSTEM_APP_SECRET_KEY_BASE	システムアプリケーションの秘密鍵ベース	該当なし	必須
APICAST_MANAGEMENT_API	APIcast Management API のスコープ。disable、status、または debug を設定できます。ヘルスチェックには最低でも status が必要です。	**status**	任意
APICAST_OPENSSL_VERIFY	設定のダウンロード時に OpenSSL ピア検証を有効または無効にします。true または false を設定できます。	**false**	任意
APICAST_RESPONSE_CODES	APIcast のロギングレスポンスコードを有効にします。	true	任意
APICAST_REGISTRY_URL	APIcast ポリシーの場所に解決する URL	**http://apicast-staging:8090/policies**	必須

名前	説明	デフォルト値	必須/任意
MASTER_USER	マスター管理者アカウントのユーザー名	**master**	必須
MASTER_NAME	マスター管理ポータルのサブドメイン値。-**master** 接尾辞が付けられます。	**master**	必須
MASTER_PASSWORD	無作為に生成されるマスター管理者のパスワード	該当なし	必須
MASTER_ACCESS_TOKEN	API 呼び出しのマスターレベル権限が設定されたトークン	該当なし	必須
IMAGESTREAM_TAG_IMPORT_INSECURE	イメージのインポート中にサーバーが証明書の検証を回避できる、または HTTP 経由で直接接続できる場合は、true を設定します。	**false**	必須

1.6. OPENSHIFT 上での 3SCALE と APICAST の使用

ホスト型 3scale および OpenShift Container Platform におけるオンプレミスインストールでは、API Manager を使用して APIcast を利用できます。両設定で、設定手順は異なります。

本セクションでは、OpenShift で API Manager を使用して APIcast をデプロイする方法を説明します。

- 3scale が含まれる既存 OpenShift クラスターでの APIcast テンプレートのデプロイ
- 異なる OpenShift クラスターからの APIcast への接続
- Embedded APIcast のデフォルト動作の変更
- 内部サービスルートを介した、単一 OpenShift クラスター上の複数 APIcast デプロイメントの接続
- 他のデプロイメント上の APIcast の接続

1.6.1. 3scale が含まれる既存 OpenShift クラスターでの APIcast テンプレートのデプロイ

3scale OpenShift テンプレートには Embedded APIcast が 2 つデフォルトで含まれています。より多くの API ゲートウェイが必要な場合や、別の APIcast デプロイメントが必要な場合は、追加の APIcast テンプレートを OpenShift クラスターにデプロイすることができます。

追加の API ゲートウェイを OpenShift クラスターにデプロイするには、以下の手順を実施します。

手順

1. 以下の設定で アクセストークン を作成します。
   - スコープ: Account Management API
   - アクセス権限: 読み取り専用
2. APIcast クラスターにログインします。

```
oc login
```

3. APIcast が 3scale と通信できるようにするシークレットを作成します。3scale デプロイメントのアクセストークン、テナント名、およびワイルドカードドメインと共に、**create secret** および **apicast-configuration-url-secret** を指定します。

```
oc create secret generic apicast-configuration-url-secret --from-
literal=password=https://<ACCESS_TOKEN>@<TENANT_NAME>-admin.
<WILDCARD_DOMAIN>
```

注記

TENANT_NAME は、管理ポータルにアクセスすることのできるルート下の名前です。**TENANT_NAME** のデフォルト値は **3scale** です。3scale デプロイメントでカスタム値を使用した場合は、ここでもその値を使用する必要があります。

4. **--file** オプションで **apicast.yml** ファイルを指定して、**oc new-app** コマンドを使用して APIcast テンプレートをインポートします。

```
oc new-app --file /opt/amp/templates/apicast.yml
```

注記

ノードおよびエンタイトルメントの設定 で説明するように、最初に APIcast テンプレートをインストールします。

1.6.2. 異なる OpenShift クラスターからの APIcast への接続

3scale クラスター外部の別の OpenShift クラスターに APIcast をデプロイする場合は、パブリックルート経由で接続する必要があります。

手順

1. 以下の設定で アクセストークン を作成します。
   - スコープ: Account Management API
   - アクセス権限: 読み取り専用
2. APIcast クラスターにログインします。

```
oc login
```

3. APIcast が 3scale と通信できるようにするシークレットを作成します。3scale デプロイメントのアクセストークン、テナント名、およびワイルドカードドメインと共に、**create secret** および **apicast-configuration-url-secret** を指定します。

```
oc create secret generic apicast-configuration-url-secret --from-
literal=password=https://<ACCESS_TOKEN>@<TENANT_NAME>-admin.
<WILDCARD_DOMAIN>
```

注記

TENANT_NAME は、管理ポータルにアクセスすることのできるルート下の名前です。**TENANT_NAME** のデフォルト値は **3scale** です。3scale デプロイメントでカスタム値を使用した場合は、その値を使用する必要があります。

4. **oc new-app** コマンドで、別の OpenShift クラスターに APIcast をデプロイします。 **--file** オプションで **apicast.yml** ファイルへのパスを指定します。

```
oc new-app --file /path/to/file/apicast.yml
```

1.6.3. Embedded APIcast のデフォルト動作の変更

外部の APIcast デプロイメントでは、APIcast OpenShift テンプレートの テンプレートパラメーターを変更する ことにより、デフォルトの動作を変更できます。

Embedded APIcast デプロイメントでは、3scale および APIcast は単一のテンプレートからデプロイされます。Embedded APIcast デプロイメントのデフォルト動作を変更する場合は、デプロイメントの後に環境変数を編集する必要があります。

1.6.4. 内部サービスルートを介した、単一 OpenShift クラスター上の複数 APIcast デプロイメントの接続

同じ OpenShift クラスターに複数の APIcast ゲートウェイをデプロイする場合、デフォルトの外部ルート設定ではなく、バックエンドリスナーサービスを介して内部ルートを使用して接続するよう設定できます。

内部サービスルート経由で接続するには OpenShift Software-Defined Networking (SDN) プラグインがインストールされている必要があります。接続方法は、インストールされた SDN によって異なります。

ovs-subnet

ovs-subnet OpenShift SDN プラグインを使用している場合は、以下の手順を実施して内部ルート経由で接続します。

手順

1. OpenShift クラスターにログインしていない場合はログインします。

```
oc login
```

2. 以下のコマンドを入力し、**backend-listener** ルートの URL を表示します。

```
oc get route backend
```

3. **apicast.yml** へのパスを指定して **oc new-app** コマンドを入力します。

```
oc new-app -f apicast.yml
```

ovs-multitenant

ovs-multitenant OpenShift SDN プラグインを使用している場合は、以下の手順を実施して内部ルート経由で接続します。

手順

1. OpenShift クラスターにログインしていない場合はログインします。

```
oc login
```

2. 管理者として、**oadm** コマンドに **pod-network** および **join-projects** オプションを指定し、両方のプロジェクト間の通信を設定します。

```
oadm pod-network join-projects --to=<3SCALE_PROJECT> <APICAST_PROJECT>
```

3. 以下のコマンドを入力し、**backend-listener** ルートの URL を表示します。

```
oc get route backend
```

4. **apicast.yml** へのパスを指定して **oc new-app** コマンドを入力します。

```
oc new-app -f apicast.yml
```

関連情報

OpenShift SDN およびプロジェクトネットワークの分離についての情報は、OpenShift Container Platform ネットワークの OpenShift SDN を参照してください。

1.6.5. 他のデプロイメント上の APIcast の接続

APIcast を Docker にデプロイする場合には、**THREESCALE_PORTAL_ENDPOINT** パラメーターを OpenShift 上にデプロイした 3scale 管理ポータル の URL およびアクセストークンに設定することで、APIcast を OpenShift 上にデプロイした 3scale に接続することができます。この場合、**BACKEND_ENDPOINT_OVERRIDE** パラメーターを設定する必要はありません。

関連情報

詳細については、Docker コンテナー環境への APIcast のデプロイ を参照してください。

1.7. OPERATOR を使用した 3SCALE のデプロイ

本セクションでは、**APIManager** カスタムリソースを使用して、3scale operator 経由で 3scale ソリューションをインストールおよびデプロイする方法を説明します。

注記

- ワイルドカードルートは、3scale 2.6 以降 廃止されています。
  - この機能は、バックグラウンドで Zync により処理されます。
- API プロバイダーが作成、更新、または削除されると、これらの変更が自動的にルートに反映されます。

前提条件

- コンテナーイメージの registry.redhat.io を使用した認証
- 先に OpenShift への 3scale operator のインストール の記載の手順に従って Operator を使用して 3scale をデプロイする。
- OpenShift Container Platform 4
  - OpenShift クラスターの管理者権限を持つユーザーアカウント
  - **注記:** OCP 4 は、operator を使用した 3scale のデプロイメントのみをサポートしています。
  - サポート対象設定の情報については、Red Hat 3scale API Management のサポート対象設定 のアーティクルを参照してください。

以下の手順に従って、operator を使用して 3scale をデプロイします。

- APIManager カスタムリソースのデプロイ
- APIManager 管理ポータルとマスター管理ポータルの認証情報を取得する
- 管理ポータルの URL の取得
- operator を使用した 3scale での高可用性

1.7.1. APIManager カスタムリソースのデプロイ

APIManager カスタムリソースをデプロイすると、operator がプロセスを開始し、そこから 3scale ソリューションがデプロイされます。

手順

1. **Catalog > Installed Operators** の順にクリックします。
   a. **Installed Operators** のリストで、**3scale Operator** をクリックします。
2. **API Manager** タブをクリックします。
3. **Create APIManager** をクリックします。
4. サンプルのコンテンツを消去して以下の **YAML** 定義をエディターに追加し、続いて **Create** をクリックします。
   - 3scale 2.8 より前のバージョンでは、**highAvailability** フィールドを **true** に設定してレプリカの自動追加を設定できるようになりました。3scale 2.8 以降、レプリカの追加は以下の例のように APIManager CR の replicas フィールドによって制御されます。

注記

wildcardDomain パラメーターには、有効な DNS ドメインである、IP アドレスに対して解決する任意の名前を指定できます。

- 最小要件のある APIManager CR:

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: apimanager-sample
spec:
  wildcardDomain: example.com
```

- レプリカが設定された APIManager CR:

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: apimanager-sample
spec:
  wildcardDomain: apimanager-sample
  system:
    appSpec:
      replicas: 1
    sidekiqSpec:
      replicas: 1
  zync:
    appSpec:
      replicas: 1
    queSpec:
      replicas: 1
  backend:
    cronSpec:
      replicas: 1
    listenerSpec:
      replicas: 1
    workerSpec:
      replicas: 1
  apicast:
    productionSpec:
      replicas: 1
    stagingSpec:
      replicas: 1
  wildcardDomain: example.com
```

1.7.2. APIManager 管理ポータルとマスター管理ポータルの認証情報を取得する

Operator ベースのデプロイ後に 3scale 管理ポータルまたはマスター管理ポータルのいずれかにログインするには、個別のポータルごとに認証情報が必要です。これらの認証情報を取得するには:

1. 次のコマンドを実行して、管理ポータルの認証情報を取得します。

```
oc get secret system-seed -o json | jq -r .data.ADMIN_USER | base64 -d
oc get secret system-seed -o json | jq -r .data.ADMIN_PASSWORD | base64 -d
```

a. Admin Portal 管理者としてログインして、これらの認証情報が機能していることを確認します。

2. 次のコマンドを実行して、マスター管理ポータルの認証情報を取得します。

```
oc get secret system-seed -o json | jq -r .data.MASTER_USER | base64 -d
oc get secret system-seed -o json | jq -r .data.MASTER_PASSWORD | base64 -d
```

a. マスター管理ポータル管理者としてログインして、これらの認証情報が機能していることを確認します。

関連情報

APIManager フィールドに関する詳細は、参考のドキュメント を参照してください。

1.7.3. 管理ポータルの URL の取得

operator を使用して 3scale をデプロイすると、固定 URL (**3scale-admin.${wildcardDomain}**) のデフォルトテナントが作成されます。

3scale の Dashboard には、テナントの新しいポータル URL が表示されます。たとえば、**<wildCardDomain>** が **3scale-project.example.com** の場合、管理ポータル URL は **https://3scale-admin.3scale-project.example.com** となります。

wildcardDomain は、インストール中に指定した **<wildCardDomain>** パラメーターです。以下のコマンドを使用し、ブラウザーでこの一意の URL を開きます。

```
xdg-open https://3scale-admin.3scale-project.example.com
```

オプションとして、**マスターポータル URL** (**master.${wildcardDomain}**) に新しいテナントを作成できます。

1.7.4. operator を使用した 3scale での高可用性

operator を使用した 3scale での高可用性 (HA) は、たとえば 1 つ以上のデータベースに障害が発生した場合に、中断なしのアップタイムを提供することを目的としています。

注記

.spec.highAvailability.enabled は外部データベースのみを対象としています。

3scale の operator ベースのデプロイメントで HA が必要な場合は、以下の点に注意してください。

- 3scale の重要なデータベース (具体的にはシステムデータベース、システム redis、およびバックエンド redis) を外部にデプロイおよび設定します。これらのデータベースを高可用性の設定でデプロイおよび設定するようにしてください。
- 3scale のデータベースへの接続エンドポイントを指定する際に、対応する Kubernetes Secret を事前作成します。
  - 詳細は、外部データベースモードでのインストール を参照してください。

    - データベース以外のデプロイメント設定についての詳細は、Enabling Pod Disruption Budgets を参照してください。

- APIManager CR をデプロイする際に **.spec.highAvailability.enabled** 属性を **true** に設定し、システムデータベース、システム redis、およびバックエンド redis 等の重要なデータベースの外部データベースモードを有効にします。

さらに zync データベースを高可用性にして、再起動時のキュージョブデータを失う可能性をなくす場合は、以下の点に注意してください。

- zync データベースを外部でデプロイおよび設定します。このデータベースを高可用性の設定でデプロイおよび設定するようにしてください。
- 3scale の zync データベースへの接続エンドポイントを指定する際に、対応する Kubernetes Secret を事前作成します。
    - 詳細は、Zync データベースシークレット を参照してください。
    - **spec.highAvailability.externalZyncDatabaseEnabled** 属性を true に設定して 3scale をデプロイし、zync データベースを外部データベースとして指定します。

1.8. OPERATOR を使用した OPENSHIFT への 3SCALE のデプロイメント設定オプション

本セクションでは、operator を使用した OpenShift への Red Hat 3scale API Management のデプロイメント設定オプションについて説明します。

前提条件

- コンテナーイメージの registry.redhat.io を使用した認証
- 先に OpenShift への 3scale operator のインストール の記載の手順に従って Operator を使用して 3scale をデプロイする。
- OpenShift Container Platform 4
    - OpenShift クラスターの管理者権限を持つユーザーアカウント

1.8.1. デフォルトのデプロイメント設定

デフォルトでは、以下のデプロイメント設定オプションが適用されます。

- コンテナーには、Kubernetes によるリソースの制限およびリクエスト が適用されます。
    - これにより、最低限のパフォーマンスレベルが確保されます。
    - また、外部サービスおよびソリューションの割り当てを可能にするために、リソースを制限します。
- 内部データベースのデプロイメント
- ファイルストレージは、永続ボリューム (PV) がベースになります。
    - ボリュームの 1 つには、読み取り、書き込み、実行 (RWX) アクセスモードが必要です。

    - OpenShift は、リクエストに応じてこれらを提供するように設定されている必要があります。

- MySQL を内部リレーショナルデータベースとしてデプロイします。

デフォルトの設定オプションは、お客様による概念実証 (PoC) または評価用途に適しています。

1 つ、複数、またはすべてのデフォルト設定オプションを、**APIManager** カスタムリソースの特定フィールドの値で上書きすることができます。3scale operator では可能なすべての組み合わせが許可されますが、テンプレートでは固定のデプロイメントプロファイルが許可されます。たとえば、3scale operator を使用すると、評価モードおよび外部データベースモードで 3scale をデプロイすることができます。テンプレートでは、この特定のデプロイメント設定は許可されません。テンプレートは、最も一般的な設定オプションでしか利用することができません。

1.8.2. 評価モードでのインストール

評価モードでのインストールの場合、コンテナーには Kubernetes によるリソースの制限およびリクエスト が適用されません。以下に例を示します。

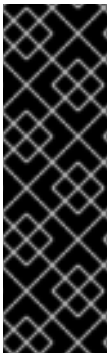
- メモリーのフットプリントが小さい。
- 起動が高速である。
- ノートパソコンで実行可能である。
- プリセールス/セールスでのデモに適する。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
spec:
  wildcardDomain: lvh.me
  resourceRequirementsEnabled: false
```

詳細は、APIManager カスタムリソースを参照してください。

1.8.3. 外部データベースモードでのインストール

外部データベースモードでのインストールは、高可用性 (HA) が必須な場合や専用のデータベースを再利用する場合の実稼働環境での使用に適しています。



重要

3scale の外部データベースインストールモードを有効にすると、以下のデータベースがすべて外部化されます。

- **backend-redis**
- **system-redis**
- **system-database** (**mysql**、**postgresql**、または **oracle**)

3scale 2.8 以降は、以下のデータベースバージョンとの組み合わせでテストを行いサポートが提供されます。

データベース	バージョン
Redis	5.0
MySQL	5.7
PostgreSQL	10.6

3scale をデプロイするために **APIManager カスタムリソース** を作成する前に、OpenShift シークレットを使用して以下に示す外部データベースの接続設定を提供する必要があります。

1.8.3.1. バックエンド Redis シークレット

2 つの外部 Redis インスタンスをデプロイし、以下の例に示すように接続設定を入力します。

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-redis
stringData:
  REDIS_STORAGE_URL: "redis://backend-redis-storage"
  REDIS_STORAGE_SENTINEL_HOSTS: "redis://sentinel-0.example.com:26379,redis://sentinel-
1.example.com:26379, redis://sentinel-2.example.com:26379"
  REDIS_STORAGE_SENTINEL_ROLE: "master"
  REDIS_QUEUES_URL: "redis://backend-redis-queues"
  REDIS_QUEUES_SENTINEL_HOSTS: "redis://sentinel-0.example.com:26379,redis://sentinel-
1.example.com:26379, redis://sentinel-2.example.com:26379"
  REDIS_QUEUES_SENTINEL_ROLE: "master"
type: Opaque
```

シークレット 名は **backend-redis** にする必要があります。

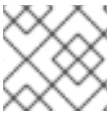
1.8.3.2. システム Redis シークレット

2 つの外部 Redis インスタンスをデプロイし、以下の例に示すように接続設定を入力します。

```
apiVersion: v1
kind: Secret
metadata:
  name: system-redis
stringData:
  URL: "redis://system-redis"
  SENTINEL_HOSTS: "redis://sentinel-0.example.com:26379,redis://sentinel-1.example.com:26379,
redis://sentinel-2.example.com:26379"
  SENTINEL_ROLE: "master"
  NAMESPACE: ""
  MESSAGE_BUS_URL: "redis://system-redis-messagebus"
  MESSAGE_BUS_SENTINEL_HOSTS: "redis://sentinel-0.example.com:26379,redis://sentinel-
1.example.com:26379, redis://sentinel-2.example.com:26379"
  MESSAGE_BUS_SENTINEL_ROLE: "master"
  MESSAGE_BUS_NAMESPACE: ""
type: Opaque
```

シークレット 名は **system-redis** にする必要があります。

1.8.3.3. システムデータベースシークレット



注記

シークレット 名は **system-database** にする必要があります。

3scale をデプロイする場合には、システムデータベースに 3 つの代替手段があります。代替手段に関連のシークレットごとに、異なる属性と値を設定します。

- MySQL
- PostgreSQL
- Oracle データベース

MySQL、PostgreSQL、または Oracle Database のシステムデータベースシークレットをデプロイするには、以下の例のように接続設定を入力します。

MySQL システムデータベースシークレット

```
apiVersion: v1
kind: Secret
metadata:
  name: system-database
stringData:
  URL: "mysql2://{DB_USER}:{DB_PASSWORD}@{DB_HOST}:{DB_PORT}/{DB_NAME}"
type: Opaque
```

PostgreSQL システムデータベースシークレット

```
apiVersion: v1
kind: Secret
metadata:
  name: system-database
stringData:
  URL: "postgresql://{DB_USER}:{DB_PASSWORD}@{DB_HOST}:{DB_PORT}/{DB_NAME}"
type: Opaque
```

Oracle システムデータベースシークレット

```
apiVersion: v1
kind: Secret
metadata:
  name: system-database
stringData:
  URL: "oracle-enhanced://{DB_USER}:{DB_PASSWORD}@{DB_HOST}:{DB_PORT}/{DB_NAME}"
  ORACLE_SYSTEM_PASSWORD: "{SYSTEM_PASSWORD}"
type: Opaque
```

1.8.3.4. Zync データベースシークレット

zync データベースの設定において、HighAvailability が有効で、**externalZyncDatabaseEnabled** フィールドも有効になっている場合、ユーザーは **zync** という名前のシークレットを事前に作成する必要があります。次に、**DATABASE_URL** および **DATABASE_PASSWORD** フィールドに外部データベースを参照する値を設定して、**zync** を設定します。外部データベースは高可用性モードである必要があります。以下の例を参照してください。

```
apiVersion: v1
kind: Secret
metadata:
  name: zync
stringData:
  DATABASE_URL: postgresql://<zync-db-user>:<zync-db-password>@<zync-db-host>:<zync-db-port>/zync_production
  ZYNC_DATABASE_PASSWORD: <zync-db-password>
type: Opaque
```

1.8.3.5. 3scale をデプロイするための APIManager カスタムリソース

注記

- **highAvailability** を有効化する場合、**backend-redis**、**system-redis**、および **system-database** シークレットを事前に作成する必要があります。
- **highAvailability** と **externalZyncDatabaseEnabled** フィールドを一緒に有効にする場合は、zync データベースシークレットを事前に作成する必要があります。
  - **system-database** の場合、外部化するデータベースのタイプを 1 つのみ選択します。

APIManager カスタムリソースの設定は、選択したデータベースが 3scale デプロイメントの外部にあるかどうかによって異なります。

バックエンド Redis、システム Redis、およびシステムデータベースが 3scale の外部になる場合、**APIManager** カスタムリソースでは **highAvailability** を **true** に設定する必要があります。以下の例を参照してください。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
spec:
  wildcardDomain: lvh.me
  highAvailability:
    enabled: true
```

zync データベースが外部である場合、**APIManager** カスタムリソースでは **highAvailability** を **true** に設定し、**externalZyncDatabaseEnabled** も **true** に設定する必要があります。以下の例を参照してください。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
```

```
spec:
  wildcardDomain: lvh.me
  highAvailability:
    enabled: true
    externalZyncDatabaseEnabled: true
```

関連情報

- Backend redis secret
- システムデータベースシークレット
- APIManager HighAvailabilitySpec
- Zync secret

1.8.4. Amazon Simple Storage Service を使用した 3scale ファイルストレージ のインストール

以下の例で、永続ボリューム要求 (PVC) の代わりに Amazon Simple Storage Service (Amazon S3) を使用した 3scale **ファイルストレージ** について説明します。

3scale をデプロイするために **APIManager** カスタムリソースを作成する前に、OpenShift シークレットを使用して S3 サービスの接続設定を提供する必要があります。

1.8.4.1. Amazon S3 シークレット

以下の例では、任意の **シークレット** 名を指定することができます。シークレット名が **APIManager** カスタムリソースで参照されるためです。

```
kind: Secret
metadata:
  creationTimestamp: null
  name: aws-auth
stringData:
  AWS_ACCESS_KEY_ID: 123456
  AWS_SECRET_ACCESS_KEY: 98765544
  AWS_BUCKET: mybucket.example.com
  AWS_REGION: eu-west-1
type: Opaque
```

最後に、3scale をデプロイするための **APIManager** カスタムリソースを作成します。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
  spec:
    wildcardDomain: lvh.me
    system:
      fileStorage:
        simpleStorageService:
          configurationSecretRef:
            name: aws-auth
```

注記

Amazon S3 リージョンおよび Amazon S3 バケット設定は、**APIManager** カスタムリソースに直接提供されます。Amazon S3 シークレット名は、**APIManager** カスタムリソースに直接提供されます。

詳細は、APIManager SystemS3Spec を参照してください。

1.8.5. PostgreSQL のインストール

MySQL 内部リレーショナルデータベースがデフォルトのデプロイメントです。このデプロイメント設定を上書きして、代わりに PostgreSQL を使用することができます。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
spec:
  wildcardDomain: lvh.me
  system:
    database:
      postgresql: {}
```

詳細は、APIManager DatabaseSpec を参照してください。

1.8.6. 調整

3scale をインストールしたら、3scale operator により、カスタムリソースからの特定パラメーターセットを更新してシステム設定オプションを変更することができます。変更は **ホットスワップ** により行われます。つまり、システムの停止やシャットダウンは発生しません。

APIManager カスタムリソース定義 (CRD) のパラメーターがすべて調整可能な訳ではありません。

調整可能なパラメーターのリストを以下に示します。

- 「リソース」
- 「バックエンドレプリカ」
- 「APIcast レプリカ」
- 「システムレプリカ」

1.8.6.1. リソース

すべての 3scale コンポーネントに対するリソースの制限およびリクエスト

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
spec:
  ResourceRequirementsEnabled: true/false
```

1.8.6.2. バックエンドレプリカ

バックエンド コンポーネントの Pod 数

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
spec:
  backend:
    listenerSpec:
      replicas: X
    workerSpec:
      replicas: Y
    cronSpec:
      replicas: Z
```

1.8.6.3. APIcast レプリカ

APIcast ステージングおよび実稼働環境コンポーネントの Pod 数

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
spec:
  apicast:
    productionSpec:
      replicas: X
    stagingSpec:
      replicas: Z
```

1.8.6.4. システムレプリカ

システム アプリケーションおよびシステム **sidekiq** コンポーネントの Pod 数

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
metadata:
  name: example-apimanager
spec:
  system:
    appSpec:
      replicas: X
    sidekiqSpec:
      replicas: Z
```

1.8.6.5. Zync レプリカ

Zync アプリケーションと que コンポーネントの Pod 数

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIManager
```

```
metadata:
  name: example-apimanager
spec:
  zync:
    appSpec:
      replicas: X
    queSpec:
      replicas: Z
```

1.9. 典型的な 3SCALE インストールの問題のトラブルシューティング

本セクションでは、典型的なインストールの問題と、その問題を解決するためのアドバイスについて説明します。

- 以前のデプロイメントがダーティーな永続ボリューム要求を残す
- 認証されたイメージレジストリーの認証情報が間違っているか、欠落している
- 誤って Docker レジストリーからプルされる
- 永続ボリュームがローカルでマウントされている場合の MySQL の権限の問題
- ロゴまたはイメージをアップロードできない
- OpenShift でテストコールが動作しない
- 3scale 以外のプロジェクトでの APIcast デプロイに失敗する

1.9.1. 以前のデプロイメントがダーティーな永続ボリューム要求を残す

問題

以前のデプロイメントがダーティーな永続ボリューム要求 (PVC) を残そうとするため、MySQL コンテナーの起動に失敗する。

原因

OpenShift のプロジェクトを削除しても、それに関連する PVC は消去されない。

解決方法

手順

1. **oc get pvc** コマンドを使用してエラーのある MySQL データが含まれる PVC を探します。

```
# oc get pvc
NAME                   STATUS    VOLUME    CAPACITY   ACCESSMODES   AGE
backend-redis-storage  Bound     vol003    100Gi      RWO,RWX       4d
mysql-storage          Bound     vol006    100Gi      RWO,RWX       4d
system-redis-storage   Bound     vol008    100Gi      RWO,RWX       4d
system-storage         Bound     vol004    100Gi      RWO,RWX       4d
```

2. OpenShift UI の **cancel deployment** をクリックして、system-mysql Pod のデプロイメントを停止します。

3. MySQL パス以下にあるものすべてを削除し、ボリュームをクリーンアップします。
4. 新たに **system-mysql** のデプロイメントを開始します。

1.9.2. 認証されたイメージレジストリーの認証情報が間違っているか、欠落している

問題

Pod が起動していません。ImageStreams に次のエラーが表示されます。

```
! error: Import failed (InternalError): ...unauthorized: Please login to the Red Hat Registry
```

原因

OpenShift 4.x に 3scale をインストールすると、ImageStreams が参照するイメージをプルできないため、OpenShift は Pod の起動に失敗します。これは、Pod が指しているレジストリーに対して認証できないために発生します。

解決方法

手順

1. 次のコマンドを入力して、コンテナーレジストリー認証の設定を確認します。

```
$ oc get secret
```

   - シークレットが存在する場合は、ターミナルに次の出力が表示されます。

```
threescale-registry-auth        kubernetes.io/dockerconfigjson        1        4m9s
```

   - ただし、出力が表示されない場合は、次の操作を行う必要があります。

2. レジストリーサービスアカウントの作成 中に以前に設定した認証情報を使用して、シークレットを作成します。
3. 提供されている **oc create secret** コマンドの **<your-registry-service-account-username>** および **<your-registry-service-account-password>** を置き換えて、OpenShift でのレジストリー認証の設定 の手順を使用します。
4. **APIManager** リソースと同じ名前空間で **threescale-registry-auth** シークレットを生成します。**<project-name>** 内で次を実行する必要があります。

```
oc project <project-name>
oc create secret docker-registry threescale-registry-auth \
  --docker-server=registry.redhat.io \
  --docker-username="<your-registry-service-account-username>" \
  --docker-password="<your-registry-service-account-password>"
  --docker-email="<email-address>"
```

5. **APIManager** リソースを削除して再作成します。

```
$ oc delete -f apimanager.yaml
apimanager.apps.3scale.net "example-apimanager" deleted
```

```
$ oc create -f apimanager.yaml
apimanager.apps.3scale.net/example-apimanager created
```

検証

1. 次のコマンドを入力して、デプロイのステータスが **Starting** または **Ready** であることを確認します。その後、Pod が以下を生成し始めます。

```
$ oc describe apimanager
(...)
Status:
  Deployments:
    Ready:
      apicast-staging
      system-memcache
      system-mysql
      system-redis
      zync
      zync-database
      zync-que
    Starting:
      apicast-production
      backend-cron
      backend-worker
      system-sidekiq
      system-sphinx
    Stopped:
      backend-listener
      backend-redis
      system-app
```

2. 以下のコマンドを実行して、各 Pod のステータスを確認します。

```
$ oc get pods
NAME                              READY   STATUS            RESTARTS   AGE
3scale-operator-66cc6d857b-sxhgm  1/1     Running           0          17h
apicast-production-1-deploy       1/1     Running           0          17m
apicast-production-1-pxkqm        0/1     Pending           0          17m
apicast-staging-1-dbwcw           1/1     Running           0          17m
apicast-staging-1-deploy          0/1     Completed         0          17m
backend-cron-1-deploy             1/1     Running           0          17m
```

1.9.3. 誤って Docker レジストリーからプルされる

問題

インストール中に以下のエラーが発生する。

```
svc/system-redis - 1EX.AMP.LE.IP:6379
  dc/system-redis deploys docker.io/rhscl/redis-32-rhel7:3.2-5.3
    deployment #1 failed 13 minutes ago: config change
```

原因

OpenShift は **docker** コマンドを実行し、コンテナーイメージを検索およびプルします。このコマンドは、**registry.redhat.io** Red Hat コンテナーレジストリーではなく、 **docker.io** Docker レジストリーを参照します。

これは、システムに予期せぬバージョンの Docker コンテナー環境が含まれる場合に発生します。

解決方法

手順

適切なバージョン の Docker コンテナー環境を使用します。

1.9.4. 永続ボリュームがローカルでマウントされている場合の MySQL の権限の問題

問題

system-msql Pod がクラッシュし、デプロイされないため、それに依存する他のシステムのデプロイメントに失敗する。Pod ログに以下のエラーが記録される。

```
[ERROR] Cannot start server : on unix socket: Permission denied
[ERROR] Do you already have another mysqld server running on socket: /var/lib/mysql/mysql.sock ?
[ERROR] Aborting
```

原因

MySQL プロセスが不適切なユーザー権限で起動されている。

解決方法

手順

1. 永続ボリュームに使用されるディレクトリーには、root グループの書き込み権限が必要です。MySQL サービスは root グループの別のユーザーとして実行されるため、root ユーザーの読み取り/書き込み権限では不十分です。root ユーザーとして以下のコマンドを実行します。

```
chmod -R g+w /path/for/pvs
```

2. 以下のコマンドを実行して、SELinux がアクセスをブロックしないようにします。

```
chcon -Rt svirt_sandbox_file_t /path/for/pvs
```

1.9.5. ロゴまたはイメージをアップロードできない

問題

ロゴをアップロードできず、**system-app** ログに以下のエラーが表示される。

```
Errno::EACCES (Permission denied @ dir_s_mkdir - /opt/system/public//system/provider-name/2
```

原因

OpenShift が永続ボリュームに書き込みを行うことができない。

解決方法

手順

OpenShift が永続ボリュームに書き込みを行えるようにします。永続ボリュームのグループ所有者を root グループにし、またグループによる書き込みを可能にしなければなりません。

1.9.6. OpenShift でテストコールが動作しない

問題

OpenShift で新しいサービスとルートを作成した後に、テストコールが動作しない。curl 経由のダイレクトコールも失敗し、**service not available** が出力される。

原因

3scale はデフォルトで HTTPS ルートが必要で、OpenShift ルートはセキュアではない。

解決方法

手順

OpenShift のルーター設定で **secure route** チェックボックスが選択されていることを確認します。

1.9.7. 3scale 以外のプロジェクトでの APIcast デプロイに失敗する

問題

APIcast のデプロイに失敗する (Pod が青にならない)。以下のエラーがログに表示される。

```
update acceptor rejected apicast-3: pods for deployment "apicast-3" took longer than 600 seconds to become ready
```

以下のエラーが Pod に表示される。

```
Error synching pod, skipping: failed to "StartContainer" for "apicast" with RunContainerError: "GenerateRunContainerOptions: secrets \"apicast-configuration-url-secret\" not found"
```

原因

シークレットが適切に設定されていない。

解決方法

手順

APIcast v3 でシークレットを作成する時に **apicast-configuration-url-secret** を指定します。

```
oc create secret generic apicast-configuration-url-secret --from-literal=password=https://<ACCESS_TOKEN>@<TENANT_NAME>-admin.<WILDCARD_DOMAIN>
```

第2章 APICAST のインストール

APIcast は、内部および外部の API サービスを Red Hat 3scale API Management Platform と統合するのに使用される NGINX ベースの API ゲートウェイです。APIcast は、ラウンドロビン形式で負荷分散を行います。

本章では、デプロイメントオプション、提供される環境、および使用を開始する方法について説明します。

前提条件

APIcast がスタンドアロンの API ゲートウェイではない。3scale API Manager への接続が必要です。

- 稼働中の オンプレミス型 3scale インスタンスが必要です。

APIcast をインストールするには、以下のセクションに概略を示す手順を実施します。

- 「APIcast デプロイメントのオプション」
- 「APIcast の環境」
- 「インテグレーション設定」
- 「サービスの設定」
- 「APIcast operator のインストール」
- 「operator を使用した Self-managed APIcast ゲートウェイソリューションのデプロイ」
- 「APIcast の WebSocket プロトコルサポート」
- 「APIcast ゲートウェイの HTTP/2」

2.1. APICAST デプロイメントのオプション

Hosted APIcast (ホスト型 APIcast) または Self-managed APIcast (自己管理型 APIcast) を使用できます。どちらの場合にも、APIcast は残りの 3scale API Management プラットフォームに接続している必要があります。

- **Embedded APIcast** (組み込み型 APIcast): 3scale API Management インストールにはデフォルトで 2 つの APIcast ゲートウェイ (ステージングと実稼働) が含まれています。これらのゲートウェイは事前設定されているため、そのまま使用することができます。
- **Self-managed APIcast** (自己管理型 APIcast): APIcast をどこにでもデプロイすることができます。APIcast のデプロイメントにおける推奨オプションの一部は以下のとおりです。
  - Docker コンテナー環境に APIcast をデプロイする: そのまま使用できる Docker 形式のコンテナーイメージをダウンロードします。これには、Docker 形式のコンテナーで APIcast を実行するための依存関係がすべて含まれています。
  - Red Hat OpenShift 上で APIcast を実行する : APIcast を サポート対象バージョン の OpenShift で実行します。Self-managed APIcast は、オンプレミス型 3scale インストール環境またはホスト型 3scale (SaaS) アカウントに接続できます。

2.2. APICAST の環境

デフォルトでは、3scale アカウントを作成すると、2 つの異なる環境の Embedded APIcast が提供されます。

- **ステージング**: API インテグレーションの設定中またはテスト中にのみ使用することが目的です。設定が想定どおりに動作していることが確認されたら、実稼働環境にデプロイすることができます。OpenShift テンプレートは、設定が各 API 呼び出し (**APICAST_CONFIGURATION_LOADER: lazy**、**APICAST_CONFIGURATION_CACHE: 0**) で再読み込みされるよう、ステージング APIcast のパラメーターを設定します。APIcast の設定変更を即座にテストするのに便利です。

- **実稼働**: 実稼働向けの環境です。**APICAST_CONFIGURATION_LOADER: boot** および **APICAST_CONFIGURATION_CACHE: 300** パラメーターは、OpenShift テンプレートの実稼働 APIcast のために設定されています。そのため、APIcast の開始時に設定が完全に読み込まれ、300 秒 (5 分) 間キャッシュに保存されます。設定は 5 分後に再読み込みされます。これにより、設定を実稼働環境にプロモートすると、APIcast の新しいデプロイメントを実行しない限り、設定の適用に 5 分程度かかる場合があります。

2.3. インテグレーション設定

[your_API_name] > Integration > Configurationの順に移動します。

Configuration ページに、**Integration settings** が表示されます。

デフォルトでは、以下の値が表示されます。

- Deployment Option: embedded APIcast
- Authentication: API Key

右上隅の **edit integration settings** をクリックすると、設定を変更することができます。

2.4. サービスの設定

Private Base URL フィールドに API バックエンドのエンドポイントホストを指定して、API バックエンドを宣言する必要があります。すべての認証、承認、流量制御、および統計が処理された後、APIcast はすべてのトラフィックを API バックエンドにリダイレクトします。

本セクションでは、サービスの設定について各手順を説明します。

- API バックエンドの宣言
- 認証の設定
- API テストコールの設定

2.4.1. API バックエンドの宣言

通常、API のプライベートベース URL は、管理するドメイン (**yourdomain.com**) 上で **https://api-backend.yourdomain.com:443** のようになります。たとえば、Twitter API と統合する場合、プライベートベース URL は **https://api.twitter.com/** になります。

この例では、3scale がホストする **Echo API** を使用します。これは、任意のパスを受け入れ、リクエストに関する情報 (パス、リクエストパラメーター、ヘッダーなど) を返すシンプルな API です。このプライベートベース URL は **https://echo-api.3scale.net:443** になります。

手順

- プライベート (アンマネージド) API が動作することをテストします。たとえば、Echo API の場合には **curl** コマンドを使用して以下の呼び出しを行うことができます。

```
curl "https://echo-api.3scale.net:443"
```

以下のレスポンスが返されます。

```
{
    "method": "GET",
    "path": "/",
    "args": "",
    "body": "",
    "headers": {
      "HTTP_VERSION": "HTTP/1.1",
      "HTTP_HOST": "echo-api.3scale.net",
      "HTTP_ACCEPT": "*/*",
      "HTTP_USER_AGENT": "curl/7.51.0",
      "HTTP_X_FORWARDED_FOR": "2.139.235.79, 10.0.103.58",
      "HTTP_X_FORWARDED_HOST": "echo-api.3scale.net",
      "HTTP_X_FORWARDED_PORT": "443",
      "HTTP_X_FORWARDED_PROTO": "https",
      "HTTP_FORWARDED": "for=10.0.103.58;host=echo-api.3scale.net;proto=https"
    },
    "uuid": "ee626b70-e928-4cb1-a1a4-348b8e361733"
  }
```

2.4.2. 認証の設定

AUTHENTICATION SETTINGS セクションで API の認証設定を行うことができます。

以下のフィールドはすべて任意です。

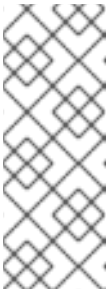
フィールド	説明
Host Header	カスタムの Host リクエストヘッダーを定義します。これは、API バックエンドが特定のホストからのトラフィックのみを許可する場合に必要です。
Secret Token	API バックエンドに直接送られる開発者リクエストをブロックするために使用します。ここにヘッダーの値を設定し、バックエンドがこのシークレットヘッダーを持つ呼び出しのみを許可するようにします。
Credentials location	クレデンシャルが HTTP ヘッダー、クエリーパラメーター、または HTTP Basic 認証として渡されるかどうかを定義します。
Auth user key	Credentials location に関連付けられたキーを設定します。

フィールド	説明
Errors	エラー発生時 (認証失敗、認証パラメーターがない、および一致するルールがない) のレスポンスコード、コンテンツタイプ、およびレスポンス本文を定義します。

2.4.3. API テストコールの設定

手順

1. Hosted ステージング環境のテストコールを設定します。
2. API に存在するパスを **API test GET request** フィールドに入力します (例: **/v1/word/good.json**)。
3. ページ右下の **Update Product** ボタンをクリックして、設定を保存します。
    a. これにより、APIcast の設定が 3scale Hosted ステージング環境にデプロイされます。すべてが正しく設定されていれば、左側の縦線が緑色に変わります。



注記

Self-managed デプロイメントオプションの 1 つを使用してる場合 は、GUI から設定を保存し、Staging Public Base URL フィールドまたは Production Public Base URL フィールドに正しいホストを追加して、デプロイされた API ゲートウェイをポイントするようにします。実稼働ゲートウェイに呼び出しを行う前に、必ず **Promote v.x to Production APIcast**ボタンを押してください。

4. ステージングセクションの最後にある **curl** コマンドの例を確認し、コンソールからコマンドを実行します。

```
curl "https://XXX.staging.apicast.io:443/v1/word/good.json?user_key=YOUR_USER_KEY"
```

注記

上記と同じレスポンスを取得するはずですが、今回はリクエストが 3scale Hosted APIcast インスタンスを通ります。**注記:** サービスに対して有効なクレデンシャルを持つアプリケーションが存在することを確認してください。3scale の登録時に作成されたデフォルトの API サービスを使用している場合はアプリケーションがすでにあるはずです。テストの curl に **USER_KEY** または **APP_ID** と **APP_KEY** の値が出力された場合は、最初にこのサービスのアプリケーションを作成する必要があります。

これで API が 3scale と統合されました。

3scale Hosted APIcast ゲートウェイはクレデンシャルの検証を行い、アプリケーションのアプリケーションプランで定義した流量制御を適用します。クレデンシャルがない、あるいは無効なクレデンシャルで呼び出しを行うと、エラーメッセージが表示されます。

2.5. APICAST OPERATOR のインストール

本セクションでは、OpenShift Container Platform (OCP) コンソールから APIcast operator をインストールする手順について説明します。

手順

1. 管理者権限を持つアカウントを使用して OCP コンソールにログインします。
2. **Projects** > **Create Project**の順に移動し、新規プロジェクト **operator-test** を作成します。
3. **Operators** > **Installed Operators**の順にクリックします。
4. **Filter by keyword** ボックスに **apicast** と入力し、APIcast operator を検索します。コミュニティーバージョンは使用しないでください。
5. APIcast operator をクリックします。APIcast operator に関する情報が表示されます。
6. **Install** をクリックします。**Create Operator Subscription** ページが表示されます。
7. **Create Operator Subscription** ページで、すべてのデフォルト設定を受け入れ **Subscribe** をクリックします。
    a. サブスクリプションのアップグレードステータスが **Up to date** と表示されます。
8. **Operators** > **Installed Operators**の順にクリックし、**operator-test** プロジェクトで APIcast operator の **ClusterServiceVersion** (CSV) ステータスが最終的に **InstallSucceeded** と表示されることを確認します。

2.6. OPERATOR を使用した SELF-MANAGED APICAST ゲートウェイソリューションのデプロイ

本セクションでは、Openshift Container Platform コンソールから APIcast operator を使用して Self-managed APIcast ゲートウェイソリューションをデプロイする手順について説明します。

前提条件

- OpenShift Container Platform (OCP) 4 以降およびその管理者権限
- まず APIcast operator のインストール に記載の手順に従う必要があります。

手順

1. 管理者権限を持つアカウントを使用して OCP コンソールにログインします。
2. **Operators** > **Installed Operators**の順にクリックします。
3. **Installed Operators** のリストで **APIcast Operator** をクリックします。
4. **APIcast** > **Create APIcast**の順にクリックします。

2.6.1. APIcast のデプロイメントおよび設定オプション

Self-managed APIcast ゲートウェイソリューションは、以下に示す 2 とおりの方法を使用してデプロイおよび設定することができます。

- 3scale システムエンドポイントの指定
- 設定シークレットを指定する

2.6.1.1. 3scale システムエンドポイントを指定する

手順

1. 3scale システム管理ポータルのエンドポイント情報が含まれる OpenShift シークレットを作成します。

```
oc create secret generic ${SOME_SECRET_NAME} --from-literal=AdminPortalURL=${MY_3SCALE_URL}
```

   - **${SOME_SECRET_NAME}** はシークレットの名前で、既存のシークレットと競合しない限り、任意の名前を付けることができます。
   - **${MY_3SCALE_URL}** は、3scale アクセストークンおよび 3scale システム管理ポータルのエンドポイントが含まれる URI です。詳細は、**THREESCALE_PORTAL_ENDPOINT** を参照してください。

     例

```
oc create secret generic 3scaleportal --from-literal=AdminPortalURL=https://access-token@account-admin.3scale.net
```

     シークレットの内容についての詳細は、APIcast Custom Resource reference のEmbeddedConfSecret を参照してください。

2. APIcast の OpenShift オブジェクトを作成します。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIcast
metadata:
  name: example-apicast
spec:
  adminPortalCredentialsRef:
    name: SOME_SECRET_NAME
```

   spec.adminPortalCredentialsRef.name は、3scale システム管理ポータルのエンドポイント情報が含まれる既存の OpenShift シークレットの名前でなければなりません。

3. APIcast オブジェクトに関連付けられた OpenShift デプロイメントの **readyReplicas** フィールドが 1 であることを確認し、APIcast Pod が動作状態にあり準備が整っていることを確認します。そうでなければ、以下のコマンドを使用してフィールドが設定されるまで待ちます。

```
$ echo $(oc get deployment apicast-example-apicast -o jsonpath='{.status.readyReplicas}')
1
```

2.6.1.1.1. APIcast ゲートウェイが動作中で利用可能であることの確認

手順

1. ローカルマシンから OpenShift Service APIcast にアクセス可能であることを確認し、テストリクエストを実行します。そのために、APIcast OpenShift Service を **localhost:8080** にポート転送します。

```
oc port-forward svc/apicast-example-apicast 8080
```

2. 設定した 3scale サービスに対してリクエストを行い、HTTP 応答が正常であることを確認します。サービスの **Staging Public Base URL** または **Production Public Base URL** 設定で指定したドメイン名を使用します。以下に例を示します。

```
$ curl 127.0.0.1:8080/test -H "Host: myhost.com"
```

2.6.1.1.2. Kubernetes Ingress 経由での APIcast の外部公開

Kubernetes Ingress 経由で APIcast を外部に公開するには、**exposedHost** セクションを設定します。**ExposedHost** セクションの **host** フィールドを設定すると、Kubernetes Ingress オブジェクトが作成されます。事前にインストールした既存の Kubernetes Ingress Controller はこの Kubernetes Ingress オブジェクトを使用し、APIcast を外部からアクセス可能にします。

APIcast を外部からアクセス可能にするのに使用できる Ingress Controllers およびその設定方法について詳しく知るには、Kubernetes Ingress Controllers のドキュメント を参照してください。

ホスト名 **myhostname.com** で APIcast を公開する例を以下に示します。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIcast
metadata:
  name: example-apicast
spec:
  ...
  exposedHost:
    host: "myhostname.com"
  ...
```

この例では、HTTP 用ポート 80 に Kubernetes Ingress オブジェクトを作成します。APIcast デプロイメントが OpenShift 環境にある場合、OpenShift のデフォルト Ingress Controller は APIcast が作成する Ingress オブジェクト使用して Route オブジェクトを作成し、APIcast インストールへの外部アクセスが可能になります。

exposedHost セクションに TLS を設定することもできます。利用可能なフィールドの詳細を以下の表に示します。

表2.1 APIcastExposedHost の参照テーブル

json/yaml フィールド	タイプ	必須/任意	デフォルト値	説明

json/yaml フィールド	タイプ	必須/任意	デフォルト値	説明
host	string	はい	該当なし	ゲートウェイにルーティングされているドメイン名
tls	[]extensions.IngressTLS	いいえ	該当なし	受信 TLS オブジェクトの配列。詳細は、TLS を参照してください。

2.6.1.2. 設定シークレットの指定

手順

1. 設定ファイルを使用してシークレットを作成します。

```
$ curl
https://raw.githubusercontent.com/3scale/APIcast/master/examples/configuration/echo.json -
o $PWD/config.json

oc create secret generic apicast-echo-api-conf-secret --from-file=$PWD/config.json
```

設定ファイルは **config.json** という名前にする必要があります。これは APIcast CRD の要件です。

シークレットの内容についての詳細は、APIcast Custom Resource reference のEmbeddedConfSecret を参照してください。

2. APIcast カスタムリソース を作成します。

```
$ cat my-echo-apicast.yaml
apiVersion: apps.3scale.net/v1alpha1
kind: APIcast
metadata:
  name: my-echo-apicast
spec:
  exposedHost:
    host: YOUR DOMAIN
  embeddedConfigurationSecretRef:
    name: apicast-echo-api-conf-secret

$ oc apply -f my-echo-apicast.yaml
```

a. 埋め込み設定シークレットの例を以下に示します。

```
apiVersion: v1
kind: Secret
metadata:
```

```
  name: SOME_SECRET_NAME
type: Opaque
stringData:
  config.json: |
    {
      "services": [
        {
          "proxy": {
            "policy_chain": [
              { "name": "apicast.policy.upstream",
                "configuration": {
                  "rules": [{
                    "regex": "/",
                    "url": "http://echo-api.3scale.net"
                  }]
                }
              }
            ]
          }
        }
      ]
    }
```

3. APIcast オブジェクトの作成時に以下の内容を設定します。

```
apiVersion: apps.3scale.net/v1alpha1
kind: APIcast
metadata:
  name: example-apicast
spec:
  embeddedConfigurationSecretRef:
    name: SOME_SECRET_NAME
```

spec.embeddedConfigurationSecretRef.name は、ゲートウェイの設定が含まれる既存の OpenShift シークレットの名前でなければなりません。

4. APIcast オブジェクトに関連付けられた OpenShift デプロイメントの **readyReplicas** フィールドが **1** であることを確認し、APIcast Pod が動作状態にあり準備が整っていることを確認します。そうでなければ、以下のコマンドを使用してフィールドが設定されるまで待ちます。

```
$ echo $(oc get deployment apicast-example-apicast -o jsonpath='{.status.readyReplicas}')
1
```

2.6.1.2.1. APIcast ゲートウェイが動作中で利用可能であることの確認

手順

1. ローカルマシンから OpenShift Service APIcast にアクセス可能であることを確認し、テストリクエストを実行します。そのために、APIcast OpenShift Service を **localhost:8080** にポート転送します。

```
oc port-forward svc/apicast-example-apicast 8080
```

2. 設定した 3scale サービスに対してリクエストを行い、HTTP 応答が正常であることを確認します。サービスの **Staging Public Base URL** または **Production Public Base URL** 設定で指定したドメイン名を使用します。以下に例を示します。

```
$  curl 127.0.0.1:8080/test -H "Host: localhost"
{
  "method": "GET",
  "path": "/test",
  "args": "",
  "body": "",
  "headers": {
    "HTTP_VERSION": "HTTP/1.1",
    "HTTP_HOST": "echo-api.3scale.net",
    "HTTP_ACCEPT": "*/*",
    "HTTP_USER_AGENT": "curl/7.65.3",
    "HTTP_X_REAL_IP": "127.0.0.1",
    "HTTP_X_FORWARDED_FOR": ...
    "HTTP_X_FORWARDED_HOST": "echo-api.3scale.net",
    "HTTP_X_FORWARDED_PORT": "80",
    "HTTP_X_FORWARDED_PROTO": "http",
    "HTTP_FORWARDED": "for=10.0.101.216;host=echo-api.3scale.net;proto=http"
  },
  "uuid": "603ba118-8f2e-4991-98c0-a9edd061f0f0"
```

2.7. APICAST の WEBSOCKET プロトコルサポート

Red Hat 3scale API Management は、バックエンド API への Websocket プロトコル接続に対する APIcast ゲートウェイをサポートします。

WebSocket プロトコルの実装を計画している場合は、以下のリストを考慮してください。

- WebSocket プロトコルは JSON Web Token (JWT) をサポートしない。
- WebSocket 標準は追加のヘッダーを許可しない。
- WebSocket プロトコルは HTTP/2 標準に含まれない。

2.7.1. WebSocket プロトコルのサポート

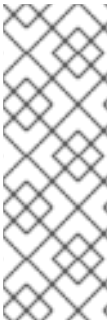
APIcast 設定ポリシーチェーンは以下のとおりです。

```
"policy_chain": [
  { "name": "apicast.policy.websocket" },
  { "name": "apicast.policy.apicast" }
],
```

API バックエンドは **http[s]`** または **ws[s]** として定義できます。

2.8. APICAST ゲートウェイの HTTP/2

Red Hat 3scale API Management は、HTTP/2 および Remote Procedure Call (gRPC) 接続の APIcast ゲートウェイをサポートします。HTTP/2 プロトコル制御を使用すると、APIcast と API バックエンド間のデータ通信が可能になります。



注記

- **api_key** 承認は使用できません。代わりに JSON Web Token (JWT) またはヘッダーを使用してください。
- gRPC エンドポイントは Transport Layer Security (TLS) を終了します。
- GRPC ポリシー (HTTP/2) は、ポリシーチェーンで APIcast ポリシーよりも上位に設定する必要があります。

2.8.1. HTTP/2 プロトコルサポート

HTTP/2 終端では、APICast が有効な HTTP/2 およびバックエンドは HTTP/1.1 プレーンテキストまたは TLS にすることができます。

このポリシーを使用する HTTP/2 エンドポイントでは、以下の制約があります。

- このポリシーが想定通りに動作しない場合には、エンドポイントは TLS をリッスンする必要があります。
- gRPC 全フローは TLS ポリシーが有効な場合にのみ機能します。

APIcast 設定ポリシーチェーンは以下のとおりです。

```
"policy_chain": [
  { "name": "apicast.policy.grpc" },
  { "name": "apicast.policy.apicast" }
],
```

2.9. 関連情報

APIcast の最新リリースとサポート対象バージョンについては、以下のアーティクルを参照してください。

- Red Hat 3scale API Management のサポート対象設定
- Red Hat 3scale API Management コンポーネントの詳細

第3章 RED HAT OPENSHIFT 上での APICAST の実行

本チュートリアルでは、Red Hat OpenShift に APIcast API ゲートウェイをデプロイする方法について説明します。

前提条件

- *2章APIcast のインストール*に従って、Red Hat 3scale API Management 管理ポータルで APIcast を設定する必要があります。
- インテグレーション設定でデプロイメントオプションに **Self-managed Gateway** が選択されていることを確認してください。
- 手順を進めるには、ステージング環境と実稼働環境の両方を設定している必要があります。

Red Hat OpenShift 上で APIcast を実行するには、以下のセクションに概略を示す手順を実施します。

- 「Red Hat OpenShift の設定」
- 「OpenShift テンプレートを使用した APIcast のデプロイ」
- 「OpenShift コンソール経由でのルートの作成」

3.1. RED HAT OPENSHIFT の設定

OpenShift クラスターが稼働中である場合は、本セクションを省略できます。稼働中でなければ、以下の手順に従ってください。

実稼働デプロイメントの場合は、OpenShift のインストール手順 に従います。

本チュートリアルでは、OpenShift クラスターは以下を使用してインストールされます。

- Red Hat Enterprise Linux (RHEL) 7
- Docker コンテナー環境 (v1.10.3)
- OpenShift Origin コマンドラインインターフェイス (CLI) v1.3.1

以下のセクションを使用して、Red Hat OpenShift を設定します。

- Docker コンテナー環境のインストール
- OpenShift クラスターの起動
- リモートサーバーでの OpenShift クラスターの設定 (任意)

3.1.1. Docker コンテナー環境のインストール

Red Hat が提供する Docker 形式のコンテナーイメージは、RHEL の Extras チャンネルの一部としてリリースされています。追加のリポジトリーを有効にするには、Subscription Manager または yum-config-manager を使用できます。詳細は、RHEL の製品ドキュメント を参照してください。

AWS EC2 インスタンスにデプロイされた RHEL 7 では、以下の手順を使用します。

手順

1. すべてのリポジトリーを一覧表示します。

```
sudo yum repolist all
```

2. ***-extras** リポジトリーを探し、有効にします。

```
sudo yum-config-manager --enable rhui-REGION-rhel-server-extras
```

3. Docker 形式のコンテナーイメージをインストールします。

```
sudo yum install docker docker-registry
```

4. **/etc/sysconfig/docker** ファイルに以下の行を追加するか、アンコメントして、**172.30.0.0/16** のセキュアでないレジストリーを追加します。

```
INSECURE_REGISTRY='--insecure-registry 172.30.0.0/16'
```

5. Docker サービスを開始します。

```
sudo systemctl start docker
```

6. 以下のコマンドを使用して、コンテナーサービスが動作中であることを確認します。

```
sudo systemctl status docker
```

3.1.2. OpenShift クラスターの起動

OpenShift クラスターを起動するには、以下の手順を実施します。

手順

1. OpenShift リリースページ から、クライアントツールの最新の安定版リリース (**openshift-origin-client-tools-VERSION-linux-64bit.tar.gz**) をダウンロードし、アーカイブから抽出した Linux **oc** バイナリーを **PATH** に置きます。

注記

docker コマンドは **root** ユーザーとして実行されるため、**oc** または docker コマンドはすべて root 権限で実行する必要があります。

2. docker コマンドを実行する権限のあるユーザーでターミナルを開き、以下のコマンドを実行します。

```
oc cluster up
```

出力の最後に、デプロイされたクラスターの情報が表示されます。

```
-- Server Information ...
  OpenShift server started.
  The server is accessible via web console at:
  https://172.30.0.112:8443
```

```
You are logged in as:
  User:     developer
  Password: developer

To login as administrator:
  oc login -u system:admin
```

3. OpenShift サーバーに割り当てられた IP アドレスを書き留めておきます。本チュートリアルでは **OPENSHIFT-SERVER-IP** をその IP アドレスに置き換えてください。

3.1.3. リモートサーバーでの OpenShift クラスターの設定 (任意)

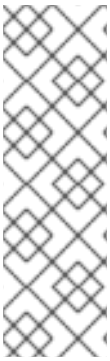
OpenShift クラスターをリモートサーバーにデプロイする場合、クラスターの起動時にパブリックホスト名とルーティング接尾辞を明示的に指定し、OpenShift Web コンソールへリモートアクセスできるようにする必要があります。

たとえば、AWS EC2 インスタンスでデプロイする場合は、以下のオプションを指定する必要があります。

```
oc cluster up --public-hostname=ec2-54-321-67-89.compute-1.amazonaws.com --routing-suffix=54.321.67.89.xip.io
```

ec2-54-321-67-89.compute-1.amazonaws.com はパブリックドメイン、**54.321.67.89** はインスタンスの IP アドレスに置き換えます。これにより、https://ec2-54-321-67-89.compute-1.amazonaws.com:8443 で OpenShift Web コンソールにアクセスできるようになります。

3.2. OPENSHIFT テンプレートを使用した APICAST のデプロイ



注記

- テンプレートを使用する場合は、OpenShift Container Platform (OCP) 3.11 にのみ APIcast をデプロイすることができます。
- operator ベースのインストールは、OCP バージョン 4.1 および 4.2 でのみサポートされます。
- サポート対象設定の情報については、3scale API Management 2.7 Supported Configurations のアーティクルを参照してください。

OpenShift テンプレートを使用して APIcast をデプロイするには、以下の手順を使用します。

手順

1. デフォルトでは、**developer** としてログインしていて、次のステップに進むことができます。そうでなければ、前の手順でダウンロードおよびインストールした OpenShift クライアントツールから **oc login** コマンドを使用して OpenShift にログインします。デフォルトのログインクレデンシャルは **username = "developer"** と **password = "developer"** です。

   ```
   oc login https://OPENSHIFT-SERVER-IP:8443
   ```

   出力に **Login successful.** が表示されるはずです。

2. プロジェクトを作成します。この例では表示名を **gateway** と設定します。

```
oc new-project "3scalegateway" --display-name="gateway" --description="3scale gateway
demo"
```

応答は以下のようになります。

```
Now using project "3scalegateway" on server "https://172.30.0.112:8443"
```

コマンドプロンプトのテキスト出力で提案される次のステップを無視し、以下に示す次のステップに進みます。

3. プロジェクトを参照する新しいシークレットを作成します。**<access_token>** および **<domain>** はご自分のクレデンシャルに置き換えます。**<access_token>** および **<domain>** の詳細は、以下を参照してください。

```
oc create secret generic apicast-configuration-url-secret --from-
literal=password=https://<access_token>@<admin_portal_domain>  --
type=kubernetes.io/basic-auth
```

ここでは、**<access_token>** は 3scale アカウントの アクセストークン で、**<domain>-admin.3scale.net** は 3scale 管理ポータルの URL になります。

応答は以下のようになります。

```
secret/apicast-configuration-url-secret
```

4. テンプレートから APIcast ゲートウェイのアプリケーションを作成し、デプロイメントを開始します。

```
oc new-app -f https://raw.githubusercontent.com/3scale/3scale-amp-openshift-
templates/2.8.0.GA/apicast-gateway/apicast.yml
```

出力の最後に以下のメッセージが表示されるはずです。

```
--> Creating resources with label app=3scale-gateway ...
    deploymentconfig "apicast" created
    service "apicast" created
--> Success
    Run 'oc status' to view your app.
```

3.3. OPENSHIFT コンソール経由でのルートの作成

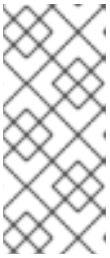
OpenShift コンソール経由でルートを作成するには、以下の手順を実施します。

手順

1. 以下の URL から、ブラウザーで OpenShift クラスターの Web コンソールを開きます。
https://OPENSHIFT-SERVER-IP:8443/console/

OpenShift クラスターをリモートサーバーで起動した場合は、**OPENSHIFT-SERVER-IP** ではなく、**--public-hostname** で指定した値を使用します。

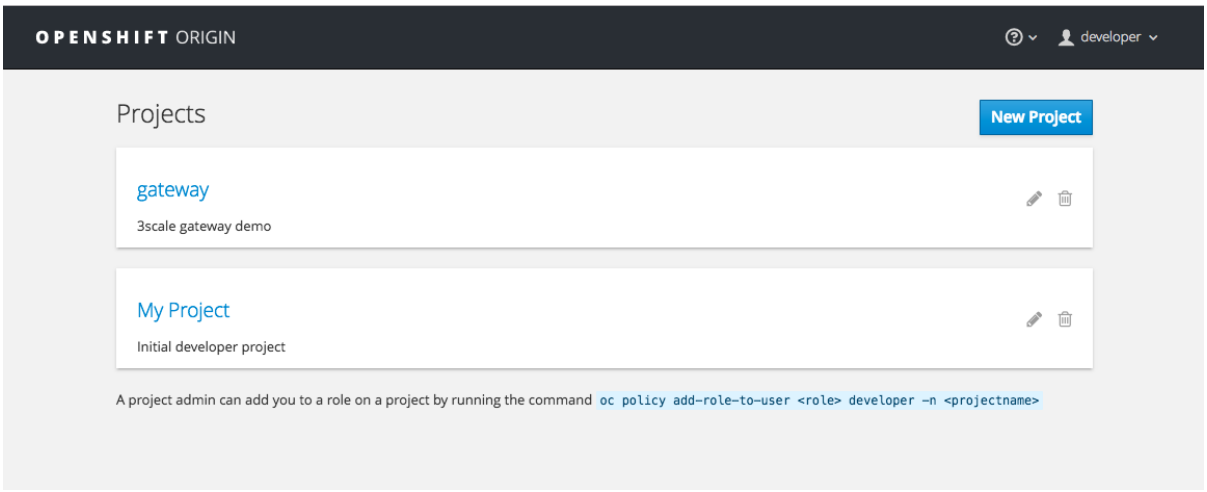
OpenShift のログイン画面が表示されます。



注記

信頼できない Web サイトに関する警告が表示される可能性があります。有効な証明書を設定せずに、セキュアなプロトコルで Web コンソールにアクセスしようとしているため、この警告は想定内です。これは本番環境で行うべきではありませんが、このテスト設定では続行してこのアドレスの例外を作成することができます。

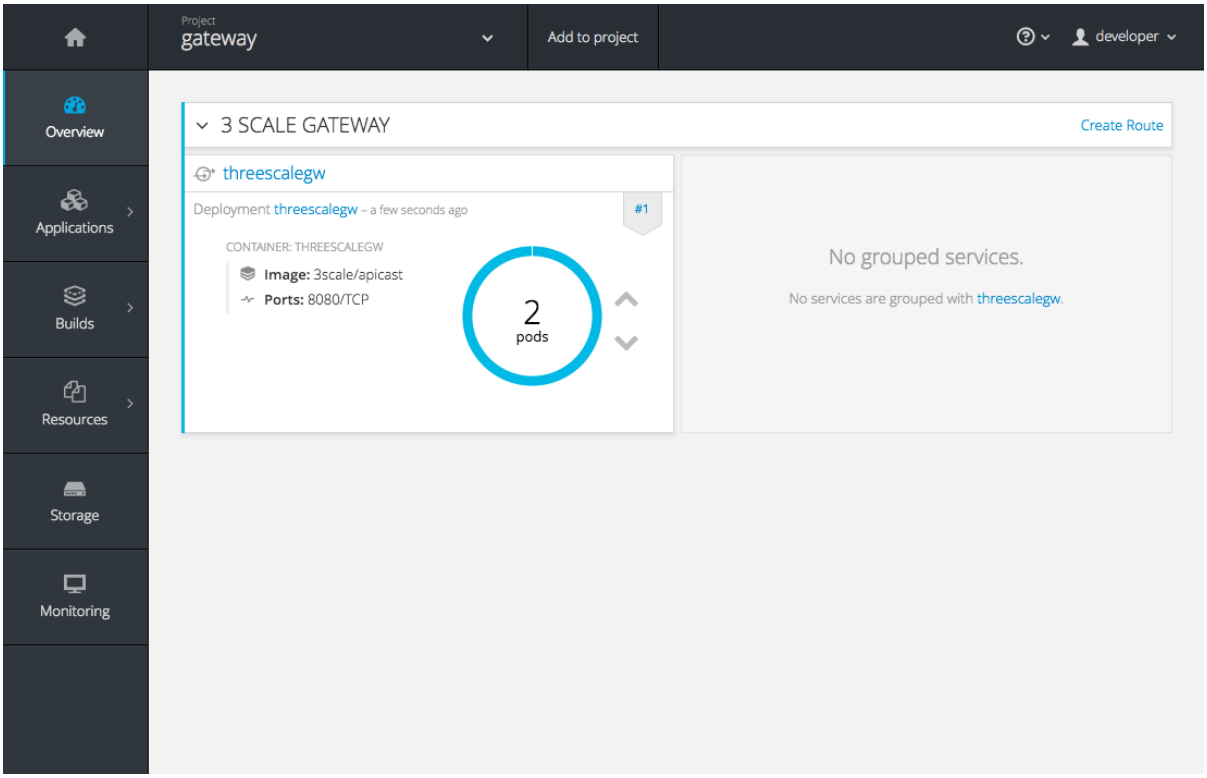
2. Red Hat OpenShift の設定 セクションで作成または取得した **developer** のクレデンシャルを使用してログインします。
上記のコマンドラインから作成した **gateway** プロジェクトが含まれる、プロジェクトのリストが表示されます。



gateway プロジェクトが表示されない場合は、別のユーザーで作成した可能性があり、ポリシーロールをこのユーザーに割り当てる必要があります。

3. **gateway** リンクをクリックすると、**Overview** タブが表示されます。
OpenShift は APIcast のコードをダウンロードし、デプロイメントを開始しました。デプロイメントの進行中に **Deployment #1 running** というメッセージが表示されることがあります。

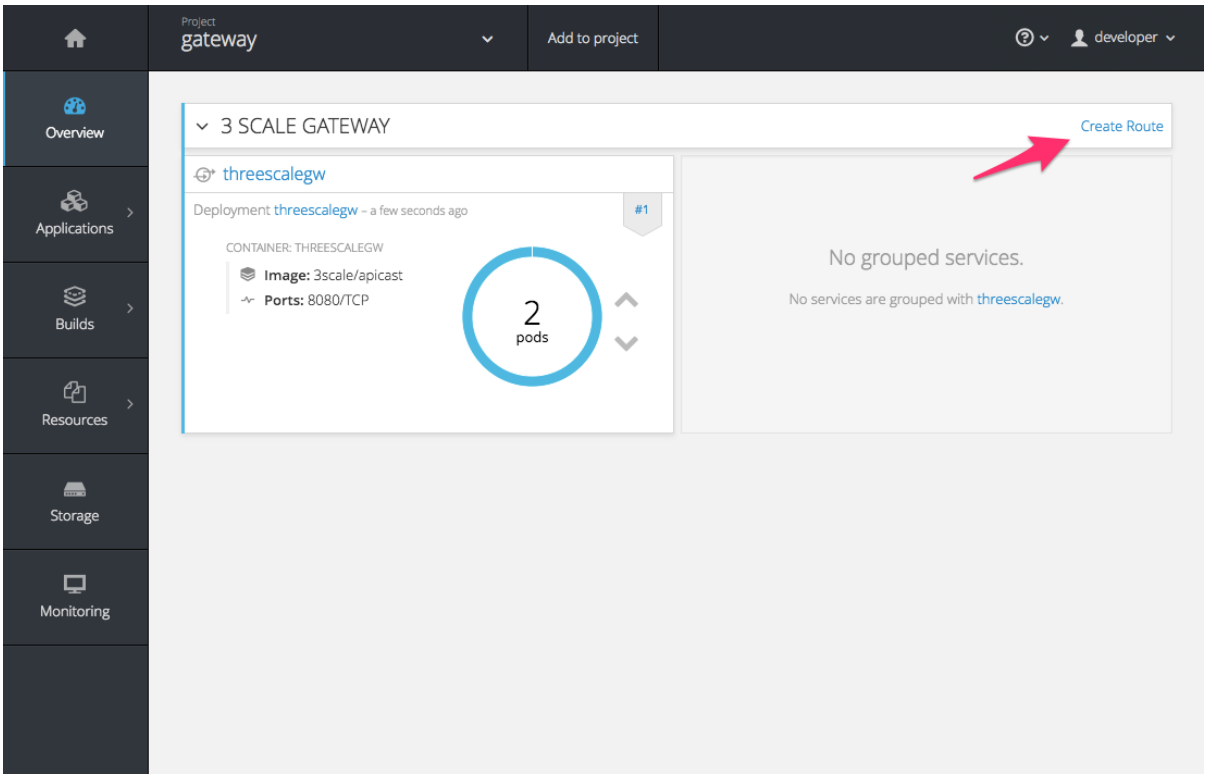
ビルドが完了すると、ユーザーインターフェイス (UI) が更新され、テンプレートで定義されたとおりに OpenShift によって起動された APIcast の 2 つのインスタンス (**2 つの Pod**) が表示されます。



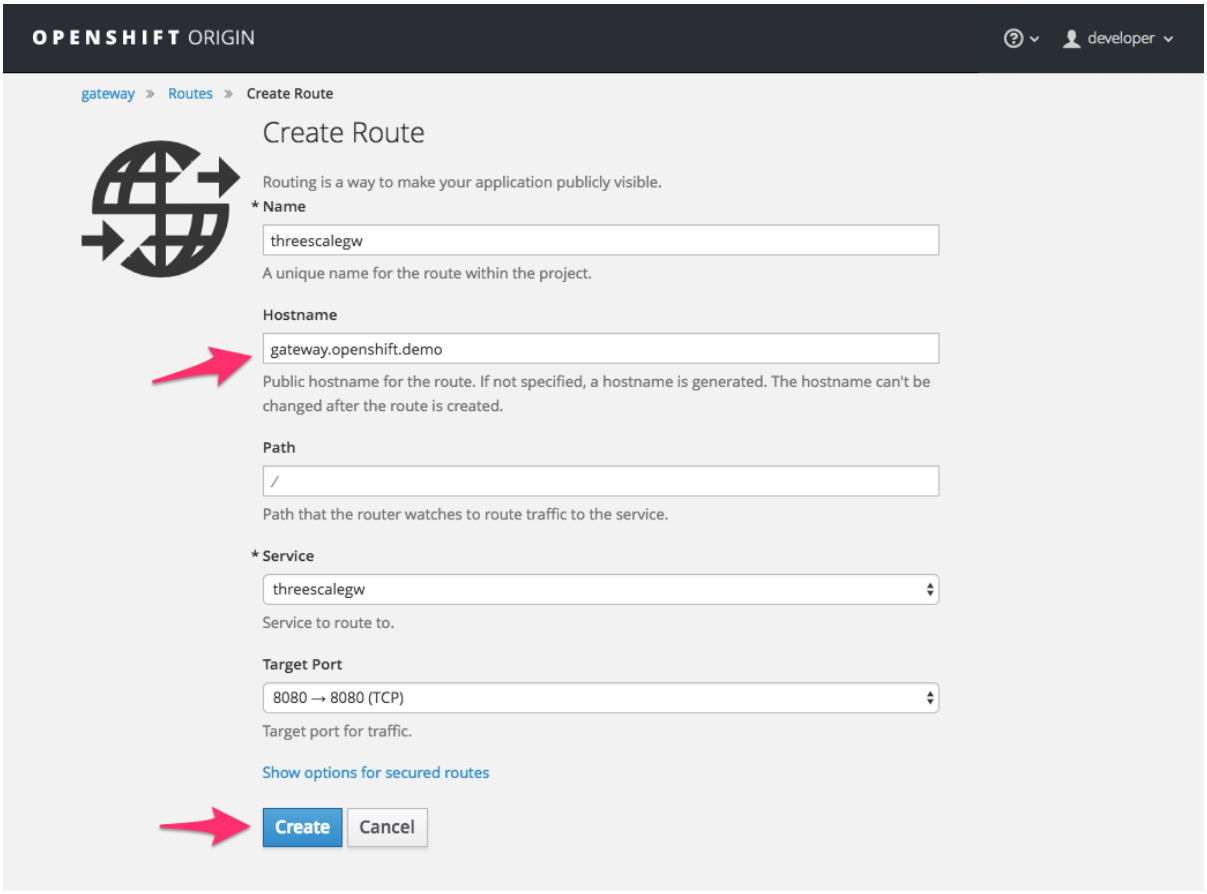
各 APIcast インスタンスが起動すると、3scale 管理ポータルの **Integration** ページの設定を使用して、3scale から必要な設定をダウンロードします。

OpenShift は 2 つの APIcast インスタンスを維持し、両方のインスタンスの状態を監視します。状態の悪い APIcast インスタンスは自動的に新しいインスタンスに置き換えられます。

4. APIcast インスタンスでトラフィックを受信できるようにするには、ルートを作成する必要があります。**Create Route** をクリックして操作を開始します。



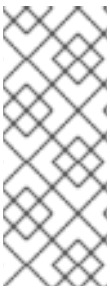
上記の **Public Base URL** フィールドで 3scale に設定したホストを、**http://** とポートを削除して入力し (例: **gateway.openshift.demo**)、**Create** ボタンをクリックします。



定義するすべての 3scale プロダクトについて、新規ルートを作成する必要があります。

第4章 DOCKER コンテナー環境への APICAST のデプロイ

ここでは、Docker コンテナーエンジン内部に Red Hat 3scale API Management API ゲートウェイとして使用する準備が整っている APIcast をデプロイする方法を、手順をおって説明します。



注記

Docker コンテナー環境に APIcast をデプロイする場合、サポートされる Red Hat Enterprise Linux (RHEL) および Docker のバージョンは以下のとおりです。

- RHEL 7.7
- Docker 1.13.1

前提条件

- *2章APIcast のインストール* に従って、3scale 管理ポータルで APIcast を設定している。
- Red Hat コンテナーカタログ へのアクセス
  - レジストリーサービスアカウントを作成するには、「レジストリーサービスアカウントの作成」 を参照してください。

Docker コンテナー環境に APIcast をデプロイするには、以下のセクションに概略を示す手順を実施します。

- 「Docker コンテナー環境のインストール」
- 「Docker コンテナー環境ゲートウェイの実行」

4.1. DOCKER コンテナー環境のインストール

本セクションでは、RHEL 7 に Docker コンテナー環境を設定する手順を説明します。

Red Hat が提供する Docker コンテナーエンジンは、RHEL の Extras チャンネルの一部としてリリースされています。追加のリポジトリーを有効にするには、Subscription Manager または **yum-config-manager** オプションを使用できます。詳細は、RHEL の製品ドキュメント を参照してください。

Amazon Web Services (AWS)、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに RHEL 7 をデプロイするには、以下の手順を実施します。

手順

1. **sudo yum repolist all** ですべてのリポジトリーを一覧表示します。
2. ***-extras** リポジトリーを探します。
3. **sudo yum-config-manager --enable rhui-REGION-rhel-server-extras** を実行し、**extras** リポジトリーを有効にします。
4. **sudo yum install docker** を実行し、Docker コンテナー環境のパッケージをインストールします。

関連情報

他のオペレーティングシステムをお使いの場合は、以下の Docker ドキュメントを参照してください。

- Installing the Docker containerized environment on Linux distributions
- Installing the Docker containerized environment on Mac
- Installing the Docker containerized environment on Windows

4.2. DOCKER コンテナー環境ゲートウェイの実行

Docker コンテナー環境ゲートウェイを実行するには、以下の手順を実施します。

手順

1. Docker デーモンを開始します。
   sudo systemctl start docker.service
2. Docker デーモンが実行されているか確認します。
   sudo systemctl status docker.service

   Red Hat レジストリーから、そのまま使用できる Docker コンテナーエンジンのイメージをダウンロードできます。

   sudo docker pull registry.redhat.io/3scale-amp2/apicast-gateway-rhel8:3scale2.8
3. Docker コンテナーエンジンで APIcast を実行します。
   sudo docker run --name apicast --rm -p 8080:8080 -e THREESCALE_PORTAL_ENDPOINT=https://<access_token>@<domain>-admin.3scale.net registry.redhat.io/3scale-amp2/apicast-gateway-rhel8:3scale2.8

   ここで、**<access_token>** は 3scale Account Management API のアクセストークンに置き換えます。アクセストークンの代わりにプロバイダーキーを使用することもできます。**<domain>-admin.3scale.net** は 3scale 管理ポータルの URL です。

このコマンドは、**apicast**という Docker コンテナーエンジンをポート **8080** で実行し、3scale 管理ポータルから JSON 設定ファイルを取得します。その他の設定オプションについては、APIcast のインストール を参照してください。

4.2.1. docker コマンドのオプション

docker run コマンドでは、以下のオプションを使用できます。

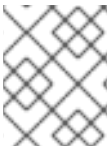
- **--rm**: 終了時にコンテナーを自動的に削除します。
- **-d** または **--detach**: コンテナーをバックグラウンドで実行し、コンテナー ID を出力します。このオプションを指定しないと、コンテナーはフォアグラウンドモードで実行され、**CTRL+c** を使用して停止することができます。デタッチモードで起動された場合、**docker attach** コマンド (例: **docker attach apicast**) を使用するとコンテナーに再アタッチすることができます。
- **-p** または **--publish**: コンテナーのポートをホストに公開します。値の書式は **<host port="">:<container port="">** とする必要があります。したがって、**-p 80:8080** の場合は、コンテナーのポート **8080** をホストマシンのポート **80** にバインドします。たとえば、Management API はポート **8090** を使用するため、**-p 8090:8090** を **docker run** コマンドに追加してこのポートを公開します。
- **-e** または **--env**: 環境変数を設定します。
- **-v** または **--volume**: ボリュームをマウントします。値は通常 **<host path="">:<container**

path="">[:<options>] で表されます。**<options>** はオプションの属性で、ボリュームを読み取り専用に指定するには、**:ro** に設定します (デフォルトでは読み取り/書き込みモードでマウントされます)。たとえば、**-v /host/path:/container/path:ro** と設定します。

4.2.2. APIcast のテスト

以下の手順は、Docker コンテナーエンジンが独自の設定ファイルと、3scale レジストリーからの Docker コンテナーイメージで実行されるようにします。呼び出しは APIcast を介してポート **8080** でテストでき、3scale アカウントから取得できる正しい認証クレデンシャルを提供できます。

テストコールは、APIcast が適切に実行されていることを確認するだけでなく、認証とレポートが正常に処理されたことも確認します。



注記

呼び出しに使用するホストが **Integration** ページの **Public Base URL** フィールドに設定されたホストと同じであるようにしてください。

関連情報

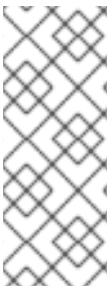
- 使用できるオプションの詳細については、Docker run reference を参照してください。

4.3. 関連情報

- テスト済みのサポート対象設定の情報については、Red Hat 3scale API Management のサポート対象設定 を参照してください。

第5章 PODMAN への APICAST のデプロイ

ここでは、Pod Manager (Podman) コンテナー環境に Red Hat 3scale API Management API ゲートウェイとして使用される APIcast をデプロイする方法を、手順を追って説明します。



注記

Podman コンテナー環境に APIcast をデプロイする場合、サポートされる Red Hat Enterprise Linux (RHEL) および Podman のバージョンは以下のとおりです。

- RHEL 8
- Podman 1.4.2

前提条件

- 2章*APIcast のインストール* に従って、3scale 管理ポータルで APIcast を設定している。
- Red Hat コンテナーカタログ へのアクセス
  - レジストリーサービスアカウントを作成するには、「レジストリーサービスアカウントの作成」 を参照してください。

Podman コンテナー環境に APIcast をデプロイするには、以下のセクションに概略を示す手順を実施します。

- 「Podman コンテナー環境のインストール」
- 「Podman 環境の実行」

5.1. PODMAN コンテナー環境のインストール

本セクションでは、RHEL 8 に Podman コンテナー環境を設定する手順を説明します。Docker は RHEL 8 に含まれていないため、コンテナーの操作には Podman を使用します。

Podman と RHEL 8 の使用については、コンテナーのコマンドに関するリファレンスドキュメント を参照してください。

手順

- Podman コンテナー環境パッケージをインストールします。
  sudo dnf install podman

関連情報

他のオペレーティングシステムをお使いの場合は、以下の Podman のドキュメントを参照してください。

- Podman Installation Instructions

5.2. PODMAN 環境の実行

Podman コンテナー環境を実行するには、以下の手順に従います。

手順

1. Red Hat レジストリーから、そのまま使用できる Podman コンテナーのイメージをダウンロードします。
   podman pull registry.redhat.io/3scale-amp2/apicast-gateway-rhel8:3scale2.8

2. Podman で APIcast を実行します。
   podman run --name apicast --rm -p 8080:8080 -e THREESCALE_PORTAL_ENDPOINT=https://<access_token>@<domain>-admin.3scale.net registry.redhat.io/3scale-amp2/apicast-gateway-rhel8:3scale2.8

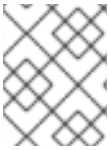
   ここで、**<access_token>** は 3scale Account Management API のアクセストークンに置き換えます。アクセストークンの代わりにプロバイダーキーを使用することもできます。**<domain>-admin.3scale.net** は 3scale 管理ポータルの URL です。

このコマンドは、**apicast**という Podman コンテナーエンジンをポート **8080** で実行し、3scale 管理ポータルから JSON 設定ファイルを取得します。その他の設定オプションについては、APIcast のインストール を参照してください。

5.2.1. Podman による APIcast のテスト

以下の手順は、Podman コンテナーエンジンが独自の設定ファイルと、3scale レジストリーからの Podman コンテナーイメージで実行されるようにします。呼び出しは APIcast を介してポート **8080** でテストでき、3scale アカウントから取得できる正しい認証クレデンシャルを提供できます。

テストコールは、APIcast が適切に実行されていることを確認するだけでなく、認証とレポートが正常に処理されたことも確認します。



注記

呼び出しに使用するホストが **Integration** ページの **Public Base URL** フィールドに設定されたホストと同じであるようにしてください。

5.3. PODMAN コマンドのオプション

podman コマンドでは、以下に例を示すオプションを使用することができます。

- **-d**: **デタッチモード** でコンテナーを実行し、コンテナー ID を出力します。このオプションを指定しないと、コンテナーはフォアグラウンドモードで実行され、**CTRL+c** を使用して停止することができます。デタッチモードで起動された場合、**podman attach** コマンド (例: **podman attach apicast**) を使用するとコンテナーに再アタッチすることができます。

- **ps** および **-a**: Podman **ps** を使用して、作成中および実行中のコンテナーを一覧表示します。**ps** コマンドに **-a** を追加すると (例: **podman ps -a**)、すべてのコンテナー (実行中および停止中の両方) が表示されます。

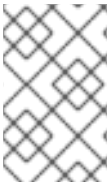
- **inspect** および **-l**: 実行中のコンテナーを調べます。たとえば、**inspect** を使用して、コンテナーに割り当てられた ID を表示します。**-l** を使用すると、最新のコンテナーの詳細を取得できます (たとえば **podman inspect -l | grep Id\":**)。

5.4. 関連情報

- テスト済みのサポート対象設定の情報については、Red Hat 3scale API Management のサポート対象設定 を参照してください。

- Podman を初めて使用する場合は、Basic Setup and Use of Podman を参照してください。

第6章 OPENSHIFT への 3SCALE OPERATOR のインストール



注記

3scale は、直近 2 つの OpenShift Container Platform (OCP) 一般提供 (GA) リリースをサポートします。詳細は、Red Hat 3scale API Management のサポート対象設定 のアーティクルを参照してください。

本セクションでは、以下の項目の実施方法について説明します。

- 新しいプロジェクトを作成する。
- Red Hat 3scale API Management インスタンスをデプロイする。
- プロジェクトで **threescale-registry-auth** シークレットを作成する。
- Operator Lifecycle Manager (OLM) を使用して 3scale operator をインストールする。
- operator をデプロイした後にカスタムリソースをデプロイする。

前提条件

- 管理者権限を持つアカウントを使用して、サポート対象バージョンの OpenShift Container Platform 4 クラスターにアクセスできる。
  - サポート対象設定の情報については、Red Hat 3scale API Management のサポート対象設定 のアーティクルを参照してください。

警告

3scale operator とカスタムリソース定義 (CRD) は、新たに作成した空の **プロジェクト** にデプロイしてください。インフラストラクチャーが含まれる既存のプロジェクトにデプロイすると、既存の要素が変更または削除されることがあります。

OpenShift に 3scale operator をインストールするには、以下のセクションに概略を示す手順を実施します。

- 「新しい OpenShift プロジェクトの作成」
- 「OLM を使用した 3scale operator のインストールと設定」

6.1. 新しい OPENSHIFT プロジェクトの作成

以下の手順で、**3scale-project** という新しい OpenShift プロジェクトを作成する方法について説明します。このプロジェクト名を実際のプロジェクト名に置き換えてください。

手順

新しい OpenShift プロジェクトを作成するには、以下の手順を実施します。

- 英数字とダッシュを使用して、有効な名前を指定します。たとえば、以下のコマンドを実行して **3scale-project** を作成します。

```
oc new-project 3scale-project
```

これにより、operator、**APIManager** カスタムリソース (CR)、および **Capabilities** カスタムリソースがインストールされる新しい **OpenShift プロジェクト** が作成されます。operator は、そのプロジェクトの OLM を通じてカスタムリソースを管理します。

6.2. OLM を使用した 3SCALE OPERATOR のインストールと設定

OLM を使用して、OpenShift Container Platform 4.1 クラスターに 3scale operator をインストールします。この際に、OpenShift Container Platform コンソールの OperatorHub を使用します。

注記

新しい OpenShift プロジェクトの作成 で定義したプロジェクトに 3scale operator をインストールおよびデプロイする必要があります。

手順

1. OpenShift Container Platform コンソールにおいて、管理者権限を持つアカウントを使用してログインします。
2. メニュー構造は、使用している OpenShift のバージョンによって異なります。
   - OCP 4.1 の場合は、**Catalog > OperatorHub** の順にクリックします。
   - OCP 4.2 の場合は、**Operators > OperatorHub** の順にクリックします。
3. **Filter by keyword** ボックスに **3scale operator** と入力し、3scale operator を検索します。
4. 3scale operator をクリックします。operator に関する情報が表示されます。
5. operator に関する情報を確認し、**Install** をクリックします。**Create Operator Subscription** ページが表示されます。
6. **Create Operator Subscription** ページで、すべてのデフォルト設定を受け入れ **Subscribe** をクリックします。

注記

operator は、選択したクラスター上の特定の単一 namespace でしか使用することができません。

3scale-operator の詳細ページが表示されるので、**Subscription Overview** を確認します。

7. サブスクリプションの **upgrade status** が **Up to date** と表示されていることを確認します。
8. 3scale operator の ClusterServiceVersion (CSV) が表示され、新しい OpenShift プロジェクトの作成 で定義したプロジェクトで operator の **Status** が最終的に **InstallSucceeded** となるのを確認します。
   - OCP 4.1 の場合は、**Catalog > Installed Operators** の順にクリックします。

- OCP 4.2 の場合は、**Operators > Installed Operators**の順にクリックします。この場合、インストールに成功すると、**APIManager** CRD および operator の **Capabilities** 機能に関連する CRD が **OpenShift API サーバー** に登録されます。

9. インストールが正常に完了したら、**oc get** を使用して CRD によって定義されたリソースタイプのクエリーを行います。

   a. たとえば、**APIManager** CRD が適切に登録されたことを確認するには、以下のコマンドを実行します。

   ```
   oc get apimanagers
   ```

10. 以下の出力が表示されるはずです。

```
No resources found.
```

関連情報

- トラブルシューティングに関する情報は、OpenShift Container Platform のドキュメント を参照してください。
- サポート対象設定の情報については、Red Hat 3scale API Management Supported Configurations のアーティクルを参照してください。

第7章 3SCALE 高可用性テンプレートおよび評価用テンプレート

ここでは、Red Hat 3scale API Management 2.8 インストール環境で使用される 高可用性 テンプレートおよび 評価用 テンプレートについて説明します。

前提条件

- 高可用性テンプレートおよび評価用テンプレートの要素をデプロイできる OpenShift クラスターが用意されている。

重要

3scale の高可用性テンプレートおよび評価用テンプレートは、テクノロジープレビューの機能としてのみ提供されます。テクノロジープレビューの機能は、Red Hat の実稼働環境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の機能は、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。

高可用性テンプレートおよび評価用テンプレートをデプロイするには、以下のセクションに概略を示す手順を実施します。

- 「高可用性テンプレート」
- 「評価用テンプレート」

7.1. 高可用性テンプレート

高可用性 (HA) テンプレートを使用すると、重要なデータベースの HA を設定できます。

前提条件

- HA テンプレートをデプロイする前に、外部データベースをデプロイおよび設定し、負荷分散されたエンドポイントで HA を設定しておく。

HA テンプレートの使用

高可用性のために **amp-ha-tech-preview.yml** という名前のテンプレートを使用すると、OpenShift 外部に重要なデータベースをデプロイできます。ただし、以下は除外されます。

- Memcached
- Sphinx
- Zync

標準の **amp.yml** テンプレートと **amp-ha-tech-preview.yml** には、以下の違いがあります。

- 以下の要素が削除されています。
  - backend-redis およびその関連コンポーネント
  - system-redis およびその関連コンポーネント

- system-mysql およびその関連コンポーネント
- Redis および MySQL 関連の ConfigMaps
- MYSQL_IMAGE、REDIS_IMAGE、MYSQL_USER、MYSQL_ROOT_PASSWORD パラメーター

- デフォルトで、データベースではない **DeploymentConfig** オブジェクトタイプのレプリカの数が 1 から 2 に増加されます。
- 以下の必須パラメーターが追加されているため、外部データベースの場所を制御できます。
  - BACKEND_REDIS_STORAGE_ENDPOINT
  - BACKEND_REDIS_QUEUES_ENDPOINT
  - SYSTEM_REDIS_URL
  - APICAST_STAGING_REDIS_URL
  - APICAST_PRODUCTION_REDIS_URL
  - SYSTEM_DATABASE_URL

amp-ha-tech-preview.yml を使用する場合、新たに追加された必須パラメーターによりクラスター外のデータベース接続を設定する必要があります (ただし、永続的なデータが含まれない **system-memcache**、**zync-database**、および **system-sphinx** は除外)。エンドポイントには、クレデンシャルを含む、データベースの負荷分散用接続文字列が必要です。また、データベースではないデプロイメントについては、アプリケーションレベルでの冗長性を確保するためにデフォルトで Pod レプリカの数が 2 に増えています。

7.1.1. 高可用性向け RWX_STORAGE_CLASS の設定

ReadWriteMany (RWX) PersistentVolumeClaim (PVC) はストレージクラス RWX_STORAGE_CLASS を使用します。

必須: false

値: **null**

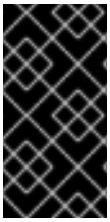
- これを **null** (値なし) に設定した場合、ストレージクラスが自動検出されることが OpenShift に通知されます。
- これを空の文字列 (特定の値または null 以外) に設定すると、文字列ストレージを空にすることが OpenShift に通知されます。これは無効な設定です。

7.2. 評価用テンプレート

評価の目的で、リソースのリクエストや制限のない 3scale 環境をデプロイする **amp-eval-tech-preview.yml** という名前のテンプレートが提供されています。

標準の **amp.yml** テンプレートとの唯一の機能的な違いは、リソースの制限とリクエストが削除されたことです。そのため、このバージョンでは CPU およびメモリーレベルでハードウェアの最低要件が Pod で削除されました。このテンプレートは、指定のハードウェアリソースを使用して、可能な限りコンポーネントをデプロイしようとするため、評価、テスト、および開発のみの使用を目的としています。

第8章 3SCALE の REDIS 高可用性 (HA) サポート



重要

Red Hat は、ゼロダウンタイムのための Redis のセットアップ、3scale のバックエンドコンポーネントの設定、または Redis データベースのレプリケーションおよびシャーディングを正式にはサポートしていません。本章に記載の内容は、参照用途としてのみ提供されています。また、3scale では、**cluster mode** の Redis はサポートされません。

高可用性 (HA) は、OpenShift Container Platform (OCP) によりほとんどのコンポーネントで提供されます。詳細は、OpenShift Container Platform 3.11 30.章、高可用性 を参照してください。

Red Hat 3scale API Management の HA 用データベースコンポーネントは、以下のとおりです。

- **backend-redis**: 統計ストレージおよび一時ジョブストレージに使用されます。
- **system-redis**: 3scale のバックグラウンドジョブの一時ストレージを提供し、**system-app** Pod の **Ruby** プロセスのメッセージバスとしても使用されます。

backend-redis と **system-redis** は、どちらもサポートされる Redis Sentinel および Redis Enterprise 用 Redis 高可用性バリアントと共に動作します。

Redis Pod が停止した場合や、OpenShift Container Platform によって停止された場合には、新しい Pod が自動作成されます。データは永続ストレージから復元されるので、Pod は動作し続けます。このような場合、新しい Pod が起動するまでの間、短いダウンタイムが発生します。これは、Redis がマルチマスター設定をサポートしないという制限によるものです。Redis をデプロイしたすべてのノードに Redis イメージを事前にインストールすることで、ダウンタイムを削減することができます。これにより、Pod の再起動にかかる時間が短縮されます。

ゼロダウンタイムとなるよう Redis をセットアップし、3scale のバックエンドコンポーネントを設定します。

- ゼロダウンタイムのための Redis 設定
- 3scale 用バックエンドコンポーネントの設定
- Redis データベースのシャーディングおよびレプリケーション

前提条件

- 管理者ロールが設定された 3scale アカウント

8.1. ゼロダウンタイムのための REDIS 設定

ゼロダウンタイムが必要な場合、3scale 管理者は OCP 外部に Redis を設定します。3scale Pod の設定オプションを使用してこの設定を行うには、いくつかの方法があります。

- 独自の自己管理型 Redis を設定する
- Redis Sentinel を使用する (Redis Sentinel Documentation を参照)
- サービスとして提供される Redis:
  例:
  - Amazon ElastiCache

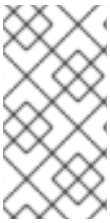
- Redis Labs

注記

Red Hat は上記のサービスにサポートを提供しません。このようなサービスの言及は、Red Hat による製品やサービスの推奨を意味するものではありません。Red Hat は、Red Hat 外部のコンテンツを使用 (または依存) して発生した損失や費用の責任を負いません。

8.2. 3SCALE 用バックエンドコンポーネントの設定

3scale 管理者は、**backend-cron**、**backend-listener**、および **backend-worker** のデプロイメント設定で、**back-end** コンポーネントの環境変数に Redis HA (フェイルオーバー) を設定します。3scale の Redis HA には、これらの設定が必要です。



注記

Redis と Sentinel を使用するには、3scale をデプロイする前に、ポイントする Redis を設定するためにすべてのフィールドを指定して **system-redis** シークレットを作成する必要があります。3scale では、フィールドはバックエンドのパラメーターとしては提供されません。

8.2.1. backend-redis と system-redis シークレットの作成

以下の手順に従い、適宜 **backend-redis** および **system-redis** シークレットを作成します。

- HA 用 3scale の新規インストールのデプロイ
- 3scale の非 HA デプロイメントの HA への移行

8.2.2. HA 用 3scale の新規インストールのデプロイ

1. 以下のフィールドを指定して、**backend-redis** および **system-redis** シークレットを作成します。

backend-redis

```
REDIS_QUEUES_SENTINEL_HOSTS
REDIS_QUEUES_SENTINEL_ROLE
REDIS_QUEUES_URL
REDIS_STORAGE_SENTINEL_HOSTS
REDIS_STORAGE_SENTINEL_ROLE
REDIS_STORAGE_URL
```

system-redis

```
MESSAGE_BUS_NAMESPACE
MESSAGE_BUS_SENTINEL_HOSTS
MESSAGE_BUS_SENTINEL_ROLE
MESSAGE_BUS_URL
NAMESPACE
```

```
SENTINEL_HOSTS
SENTINEL_ROLE
URL
```

- Redis と Sentinel を設定する場合、**backend-redis** および **system-redis** の該当する **URL** フィールドには、**redis://[:redis-password@]redis-group[/db]** のフォーマットで Redis グループを指定します。ここで、[x] はオプションの要素 **x** を意味し、**redis-password**、**redis-group**、および **db** 変数は適切な値に置き換えてください。

  例

  ```
  redis://:redispwd@mymaster/5
  ```

- **SENTINEL_HOSTS** フィールドは、以下のフォーマットの Sentinel 接続文字列のコンマ区切りリストです。

  ```
  redis://:sentinel-password@sentinel-hostname-or-ip:port
  ```

  - リスト内の各要素に関して、[x] はオプションの要素 **x** を意味し、**sentinel-password**、**sentinel-hostname-or-ip**、および **port** 変数は適切な値に置き換えてください。

    例

    ```
    :sentinelpwd@123.45.67.009:2711,:sentinelpwd@other-sentinel:2722
    ```

- **SENTINEL_ROLE** フィールドの値は、**master** または **slave** のどちらかです。

2. 最新バージョンのテンプレートを使用して、テンプレートを使用した OpenShift への 3scale のデプロイ に記載の手順に従って 3scale をデプロイします。

   a. **backend-redis** および **system-redis** がすでに存在するために表示されるエラーは無視します。

8.2.3. 3scale の非 HA デプロイメントの HA への移行

1. HA 用 3scale の新規インストールのデプロイ に記載のとおり、すべてのフィールドを指定して **backend-redis** および **system-redis** シークレットを編集します。

2. 以下の **backend-redis** 環境変数がバックエンド Pod に対して定義されていることを確認してください。

```
name: BACKEND_REDIS_SENTINEL_HOSTS
 valueFrom:
  secretKeyRef:
   key: REDIS_STORAGE_SENTINEL_HOSTS
   name: backend-redis
name: BACKEND_REDIS_SENTINEL_ROLE
 valueFrom:
  secretKeyRef:
   key: REDIS_STORAGE_SENTINEL_ROLE
   name: backend-redis
```

3. 以下の **system-redis** の環境変数が **system-(app|sidekiq|sphinx)** Pod に対して定義されていることを確認してください。

```
name: REDIS_SENTINEL_HOSTS
  valueFrom:
    secretKeyRef:
      key: SENTINEL_HOSTS
      name: system-redis
name: REDIS_SENTINEL_ROLE
  valueFrom:
    secretKeyRef:
      key: SENTINEL_ROLE
      name: system-redis
name: MESSAGE_BUS_REDIS_SENTINEL_HOSTS
  valueFrom:
    secretKeyRef:
      key: MESSAGE_BUS_SENTINEL_HOSTS
      name: system-redis
name: MESSAGE_BUS_REDIS_SENTINEL_ROLE
  valueFrom:
    secretKeyRef:
      key: MESSAGE_BUS_SENTINEL_ROLE
      name: system-redis
```

4. 指示に従って、テンプレートを使用した 3scale 2.7 から 2.8 へのアップグレード を続行します。

8.2.3.1. Redis Enterprise の使用

1. 3 つの異なる **redis-enterprise** インスタンスで、OpenShift にデプロイされた Redis Enterprise を使用します。
    a. **system-redis** シークレットを編集します。
        i. 個別の値を **MESSAGE_BUS_NAMESPACE** および **NAMESPACE** に設定します。
        ii. **URL** と **MESSAGE_BUS_URL** を同じデータベースに設定します。
    b. **backend-redis** のバックエンドデータベースを **REDIS_QUEUES_URL** に設定します。
    c. **backend-redis** の 3 番目のデータベースを **REDIS_STORAGE_URL** に設定します。

8.2.3.2. Redis Sentinel の使用

1. 3 つまたは 4 つの異なる Redis データベースで、Redis Sentinel を使用します。
    a. **system-redis** シークレットを編集します。
        i. 個別の値を **MESSAGE_BUS_NAMESPACE** および **NAMESPACE** に設定します。
        ii. **URL** および **MESSAGE_BUS_URL** を適切な Redis グループに設定します (たとえば、**redis://:redispwd@mymaster/5**)。
        iii. **SENTINEL_HOSTS** および **MESSAGE_BUS_SENTINEL_HOSTS** を、Sentinel ホストとポートのコンマ区切りリストに設定します (たとえば、**:sentinelpwd@123.45.67.009:2711,:sentinelpwd@other-sentinel:2722**)。

iv. **SENTINEL_ROLE** および **MESSAGE_BUS_SENTINEL_ROLE** を master に設定します。

2. バックエンドの **backend-redis** シークレットを、以下の値に設定します。
   - **REDIS_QUEUES_URL**
   - **REDIS_QUEUES_SENTINEL_ROLE**
   - **REDIS_QUEUES_SENTINEL_HOSTS**
3. 3 番目のデータベースの変数を以下のように設定します。
   - **REDIS_STORAGE_URL**
   - **REDIS_STORAGE_SENTINEL_ROLE**
   - **REDIS_STORAGE_SENTINEL_HOSTS**

注記

- system-app および system-sidekiq コンポーネントは、統計を取得するために **back-end** Redis に直接接続します。
  - 3scale 2.7 の時点で、これらのシステムコンポーネントは Sentinel を使用する際にも **back-end** Redis (ストレージ) に接続することができます。
- system-app および system-sidekiq コンポーネントは、**backend-redis** ストレージ **しか使用しません** (**backend-redis** キューは使用しません)。
  - システムコンポーネントに加えた変更は、**backend-redis** ストレージと Sentinel の組み合わせをサポートします。

8.3. REDIS データベースのシャーディングおよびレプリケーション

シャーディング (パーティショニングとも呼ばれる) とは、大規模なデータベースをシャードと呼ばれる小規模なデータベースに分割することを指します。レプリケーションでは、別のマシンでホストされる同じデータベースのコピーでデータベースがセットアップされます。

シャーディング

シャーディングにより、多くのリーダーインスタンスを容易に追加することができます。また、1 つのデータベースには収まらない非常に多くのデータがある場合や、CPU 負荷が 100% に近い場合にも役立ちます。

3scale の Redis HA では、以下の 2 つの理由によりシャーディングが重要となります。

- 大量のデータを分割およびスケーリングし、特定の指標に合わせてシャード数を調整することで、ボトルネックの回避に役立つ。
- 異なるノードに処理を分散させることで、パフォーマンスが向上する (例: 複数のマシンが同じクエリーで動作している場合)。

クラスターモードが無効な Redis データベースシャーディング用の 3 つの主要なソリューションを以下に示します。

- Amazon ElastiCache

- Redis sentinel による標準 Redis
- Redis Enterprise

レプリケーション

Redis データベースのレプリケーションにより、データセットを異なるマシンに複製して冗長性を確保します。レプリケーションを使用すると、リーダーがダウンした場合に Redis の動作を維持することができます。その後、データは 1 つのインスタンス (リーダー) からプルされ、高可用性が確保されます。

3scale の Redis HA を使用すると、データベースのレプリケーションにより、プライマリーシャードの高可用性レプリカが確保されます。基本的な動作は以下のとおりです。

- プライマリーシャードに障害が発生すると、レプリカシャードが自動的に新しいプライマリーシャードにプロモートされる。
- 元のプライマリーシャードが復旧すると、自動的に新しいプライマリーシャードのレプリカシャードになる。

Redis データベースレプリケーション用の 3 つの主要なソリューションを以下に示します。

- Redis Enterprise
- Amazon ElastiCache
- Redis sentinel による標準 Redis

twemproxyを使用したシャーディング

Amazon ElastiCache および標準 Redis のシャーディングでは、キーに基づいてデータを分割します。特定のキーを与えられると探すシャードを認識するプロキシーコンポーネントが必要です (例: **twemproxy**)。nutcracker としても知られる **twemproxy** は Redis プロトコル用の軽量プロキシーソリューションで、割り当てられた特定のキーまたはサーバーのマッピングに基づいてシャードを検索します。**twemproxy** により Amazon ElastiCache または標準 Redis インスタンスにシャーディング機能を追加すると、以下のメリットが得られます。

- データを自動的に複数のサーバーにシャーディングすることができる。
- 複数のハッシュモードをサポートし、一貫性のあるハッシュおよび分散できる。
- 複数のインスタンスで実行することができ、これによりクライアントは利用可能な最初のプロキシーサーバーに接続することができる。
- バックエンドのキャッシュサーバーへの接続数を減らすことができる。

注記

Redis Enterprise は独自のプロキシーを使用するため、**twemproxy** は必要ありません。

関連情報

- Redis Sentinel Documentation
- **twemproxy**

8.4. 関連情報

- 3scale と Redis データベースのサポートについては、Red Hat 3scale API Management のサポート対象設定 を参照してください。
- Redis 向け Amazon ElastiCache の詳細は、公式のAmazon ElastiCache Documentation を参照してください。
- Redis Enterprise の詳細は、最新の ドキュメント を参照してください。

第9章 外部 MYSQL データベースの設定

本章では、*7章3scale 高可用性テンプレートおよび評価用テンプレート* の MySQL データベースを外部化する方法について説明します。そのためには、デフォルトの **amp.yml** ファイルを使用します。これは、デフォルトの **system-mysql** Pod を使用するとネットワークやファイルシステムなど複数のインフラストラクチャーの問題が生じる場合に役立ちます。

本章のアプローチと *7章3scale 高可用性テンプレートおよび評価用テンプレート* のアプローチの違いは、本アプローチでは、Red Hat 3scale API Management が最初にデフォルトの **amp.yml** テンプレートを使用していた場合に、MySQL データベースを外部化することができる点です。

注記

Red Hat は外部 MySQL データベースを使用する 3scale の設定をサポートしています。ただし、データベース自体はサポートの範囲外です。

前提条件

- 管理者権限を持つアカウントを使用して OpenShift Container Platform 3.11 クラスターにアクセスできること。
- OpenShift クラスター上にインストールされた 3scale インスタンス。*1章OpenShift への 3scale のインストール* を参照してください。

High Availability (HA) 用に外部 MySQL データベースを設定するには、以下のセクションに概略を示す手順を実施します。

- 「外部 MySQL データベースに関する制約」
- 「MySQL データベースの外部化」
- 「ロールバック」

9.1. 外部 MYSQL データベースに関する制約

MySQL データベースを外部化するプロセスの制約は以下のとおりです。

オンプレミス型 3scale のバージョン

オンプレミス型 3scale のバージョン 2.5 および 2.6 のみテストおよび検証済みです。

MySQL データベースユーザー

mysql2:// 形式の URL で、**'root'@'%'** を使用する必要があります。そうでないと、データベースへの接続に失敗します。3scale では **'root'@'%'** が使用されるため、**ユーザー名** と **パスワード** の組み合わせは、一切サポートされません。

MySQL ホスト

ホスト名 ではなく外部 MySQL データベースの **IP アドレス** を使用します。そうでない場合は、解決されません。たとえば、**mysql.mydomain.com** ではなく **1.1.1.1** を使用します。

9.2. MYSQL データベースの外部化

MySQL データベースを完全に外部化するには、以下の手順を使用します。

警告

この操作により、プロセスの進行中に環境でダウンタイムが発生します。

手順

1. オンプレミス型 3scale インスタンスをホストする OpenShift ノードにログインし、そのプロジェクトに切り替えます。

```
oc login -u <user> <url>
oc project <3scale-project>
```

<user>、**<url>**、および **<3scale-project>** を、実際のクレデンシャルとプロジェクト名に置き換えます。

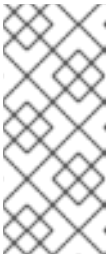
2. 以下に示す順序で手順実施し、すべての Pod をスケールダウンします。これにより、データの喪失が回避されます。

オンプレミス型 3scale の停止

OpenShift Web コンソールまたはコマンドラインインターフェイス (CLI) から、すべてのデプロイメント設定を以下の順序でゼロレプリカにスケールダウンします。

- 3scale 2.6 より前のバージョンの場合は **apicast-wildcard-router** と **zync**、3scale 2.6 以降の場合は **zync-que** と **zync**
- **apicast-staging** と **apicast-production**
- **system-sidekiq**、**backend-cron**、および **system-sphinx**
  - 3scale 2.3 の場合には **system-resque** を対象に含めます。
- **system-app**
- **backend-listener** と **backend-worker**
- **backend-redis**、**system-memcache**、**system-mysql**、**system-redis**、および **zync-database**
  以下の例は、**apicast-wildcard-router** と **zync** について、CLI でこの操作を実施する方法を示しています。

```
oc scale dc/apicast-wildcard-router --replicas=0
oc scale dc/zync --replicas=0
```



注記

各ステップのデプロイメント設定は同時にスケールダウンできます。たとえば、**apicast-wildcard-router** と **zync** を一緒にスケールダウンできます。ただし、各ステップの Pod が終了するのを待ってから、次の Pod をスケールダウンすることをお勧めします。3scale インスタンスは、完全に再起動されるまで一切アクセスできなくなります。

3. 3scale プロジェクトで実行中の Pod がないことを確認するには、以下のコマンドを使用します。

```
oc get pod
```

このコマンドは、**No resources found** を返すはずです。

4. 以下のコマンドを使用して、データベースレベルの Pod を再度スケールアップします。

```
oc scale dc/{backend-redis,system-memcache,system-mysql,system-redis,zync-database} --replicas=1
```

5. 次のステップに進む前に、**system-mysql** Pod を通じて外部 MySQL データベースにログインできることを確認してください。

```
oc rsh system-mysql-<system_mysql_pod_id>
mysql -u root -p -h <host>
```

- **<system_mysql_pod_id>**: system-mysql Pod の識別子
- ユーザーは必ず root でなければなりません。詳しくは、外部 MySQL データベースに関する制約 を参照してください。

    a. CLI に **mysql>** が表示されるようになります。**exit** と入力してから **enter** キーを押します。次のプロンプトで再度 **exit** と入力して、OpenShift ノードのコンソールに戻ります。

6. 以下のコマンドを使用して、MySQL のフルダンプを実行します。

```
oc rsh system-mysql-<system_mysql_pod_id> /bin/bash -c "mysqldump -u root --single-transaction --routines --triggers --all-databases" > system-mysql-dump.sql
```

- **<system_mysql_pod_id>** を一意の **system-mysql** Pod **ID** に置き換えます。
- 次の例のように、ファイル **system-mysql-dump.sql** に有効な MySQL レベルのダンプが含まれていることを確認します。

```
$ head -n 10 system-mysql-dump.sql
-- MySQL dump 10.13  Distrib 5.7.24, for Linux (x86_64)
--
-- Host: localhost    Database:
-- ------------------------------------------------------
-- Server version   5.7.24

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET
@OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION
*/;
/*!40101 SET NAMES utf8 */;
```

7. **system-mysql** Pod をスケールダウンし、レプリカが 0 (ゼロ) のままにします。

```
oc scale dc/system-mysql --replicas=0
```

8. **<password>** と **<host>** を適宜置き換え、URL **mysql2://root:<password>@<host>/system** の **base64** 変換値を取得します。

```
echo "mysql2://root:<password>@<host>/system" | base64
```

9. リモート MySQL データベースのデフォルトの **'user'**@'%' を作成します。これには SELECT 権限しか付与する必要はありません。また、その **base64** 変換値を取得します。

```
echo "user" | base64
echo "<password>" | base64
```

- <password> を **'user'**@'%' のパスワードに置き換えます。

10. バックアップを実行し、OpenShift シークレット **system-database** を編集します。

```
oc get secret system-database -o yaml > system-database-orig.bkp.yml
oc edit secret system-database
```

- **URL**: これを [step-8] で取得した値に置き換えます。
- **DB_USER** および **DB_PASSWORD**: 共に前のステップの値を使用します。

11. **system-mysql-dump.sql** をリモートデータベースサーバーに送信し、ダンプをインポートします。インポートには、以下のコマンドを使用します。

12. 以下のコマンドを使用して **system-mysql-dump.sql** をリモートデータベースサーバーに送信し、ダンプをサーバーにインポートします。

```
mysql -u root -p < system-mysql-dump.sql
```

13. **system** という新しいデータベースが作成されたことを確認します。

```
mysql -u root -p -se "SHOW DATABASES"
```

14. 以下の手順を使用して、**オンプレミス型 3scale を起動します**。これにより、すべての Pod が正しい順序でスケールアップされます。

オンプレミス型 3scale の起動

- **backend-redis**、**system-memcache**、**system-mysql**、**system-redis**、および **zync-database**
- **backend-listener** と **backend-worker**
- **system-app**
- **system-sidekiq**、**backend-cron**、および **system-sphinx**
  - 3scale 2.3 の場合には **system-resque** を対象に含めます。
- **apicast-staging** と **apicast-production**
- 3scale 2.6 より前のバージョンの場合は **apicast-wildcard-router** と **zync**、3scale 2.6 以降の場合は **zync-que** と **zync**

以下の例は、**backend-redis**、**system-memcache**、**system-mysql**、**system-redis**、および **zync-database** について、CLI でこの操作を実行する方法を示しています。

```
oc scale dc/backend-redis --replicas=1
oc scale dc/system-memcache --replicas=1
oc scale dc/system-mysql --replicas=1
oc scale dc/system-redis --replicas=1
oc scale dc/zync-database --replicas=1
```

system-app Pod が問題なく起動し、実行されるはずです。

15. 確認後、上記の順序 で他の Pod をスケールアップして元の状態に戻します。

16. **system-mysql DeploymentConfig** オブジェクトのバックアップを作成します。数日後、すべて正常に動作していることが確認できたら、削除してかまいません。**system-mysql DeploymentConfig** を削除することで、この手順を今後再び実行する場合の混乱を防ぐことができます。

9.3. ロールバック

ステップ 14 を実施した後、**system-app** Pod が完全には動作状態に戻らず、その根本的な原因が判断できない、または対処できない場合、ロールバックの手順を実施します。

1. **system-database-orig.bkp.yml** の元の値を使用して、シークレット **system-database** を編集します。[step-10] を参照してください。

```
oc edit secret system-database
```

URL、**DB_USER**、および **DB_PASSWORD** を元の値に置き換えます。

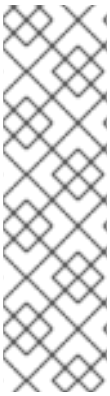
2. **system-mysql** を含め、すべての Pod をスケールダウンしてから、再度スケールアップして元の状態に戻します。**system-app** Pod およびその後に起動されるその他の Pod が、再び起動して実行されるはずです。以下のコマンドを実行して、すべての Pod が元どおりに起動、実行されていることを確認します。

```
oc get pods -n <3scale-project>
```

9.4. 関連情報

- 3scale と MySQL データベースのサポートについては、Red Hat 3scale API Management のサポート対象設定 を参照してください。

第10章 ORACLE DATABASE を使用した 3SCALE システムイメージの設定



注記

- テンプレートベースで 3scale のインストールを実行する場合には、Oracle Database は OpenShift Container Platform (OCP) 3.11 のみでサポートされます。
- operator のみで 3scale のインストールを実行する場合には、Oracle Database は OCP のバージョン 4.2 および 4.3 ではサポートされません。
- サポート対象設定の情報については、Red Hat 3scale API Management Supported Configurations のアーティクルを参照してください。

本セクションでは、Red Hat 3scale API Management の管理者が Oracle Database を使用して 3scale のシステムイメージを設定する方法を説明します。デフォルトでは、3scale 2.8 には設定データを MySQL データベースに保管する system というコンポーネントが含まれています。このデフォルトのデータベースをオーバーライドし、情報を外部の Oracle Database に保管することができます。本章の手順に従って、独自の Oracle Database クライアントバイナリーでカスタムのシステムコンテナーイメージをビルドし、3scale を OpenShift にデプロイします。

前提条件

以下の Oracle ソフトウェアコンポーネントの サポート対象バージョン

- Oracle Instant Client パッケージ: Basic または Basic Light
- Oracle Instant Client パッケージ: SDK
- Oracle Instant Client パッケージ: ODBC

パッケージの例

- instantclient-basiclite-linux.x64-12.2.0.1.0.zip または instantclient-basic-linux.x64-12.2.0.1.0.zip
- instantclient-sdk-linux.x64-12.2.0.1.0.zip
- instantclient-odbc-linux.x64-12.2.0.1.0-2.zip

Oracle Database を使用して 3scale のシステムイメージを設定するには、以下のセクションに概略を示す手順を実施します。

- 「Oracle Database の準備」
- 「システムイメージのビルド」

10.1. ORACLE DATABASE の準備

本セクションでは、Oracle Database を準備する手順を説明します。

前提条件

- OpenShift クラスターからアクセスできる Oracle Database の サポート対象バージョン

- インストール手順に必要な Oracle Database の **system** ユーザーへのアクセス
- 3scale 2.8 **amp.yml** テンプレート

手順

1. 新しいデータベースを作成します。
   Oracle Database が 3scale と動作するようにするには、以下の設定が必要です。

```
ALTER SYSTEM SET max_string_size=extended SCOPE=SPFILE;
ALTER SYSTEM SET compatible='12.2.0.1' SCOPE=SPFILE;
```

2. データベースの詳細を収集します。
   3scale の設定に必要な以下の情報を取得します。
   - Oracle Database の URL
   - Oracle Database の サービス名
   - Oracle Database の **システム** のパスワード
     DATABASE_URL パラメーターは、**oracle-enhanced://${user}:${password}@${host}:${port}/${database}** の形式にする必要があります。

例

```
DATABASE_URL="oracle-enhanced://user:password@my-oracle-
database.com:1521/threescalepdb"
```

関連情報

- Oracle Database での新規データベース作成については、Oracle のドキュメント を参照してください。

10.2. システムイメージのビルド

本セクションでは、システムイメージをビルドする手順について説明します。

前提条件

- Oracle Database の準備 の手順をすべて実行しているようにしてください。

手順

1. 3scale API Management OpenShift Templates GitHub リポジトリーをクローンします。以下のコマンドを使用します。

```
$ git clone --branch 2.8.0.GA https://github.com/3scale/3scale-amp-openshift-templates.git
```

2. Oracle Database の Instant Client パッケージファイルを **3scale-amp-openshift-templates/amp/system-oracle/oracle-client-files** ディレクトリーに置きます。
3. 3scale 2.8 **amp.yml** テンプレートをダウンロードします。

4. **-f** オプションで **build.yml** OpenShift テンプレートを指定して、**oc new-app** コマンドを実行します。

```
$ oc new-app -f build.yml
```

5. **-f** オプションで **amp.yml** OpenShift テンプレートを指定し、**-p** オプションで **WILDCARD_DOMAIN** パラメーターに OpenShift クラスターのドメインを指定して、**oc new-app** コマンドを実行します。

```
$ oc new-app -f amp.yml -p WILDCARD_DOMAIN=mydomain.com
```

6. 以下の **oc patch** コマンドを入力します。**SYSTEM_PASSWORD** はOracle Database の準備 で設定した Oracle Database の **system** パスワードに置き換えます。

```
$ oc patch dc/system-app -p '[{"op": "add", "path":
"/spec/strategy/rollingParams/pre/execNewPod/env/-", "value": {"name":
"ORACLE_SYSTEM_PASSWORD", "value": "SYSTEM_PASSWORD"}}]' --type=json

$ oc patch dc/system-app -p '{"spec": {"strategy": {"rollingParams": {"post":{"execNewPod":
{"env": [{"name": "ORACLE_SYSTEM_PASSWORD", "value":
"SYSTEM_PASSWORD"}]}}}}}}'
```

7. 以下のコマンドを入力します。**DATABASE_URL** はOracle Database の準備 で指定した Oracle Database を参照するように置き換えます。

```
$ oc patch secret/system-database -p '{"stringData": {"URL": "DATABASE_URL"}}'
```

8. 以下のコマンドを実行してプルシークレットをビルダーにリンクします。

```
$ oc secrets link builder threescale-registry-auth
```

9. **oc start-build** コマンドを入力し、新しいシステムイメージをビルドします。

```
$ oc start-build 3scale-amp-system-oracle --from-dir=.
```

- 3scale と Oracle Database のサポートについては、Red Hat 3scale API Management のサポート対象設定 を参照してください。