



# Red Hat OpenShift Container Storage 4.8

## Amazon Web サービスを使用した OpenShift Container Storage のデプロイ

OpenShift Container Storage の OpenShift Container Platform AWS クラスターへの  
インストールおよび設定方法



## Red Hat OpenShift Container Storage 4.8 Amazon Web サービスを使用した OpenShift Container Storage のデプロイ

---

OpenShift Container Storage の OpenShift Container Platform AWS クラスターへのインストール  
および設定方法

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\_Container\_Storage\_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<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

クラウドストレージに Amazon Web Services を使用して Red Hat OpenShift Container Storage 4.8 をインストールする方法については、本書をお読みください。

---

## 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
<b>第1章 OPENSIFT CONTAINER STORAGE のデプロイの準備 .....</b>	<b>6</b>
1.1. RED HAT ENTERPRISE LINUX ベースのノード上のコンテナでのファイルシステムアクセスの有効化	6
1.2. VAULT でのキー値のバックエンドパスおよびポリシーの有効化	7
<b>第2章 動的ストレージデバイスを使用したデプロイ .....</b>	<b>8</b>
2.1. RED HAT OPENSIFT CONTAINER STORAGE OPERATOR のインストール	8
2.2. 内部モードでの OPENSIFT CONTAINER STORAGE CLUSTER SERVICE の作成	9
<b>第3章 OPENSIFT CONTAINER STORAGE デプロイメントの検証 .....</b>	<b>13</b>
3.1. POD の状態の確認	13
3.2. OPENSIFT CONTAINER STORAGE クラスタが正常であることの確認	14
3.3. MULTICLOUD OBJECT GATEWAY が正常であることの確認	15
3.4. OPENSIFT CONTAINER STORAGE 固有のストレージクラスが存在することの確認	15
<b>第4章 OPENSIFT CONTAINER STORAGE のアンインストール .....</b>	<b>16</b>
4.1. 内部モードでの OPENSIFT CONTAINER STORAGE のアンインストール	16
4.2. OPENSIFT CONTAINER STORAGE からのモニターリングスタックの削除	22
4.3. OPENSIFT CONTAINER STORAGE からの OPENSIFT CONTAINER PLATFORM レジストリーの削除	25
4.4. OPENSIFT CONTAINER STORAGE からのクラスタロギング OPERATOR の削除	26



## 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 Container Storage 4.8 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 Container Storage クラスターのみがサポートされます。導入要件の詳細については、[Planning your deployment](#) および [Preparing to deploy OpenShift Container Storage](#) を参照してください。

OpenShift Container Storage をデプロイするには、[OpenShift Container Storage のデプロイの準備についての章](#) の要件を確認し、環境のデプロイメントプロセスを実行します。

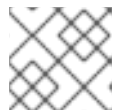
- [動的ストレージデバイスを使用したデプロイ](#)

## 第1章 OPENSIFT CONTAINER STORAGE のデプロイの準備

ダイナミックストレージデバイスを使用して OpenShift Container Storage 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。

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

1. ワーカーノード向けの Red Hat Enterprise Linux ベースのホストについては、[Red Hat Enterprise Linux ベースのノードでのコンテナのファイルシステムのアクセスを有効にします](#)。



### 注記

Red Hat Enterprise Linux CoreOS(RHCOS) の場合は、この手順を省略します。

2. オプション: 外部鍵管理システム (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:
  - トークンのあるポリシーが存在し、Vault のキー値のバックエンドパスが有効にされていることを確認します。[Vault でのキー値のバックエンドパスおよびポリシーの有効化について参照してください](#)。
  - 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。
3. ノードの最小要件 [テクノロジープレビュー]
 

OpenShift Container Storage 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 [リソース要件](#) のセクションを参照してください。

### 1.1. RED HAT ENTERPRISE LINUX ベースのノード上のコンテナでのファイルシステムアクセスの有効化

ユーザーによってプロビジョニングされるインフラストラクチャー (UPI) で Red Hat Enterprise Linux がベースの OpenShift Data Foundation にワーカーノードを含めて OpenShift Container Storage をデプロイしても自動的に、基盤の Ceph ファイルシステムへのコンテナアクセスが提供されるわけではありません。



### 注記

Red Hat Enterprise Linux CoreOS(RHCOS) をベースとするホストの場合は、このセクションを省略します。

### 手順

1. Red Hat Enterprise Linux ベースのノードにログインし、ターミナルを開きます。
2. クラスター内の各ノードについて、以下を実行します。
  - a. ノードが `rhel-7-server-extras-rpms` リポジトリにアクセスできることを確認します。

```
# subscription-manager repos --list-enabled | grep rhel-7-server
```

出力に **rhel-7-server-rpms** と **rhel-7-server-extras-rpms** の両方が表示されない場合は、以下のコマンドを実行して各リポジトリを有効にします。

```
# subscription-manager repos --enable=rhel-7-server-rpms
# subscription-manager repos --enable=rhel-7-server-extras-rpms
```

- b. 必要なパッケージをインストールします。

```
# yum install -y polycycoreutils container-selinux
```

- c. SELinux での Ceph ファイルシステムのコンテナの使用を永続的に有効にします。

```
# setsebool -P container_use_cephfs on
```

## 1.2. VAULT でのキー値のバックエンドパスおよびポリシーの有効化

### 前提条件

- Vault への管理者アクセス。
- 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=ocs 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=ocs 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 "ocs/*" {
  capabilities = ["create", "read", "update", "delete", "list"]
}
path "sys/mounts" {
  capabilities = ["read"]
}' | vault policy write ocs -
```

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=ocs -format json
```

## 第2章 動的ストレージデバイスを使用したデプロイ

AWS EBS (タイプ: gp2) で提供される動的ストレージデバイスを使用して OpenShift Container Storage 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。



### 注記

AWS では、内部の OpenShift Container Storage 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についての詳細は、[Planning your deployment](#) を参照してください。

[OpenShift Container Storage のデプロイの準備](#) について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 Container Storage Operator をインストールする](#)
2. [OpenShift Container Storage Cluster Service を作成します](#)。

### 2.1. RED HAT OPENSIFT CONTAINER STORAGE OPERATOR のインストール

Red Hat OpenShift Container Storage 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。
- 必要な追加要件をすべて満たしています。詳細は、[Planning your deployment](#) を参照してください。



### 注記

- OpenShift Container Storage 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 namespace を作成します)。

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

- ノードに Red Hat OpenShift Container Storage リソースのみがスケジュールされるように、そのノードに **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 Container Storage に専用のワーカーノードを使用する方法](#) 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. Operator の一覧から **OpenShift Container Storage** を検索し、これをクリックします。
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-4.8** 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。
  - e. **Install** をクリックします。

**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 が新規バージョンに更新されるように更新要求を手動で承認する必要があります。

#### 検証手順

- **OpenShift Container 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。

## 2.2. 内部モードでの OPENSIFT CONTAINER STORAGE CLUSTER SERVICE の作成

以下の手順を使用して、OpenShift Container Storage Operator のインストール後に OpenShift Container Storage Cluster Service を作成します。

#### 前提条件

- OpenShift Container Storage は Operator Hub からインストールする必要があります。詳細は、[Operator Hub を使用した OpenShift Container Storage Operator のインストール](#) について参照してください。

#### 手順

1. OpenShift Web コンソールにログインします。
2. **Operators** → **Installed Operators** をクリックし、インストールされた Operator をすべて表示します。  
選択された **Project** が **openshift-storage** であることを確認します。
3. Storage Cluster の **OpenShift Container Storage** > **Create Instance** リンクをクリックします。

4. **Mode** がデフォルトで **Internal** に設定されます。
5. **Capacity and nodes** を選択します。
  - a. **Storage Class** を選択します。デフォルトでは **gp2** に設定されます。
  - b. ドロップダウンリストから **Requested Capacity** を選択します。デフォルトで、これは **2 TiB** に設定されます。ドロップダウンを使用して容量の値を変更できます。



### 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)。

- c. **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。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 Container Storage 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。
6. (オプション) **Security and network** 設定を設定します。
    - a. **Enable encryption** チェックボックスを選択して、ブロックおよびファイルストレージを暗号化します。
    - b. 1 つまたは両方の **Encryption level** を選択します。
      - **クラスター全体の暗号化** 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。
      - **Storage class encryption** (ストレージクラスの暗号化): 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. **Vault Service Name**、Vault サーバーのホスト **Address** ('https://<hostname または ip>')、**Port number** および **Token** を入力します。
      - iii. **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。
        - A. OpenShift Container Storage 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。
        - B. (オプション) **TLS Server Name** および **Vault Enterprise Namespace** を入力します。
        - C. 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て、**CA Certificate**、**Client Certificate**、および **Client Private Key** を指定します。

D. **Save** をクリックします。

7. 単一のネットワークを使用する場合は **Default (SDN)** を選択し、複数のネットワークインターフェイスを使用する場合は **Custom (Multus)** ネットワークを選択します。
  - a. ドロップダウンメニューから **Public Network Interface** を選択します。
  - b. ドロップダウンメニューから **Cluster Network Interface** を選択します。



### 注記

1つの追加ネットワークインターフェイスのみを使用する場合は、パブリックネットワークインターフェイス (例: ocs-public-cluster) の単一の NetworkAttachmentDefinition を選択し、Cluster Network Interface を空白のままにします。

8. **Next** をクリックします。
9. 設定の詳細を確認します。設定を変更するには、**Back** をクリックして以前の設定ページに戻ります。
10. **Create** をクリックします。
11. Vault Key/Value (KV) シークレットエンジン API の場合に configmap を編集します。バージョン 2 は、鍵管理システム (KMS) のクラスター全体の暗号化に使用されます。
  - a. OpenShift Web コンソールで **Workloads** → **ConfigMaps** に移動します。
  - b. KMS 接続の詳細を表示するには、**ocs -kms-connection-details** をクリックします。
  - c. configmap を編集します。
    - i. **Action menu (⋮)** → **Edit ConfigMap** をクリックします。
    - ii. **VAULT\_BACKEND** パラメーターを **v2** に設定します。

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: ocs-kms-connection-details
  [...]
data:
  KMS_PROVIDER: vault
  KMS_SERVICE_NAME: vault
  [...]
  VAULT_BACKEND: v2
  [...]
```

- iii. **Save** をクリックします。

### 検証手順

1. ストレージクラスターの詳細ページで、ストレージクラスター名の横に緑色のチェックマークが表示され、クラスターが正常に作成されたことを示します。

2. インストールされたストレージクラスターの最後の **Status** が緑色のチェックマークと共に **Phase: Ready** と表示されていることを確認します。
  - **Operators** → **Installed Operators** → **Storage Cluster**のリンクをクリックして、ストレージクラスターのインストールのステータスを表示します。
  - または、Operator **Details** タブで、**Storage Cluster** タブをクリックすると、ステータスを表示できます。
3. OpenShift Container Storage 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、[OpenShift Container Storage インストールの確認](#) を参照してください。



## 第3章 OPENSIFT CONTAINER STORAGE デプロイメントの検証

このセクションを使用して、OpenShift Container Storage が正常にデプロイされていることを確認します。

### 3.1. POD の状態の確認

OpenShift Containers Storage の Pod が実行状態にあることを確認するには、以下の手順に従います。

#### 手順

1. OpenShift Web コンソールにログインします。
2. OpenShift Web コンソールの左側のペインから **Workloads** → **Pods** をクリックします。
3. **Project** ドロップダウンリストから **openshift-storage** を選択します。  
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3.1「OpenShift Container Storage クラスタに対応する Pod」](#) を参照してください。
4. **Running** タブと **Completed** タブをクリックして、Pod が実行中で完了状態になっていることを確認します。

表3.1 OpenShift Container Storage クラスタに対応する Pod

コンポーネント	対応する Pod
OpenShift Container Storage 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></li> </ul>
Rook-ceph Operator	<b>rook-ceph-operator-*</b> (任意のワーカーノードに 1 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 1 Pod)</li> <li>● <b>noobaa-core-*</b> (任意のストレージノードに 1 Pod)</li> <li>● <b>noobaa-db-pg-*</b> (任意のストレージノードに 1 Pod)</li> <li>● <b>noobaa-endpoint-*</b> (任意のストレージノードに 1 Pod)</li> </ul>
MON	<b>rook-ceph-mon-*</b> (ストレージノードに分散する 3 Pod)

コンポーネント	対応する Pod
MGR	<b>rook-ceph-mgr-*</b> (任意のストレージノードに 1 Pod)
MDS	<b>rook-ceph-mds-ocs-storagecluster-cephfilesystem-*</b> (ストレージノードに分散する 2 Pod)
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 1 Pod)</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 1 Pod)</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 1 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-device-*</b> (各デバイス用に 1 Pod)</li> </ul>

### 3.2. OPENSIFT CONTAINER STORAGE クラスタが正常であることの確認

OpenShift Container Storage のクラスタが正常であることを確認するには、手順の手順に従います。

#### 手順

1. **Storage → Overview** をクリックし、**Block and File** タブをクリックします。
2. **Status** カードで、**Storage Cluster** および **Data Resiliency** 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。
3. **Details** カードで、クラスタ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 Container Storage クラスタの正常性については、[OpenShift Container Storage のモニターリング](#) を参照してください。

### 3.3. MULTICLOUD OBJECT GATEWAY が正常であることの確認

OpenShift Container Storage Multicloud Object Gateway が正常であることを確認するには、手順のステップに従います。

#### 手順

1. OpenShift Web コンソールから **Storage → Overview** をクリックし、**Object** タブをクリックします。
2. **Status card** で、**Object Service** と **Data Resiliency** の両方が **Ready** 状態 (緑のチェックマーク) にあることを確認します。
3. **Details カード** で、Multicloud Object Gateway 情報が表示されることを確認します。

オブジェクトサービスダッシュボードを使用した OpenShift Container Storage クラスターの正常性については、[OpenShift Container Storage のモニタリング](#) を参照してください。

### 3.4. OPENSIFT CONTAINER STORAGE 固有のストレージクラスが存在することの確認

ストレージクラスがクラスターに存在することを確認するには、手順のステップに従います。

#### 手順

1. OpenShift Web コンソールから **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 Container Storage 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4章 OPENSIFT CONTAINER STORAGE のアンインストール

### 4.1. 内部モードでの OPENSIFT CONTAINER STORAGE のアンインストール

このセクションの手順に従って OpenShift Container Storage をアンインストールします。

#### アノテーションのアンインストール

Storage Cluster のアノテーションは、アンインストールプロセスの動作を変更するために使用されます。アンインストールの動作を定義するために、ストレージクラスターに以下の2つのアノテーションが導入されました。

- `uninstall.ocs.openshift.io/cleanup-policy: delete`
- `uninstall.ocs.openshift.io/mode: graceful`

以下の表は、これらのアノテーションで使用できる各種値に関する情報を示しています。

表4.1 `uninstall.ocs.openshift.io` でアノテーションの説明をアンインストールする

Annotation	値	デフォルト	動作
<code>cleanup-policy</code>	<code>delete</code>	はい	Rook は物理ドライブおよび <b>DataDirHostPath</b> をクリーンアップします。
<code>cleanup-policy</code>	<code>Retain</code>	いいえ	Rook は物理ドライブおよび <b>DataDirHostPath</b> をクリーンアップし <b>ません</b> 。
<code>mode</code>	<code>graceful</code>	はい	Rook および NooBaa は PVC および OBC が管理者/ユーザーによって削除されるまでアンインストールプロセスを一時停止します。
<code>mode</code>	<code>forced</code>	いいえ	Rook および NooBaa は、Rook および NooBaa を使用してプロビジョニングされた PVC/OBC がそれぞれ存在している場合でもアンインストールを続行します。

以下のコマンドを使用してアノテーションの値を編集し、クリーンアップポリシーまたはアンインストールモードを変更できます。

```
$ oc annotate storagecluster -n openshift-storage ocs-storagecluster
uninstall.ocs.openshift.io/cleanup-policy="retain" --overwrite
storagecluster.ocs.openshift.io/ocs-storagecluster annotated
```

```
$ oc annotate storagecluster -n openshift-storage ocs-storagecluster
uninstall.ocs.openshift.io/mode="forced" --overwrite
storagecluster.ocs.openshift.io/ocs-storagecluster annotated
```

## 前提条件

- OpenShift Container Storage クラスターの状態が正常であることを確認します。リソースまたはノードの不足により一部の Pod が正常に終了されないと、アンインストールプロセスに失敗する可能性があります。クラスターが状態が正常でない場合は、OpenShift Container Storage をアンインストールする前に Red Hat カスタマーサポートにお問い合わせください。
- アプリケーションが OpenShift Container Storage によって提供されるストレージクラスを使用して永続ボリューム要求 (PVC) またはオブジェクトバケット要求 (OBC) を使用していないことを確認します。
- カスタムリソース (カスタムストレージクラス、cephblockpools など) が管理者によって作成された場合、それらを消費したリソースを削除した後に管理者によって削除される必要があります。

## 手順

1. OpenShift Container Storage を使用しているボリュームスナップショットを削除します。
  - a. すべての namespace からボリュームスナップショットを一覧表示します。

```
$ oc get volumesnapshot --all-namespaces
```

- b. 直前のコマンドの出力から、OpenShift Container Storage を使用しているボリュームスナップショットを特定し、削除します。

```
$ oc delete volumesnapshot <VOLUME-SNAPSHOT-NAME> -n <NAMESPACE>
```

2. OpenShift Container Storage を使用している PVC および OBC を削除します。  
デフォルトのアンインストールモード (graceful) では、アンインストーラーは OpenShift Container Storage を使用するすべての PVC および OBC が削除されるまで待機します。

PVC を事前に削除せずに Storage Cluster を削除する場合は、アンインストールモードのアンインストールを **forced** に設定し、この手順を省略できます。これを行うと、システム内に孤立した PVC と OBC が発生します。

- a. OpenShift Container Storage を使用して、OpenShift Container Platform モニターリングスタック PVC を削除します。  
詳細は、「[OpenShift Container Storage からのモニターリングスタックの削除](#)」を参照してください。
- b. OpenShift Container Storage を使用して、OpenShift Container Platform レジストリー PVC を削除します。  
詳細は、「[OpenShift Container Storage からの OpenShift Container Platform レジストリーの削除](#)」を参照してください。

- c. OpenShift Container Storage を使用して、OpenShift Container Platform ロギング PVC を削除します。  
詳細は、「[OpenShift Container Storage からのクラスターロギング Operator の削除](#)」を参照してください。
- d. OpenShift Container Storage を使用してプロビジョニングした PVC および OBC を削除します。
- 次のスクリプトは、OpenShift Container Storage を使用してプロビジョニングされた PVC および OBC を識別するためのサンプルスクリプトです。このスクリプトは、OpenShift Container Storage によって内部で使用される PVC を無視します。

```
#!/bin/bash

RBD_PROVISIONER="openshift-storage.rbd.csi.ceph.com"
CEPHFS_PROVISIONER="openshift-storage.cephfs.csi.ceph.com"
NOOBAA_PROVISIONER="openshift-storage.noobaa.io/obc"
RGW_PROVISIONER="openshift-storage.ceph.rook.io/bucket"

NOOBAA_DB_PVC="noobaa-db"
NOOBAA_BACKINGSTORE_PVC="noobaa-default-backing-store-noobaa-pvc"

# Find all the OCS StorageClasses
OCS_STORAGECLASSES=$(oc get storageclasses | grep -e
"$RBD_PROVISIONER" -e "$CEPHFS_PROVISIONER" -e
"$NOOBAA_PROVISIONER" -e "$RGW_PROVISIONER" | awk '{print $1}')

# List PVCs in each of the StorageClasses
for SC in $OCS_STORAGECLASSES
do
    echo
    "=====
=="
    echo "$SC StorageClass PVCs and OBCs"
    echo
    "=====
=="
    oc get pvc --all-namespaces --no-headers 2>/dev/null | grep $SC | grep -v -e
"$NOOBAA_DB_PVC" -e "$NOOBAA_BACKINGSTORE_PVC"
    oc get obc --all-namespaces --no-headers 2>/dev/null | grep $SC
    echo
done
```



### 注記

クラウドプラットフォームの **RGW\_PROVISIONER** を省略します。

- OBC を削除します。

```
$ oc delete obc <obc name> -n <project name>
```

- PVC を削除します。

```
$ oc delete pvc <pvc name> -n <project-name>
```



## 注記

クラスターに作成されているカスタムバックリングストア、バケットクラスなどを削除していることを確認します。

- Storage Cluster オブジェクトを削除し、関連付けられたリソースが削除されるのを待機します。

```
$ oc delete -n openshift-storage storagecluster --all --wait=true
```

- `uninstall.ocs.openshift.io/cleanup-policy` が **delete** (default) に設定されている場合にクリーンアップ Pod の有無を確認し、それらのステータスが **Completed** していることを確認します。

```
$ oc get pods -n openshift-storage | grep -i cleanup
NAME                                READY STATUS RESTARTS AGE
cluster-cleanup-job-<xx>            0/1   Completed 0      8m35s
cluster-cleanup-job-<yy>            0/1   Completed 0      8m35s
cluster-cleanup-job-<zz>            0/1   Completed 0      8m35s
```

- `/var/lib/rook` ディレクトリーが空であることを確認します。このディレクトリーは空になるのは、`uninstall.ocs.openshift.io/cleanup-policy` アノテーションが **delete** (デフォルト) に設定されている場合に限られます。

```
$ for i in $(oc get node -l cluster.ocs.openshift.io/openshift-storage= -o jsonpath='{.items[*].metadata.name}'); do oc debug node/${i} -- chroot /host ls -l /var/lib/rook; done
```

- 暗号化がインストール時に有効にされている場合は、すべての OpenShift Container Storage ノードの OSD デバイスから **dm-crypt** で管理される **device-mapper** マッピングを削除します。

- デバッグ Pod を作成し、ストレージノードのホストに対して **chroot** を作成します。

```
$ oc debug node/<node name>
$ chroot /host
```

- デバイス名を取得し、OpenShift Container Storage デバイスについてメモします。

```
$ dmsetup ls
ocs-deviceset-0-data-0-57snx-block-dmccrypt (253:1)
```

- マップ済みデバイスを削除します。

```
$ cryptsetup luksClose --debug --verbose ocs-deviceset-0-data-0-57snx-block-dmccrypt
```



## 注記

権限が十分でないため、コマンドがスタックした場合には、以下のコマンドを実行します。

- **CTRL+Z** を押して上記のコマンドを終了します。
- スタックしたプロセスの PID を検索します。

```
$ ps -ef | grep crypt
```

- **kill** コマンドを使用してプロセスを終了します。

```
$ kill -9 <PID>
```

- デバイス名が削除されていることを確認します。

```
$ dmsetup ls
```

7. namespace を削除し、削除が完了するまで待機します。**openshift-storage** がアクティブなプロジェクトである場合は、別のプロジェクトに切り替える必要があります。以下に例を示します。

```
$ oc project default
$ oc delete project openshift-storage --wait=true --timeout=5m
```

以下のコマンドが NotFound エラーを返すと、プロジェクトが削除されます。

```
$ oc get project openshift-storage
```



## 注記

OpenShift Container Storage のアンインストール時に、**namespace** が完全に削除されず、**Terminating** 状態のままである場合は、[Troubleshooting and deleting remaining resources during Uninstall](#) の記事に記載の手順を実行して namespace の終了をブロックしているオブジェクトを特定します。

8. ストレージノードのラベルを解除します。

```
$ oc label nodes --all cluster.ocs.openshift.io/openshift-storage-
$ oc label nodes --all topology.rook.io/rack-
```

9. ノードにテイントのマークが付けられている場合に OpenShift Container Storage テイントを削除します。

```
$ oc adm taint nodes --all node.ocs.openshift.io/storage-
```

10. OpenShift Container Storage を使用してプロビジョニングした PV がすべて削除されていることを確認します。**Released** 状態のままの PV がある場合は、これを削除します。

```
$ oc get pv
$ oc delete pv <pv name>
```



11. Multicloud Object Gateway storageclass を削除します。

```
$ oc delete storageclass openshift-storage.noobaa.io --wait=true --timeout=5m
```

12. **CustomResourceDefinitions** を削除します。

```
$ oc delete crd backingstores.noobaa.io bucketclasses.noobaa.io
cephblockpools.ceph.rook.io cephclusters.ceph.rook.io cephfilesystems.ceph.rook.io
cephnfses.ceph.rook.io cephobjectstores.ceph.rook.io cephobjectstoreusers.ceph.rook.io
noobaas.noobaa.io ocsinitializations.ocs.openshift.io storageclusters.ocs.openshift.io
cephclients.ceph.rook.io cephobjectrealms.ceph.rook.io cephobjectzonegroups.ceph.rook.io
cephobjectzones.ceph.rook.io cephrbdmirrors.ceph.rook.io --wait=true --timeout=5m
```

13. オプション: vault キーが完全に削除されるようにするには、vault キーに関連付けられているメタデータを手動で削除する必要があります。



### 注記

このステップは、Vault Key/Value (KV) シークレットエンジン API バージョン 2 が、OpenShift Container Storage のアンインストール中に Vault キーが削除済みとしてマークされ、完全に削除されないため、Key Management System (KMS) によるクラスター全体の暗号化に使用される場合にのみ実行してください。必要に応じて、後でいつでも復元できます。

- a. Vault 内のキーを一覧表示します。

```
$ vault kv list <backend_path>
```

<backend\_path>

暗号化キーが保存されている Vault 内のパスです。  
以下に例を示します。

```
$ vault kv list kv-v2
```

出力例:

```
Keys
-----
NOOBAA_ROOT_SECRET_PATH/
rook-ceph-osd-encryption-key-ocs-deviceset-thin-0-data-0m27q8
rook-ceph-osd-encryption-key-ocs-deviceset-thin-1-data-0sq227
rook-ceph-osd-encryption-key-ocs-deviceset-thin-2-data-0xzszb
```

- b. Vault キーに関連付けられているメタデータを一覧表示します。

```
$ vault kv get kv-v2/<key>
```

Multicloud Object Gateway (MCG) キーの場合:

```
$ vault kv get kv-v2/NOOBAA_ROOT_SECRET_PATH/<key>
```

**<key>**

暗号化キーです。  
以下に例を示します。

```
$ vault kv get kv-v2/rook-ceph-osd-encryption-key-ocs-deviceset-thin-0-data-0m27q8
```

出力例:

```
=====  
Key      Value  
----  
created_time 2021-06-23T10:06:30.650103555Z  
deletion_time 2021-06-23T11:46:35.045328495Z  
destroyed    false  
version      1
```

- c. メタデータを削除します。

```
$ vault kv metadata delete kv-v2/<key>
```

MCG キーの場合:

```
$ vault kv metadata delete kv-v2/NOOBAA_ROOT_SECRET_PATH/<key>
```

**<key>**

暗号化キーです。  
以下に例を示します。

```
$ vault kv metadata delete kv-v2/rook-ceph-osd-encryption-key-ocs-deviceset-thin-0-  
data-0m27q8
```

出力例:

```
Success! Data deleted (if it existed) at: kv-v2/metadata/rook-ceph-osd-encryption-key-  
ocs-deviceset-thin-0-data-0m27q8
```

- d. これらの手順を繰り返して、すべての Vault キーに関連付けられているメタデータを削除します。

14. OpenShift Container Platform Web コンソールで、OpenShift Container Storage が完全にアンインストールされていることを確認するには、以下を実行します。

- a. **ストレージ** をクリックします。
- b. **Overview** が Storage に表示されていないことを確認します。

## 4.2. OPENSIFT CONTAINER STORAGE からのモニターリングスタックの削除

このセクションでは、モニタリングスタックを OpenShift Container Storage からクリーンアップします。

モニタリングスタックの設定の一部として作成される PVC は **openshift-monitoring** namespace に置かれます。

## 前提条件

- PVC は OpenShift Container Platform モニタリングスタックを使用できるように設定されま  
す。  
詳細は、[モニタリングスタックの設定](#) を参照してください。

## 手順

1. **openshift-monitoring** namespace で現在実行されている Pod および PVC を一覧表示します。

```
$ oc get pod,pvc -n openshift-monitoring
```

NAME	READY	STATUS	RESTARTS	AGE
pod/alertmanager-main-0	3/3	Running	0	8d
pod/alertmanager-main-1	3/3	Running	0	8d
pod/alertmanager-main-2	3/3	Running	0	8d
pod/cluster-monitoring-operator-84457656d-pkrxm	1/1	Running	0	8d
pod/grafana-79ccf6689f-2ll28	2/2	Running	0	8d
pod/kube-state-metrics-7d86fb966-rvd9w	3/3	Running	0	8d
pod/node-exporter-25894	2/2	Running	0	8d
pod/node-exporter-4dsd7	2/2	Running	0	8d
pod/node-exporter-6p4zc	2/2	Running	0	8d
pod/node-exporter-jbjvg	2/2	Running	0	8d
pod/node-exporter-jj4t5	2/2	Running	0	6d18h
pod/node-exporter-k856s	2/2	Running	0	6d18h
pod/node-exporter-rf8gn	2/2	Running	0	8d
pod/node-exporter-rmb5m	2/2	Running	0	6d18h
pod/node-exporter-zj7kx	2/2	Running	0	8d
pod/openshift-state-metrics-59dbd4f654-4clng	3/3	Running	0	8d
pod/prometheus-adapter-5df5865596-k8dzn	1/1	Running	0	7d23h
pod/prometheus-adapter-5df5865596-n2gj9	1/1	Running	0	7d23h
pod/prometheus-k8s-0	6/6	Running	1	8d
pod/prometheus-k8s-1	6/6	Running	1	8d
pod/prometheus-operator-55cfb858c9-c4zd9	1/1	Running	0	6d21h
pod/telemeter-client-78fc8fc97d-2rgfp	3/3	Running	0	8d

NAME	CAPACITY	ACCESS MODES	STATUS	VOLUME STORAGECLASS	AGE
persistentvolumeclaim/my-alertmanager-claim-alertmanager-main-0	40Gi	RWO	Bound	pvc-0d519c4f-15a5-11ea-baa0-026d231574aa	8d
persistentvolumeclaim/my-alertmanager-claim-alertmanager-main-1	40Gi	RWO	Bound	pvc-0d5a9825-15a5-11ea-baa0-026d231574aa	8d
persistentvolumeclaim/my-alertmanager-claim-alertmanager-main-2			Bound	pvc-	

```

0d6413dc-15a5-11ea-baa0-026d231574aa 40Gi RWO ocs-storagecluster-ceph-
rbd 8d
persistentvolumeclaim/my-prometheus-claim-prometheus-k8s-0 Bound pvc-0b7c19b0-
15a5-11ea-baa0-026d231574aa 40Gi RWO ocs-storagecluster-ceph-rbd 8d
persistentvolumeclaim/my-prometheus-claim-prometheus-k8s-1 Bound pvc-0b8aed3f-
15a5-11ea-baa0-026d231574aa 40Gi RWO ocs-storagecluster-ceph-rbd 8d

```

2. モニタリング **configmap** を編集します。

```
$ oc -n openshift-monitoring edit configmap cluster-monitoring-config
```

3. 以下の例が示すように、OpenShift Container Storage ストレージクラスを参照する **config** セクションを削除し、これを保存します。

編集前

```

.
.
.
apiVersion: v1
data:
  config.yaml: |
    alertmanagerMain:
      volumeClaimTemplate:
        metadata:
          name: my-alertmanager-claim
        spec:
          resources:
            requests:
              storage: 40Gi
          storageClassName: ocs-storagecluster-ceph-rbd
    prometheusK8s:
      volumeClaimTemplate:
        metadata:
          name: my-prometheus-claim
        spec:
          resources:
            requests:
              storage: 40Gi
          storageClassName: ocs-storagecluster-ceph-rbd
kind: ConfigMap
metadata:
  creationTimestamp: "2019-12-02T07:47:29Z"
  name: cluster-monitoring-config
  namespace: openshift-monitoring
  resourceVersion: "22110"
  selfLink: /api/v1/namespaces/openshift-monitoring/configmaps/cluster-monitoring-config
  uid: fd6d988b-14d7-11ea-84ff-066035b9efa8
.
.
.

```

編集後

```

.
.
.
.
apiVersion: v1
data:
  config.yaml: |
kind: ConfigMap
metadata:
  creationTimestamp: "2019-11-21T13:07:05Z"
  name: cluster-monitoring-config
  namespace: openshift-monitoring
  resourceVersion: "404352"
  selfLink: /api/v1/namespaces/openshift-monitoring/configmaps/cluster-monitoring-config
  uid: d12c796a-0c5f-11ea-9832-063cd735b81c
.
.
.

```

この例では、**alertmanagerMain** および **prometheusK8s** モニターリングコンポーネントは OpenShift Container Storage PVC を使用しています。

4. 関連する PVC を削除します。ストレージクラスを使用するすべての PVC を削除してください。

```
$ oc delete -n openshift-monitoring pvc <pvc-name> --wait=true --timeout=5m
```

### 4.3. OPENSIFT CONTAINER STORAGE からの OPENSIFT CONTAINER PLATFORM レジストリーの削除

OpenShift Container Storage から OpenShift Container Platform レジストリーをクリーンアップするには、手順のステップに従います。

代替ストレージを設定する必要がある場合、[イメージレジストリー](#) を参照してください。

OpenShift Container Platform レジストリーの設定の一部として作成される PVC は **openshift-image-registry** namespace に置かれます。

#### 前提条件

- イメージレジストリーは、OpenShift Container Storage PVC を使用するように設定する必要があります。

#### 手順

1. **configs.imageregistry.operator.openshift.io** オブジェクトを編集し、**storage** セクションのコンテンツを削除します。

```
$ oc edit configs.imageregistry.operator.openshift.io
```

<p>編集前</p> <pre> . . . storage:   pvc:     claim: registry-cephfs-rwx-pvc . . . </pre>
<p>編集後</p> <pre> . . . storage: . . . </pre>

この例では、PVC は **registry-cephfs-rwx-pvc** と呼ばれ、これは安全に削除できます。

2. PVC を削除します。

```
$ oc delete pvc <pvc-name> -n openshift-image-registry --wait=true --timeout=5m
```

## 4.4. OPENSIFT CONTAINER STORAGE からのクラスターロギング OPERATOR の削除

OpenShift Container Storage からクラスターロギングオペレーターを削除するには、手順のステップに従います。

クラスターロギング Operator の設定の一部として作成される PVC は **openshift-logging** namespace にあります。

### 前提条件

- クラスターロギングインスタンスは、OpenShift Container Storage PVC を使用するように設定する必要があります。

### 手順

1. namespace の **ClusterLogging** インスタンスを削除します。

```
$ oc delete clusterlogging instance -n openshift-logging --wait=true --timeout=5m
```

**openshift-logging** namespace の PVC は安全に削除できます。

2. PVC を削除します。

```
$ oc delete pvc <pvc-name> -n openshift-logging --wait=true --timeout=5m
```