



# Protezione dei dati mediante strumenti di terze parti

NetApp Solutions

NetApp  
September 26, 2024

# Sommario

- Protezione dei dati mediante strumenti di terze parti ..... 1
  - Protezione dei dati delle VM in OpenShift Virtualization con OpenShift API for Data Protection (OADP) . . . . 1
  - Installazione dell'operatore OpenShift API for Data Protection (OADP) ..... 3
  - Creazione di backup su richiesta per le VM in OpenShift Virtualization ..... 13
  - Ripristinare una VM da un backup ..... 16
  - Eliminazione di backup e ripristini mediante Velero ..... 22

# Protezione dei dati mediante strumenti di terze parti

## Protezione dei dati delle VM in OpenShift Virtualization con OpenShift API for Data Protection (OADP)

Autore: Banu Sundhar, NetApp

Questa sezione del documento di riferimento fornisce dettagli per la creazione di backup di macchine virtuali utilizzando l'API OpenShift per la protezione dei dati (OADP) con Velero su NetApp ONTAP S3 o NetApp StorageGRID S3. I backup dei volumi persistenti (PVS) dei dischi della macchina virtuale vengono creati utilizzando gli Snapshot CSI Astra Trident.

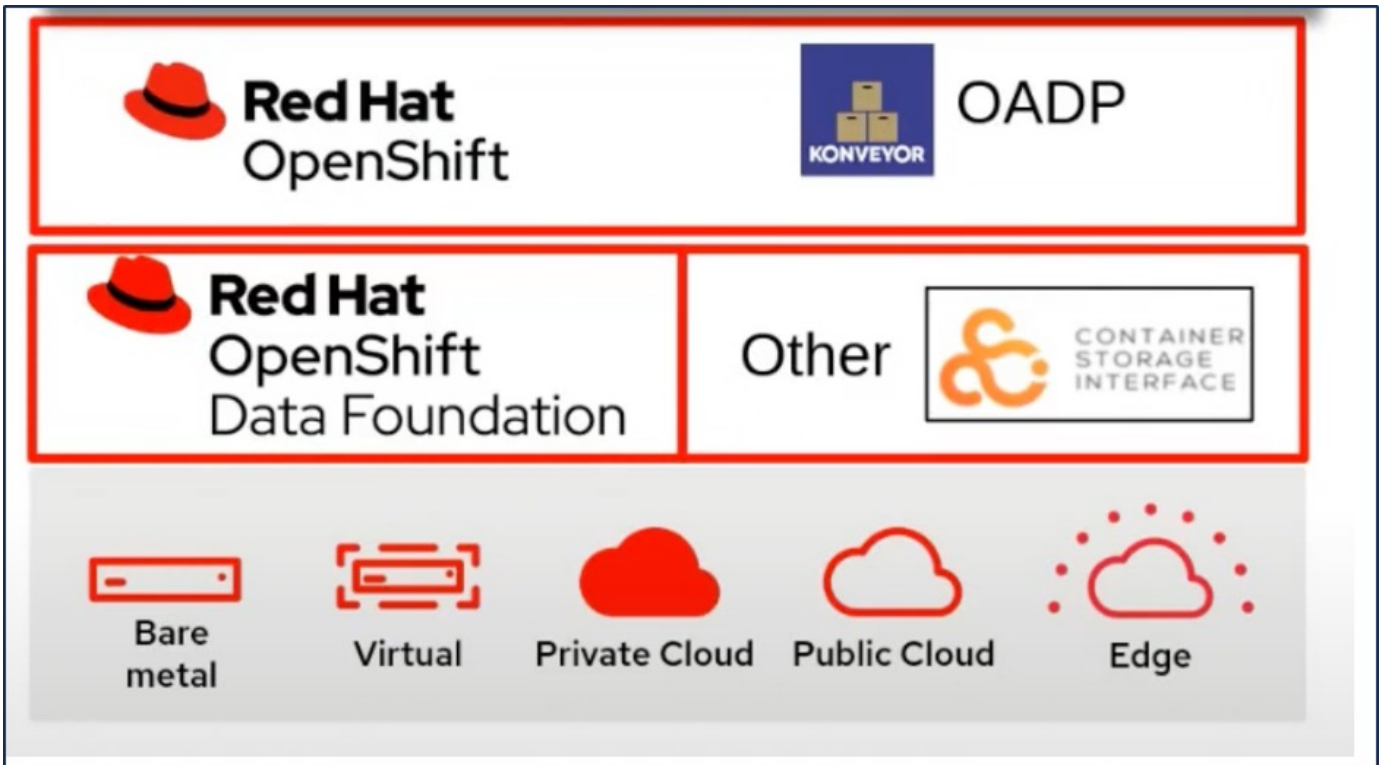
Le macchine virtuali nell'ambiente di virtualizzazione OpenShift sono applicazioni containerizzate che vengono eseguite nei nodi di lavoro della piattaforma container OpenShift. È importante proteggere i metadati delle macchine virtuali e i dischi persistenti delle macchine virtuali, in modo che in caso di perdita o danneggiamento possano essere ripristinati.

I dischi persistenti delle macchine virtuali di virtualizzazione OpenShift possono essere sottoposti a backup dallo storage ONTAP integrato nel cluster OpenShift utilizzando "[CSI Astra Trident](#)". In questa sezione usiamo "[OpenShift API per la protezione dei dati \(OADP\)](#)" Per eseguire il backup delle VM, inclusi i relativi volumi di dati su

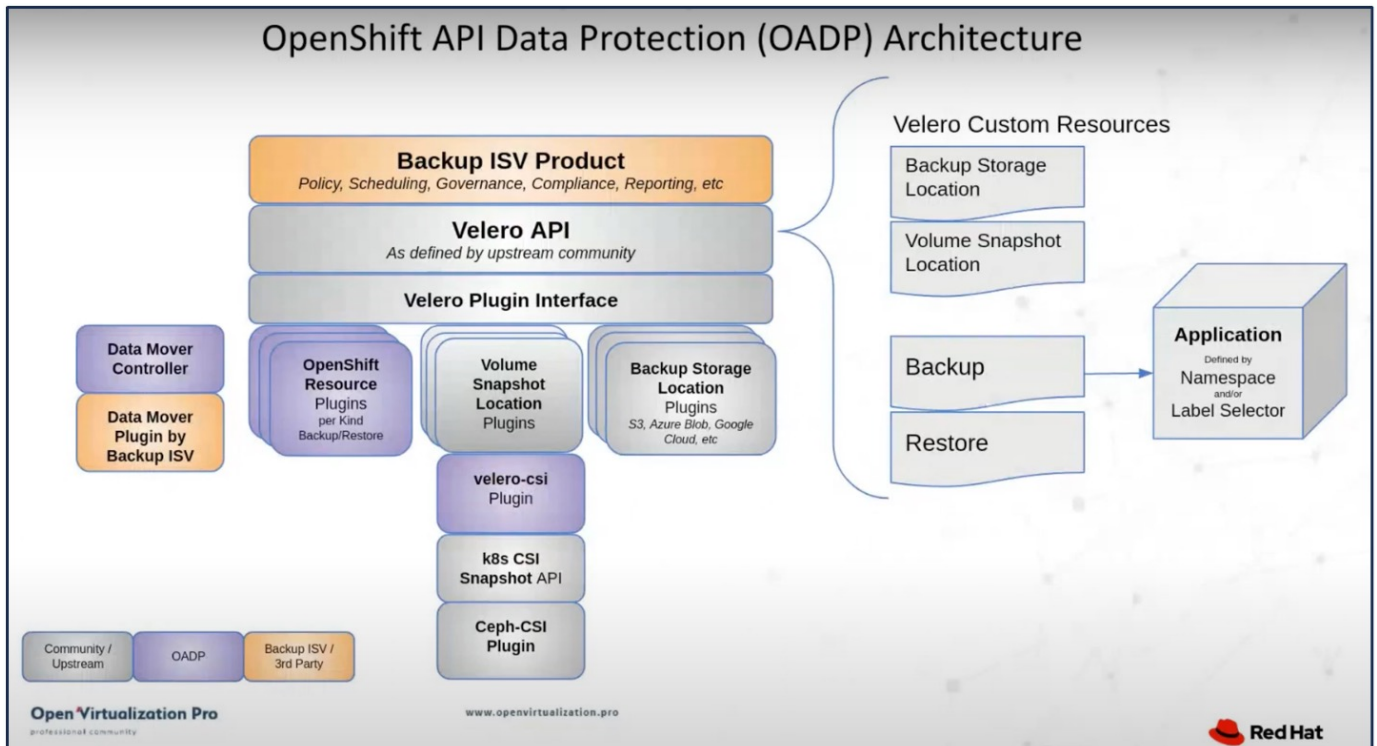
- Storage a oggetti ONTAP
- StorageGRID

Quindi, eseguiamo il ripristino dal backup quando necessario.

OADP consente il backup, il ripristino e il disaster recovery delle applicazioni su un cluster OpenShift. I dati che possono essere protetti con OADP includono oggetti risorsa Kubernetes, volumi persistenti e immagini interne.



Red Hat OpenShift ha sfruttato le soluzioni sviluppate dalla comunità OpenSource per la protezione dei dati. "Velero" È uno strumento open-source per eseguire backup e ripristino in tutta sicurezza, eseguire disaster recovery e migrare risorse del cluster e volumi persistenti di Kubernetes. Per utilizzare Velero facilmente, OpenShift ha sviluppato l'operatore OADP e il plugin Velero per integrarsi con i driver di storage CSI. Il nucleo delle API OADP esposte si basa sulle API di Velero. Dopo aver installato e configurato l'operatore OADP, le operazioni di backup/ripristino che possono essere eseguite si basano sulle operazioni esposte dall'API Velero.



OADP 1,3 è disponibile dall'hub operatore del gruppo OpenShift 4,12 e versioni successive. Dispone di un Data Mover integrato che può spostare gli snapshot di volume CSI in un archivio di oggetti remoto. In questo modo è possibile ottenere portabilità e durata spostando le snapshot in una posizione di storage a oggetti durante il backup. Le snapshot sono quindi disponibili per il ripristino dopo un disastro.

**Di seguito sono riportate le versioni dei vari componenti utilizzati per gli esempi di questa sezione**

- Gruppo OpenShift 4,14
- OpenShift Virtualization installato tramite OperatorOpenShift Virtualization Operator fornito da Red Hat
- OADP Operator 1,13 fornito da Red Hat
- Velero CLI 1,13 per Linux
- Astra Trident 24,02
- ONTAP 9,12

["CSI Astra Trident"](#)

["OpenShift API per la protezione dei dati \(OADP\)"](#)

["Velero"](#)

## Installazione dell'operatore OpenShift API for Data Protection (OADP)

In questa sezione viene descritta l'installazione dell'operatore OpenShift API for Data Protection (OADP).

### Prerequisiti

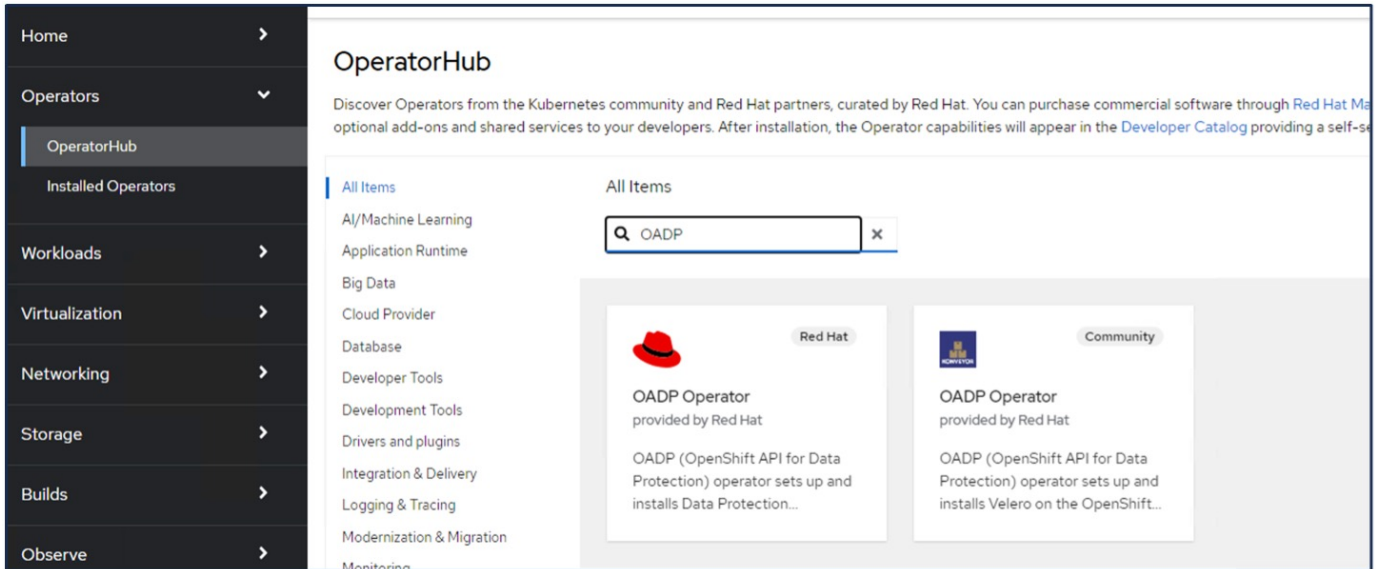
- Un cluster Red Hat OpenShift (versione successiva alla 4,12) installato in un'infrastruttura bare-metal con nodi di lavoro RHCOS
- Un cluster NetApp ONTAP integrato con il cluster utilizzando Astra Trident
- Un backend Trident configurato con una SVM sul cluster ONTAP
- StorageClass configurato sul cluster OpenShift con Astra Trident come provisioner
- Classe Snapshot Trident creata nel cluster
- Accesso cluster-admin al cluster Red Hat OpenShift
- Accesso amministrativo al cluster NetApp ONTAP
- Operatore di virtualizzazione OpenShift installato e configurato
- VM implementate in uno spazio dei nomi su OpenShift Virtualization
- Una workstation di amministrazione con tridentctl e oc tools installati e aggiunti al percorso dei dollari



Se si desidera eseguire un backup di una macchina virtuale quando è in esecuzione, è necessario installare l'agente guest QEMU su tale macchina virtuale. Se si installa la macchina virtuale utilizzando un modello esistente, l'agente QEMU viene installato automaticamente. QEMU consente all'agente ospite di disattivare i dati in-flight nel sistema operativo guest durante il processo di snapshot ed evitare possibili danneggiamenti dei dati. Se QEMU non è installato, è possibile arrestare la macchina virtuale prima di eseguire un backup.

## Procedura per l'installazione dell'operatore OADP

1. Andare all'Operator Hub del cluster e selezionare Red Hat OADP operator. Nella pagina Installa, utilizzare tutte le selezioni predefinite e fare clic su Installa. Nella pagina successiva, utilizzare nuovamente tutte le impostazioni predefinite e fare clic su Installa. L'operatore OADP sarà installato nello spazio dei nomi openshift-adp.





# 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
<b>OpenShift Virtualization</b> 4.14.4 provided by Red Hat	openshift-cnv	openshift-cnv	Succeeded Up to date
<b>OADP Operator</b> 1.3.0 provided by Red Hat	openshift-adp	openshift-adp	Succeeded Up to date
<b>Package Server</b> 0.0.1-snapshot provided by	openshift-operator-lifecycle-manager	openshift-operator-lifecycle-manager	Succeeded

## Prerequisiti per la configurazione di Velero con i dettagli di ONTAP S3

Una volta completata l'installazione dell'operatore, configurare l'istanza di Velero.

Velero può essere configurato per utilizzare l'archiviazione oggetti compatibile con S3. Configurare ONTAP S3 utilizzando le procedure illustrate nella "[Sezione Gestione dello storage a oggetti della documentazione di ONTAP](#)". Per l'integrazione con Velero, sono necessarie le seguenti informazioni della configurazione di ONTAP S3.

- Un'interfaccia logica (LIF) che può essere usata per accedere a S3
- Credenziali utente per accedere a S3 che include la chiave di accesso e la chiave di accesso segreta
- Un nome bucket in S3 per i backup con autorizzazioni di accesso per l'utente
- Per un accesso sicuro all'archiviazione a oggetti, è necessario installare il certificato TLS sul server di archiviazione a oggetti.

## Prerequisiti per la configurazione di Velero con i dettagli di StorageGRID S3

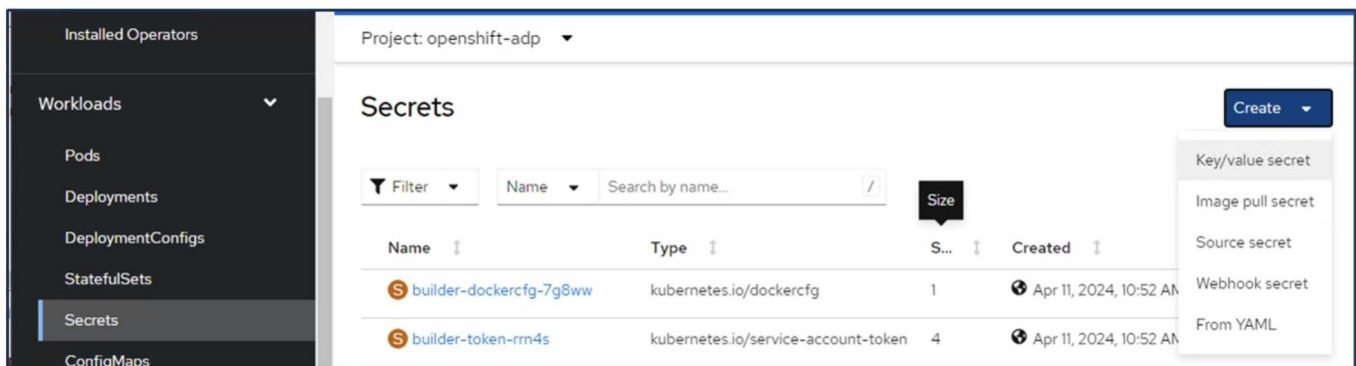
Velero può essere configurato per utilizzare l'archiviazione oggetti compatibile con S3. È possibile configurare StorageGRID S3 utilizzando le procedure illustrate nella "[Documentazione StorageGRID](#)". Per l'integrazione con Velero, sono necessarie le seguenti informazioni della configurazione di StorageGRID S3.

- L'endpoint che può essere utilizzato per accedere a S3
- Credenziali utente per accedere a S3 che include la chiave di accesso e la chiave di accesso segreta
- Un nome bucket in S3 per i backup con autorizzazioni di accesso per l'utente
- Per un accesso sicuro all'archiviazione a oggetti, è necessario installare il certificato TLS sul server di archiviazione a oggetti.

## Procedura di configurazione di Velero

- Innanzitutto, creare un segreto per una credenziale utente ONTAP S3 o per le credenziali utente StorageGRID tenant. Verrà utilizzato per configurare Velero in un secondo momento. È possibile creare un segreto dall'interfaccia CLI o dalla console Web.

Per creare un segreto dalla console Web, selezionare segreti, quindi fare clic su chiave/valore segreto. Fornire i valori per il nome della credenziale, la chiave e il valore come mostrato. Assicurarsi di utilizzare l'ID chiave di accesso e la chiave di accesso segreta dell'utente S3. Assegnare un nome appropriato al segreto. Nell'esempio seguente, viene creato un segreto con credenziali utente di ONTAP S3 denominato credenziali ontap-S3.



The screenshot shows the OpenShift console interface for managing secrets. The left sidebar contains navigation options: Installed Operators, Workloads (expanded), Pods, Deployments, DeploymentConfigs, StatefulSets, Secrets (selected), and ConfigMaps. The main content area is titled 'Secrets' and shows a table of existing secrets. The table has columns for Name, Type, Size, and Created. Two secrets are listed:

Name	Type	Size	Created
builder-dockercfg-7g8ww	kubernetes.io/dockercfg	1	Apr 11, 2024, 10:52 AM
builder-token-rm4s	kubernetes.io/service-account-token	4	Apr 11, 2024, 10:52 AM

A 'Create' button is located in the top right corner. A dropdown menu is open, showing options for creating a secret: Key/value secret, Image pull secret, Source secret, Webhook secret, and From YAML.



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 \***

ontap-s3-credentials

Unique name of the new secret.

**Key \***

cloud

**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

Save Cancel

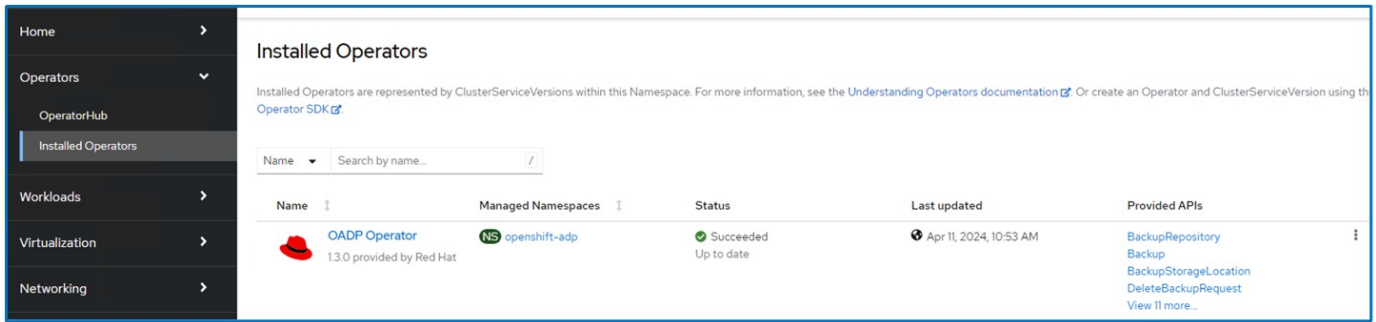
Per creare un segreto denominato sg-S3-credenziali dall'interfaccia CLI, è possibile utilizzare il seguente comando.

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

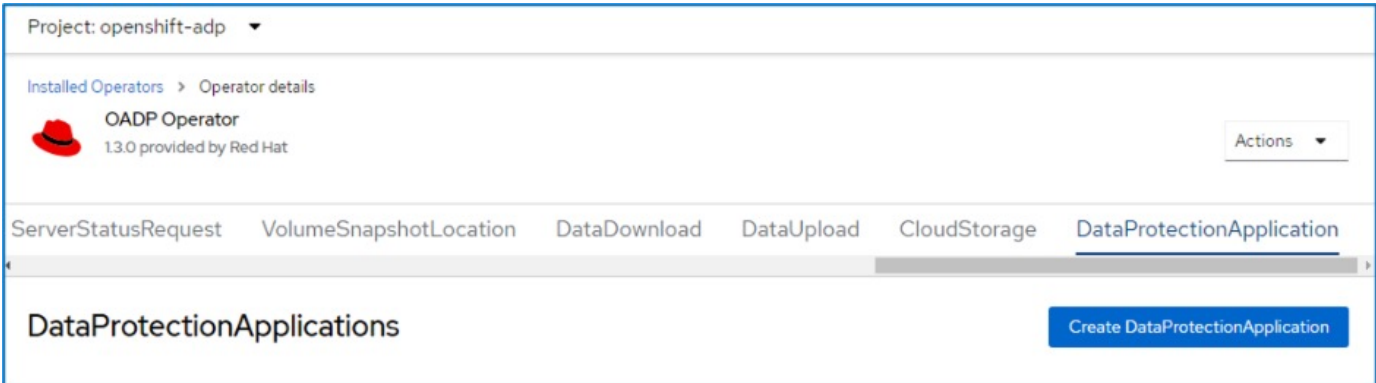
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

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

- Quindi, per configurare Velero, selezionare Installed Operators dalla voce di menu in Operators, fare clic sull'operatore OADP, quindi selezionare la scheda DataProtectionApplication.



Fare clic su Create DataProtectionApplication. Nella vista modulo, specificare un nome per l'applicazione DataProtection o utilizzare il nome predefinito.



Passare ora alla visualizzazione YAML e sostituire le informazioni sulle specifiche come mostrato negli esempi di file yaml riportati di seguito.

### Esempio di file yaml per la configurazione di Velero con ONTAP S3 come backupLocation

```

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

```

**File yaml di esempio per la configurazione di Velero con StorageGRID S3 come backupLocation e snapshotLocation**

```

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

```

La sezione delle specifiche nel file yaml deve essere configurata in modo appropriato per i seguenti parametri, come nell'esempio precedente

### BackupLocations

ONTAP S3 o StorageGRID S3 (con le relative credenziali e altre informazioni come mostrato in yaml) è configurato come BackupLocation predefinito per velero.

### SnapshotLocations

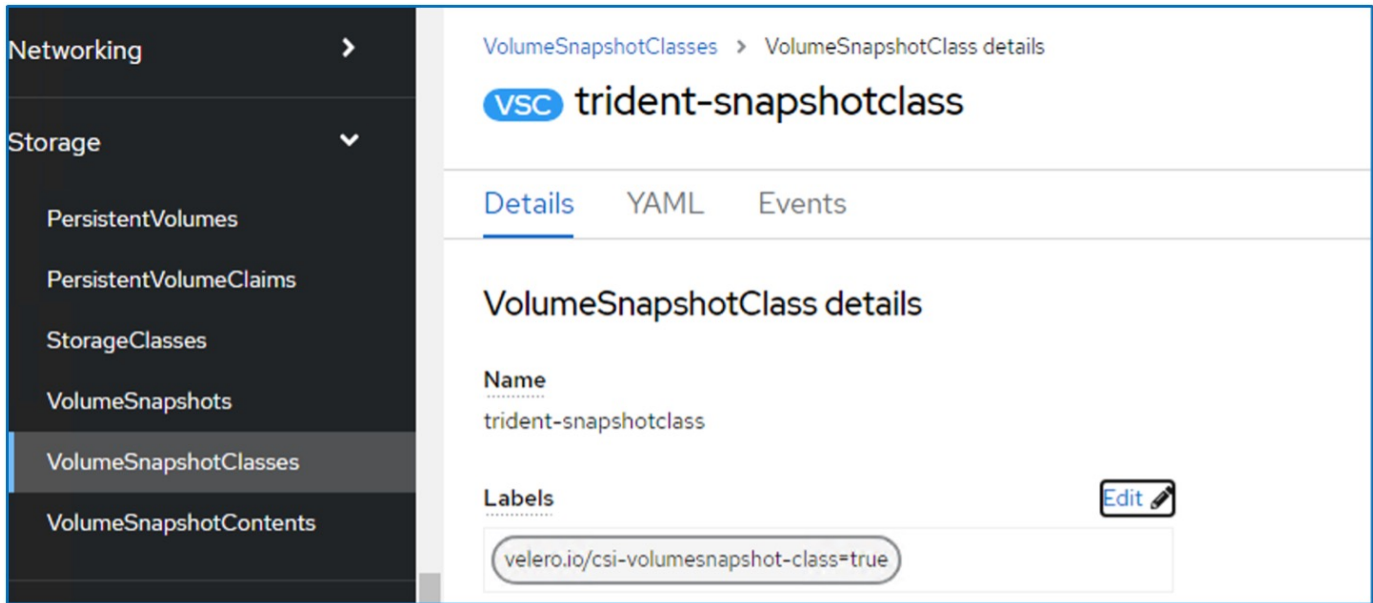
Se si utilizzano gli snapshot Container Storage Interface (CSI), non è necessario specificare una posizione dello snapshot perché si creerà un VolumeSnapshotClass CR per registrare il driver CSI. Nel nostro esempio, si utilizza Astra Trident CSI e in precedenza si è creato VolumeSnapShotClass CR utilizzando il driver Trident CSI.

### Attiva plugin CSI

Aggiungere csi ai prefaultPlugin per Velero per eseguire il backup dei volumi persistenti con gli snapshot CSI. I plug-in di Velero CSI, per eseguire il backup dei PVC supportati da CSI, sceglieranno VolumeSnapshotClass nel cluster su cui è impostata l'etichetta **velero.io/csi-volumesnapshot-class**. Per questo

- È necessario creare il tridente VolumeSnapshotClass.

- Modificare l'etichetta della classe trident-snapshotclass e impostarla su **velero.io/csi-volumesnapshot-class=true** come mostrato di seguito.



The screenshot shows the Kubernetes dashboard interface. On the left, a navigation sidebar is visible with 'Storage' expanded and 'VolumeSnapshotClasses' selected. The main content area displays the details for the 'trident-snapshotclass' VolumeSnapshotClass. The 'Name' field is 'trident-snapshotclass'. The 'Labels' field is highlighted, showing the label 'velero.io/csi-volumesnapshot-class=true'. An 'Edit' button is visible next to the labels field.

Verificare che gli snapshot possano persistere anche se gli oggetti VolumeSnapshot vengono eliminati. A tale scopo, impostare **deletionPolicy** su Retain. In caso contrario, l'eliminazione di uno spazio dei nomi perderà completamente tutti i PVC di cui è stato eseguito il backup.

```
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

Verificare che DataProtectionApplication sia stato creato e che sia in condizioni: riconciliato.

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
 velero-demo	DataProtectionApplication	Condition: Reconciled	No labels

L'operatore OADP creerà un BackupStorageLocation corrispondente. Questo verrà utilizzato durante la creazione di un backup.

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

## Creazione di backup su richiesta per le VM in OpenShift Virtualization

In questa sezione viene descritto come creare backup su richiesta per le VM in OpenShift Virtualization.

### Procedura per creare un backup di una VM

Per creare un backup su richiesta dell'intera VM (metadati VM e dischi VM), fare clic sulla scheda **Backup**. In questo modo viene creata una risorsa personalizzata di backup (CR). Viene fornito un yaml di esempio per creare la CR di backup. Utilizzando questo yaml, verrà eseguito il backup della VM e dei relativi dischi nello spazio dei nomi specificato. È possibile impostare parametri aggiuntivi come illustrato nella ["documentazione"](#).

Uno snapshot dei volumi persistenti che eseguono il backup dei dischi verrà creato dal CSI. Viene creato un backup della macchina virtuale insieme all'istantanea dei relativi dischi e memorizzato nella posizione di backup specificata nel codice yaml. Il backup rimarrà nel sistema per 30 giorni come specificato nel ttl.

```

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

```

Una volta completato il backup, la sua fase viene visualizzata come completata.

Project: openshift-adp

Installed Operators > Operator details

OADP Operator  
1.3.0 provided by Red Hat

Actions

Details | YAML | Subscription | Events | All instances | BackupRepository | **Backup** | BackupStorageLocation | DeleteBa

**Backups** Create Backup

Name Search by name...

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

È possibile esaminare il backup nell'archiviazione a oggetti con l'aiuto di un'applicazione browser S3. Il percorso del backup viene visualizzato nel bucket configurato con il nome del prefisso (velero/demobackup). Il contenuto del backup include gli snapshot del volume, i log e altri metadati della macchina virtuale.



In StorageGRID, è anche possibile utilizzare la console S3 disponibile in Gestione tenant per visualizzare gli oggetti di backup.



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

## Creazione di backup pianificati per le VM in OpenShift Virtualization

Per creare backup in base a una pianificazione, è necessario creare una pianificazione CR.

La pianificazione è semplicemente un'espressione Cron che consente di specificare l'ora in cui si desidera creare il backup. Un esempio di yaml per creare una pianificazione CR.

```

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 Expression 0 7 \* \* \* significa che ogni giorno verrà creato un backup alle 7:00:00.

Vengono inoltre specificati gli spazi dei nomi da includere nel backup e la posizione di archiviazione per il backup. Quindi, invece di un CR di backup, il CR di pianificazione viene utilizzato per creare un backup all'ora e alla frequenza specificate.

Una volta creata, la pianificazione viene attivata.

Project: openshift-adp ▾



Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat

storageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRestore Restore Schedule

## Schedules


Name ▾ Search by name... /

Name	Kind	Status	Labels
 schedule1	Schedule	Phase:  Enabled	No labels

I backup verranno creati in base a questa pianificazione e possono essere visualizzati dalla scheda Backup.

Project: openshift-adp ▾

Installed Operators > Operator details


 **OADP Operator**  
1.3.0 provided by Red Hat

Events All instances BackupRepository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest

## Backups

[Create Backup](#)

Name ▾ Search by name... /

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

## Ripristinare una VM da un backup

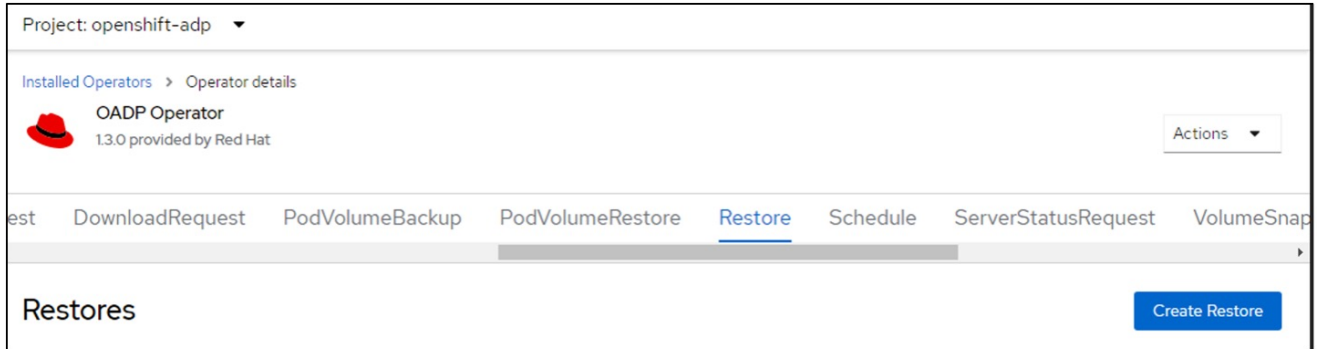
In questa sezione viene descritto come ripristinare le macchine virtuali da un backup.

### Prerequisiti

Per eseguire il ripristino da un backup, supponiamo che lo spazio dei nomi in cui esisteva la macchina virtuale sia stato eliminato accidentalmente.

## Ripristinare nello stesso namespace

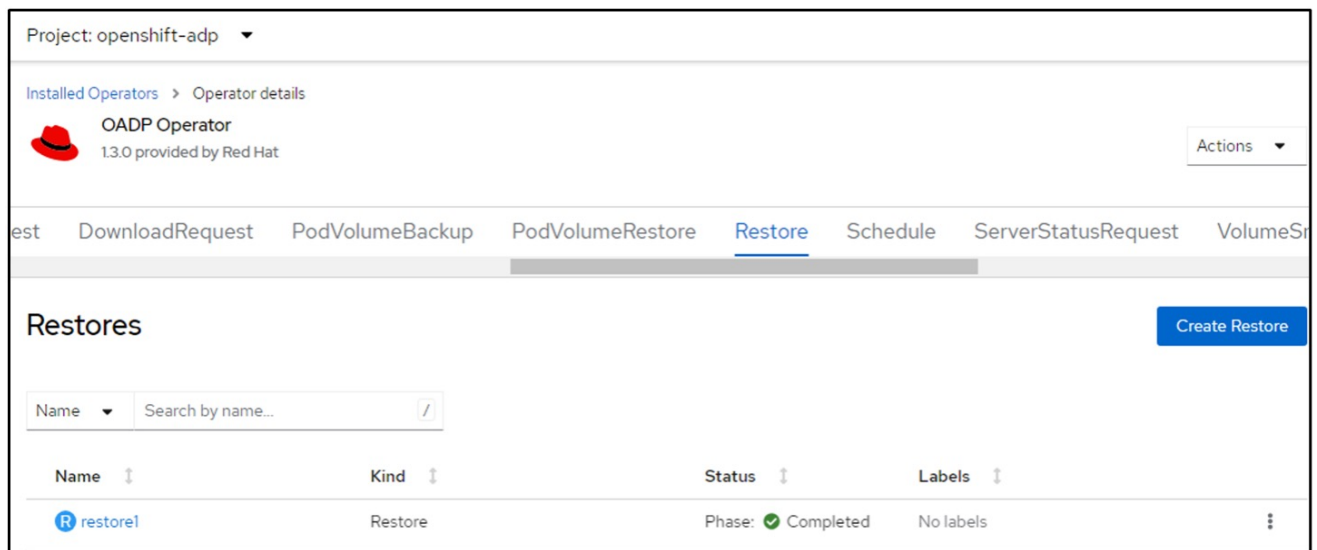
Per eseguire il ripristino dal backup appena creato, è necessario creare una risorsa personalizzata di ripristino (CR). Dobbiamo fornirgli un nome, fornire il nome del backup da cui eseguire il ripristino e impostare su true. È possibile impostare parametri aggiuntivi come illustrato nella "documentazione". Fare clic sul pulsante Crea.



The screenshot shows the OADP Operator interface. At the top, it says "Project: openshift-adp". Below that, there's a breadcrumb "Installed Operators > Operator details" and the "OADP Operator" logo with version "1.3.0 provided by Red Hat". A navigation bar includes "DownloadRequest", "PodVolumeBackup", "PodVolumeRestore", "Restore" (highlighted), "Schedule", "ServerStatusRequest", and "VolumeSnap". Below the navigation bar, the "Restores" section is visible with a "Create Restore" button.

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

Quando la fase è completata, è possibile vedere che le macchine virtuali sono state ripristinate allo stato in cui è stato acquisito lo snapshot. (Se il backup è stato creato quando la VM era in esecuzione, ripristinando la VM dal backup si avvia la VM ripristinata e la si porta in esecuzione). La VM viene ripristinata nello stesso namespace.



The screenshot shows the OADP Operator interface with the "Restores" section. A search bar is present with "Name" and "Search by name...". Below it, a table lists the restore resources:

Name	Kind	Status	Labels
restore1	Restore	Phase: <span style="color: green;">✔</span> Completed	No labels

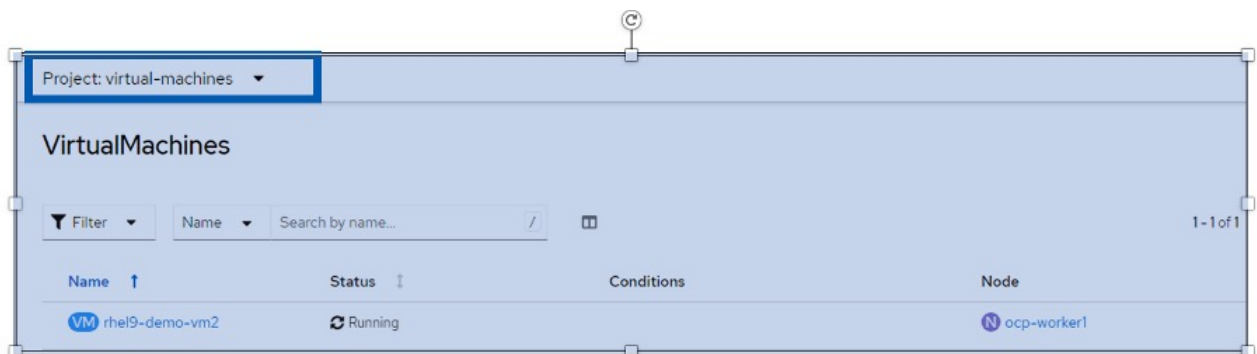
## Ripristinare in un namespace diverso

Per ripristinare la macchina virtuale in uno spazio dei nomi diverso, è possibile fornire un namespaceMapping nella definizione yaml di Restore CR.

Il seguente file yaml di esempio crea un Restore CR per ripristinare una VM e i relativi dischi nello spazio dei nomi virtual-machine-demo quando il backup è stato eseguito nello spazio dei nomi virtual-machine.

```
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
```

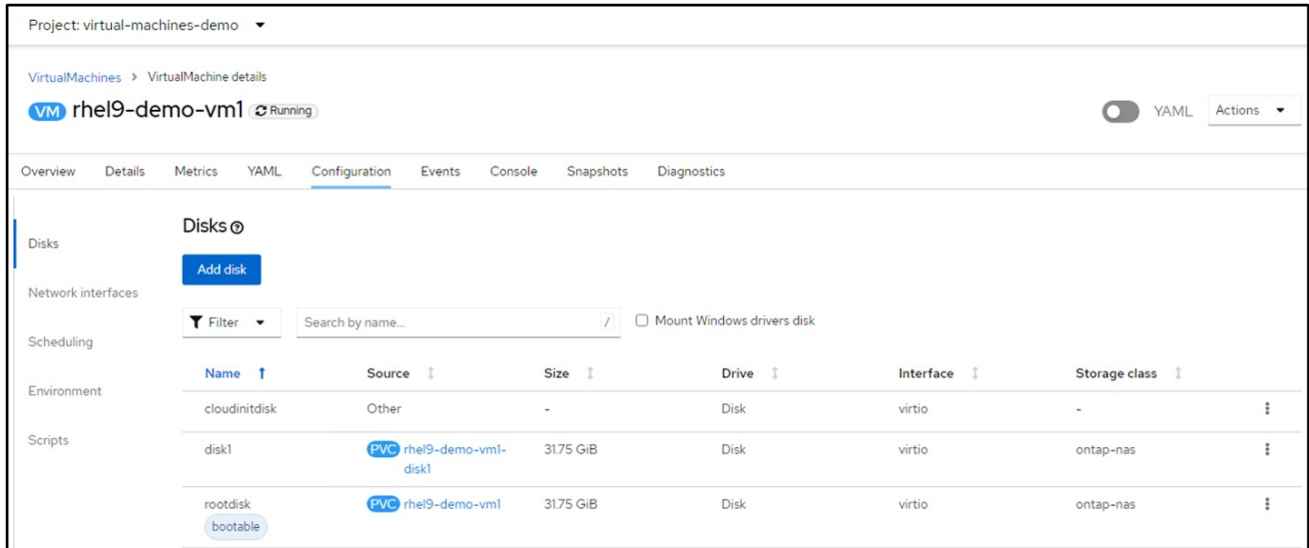
Quando la fase è completata, è possibile vedere che le macchine virtuali sono state ripristinate allo stato in cui è stato acquisito lo snapshot. (Se il backup è stato creato quando la VM era in esecuzione, ripristinando la VM dal backup si avvia la VM ripristinata e la si porta in esecuzione). La VM viene ripristinata in uno spazio dei nomi diverso, come specificato in yaml.



## Ripristinare in una classe di archiviazione diversa

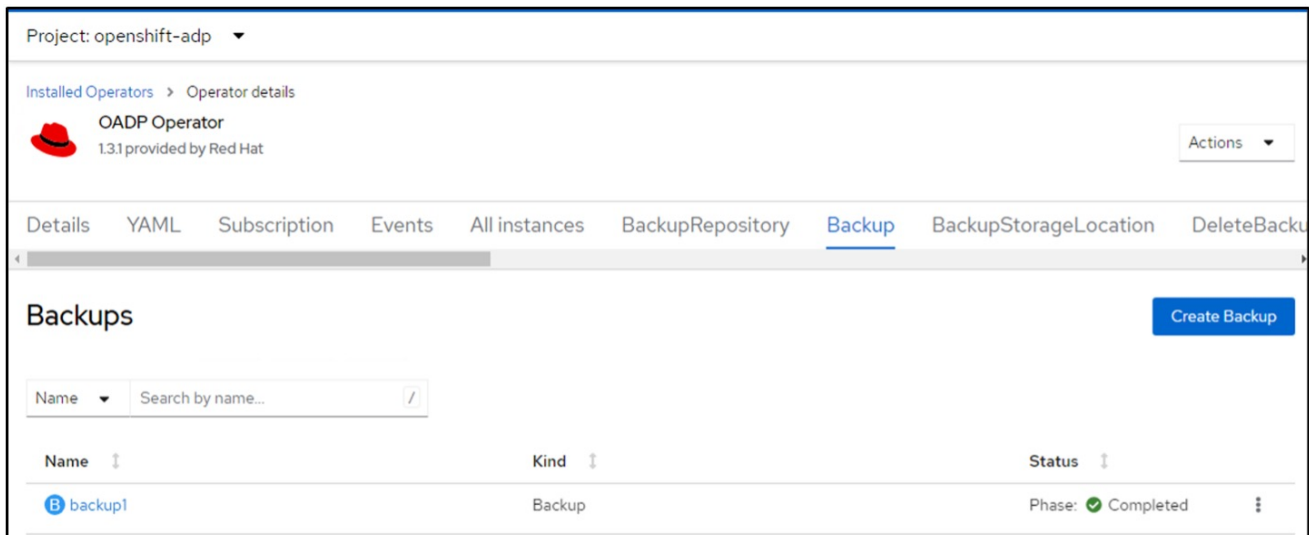
Velero fornisce una capacità generica di modificare le risorse durante il ripristino specificando le patch json. Le patch json vengono applicate alle risorse prima di essere ripristinate. Le patch json sono specificate in una configmap e la configmap è referenziata nel comando restore. Questa funzione consente di eseguire il ripristino utilizzando una classe di archiviazione diversa.

Nell'esempio seguente, la macchina virtuale, in fase di creazione, utilizza ontap-nas come classe di storage per i dischi. Viene creato un backup della macchina virtuale denominata Backup1.



The screenshot shows the configuration page for a virtual machine named 'rhel9-demo-vm1' in the 'virtual-machines-demo' project. The 'Configuration' tab is active, displaying a table of disks. The table has columns for Name, Source, Size, Drive, Interface, and Storage class. Two disks are listed: 'disk1' and 'rootdisk', both with a size of 31.75 GiB and using the 'ontap-nas' storage class.

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' page for the 'OADP Operator' in the 'openshift-adp' project. The 'Backup' tab is active, displaying a table of backups. One backup is listed: 'backup1', which is of kind 'Backup' and has a status of 'Completed'.

Name	Kind	Status
backup1	Backup	Phase: Completed

Simula la perdita della macchina virtuale eliminando la macchina virtuale.

Per ripristinare la macchina virtuale utilizzando una classe di storage diversa, ad esempio ontap-nas-eco storage, devi effettuare i due seguenti passaggi:

### Passo 1

Creare una mappa di configurazione (console) nello spazio dei nomi openshift-adp come segue:  
Inserisci i dettagli come mostrato nella schermata:  
Selezionare spazio dei nomi : openshift-adp

Nome: Change-storage-class-config (può essere qualsiasi nome)

Chiave: Change-storage-class-config.yaml:

Valore:

```
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

[Remove key/value](#)

**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](#)

L'oggetto della mappa di configurazione risultante dovrebbe essere simile al seguente (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>

```

Questa mappa di configurazione applicherà la regola del modificatore di risorse quando viene creato il ripristino. Verrà applicata una patch per sostituire il nome della classe storage in ontap-nas-eco per tutte le richieste di volume persistenti a partire da rhel.

## Passo 2

Per ripristinare la macchina virtuale, utilizzare il seguente comando dall'interfaccia CLI di Velero:

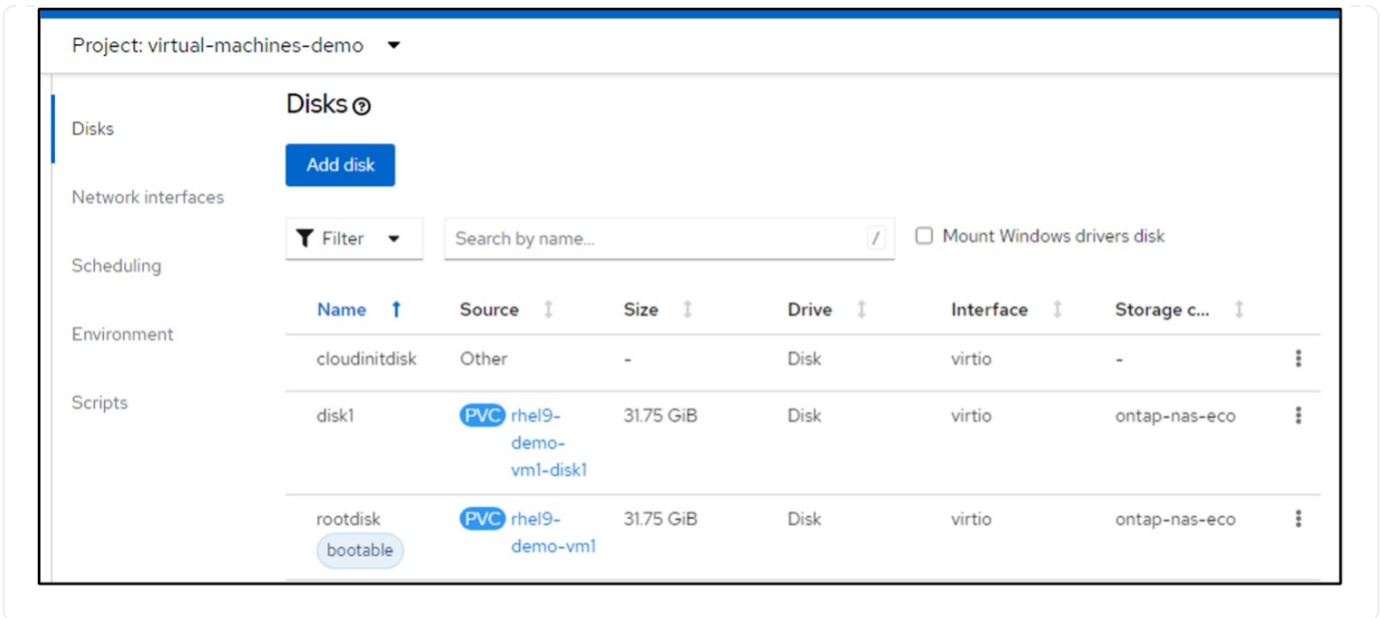
```

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

```

La macchina virtuale viene ripristinata con lo stesso namespace con i dischi creati utilizzando la classe storage ontap-nas-eco.





## Eliminazione di backup e ripristini mediante Velero

In questa sezione viene descritto come eliminare backup e ripristini per le macchine virtuali in OpenShift Virtualization utilizzando Velero.

### Eliminazione di un backup

È possibile eliminare una CR di backup senza eliminare i dati di archiviazione oggetti utilizzando lo strumento CLI OC.

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

Se si desidera eliminare la CR di backup ed eliminare i dati di archiviazione degli oggetti associati, è possibile farlo utilizzando lo strumento CLI Velero.

Scaricare l'interfaccia CLI come indicato nelle istruzioni nella "[Documentazione Velero](#)".

Eeguire il seguente comando delete utilizzando l'interfaccia CLI di Velero

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

### Eliminazione di un ripristino

È possibile eliminare l'opzione Ripristina CR utilizzando l'interfaccia CLI di Velero

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

È possibile utilizzare il comando oc e l'interfaccia utente per eliminare la CR di ripristino



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

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.