Red Hat OpenShift Data Foundation 4.15

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

Last Updated: 2024-03-19

Red Hat OpenShift Data Foundation 4.15 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

法律上の通知

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

Red Hat では、コード、ドキュメント、Web プロパティー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)

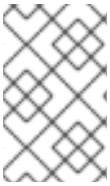
Red Hat ドキュメントに対するご意見をお聞かせください。ドキュメントの改善点があれば、ぜひお知らせください。

フィードバックを送信するには、Bugzilla チケットを作成します。

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、プロキシー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 OPENSHIFT 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されます。

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。

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。

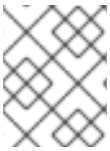
- 有効な Red Hat OpenShift Data Foundation Advanced サブスクリプション
- 有効な Red Hat Advanced Cluster Management for Kubernetes サブスクリプション
OpenShift Data Foundation のサブスクリプションの仕組みを確認するには、OpenShift Data Foundation subscriptions に関するナレッジベースの記事 を参照してください。

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。

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

Amazon Web Services (AWS) EBS(タイプ **gp2-csi** または **gp3-csi**) 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。

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。

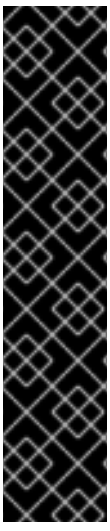
1. Red Hat OpenShift Data Foundation Operator のインストール
2. OpenShift Data Foundation クラスターの作成

2.1. RED HAT 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またはインフラストラクチャーノードが少なくとも 3 つある。
- その他のリソース要件は、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と割り当て 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. チャネルを **stable-4.15** に更新します。
   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
```

2. 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 -
```

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

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. **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_CRT=$(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="$SA_CA_CRT" \
        issuer="$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_CRT"
```

8. 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
```

9. 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 -
```

10. 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. OPENSHIFT 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. **Storage Class** を選択します。
   OpenShift Data Foundation バージョン 4.12 以降、ストレージクラスとして **gp2-csi** または **gp3-csi** を選択できます。

   d. オプション: 外部 PostgreSQL を使用するには、**Use external PostgreSQL** チェックボックスを選択します **[テクノロジープレビュー]**。
   これにより、PostgreSQL Pod が単一障害点となるマルチクラウドオブジェクトゲートウェイの高可用性ソリューションが提供されます。

      i. 以下の接続の詳細を指定します。

         - **ユーザー名**
         - **Password**
         - **サーバー名** と **ポート**
         - **データベース名**

      ii. **Enable TLS/SSL** チェックボックスを選択して、Postgres サーバーの暗号化を有効にします。

   e. **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. **Configure performance** セクションで、以下のパフォーマンスプロファイルのいずれかを選択します。

- Lean
  これは、最小リソースが推奨値よりも少ない、リソースに制約のある環境で使用します。このプロファイルでは、割り当てられる CPU とメモリーの数が少なくなり、リソースの消費が最小限に抑えられます。

- balanced (デフォルト)
  推奨リソースが利用可能な場合にこれを使用します。このプロファイルは、さまざまなワークロードのリソース消費とパフォーマンスのバランスを提供します。

- パフォーマンス
  最高のパフォーマンスを得るために十分なリソースがある環境でこれを使用してください。このプロファイルは、負荷の高いワークロードを最適に実行できるように十分なメモリーと CPU を割り当てることで、高いパフォーマンスを実現するように調整されています。

注記

StorageSystems タブのオプションメニューから **Configure performance** オプションを使用して、デプロイメント後にパフォーマンスプロファイルを設定するオプションがあります。

重要

リソースプロファイルを選択する前に、クラスター内のリソースの現在の可用性を必ず確認してください。リソースが不十分なクラスターでより高いリソースプロファイルを選択すると、インストールが失敗する可能性があります。

リソース要件の詳細は、パフォーマンスプロファイルのリソース要件 を参照してください。

d. 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ー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/アベイラビリティー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。

e. **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。

        i. 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。

        ii. 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** をデプロイメントして、**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** をデプロイメントして、**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 エントリー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。

b. 転送中の暗号化を有効にするには、**In-transit encryption** を選択します。

i. **Network** を選択します。

ii. **Next** をクリックします。

6. **Data Protection** ページで、Openshift Data Foundation のリージョナル DR ソリューションを設定している場合は、**Prepare cluster for disaster recovery(Regional-DR only)**チェックボックスを選択し、それ以外の場合は **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。

注記

デプロイメントに 5 つ以上のノード、ラック、またはルームがあり、デプロイメント内に 5 つ以上の障害ドメインが存在する場合、ラックまたはゾーンの数に基づいて Ceph モニター数を設定できます。OpenShift Web コンソールの通知パネルまたはアラートセンターにアラートが表示され、Ceph モニター数を増やすオプションが示されます。アラートで **Configure** オプションを使用して、Ceph モニター数を設定できます。詳細は、 Ceph モニターの低いアラート数の解決 を参照してください。

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、それ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. OPENSHIFT 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 の状態を確認します。
2. OpenShift Data Foundation クラスターが正常であることを確認します。
3. Multicloud Object Gateway が正常であることを確認
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します。

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リスト表示します。

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. 実行中および完了した Pod のフィルターを設定して、次の Pod が **Running** および **Completed** 状態で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
OpenShift Data Foundation Operator	• **ocs-operator-*** (任意のストレージノードに 1 Pod) • **ocs-metrics-exporter-*** (任意のストレージノードに 1 Pod) • **odf-operator-controller-manager-*** (任意のストレージノードに 1 Pod) • **odf-console-*** (任意のストレージノードに 1 Pod) • **csi-addons-controller-manager-*** (任意のストレージノードに 1 Pod)
Rook-ceph Operator	**rook-ceph-operator-*** (任意のストレージノードに 1 Pod)
Multicloud Object Gateway	• **noobaa-operator-*** (任意のストレージノードに 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	**rook-ceph-mon-*** (ストレージノードに分散する 3 Pod)
MGR	**rook-ceph-mgr-*** (任意のストレージノードに 1 Pod)
MDS	**rook-ceph-mds-ocs-storagecluster-cephfilesystem-*** (ストレージノードに分散する 2 Pod)

コンポーネント	対応する Pod

CSI	• **cephfs**
	  ◦ **csi-cephfsplugin-*** (各ストレージノードに 1 Pod)
	  ◦ **csi-cephfsplugin-provisioner-*** (ストレージノードに分散する 2 Pod)
	• **rbd**
	  ◦ **csi-rbdplugin-*** (各ストレージノードに 1 Pod)
	  ◦ **csi-rbdplugin-provisioner-*** (ストレージノードに分散する 2 Pod)

rook-ceph-crashcollector	**rook-ceph-crashcollector-*** (各ストレージノードに 1 Pod)
OSD	• **rook-ceph-osd-*** (各デバイス用に 1 Pod) • **rook-ceph-osd-prepare-ocs-deviceset-*** (各デバイス用に 1 Pod)

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。

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については、OpenShift Data Foundation の監視 を参照してください。

2.5.4. 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**

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 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またはインフラストラクチャーノードが少なくとも 3 つある。
- その他のリソース要件は、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と割り当て 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. チャネルを **stable-4.15** に更新します。

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。

3.2. 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>') サーバーの一意の **Connection Name**、ホストの **Address**、**Port** 番号および **Token** を入力します。
      - **Advanced Settings** をデプロイメントして、**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** をデプロイメントして、**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 エントリー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 クラスター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。

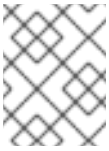
   a. **Object** タブの **Status card** で、**Object Service** と **Data Resiliency** の両方に緑色のチェックマークが表示されていることを確認します。

   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リスト表示します。

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	• **ocs-operator-*** (任意のストレージノードに 1 Pod) • **ocs-metrics-exporter-*** (任意のストレージノードに 1 Pod) • **odf-operator-controller-manager-*** (任意のストレージノードに 1 Pod) • **odf-console-*** (任意のストレージノードに 1 Pod) • **csi-addons-controller-manager-*** (任意のストレージノードに 1 Pod)
Rook-ceph Operator	**rook-ceph-operator-*** (任意のストレージノードに 1 Pod)
Multicloud Object Gateway	• **noobaa-operator-*** (任意のストレージノードに 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)

第4章 OPENSHIFT DATA FOUNDATION トポロジーの表示

トポロジーは、OpenShift Data Foundation ストレージクラスターをマップしたた視覚情報をさまざまな抽象化レベルで示し、このような階層の操作も可能にします。このビューでは、ストレージクラスターがさまざまな要素でどのように構成されているかがわかります。

手順

1. OpenShift Web コンソールで、**Storage → Data Foundation → Topology** に移動します。このビューには、ストレージクラスターとその内部のゾーンが表示されます。ノードがゾーン内 (点線で示されている) にある円形のエンティティーで表示されていることが分かります。各アイテムまたはリソースのラベルには、ステータスやヘルス、アラートの状態などの基本情報が含まれています。

2. ノードを選択すると、右側のパネルにノードの詳細が表示されます。検索/プレビューデコレーターアイコンをクリックして、ノード内のリソースまたはデプロイメントにアクセスすることもできます。

3. デプロイメントの詳細を表示します。

    a. ノード上のプレビューデコレーターをクリックします。ノードの上にモーダルウィンドウが表示され、そのノードに関連付けられているすべてのデプロイメントとそのステータスが表示されます。

    b. モデルの左上隅にある **Back to main view**ボタンをクリックしてモデルを閉じ、前のビューに戻ります。

    c. 特定のデプロイメントを選択すると、そのデプロイメントに関する詳細が表示されます。関連するデータがすべてサイドパネルに表示されます。

4. **Resources** タブをクリックして Pod 情報を表示します。このタブを使用すると、問題の理解を深めることができるだけでなく、複数の詳細レベルが提供されるので適切にトラブルシューティングができるようになります。

5. Pod のリンクをクリックして、OpenShift Container Platform の Pod 情報ページを表示します。リンクは新しいウィンドウで開きます。

第5章 OPENSHIFT DATA FOUNDATION のアンインストール

5.1. 内部モードでの OPENSHIFT 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。