



타사 도구를 사용한 데이터 보호

NetApp Solutions

NetApp
September 23, 2024

목차

타사 도구를 사용한 데이터 보호	1
OpenShift Virtualization에서 OADP(OpenShift API for Data Protection)를 사용한 VM에 대한 데이터 보호	1
OADP(OpenShift API for Data Protection) Operator 설치	2
OpenShift Virtualization에서 VM에 대한 주문형 백업 생성	12
백업에서 VM 복원	15
Velero를 사용하여 에서 백업 및 복구 삭제	21

타사 도구를 사용한 데이터 보호

OpenShift Virtualization에서 OADP(OpenShift API for Data Protection)를 사용한 VM에 대한 데이터 보호

저자: 바누 선다, NetApp

참조 문서의 이 섹션에서는 NetApp ONTAP S3 또는 NetApp StorageGRID S3의 Velero를 사용하여 OADP(OpenShift API for Data Protection)를 사용하여 VM의 백업을 생성하는 방법에 대해 자세히 설명합니다. VM 디스크의 영구 볼륨(PVS) 백업은 CSI Astra Trident Snapshots을 사용하여 생성됩니다.

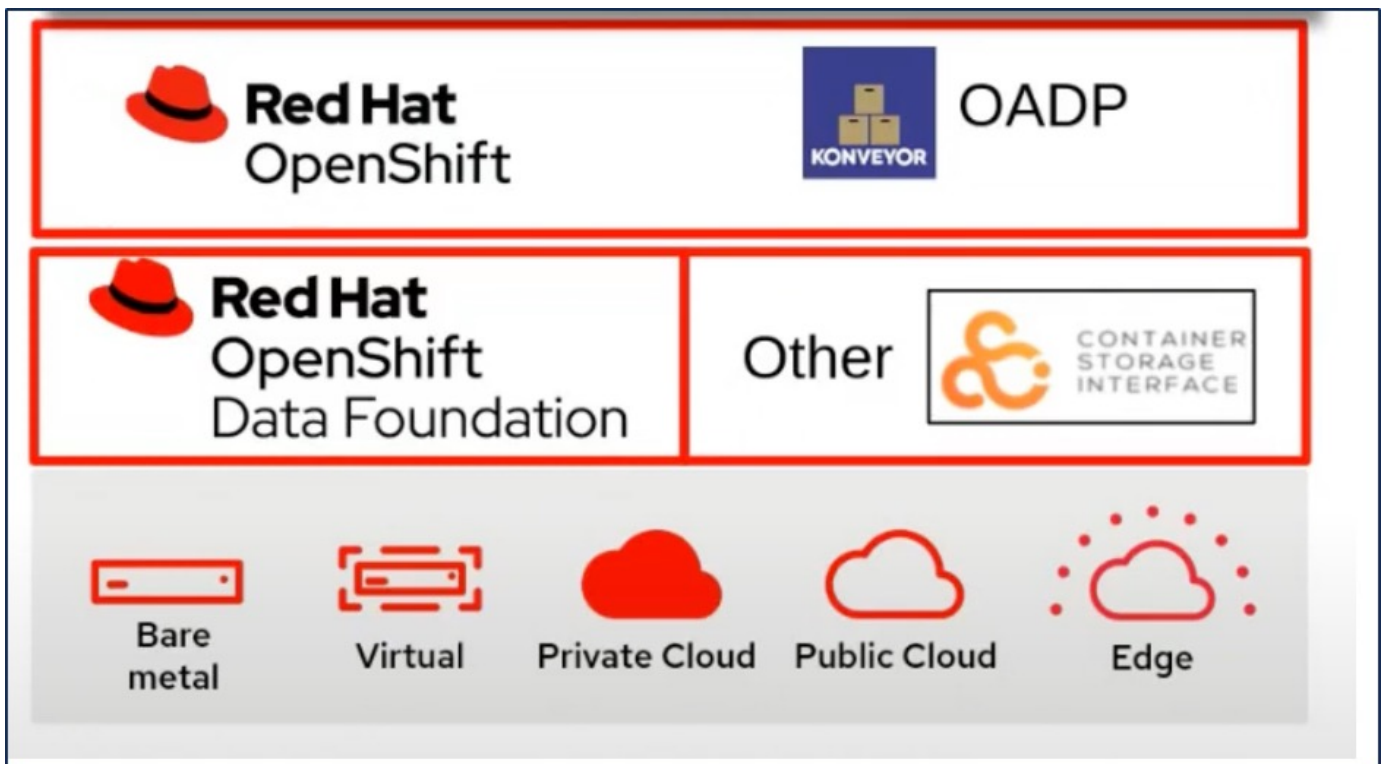
OpenShift 가상화 환경의 가상 머신은 OpenShift Container 플랫폼의 작업자 노드에서 실행되는 컨테이너화된 애플리케이션입니다. VM 메타데이터와 VM의 영구 디스크를 보호하여 VM이 손실되거나 손상된 경우 복구할 수 있도록 하는 것이 중요합니다.

를 사용하여 OpenShift 클러스터에 통합된 ONTAP 스토리지를 통해 OpenShift 가상화 VM의 영구 디스크를 백업할 수 있습니다 "Astra Trident CSI". 이 섹션에서는 를 사용합니다 "데이터 보호를 위한 OpenShift API(OADP)" 데이터 볼륨을 포함한 VM의 백업을 에 수행합니다

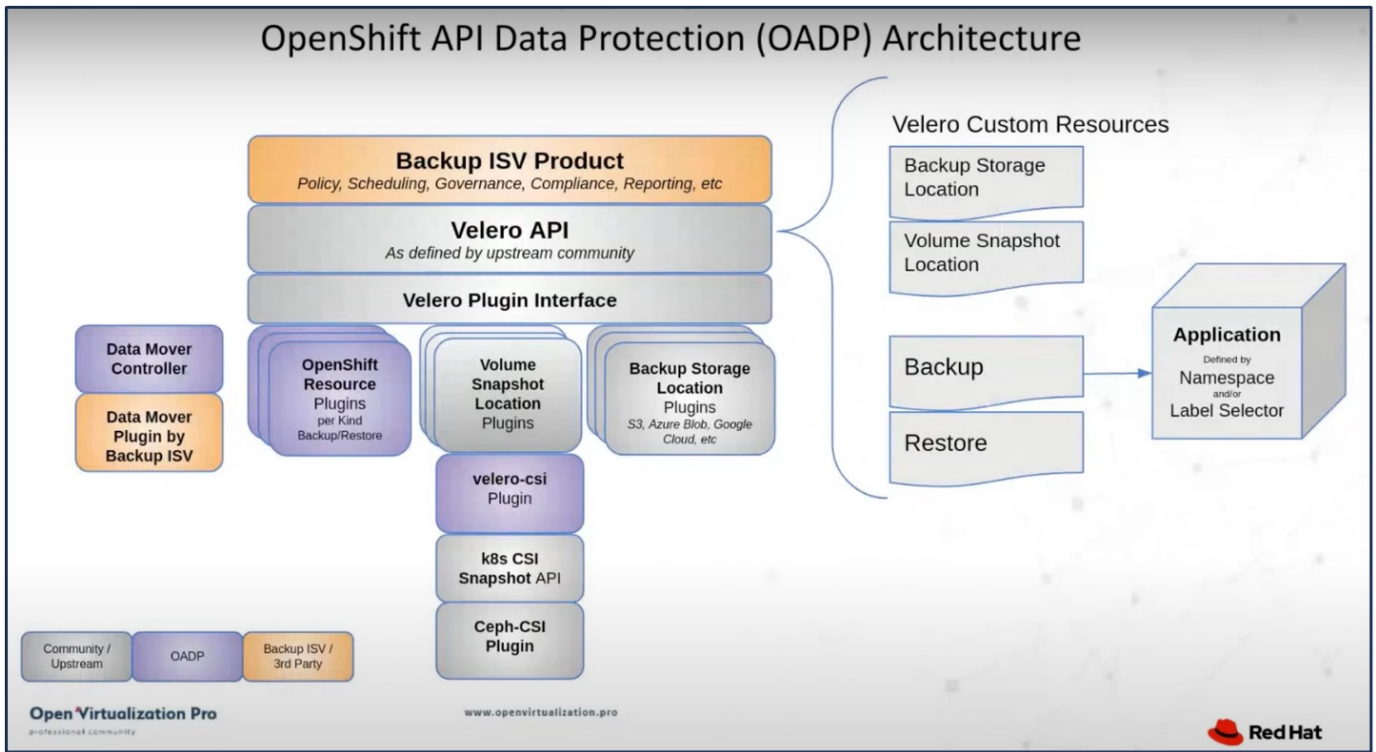
- ONTAP 오브젝트 스토리지
- StorageGRID

그런 다음 필요할 때 백업에서 복원합니다.

OADP는 OpenShift 클러스터에서 애플리케이션의 백업, 복원 및 재해 복구를 지원합니다. OADP로 보호할 수 있는 데이터에는 Kubernetes 리소스 개체, 영구 볼륨 및 내부 이미지가 포함됩니다.



Red Hat OpenShift는 데이터 보호를 위해 OpenSource 커뮤니티에서 개발한 솔루션을 활용했습니다. "벨레로"는 Kubernetes 클러스터 리소스 및 영구 볼륨을 안전하게 백업 및 복원, 재해 복구 수행, 마이그레이션하기 위한 오픈 소스 툴입니다. Velero를 쉽게 사용하기 위해 OpenShift는 OADP 운영자와 Velero 플러그인을 개발하여 CSI 스토리지 드라이버와 통합했습니다. 표시되는 OADP API의 핵심은 Velero API를 기반으로 합니다. OADP 운영자를 설치하고 구성한 후 수행할 수 있는 백업/복구 작업은 Velero API에 의해 노출되는 작업을 기반으로 합니다.



OADP 1.3은 OpenShift 클러스터 4.12 이상의 운영자 허브에서 사용할 수 있습니다. CSI 볼륨 스냅샷을 원격 객체 저장소로 이동할 수 있는 Data Mover가 내장되어 있습니다. 따라서 백업 중에 스냅샷을 객체 스토리지 위치로 이동하여 이동성 및 내구성을 제공합니다. 그러면 재해 후 스냅샷을 복원에 사용할 수 있습니다.

다음은 이 단원의 예제에 사용된 다양한 구성 요소의 버전입니다

- OpenShift 클러스터 4.14
- Red Hat에서 제공하는 OperatorOpenShift Virtualization Operator를 통해 OpenShift Virtualization 설치
- Red Hat에서 제공하는 OADP Operator 1.13
- Linux용 Velero CLI 1.13
- Astra Trident 24.02
- ONTAP 9.12 를 참조하십시오

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

OADP(OpenShift API for Data Protection) Operator 설치

이 섹션에서는 OADP(OpenShift API for Data Protection) Operator의 설치에 대해 간략하게 설명합니다.

필수 구성 요소

- RHCOS 작업자 노드가 있는 베어 메탈 인프라에 설치된 Red Hat OpenShift 클러스터(버전 4.12 이상)
- Astra Trident를 사용하여 클러스터에 통합된 NetApp ONTAP 클러스터
- ONTAP 클러스터에서 SVM으로 구성된 Trident 백엔드
- OpenShift 클러스터에 구성된 StorageClass로, Astra Trident를 프로비저닝자로 사용합니다
- 클러스터에 생성된 Trident 스냅샷 클래스입니다
- Red Hat OpenShift 클러스터에 대한 클러스터 관리자 액세스
- NetApp ONTAP 클러스터에 대한 관리 액세스
- OpenShift Virtualization 운영자가 설치 및 구성되었습니다
- OpenShift Virtualization에서 네임스페이스로 배포된 VM
- tridentctl 및 OC 도구가 설치되고 \$PATH에 추가된 관리 워크스테이션



VM이 실행 중인 상태일 때 VM을 백업하려면 해당 가상 머신에 QEMU 게스트 에이전트를 설치해야 합니다. 기존 템플릿을 사용하여 VM을 설치하는 경우 QEMU 에이전트가 자동으로 설치됩니다. QEMU를 사용하면 게스트 에이전트가 스냅샷 프로세스 중에 게스트 OS의 전송 중인 데이터를 정지하고 데이터 손상을 방지할 수 있습니다. QEMU가 설치되어 있지 않은 경우 백업을 수행하기 전에 가상 컴퓨터를 중지할 수 있습니다.

OADP Operator를 설치하는 단계입니다

1. 클러스터의 운영자 허브로 이동하여 Red Hat OADP 연산자를 선택합니다. 설치 페이지에서 모든 기본 선택 항목을 사용하고 설치를 클릭합니다. 다음 페이지에서 모든 기본값을 사용하고 Install(설치) 을 클릭합니다. OADP 운영자는 OpenShift-ADP 네임스페이스에 설치됩니다.

The screenshot shows the OperatorHub interface. On the left is a navigation sidebar with categories like Home, Operators, Workloads, Virtualization, Networking, Storage, Builds, and Observe. The 'Operators' section is expanded, and 'OperatorHub' is selected. The main content area displays a search for 'OADP' under the 'All Items' tab. Two search results are shown: one from Red Hat and one from the Community. Both results describe the OADP Operator as an OpenShift API for Data Protection operator that sets up and installs Data Protection and Velero on the OpenShift cluster.



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](#)

Activate Windows

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	openshift-cnrv	openshift-cnrv	Succeeded Up to date
OADP Operator 1.3.0 provided by Red Hat	openshift-adp	openshift-adp	Succeeded Up to date
Package Server 0.0.1-snapshot provided by	openshift-operator-lifecycle-manager	openshift-operator-lifecycle-manager	Succeeded

ONTAP S3 세부 정보를 포함한 Velero 구성을 위한 사전 요구 사항

조작자가 성공적으로 설치되면 Velero 인스턴스를 구성합니다.

S3 호환 객체 스토리지를 사용하도록 Velero를 구성할 수 있습니다. 에 표시된 절차를 사용하여 ONTAP S3를 구성합니다 "[ONTAP 설명서의 "객체 스토리지 관리" 섹션을 참조하십시오](#)". Velero와 통합하려면 ONTAP S3 구성에서 다음 정보가 필요합니다.

- S3에 액세스하는 데 사용할 수 있는 논리 인터페이스(LIF)
- 액세스 키 및 비밀 액세스 키가 포함된 S3에 액세스하기 위한 사용자 자격 증명입니다
- 사용자에게 대한 액세스 권한이 있는 백업을 위한 S3의 버킷 이름입니다
- 개체 저장소에 대한 보안 액세스를 위해 TLS 인증서를 개체 저장소 서버에 설치해야 합니다.

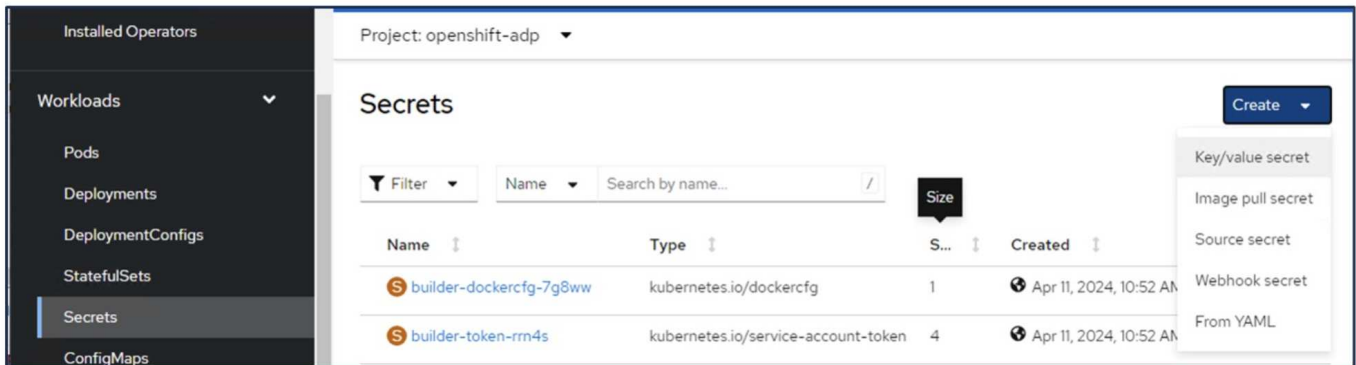
StorageGRID S3 세부 정보를 포함한 Velero 구성을 위한 사전 요구 사항

S3 호환 객체 스토리지를 사용하도록 Velero를 구성할 수 있습니다. 에 나와 있는 절차를 사용하여 StorageGRID S3를 구성할 수 있습니다 "[StorageGRID 설명서](#)". Velero와 통합하려면 StorageGRID S3 구성에서 다음 정보가 필요합니다.

- S3에 액세스하는 데 사용할 수 있는 끝점입니다
- 액세스 키 및 비밀 액세스 키가 포함된 S3에 액세스하기 위한 사용자 자격 증명입니다
- 사용자에게 대한 액세스 권한이 있는 백업을 위한 S3의 버킷 이름입니다
- 개체 저장소에 대한 보안 액세스를 위해 TLS 인증서를 개체 저장소 서버에 설치해야 합니다.

Velero 구성 단계

- 먼저 ONTAP S3 사용자 자격 증명 또는 StorageGRID 테넌트 사용자 자격 증명에 대한 암호를 생성합니다. 나중에 Velero를 구성하는 데 사용됩니다. CLI 또는 웹 콘솔에서 암호를 생성할 수 있습니다. 웹 콘솔에서 암호를 생성하려면 비밀 을 선택한 다음 키/값 비밀 을 클릭합니다. 그림과 같이 자격 증명 이름, 키 및 값을 입력합니다. S3 사용자의 액세스 키 ID와 비밀 액세스 키를 사용해야 합니다. 암호의 이름을 적절하게 지정합니다. 아래 샘플에서 ontap-s3-credentials라는 ONTAP S3 사용자 자격 증명으로 구성된 암호가 생성됩니다.



Project: openshift-adp ▾

Edit key/value secret

Key/value secrets let you inject sensitive data into your application as files or environment variables.

Secret name *

 Unique name of the new secret.

Key *

Value

 Browse...

Drag and drop file with your value here or browse to upload it.

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

+ Add key/value

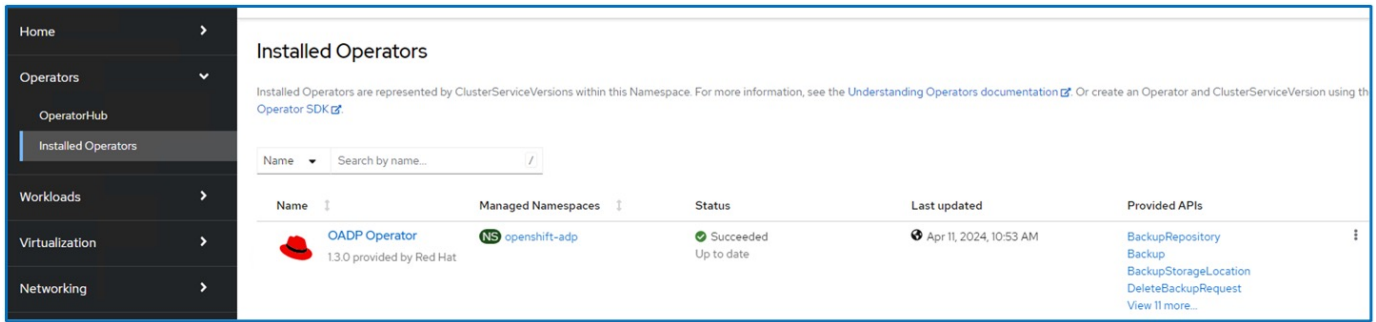
CLI에서 sg-s3-credentials라는 암호를 생성하려면 다음 명령을 사용할 수 있습니다.

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

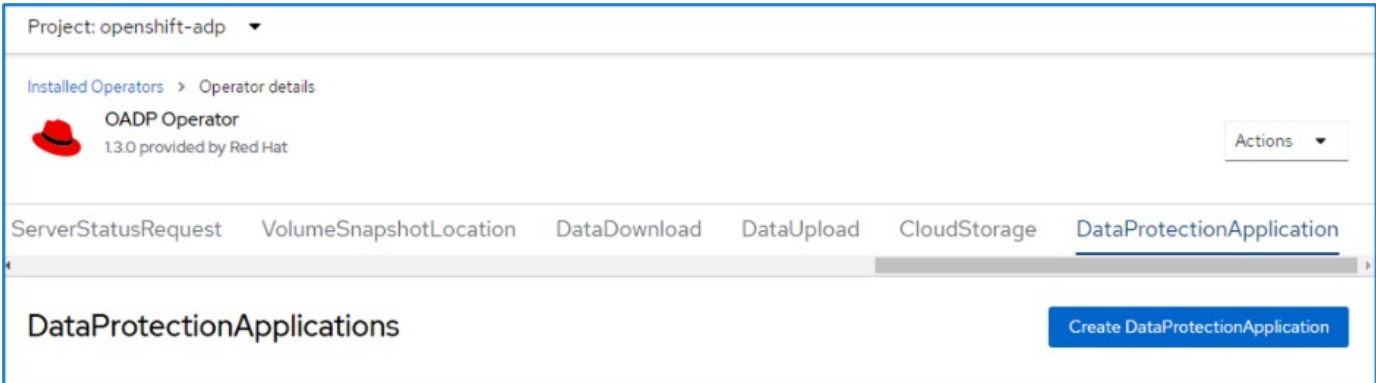
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

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

- 그런 다음 Velero를 구성하려면 Operators(오퍼레이터) 아래의 메뉴 항목에서 Installed Operators(설치된 운영자)를 선택하고 OADP operator(OADP 운영자)를 클릭한 다음 DataProtectionApplication(DataProtectionApplication) 탭을 선택합니다.



Create DataProtectionApplication을 클릭합니다. 폼 보기에서 DataProtection 응용 프로그램의 이름을 제공하거나 기본 이름을 사용합니다.



이제 YAML 보기로 이동하여 아래의 YAML 파일 예제에 표시된 사양 정보를 대체합니다.

- ONTAP S3을 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 S3을 BackupLocation 및 snapshotLocation으로 Velero를 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 유사한 다음 매개 변수에 맞게 구성해야 합니다

backupLocations

ONTAP S3 또는 StorageGRID S3(YAML에 표시된 자격 증명 및 기타 정보 포함)는 velero의 기본 BackupLocation으로 구성됩니다.

- 스냅샷 위치**
CSI(Container Storage Interface) 스냅샷을 사용하는 경우, CSI 드라이버를 등록하기 위해 VolumeSnapshotClass CR을 생성하므로 스냅샷 위치를 지정할 필요가 없습니다. 이 예에서는 Astra Trident CSI를 사용하며 이전에 Trident CSI 드라이버를 사용하여 VolumeSnapShotClass CR을 생성한 적이 있습니다.
- CSI 플러그인 활성화
CSI 스냅샷을 사용하여 영구 볼륨을 백업하려면 **Velero**용 기본 플러그인에 **CSI**를 추가합니다.
CSI 백업 **PVC**를 백업하기 위한 **Velero CSI** 플러그인은 `velero.io/csi-volumesnapshot-class**` 라벨이 설정된 클러스터에서 VolumeSnapshotClass를 선택합니다. 이를 위해
 - 트라이덴트 VolumeSnapshotClass를 생성해야 합니다.
 - trident-snapshotclass의 라벨을 편집하여 로 설정합니다
velero.io/csi-volumesnapshot-class=true 아래 표시된 대로.

The screenshot shows the Kubernetes dashboard interface. On the left, a dark sidebar contains a navigation menu with categories 'Networking' and 'Storage'. Under 'Storage', several options are listed: 'PersistentVolumes', 'PersistentVolumeClaims', 'StorageClasses', 'VolumeSnapshots', 'VolumeSnapshotClasses' (which is highlighted with a blue bar), and 'VolumeSnapshotContents'. The main content area on the right is titled 'VolumeSnapshotClasses > VolumeSnapshotClass details'. At the top, there is a blue badge with 'VSC' and the text 'trident-snapshotclass'. Below this, there are three tabs: 'Details' (which is active), 'YAML', and 'Events'. The 'Details' tab shows the 'VolumeSnapshotClass details' section. It includes a 'Name' field with the value 'trident-snapshotclass' and a 'Labels' field with the value 'velero.io/csi-volumesnapshot-class=true'. An 'Edit' button with a pencil icon is located to the right of the labels field.

VolumeSnapshot 개체가 삭제된 경우에도 스냅샷이 유지될 수 있는지 확인하십시오. 이 작업은 * deletionPolicy * 를 보존하도록 설정하여 수행할 수 있습니다. 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

```

VolumeSnapshotClasses > VolumeSnapshotClass details

VSC trident-snapshotclass

Details | YAML | Events

VolumeSnapshotClass details

Name
trident-snapshotclass

Labels Edit

velero.io/csi-volumesnapshot-class=true


Annotations
1 annotation

Driver
csi.trident.netapp.io

Deletion policy
Retain

DataProtectionApplication 이 만들어지고 상태가 Reconciled 인지 확인합니다.

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat Actions

ServerStatusRequest | VolumeSnapshotLocation | DataDownload | DataUpload | CloudStorage | **DataProtectionApplication**

DataProtectionApplications

Create DataProtectionApplication


Name Search by name... /

Name	Kind	Status	Labels
DPA velero-demo	DataProtectionApplication	Condition: Reconciled	No labels

OADP 운영자가 해당 BackupStorageLocation을 생성합니다. 이 값은 백업을 생성할 때 사용됩니다.

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat


Actions ▾

Repository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRe

BackupStorageLocations

Create BackupStorageLocation

Name ▾ Search by name... /

Name ↓	Kind ↓	Status ↓	Labels ↓
 velero-demo-1	BackupStorageLocation	Phase: Available	<ul style="list-style-type: none"> app.kubernetes.io/component=bsl app.kubernetes.io/instance=velero-demo-1 app.kubernetes.io/manager=oadp-oper... app.kubernetes.io/n...=oadp-operator-ve... openshift.io/oadp=True openshift.io/oadp-registry=True

OpenShift Virtualization에서 VM에 대한 주문형 백업 생성

이 섹션에서는 OpenShift Virtualization에서 VM에 대한 주문형 백업을 생성하는 방법에 대해 간략하게 설명합니다.

VM 백업을 생성하는 단계입니다

전체 VM(VM 메타데이터 및 VM 디스크)의 주문형 백업을 생성하려면 **Backup** 탭을 클릭합니다. 그러면 백업 사용자 지정 리소스(CR)가 생성됩니다. Backup CR을 생성하기 위한 샘플 YAML이 제공됩니다. 이 YAML을 사용하면 지정된 네임스페이스의 VM 및 해당 디스크가 백업됩니다. 예 표시된 대로 추가 매개변수를 설정할 수 있습니다 "[문서화](#)".

디스크를 지원하는 영구 볼륨의 스냅샷이 CSI에 의해 생성됩니다. VM의 백업과 해당 디스크의 스냅샷이 생성되어 YAML에 지정된 백업 위치에 저장됩니다. 백업은 TTL에 지정된 대로 30일 동안 시스템에 유지됩니다.

```

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 완료된 것으로 표시됩니다.

The screenshot shows the OpenShift console interface for the OADP Operator. The 'Backups' tab is selected, showing a table with the following data:

Name	Kind	Status	Labels
backup1	Backup	Phase: ✔ Completed	velero.io/storage-location=velero-demo-1

S3 브라우저 애플리케이션을 사용하여 오브젝트 스토리지에서 백업을 검사할 수 있습니다. 백업 경로가 구성된 버킷에 접두사 이름(velero/demobBackup)과 함께 표시됩니다. 백업 콘텐츠에는 볼륨 스냅샷, 로그 및 가상 머신의 기타 메타데이터가 포함됩니다.



StorageGRID에서는 테넌트 관리자에서 사용할 수 있는 S3 콘솔을 사용하여 백업 개체를 볼 수도 있습니다.

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 생성하려면 예약 CR을 생성해야 합니다.

스케줄은 단순히 cron 표현식일 뿐이므로 백업을 생성할 시간을 지정할 수 있습니다. 일정 CR을 생성하기 위한 샘플 YAML

```

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 * * * 은 매일 7:00에 백업이 생성됨을 의미합니다.

백업에 포함할 네임스페이스와 백업에 대한 스토리지 위치도 지정됩니다. 따라서 Backup CR 대신 Schedule CR을 사용하여 지정된 시간과 빈도에 백업을 생성합니다.

스케줄이 생성되면 Enabled(활성화) 가 됩니다.



OADP Operator
1.3.0 provided by Red Hat

storageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRestore Restore Schedule

Schedules

Name	Kind	Status	Labels
schedule1	Schedule	Phase: ✔ Enabled	No labels

백업은 이 일정에 따라 생성되며 백업 탭에서 볼 수 있습니다.

Project: openshift-adp

Installed Operators > Operator details

OADP Operator
1.3.0 provided by Red Hat

Actions

Events All instances BackupRepository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest

Backups

Create Backup

Name	Kind	Status	Labels
schedule1-20240416140507	Backup	Phase: InProgress	velero.io/schedule-name=schedule1 velero.io/storage-location=velero-demo-1

백업에서 VM 복원

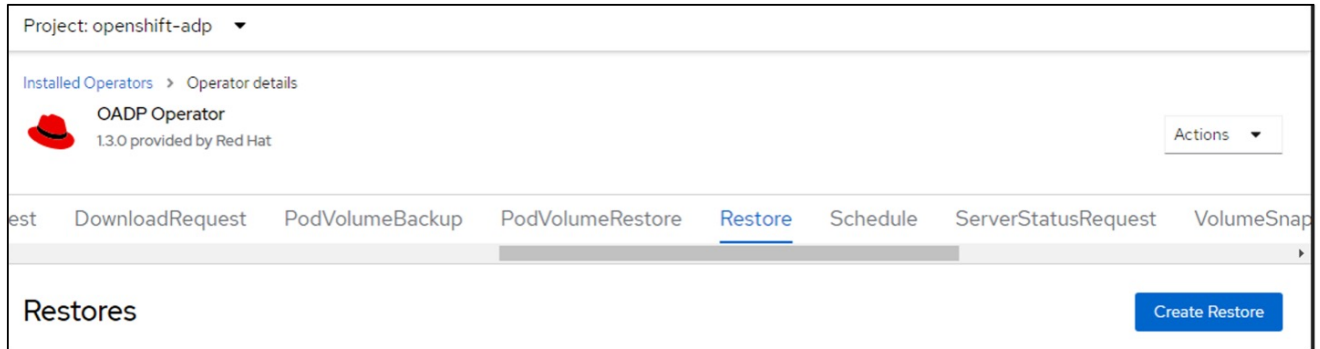
이 섹션에서는 백업에서 가상 머신을 복구하는 방법에 대해 설명합니다.

필수 구성 요소

백업에서 복원하기 위해 가상 시스템이 있던 네임스페이스가 실수로 삭제되었다고 가정합니다.

동일한 네임스페이스로 복원합니다

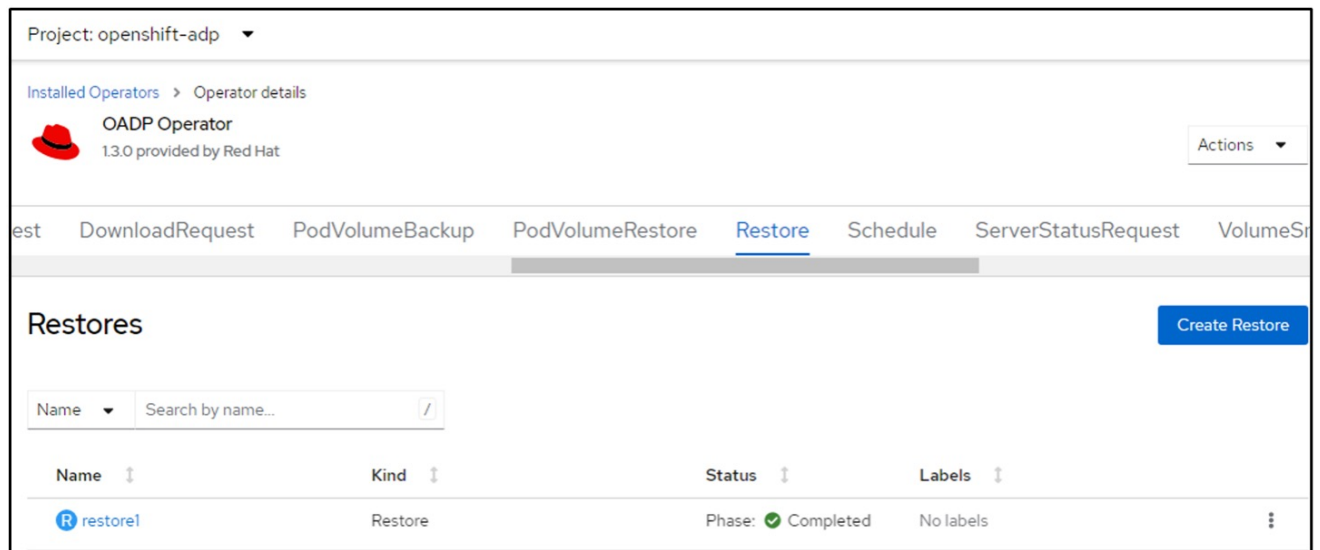
방금 만든 백업에서 복원하려면 CR(사용자 지정 리소스 복원)을 만들어야 합니다. 이름을 지정하고 복원할 백업 이름을 지정한 다음 restorePV를 true로 설정해야 합니다. 에 표시된 대로 추가 매개변수를 설정할 수 있습니다 "문서화". 생성 버튼을 클릭합니다.



The screenshot shows the OADP Operator interface for the 'openshift-adp' project. The 'Restore' tab is selected, and a 'Create Restore' button is visible in the top right corner.

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

단계가 완료됨으로 표시되면 가상 시스템이 스냅샷을 생성한 상태로 복구되었음을 알 수 있습니다. (VM이 실행 중일 때 백업이 생성된 경우 백업에서 VM을 복원하면 복원된 VM이 시작되고 실행 중 상태가 됩니다.) VM이 동일한 네임스페이스로 복원됩니다.



The screenshot shows the OADP Operator interface for the 'openshift-adp' project. The 'Restore' tab is selected, and a table of restores is displayed. The table has columns for Name, Kind, Status, and Labels. A single restore named 'restore1' is listed with a status of 'Phase: Completed' and 'No labels'.

Name	Kind	Status	Labels
restore1	Restore	Phase: ✔ Completed	No labels

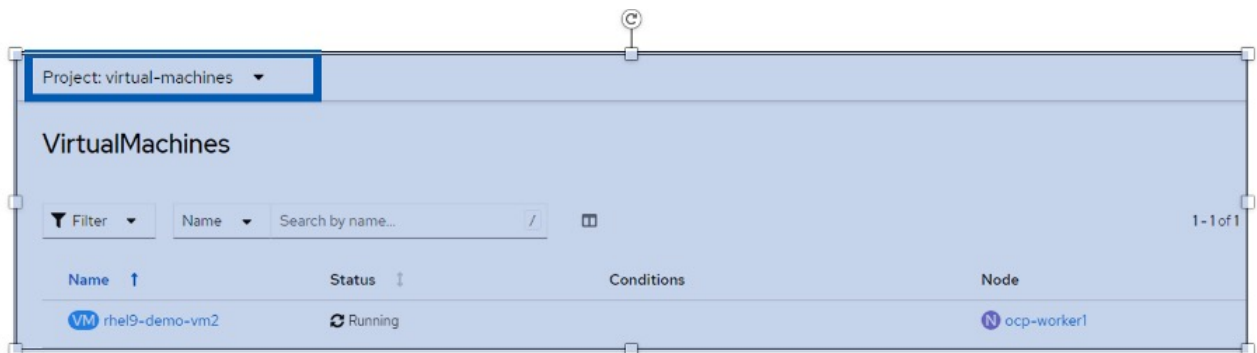
다른 네임스페이스로 복원합니다

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

다음 샘플 YAML 파일은 가상 머신 네임스페이스로 백업이 수행되었을 때 가상 머신 데모 네임스페이스에서 VM 및 해당 디스크를 복원하는 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 완료됨으로 표시되면 가상 시스템이 스냅샷을 생성한 상태로 복구되었음을 알 수 있습니다. (VM이 실행 중일 때 백업이 생성된 경우 백업에서 VM을 복원하면 복원된 VM이 시작되고 실행 중 상태가 됩니다.) VM은 YAML에 지정된 다른 네임스페이스로 복원됩니다.



다른 저장소 클래스로 복원합니다

Velero는 복구 중에 json 패치를 지정하여 리소스를 수정할 수 있는 일반 기능을 제공합니다. json 패치는 복구되기 전에 리소스에 적용됩니다. json 패치는 configmap에 지정되고 configmap은 restore 명령에서 참조됩니다. 이 기능을 사용하면 다른 저장소 클래스를 사용하여 복원할 수 있습니다.

아래 예에서 가상 머신은 생성 중 ONTAP-NAS를 디스크의 스토리지 클래스로 사용합니다. backup1이라는 이름의 가상 머신의 백업이 생성됩니다.

The screenshot shows the 'Configuration' tab for a virtual machine named 'rhel9-demo-vm1'. Under the 'Disks' section, there is a table listing the disks:

Name	Source	Size	Drive	Interface	Storage class
cloudinitdisk	Other	-	Disk	virtio	-
disk1	PVC rhel9-demo-vm1-disk1	31.75 GiB	Disk	virtio	ontap-nas
rootdisk	PVC rhel9-demo-vm1	31.75 GiB	Disk	virtio	ontap-nas

The screenshot shows the 'Backup' tab for the OADP Operator. It displays a table with one backup entry:

Name	Kind	Status
backup1	Backup	Phase: Completed

VM을 삭제하여 VM의 손실을 시뮬레이션합니다.

다른 스토리지 클래스(예: ONTAP-NAS-eco 스토리지 클래스)를 사용하여 VM을 복원하려면 다음 두 단계를 수행해야 합니다.

- 1단계**

OpenShift-ADP 네임스페이스에서 다음과 같이 구성 맵(콘솔)을 생성합니다.

스크린샷에 표시된 대로 세부 정보를 입력합니다.

네임스페이스: OpenShift-ADP를 선택합니다

이름: change-storage-class-config(모든 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"
```

Project: openshift-adp

Edit ConfigMap

Config maps hold key-value pairs that can be used in pods to read application configuration.

Configure via: Form view YAML view

Name *

change-storage-class-config

A unique name for the ConfigMap within the project

Immutable
Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated

Data

Data contains the configuration data that is in UTF-8 range

Key *

change-storage-class-config.yaml

Value

Browse...

Drag and drop file with your value here or browse to upload it.

```
version: v1
resourceModifierRules:
- conditions:
  groupResource: persistentvolumeclaims
```

[+ Add key/value](#)

결과 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 복구가 생성될 때 리소스 한정자 규칙을 적용합니다. rhel로 시작하는 모든 영구 볼륨 클레임에 대해 스토리지 클래스 이름을 ONTAP-nas-eco로 대체하는 패치가 적용됩니다.

- 2단계**

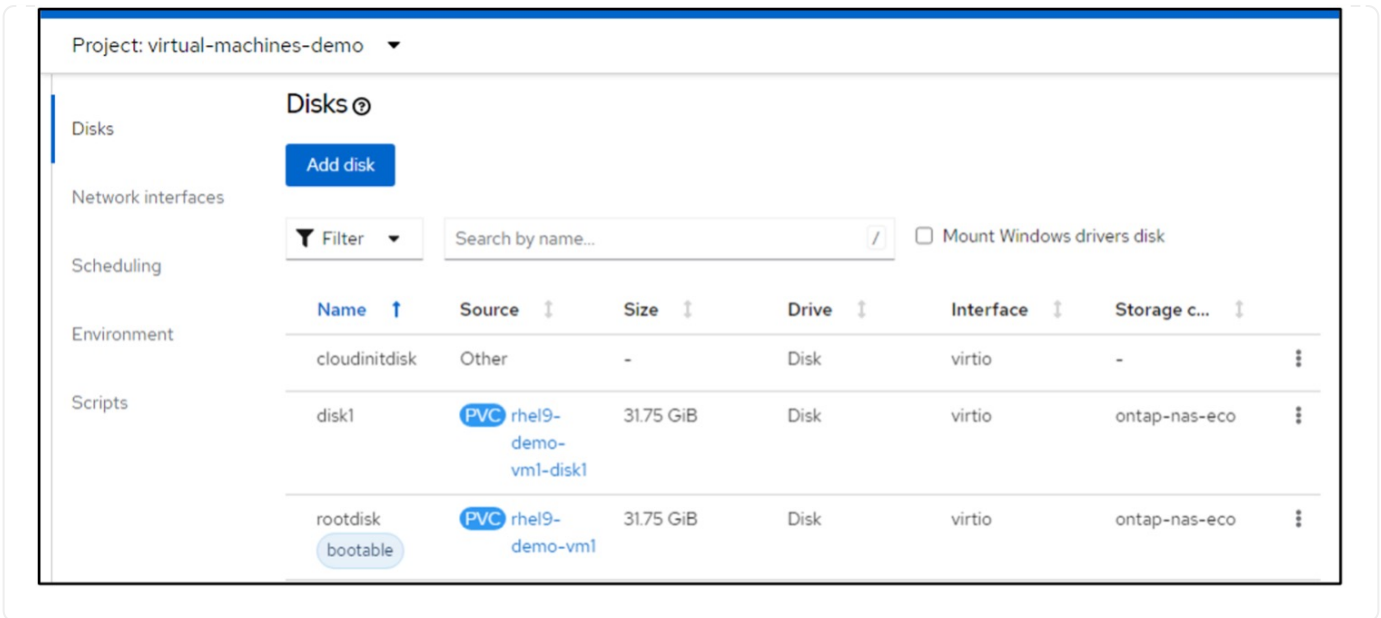
VM을 복원하려면 Velero CLI에서 다음 명령을 사용합니다.

```

#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 디스크를 사용하여 동일한 네임스페이스에서 복원됩니다.



Velero를 사용하여 에서 백업 및 복구 삭제

이 섹션에서는 Velero를 사용하여 OpenShift Virtualization에서 VM에 대한 백업 및 복원을 삭제하는 방법에 대해 간략하게 설명합니다.

백업을 삭제하는 중입니다

OC CLI 도구를 사용하여 개체 저장소 데이터를 삭제하지 않고 백업 CR을 삭제할 수 있습니다.

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

Backup CR을 삭제하고 연결된 객체 스토리지 데이터를 삭제하려면 Velero CLI 툴을 사용하여 삭제할 수 있습니다.

의 지침에 설명된 대로 CLI를 다운로드합니다 "[Velero 설명서](#)".

Velero CLI를 사용하여 다음 delete 명령을 실행합니다

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

복원 삭제

Velero CLI를 사용하여 Restore CR을 삭제할 수 있습니다

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

UI와 OC 명령을 사용하여 복원 CR을 삭제할 수 있습니다

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


저작권 정보

Copyright © 2024 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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