Proteggere i dati utilizzando strumenti di terze parti

NetApp virtualization solutions

NetApp
August 18, 2025

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

Sommario

Proteggere i dati utilizzando strumenti di terze parti . . . 1
Scopri di più sulla protezione dei dati per le VM in Red Hat OpenShift Virtualization utilizzando OpenShift API for Data Protection (OADP) . . . 1
Installa l'operatore Red Hat OpenShift API for Data Protection (OADP) . . . 3
Prerequisiti . . . 3
Passaggi per installare l'operatore OADP . . . 4
Crea backup su richiesta per VM in Red Hat OpenShift Virtualization utilizzando Velero . . . 13
Passaggi per creare un backup di una VM . . . 13
Creazione di backup pianificati per le VM in OpenShift Virtualization . . . 15
Ripristina una VM dal backup in Red Hat OpenShift Virtualization utilizzando Velero . . . 16
Prerequisiti . . . 16
Elimina un CR di backup o ripristina CR in Red Hat OpenShift Virtualization utilizzando Velero . . . 22
Eliminazione di un backup . . . 22
Eliminazione di un ripristino . . . 22

Proteggere i dati utilizzando strumenti di terze parti

Scopri di più sulla protezione dei dati per le VM in Red Hat OpenShift Virtualization utilizzando OpenShift API for Data Protection (OADP)

OpenShift API for Data Protection (OADP) con Velero fornisce funzionalità di backup, ripristino e disaster recovery per le VM in OpenShift Virtualization. Utilizzare gli snapshot Trident CSI per eseguire il backup di volumi persistenti e metadati delle VM su NetApp ONTAP S3 o StorageGRID S3. OADP si integra con le API Velero e i driver di archiviazione CSI per gestire le operazioni di protezione dei dati per le VM containerizzate.

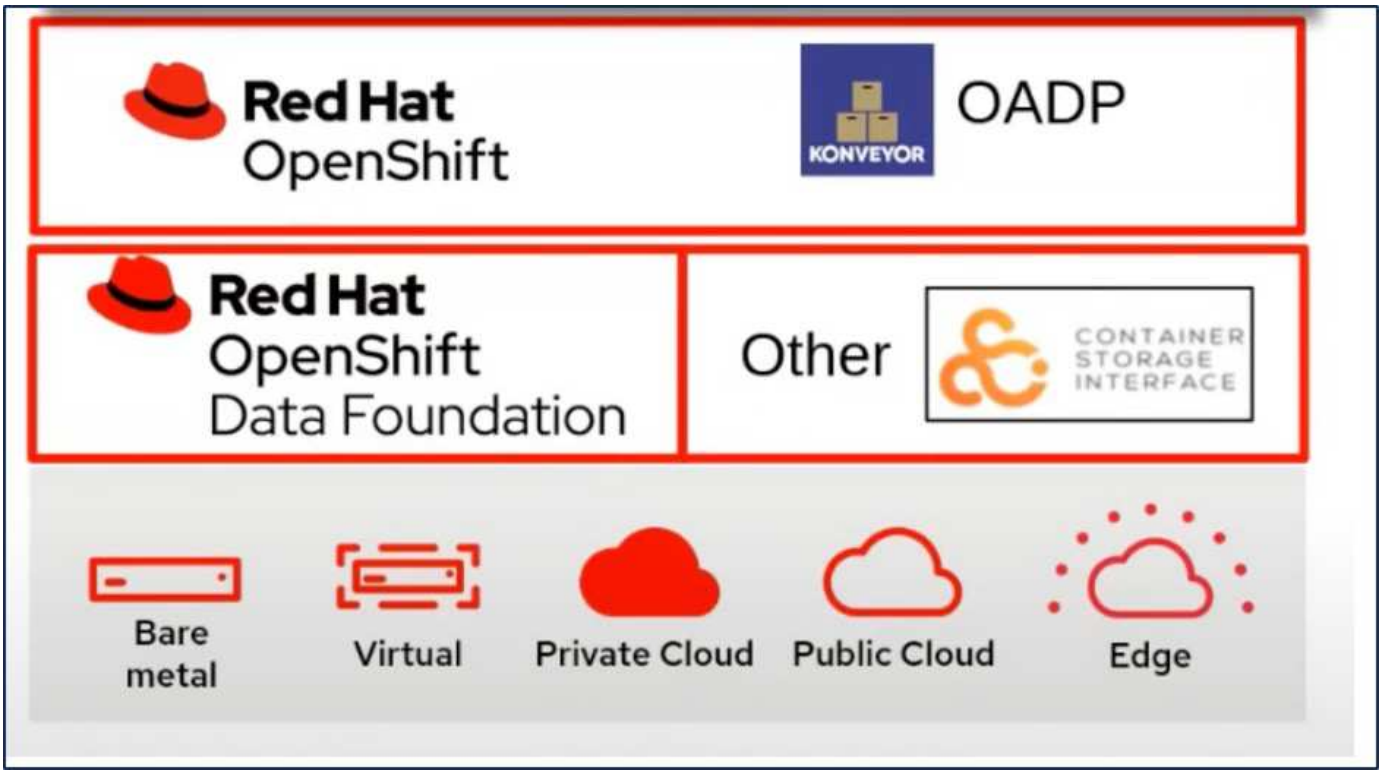
Le macchine virtuali nell'ambiente di virtualizzazione OpenShift sono applicazioni containerizzate che vengono eseguite nei nodi worker della piattaforma OpenShift Container. È importante proteggere i metadati delle VM e i dischi persistenti delle VM, in modo che sia possibile recuperarli quando vengono persi o danneggiati.

I dischi persistenti delle VM di virtualizzazione OpenShift possono essere supportati dallo storage ONTAP integrato nel cluster OpenShift utilizzando"Trident CSI" . In questa sezione utilizziamo"API OpenShift per la protezione dei dati (OADP)" per eseguire il backup delle VM, inclusi i relativi volumi di dati

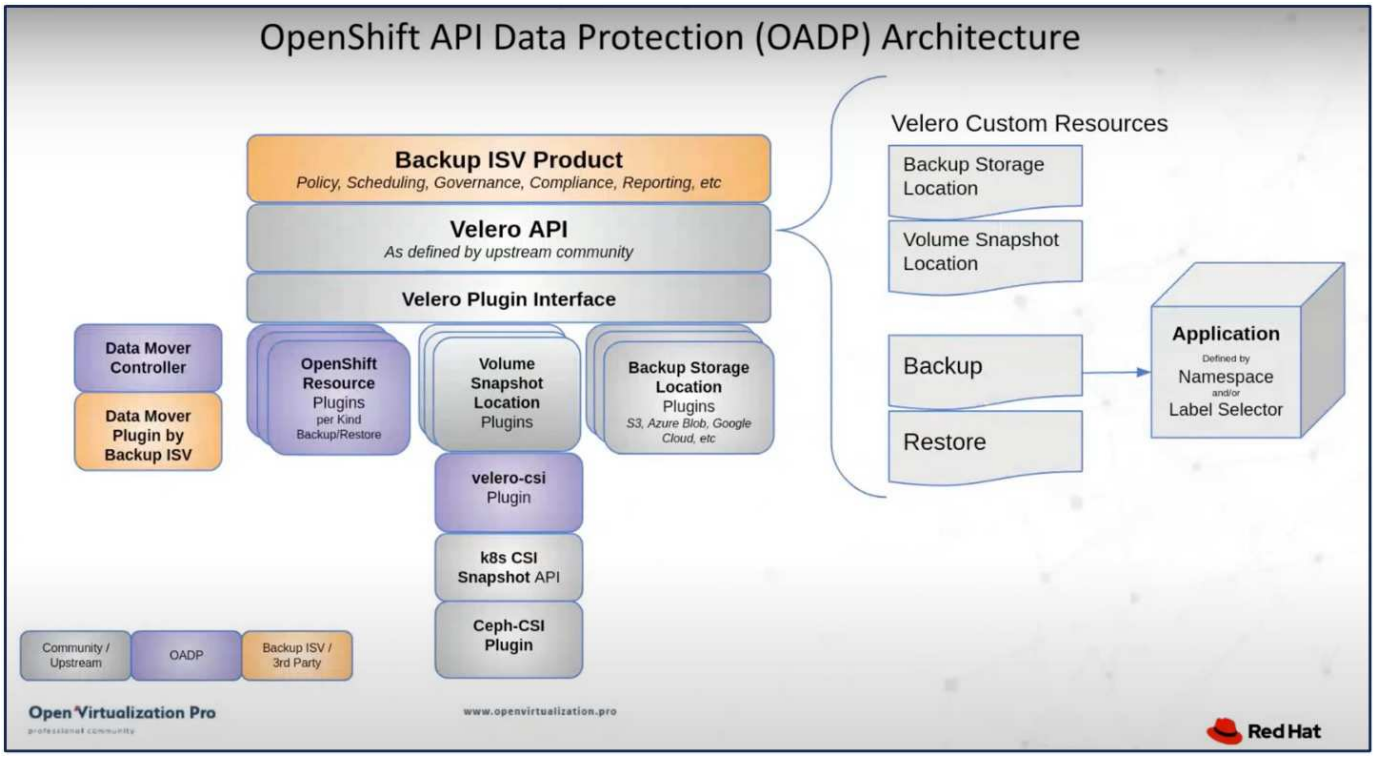
- Archiviazione di oggetti ONTAP
- StorageGrid

Quando necessario, eseguiamo il ripristino dal backup.

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 di risorse Kubernetes, volumi persistenti e immagini interne.



Red Hat OpenShift ha sfruttato le soluzioni sviluppate dalle comunità OpenSource per la protezione dei dati. "Velero" è uno strumento open source per eseguire backup e ripristini in modo sicuro, eseguire il disaster recovery e migrare le risorse del cluster Kubernetes e i volumi persistenti. Per utilizzare Velero in modo semplice, OpenShift ha sviluppato l'operatore OADP e il plugin Velero per integrarli con i driver di archiviazione CSI. Il nucleo delle API OADP esposte si basa sulle API 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 nell'hub operatore del cluster OpenShift 4.12 e versioni successive. Dispone di un Data Mover integrato in grado di spostare gli snapshot del volume CSI in un archivio oggetti remoto. Ciò garantisce portabilità e durata spostando gli snapshot in una posizione di archiviazione degli oggetti durante il backup. Gli snapshot sono quindi disponibili per il ripristino dopo i disastri.

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

- Cluster OpenShift 4.14
- OpenShift Virtualization installato tramite OperatorOpenShift Virtualization Operator fornito da Red Hat
- Operatore OADP 1.13 fornito da Red Hat
- Velero CLI 1.13 per Linux
- Trident 24.02
- ONTAP 9.12

"Trident CSI" "API OpenShift per la protezione dei dati (OADP)" "Velero"

Installa l'operatore Red Hat OpenShift API for Data Protection (OADP)

Installa l'operatore OpenShift API for Data Protection (OADP) per abilitare le funzionalità di backup e ripristino per le VM in OpenShift Virtualization. Questa procedura include la distribuzione dell'operatore OADP dall'OpenShift Operator Hub, la configurazione di Velero per utilizzare NetApp ONTAP S3 o StorageGRID come destinazione di backup e l'impostazione dei segreti e delle posizioni di backup necessari.

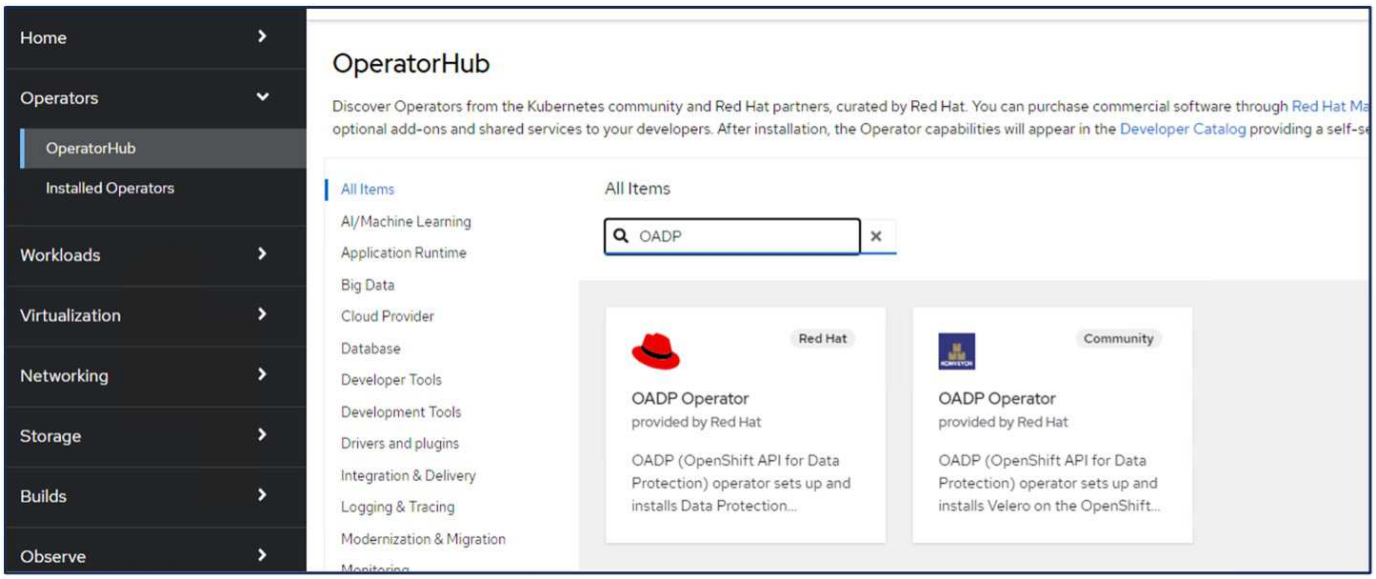
Prerequisiti

- Un cluster Red Hat OpenShift (successivo alla versione 4.12) installato su un'infrastruttura bare-metal con nodi worker RHCOS
- Un cluster NetApp ONTAP integrato con il cluster tramite Trident
- Un backend Trident configurato con un SVM su cluster ONTAP
- Una StorageClass configurata sul cluster OpenShift con Trident come provisioner
- Classe Trident Snapshot creata sul cluster
- Accesso di amministrazione del cluster al cluster Red Hat OpenShift
- Accesso amministratore al cluster NetApp ONTAP
- Operatore di virtualizzazione OpenShift installato e configurato
- VM distribuite in uno spazio dei nomi su OpenShift Virtualization
- Una postazione di lavoro di amministrazione con gli strumenti tridentctl e oc installati e aggiunti a $PATH

> Se si desidera eseguire un backup di una macchina virtuale quando è in stato di esecuzione, è necessario installare l'agente guest QEMU su tale macchina virtuale. Se si installa la VM utilizzando un modello esistente, l'agente QEMU verrà installato automaticamente. QEMU consente all'agente guest di mettere in pausa i dati in transito nel sistema operativo guest durante il processo di snapshot, evitando così possibili danneggiamenti dei dati. Se QEMU non è installato, è possibile arrestare la macchina virtuale prima di eseguire un backup.

Passaggi per installare l'operatore OADP

1. Accedere all'Operator Hub del cluster e selezionare l'operatore Red Hat OADP. Nella pagina Installa, utilizza tutte le selezioni predefinite e fai clic su Installa. Nella pagina successiva, utilizzare nuovamente tutte le impostazioni predefinite e fare clic su Installa. L'operatore OADP verrà 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
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

Prerequisiti per la configurazione Velero con dettagli Ontap S3

Dopo aver completato l'installazione dell'operatore, configurare l'istanza di Velero. Velero può essere configurato per utilizzare Object Storage compatibile con S3. Configurare ONTAP S3 utilizzando le procedure mostrate nel"Sezione Gestione dell'archiviazione degli oggetti della documentazione ONTAP" . Per l'integrazione con Velero, avrai bisogno delle seguenti informazioni dalla configurazione ONTAP S3.

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

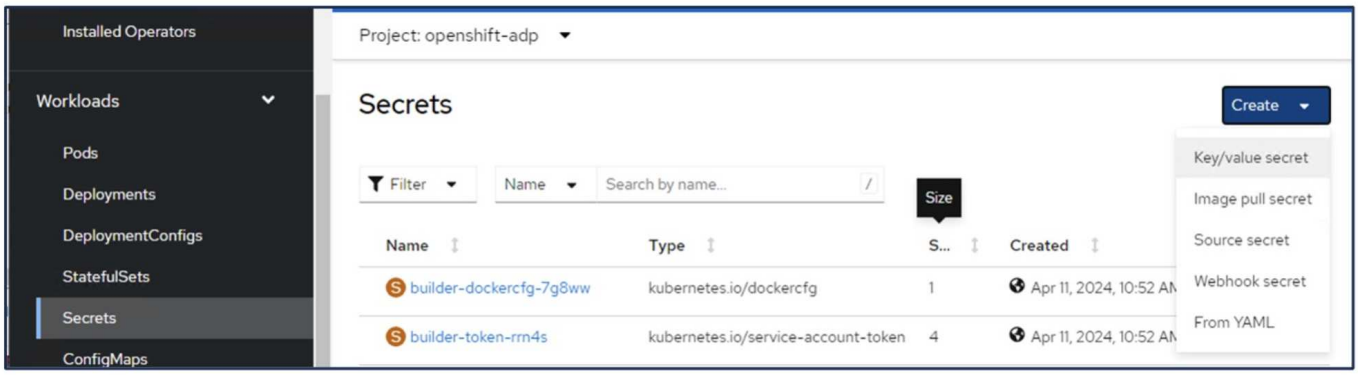
Prerequisiti per la configurazione di Velero con StorageGrid S3

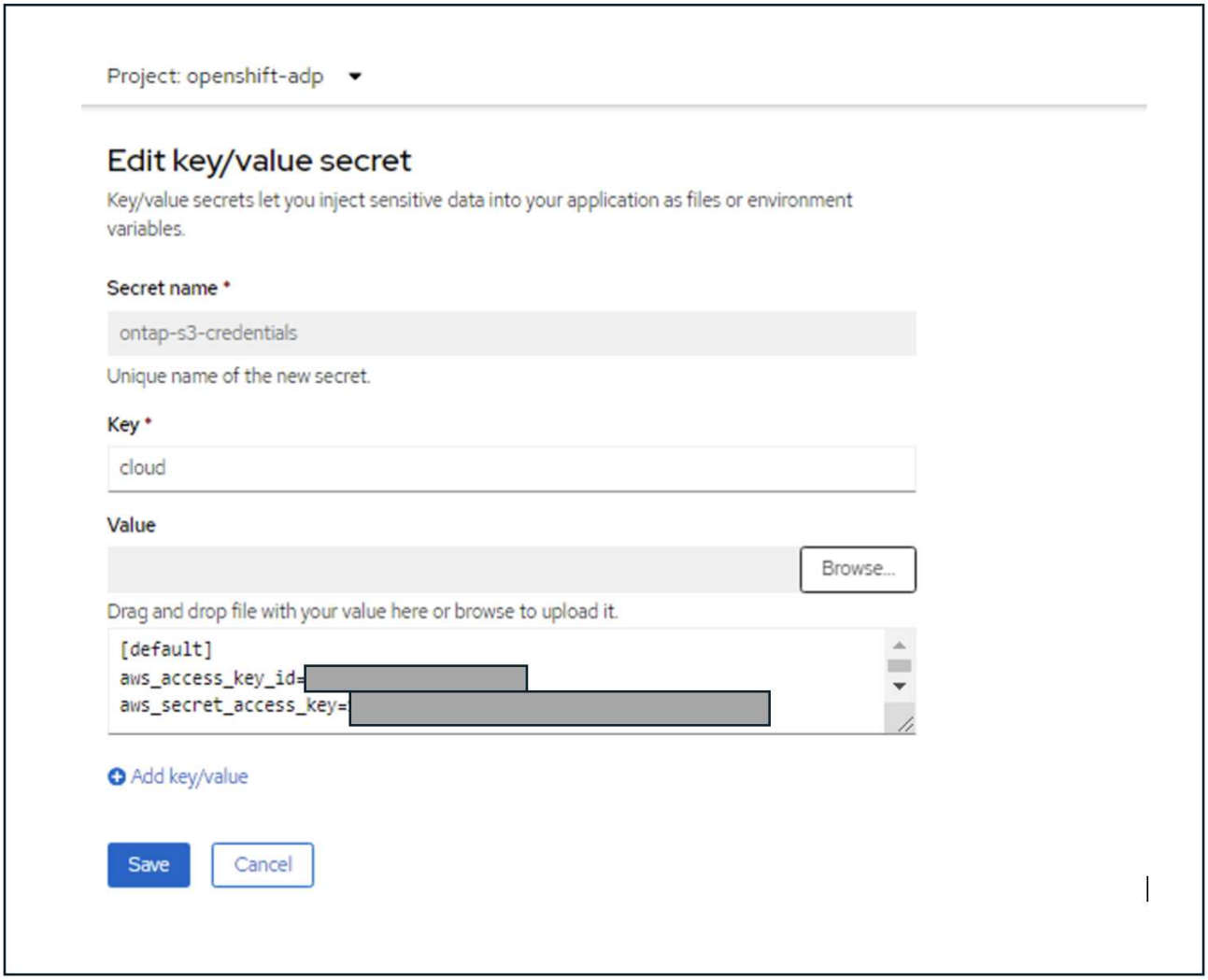
Velero può essere configurato per utilizzare Object Storage compatibile con S3. È possibile configurare StorageGrid S3 utilizzando le procedure illustrate in"Documentazione StorageGrid" . Per l'integrazione con Velero, saranno necessarie le seguenti informazioni dalla configurazione di StorageGrid S3.

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

Passaggi per configurare Velero

- Per prima cosa, crea un segreto per le credenziali utente ONTAP S3 o per le credenziali utente StorageGrid Tenant. Questo verrà utilizzato per configurare Velero in seguito. È possibile creare un segreto dalla CLI o dalla console Web. Per creare un segreto dalla console Web, seleziona Segreti, quindi fai clic su Segreto chiave/valore. Fornire i valori per il nome della credenziale, la chiave e il valore come mostrato. Assicurati di utilizzare l'ID della chiave di accesso e la chiave di accesso segreta del tuo utente S3. Dai un nome appropriato al segreto. Nell'esempio seguente viene creato un segreto con credenziali utente ONTAP S3 denominato ontap-s3-credentials.

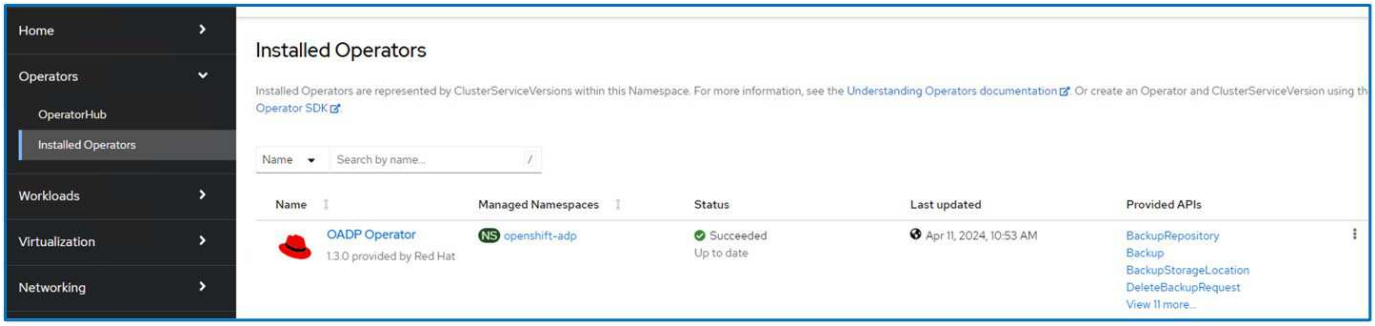




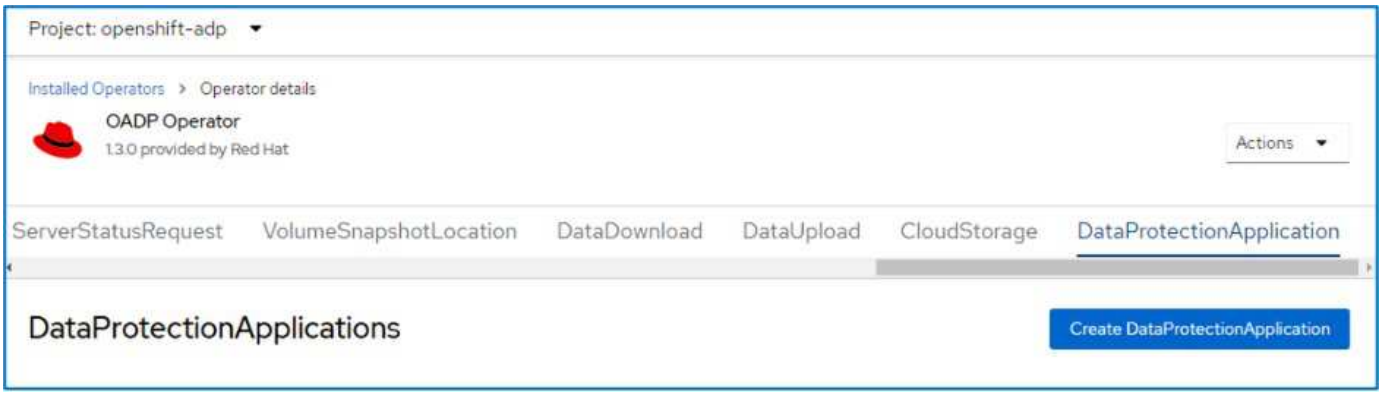
Per creare un segreto denominato sg-s3-credentials dalla CLI è possibile utilizzare il seguente comando.

```
# 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>
```

- Successivamente, per configurare Velero, seleziona Operatori installati dalla voce di menu in Operatori, fai clic sull'operatore OADP e seleziona la scheda DataProtectionApplication.



Fare clic su Crea applicazione di protezione dati. Nella visualizzazione del modulo, specificare un nome per l'applicazione DataProtection oppure utilizzare il nome predefinito.



Ora vai alla vista YAML e sostituisci le informazioni 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
```

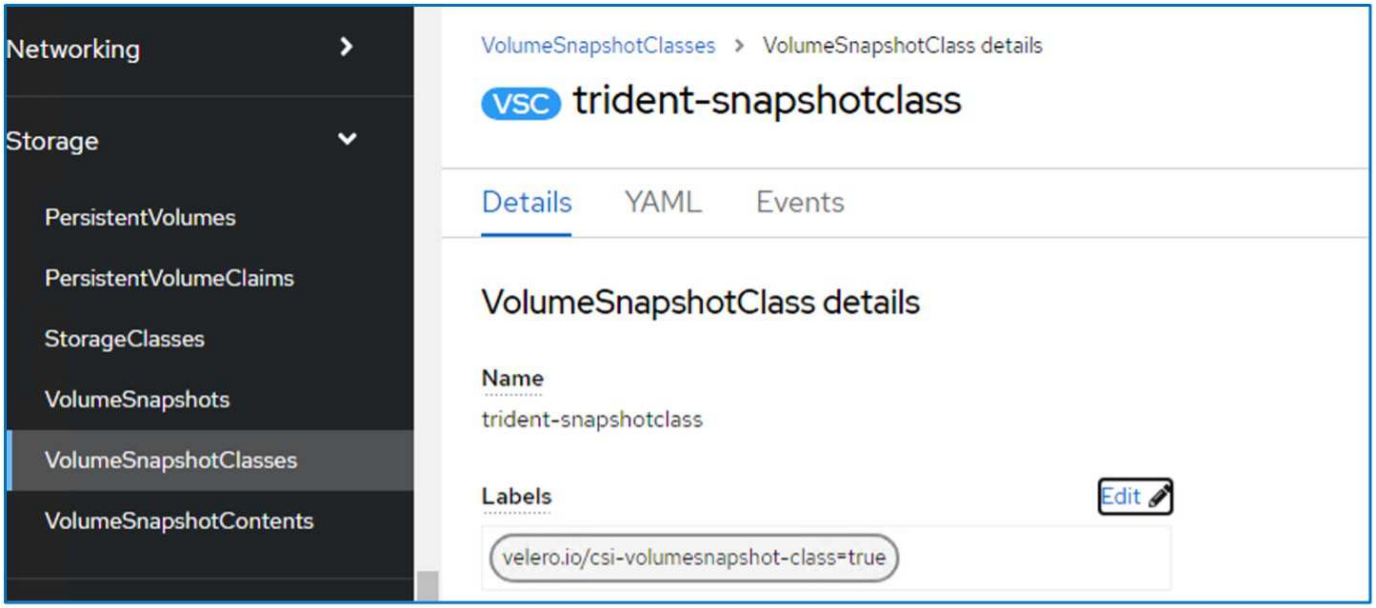
La sezione spec nel file yaml dovrebbe essere configurata in modo appropriato per i seguenti parametri simili all'esempio sopra

backupLocations ONTAP S3 o StorageGrid S3 (con le relative credenziali e altre informazioni come mostrato nel file yaml) è configurato come BackupLocation predefinito per velero.

snapshotLocations Se si utilizzano snapshot Container Storage Interface (CSI), non è necessario specificare una posizione per lo snapshot perché verrà creato un CR VolumeSnapshotClass per registrare il driver CSI. Nel nostro esempio, utilizzi Trident CSI e in precedenza hai creato VolumeSnapShotClass CR utilizzando il driver Trident CSI.

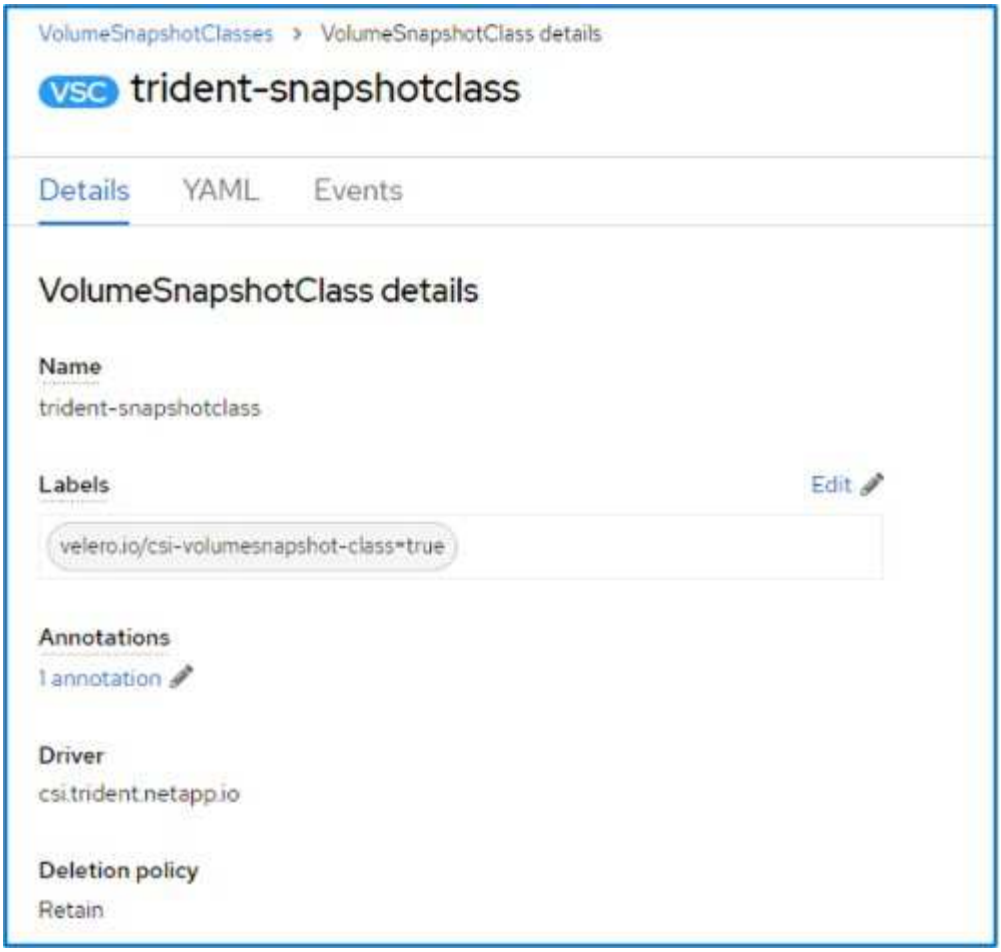
Abilita il plugin CSI Aggiungi csi ai plugin predefiniti per Velero per eseguire il backup di volumi persistenti con snapshot CSI. I plugin Velero CSI, per eseguire il backup dei PVC supportati da CSI, sceglieranno VolumeSnapshotClass nel cluster su cui è impostata l'etichetta **velero.io/csi-volumesnapshot-class**.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

- È necessario aver creato il tridente VolumeSnapshotClass.
- Modifica l'etichetta della classe trident-snapshot e impostala su **velero.io/csi-volumesnapshot-class=true** come mostrato di seguito.

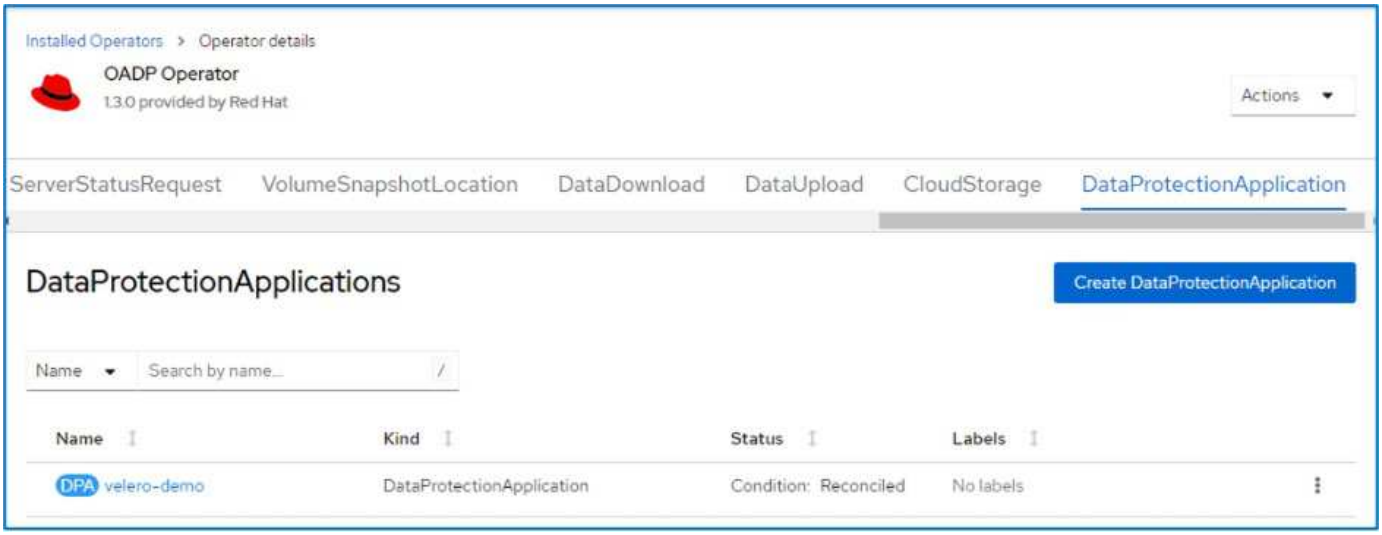


Assicurarsi che gli snapshot possano essere mantenuti anche se gli oggetti VolumeSnapshot vengono eliminati. Ciò può essere fatto impostando **deletionPolicy** su Retain. In caso contrario, l'eliminazione di uno spazio dei nomi comporterà la perdita completa di tutti i PVC in esso contenuti.

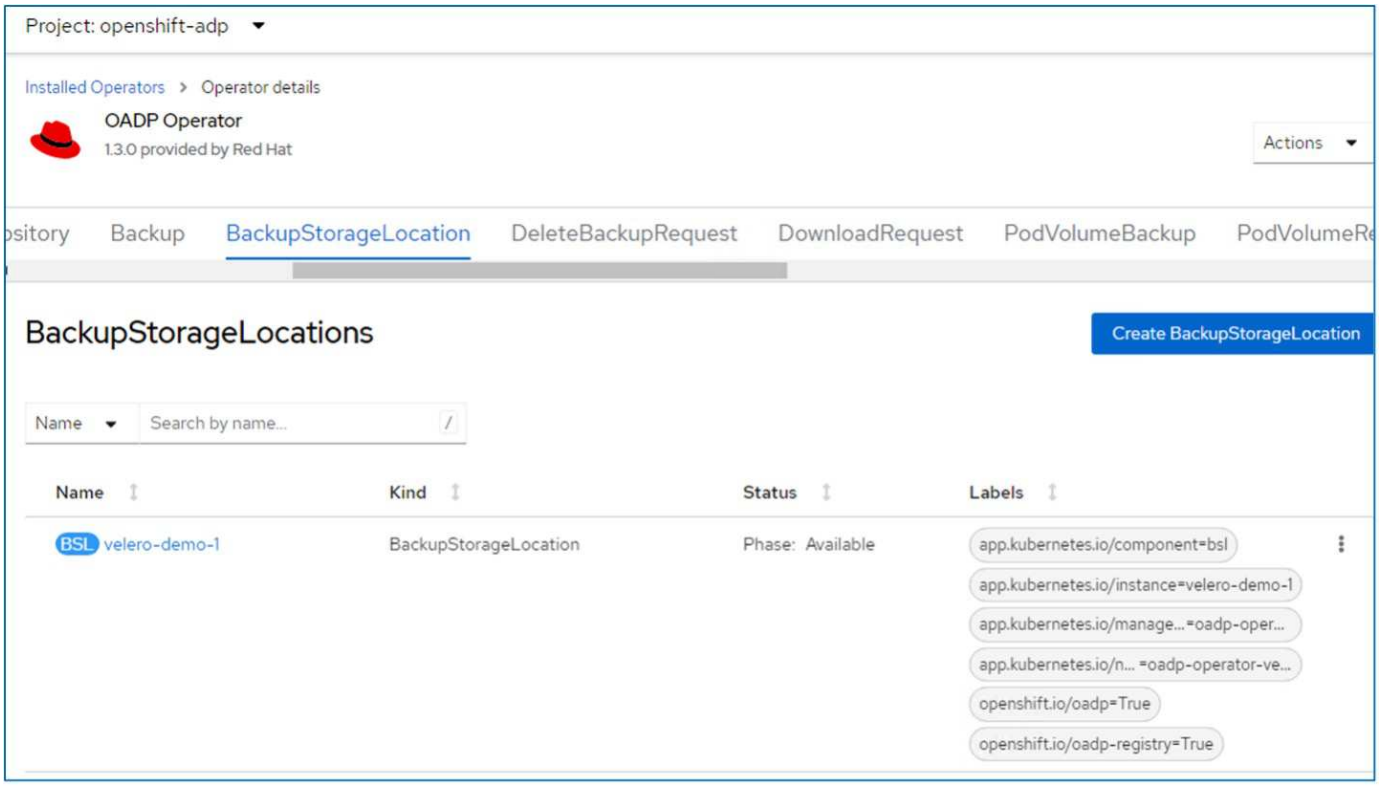
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Assicurarsi che DataProtectionApplication sia stato creato e che sia in condizione: Riconciliato.



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



Crea backup su richiesta per VM in Red Hat OpenShift Virtualization utilizzando Velero

Eseguire il backup delle VM in OpenShift Virtualization utilizzando Velero e NetApp ONTAP S3 o StorageGRID. Questa procedura include la creazione di risorse di backup personalizzate (CR) per i backup su richiesta e di CR pianificate per i backup pianificati. Ogni backup acquisisce i metadati della VM e i volumi persistenti, archiviandoli nella posizione di archiviazione degli oggetti specificata per scopi di ripristino o conformità.

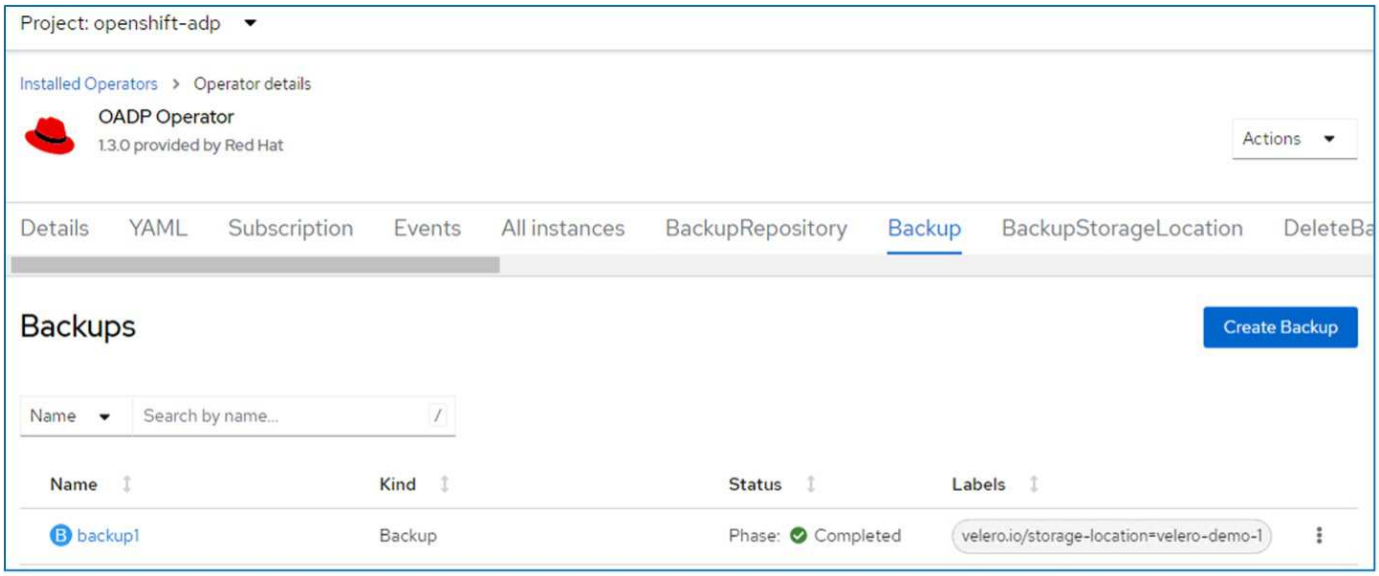
Passaggi per creare un backup di una VM

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

Il CSI creerà uno snapshot dei volumi persistenti che supportano i dischi. Un backup della VM insieme allo snapshot dei suoi dischi vengono creati e archiviati nella posizione di backup specificata nel file 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 relativa fase verrà visualizzata come completata.



È possibile ispezionare il backup nell'archivio oggetti con l'ausilio di un'applicazione browser S3. Il percorso del backup viene visualizzato nel bucket configurato con il nome del prefisso (velero/demobackup). È possibile visualizzare il contenuto del backup, inclusi gli snapshot del volume, i registri e altri metadati della macchina virtuale.

> In StorageGrid è anche possibile utilizzare la console S3 disponibile in Tenant Manager 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

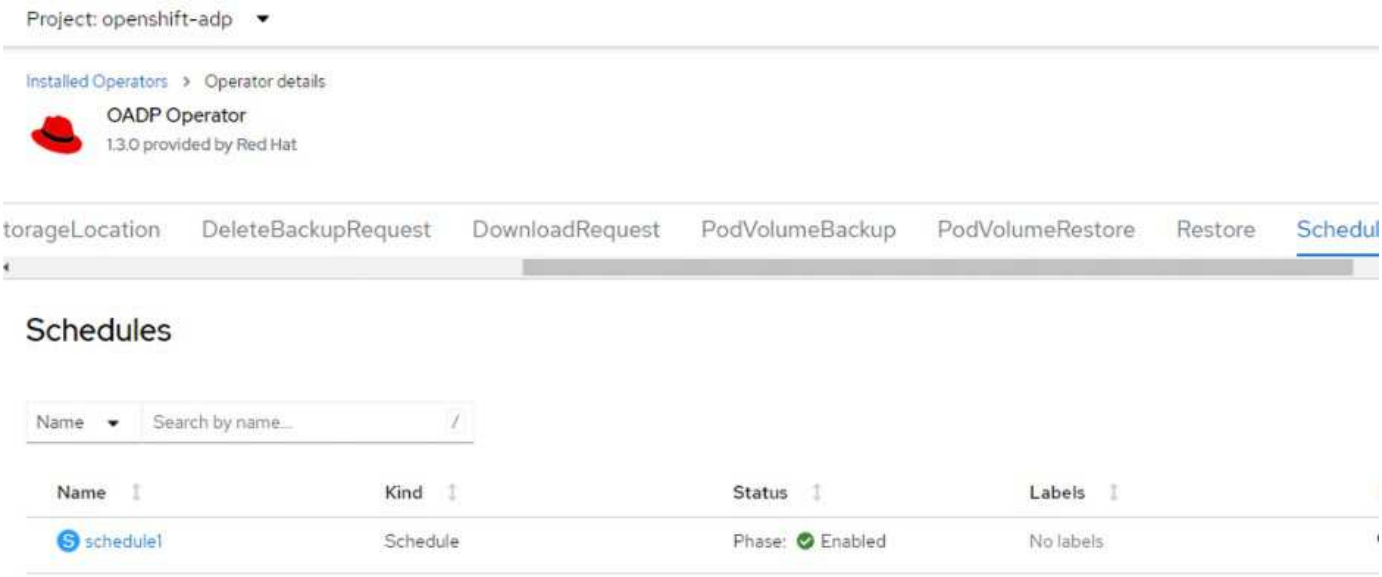
Creazione di backup pianificati per le VM in OpenShift Virtualization

Per creare backup pianificati, è necessario creare un CR pianificato. La pianificazione è semplicemente un'espressione Cron che consente di specificare l'ora in cui si desidera creare il backup. Un esempio di file YAML per creare una Schedule CR.

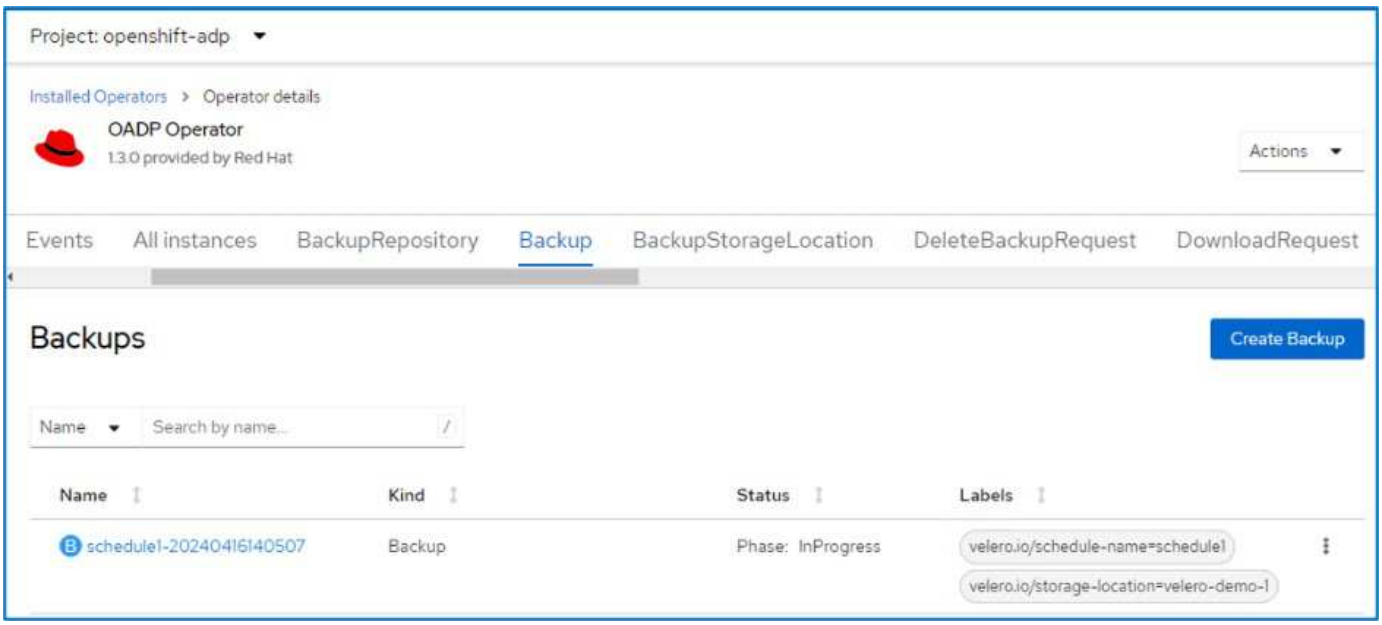
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

L'espressione Cron 0 7 * * * significa che ogni giorno verrà creato un backup alle 7:00. Vengono inoltre specificati gli spazi dei nomi da includere nel backup e la posizione di archiviazione per il backup. Quindi, invece di un Backup CR, viene utilizzato il metodo Schedule CR per creare un backup all'ora e con la frequenza specificate.

Una volta creata, la pianificazione sarà abilitata.



I backup verranno creati in base a questa pianificazione e potranno essere visualizzati nella scheda Backup.



Ripristina una VM dal backup in Red Hat OpenShift Virtualization utilizzando Velero

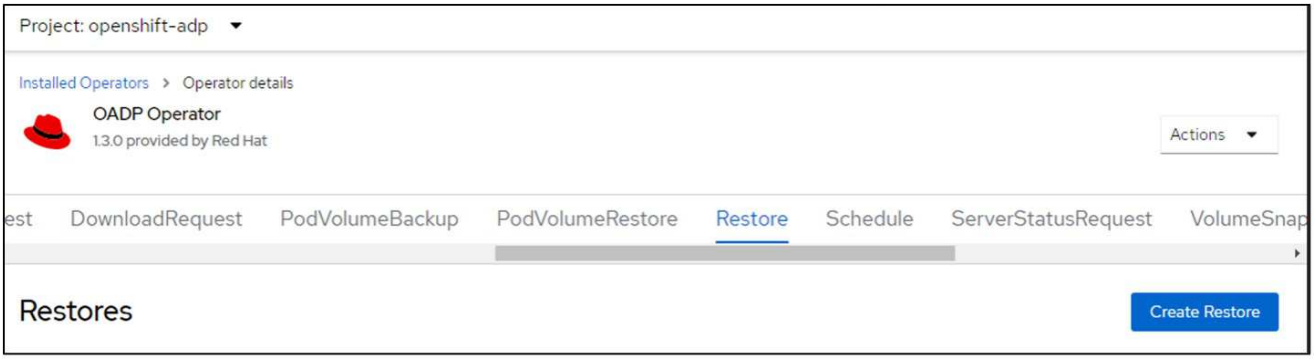
Ripristina le VM in OpenShift Virtualization utilizzando Velero e l'API OpenShift per la protezione dei dati (OADP). Questa procedura include la creazione di una risorsa personalizzata di ripristino (CR) per recuperare le VM e i relativi volumi persistenti dai backup, con opzioni per il ripristino nello spazio dei nomi originale, in uno spazio dei nomi diverso o utilizzando una classe di archiviazione alternativa.

Prerequisiti

Per ripristinare da un backup, supponiamo che lo spazio dei nomi in cui era presente la macchina virtuale sia stato eliminato accidentalmente.

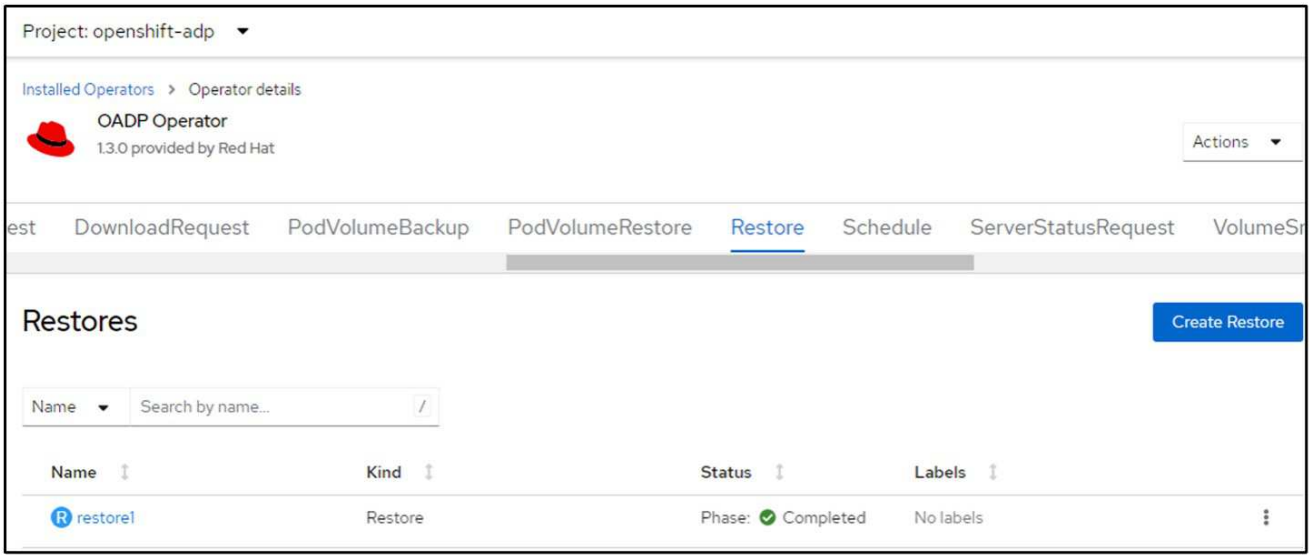
Ripristina nello stesso namespace

Per ripristinare dal backup appena creato, dobbiamo creare una risorsa personalizzata di ripristino (CR). Dobbiamo fornirgli un nome, specificare il nome del backup da cui vogliamo effettuare il ripristino e impostare restorePVs su true. È possibile impostare parametri aggiuntivi come mostrato in"documentazione" . Fare clic sul pulsante Crea.




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

Quando la fase risulta completata, è possibile vedere che le macchine virtuali sono state ripristinate allo stato in cui si trovava al momento dell'acquisizione dello snapshot. (Se il backup è stato creato quando la VM era in esecuzione, il ripristino della VM dal backup avvierà la VM ripristinata e la riporterà in stato di esecuzione). La VM viene ripristinata nello stesso namespace.



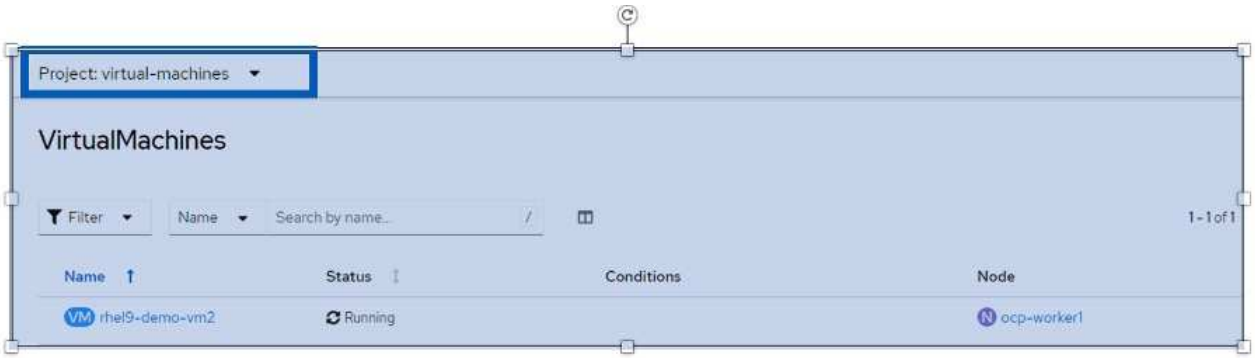
Ripristina in uno spazio dei nomi diverso

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

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

```
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
```

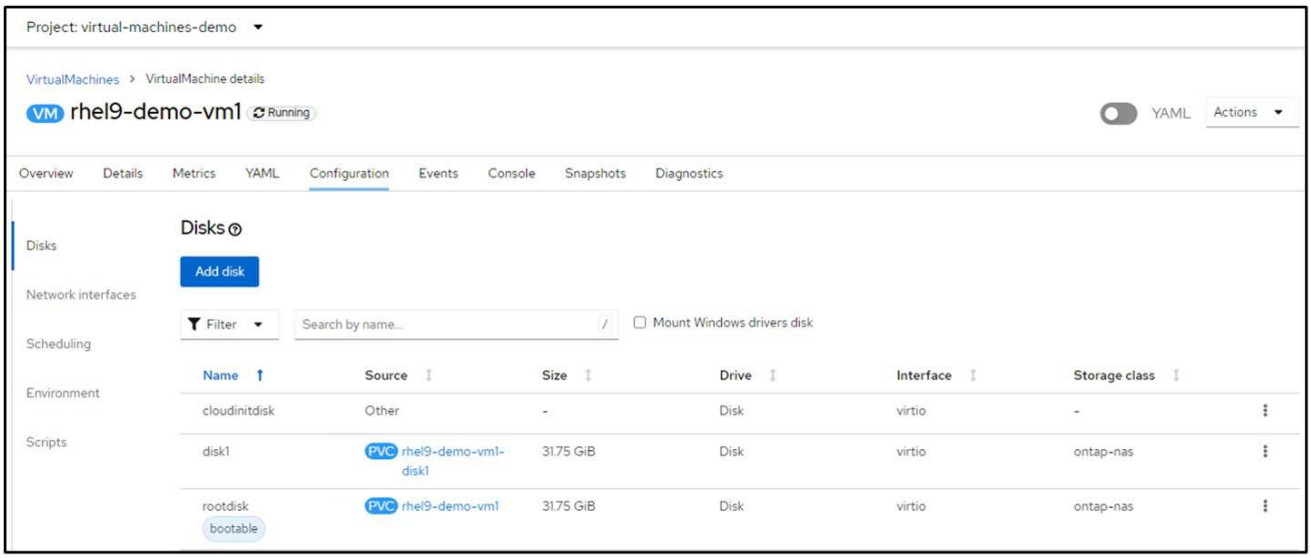
Quando la fase risulta completata, è possibile vedere che le macchine virtuali sono state ripristinate allo stato in cui si trovava al momento dell'acquisizione dello snapshot. (Se il backup è stato creato quando la VM era in esecuzione, il ripristino della VM dal backup avvierà la VM ripristinata e la riporterà in esecuzione). La VM viene ripristinata in uno spazio dei nomi diverso, come specificato nel file yaml.

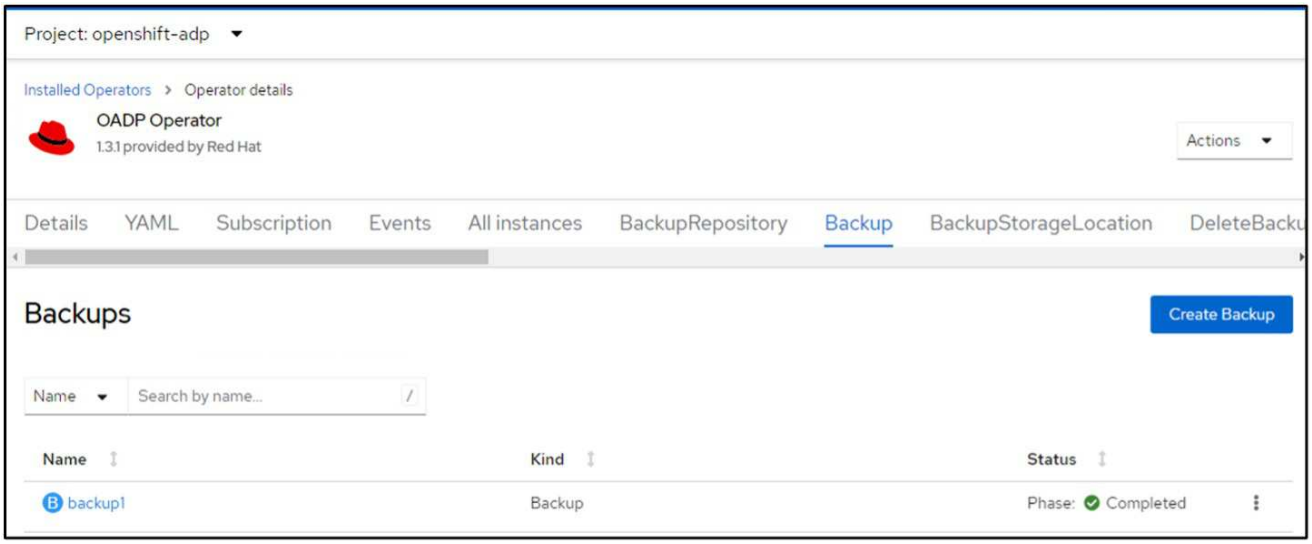


Ripristina in una classe di archiviazione diversa

Velero offre la possibilità generica di modificare le risorse durante il ripristino specificando patch JSON. Le patch json vengono applicate alle risorse prima che vengano ripristinate. Le patch json sono specificate in una configmap e la configmap è referenziata nel comando restore. Questa funzionalità consente di eseguire il ripristino utilizzando classi di archiviazione diverse.

Nell'esempio seguente, la macchina virtuale, durante la creazione, utilizza ontap-nas come classe di archiviazione per i suoi dischi. Viene creato un backup della macchina virtuale denominato backup1.





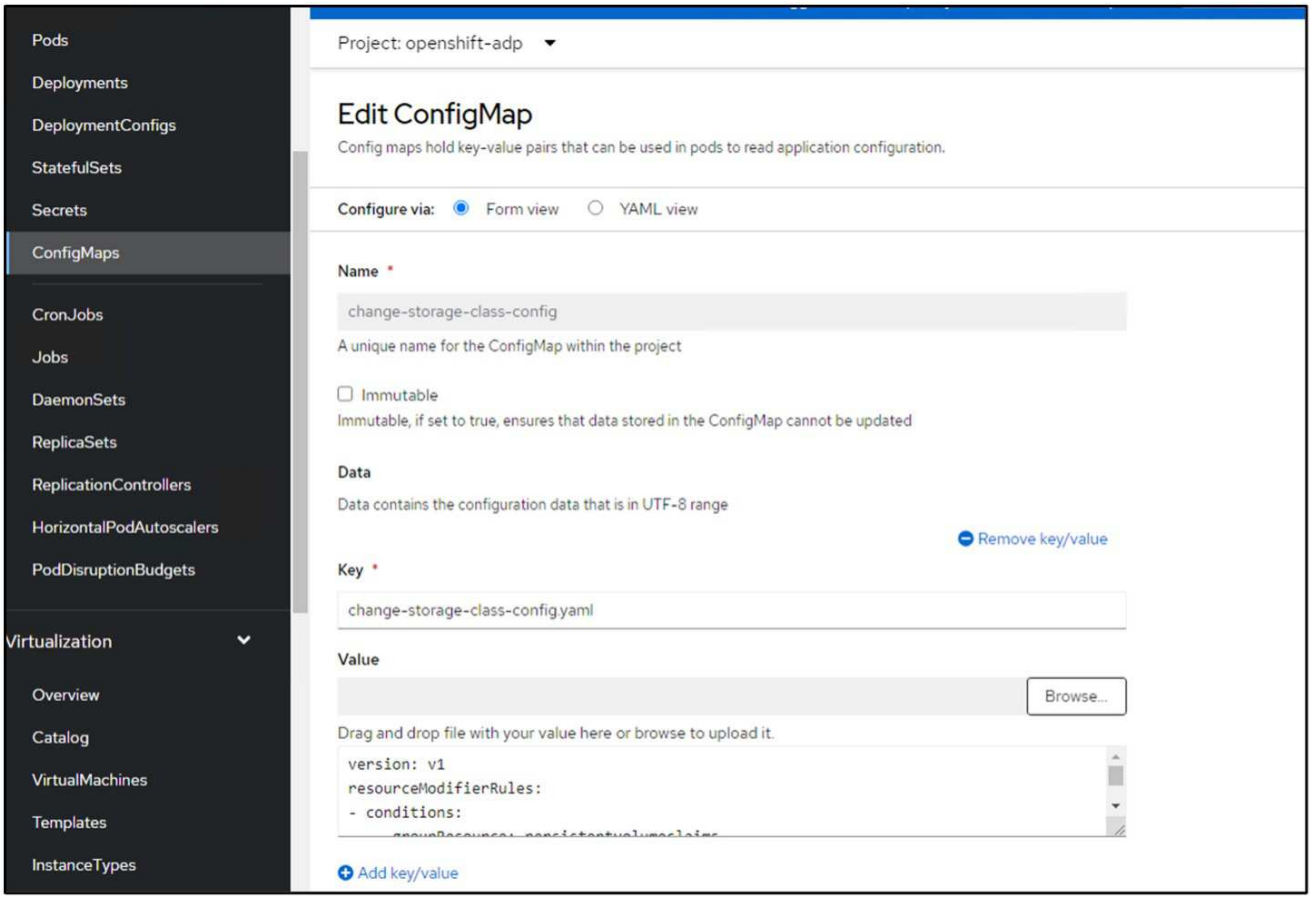
Simula la perdita della VM eliminandola.

Per ripristinare la VM utilizzando una classe di archiviazione diversa, ad esempio la classe di archiviazione ontap-nas-eco, è necessario eseguire i due passaggi seguenti:

Passaggio 1

Crea una mappa di configurazione (console) nello spazio dei nomi openshift-adp come segue: Compila i dettagli come mostrato nello screenshot: Seleziona lo 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"
```



L’oggetto mappa di configurazione risultante dovrebbe apparire così (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>
```

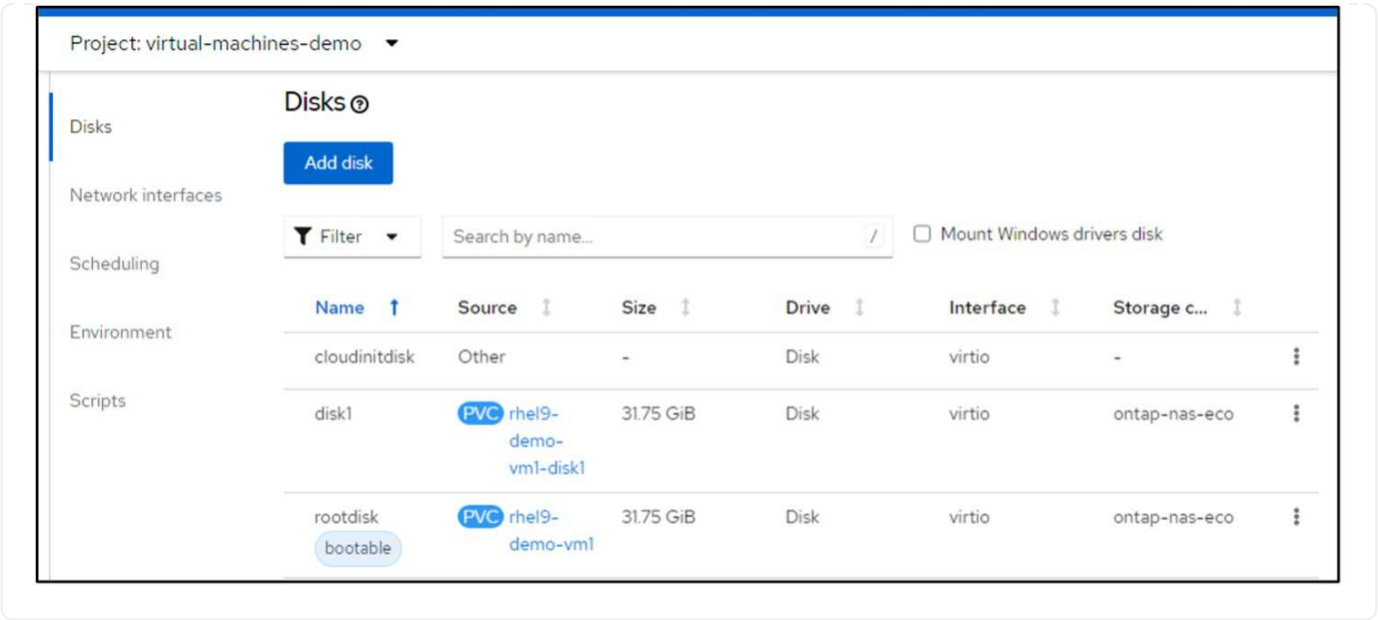
Questa mappa di configurazione applicherà la regola del modificatore di risorse quando viene creato il ripristino. Verrà applicata una patch per sostituire il nome della classe di archiviazione in ontap-nas-eco per tutte le richieste di volume persistenti che iniziano con rhel.

Passaggio 2

Per ripristinare la VM utilizzare il seguente comando dalla CLI di Velero:

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

La VM viene ripristinata nello stesso namespace con i dischi creati utilizzando la classe di archiviazione ontap-nas-eco.



Elimina un CR di backup o ripristina CR in Red Hat OpenShift Virtualization utilizzando Velero

Eliminare le risorse di backup e ripristino per le VM in OpenShift Virtualization utilizzando Velero. Utilizzare l'interfaccia della riga di comando di OpenShift per eliminare i backup mantenendo i dati di archiviazione degli oggetti oppure l'interfaccia della riga di comando di Velero per eliminare sia la risorsa personalizzata di backup (CR) sia i dati di archiviazione associati.

Eliminazione di un backup

È possibile eliminare un Backup CR senza eliminare i dati di Object Storage utilizzando lo strumento OC CLI.

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

Se si desidera eliminare il Backup CR e i dati di archiviazione degli oggetti associati, è possibile farlo utilizzando lo strumento Velero CLI.

Scaricare la CLI come indicato nelle istruzioni nel"Documentazione Velero" .

Eseguire il seguente comando di eliminazione utilizzando la CLI di Velero

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

Eliminazione di un ripristino

È possibile eliminare il ripristino CR utilizzando la CLI di Velero

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

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

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

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.