



# Red Hat OpenShift Data Foundation 4.12

## Red Hat Virtualization プラットフォームを使用した OpenShift Data Foundation のデプロイ

Red Hat Virtualization Platform 上で OpenShift Data Foundation をデプロイする手順



# Red Hat OpenShift Data Foundation 4.12 Red Hat Virtualization プラットフォームを使用した OpenShift Data Foundation のデプロイ

---

Red Hat Virtualization Platform 上で OpenShift Data Foundation をデプロイする手順

## 法律上の通知

Copyright © 2023 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

Red Hat Virtualization プラットフォームで 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 RED HAT VIRTUALIZATION プラットフォームを使用した OPENSIFT DATA FOUNDATION のデプロイの準備 .....	6
1.1. ローカルストレージデバイスを使用して OPENSIFT DATA FOUNDATION をインストールするための要件	7
第2章 動的ストレージデバイスを使用したデプロイ .....	9
2.1. RED HAT OPENSIFT DATA FOUNDATION OPERATOR のインストール	9
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	10
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	11
2.4. OPENSIFT DATA FOUNDATION クラスターの作成	13
第3章 ローカルストレージデバイスを使用したデプロイ .....	17
3.1. ローカルストレージ OPERATOR のインストール	17
3.2. RED HAT OPENSIFT DATA FOUNDATION OPERATOR のインストール	17
3.3. RED HAT VIRTUALIZATION プラットフォームでの OPENSIFT DATA FOUNDATION クラスターの作成	19
第4章 OPENSIFT DATA FOUNDATION デプロイメントの確認 .....	24
4.1. POD の状態の確認	24
4.2. OPENSIFT DATA FOUNDATION クラスターの正常性の確認	26
4.3. MULTICLOUD OBJECT GATEWAY が正常であることの確認	26
4.4. 特定のストレージクラスが存在することの確認	26
第5章 スタンドアロンの MULTICLOUD OBJECT GATEWAY のデプロイ .....	28
5.1. 動的ストレージデバイスを使用したスタンドアロン MULTICLOUD OBJECT GATEWAY のデプロイ	28
5.2. ローカルストレージデバイスを使用したスタンドアロン MULTICLOUD OBJECT GATEWAY のデプロイ	32
第6章 OPENSIFT DATA FOUNDATION のアンインストール .....	39
6.1. 内部モードでの OPENSIFT DATA FOUNDATION のアンインストール	39



## 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、[Red Hat CTO である Chris Wright のメッセージ](#) をご覧ください。

## RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに対する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 では、既存の Red Hat OpenShift Container Platform (RHOCP) Red Hat Virtualization プラットフォームクラスターでのデプロイメントをサポートします。

Red Hat Virtualization の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 (IPI) によって提供される共有ストレージデバイスを使用して OpenShift Container Storage を OpenShift Data Foundation にデプロイすると、内部クラスターリソースを作成できます。

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。



### 注記

Red Hat Virtualization 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。

要件に基づいて、デプロイメントの以下の方法のいずれかを実行します。

- 動的ストレージデバイスを使用する OpenShift Data Foundation を完全デプロイするために [動的ストレージデバイスを使用してデプロイします](#)。
- ローカルストレージデバイスを使用する OpenShift Data Foundation を完全デプロイするために [ローカルストレージデバイスを使用してデプロイします](#)。
- OpenShift Data Foundation で Multicloud Object Gateway コンポーネントのみをデプロイするために、[スタンドアロンの Multicloud Object Gateway コンポーネントをデプロイします](#)。

## 第1章 RED HAT VIRTUALIZATION プラットフォームを使用した OPENSIFT DATA FOUNDATION のデプロイの準備

動的またはローカルストレージを使用して Red Hat OpenShift Data Foundation のデプロイメントを開始する前に、リソース要件を満たしていることを確認してください。 [デプロイメントのプランニング](#) を参照してください。

1. オプション: 外部の鍵管理システム (KMS) HashiCorp Vault 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の仕組みを確認するには、 [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. オプション: 外部の鍵管理システム (KMS) Thales CipherTrust Manager 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、まず Key Management Interoperability Protocol (KMIP) を有効にして、サーバーで署名付き証明書を使用する必要があります。以下の手順に従ってください。
  - a. KMIP クライアントが存在しない場合は作成します。ユーザーインターフェイスから、 **KMIP → Client Profile → Add Profile** を選択します。
    - i. プロファイルの作成中に、 **CipherTrust** のユーザー名を **Common Name** フィールドに追加します。
  - b. **KMIP → Registration Token → New Registration Token** に移動してトークンを作成します。次のステップのためにトークンをコピーしておきます。
  - c. クライアントを登録するために、 **KMIP → Registered Clients → Add Client** に移動します。 **Name** を指定します。前のステップの **Registration Token** を貼り付けて、 **Save** をクリックします。
  - d. **Save Private Key** と **Save Certificate** をクリックして、それぞれ秘密鍵とクライアント証明書をダウンロードします。
  - e. 新しい KMIP インターフェイスを作成するために、 **Admin Settings → Interfaces → Add Interface** に移動します。
    - i. **KMIP Key Management Interoperability Protocol** を選択し、 **Next** をクリックします。
    - ii. 空いている **Port** を選択します。
    - iii. **Network Interface** として **all** を選択します。
    - iv. **Interface Mode** として **TLS, verify client cert, user name taken from client cert, auth request is optional** を選択します。

- v. (オプション) 物理削除を有効にして、鍵が削除されたときにメタデータとマテリアルの両方を削除することができます。これはデフォルトでは無効になります。
  - vi. 使用する CA を選択し、**Save** をクリックします。
- f. サーバー CA 証明書を取得するために、新しく作成されたインターフェイスの右側にあるアクションメニュー (⋮) をクリックし、**Download Certificate** をクリックします。
- g. オプション: デプロイ時に StorageClass 暗号化を有効にする場合は、キー暗号化キー (KEK) として機能するキーを作成します。
- i. **Keys** → **Add Key** に移動します。
  - ii. **Key Name** を入力します。
  - iii. **Algorithm** と **Size** をそれぞれ **AES** と **256** に設定します。
  - iv. **Create a key in Pre-Active state** を有効にして、アクティベーションの日時を設定します。
  - v. **Key Usage** で **Encrypt** と **Decrypt** が有効になっていることを確認します。
  - vi. 新しく作成した鍵の ID をコピーして、デプロイメント中に一意の識別子として使用します。
3. ノードの最小要件
- OpenShift Data Foundation クラスタは、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 [リソース要件](#) セクションを参照してください。
4. 障害復旧の要件 テクノロジープレビュー
- 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をすべて満たす必要があります。
- 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の仕組みを確認するには、[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。
- 詳細な要件については、[OpenShift ワークロード用の OpenShift Data Foundation Disaster Recovery の設定](#) ガイド、および Red Hat Advanced Cluster Management for Kubernetes ドキュメントの [インストールガイド](#) の [要件と推奨事項](#) のセクションを参照してください。
5. [ローカルストレージデバイスを使用して OpenShift Data Foundation をインストールするための要件](#) を満たしていることを確認します。

## 1.1. ローカルストレージデバイスを使用して OPENSIFT DATA FOUNDATION をインストールするための要件

### ノードの要件

クラスタは少なくとも 3 つの OpenShift Container Platform ワーカーノードで設定されており、ノードごとにローカルに接続されたストレージデバイスを備えている。

- 選択した 3 つのノードのそれぞれで、少なくとも 1 つの raw ブロックデバイスが使用できる。OpenShift Data Foundation は、1 つ以上の使用可能な raw ブロックデバイスを使用します。

- 使用するデバイスが空である。ディスクには物理ボリューム (PV)、ボリュームグループ (VG)、または論理ボリューム (LV) を含めないでください。

詳細は、[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。

## ディザスタリカバリーの要件 テクノロジープレビュー

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をすべて満たす必要があります。

- 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 (RHACM) for Kubernetes サブスクリプション。

OpenShift Data Foundation のサブスクリプションの仕組みを確認するには、[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。

詳細な障害復旧の要件は、[OpenShift ワークロード用の OpenShift Data Foundation Disaster Recovery の設定](#) ガイド、および Red Hat Advanced Cluster Management for Kubernetes ドキュメントの [インストールガイド](#) の **要件と推奨事項** のセクションを参照してください。

## Arbiter ストレッチクラスターの要件 [テクノロジープレビュー]

この例では、3 番目のゾーンを Arbiter の場所とした上で、単一クラスターが 2 つのゾーンに展開されます。これはテクノロジープレビュー機能であり、現時点では OpenShift Container Platform オンプレミスおよび同じデータセンターでのデプロイメントを目的としています。このソリューションは、複数のデータセンターにまたがる展開にはお勧めできません。代わりに、Metro-DR を、低遅延ネットワークを備えた複数のデータセンターに展開されたデータ損失のない DR ソリューションの最初のオプションとして検討してください。

詳細な要件と手順については、[ストレッチクラスター用の OpenShift Data Foundation の設定](#) 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 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。



### 注記

スケーリングロジックが競合しているため、フレキシブルスケーリングと arbiter の両方を同時に有効にすることはできません。フレキシブルスケーリングを使用すると、一度に 1 つのノードを OpenShift Data Foundation クラスターに追加することができます。Arbiter クラスターでは、2 つのデータゾーンごとに 1 つ以上のノードを追加する必要があります。

## 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。

詳細は、[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。

## 第2章 動的ストレージデバイスを使用したデプロイ

Red Hat Virtualization 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できるようになります。

[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関する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クターを上書きする必要がある場合は、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** 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 **Red Hat OpenShift Data Foundation に専用のワーカーノードを使用する方法** 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、**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-4.12** 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

- 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 **Refresh web console** をクリックして、反映するコンソールを変更します。
- Web コンソールに移動します。
  - Installed Operators に移動し、**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。
  - **Storage** に移動し、**Data Foundation** ダッシュボードが使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

トークン認証のために、Vault でキーと値のバックエンドパスおよびポリシーを有効にできます。

### 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。
- 後で変更できないため、命名規則に従って一意のパス名をバックエンド **path** として慎重に選択してください。

### 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 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 を使用します。

```
$ 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 -
```

- 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 からインストールしておく。
- バックエンド **path** として一意のパス名を選択する。これは命名規則に厳密に準拠する必要があります。このパス名は後で変更できません。

### 手順

- 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. **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。

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

- 5. OCP 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}")
```

- 6. 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
```

- 7. 前の手順で収集した情報を使用して、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

発行者が空の場合は Vault で Kubernetes 認証方法を設定します。

```
$ 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 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 を使用します。

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

- シークレットに対して **write** または **delete** 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 からインストールしておく。詳細は、[Installing OpenShift Data Foundation Operator](#) を参照してください。

## 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** 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. **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。
  - 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. オプション: **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** ドロップダウンリストから、**Vault** または **Thales CipherTrust Manager (using KMIP)** を選択します。**Vault** を選択した場合は、次の手順に進みます。**Thales CipherTrust Manager (using KMIP)** を選択した場合は、手順 iii に進みます。
- 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**、ホストの **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と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。
  - PEM でエンコードされた、該当の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** を指定します。
  - **Save** をクリックして、手順 iv に進みます。

#### Kubernetes 認証方式の使用

- **Vault** ('https://<hostname or ip>') サーバーの一意的 **Connection Name**、ホストの **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と値のシークレットパスを **Backend Path** に入力します。
    - 該当する場合は、**TLS Server Name** および **Authentication Path** を入力します。
    - PEM でエンコードされた、該当の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** を指定します。
    - **Save** をクリックして、手順 iv に進みます。
- iii. **Thales CipherTrust Manager (using KMIP)** を KMS プロバイダーとして使用するには、次の手順に従います。
- A. プロジェクト内のキー管理サービスの一意的 **Connection Name** を入力します。
- B. **Address** および **Port** セクションで、Thales CipherTrust Manager の IP と、KMIP インターフェイスが有効になっているポートを入力します。以下に例を示します。

- **Address:** 123.34.3.2
  - **Port:** 5696
- C. **クライアント証明書、CA 証明書、およびクライアント秘密鍵** をアップロードします。
  - D. StorageClass 暗号化が有効になっている場合は、上記で生成された暗号化および復号化に使用する一意の識別子を入力します。
  - E. **TLS Server** フィールドはオプションであり、KMIP エンドポイントの DNS エントリがない場合に使用します。たとえば、**kmip\_all\_<port>.ciphertrustmanager.local** などです。
- iv. **Network** を選択します。
  - v. **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。

## 第3章 ローカルストレージデバイスを使用したデプロイ

ローカル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できるようになります。

このセクションを使用して、OpenShift Container Platform がインストールされている Red Hat Virtualization に OpenShift Data Foundation をデプロイします。

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、以下の手順に進んでください。

1. [ローカルストレージ Operator のインストール](#)
2. [Red Hat OpenShift Data Foundation Operator のインストール](#)
3. [OpenShift Data Foundation クラスターの作成](#)

### 3.1. ローカルストレージ OPERATOR のインストール

ローカルストレージデバイスに Red Hat OpenShift Data Foundation クラスターを作成する前に、Operator Hub からローカルストレージ Operator をインストールします。

#### 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. **Filter by keyword** ボックスに **local storage** を入力し、Operator の一覧から **Local Storage Operator** を見つけ、これをクリックします。
4. **Install Operator** ページで、以下のオプションを設定します。
  - a. チャンネルを **4.12** または **stable** のいずれかにして更新します。
  - b. インストールモードに **A specific namespace on the cluster** を選択します。
  - c. Installed Namespace に **Operator recommended namespace openshift-local-storage** を選択します。
  - d. 承認を **Automatic** として更新します。
5. **Install** をクリックします。

#### 検証手順

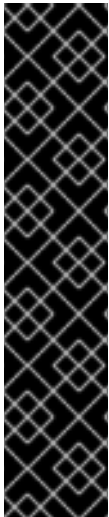
- Local Storage Operator に、インストールが正常に実行されたことを示す緑色のチェックマークが表示されていることを確認します。

### 3.2. 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、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** 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 **Red Hat OpenShift Data Foundation に専用のワーカーノードを使用する方法** 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、**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-4.12** 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

- 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 **Refresh web console** をクリックして、反映するコンソールを変更します。
- Web コンソールに移動します。
  - Installed Operators に移動し、**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。
  - **Storage** に移動し、**Data Foundation** ダッシュボードが使用可能かどうかを確認します。

### 3.3. RED HAT VIRTUALIZATION プラットフォームでの OPENSIFT DATA FOUNDATION クラスターの作成

この手順を使用して、OpenShift Data Foundation Operator のインストール後にローカルストレージデバイスを使用して OpenShift Data Foundation Cluster を作成します。

#### 前提条件

- OpenShift Data Foundation Operator は Operator Hub からインストールしておく。詳細は、[Installing OpenShift Data Foundation Operator](#) を参照してください。
- [ローカルストレージデバイスを使用して OpenShift Data Foundation をインストールするための要件](#) セクションにあるすべての要件を満たし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、以下を実行します。
  - a. **Deployment type** オプションで **Full Deployment** を選択します。
  - b. **Create a new StorageClass using the local storage devices** オプションを選択します。
  - c. **Next** をクリックします。



#### 注記

Local Storage Operator がまだインストールされていない場合は、インストールするように求められます。**Install** をクリックし、[ローカルストレージ Operator のインストール](#) で説明されているように手順に従います。

4. Create local volume set ページで、以下の情報を提供します。

- a. **LocalVolumeSet** および **StorageClass** の名前を入力します。  
デフォルトで、ローカルボリュームセット名がストレージクラス名について表示されま  
す。名前を変更できます。
- b. 以下のいずれかを選択します。
  - **Disks on all nodes** すべてのノードにある選択したフィルターに一致する利用可能な  
ディスクを使用します。
  - **Disks on selected nodes** 選択したノードにある選択したフィルターに一致する利用可  
能なディスクを使用します。



### 重要

- フレキシブルスケール機能は、3つ以上のノードで作成したス  
トレージクラスターが3つ以上のアベイラビリティゾーンの最低  
要件未滿に分散されている場合にのみ有効になります。  
フレキシブルスケールの詳細は、[フレキシブルスケールが  
有効な場合に YAML を使用した OpenShift Data Foundation クラス  
ターのスケールに関する ナレッジベースの記事](#) を参照してく  
ださい。
- フレキシブルスケール機能はデプロイ時に有効になり、後で有  
効または無効にすることはできません。
- 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。

- c. **Disk Type** の利用可能な一覧から、**SSD/NVMe** を選択します。
- d. **Advanced** セクションを拡張し、以下のオプションを設定します。

ボリューム モード	デフォルトではブロックが選択されます。
デバイスタ イプ	ドロップダウンリストから1つ以上のデバイスタイプを選択します。
ディスクサ イズ	デバイスの最小サイズ 100GB と、含める必要のあるデバイスの最大サイズを設 定します。
ディスクの 最大数の制 限	これは、ノードで作成できる PV の最大数を示します。このフィールドが空のままの場合、PV は一致するノードで利用可能なすべてのディスクに作成されま す。

- e. **Next** をクリックします。  
LocalVolumeSet の作成を確認するポップアップが表示されます。
- f. **Yes** をクリックして続行します。

1. **Capacity and nodes page** で、以下を設定します。



- a. **Available raw capacity** には、ストレージクラスに関連付けられた割り当てられたすべてのディスクに基づいて容量の値が設定されます。これには少し時間がかかります。**Selected nodes** 一覧には、ストレージクラスに基づくノードが表示されます。
  - b. 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。
  - c. **Next** をクリックします。
2. 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. 以下の **Encryption level** (暗号化レベル) のいずれかを選択します。
    - **Cluster-wide encryption**: クラスター全体 (ブロックおよびファイル) を暗号化します。
    - **StorageClass encryption**: 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. オプション: **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** ドロップダウンリストから、**Vault** または **Thales CipherTrust Manager (using KMIP)** を選択します。**Vault** を選択した場合は、次の手順に進みます。**Thales CipherTrust Manager (using KMIP)** を選択した場合は、手順 iii に進みます。
- 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**、ホストの **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と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。
  - PEM でエンコードされた、該当の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** を指定します。
  - **Save** をクリックして、手順 iv に進みます。

#### Kubernetes 認証方式の使用

- Vault ('https://<hostname or ip>') サーバーの一意的 **Connection Name**、ホストの **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と値のシークレットパスを **Backend Path** に入力します。
  - 該当する場合は、**TLS Server Name** および **Authentication Path** を入力します。
  - PEM でエンコードされた、該当の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** を指定します。
  - **Save** をクリックして、手順 iv に進みます。
- iii. **Thales CipherTrust Manager (using KMIP)** を KMS プロバイダーとして使用するには、次の手順に従います。
  - A. プロジェクト内のキー管理サービスの一意の **Connection Name** を入力します。
  - B. **Address** および **Port** セクションで、Thales CipherTrust Manager の IP と、KMIP インターフェイスが有効になっているポートを入力します。以下に例を示します。
    - **Address:** 123.34.3.2
    - **Port:** 5696
  - C. **クライアント証明書**、**CA 証明書**、および **クライアント秘密鍵** をアップロードします。
  - D. StorageClass 暗号化が有効になっている場合は、上記で生成された暗号化および復号化に使用する一意の識別子を入力します。
  - E. **TLS Server** フィールドはオプションであり、KMIP エンドポイントの DNS エントリがない場合に使用します。たとえば、**kmip\_all\_<port>.ciphertrustmanager.local** などです。
- iv. **Network** を選択します。

a. **Next** をクリックします。

1. 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** をクリックして前の設定ページに戻ります。
2. **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。

- フレキシブルスケーリングがストレージクラスターで有効にされているかどうかを確認するには、以下の手順を実行します (arbiter モードの場合、フレキシブルスケーリングが無効になります)。
  1. 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。
  2. YAML タブで、**spec** セクションのキー **flexibleScaling** と **status** セクションの **flexibleScaling** を検索します。 **flexible scaling** が **true** であり、 **failureDomain** が **host** に設定されている場合、フレキシブルスケーリング機能が有効になります。

```
spec:  
  flexibleScaling: true  
  [...]  
status:  
  failureDomain: host
```

- 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

- 初期クラスターの容量を拡張するには、[ストレージのスケーリング](#) を参照してください。

## 第4章 OPENSIFT DATA FOUNDATION デプロイメントの確認

このセクションを使用して、OpenShift Data Foundation が正しくデプロイされていることを確認します。

### 4.1. 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。

コンポーネントごとに想定される Pod 数や、ノード数に合わせてこの数値がどのように変化するかなどの詳細は、[表4.1「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4.1 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
OpenShift Data Foundation Operator	<ul style="list-style-type: none"> <li>● <b>ocs-operator-*</b> (任意のワーカーノードに 1 Pod)</li> <li>● <b>ocs-metrics-exporter-*</b> (任意のワーカーノードに 1 Pod)</li> <li>● <b>odf-operator-controller-manager-*</b> (任意のワーカーノードに 1 Pod)</li> <li>● <b>odf-console-*</b> (任意のワーカーノードに 1 Pod)</li> <li>● <b>csi-addons-controller-manager-*</b> (任意のワーカーノードに 1つの Pod)</li> </ul>
Rook-ceph Operator	<p><b>rook-ceph-operator-*</b></p> <p>(任意のワーカーノードに 1 Pod)</p>

コンポーネント	対応する Pod
Multicloud Object Gateway	<ul style="list-style-type: none"> <li>● <b>noobaa-operator-*</b> (任意のワーカーノードに1Pod)</li> <li>● <b>noobaa-core-*</b> (任意のストレージノードに1Pod)</li> <li>● <b>noobaa-db-pg-*</b> (任意のストレージノードに1Pod)</li> <li>● <b>noobaa-endpoint-*</b> (任意のストレージノードに1Pod)</li> </ul>
MON	<b>rook-ceph-mon-*</b> (ストレージノードに分散する 3 Pod)
MGR	<b>rook-ceph-mgr-*</b> (任意のストレージノードに1Pod)
MDS	<b>rook-ceph-mds-ocs-storagecluster-cephfilesystem-*</b> (ストレージノードに分散する 2 Pod)
RGW	<b>rook-ceph-rgw-ocs-storagecluster-cephobjectstore-*</b> (任意のストレージノードに1Pod)
CSI	<ul style="list-style-type: none"> <li>● <b>cephfs</b> <ul style="list-style-type: none"> <li>○ <b>csi-cephfsplugin-*</b> (各ワーカーノードに1Pod)</li> <li>○ <b>csi-cephfsplugin-provisioner-*</b> (ワーカーノードに分散する 2 Pod)</li> </ul> </li> <li>● <b>rbd</b> <ul style="list-style-type: none"> <li>○ <b>csi-rbdplugin-*</b> (各ワーカーノードに1Pod)</li> <li>○ <b>csi-rbdplugin-provisioner-*</b> (ストレージノードに分散する 2 Pod)</li> </ul> </li> </ul>
rook-ceph-crashcollector	<b>rook-ceph-crashcollector-*</b> (各ストレージノードに1Pod)

コンポーネント	対応する Pod
OSD	<ul style="list-style-type: none"> <li>● <b>rook-ceph-osd-*</b> (各デバイス用に 1 Pod)</li> <li>● <b>rook-ceph-osd-prepare-ocs-deviceset-*</b> (各デバイス用に 1 Pod)</li> </ul>

## 4.2. OPENSIFT 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。

## 4.3. 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。
  - a. **Object** タブの **Status card** 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は、[OpenShift Data Foundation の監視](#) を参照してください。

## 4.4. 特定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`
- `ocs-storagecluster-ceph-rgw`

## 第5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。Multicloud Object Gateway コンポーネントは、動的ストレージデバイスを使用するか、ローカルストレージデバイスを使用してデプロイできます。

### 5.1. 動的ストレージデバイスを使用したスタンドアロン MULTICLOUD OBJECT GATEWAY のデプロイ

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

#### 5.1.1. Red Hat OpenShift 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 クラスタにアクセスできる。
- Red Hat OpenShift Container Platform クラスタ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、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** 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 **Red Hat OpenShift Data Foundation に専用のワーカーノードを使用する方法** 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、**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-4.12** 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

- 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 **Refresh web console** をクリックして、反映するコンソールを変更します。
- Web コンソールに移動します。
  - Installed Operators に移動し、**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。
  - **Storage** に移動し、**Data Foundation** ダッシュボードが使用可能かどうかを確認します。

#### 5.1.2. 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。

#### 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: **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。
  - a. **Key Management Service Provider** ドロップダウンリストから、**Vault** または **Thales CipherTrust Manager (using KMIP)** を選択します。**Vault** を選択した場合は、次の手順に進みます。**Thales CipherTrust Manager (using KMIP)** を選択した場合は、手順 iii に進みます。
  - b. **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**、ホストの **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と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。
  - PEM でエンコードされた、該当の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** を指定します。
  - **Save** をクリックして、手順 iv に進みます。

#### Kubernetes 認証方式の使用

- Vault ('https://<hostname or ip>') サーバーの一意的 **Connection Name**、ホストの **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と値のシークレットパスを **Backend Path** に入力します。
  - 該当する場合は、**TLS Server Name** および **Authentication Path** を入力します。
  - PEM でエンコードされた、該当の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** を指定します。
  - **Save** をクリックして、手順 iv に進みます。

- c. **Thales CipherTrust Manager (using KMIP)** を KMS プロバイダーとして使用するには、次の手順に従います。
    - i. プロジェクト内のキー管理サービスの一意の **Connection Name** を入力します。
    - ii. **Address** および **Port** セクションで、Thales CipherTrust Manager の IP と、KMIP インターフェイスが有効になっているポートを入力します。以下に例を示します。
      - **Address:** 123.34.3.2
      - **Port:** 5696
    - iii. **クライアント証明書**、**CA 証明書**、および **クライアント秘密鍵** をアップロードします。
    - iv. StorageClass 暗号化が有効になっている場合は、上記で生成された暗号化および復号化に使用する一意の識別子を入力します。
    - v. **TLS Server** フィールドはオプションであり、KMIP エンドポイントの DNS エントリがない場合に使用します。たとえば、**kmip\_all\_<port>.ciphertrustmanager.local** などです。
  - d. **Network** を選択します。
  - e. **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 card** 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"> <li>● <b>ocs-operator-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>ocs-metrics-exporter-*</b>(任意のワーカーノードに 1Pod)</li> <li>● <b>odf-operator-controller-manager-*</b>(任意のワーカーノードに 1Pod)</li> <li>● <b>odf-console-*</b>(任意のワーカーノードに 1Pod)</li> <li>● <b>csi-addons-controller-manager-*</b> (任意のワーカーノードに 1つの Pod)</li> </ul>
Rook-ceph Operator	<b>rook-ceph-operator-*</b> (任意のワーカーノードに 1Pod)
Multicloud Object Gateway	<ul style="list-style-type: none"> <li>● <b>noobaa-operator-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>noobaa-core-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>noobaa-db-pg-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>noobaa-endpoint-*</b> (任意のワーカーノードに 1Pod)</li> </ul>

## 5.2. ローカルストレージデバイスを使用したスタンドアロン MULTICLOUD OBJECT GATEWAY のデプロイ

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。

- ローカルストレージ Operator のインストール
- 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

### 5.2.1. ローカルストレージ Operator のインストール

ローカルストレージデバイスに Red Hat OpenShift Data Foundation クラスターを作成する前に、Operator Hub からローカルストレージ Operator をインストールします。

#### 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. **Filter by keyword** ボックスに **local storage** を入力し、Operator の一覧から **Local Storage Operator** を見つけ、これをクリックします。

4. **Install Operator** ページで、以下のオプションを設定します。
  - a. チャンネルを **4.12** または **stable** のいずれかにして更新します。
  - b. インストールモードに **A specific namespace on the cluster** を選択します。
  - c. Installed Namespace に **Operator recommended namespace openshift-local-storage** を選択します。
  - d. 承認を **Automatic** として更新します。
5. **Install** をクリックします。

#### 検証手順

- Local Storage 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。

### 5.2.2. Red Hat OpenShift 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、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** 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 **Red Hat OpenShift Data Foundation に専用のワーカーノードを使用する方法** 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、**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-4.12** 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

- 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 **Refresh web console** をクリックして、反映するコンソールを変更します。
- Web コンソールに移動します。
  - Installed Operators に移動し、**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。
  - **Storage** に移動し、**Data Foundation** ダッシュボードが使用可能かどうかを確認します。

### 5.2.3. 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。

#### 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. **Create a new StorageClass using the local storage devices** オプションを選択します。
  - c. **Next** をクリックします。



### 注記

Local Storage Operator がまだインストールされていない場合は、インストールするように求められます。**Install** をクリックし、[ローカルストレージ Operator のインストール](#)で説明されているように手順に従います。

4. **Create local volume set** ページで、以下の情報を提供します。
  - a. **LocalVolumeSet** および **StorageClass** の名前を入力します。  
デフォルトで、ローカルボリュームセット名がストレージクラス名について表示されます。名前を変更できます。
  - b. 以下のいずれかを選択します。
    - **Disks on all nodes**  
すべてのノードにある選択したフィルターに一致する利用可能なディスクを使用します。
    - **Disks on selected nodes**  
選択したノードにある選択したフィルターにのみ一致する利用可能なディスクを使用します。
  - c. **Disk Type** の利用可能な一覧から、**SSD/NVMe** を選択します。
  - d. **Advanced** セクションを拡張し、以下のオプションを設定します。
 

ボリュームモード	デフォルトではファイルシステムが選択されています。 <b>Volume Mode</b> でファイルシステムが選択されていることを常に確認してください。
デバイスタイプ	ドロップダウンリストから1つ以上のデバイスタイプを選択します。
ディスクサイズ	デバイスの最小サイズ 100GB と、含める必要のあるデバイスの最大サイズを設定します。
ディスクの最大数の制限	これは、ノードで作成できる PV の最大数を示します。このフィールドが空のままの場合、PV は一致するノードで利用可能なすべてのディスクに作成されます。
  - e. **Next** をクリックします。  
LocalVolumeSet の作成を確認するポップアップが表示されます。
  - f. **Yes** をクリックして続行します。

## 5. Capacity and nodes ページで、以下を設定します。

- a. **Available raw capacity** には、ストレージクラスに関連付けられた割り当てられたすべてのディスクに基づいて容量の値が設定されます。これには少し時間がかかります。**Selected nodes** 一覧には、ストレージクラスに基づくノードが表示されます。
  - b. **Next** をクリックします。
6. オプション: **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。

- a. **Key Management Service Provider** ドロップダウンリストから、**Vault** または **Thales CipherTrust Manager (using KMIP)** を選択します。**Vault** を選択した場合は、次の手順に進みます。**Thales CipherTrust Manager (using KMIP)** を選択した場合は、手順 iii に進みます。
- b. **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>') サーバーの一意の **Connection Name**、ホストの **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と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。
  - PEM でエンコードされた、該当の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** を指定します。
  - **Save** をクリックして、手順 iv に進みます。

### Kubernetes 認証方式の使用

- Vault ('https://<hostname or ip>') サーバーの一意の **Connection Name**、ホストの **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と値のシークレットパスを **Backend Path** に入力します。
  - 該当する場合は、**TLS Server Name** および **Authentication Path** を入力します。
  - PEM でエンコードされた、該当の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** を指定します。
  - **Save** をクリックして、手順 iv に進みます。



- c. **Thales CipherTrust Manager (using KMIP)** を KMS プロバイダーとして使用するには、次の手順に従います。
  - i. プロジェクト内のキー管理サービスの一意の **Connection Name** を入力します。
  - ii. **Address** および **Port** セクションで、Thales CipherTrust Manager の IP と、KMIP インターフェイスが有効になっているポートを入力します。以下に例を示します。
    - **Address:** 123.34.3.2
    - **Port:** 5696
  - iii. **クライアント証明書**、**CA 証明書**、および **クライアント秘密鍵** をアップロードします。
  - iv. StorageClass 暗号化が有効になっている場合は、上記で生成された暗号化および復号化に使用する一意の識別子を入力します。
  - v. **TLS Server** フィールドはオプションであり、KMIP エンドポイントの DNS エントリがない場合に使用します。たとえば、**kmip\_all\_<port>.ciphertrustmanager.local** などです。
- d. **Network** を選択します。
- e. **Next** をクリックします。
7. **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。
8. **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 card** 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"> <li>● <b>ocs-operator-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>ocs-metrics-exporter-*</b>(任意のワーカーノードに 1Pod)</li> <li>● <b>odf-operator-controller-manager-*</b>(任意のワーカーノードに 1Pod)</li> <li>● <b>odf-console-*</b>(任意のワーカーノードに 1Pod)</li> <li>● <b>csi-addons-controller-manager-*</b> (任意のワーカーノードに 1つの Pod)</li> </ul>
Rook-ceph Operator	<p><b>rook-ceph-operator-*</b></p> <p>(任意のワーカーノードに 1Pod)</p>
Multicloud Object Gateway	<ul style="list-style-type: none"> <li>● <b>noobaa-operator-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>noobaa-core-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>noobaa-db-pg-*</b> (任意のワーカーノードに 1Pod)</li> <li>● <b>noobaa-endpoint-*</b> (任意のワーカーノードに 1Pod)</li> </ul>

## 第6章 OPENSIFT DATA FOUNDATION のアンインストール

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

OpenShift Data Foundation を内部モードでアンインストールするには、[Uninstalling OpenShift Data Foundation](#) のナレッジベース記事を参照してください。