



Red Hat OpenShift Data Foundation 4.10

Amazon Web サービスを使用した OpenShift Data Foundation のデプロイ

クラウドストレージの Amazon Web Services を使用した OpenShift Data Foundation
のデプロイ手順

Red Hat OpenShift Data Foundation 4.10 Amazon Web サービスを使用した OpenShift Data Foundation のデプロイ

クラウドストレージの Amazon Web Services を使用した OpenShift Data Foundation のデプロイ手順

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Deploying_OpenShift_Data_Foundation_using_Amazon_Web_Services.ent file |.

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[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

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

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] 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[®] 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

Amazon Web Services で Red Hat OpenShift Container Platform を使用して Red Hat OpenShift Data Foundation をインストールする方法については、このドキュメントをご覧ください。

目次

多様性を受け入れるオープンソースの強化	3
RED HAT ドキュメントへのフィードバック (英語のみ)	4
はじめに	5
第1章 OPENSIFT DATA FOUNDATION のデプロイの準備	6
第2章 動的ストレージデバイスを使用した OPENSIFT DATA FOUNDATION のデプロイ	7
2.1. RED HAT OPENSIFT DATA FOUNDATION OPERATOR のインストール	7
2.2. トークン認証方法を使用した KMS を使用したクラスター全体の暗号化の有効化	8
2.3. KUBERNETES 認証方式を使用した KMS でのクラスター全体の暗号化の有効化	9
2.4. OPENSIFT DATA FOUNDATION クラスターの作成	12
2.5. OPENSIFT DATA FOUNDATION デプロイメントの確認	15
2.5.1. Pod の状態の確認	15
2.5.2. OpenShift Data Foundation クラスターの正常性の確認	17
2.5.3. Multicloud Object Gateway が正常であることの確認	17
2.5.4. OpenShift Data Foundation 固有のストレージクラスが存在することの確認	18
第3章 スタンドアロンの MULTICLOUD OBJECT GATEWAY のデプロイ	19
3.1. RED HAT OPENSIFT DATA FOUNDATION OPERATOR のインストール	19
3.2. スタンドアロンの MULTICLOUD OBJECT GATEWAY の作成	20
第4章 OPENSIFT DATA FOUNDATION のアンインストール	23
4.1. 内部モードでの OPENSIFT DATA FOUNDATION のアンインストール	23

多様性を受け入れるオープンソースの強化

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

RED HAT ドキュメントへのフィードバック (英語のみ)

弊社のドキュメントについてのご意見をお聞かせください。ドキュメントの改善点があれば、ぜひお知らせください。フィードバックをお寄せいただくには、以下をご確認ください。

- 特定の部分についての簡単なコメントをお寄せいただく場合は、以下をご確認ください。
 1. ドキュメントの表示が **Multi-page HTML** 形式になっていることを確認してください。ドキュメントの右上隅に **Feedback** ボタンがあることを確認してください。
 2. マウスカーソルを使用して、コメントを追加するテキストの部分を強調表示します。
 3. 強調表示されたテキストの下に表示される **Add Feedback** ポップアップをクリックします。
 4. 表示される指示に従ってください。
- より詳細なフィードバックをお寄せいただく場合は、Bugzilla のチケットを作成してください。
 1. [Bugzilla](#) の Web サイトに移動します。
 2. **Component** セクションで、**documentation** を選択します。
 3. **Description** フィールドに、ドキュメントの改善に向けたご提案を記入してください。ドキュメントの該当部分へのリンクも追加してください。
 4. **Submit Bug** をクリックします。

はじめに

Red Hat OpenShift Data Foundation は、接続環境または非接続環境での既存の Red Hat OpenShift Container Platform (RHOCP) AWS クラスターへのデプロイメントをサポートし、プロキシ環境に対する追加設定なしのサポートを提供します。



注記

AWS では、内部の OpenShift Data Foundation クラスターのみがサポートされます。デプロイメントの要件の詳細は、[デプロイメントのプランニング](#) および [OpenShift Data Foundation のデプロイの準備](#) を参照してください。

OpenShift Data Foundation をデプロイするには、[OpenShift Data Foundation のデプロイの準備](#) の章の要件を確認し、要件に基づいた環境のデプロイメントプロセスを実行します。

- [動的ストレージデバイスを使用したデプロイ](#)
- [スタンドアロンの Multicloud Object Gateway コンポーネントのデプロイ](#)

第1章 OPENSIFT DATA FOUNDATION のデプロイの準備

動的ストレージデバイスを使用して OpenShift Data Foundation を OpenShift Container Platform にデプロイすると、内部クラスターリソースを作成するオプションが提供されます。

OpenShift Data Foundation のデプロイを開始する前に、以下を実行します。

1. オプション:外部キー管理システム (KMS) を使用してクラスター全体の暗号化を有効にする場合は、次の手順に従います。
 - 有効な Red Hat OpenShift Data Foundation Advanced サブスクリプションがあることを確認してください。OpenShift Data Foundation のサブスクリプションがどのように機能するかを知るには、[OpenShift Data Foundation subscriptions に関するナレッジベースの記事](#)を参照してください。
 - 暗号化にトークン認証方法が選択されている場合は、[Enabling cluster-wide encryption with the Token authentication using KMS](#) を参照してください。
 - 暗号化に Kubernetes 認証方式が選択されている場合は、[KMS を使用した Kubernetes 認証によるクラスター全体の暗号化の有効化](#) を参照してください。
 - Vault サーバーで署名済みの証明書を使用していることを確認します。

2. ノードの最小要件

OpenShift Data Foundation クラスターは、標準のデプロイメントリソース要件を満たしていない場合に、最小の設定でデプロイされます。[プランニングガイド](#)の [Resource requirements](#) のセクションを参照してください。

3. Regional-DR 要件 [開発者プレビュー]

Red Hat OpenShift Data Foundation でサポートされる障害復旧機能では、障害復旧ソリューションを正常に実装するために以下の前提条件がすべて必要になります。

- 有効な Red Hat OpenShift Data Foundation Advanced サブスクリプション
- 有効な Red Hat Advanced Cluster Management for Kubernetes サブスクリプション
OpenShift Data Foundation のサブスクリプションがどのように機能するかを知るには、[OpenShift Data Foundation subscriptions に関するナレッジベースの記事](#) を参照してください。

詳細な要件は、[Regional-DR requirements](#) および [RHACM requirements](#) を参照してください。

第2章 動的ストレージデバイスを使用した OPENSIFT DATA FOUNDATION のデプロイ

Amazon Web Services (AWS) EBS(タイプ **gp2** または **gp3**) が提供する動的ストレージデバイスを使用して OpenShift Data Foundation を OpenShift Container Platform にデプロイすると、内部クラスターリソースを作成するオプションが提供されます。これにより、ベースサービスの内部プロビジョニングが可能になり、追加のストレージクラスをアプリケーションで使用可能にすることができます。

また、OpenShift Data Foundation で Multicloud Object Gateway (MCG) コンポーネントのみをデプロイすることもできます。詳細は、[Deploy standalone Multicloud Object Gateway](#) を参照してください。



注記

AWS では、内部の OpenShift Data Foundation クラスターのみがサポートされます。デプロイメント要件の詳細は、[Planning your deployment](#) を参照してください。

また、[OpenShift Data Foundation のデプロイの準備](#) の章にある要件に対応していることを確認してから、動的ストレージデバイスを使用したデプロイについて以下の手順を実行してください。

1. [Red Hat OpenShift Data Foundation Operator のインストール](#)
2. [OpenShift Data Foundation クラスターの作成](#)

2.1. RED HAT OPENSIFT DATA FOUNDATION OPERATOR のインストール

Red Hat OpenShift Data Foundation Operator は、Red Hat OpenShift Container Platform Operator Hub を使用してインストールできます。

前提条件

- **cluster-admin** および Operator インストールのパーミッションを持つアカウントを使用して OpenShift Container Platform クラスターにアクセスできる。
- Red Hat OpenShift Container Platform クラスターにワーカーノードが少なくとも 3 つある。
- その他のリソース要件については、[デプロイメントのプランニング](#) ガイドを参照してください。



重要

- OpenShift Data Foundation のクラスター全体でのデフォルトノードセレクターを上書きする必要がある場合は、コマンドラインインターフェイスで以下のコマンドを使用し、**openshift-storage** namespace の空のノードセレクターを指定できます (この場合、openshift-storage namespace を作成します)。

```
$ oc annotate namespace openshift-storage openshift.io/node-selector=
```

- ノードに Red Hat OpenShift Data Foundation リソースのみがスケジュールされるように **infra** のテイントを設定します。これにより、サブスクリプションコストを節約できます。詳細は、[ストレージリソースの管理および割り当てガイド](#) の [How to use dedicated worker nodes for Red Hat OpenShift Data Foundation](#) の章を参照してください。

手順

1. OpenShift Web コンソールにログインします。
2. **Operators** → **OperatorHub** をクリックします。
3. スクロールするか、または **OpenShift Data Foundation** を **Filter by keyword** ボックスに入力し、**OpenShift Data Foundation Operator** を検索します。
4. **Install** をクリックします。
5. **Install Operator** ページで、以下のオプションを設定します。
 - a. Channel を **stable-4.10** として更新します。
 - b. Installation Mode オプションに **A specific namespace on the cluster** を選択します。
 - c. Installed Namespace に **Operator recommended namespace openshift-storage** を選択します。namespace **openshift-storage** が存在しない場合、これは Operator のインストール時に作成されます。
 - d. 承認ストラテジー を **Automatic** または **Manual** として選択します。

Automatic (自動) 更新を選択した場合、Operator Lifecycle Manager (OLM) は介入なしに、Operator の実行中のインスタンスを自動的にアップグレードします。

Manual 更新を選択した場合、OLM は更新要求を作成します。クラスター管理者は、Operator を新しいバージョンに更新できるように更新要求を手動で承認する必要があります。
 - e. **Console プラグイン** に **Enable** オプションが選択されていることを確認します。
 - f. **Install** をクリックします。

検証手順

- **OpenShift Data Foundation Operator** に、インストールが正常に実行されたことを示す緑色のチェックマークが表示されていることを確認します。
- Operator が正常にインストールされると、**Web console update is available** メッセージを含むポップアップがユーザーインターフェイスに表示されます。このポップアップから **Web コンソールのリフレッシュ** をクリックして、反映するコンソールを変更します。
 - Web コンソールで、**Operators** に移動し、**OpenShift Data Foundation** が利用可能かどうかを確認します。

2.2. トークン認証方法を使用した KMS を使用したクラスター全体の暗号化の有効化

Valut でトークン認証のキー値バックエンドパスとポリシーを有効にするには、次の手順に従います。

前提条件

- Vault への管理者アクセス。

- 有効な Red Hat OpenShift Data Foundation Advanced サブスクリプション詳細については、[OpenShift Data Foundation サブスクリプションに関するナレッジベースの記事](#) を参照してください。
- 注: 後に変更することはできないため、命名規則に基づいてバックエンド **path** として一意のパス名を選択します。

手順

1. Vault で Key/Value (KV) バックエンドパスを有効にします。
Vault KV シークレットエンジン API の場合は、バージョン 1 を使用します。

```
$ vault secrets enable -path=odf kv
```

Vault KV シークレットエンジン API の場合は、バージョン 2 です。

```
$ vault secrets enable -path=odf kv-v2
```

2. 以下のコマンドを使用して、シークレットでの書き込み操作または削除操作の実行をユーザーを制限するポリシーを作成します。

```
echo '
path "odf/*" {
  capabilities = ["create", "read", "update", "delete", "list"]
}
path "sys/mounts" {
  capabilities = ["read"]
}' | vault policy write odf -
```

3. 上記のポリシーに一致するトークンを作成します。

```
$ vault token create -policy=odf -format json
```

2.3. KUBERNETES 認証方式を使用した KMS でのクラスター全体の暗号化の有効化

キー管理システム (KMS) を使用して、クラスター全体の暗号化に対して Kubernetes 認証方式を有効にできます。

前提条件

- Vault への管理者アクセス。
- 有効な Red Hat OpenShift Data Foundation Advanced サブスクリプション詳細については、[OpenShift Data Foundation サブスクリプションに関するナレッジベースの記事](#) を参照してください。
- OpenShift Data Foundation Operator は Operator Hub からインストールする必要があります。
- 後に変更することはできないため、命名規則に基づいてバックエンド **path** として一意のパス名を選択します。



注記

Vault namespace の使用は、OpenShift Data Foundation 4.10 の Kubernetes 認証方式ではサポートされていません

手順

1. サービスアカウントを作成します。

```
$ oc -n openshift-storage create serviceaccount <serviceaccount_name>
```

ここで、**<serviceaccount_name>** はサービスアカウントの名前を指定します。

以下に例を示します。

```
$ oc -n openshift-storage create serviceaccount odf-vault-auth
```

2. **clusterrolebindings** と **clusterroles** を作成します。

```
$ oc -n openshift-storage create clusterrolebinding vault-tokenreview-binding --
clusterrole=system:auth-delegator --serviceaccount=openshift-
storage:<serviceaccount_name>
```

以下に例を示します。

```
$ oc -n openshift-storage create clusterrolebinding vault-tokenreview-binding --
clusterrole=system:auth-delegator --serviceaccount=openshift-storage:odf-vault-auth
```

3. OpenShift Container Platform のバージョンに応じて、以下のいずれかを実行します。

- OpenShift Container Platform 4.10 の場合:
 - 上記で作成された serviceaccount (SA) に関連付けられたシークレット名を特定します。

```
$ VAULT_SA_SECRET_NAME=$(oc -n openshift-storage get sa <SA_NAME> -o
jsonpath="{.secrets[*]['name']}") | grep -o "[^[:space:]]*-token-[^[:space:]]*"
```

以下に例を示します。

```
$ VAULT_SA_SECRET_NAME=$(oc -n openshift-storage get sa odf-vault-auth -o
jsonpath="{.secrets[*]['name']}") | grep -o "[^[:space:]]*-token-[^[:space:]]*"
```

- OpenShift Container Platform 4.11 の場合:
 - **serviceaccount** トークンおよび CA 証明書のシークレットを作成します。

```
$ cat <<EOF | oc create -f -
apiVersion: v1
kind: Secret
metadata:
  name: odf-vault-auth-token
  namespace: openshift-storage
annotations:
```

```
kubernetes.io/service-account.name: <serviceaccount_name>
type: kubernetes.io/service-account-token
data: {}
EOF
```

ここで、<serviceaccount_name> は、前の手順で作成したサービスアカウントです。

```
$ VAULT_SA_SECRET_NAME=odf-vault-auth-token
```

- シークレットからトークンと CA 証明書を取得します。

```
$ SA_JWT_TOKEN=$(oc -n openshift-storage get secret "$VAULT_SA_SECRET_NAME" -o
jsonpath="{.data.token}" | base64 --decode; echo)
$ SA_CA_CERT=$(oc -n openshift-storage get secret "$VAULT_SA_SECRET_NAME" -o
jsonpath="{.data['ca.crt']}" | base64 --decode; echo)
```

- OCF クラスターエンドポイントを取得します。

```
$ OCP_HOST=$(oc config view --minify --flatten -o jsonpath="{.clusters[0].cluster.server}")
```

- サービスアカウントの発行者を取得します。

```
$ oc proxy &
$ proxy_pid=$!
$ issuer="$( curl --silent http://127.0.0.1:8001/.well-known/openid-configuration | jq -r
.issuer)"
$ kill $proxy_pid
```

- 上記の手順で収集した情報を使用して、以下に示すように Vault で Kubernetes 認証方法を設定します。

```
$ vault auth enable kubernetes
$ vault write auth/kubernetes/config \
  token_reviewer_jwt="$SA_JWT_TOKEN" \
  kubernetes_host="$OCP_HOST" \
  kubernetes_ca_cert="$SA_CA_CERT" \
  issuer="$issuer"
```

重要

発行者が空の場合に Vault で Kubernetes 認証方法を設定するには、以下を行います。

```
$ vault write auth/kubernetes/config \
  token_reviewer_jwt="$SA_JWT_TOKEN" \
  kubernetes_host="$OCP_HOST" \
  kubernetes_ca_cert="$SA_CA_CERT"
```

- Vault で Key/Value (KV) バックエンドパスを有効にします。
Vault KV シークレットエンジン API の場合は、バージョン 1 です。

```
$ vault secrets enable -path=odf kv
```

Vault KV シークレットエンジン API の場合は、バージョン 2 です。

```
$ vault secrets enable -path=odf kv-v2
```

- シークレットに対して書き込み操作または削除操作を実行するようにユーザーを制限するポリシーを作成します。

```
echo '
path "odf/*" {
  capabilities = ["create", "read", "update", "delete", "list"]
}
path "sys/mounts" {
  capabilities = ["read"]
}' | vault policy write odf -
```

- ロールを作成します。

```
$ vault write auth/kubernetes/role/odf-rook-ceph-op \
  bound_service_account_names=rook-ceph-system,rook-ceph-osd,noobaa \
  bound_service_account_namespaces=openshift-storage \
  policies=odf \
  ttl=1440h
```

ロール **odf-rook-ceph-op** は、後でストレージシステムの作成中に KMS 接続の詳細を設定するときに使用されます。

```
$ vault write auth/kubernetes/role/odf-rook-ceph-osd \
  bound_service_account_names=rook-ceph-osd \
  bound_service_account_namespaces=openshift-storage \
  policies=odf \
  ttl=1440h
```

2.4. OPENSIFT DATA FOUNDATION クラスターの作成

OpenShift Data Foundation Operator のインストール後に OpenShift Data Foundation クラスターを作成します。

前提条件

- OpenShift Data Foundation Operator は Operator Hub からインストールする必要があります。詳細は、[Installing OpenShift Data Foundation Operator](#) を参照してください。

手順

- OpenShift Web コンソールで、**Operators → Installed Operators** をクリックし、インストールされた Operator を表示します。
選択された **Project** が **openshift-storage** であることを確認します。
- OpenShift Data Foundation Operator** をクリックした後、**Create StorageSystem** をクリックします。
- Backing storage** ページで、以下を選択します。

- a. **Deployment type** オプションで **Full Deployment** を選択します。
 - b. **Use an existing StorageClass** オプションを選択します。
 - c. **Storage Class** を選択します。
OpenShift Data Foundation バージョン 4.10 以降、ストレージクラスとして **gp3** を選択できません。デフォルトでは **gp2** に設定されます。
 - d. **Next** をクリックします。
4. **Capacity and nodes** ページで、必要な情報を提供します。
- a. ドロップダウンリストから **Requested Capacity** の値を選択します。デフォルトで、これは **2 TiB** に設定されます。



注記

初期ストレージ容量を選択すると、クラスターの拡張は、選択された使用可能な容量を使用してのみ実行されます (raw ストレージの 3 倍)。

- b. **Select Nodes** セクションで、少なくとも 3 つの利用可能なノードを選択します。
 - c. オプション: 選択したノードを OpenShift Data Foundation 専用にする場合は、**Taint nodes** チェックボックスを選択します。
複数のアベイラビリティゾーンを持つクラウドプラットフォームの場合は、ノードが異なる場所/アベイラビリティゾーンに分散されていることを確認します。

選択したノードが集約された 30 CPU および 72 GiB の RAM の OpenShift Data Foundation クラスターの要件と一致しない場合は、最小クラスターがデプロイされます。ノードの最小要件については、[プランニングガイドのリソース要件](#) セクションを参照してください。
 - d. **Next** をクリックします。
5. オプション: **Security and network** ページで、要件に応じて以下を設定します。
- a. 暗号化を有効にするには、**Enable data encryption for block and file storage** を選択します。
 - b. 暗号化レベルのいずれかまたは両方を選択します。
 - **クラスター全体の暗号化**
クラスター全体を暗号化します (ブロックおよびファイル)。
 - **StorageClass の暗号化**
暗号化対応のストレージクラスを使用して、暗号化された永続ボリューム (ブロックのみ) を作成します。
 - c. **Connect to an external key management service** チェックボックスを選択します。これはクラスター全体の暗号化の場合はオプションになります。
 - i. **Key Management Service Provider** はデフォルトで **Vault** に設定されます。
 - ii. **認証方法** を選択します。

トークン認証方式の使用

- Vault ('https://<hostname or ip>') サーバーの一意的 **Connection Name**、**host Address**、**Port** 番号および **Token** を入力します。
- **Advanced Settings** を展開して、**Vault** 設定に基づいて追加の設定および証明書の詳細を入力します。
 - OpenShift Data Foundation 専用かつ特有のキー値のシークレットパスを **Backend Path** に入力します。
 - オプション: **TLS Server Name** および **Vault Enterprise Namespace** を入力します。
 - それぞれの PEM でエンコードされた証明書ファイルをアップロードし、**CA 証明書**、**クライアント証明書**、および **クライアントの秘密鍵** を提供します。
 - **Save** をクリックします。

Kubernetes 認証方式の使用

- Vault ('https://<hostname or ip>') サーバーの一意的 **Connection Name**、**host Address**、**Port** 番号および **Role** 名を入力します。
- **Advanced Settings** を展開して、**Vault** 設定に基づいて追加の設定および証明書の詳細を入力します。
 - OpenShift Data Foundation 専用かつ特有のキー値のシークレットパスを **Backend Path** に入力します。
 - オプション: 該当する場合は、**TLS サーバー名** および **認証パス** を入力します。
 - それぞれの PEM でエンコードされた証明書ファイルをアップロードし、**CA 証明書**、**クライアント証明書**、および **クライアントの秘密鍵** を提供します。
 - **Save** をクリックします。

d. **Next** をクリックします。

6. **Review and create** ページで、設定の詳細を確認します。
設定を変更するには、**Back** をクリックします。

7. **Create StorageSystem** をクリックします。

検証手順

- インストールされたストレージクラスターの最終ステータスを確認するには、以下を実行します。
 - a. OpenShift Web コンソールで、**Installed Operators** → **OpenShift Data Foundation** → **Storage System** → **ocs-storagecluster-storagesystem** → **Resources** の順に移動します。
 - b. **StorageCluster** の **Status** が **Ready** になっており、その横に緑色のチェックマークが表示されていることを確認します。

- OpenShift Data Foundation のすべてのコンポーネントが正常にインストールされていることを確認するには、[Verifying your OpenShift Data Foundation deployment](#) を参照してください。

関連情報

Overprovision Control アラートを有効にするには、モニタリングガイドの [アラート](#) を参照してください。

2.5. OPENSIFT DATA FOUNDATION デプロイメントの確認

OpenShift Data Foundation が正常にデプロイされていることを確認するには、以下を実行します。

1. [Pod の状態を確認](#)
2. [OpenShift Data Foundation クラスターが正常であることを確認](#)
3. [Multicloud Object Gateway が正常であることを確認](#) します。
4. [OpenShift Data Foundation 固有のストレージクラスが存在することを確認](#)

2.5.1. Pod の状態の確認

手順

1. OpenShift Web コンソールから **Workloads** → **Pods** をクリックします。
2. **Project** ドロップダウンリストから **openshift-storage** を選択します。



注記

Show default projects オプションが無効になっている場合は、切り替えボタンを使用して、すべてのデフォルトプロジェクトを一覧表示します。

各コンポーネントについて予想される Pod 数や、これがノード数によってどのように異なるかについての詳細は、[表2.1「OpenShift Data Foundation クラスターに対応する Pod」](#) を参照してください。

3. **Running** タブおよび **Completed** タブをクリックして、以下の Pod が **Running** 状態および **Completed** 状態にあることを確認します。

表2.1 OpenShift Data Foundation クラスターに対応する Pod

コンポーネント	対応する Pod
---------	----------

コンポーネント	対応する Pod
OpenShift Data Foundation Operator	<ul style="list-style-type: none"> ● ocs-operator-* (任意のワーカーノードに 1 Pod) ● ocs-metrics-exporter-* (任意のワーカーノードに 1 Pod) ● odf-operator-controller-manager-* (任意のワーカーノードに 1 Pod) ● odf-console-* (任意のワーカーノードに 1 Pod) ● csi-addons-controller-manager-* (任意のワーカーノードに 1つの Pod)
Rook-ceph Operator	<p>rook-ceph-operator-*</p> <p>(任意のワーカーノードに 1 Pod)</p>
Multicloud Object Gateway	<ul style="list-style-type: none"> ● noobaa-operator-* (任意のワーカーノードに 1 Pod) ● noobaa-core-* (任意のストレージノードに 1 Pod) ● noobaa-db-pg-* (任意のストレージノードに 1 Pod) ● noobaa-endpoint-* (任意のストレージノードに 1 Pod)
MON	<p>rook-ceph-mon-*</p> <p>(ストレージノードに分散する 3 Pod)</p>
MGR	<p>rook-ceph-mgr-*</p> <p>(任意のストレージノードに 1 Pod)</p>
MDS	<p>rook-ceph-mds-ocs-storagecluster-cephfilesystem-*</p> <p>(ストレージノードに分散する 2 Pod)</p>

コンポーネント	対応する Pod
CSI	<ul style="list-style-type: none"> ● cephfs <ul style="list-style-type: none"> ○ csi-cephfsplugin-* (各ワーカーノードに1Pod) ○ csi-cephfsplugin-provisioner-* (ワーカーノードに分散する2Pod) ● rbd <ul style="list-style-type: none"> ○ csi-rbdplugin-* (各ワーカーノードに1Pod) ○ csi-rbdplugin-provisioner-* (ストレージノードに分散する2Pod)
rook-ceph-crashcollector	rook-ceph-crashcollector-* (各ストレージノードに1Pod)
OSD	<ul style="list-style-type: none"> ● rook-ceph-osd-* (各デバイス用に1Pod) ● rook-ceph-osd-prepare-ocs-device-* (各デバイス用に1Pod)

2.5.2. OpenShift Data Foundation クラスターの正常性の確認

手順

1. OpenShift Web コンソールで、**Storage → Data Foundation** をクリックします。
2. **Overview** タブの **Status** カードで **Storage System** をクリックし、表示されたポップアップからストレージシステムリンクをクリックします。
3. **Block and File** タブの **Status** カードで、**Storage Cluster** に緑色のチェックマークが表示されていることを確認します。
4. **Details** カードで、クラスター情報が表示されていることを確認します。

ブロックおよびファイルダッシュボードを使用した OpenShift Data Foundation クラスターの正常性については、[Monitoring OpenShift Data Foundation](#) を参照してください。

2.5.3. Multicloud Object Gateway が正常であることの確認

手順

1. OpenShift Web コンソールで、**Storage → Data Foundation** をクリックします。
2. **Overview** タブの **Status** カードで **Storage System** をクリックし、表示されたポップアップからストレージシステムリンクをクリックします。
3. **Object** タブの **Status** カードで、**Object Service** と **Data Resiliency** の両方に緑色の

- a. Object ツールの Status カードで、Object Service と Data Resiliency の両方に緑色のチェックマークが表示されていることを確認します。
- b. Details カードで、MCG 情報が表示されることを確認します。

ブロックおよびファイルダッシュボードを使用した OpenShift Data Foundation クラスターの正常性については、[OpenShift Data Foundation の監視](#) を参照してください。

2.5.4. OpenShift Data Foundation 固有のストレージクラスが存在することの確認

手順

1. OpenShift Web コンソールの左側のペインから **Storage** → **Storage Classes** をクリックします。
2. 以下のストレージクラスが OpenShift Data Foundation クラスターの作成時に作成されることを確認します。
 - **ocs-storagecluster-ceph-rbd**
 - **ocs-storagecluster-cephfs**
 - **openshift-storage.noobaa.io**

第3章 スタンドアロンの MULTICLOUD OBJECT GATEWAY のデプロイ

OpenShift Data Foundation で Multicloud Object Gateway コンポーネントのみをデプロイすると、デプロイメントで柔軟性が高まり、リソース消費を減らすことができます。このセクションでは、以下のステップで、スタンドアロンの Multicloud Object Gateway コンポーネントのみをデプロイします。

- Red Hat OpenShift Data Foundation Operator のインストール
- スタンドアロンの Multicloud Object Gateway の作成

3.1. RED HAT OPENSIFT DATA FOUNDATION OPERATOR のインストール

Red Hat OpenShift Data Foundation Operator は、Red Hat OpenShift Container Platform Operator Hub を使用してインストールできます。

前提条件

- **cluster-admin** および Operator インストールのパーミッションを持つアカウントを使用して OpenShift Container Platform クラスターにアクセスできる。
- Red Hat OpenShift Container Platform クラスターにワーカーノードが少なくとも3つある。
- その他のリソース要件については、[デプロイメントのプランニング](#) ガイドを参照してください。

重要

- OpenShift Data Foundation のクラスター全体でのデフォルトノードセクターを上書きする必要がある場合は、コマンドラインインターフェイスで以下のコマンドを使用し、**openshift-storage** namespace の空のノードセクターを指定できます (この場合、openshift-storage namespace を作成します)。

```
$ oc annotate namespace openshift-storage openshift.io/node-selector=
```

- ノードに Red Hat OpenShift Data Foundation リソースのみがスケジュールされるように **infra** のテイントを設定します。これにより、サブスクリプションコストを節約できます。詳細は、[ストレージリソースの管理および割り当てガイド](#) の [How to use dedicated worker nodes for Red Hat OpenShift Data Foundation](#) の章を参照してください。

手順

1. OpenShift Web コンソールにログインします。
2. **Operators** → **OperatorHub** をクリックします。
3. スクロールするか、または **OpenShift Data Foundation** を **Filter by keyword** ボックスに入力し、**OpenShift Data Foundation Operator** を検索します。
4. **Install** をクリックします。
5. **Install Operator** ページで、以下のオプションを設定します。

- a. Channel を **stable-4.10** として更新します。
- b. Installation Mode オプションに **A specific namespace on the cluster** を選択します。
- c. Installed Namespace に **Operator recommended namespace openshift-storage** を選択します。namespace **openshift-storage** が存在しない場合、これは Operator のインストール時に作成されます。
- d. 承認ストラテジー を **Automatic** または **Manual** として選択します。
Automatic (自動) 更新を選択した場合、Operator Lifecycle Manager (OLM) は介入なしに、Operator の実行中のインスタンスを自動的にアップグレードします。
Manual 更新を選択した場合、OLM は更新要求を作成します。クラスター管理者は、Operator を新しいバージョンに更新できるように更新要求を手動で承認する必要があります。
- e. **Console プラグイン** に **Enable** オプションが選択されていることを確認します。
- f. **Install** をクリックします。

検証手順

- **OpenShift Data Foundation Operator** に、インストールが正常に実行されたことを示す緑色のチェックマークが表示されていることを確認します。
- Operator が正常にインストールされると、**Web console update is available** メッセージを含むポップアップがユーザーインターフェイスに表示されます。このポップアップから **Web コンソールのリフレッシュ** をクリックして、反映するコンソールを変更します。
 - Web コンソールで、**Operators** に移動し、**OpenShift Data Foundation** が利用可能かどうかを確認します。

3.2. スタンドアロンの MULTICLOUD OBJECT GATEWAY の作成

OpenShift Data Foundation のデプロイ中には、スタンドアロンの Multicloud Object Gateway コンポーネントのみを作成できます。

前提条件

- OpenShift Data Foundation Operator がインストールされていることを確認します。

手順

1. OpenShift Web コンソールで、**Operators** → **Installed Operators** をクリックし、インストールされた Operator を表示します。
 選択された **Project** が **openshift-storage** であることを確認します。
2. **OpenShift Data Foundation Operator** をクリックした後、**Create StorageSystem** をクリックします。
3. **Backing storage** ページで、以下を選択します。
 - a. **Deployment type** の **Multicloud Object Gateway** を選択します。
 - b. **Use an existing StorageClass** オプションを選択します。

- c. **Next** をクリックします。
4. オプション:Security ページで、**Connect to an external key management service**を選択します。
 - a. **Key Management Service Provider**はデフォルトで **Vault** に設定されます。
 - b. Vault **Service Name**、Vault サーバーのホスト Address('https://<hostname or ip>')、**Port number** および **Token** を入力します。
 - c. **Advanced Settings** を展開して、**Vault** 設定に基づいて追加の設定および証明書の詳細を入力します。
 - i. OpenShift Data Foundation 専用で固有のキーバリュースークレットパスを **Backend Path**に入力します。
 - ii. オプション:TLS Server Name および **Vault Enterprise Namespace**を入力します。
 - iii. それぞれの PEM でエンコードされた証明書ファイルをアップロードし、**CA 証明書**、**クライアント証明書**、および **クライアントの秘密鍵**を提供します。
 - iv. **Save** をクリックします。
 - d. **Next** をクリックします。
5. **Review and create** ページで、設定の詳細を確認します。
設定を変更するには、**Back** をクリックします。
6. **Create StorageSystem** をクリックします。

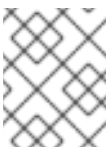
検証手順

OpenShift Data Foundation クラスタが正常であることの確認

1. OpenShift Web コンソールで、**Storage** → **Data Foundation** をクリックします。
2. **Overview** タブの **Status** カードで **Storage System** をクリックし、表示されたポップアップからストレージシステムリンクをクリックします。
 - a. **Object** タブの **Status** カードで、**Object Service** と **Data Resiliency** の両方に緑色のチェックマークが表示されていることを確認します。
 - b. **Details** カードで、MCG 情報が表示されることを確認します。

Pod の状態の確認

1. OpenShift Web コンソールから **Workloads** → **Pods** をクリックします。
2. **Project** ドロップダウンリストから **openshift-storage** を選択し、以下の Pod が **Running** 状態にあることを確認します。



注記

Show default projects オプションが無効になっている場合は、切り替えボタンを使用して、すべてのデフォルトプロジェクトを一覧表示します。

コンポーネント	対応する Pod
OpenShift Data Foundation Operator	<ul style="list-style-type: none">● ocs-operator-* (任意のワーカーノードに 1 Pod)● ocs-metrics-exporter-*(任意のワーカーノードに 1 Pod)● odf-operator-controller-manager-*(任意のワーカーノードに 1 Pod)● odf-console-*(任意のワーカーノードに 1 Pod)● csi-addons-controller-manager-* (任意のワーカーノードに 1つの Pod)
Rook-ceph Operator	rook-ceph-operator-* (任意のワーカーノードに 1 Pod)
Multicloud Object Gateway	<ul style="list-style-type: none">● noobaa-operator-* (任意のワーカーノードに 1 Pod)● noobaa-core-* (任意のワーカーノードに 1 Pod)● noobaa-db-pg-* (任意のワーカーノードに 1 Pod)● noobaa-endpoint-* (任意のワーカーノードに 1 Pod)

第4章 OPENSIFT DATA FOUNDATION のアンインストール

4.1. 内部モードでの OPENSIFT DATA FOUNDATION のアンインストール

OpenShift Data Foundation を Internal モードでアンインストールするには、[knowledge base article on Uninstalling OpenShift Data Foundation](#) を参照してください。