



# OpenShift Container Platform 4.12

## イメージ

OpenShift Container Platform でのイメージおよびイメージストリームの作成および管理



# OpenShift Container Platform 4.12 イメージ

---

OpenShift Container Platform でのイメージおよびイメージストリームの作成および管理

## 法律上の通知

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 概要

本書では、OpenShift Container Platform でイメージおよびイメージストリームを作成し、管理する方法を説明します。さらに、テンプレートの使用方法についても説明します。

## 目次

|  |           |
|--|-----------|
| <b>第1章 イメージの概要</b> .....   | <b>4</b>  |
| 1.1. コンテナ、イメージおよびイメージストリームについて   | 4         |
| 1.2. イメージ  | 4         |
| 1.3. イメージレジストリー  | 4         |
| 1.4. イメージリポジトリー  | 4         |
| 1.5. イメージタグ  | 5         |
| 1.6. イメージ ID   | 5         |
| 1.7. コンテナ  | 5         |
| 1.8. イメージストリームを使用する理由  | 5         |
| 1.9. イメージストリームタグ   | 7         |
| 1.10. イメージストリームイメージ  | 7         |
| 1.11. イメージストリームトリガー  | 7         |
| 1.12. CLUSTER SAMPLES OPERATOR の使用方法                                     | 7         |
| 1.13. テンプレートについて   | 7         |
| 1.14. RUBY ON RAILS の使い方   | 7         |
| <b>第2章 CLUSTER SAMPLES OPERATOR の設定</b> .....                            | <b>9</b>  |
| 2.1. CLUSTER SAMPLES OPERATOR について                                       | 9         |
| 2.2. CLUSTER SAMPLES OPERATOR の設定パラメーター                                  | 12        |
| 2.3. CLUSTER SAMPLES OPERATOR 設定へのアクセス                                   | 14        |
| 2.4. CLUSTER SAMPLES OPERATOR からの非推奨のイメージストリームタグの削除                      | 15        |
| <b>第3章 代替レジストリーでの CLUSTER SAMPLES OPERATOR の使用</b> .....                 | <b>16</b> |
| 3.1. ミラーレジストリーについて   | 16        |
| 3.2. イメージのミラーリングを可能にする認証情報の設定  | 19        |
| 3.3. OPENSIFT CONTAINER PLATFORM イメージリポジトリーのミラーリング                       | 20        |
| 3.4. 代替のレジストリーまたはミラーリングされたレジストリーでの CLUSTER SAMPLES OPERATOR イメージストリームの使用 | 24        |
| <b>第4章 イメージの作成</b> .....   | <b>27</b> |
| 4.1. コンテナのベストプラクティスについて  | 27        |
| 4.2. イメージへのメタデータの組み込み  | 33        |
| 4.3. SOURCE-TO-IMAGE によるソースコードからのイメージの作成                                 | 34        |
| 4.4. SOURCE-TO-IMAGE イメージのテストについて  | 37        |
| <b>第5章 イメージの管理</b> .....   | <b>41</b> |
| 5.1. イメージの管理の概要  | 41        |
| 5.2. イメージのタグ付け   | 41        |
| 5.3. イメージプルポリシー  | 44        |
| 5.4. イメージプルシークレットの使用   | 45        |
| <b>第6章 イメージストリームの管理</b> .....  | <b>50</b> |
| 6.1. イメージストリームを使用する理由  | 50        |
| 6.2. イメージストリームの設定  | 51        |
| 6.3. イメージストリームイメージ   | 52        |
| 6.4. イメージストリームタグ   | 52        |
| 6.5. イメージストリーム変更トリガー   | 53        |
| 6.6. イメージストリームのマッピング   | 54        |
| 6.7. イメージストリームの使用  | 56        |
| 6.8. プライベートレジストリーからのイメージおよびイメージストリームのインポート                               | 60        |
| 6.9. IMAGESTREAMIMPORT によるマニフェストリストのインポート                                | 62        |
| <b>第7章 KUBERNETES リソースでのイメージストリームの使用</b> .....                           | <b>64</b> |

---

|  |            |
|--|------------|
| 7.1. KUBERNETES リソースでのイメージストリームの有効化                | 64         |
| <b>第8章 イメージストリームの変更時の更新のトリガー</b> .....             | <b>66</b>  |
| 8.1. OPENSIFT CONTAINER PLATFORM リソース              | 66         |
| 8.2. KUBERNETES リソースのトリガー                          | 66         |
| 8.3. KUBERNETES リソースでのイメージトリガーの設定                  | 67         |
| <b>第9章 イメージ設定リソース</b> .....                        | <b>68</b>  |
| 9.1. イメージコントローラー設定パラメーター                           | 68         |
| 9.2. イメージレジストリーの設定                                 | 70         |
| <b>第10章 テンプレートの使用</b> .....                        | <b>91</b>  |
| 10.1. テンプレートについて                                   | 91         |
| 10.2. テンプレートのアップロード                                | 91         |
| 10.3. WEB コンソールを使用したアプリケーションの作成                    | 91         |
| 10.4. CLI を使用してテンプレートからオブジェクトを作成する手順               | 92         |
| 10.5. アップロードしたテンプレートの変更                            | 95         |
| 10.6. インスタントアプリとクイックスタートテンプレートの使用                  | 95         |
| 10.7. テンプレートの作成                                    | 96         |
| <b>第11章 RUBY ON RAILS の使用</b> .....                | <b>111</b> |
| 11.1. 前提条件   | 111        |
| 11.2. データベースの設定                                    | 111        |
| 11.3. アプリケーションの作成                                  | 112        |
| 11.4. アプリケーションの OPENSIFT CONTAINER PLATFORM へのデプロイ | 115        |
| <b>第12章 イメージの使用</b> .....                          | <b>119</b> |
| 12.1. イメージの使用の概要                                   | 119        |
| 12.2. SOURCE-TO-IMAGE (S2I)                        | 119        |
| 12.3. SOURCE-TO-IMAGE イメージのカスタマイズ                  | 120        |



# 第1章 イメージの概要

## 1.1. コンテナ、イメージおよびイメージストリームについて

コンテナ、イメージ、およびイメージストリームは、コンテナ化されたソフトウェアを作成し、管理する際に理解しておくべき重要な概念です。イメージは、コンテナがコンテナイメージの実行中のインスタンスである場合に、実行の準備ができている一連のソフトウェアを保持します。イメージストリームは、同一の基本的なイメージの異なるバージョンを保存する1つの方法です。それらの異なるバージョンは、同じイメージ名の異なるタグによって表されます。

## 1.2. イメージ

OpenShift Container Platform のコンテナは OCI または Docker 形式のコンテナの **イメージ** をベースにしています。イメージは、単一コンテナを実行するためのすべての要件、およびそのニーズおよび機能を記述するメタデータを含むバイナリーです。

これはパッケージ化テクノロジーとして考えることができます。コンテナには、作成時にコンテナに追加のアクセスを付与しない限り、イメージで定義されるリソースにのみアクセスできます。同じイメージを複数のホストにまたがって複数のコンテナにデプロイし、それらの間で負荷を分散することにより、OpenShift Container Platform はイメージにパッケージ化されたサービスの冗長性および水平的なスケーリングを提供できます。

イメージをビルドするために **podman** または **docker** CLI を直接使用することはできますが、OpenShift Container Platform は、コードまたは設定を既存イメージに追加して新規イメージの作成を支援するビルダーイメージも提供します。

アプリケーションは一定期間をかけて開発されるため、単一のイメージ名が同じイメージの数多くの異なるバージョンを参照する場合があります。それぞれの異なるイメージは、通常は 12 文字 (例: **fd44297e2ddb**) に省略されるそのハッシュ (**fd44297e2ddb050ec4f...** などの長い 16 進数) で一意に参照されます。

コンテナイメージを **作成**、**管理**、および**使用**できます。

## 1.3. イメージレジストリー

イメージレジストリーは、コンテナイメージを保管し、提供するコンテナサーバーです。以下に例を示します。

```
registry.redhat.io
```

レジストリーには、1つ以上のタグ付けされたイメージを持つ1つ以上のイメージリポジトリーのコレクションが含まれます。Red Hat は、サブスクリプションをお持ちのお客様に対して **registry.redhat.io** でレジストリーを提供しています。OpenShift Container Platform は、カスタムコンテナイメージを管理するための独自の OpenShift イメージレジストリーを提供することもできます。

## 1.4. イメージリポジトリー

イメージリポジトリーは、関連するコンテナイメージおよびそれらを特定するタグのコレクションです。たとえば、OpenShift Container Platform Jenkins イメージはリポジトリーにあります。

```
docker.io/openshift/jenkins-2-centos7
```



## 1.5. イメージタグ

イメージタグは、イメージストリーム内の他のイメージから特定のイメージを識別するリポジトリのコンテナイメージに適用されるラベルです。通常、タグはある種のバージョン番号を表します。たとえば、ここでは **:v3.11.59-2** がタグになります。

```
registry.access.redhat.com/openshift3/jenkins-2-rhel7:v3.11.59-2
```

イメージにタグを追加することができます。たとえば、イメージには **:v3.11.59-2** および **:latest** というタグが割り当てられる可能性があります。

OpenShift Container Platform は **docker tag** コマンドに似た **oc tag** コマンドを提供しますが、これらはイメージ上で直接動作するのではなくイメージストリームで動作します。

## 1.6. イメージ ID

イメージ ID は、イメージをプルするために使用できる SHA (Secure Hash Algorithm) コードです。SHA イメージ ID は変更できません。特定の SHA ID は同一のコンテナイメージコンテンツを常に参照します。以下に例を示します。

```
docker.io/openshift/jenkins-2-centos7@sha256:ab312bda324
```

## 1.7. コンテナ

OpenShift Container Platform アプリケーションの基本的な単位は **コンテナ**と呼ばれています。[Linux コンテナテクノロジー](#) は、指定されたリソースのみと対話するために実行中のプロセスを分離する軽量なメカニズムです。このコンテナという用語は、コンテナイメージの実行中または一時停止している特定のインスタンスとして定義されています。

数多くのアプリケーションインスタンスは、相互のプロセス、ファイル、ネットワークなどを可視化せずに単一ホストのコンテナで実行される可能性があります。通常、コンテナは任意のワークロードで使用されますが、各コンテナは Web サーバーまたはデータベースなどの (通常はマイクロサービスと呼ばれることの多い) 単一サービスを提供します。

Linux カーネルは数年にわたりコンテナテクノロジーの各種機能を統合してきました。Docker プロジェクトはホスト上の Linux コンテナの便利な管理インターフェイスを開発しました。さらに最近では、[Open Container Initiative](#) により、コンテナ形式およびコンテナランタイムのオープン標準が策定されています。OpenShift Container Platform および Kubernetes は複数ホストのインストール間で OCI および Docker 形式のコンテナのオーケストレーションを実行する機能を追加しています。

OpenShift Container Platform を使用する際にコンテナランタイムと直接対話することはありませんが、それらの OpenShift Container Platform におけるロールやコンテナ内でのアプリケーションの機能を理解する上で、それらの機能および用語を理解しておくことは重要です。

[podman](#) などのツールは、コンテナを直接実行し、管理するための **docker** コマンドラインツールを置き換えるために使用できます。**podman** を使用すると、OpenShift Container Platform と切り離してコンテナの実験を行うことができます。

## 1.8. イメージストリームを使用する理由

イメージストリームおよびその関連付けられたタグは、OpenShift Container Platform 内でコンテナイメージを参照するための抽象化を提供します。イメージストリームとそのタグを使用して、利用可能なイメージを確認し、リポジトリのイメージが変更される場合でも必要な特定のイメージを使用していることを確認できます。

イメージストリームには実際のイメージデータは含まれませんが、イメージリポジトリと同様に、関連するイメージの単一の仮想ビューが提示されます。

ビルドおよびデプロイメントをそれぞれ実行し、ビルドおよびデプロイメントを、新規イメージが追加される際やこれに対応する際の通知をイメージストリームで確認できるように設定できます。

たとえば、デプロイメントで特定のイメージを使用していて、そのイメージの新規バージョンが作成される場合、デプロイメントを、そのイメージの新規バージョンを選択できるように自動的に実行します。

デプロイメントまたはビルドで使用するイメージストリームタグが更新されない場合には、コンテナイメージレジストリーのコンテナイメージが更新されても、ビルドまたはデプロイメントは以前の、既知でおそらく適切であると予想されるイメージをそのまま使用します。

ソースイメージは以下のいずれかに保存できます。

- OpenShift Container Platform の統合レジストリー
- registry.redhat.io or Quay.io などの外部レジストリー
- OpenShift Container Platform クラスターの他のイメージストリーム

ビルドまたはデプロイメント設定などのイメージストリームタグを参照するオブジェクトを定義する場合には、リポジトリではなく、イメージストリームタグを参照します。アプリケーションのビルドまたはデプロイ時に、OpenShift Container Platform がこのイメージストリームタグを使用してリポジトリに対してクエリーし、対象のイメージに関連付けられた ID を特定して、そのイメージを使用します。

イメージストリームメタデータは他のクラスター情報と共に etcd インスタンスに保存されます。

イメージストリームの使用には、いくつかの大きな利点があります。

- コマンドラインを使用して再プッシュすることなく、タグ付けや、タグのロールバック、およびイメージの迅速な処理を実行できます。
- 新規イメージがレジストリーにプッシュされると、ビルドおよびデプロイメントをトリガーできます。また、OpenShift Container Platform には他のリソースの汎用トリガーがあります (Kubernetes オブジェクトなど)。
- 定期的な再インポートを実行するためにタグにマークを付けることができます。ソースイメージが変更されると、その変更は選択され、イメージストリームに反映されます。これにより、ビルドまたはデプロイメント設定に応じてビルドまたはデプロイメントフローがトリガーされます。
- 詳細なアクセス制御を使用してイメージを共有し、チーム間でイメージを迅速に分散できます。
- ソースイメージが変更されると、イメージストリームタグはイメージの既知の適切なバージョンをポイントしたままになり、アプリケーションが予期せずに損傷しないようにします。
- イメージストリームオブジェクトのパーミッションを使用して、イメージを表示し、使用できるユーザーについてセキュリティーを設定することができます。
- クラスターレベルでイメージを読み込んだり、リスト表示するパーミッションのないユーザーは、イメージストリームを使用してプロジェクトでタグ付けされたイメージを取得できます。

イメージストリームを管理し、Kubernetes リソースでイメージストリームを使用し、イメージストリームの更新で更新をトリガーできます。

## 1.9. イメージストリームタグ

イメージストリームタグは、イメージストリームのイメージに対する名前付きポインターです。イメージストリームタグはコンテナイメージタグに似ています。

## 1.10. イメージストリームイメージ

イメージストリームイメージは、これがタグ付けされている特定のイメージストリームから特定のコンテナイメージを取得できるようにします。イメージストリームイメージは、特定のイメージの SHA ID についてのメタデータをプルする API リソースオブジェクトです。

## 1.11. イメージストリームトリガー

イメージストリームのトリガーは、イメージストリームタグの変更時に特定のアクションを生じさせます。たとえば、インポートにより、タグの値が変更され、これによりデプロイメント、ビルドまたはそれらをリッスンする他のリソースがある場合にトリガーが実行されます。

## 1.12. CLUSTER SAMPLES OPERATOR の使用方法

初期の起動時に、Operator はデフォルトサンプルを作成してイメージストリームおよびテンプレートの作成を開始します。Cluster Samples Operator は、**openshift** namespace に保存されるサンプルイメージストリームおよびテンプレートを管理できます。

クラスター管理者は、Cluster Samples Operator を使用して次のことができます。

- [オペレーターの設定](#)
- [代替レジストリーで Operator の使用](#)

## 1.13. テンプレートについて

テンプレートは、複製されるオブジェクトの定義です。[テンプレート](#) を使用して、設定を構築およびデプロイできます。

## 1.14. RUBY ON RAILS の使い方

開発者は、[Ruby on Rails](#) を使用して次のことができます。

- アプリケーションを作成します。
  - データベースを設定します。
  - ウェルカムページを作成します。
  - OpenShift Container Platform 用にアプリケーションを設定します。
  - アプリケーションを Git に保存します。
- OpenShift Container Platform にアプリケーションをデプロイします。
  - データベースサービスを作成します。

- フロントエンドサービスを作成します。
- アプリケーションのルートを作成します。

## 第2章 CLUSTER SAMPLES OPERATOR の設定

**openshift** namespace で動作する Cluster Samples Operator は、Red Hat Enterprise Linux (RHEL) ベースの OpenShift Container Platform イメージストリームおよび OpenShift Container Platform テンプレートを実インストールし、更新します。

### 2.1. CLUSTER SAMPLES OPERATOR について

Operator はインストール時に独自にデフォルト設定オブジェクトを作成し、その後にクイックスタートテンプレートを含む、サンプルのイメージストリームおよびテンプレートを作成します。

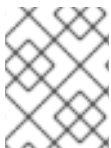


#### 注記

認証情報を必要とする他のレジストリーからのイメージストリームのインポートを容易にするには、クラスター管理者は、イメージのインポートに必要な Docker **config.json** ファイルの内容を含む追加のシークレットを **openshift** namespace に作成できます。

Cluster Samples Operator 設定はクラスター全体で使用されるリソースであり、デプロイメントは **openshift-cluster-samples-operator** namespace 内に含まれます。

Cluster Samples Operator のイメージには、関連付けられた OpenShift Container Platform リリースのイメージストリームおよびテンプレートの定義が含まれます。各サンプルが作成または更新されると、Cluster Samples Operator には OpenShift Container Platform のバージョンを示すアノテーションが含まれます。Operator はこのアノテーションを使用して、各サンプルをリリースバージョンに一致させるようにします。このインベントリーの外にあるサンプルは省略されるサンプルであるために無視されます。バージョンのアノテーションが変更または削除されると、Operator が管理するサンプルに変更が加えてもそれらの変更は自動的に元に戻されます。



#### 注記

Jenkins イメージはインストールからのイメージペイロードの一部であり、イメージストリームに直接タグ付けされます。

Cluster Samples Operator 設定リソースには、削除時に以下を消去するファイナライザーが含まれます。

- Operator 管理のイメージストリーム
- Operator 管理のテンプレート
- Operator が生成する設定リソース
- クラスターステータスのリソース

サンプルリソースの削除時に、Cluster Samples Operator はデフォルト設定を使用してリソースを再作成します。

#### 2.1.1. Cluster Samples Operator の管理状態の使用

Cluster Samples Operator はデフォルトで **Managed** としてブートストラップされるか、グローバルプロキシが設定されている場合にブートストラップされます。**Managed** 状態で、Cluster Samples Operator は、イメージストリームおよびイメージをレジストリーからプルし、必要なサンプルテンプレートがインストールされた状態になるように、リソースをアクティブに管理し、コンポーネントをアクティブな状態に維持します。

以下を含む特定の状況では、Cluster Samples Operator が **Removed** としてそれ自体をブートストラップします。

- Cluster Samples Operator が、クリーンインストール後の初回起動から 3 分後に [registry.redhat.io](https://registry.redhat.io) に到達できない場合。
- Cluster Samples Operator がこれが IPv6 ネットワーク上にあることを検出する場合。
- [イメージコントローラーの設定パラメーター](#)により、デフォルトのイメージレジストリーまたは [samplesRegistry](#) 設定で指定されたイメージレジストリーを使用してイメージストリームを作成できない場合。



### 注記

OpenShift Container Platform の場合、デフォルトのイメージレジストリーは [registry.redhat.io](https://registry.redhat.io) です。

ただし、Cluster Samples Operator がそれが IPv6 ネットワーク上にあり、OpenShift Container Platform グローバルプロキシが設定されていることを検出した場合は、IPv6 チェックがすべてのチェックに取って代わります。その結果、Cluster Samples Operator はそれ自体を **Removed** としてブートストラップします。



### 重要

現在、IPv6 インストールは [registry.redhat.io](https://registry.redhat.io) によってサポートされていません。Cluster Samples Operator は、ほとんどのサンプルイメージストリームおよびイメージを [registry.redhat.io](https://registry.redhat.io) からプルします。

#### 2.1.1.1. ネットワークが制限されたインストール

[registry.redhat.io](https://registry.redhat.io) にアクセスできない場合に **Removed** としてすると、ネットワークの制限がすでに有効な場合にネットワークが制限されたインストールを容易にします。ネットワークアクセスが制限されている場合に **Removed** としてインストールすると、クラスター管理者がサンプルが必要かどうかを判別する時間をより長く確保できます。これは、Cluster Samples Operator は管理状態が **Removed** に設定されている場合にサンプルのイメージストリームのインポートに失敗しているアラートを送信しないためです。Cluster Samples Operator が **Managed** として起動し、サンプルイメージストリームのインストールを試みると、インポートに失敗している場合に初回インストールから 2 時間後にアラートが開始されます。

#### 2.1.1.2. 初期のネットワークアクセスが設定された状態でのネットワークが制限されたインストール

ネットワークが制限された環境のクラスターまたは非接続クラスターとすることが意図されたクラスターが、ネットワークアクセスがある状態で最初にインストールされた場合、Cluster Samples Operator はアクセス可能なために [registry.redhat.io](https://registry.redhat.io) からコンテンツをインストールします。Cluster Samples Operator を **Removed** としてブートストラップして、必要なサンプルを判別するまでサンプルのインストールを遅らせる場合、イメージミラーのセットアップなどを行ってから、代替レジストリーで Samples Operator を使用し、ノードをカスタマイズする手順 (どちらも追加のリソースセクションにリンクされている) に従い、Cluster Samples Operator のデフォルト設定を上書きし、最初に **Removed** として起動します。

以下の追加の YAML ファイルを、`openshift-install create manifest` で作成される `openshift` ディレクトリーに置く必要があります。

## managementState: Removed が設定された Cluster Samples Operator YAML ファイルのサンプル

```
apiVersion: samples.operator.openshift.io/v1
kind: Config
metadata:
  name: cluster
spec:
  architectures:
  - x86_64
  managementState: Removed
```

### 2.1.2. Cluster Samples Operator でのイメージストリームのインポートの追跡およびエラー回復

サンプルイメージストリームの作成または更新後に、Cluster Samples Operator はそれぞれのイメージストリームタグのイメージインポートの進捗をモニターします。

インポートが失敗すると、Cluster Samples Operator はイメージストリームイメージインポート API を使用してインポートを再試行します。これは **oc import-image** コマンドで使用されるのと同じ API であり、インポートの成功が確認されるまで約 15 分ごとに、またはイメージストリームのいずれかが **skippedImagestreams** 一覧に追加されるように Cluster Samples Operator の設定が変更されるか、管理状態が **Removed** に変更される場合に再試行されます。

#### 関連情報

- Cluster Samples Operator がインストール時に削除される場合、[Cluster Samples Operator を代替レジストリーと共に使用](#) し、コンテンツをインポートし、サンプルを取得するために Cluster Samples Operator を **Managed** に設定できるようにします。
- Cluster Samples Operator を初期のネットワークアクセスのある状態でネットワークが制限されたインストールで **Removed** としてブートラップし、必要なサンプルを判別するまでサンプルのインストールを遅らせる場合、[ノードのカスタマイズ](#) についての手順に従い、Cluster Samples Operator のデフォルト設定を上書きし、最初に **Removed** として起動させます。
  - 非接続環境でサンプルをホストするには、[代替レジストリーで Cluster Samples Operator を使用する](#) 手順に従います。

### 2.1.3. ミラーリングの Cluster Samples Operator のサポート

インストール時に、OpenShift Container Platform は **imagestreamtag-to-image** という名前の設定マップを **openshift-cluster-samples-operator** namespace に作成します。**imagestreamtag-to-image** 設定マップには、各イメージストリームタグのエントリー (設定されるイメージ) が含まれます。

設定マップの data フィールドの各エントリーのキーの形式は、**<image\_stream\_name>\_<image\_stream\_tag\_name>** です。

OpenShift Container Platform の非接続インストール時に、Cluster Samples Operator のステータスは **Removed** に設定されます。これを **Managed** に変更することを選択する場合、サンプルがインストールされます。



## 注記

ネットワークが制限されている環境または切断されている環境でサンプルを使用するには、ネットワークの外部のサービスにアクセスする必要がある場合があります。サービスの例には、Github、Maven Central、npm、RubyGems、PyPi などがあります。場合によっては、Cluster Samples Operator のオブジェクトが必要なサービスに到達できるようにするために、追加の手順を実行する必要があります。

この config map は、イメージストリームをインポートするためにミラーリングする必要があるイメージの参照情報として使用できます。

- Cluster Samples Operator が **Removed** に設定される場合、ミラーリングされたレジストリーを作成するか、使用する必要がある既存のミラーリングされたレジストリーを判別できます。
- 新しい config map をガイドとして使用し、ミラーリングされたレジストリーに必要なサンプルをミラーリングします。
- Cluster Samples Operator 設定オブジェクトの **skippedImagestreams** リストに、ミラーリングされていないイメージストリームを追加します。
- Cluster Samples Operator 設定オブジェクトの **samplesRegistry** をミラーリングされたレジストリーに設定します。
- 次に、Cluster Samples Operator を **Managed** に設定し、ミラーリングしたイメージストリームをインストールします。

詳細の手順については、[代替のレジストリーまたはミラーリングされたレジストリーでの Cluster Samples Operator イメージストリームの使用](#) について参照してください。

## 2.2. CLUSTER SAMPLES OPERATOR の設定パラメーター

サンプルリソースは以下の設定フィールドを提供します。

| パラメーター                 | 説明   |
|------------------------|--|
| <b>managementState</b> | <p><b>Managed:</b> Cluster Samples Operator は設定の指示に応じてサンプルを更新します。</p> <p><b>Unmanaged:</b> Cluster Samples Operator は、その設定リソースオブジェクトおよび <b>openshift</b> namespace のイメージストリームまたはテンプレートへの更新を無視します。</p> <p><b>Removed:</b> Cluster Samples Operator は <b>openshift</b> namespace の一連の <b>Managed</b> 状態のイメージストリームおよびテンプレートを除去します。これは、クラスター管理者によって作成される新規サンプルや、省略されたリストにあるサンプルを無視します。除去されると、Cluster Samples Operator は <b>Unmanaged</b> 状態にあるかのように機能し、サンプルリソース、イメージストリーム、またはテンプレートに対する監視イベントを無視します。</p> |



| パラメーター                     | 説明   |
|----------------------------|--|
| <b>samplesRegistry</b>     | <p>イメージコンテンツについてイメージストリームがアクセスするレジストリーを指定できます。<b>samplesRegistry</b> はデフォルトで OpenShift Container Platform の <b>registry.redhat.io</b> に設定されます。</p> <div style="display: flex; align-items: flex-start;"> <div style="width: 20px; height: 100px; border: 1px solid black; background: repeating-linear-gradient(45deg, transparent, transparent 2px, black 2px, black 4px); margin-right: 10px;"></div> <div> <p><b>注記</b></p> <p>RHEL コンテンツの作成または更新は、<b>Samples Registry</b> が明示的に設定されていない場合、空の文字列を残す場合やこれが registry.redhat.io に設定されている場合にプルアクセスのシークレットが有効でないと開始されません。いずれの場合も、イメージのインポートは registry.redhat.io の外で機能し、これには認証情報が必要になります。</p> <p>RHEL コンテンツの作成または更新は、<b>Samples Registry</b> が空の文字列または registry.redhat.io 以外の値に上書きされる場合、プルシークレットの存在によって制御されることはありません。</p> </div> </div> |
| <b>architectures</b>       | アーキテクチャーのタイプを選択するためのプレースホルダー。  |
| <b>skippedImagestreams</b> | Cluster Samples Operator のインベントリーにあるものの、クラスター管理者が Operator に無視させるか、管理させないようにするイメージストリーム。このパラメーターにイメージストリーム名のリストを追加できます。例:<br><b>["httpd","perl"]</b>   |
| <b>skippedTemplates</b>    | Cluster Samples Operator のインベントリーにあるものの、クラスター管理者が Operator に無視させるか、管理させないようにするテンプレート。  |

シークレット、イメージストリーム、およびテンプレート監視イベントは、初期サンプルリソースオブジェクトの作成前に追加することができ、Cluster Samples Operator はイベントを検出し、再度キューに入れます。

### 2.2.1. 設定の制限

Cluster Samples Operator が複数のアーキテクチャーをサポートする際に、アーキテクチャーのリストは、**Managed** 状態の場合は変更できません。

アーキテクチャーの値を変更するために、クラスター管理者は以下を実行する必要があります。

- **Management State** に **Removed** のマークを付け、変更を保存します。
- その後の変更では、アーキテクチャーを編集し、**Management State** を **Managed** に戻します。

Cluster Samples Operator は **Removed** 状態の場合に依然としてシークレットを処理します。**Removed** に切り替える前にシークレットを作成でき、**Managed** に切り替える前の **Removed** 状態で、または **Managed** 状態に切り替えた後にシークレットを作成できます。**Managed** への切り替え後にシークレットを作成する場合に、シークレットイベントが処理されるまでサンプルの作成に遅延が

生じます。これは、レジストリーの変更を容易にするために実行されます。ここでは、クリーンな状態にするために、切り替え前にすべてのサンプルを削除することを選択できます。切り替え前にすべてのサンプルを削除する必要はありません。

### 2.2.2. 条件

サンプルリソースには以下の条件とそのステータスが適用されます。

| 条件                            | 説明   |
|-------------------------------|--|
| <b>SamplesExists</b>          | サンプルが <b>openshift</b> namespace に作成されていることを示します。  |
| <b>ImageChangesInProgress</b> | <p><b>True</b> イメージストリームが作成または更新される場合に、タグ仕様の生成およびタグステータスの生成のすべてが一致する訳ではありません。</p> <p><b>False</b> すべての生成が一致するか、修復不可能なエラーがインポート時に発生した場合、最後に表示されるエラーは message フィールドに置かれます。保留中のイメージストリームのリストは reason フィールドに置かれます。</p> <p>これは OpenShift Container Platform では非推奨にされています。</p> |
| <b>ConfigurationValid</b>     | 前述の制限された変更のいずれかが送信されるかどうかに応じて <b>True</b> または <b>False</b> になります。  |
| <b>RemovePending</b>          | <b>Management State: Removed</b> 設定が保留中であるものの、Cluster Samples Operator は削除が完了するまで待機していることを示します。  |
| <b>ImportImageErrorsExist</b> | <p>イメージストリームのタグのいずれかについて、イメージストリームでイメージインポートフェーズにエラーがあったことを示すインジケーター。</p> <p><b>True</b> エラーが発生した場合。エラーのあるイメージストリームのリストは reason フィールドに置かれます。報告されるそれぞれのエラーの詳細は message フィールドに置かれます。</p>   |
| <b>MigrationInProgress</b>    | <p><b>True:</b> バージョンが現在のサンプルセットのインストールに使用した Samples Operator バージョンと異なることを Samples Operator が検知する場合。</p> <p>これは OpenShift Container Platform では非推奨にされています。</p>   |

## 2.3. CLUSTER SAMPLES OPERATOR 設定へのアクセス

Cluster Samples Operator は、提供されるパラメーターでファイルを編集して設定できます。

### 前提条件

- OpenShift CLI (**oc**) がインストールされている。

### 手順

- Cluster Samples Operator 設定にアクセスします。

```
$ oc edit configs.samples.operator.openshift.io/cluster -o yaml
```

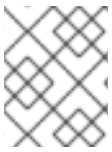
Cluster Samples Operator 設定は以下の例のようになります。

```
apiVersion: samples.operator.openshift.io/v1
kind: Config
# ...
```

## 2.4. CLUSTER SAMPLES OPERATOR からの非推奨のイメージストリームタグの削除

Cluster Samples Operator は、ユーザーが非推奨のイメージストリームタグを使用するデプロイメントを持っている可能性があるため、非推奨のイメージストリームタグをイメージストリームに残します。

**oc tag** コマンドでイメージストリームを編集して、非推奨のイメージストリームタグを削除できます。



### 注記

サンプルプロバイダーがイメージストリームから削除した非推奨のイメージストリームタグは初期インストールに含まれません。

### 前提条件

- **oc** CLI をインストールしていること。

### 手順

- **oc tag** コマンドでイメージストリームを編集して、非推奨のイメージストリームタグを削除します。

```
$ oc tag -d <image_stream_name:tag>
```

### 出力例

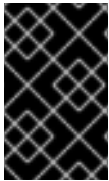
```
Deleted tag default/<image_stream_name:tag>.
```

### 関連情報

- 認証情報の詳細は、[イメージプルシークレットの使用](#) を参照してください。

## 第3章 代替レジストリーでの CLUSTER SAMPLES OPERATOR の使用

最初にミラーレジストリーを作成して、別のレジストリーで Cluster Samples Operator を使用できません。



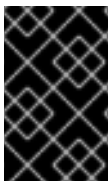
### 重要

必要なコンテナイメージを取得するには、インターネットへのアクセスが必要です。この手順では、ご使用のネットワークとインターネットのどちらにもアクセスできるミラーホストにミラーレジストリーを配置します。

### 3.1. ミラーレジストリーについて

OpenShift Container Platform のインストールとその後の製品更新に必要なイメージは、Red Hat Quay、JFrog Artifactory、Sonatype Nexus Repository、Harbor などのコンテナミラーレジストリーにミラーリングできます。大規模なコンテナレジストリーにアクセスできない場合は、OpenShift Container Platform サブスクリプションに含まれる小規模なコンテナレジストリーである **Red Hat OpenShift 導入用のミラーレジストリー** を使用できます。

Red Hat Quay、**Red Hat OpenShift 導入用のミラーレジストリー**、Artifactory、Sonatype Nexus リポジトリ、Harbor など、[Docker v2-2](#) をサポートする任意のコンテナレジストリーを使用できます。選択したレジストリーに関係なく、インターネット上の Red Hat がホストするサイトから分離されたイメージレジストリーにコンテンツをミラーリングする手順は同じです。コンテンツをミラーリングした後に、各クラスターをミラーレジストリーからこのコンテンツを取得するように設定します。



### 重要

OpenShift イメージレジストリーはターゲットレジストリーとして使用できません。これは、ミラーリングプロセスで必要となるタグを使わないプッシュをサポートしないためです。

**Red Hat OpenShift 導入用のミラーレジストリー**以外のコンテナレジストリーを選択する場合は、プロビジョニングするクラスター内の全マシンから到達可能である必要があります。レジストリーに到達できない場合、インストール、更新、またはワークロードの再配置などの通常の操作が失敗する可能性があります。そのため、ミラーレジストリーは可用性の高い方法で実行し、ミラーレジストリーは少なくとも OpenShift Container Platform クラスターの実稼働環境の可用性の条件に一致している必要があります。

ミラーレジストリーを OpenShift Container Platform イメージで設定する場合、2つのシナリオを実行することができます。インターネットとミラーレジストリーの両方にアクセスできるホストがあり、クラスターノードにアクセスできない場合は、そのマシンからコンテンツを直接ミラーリングできます。このプロセスは、**connected mirroring** (接続ミラーリング) と呼ばれます。このようなホストがない場合は、イメージをファイルシステムにミラーリングしてから、そのホストまたはリムーバブルメディアを制限された環境に配置する必要があります。このプロセスは、**disconnected mirroring** (非接続ミラーリング) と呼ばれます。

ミラーリングされたレジストリーの場合は、プルされたイメージのソースを表示するには、CRI-O ログで **Trying to access** のログエントリーを確認する必要があります。ノードで **crictl images** コマンドを使用するなど、イメージのプルソースを表示する他の方法では、イメージがミラーリングされた場所からプルされている場合でも、ミラーリングされていないイメージ名を表示します。



## 注記

Red Hat は、OpenShift Container Platform を使用してサードパーティーのレジストリーをテストしません。

## 関連情報

CRI-O ログを表示してイメージソースを表示する方法は、[イメージのプルソースの表示](#) を参照してください。

### 3.1.1. ミラーホストの準備

ミラーレジストリーを作成する前に、ミラーホストを準備する必要があります。

### 3.1.2. バイナリーのダウンロードによる OpenShift CLI のインストール

コマンドラインインターフェイスを使用して OpenShift Container Platform と対話するために CLI (**oc**) をインストールすることができます。**oc** は Linux、Windows、または macOS にインストールできます。



## 重要

以前のバージョンの **oc** をインストールしている場合、これを使用して OpenShift Container Platform 4.12 のすべてのコマンドを実行することはできません。新規バージョンの **oc** をダウンロードし、インストールします。

## Linux への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Linux にインストールできます。

## 手順

1. Red Hat カスタマーポータルでの [OpenShift Container Platform ダウンロードページ](#) に移動します。
2. **Product Variant** ドロップダウンリストからアーキテクチャーを選択します。
3. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
4. **OpenShift v4.12 Linux Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
5. アーカイブを展開します。

```
$ tar xvf <file>
```

6. **oc** バイナリーを、**PATH** にあるディレクトリーに配置します。**PATH** を確認するには、以下のコマンドを実行します。

```
$ echo $PATH
```

## 検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

-

```
$ oc <command>
```

### Windows への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Windows にインストールできます。

#### 手順

1. Red Hat カスタマーポータルでの [OpenShift Container Platform ダウンロードページ](#) に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.12 Windows Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
4. ZIP プログラムでアーカイブを解凍します。
5. **oc** バイナリーを、**PATH** にあるディレクトリーに移動します。  
**PATH** を確認するには、コマンドプロンプトを開いて以下のコマンドを実行します。

```
C:\> path
```

#### 検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
C:\> oc <command>
```

### macOS への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを macOS にインストールできます。

#### 手順

1. Red Hat カスタマーポータルでの [OpenShift Container Platform ダウンロードページ](#) に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.12 macOS Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。



#### 注記

macOS arm64 の場合は、**OpenShift v4.12 macOS arm64 Client** エントリーを選択します。

4. アーカイブを展開し、解凍します。
5. **oc** バイナリーをパスにあるディレクトリーに移動します。  
**PATH** を確認するには、ターミナルを開き、以下のコマンドを実行します。

```
$ echo $PATH
```

## 検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

## 3.2. イメージのミラーリングを可能にする認証情報の設定

Red Hat からミラーへのイメージのミラーリングを可能にするコンテナイメージレジストリーの認証情報ファイルを作成します。

### 前提条件

- 切断された環境で使用するミラーレジストリーを設定しました。

### 手順

インストールホストで以下の手順を実行します。

1. [Red Hat OpenShift Cluster Manager サイトの Pull Secret](#) ページから **registry.redhat.io** プルシークレットをダウンロードします。
2. JSON 形式でプルシークレットのコピーを作成します。

```
$ cat ./pull-secret | jq . > <path>/<pull_secret_file_in_json> ❶
```

- ❶ プルシークレットを保存するフォルダーへのパスおよび作成する JSON ファイルの名前を指定します。

ファイルの内容は以下の例のようになります。

```
{
  "auths": {
    "cloud.openshift.com": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "quay.io": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "registry.connect.redhat.com": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    },
    "registry.redhat.io": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    }
  }
}
```

3. ミラーレジストリーの base64 でエンコードされたユーザー名およびパスワードまたはトークンを生成します。

```
$ echo -n '<user_name>:<password>' | base64 -w0 ❶
BGVtbYk3ZHAAtqXs=
```

- ❶ **<user\_name>** および **<password>** については、レジストリーに設定したユーザー名およびパスワードを指定します。

4. JSON ファイルを編集し、レジストリーについて記述するセクションをこれに追加します。

```
"auths": {
  "<mirror_registry>": { ❶
    "auth": "<credentials>", ❷
    "email": "you@example.com"
  }
},
```

- ❶ **<mirror\_registry>** については、レジストリードメイン名と、ミラーレジストリーがコンテンツを提供するために使用するポートをオプションで指定します。例:  
**registry.example.com** または **registry.example.com:8443**
- ❷ **<credentials>** については、ミラーレジストリーの base64 でエンコードされたユーザー名およびパスワードを指定します。

ファイルは以下の例のようになります。

```
{
  "auths": {
    "registry.example.com": {
      "auth": "BGVtbYk3ZHAAtqXs=",
      "email": "you@example.com"
    },
    "cloud.openshift.com": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "quay.io": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "registry.connect.redhat.com": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    },
    "registry.redhat.io": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    }
  }
}
```

### 3.3. OPENSIFT CONTAINER PLATFORM イメージリポジトリーのミラーリング



クラスターのインストールまたはアップグレード時に使用するために、OpenShift Container Platform イメージリポジトリをお使いのレジストリーにミラーリングします。

## 前提条件

- ミラーホストがインターネットにアクセスできる。
- ネットワークが制限された環境で使用するミラーレジストリーを設定し、設定した証明書および認証情報にアクセスできる。
- [Red Hat OpenShift Cluster Manager からプルシークレット](#) をダウンロードし、ミラーリポジトリへの認証を含めるようにこれを変更している。
- 自己署名証明書を使用する場合は、証明書にサブジェクトの別名を指定しています。

## 手順

ミラーホストで以下の手順を実行します。

1. [OpenShift Container Platform ダウンロード](#) ページを確認し、インストールする必要がある OpenShift Container Platform のバージョンを判別し、[Repository Tags](#) ページで対応するタグを判別します。
2. 必要な環境変数を設定します。

- a. リリースバージョンをエクスポートします。

```
$ OCP_RELEASE=<release_version>
```

**<release\_version>** について、インストールする OpenShift Container Platform のバージョンに対応するタグを指定します (例: **4.5.4**)。

- b. ローカルレジストリー名とホストポートをエクスポートします。

```
$ LOCAL_REGISTRY='<local_registry_host_name>:<local_registry_host_port>'
```

**<local\_registry\_host\_name>** については、ミラーレジストリーのレジストリードメイン名を指定し、**<local\_registry\_host\_port>** については、コンテンツの送信に使用するポートを指定します。

- c. ローカルリポジトリ名をエクスポートします。

```
$ LOCAL_REPOSITORY='<local_repository_name>'
```

**<local\_repository\_name>** については、**ocp4/openshift4** などのレジストリーに作成するリポジトリの名前を指定します。

- d. ミラーリングするリポジトリの名前をエクスポートします。

```
$ PRODUCT_REPO='openshift-release-dev'
```

実稼働環境のリリースの場合には、**openshift-release-dev** を指定する必要があります。

- e. パスをレジストリープルシークレットにエクスポートします。

```
$ LOCAL_SECRET_JSON='<path_to_pull_secret>'
```

<path\_to\_pull\_secret> については、作成したミラーレジストリーのプルシークレットの絶対パスおよびファイル名を指定します。

- f. リリースミラーをエクスポートします。

```
$ RELEASE_NAME="ocp-release"
```

実稼働環境のリリースについては、**ocp-release** を指定する必要があります。

- g. **x86\_64** や **aarch64** など、サーバーのアーキテクチャーの種類をエクスポートします。

```
$ ARCHITECTURE=<server_architecture>
```

- h. ミラーリングされたイメージをホストするためにディレクトリーへのパスをエクスポートします。

```
$ REMOVABLE_MEDIA_PATH=<path> 1
```

- 1 最初のスラッシュ (/) 文字を含む完全パスを指定します。

3. バージョンイメージをミラーレジストリーにミラーリングします。

- ミラーホストがインターネットにアクセスできない場合は、以下の操作を実行します。

- リムーバブルメディアをインターネットに接続しているシステムに接続します。
- ミラーリングするイメージおよび設定マニフェストを確認します。

```
$ oc adm release mirror -a ${LOCAL_SECRET_JSON} \
  --from=quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE}-
  ${ARCHITECTURE} \
  --to=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY} \
  --to-release-
  image=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
  ${ARCHITECTURE} --dry-run
```

- 直前のコマンドの出力の **imageContentSources** セクション全体を記録します。ミラーの情報はミラーリングされたリポジトリーに一意であり、インストール時に **imageContentSources** セクションを **install-config.yaml** ファイルに追加する必要があります。
- イメージをリムーバブルメディア上のディレクトリーにミラーリングします。

```
$ oc adm release mirror -a ${LOCAL_SECRET_JSON} --to-
  dir=${REMOVABLE_MEDIA_PATH}/mirror
  quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE}-
  ${ARCHITECTURE}
```

- メディアをネットワークが制限された環境に移し、イメージをローカルコンテナレジストリーにアップロードします。

```
$ oc image mirror -a ${LOCAL_SECRET_JSON} --from-
  dir=${REMOVABLE_MEDIA_PATH}/mirror
  "file://openshift/release:${OCP_RELEASE}*"
```

`${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}` **1**

- 1** **REMOVABLE\_MEDIA\_PATH** の場合、イメージのミラーリング時に指定した同じパスを使用する必要があります。



### 重要

`oc image mirror` を実行すると、**error: unable to retrieve source image** エラーが発生する場合があります。このエラーは、イメージレジストリーに存在しなくなったイメージへの参照がイメージインデックスに含まれている場合に発生します。イメージインデックスは、それらのイメージを実行しているユーザーがアップグレードグラフの新しいポイントへのアップグレードパスを実行できるように、古い参照を保持する場合があります。一時的な回避策として、`--skip-missing` オプションを使用してエラーを回避し、イメージインデックスのダウンロードを続行できます。詳細は、[Service Mesh Operator mirroring failed](#) を参照してください。

- ローカルコンテナレジストリーがミラーホストに接続されている場合は、以下の操作を実行します。
  - i. 以下のコマンドを使用して、リリースイメージをローカルレジストリーに直接プッシュします。

```
$ oc adm release mirror -a ${LOCAL_SECRET_JSON} \
  --from=quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE}-
  ${ARCHITECTURE} \
  --to=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY} \
  --to-release-
  image=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
  ${ARCHITECTURE}
```

このコマンドは、リリース情報をダイジェストとしてプルします。その出力には、クラスタのインストール時に必要な **imageContentSources** データが含まれます。

- ii. 直前のコマンドの出力の **imageContentSources** セクション全体を記録します。ミラーの情報はミラーリングされたリポジトリーに一意であり、インストール時に **imageContentSources** セクションを **install-config.yaml** ファイルに追加する必要があります。



### 注記

ミラーリングプロセス中にイメージ名に Quay.io のパッチが適用され、podman イメージにはブートストラップ仮想マシンのレジストリーに Quay.io が表示されます。

4. ミラーリングしたコンテンツに基づくインストールプログラムを作成するために、インストールプログラムを展開してリリースに固定します。

- ミラーホストがインターネットにアクセスできない場合は、以下のコマンドを実行します。

```
$ oc adm release extract -a ${LOCAL_SECRET_JSON} --icsp-file=<file> \ --
command=openshift-install
"${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}"
```

- ローカルコンテナーレジストリーがミラーホストに接続されている場合は、以下のコマンドを実行します。

```
$ oc adm release extract -a ${LOCAL_SECRET_JSON} --command=openshift-install
"${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
${ARCHITECTURE}"
```



### 重要

選択した OpenShift Container Platform のバージョンに適したイメージを確実に使用するために、ミラーリングしたコンテンツからインストールプログラムを展開する必要があります。

インターネット接続のあるマシンで、このステップを実行する必要があります。

- インストーラーでプロビジョニングされるインフラストラクチャーを使用するクラスターの場合は、以下のコマンドを実行します。

```
$ openshift-install
```

## 3.4. 代替のレジストリーまたはミラーリングされたレジストリーでの CLUSTER SAMPLES OPERATOR イメージストリームの使用

Cluster Samples Operator によって管理される **openshift** namespace のほとんどのイメージストリームは、Red Hat レジストリーの [registry.redhat.io](https://registry.redhat.io) にあるイメージを参照します。



### 注記

**cli**、**installer**、**must-gather**、および **tests** イメージストリームはインストールペイロードの一部ですが、Cluster Samples Operator によって管理されません。これらについては、この手順で扱いません。



### 重要

Cluster Samples Operator は、非接続環境では **Managed** に設定する必要があります。イメージストリームをインストールするには、ミラーリングされたレジストリーが必要です。

### 前提条件

- cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- ミラーレジストリーのプルシークレットの作成。

### 手順

- ミラーリングする特定のイメージストリームのイメージにアクセスします。

```
$ oc get is <imagestream> -n openshift -o json | jq .spec.tags[].from.name | grep registry.redhat.io
```

- 必要なイメージストリームに関連付けられた [registry.redhat.io](https://registry.redhat.io) のイメージをミラーリングします。

```
$ oc image mirror registry.redhat.io/rhsc/ruby-25-rhel7:latest ${MIRROR_ADDR}/rhsc/ruby-25-rhel7:latest
```

- クラスターのイメージ設定オブジェクトを作成します。

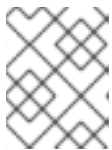
```
$ oc create configmap registry-config --from-file=${MIRROR_ADDR_HOSTNAME}..5000=$path/ca.crt -n openshift-config
```

- クラスターのイメージ設定オブジェクトに、ミラーに必要な信頼される CA を追加します。

```
$ oc patch image.config.openshift.io/cluster --patch '{"spec":{"additionalTrustedCA":{"name":"registry-config"}}}' --type=merge
```

- Cluster Samples Operator 設定オブジェクトの **samplesRegistry** フィールドを、ミラー設定で定義されたミラーの場所の **hostname** の部分を含むように更新します。

```
$ oc edit configs.samples.operator.openshift.io -n openshift-cluster-samples-operator
```



### 注記

これは、イメージストリームのインポートプロセスでミラーまたは検索メカニズムが使用されないのが必要になります。

- Cluster Samples Operator 設定オブジェクトの **skippedImagestreams** フィールドにミラーリングされないイメージストリームを追加します。または、サンプルイメージストリームのいずれもサポートする必要がない場合は、Cluster Samples Operator を Cluster Samples Operator 設定オブジェクトの **Removed** に設定します。



### 注記

Cluster Samples Operator は、イメージストリームのインポートに失敗した場合にアラートを発行しますが、Cluster Samples Operator は定期的に再試行する場合もあれば、それらを再試行していないように見える場合もあります。

**openshift** namespace のテンプレートの多くはイメージストリームを参照します。そのため、**Removed** を使用してイメージストリームとテンプレートの両方を除去すると、イメージストリームのいずれかが欠落しているためにテンプレートが正常に機能しない場合にテンプレートの使用を試行する可能性がなくなります。

## 3.4.1. ミラーリングの Cluster Samples Operator のサポート

インストール時に、OpenShift Container Platform は **imagestreamtag-to-image** という名前の設定マップを **openshift-cluster-samples-operator** namespace に作成します。 **imagestreamtag-to-image** 設定マップには、各イメージストリームタグのエントリ (設定されるイメージ) が含まれます。

設定マップの data フィールドの各エントリーのキーの形式は、`<image_stream_name>_<image_stream_tag_name>` です。

OpenShift Container Platform の非接続インストール時に、Cluster Samples Operator のステータスは **Removed** に設定されます。これを **Managed** に変更することを選択する場合、サンプルがインストールされます。



### 注記

ネットワークが制限されている環境または切断されている環境でサンプルを使用するには、ネットワークの外部のサービスにアクセスする必要がある場合があります。サービスの例には、Github、Maven Central、npm、RubyGems、PyPi などがあります。場合によっては、Cluster Samples Operator のオブジェクトが必要なサービスに到達できるようにするために、追加の手順を実行する必要があります。

この config map は、イメージストリームをインポートするためにミラーリングする必要があるイメージの参照情報として使用できます。

- Cluster Samples Operator が **Removed** に設定される場合、ミラーリングされたレジストリーを作成するか、使用する必要のある既存のミラーリングされたレジストリーを判別できます。
- 新しい config map をガイドとして使用し、ミラーリングされたレジストリーに必要なサンプルをミラーリングします。
- Cluster Samples Operator 設定オブジェクトの **skippedImagestreams** リストに、ミラーリングされていないイメージストリームを追加します。
- Cluster Samples Operator 設定オブジェクトの **samplesRegistry** をミラーリングされたレジストリーに設定します。
- 次に、Cluster Samples Operator を **Managed** に設定し、ミラーリングしたイメージストリームをインストールします。

詳細の手順については、[代替のレジストリーまたはミラーリングされたレジストリーでの Cluster Samples Operator イメージストリームの使用](#) について参照してください。

## 第4章 イメージの作成

使用可能な事前にビルドされたイメージを使用して独自のコンテナイメージを作成する方法について確認します。このプロセスには、イメージの作成、イメージのメタデータの定義、イメージのテストおよびカスタムビルダーワークフローを使用した OpenShift Container Platform で使用するイメージの作成のベストプラクティスを理解することが含まれます。イメージを作成したら、それを OpenShift イメージレジストリーにプッシュできます。

### 4.1. コンテナのベストプラクティスについて

OpenShift Container Platform で実行するコンテナイメージを作成する場合には、イメージの作成者は、イメージの使いやすさの点で数多くのベストプラクティスを考慮する必要があります。イメージは変更不可で、そのままの状態で使用されることが意図されているため、以下のガイドラインは、イメージを使用しやすく、OpenShift Container Platform で簡単に使用できるようにするのに役立ちます。

#### 4.1.1. コンテナイメージの一般的なガイドライン

以下のガイドラインは、イメージが OpenShift Container Platform で使用されるかどうかにかかわらず、コンテナイメージの作成時に一般的に適用されます。

##### イメージの再利用

可能な場合は、**FROM** ステートメントを使用し、適切なアップストリームイメージをベースとしてイメージを設定します。これにより、依存関係を直接更新する必要なく、イメージが更新時にアップストリームイメージからセキュリティー修正を簡単に取得できるようになります。

さらに、**FROM** 命令 (例: `rhel:rhel7`) のタグを使用して、お使いのイメージがどのバージョンのイメージをベースとしているかを明確にします。アップストリームイメージの **latest** バージョンを使用すると互換性に影響のある変更が組み込まれる可能性があるため、**latest** 以外のタグを使用することができます。

##### タグ内の互換性の維持

独自のイメージにタグを付ける場合には、タグ内で後方互換性が維持されるようにします。たとえば、**image** という名前のイメージがあり、現時点でバージョン **1.0** が含まれている場合には、**image:v1** のタグを指定します。イメージの更新時には、元のイメージとの互換性がある限り、新しいイメージに **image:v1** のタグを付けることができ、このタグのダウストリームのコンシューマーは、互換性に関する影響を被ることなく更新を取得できるようになります。

互換性のない更新を後にリリースした場合には、**image:v2** などの新しいタグに切り替えます。これにより、ダウストリームのコンシューマーはいつでも新しいバージョンに移行できますが、意図せずにこの互換性のない新規イメージによる影響を受けることはありません。**image:latest** を使用するダウストリームコンシューマーには、互換性のない変更が導入されるリスクがあります。

##### 複数プロセスの回避

データベースや **SSHD** など複数のサービスを1つのコンテナ内で起動しないようにしてください。コンテナは軽量で、複数のプロセスをオーケストレーションするために簡単にリンクできるので、複数プロセスの実行は不要です。OpenShift Container Platform では、関連のあるイメージを1つの Pod にグループ化して、簡単に共存させ、共同管理することができます。

このように共存させることで、コンテナはネットワークの namespace とストレージを通信用に共有できるようになります。また、イメージの更新頻度が低く、個別に更新されるので、更新による中断の可能性が低くなります。シグナル処理フローは、複数の起動したプロセスへのルーティングシグナルを管理する必要がないので、単一プロセスによって明確になります。

##### ラッパースクリプトでの `exec` の使用

多くのイメージはラッパースクリプトを使用して、実行されるソフトウェアのプロセスを開始する前に

いくつかの設定を行います。イメージがこのようなスクリプトを使用する場合、そのスクリプトは、スクリプトのプロセスがソフトウェアによって置き換えられるように **exec** を使用します。**exec** を使用しない場合、コンテナランタイムによって送信されるシグナルが、ソフトウェアのプロセスではなくラッパースクリプトに送られます。これは望ましい動作ではありません。

一部のサーバーのプロセスを開始するラッパースクリプトがあるとします。**podman run -i** などを使用してコンテナを起動すると、それによりラッパースクリプトが実行され、次にプロセスが開始されます。**CTRL+C** でコンテナを閉じる必要があるとします。ラッパースクリプトがサーバープロセスを開始するために **exec** を使用している場合、**podman** は SIGINT をサーバープロセスに送信し、すべてが予想通りに機能します。ラッパースクリプトで **exec** を使用しなかった場合、**podman** はラッパースクリプトのプロセスに SIGINT を送信し、プロセスは何も生じなかったかのように実行し続けます。

また、コンテナ内で実行されると、プロセスは **PID 1** として実行される点に留意してください。つまり、主なプロセスが中断された場合には、コンテナ全体が停止され、**PID 1** プロセスから起動した子プロセスが終了します。

### 一時ファイルの消去

ビルドプロセスで作成される一時ファイルはすべて削除します。これには、**ADD** コマンドで追加したファイルも含まれます。たとえば、**yum install** の操作を実行してから、**yum clean** コマンドを実行します。

**yum** キャッシュがイメージレイヤーに残らないように、以下のように **RUN** ステートメントを作成します。

```
RUN yum -y install mypackage && yum -y install myotherpackage && yum clean all -y
```

以下のように記述した場合には注意してください。

```
RUN yum -y install mypackage  
RUN yum -y install myotherpackage && yum clean all -y
```

上記のように記述すると、最初の **yum** 呼び出しにより、対象のレイヤーに追加のファイルが残り、**yum clean** 操作を後に実行してもこれらのファイルは削除できません。これらの追加ファイルは最終イメージでは確認できませんが、下位レイヤーには存在します。

現在のコンテナビルドプロセスでは、前のレイヤーで何かが削除された場合でも、後のレイヤーでコマンドを実行してイメージが使用する容量を縮小できません。ただし、これについては今後変更される可能性はあります。後のレイヤーでファイルが表示されていなくても **rm** コマンドを実行したとしても、ダウンロードするイメージの全体のサイズを縮小することになりません。そのため、**yum clean** の場合のように、可能な場合は後にレイヤーに書き込まれないように、ファイルの作成に使用したのと同じコマンドでファイルを削除することが最も適切と言えます。

また、単一の **RUN** ステートメントで複数のコマンドを実行すると、イメージのレイヤー数が減り、ダウンロードと実行時間が短縮されます。

### 正しい順序での命令の指定

コンテナビルダーは **Dockerfile** を読み取り、トップダウンで命令を実行します。命令が正常に実行されると、同じイメージが次回ビルドされる時や、別のイメージがビルドされる時に再利用することができるレイヤーが作成されます。**Dockerfile** の上部にほとんど変更されない命令を配置することは非常に重要です。こうすることで、上位レイヤーで加えられた変更によってキャッシュが無効にならないので、同じイメージの次のビルドをすばやく実行できます。

たとえば、反復するファイルをインストールするための **ADD** コマンドと、パッケージを **yum install** する **RUN** コマンドが含まれる **Dockerfile** で作業を行う場合には、**ADD** コマンドを最後に配置することが最善の方法です。



```
FROM foo
RUN yum -y install mypackage && yum clean all -y
ADD myfile /test/myfile
```

これにより、**myfile** を編集して **podman build** または **docker build** を返すたびに、システムは **yum** コマンドのキャッシュされたレイヤーを再利用し、**ADD** 操作に対してのみ新規レイヤーを生成します。

代わりに **Dockerfile** を以下のように作成した場合:

```
FROM foo
ADD myfile /test/myfile
RUN yum -y install mypackage && yum clean all -y
```

**myfile** を変更して、**podman build** または **docker build** を再実行するたびに、**ADD** 操作は **RUN** レイヤーのキャッシュを無効にするので、**yum** 操作も再実行する必要があります。

### 重要なポートのマーク付け

EXPOSE 命令は、ホストシステムで利用できるコンテナおよび他のコンテナにポートを作成します。ポートを **podman run** の起動で公開されるように指定できますが、**Dockerfile** で EXPOSE 命令を使用すると、ソフトウェアが実行する必要のあるポートを明示的に宣言することで、人間とソフトウェアの両方がイメージをより簡単に使用できるようになります。

- 公開されるポートは、イメージから作成されるコンテナに関連付けられる **podman ps** の下に表示されます。
- 公開されるポートは、**podman inspect** によって返されるイメージのメタデータに表示されません。
- 公開されるポートは、1つのコンテナを別のコンテナにリンクする際にリンクされます。

### 環境変数の設定

**ENV** 命令で環境変数を設定することが適切です。一例として、プロジェクトのバージョンを設定するなどが挙げられます。バージョンを設定することで、**Dockerfile** を確認せずにバージョンを簡単に見つけ出すことができます。別の例としては、**JAVA\_HOME** など、別のプロセスで使用可能なシステムでパスを公開する場合などです。

### デフォルトのパスワードの回避

デフォルトのパスワードは設定しないようにしてください。イメージを拡張して、デフォルトのパスワードを削除または変更するのを忘れることが多くあります。これは、実稼働環境で使用するユーザーに誰でも知っているパスワードが割り当てられると、セキュリティの問題に発展する可能性があります。パスワードは、環境変数を使用して設定できます。

デフォルトのパスワードを設定することにした場合には、コンテナの起動時に適切な警告メッセージが表示されるようにしてください。メッセージはデフォルトパスワードの値をユーザーに通知し、環境変数の設定など、パスワードの変更方法を説明するものである必要があります。

### SSHD の回避

イメージで **sshd** を実行しないようにしてください。ローカルホストで実行中のコンテナにアクセスするには、**podman exec** または **docker exec** コマンドを使用できます。または、**oc exec** コマンドまたは **oc rsh** コマンドを使用して、OpenShift Container Platform クラスタで実行中のコンテナにアクセスできます。イメージで **sshd** をインストールし、実行すると、攻撃の経路が増え、セキュリティ修正が必要になります。

### 永続データ向けのボリュームの使用

イメージは、永続データ用に **ボリューム** を使用する必要があります。こうすることで、OpenShift

Container Platform により、コンテナを実行するノードにネットワークストレージがマウントされ、コンテナが新しいノードに移動した場合に、ストレージはそのノードに再度割り当てられます。永続ストレージのすべての要件に対応するようにボリュームを使用することで、コンテナが再起動されたり、移動されたりしても、コンテンツは保存されます。イメージがコンテナ内の任意の場所にデータを書き込む場合には、コンテンツは保存されない可能性があります。

コンテナが破棄された後も保存する必要があるデータはすべて、ボリュームに書き込む必要があります。コンテナエンジンはコンテナの **readonly** フラグをサポートしており、このフラグを使用して、コンテナの一時ストレージにデータが決して記述されないようにすることができます。イメージをこの機能に基づいて設計すると、この機能を後に利用することがより簡単になります。

**Dockerfile** でボリュームを明示的に定義すると、イメージの利用者がイメージの実行時に定義する必要のあるボリュームがどれかを簡単に理解できるようになります。

OpenShift Container Platform でのボリュームの使用方法についての詳細は、[Kubernetes ドキュメント](#) を参照してください。



### 注記

永続ボリュームでも、イメージの各インスタンスには独自のボリュームがあり、ファイルシステムはインスタンス間で共有されません。つまり、ボリュームを使用してクラスターの状態を共有できません。

## 4.1.2. OpenShift Container Platform 固有のガイドライン

以下は、OpenShift Container Platform で使用するためのコンテナイメージの作成時に適用されるガイドラインです。

### 4.1.2.1. Source-To-Image (S2I) 向けのイメージの有効化

開発者が提供した Ruby コードを実行するように設計された Ruby イメージなど、サードパーティー提供のアプリケーションコードを実行することが目的のイメージの場合には、イメージを [Source-to-Image \(S2I\)](#) ビルドツールと連携できるようにすることができます。S2I は、インプットとして、アプリケーションのソースコードを受け入れるイメージを簡単に記述でき、アセンブルされたアプリケーションをアウトプットとして実行する新規イメージを簡単に生成することができるフレームワークです。

### 4.1.2.2. 任意のユーザー ID のサポート

デフォルトでは OpenShift Container Platform は、任意に割り当てられたユーザー ID を使用してコンテナを実行します。こうすることで、コンテナエンジンの脆弱性が原因でコンテナから出ていくプロセスに対して追加のセキュリティーを設定でき、ホストノードでパーミッションのエスカレーションが可能になります。

イメージが任意ユーザーとしての実行をサポートできるように、イメージ内のプロセスで記述されるディレクトリーやファイルは、root グループが所有し、このグループに対して読み取り/書き込みの権限を割り当てる必要があります。実行予定のファイルには、グループの実行権限も必要です。

以下を Dockerfile に追加すると、root グループのユーザーがビルドされたイメージでアクセスできるように、ディレクトリーおよびファイルのパーミッションが設定されます。

```
RUN chgrp -R 0 /some/directory && \
    chmod -R g=u /some/directory
```

コンテナユーザーは常に root グループのメンバーであるため、コンテナユーザーはこれらのファイルに対する読み取り、書き込みが可能です。

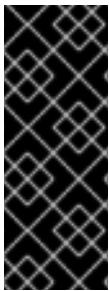


### 警告

コンテナの機密領域のディレクトリーとファイルパーミッションを変更する場合は注意が必要です。`/etc/passwd` ファイルなどの機密領域に変更を適用すると、意図しないユーザーによるこれらのファイルの変更が許可され、コンテナまたはホストがセキュリティーリスクにさらされる可能性があります。CRI-O は、コンテナの `/etc/passwd` ファイルへに対する任意のユーザー ID の挿入をサポートしています。そのため、パーミッションを変更する必要はありません。

また、いずれのコンテナイメージにも `/etc/passwd` ファイルが存在しないはずで、存在する場合、CRI-O コンテナランタイムはランダムな UID を `/etc/passwd` ファイルに挿入できません。このような場合、コンテナがアクティブな UID を解決する際に問題が発生する可能性があります。この要件を満たさない場合、特定のコンテナ化されたアプリケーションの機能に影響が及び可能性があります。

さらに、コンテナで実行中のプロセスは、特権のあるユーザーとして実行されていないので、特権のあるポート (1024 未満のポート) をリッスンできません。



### 重要

S2I イメージに、ユーザーを数値で指定した **USER** 宣言が含まれない場合には、デフォルトで、ビルドが失敗します。名前が指定されたユーザーや `root (0)` ユーザーを使用するイメージを OpenShift Container Platform でビルドできるようにするには、プロジェクトのビルダーサービスアカウント (`system:serviceaccount:<your-project>:builder`) を `anyuid` SCC (security context constraint) に追加できます。または、すべてのイメージをどのユーザーでも実行できるようにできます。

#### 4.1.2.3. イメージ間通信でのサービスの使用

データの保存や取得のためにデータベースイメージにアクセスする必要のある Web フロントエンドイメージなど、別のイメージが提供するサービスとイメージが通信する場合には、イメージは OpenShift Container Platform サービスを使用します。サービスは、コンテナが停止、開始、または移動しても変更されない静的アクセスエンドポイントを提供します。さらに、サービスにより、要求が負荷分散されます。

#### 4.1.2.4. 共通のライブラリーの提供

サードパーティーが提供するアプリケーションコードの実行を目的とするイメージの場合は、プラットフォーム用として共通に使用されるライブラリーをイメージに含めるようにしてください。とくに、プラットフォームで使用する共通のデータベース用のデータベースドライバーを設定してください。たとえば、Java フレームワークイメージを作成する場合に、MySQL や PostgreSQL には JDBC ドライバーを設定します。このように設定することで、アプリケーションのアセンブリー時に共通の依存関係をダウンロードする必要がなくなり、アプリケーションイメージのビルドがスピードアップします。また、すべての依存関係の要件を満たすためのアプリケーション開発者の作業が簡素化されます。

#### 4.1.2.5. 設定での環境変数の使用

イメージのユーザーは、ダウンストリームイメージをイメージに基づいて作成しなくても、イメージを設定できます。つまり、ランタイム設定は環境変数を使用して処理されます。単純な設定の場合、実行中のプロセスは環境変数を直接使用できます。より複雑な設定や、これをサポートしないランタイムの

場合、起動時に処理されるテンプレート設定ファイルを定義してランタイムを設定します。このプロセス時に、環境変数を使用して渡される値は設定ファイルで置き換えることも、この値を使用して、設定ファイルに指定するオプションを決定することもできます。

環境変数を使用して、コンテナに証明書やキーなどのシークレットを渡すこともでき、これは推奨されています。環境変数を使用することで、シークレット値がイメージにコミットされたり、コンテナイメージレジストリーに漏洩されることはありません。

環境変数を指定することで、イメージの利用者は、イメージ上に新しいレイヤーを作成することなく、データベースの設定、パスワード、パフォーマンスチューニングなどの動作をカスタマイズできます。Pod の定義時に環境変数の値を定義するだけで、イメージの再ビルドなしに設定を変更できます。

非常に複雑なシナリオの場合、ランタイム時にコンテナにマウントされるボリュームを使用して設定を指定することも可能です。ただし、この方法を使用する場合には、必要なボリュームや設定が存在しない場合に明確なエラーメッセージが起動時に表示されるように、イメージが設定されている必要があります。

サービスエンドポイントの情報を渡す環境変数としてデータソースなどの設定を定義される点で、これはイメージ間の通信でのサービスの使用についてのトピックと関連しています。これにより、アプリケーションは、アプリケーションイメージを変更せずに、OpenShift Container Platform 環境に定義されているデータソースサービスを動的に使用できます。

さらに、コンテナの **cgroups** 設定を確認して、調整します。これにより、イメージは利用可能なメモリー、CPU、他のリソースに合わせてチューニングが可能になります。たとえば、Java ベースのイメージは、制限を超えず、メモリー不足のエラーが表示されないように、**cgroup** の最大メモリーパラメーターを基にヒープをチューニングします。

#### 4.1.2.6. イメージのメタデータ設定

イメージのメタデータを定義することで、OpenShift Container Platform によるコンテナイメージの使用が改善され、開発者が OpenShift Container Platform でイメージを使用しやすくなります。たとえば、メタデータを追加して、イメージに関する役立つ情報を提供したり、必要とされる他のイメージを提案したりできます。

#### 4.1.2.7. クラスタリング

イメージの複数のインスタンスを実行するとはどういうことかを十分に理解しておく必要があります。最も単純な例では、サービスの負荷分散機能は、イメージのすべてのインスタンスにトラフィックをルーティングします。ただし、セッションの複製などで、リーダーの選択やフェイルオーバーの状態を実行するには、多くのフレームワークが情報を共有する必要があります。

OpenShift Container Platform での実行時に、インスタンスでこのような通信を実現する方法を検討します。Pod 同士は直接通信できますが、Pod が起動、停止、移動するたびに IP アドレスが変更されます。そのため、クラスタリングスキームを動的にしておくことが重要です。

#### 4.1.2.8. ロギング

すべてのロギングを標準出力に送信することが推奨されます。OpenShift Container Platform はコンテナから標準出力を収集し、表示が可能な中央ロギングサービスに送信します。ログコンテンツを分離する必要がある場合には、出力の接頭辞に適切なキーワードを指定して、メッセージをフィルタリングできるようにしてください。

お使いのイメージがファイルにロギングをする場合には、手動で実行中のコンテナに入り、ログファイルを取得または表示する必要があります。

#### 4.1.2.9. Liveness および Readiness プローブ

イメージで使用可能な liveness および readiness プローブの例をまとめます。これらのプローブにより、処理の準備ができるまでトラフィックがコンテナにルーティングされず、プロセスが正常でない状態になる場合にコンテナが再起動されるので、ユーザーはイメージを安全にデプロイできます。

#### 4.1.2.10. テンプレート

イメージと共にテンプレートサンプルを提供することも検討してください。テンプレートがあると、ユーザーは、正しく機能する設定を指定してイメージをすばやく簡単にデプロイできるようになります。完全を期するため、テンプレートには、イメージに関連して記述した liveness および readiness プローブを含めるようにしてください。

### 4.2. イメージへのメタデータの組み込み

イメージのメタデータを定義することで、OpenShift Container Platform によるコンテナイメージの使用が改善され、開発者が OpenShift Container Platform でイメージを使用しやすくなります。たとえば、メタデータを追加して、イメージに関する役立つ情報を提供したり、必要とされる可能性のある他のイメージを提案したりできます。

このトピックでは、現在の一連のユースケースに必要なメタデータのみを定義します。他のメタデータまたはユースケースは、今後追加される可能性があります。

#### 4.2.1. イメージメタデータの定義

**Dockerfile** で **LABEL** 命令を使用して、イメージのメタデータを定義することができます。ラベルは、イメージやコンテナに割り当てるキーと値のペアである点で環境変数と似ています。ただし、ラベルは、実行中のアプリケーションに表示されず、イメージやコンテナをすばやく検索する場合にも使用できる点で、環境変数とは異なります。

**LABEL** 命令に関する詳細は、[Docker ドキュメント](#) を参照してください。

通常、ラベル名には namespace が使用されます。namespace は、対象のラベルを選択して使用するプロジェクトを反映するように設定されます。OpenShift Container Platform の場合、namespace は **io.openshift** に、Kubernetes の場合は、namespace は **io.k8s** に設定されます。

形式に関する詳細は、[Docker のカスタムメタデータ](#) に関するドキュメントを参照してください。

表4.1 サポートされるメタデータ

| 変数                       | 説明  |
|--------------------------|---|
| <b>io.openshift.tags</b> | <p>このラベルには、コンマ区切りの文字列値のリストとして表現されているタグのリストが含まれます。タグを使用して、コンテナイメージを幅広い機能エリアに分類します。タグを使用すると、UI および生成ツールがアプリケーションの作成プロセスで適切なコンテナイメージを提案しやすくなります。</p> <pre> <b>LABEL</b> io.openshift.tags mongodb,mongodb24,nosql </pre> |

| 変数   | 説明  |
|--|---|
| <b>io.openshift.wants</b>                                      | <p>コンテナイメージにすでにタグが指定されていない場合に、生成ツールと UI が適切な提案を行うのに使用するタグのリストを指定します。たとえば、コンテナイメージに <b>mysql</b> と <b>redis</b> が必要で、コンテナイメージに <b>redis</b> タグが指定されていない場合には、UI はこのイメージをデプロイメントに追加するように提案する可能性があります。</p> <pre> LABEL io.openshift.wants  mongodb,redis </pre> |
| <b>io.k8s.description</b>                                      | <p>このラベルは、コンテナイメージの利用者に、このイメージが提供するサービスや機能に関する詳細情報を提供するのに使用できます。UI は、この説明とコンテナイメージ名を使用して、人間が解読しやすい情報をエンドユーザーに提供します。</p> <pre> LABEL io.k8s.description  The MySQL 5.5 Server with master-slave replication support </pre>                                   |
| <b>io.openshift.non-scalable</b>                               | <p>イメージは、この変数を使用して、スケーリングがサポートされていないことを示す場合があります。その後、UI はこれをそのイメージのコンシューマーに通知します。スケーリング不可にした場合は <b>replicas</b> の値を最初に <b>1</b> よりも大きい値に設定することはできません。</p> <pre> LABEL io.openshift.non-scalable  true </pre>  |
| <b>io.openshift.min-memory</b> および <b>io.openshift.min-cpu</b> | <p>このラベルは、コンテナイメージが正しく機能するにはどの程度リソースが必要かを提案します。UI でユーザーに対し、このコンテナイメージをデプロイすると、ユーザークォータを超過する可能性があることを警告する場合があります。この値は、Kubernetes の数量と互換性がある必要があります。</p> <pre> LABEL io.openshift.min-memory  16Gi LABEL io.openshift.min-cpu     4 </pre>                    |

## 4.3. SOURCE-TO-IMAGE によるソースコードからのイメージの作成

Source-to-Image (S2I) は、アプリケーションのソースコードを入力として取り、アセンブルされたアプリケーションを出力として実行する新規イメージを生成するイメージを簡単に作成できるようにするフレームワークです。

再生成可能なコンテナイメージのビルドに S2I を使用する主な利点として、開発者の使い勝手の良さが挙げられます。ビルダーイメージの作成者は、イメージが最適な S2I パフォーマンスを実現できるように、ビルドプロセスと S2I スクリプトの基本的なコンセプト 2 点を理解する必要があります。

### 4.3.1. Source-to-Image ビルドプロセスについて

ビルドプロセスは次の 3 つの基本要素で構成されます。これらを組み合わせて最終的なコンテナイメージが作成されます。

- ソース

- Source-to-Image (S2I) スクリプト
- ビルダーイメージ

S2I は、最初の **FROM** 命令として、ビルダーイメージで Dockerfile を生成します。S2I によって生成される Dockerfile は Buildah に渡されます。

### 4.3.2. Source-to-Image スクリプトの作成方法

Source-to-Image (S2I) スクリプトは、ビルダーイメージ内でスクリプトを実行できる限り、どのプログラム言語でも記述できます。S2I は **assemble/run/save-artifacts** スクリプトを提供する複数のオプションをサポートします。ビルドごとに、これらの場所はすべて、以下の順番にチェックされます。

1. ビルド設定に指定されるスクリプト
2. アプリケーションソースの **.s2i/bin** ディレクトリーにあるスクリプト
3. **io.openshift.s2i.scripts-url** ラベルを含むデフォルトの URL にあるスクリプト

イメージで指定した **io.openshift.s2i.scripts-url** ラベルも、ビルド設定で指定したスクリプトも、以下の形式のいずれかを使用します。

- **image:///path\_to\_scripts\_dir**: S2I スクリプトが配置されているディレクトリーへのイメージ内の絶対パス。
- **file:///path\_to\_scripts\_dir**: S2I スクリプトが配置されているディレクトリーへのホスト上の相対パスまたは絶対パス。
- **http(s)://path\_to\_scripts\_dir**: S2I スクリプトが配置されているディレクトリーの URL。

表4.2 S2I スクリプト

| スクリプト           | 説明   |
|-----------------|--|
| <b>assemble</b> | <p><b>assemble</b> スクリプトは、ソースからアプリケーションアーティファクトをビルドし、イメージ内の適切なディレクトリーに配置します。このスクリプトが必要です。このスクリプトのワークフローは以下のとおりです。</p> <ol style="list-style-type: none"> <li>1. オプション: ビルドのアーティファクトを復元します。増分ビルドをサポートする必要がある場合、<b>save-artifacts</b> も定義するようにしてください (オプション)。</li> <li>2. 任意の場所に、アプリケーションソースを配置します。</li> <li>3. アプリケーションのアーティファクトをビルドします。</li> <li>4. 実行に適した場所に、アーティファクトをインストールします。</li> </ol> |
| <b>run</b>      | <p><b>run</b> スクリプトはアプリケーションを実行します。このスクリプトが必要です。</p>   |

| スクリプト                 | 説明   |
|-----------------------|--|
| <b>save-artifacts</b> | <p><b>save-artifacts</b> スクリプトは、次に続くビルドプロセスを加速できるようにすべての依存関係を収集します。このスクリプトはオプションです。以下に例を示します。</p> <ul style="list-style-type: none"> <li>● Ruby の場合は、Bundler でインストールされる <b>gems</b></li> <li>● Java の場合は、<b>.m2</b> のコンテンツ</li> </ul> <p>これらの依存関係は <b>tar</b> ファイルに集められ、標準出力としてストリーミングされます。</p>  |
| <b>usage</b>          | <p><b>usage</b> スクリプトでは、ユーザーに、イメージの正しい使用方法を通知します。このスクリプトはオプションです。</p>  |
| <b>test/run</b>       | <p><b>test/run</b> スクリプトでは、イメージが正しく機能しているかどうかを確認するためのプロセスを作成できます。このスクリプトはオプションです。このプロセスの推奨フローは以下のとおりです。</p> <ol style="list-style-type: none"> <li>1. イメージをビルドします。</li> <li>2. イメージを実行して <b>usage</b> スクリプトを検証します。</li> <li>3. <b>s2i build</b> を実行して <b>assemble</b> スクリプトを検証します。</li> <li>4. オプション: 再度 <b>s2i build</b> を実行して、<b>save-artifacts</b> と <b>assemble</b> スクリプトの保存、復元アーティファクト機能を検証します。</li> <li>5. イメージを実行して、テストアプリケーションが機能していることを確認します。</li> </ol> <div style="display: flex; align-items: flex-start; margin-top: 20px;"> <div style="flex: 1; text-align: center;">  </div> <div style="flex: 2;"> <p><b>注記</b></p> <p><b>test/run</b> スクリプトでビルドしたテストアプリケーションを配置するための推奨される場所は、イメージリポジトリの <b>test/test-app</b> ディレクトリーです。</p> </div> </div> |

## S2I スクリプトの例

以下の S2I スクリプトの例は Bash で記述されています。それぞれの例では、**tar** の内容は **/tmp/s2i** ディレクトリーにデプロイメントされることが前提とされています。

### assemble スクリプト:

```
#!/bin/bash

# restore build artifacts
if [ "$(ls /tmp/s2i/artifacts/ 2>/dev/null)" ]; then
  mv /tmp/s2i/artifacts/* $HOME/.
fi

# move the application source
mv /tmp/s2i/src $HOME/src
```



```
# build application artifacts
pushd ${HOME}
make all

# install the artifacts
make install
popd
```

#### run スクリプト:

```
#!/bin/bash

# run the application
/opt/application/run.sh
```

#### save-artifacts スクリプト:

```
#!/bin/bash

pushd ${HOME}
if [ -d deps ]; then
    # all deps contents to tar stream
    tar cf - deps
fi
popd
```

#### usage スクリプト:

```
#!/bin/bash

# inform the user how to use the image
cat <<EOF
This is a S2I sample builder image, to use it, install
https://github.com/openshift/source-to-image
EOF
```

#### 関連情報

- [S2I イメージ作成のチュートリアル](#)

## 4.4. SOURCE-TO-IMAGE イメージのテストについて

Source-to-Image (S2I) ビルダ-イメージの作成者は、S2I イメージをローカルでテストして、自動テストや継続的な統合に OpenShift Container Platform ビルドシステムを使用できます。

S2I ビルドを正常に実行するには、S2I に **assemble** と **run** スクリプトが必要です。S2I 外のコンテナイメージを実行した場合に、**save-artifacts** スクリプトがあると、ビルドのアーティファクトが再利用され、**usage** スクリプトがあると、使用についての情報がコンソールに出力されるようになります。

S2I イメージのテストは、ベースのコンテナイメージを変更したり、コマンドが使用するツールが更新されたりした場合でも、上記のコマンドが正しく機能することを確認するのが目的です。

### 4.4.1. テスト要件について

**test** スクリプトは、基本的に **test/run** に配置されます。このスクリプトは、OpenShift Container Platform S2I イメージビルダーが呼び出し、単純な Bash スクリプトか静的な Go バイナリーのいずれかの形式を取ることができます。

**test/run** スクリプトは S2I ビルドを実行するので、S2I バイナリーを **\$PATH** で利用可能にしておく必要があります。必要に応じて、[S2I README](#) のインストール手順に従います。

S2I は、アプリケーションのソースコードおよびビルダーイメージを統合します。これをテストするには、ソースが実行可能なコンテナイメージに変換されることを検証するためのサンプルアプリケーションのソースが必要です。サンプルアプリケーションは単純なものである必要がありますが、**assemble** および **run** スクリプトの重要な手順を実行できる必要があります。

### 4.4.2. スクリプトおよびツールの生成

S2I ツールは、新しい S2I イメージの作成プロセスを加速化する強力な生成ツールと共に提供されます。**s2i create** コマンドでは、**Makefile** 以外に、必要とされる S2I スクリプトとテストツールすべてが生成されます。

```
$ s2i create _<image name>_ _<destination directory>_
```

生成された **test/run** スクリプトは、より使いやすくするために調整する必要がありますが、このスクリプトを開発の開始段階で使用することが推奨されます。



#### 注記

**s2i create** コマンドで生成した **test/run** スクリプトでは、サンプルアプリケーションのソースを **test/test-app** ディレクトリーに配置しておく必要があります。

### 4.4.3. ローカルでのテスト

S2I イメージテストをローカルに実行する最も簡単な方法として、生成した **Makefile** を使用することができます。

**s2i create** コマンドを使用しない場合には、以下の **Makefile** テンプレートをコピーして、**IMAGE\_NAME** パラメーターをお使いのイメージ名に置き換えることができます。

#### Makefile の例

```
IMAGE_NAME = openshift/ruby-20-centos7
CONTAINER_ENGINE := $(shell command -v podman 2> /dev/null | echo docker)

build:
  ${CONTAINER_ENGINE} build -t $(IMAGE_NAME) .

.PHONY: test
test:
  ${CONTAINER_ENGINE} build -t $(IMAGE_NAME)-candidate .
  IMAGE_NAME=$(IMAGE_NAME)-candidate test/run
```

### 4.4.4. テストの基本的なワークフロー

**test** スクリプトは、テストするイメージをすでにビルドしていることが前提です。必要に応じて、以下のコマンドで S2I イメージを先にビルドしてください。以下のいずれかのコマンドを実行してください。

- Podman を使用する場合は、以下のコマンドを実行します。

```
$ podman build -t <builder_image_name>
```

- Docker を使用する場合は、以下のコマンドを実行します。

```
$ docker build -t <builder_image_name>
```

以下の手順では、S2I イメージビルダーをテストするデフォルトのワークフローを説明しています。

1. **usage** スクリプトが機能していることを確認します。

- Podman を使用する場合は、以下のコマンドを実行します。

```
$ podman run <builder_image_name> .
```

- Docker を使用する場合は、以下のコマンドを実行します。

```
$ docker run <builder_image_name> .
```

2. イメージをビルドします。

```
$ s2i build file:///path-to-sample-app _<BUILDER_IMAGE_NAME>_  
_<OUTPUT_APPLICATION_IMAGE_NAME>_
```

3. オプション: **save-artifacts** をサポートする場合には、再度手順 2 を実行して、保存して復元するアーティファクトが正しく機能することを確認します。

4. コンテナを実行します。

- Podman を使用する場合は、以下のコマンドを実行します。

```
$ podman run <output_application_image_name>
```

- Docker を使用する場合は、以下のコマンドを実行します。

```
$ docker run <output_application_image_name>
```

5. コンテナが実行され、アプリケーションが応答していることを確認します。

これらの手順を実行すると、通常はビルダーイメージが予想通りに機能しているかどうか分かります。

#### 4.4.5. イメージのビルドでの OpenShift Container Platform の使用

新しい S2I ビルダーイメージを設定する **Dockerfile** と他のアーティファクトが準備できたら、それらを git リポジトリに配置して、OpenShift Container Platform を使用し、イメージをビルドしてプッシュします。お使いのリポジトリを参照する Docker ビルドを定義します。

OpenShift Container Platform インスタンスが公開 IP アドレスでホストされる場合、ビルドは、S2I ビルダーイメージ GitHub リポジトリにプッシュするたびにトリガーされます。

**ImageChangeTrigger** を使用して、更新した S2I ビルダーイメージに基づくアプリケーションの再ビルドをトリガーすることもできます。

## 第5章 イメージの管理

### 5.1. イメージの管理の概要

OpenShift Container Platform では、イメージのレジストリーが置かれる場所やレジストリー関連の認証要件、およびビルドとデプロイメントで必要とされる動作に応じてイメージと対話し、イメージストリームをセットアップできます。

#### 5.1.1. イメージの概要

イメージストリームは、タグによって識別される任意の数のコンテナイメージで構成されます。これはコンテナイメージリポジトリのように関連イメージの単一仮想ビューを提供します。

イメージストリームの監視により、ビルドおよびデプロイメントは新規イメージの追加または変更時に通知を受信し、それぞれビルドまたはデプロイメントを実行してこれに対応します。

### 5.2. イメージのタグ付け

以下のセクションでは、OpenShift Container Platform イメージストリームおよびそれらのタグを操作するためにコンテナイメージのコンテキストでイメージタグを使用する概要および方法について説明します。

#### 5.2.1. イメージタグ

イメージタグは、イメージストリーム内の他のイメージから特定のイメージを識別するリポジトリのコンテナイメージに適用されるラベルです。通常、タグはある種のバージョン番号を表します。たとえば、ここでは **:v3.11.59-2** がタグになります。

```
registry.access.redhat.com/openshift3/jenkins-2-rhel7:v3.11.59-2
```

イメージにタグを追加することができます。たとえば、イメージには **:v3.11.59-2** および **:latest** というタグが割り当てられる可能性があります。

OpenShift Container Platform は **docker tag** コマンドに似た **oc tag** コマンドを提供しますが、これらはイメージ上で直接動作するのではなくイメージストリームで動作します。

#### 5.2.2. イメージタグの規則

イメージは時間の経過と共に変化するもので、それらのタグはその変化を反映します。ほとんどの場合、イメージタグはビルドされる最新イメージを常に参照します。

**v2.0.1-may-2019** のように、タグ名に非常に多くの情報が組み込まれる場合、タグはイメージの単一のリビジョンのみを参照し、更新されることはありません。デフォルトのイメージのプルニングオプションを使用しても、このようなイメージは削除されません。非常に大規模なクラスターでは、イメージが修正されるたびに新規タグが作成される設定の場合、古くなって久しいイメージの余分のタグメタデータで etcd データストアが一杯になる可能性があります。

タグの名前が **v2.0** である場合はイメージのリビジョンの数が増えることが予想されます。これによりタグ履歴が長くなるため、イメージプルーナーが古くなり使われなくなったイメージを削除する可能性が高くなります。

タグの名前付け規則は各自で定めることができますが、ここでは **<image\_name>:<image\_tag>** 形式のいくつかの例を見てみましょう。

表5.1 イメージタグの名前付け規則

| 説明              | 例                                 |
|-----------------|-----------------------------------|
| リビジョン           | <code>myimage:v2.0.1</code>       |
| アーキテクチャー        | <code>myimage:v2.0-x86_64</code>  |
| ベースイメージ         | <code>myimage:v1.2-centos7</code> |
| 最新 (不安定な可能性がある) | <code>myimage:latest</code>       |
| 最新 (安定性がある)     | <code>myimage:stable</code>       |

タグ名に日付を含める必要がある場合、古くなり使用されなくなったイメージおよび **istags** を定期的に検査し、これらを削除してください。そうしないと、古いイメージを保持して、リソースの使用量が增大する可能性があります。

### 5.2.3. タグのイメージストリームへの追加

OpenShift Container Platform のイメージストリームは、タグで識別される 0 個以上のコンテナイメージで設定されます。

各種のタグを利用できます。デフォルト動作では、特定の時点の特定のイメージを参照する **永続** タグを使用します。**permanent** タグが使用され、ソースが変更される場合、タグは宛先について変更されません。

**tracking** タグの場合は、宛先タグのメタデータがソースタグのインポート時に更新されます。

#### 手順

- **oc tag** コマンドを使用して、タグをイメージストリームに追加できます。

```
$ oc tag <source> <destination>
```

たとえば、**ruby** イメージストリームの **static-2.0** タグを **ruby** イメージストリーム **2.0** タグの現行のイメージを常に参照するように設定するには、以下を実行します。

```
$ oc tag ruby:2.0 ruby:static-2.0
```

これにより、**ruby** イメージストリームに **static-2.0** という名前のイメージストリームタグが新たに作成されます。この新規タグは、**oc tag** の実行時に **ruby:2.0** イメージストリームタグが参照したイメージ ID を直接参照し、これが参照するイメージが変更されることがありません。

- 宛先タグがソースタグの変更時に更新されるようにするには、**--alias=true** フラグを使用します。

```
$ oc tag --alias=true <source> <destination>
```



## 注記

永続的なエイリアス (**latest** または **stable** など) を作成するには、tracking タグを使用します。このタグは単一イメージストリーム内でのみ適切に機能します。複数のイメージストリーム間で使用されるエイリアスを作成しようとするとエラーが生じます。

- また、**--scheduled=true** フラグを追加して、宛先タグが定期的に更新 (再インポート) されるようにもできます。期間はシステムレベルでグローバルに設定できます。
- **--reference** フラグはインポートされないイメージストリームを作成します。このタグはソースの場所を参照しますが、これを永続的に参照します。  
統合レジストリーのタグ付けされたイメージを常にフェッチするように OpenShift Container Platform に指示するには、**--reference-policy=local** を使用します。レジストリーはプルスルー (pull-through) 機能を使用してイメージをクライアントに提供します。デフォルトで、イメージ Blob はレジストリーによってローカルにミラーリングされます。その結果、それらが次回必要となる場合により迅速にプルされます。また、このフラグは **--insecure-registry** をコンテナランタイムに指定しなくても、イメージストリームに非セキュアなアノテーションがあるか、タグに非セキュアなインポートポリシーがある限り、非セキュアなレジストリーからのプルを許可します。

### 5.2.4. タグのイメージストリームからの削除

タグをイメージストリームから削除できます。

#### 手順

- タグをイメージストリームから完全に削除するには、以下を実行します。

```
$ oc delete istag/ruby:latest
```

または、以下を実行します。

```
$ oc tag -d ruby:latest
```

### 5.2.5. イメージストリームでのイメージの参照

タグを使用してイメージストリームのイメージを参照するには、以下の参照タイプを使用します。

表5.2 イメージストリームの参照タイプ

| 参照タイプ                   | 説明  |
|-------------------------|---|
| <b>ImageStreamTag</b>   | <b>ImageStreamTag</b> は、所定のイメージストリームおよびタグのイメージを参照し、取得するために使用されます。                 |
| <b>ImageStreamImage</b> | <b>ImageStreamImage</b> は、所定のイメージストリームおよびイメージ <b>sha</b> ID を参照するか、取得するために使用されます。 |

| 参照タイプ              | 説明   |
|--------------------|--|
| <b>DockerImage</b> | <b>DockerImage</b> は、所定の外部レジストリーのイメージを参照または取得するために使用されます。この名前は、標準の Docker <b>pull specification</b> に基づいて付けられます。 |

イメージストリーム定義のサンプルを表示すると、これらには **ImageStreamTag** の定義と **DockerImage** の参照が含まれていますが、**ImageStreamImage** に関連するものは何も含まれていないことに気づくでしょう。

これは、**ImageStreamImage** オブジェクトが、イメージをイメージストリームにインポートしたり、タグ付けしたりする際に OpenShift Container Platform に自動的に作成されるためです。イメージストリームを作成するために使用するイメージストリーム定義で **ImageStreamImage** オブジェクトを明示的に定義する必要はありません。

## 手順

- 所定のイメージストリームおよびタグのイメージを参照するには、**ImageStreamTag** を使用します。

```
<image_stream_name>:<tag>
```

- 所定のイメージストリームおよびイメージの **sha** ID のイメージを参照するには、**ImageStreamImage** を使用します。

```
<image_stream_name>@<id>
```

<id> は、ダイジェストとも呼ばれる特定イメージのイミュータブルな ID です。

- 所定の外部レジストリーのイメージを参照または取得するには、**DockerImage** を使用します。

```
openshift/ruby-20-centos7:2.0
```



### 注記

タグが指定されていない場合、**latest** タグが使用されることが想定されます。

サードパーティーのレジストリーを参照することもできます。

```
registry.redhat.io/rhel7:latest
```

またはダイジェストでイメージを参照できます。

```
centos/ruby-22-
centos7@sha256:3a335d7d8a452970c5b4054ad7118ff134b3a6b50a2bb6d0c07c746e8986b2
8e
```

## 5.3. イメージプルポリシー



Podのそれぞれのコンテナにはコンテナイメージがあります。イメージを作成し、これをレジストリーにプッシュすると、イメージをPodで参照できます。

### 5.3.1. イメージプルポリシーの概要

OpenShift Container Platformはコンテナを作成する際に、コンテナの **imagePullPolicy** を使用して、コンテナの起動前にイメージをプルする必要があるかどうかを判別します。**imagePullPolicy**には以下の3つの値があります。

表5.3 **imagePullPolicy** の値

| 値                   | 説明                           |
|---------------------|------------------------------|
| <b>Always</b>       | 常にイメージをプルします。                |
| <b>IfNotPresent</b> | イメージがノード上にない場合にのみイメージをプルします。 |
| <b>Never</b>        | イメージをプルしません。                 |

コンテナの **imagePullPolicy** パラメーターが指定されていない場合、OpenShift Container Platformはイメージのタグに基づいてこれを設定します。

1. タグが **latest** の場合、OpenShift Container Platformは **imagePullPolicy** を **Always** にデフォルト設定します。
2. それ以外の場合に、OpenShift Container Platformは **imagePullPolicy** を **IfNotPresent** にデフォルト設定します。

## 5.4. イメージプルシークレットの使用

OpenShift イメージレジストリーを使用し、同じプロジェクトにあるイメージストリームからプルしている場合は、Podのサービスアカウントに適切なパーミッションがすでに設定されているために追加のアクションは不要です。

ただし、OpenShift Container Platform プロジェクト全体でイメージを参照する場合や、セキュリティー保護されたレジストリーからイメージを参照するなどの他のシナリオでは、追加の設定手順が必要になります。

イメージの **プルシークレット**は、[Red Hat OpenShift Cluster Manager](#) から取得 できます。このプルシークレットは **pullSecret** と呼ばれます。

このプルシークレットを使用し、OpenShift Container Platform コンポーネントのコンテナイメージを提供する組み込まれた各種の認証局 ([Quay.io](#) および [registry.redhat.io](#)) によって提供されるサービスで認証できます。

### 5.4.1. Pod が複数のプロジェクト間でイメージを参照できるようにする設定

OpenShift イメージレジストリーを使用している場合で **project-a** の Pod が **project-b** のイメージを参照できるようにするには、**project-a** のサービスアカウントが **project-b** の **system:image-puller** ロールにバインドされている必要があります。



## 注記

Pod サービスアカウントまたは namespace を作成するときは、サービスアカウントが Docker プルシークレットでプロビジョニングされるまで待ちます。サービスアカウントが完全にプロビジョニングされる前に Pod を作成すると、Pod は OpenShift イメージレジストリーにアクセスできません。

## 手順

1. **project-a** の Pod が **project-b** のイメージを参照できるようにするには、**project-a** のサービスアカウントを **project-b** の **system:image-puller** ロールにバインドします。

```
$ oc policy add-role-to-user \
  system:image-puller system:serviceaccount:project-a:default \
  --namespace=project-b
```

このロールを追加すると、デフォルトのサービスアカウントを参照する **project-a** の Pod は **project-b** からイメージをプルできるようになります。

2. **project-a** のすべてのサービスアカウントにアクセスを許可するには、グループを使用します。

```
$ oc policy add-role-to-group \
  system:image-puller system:serviceaccounts:project-a \
  --namespace=project-b
```

### 5.4.2. Pod が他のセキュリティー保護されたレジストリーからイメージを参照できるようにする設定

Docker クライアントの **.dockercfg \$HOME/.docker/config.json** ファイルは、セキュア/非セキュアなレジストリーに事前にログインしている場合に認証情報を保存する Docker 認証情報ファイルです。

OpenShift イメージレジストリーにないセキュリティー保護されたコンテナイメージをプルするには、Docker 認証情報でプルシークレットを作成し、これをサービスアカウントに追加する必要があります。

Docker 認証情報ファイルと関連するプルシークレットには、同じレジストリーに対して、それぞれに独自の認証情報セットがある、複数の参照を含めることができます。

#### config.json ファイルのサンプル

```
{
  "auths":{
    "cloud.openshift.com":{
      "auth":"b3Blb=",
      "email":"you@example.com"
    },
    "quay.io":{
      "auth":"b3Blb=",
      "email":"you@example.com"
    },
    "quay.io/repository-main":{
      "auth":"b3Blb=",
      "email":"you@example.com"
    }
  }
}
```

```

}
}
}

```

## プルシークレットの例

```

apiVersion: v1
data:
  .dockerconfigjson:
ewogICAgYXV0aHMiOnsKICAgICAgIm0iOnsKICAgICAgIsKICAgICAgICAgImF1dGgiOiJiM0JsYj0iLAogI
CAGlCAglCAiZW1haWwiOiJ5b3VAZXhhbXBsZS5jb20iCiAgICAgIH0KICAgfQp9Cg==
kind: Secret
metadata:
  creationTimestamp: "2021-09-09T19:10:11Z"
  name: pull-secret
  namespace: default
  resourceVersion: "37676"
  uid: e2851531-01bc-48ba-878c-de96cfe31020
type: Opaque

```

## 手順

- セキュリティー保護されたレジストリーの **.dockercfg** ファイルがすでにある場合は、以下を実行してそのファイルからシークレットを作成できます。

```

$ oc create secret generic <pull_secret_name> \
  --from-file=.dockercfg=<path/to/.dockercfg> \
  --type=kubernetes.io/dockercfg

```

- または、**\$HOME/.docker/config.json** ファイルがある場合は以下を実行します。

```

$ oc create secret generic <pull_secret_name> \
  --from-file=.dockerconfigjson=<path/to/.docker/config.json> \
  --type=kubernetes.io/dockerconfigjson

```

- セキュアなレジストリーについての Docker 認証情報ファイルがまだない場合には、以下のコマンドを実行してシークレットを作成することができます。

```

$ oc create secret docker-registry <pull_secret_name> \
  --docker-server=<registry_server> \
  --docker-username=<user_name> \
  --docker-password=<password> \
  --docker-email=<email>

```

- Pod のイメージをプルするためのシークレットを使用するには、そのシークレットをサービスアカウントに追加する必要があります。この例では、サービスアカウントの名前は、Pod が使用するサービスアカウントの名前に一致する必要があります。デフォルトのサービスアカウントは **default** です。

```

$ oc secrets link default <pull_secret_name> --for=pull

```

### 5.4.2.1. 委任された認証を使用したプライベートレジストリーからのプル

プライベートレジストリーは認証を別個のサービスに委任できます。この場合、イメージプルシークレットは認証およびレジストリーのエンドポイントの両方に対して定義される必要があります。

## 手順

1. 委任された認証サーバーのシークレットを作成します。

```
$ oc create secret docker-registry \
  --docker-server=sso.redhat.com \
  --docker-username=developer@example.com \
  --docker-password=***** \
  --docker-email=unused \
  redhat-connect-sso

secret/redhat-connect-sso
```

2. プライベートレジストリーのシークレットを作成します。

```
$ oc create secret docker-registry \
  --docker-server=privateregistry.example.com \
  --docker-username=developer@example.com \
  --docker-password=***** \
  --docker-email=unused \
  private-registry

secret/private-registry
```

### 5.4.3. グローバルクラスターのプルシークレットの更新

現在のプルシークレットを置き換えるか、新しいプルシークレットを追加することで、クラスターのグローバルプルシークレットを更新できます。



#### 重要

クラスターを別の所有者に転送するには、まず [OpenShift Cluster Manager Hybrid Cloud Console](#) で転送を開始し、次にクラスターのプルシークレットを更新する必要があります。OpenShift Cluster Manager で委譲を開始せずに、クラスターのプルシークレットを更新すると、クラスターは OpenShift Cluster Manager での Telemetry メトリクスの報告を停止します。

[クラスターの所有権の委譲](#) に関する詳細は、Red Hat OpenShift Cluster Manager ドキュメントの [クラスター所有権の委譲](#) を参照してください。

## 前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。

## 手順

1. オプション: 既存のプルシークレットに新しいプルシークレットを追加するには、以下の手順を実行します。
  - a. 以下のコマンドを入力してプルシークレットをダウンロードします。

```
$ oc get secret/pull-secret -n openshift-config --template='{{index .data ".dockerconfigjson" | base64decode}}' ><pull_secret_location> ❶
```

- ❶ プルシークレットファイルへのパスを指定します。

b. 以下のコマンドを実行して、新しいプルシークレットを追加します。

```
$ oc registry login --registry="<registry>" \ ❶  
--auth-basic="<username>:<password>" \ ❷  
--to=<pull_secret_location> ❸
```

- ❶ 新しいレジストリーを指定します。同じレジストリー内に複数のリポジトリを含めることができます (例: `--registry="<registry/my-namespace/my-repository>"`)。
- ❷ 新しいレジストリーの認証情報を指定します。
- ❸ プルシークレットファイルへのパスを指定します。

または、プルシークレットファイルを手動で更新することもできます。

2. 以下のコマンドを実行して、クラスターのグローバルプルシークレットを更新します。

```
$ oc set data secret/pull-secret -n openshift-config --from-file=.dockerconfigjson=  
<pull_secret_location> ❶
```

- ❶ 新規プルシークレットファイルへのパスを指定します。

この更新はすべてのノードにロールアウトされます。これには、クラスターのサイズに応じて多少時間がかかる場合があります。



### 注記

OpenShift Container Platform 4.7.4 の時点で、グローバルプルシークレットへの変更によってノードドレインまたは再起動がトリガーされなくなりました。

## 第6章 イメージストリームの管理

イメージストリームは、継続的な方法でコンテナイメージの作成および更新を行う手段を提供します。イメージの改良により、タグを使用して新規バージョン番号を割り当て、変更を追跡できるようになりました。本書では、イメージストリームの管理方法について説明します。

### 6.1. イメージストリームを使用する理由

イメージストリームおよびその関連付けられたタグは、OpenShift Container Platform 内でコンテナイメージを参照するための抽象化を提供します。イメージストリームとそのタグを使用して、利用可能なイメージを確認し、リポジトリのイメージが変更される場合でも必要な特定のイメージを使用していることを確認できます。

イメージストリームには実際のイメージデータは含まれませんが、イメージリポジトリと同様に、関連するイメージの単一の仮想ビューが提示されます。

ビルドおよびデプロイメントをそれぞれ実行し、ビルドおよびデプロイメントを、新規イメージが追加される際やこれに対応する際の通知をイメージストリームで確認できるように設定できます。

たとえば、デプロイメントで特定のイメージを使用していて、そのイメージの新規バージョンが作成される場合、デプロイメントを、そのイメージの新規バージョンを選択できるように自動的に実行します。

デプロイメントまたはビルドで使用するイメージストリームタグが更新されない場合には、コンテナイメージレジストリーのコンテナイメージが更新されても、ビルドまたはデプロイメントは以前の、既知でおそらく適切であると予想されるイメージをそのまま使用します。

ソースイメージは以下のいずれかに保存できます。

- OpenShift Container Platform の統合レジストリー
- registry.redhat.io or Quay.io などの外部レジストリー
- OpenShift Container Platform クラスターの他のイメージストリーム

ビルドまたはデプロイメント設定などのイメージストリームタグを参照するオブジェクトを定義する場合には、リポジトリではなく、イメージストリームタグを参照します。アプリケーションのビルドまたはデプロイ時に、OpenShift Container Platform がこのイメージストリームタグを使用してリポジトリに対してクエリーし、対象のイメージに関連付けられた ID を特定して、そのイメージを使用します。

イメージストリームメタデータは他のクラスター情報と共に etcd インスタンスに保存されます。

イメージストリームの使用には、いくつかの大きな利点があります。

- コマンドラインを使用して再プッシュすることなく、タグ付けや、タグのロールバック、およびイメージの迅速な処理を実行できます。
- 新規イメージがレジストリーにプッシュされると、ビルドおよびデプロイメントをトリガーできます。また、OpenShift Container Platform には他のリソースの汎用トリガーがあります (Kubernetes オブジェクトなど)。
- 定期的な再インポートを実行するためにタグにマークを付けることができます。ソースイメージが変更されると、その変更は選択され、イメージストリームに反映されます。これにより、ビルドまたはデプロイメント設定に応じてビルドまたはデプロイメントフローがトリガーされます。

- 詳細なアクセス制御を使用してイメージを共有し、チーム間でイメージを迅速に分散できます。
- ソースイメージが変更されると、イメージストリームタグはイメージの既知の適切なバージョンをポイントしたままになり、アプリケーションが予期せずに損傷しないようにします。
- イメージストリームオブジェクトのパーミッションを使用して、イメージを表示し、使用できるユーザーについてセキュリティーを設定することができます。
- クラスターレベルでイメージを読み込んだり、リスト表示するパーミッションのないユーザーは、イメージストリームを使用してプロジェクトでタグ付けされたイメージを取得できます。

## 6.2. イメージストリームの設定

**ImageStream** オブジェクトには以下の要素が含まれます。

### イメージストリームオブジェクト定義

```

apiVersion: image.openshift.io/v1
kind: ImageStream
metadata:
  annotations:
    openshift.io/generated-by: OpenShiftNewApp
  labels:
    app: ruby-sample-build
    template: application-template-stibuild
  name: origin-ruby-sample ❶
  namespace: test
spec: {}
status:
  dockerImageRepository: 172.30.56.218:5000/test/origin-ruby-sample ❷
  tags:
  - items:
    - created: 2017-09-02T10:15:09Z
      dockerImageReference: 172.30.56.218:5000/test/origin-ruby-
sample@sha256:47463d94eb5c049b2d23b03a9530bf944f8f967a0fe79147dd6b9135bf7dd13d ❸
      generation: 2
      image: sha256:909de62d1f609a717ec433cc25ca5cf00941545c83a01fb31527771e1fab3fc5 ❹
    - created: 2017-09-01T13:40:11Z
      dockerImageReference: 172.30.56.218:5000/test/origin-ruby-
sample@sha256:909de62d1f609a717ec433cc25ca5cf00941545c83a01fb31527771e1fab3fc5
      generation: 1
      image: sha256:47463d94eb5c049b2d23b03a9530bf944f8f967a0fe79147dd6b9135bf7dd13d
      tag: latest ❺

```

- ❶ イメージストリームの名前です。
- ❷ 新規イメージをこのイメージストリームで追加または更新するためにプッシュできる Docker リポジトリパスです。
- ❸ イメージストリームが現在参照する SHA ID です。このイメージストリームタグを参照するリソースはこの ID を使用します。
- ❹ このイメージストリームタグが以前に参照した SHA ID です。古いイメージにロールバックするために使用できます。

- 5 イメージストリームタグ名です。

### 6.3. イメージストリームイメージ

イメージストリームイメージは、イメージストリームから特定のイメージ ID をポイントします。

イメージストリームイメージにより、タグ付けされている特定のイメージストリームからイメージについてのメタデータを取得できます。

イメージストリームイメージオブジェクトは、イメージをイメージストリームにインポートしたり、タグ付けしたりする場合には OpenShift Container Platform に常に自動的に作成されます。イメージストリームを作成するために使用するイメージストリームイメージオブジェクトをイメージストリーム定義に明示的に定義する必要はありません。

イメージストリームのイメージは、リポジトリからのイメージストリーム名とイメージ ID で構成されており、@ 記号で区切られています。

```
<image-stream-name>@<image-id>
```

**ImageStream** オブジェクトのサンプルでイメージを参照する際、イメージストリームのイメージは以下のようになります。

```
origin-ruby-
sample@sha256:47463d94eb5c049b2d23b03a9530bf944f8f967a0fe79147dd6b9135bf7dd13d
```

### 6.4. イメージストリームタグ

イメージストリームタグは、イメージストリームのイメージに対する名前付きポインターです。これは **istag** として省略されます。イメージストリームタグは、指定のイメージストリームおよびタグのイメージを参照するか、取得するために使用されます。

イメージストリームタグは、ローカル、または外部で管理されるイメージを参照できます。これには、タグが参照したすべてのイメージのスタックとして表されるイメージの履歴が含まれます。新規または既存のイメージが特定のイメージストリームタグでタグ付けされる場合はいつでも、これは履歴スタックの最初の位置に置かれます。これまで先頭の位置を占めていたイメージは 2 番目の位置に置かれます。これにより、タグを過去のイメージに再び参照させるよう簡単にロールバックできます。

以下のイメージストリームタグは、**ImageStream** オブジェクトからのものです。

#### 履歴の 2 つのイメージを持つイメージストリームタグ

```
kind: ImageStream
apiVersion: image.openshift.io/v1
metadata:
  name: my-image-stream
# ...
tags:
- items:
  - created: 2017-09-02T10:15:09Z
    dockerImageReference: 172.30.56.218:5000/test/origin-ruby-
sample@sha256:47463d94eb5c049b2d23b03a9530bf944f8f967a0fe79147dd6b9135bf7dd13d
    generation: 2
    image: sha256:909de62d1f609a717ec433cc25ca5cf00941545c83a01fb31527771e1fab3fc5
```



```
- created: 2017-09-01T13:40:11Z
dockerImageReference: 172.30.56.218:5000/test/origin-ruby-
sample@sha256:909de62d1f609a717ec433cc25ca5cf00941545c83a01fb31527771e1fab3fc5
generation: 1
image: sha256:47463d94eb5c049b2d23b03a9530bf944f8f967a0fe79147dd6b9135bf7dd13d
tag: latest
# ...
```

イメージストリームタグには permanent タグまたは tracking タグを使用できます。

- Permanent タグは、Python 3.5 などの特定バージョンのイメージを参照するバージョン固有のタグです。
- tracking タグは別のイメージストリームタグに従う参照タグで、シンボリックリンクなどのように、フォローするイメージを変更するために更新される可能性があります。このような新規レベルでは後方互換性が確保されません。

たとえば、OpenShift Container Platform に同梱される **latest** イメージストリームタグはトラッキングタグです。これは、**latest** イメージストリームタグのコンシューマーが、新規レベルが利用可能になるとイメージで提供されるフレームワークの最新レベルに更新されることを意味します。**v3.10** への **latest** イメージストリームタグは **v3.11** に変更される可能性が常にあります。これらの **latest** イメージストリームタグは Docker **latest** タグと異なる動作をすることに注意してください。この場合、**latest** イメージストリームタグは Docker リポジトリの最新イメージを参照しません。これは別のイメージストリームタグを参照し、これはイメージの最新バージョンではない可能性があります。たとえば、**latest** イメージストリームタグがイメージの **v3.10** を参照する場合、**3.11** バージョンがリリースされても **latest** タグは **v3.11** に自動的に更新されず、これが **v3.11** イメージストリームタグを参照するように手動で更新されるまで **v3.10** を参照したままになります。



### 注記

トラッキングタグは単一のイメージストリームに制限され、他のイメージストリームを参照できません。

各自のニーズに合わせて独自のイメージストリームタグを作成できます。

イメージストリームタグは、コロンで区切られた、イメージストリームの名前とタグで設定されています。

```
<imagestream name>:<tag>
```

たとえば、上記の **ImageStream** オブジェクトのサンプルで **sha256:47463d94eb5c049b2d23b03a9530bf944f8f967a0fe79147dd6b9135bf7dd13d** イメージを参照するには、イメージストリームタグは以下のようになります。

```
origin-ruby-sample:latest
```

## 6.5. イメージストリーム変更トリガー

イメージストリームトリガーにより、ビルドおよびデプロイメントは、アップストリームの新規バージョンが利用可能になると自動的に起動します。

たとえば、ビルドおよびデプロイメントは、イメージストリームタグの変更時に自動的に起動します。これは、特定のイメージストリームタグをモニターし、変更の検出時にビルドまたはデプロイメントに通知することで実行されます。

## 6.6. イメージストリームのマッピング

統合レジストリーが新規イメージを受信する際、これは OpenShift Container Platform にマップするイメージストリームを作成し、送信し、イメージのプロジェクト、名前、タグおよびイメージメタデータを提供します。



### 注記

イメージストリームのマッピングの設定は高度な機能です。

この情報は、新規イメージを作成する際 (すでに存在しない場合) やイメージをイメージストリームにタグ付けする際に使用されます。OpenShift Container Platform は、コマンド、エントリーポイント、および環境変数などの各イメージについての完全なメタデータを保存します。OpenShift Container Platform のイメージはイミュータブル (変更不可能) であり、名前の最大長さは 63 文字です。

以下のイメージストリームマッピングのサンプルにより、イメージが **test/origin-ruby-sample:latest** としてタグ付けされます。

### イメージストリームマッピングオブジェクト定義

```
apiVersion: image.openshift.io/v1
kind: ImageStreamMapping
metadata:
  creationTimestamp: null
  name: origin-ruby-sample
  namespace: test
tag: latest
image:
  dockerImageLayers:
  - name: sha256:5f70bf18a086007016e948b04aed3b82103a36bea41755b6cddf10ace3c6ef
    size: 0
  - name: sha256:ee1dd2cb6df21971f4af6de0f1d7782b81fb63156801cfde2bb47b4247c23c29
    size: 196634330
  - name: sha256:5f70bf18a086007016e948b04aed3b82103a36bea41755b6cddf10ace3c6ef
    size: 0
  - name: sha256:5f70bf18a086007016e948b04aed3b82103a36bea41755b6cddf10ace3c6ef
    size: 0
  - name: sha256:ca062656bff07f18bff46be00f40cfbb069687ec124ac0aa038fd676cfaea092
    size: 177723024
  - name: sha256:63d529c59c92843c395befd065de516ee9ed4995549f8218eac6ff088bfa6b6e
    size: 55679776
  - name: sha256:92114219a04977b5563d7dff71ec4caa3a37a15b266ce42ee8f43dba9798c966
    size: 11939149
  dockerImageMetadata:
    Architecture: amd64
    Config:
      Cmd:
      - /usr/libexec/s2i/run
      Entrypoint:
      - container-entrypoint
      Env:
      - RACK_ENV=production
      - OPENSIFT_BUILD_NAMESPACE=test
      - OPENSIFT_BUILD_SOURCE=https://github.com/openshift/ruby-hello-world.git
      - EXAMPLE=sample-app
```

```

- OPENSIFT_BUILD_NAME=ruby-sample-build-1
- PATH=/opt/app-root/src/bin:/opt/app-
root/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
- STI_SCRIPTS_URL=image:///usr/libexec/s2i
- STI_SCRIPTS_PATH=/usr/libexec/s2i
- HOME=/opt/app-root/src
- BASH_ENV=/opt/app-root/etc/scl_enable
- ENV=/opt/app-root/etc/scl_enable
- PROMPT_COMMAND=. /opt/app-root/etc/scl_enable
- RUBY_VERSION=2.2
ExposedPorts:
  8080/tcp: {}
Labels:
  build-date: 2015-12-23
  io.k8s.description: Platform for building and running Ruby 2.2 applications
  io.k8s.display-name: 172.30.56.218:5000/test/origin-ruby-sample:latest
  io.openshift.build.commit.author: Ben Parees <bparees@users.noreply.github.com>
  io.openshift.build.commit.date: Wed Jan 20 10:14:27 2016 -0500
  io.openshift.build.commit.id: 00cadc392d39d5ef9117cbc8a31db0889eedd442
  io.openshift.build.commit.message: 'Merge pull request #51 from php-coder/fix_url_and_sti'
  io.openshift.build.commit.ref: master
  io.openshift.build.image: centos/ruby-22-
centos7@sha256:3a335d7d8a452970c5b4054ad7118ff134b3a6b50a2bb6d0c07c746e8986b28e
  io.openshift.build.source-location: https://github.com/openshift/ruby-hello-world.git
  io.openshift.builder-base-version: 8d95148
  io.openshift.builder-version: 8847438ba06307f86ac877465eadc835201241df
  io.openshift.s2i.scripts-url: image:///usr/libexec/s2i
  io.openshift.tags: builder,ruby,ruby22
  io.s2i.scripts-url: image:///usr/libexec/s2i
  license: GPLv2
  name: CentOS Base Image
  vendor: CentOS
User: "1001"
WorkingDir: /opt/app-root/src
Container: 86e9a4a3c760271671ab913616c51c9f3cea846ca524bf07c04a6f6c9e103a76
ContainerConfig:
  AttachStdout: true
  Cmd:
  - /bin/sh
  - -c
  - tar -C /tmp -xf - && /usr/libexec/s2i/assemble
  Entrypoint:
  - container-entrypoint
  Env:
  - RACK_ENV=production
  - OPENSIFT_BUILD_NAME=ruby-sample-build-1
  - OPENSIFT_BUILD_NAMESPACE=test
  - OPENSIFT_BUILD_SOURCE=https://github.com/openshift/ruby-hello-world.git
  - EXAMPLE=sample-app
  - PATH=/opt/app-root/src/bin:/opt/app-
root/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
  - STI_SCRIPTS_URL=image:///usr/libexec/s2i
  - STI_SCRIPTS_PATH=/usr/libexec/s2i
  - HOME=/opt/app-root/src
  - BASH_ENV=/opt/app-root/etc/scl_enable
  - ENV=/opt/app-root/etc/scl_enable

```

```

- PROMPT_COMMAND=. /opt/app-root/etc/scl_enable
- RUBY_VERSION=2.2
ExposedPorts:
  8080/tcp: {}
Hostname: ruby-sample-build-1-build
Image: centos/ruby-22-
centos7@sha256:3a335d7d8a452970c5b4054ad7118ff134b3a6b50a2bb6d0c07c746e8986b28e
  OpenStdin: true
  StdinOnce: true
  User: "1001"
  WorkingDir: /opt/app-root/src
Created: 2016-01-29T13:40:00Z
DockerVersion: 1.8.2.fc21
Id: 9d7fd5e2d15495802028c569d544329f4286dcd1c9c085ff5699218dbaa69b43
Parent: 57b08d979c86f4500dc8cad639c9518744c8dd39447c055a3517dc9c18d6fccd
Size: 441976279
apiVersion: "1.0"
kind: DockerImage
dockerImageMetadataVersion: "1.0"
dockerImageReference: 172.30.56.218:5000/test/origin-ruby-
sample@sha256:47463d94eb5c049b2d23b03a9530bf944f8f967a0fe79147dd6b9135bf7dd13d

```

## 6.7. イメージストリームの使用

以下のセクションでは、イメージストリームおよびイメージストリームタグを使用する方法について説明します。

### 6.7.1. イメージストリームについての情報の取得

イメージストリームについての一般的な情報およびこれがポイントするすべてのタグについての詳細情報を取得することができます。

#### 手順

- イメージストリームについての一般的な情報およびこれがポイントするすべてのタグについての詳細情報を取得します。

```
$ oc describe is/<image-name>
```

以下に例を示します。

```
$ oc describe is/python
```

#### 出力例

```

Name: python
Namespace: default
Created: About a minute ago
Labels: <none>
Annotations: openshift.io/image.dockerRepositoryCheck=2017-10-02T17:05:11Z
Docker Pull Spec: docker-registry.default.svc:5000/default/python
Image Lookup: local=false
Unique Images: 1

```

Tags: 1

3.5

tagged from centos/python-35-centos7

\* centos/python-35-centos7@sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25  
About a minute ago

- 特定のイメージストリームタグについて利用可能な情報をすべて取得します。

```
$ oc describe istag/<image-stream>:<tag-name>
```

以下に例を示します。

```
$ oc describe istag/python:latest
```

### 出力例

```
Image Name: sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25
Docker Image: centos/python-35-centos7@sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25
Name: sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25
Created: 2 minutes ago
Image Size: 251.2 MB (first layer 2.898 MB, last binary layer 72.26 MB)
Image Created: 2 weeks ago
Author: <none>
Arch: amd64
Entrypoint: container-entrypoint
Command: /bin/sh -c $STI_SCRIPTS_PATH/usage
Working Dir: /opt/app-root/src
User: 1001
Exposes Ports: 8080/tcp
Docker Labels: build-date=20170801
```



### 注記

表示されている以上の情報が出力されます。

## 6.7.2. タグのイメージストリームへの追加

追加タグをイメージストリームに追加できます。

### 手順

- 既存タグのいずれかを参照するタグを追加するには、`oc tag` コマンドを使用できます。

```
$ oc tag <image-name:tag1> <image-name:tag2>
```

以下に例を示します。

```
$ oc tag python:3.5 python:latest
```

## 出力例

```
Tag python:latest set to
python@sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25.
```

- イメージストリームに、外部コンテナイメージを参照するタグ (**3.5**) と、この最初のタグに基づいて作成されているために同じイメージを参照する別のタグ (**latest**) の2つのタグが含まれることを確認します。

```
$ oc describe is/python
```

## 出力例

```
Name: python
Namespace: default
Created: 5 minutes ago
Labels: <none>
Annotations: openshift.io/image.dockerRepositoryCheck=2017-10-02T17:05:11Z
Docker Pull Spec: docker-registry.default.svc:5000/default/python
Image Lookup: local=false
Unique Images: 1
Tags: 2
```

```
latest
  tagged from
  python@sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25
```

```
  * centos/python-35-
  centos7@sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25
    About a minute ago
```

```
  3.5
  tagged from centos/python-35-centos7
```

```
  * centos/python-35-
  centos7@sha256:49c18358df82f4577386404991c51a9559f243e0b1bdc366df25
    5 minutes ago
```

### 6.7.3. 外部イメージのタグの追加

外部イメージのタグを追加することができます。

#### 手順

- タグ関連のすべての操作に **oc tag** コマンドを使用して、内部または外部イメージをポイントするタグを追加します。

```
$ oc tag <repository/image> <image-name:tag>
```

たとえば、このコマンドは **docker.io/python:3.6.0** イメージを **python** イメージストリームの **3.6** タグにマップします。

```
$ oc tag docker.io/python:3.6.0 python:3.6
```

## 出力例

```
Tag python:3.6 set to docker.io/python:3.6.0.
```

外部イメージのセキュリティーが保護されている場合、そのレジストリーにアクセスするために認証情報を使用してシークレットを作成する必要があります

### 6.7.4. イメージストリームタグの更新

別のタグをイメージストリームに反映するようタグを更新できます。

#### 手順

- タグを更新します。

```
$ oc tag <image-name:tag> <image-name:latest>
```

たとえば、以下は **latest** タグを更新し、**3.6** タグをイメージタグに反映させます。

```
$ oc tag python:3.6 python:latest
```

## 出力例

```
Tag python:latest set to  
python@sha256:438208801c4806548460b27bd1fbc7bb188273d13871ab43f.
```

### 6.7.5. イメージストリームタグの削除

古いタグをイメージストリームから削除できます。

#### 手順

- 古いタグをイメージストリームから削除します。

```
$ oc tag -d <image-name:tag>
```

以下に例を示します。

```
$ oc tag -d python:3.6
```

## 出力例

```
Deleted tag default/python:3.6
```

Cluster Samples Operator による非推奨のイメージストリームタグの処理方法についての詳細は、[Cluster Samples Operator からの非推奨のイメージストリームタグの削除](#) を参照してください。

### 6.7.6. イメージストリームタグの定期的なインポートの設定

外部コンテナイメージレジストリーを使用している場合、(最新のセキュリティー更新を取得する場合などに) イメージを定期的に再インポートするには、**--scheduled** フラグを使用します。

## 手順

1. イメージインポートのスケジュール

```
$ oc tag <repository/image> <image-name:tag> --scheduled
```

以下に例を示します。

```
$ oc tag docker.io/python:3.6.0 python:3.6 --scheduled
```

## 出力例

```
Tag python:3.6 set to import docker.io/python:3.6.0 periodically.
```

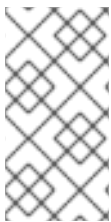
このコマンドにより、OpenShift Container Platform はこの特定のイメージストリームタグを定期的に更新します。この期間はクラスター全体のデフォルトで 15 分に設定されます。

2. 定期的なチェックを削除するには、上記のコマンド再実行しますが、**--scheduled** フラグを省略します。これにより、その動作がデフォルトに再設定されます。

```
$ oc tag <repository/image> <image-name:tag>
```

## 6.8. プライベートレジストリーからのイメージおよびイメージストリームのインポート

イメージストリームは、プライベートレジストリーからタグおよびイメージメタデータをインポートするように設定できます。これには認証が必要です。この手順は、Cluster Samples Operator が [registry.redhat.io](https://registry.redhat.io) 以外からコンテンツをプルするために使用するレジストリーを変更する場合に適用されます。



### 注記

セキュアでないレジストリーからインポートする場合には、シークレットに定義されたレジストリーの URL に **:80** ポートの接尾辞を追加するようにしてください。追加していない場合にレジストリーからインポートしようとする、このシークレットは使用されません。

## 手順

1. 以下のコマンドを入力して、認証情報を保存するために使用する **secret** オブジェクトを作成する必要があります。

```
$ oc create secret generic <secret_name> --from-file=.dockerconfigjson=  
<file_absolute_path> --type=kubernetes.io/dockerconfigjson
```

2. シークレットが設定されたら、新規イメージストリームを作成するか、**oc import-image** コマンドを入力します。

```
$ oc import-image <imagestreamtag> --from=<image> --confirm
```

インポートプロセスで OpenShift Container Platform はシークレットを取得してリモートパーティーに提供します。



### 6.8.1. Pod が他のセキュリティー保護されたレジストリーからイメージを参照できるようにする設定

Docker クライアントの `.dockercfg $HOME/.docker/config.json` ファイルは、セキュア/非セキュアなレジストリーに事前にログインしている場合に認証情報を保存する Docker 認証情報ファイルです。

OpenShift イメージレジストリーにないセキュリティー保護されたコンテナイメージをプルするには、Docker 認証情報でプルシークレットを作成し、これをサービスアカウントに追加する必要があります。

Docker 認証情報ファイルと関連するプルシークレットには、同じレジストリーに対して、それぞれに独自の認証情報セットがある、複数の参照を含めることができます。

#### config.json ファイルのサンプル

```
{
  "auths":{
    "cloud.openshift.com":{
      "auth":"b3Blb=",
      "email":"you@example.com"
    },
    "quay.io":{
      "auth":"b3Blb=",
      "email":"you@example.com"
    },
    "quay.io/repository-main":{
      "auth":"b3Blb=",
      "email":"you@example.com"
    }
  }
}
```

#### プルシークレットの例

```
apiVersion: v1
data:
  .dockerconfigjson:
    ewogICAgYXV0aHMiOmsKICAgICAgIm0iOmsKICAgICAgIksKICAgICAgICAgImF1dGgiOiJiM0JsYj0iLAogI
    CAgICAgICAgIiZW1haWwiOiJ5b3VAZXhhbXBsZS5jb20iCiAgICAgIH0KICAgfQp9Cg==
kind: Secret
metadata:
  creationTimestamp: "2021-09-09T19:10:11Z"
  name: pull-secret
  namespace: default
  resourceVersion: "37676"
  uid: e2851531-01bc-48ba-878c-de96cfe31020
type: Opaque
```

#### 手順

- セキュリティー保護されたレジストリーの `.dockercfg` ファイルがすでにある場合は、以下を実行してそのファイルからシークレットを作成できます。

```
$ oc create secret generic <pull_secret_name> \
  --from-file=.dockercfg=<path/to/.dockercfg> \
  --type=kubernetes.io/dockercfg
```

- または、**\$HOME/.docker/config.json** ファイルがある場合は以下を実行します。

```
$ oc create secret generic <pull_secret_name> \
  --from-file=.dockerconfigjson=<path/to/.docker/config.json> \
  --type=kubernetes.io/dockerconfigjson
```

- セキュアなレジストリーについての Docker 認証情報ファイルがまだない場合には、以下のコマンドを実行してシークレットを作成することができます。

```
$ oc create secret docker-registry <pull_secret_name> \
  --docker-server=<registry_server> \
  --docker-username=<user_name> \
  --docker-password=<password> \
  --docker-email=<email>
```

- Pod のイメージをプルするためのシークレットを使用するには、そのシークレットをサービスアカウントに追加する必要があります。この例では、サービスアカウントの名前は、Pod が使用するサービスアカウントの名前に一致する必要があります。デフォルトのサービスアカウントは **default** です。

```
$ oc secrets link default <pull_secret_name> --for=pull
```

## 6.9. IMAGESTREAMIMPORT によるマニフェストリストのインポート

**ImageStreamImport** リソースを使用して、イメージマニフェストを検索し、他のコンテナイメージレジストリーからクラスターにインポートできます。個々のイメージまたはイメージリポジトリー全体をインポートできます。

次の手順を使用して、**importMode** 値を指定し、**ImageStreamImport** オブジェクトを介してマニフェストリストをインポートします。

### 手順

1. **ImageStreamImport** YAML ファイルを作成し、マニフェストリストとしてインポートするタグの **importMode** パラメーターを **PreserveOriginal** に設定します。

```
apiVersion: image.openshift.io/v1
kind: ImageStreamImport
metadata:
  name: app
  namespace: myapp
spec:
  import: true
  images:
  - from:
    kind: DockerImage
    name: <registry>/<user_name>/<image_name>
  to:
    name: latest
```

```
referencePolicy:
  type: Source
importPolicy:
  importMode: "PreserveOriginal"
```

2. 次のコマンドを実行して **ImageStreamImport** を作成します。

```
$ oc create -f <your_imagestreamimport.yaml>
```

### 6.9.1. importMode 設定フィールド

次の表では、**importMode** 値に使用できる設定フィールドについて説明します。

| パラメーター           | 説明   |
|------------------|--|
| Legacy           | <p><b>importMode</b> のデフォルト値。アクティブな場合、マニフェストリストは破棄され、単一のサブマニフェストがインポートされます。プラットフォームは、以下の優先順位で選択されます。</p> <ol style="list-style-type: none"> <li>1. タグのアノテーション</li> <li>2. コントロールプレーンアーキテクチャー</li> <li>3. Linux/AMD64</li> <li>4. 一覧の最初のマニフェスト</li> </ol> |
| PreserveOriginal | <p>アクティブな場合、元のマニフェストが保持されます。マニフェスト一覧の場合は、マニフェストの一覧とそのすべてのサブマニフェストがインポートされます。</p>   |

## 第7章 KUBERNETES リソースでのイメージストリームの使用

OpenShift Container Platform のネイティブリソースであるイメージストリームは、**Build** リソース、**DeploymentConfigs** リソースなどの OpenShift Container Platform で利用可能なネイティブリソースすべてで動作します。これらは、**Job** リソース、**ReplicationController** リソース、**ReplicaSet** リソース、Kubernetes **Deployment** リソースなどのネイティブ Kubernetes リソースと共に機能することもできます。

### 7.1. KUBERNETES リソースでのイメージストリームの有効化

Kubernetes リソースでイメージストリームを使用する場合、リソースと同じプロジェクトにあるイメージストリームのみを参照できます。イメージストリームの参照は、単一セグメントの値で設定される必要があります。たとえば **ruby:2.5** の場合、**ruby** は **2.5** という名前のタグを持ち、参照するリソースと同じプロジェクトにあるイメージストリームの名前になります。



#### 注記

この機能は、**default** の namespace や **openshift-** または **kube-** の namespace では使用できません。

Kubernetes リソースでイメージストリームを有効にする方法は 2 つあります。

- 特定のリソースでイメージストリームの解決を有効にする。これにより、このリソースのみがイメージフィールドのイメージストリーム名を使用できます。
- イメージストリームでイメージストリームの解決を有効にする。これにより、このイメージストリームを参照するすべてのリソースがイメージフィールドのイメージストリーム名を使用できます。

#### 手順

**oc set image-lookup** を使用して、特定のリソース上のイメージストリームの解決またはイメージストリーム上のイメージストリームの解決を有効にすることができます。

1. すべてのリソースが **mysql** という名前のイメージストリームを参照できるようにするには、以下のコマンドを入力します。

```
$ oc set image-lookup mysql
```

これにより、**ImageStream.spec.lookupPolicy.local** フィールドが **true** に設定されます。

#### イメージルックアップが有効なイメージストリーム

```
apiVersion: image.openshift.io/v1
kind: ImageStream
metadata:
  annotations:
    openshift.io/display-name: mysql
  name: mysql
  namespace: myproject
spec:
  lookupPolicy:
    local: true
```

有効な場合には、この動作はイメージストリーム内のすべてのタグに対して有効化されます。

- 次に、イメージストリームをクエリーし、このオプションが設定されているかどうかを確認できます。

```
$ oc set image-lookup imagestream --list
```

特定のリソースでイメージルックアップを有効にすることができます。

- **mysql** という名前の Kubernetes デプロイメントがイメージストリームを使用できるようにするには、以下のコマンドを実行します。

```
$ oc set image-lookup deploy/mysql
```

これにより、**alpha.image.policy.openshift.io/resolve-names** アノテーションがデプロイメントに設定されます。

### イメージルックアップが有効にされたデプロイメント

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: mysql
  namespace: myproject
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        alpha.image.policy.openshift.io/resolve-names: '*'
    spec:
      containers:
        - image: mysql:latest
          imagePullPolicy: Always
          name: mysql
```

イメージルックアップを無効にすることができます。

- イメージルックアップを無効にするには、**--enabled=false** を渡します。

```
$ oc set image-lookup deploy/mysql --enabled=false
```

## 第8章 イメージストリームの変更時の更新のトリガー

イメージストリームタグが新規イメージを参照するように更新される場合、OpenShift Container Platform は、古いイメージを使用していたリソースに新規イメージをロールアウトするためのアクションを自動的に実行します。イメージストリームタグを参照しているリソースのタイプに応じ、この動作はさまざまな方法で設定できます。

### 8.1. OPENSIFT CONTAINER PLATFORM リソース

OpenShift Container Platform デプロイメントの設定およびビルド設定は、イメージストリームタグの変更によって自動的にトリガーされます。トリガーされたアクションは更新されたイメージストリームタグで参照されるイメージの新規の値を使用して実行できます。

### 8.2. KUBERNETES リソースのトリガー

API 定義の一部としてトリガーを制御するためのフィールドセットを含むデプロイメントおよびビルド設定とは異なり、Kubernetes リソースにはトリガー用のフィールドがありません。その代わりに、OpenShift Container Platform でアノテーションを使用してトリガーを要求できるようにします。

アノテーションは以下のように定義されます。

```
apiVersion: v1
kind: Pod
metadata:
  annotations:
    image.openshift.io/triggers:
      [
        {
          "from": {
            "kind": "ImageStreamTag", ❶
            "name": "example:latest", ❷
            "namespace": "myapp" ❸
          },
          "fieldPath": "spec.template.spec.containers[?(@.name=='web')].image", ❹
          "paused": false ❺
        },
        # ...
      ]
    # ...
```

- ❶ 必須: **kind** は、トリガーするリソースであり、**ImageStreamTag** である必要があります。
- ❷ 必須: **name** はイメージストリームタグの名前である必要があります。
- ❸ オプション: **namespace** はデフォルトでオブジェクトの namespace に設定されます。
- ❹ 必須: **fieldPath** は変更する JSON パスです。このフィールドは制限され、ID またはインデックスでコンテナに正確に一致する JSON パス式のみを受け入れます。Pod の場合、JSON パスは **spec.containers[?(@.name='web')].image** です。
- ❺ オプション: **paused** はトリガーが一時停止されるかどうかを意味し、デフォルト値は **false** です。このトリガーを一時的に無効にするには、**paused** を **true** に設定します。

コア Kubernetes リソースの1つに Pod テンプレートとこのアノテーションの両方が含まれる場合、OpenShift Container Platform は現時点でトリガーで参照されるイメージストリームタグに関連付けられているイメージを使用してオブジェクトの更新を試行します。この更新は、指定の **fieldPath** に対して実行されます。

Pod テンプレートおよびアノテーションの両方が含まれるコア Kubernetes リソースの例には、以下が含まれます。

- **CronJobs**
- **Deployments**
- **StatefulSets**
- **DaemonSets**
- **Jobs**
- **ReplicationControllers**
- **Pods**

### 8.3. KUBERNETES リソースでのイメージトリガーの設定

イメージトリガーをデプロイメントに追加する際に、**oc set triggers** コマンドを使用できます。たとえば、この手順のコマンド例は、イメージ変更トリガーを **example** という名前のデプロイメントに追加し、**example:latest** イメージストリームタグの更新時に、デプロイメント内の **web** コンテナが新規の値で更新されるようにします。このコマンドは、デプロイメントリソースに正しい **image.openshift.io/triggers** アノテーションを設定します。

#### 手順

- **oc set triggers** コマンドを入力して Kubernetes リソースをトリガーします。

```
$ oc set triggers deploy/example --from-image=example:latest -c web
```

#### トリガーアノテーションを使用したデプロイメントの例

```
apiVersion: apps/v1
kind: Deployment
metadata:
  annotations:
    image.openshift.io/triggers: '[{"from":
{"kind":"ImageStreamTag","name":"example:latest"},"fieldPath":"spec.template.spec.containers[
?(@.name=="container").image}]]'
# ...
```

デプロイメントが一時停止されない限り、この Pod テンプレートの更新により、デプロイメントはイメージの新規の値で自動的に実行されます。

## 第9章 イメージ設定リソース

以下の手順でイメージレジストリーを設定します。

### 9.1. イメージコントローラー設定パラメーター

`image.config.openshift.io/cluster` resource は、イメージの処理方法についてのクラスター全体の情報を保持します。正規名および唯一の有効な名前となるのは `cluster` です。 `spec` は以下の設定パラメーターを提供します。



#### 注記

`DisableScheduledImport`、`MaxImagesBulkImportedPerRepository`、`MaxScheduledImportsPerMinute`、`ScheduledImageImportMinimumIntervalSeconds`、`InternalRegistryHostname` などのパラメーターは設定できません。

| パラメーター                                  | 説明  |
|---|---|
| <code>allowedRegistriesForImport</code> | <p>標準ユーザーがイメージのインポートに使用できるコンテナイメージレジストリーを制限します。このリストを、有効なイメージを含むものとしてユーザーが信頼し、アプリケーションのインポート元となるレジストリーに設定します。イメージまたは <code>ImageStreamMappings</code> を API 経由で作成するパーミッションを持つユーザーは、このポリシーによる影響を受けません。通常、これらのパーミッションを持っているのはクラスター管理者のみです。</p> <p>このリストのすべての要素に、レジストリーのドメイン名で指定されるレジストリーの場所が含まれます。</p> <p><b>domainName:</b> レジストリーのドメイン名を指定します。レジストリーが標準以外の (80 または 443) ポートを使用する場合、ポートはドメイン名にも含まれる必要があります。</p> <p><b>insecure:</b> <code>insecure</code> はレジストリーがセキュアか、非セキュアであることを示します。指定がない場合には、デフォルトでレジストリーはセキュアであることが想定されます。</p> |
| <code>additionalTrustedCA</code>        | <p><code>image stream import</code>、<code>pod image pull</code>、<code>openshift-image-registry pullthrough</code>、およびビルド時に信頼される必要のある追加の CA が含まれる <code>config map</code> の参照です。</p> <p>この <code>config map</code> の namespace は <code>openshift-config</code> です。 <code>config map</code> の形式では、信頼する追加のレジストリー CA についてレジストリーのホスト名をキーとして使用し、PEM エンコード証明書を値として使用します。</p>   |
| <code>externalRegistryHostnames</code>  | <p>デフォルトの外部イメージレジストリーのホスト名を指定します。外部ホスト名は、イメージレジストリーが外部に公開される場合にのみ設定される必要があります。最初の値は、イメージストリームの <code>publicDockerImageRepository</code> フィールドで使用されます。値は <code>hostname[:port]</code> 形式の値である必要があります。</p>  |



| パラメーター                 | 説明  |
|------------------------|---|
| <b>registrySources</b> | <p>コンテナランタイムがビルドおよび Pod のイメージへのアクセス時に個々のレジストリーを処理する方法を決定する設定が含まれます。たとえば、非セキュアなアクセスを許可するかどうかを設定します。内部クラスターレジストリーの設定は含まれません。</p> <p><b>insecureRegistries:</b> 有効な TLS 証明書を持たないか、HTTP 接続のみをサポートするレジストリーです。すべてのサブドメインを指定するには、ドメイン名に接頭辞としてアスタリスク (*) ワイルドカード文字を追加します。例: <b>*.example.com</b> レジストリー内で個別のリポジトリーを指定できます。例: <b>reg1.io/myrepo/myapp:latest</b></p> <p><b>blockedRegistries:</b> イメージのプルおよびプッシュアクションが拒否されるレジストリーです。すべてのサブドメインを指定するには、ドメイン名に接頭辞としてアスタリスク (*) ワイルドカード文字を追加します。例: <b>*.example.com</b> レジストリー内で個別のリポジトリーを指定できます。例: <b>reg1.io/myrepo/myapp:latest</b> 他のすべてのレジストリーは許可されます。</p> <p><b>allowedRegistries:</b> イメージのプルおよびプッシュアクションが許可されるレジストリーです。すべてのサブドメインを指定するには、ドメイン名に接頭辞としてアスタリスク (*) ワイルドカード文字を追加します。例: <b>*.example.com</b> レジストリー内で個別のリポジトリーを指定できます。例: <b>reg1.io/myrepo/myapp:latest</b> 他のすべてのレジストリーはブロックされます。</p> <p><b>containerRuntimeSearchRegistries:</b> イメージの短縮名を使用したイメージのプルおよびプッシュアクションが許可されるレジストリーです。他のすべてのレジストリーはブロックされます。</p> <p><b>blockedRegistries</b> または <b>allowedRegistries</b> のいずれかを設定できますが、両方を設定することはできません。</p> |



### 警告

**allowedRegistries** パラメーターが定義されると、明示的に一覧表示されない限り、**registry.redhat.io** レジストリーと **quay.io** レジストリー、およびデフォルトの OpenShift イメージレジストリーを含むすべてのレジストリーがブロックされます。パラメーターを使用する場合は、Pod の失敗を防ぐために、**registry.redhat.io** レジストリーと **quay.io** レジストリー、および **internalRegistryHostname** を含むすべてのレジストリーを **allowedRegistries** 一覧に追加します。これらは、お使いの環境内のペイロードイメージで必要とされます。非接続クラスターの場合、ミラーレジストリーも追加する必要があります。

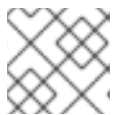
**image.config.openshift.io/cluster** リソースの **status** フィールドは、クラスターから観察される値を保持します。

| パラメーター                           | 説明  |
|----------------------------------|---|
| <b>internalRegistryHostname</b>  | <b>internalRegistryHostname</b> を制御する Image Registry Operator によって設定されます。これはデフォルトの OpenShift イメージレジストリーのホスト名を設定します。値は <b>hostname[:port]</b> 形式の値である必要があります。後方互換性を確保するために、 <b>OPENSIFT_DEFAULT_REGISTRY</b> 環境変数を依然として使用できますが、この設定によってこの環境変数は上書きされます。 |
| <b>externalRegistryHostnames</b> | Image Registry Operator によって設定され、イメージレジストリーが外部に公開されるときに、イメージレジストリーの外部ホスト名を提供します。最初の値は、イメージストリームの <b>publicDockerImageRepository</b> フィールドで使用されます。値は <b>hostname[:port]</b> 形式の値である必要があります。  |

## 9.2. イメージレジストリーの設定

**image.config.openshift.io/cluster** カスタムリソース (CR) を編集してイメージレジストリーの設定を行うことができます。レジストリーへの変更が **image.config.openshift.io/cluster** CR に適用されると、Machine Config Operator (MCO) は以下の一連のアクションを実行します。

1. ノードを封鎖します
2. CRI-O を再起動して変更を適用します
3. ノードを解放します



### 注記

MCO は、変更を検出してもノードを再起動しません。

### 手順

1. **image.config.openshift.io/cluster** カスタムリソースを編集します。

```
$ oc edit image.config.openshift.io/cluster
```

以下は、**image.config.openshift.io/cluster** CR の例になります。

```
apiVersion: config.openshift.io/v1
kind: Image 1
metadata:
  annotations:
    release.openshift.io/create-only: "true"
    creationTimestamp: "2019-05-17T13:44:26Z"
  generation: 1
  name: cluster
  resourceVersion: "8302"
  selfLink: /apis/config.openshift.io/v1/images/cluster
  uid: e34555da-78a9-11e9-b92b-06d6c7da38dc
spec:
  allowedRegistriesForImport: 2
    - domainName: quay.io
```

```

insecure: false
additionalTrustedCA: 3
  name: myconfigmap
registrySources: 4
  allowedRegistries:
  - example.com
  - quay.io
  - registry.redhat.io
  - image-registry.openshift-image-registry.svc:5000
  - reg1.io/myrepo/myapp:latest
  insecureRegistries:
  - insecure.com
status:
  internalRegistryHostname: image-registry.openshift-image-registry.svc:5000

```

- 1 **Image:** イメージの処理方法についてのクラスター全体の情報を保持します。正規名および唯一の有効な名前となるのは **cluster** です。
- 2 **allowedRegistriesForImport:** 標準ユーザーがイメージのインポートに使用するコンテナイメージレジストリーを制限します。このリストを、有効なイメージを含むものとしてユーザーが信頼し、アプリケーションのインポート元となるレジストリーに設定します。イメージまたは **ImageStreamMappings** を API 経由で作成するパーミッションを持つユーザーは、このポリシーによる影響を受けません。通常、これらのパーミッションを持っているのはクラスター管理者のみです。
- 3 **additionalTrustedCA:** イメージストリームのインポート、Pod のイメージプル、**openshift-image-registry** プルスルー、およびビルド時に信頼される追加の認証局 (CA) が含まれる config map の参照です。この config map の namespace は **openshift-config** です。config map の形式では、信頼する追加のレジストリー CA についてレジストリーのホスト名をキーとして使用し、PEM 証明書を値として使用します。
- 4 **registrySources:** ビルドおよび Pod のイメージにアクセスする際に、コンテナランタイムが個々のレジストリーを許可するかブロックするかを決定する設定が含まれます。**allowedRegistries** パラメーターまたは **blockedRegistries** パラメーターのいずれかを設定できますが、両方を設定することはできません。安全でないレジストリーまたはイメージの短い名前を使用するレジストリーを許可するレジストリーへのアクセスを許可するかどうかを定義することもできます。この例では、使用が許可されるレジストリーを定義する **allowedRegistries** パラメーターを使用します。安全でないレジストリー **insecure.com** も許可されます。**registrySources** パラメーターには、内部クラスターレジストリーの設定は含まれません。



## 注記

**allowedRegistries** パラメーターが定義されると、明示的に一覧表示されない限り、registry.redhat.io レジストリーと quay.io レジストリー、およびデフォルトの OpenShift イメージレジストリーを含むすべてのレジストリーがブロックされます。パラメーターを使用する場合は、Pod の失敗を防ぐために、**registry.redhat.io** レジストリーと **quay.io** レジストリー、および **internalRegistryHostname** を **allowedRegistries** 一覧に追加する必要があります。これらは、お使いの環境内のペイロードイメージで必要とされます。**registry.redhat.io** および **quay.io** レジストリーを **blockedRegistries** 一覧に追加しないでください。

**allowedRegistries**、**blockedRegistries**、または **insecureRegistries** パラメーターを使用する場合は、レジストリー内に個別のリポジトリを指定できます。  
例: **reg1.io/myrepo/myapp:latest**

セキュリティ上のリスクを軽減するために、非セキュアな外部レジストリーは回避する必要があります。

2. 変更が適用されたことを確認するには、ノードを一覧表示します。

```
$ oc get nodes
```

## 出力例

| NAME                                       | STATUS                   | ROLES         | AGE | VERSION         |
|--|--------------------------|---------------|-----|-----------------|
| ip-10-0-137-182.us-east-2.compute.internal | Ready,SchedulingDisabled | worker        | 65m | v1.25.4+77bec7a |
| ip-10-0-139-120.us-east-2.compute.internal | Ready,SchedulingDisabled | control-plane | 74m | v1.25.4+77bec7a |
| ip-10-0-176-102.us-east-2.compute.internal | Ready                    | control-plane | 75m | v1.25.4+77bec7a |
| ip-10-0-188-96.us-east-2.compute.internal  | Ready                    | worker        | 65m | v1.25.4+77bec7a |
| ip-10-0-200-59.us-east-2.compute.internal  | Ready                    | worker        | 63m | v1.25.4+77bec7a |
| ip-10-0-223-123.us-east-2.compute.internal | Ready                    | control-plane | 73m | v1.25.4+77bec7a |

### 9.2.1. 特定のレジストリーの追加

**image.config.openshift.io/cluster** カスタムリソース (CR) を編集してイメージのプおよびプッシュアクションで許可されるレジストリーのリスト、およびオプションでレジストリー内の個別のリポジトリを追加できます。OpenShift Container Platform は、この CR への変更をクラスター内のすべてのノードに適用します。

イメージをプルまたはプッシュする場合、コンテナランタイムは **image.config.openshift.io/cluster** CR の **registrySources** パラメーターの下にリスト表示されるレジストリーを検索します。**allowedRegistries** パラメーターの下にレジストリーのリストを作成している場合、コンテナランタイムはそれらのレジストリーのみを検索します。一覧に含まれていないレジストリーはブロックされます。



## 警告

**allowedRegistries** パラメーターが定義されると、明示的に一覧表示されない限り、**registry.redhat.io** レジストリーと **quay.io** レジストリー、およびデフォルトの OpenShift イメージレジストリーを含むすべてのレジストリーがブロックされます。パラメーターを使用する場合は、Pod の失敗を防ぐために、**registry.redhat.io** レジストリーと **quay.io** レジストリー、および **internalRegistryHostname** を **allowedRegistries** リストに追加します。これらは、お使いの環境内のペイロードイメージで必要とされます。非接続クラスターの場合、ミラーレジストリーも追加する必要があります。

## 手順

1. **image.config.openshift.io/cluster** CR を編集します。

```
$ oc edit image.config.openshift.io/cluster
```

以下は、許可リストを含む **image.config.openshift.io/cluster** リソースの例になります。

```
apiVersion: config.openshift.io/v1
kind: Image
metadata:
  annotations:
    release.openshift.io/create-only: "true"
  creationTimestamp: "2019-05-17T13:44:26Z"
  generation: 1
  name: cluster
  resourceVersion: "8302"
  selfLink: /apis/config.openshift.io/v1/images/cluster
  uid: e34555da-78a9-11e9-b92b-06d6c7da38dc
spec:
  registrySources: ①
  allowedRegistries: ②
  - example.com
  - quay.io
  - registry.redhat.io
  - reg1.io/myrepo/myapp:latest
  - image-registry.openshift-image-registry.svc:5000
status:
  internalRegistryHostname: image-registry.openshift-image-registry.svc:5000
```

- ① コンテナランタイムがビルドおよび Pod のイメージへのアクセス時に個々のレジストリーを処理する方法を決定する設定が含まれます。内部クラスターレジストリーの設定は含まれません。
- ② レジストリー、およびイメージのプルおよびプッシュアクションに使用するレジストリー内のリポジトリーを指定します。他のすべてのレジストリーはブロックされます。



## 注記

**allowedRegistries** パラメーターまたは **blockedRegistries** パラメーターのいずれかを設定できますが、両方を設定することはできません。

Machine Config Operator (MCO) は、**image.config.openshift.io/cluster** リソースでレジストリーへの変更の有無を監視します。MCO が変更を検出すると、これはノードをドレイン (解放) し、その変更を適用してノードの遮断を解除します。ノードが **Ready** 状態に戻った後に、許可されるレジストリーリストは、各ノードの `/etc/containers/policy.json` ファイルでイメージ署名ポリシーを更新するために使用されます。

## 検証

- 次のコマンドを入力して、ノードのリストを取得します。

```
$ oc get nodes
```

出力例

```
NAME           STATUS ROLES           AGE VERSION
<node_name>    Ready  control-plane,master 37m v1.27.8+4fab27b
```

- 次のコマンドを実行し、ノード上でデバッグモードに入ります。

```
$ oc debug node/<node_name>
```

- プロンプトが表示されたら、ターミナルに **chroot /host** を入力します。

```
sh-4.4# chroot /host
```

- 次のコマンドを入力して、レジストリーがポリシーファイルに追加されたことを確認します。

```
sh-5.1# cat /etc/containers/policy.json | jq '.'
```

以下のポリシーは、イメージのプルおよびプッシュで、example.com、quay.io、および registry.redhat.io レジストリーからのイメージのみを許可されることを示しています。

### 例9.1 イメージ署名ポリシーファイルの例

```
{
  "default":[
    {
      "type":"reject"
    }
  ],
  "transports":{
    "atomic":{
      "example.com":[
        {
          "type":"insecureAcceptAnything"
        }
      ]
    }
  ]
}
```

```
"image-registry.openshift-image-registry.svc:5000":[
  {
    "type":"insecureAcceptAnything"
  }
],
"insecure.com":[
  {
    "type":"insecureAcceptAnything"
  }
],
"quay.io":[
  {
    "type":"insecureAcceptAnything"
  }
],
"reg4.io/myrepo/myapp:latest":[
  {
    "type":"insecureAcceptAnything"
  }
],
"registry.redhat.io":[
  {
    "type":"insecureAcceptAnything"
  }
]
},
"docker":{
  "example.com":[
    {
      "type":"insecureAcceptAnything"
    }
  ],
  "image-registry.openshift-image-registry.svc:5000":[
    {
      "type":"insecureAcceptAnything"
    }
  ],
  "insecure.com":[
    {
      "type":"insecureAcceptAnything"
    }
  ],
  "quay.io":[
    {
      "type":"insecureAcceptAnything"
    }
  ],
  "reg4.io/myrepo/myapp:latest":[
    {
      "type":"insecureAcceptAnything"
    }
  ],
  "registry.redhat.io":[
    {
      "type":"insecureAcceptAnything"
    }
  ]
}
```

```

    ]
  },
  "docker-daemon":{
    "insecureRegistries":[
      {
        "type":"insecureAcceptAnything"
      }
    ]
  }
}

```

### 注記

クラスターが **registrySources.insecureRegistries** パラメーターを使用する場合、非セキュアなレジストリーが許可リストに含まれることを確認します。

以下に例を示します。

```

spec:
  registrySources:
    insecureRegistries:
      - insecure.com
    allowedRegistries:
      - example.com
      - quay.io
      - registry.redhat.io
      - insecure.com
      - image-registry.openshift-image-registry.svc:5000

```

## 9.2.2. 特定のレジストリーのブロック

**image.config.openshift.io/cluster** カスタムリソース (CR) を編集してレジストリー、およびオプションでレジストリー内の個別のリポジトリーをブロックできます。OpenShift Container Platform は、この CR への変更をクラスター内のすべてのノードに適用します。

イメージをプルまたはプッシュする場合、コンテナーランタイムは **image.config.openshift.io/cluster** CR の **registrySources** パラメーターの下にリスト表示されるレジストリーを検索します。**blockedRegistries** パラメーターの下にレジストリーのリストを作成した場合、コンテナーランタイムはそれらのレジストリーを検索しません。他のすべてのレジストリーは許可されます。



### 警告

Pod の失敗を防ぐために、**registry.redhat.io** レジストリーおよび **quay.io** レジストリーを **blockedRegistries** リストに追加しないでください。これらは、お使いの環境内のペイロードイメージで必要とされます。



1. `image.config.openshift.io/cluster` CR を編集します。

```
$ oc edit image.config.openshift.io/cluster
```

以下は、ブロックリストを含む `image.config.openshift.io/cluster` CR の例です。

```
apiVersion: config.openshift.io/v1
kind: Image
metadata:
  annotations:
    release.openshift.io/create-only: "true"
  creationTimestamp: "2019-05-17T13:44:26Z"
  generation: 1
  name: cluster
  resourceVersion: "8302"
  selfLink: /apis/config.openshift.io/v1/images/cluster
  uid: e34555da-78a9-11e9-b92b-06d6c7da38dc
spec:
  registrySources: 1
  blockedRegistries: 2
  - untrusted.com
  - reg1.io/myrepo/myapp:latest
status:
  internalRegistryHostname: image-registry.openshift-image-registry.svc:5000
```

- 1 コンテナランタイムがビルドおよび Pod のイメージへのアクセス時に個々のレジストリーを処理する方法を決定する設定が含まれます。内部クラスターレジストリーの設定は含まれません。
- 2 レジストリー、およびオプションでイメージのプルおよびプッシュアクションに使用できないレジストリー内のリポジトリーを指定します。他のすべてのレジストリーは許可されます。



## 注記

**blockedRegistries** レジストリーまたは **allowedRegistries** レジストリーのいずれかを設定できますが、両方を設定することはできません。

Machine Config Operator (MCO) は、`image.config.openshift.io/cluster` リソースでレジストリーへの変更の有無を監視します。MCO が変更を検出すると、これはノードをドレイン (解放) し、その変更を適用してノードの遮断を解除します。ノードが **Ready** 状態に戻った後に、ブロックされたレジストリーへの変更は各ノードの `/etc/containers/registries.conf` ファイルに表示されます。

## 検証

- 次のコマンドを入力して、ノードのリストを取得します。

```
$ oc get nodes
```

出力例

```

NAME          STATUS  ROLES          AGE  VERSION
<node_name>  Ready  control-plane,master  37m  v1.27.8+4fab27b

```

1. 次のコマンドを実行し、ノード上でデバッグモードに入ります。

```
$ oc debug node/<node_name>
```

2. プロンプトが表示されたら、ターミナルに **chroot /host** を入力します。

```
sh-4.4# chroot /host
```

3. 次のコマンドを入力して、レジストリーがポリシーファイルに追加されたことを確認します。

```
sh-5.1# cat etc/containers/registries.conf
```

以下の例では、**untrusted.com** レジストリーからのイメージが、イメージのプルおよびプッシュで許可されないことを示しています。

### 出力例

```

unqualified-search-registries = ["registry.access.redhat.com", "docker.io"]

[[registry]]
  prefix = ""
  location = "untrusted.com"
  blocked = true

```

#### 9.2.2.1. ペイロードレジストリーのブロック

ミラーリング設定では、**ImageContentSourcePolicy** (ICSP) オブジェクトを使用して、切断された環境でアップストリームペイロードレジストリーをブロックできます。以下の手順例は、**quay.io/openshift-payload** ペイロードレジストリーをブロックする方法を示しています。

#### 手順

1. **ImageContentSourcePolicy** (ICSP) オブジェクトを使用してミラー設定を作成し、ペイロードをインスタンスのレジストリーにミラーリングします。以下の ICSP ファイルの例は、ペイロード **internal-mirror.io/openshift-payload** をミラーリングします。

```

apiVersion: operator.openshift.io/v1alpha1
kind: ImageContentSourcePolicy
metadata:
  name: my-icsp
spec:
  repositoryDigestMirrors:
  - mirrors:
    - internal-mirror.io/openshift-payload
    source: quay.io/openshift-payload

```

2. オブジェクトがノードにデプロイされたら、**/etc/containers/registries.conf** ファイルをチェックして、ミラー設定が設定されていることを確認します。

## 出力例

```
[[registry]]
  prefix = ""
  location = "quay.io/openshift-payload"
  mirror-by-digest-only = true

[[registry.mirror]]
  location = "internal-mirror.io/openshift-payload"
```

3. 次のコマンドを使用して、**image.config.openshift.io** カスタムリソースファイルを編集します。

```
$ oc edit image.config.openshift.io cluster
```

4. ペイロードレジストリーをブロックするには、次の設定を **image.config.openshift.io** カスタムリソースファイルに追加します。

```
spec:
  registrySource:
    blockedRegistries:
      - quay.io/openshift-payload
```

## 検証

- ノードの **/etc/containers/registries.conf** ファイルをチェックして、上流のペイロードレジストリーがブロックされていることを確認します。

## 出力例

```
[[registry]]
  prefix = ""
  location = "quay.io/openshift-payload"
  blocked = true
  mirror-by-digest-only = true

[[registry.mirror]]
  location = "internal-mirror.io/openshift-payload"
```

### 9.2.3. 非セキュアなレジストリー

**image.config.openshift.io/cluster** カスタムリソース (CR) を編集して、非セキュアなレジストリー、およびオプションでレジストリー内の個別のリポジトリーを追加できます。OpenShift Container Platform は、この CR への変更をクラスター内のすべてのノードに適用します。

有効な SSL 証明書を使用しないレジストリー、または HTTPS 接続を必要としないレジストリーは、非セキュアであると見なされます。



## 警告

セキュリティ上のリスクを軽減するために、非セキュアな外部レジストリーは回避する必要があります。

## 手順

1. **image.config.openshift.io/cluster** CR を編集します。

```
$ oc edit image.config.openshift.io/cluster
```

以下は、非セキュアなレジストリーのリストを含む **image.config.openshift.io/cluster** CR の例になります。

```
apiVersion: config.openshift.io/v1
kind: Image
metadata:
  annotations:
    release.openshift.io/create-only: "true"
    creationTimestamp: "2019-05-17T13:44:26Z"
  generation: 1
  name: cluster
  resourceVersion: "8302"
  selfLink: /apis/config.openshift.io/v1/images/cluster
  uid: e34555da-78a9-11e9-b92b-06d6c7da38dc
spec:
  registrySources: ❶
  insecureRegistries: ❷
  - insecure.com
  - reg4.io/myrepo/myapp:latest
  allowedRegistries:
  - example.com
  - quay.io
  - registry.redhat.io
  - insecure.com ❸
  - reg4.io/myrepo/myapp:latest
  - image-registry.openshift-image-registry.svc:5000
status:
  internalRegistryHostname: image-registry.openshift-image-registry.svc:5000
```

- ❶ コンテナランタイムがビルドおよび Pod のイメージへのアクセス時に個々のレジストリーを処理する方法を決定する設定が含まれます。内部クラスターレジストリーの設定は含まれません。
- ❷ 非セキュアなレジストリーを指定します。そのレジストリーでリポジトリを指定できます。
- ❸ 非セキュアなレジストリーが **allowedRegistries** 一覧に含まれていることを確認します。



## 注記

**allowedRegistries** パラメーターが定義されると、明示的に一覧表示されない限り、registry.redhat.io レジストリーと quay.io レジストリー、およびデフォルトの OpenShift イメージレジストリーを含むすべてのレジストリーがブロックされます。パラメーターを使用する場合は、Pod の失敗を防ぐために、**registry.redhat.io** レジストリーと **quay.io** レジストリー、および **internalRegistryHostname** を含むすべてのレジストリーを **allowedRegistries** リストに追加します。これらは、お使いの環境内のペイロードイメージが必要とされます。非接続クラスターの場合、ミラーレジストリーも追加する必要があります。

Machine Config Operator (MCO) は、**image.config.openshift.io/cluster** CR でレジストリーへの変更の有無を監視し、変更を検出するとノードをドレイン (解放) し、遮断を解除します。ノードが **Ready** 状態に戻った後に、非セキュアな、およびブロックされたレジストリーへの変更は、各ノードの **/etc/containers/registries.conf** ファイルに表示されます。

## 検証

- レジストリーがポリシーファイルに追加されていることを確認するには、ノードで以下のコマンドを使用します。

```
$ cat /etc/containers/registries.conf
```

以下の例は、**insecure.com** レジストリーからのイメージが非セキュアであり、イメージのプルおよびプッシュで許可されることを示しています。

## 出力例

```
unqualified-search-registries = ["registry.access.redhat.com", "docker.io"]

[[registry]]
  prefix = ""
  location = "insecure.com"
  insecure = true
```

### 9.2.4. イメージの短縮名を許可するレジストリーの追加

**image.config.openshift.io/cluster** カスタムリソース (CR) を編集して、イメージの短縮名を検索するためにレジストリーを追加できます。OpenShift Container Platform は、この CR への変更をクラスター内のすべてのノードに適用します。

イメージの短縮名を使用して、プル仕様に完全修飾ドメイン名を追加せずに、イメージを検索できます。たとえば、**registry.access.redhat.com/rhe7/etcd** の代わりに **rhel7/etcd** を使用できます。

完全パスを使用することが実際的ではない場合に、短縮名を使用できる場合があります。たとえば、クラスターが DNS が頻繁に変更される複数の内部レジストリーを参照する場合、毎回の変更ごとにプル仕様の完全修飾ドメイン名を更新する必要が生じる可能性があります。この場合は、イメージの短縮名を使用した方が良いでしょう。

イメージをプルまたはプッシュする場合、コンテナーランタイムは **image.config.openshift.io/cluster** CR の **registrySources** パラメーターの下にリスト表示されるレジストリーを検索します。短縮名を使用してイメージをプル際に、**containerRuntimeSearchRegistries** パラメーターでレジストリーのリストを作成している場合、コンテナーランタイムはそれらのレジストリーを検索します。



## 警告

公開レジストリーで認証が必要な場合、イメージがデプロイされない可能性があるため、公開レジストリーでイメージの短縮名を使用することは推奨しません。公開レジストリーで完全修飾イメージ名を使用します。

通常、Red Hat の内部レジストリーまたはプライベートレジストリーは、イメージの短縮名の使用をサポートしています。

### **containerRuntimeSearchRegistries** パラメーター

(**registry.redhat.io**、**docker.io**、および **quay.io** レジストリーを含む) にパブリックレジストリーをリスト表示する場合、認証情報はリスト上のすべてのレジストリーに公開され、ネットワークおよびレジストリーの攻撃にされされるリスクが生じます。イメージをプルするためのプルシークレットは1つしかないため、グローバルプルシークレットで定義されているように、そのシークレットは、そのリスト内のすべてのレジストリーに対して認証するために使用されます。したがって、リストにパブリックレジストリーを含めると、セキュリティリスクが発生します。

各パブリックレジストリーが異なる認証情報を必要とし、クラスターでグローバルプルシークレットにパブリックレジストリーがリストされない場合には、**containerRuntimeSearchRegistries** パラメーターの下に複数のパブリックレジストリーをリストできません。

認証が必要なパブリックレジストリーの場合、レジストリーの認証情報がグローバルプルシークレットに格納されている場合にのみ、イメージの短縮名を使用できます。

Machine Config Operator (MCO) は、**image.config.openshift.io/cluster** リソースでレジストリーへの変更の有無を監視します。MCO が変更を検出すると、これはノードをドレイン (解放) し、その変更を適用してノードの遮断を解除します。ノードが **Ready** 状態に戻った後に、**containerRuntimeSearchRegistries** パラメーターが追加されると、MCO はリスト表示されるレジストリーで各ノードの `/etc/containers/registries.conf.d` ディレクトリーにファイルを作成します。このファイルは、`/etc/containers/registries.conf` ファイルの非修飾検索レジストリーのデフォルトリストをオーバーライドします。修飾されていない検索レジストリーのデフォルトリストにフォールバックする方法はありません。

**containerRuntimeSearchRegistries** パラメーターは、Podman および CRI-O コンテナエンジンを使用する場合のみ機能します。リストのレジストリーは、ビルドおよびイメージストリームではなく、Pod 仕様でのみ使用できます。

## 手順

1. **image.config.openshift.io/cluster** CR を編集します。

```
$ oc edit image.config.openshift.io/cluster
```

以下は、**image.config.openshift.io/cluster** CR の例になります。

```
apiVersion: config.openshift.io/v1
kind: Image
metadata:
```

```

annotations:
  release.openshift.io/create-only: "true"
creationTimestamp: "2019-05-17T13:44:26Z"
generation: 1
name: cluster
resourceVersion: "8302"
selfLink: /apis/config.openshift.io/v1/images/cluster
uid: e34555da-78a9-11e9-b92b-06d6c7da38dc
spec:
  allowedRegistriesForImport:
    - domainName: quay.io
      insecure: false
  additionalTrustedCA:
    name: myconfigmap
  registrySources:
    containerRuntimeSearchRegistries: ❶
    - reg1.io
    - reg2.io
    - reg3.io
    allowedRegistries: ❷
    - example.com
    - quay.io
    - registry.redhat.io
    - reg1.io
    - reg2.io
    - reg3.io
    - image-registry.openshift-image-registry.svc:5000
  ...
status:
  internalRegistryHostname: image-registry.openshift-image-registry.svc:5000

```

- ❶ イメージの短縮名で使用するレジストリーを指定します。セキュリティ上のリスクが発生する可能性を軽減するために、内部レジストリーまたはプライベートレジストリーでのみイメージの短縮名を使用する必要があります。
- ❷ **containerRuntimeSearchRegistries** に一覧表示されるレジストリーが **allowedRegistries** 一覧に含まれることを確認します。



### 注記

**allowedRegistries** パラメーターが定義されると、明示的に一覧表示されない限り、**registry.redhat.io** レジストリーと **quay.io** レジストリー、およびデフォルトの OpenShift イメージレジストリーを含むすべてのレジストリーがブロックされます。このパラメーターを使用する場合は、Pod の失敗を防ぐために、**registry.redhat.io** レジストリーと **quay.io** レジストリー、および **internalRegistryHostname** を含むすべてのレジストリーを **allowedRegistries** リストに追加します。これらは、お使いの環境内のペイロードイメージで必要とされます。非接続クラスターの場合、ミラーレジストリーも追加する必要があります。

### 検証

- 次のコマンドを入力して、ノードのリストを取得します。

```
$ oc get nodes
```

出力例

```
NAME          STATUS ROLES          AGE VERSION
<node_name>   Ready  control-plane,master 37m v1.27.8+4fab27b
```

1. 次のコマンドを実行し、ノード上でデバッグモードに入ります。

```
$ oc debug node/<node_name>
```

2. プロンプトが表示されたら、ターミナルに **chroot /host** を入力します。

```
sh-4.4# chroot /host
```

3. 次のコマンドを入力して、レジストリーがポリシーファイルに追加されたことを確認します。

```
sh-5.1# cat /etc/containers/registries.conf.d/01-image-searchRegistries.conf
```

出力例

```
unqualified-search-registries = ['reg1.io', 'reg2.io', 'reg3.io']
```

## 9.2.5. イメージレジストリーアクセス用の追加のトラストストアの設定

**image.config.openshift.io/cluster** カスタムリソースには、イメージレジストリーのアクセス時に信頼される追加の認証局が含まれる config map への参照を含めることができます。

### 前提条件

- 認証局 (CA) は PEM でエンコードされている。

### 手順

**openshift-config** namespace で config map を作成し、**image.config.openshift.io** カスタムリソースの **AdditionalTrustedCA** でその名前を使用して、外部レジストリーにアクセスするときに信頼する必要がある追加の CA を提供できます。

config map のキーは、この CA を信頼するポートがあるレジストリーのホスト名であり、値は各追加レジストリー CA が信頼する証明書のコンテンツです。

### イメージレジストリー CA の config map の例

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: my-registry-ca
data:
  registry.example.com: |
    -----BEGIN CERTIFICATE-----
    ...
    -----END CERTIFICATE-----
```



```
registry-with-port.example.com.:5000: | 1
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

- 1 レジストリーにポートがある場合 (例: **registry-with-port.example.com:5000**)、: は .. に置き換える必要があります。

以下の手順で追加の CA を設定できます。

- 追加の CA を設定するには、以下を実行します。

```
$ oc create configmap registry-config --from-file=<external_registry_address>=ca.crt -n
openshift-config
```

```
$ oc edit image.config.openshift.io cluster
```

```
spec:
  additionalTrustedCA:
    name: registry-config
```

### 9.2.6. イメージレジストリーのリポジトリミラーリングの設定

コンテナレジストリーのリポジトリミラーリングの設定により、以下が可能になります。

- ソースイメージのレジストリーのリポジトリからイメージをプルする要求をリダイレクトするように OpenShift Container Platform クラスターを設定し、これをミラーリングされたイメージレジストリーのリポジトリで解決できるようにします。
- 各ターゲットリポジトリに対して複数のミラーリングされたリポジトリを特定し、1つのミラーがダウンした場合に別のミラーを使用できるようにします。

以下は、OpenShift Container Platform のリポジトリミラーリングの属性の一部です。

- イメージプルには、レジストリーのダウンタイムに対する回復性があります。
- 切断された環境のクラスターは、quay.io などの重要な場所からイメージをプルし、会社のファイアウォールの背後にあるレジストリーに要求されたイメージを提供することができます。
- イメージのプル要求時にレジストリーへの接続が特定の順序で試行され、通常は永続レジストリーが最後に試行されます。
- 入力したミラー情報は、OpenShift Container Platform クラスターの全ノードの `/etc/containers/registries.conf` ファイルに追加されます。
- ノードがソースリポジトリからイメージの要求を行うと、要求されたコンテンツを見つけるまで、ミラーリングされた各リポジトリに対する接続を順番に試行します。すべてのミラーで障害が発生した場合、クラスターはソースリポジトリに対して試行します。成功すると、イメージはノードにプルされます。

リポジトリミラーリングのセットアップは次の方法で実行できます。

- OpenShift Container Platform のインストール時:

OpenShift Container Platform に必要なコンテナイメージをプルし、それらのイメージを会社のファイアウォールの背後に配置することで、切断された環境にあるデータセンターに OpenShift Container Platform をインストールできます。

- OpenShift Container Platform の新規インストール後:  
OpenShift Container Platform インストール時にミラーリングを設定しなくても、**ImageContentSourcePolicy** オブジェクトを使用して後で設定することができます。

次の手順では、インストール後のミラー設定を行います。ここでは、以下を特定する **ImageContentSourcePolicy** オブジェクトを作成します。

- ミラーリングするコンテナイメージリポジトリのソース
- ソースリポジトリから要求されたコンテンツを提供する各ミラーリポジトリの個別のエントリー。



### 注記

**ImageContentSourcePolicy** オブジェクトを持つクラスターのグローバルプルシークレットのみを設定できます。プロジェクトにプルシークレットを追加することはできません。

### 前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。

### 手順

1. ミラーリングされたりポジトリを設定します。以下のいずれかを実行します。
  - [Repository Mirroring in Red Hat Quay](#) で説明されているように、Red Hat Quay でミラーリングされたりポジトリを設定します。Red Hat Quay を使用すると、あるリポジトリから別のリポジトリにイメージをコピーでき、これらのリポジトリを一定期間繰り返し自動的に同期することもできます。
  - **skopeo** などのツールを使用して、ソースディレクトリーからミラーリングされたりポジトリにイメージを手動でコピーします。  
たとえば、Red Hat Enterprise Linux (RHEL 7 または RHEL 8) システムに **skopeo** RPM パッケージをインストールした後、以下の例に示すように **skopeo** コマンドを使用します。

```
$ skopeo copy \
docker://registry.access.redhat.com/ubi8/ubi-
minimal@sha256:5cfbaf45ca96806917830c183e9f37df2e913b187adb32e89fd83fa455eba
a6 \
docker://example.io/example/ubi-minimal
```

この例では、**example.io** という名前のコンテナイメージレジストリーと **example** という名前のイメージリポジトリがあり、そこに **registry.access.redhat.com** から **ubi8/ubi-minimal** イメージをコピーします。レジストリーを作成した後、OpenShift Container Platform クラスターを設定して、ソースリポジトリで作成される要求をミラーリングされたりポジトリにリダイレクトできます。

2. OpenShift Container Platform クラスターにログインします。

3. **ImageContentSourcePolicy** ファイル (例: **registryrepomirror.yaml**) を作成し、ソースとミラーを固有のレジストリー、およびリポジトリーのペアとイメージのものに置き換えます。

```

apiVersion: operator.openshift.io/v1alpha1
kind: ImageContentSourcePolicy
metadata:
  name: ubi8repo
spec:
  repositoryDigestMirrors:
  - mirrors:
    - example.io/example/ubi-minimal ①
    - example.com/example/ubi-minimal ②
    source: registry.access.redhat.com/ubi8/ubi-minimal ③
  - mirrors:
    - mirror.example.com/redhat
    source: registry.redhat.io/openshift4 ④
  - mirrors:
    - mirror.example.com
    source: registry.redhat.io ⑤
  - mirrors:
    - mirror.example.net/image
    source: registry.example.com/example/myimage ⑥
  - mirrors:
    - mirror.example.net
    source: registry.example.com/example ⑦
  - mirrors:
    - mirror.example.net/registry-example-com
    source: registry.example.com ⑧

```

- ① イメージレジストリーおよびリポジトリーの名前を示します。
- ② 各ターゲットリポジトリーの複数のミラーリポジトリーを示します。1つのミラーがダウンした場合、ターゲットリポジトリーは別のミラーを使用できます。
- ③ ミラーリングされているコンテンツが含まれるレジストリーおよびリポジトリーを示します。
- ④ レジストリー内の namespace を、その namespace の任意のイメージを使用するように設定できます。レジストリードメインをソースとして使用する場合は、**ImageContentSourcePolicy** リソースはレジストリーからすべてのリポジトリーに適用されます。
- ⑤ レジストリー名を設定すると、ソースレジストリーからミラーレジストリーまでのすべてのリポジトリーに **ImageContentSourcePolicy** リソースが適用されます。
- ⑥ イメージ **mirror.example.net/image@sha256:...** をプルします。
- ⑦ ミラー **mirror.example.net/myimage@sha256:...** からソースレジストリー namespace のイメージ **myimage** をプルします。
- ⑧ ミラーレジストリー **mirror.example.net/registry-example-com/example/myimage@sha256:...** からイメージ **registry.example.com/example/myimage** をプルします。**ImageContentSourcePolicy** リソースは、ソースレジストリーからミラーレジストリー **mirror.example.net/registry-example-com** までのすべてのリポジトリーに適用されます。

4. 新しい **ImageContentSourcePolicy** オブジェクトを作成します。

```
$ oc create -f registryrepomirror.yaml
```

**ImageContentSourcePolicy** オブジェクトが作成されると、新しい設定が各ノードにデプロイされ、クラスターはソースリポジトリへの要求のためにミラーリングされたリポジトリの使用を開始します。

5. ミラーリングされた設定が適用されていることを確認するには、ノードのいずれかで以下を実行します。
- ノードのリストを表示します。

```
$ oc get node
```

#### 出力例

| NAME                         | STATUS | ROLES  | AGE | VERSION |
|------------------------------|--------|--------|-----|---------|
| ip-10-0-137-44.ec2.internal  | Ready  | worker | 7m  | v1.25.0 |
| ip-10-0-138-148.ec2.internal | Ready  | master | 11m | v1.25.0 |
| ip-10-0-139-122.ec2.internal | Ready  | master | 11m | v1.25.0 |
| ip-10-0-147-35.ec2.internal  | Ready  | worker | 7m  | v1.25.0 |
| ip-10-0-153-12.ec2.internal  | Ready  | worker | 7m  | v1.25.0 |
| ip-10-0-154-10.ec2.internal  | Ready  | master | 11m | v1.25.0 |

**Imagecontentsourcepolicy** リソースはノードを再起動しません。

- デバッグプロセスを開始し、ノードにアクセスします。

```
$ oc debug node/ip-10-0-147-35.ec2.internal
```

#### 出力例

```
Starting pod/ip-10-0-147-35ec2internal-debug ...
To use host binaries, run `chroot /host`
```

- ルートディレクトリを **/host** に変更します。

```
sh-4.2# chroot /host
```

- /etc/containers/registries.conf** ファイルをチェックして、変更が行われたことを確認します。

```
sh-4.2# cat /etc/containers/registries.conf
```

#### 出力例

```
unqualified-search-registries = ["registry.access.redhat.com", "docker.io"]
short-name-mode = ""

[[registry]]
  prefix = ""
  location = "registry.access.redhat.com/ubi8/ubi-minimal"
```

```

mirror-by-digest-only = true

[[registry.mirror]]
  location = "example.io/example/ubi-minimal"

[[registry.mirror]]
  location = "example.com/example/ubi-minimal"

[[registry]]
  prefix = ""
  location = "registry.example.com"
  mirror-by-digest-only = true

[[registry.mirror]]
  location = "mirror.example.net/registry-example-com"

[[registry]]
  prefix = ""
  location = "registry.example.com/example"
  mirror-by-digest-only = true

[[registry.mirror]]
  location = "mirror.example.net"

[[registry]]
  prefix = ""
  location = "registry.example.com/example/myimage"
  mirror-by-digest-only = true

[[registry.mirror]]
  location = "mirror.example.net/image"

[[registry]]
  prefix = ""
  location = "registry.redhat.io"
  mirror-by-digest-only = true

[[registry.mirror]]
  location = "mirror.example.com"

[[registry]]
  prefix = ""
  location = "registry.redhat.io/openshift4"
  mirror-by-digest-only = true

[[registry.mirror]]
  location = "mirror.example.com/redhat"

```

- e. ソースからノードにイメージダイジェストをプルし、ミラーによって解決されているかどうかを確認します。 **ImageContentSourcePolicy** オブジェクトはイメージダイジェストのみをサポートし、イメージタグはサポートしません。

```

sh-4.2# podman pull --log-level=debug registry.access.redhat.com/ubi8/ubi-
minimal@sha256:5cfbaf45ca96806917830c183e9f37df2e913b187adb32e89fd83fa455eba
a6

```

## リポジトリのミラーリングのトラブルシューティング

リポジトリのミラーリング手順が説明どおりに機能しない場合は、リポジトリミラーリングの動作方法についての以下の情報を使用して、問題のトラブルシューティングを行うことができます。

- 最初に機能するミラーは、プルされるイメージを指定するために使用されます。
- メインレジストリーは、他のミラーが機能していない場合にのみ使用されます。
- システムコンテキストによって、**Insecure** フラグがフォールバックとして使用されます。
- `/etc/containers/registries.conf` ファイルの形式が最近変更されました。現在のバージョンはバージョン 2 で、TOML 形式です。

### 関連情報

- グローバルプルシークレットの詳細は、[グローバルクラスタープルシークレットの更新](#) を参照してください。

## 第10章 テンプレートの使用

以下のセクションでは、テンプレートの概要と共に、それらを使用し、作成する方法についての概要を説明します。

### 10.1. テンプレートについて

テンプレートでは、パラメーター化や処理が可能な一連のオブジェクトを記述し、OpenShift Container Platform で作成するためのオブジェクトのリストを生成します。テンプレートは、サービス、ビルド設定およびデプロイメント設定など、プロジェクト内で作成パーミッションがあるすべてのものを作成するために処理できます。また、テンプレートではラベルのセットを定義して、これをテンプレート内に定義されたすべてのオブジェクトに適用できます。

オブジェクトのリストは CLI を使用してテンプレートから作成することも、テンプレートがプロジェクトまたはグローバルテンプレートライブラリーにアップロードされている場合、Web コンソールを使用することもできます。

### 10.2. テンプレートのアップロード

テンプレートを定義する JSON または YAML ファイルがある場合は、CLI を使用してテンプレートをプロジェクトにアップロードできます。こうすることで、プロジェクトにテンプレートが保存され、対象のプロジェクトに対して適切なアクセス権があるユーザーがこれを繰り返し使用できます。独自のテンプレートの記述方法については、このトピックの後半で説明します。

#### 手順

- 次のいずれかの方法を使用してテンプレートをアップロードします。
  - 現在のプロジェクトのテンプレートライブラリーにテンプレートをアップロードするには、JSON または YAML ファイルを以下のコマンドで渡します。

```
$ oc create -f <filename>
```

- **-n** オプションを使用してプロジェクト名を指定することで、別のプロジェクトにテンプレートをアップロードできます。

```
$ oc create -f <filename> -n <project>
```

テンプレートは、Web コンソールまたは CLI を使用して選択できるようになりました。

### 10.3. WEB コンソールを使用したアプリケーションの作成

Web コンソールを使用して、テンプレートからアプリケーションを作成することができます。

#### 手順

1. Web コンソールのナビゲーションメニューの上部にあるコンテキストセレクトターから **Developer** を選択します。
2. 目的のプロジェクト内で、**+Add** をクリックします。
3. **Developer Catalog** タイルの **All services** をクリックします。

4. **Type** の下の **Builder Images** をクリックして、利用可能なビルダーイメージを表示します。



### 注記

以下に示すように、**builder** タグがアノテーションにリスト表示されているイメージストリームタグのみがリストに表示されます。

```
kind: "ImageStream"
apiVersion: "v1"
metadata:
  name: "ruby"
  creationTimestamp: null
spec:
# ...
  tags:
    - name: "2.6"
      annotations:
        description: "Build and run Ruby 2.6 applications"
        iconClass: "icon-ruby"
        tags: "builder,ruby" ❶
        supports: "ruby:2.6,ruby"
        version: "2.6"
# ...
```

- ❶ ここに **builder** を含めると、このイメージストリームがビルダーとして Web コンソールに表示されます。

5. 新規アプリケーション画面で設定を変更し、オブジェクトをアプリケーションをサポートするように設定します。

## 10.4. CLI を使用してテンプレートからオブジェクトを作成する手順

CLI を使用して、テンプレートを処理し、オブジェクトを作成するために生成された設定を使用できません。

### 10.4.1. ラベルの追加

ラベルは、Pod などの生成されたオブジェクトを管理し、整理するために使用されます。テンプレートで指定されるラベルは、テンプレートから生成されるすべてのオブジェクトに適用されます。

#### 手順

- コマンドラインからテンプレートにラベルを追加します。

```
$ oc process -f <filename> -l name=otherLabel
```

### 10.4.2. パラメーターのリスト表示

上書きできるパラメーターのリストは、テンプレートの **parameters** セクションに表示されます。

#### 手順



1. CLI で以下のコマンドを使用し、使用するファイルを指定して、パラメーターをリスト表示することができます。

```
$ oc process --parameters -f <filename>
```

または、テンプレートがすでにアップロードされている場合には、以下を実行します。

```
$ oc process --parameters -n <project> <template_name>
```

たとえば、デフォルトの **openshift** プロジェクトにあるクイックスタートテンプレートのいずれかに対してパラメーターを一覧表示する場合に、以下のような出力が表示されます。

```
$ oc process --parameters -n openshift rails-postgresql-example
```

### 出力例

```
NAME          DESCRIPTION
GENERATOR     VALUE
SOURCE_REPOSITORY_URL  The URL of the repository with your application source
code          https://github.com/sclorg/rails-ex.git
SOURCE_REPOSITORY_REF  Set this to a branch name, tag or other ref of your
repository if you are not using the default branch
CONTEXT_DIR    Set this to the relative path to your project if it is not in the root of
your repository
APPLICATION_DOMAIN  The exposed hostname that will route to the Rails service
rails-postgresql-example.openshiftapps.com
GITHUB_WEBHOOK_SECRET  A secret string used to configure the GitHub webhook
expression      [a-zA-Z0-9]{40}
SECRET_KEY_BASE      Your secret key for verifying the integrity of signed cookies
expression      [a-z0-9]{127}
APPLICATION_USER    The application user that is used within the sample application
to authorize access on pages      openshift
APPLICATION_PASSWORD  The application password that is used within the sample
application to authorize access on pages      secret
DATABASE_SERVICE_NAME  Database service name
postgresql
POSTGRES_USER        database username
expression          user[A-Z0-9]{3}
POSTGRES_PASSWORD    database password
expression          [a-zA-Z0-9]{8}
POSTGRES_DATABASE    database name
root
POSTGRES_MAX_CONNECTIONS  database max connections
10
POSTGRES_SHARED_BUFFERS  database shared buffers
12MB
```

この出力から、テンプレートの処理時に正規表現のようなジェネレーターで生成された複数のパラメーターを特定できます。

### 10.4.3. オブジェクトリストの生成

CLI を使用して、標準出力にオブジェクトリストを返すテンプレートを定義するファイルを処理できます。

## 手順

1. 標準出力にオブジェクトリストを返すテンプレートを定義するファイル进行处理します。

```
$ oc process -f <filename>
```

または、テンプレートがすでに現在のプロジェクトにアップロードされている場合には以下を実行します。

```
$ oc process <template_name>
```

2. テンプレートを処理し、**oc create** の出力をパイプして、テンプレートからオブジェクトを作成します。

```
$ oc process -f <filename> | oc create -f -
```

または、テンプレートがすでに現在のプロジェクトにアップロードされている場合には以下を実行します。

```
$ oc process <template> | oc create -f -
```

3. 上書きする **<name>=<value>** の各ペアに、**-p** オプションを追加することで、ファイルに定義されたパラメーターの値を上書きできます。パラメーター参照は、テンプレートアイテム内のテキストフィールドに表示されます。  
たとえば、テンプレートの以下の **POSTGRESQL\_USER** および **POSTGRESQL\_DATABASE** パラメーターを上書きし、カスタマイズされた環境変数の設定を出力します。

- a. テンプレートからのオブジェクトリストの作成

```
$ oc process -f my-rails-postgresql \
  -p POSTGRESQL_USER=bob \
  -p POSTGRESQL_DATABASE=mydatabase
```

- b. JSON ファイルは、ファイルにリダイレクトすることも、**oc create** コマンドで処理済みの出力をパイプして、テンプレートをアップロードせずに直接適用することも可能です。

```
$ oc process -f my-rails-postgresql \
  -p POSTGRESQL_USER=bob \
  -p POSTGRESQL_DATABASE=mydatabase \
  | oc create -f -
```

- c. 多数のパラメーターがある場合は、それらをファイルに保存してからそのファイルを **oc process** に渡すことができます。

```
$ cat postgres.env
POSTGRESQL_USER=bob
POSTGRESQL_DATABASE=mydatabase
```

```
$ oc process -f my-rails-postgresql --param-file=postgres.env
```

- d. **--param-file** の引数として **"-"** を使用して、標準入力から環境を読み込むこともできます。

```
$ sed s/bob/alice/ postgres.env | oc process -f my-rails-postgresql --param-file=-
```

## 10.5. アップロードしたテンプレートの変更

すでにプロジェクトにアップロードされているテンプレートを編集できます。

### 手順

- すでにアップロードされているテンプレートを変更します。

```
$ oc edit template <template>
```

## 10.6. インスタントアプリとクイックスタートテンプレートの使用

OpenShift Container Platform では、デフォルトで、インスタントアプリとクイックスタートテンプレートを複数提供しており、各種言語で簡単に新規アプリの構築を開始できます。Rails (Ruby)、Django (Python)、Node.js、CakePHP (PHP) および Dancer (Perl) 用のテンプレートを利用できます。クラスター管理者は、これらのテンプレートを利用できるようにデフォルトのグローバル **openshift** プロジェクトにこれらのテンプレートを作成している必要があります。

デフォルトで、テンプレートビルドは必要なアプリケーションコードが含まれる GitHub の公開ソースリポジトリを使用して行われます。

### 手順

1. 以下のように、利用可能なデフォルトのインスタントアプリとクイックスタートテンプレートをリスト表示できます。

```
$ oc get templates -n openshift
```

2. ソースを変更し、アプリケーションの独自のバージョンをビルドするには、以下を実行します。
  - a. テンプレートのデフォルト **SOURCE\_REPOSITORY\_URL** パラメーターが参照するリポジトリをフォークします。
  - b. テンプレートから作成する場合には、**SOURCE\_REPOSITORY\_URL** パラメーターの値を上書きします。デフォルト値ではなく、フォークを指定してください。これにより、テンプレートで作成したビルド設定はアプリケーションコードのフォークを参照するようになり、コードを変更し、アプリケーションを自由に再ビルドできます。



### 注記

一部のインスタントアプリおよびクイックスタートのテンプレートで、データベースのデプロイメント設定を定義します。テンプレートが定義する設定では、データベースコンテンツ用に一時ストレージを使用します。データベース Pod が何らかの理由で再起動されると、データベースの全データが失われてしまうので、これらのテンプレートはデモ目的でのみ使用する必要があります。

### 10.6.1. クイックスタートテンプレート

クイックスタートテンプレートは、OpenShift Container Platform で実行されるアプリケーションの基本的な例です。クイックスタートはさまざまな言語やフレームワークが含まれており、サービスのセット、ビルド設定およびデプロイメント設定などで設定されるテンプレートで定義されています。このテ

ンプレートは、必要なイメージやソースリポジトリを参照して、アプリケーションをビルドし、デプロイします。

クイックスタートを確認するには、テンプレートからアプリケーションを作成します。管理者がこれらのテンプレートを OpenShift Container Platform クラスターにすでにインストールしている必要がありますが、その場合には、Web コンソールからこれを簡単に選択できます。

クイックスタートは、アプリケーションのソースコードを含むソースリポジトリを参照します。クイックスタートをカスタマイズするには、リポジトリをフォークし、テンプレートからアプリケーションを作成する時に、デフォルトのソースリポジトリ名をフォークしたリポジトリに置き換えます。これにより、提供されたサンプルのソースではなく、独自のソースコードを使用してビルドが実行されます。ソースリポジトリでコードを更新し、新しいビルドを起動して、デプロイされたアプリケーションで変更が反映されていることを確認できます。

### 10.6.1.1. Web フレームワーククイックスタートテンプレート

以下のクイックスタートテンプレートでは、指定のフレームワークおよび言語の基本アプリケーションを提供します。

- CakePHP: PHP Web フレームワーク (MySQL データベースを含む)
- Dancer: Perl Web フレームワーク (MySQL データベースを含む)
- Django: Python Web フレームワーク (PostgreSQL データベースを含む)
- NodeJS: NodeJS web アプリケーション (MongoDB データベースを含む)
- Rails: Ruby Web フレームワーク (PostgreSQL データベースを含む)

## 10.7. テンプレートの作成

アプリケーションの全オブジェクトを簡単に再作成するために、新規テンプレートを定義できます。テンプレートでは、作成するオブジェクトと、これらのオブジェクトの作成をガイドするメタデータを定義します。

以下は、単純なテンプレートオブジェクト定義 (YAML) の例です。

```
apiVersion: template.openshift.io/v1
kind: Template
metadata:
  name: redis-template
  annotations:
    description: "Description"
    iconClass: "icon-redis"
    tags: "database,nosql"
objects:
- apiVersion: v1
  kind: Pod
  metadata:
    name: redis-master
  spec:
    containers:
    - env:
      - name: REDIS_PASSWORD
        value: ${REDIS_PASSWORD}
      image: dockerfile/redis
```

```

name: master
ports:
- containerPort: 6379
  protocol: TCP
parameters:
- description: Password used for Redis authentication
  from: '[A-Z0-9]{8}'
  generate: expression
  name: REDIS_PASSWORD
labels:
redis: master

```

### 10.7.1. テンプレート記述の作成

テンプレートの記述により、テンプレートの内容に関する情報を提供でき、Web コンソールでの検索時に役立ちます。テンプレート名以外のメタデータは任意ですが、使用できると便利です。メタデータには、一般的な説明などの情報以外にタグのセットも含まれます。便利なタグにはテンプレートで使用する言語名などがあります (例: Java、PHP、Ruby)。

以下は、テンプレート記述メタデータの例です。

```

kind: Template
apiVersion: template.openshift.io/v1
metadata:
name: cakephp-mysql-example ❶
annotations:
openshift.io/display-name: "CakePHP MySQL Example (Ephemeral)" ❷
description: >-
An example CakePHP application with a MySQL database. For more information
about using this template, including OpenShift considerations, see
https://github.com/sclorg/cakephp-ex/blob/master/README.md.

WARNING: Any data stored will be lost upon pod destruction. Only use this
template for testing." ❸
openshift.io/long-description: >-
This template defines resources needed to develop a CakePHP application,
including a build configuration, application DeploymentConfig, and
database DeploymentConfig. The database is stored in
non-persistent storage, so this configuration should be used for
experimental purposes only. ❹
tags: "quickstart,php,cakephp" ❺
iconClass: icon-php ❻
openshift.io/provider-display-name: "Red Hat, Inc." ❼
openshift.io/documentation-url: "https://github.com/sclorg/cakephp-ex" ❽
openshift.io/support-url: "https://access.redhat.com" ❾
message: "Your admin credentials are ${ADMIN_USERNAME}:${ADMIN_PASSWORD}" ❿

```

- ❶ テンプレートの一意の名前。
- ❷ ユーザーインターフェイスで利用できるように、ユーザーに分かりやすく、簡単な名前。
- ❸ テンプレートの説明。デプロイされる内容、デプロイ前に知っておく必要のある注意点をユーザーが理解できるように詳細を追加します。README ファイルなど、追加情報へのリンクも追加します。

す。バラグラフを作成するには、改行を追加できます。

- 4 追加の説明。たとえば、サービスカタログに表示されます。
- 5 検索およびグループ化を実行するためにテンプレートに関連付けられるタグ。これを指定されるカタログカテゴリのいずれかに組み込むタグを追加します。コンソールの定数ファイルの **CATALOG\_CATEGORIES** で **id** および **categoryAliases** を参照してください。カテゴリはクラスター全体に対してカスタマイズすることもできます。
- 6 Web コンソールでテンプレートと一緒に表示されるアイコン。

#### 例10.1 利用可能なアイコン

- **icon-3scale**
- **icon-aerogear**
- **icon-amq**
- **icon-angularjs**
- **icon-ansible**
- **icon-apache**
- **icon-beaker**
- **icon-camel**
- **icon-capedwarf**
- **icon-cassandra**
- **icon-catalog-icon**
- **icon-clojure**
- **icon-codeigniter**
- **icon-cordova**
- **icon-datagrid**
- **icon-datavirt**
- **icon-debian**
- **icon-decisionserver**
- **icon-django**
- **icon-dotnet**
- **icon-drupal**
- **icon-eap**
- **icon-elastic**

- `icon-erlang`
- `icon-fedora`
- `icon-freebsd`
- `icon-git`
- `icon-github`
- `icon-gitlab`
- `icon-glassfish`
- `icon-go-gopher`
- `icon-golang`
- `icon-grails`
- `icon-hadoop`
- `icon-haproxy`
- `icon-helm`
- `icon-infinispan`
- `icon-jboss`
- `icon-jenkins`
- `icon-jetty`
- `icon-joomla`
- `icon-jruby`
- `icon-js`
- `icon-knative`
- `icon-kubevirt`
- `icon-laravel`
- `icon-load-balancer`
- `icon-mariadb`
- `icon-mediawiki`
- `icon-memcached`
- `icon-mongodb`
- `icon-mssql`

- **icon-mysql-database**
- **icon-nginx**
- **icon-nodejs**
- **icon-openjdk**
- **icon-openliberty**
- **icon-openshift**
- **icon-openstack**
- **icon-other-linux**
- **icon-other-unknown**
- **icon-perl**
- **icon-phalcon**
- **icon-php**
- **icon-play**
- **iconpostgresql**
- **icon-processserver**
- **icon-python**
- **icon-quarkus**
- **icon-rabbitmq**
- **icon-rails**
- **icon-redhat**
- **icon-redis**
- **icon-rh-integration**
- **icon-rh-spring-boot**
- **icon-rh-tomcat**
- **icon-ruby**
- **icon-scala**
- **icon-serverlessfx**
- **icon-shadowman**
- **icon-spring-boot**



- **icon-spring**
- **icon-sso**
- **icon-stackoverflow**
- **icon-suse**
- **icon-symfony**
- **icon-tomcat**
- **icon-ubuntu**
- **icon-vertx**
- **icon-wildfly**
- **icon-windows**
- **icon-wordpress**
- **icon-xamarin**
- **icon-zend**

- 7 テンプレートを提供する人または組織の名前
- 8 テンプレートに関する他のドキュメントを参照する URL
- 9 テンプレートに関するサポートを取得できる URL
- 10 テンプレートがインスタンス化された時に表示される説明メッセージ。このフィールドで、新規作成されたリソースの使用方法をユーザーに通知します。生成された認証情報や他のパラメーターを出力に追加できるように、メッセージの表示前にパラメーターの置換が行われます。ユーザーが従うべき次の手順が記載されたドキュメントへのリンクを追加してください。

### 10.7.2. テンプレートラベルの作成

テンプレートにはラベルのセットを追加できます。これらのラベルは、テンプレートがインスタンス化される時に作成されるオブジェクトごとに追加します。このようにラベルを定義すると、特定のテンプレートから作成された全オブジェクトの検索、管理が簡単になります。

以下は、テンプレートオブジェクトのラベルの例です。

```
kind: "Template"
apiVersion: "v1"
...
labels:
  template: "cakephp-mysql-example" 1
  app: "${NAME}" 2
```

- 1 このテンプレートから作成する全オブジェクトに適用されるラベル

- 2 パラメーター化されたラベル。このラベルは、このテンプレートを基に作成された全オブジェクトに適用されます。パラメーターは、ラベルキーおよび値の両方で拡張されます。

### 10.7.3. テンプレートパラメーターの作成

パラメーターにより、テンプレートがインスタンス化される時に値を生成するか、ユーザーが値を指定できるようになります。パラメーターが参照されると、値が置換されます。参照は、オブジェクト一覧フィールドであればどこでも定義できます。これは、無作為にパスワードを作成したり、テンプレートのカスタマイズに必要なユーザー固有の値やホスト名を指定したりできるので便利です。パラメーターは、2種類の方法で参照可能です。

- 文字列の値として、テンプレートの文字列フィールドに `${PARAMETER_NAME}` の形式で配置する
- JSON/YAML の値として、テンプレートのフィールドに `${{PARAMETER_NAME}}` の形式で配置する

`${PARAMETER_NAME}` 構文を使用すると、複数のパラメーター参照を1つのフィールドに統合でき、`"http://${PARAMETER_1}${PARAMETER_2}"` などのように、参照を固定データ内に埋め込むことができます。どちらのパラメーター値も置換されて、引用された文字列が最終的な値になります。

`${{PARAMETER_NAME}}` 構文のみを使用する場合は、単一のパラメーター参照のみが許可され、先頭文字や終了文字は使用できません。結果の値は、置換後に結果が有効な JSON オブジェクトの場合は引用されません。結果が有効な JSON 値でない場合に、結果の値は引用され、標準の文字列として処理されます。

単一のパラメーターは、テンプレート内で複数回参照でき、1つのテンプレート内で両方の置換構文を使用して参照することができます。

デフォルト値を指定でき、ユーザーが別の値を指定していない場合に使用されます。

以下は、明示的な値をデフォルト値として設定する例です。

```
parameters:
- name: USERNAME
  description: "The user name for Joe"
  value: joe
```

パラメーター値は、パラメーター定義に指定したルールを基に生成することも可能です。以下は、パラメーター値の生成例です。

```
parameters:
- name: PASSWORD
  description: "The random user password"
  generate: expression
  from: "[a-zA-Z0-9]{12}"
```

上記の例では、処理後に、英字の大文字、小文字、数字すべてを含む 12 文字長のパスワードが無作為に作成されます。

利用可能な構文は、完全な正規表現構文ではありません。ただし、`\w`、`\d`、`\a`、および `\A` 修飾子を使用できます。

- `[w]{10}` は、10 桁の英字、数字、およびアンダースコアを生成します。これは PCRE 標準に準拠し、`[a-zA-Z0-9_]{10}` に相当します。

- `[d]{10}` は 10 桁の数字を生成します。これは `[0-9]{10}` に相当します。
- `[a]{10}` は 10 桁の英字を生成します。これは `[a-zA-Z]{10}` に相当します。
- `[A]{10}` は 10 の句読点または記号文字を生成します。これは `[~!@#$$%^&*()\- _+={}\|\\\|<, > . ? / ' " ; : ] { 10}` に相当します。

## 注記

テンプレートが YAML または JSON で記述されているかどうか、また修飾子が組み込まれている文字列のタイプによっては、2 番目のバックスラッシュでバックスラッシュをエスケープする必要がある場合があります。以下は例になります。

## 修飾子を含む YAML テンプレートの例

```
parameters:
- name: singlequoted_example
  generate: expression
  from: '[A]{10}'
- name: doublequoted_example
  generate: expression
  from: "[\A]{10}"
```

## 修飾子を含む JSON テンプレートの例

```
{
  "parameters": [
    {
      "name": "json_example",
      "generate": "expression",
      "from": "[\A]{10}"
    }
  ]
}
```

以下は、パラメーター定義と参照を含む完全なテンプレートの例です。

```
kind: Template
apiVersion: template.openshift.io/v1
metadata:
  name: my-template
objects:
- kind: BuildConfig
  apiVersion: build.openshift.io/v1
  metadata:
    name: cakephp-mysql-example
  annotations:
    description: Defines how to build the application
  spec:
    source:
      type: Git
      git:
        uri: "${SOURCE_REPOSITORY_URL}" ❶
        ref: "${SOURCE_REPOSITORY_REF}"
```

```

  contextDir: "${CONTEXT_DIR}"
- kind: DeploymentConfig
  apiVersion: apps.openshift.io/v1
  metadata:
    name: frontend
  spec:
    replicas: "${REPLICA_COUNT}" ❷
parameters:
- name: SOURCE_REPOSITORY_URL ❸
  displayName: Source Repository URL ❹
  description: The URL of the repository with your application source code ❺
  value: https://github.com/sclorg/cakephp-ex.git ❻
  required: true ❼
- name: GITHUB_WEBHOOK_SECRET
  description: A secret string used to configure the GitHub webhook
  generate: expression ❽
  from: "[a-zA-Z0-9]{40}" ❾
- name: REPLICA_COUNT
  description: Number of replicas to run
  value: "2"
  required: true
message: "... The GitHub webhook secret is ${GITHUB_WEBHOOK_SECRET} ..." ❿

```

- ❶ この値は、テンプレートがインスタンス化された時点で **SOURCE\_REPOSITORY\_URL** パラメーターに置き換えられます。
- ❷ この値は、テンプレートがインスタンス化された時点で、**REPLICA\_COUNT** パラメーターの引用なしの値に置き換えられます。
- ❸ パラメーター名。この値は、テンプレート内でパラメーターを参照するのに使用します。
- ❹ 分かりやすいパラメーターの名前。これは、ユーザーに表示されます。
- ❺ パラメーターの説明。期待値に対する制約など、パラメーターの目的を詳細にわたり説明します。説明には、コンソールのテキスト標準に従い、完結した文章を使用するようにしてください。表示名と同じ内容を使用しないでください。
- ❻ テンプレートをインスタンス化する時に、ユーザーにより値が上書きされない場合に使用されるパラメーターのデフォルト値。パスワードなどのデフォルト値の使用を避けるようにしてください。シークレットと組み合わせた生成パラメーターを使用するようにしてください。
- ❼ このパラメーターが必須であることを示します。つまり、ユーザーは空の値で上書きできません。パラメーターでデフォルト値または生成値が指定されていない場合には、ユーザーは値を指定する必要があります。
- ❽ 値が生成されるパラメーター
- ❾ ジェネレーターへの入力。この場合、ジェネレーターは、大文字、小文字を含む 40 桁の英数字の値を生成します。
- ❿ パラメーターはテンプレートメッセージに含めることができます。これにより、生成された値がユーザーに通知されます。

#### 10.7.4. テンプレートオブジェクトリストの作成

テンプレートの主な部分は、テンプレートがインスタンス化される時に作成されるオブジェクトのリストです。これには、ビルド設定、デプロイメント設定、またはサービスなどの有効な API オブジェクトを使用できます。オブジェクトはここで定義された通りに作成され、パラメーターの値は作成前に置換されます。これらのオブジェクトの定義では、以前に定義したパラメーターを参照できます。

以下は、オブジェクトリストの例です。

```
kind: "Template"
apiVersion: "v1"
metadata:
  name: my-template
objects:
- kind: "Service" 1
  apiVersion: "v1"
  metadata:
    name: "cakephp-mysql-example"
    annotations:
      description: "Exposes and load balances the application pods"
  spec:
    ports:
      - name: "web"
        port: 8080
        targetPort: 8080
    selector:
      name: "cakephp-mysql-example"
```

**1** サービスの定義。このテンプレートにより作成されます。



### 注記

オブジェクト定義のメタデータに **namespace** フィールドの固定値が含まれる場合、フィールドはテンプレートのインスタンス化の際に定義から取り除かれます。**namespace** フィールドにパラメーター参照が含まれる場合には、通常のパラメーター置換が行われ、パラメーターの置換による値の解決が実行された namespace で、オブジェクトが作成されます。この場合、ユーザーは対象の namespace でオブジェクトを作成するパーミッションがあることが前提になります。

## 10.7.5. テンプレートをバインド可能としてマーキングする

テンプレートサービスブローカーは、認識されているテンプレートオブジェクトごとに、カタログ内にサービスを1つ公開します。デフォルトでは、これらのサービスはそれぞれバインド可能として公開され、エンドユーザーがプロビジョニングしたサービスに対してバインドできるようにします。

### 手順

テンプレートの作成者は、エンドユーザーが指定テンプレートからプロビジョニングされたサービスに対してバインディングすることを防ぐことができます。

- **template.openshift.io/bindable: "false"** のアノテーションをテンプレートに追加して、エンドユーザーが指定のテンプレートからプロビジョニングされるサービスをバインドできないようにできます。

## 10.7.6. テンプレートオブジェクトフィールドの公開

テンプレートの作成者は、テンプレートに含まれる特定のオブジェクトのフィールドを公開すべきかどうかを指定できます。テンプレートサービスブローカーは、**ConfigMap**、**Secret**、**Service**、および **Route** オブジェクトに公開されたフィールドを認識し、ユーザーがブローカーでサポートされているサービスをバインドする際に公開されたフィールドの値を返します。

オブジェクトのフィールドを1つまたは複数公開するには、テンプレート内のオブジェクトに、接頭辞が **template.openshift.io/expose-** または **template.openshift.io/base64-expose-** のアノテーションを追加します。

各アノテーションキーは、**bind** 応答のキーになるように、接頭辞が削除されてパススルーされます。

各アノテーションの値は Kubernetes JSONPath 式の値であり、バインド時に解決され、**bind** 応答で返される値が含まれるオブジェクトフィールドを指定します。



### 注記

**Bind** 応答のキーと値のペアは、環境変数として、システムの他の場所で使用できます。そのため、アノテーションキーで接頭辞を取り除いた値を有効な環境変数名として使用することが推奨されます。先頭に **A-Z**、**a-z** または **\_** を指定して、その後に、ゼロか、他の文字 **A-Z**、**a-z**、**0-9** または **\_** を指定してください。



### 注記

バックスラッシュでエスケープしない限り、Kubernetes の JSONPath 実装は表現内のどの場所に使用されていても、**.**、**@** などはメタ文字として解釈します。そのため、たとえば、**my.key** という名前の **ConfigMap** のデータを参照するには、JSONPath 式は **{.data['my\\.key']}** とする必要があります。JSONPath 式が YAML でどのように記述されているかによって、**"{.data['my\\.key']}"** などのように、追加でバックスラッシュが必要になる場合があります。

以下は、公開されるさまざまなオブジェクトのフィールドの例です。

```
kind: Template
apiVersion: template.openshift.io/v1
metadata:
  name: my-template
objects:
- kind: ConfigMap
  apiVersion: v1
  metadata:
    name: my-template-config
  annotations:
    template.openshift.io/expose-username: "{.data['my\\.username']}"
  data:
    my.username: foo
- kind: Secret
  apiVersion: v1
  metadata:
    name: my-template-config-secret
  annotations:
    template.openshift.io/base64-expose-password: "{.data['password']}"
  stringData:
    password: <password>
- kind: Service
  apiVersion: v1
```

```

metadata:
  name: my-template-service
  annotations:
    template.openshift.io/expose-service_ip_port: "{.spec.clusterIP}:{.spec.ports[?
(.name==\"web\").port]}"
spec:
  ports:
    - name: "web"
      port: 8080
- kind: Route
  apiVersion: route.openshift.io/v1
  metadata:
    name: my-template-route
    annotations:
      template.openshift.io/expose-uri: "http://{.spec.host}{.spec.path}"
  spec:
    path: mypath

```

上記の部分的なテンプレートでの **bind** 操作に対する応答例は以下のようになります。

```

{
  "credentials": {
    "username": "foo",
    "password": "YmFy",
    "service_ip_port": "172.30.12.34:8080",
    "uri": "http://route-test.router.default.svc.cluster.local/mypath"
  }
}

```

## 手順

- **template.openshift.io/expose-** アノテーションを使用して、値を文字列として返します。これは、任意のバイナリーデータを処理しないものの、便利な方法です。
- バイナリーデータを返す必要がある場合、**template.openshift.io/base64-expose-** アノテーションを使用して、データが返される前にデータを base64 でエンコードします。

### 10.7.7. テンプレートの準備ができるまで待機する

テンプレートの作成者は、テンプレート内の特定のオブジェクトがサービスカタログ、Template Service Broker または **TemplateInstance** API によるテンプレートのインスタンス化が完了したとされるまで待機する必要があるかを指定できます。

この機能を使用するには、テンプレート内の

**Build**、**BuildConfig**、**Deployment**、**DeploymentConfig**、**Job** または **StatefulSet** のオブジェクト 1 つ以上に、次のアノテーションでマークを付けてください。

```
"template.alpha.openshift.io/wait-for-ready": "true"
```

テンプレートのインスタンス化は、アノテーションのマークが付けられたすべてのオブジェクトが準備できたと報告されるまで、完了しません。同様に、アノテーションが付けられたオブジェクトが失敗したと報告されるか、固定タイムアウトである 1 時間以内にテンプレートの準備が整わなかった場合に、テンプレートのインスタンス化は失敗します。

インスタンス化の目的で、各オブジェクトの種類の準備状態および失敗は以下のように定義されます。

| 種類                      | 準備状態 (Readiness)  | 失敗 (Failure)  |
|-------------------------|---|---|
| <b>Build</b>            | オブジェクトが Complete (完了) フェーズを報告する   | オブジェクトが Canceled (キャンセル)、Error (エラー)、または Failed (失敗) を報告する              |
| <b>BuildConfig</b>      | 関連付けられた最新のビルドオブジェクトが Complete (完了) フェーズを報告する  | 関連付けられた最新のビルドオブジェクトが Canceled (キャンセル)、Error (エラー)、または Failed (失敗) を報告する |
| <b>Deployment</b>       | オブジェクトは、新しいレプリカセットとデプロイメントが利用可能であると報告する。これにより、オブジェクトで定義される readiness プロブが有効になります。         | オブジェクトで、Progressing (進捗中) の状態が false であると報告される                          |
| <b>DeploymentConfig</b> | オブジェクトは新規レプリケーションコントローラーおよびデプロイメントが利用可能であると報告する。これにより、オブジェクトで定義される readiness プロブが有効になります。 | オブジェクトで、Progressing (進捗中) の状態が false であると報告される                          |
| <b>Job</b>              | オブジェクトが完了 (completion) を報告する  | オブジェクトが1つ以上の失敗が発生したことを報告する  |
| <b>StatefulSet</b>      | オブジェクトはすべてのレプリカが Ready (準備状態) であることを報告する。これにより、オブジェクトで定義される readiness プロブが有効になります。        | 該当なし  |

以下は、テンプレートサンプルを一部抜粋したものです。この例では、**wait-for-ready** アノテーションが使用されています。他のサンプルは、OpenShift Container Platform クイックスタートテンプレートにあります。

```
kind: Template
apiVersion: template.openshift.io/v1
metadata:
  name: my-template
objects:
- kind: BuildConfig
  apiVersion: build.openshift.io/v1
  metadata:
    name: ...
  annotations:
    # wait-for-ready used on BuildConfig ensures that template instantiation
    # will fail immediately if build fails
    template.alpha.openshift.io/wait-for-ready: "true"
  spec:
    ...
- kind: DeploymentConfig
  apiVersion: apps.openshift.io/v1
  metadata:
```



```

name: ...
annotations:
  template.alpha.openshift.io/wait-for-ready: "true"
spec:
  ...
- kind: Service
  apiVersion: v1
  metadata:
    name: ...
  spec:
    ...

```

### その他の推奨事項

- アプリケーションにスムーズに実行するのに十分なリソースが提供されるようにメモリー、CPU、およびストレージのデフォルトサイズを設定します。
- **latest** タグが複数のメジャーバージョンで使用されている場合には、イメージからこのタグを参照しないようにします。新規イメージがそのタグにプッシュされると、実行中のアプリケーションが破損してしまう可能性があります。
- 適切なテンプレートの場合、テンプレートのデプロイ後に変更する必要なしに、ビルドおよびデプロイが正常に行われます。

### 10.7.8. 既存オブジェクトからのテンプレートの作成

テンプレートをゼロから作成するのではなく、プロジェクトから既存のオブジェクトを YAML 形式でエクスポートして、パラメーターを追加したり、テンプレート形式としてカスタマイズしたりして、YAML 形式を変更することもできます。

#### 手順

- オブジェクトを YAML 形式でプロジェクトにエクスポートします。

```
$ oc get -o yaml all > <yaml_filename>
```

**all** ではなく、特定のリソースタイプや複数のリソースを置き換えることも可能です。他の例については、**oc get -h** を実行してください。

**oc get -o yaml all** に含まれるオブジェクトタイプは以下の通りです。

- **BuildConfig**
- **Build**
- **DeploymentConfig**
- **ImageStream**
- **Pod**
- **ReplicationController**
- **Route**
- **Service**



## 注記

コンテンツはクラスターやバージョンによって異なる可能性があるため、**all** エイリアスの使用は推奨されません。代わりに、必要なすべてのリソースを指定してください。

## 第11章 RUBY ON RAILS の使用

Ruby on Rails は Ruby で記述される Web フレームワークです。本書では、OpenShift Container Platform での Rails 4 の使用について扱います。



### 警告

チュートリアル全体をチェックして、OpenShift Container Platform でアプリケーションを実行するために必要なすべての手順を概観してください。問題に直面した場合には、チュートリアル全体を振り返り、もう一度問題に対応してください。またチュートリアルは、実行済みの手順を確認し、すべての手順が適切に実行されていることを確認するのに役立ちます。

### 11.1. 前提条件

- Ruby および Rails の基本知識
- Ruby 2.0.0+、Rubygems、Bundler のローカルにインストールされたバージョン
- Git の基本知識
- OpenShift Container Platform v4 の実行インスタンス
- OpenShift Container Platform のインスタンスが実行中であり、利用可能であることを確認してください。さらに、**oc** CLI クライアントがインストールされており、コマンドがコマンドシェルからアクセスできることを確認し、メールアドレスおよびパスワードを使用してログインする際にこれを使用できるようにします。

### 11.2. データベースの設定

Rails アプリケーションはほぼ常にデータベースと併用されます。ローカル開発の場合は、PostgreSQL データベースを使用します。

#### 手順

1. データベースをインストールします。

```
$ sudo yum install -y postgresql postgresql-server postgresql-devel
```

2. データベースを初期化します。

```
$ sudo postgresql-setup initdb
```

このコマンドで **/var/lib/pgsql/data** ディレクトリーが作成され、このディレクトリーにデータが保存されます。

3. データベースを起動します。

```
$ sudo systemctl start postgresql.service
```

4. データベースが実行されたら、**rails** ユーザーを作成します。

```
$ sudo -u postgres createuser -s rails
```

作成をしたユーザーのパスワードは作成されていない点に留意してください。

## 11.3. アプリケーションの作成

Rails アプリケーションをゼロからビルドするには、Rails gem を先にインストールする必要があります。その後に、アプリケーションを作成することができます。

### 手順

1. Rails gem をインストールします。

```
$ gem install rails
```

### 出力例

```
Successfully installed rails-4.3.0  
1 gem installed
```

2. Rails gem のインストール後に、PostgreSQL をデータベースとして 指定して新規アプリケーションを作成します。

```
$ rails new rails-app --database=postgresql
```

3. 新規アプリケーションディレクトリーに切り替えます。

```
$ cd rails-app
```

4. アプリケーションがすでにある場合には **pg** (postgresql) gem が **Gemfile** に配置されていることを確認します。配置されていない場合には、gem を追加して **Gemfile** を編集します。

```
gem 'pg'
```

5. すべての依存関係を含む **Gemfile.lock** を新たに生成します。

```
$ bundle install
```

6. **pg** gem で **postgresql** データベースを使用するほか、**config/database.yml** が **postgresql** アダプターを使用していることを確認する必要があります。

**config/database.yml** ファイルの **default** セクションを以下のように更新するようにしてください。

```
default: &default  
  adapter: postgresql  
  encoding: unicode  
  pool: 5  
  host: localhost  
  username: rails  
  password: <password>
```

7. アプリケーションの開発およびテスト用のデータベースを作成します。

```
$ rake db:create
```

これで PostgreSQL サーバーに **development** および **test** データベースが作成されます。

### 11.3.1. Welcome ページの作成

Rails 4 では静的な **public/index.html** ページが実稼働環境で提供されなくなったので、新たに root ページを作成する必要があります。

Welcome ページをカスタマイズするには、以下の手順を実行する必要があります。

- index アクションでコントローラーを作成します。
- welcome コントローラーの index アクションの view ページを作成します。
- 作成したコントローラーとビューと共にアプリケーションの root ページを提供するルートを作成します。

Rails には、これらの必要な手順をすべて実行するジェネレーターがあります。

#### 手順

1. Rails ジェネレーターを実行します。

```
$ rails generate controller welcome index
```

すべての必要なファイルが作成されます。

2. 以下のように **config/routes.rb** ファイルの 2 行目を編集します。

```
root 'welcome#index'
```

3. rails server を実行して、ページが利用できることを確認します。

```
$ rails server
```

ブラウザで <http://localhost:3000> に移動してページを表示してください。このページが表示されない場合は、サーバーに出力されるログを確認してデバッグを行ってください。

### 11.3.2. OpenShift Container Platform のアプリケーションの設定

アプリケーションが OpenShift Container Platform で実行中の PostgreSQL データベースサービスと通信できるようにするには、後のデータベースサービスの作成時に定義する必要のある環境変数を使用できるように **config/database.yml** の **default** セクションを編集する必要があります。

#### 手順

- 以下のように事前に定義した変数で、**config/database.yml** の **default** セクションを編集します。

#### **config/database** YAML ファイルのサンプル

```

<% user = ENV.key?("POSTGRESQL_ADMIN_PASSWORD") ? "root" :
ENV["POSTGRESQL_USER"] %>
<% password = ENV.key?("POSTGRESQL_ADMIN_PASSWORD") ?
ENV["POSTGRESQL_ADMIN_PASSWORD"] : ENV["POSTGRESQL_PASSWORD"] %>
<% db_service = ENV.fetch("DATABASE_SERVICE_NAME", "").upcase %>

default: &default
  adapter: postgresql
  encoding: unicode
  # For details on connection pooling, see rails configuration guide
  # http://guides.rubyonrails.org/configuring.html#database-pooling
  pool: <%= ENV["POSTGRESQL_MAX_CONNECTIONS"] || 5 %>
  username: <%= user %>
  password: <%= password %>
  host: <%= ENV["#{db_service}_SERVICE_HOST"] %>
  port: <%= ENV["#{db_service}_SERVICE_PORT"] %>
  database: <%= ENV["POSTGRESQL_DATABASE"] %>

```

### 11.3.3. アプリケーションの Git への保存

通常 OpenShift Container Platform でアプリケーションをビルドする場合、ソースコードを git リポジトリに保存する必要があるため、**git** がない場合にはインストールしてください。

#### 前提条件

- git をインストールします。

#### 手順

1. **ls -l** コマンドを実行して、Rails アプリケーションのディレクトリーで操作を行っていることを確認します。コマンドの出力は以下のようになります。

```
$ ls -l
```

#### 出力例

```

app
bin
config
config.ru
db
Gemfile
Gemfile.lock
lib
log
public
Rakefile
README.rdoc
test
tmp
vendor

```

2. Rails app ディレクトリーで以下のコマンドを実行して、コードを初期化し、git にコミットします。

```
$ git init
```

```
$ git add .
```

```
$ git commit -m "initial commit"
```

アプリケーションがコミットされたら、これをリモートリポジトリにプッシュする必要があります。新規リポジトリを作成する GitHub アカウントです。

3. お使いの **git** リポジトリを参照するリモートを設定します。

```
$ git remote add origin git@github.com:<namespace/repository-name>.git
```

4. アプリケーションをリモートの git リポジトリにプッシュします。

```
$ git push
```

## 11.4. アプリケーションの OPENSIFT CONTAINER PLATFORM へのデプロイ

OpenShift Container Platform にアプリケーションをデプロイすることができます。

**rails-app** プロジェクトの作成後、新規プロジェクトの namespace に自動的に切り替えられます。

OpenShift Container Platform へのアプリケーションのデプロイでは 3 つの手順を実行します。

- OpenShift Container Platform の PostgreSQL イメージからデータベースサービスを作成します。
- データベースサービスと連動する OpenShift Container Platform の Ruby 2.0 ビルダーイメージおよび Ruby on Rails ソースコードのフロントエンドサービスを作成します。
- アプリケーションのルートを作成します。

### 手順

- Ruby on Rails アプリケーションをデプロイするには、アプリケーション用に新規のプロジェクトを作成します。

```
$ oc new-project rails-app --description="My Rails application" --display-name="Rails Application"
```

### 11.4.1. データベースサービスの作成

Rails アプリケーションには実行中のデータベースサービスが必要です。このサービスには、PostgreSQL データベースイメージを使用します。

データベースサービスを作成するために、**oc new-app** コマンドを使用します。このコマンドには、必要な環境変数を渡す必要があります。この環境変数は、データベースコンテナ内で使用します。これらの環境変数は、ユーザー名、パスワード、およびデータベースの名前を設定するために必要です。これらの環境変数の値を任意の値に変更できます。変数は以下のようになります。

- POSTGRESQL\_DATABASE
- POSTGRESQL\_USER
- POSTGRESQL\_PASSWORD

これらの変数を設定すると、以下を確認できます。

- 指定の名前のデータベースが存在する
- 指定の名前のユーザーが存在する
- ユーザーは指定のパスワードで指定のデータベースにアクセスできる

## 手順

1. データベースサービスを作成します。

```
$ oc new-app postgresql -e POSTGRESQL_DATABASE=db_name -e  
POSTGRESQL_USER=username -e POSTGRESQL_PASSWORD=password
```

データベース管理者のパスワードを設定するには、直前のコマンドに以下を追加します。

```
-e POSTGRESQL_ADMIN_PASSWORD=admin_pw
```

2. 進行状況を確認します。

```
$ oc get pods --watch
```

### 11.4.2. フロントエンドサービスの作成

アプリケーションを OpenShift Container Platform にデプロイするには、アプリケーションが置かれるリポジトリを指定する必要があります。

## 手順

1. フロントエンドサービスを作成し、データベースサービスの作成時に設定されたデータベース関連の環境変数を指定します。

```
$ oc new-app path/to/source/code --name=rails-app -e POSTGRESQL_USER=username -e  
POSTGRESQL_PASSWORD=password -e POSTGRESQL_DATABASE=db_name -e  
DATABASE_SERVICE_NAME=postgresql
```

このコマンドでは、OpenShift Container Platform は指定された環境変数を使用してソースコードの取得、ビルダーのセットアップ、アプリケーションイメージのビルド、新規に作成されたイメージのデプロイを実行します。このアプリケーションには **rails-app** という名前を指定します。

2. **rails-app** デプロイメント設定の JSON ドキュメントを参照して、環境変数が追加されたかどうかを確認できます。

```
$ oc get dc rails-app -o json
```

以下のセクションが表示されるはずですが。



## 出力例

```
env": [
  {
    "name": "POSTGRESQL_USER",
    "value": "username"
  },
  {
    "name": "POSTGRESQL_PASSWORD",
    "value": "password"
  },
  {
    "name": "POSTGRESQL_DATABASE",
    "value": "db_name"
  },
  {
    "name": "DATABASE_SERVICE_NAME",
    "value": "postgresql"
  }
],
```

- ビルドプロセスを確認します。

```
$ oc logs -f build/rails-app-1
```

- ビルドが完了すると、OpenShift Container Platform で Pod が実行されていることを確認します。

```
$ oc get pods
```

**myapp-<number>-<hash>** で始まる行が表示されますが、これは OpenShift Container Platform で実行中のアプリケーションです。

- データベースの移行スクリプトを実行してデータベースを初期化してからでないと、アプリケーションは機能しません。これを実行する 2 種類の方法があります。

- 実行中のフロントエンドコンテナから手動で実行する
  - rsh** コマンドでフロントエンドコンテナに `exec` を実行します。

```
$ oc rsh <frontend_pod_id>
```

- コンテナ内から移行を実行します。

```
$ RAILS_ENV=production bundle exec rake db:migrate
```

**development** または **test** 環境で Rails アプリケーションを実行する場合には、**RAILS\_ENV** の環境変数を指定する必要はありません。

- デプロイメント前のライフサイクルフックをテンプレートに追する

### 11.4.3. アプリケーションのルートの作成

アプリケーションのルートを作成するためにサービスを公開できます。

## 手順

- **www.example.com** などの外部からアクセスできるホスト名を指定してサービスを公開するには、OpenShift Container Platform のルートを使用します。この場合は、以下を入力してフロントエンドサービスを公開する必要があります。

```
$ oc expose service rails-app --hostname=www.example.com
```



### 警告

指定するホスト名がルーターの IP アドレスに解決することを確認します。

## 第12章 イメージの使用

### 12.1. イメージの使用の概要

以下のトピックを使用して、OpenShift Container Platform ユーザーに提供されているさまざまな Source-to-Image (S2I)、データベース、その他のコンテナイメージを確認します。

Red Hat の公式コンテナイメージは、[registry.redhat.io](https://registry.redhat.io) の Red Hat レジストリーで提供されています。OpenShift Container Platform がサポートする S2I、データベース、Jenkins イメージは、Red Hat Quay レジストリーの **openshift4** リポジトリにあります。たとえば、**quay.io/openshift-release-dev/ocp-v4.0-<address>** は OpenShift Application Platform イメージの名前です。

xPaaS ミドルウェアイメージは、Red Hat レジストリーの適切な製品リポジトリで提供されていますが、接尾辞として **-openshift** が付いています。たとえば、**registry.redhat.io/jboss-eap-6/eap64-openshift** は JBoss EAP イメージの名前です。

このセクションで説明する Red Hat がサポートするイメージはすべて [Red Hat Ecosystem Catalog のコンテナイメージのセクション](#) に記載されています。各イメージのすべてのバージョンについて、そのコンテンツや用途の詳細を確認できます。関連するイメージを参照または検索してください。



#### 重要

コンテナイメージの新しいバージョンは、OpenShift Container Platform の以前のバージョンとは互換性がありません。お使いの OpenShift Container Platform のバージョンに基づいて、正しいバージョンのコンテナイメージを確認し、使用するようしてください。

### 12.2. SOURCE-TO-IMAGE (S2I)

[Red Hat Software Collections](#) イメージを、Node.js、Perl、Python などの特定のランタイム環境に依存するアプリケーションの基盤として使用することができます。Java を使用するランタイム環境のリファレンスとして、[Red Hat Java Source-to-Image for OpenShift](#) ドキュメントを使用できます。これらのランタイムベースイメージの特殊なバージョンは Source-to-image (S2I) イメージと呼ばれています。S2I イメージを使用して、コードを、そのコードを実行できるベースイメージ環境に挿入することができます。

S2I イメージには、以下が含まれます。

- .NET
- Java
- Go
- Node.js
- Perl
- PHP
- Python
- Ruby

S2I イメージは、以下の手順で OpenShift Container Platform コンソールから直接使用できます。

1. ログイン認証情報を使用して OpenShift Container Platform Web コンソールにログインします。OpenShift Container Platform Web コンソールのデフォルトビューは **Administrator** パースペクティブです。
2. パースペクティブスイッチャーを使用して、**Developer** パースペクティブに切り替えます。
3. **+Add** ビューで、**Project** ドロップダウンリストを使用して既存プロジェクトを選択するか、新規プロジェクトを作成します。
4. **Developer Catalog** タイルの **All services** をクリックします。
5. **Type** の下の **Builder Images** をクリックして、利用可能な S2I イメージを表示します。

S2I イメージは、[Cluster Samples Operator](#) を設定して利用可能にすることもできます。

### 12.2.1. Source-to-Image ビルドプロセスの概要

Source-to-Image (S2I) は、ソースコードをコンテナに挿入してソースコードを実行可能にすることで、実行可能な状態のイメージを生成します。S2I では、以下の手順を実行します。

1. **FROM <builder image>** コマンドを実行します。
2. ソースコードをビルダーイメージの定義された場所にコピーします。
3. ビルダーイメージから assemble スクリプトを実行します。
4. デフォルトコマンドとしてビルダーイメージに run スクリプトを設定します。

Buildah は次にコンテナイメージを作成します。

### 12.2.2. 関連情報

- [Cluster Samples Operator の設定](#)
- [ビルドストラテジーの使用](#)
- [Source-to-Image \(S2I\) プロセスのトラブルシューティング](#)
- [Source-to-Image によるソースコードからのイメージの作成](#)
- [Source-to-Image イメージのテストについて](#)
- [Source-to-Image によるソースコードからのイメージの作成](#)

## 12.3. SOURCE-TO-IMAGE イメージのカスタマイズ

Source-to-Image (S2I) ビルダーイメージには、assemble および run スクリプトが含まれますが、それらのスクリプトのデフォルト動作はすべてのユーザーに適している訳ではありません。デフォルトのスクリプトを含む S2I ビルダーの動作をカスタマイズできます。

### 12.3.1. イメージに埋め込まれたスクリプトの呼び出し

ビルダーイメージは、最も一般的なユースケースを含む、独自のバージョンの source-to-image (S2I) スクリプトを提供します。これらのスクリプトで各自のニーズが満たされない場合に向け、S2I には **.s2i/bin** ディレクトリーにカスタムスクリプトを追加して上書きできる手段があります。ただし、カスタムスクリプトを追加すると、標準のスクリプトを完全に置き換えてしまいます。スクリプトの置

き換えは許容できる場合もありますが、場合によっては、イメージに含まれるスクリプトのロジックを保持しつつ、スクリプトの前後にコマンドをいくつか実行できる場合があります。標準的なスクリプトを再利用するには、カスタムのロジックを実行し、イメージ内のデフォルトのスクリプトに追加の作業を委任するラッパースクリプトを作成できます。

## 手順

- ビルダーイメージ内のスクリプトの場所を判別するには、**io.openshift.s2i.scripts-url** ラベルの値を確認します。

```
$ podman inspect --format='{{ index .Config.Labels "io.openshift.s2i.scripts-url" }}'
wildfly/wildfly-centos7
```

## 出力例

```
image:///usr/libexec/s2i
```

**wildfly/wildfly-centos7** ビルダーイメージを検査し、スクリプトが **/usr/libexec/s2i** ディレクトリーにあることを確認できます。

- 他のコマンドでラップされた標準スクリプトのいずれかの呼び出しを含むスクリプトを作成します。

### **.s2i/bin/assemble** スクリプト

```
#!/bin/bash
echo "Before assembling"

/usr/libexec/s2i/assemble
rc=$?

if [ $rc -eq 0 ]; then
    echo "After successful assembling"
else
    echo "After failed assembling"
fi

exit $rc
```

以下の例では、メッセージを出力するカスタムの **assemble** スクリプトを表示し、イメージから標準の **assemble** スクリプトを実行して、**assemble** スクリプトの終了コードに応じて別のメッセージを出力します。



### 重要

**run** スクリプトをラップする場合には、スクリプトの呼び出しに **exec** を実行して、シグナルが正しく処理されるようにする必要があります。**exec** を使用すると、デフォルトのイメージ実行スクリプトを呼び出した後に追加でコマンドを実行できなくなります。

### **.s2i/bin/run** スクリプト

```
#!/bin/bash
echo "Before running application"
exec /usr/libexec/s2i/run
```