타사 도구를 사용하여 데이터 보호

NetApp virtualization solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions-virtualization/openshift/osv-vm-dp-using-velero-overview.html on August 18, 2025. Always check docs.netapp.com for the latest.

목차

타사 도구를 사용하여 데이터 보호 . . . 1

OpenShift API for Data Protection(OADP)을 사용하여 Red Hat OpenShift Virtualization에서 VM의 데이터 보호에 대해 알아보세요. . . . 1

OADP(Red Hat OpenShift API for Data Protection) 운영자 설치 . . . 3

필수 조건 . . . 3

OADP Operator 설치 단계 . . . 4

Velero를 사용하여 Red Hat OpenShift Virtualization의 VM에 대한 주문형 백업을 만듭니다. . . . 13

VM 백업을 생성하는 단계 . . . 13

OpenShift Virtualization에서 VM에 대한 예약된 백업 생성 . . . 15

Velero를 사용하여 Red Hat OpenShift Virtualization에서 백업된 VM 복원 . . . 16

필수 조건 . . . 16

Velero를 사용하여 Red Hat OpenShift Virtualization에서 백업 CR을 삭제하거나 CR을 복원합니다. . . . 22

백업 삭제 . . . 22

복원 삭제 . . . 22

타사 도구를 사용하여 데이터 보호

OpenShift API for Data Protection(OADP)을 사용하여 Red Hat OpenShift Virtualization에서 VM의 데이터 보호에 대해 알아보세요.

Velero가 제공하는 OADP(OpenShift API for Data Protection)는 OpenShift Virtualization의 VM에 대한 백업, 복원 및 재해 복구 기능을 제공합니다. Trident CSI 스냅샷을 사용하여 영구 볼륨과 VM 메타데이터를 NetApp ONTAP S3 또는 StorageGRID S3에 백업합니다. OADP는 Velero API 및 CSI 스토리지 드라이버와 통합되어 컨테이너화된 VM에 대한 데이터 보호 작업을 관리합니다.

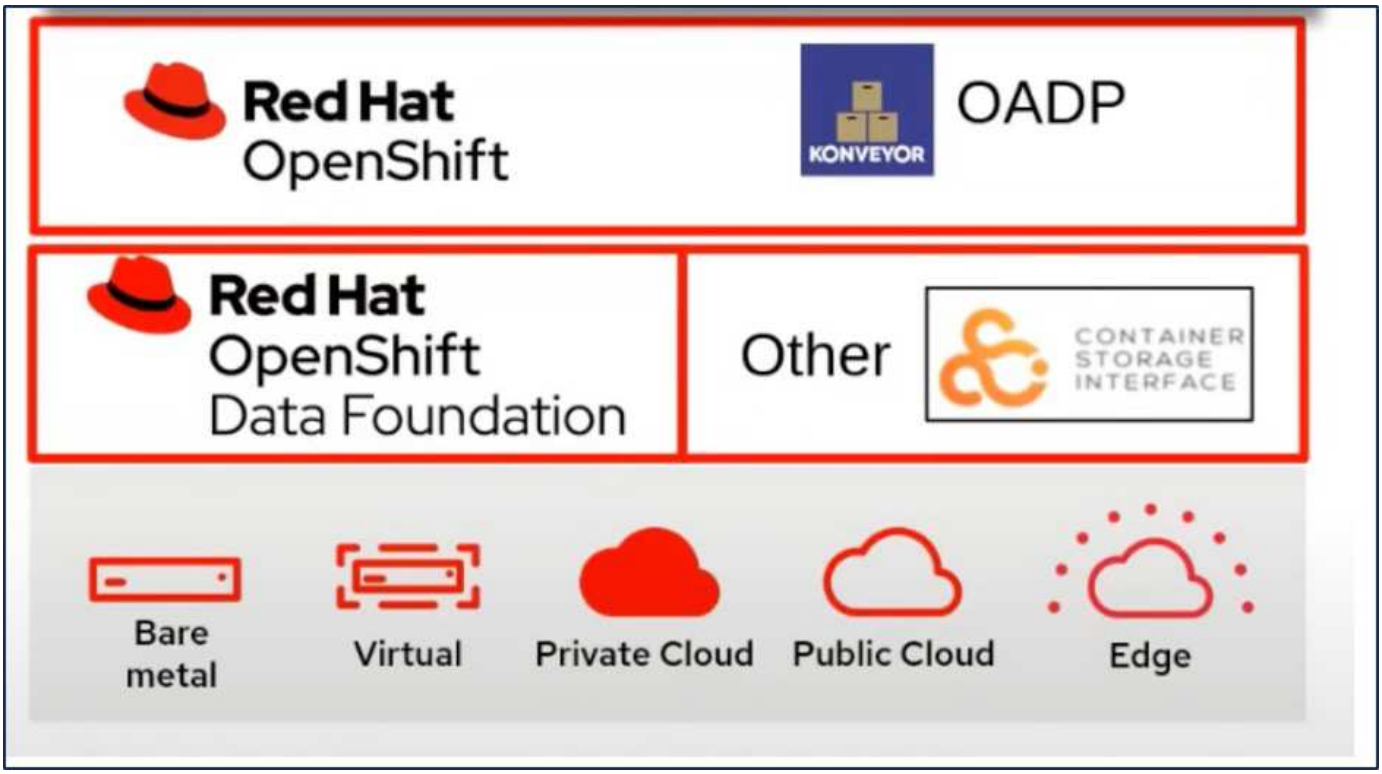
OpenShift 가상화 환경의 가상 머신은 OpenShift 컨테이너 플랫폼의 워커 노드에서 실행되는 컨테이너화된 애플리케이션입니다. VM 메타데이터와 VM의 영구 디스크를 보호하는 것은 손실되거나 손상될 경우 복구할 수 있도록 하는 데 중요합니다.

OpenShift Virtualization VM의 영구 디스크는 OpenShift 클러스터에 통합된 ONTAP 스토리지로 백업할 수 있습니다."Trident CSI" . 이 섹션에서는 다음을 사용합니다."데이터 보호를 위한 OpenShift API(OADP)" 데이터 볼륨을 포함한 VM의 백업을 수행합니다.

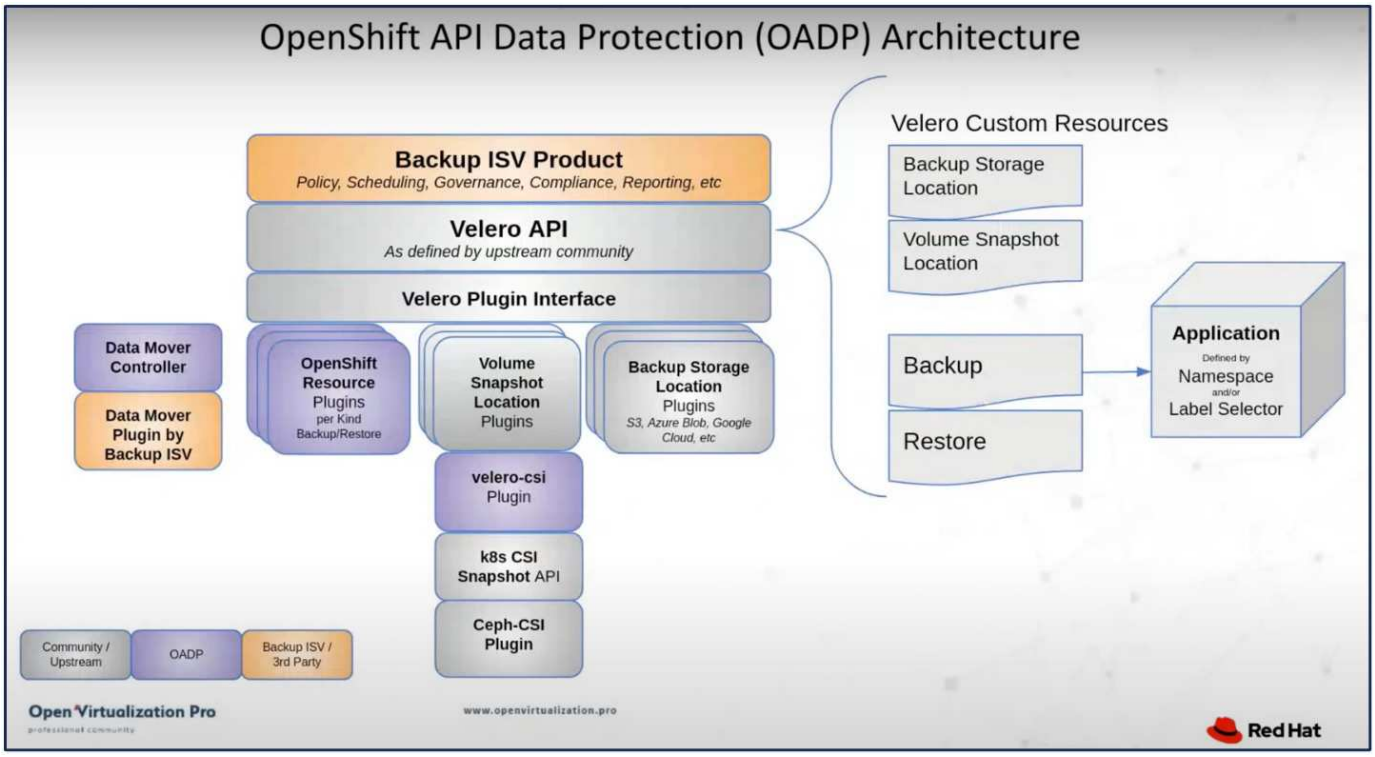
- ONTAP 객체 스토리지
- 스토리지그리드

필요할 때 백업에서 복원합니다.

OADP를 사용하면 OpenShift 클러스터에서 애플리케이션의 백업, 복원 및 재해 복구가 가능합니다. OADP로 보호할 수 있는 데이터에는 Kubernetes 리소스 개체, 영구 볼륨 및 내부 이미지가 포함됩니다.



Red Hat OpenShift는 오픈소스 커뮤니티에서 개발한 솔루션을 활용하여 데이터 보호를 구현했습니다. "벨레로" Kubernetes 클러스터 리소스와 영구 볼륨을 안전하게 백업하고 복원하고, 재해 복구를 수행하고, 마이그레이션하는 오픈 소스 도구입니다. Velero를 쉽게 사용할 수 있도록 OpenShift는 OADP 연산자와 Velero 플러그인을 개발하여 CSI 스토리지 드라이버와 통합했습니다. 공개된 OADP API의 핵심은 Velero API를 기반으로 합니다. OADP 운영자를 설치하고 구성한 후에는 Velero API에서 제공하는 작업에 따라 백업/복원 작업을 수행할 수 있습니다.



OADP 1.3은 OpenShift 클러스터 4.12 이상의 운영자 허브에서 사용할 수 있습니다. CSI 볼륨 스냅샷을 원격 개체 저장소로 옮길 수 있는 내장형 Data Mover가 있습니다. 이렇게 하면 백업하는 동안 스냅샷을 개체 스토리지 위치로

이동하여 이동성과 내구성을 제공합니다. 재난 발생 후 스냅샷을 복원하는 데 사용할 수 있습니다.

다음은 이 섹션의 예제에 사용된 다양한 구성 요소의 버전입니다.

- 오픈시프트 클러스터 4.14
- Red Hat에서 제공하는 Operator를 통해 설치된 OpenShift Virtualization
- Red Hat에서 제공하는 OADP Operator 1.13
- Linux용 Velero CLI 1.13
- Trident 24.02
- ONTAP 9.12

"Trident CSI" "데이터 보호를 위한 OpenShift API(OADP)" "벨레로"

OADP(Red Hat OpenShift API for Data Protection) 운영자 설치

OpenShift Virtualization에서 VM의 백업 및 복원 기능을 활성화하려면 OpenShift API for Data Protection(OADP) Operator를 설치합니다. 이 절차에는 OpenShift Operator Hub에서 OADP Operator를 배포하고, Velero가 NetApp ONTAP S3 또는 StorageGRID 백업 대상으로 사용하도록 구성하고, 필요한 비밀과 백업 위치를 설정하는 작업이 포함됩니다.

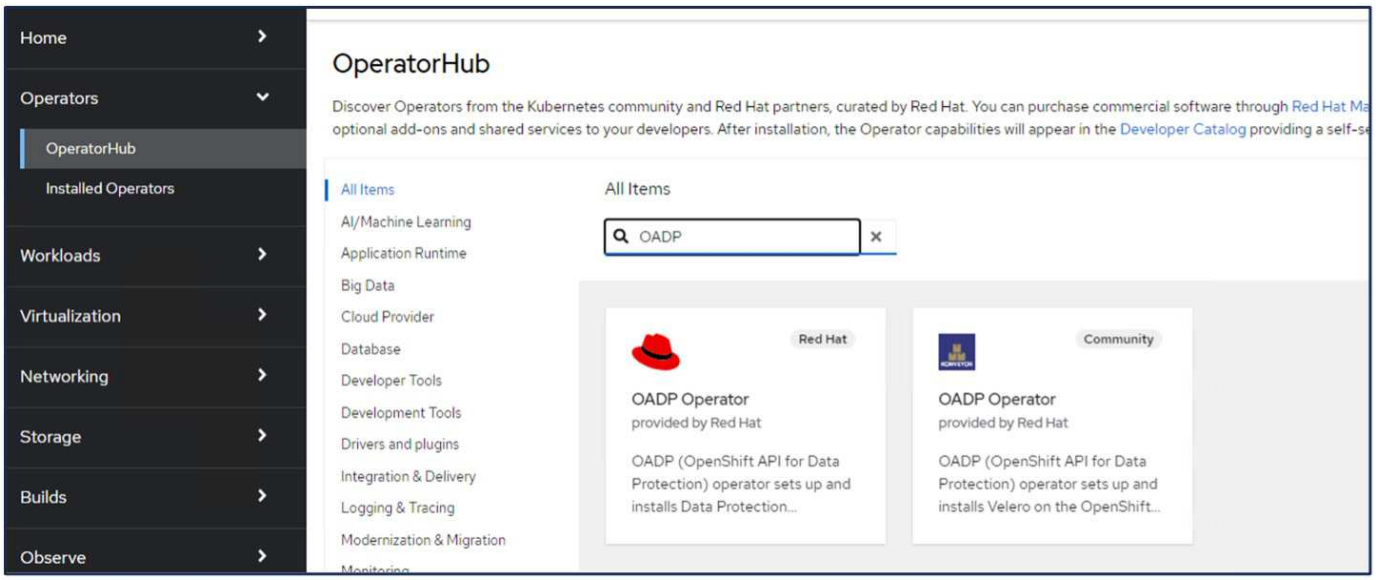
필수 조건

- RHCOS 작업자 노드가 있는 베어 메탈 인프라에 설치된 Red Hat OpenShift 클러스터(버전 4.12 이상)
- Trident 사용하여 클러스터와 통합된 NetApp ONTAP 클러스터
- ONTAP 클러스터의 SVM으로 구성된 Trident 백엔드
- Trident 프로비저너로 사용하여 OpenShift 클러스터에 구성된 StorageClass
- 클러스터에 생성된 Trident Snapshot 클래스
- Red Hat OpenShift 클러스터에 대한 클러스터 관리자 액세스
- NetApp ONTAP 클러스터에 대한 관리자 액세스
- OpenShift Virtualization 운영자 설치 및 구성
- OpenShift Virtualization의 네임스페이스에 배포된 VM
- $PATH에 tridentctl 및 oc 도구가 설치되고 추가된 관리자 워크스테이션

> 실행 상태인 VM을 백업하려면 해당 가상 머신에 QEMU 게스트 에이전트를 설치해야 합니다. 기존 템플릿을 사용하여 VM을 설치하는 경우 QEMU 에이전트가 자동으로 설치됩니다. QEMU를 사용하면 스냅샷 프로세스 중에 게스트 에이전트가 게스트 OS에서 전송 중인 데이터를 중지하고 잠재적인 데이터 손상을 방지할 수 있습니다. QEMU가 설치되어 있지 않으면 백업을 수행하기 전에 가상 머신을 중지할 수 있습니다.

OADP Operator 설치 단계

1. 클러스터의 운영자 허브로 이동하여 Red Hat OADP 운영자를 선택합니다. 설치 페이지에서 모든 기본 선택 사항을 사용하고 설치를 클릭합니다. 다음 페이지에서도 기본값을 모두 사용하고 설치를 클릭합니다. OADP 운영자는 openshift-adp 네임스페이스에 설치됩니다.



OADP Operator

1.3.0 provided by Red Hat

Install

Channel

stable-1.3

Version

1.3.0

Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected

OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.

Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.

OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.

- Installing OADP for application backup and restore
- Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
- Frequently Asked Questions

Project: All Projects

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation Operator and ClusterServiceVersion using the Operator SDK.

Name | Search by name... /

Name	Namespace	Managed Namespaces	Status
OpenShift Virtualization 4.14.4 provided by Red Hat	NS openshift-cnv	NS openshift-cnv	Succeeded Up to date
OADP Operator 1.3.0 provided by Red Hat	NS openshift-adp	NS openshift-adp	Succeeded Up to date
Package Server 0.0.1-snapshot provided by	NS openshift-operator-lifecycle-manager	NS openshift-operator-lifecycle-manager	Succeeded

Ontap S3 세부 정보를 사용한 Velero 구성을 위한 전제 조건

운영자 설치가 성공적으로 완료되면 Velero 인스턴스를 구성합니다. Velero는 S3 호환 개체 스토리지를 사용하도록 구성할 수 있습니다. 다음 절차를 사용하여 ONTAP S3를 구성합니다."ONTAP 설명서의 개체 스토리지 관리 섹션" . Velero와 통합하려면 ONTAP S3 구성에서 다음 정보가 필요합니다.

- S3에 액세스하는 데 사용할 수 있는 논리 인터페이스(LIF)
- 액세스 키와 비밀 액세스 키가 포함된 S3에 액세스하기 위한 사용자 자격 증명
- 사용자에 대한 액세스 권한이 있는 백업을 위한 S3의 버킷 이름
- Object Storage에 안전하게 액세스하려면 Object Storage 서버에 TLS 인증서를 설치해야 합니다.

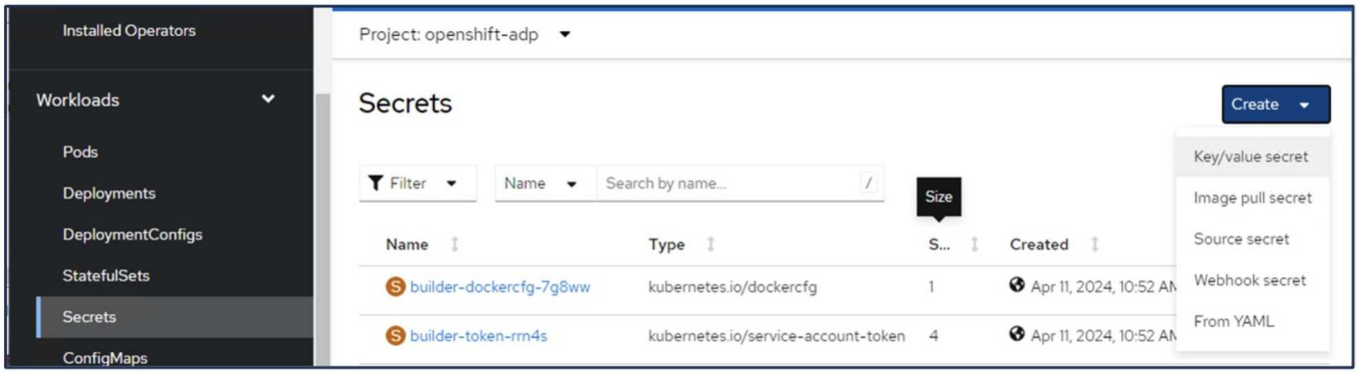
StorageGrid S3 세부 정보를 사용한 Velero 구성을 위한 필수 구성 요소

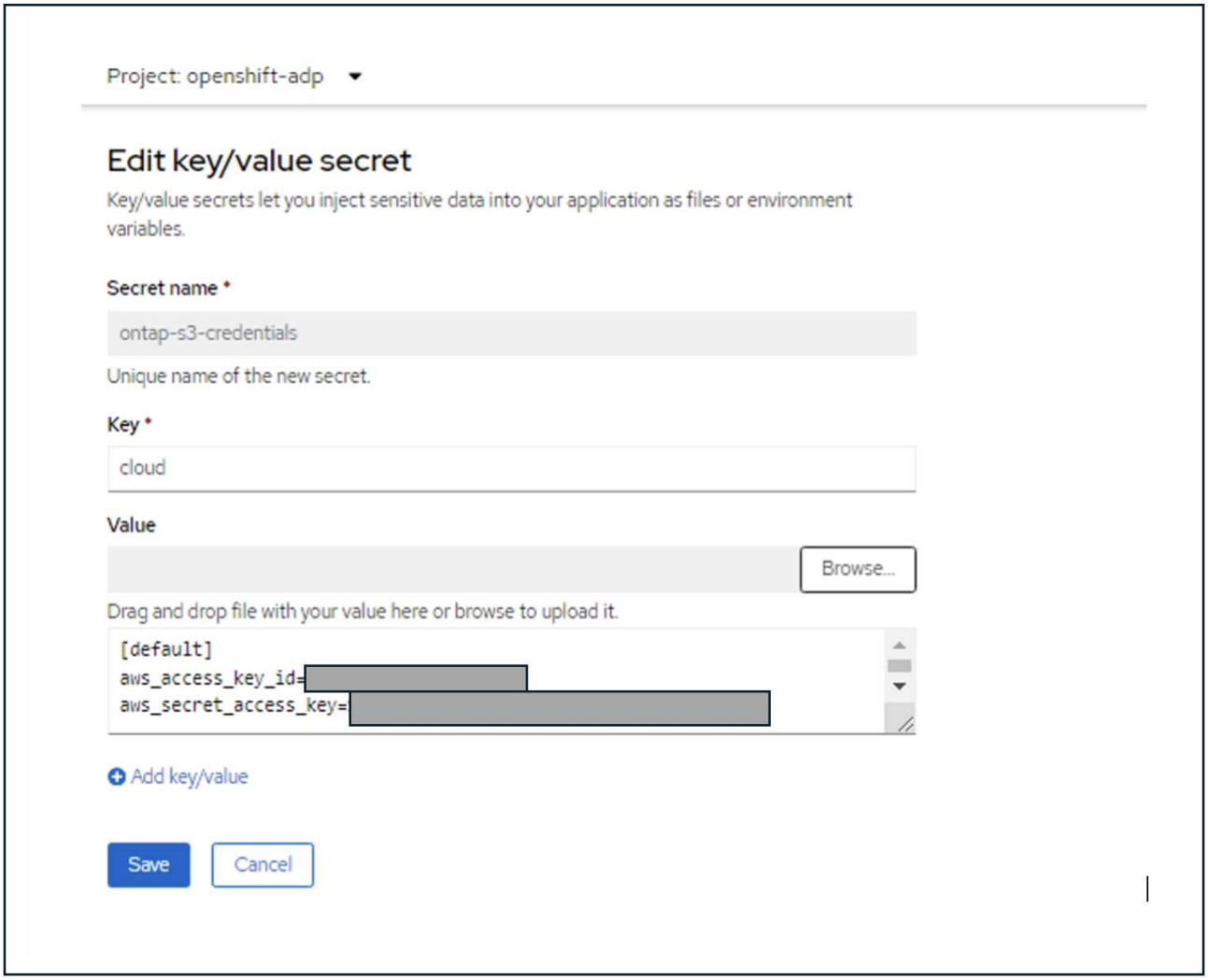
Velero는 S3 호환 개체 스토리지를 사용하도록 구성할 수 있습니다. 다음 절차에 따라 StorageGrid S3를 구성할 수 있습니다."StorageGrid 문서" . Velero와 통합하려면 StorageGrid S3 구성에서 다음 정보가 필요합니다.

- S3에 접속할 수 있는 엔드포인트
- 액세스 키와 비밀 액세스 키가 포함된 S3에 액세스하기 위한 사용자 자격 증명
- 사용자에 대한 액세스 권한이 있는 백업을 위한 S3의 버킷 이름
- Object Storage에 안전하게 액세스하려면 Object Storage 서버에 TLS 인증서를 설치해야 합니다.

Velero 구성 단계

- 먼저 ONTAP S3 사용자 자격 증명이나 StorageGrid 테넌트 사용자 자격 증명에 대한 비밀을 만듭니다. 이는 나중에 Velero를 구성하는 데 사용됩니다. CLI나 웹 콘솔에서 비밀을 생성할 수 있습니다. 웹 콘솔에서 비밀을 생성하려면 비밀을 선택한 다음 키/값 비밀을 클릭합니다. 표시된 대로 자격 증명 이름, 키 및 값에 대한 값을 제공합니다. 반드시 S3 사용자의 액세스 키 ID와 비밀 액세스 키를 사용하세요. 비밀에 적절한 이름을 붙이세요. 아래 샘플에서는 ontap-s3-credentials라는 이름의 ONTAP S3 사용자 자격 증명이 포함된 비밀이 생성됩니다.

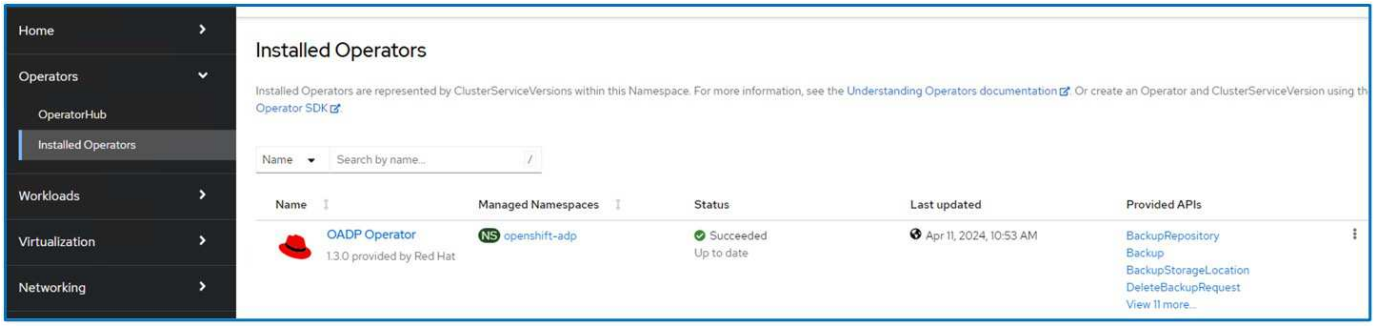




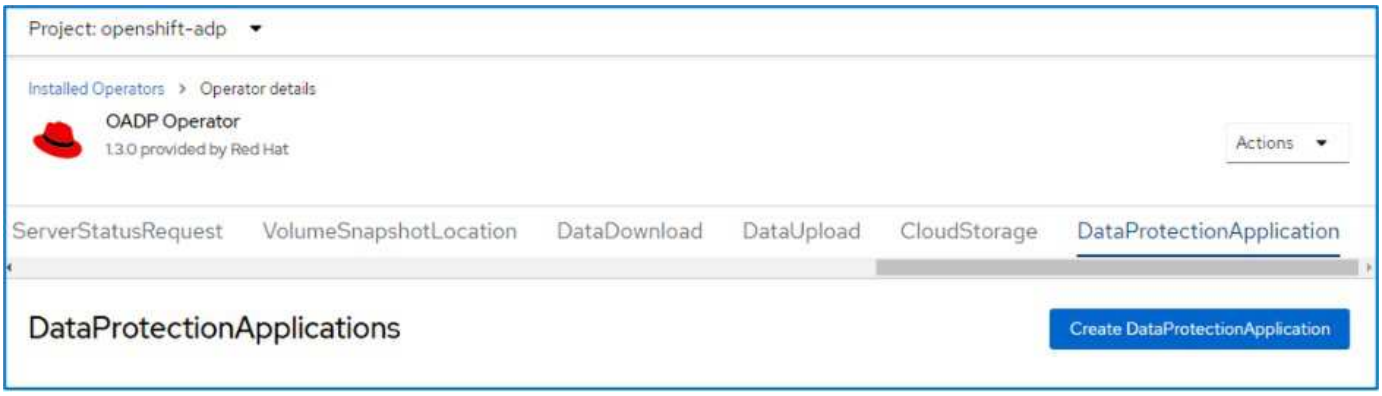
CLI에서 sg-s3-credentials라는 이름의 비밀을 생성하려면 다음 명령을 사용할 수 있습니다.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- 다음으로, Velero를 구성하려면 운영자 아래의 메뉴 항목에서 설치된 운영자를 선택하고, OADP 운영자를 클릭한 다음, DataProtectionApplication 탭을 선택합니다.



DataProtectionApplication 만들기를 클릭합니다. 양식 보기에서 DataProtection 애플리케이션의 이름을 제공하거나 기본 이름을 사용합니다.



이제 YAML 뷰로 가서 아래 yaml 파일 예시에 표시된 대로 사양 정보를 바꾸세요.

- ONTAP S3를 backupLocation으로 사용하여 Velero를 구성하기 위한 샘플 yaml 파일**

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'True' ->This allows use of IP in s3URL
          s3Url: 'https://10.xx.xx.xx' ->LIF to access S3. Ensure TLS
certificate for S3 is configured
        credential:
          key: cloud
          name: ontap-s3-credentials ->previously created secret
        default: true
        objectStorage:
          bucket: velero ->Your bucket name previously created in S3 for
backups
          prefix: demobackup ->The folder that will be created in the
bucket
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->Add this plugin
        - openshift
        - aws
        - kubevirt ->Add this plugin
```

StorageGrid S3를 **backupLocation** 및 **snapshotLocation**으로 사용하여 **Velero**를 구성하기 위한 샘플 **yaml** 파일

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

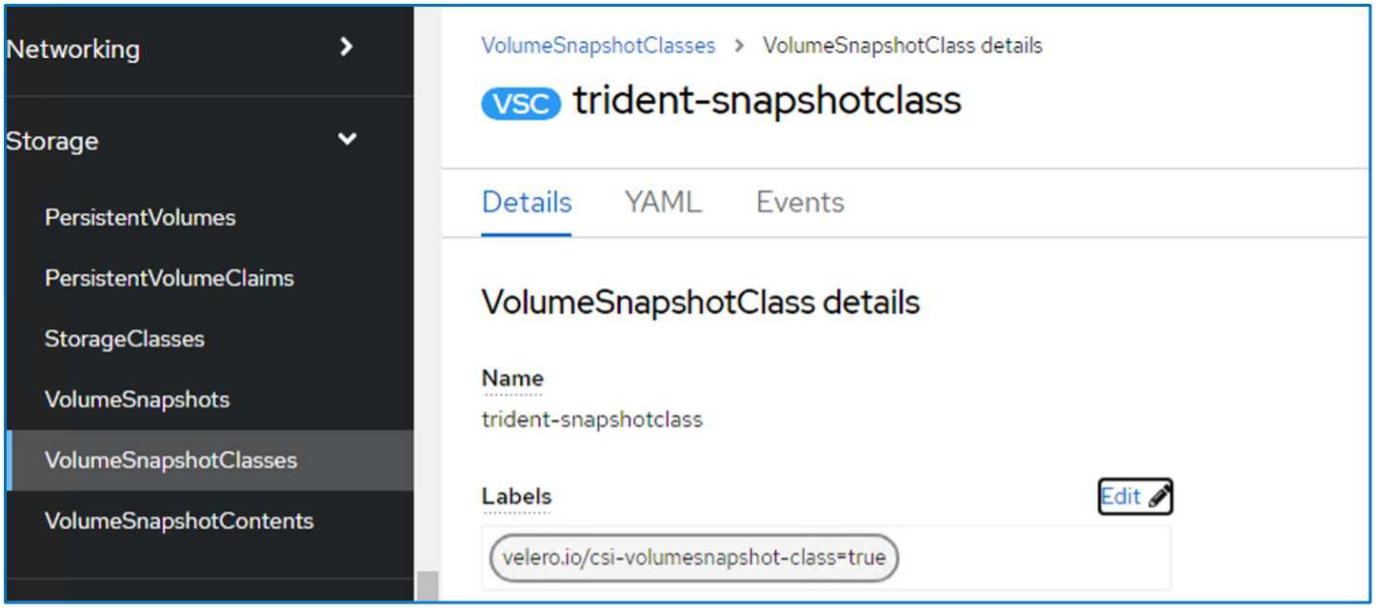
yaml 파일의 spec 섹션은 위의 예와 유사하게 다음 매개변수에 대해 적절하게 구성되어야 합니다.

backupLocations ONTAP S3 또는 StorageGrid S3(yaml에 표시된 자격 증명 및 기타 정보 포함)가 velero의 기본 BackupLocation으로 구성됩니다.

snapshotLocations CSI(Container Storage Interface) 스냅샷을 사용하는 경우 CSI 드라이버를 등록하기 위해 VolumeSnapshotClass CR을 생성하므로 스냅샷 위치를 지정할 필요가 없습니다. 우리의 예에서, 여러분은 Trident CSI를 사용하고 있으며, 이전에 Trident CSI 드라이버를 사용하여 VolumeSnapShotClass CR을 생성했습니다.

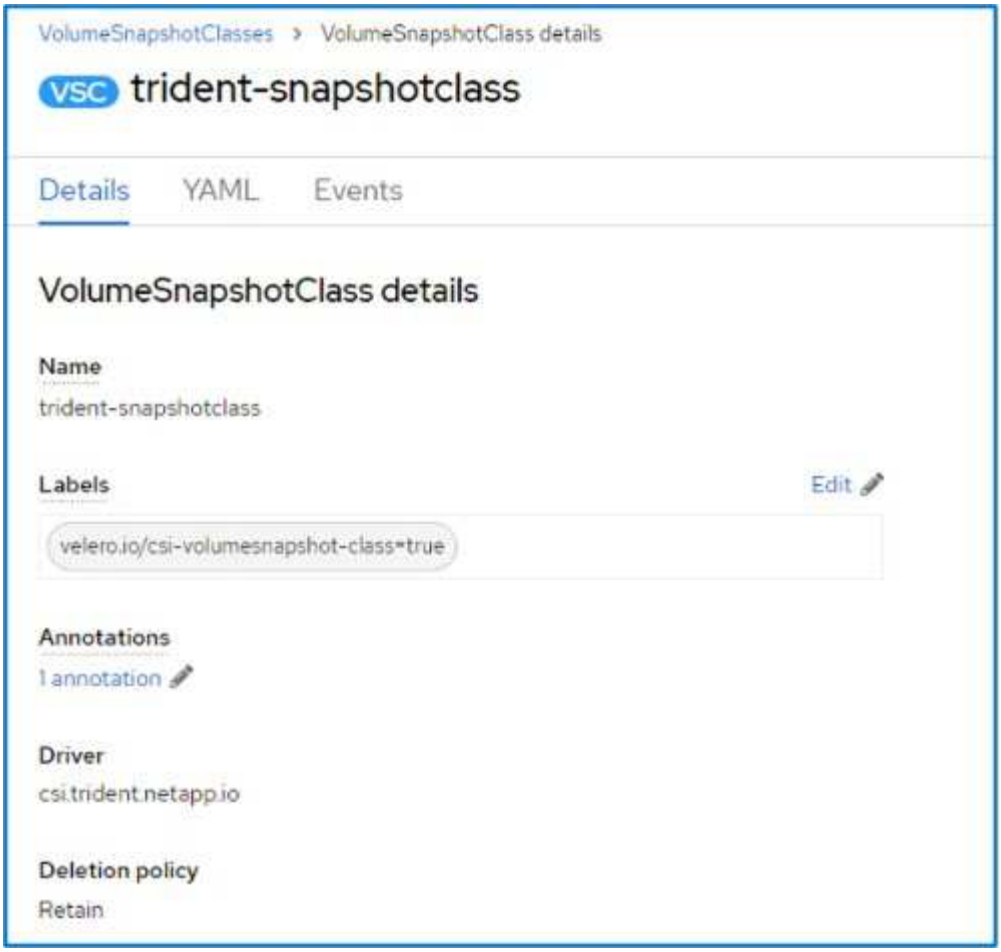
CSI 플러그인 활성화 Velero의 defaultPlugins에 csi를 추가하여 CSI 스냅샷으로 영구 볼륨을 백업합니다. CSI 지원 PVC를 백업하는 Velero CSI 플러그인은 **velero.io/csi-volumesnapshot-class** 레이블이 설정된 클러스터에서 VolumeSnapshotClass를 선택합니다. 이를 위해

- 트라이던트 VolumeSnapshotClass를 생성해야 합니다.
- 아래와 같이 trident-snapshotclass의 라벨을 편집하여 **velero.io/csi-volumesnapshot-class=true**로 설정합니다.

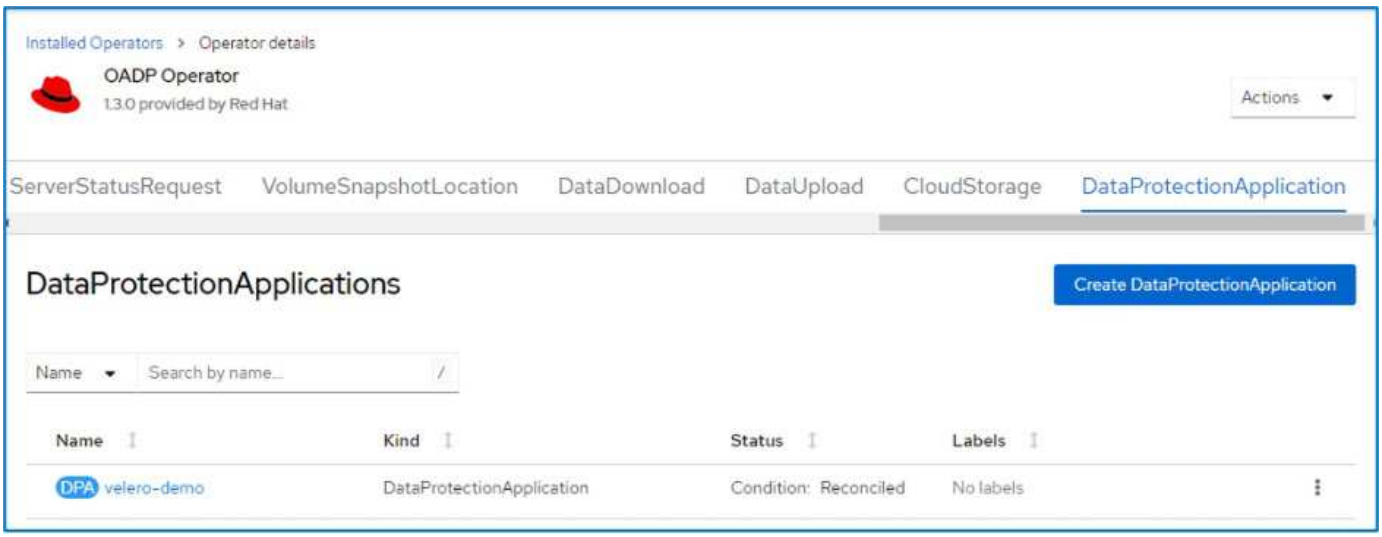


VolumeSnapshot 개체가 삭제된 경우에도 스냅샷이 유지되는지 확인하세요. *deletionPolicy*를 Retain으로 설정하면 됩니다. 그렇지 않은 경우 네임스페이스를 삭제하면 해당 네임스페이스에 백업된 모든 PVC가 완전히 손실됩니다.

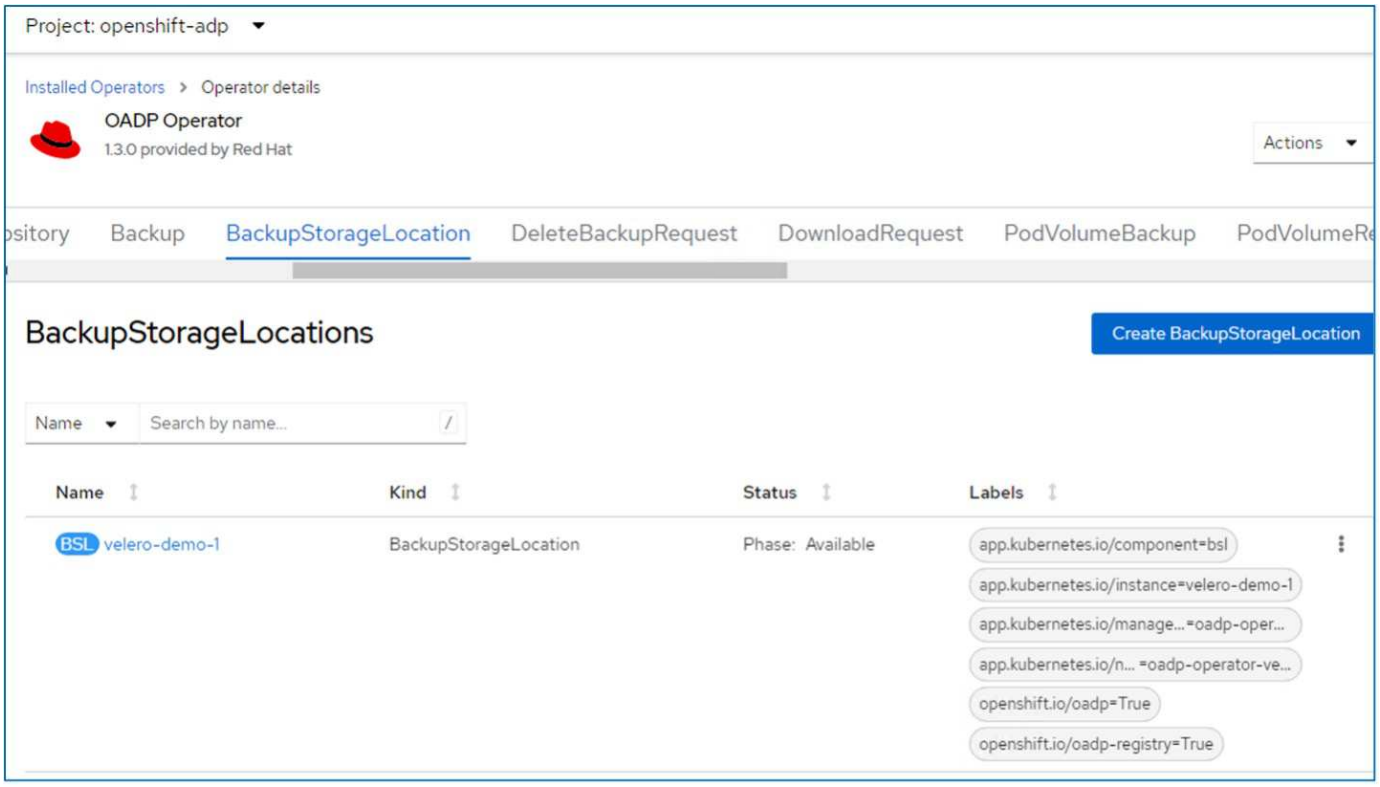
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



DataProtectionApplication이 생성되었고 조건이 Reconciled인지 확인하세요.



OADP 운영자는 해당 BackupStorageLocation을 생성합니다. 이는 백업을 생성할 때 사용됩니다.



Velero를 사용하여 Red Hat OpenShift Virtualization의 VM에 대한 주문형 백업을 만듭니다.

Velero 및 NetApp ONTAP S3 또는 StorageGRID 사용하여 OpenShift Virtualization에서 VM을 백업합니다. 이 절차에는 주문형 백업을 위한 백업 사용자 정의 리소스(CR)와 예약된 백업을 위한 일정 CR을 만드는 작업이 포함됩니다. 각 백업은 VM 메타데이터와 영구 볼륨을 캡처하여 복구 또는 규정 준수 목적으로 지정된 개체 스토리지 위치에 저장합니다.

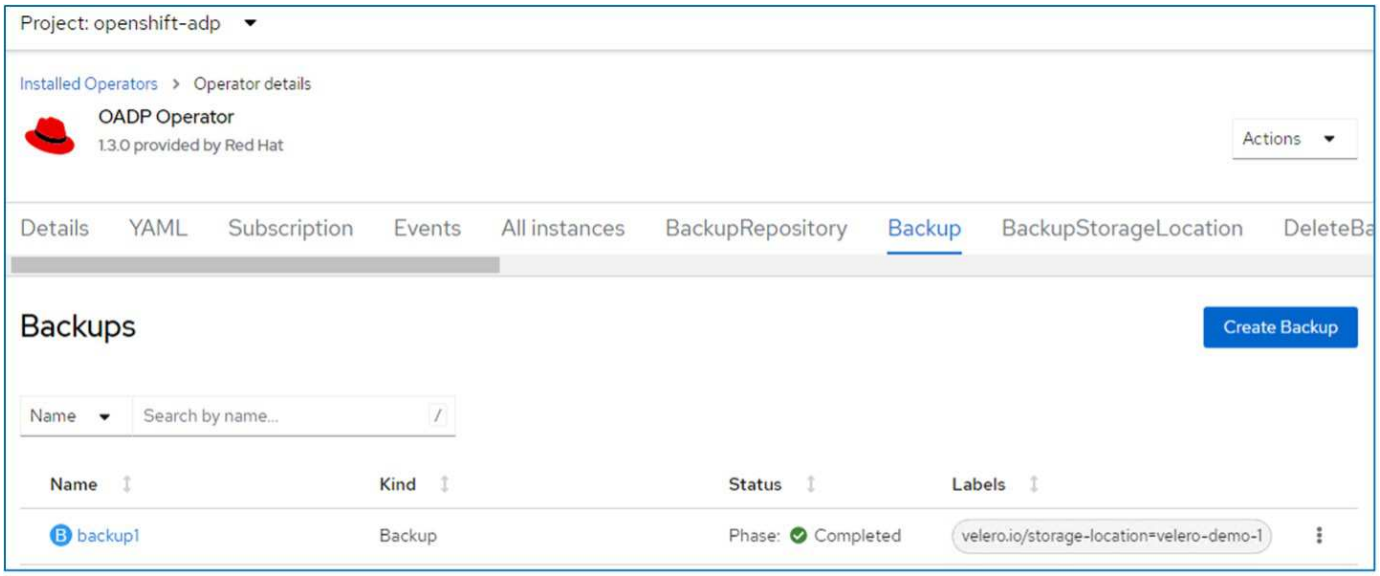
VM 백업을 생성하는 단계

전체 VM(VM 메타데이터 및 VM 디스크)의 주문형 백업을 만들려면 백업 탭을 클릭하세요. 이렇게 하면 백업 사용자 정의 리소스(CR)가 생성됩니다. 백업 CR을 생성하기 위한 샘플 yaml이 제공됩니다. 이 yaml을 사용하면 지정된 네임스페이스에 있는 VM과 디스크가 백업됩니다. 추가 매개변수는 표시된 대로 설정할 수 있습니다."선적 서류 비치" .

디스크를 백업하는 영구 볼륨의 스냅샷은 CSI에 의해 생성됩니다. VM의 백업과 디스크의 스냅샷이 생성되어 yaml에 지정된 백업 위치에 저장됩니다. 백업은 TTL에 지정된 대로 30일 동안 시스템에 보관됩니다.

```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
previously created
                                    when Velero is configured.
  ttl: 720h0m0s
```

백업이 완료되면 해당 단계가 완료로 표시됩니다.



S3 브라우저 애플리케이션을 사용하면 Object Storage에서 백업을 검사할 수 있습니다. 백업 경로는 구성된 버킷에 접두사 이름(velero/demobackup)과 함께 표시됩니다. 백업 내용에는 가상 머신의 볼륨 스냅샷, 로그 및 기타 메타데이터가 포함되어 있는 것을 볼 수 있습니다.

> StorageGrid에서는 테넌트 관리자에서 제공하는 S3 콘솔을 사용하여 백업 객체를 볼 수도 있습니다.

Path: / demobackup/ backups/ backup1/

Name	Size	Type	Last Modified	Storage Class
..				
backup1.tar.gz	230.36 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
velero-backup.json	3.35 KB	JSON File	4/15/2024 10:26:29 PM	STANDARD
backup1-resource-list.json.gz	1.12 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
backup1-itemoperations.json.gz	600 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-volumesnapshots.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-podvolumebackups.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-results.gz	49 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotclasses.json.gz	426 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotcontents.json.gz	1.43 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshots.json.gz	1.34 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-logs.gz	13.49 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD

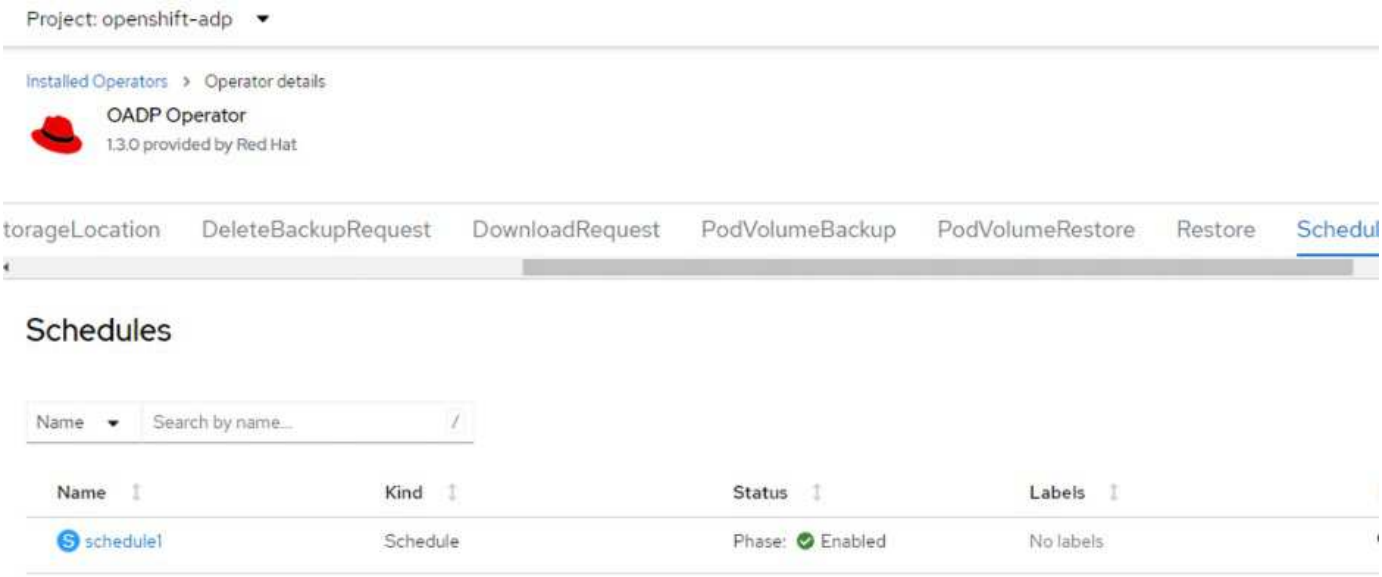
OpenShift Virtualization에서 VM에 대한 예약된 백업 생성

일정에 따라 백업을 만들려면 일정 CR을 만들어야 합니다. 일정은 백업을 만들고 싶은 시간을 지정할 수 있게 해주는 Cron 표현식입니다. 일정 CR을 만드는 샘플 YAML입니다.

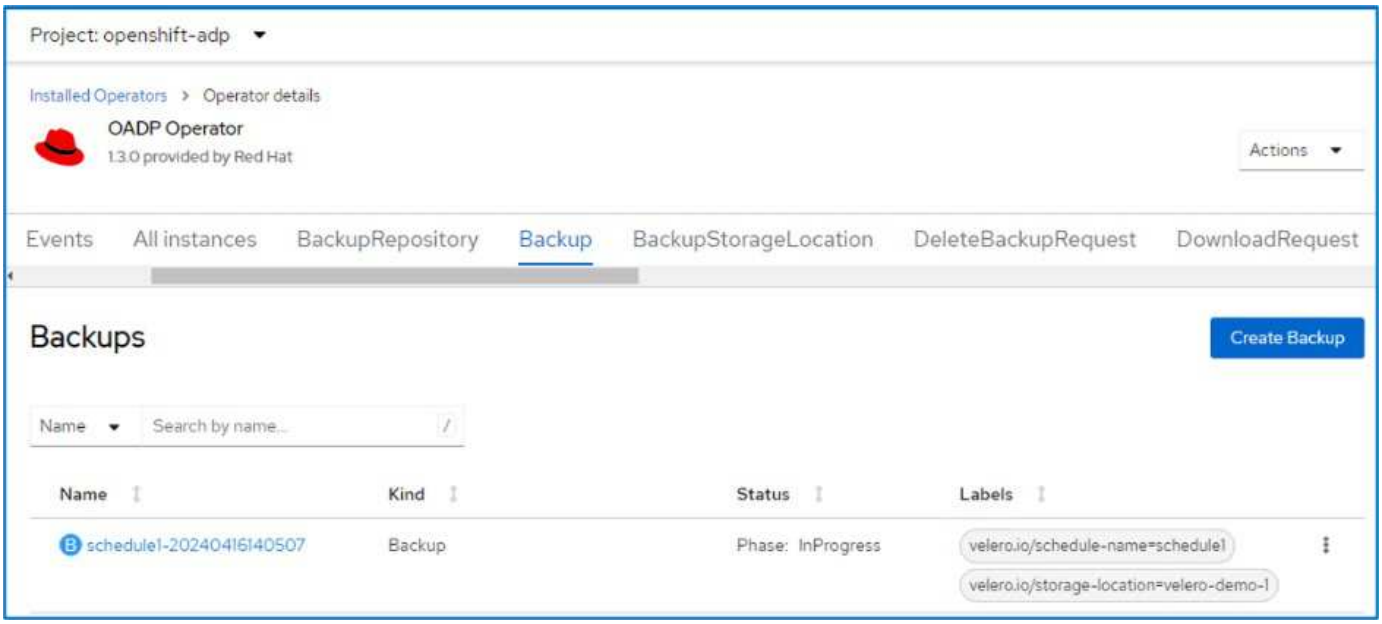
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

Cron 표현식 0 7 * * *는 매일 7시에 백업이 생성됨을 의미합니다. 백업에 포함될 네임스페이스와 백업의 저장 위치도 지정됩니다. 따라서 백업 CR 대신 일정 CR을 사용하여 지정된 시간과 빈도로 백업을 생성합니다.

일정이 생성되면 활성화됩니다.



백업은 이 일정에 따라 생성되며, 백업 탭에서 볼 수 있습니다.



Velero를 사용하여 Red Hat OpenShift Virtualization에서 백업된 VM 복원

Velero와 OpenShift API for Data Protection(OADP)을 사용하여 OpenShift Virtualization에서 VM을 복원합니다. 이 절차에는 백업에서 VM과 해당 영구 볼륨을 복구하기 위한 복원 사용자 지정 리소스(CR)를 만드는 작업이 포함되며, 원래 네임스페이스, 다른 네임스페이스로 복원하거나 대체 스토리지 클래스를 사용하는 옵션이 제공됩니다.

필수 조건

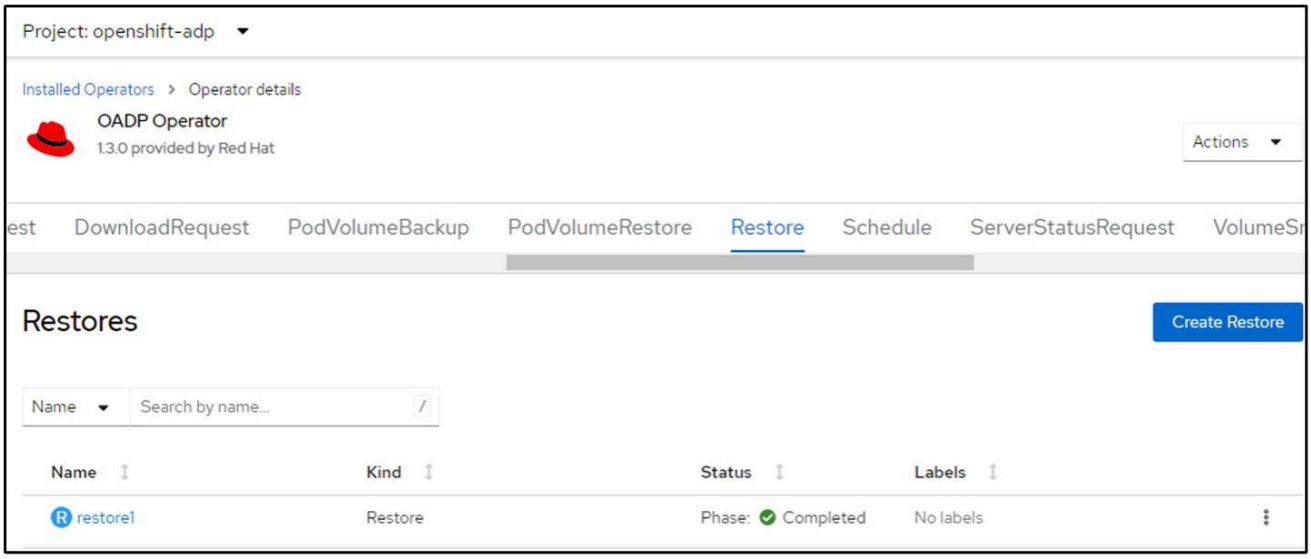
백업에서 복원하려면 가상 머신이 있던 네임스페이스가 실수로 삭제되었다고 가정해 보겠습니다.

동일한 네임스페이스로 복원

방금 만든 백업에서 복원하려면 복원 사용자 지정 리소스(CR)를 만들어야 합니다. 이름을 지정하고, 복원하려는 백업의 이름을 지정한 다음 restorePVs를 true로 설정해야 합니다. 추가 매개변수는 표시된 대로 설정할 수 있습니다."선적 서류 비치" . 만들기 버튼을 클릭하세요.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore1
  namespace: openshift-adp
spec:
  backupName: backup1
  restorePVs: true
```

단계가 완료로 표시되면 스냅샷이 촬영된 시점의 상태로 가상 머신이 복원된 것을 확인할 수 있습니다. (VM이 실행 중일 때 백업이 생성된 경우, 백업에서 VM을 복원하면 복원된 VM이 시작되고 실행 상태가 됩니다.) VM이 동일한 네임스페이스로 복원됩니다.



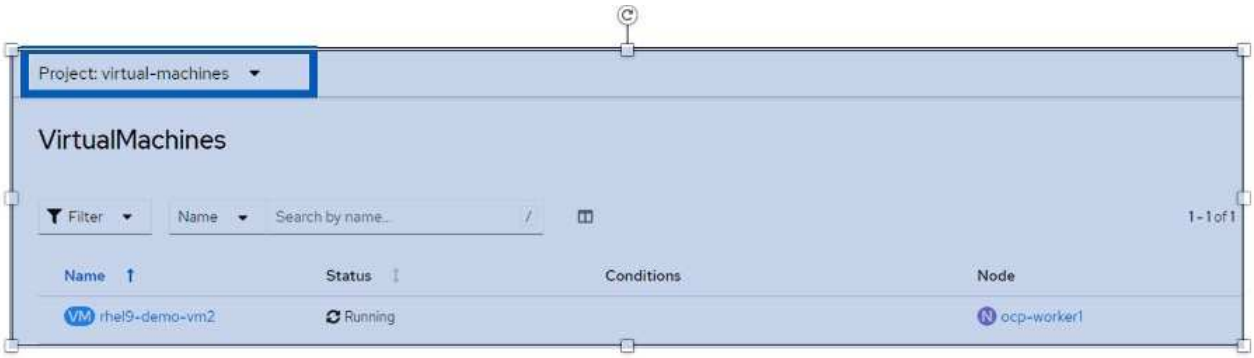
다른 네임스페이스로 복원

VM을 다른 네임스페이스로 복원하려면 Restore CR의 YAML 정의에 namespaceMapping을 제공할 수 있습니다.

다음 샘플 yaml 파일은 백업이 virtual-machines 네임스페이스로 수행되었을 때 virtual-machines-demo 네임스페이스의 VM과 해당 디스크를 복원하기 위한 Restore CR을 생성합니다.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
  includedNamespaces:
  - virtual-machines-demo
  namespaceMapping:
    virtual-machines-demo: virtual-machines
```

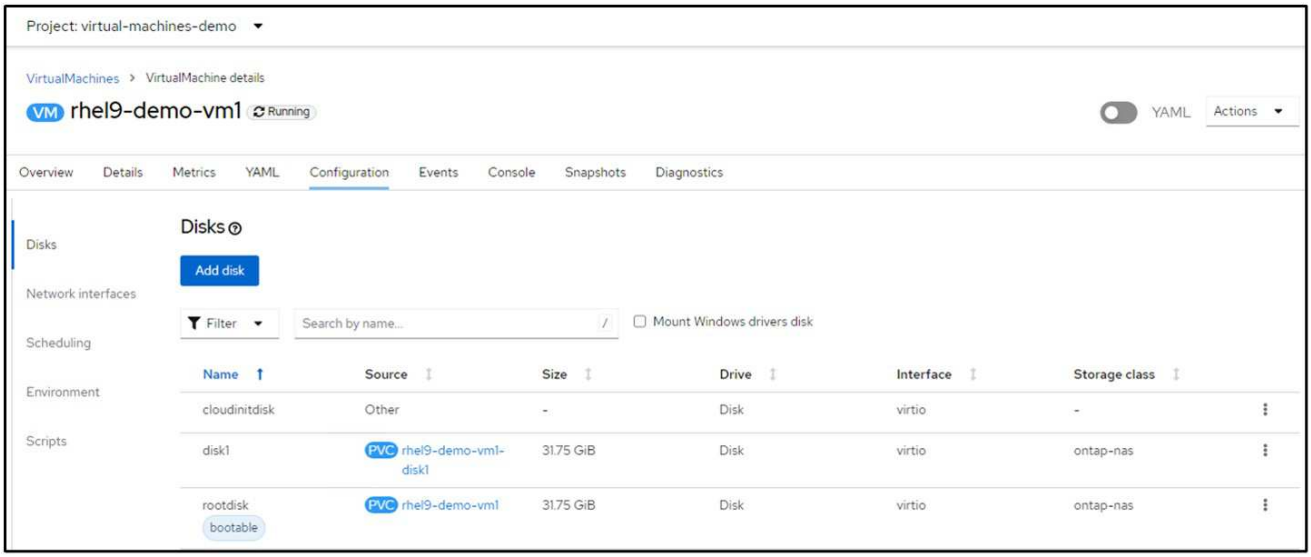
단계가 완료로 표시되면 스냅샷이 촬영된 시점의 상태로 가상 머신이 복원된 것을 확인할 수 있습니다. (VM이 실행 중일 때 백업이 생성된 경우, 백업에서 VM을 복원하면 복원된 VM이 시작되고 실행 상태가 됩니다.) VM은 yaml에 지정된 다른 네임스페이스로 복원됩니다.

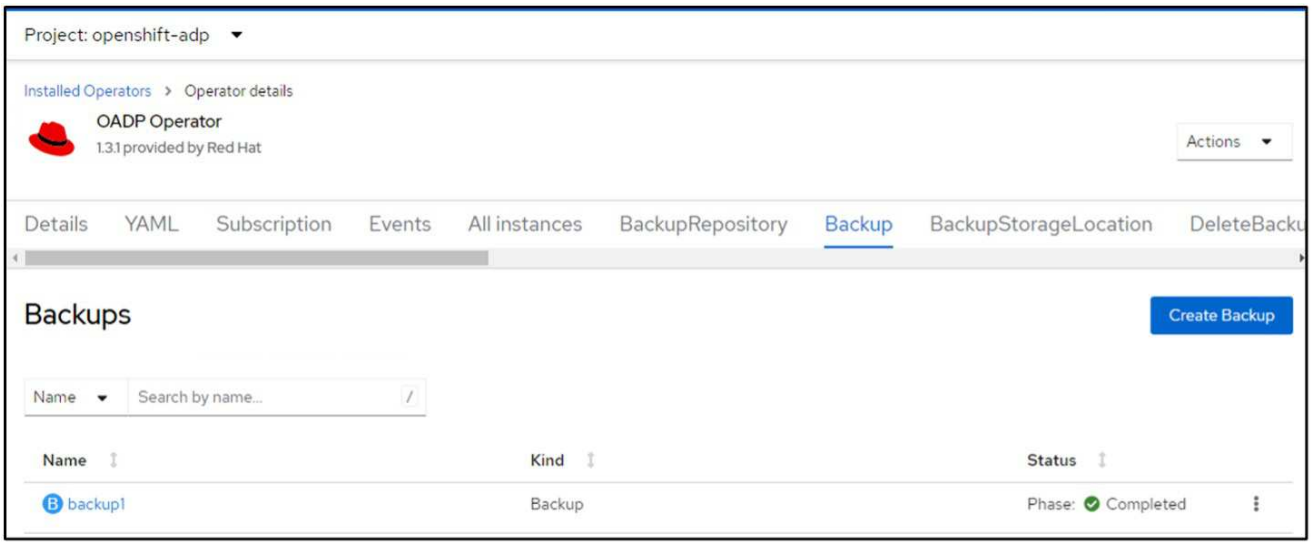


다른 스토리지 클래스로 복원

Velero는 JSON 패치를 지정하여 복원 중에 리소스를 수정하는 일반적인 기능을 제공합니다. JSON 패치는 리소스가 복원되기 전에 리소스에 적용됩니다. JSON 패치는 configmap에 지정되고 configmap은 restore 명령에서 참조됩니다. 이 기능을 사용하면 다양한 저장 클래스를 사용하여 복원할 수 있습니다.

아래 예에서 가상 머신은 생성 중에 디스크의 스토리지 클래스로 ontap-nas를 사용합니다. backup1이라는 이름의 가상 머신 백업이 생성됩니다.





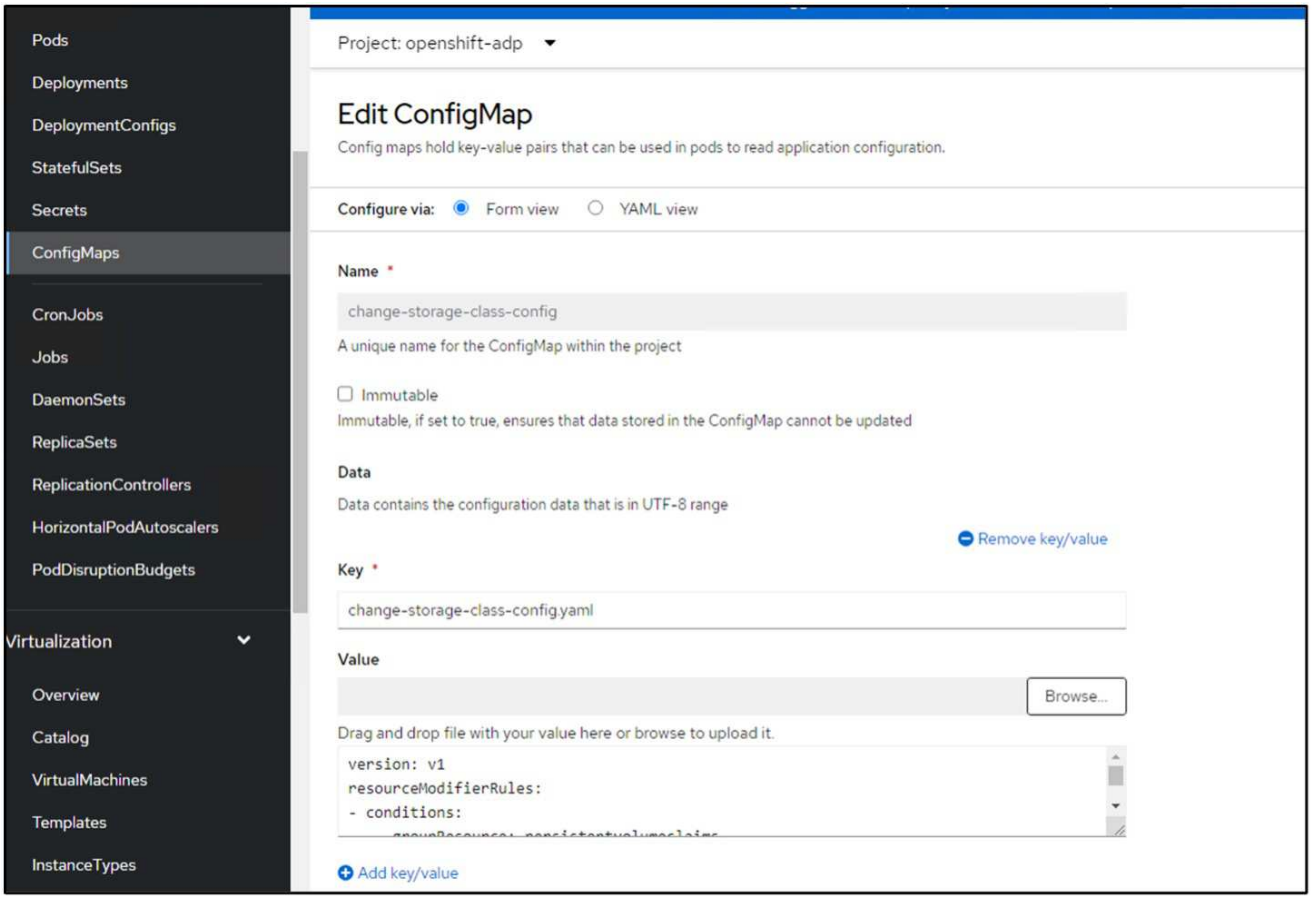
VM을 삭제하여 VM 손실을 시뮬레이션합니다.

예를 들어 ontap-nas-eco 스토리지 클래스와 같이 다른 스토리지 클래스를 사용하여 VM을 복원하려면 다음 두 단계를 수행해야 합니다.

1단계

다음과 같이 openshift-adp 네임스페이스에 구성 맵(콘솔)을 만듭니다. 스크린샷에 표시된 대로 세부 정보를 입력합니다. 네임스페이스 선택: openshift-adp 이름: change-storage-class-config(원하는 이름 사용 가능) 키: change-storage-class-config.yaml: 값:

```
version: v1
    resourceModifierRules:
    - conditions:
         groupResource: persistentvolumeclaims
         resourceNameRegex: "^rhel*"
         namespaces:
         - virtual-machines-demo
      patches:
      - operation: replace
        path: "/spec/storageClassName"
        value: "ontap-nas-eco"
```



결과적으로 생성되는 구성 맵 객체는 다음과 같습니다(CLI):

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"



BinaryData
====

Events:  <none>
```

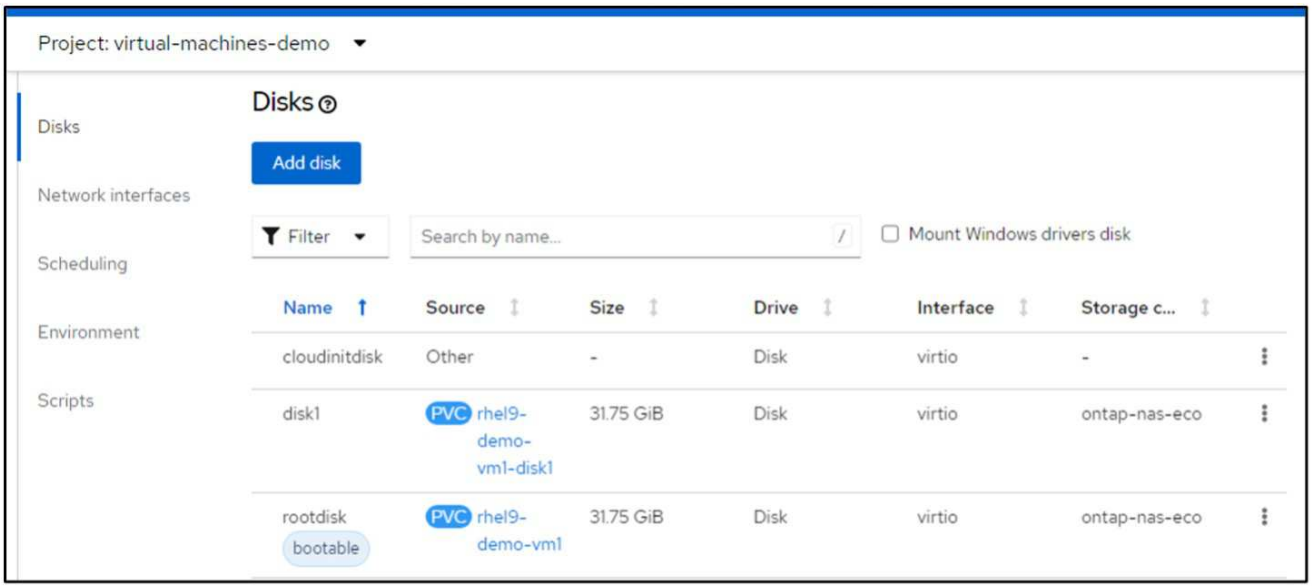
이 구성 맵은 복원이 생성될 때 리소스 수정자 규칙을 적용합니다. rhel로 시작하는 모든 영구 볼륨 클레임에 대해 스토리지 클래스 이름을 ontap-nas-eco로 바꾸는 패치가 적용됩니다.

2단계

VM을 복원하려면 Velero CLI에서 다음 명령을 사용하세요.

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

VM은 ontap-nas-eco 스토리지 클래스를 사용하여 생성된 디스크와 동일한 네임스페이스에 복원됩니다.



Velero를 사용하여 Red Hat OpenShift Virtualization에서 백업 CR을 삭제하거나 CR을 복원합니다.

Velero를 사용하여 OpenShift Virtualization의 VM에 대한 백업을 삭제하고 리소스를 복원합니다. OpenShift CLI를 사용하여 개체 스토리지 데이터를 보존하면서 백업을 삭제하거나, Velero CLI를 사용하여 백업 사용자 정의 리소스(CR)와 관련 스토리지 데이터를 모두 삭제합니다.

백업 삭제

OC CLI 도구를 사용하면 개체 스토리지 데이터를 삭제하지 않고도 백업 CR을 삭제할 수 있습니다.

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

백업 CR을 삭제하고 연관된 개체 스토리지 데이터를 삭제하려면 Velero CLI 도구를 사용하면 됩니다.

지침에 따라 CLI를 다운로드하세요."Velero 문서" .

Velero CLI를 사용하여 다음 삭제 명령을 실행하세요.

```
velero backup delete <backup_CR_name> -n <velero_namespace>
```

복원 삭제

Velero CLI를 사용하여 CR 복원을 삭제할 수 있습니다.

```
velero restore delete restore --namespace openshift-adp
```

oc 명령과 UI를 사용하여 복원 CR을 삭제할 수 있습니다.

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.