Protezione dei dati delle applicazioni dei container mediante strumenti di terze parti

NetApp Solutions

NetApp
July 18, 2024

Sommario

Protezione dei dati per container Apps in OpenShift Container Platform utilizzando OpenShift API for Data Protection (OADP)

Autore: Banu Sundhar, NetApp

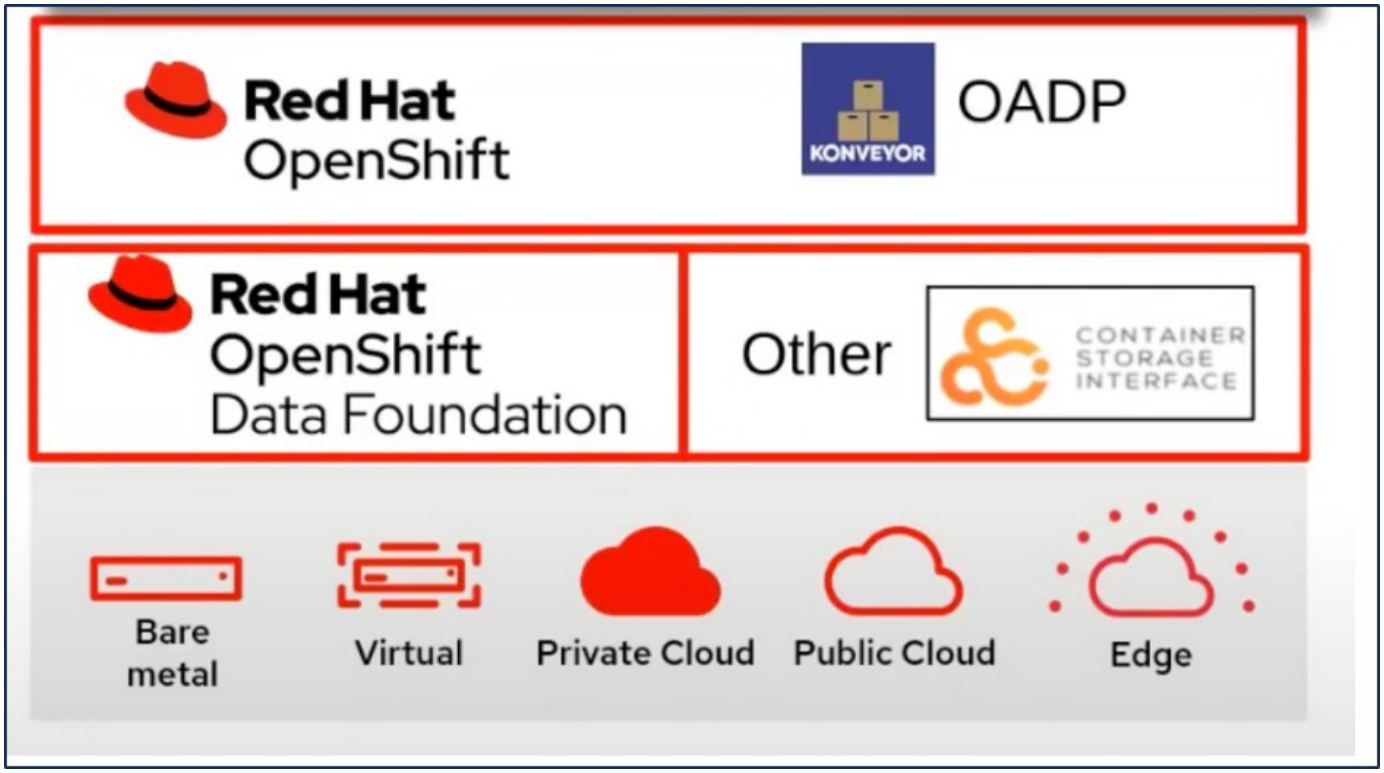
Questa sezione del documento di riferimento fornisce dettagli per la creazione di backup di app container utilizzando l'API OpenShift per la protezione dei dati (OADP) con Velero su NetApp ONTAP S3 o NetApp StorageGRID S3. I backup delle risorse con ambito del namespace, inclusi i volumi persistenti (PVS) dell'applicazione, vengono creati utilizzando gli Snapshot CSI Astra Trident.

Lo storage persistente per le app container può essere supportato dallo storage ONTAP integrato nel cluster OpenShift utilizzando "CSI Astra Trident". In questa sezione "OpenShift API per la protezione dei dati (OADP)" eseguiamo il backup di app, inclusi i volumi di dati in

- Storage a oggetti ONTAP
- StorageGRID

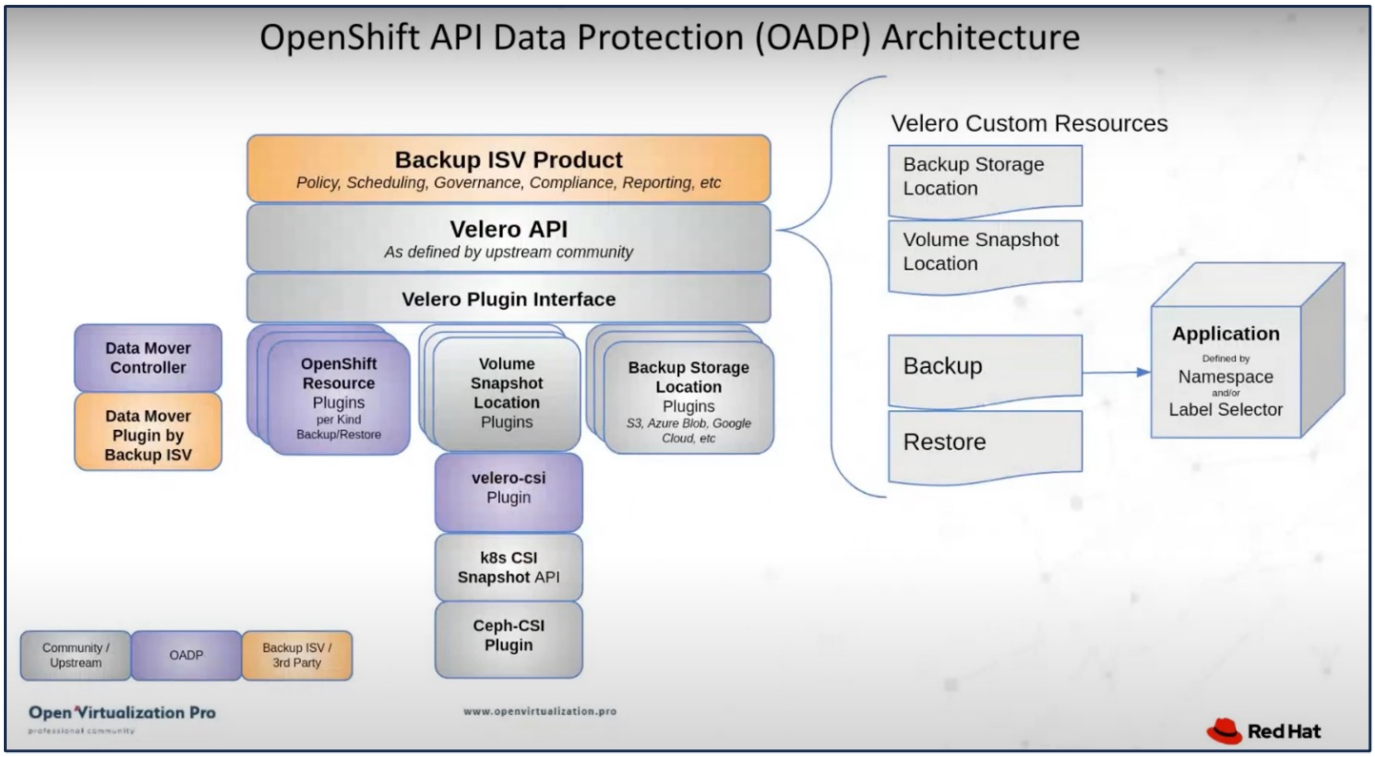
Quindi, eseguiamo il ripristino dal backup quando necessario. L'app può essere ripristinata solo nel cluster da cui è stato creato il backup.

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 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
- OADP Operator 1,13 fornito da Red Hat
- Velero CLI 1,13 per Linux
- Astra Trident 24,02
- ONTAP 9,12
- postgresql installato utilizzando helm.

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

Protezione dei dati per container Apps in OpenShift Container Platform utilizzando OpenShift API for Data Protection (OADP)

Autore: Banu Sundhar, NetApp

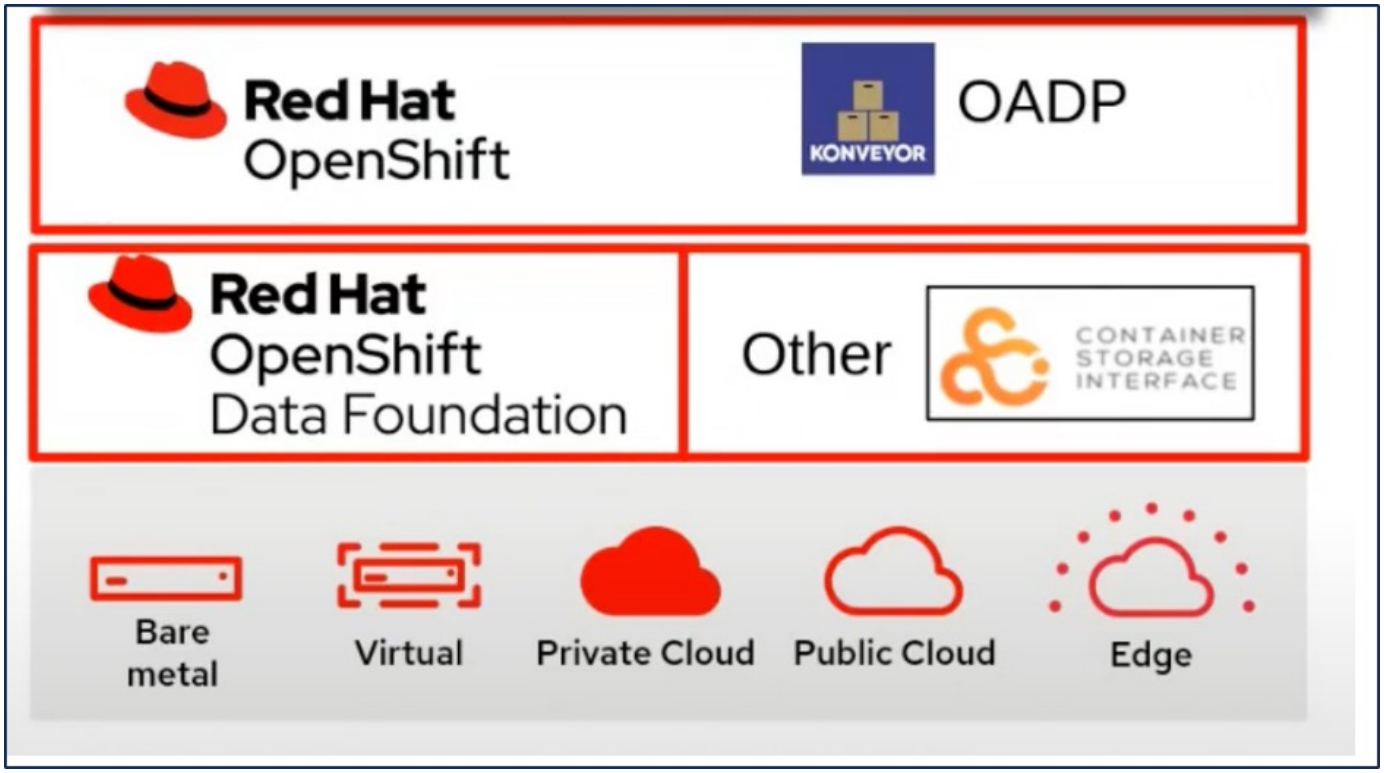
Questa sezione del documento di riferimento fornisce dettagli per la creazione di backup di app container utilizzando l'API OpenShift per la protezione dei dati (OADP) con Velero su NetApp ONTAP S3 o NetApp StorageGRID S3. I backup delle risorse con ambito del namespace, inclusi i volumi persistenti (PVS) dell'applicazione, vengono creati utilizzando gli Snapshot CSI Astra Trident.

Lo storage persistente per le app container può essere supportato dallo storage ONTAP integrato nel cluster OpenShift utilizzando "CSI Astra Trident". In questa sezione "OpenShift API per la protezione dei dati (OADP)" eseguiamo il backup di app, inclusi i volumi di dati in

- Storage a oggetti ONTAP
- StorageGRID

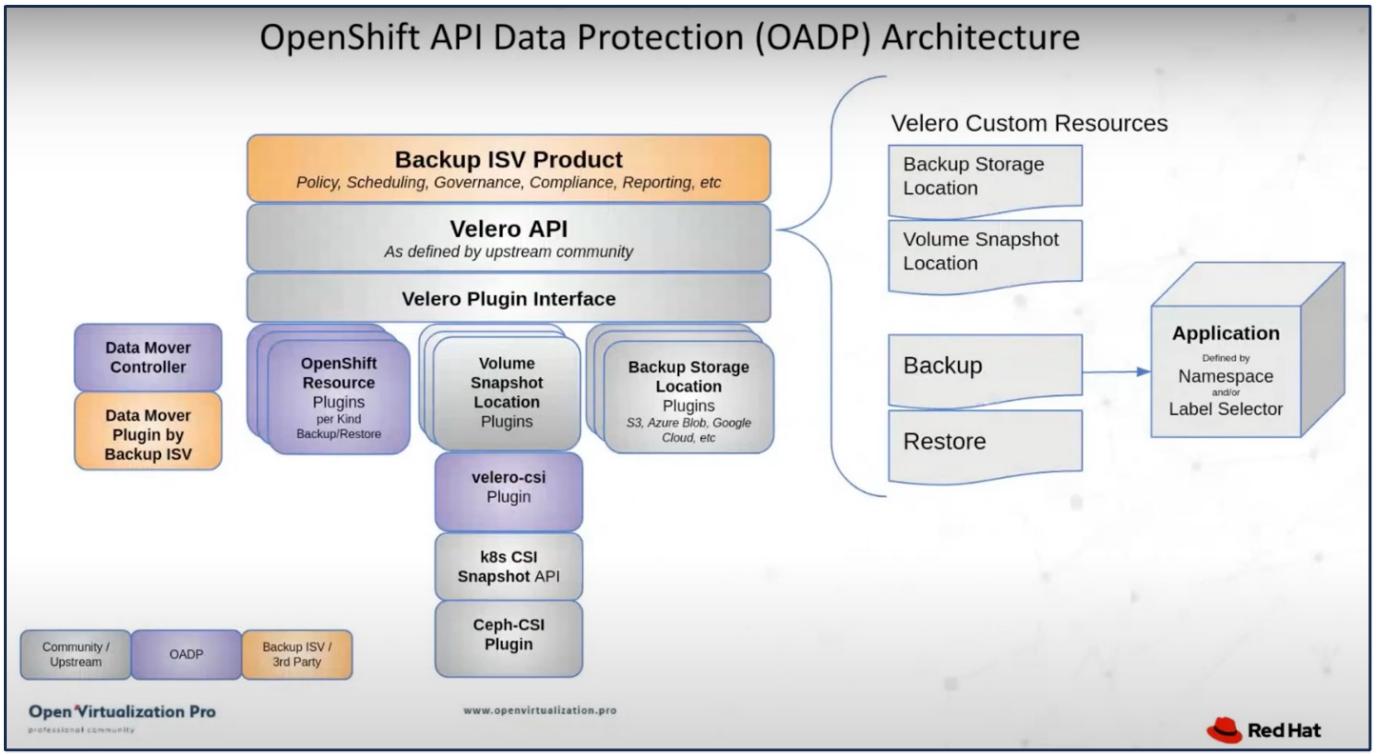
Quindi, eseguiamo il ripristino dal backup quando necessario. L'app può essere ripristinata solo nel cluster da cui è stato creato il backup.

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 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
- OADP Operator 1,13 fornito da Red Hat
- Velero CLI 1,13 per Linux
- Astra Trident 24,02
- ONTAP 9,12
- postgresql installato utilizzando helm.

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

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

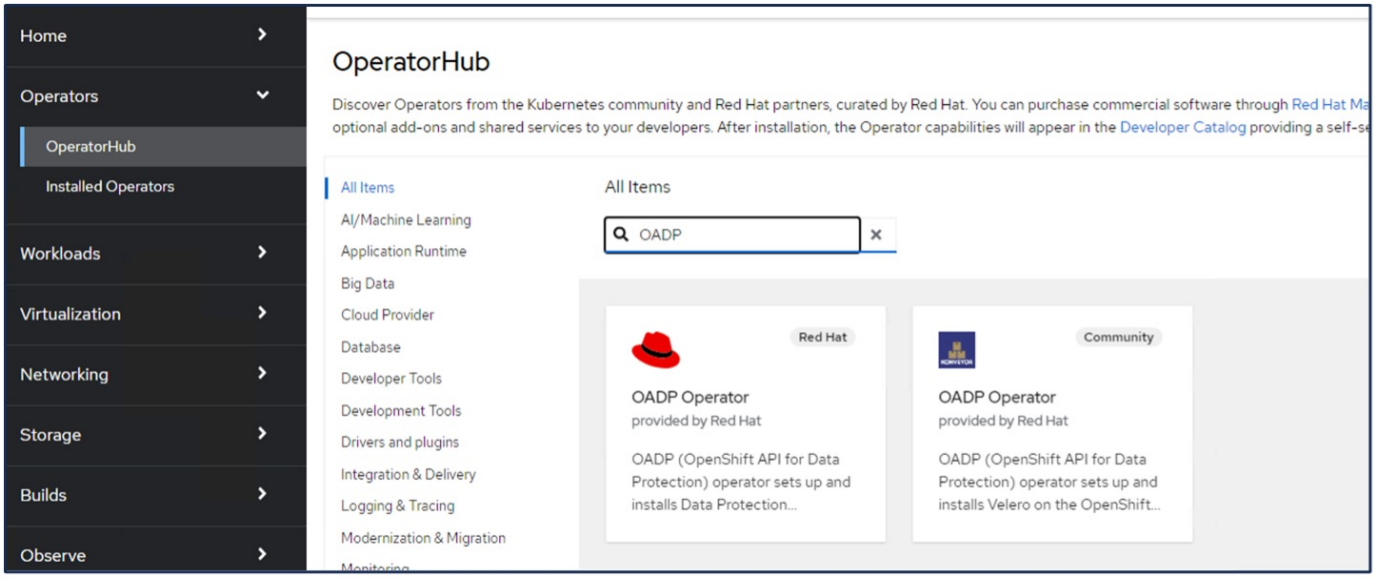
In questa sezione viene descritta l'installazione dell'operatore OpenShift API for Data Protection (OADP).

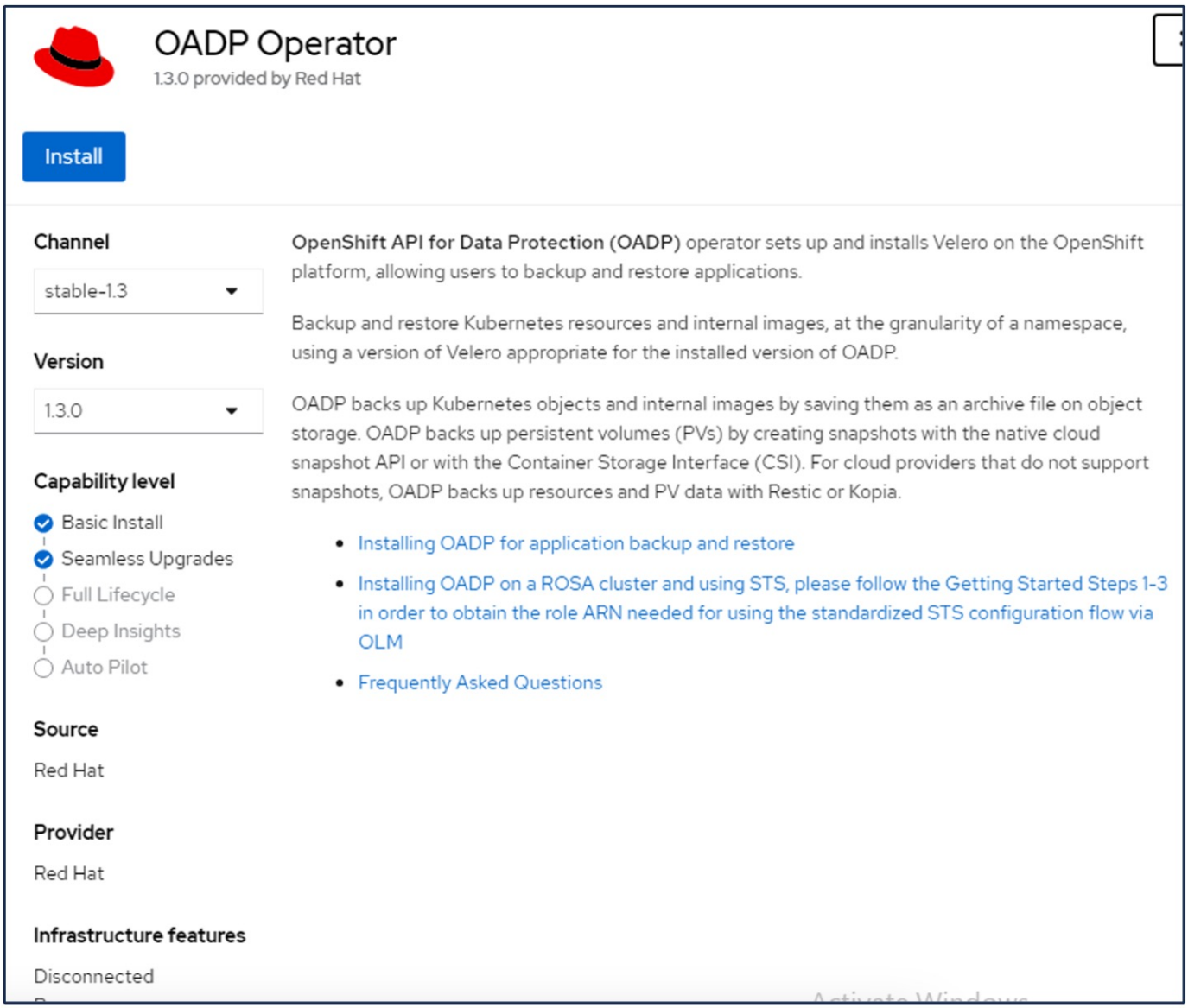
Prerequisiti

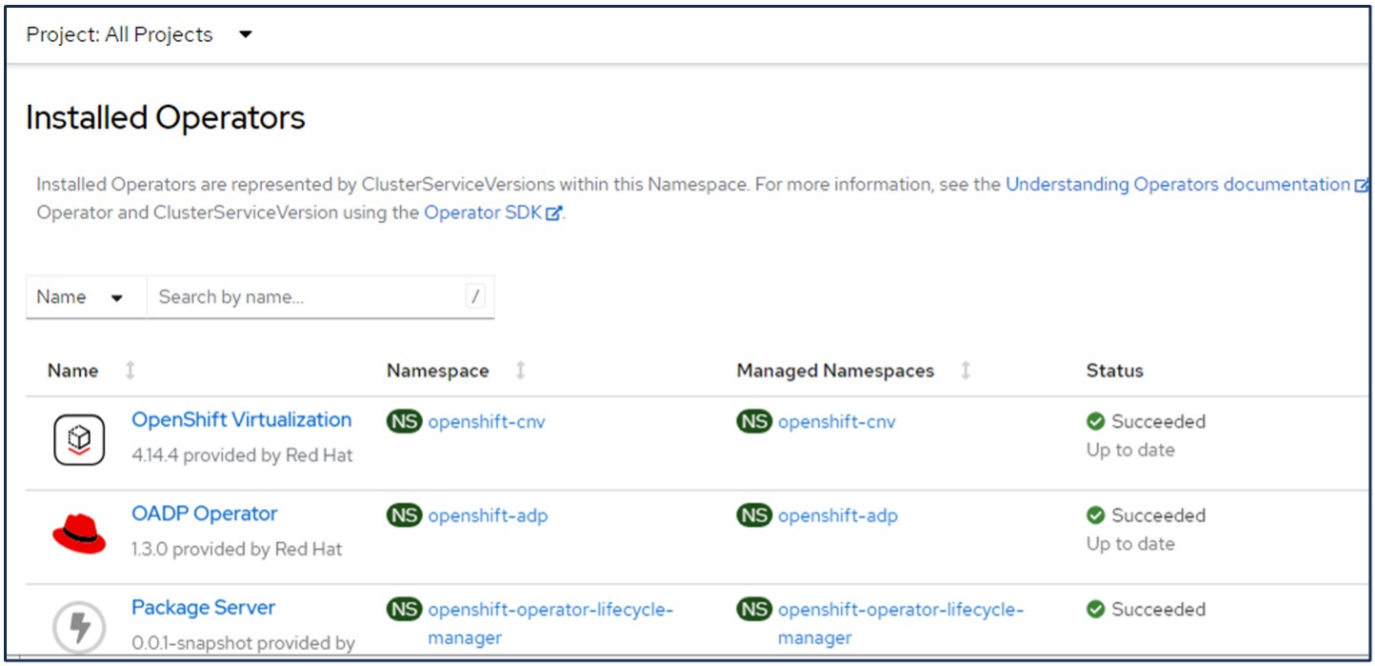
- Un cluster Red Hat OpenShift (versione successiva alla 4,12) installato in un'infrastruttura bare-metal con nodi di lavoro RHCOS
- Un cluster NetApp ONTAP integrato con il cluster utilizzando Astra Trident
- Un backend Trident configurato con una SVM sul cluster ONTAP
- StorageClass configurato sul 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
- Un'applicazione, ad esempio postgresql, distribuita sul cluster
- Una workstation di amministrazione con tridentctl e oc tools installati e aggiunti al percorso dei dollari

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
OpenShift Virtualization
4.14.4 provided by Red Hat
openshift-cnv
openshift-cnv
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

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.

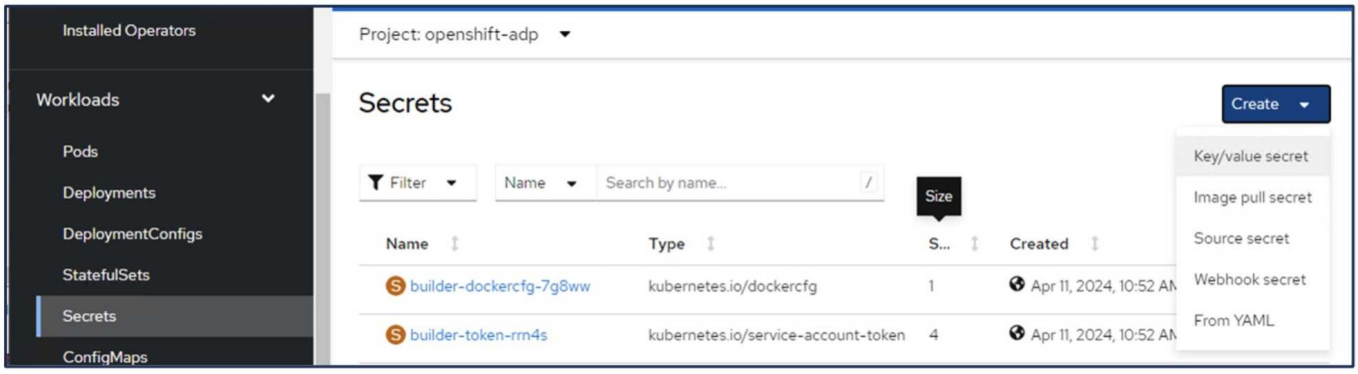
Prerequisiti per la configurazione di Velero con i dettagli di StorageGRID S3

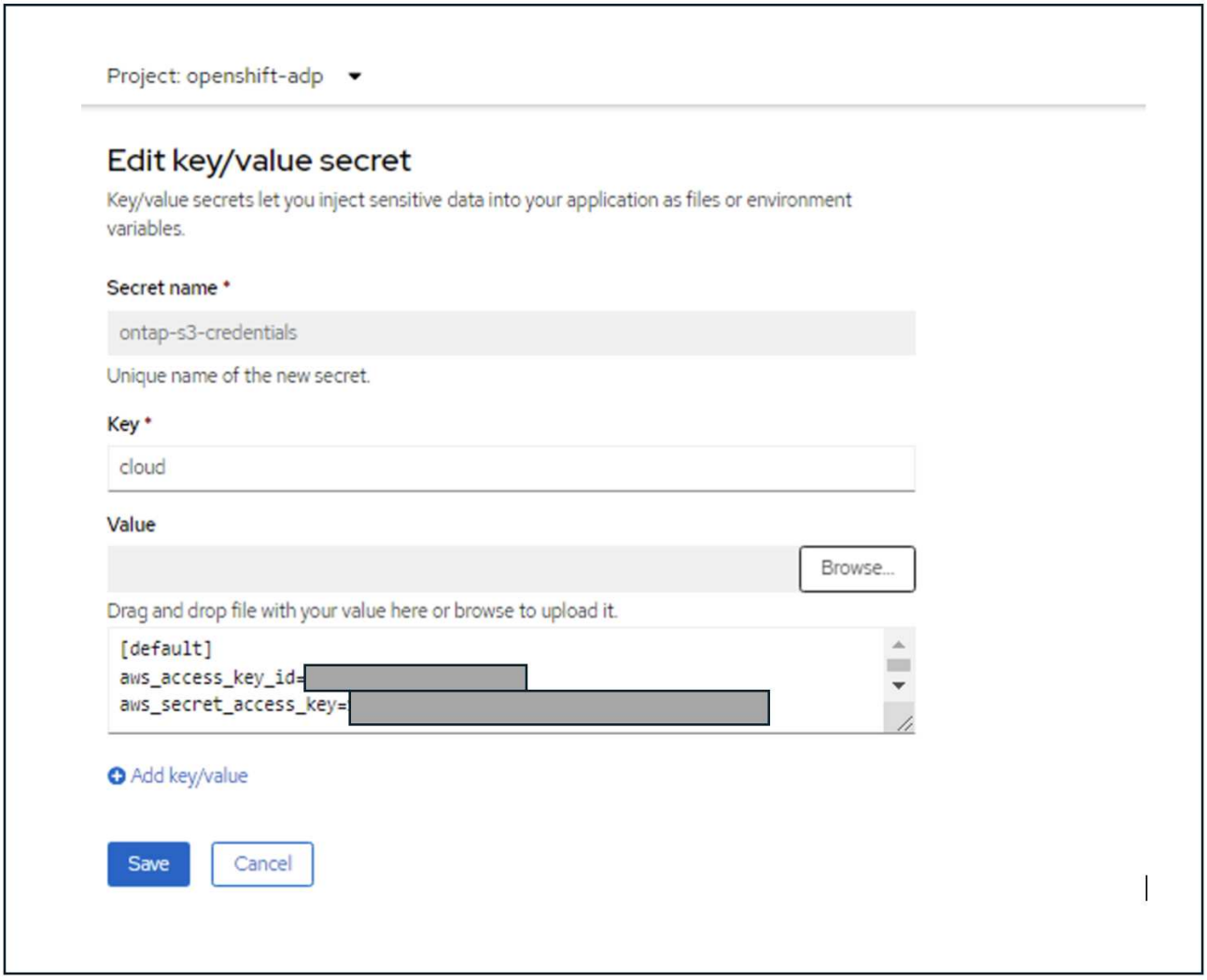
Velero può essere configurato per utilizzare l'archiviazione oggetti compatibile con S3. È possibile configurare StorageGRID S3 utilizzando le procedure illustrate nella "Documentazione StorageGRID". Per l'integrazione con Velero, sono necessarie le seguenti informazioni della configurazione di StorageGRID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

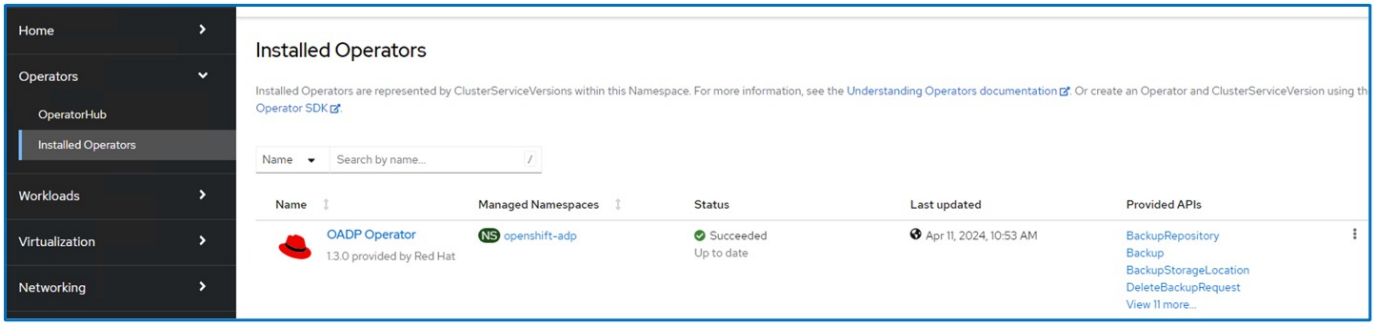




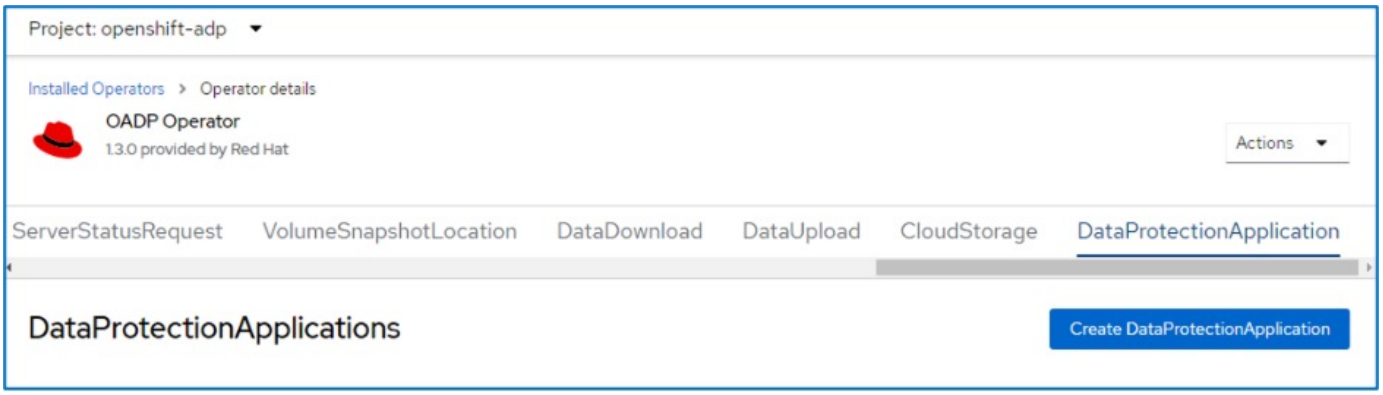
Per creare un segreto denominato sg-S3-credenziali dall'interfaccia CLI, è possibile utilizzare il seguente comando.

```
# 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://10.61.181.161' ->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: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

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

```
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

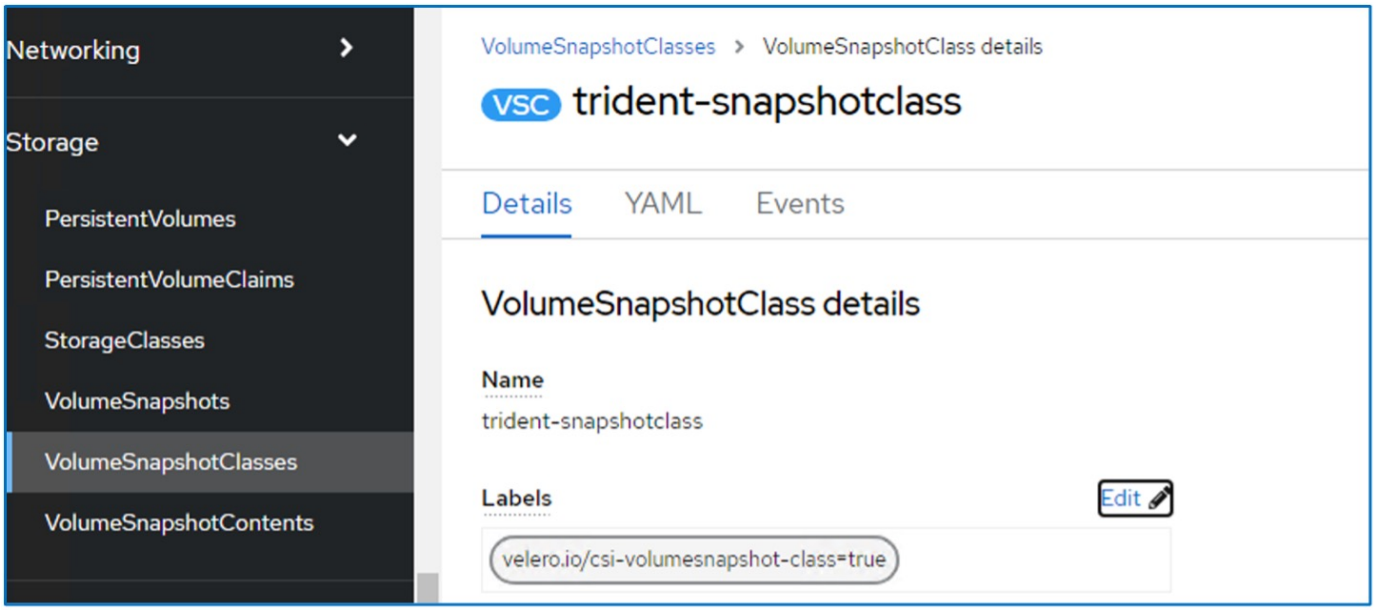
BackupLocations
ONTAP S3 o StorageGRID S3 (con le relative credenziali e altre informazioni come mostrato in yaml) è configurato come BackupLocation predefinito per velero.

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

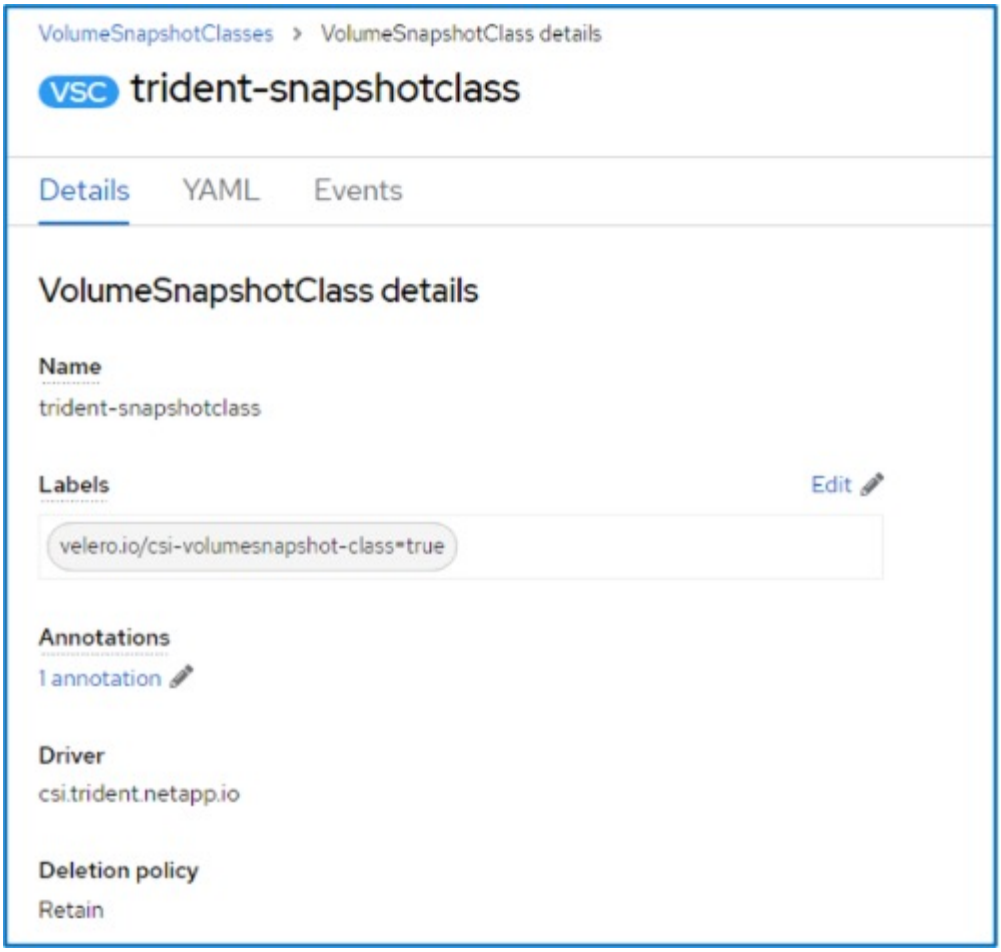
- È necessario creare il tridente VolumeSnapshotClass.

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

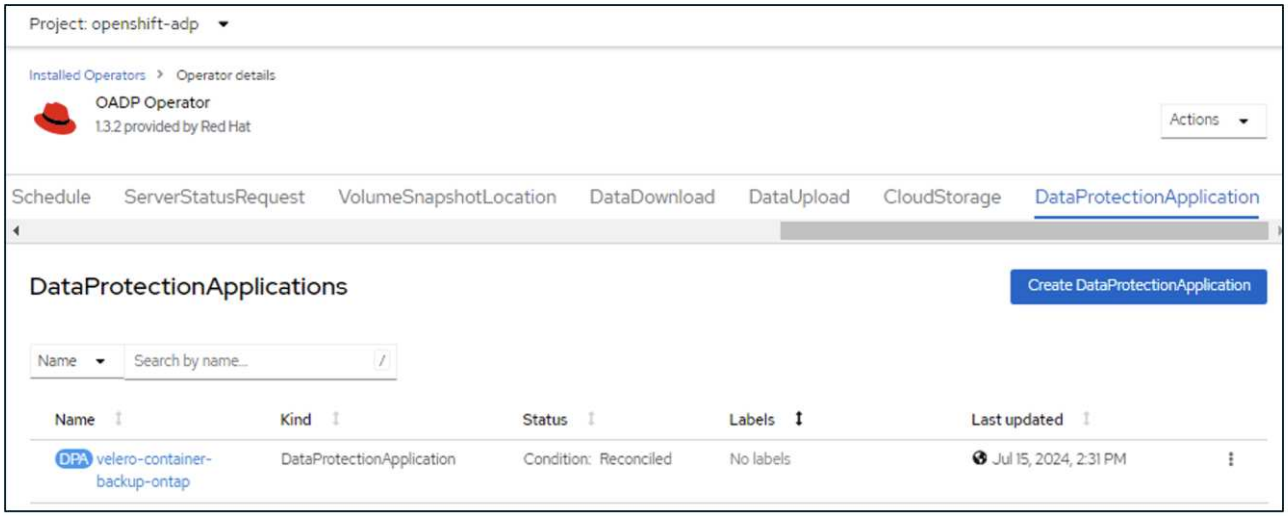


Verificare che gli snapshot possano persistere anche se gli oggetti VolumeSnapshot vengono eliminati. A tale scopo, impostare **deletionPolicy** su Retain. In caso contrario, l'eliminazione di uno spazio dei nomi perderà completamente tutti i PVC di cui è stato eseguito il backup.

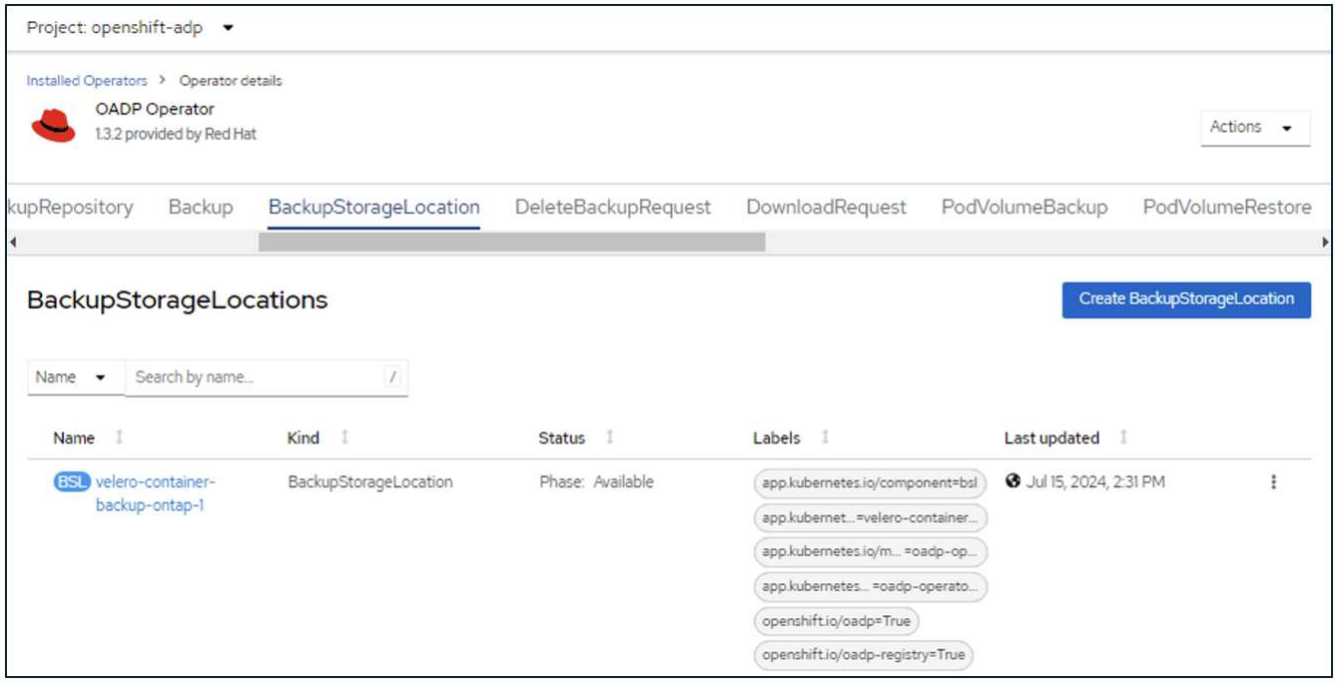
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



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



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



Creazione di backup on-demand per le app in OpenShift Container Platform

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

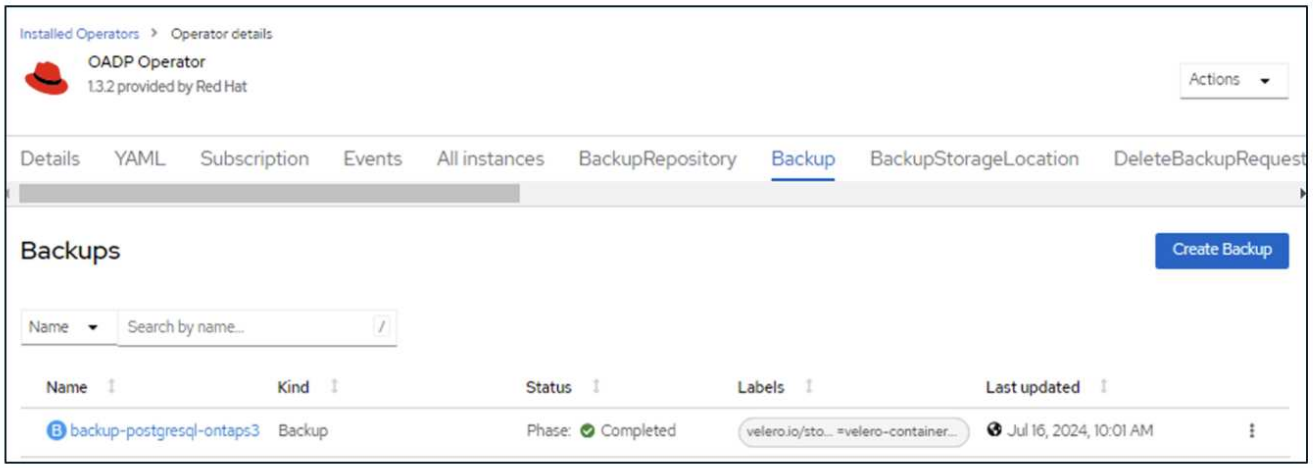
Procedura per creare un backup di un'applicazione

Per creare un backup su richiesta di un'app (metadati dell'app e volumi persistenti dell'app), fare clic sulla scheda **Backup** per creare una CR (Backup Custom Resource). Viene fornito un yaml di esempio per creare la CR di backup. Utilizzando questo yaml, verrà eseguito il backup dell'app e del relativo spazio dei nomi persistente nello spazio dei nomi specificato. È possibile impostare parametri aggiuntivi come illustrato nella "documentazione".

Un'istantanea dei volumi persistenti e delle risorse dell'app nello spazio dei nomi specificato verrà creata dal CSI. Questa istantanea verrà memorizzata nella posizione di backup specificata in yaml. Il backup rimarrà nel sistema per 30 giorni come specificato nel ttl.

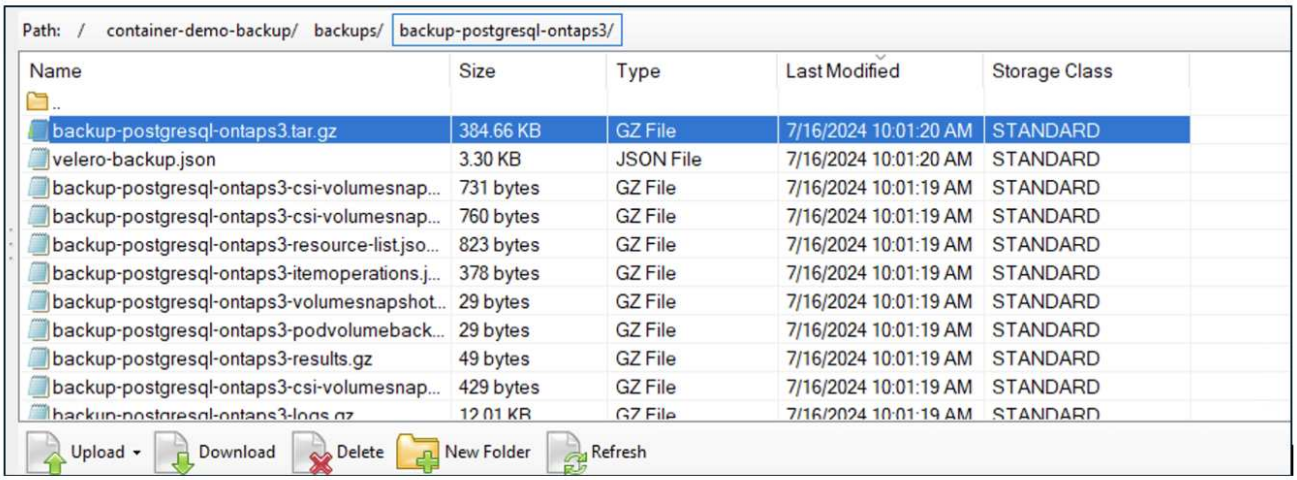
```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
  ttl: 720h0m0s
```

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



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/container-demo-backup). Il contenuto del backup comprende snapshot del volume, log e altri metadati dell'applicazione.

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



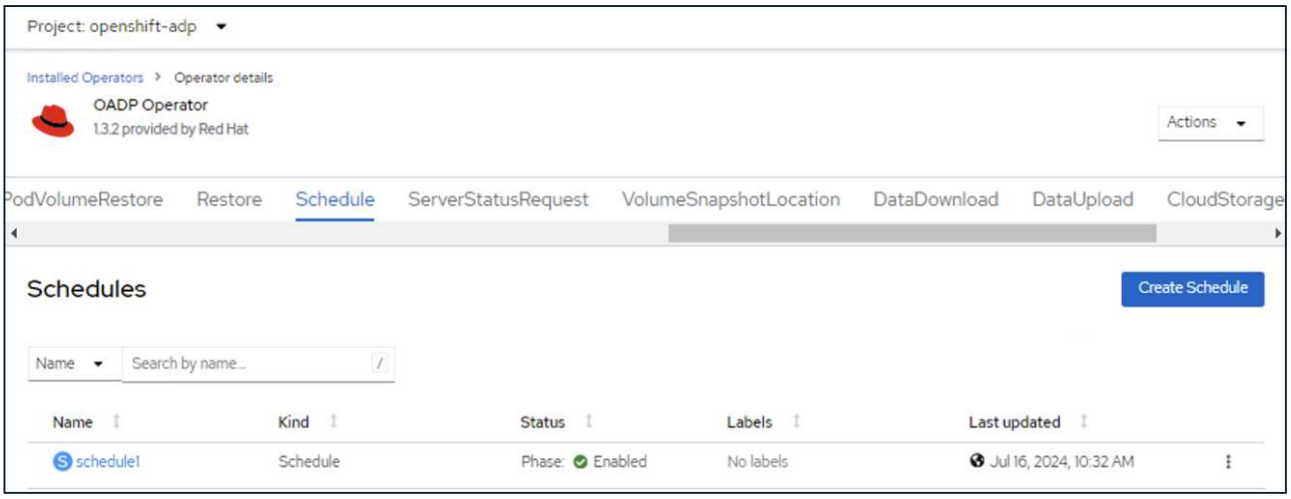
Creazione di backup pianificati per le applicazioni

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. Di seguito è riportato un esempio di yaml per la creazione di una pianificazione CR.

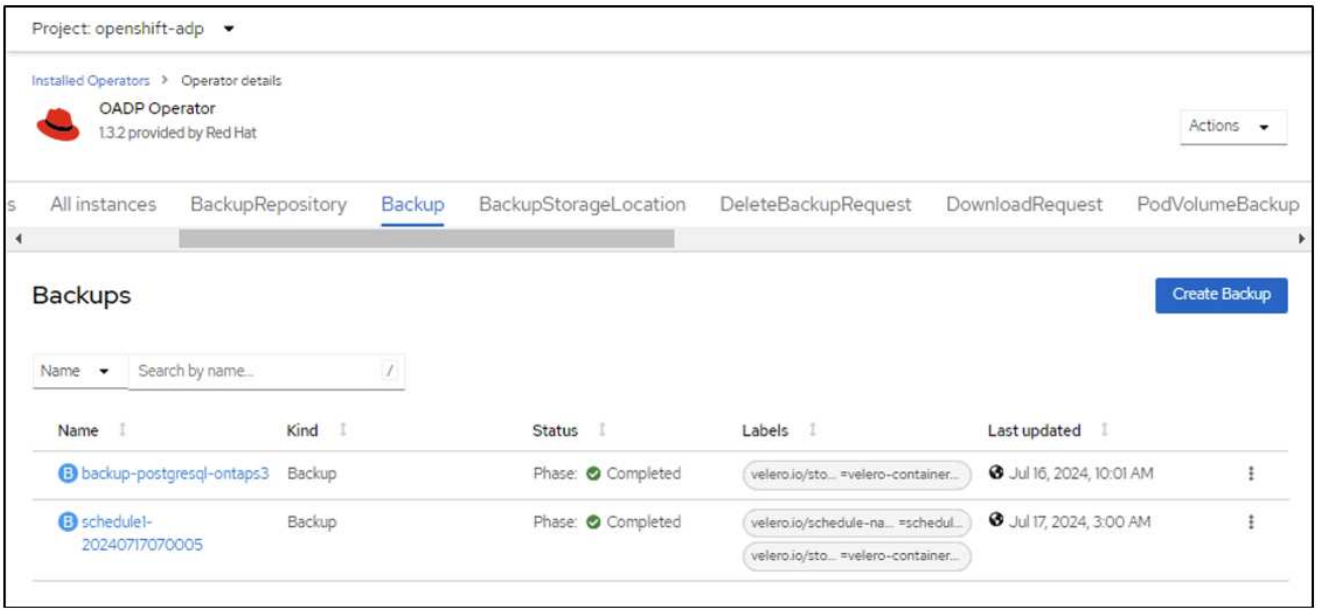
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

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.



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

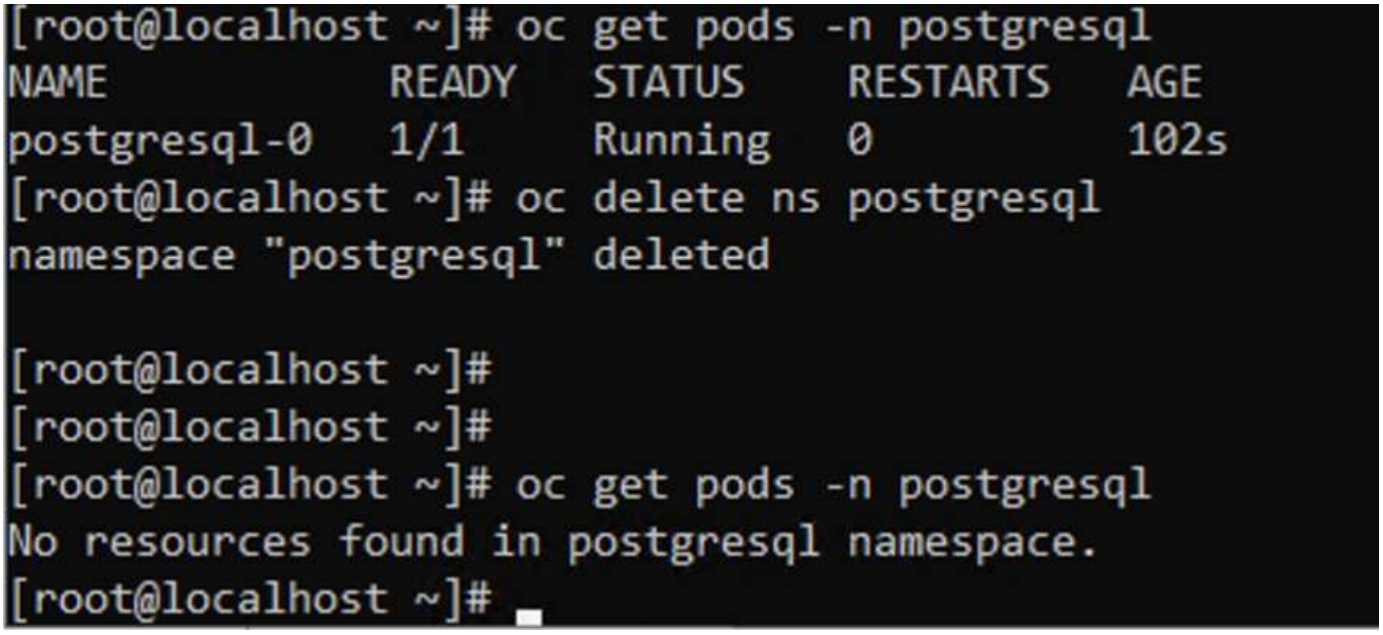


Ripristinare un'applicazione da un backup

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

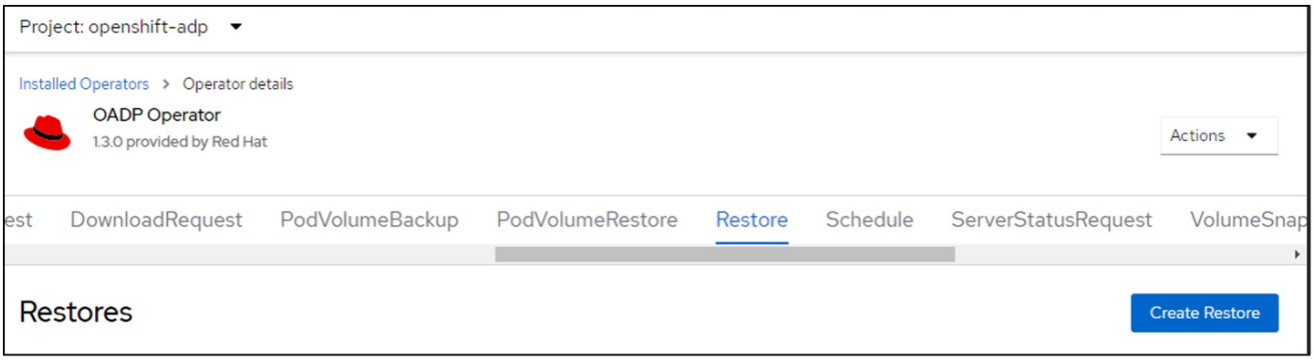
Prerequisiti

Per eseguire il ripristino da un backup, presupponiamo che lo spazio dei nomi in cui esisteva l'applicazione sia stato eliminato accidentalmente.


[root@localhost ~]# oc get pods -n postgresql
NAME READY STATUS RESTARTS AGE
postgresql-0 1/1 Running 0 102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#

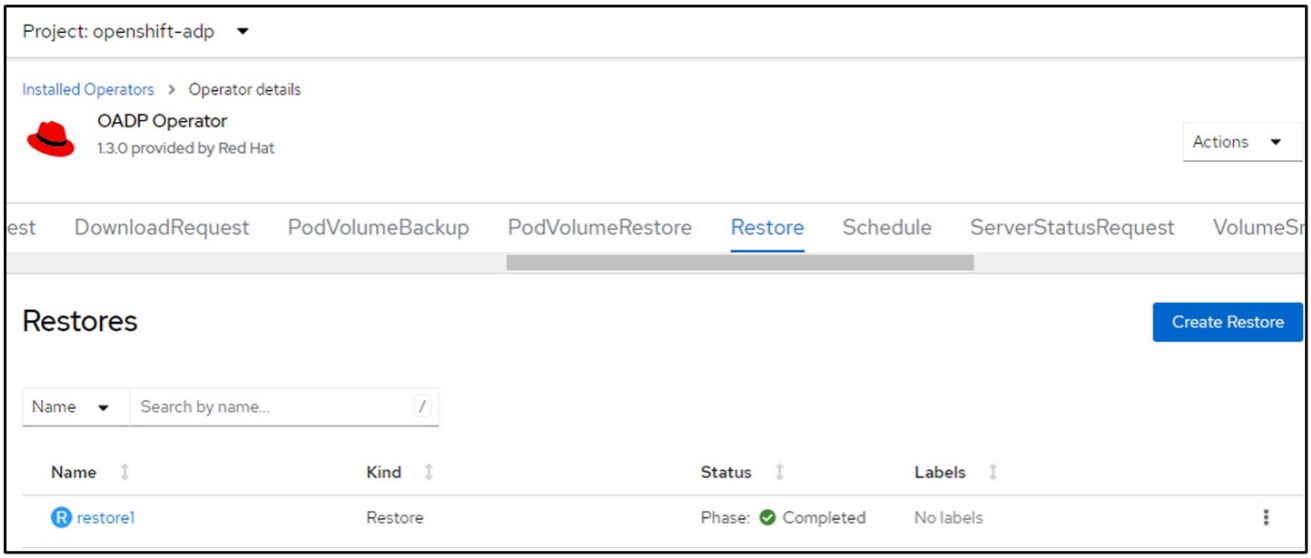
Ripristinare nello stesso namespace

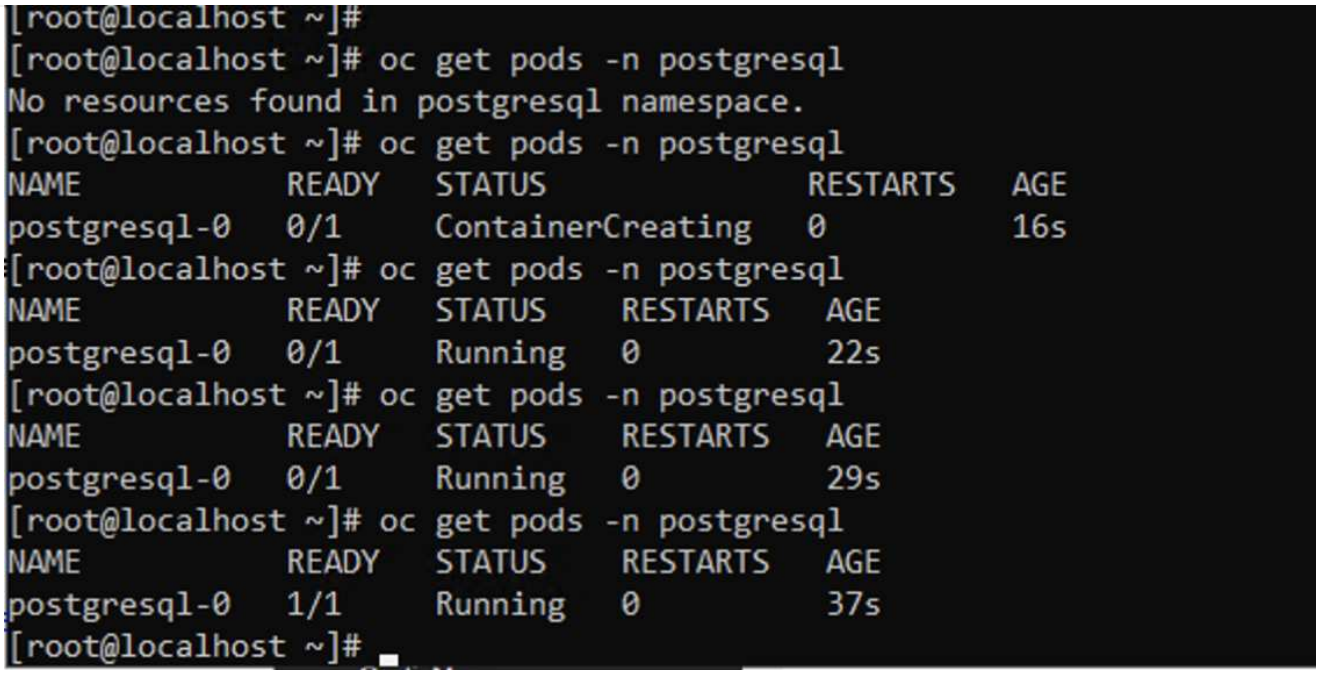
Per eseguire il ripristino dal backup appena creato, è necessario creare una risorsa personalizzata di ripristino (CR). Dobbiamo fornirgli un nome, fornire il nome del backup da cui eseguire il ripristino e impostare su true. È possibile impostare parametri aggiuntivi come illustrato nella "documentazione".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




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

Quando la fase viene visualizzata come completata, è possibile vedere che l'app è stata ripristinata allo stato in cui è stata scattata l'istantanea. L'applicazione viene ripristinata nello stesso spazio dei nomi.




[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME READY STATUS RESTARTS AGE
postgresql-0 0/1 ContainerCreating 0 16s
[root@localhost ~]# oc get pods -n postgresql
NAME READY STATUS RESTARTS AGE
postgresql-0 0/1 Running 0 22s
[root@localhost ~]# oc get pods -n postgresql
NAME READY STATUS RESTARTS AGE
postgresql-0 0/1 Running 0 29s
[root@localhost ~]# oc get pods -n postgresql
NAME READY STATUS RESTARTS AGE
postgresql-0 1/1 Running 0 37s
[root@localhost ~]#

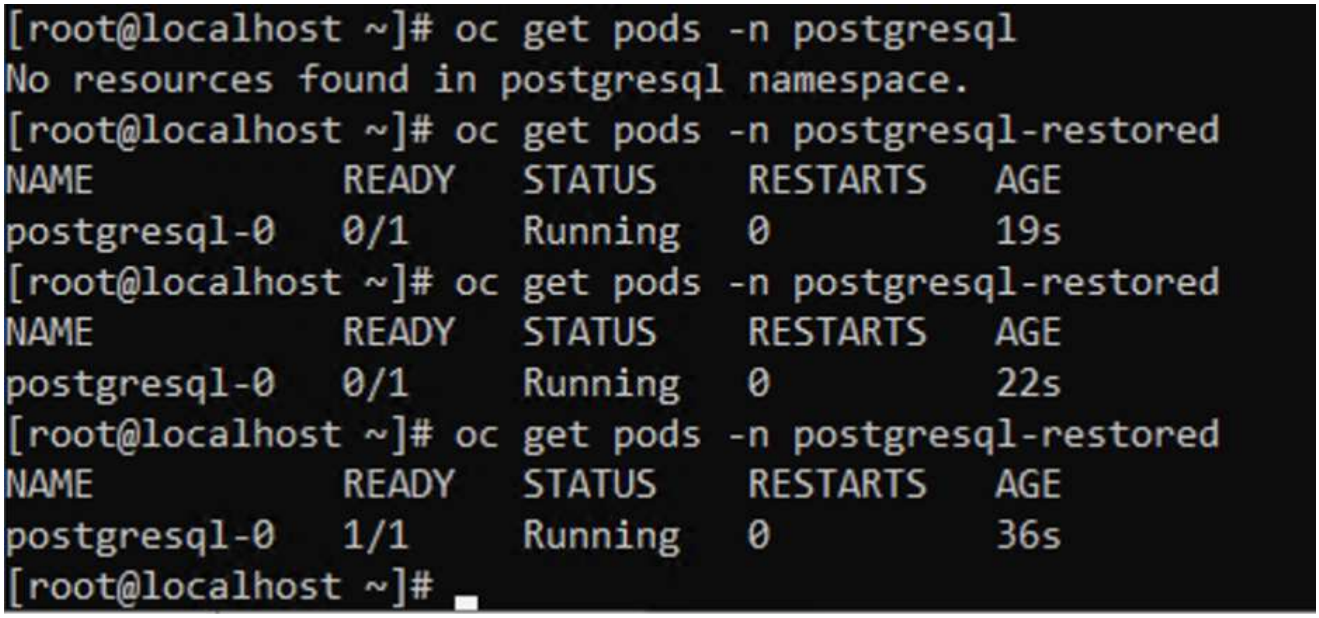
Ripristinare in un namespace diverso

Per ripristinare l'app in uno spazio dei nomi diverso, è possibile fornire un namespaceMapping nella definizione yaml di Restore CR.

Il seguente file yaml di esempio crea una CR di ripristino per ripristinare un'app e la relativa memoria persistente dallo spazio dei nomi postgresql al nuovo spazio dei nomi postgresql-ripristinato.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

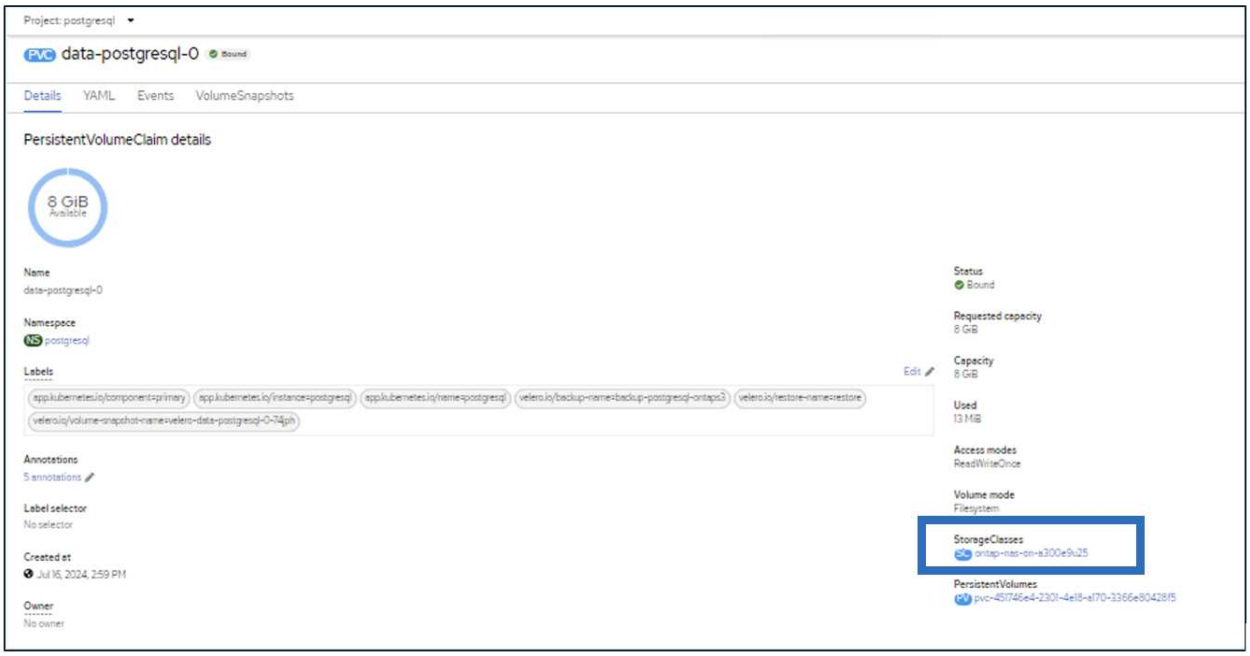
Quando la fase viene visualizzata come completata, è possibile vedere che l'app è stata ripristinata allo stato in cui è stata scattata l'istantanea. L'app viene ripristinata in uno spazio dei nomi diverso, come specificato in yaml.

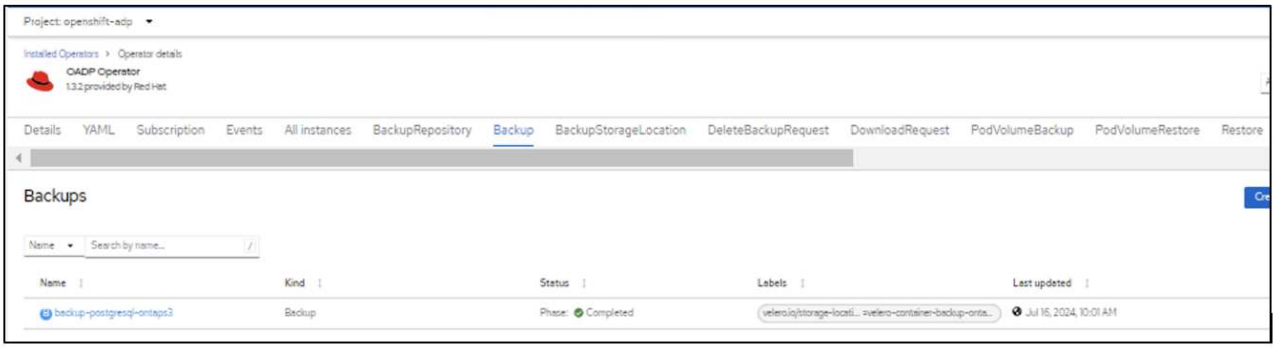


Ripristinare in una classe di archiviazione diversa

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, l'applicazione, in fase di implementazione, utilizza ontap-nas come classe di storage per i propri volumi persistenti. Viene creato un backup dell'applicazione denominata backup-postgresql-ontaps3.





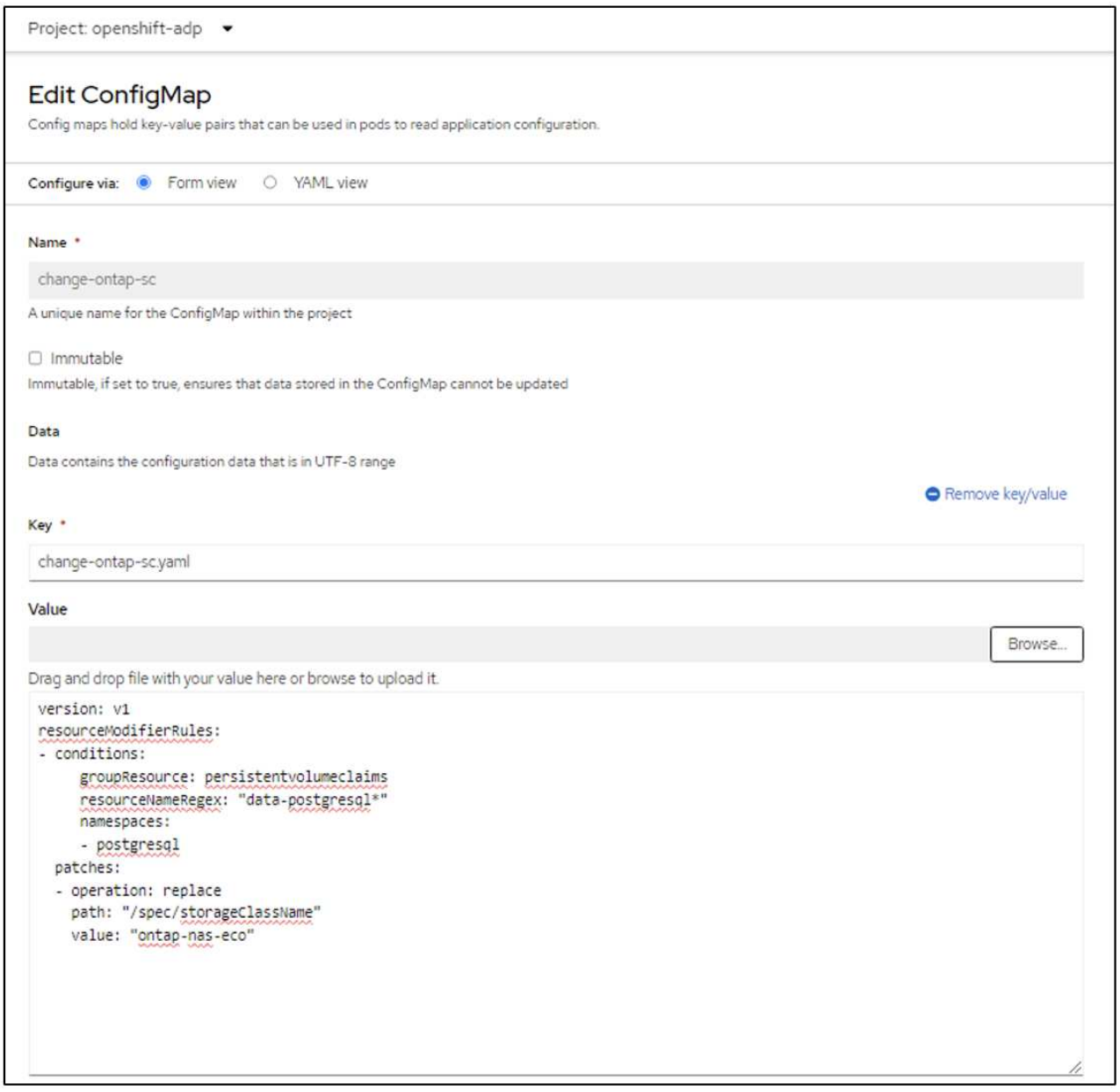
Simula una perdita dell'app disinstallando l'app.

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: Inserire i dettagli come mostrato nella schermata: Selezionare namespace : openshift-adp Nome: Change-ontap-sc (può essere qualsiasi nome) chiave: Change-ontap-sc-config.yaml: Valore:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



L'oggetto della mappa di configurazione risultante dovrebbe essere simile al seguente (CLI):

```
[root@localhost ~]# kubectl describe cm/change-ontap-sc -n openshift-adp
Name:         change-ontap-sc
Namespace:    openshift-adp
Labels:       <none>
Annotations:  <none>

Data
====
change-ontap-sc.yaml:
----
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "data-postgresql*"
    namespaces:
    - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"

BinaryData
====

Events:  <none>
[root@localhost ~]#
```

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
```

L'applicazione viene ripristinata con lo stesso namespace con le persistenti richieste di volume create utilizzando la classe di storage ontap-nas-eco.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          11m
[root@localhost ~]# oc get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS    AGE
data-postgresql-0   Bound    pvc-33526ea4-37c2-4180-a9f6-fb47aea3b4e2   8Gi        RWO            ontap-nas-eco   11m
[root@localhost ~]#
```

Eliminazione di backup e ripristini mediante Velero

In questa sezione viene descritto come eliminare i backup e i ripristini delle applicazioni nella piattaforma contenitore OpenShift utilizzando Velero.

Elenca tutti i backup

È possibile elencare tutti i CRS di backup utilizzando lo strumento CLI OC o Velero CLI. Scaricare l'interfaccia CLI di Velero come indicato nelle istruzioni riportate nella "Documentazione Velero".

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Eliminazione di un backup

È possibile eliminare una CR di backup senza eliminare i dati di archiviazione oggetti utilizzando lo strumento CLI OC. Il backup verrà rimosso dall'output CLI/Console. Tuttavia, poiché il backup corrispondente non viene rimosso dallo storage a oggetti, verrà nuovamente visualizzato nell'output CLI/console.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
schedule1-20240717070005    6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     24s
schedule1-20240717070005    6h50m
[root@localhost ~]#
```

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

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Eliminazione del ripristino

È possibile eliminare l'oggetto Restore CR utilizzando l'interfaccia CLI OC o l'interfaccia CLI Velero

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                      STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME      BACKUP                      STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore   backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Informazioni sul copyright

Informazioni sul marchio commerciale