Red Hat OpenShift Data Foundation 4.12

Deploying OpenShift Data Foundation using Red Hat Virtualization platform

Red Hat Virtualization Platform에 OpenShift Data Foundation을 배포하는 방법

Last Updated: 2023-09-19

Red Hat OpenShift Data Foundation 4.12 Deploying OpenShift Data Foundation using Red Hat Virtualization platform

Red Hat Virtualization Platform에 OpenShift Data Foundation을 배포하는 방법

법적 공지

초록

Red Hat Virtualization 플랫폼에 Red Hat OpenShift Container Platform을 사용하여 Red Hat OpenShift Data Foundation을 설치하는 방법에 대한 자세한 내용은 이 문서를 참조하십시오.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견을 보내 주십시오. 개선할 내용에 대해 알려주십시오. 피드백을 보내주시려면 다음을 확인하십시오.

- 특정 문구에 대한 간단한 의견 작성 방법은 다음과 같습니다.
  1. 문서가 *Multi-page HTML* 형식으로 표시되는지 확인합니다. 또한 문서 오른쪽 상단에 **피드백** 버튼이 있는지 확인합니다.
  2. 마우스 커서를 사용하여 주석 처리하려는 텍스트 부분을 강조 표시합니다.
  3. 강조 표시된 텍스트 아래에 표시되는 **피드백 추가** 팝업을 클릭합니다.
  4. 표시된 지침을 따릅니다.
- 보다 상세하게 피드백을 제출하려면 다음과 같이 Bugzilla 티켓을 생성하십시오.
  1. Bugzilla 웹 사이트로 이동하십시오.
  2. 구성 **요소** 섹션에서 **설명서**를 선택합니다.
  3. **설명** 필드에 문서 개선을 위한 제안 사항을 기입하십시오. 관련된 문서의 해당 부분 링크를 알려주십시오.
  4. **버그 제출**을 클릭합니다.

머리말

Red Hat OpenShift Data Foundation은 기존 Red Hat OpenShift Container Platform (RHOCP) Red Hat Virtualization 플랫폼 클러스터에서 배포를 지원합니다.

Red Hat Virtualization 설치 관리자 프로비저닝 인프라(IPI)에서 제공하는 공유 스토리지 장치를 사용하여 OpenShift Container Platform에 OpenShift Data Foundation을 배포하면 내부 클러스터 리소스를 생성할 수 있습니다.

또한 OpenShift Data Foundation을 사용하여 MCG(Multicloud Object Gateway) 구성 요소만 배포할 수 있습니다.

참고

Red Hat Virtualization 플랫폼에서는 내부 OpenShift Data Foundation 클러스터만 지원됩니다. 배포 요구 사항에 대한 자세한 내용은 배포 계획을 참조하십시오.

요구 사항에 따라 다음 배포 방법 중 하나를 수행합니다.

- 동적 스토리지 장치를 사용하여 OpenShift Data Foundation의 전체 배포를 위해 동적 스토리지 장치를 사용하여 배포 합니다.
- 로컬 스토리지 장치를 사용하여 OpenShift Data Foundation의 전체 배포를 위해 로컬 스토리지 장치를 사용하여 배포 합니다.
- OpenShift Data Foundation을 사용하여 Multicloud Object Gateway 구성 요소만 배포하기 위해 독립형 Multicloud Object Gateway 구성 요소를 배포 합니다.

1장. RED HAT VIRTUALIZATION 플랫폼을 사용하여 OPENSHIFT DATA FOUNDATION 배포 준비

동적 또는 로컬 스토리지를 사용하여 Red Hat OpenShift Data Foundation 배포를 시작하기 전에 리소스 요구 사항을 충족하는지 확인해야 합니다. 배포 계획을 참조하십시오.

1. 선택 사항: 외부 키 관리 시스템(KMS) HashiCorp Vault를 사용하여 클러스터 전체 암호화를 활성화하려면 다음 단계를 따르십시오.
   - 유효한 Red Hat OpenShift Data Foundation Advanced 서브스크립션이 있는지 확인합니다. OpenShift Data Foundation에 대한 서브스크립션이 작동하는 방법을 알아보려면 OpenShift Data Foundation 서브스크립션에 대한 지식 베이스 문서 를 참조하십시오.
   - 암호화를 위해 토큰 인증 방법을 선택하면 KMS를 사용하여 토큰 인증으로 클러스터 전체 암호화 활성화를 참조하십시오.
   - 암호화를 위해 Kubernetes 인증 방법을 선택하면 KMS를 사용하여 Kubernetes 인증으로 클러스터 전체 암호화 활성화를 참조하십시오.
   - Vault 서버에서 서명된 인증서를 사용하고 있는지 확인합니다.
2. 선택 사항: 외부 키 관리 시스템(KMS) Thales CipherTrust Manager를 사용하여 클러스터 전체 암호화를 활성화하려면 먼저 KMIP(키 관리 상호 운용성 프로토콜)를 활성화하고 서버에서 서명된 인증서를 사용해야 합니다. 다음 단계를 따릅니다:
   a. KMIP 클라이언트가 없는 경우 해당 클라이언트를 생성합니다. 사용자 인터페이스에서 **KMIP → 클라이언트 프로필 → 프로필 추가를** 선택합니다.
      i. 프로필 생성 중에 **CipherTrust** 사용자 이름을 **Common Name** 필드에 추가합니다.
   b. **KMIP → 등록 토큰 → 새로운 등록 토큰으로 이동하여 토큰**을 생성합니다. 다음 단계를 위해 토큰을 복사합니다.
   c. 클라이언트를 등록하려면 **KMIP → Registered Clients → Add Client** 로 이동합니다. 이름을 **지정합니다**. 이전 단계에서 **등록 토큰** 을 붙여넣은 다음 **저장을** 클릭합니다.
   d. 개인 키 저장을 클릭하고 인증서 **저장을 클릭하여 개인 키와** 클라이언트 **인증서를** 다운로드합니다.
   e. 새 KMIP 인터페이스를 생성하려면 **관리자 설정 → 인터페이스 → 인터페이스 추가로** 이동합니다.
      i. **KMIP 키 관리 상호 운용성 프로토콜**을 선택하고 **다음을** 클릭합니다.
      ii. 무료 **포트** 를 선택합니다.
      iii. **네트워크 인터페이스를 모두** 선택합니다.
      iv. **Interface Mode** 를 **TLS로 선택하고 클라이언트 인증서에서 가져온 사용자 이름, auth request는 선택 사항입니다**.
      v. (선택 사항) 키가 삭제될 때 메타데이터와 자료를 모두 삭제하도록 하드 삭제를 활성화할 수 있습니다. 이는 기본적으로 비활성화되어 있습니다.
      vi. 사용할 CA를 선택하고 **저장을** 클릭합니다.

f. 서버 CA 인증서를 가져오려면 새로 생성된 인터페이스 오른쪽에 **있는 작업 메뉴(ECDHE)**를 클릭하고 **인증서 다운로드**를 클릭합니다.

g. 선택 사항: 배포 중에 StorageClass 암호화를 사용하도록 설정하는 경우 KEK(키 암호화 키)로 작동할 키를 만듭니다.

i. **키 → 키 추가로** 이동합니다.

ii. **키 이름**을 입력합니다.

iii. **Algorithm** 및 **Size**를 각각 **AES** 및 **256**으로 설정합니다.

iv. **Pre-Active 상태에서 키 만들기**를 활성화하고 활성화할 날짜와 시간을 설정합니다.

v. **Key Usage**에서 **Encrypt** 및 **Decrypt**가 활성화되어 있는지 확인합니다.

vi. 배포 중에 사용할 새로 생성된 키의 ID를 복사합니다.

3. 최소 노드 시작 요구 사항
표준 배포 리소스 요구 사항이 충족되지 않으면 OpenShift Data Foundation 클러스터는 최소 구성으로 배포됩니다. 계획 가이드의 리소스 요구 사항 섹션을 참조하십시오.

4. 재해 복구 요구 사항 [기술 프리뷰]
Red Hat OpenShift Data Foundation에서 지원하는 재해 recovery 기능에는 재해 복구 솔루션을 성공적으로 구현하려면 다음 사전 요구 사항이 모두 필요합니다.

- 유효한 Red Hat OpenShift Data Foundation Advanced 서브스크립션
- 유효한 Red Hat Advanced Cluster Management for Kubernetes 서브스크립션
OpenShift Data Foundation에 대한 서브스크립션이 작동하는 방법을 알아보려면 OpenShift Data Foundation 서브스크립션에 대한 지식 베이스 문서를 참조하십시오.

자세한 요구 사항은 Red Hat Advanced Cluster Management for Kubernetes 문서의 OpenShift Data Foundation 재해 복구 가이드 *및 설치 가이드의 요구 사항 및 권장* 사항 섹션을 참조하십시오.

5. 로컬 스토리지 장치를 사용하여 OpenShift Data Foundation을 설치하기 위한 요구 사항이 충족되었는지 확인합니다.

1.1. 로컬 스토리지 장치를 사용하여 OPENSHIFT DATA FOUNDATION을 설치하기 위한 요구사항

노드 요구 사항

클러스터는 각각 로컬에 연결된 3개 이상의 OpenShift Container Platform 작업자 노드로 구성되어야 합니다.

- 선택한 세 개의 노드 각각을 사용할 수 있는 원시 블록 장치가 하나 이상 있어야 합니다.
OpenShift Data Foundation에서는 사용 가능한 하나 이상의 원시 블록 장치를 사용합니다.
- 사용하는 장치는 비어 있어야 합니다. 디스크에 남아 있는 물리 볼륨(PV), 볼륨 그룹(VG) 또는 논리 볼륨(LV)을 포함하지 않아야 합니다.

자세한 내용은 계획 가이드의 *리소스 요구 사항* 섹션을 참조하십시오.

재해 복구 요구 사항 [기술 프리뷰]

Red Hat OpenShift Data Foundation에서 지원하는 재해 recovery 기능에는 재해 복구 솔루션을 성공적으로 구현하려면 다음 사전 요구 사항이 모두 필요합니다.

- 유효한 Red Hat OpenShift Data Foundation Advanced 서브스크립션.
- Kubernetes용 유효한 RHACM(Red Hat Advanced Cluster Management) 서브스크립션입니다.

OpenShift Data Foundation에 대한 서브스크립션이 작동하는 방법을 자세히 알아보려면 OpenShift Data Foundation 서브스크립션에 대한 지식 베이스 문서 를 참조하십시오.

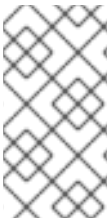
재해 복구 솔루션 요구 사항에 대한 자세한 내용은 OpenShift Data Foundation Disapplication for OpenShift Workloads 가이드 및 Red Hat Advanced Cluster Management for Kubernetes 문서의 설치 가이드 의 *요구 사항 및 권장* 사항 섹션을 참조하십시오.

Arbiter 확장 클러스터 요구 사항 [기술 프리뷰]

이 경우 단일 클러스터가 두 개의 영역으로 확장되고 세 번째 영역이 중재자의 위치로 확장됩니다. 이는 현재 OpenShift Container Platform 온프레미스 및 동일한 데이터 센터 내 배포를 위한 기술 프리뷰 기능입니다. 이 솔루션은 여러 데이터 센터 이상으로 확장되는 배포에는 권장되지 않습니다. 대신, Metro-DR을 여러 데이터 센터에 배포된 데이터 손실 DR 솔루션보다 낮은 대기 시간 네트워크를 제공하는 첫 번째 옵션으로 고려해 보십시오.

자세한 요구 사항 및 지침은 *클러스터 확장용 OpenShift Data Foundation 구성의* 지식베이스 문서 를 참조하십시오.

OpenShift Data Foundation에 대한 서브스크립션이 작동하는 방법을 자세히 알아보려면 OpenShift Data Foundation 서브스크립션에 대한 지식 베이스 문서 를 참조하십시오.



참고

hugeible scaling 및 Arbiter 모두 스케일링 논리와 충돌하는 동시에 활성화할 수 없습니다. 유연한 확장을 사용하면 OpenShift Data Foundation 클러스터에 한 번에 하나의 노드를 추가할 수 있습니다. 반면 Arbiter 클러스터에서는 두 데이터 영역 각각에 하나 이상의 노드를 추가해야 합니다.

최소 노드 시작 요구 사항

OpenShift Data Foundation 클러스터는 표준 배포의 리소스 요구 사항이 충족되지 않는 경우 최소 구성으로 배포됩니다.

자세한 내용은 계획 가이드의 *리소스 요구 사항* 섹션을 참조하십시오.

2장. 동적 스토리지 장치를 사용하여 배포

Red Hat Virtualization에서 제공하는 동적 스토리지 장치를 사용하여 OpenShift Container Platform에 OpenShift Data Foundation을 배포하면 내부 클러스터 리소스를 생성할 수 있습니다. 이로 인해 기본 서비스가 내부 프로비저닝되므로 애플리케이션에서 추가 스토리지 클래스를 사용할 수 있습니다.

동적 스토리지 장치를 사용하여 배포하는 다음 단계를 진행하기 전에 OpenShift Data Foundation 배포 준비 장을 처리했는지 확인하십시오.

1. Red Hat OpenShift Data Foundation Operator를 설치합니다.
2. OpenShift Data Foundation 클러스터를 생성합니다.

2.1. RED HAT OPENSHIFT DATA FOUNDATION OPERATOR 설치

Red Hat OpenShift Container Platform Operator Hub를 사용하여 Red Hat OpenShift Data Foundation Operator를 설치할 수 있습니다.

사전 요구 사항

- **cluster-admin** 및 Operator 설치 권한이 있는 계정을 사용하여 OpenShift Container Platform 클러스터에 액세스할 수 있습니다.
- Red Hat OpenShift Container Platform 클러스터에 3개 이상의 작업자 노드가 있어야 합니다.
- 추가 리소스 요구 사항은 배포 계획 가이드를 참조하십시오.

중요

- OpenShift Data Foundation에 대한 클러스터 전체 기본 노드 선택기를 재정의해야 하는 경우 다음 명령을 사용하여 **openshift-storage** 네임스페이스에 빈 노드 선택기를 지정할 수 있습니다(이 경우 **openshift-storage** 네임스페이스 생성).

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

- 노드에 Red Hat OpenShift Data Foundation 리소스만 예약되도록 **infra** 테인트를 구성합니다. 이를 통해 서브스크립션 비용을 절감할 수 있습니다. 자세한 내용은 스토리지 리소스 관리 및 할당 가이드의 *Red Hat OpenShift Data Foundation 전용 작업자 노드를 사용하는 방법을* 참조하십시오.

절차

1. OpenShift 웹 콘솔에 로그인합니다.
2. **Operators → OperatorHub**를 클릭합니다.
3. **OpenShift Data Foundation**을 **키워드로 필터링** 상자에 스크롤하여 **OpenShift Data Foundation** Operator를 찾습니다.
4. **설치**를 클릭합니다.
5. **Operator 설치** 페이지에서 다음 옵션을 설정합니다.
   a. **stable-4.12** 로 채널을 업데이트합니다.

b. 설치 모드에서 **클러스터의 특정 네임스페이스**를 선택합니다.

c. 설치된 네임스페이스에서 **Operator 권장 네임스페이스 openshift-storage**를 선택합니다. 네임스페이스 **openshift-storage**가 없으면 Operator 설치 중에 생성됩니다.

d. 승인 전략을 **자동** 또는 **수동**으로 선택합니다.
자동 업데이트를 선택하면 OLM(Operator Lifecycle Manager)은 개입 없이 Operator의 실행 중인 인스턴스를 자동으로 업그레이드합니다.

수동 업데이트를 선택하면 OLM에서 업데이트 요청을 생성합니다. 클러스터 관리자는 Operator를 최신 버전으로 업데이트하기 위해 해당 업데이트 요청을 수동으로 승인해야 합니다.

e. **Console 플러그인**에 대해 **Enable** 옵션이 선택되어 있는지 확인합니다.

f. **설치**를 클릭합니다.

검증 단계

- Operator가 성공적으로 설치되면 메시지가 포함된 팝업 **Web console update is available**이 사용자 인터페이스에 표시됩니다. 콘솔 변경 사항을 반영하려면 이 팝업 창에서 **웹 콘솔 새로 고침**을 클릭합니다.
- 웹 콘솔에서 다음을 수행합니다.
  - Installed Operators로 이동하여 **OpenShift Data Foundation** Operator에 설치에 성공했음을 나타내는 녹색 눈금이 표시되는지 확인합니다.
  - **Storage** 로 이동하여 **Data Foundation** 대시보드를 사용할 수 있는지 확인합니다.

2.2. 토큰 인증 방법을 사용하여 KMS로 클러스터 전체 암호화 활성화

토큰 인증을 위해 자격 증명 모음에서 키 값 백엔드 경로 및 정책을 활성화할 수 있습니다.

사전 요구 사항

- 자격 증명 모음에 대한 관리자 액세스.
- 유효한 Red Hat OpenShift Data Foundation Advanced 서브스크립션. 자세한 내용은 OpenShift Data Foundation 서브스크립션에 대한 지식 베이스 문서 를 참조하십시오.
- 나중에 변경할 수 없으므로 이름 지정 규칙을 따르는 백엔드 **경로로** 고유한 경로 이름을 선택하십시오.

절차

1. 자격 증명 모음에서 KV(키/값) 백엔드 경로를 활성화합니다.
자격 증명 모음 KV 시크릿 엔진 API의 경우 버전 1

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

자격 증명 모음 KV 시크릿 엔진 API의 경우 버전 2

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

2. 시크릿에서 쓰기 또는 삭제 작업을 수행하도록 사용자를 제한하는 정책을 생성합니다.

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

3. 위 정책과 일치하는 토큰을 생성합니다.

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

2.3. KUBERNETES 인증 방법을 사용하여 KMS로 클러스터 전체 암호화 활성화

KMS(Key Management System)를 사용하여 클러스터 전체의 암호화에 대해 Kubernetes 인증 방법을 활성화할 수 있습니다.

사전 요구 사항

- Vault에 대한 관리자 액세스 권한이 있어야 합니다.
- 유효한 Red Hat OpenShift Data Foundation Advanced 서브스크립션. 자세한 내용은 OpenShift Data Foundation 서브스크립션에 대한 지식 베이스 문서 를 참조하십시오.
- OpenShift Data Foundation Operator는 Operator Hub에서 설치해야 합니다.
- 이름 지정 규칙을 따르는 백엔드 경로로 고유한 **경로** 이름을 신중하게 선택합니다. 이 경로 이름은 나중에 변경할 수 없습니다.

절차

1. 서비스 계정을 생성합니다.

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

여기서 &***lt;serviceaccount_name&***gt;은 서비스 계정의 이름을 지정합니다.

예를 들면 다음과 같습니다.

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

2. **clusterrolebindings** 및 **clusterroles** 를 생성합니다.

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

예를 들면 다음과 같습니다.

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

3. **serviceaccount** 토큰 및 CA 인증서에 대한 시크릿을 생성합니다.

```
$ 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
```

여기서 &***lt;serviceaccount_name***>은 이전 단계에서 생성한 서비스 계정입니다.

4. 시크릿에서 토큰과 CA 인증서를 가져옵니다.

```
$ 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 클러스터 끝점을 검색합니다.

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

6. 서비스 계정 발행자를 가져옵니다.

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

7. 이전 단계에서 수집한 정보를 사용하여 Vault에서 Kubernetes 인증 방법을 설정합니다.

```
$ 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"
```

중요

발행자가 비어 있을 때 Vault에서 Kubernetes 인증 방법을 구성하려면 다음을 수행합니다.

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

8. Vault에서 KV(Key/Value) 백엔드 경로를 활성화합니다.
   Vault KV 시크릿 엔진 API의 경우 버전 1:

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

   Vault KV 시크릿 엔진 API의 경우 버전 2:

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

9. 시크릿에서 **쓰기** 또는 **삭제** 작업을 수행하도록 사용자를 제한하는 정책을 생성합니다.

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

10. 역할을 생성합니다.

```
$ 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
```

   스토리지 시스템 생성 중에 KMS 연결 세부 정보를 구성하는 동안 **odf-rook-ceph-op** 역할이 나중에 사용됩니다.

```
$ 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 클러스터 생성

OpenShift Data Foundation Operator를 설치한 후 OpenShift Data Foundation 클러스터를 생성합니다.

사전 요구 사항

- OpenShift Data Foundation Operator는 Operator Hub에서 설치해야 합니다. 자세한 내용은 OpenShift Data Foundation Operator설치를 참조하십시오.

절차

1. OpenShift 웹 콘솔에서 **Operator → 설치된 Operator**를 클릭하여 설치된 모든 Operator를 확인합니다.
   선택한 **프로젝트**가 **openshift-storage** 인지 확인합니다.
2. **OpenShift Data Foundation** Operator를 클릭한 다음 **스토리지 시스템 만들기**를 클릭합니다.
3. **백업 스토리지** 페이지에서 다음을 선택합니다.
   a. **배포 유형** 옵션에 대해 **Full Deployment**를 선택합니다.
   b. **기존 스토리지 클래스 사용** 옵션을 선택합니다.
   c. **다음**을 클릭합니다.
4. **용량 및 노드** 페이지에서 필요한 정보를 제공합니다.
   a. 드롭다운 목록에서 **요청 용량** 값을 선택합니다. 기본적으로 **2TiB**로 설정됩니다.

   참고

   초기 스토리지 용량을 선택하면 선택한 사용 가능한 용량(원시 스토리지의 3배)만을 사용하여 클러스터 확장이 수행됩니다.

   b. **노드 선택** 섹션에서 사용 가능한 노드를 3개 이상 선택합니다.
   c. 선택 사항: **Taint nodes** 확인란을 선택하여 OpenShift Data Foundation에 대해 선택한 노드를 전용으로 지정합니다.
   d. **다음**을 클릭합니다.
5. 선택 사항: **보안 및 네트워크** 페이지에서 요구 사항에 따라 다음을 구성합니다.
   a. 암호화를 활성화하려면 **블록 및 파일 스토리지에 데이터 암호화 사용**을 선택합니다.
   b. 암호화 수준을 하나 또는 둘 다 선택합니다.
      - **클러스터 전체 암호화**
        전체 클러스터(블록 및 파일)를 암호화합니다.
      - **스토리지 클래스 암호화**
        암호화 활성화된 스토리지 클래스를 사용하여 암호화된 영구 볼륨(블록만 해당)을 생성합니다.
   c. 선택 사항: **외부 키 관리 서비스에 연결** 확인란을 선택합니다. 이는 클러스터 전체 암호화의 경우 선택 사항입니다.
      i. **Key Management Service Provider** 드롭다운 목록에서 **Vault** 또는 **Thales CipherTrust Manager (KMIP 사용)** 를 선택합니다. **Vault** 를 선택한 경우 다음 단계로 이동합니다. **Thales CipherTrust Manager (KMIP 사용)** 를 선택한 경우 iii 단계로 이동합니다.
      ii. **인증 방법**을 선택합니다.

토큰 인증 방법 사용

- 고유한 **연결 이름**, Vault 서버의 호스트 **주소** (https://<hostname 또는 ip>'), **포트** 번호 및 **토큰** 을 입력합니다.
- **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
  - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
  - 선택 사항: **TLS 서버 이름** 및 **Vault Enterprise 네임스페이스** 를 입력합니다.
  - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키**를 제공합니다.
  - **저장을** 클릭하고 iv 단계로 건너뜁니다.

Kubernetes 인증 방법 사용

- 고유한 Vault **연결 이름**, Vault 서버의 호스트 **주소** ('https://<hostname 또는 ip>'), **포트** 번호 및 **역할** 이름을 입력합니다.
- **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
  - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
  - 선택 사항: 해당하는 경우 **TLS 서버 이름** 및 **인증** 경로를 입력합니다.
  - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키**를 제공합니다.
  - **저장을** 클릭하고 iv 단계로 건너뜁니다.

iii. KMS 공급자로 **Thales CipherTrust Manager (KMIP 사용)** 를 사용하려면 다음 단계를 따르십시오.

A. 프로젝트 내에서 키 관리 서비스에 대한 고유한 **연결** 이름을 입력합니다.

B. **주소** 및 **포트** 섹션에서 Thales CipherTrust Manager의 IP와 KMIP 인터페이스가 활성화된 포트를 입력합니다. 예를 들면 다음과 같습니다.

- **주소**: 12.34.3.2
- **포트**:ECDHE96

C. **클라이언트 인증서**,**CA 인증서** 및 **클라이언트 개인 키를 업로드합니다**.

D. StorageClass 암호화가 활성화된 경우 위에서 생성된 암호화 및 암호 해독에 사용할 고유 식별자를 입력합니다.

E. **TLS Server** 필드는 선택 사항이며 KMIP 엔드포인트에 대한 DNS 항목이 없는 경우 사용됩니다. 예를 들어, **kmip_all_<port>.ciphertrustmanager.local**.

iv. 네트워크를 **선택합니다**.

v. **다음**을 클릭합니다.

6. **검토 및 생성** 페이지에서 구성 세부 정보를 검토합니다.
   구성 설정을 수정하려면 **뒤로**를 클릭합니다.

7. **스토리지 시스템 생성**을 클릭합니다.

검증 단계

- 설치된 스토리지 클러스터의 최종 상태를 확인하려면 다음을 수행합니다.

  a. OpenShift 웹 콘솔에서 **설치된 Operator → OpenShift Data Foundation → 스토리지 시스템 → ocs-storagecluster-storagesystem → Resources** 로 이동합니다.

  b. **StorageCluster**의 **Status**가 **Ready** 이고 옆에 녹색 눈금이 표시되어 있는지 확인합니다.

- OpenShift Data Foundation의 모든 구성 요소가 설치되었는지 확인하려면 OpenShift Data Foundation 배포 확인을 참조하십시오.

추가 리소스

Overprovision Control 경고를 활성화하려면 모니터링 가이드의 경고를 참조하십시오.

3장. 로컬 스토리지 장치를 사용하여 배포

로컬 스토리지 장치를 사용하여 OpenShift Container Platform에 OpenShift Data Foundation을 배포하면 내부 클러스터 리소스를 생성할 수 있는 옵션이 제공됩니다. 이로 인해 기본 서비스가 내부 프로비저닝되므로 애플리케이션에서 추가 스토리지 클래스를 사용할 수 있습니다.

이 섹션을 사용하여 OpenShift Container Platform이 이미 설치된 Red Hat Virtualization에 OpenShift Data Foundation을 배포합니다.

또한 다음 단계를 진행하기 전에 OpenShift Data Foundation 배포 준비 에 있는 요구 사항을 해결했는지 확인하십시오.

1. 로컬 스토리지 Operator 설치
2. Red Hat OpenShift Data Foundation Operator를 설치합니다 .
3. OpenShift Data Foundation 클러스터를 생성합니다 .

3.1. 로컬 스토리지 OPERATOR 설치

로컬 스토리지 장치에서 Red Hat OpenShift Data Foundation 클러스터를 생성하기 전에 Operator Hub에서 Local Storage Operator를 설치합니다.

절차

1. OpenShift 웹 콘솔에 로그인합니다.
2. **Operators → OperatorHub**를 클릭합니다.
3. **키워드로 필터링**상자에 **로컬 스토리지** 를 입력하여 운영자 목록에서 **Local Storage Operator** 를 찾은 다음 클릭합니다.
4. **Operator 설치** 페이지에서 다음 옵션을 설정합니다.
   a. **4.12** 또는 **stable** 로 채널을 업데이트합니다.
   b. 설치 모드에서 **클러스터의 특정 네임스페이스**를 선택합니다.
   c. 설치된 네임스페이스를 **Operator 권장 네임스페이스 openshift-local-storage**를 선택합니다.
   d. 승인을 **자동**으로 업데이트합니다.
5. **설치**를 클릭합니다.

검증 단계

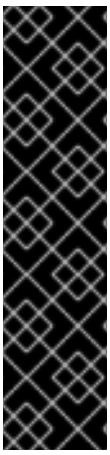
- Local Storage Operator에 성공적인 설치를 나타내는 녹색 눈금이 표시되는지 확인합니다.

3.2. RED HAT OPENSHIFT DATA FOUNDATION OPERATOR 설치

Red Hat OpenShift Container Platform Operator Hub를 사용하여 Red Hat OpenShift Data Foundation Operator를 설치할 수 있습니다.

사전 요구 사항

- **cluster-admin** 및 Operator 설치 권한이 있는 계정을 사용하여 OpenShift Container Platform 클러스터에 액세스할 수 있습니다.
- Red Hat OpenShift Container Platform 클러스터에 3개 이상의 작업자 노드가 있어야 합니다.
- 추가 리소스 요구 사항은 배포 계획 가이드를 참조하십시오.



중요

- OpenShift Data Foundation에 대한 클러스터 전체 기본 노드 선택기를 재정의해야 하는 경우 다음 명령을 사용하여 **openshift-storage** 네임스페이스에 빈 노드 선택기를 지정할 수 있습니다(이 경우 **openshift-storage** 네임스페이스 생성).

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

- 노드에 Red Hat OpenShift Data Foundation 리소스만 예약되도록 **infra** 테인트를 구성합니다. 이를 통해 서브스크립션 비용을 절감할 수 있습니다. 자세한 내용은 스토리지 리소스 관리 및 할당 가이드의 *Red Hat OpenShift Data Foundation 전용 작업자 노드를 사용하는 방법을* 참조하십시오.

절차

1. OpenShift 웹 콘솔에 로그인합니다.
2. **Operators → OperatorHub**를 클릭합니다.
3. **OpenShift Data Foundation**을 **키워드로 필터링** 상자에 스크롤하여 **OpenShift Data Foundation** Operator를 찾습니다.
4. **설치**를 클릭합니다.
5. **Operator 설치** 페이지에서 다음 옵션을 설정합니다.
   a. **stable-4.12** 로 채널을 업데이트합니다.
   b. 설치 모드에서 **클러스터의 특정 네임스페이스**를 선택합니다.
   c. 설치된 네임스페이스에서 **Operator 권장 네임스페이스 openshift-storage**를 선택합니다. 네임스페이스 **openshift-storage**가 없으면 Operator 설치 중에 생성됩니다.
   d. 승인 전략을 **자동** 또는 **수동**으로 선택합니다.
   자동 업데이트를 선택하면 OLM(Operator Lifecycle Manager)은 개입 없이 Operator의 실행 중인 인스턴스를 자동으로 업그레이드합니다.

   수동 업데이트를 선택하면 OLM에서 업데이트 요청을 생성합니다. 클러스터 관리자는 Operator를 최신 버전으로 업데이트하기 위해 해당 업데이트 요청을 수동으로 승인해야 합니다.
   e. **Console 플러그인**에 대해 **Enable** 옵션이 선택되어 있는지 확인합니다.
   f. **설치**를 클릭합니다.

검증 단계

- Operator가 성공적으로 설치되면 메시지가 포함된 팝업 **Web console update is available**이 사용자 인터페이스에 표시됩니다. 콘솔 변경 사항을 반영하려면 이 팝업 창에서 **웹 콘솔 새로 고침**을 클릭합니다.
- 웹 콘솔에서 다음을 수행합니다.
  - Installed Operators로 이동하여 **OpenShift Data Foundation** Operator에 설치에 성공했음을 나타내는 녹색 눈금이 표시되는지 확인합니다.
  - **Storage** 로 이동하여 **Data Foundation** 대시보드를 사용할 수 있는지 확인합니다.

3.3. RED HAT VIRTUALIZATION 플랫폼에서 OPENSHIFT DATA FOUNDATION 클러스터 생성

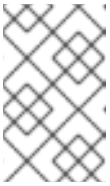
OpenShift Data Foundation Operator를 설치한 후 로컬 스토리지 장치를 사용하여 OpenShift Data Foundation 클러스터를 생성하려면 다음 절차를 사용하십시오.

사전 요구 사항

- OpenShift Data Foundation Operator는 Operator Hub에서 설치해야 합니다. 자세한 내용은 OpenShift Data Foundation Operator 설치 를 참조하십시오.
- 로컬 스토리지 장치 섹션을 사용하여 OpenShift Data Foundation 설치 요구 사항 의 모든 요구 사항이 충족되었는지 확인합니다.

절차

1. OpenShift 웹 콘솔에서 **Operator → 설치된 Operator**를 클릭하여 설치된 모든 Operator를 확인합니다.
   선택한 **프로젝트**가 **openshift-storage** 인지 확인합니다.
2. **OpenShift Data Foundation** Operator를 클릭한 다음 **스토리지 시스템 만들기**를 클릭합니다.
3. 백업 스토리지 페이지에서 다음을 수행합니다.
   a. **배포 유형** 옵션에 대해 **Full Deployment**를 선택합니다.
   b. **로컬 스토리지 장치 옵션을 사용하여 새 StorageClass 만들기**옵션을 선택합니다.
   c. 다음을 클릭합니다.

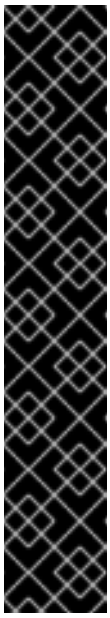


참고

아직 설치되지 않은 경우 Local Storage Operator를 설치하라는 메시지가 표시됩니다. **설치**를 클릭하고 Local Storage Operator 설치 에 설명된 절차를 따릅니다.

4. 로컬 볼륨 세트 생성 페이지에서 다음 정보를 제공합니다.
   a. **로컬 볼륨 세트**의 이름과 **스토리지 클래스**를 입력합니다.
   기본적으로 스토리지 클래스 이름에 로컬 볼륨 세트 이름이 표시됩니다. 이름을 변경할 수 있습니다.
   b. 다음 중 하나를 선택합니다.

- **모든 노드의 디스크**는 모든 노드에서 선택한 필터와 일치하는 사용 가능한 디스크를 사용합니다.
- **선택한 노드의 디스크**가 선택한 노드에서만 선택한 필터와 일치하는 사용 가능한 디스크를 사용합니다.



중요

- 3개 이상의 노드로 생성한 스토리지 클러스터가 3개 이상의 가용성 영역의 최소 요구 사항보다 적은 경우에만 유연한 확장 기능을 사용할 수 있습니다.
  유연한 확장에 대한 자세한 내용은 유연한 확장이 가능한 *경우 YAML을 사용하여 OpenShift Data Foundation 클러스터 확장에 대한 지식 베이스 문서를 참조하십시오*.
- 배포 시 유연한 확장 기능을 사용하도록 설정하고 나중에 활성화하거나 비활성화할 수 없습니다.
- 선택한 노드가 집계된 30 개의 CPU 및 72GiB RAM의 OpenShift Data Foundation 클러스터 요구 사항과 일치하지 않으면 최소 클러스터가 배포됩니다.
  최소 노드 요구 사항은 계획 가이드의 리소스 요구 사항 섹션을 참조하십시오.

c. 사용 가능한 **디스크 유형** 목록에서 **SSD/NVMe**을 선택합니다.

d. **고급** 섹션을 확장하고 다음 옵션을 설정합니다.

볼륨 모드	블록은 기본적으로 선택됩니다.
장치 유형	드롭다운 목록에서 하나 이상의 장치 유형을 선택합니다.
디스크 크기	장치에 대해 최소 크기 100GB와 포함되어야 하는 장치의 사용 가능한 최대 크기를 설정합니다.
최대 디스크 제한	이는 노드에서 생성할 수 있는 최대 PV 수를 나타냅니다. 이 필드가 비어 있으면 일치하는 노드에서 사용 가능한 모든 디스크에 PV가 생성됩니다.

e. **다음**을 클릭합니다.
로컬 볼륨 세트 생성이 표시되는지 확인하는 팝업이 표시됩니다.

f. 계속하려면 **예**를 클릭합니다.

1. **용량 및 노드 페이지에서** 다음을 구성합니다.

a. **사용 가능한 원시 용량**은 스토리지 클래스와 연결된 모든 디스크에 따라 용량 값으로 채워집니다. 이 작업을 수행하는 데 시간이 다소 걸립니다. **선택한 노드** 목록에는 스토리지 클래스를 기반으로 하는 노드가 표시됩니다.

b. 선택 사항: **Taint nodes** 확인란을 선택하여 OpenShift Data Foundation에 대해 선택한 노드를 전용으로 지정합니다.

c. **다음**을 클릭합니다.

2. 선택 사항: 보안 및 네트워크 페이지에서 요구 사항에 따라 다음을 구성합니다.

   a. 암호화를 활성화하려면 **블록 및 파일 스토리지에 데이터 암호화 사용**을 선택합니다.

   b. 다음 **암호화 수준** 중 하나를 선택합니다.

      - **전체 클러스터를 암호화**하는 클러스터 전체 (블록 및 파일) 암호화
      - 암호화가 활성화된 스토리지 클래스를 사용하여 암호화된 영구 볼륨(블록만 해당)을 생성하는 **스토리지 클래스 암호화**입니다.

   c. 선택 사항: **외부 키 관리 서비스에 연결** 확인란을 선택합니다. 이는 클러스터 전체 암호화의 경우 선택 사항입니다.

      i. **Key Management Service Provider** 드롭다운 목록에서 **Vault** 또는 **Thales CipherTrust Manager (KMIP 사용)** 를 선택합니다. **Vault** 를 선택한 경우 다음 단계로 이동합니다. **Thales CipherTrust Manager (KMIP 사용)** 를 선택한 경우 iii 단계로 이동합니다.

      ii. **인증 방법**을 선택합니다.

      토큰 인증 방법 사용

      - 고유한 **연결 이름**, Vault 서버의 호스트 **주소** (https://<hostname 또는 ip>'), **포트** 번호 및 **토큰** 을 입력합니다.
      - **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
        - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
        - 선택 사항: **TLS 서버 이름** 및 **Vault Enterprise 네임스페이스** 를 입력합니다.
        - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키**를 제공합니다.
        - **저장을** 클릭하고 iv 단계로 건너뜁니다.

      Kubernetes 인증 방법 사용

      - 고유한 Vault **연결 이름**, Vault 서버의 호스트 **주소** ('https://<hostname 또는 ip>'), **포트** 번호 및 **역할** 이름을 입력합니다.
      - **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
        - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
        - 선택 사항: 해당하는 경우 **TLS 서버 이름** 및 **인증** 경로를 입력합니다.
        - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키**를 제공합니다.
        - **저장을** 클릭하고 iv 단계로 건너뜁니다.

      iii. KMS 공급자로 **Thales CipherTrust Manager (KMIP 사용)** 를 사용하려면 다음 단계를 따르십시오.

A. 프로젝트 내에서 키 관리 서비스에 대한 고유한 **연결** 이름을 입력합니다.

B. **주소** 및 **포트** 섹션에서 Thales CipherTrust Manager의 IP와 KMIP 인터페이스가 활성화된 포트를 입력합니다. 예를 들면 다음과 같습니다.

- **주소**: 12.34.3.2
- **포트**:ECDHE96

C. **클라이언트 인증서**,**CA 인증서** 및 **클라이언트 개인 키를 업로드합니다**.

D. StorageClass 암호화가 활성화된 경우 위에서 생성된 암호화 및 암호 해독에 사용할 고유 식별자를 입력합니다.

E. **TLS Server** 필드는 선택 사항이며 KMIP 엔드포인트에 대한 DNS 항목이 없는 경우 사용됩니다. 예를 들어, **kmip_all_<port>.ciphertrustmanager.local**.

iv. 네트워크를 **선택합니다**.

a. **다음**을 클릭합니다.

1. 검토 및 생성 페이지에서 구성 세부 정보를 검토합니다.
   - 구성 설정을 수정하려면 **뒤로** 이동하여 이전 구성 페이지로 돌아갑니다.
2. **스토리지 시스템 생성**을 클릭합니다.

검증 단계

- 설치된 스토리지 클러스터의 최종 상태를 확인하려면 다음을 수행합니다.
  a. OpenShift 웹 콘솔에서 **설치된 Operator → OpenShift Data Foundation → 스토리지 시스템 → ocs-storagecluster-storagesystem → Resources** 로 이동합니다.
  b. **StorageCluster**의 **Status**가 **Ready** 이고 옆에 녹색 눈금이 표시되어 있는지 확인합니다.
- 스토리지 클러스터에서 유연한 확장이 활성화되어 있는지 확인하려면 다음 단계를 수행합니다 (rbiter 모드의 경우 유연한 확장은 비활성화됨).
  1. OpenShift 웹 콘솔에서 **설치된 Operator → OpenShift Data Foundation → 스토리지 시스템 → ocs-storagecluster-storagesystem → Resources** 로 이동합니다.
  2. YAML 탭의 **spec** 섹션에서 **flexibleScaling** 키를 검색하고 **status** 섹션에서 **failureDomain**을 검색합니다. **유연한 확장이 true** 이고 **failureDomain** 이 **호스트** 로 설정된 경우 유연한 확장 기능이 활성화됩니다.

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

- OpenShift Data Foundation의 모든 구성 요소가 성공적으로 설치되었는지 확인하려면 OpenShift Data Foundation 배포 확인 을 참조하십시오.

추가 리소스

- 초기 클러스터의 용량을 확장하려면 스토리지 확장을 참조하십시오.

4장. OPENSHIFT DATA FOUNDATION 배포 확인

이 섹션을 사용하여 OpenShift Data Foundation이 올바르게 배포되었는지 확인합니다.

4.1. POD 상태 확인

절차

1. OpenShift 웹 콘솔에서 **워크로드 → Pod**를 클릭합니다.
2. **프로젝트** 드롭다운 목록에서 **openshift-storage** 를 선택합니다.

참고

기본 프로젝트 표시 옵션이 비활성화된 경우 토글 버튼을 사용하여 모든 기본 프로젝트를 나열합니다.

각 구성 요소에 대해 예상되는 Pod 수 및 노드 수에 따라 달라지는 방법에 대한 자세한 내용은 표 4.1. "OpenShift Data Foundation 클러스터에 해당하는 Pod" 을 참조하십시오.

3. **실행** 및 **완료** 탭을 클릭하여 다음 Pod가 **Running** 및 **Completed** 상태인지 확인합니다.

표 4.1. OpenShift Data Foundation 클러스터에 해당하는 Pod

구성 요소	해당 Pod
OpenShift Data Foundation Operator	• **OCS-operator-*** (모든 작업자 노드에 1 Pod) • **OCS-metrics-exporter-*** (모든 작업자 노드에 1 Pod) • **ODF-operator-controller-manager-*** (모든 작업자 노드에 1 Pod) • **ODF-console-*** (모든 작업자 노드에 1 Pod) • **CSI-addons-controller-manager-*** (모든 작업자 노드의 Pod)
Rook-ceph Operator	**Rook-ceph-operator-*** (모든 작업자 노드에 1 Pod)

구성 요소	해당 Pod
Multicloud Object Gateway	• **NooBaa-operator-*** (모든 작업자 노드에 1 Pod) • **NooBaa-core-*** (모든 스토리지 노드에 1 Pod) • **NooBaa-db-pg-*** (모든 스토리지 노드에 1 Pod) • **NooBaa-endpoint-*** (모든 스토리지 노드에 1 Pod)
MON	**rook-ceph-mon-*** (스토리지 노드에 분산된 3 Pod)
MGR	**rook-ceph-mgr-*** (모든 스토리지 노드에 1 Pod)
MDS	**rook-ceph-mds-ocs-storagecluster-cephfilesystem-*** (스토리지 노드에 분산된 2 Pod)
RGW	**rook-ceph-rgw-ocs-storagecluster-cephobjectstore-*** (모든 스토리지 노드에 1 Pod)

CSI	• **cephfs**
	  ◦ **CSI-cephfsplugin-*** (모든 작업자 노드에 1 Pod)
	  ◦ **CSI-cephfsplugin-provisioner-*** (작업자 노드에 분산된 2 Pod)
	• **rbd**
	  ◦ **CSI-rbdplugin-*** (각 작업자 노드에서 1 Pod)
	  ◦ **CSI-rbdplugin-provisioner-*** (2 작업자 노드에 분산된 2 Pod)

rook-ceph-crashcollector	**rook-ceph-crashcollector-*** (각 스토리지 노드에서 1 pod)

구성 요소	해당 Pod
OSD	• **rook-ceph-osd-*** (각 장치의 1 Pod) • **rook-ceph-osd-prepare-ocs-deviceset-*** (각 장치의 1 Pod)

4.2. OPENSHIFT DATA FOUNDATION 클러스터 상태 확인

절차

1. OpenShift 웹 콘솔에서 **스토리지 → Data Foundation** 을 클릭합니다.
2. **개요** 탭의 **상태** 카드에서 **스토리지 시스템**을 클릭한 다음 해당 팝업에서 스토리지 시스템 링크를 클릭합니다.
3. **블록 및 파일** 탭의 **상태** 카드에서 *스토리지 클러스터*에 녹색 체크 표시가 있는지 확인합니다.
4. **세부 정보** 카드에서 클러스터 정보가 표시되는지 확인합니다.

블록 및 파일 대시보드를 사용하는 OpenShift Data Foundation 클러스터의 상태에 대한 자세한 내용은 OpenShift Data Foundation 모니터링 을 참조하십시오.

4.3. MULTICLOUD OBJECT GATEWAY의 상태 확인

절차

1. OpenShift 웹 콘솔에서 **스토리지 → Data Foundation** 을 클릭합니다.
2. **개요** 탭의 **상태** 카드에서 **스토리지 시스템**을 클릭한 다음 해당 팝업에서 스토리지 시스템 링크를 클릭합니다.
   a. **Object** 탭의 **상태 카드**에서 *Object Service* 및 *Data Resiliency* 모두 녹색 눈금이 있는지 확인합니다.
   b. **세부 정보** 카드에 MCG 정보가 표시되는지 확인합니다.

오브젝트 서비스 대시보드를 사용하는 OpenShift Data Foundation 클러스터의 상태에 대한 자세한 내용은 Monitoring OpenShift Data Foundation 을 참조하십시오.

4.4. 특정 스토리지 클래스가 있는지 확인

절차

1. OpenShift 웹 콘솔의 왼쪽 창에서 **스토리지 → 스토리지 클래스**를 클릭합니다.
2. OpenShift Data Foundation 클러스터 생성과 함께 다음 스토리지 클래스가 생성되었는지 확인합니다.
   - **ocs-storagecluster-ceph-rbd**
   - **ocs-storagecluster-cephfs**

- **openshift-storage.noobaa.io**
- **ocs-storagecluster-ceph-rgw**

5장. 독립 실행형 MULTICLOUD OBJECT GATEWAY 배포

OpenShift Data Foundation을 사용하여 Multicloud Object Gateway 구성 요소만 배포하면 배포 유연성을 제공하고 리소스 소비를 줄이는 데 도움이 됩니다. 동적 스토리지 장치를 사용하거나 로컬 스토리지 장치를 사용하여 Multicloud Object Gateway 구성 요소를 배포할 수 있습니다.

5.1. 동적 스토리지 장치를 사용하여 독립 실행형 MULTICLOUD OBJECT GATEWAY 배포

다음 단계를 포함하는 독립 실행형 Multicloud Object Gateway 구성 요소만 배포하려면 이 섹션을 사용합니다.

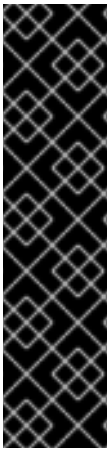
- Red Hat OpenShift Data Foundation Operator 설치
- 독립 실행형 Multicloud Object Gateway 생성

5.1.1. Red Hat OpenShift Data Foundation Operator 설치

Red Hat OpenShift Container Platform Operator Hub를 사용하여 Red Hat OpenShift Data Foundation Operator를 설치할 수 있습니다.

사전 요구 사항

- **cluster-admin** 및 Operator 설치 권한이 있는 계정을 사용하여 OpenShift Container Platform 클러스터에 액세스할 수 있습니다.
- Red Hat OpenShift Container Platform 클러스터에 3개 이상의 작업자 노드가 있어야 합니다.
- 추가 리소스 요구 사항은 배포 계획 가이드를 참조하십시오.



중요

- OpenShift Data Foundation에 대한 클러스터 전체 기본 노드 선택기를 재정의해야 하는 경우 다음 명령을 사용하여 **openshift-storage** 네임스페이스에 빈 노드 선택기를 지정할 수 있습니다(이 경우 **openshift-storage** 네임스페이스 생성).

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

- 노드에 Red Hat OpenShift Data Foundation 리소스만 예약되도록 **infra** 테인트를 구성합니다. 이를 통해 서브스크립션 비용을 절감할 수 있습니다. 자세한 내용은 스토리지 리소스 관리 및 할당 가이드의 *Red Hat OpenShift Data Foundation 전용 작업자 노드를 사용하는 방법을* 참조하십시오.

절차

1. OpenShift 웹 콘솔에 로그인합니다.
2. **Operators → OperatorHub**를 클릭합니다.
3. **OpenShift Data Foundation**을 **키워드로 필터링** 상자에 스크롤하여 **OpenShift Data Foundation** Operator를 찾습니다.
4. **설치**를 클릭합니다.

5. **Operator 설치** 페이지에서 다음 옵션을 설정합니다.

   a. **stable-4.12** 로 채널을 업데이트합니다.

   b. 설치 모드에서 **클러스터의 특정 네임스페이스**를 선택합니다.

   c. 설치된 네임스페이스에서 **Operator 권장 네임스페이스 openshift-storage**를 선택합니다. 네임스페이스 **openshift-storage**가 없으면 Operator 설치 중에 생성됩니다.

   d. 승인 전략을 **자동** 또는 **수동**으로 선택합니다.
   자동 업데이트를 선택하면 OLM(Operator Lifecycle Manager)은 개입 없이 Operator의 실행 중인 인스턴스를 자동으로 업그레이드합니다.

   수동 업데이트를 선택하면 OLM에서 업데이트 요청을 생성합니다. 클러스터 관리자는 Operator를 최신 버전으로 업데이트하기 위해 해당 업데이트 요청을 수동으로 승인해야 합니다.

   e. **Console 플러그인**에 대해 **Enable** 옵션이 선택되어 있는지 확인합니다.

   f. **설치**를 클릭합니다.

검증 단계

- Operator가 성공적으로 설치되면 메시지가 포함된 팝업 **Web console update is available**이 사용자 인터페이스에 표시됩니다. 콘솔 변경 사항을 반영하려면 이 팝업 창에서 **웹 콘솔 새로 고침**을 클릭합니다.
- 웹 콘솔에서 다음을 수행합니다.
  - Installed Operators로 이동하여 **OpenShift Data Foundation** Operator에 설치에 성공했음을 나타내는 녹색 눈금이 표시되는지 확인합니다.
  - **Storage** 로 이동하여 **Data Foundation** 대시보드를 사용할 수 있는지 확인합니다.

5.1.2. 독립 실행형 Multicloud Object Gateway 생성

OpenShift Data Foundation을 배포하는 동안 독립 실행형 Multicloud Object Gateway 구성 요소만 생성할 수 있습니다.

사전 요구 사항

- OpenShift Data Foundation Operator가 설치되어 있는지 확인합니다.

절차

1. OpenShift 웹 콘솔에서 **Operators → 설치된 Operator**를 클릭하여 설치된 모든 Operator를 확인합니다.
   선택한 **프로젝트**가 **openshift-storage** 인지 확인합니다.

2. **OpenShift Data Foundation** Operator를 클릭한 다음 **스토리지 시스템 생성**을 클릭합니다.

3. **백업 스토리지** 페이지에서 다음을 선택합니다.

   a. **배포 유형** 용으로 **Multicloud Object Gateway**를 선택합니다.

   b. **기존 스토리지 클래스 사용** 옵션을 선택합니다.

c. **다음**을 클릭합니다.

4. 선택 사항: **외부 키 관리 서비스에 연결** 확인란을 선택합니다. 이는 클러스터 전체 암호화의 경우 선택 사항입니다.

   a. **Key Management Service Provider** 드롭다운 목록에서 **Vault** 또는 **Thales CipherTrust Manager (KMIP 사용)** 를 선택합니다. **Vault** 를 선택한 경우 다음 단계로 이동합니다. **Thales CipherTrust Manager (KMIP 사용)** 를 선택한 경우 iii 단계로 이동합니다.

   b. **인증 방법을** 선택합니다.

      토큰 인증 방법 사용

      - 고유한 **연결 이름**, Vault 서버의 호스트 **주소** (https://<hostname 또는 ip>'), **포트** 번호 및 **토큰** 을 입력합니다.
      - **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
        - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
        - 선택 사항: **TLS 서버 이름** 및 **Vault Enterprise 네임스페이스** 를 입력합니다.
        - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키** 를 제공합니다.
        - **저장을** 클릭하고 iv 단계로 건너뜁니다.

      Kubernetes 인증 방법 사용

      - 고유한 Vault **연결 이름**, Vault 서버의 호스트 **주소** ('https://<hostname 또는 ip>'), **포트** 번호 및 **역할** 이름을 입력합니다.
      - **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
        - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
        - 선택 사항: 해당하는 경우 **TLS 서버 이름** 및 **인증** 경로를 입력합니다.
        - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키** 를 제공합니다.
        - **저장을** 클릭하고 iv 단계로 건너뜁니다.

   c. KMS 공급자로 **Thales CipherTrust Manager (KMIP 사용)** 를 사용하려면 다음 단계를 따르십시오.

      i. 프로젝트 내에서 키 관리 서비스에 대한 고유한 **연결** 이름을 입력합니다.

      ii. **주소** 및 **포트** 섹션에서 Thales CipherTrust Manager의 IP와 KMIP 인터페이스가 활성화된 포트를 입력합니다. 예를 들면 다음과 같습니다.

      - **주소**: 12.34.3.2
      - **포트**:ECDHE96

iii. **클라이언트 인증서,CA 인증서** 및 **클라이언트 개인 키를 업로드합니다**.

iv. StorageClass 암호화가 활성화된 경우 위에서 생성된 암호화 및 암호 해독에 사용할 고유 식별자를 입력합니다.

v. **TLS Server** 필드는 선택 사항이며 KMIP 엔드포인트에 대한 DNS 항목이 없는 경우 사용됩니다. 예를 들어, **kmip_all_<port>.ciphertrustmanager.local**.

d. 네트워크를 **선택합니다**.

e. **다음**을 클릭합니다.

5. **검토 및 생성** 페이지에서 구성 세부 정보를 검토합니다.
구성 설정을 수정하려면 **뒤로**를 클릭합니다.

6. **스토리지 시스템 생성**을 클릭합니다.

검증 단계

OpenShift Data Foundation 클러스터 상태 확인

1. OpenShift 웹 콘솔에서 **스토리지 → Data Foundation** 을 클릭합니다.

2. **개요** 탭의 **상태** 카드에서 **스토리지 시스템**을 클릭한 다음 해당 팝업에서 스토리지 시스템 링크를 클릭합니다.

a. **Object** 탭의 **상태 카드**에서 *Object Service* 및 *Data Resiliency* 모두 녹색 눈금이 있는지 확인합니다.

b. **세부 정보** 카드에 MCG 정보가 표시되는지 확인합니다.

Pod 상태 확인

1. OpenShift 웹 콘솔에서 **워크로드 → Pod**를 클릭합니다.

2. **프로젝트** 드롭다운 목록에서 **openshift-storage**를 선택하고 다음 Pod가 **Running** 상태인지 확인합니다.

참고

기본 프로젝트 표시 옵션이 비활성화된 경우 토글 버튼을 사용하여 모든 기본 프로젝트를 나열합니다.

구성 요소	해당 Pod

구성 요소	해당 Pod
OpenShift Data Foundation Operator	• **OCS-operator-*** (모든 작업자 노드에 1 Pod) • **OCS-metrics-exporter-*** (모든 작업자 노드에 1 Pod) • **ODF-operator-controller-manager-*** (모든 작업자 노드에 1 Pod) • **ODF-console-*** (모든 작업자 노드에 1 Pod) • **CSI-addons-controller-manager-*** (모든 작업자 노드의 Pod)
Rook-ceph Operator	**Rook-ceph-operator-*** (모든 작업자 노드에 1 Pod)
Multicloud Object Gateway	• **noobaa-operator-*** (모든 작업자 노드에 1 Pod) • **noobaa-core-*** (모든 작업자 노드에 1 Pod) • **noobaa-db-pg-*** (모든 작업자 노드에서 1 pod) • **noobaa-endpoint-*** (모든 작업자 노드에서 1 Pod)

5.2. 로컬 스토리지 장치를 사용하여 독립 실행형 MULTICLOUD OBJECT GATEWAY 배포

다음 단계를 포함하는 독립 실행형 Multicloud Object Gateway 구성 요소만 배포하려면 이 섹션을 사용합니다.

- Local Storage Operator 설치
- Red Hat OpenShift Data Foundation Operator 설치
- 독립 실행형 Multicloud Object Gateway 생성

5.2.1. 로컬 스토리지 Operator 설치

로컬 스토리지 장치에서 Red Hat OpenShift Data Foundation 클러스터를 생성하기 전에 Operator Hub에서 Local Storage Operator를 설치합니다.

절차

1. OpenShift 웹 콘솔에 로그인합니다.
2. **Operators → OperatorHub**를 클릭합니다.
3. **키워드로 필터링**상자에 **로컬 스토리지** 를 입력하여 운영자 목록에서 **Local Storage Operator** 를 찾은 다음 클릭합니다.

4. **Operator 설치** 페이지에서 다음 옵션을 설정합니다.
   a. **4.12** 또는 **stable** 로 채널을 업데이트합니다.
   b. 설치 모드에서 **클러스터의 특정 네임스페이스**를 선택합니다.
   c. 설치된 네임스페이스를 **Operator 권장 네임스페이스 openshift-local-storage**를 선택합니다.
   d. 승인을 **자동**으로 업데이트합니다.
5. **설치**를 클릭합니다.

검증 단계

- Local Storage Operator에 성공적인 설치를 나타내는 녹색 눈금이 표시되는지 확인합니다.

5.2.2. Red Hat OpenShift Data Foundation Operator 설치

Red Hat OpenShift Container Platform Operator Hub를 사용하여 Red Hat OpenShift Data Foundation Operator를 설치할 수 있습니다.

사전 요구 사항

- **cluster-admin** 및 Operator 설치 권한이 있는 계정을 사용하여 OpenShift Container Platform 클러스터에 액세스할 수 있습니다.
- Red Hat OpenShift Container Platform 클러스터에 3개 이상의 작업자 노드가 있어야 합니다.
- 추가 리소스 요구 사항은 배포 계획 가이드를 참조하십시오.

중요

- OpenShift Data Foundation에 대한 클러스터 전체 기본 노드 선택기를 재정의해야 하는 경우 다음 명령을 사용하여 **openshift-storage** 네임스페이스에 빈 노드 선택기를 지정할 수 있습니다(이 경우 **openshift-storage** 네임스페이스 생성).

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

- 노드에 Red Hat OpenShift Data Foundation 리소스만 예약되도록 **infra** 테인트를 구성합니다. 이를 통해 서브스크립션 비용을 절감할 수 있습니다. 자세한 내용은 스토리지 리소스 관리 및 할당 가이드의 *Red Hat OpenShift Data Foundation 전용 작업자 노드를 사용하는 방법을* 참조하십시오.

절차

1. OpenShift 웹 콘솔에 로그인합니다.
2. **Operators → OperatorHub**를 클릭합니다.
3. **OpenShift Data Foundation**을 **키워드로 필터링** 상자에 스크롤하여 **OpenShift Data Foundation** Operator를 찾습니다.
4. **설치**를 클릭합니다.

5. **Operator 설치** 페이지에서 다음 옵션을 설정합니다.

   a. **stable-4.12** 로 채널을 업데이트합니다.

   b. 설치 모드에서 **클러스터의 특정 네임스페이스**를 선택합니다.

   c. 설치된 네임스페이스에서 **Operator 권장 네임스페이스 openshift-storage**를 선택합니다. 네임스페이스 **openshift-storage**가 없으면 Operator 설치 중에 생성됩니다.

   d. 승인 전략을 **자동** 또는 **수동**으로 선택합니다.
   자동 업데이트를 선택하면 OLM(Operator Lifecycle Manager)은 개입 없이 Operator의 실행 중인 인스턴스를 자동으로 업그레이드합니다.

   수동 업데이트를 선택하면 OLM에서 업데이트 요청을 생성합니다. 클러스터 관리자는 Operator를 최신 버전으로 업데이트하기 위해 해당 업데이트 요청을 수동으로 승인해야 합니다.

   e. **Console 플러그인**에 대해 **Enable** 옵션이 선택되어 있는지 확인합니다.

   f. **설치**를 클릭합니다.

검증 단계

- Operator가 성공적으로 설치되면 메시지가 포함된 팝업 **Web console update is available**이 사용자 인터페이스에 표시됩니다. 콘솔 변경 사항을 반영하려면 이 팝업 창에서 **웹 콘솔 새로 고침**을 클릭합니다.
- 웹 콘솔에서 다음을 수행합니다.
  - Installed Operators로 이동하여 **OpenShift Data Foundation** Operator에 설치에 성공했음을 나타내는 녹색 눈금이 표시되는지 확인합니다.
  - **Storage** 로 이동하여 **Data Foundation** 대시보드를 사용할 수 있는지 확인합니다.

5.2.3. 독립 실행형 Multicloud Object Gateway 생성

OpenShift Data Foundation을 배포하는 동안 독립 실행형 Multicloud Object Gateway 구성 요소만 생성할 수 있습니다.

사전 요구 사항

- OpenShift Data Foundation Operator가 설치되어 있는지 확인합니다.

절차

1. OpenShift 웹 콘솔에서 **Operators → 설치된 Operator**를 클릭하여 설치된 모든 Operator를 확인합니다.
   선택한 **프로젝트**가 **openshift-storage** 인지 확인합니다.

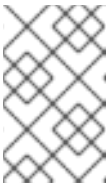
2. **OpenShift Data Foundation** Operator를 클릭한 다음 **스토리지 시스템 생성**을 클릭합니다.

3. **백업 스토리지** 페이지에서 다음을 선택합니다.

   a. **배포 유형** 용으로 **Multicloud Object Gateway**를 선택합니다.

   b. **로컬 스토리지 장치 옵션을 사용하여 새 StorageClass 만들기**옵션을 선택합니다.

c. **다음**을 클릭합니다.



참고

아직 설치되지 않은 경우 Local Storage Operator를 설치하라는 메시지가 표시됩니다. **설치**를 클릭하고 Local Storage Operator 설치 에 설명된 절차를 따릅니다.

4. **로컬 볼륨 세트 생성** 페이지에서 다음 정보를 제공합니다.

a. **로컬 볼륨 세트**의 이름과 **스토리지 클래스**를 입력합니다.
기본적으로 스토리지 클래스 이름에 로컬 볼륨 세트 이름이 표시됩니다. 이름을 변경할 수 있습니다.

b. 다음 중 하나를 선택합니다.

- **모든 노드의 디스크**
모든 노드에서 선택한 필터와 일치하는 사용 가능한 디스크를 사용합니다.
- **선택한 노드의 디스크**
선택한 노드에서만 선택한 필터와 일치하는 사용 가능한 디스크를 사용합니다.

c. 사용 가능한 **디스크 유형** 목록에서 **SSD/NVMe**을 선택합니다.

d. **고급** 섹션을 확장하고 다음 옵션을 설정합니다.

볼륨 모드	파일 시스템은 기본적으로 선택됩니다. 항상 **볼륨 모드**의 파일 시스템이 선택되어 있는지 확인하십시오.
장치 유형	드롭다운 목록에서 하나 이상의 장치 유형을 선택합니다.
디스크 크기	장치에 대해 최소 크기 100GB와 포함되어야 하는 장치의 사용 가능한 최대 크기를 설정합니다.
최대 디스크 제한	이는 노드에서 생성할 수 있는 최대 PV 수를 나타냅니다. 이 필드가 비어 있으면 일치하는 노드에서 사용 가능한 모든 디스크에 PV가 생성됩니다.

e. **다음**을 클릭합니다.
로컬 볼륨 세트 생성이 표시되는지 확인하는 팝업이 표시됩니다.

f. 계속하려면 **예**를 클릭합니다.

5. **용량 및 노드** 페이지에서 다음을 구성합니다.

a. **사용 가능한 원시 용량**은 스토리지 클래스와 연결된 모든 디스크에 따라 용량 값으로 채워집니다. 이 작업을 수행하는 데 시간이 다소 걸립니다. **선택한 노드** 목록에는 스토리지 클래스를 기반으로 하는 노드가 표시됩니다.

b. **다음**을 클릭합니다.

6. 선택 사항: **외부 키 관리 서비스에 연결** 확인란을 선택합니다. 이는 클러스터 전체 암호화의 경우 선택 사항입니다.

a. **Key Management Service Provider** 드롭다운 목록에서 **Vault** 또는 **Thales CipherTrust Manager (KMIP 사용)** 를 선택합니다. **Vault** 를 선택한 경우 다음 단계로 이동합니다. **Thales CipherTrust Manager (KMIP 사용)** 를 선택한 경우 iii 단계로 이동합니다.

b. **인증 방법을** 선택합니다.

토큰 인증 방법 사용

- 고유한 **연결 이름**, Vault 서버의 호스트 **주소** (https://<hostname 또는 ip>'), **포트** 번호 및 **토큰** 을 입력합니다.
- **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
  - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
  - 선택 사항: **TLS 서버 이름** 및 **Vault Enterprise 네임스페이스** 를 입력합니다.
  - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키** 를 제공합니다.
  - **저장을** 클릭하고 iv 단계로 건너뜁니다.

Kubernetes 인증 방법 사용

- 고유한 Vault **연결 이름**, Vault 서버의 호스트 **주소** ('https://<hostname 또는 ip>'), **포트** 번호 및 **역할** 이름을 입력합니다.
- **고급** 설정을 확장하여 **Vault** 구성에 따라 추가 설정 및 인증서 세부 정보를 입력합니다.
  - OpenShift Data Foundation 전용 및 고유한 **백엔드** 경로에 키 값 시크릿 경로를 입력합니다.
  - 선택 사항: 해당하는 경우 **TLS 서버 이름** 및 **인증** 경로를 입력합니다.
  - 각 PEM 인코딩 인증서 파일을 업로드하여 **CA 인증서**,**클라이언트 인증서** 및 **클라이언트 개인 키** 를 제공합니다.
  - **저장을** 클릭하고 iv 단계로 건너뜁니다.

c. KMS 공급자로 **Thales CipherTrust Manager (KMIP 사용)** 를 사용하려면 다음 단계를 따르십시오.

i. 프로젝트 내에서 키 관리 서비스에 대한 고유한 **연결** 이름을 입력합니다.

ii. **주소** 및 **포트** 섹션에서 Thales CipherTrust Manager의 IP와 KMIP 인터페이스가 활성화된 포트를 입력합니다. 예를 들면 다음과 같습니다.

- **주소**: 12.34.3.2
- **포트**:ECDHE96

iii. **클라이언트 인증서**,**CA 인증서** 및 **클라이언트 개인 키를 업로드합니다**.

iv. StorageClass 암호화가 활성화된 경우 위에서 생성된 암호화 및 암호 해독에 사용할 고유 식별자를 입력합니다.

v. **TLS Server** 필드는 선택 사항이며 KMIP 엔드포인트에 대한 DNS 항목이 없는 경우 사용됩니다. 예를 들어, **kmip_all_<port>.ciphertrustmanager.local**.

d. 네트워크를 **선택합니다**.

e. **다음**을 클릭합니다.

7. **검토 및 생성** 페이지에서 구성 세부 정보를 검토합니다.
구성 설정을 수정하려면 **뒤로**를 클릭합니다.

8. **스토리지 시스템 생성**을 클릭합니다.

검증 단계

OpenShift Data Foundation 클러스터 상태 확인

1. OpenShift 웹 콘솔에서 **스토리지 → Data Foundation** 을 클릭합니다.

2. **개요** 탭의 **상태** 카드에서 **스토리지 시스템**을 클릭한 다음 해당 팝업에서 스토리지 시스템 링크를 클릭합니다.

a. **Object** 탭의 **상태 카드**에서 *Object Service* 및 *Data Resiliency* 모두 녹색 눈금이 있는지 확인합니다.

b. **세부 정보** 카드에 MCG 정보가 표시되는지 확인합니다.

Pod 상태 확인

1. OpenShift 웹 콘솔에서 **워크로드 → Pod**를 클릭합니다.

2. **프로젝트** 드롭다운 목록에서 **openshift-storage**를 선택하고 다음 Pod가 **Running** 상태인지 확인합니다.

참고

기본 프로젝트 표시 옵션이 비활성화된 경우 토글 버튼을 사용하여 모든 기본 프로젝트를 나열합니다.

구성 요소	해당 Pod
OpenShift Data Foundation Operator	• **OCS-operator-*** (모든 작업자 노드에 1 Pod) • **OCS-metrics-exporter-*** (모든 작업자 노드에 1 Pod) • **ODF-operator-controller-manager-*** (모든 작업자 노드에 1 Pod) • **ODF-console-*** (모든 작업자 노드에 1 Pod) • **CSI-addons-controller-manager-*** (모든 작업자 노드의 Pod)

구성 요소	해당 Pod
Rook-ceph Operator	**Rook-ceph-operator-*** (모든 작업자 노드에 1 Pod)
Multicloud Object Gateway	• **noobaa-operator-*** (모든 작업자 노드에 1 Pod) • **noobaa-core-*** (모든 작업자 노드에 1 Pod) • **noobaa-db-pg-*** (모든 작업자 노드에서 1 pod) • **noobaa-endpoint-*** (모든 작업자 노드에서 1 Pod)

6장. OPENSHIFT DATA FOUNDATION 설치 제거

6.1. 내부 모드에서 OPENSHIFT DATA FOUNDATION 설치 제거

내부 모드에서 OpenShift Data Foundation을 설치 제거하려면 OpenShift Data Foundation 설치 제거에 대한 지식 기반 문서를 참조하십시오.