Protección de datos de máquinas virtuales usando herramientas de terceros

NetApp Solutions

NetApp
December 19, 2024

Tabla de contenidos

Protección de datos de máquinas virtuales usando herramientas de terceros

Protección de datos para máquinas virtuales de OpenShift Virtualization mediante OpenShift API for Data Protection (OADP)

Autor: Banu Sundhar, NetApp

Esta sección del documento de referencia proporciona detalles para la creación de backups de máquinas virtuales mediante la API de OpenShift para protección de datos (OADP) con Velero en NetApp ONTAP S3 o NetApp StorageGRID S3. Los backups de los volúmenes persistentes (VP) de los discos de los equipos virtuales se crean mediante snapshots de CSI Trident.

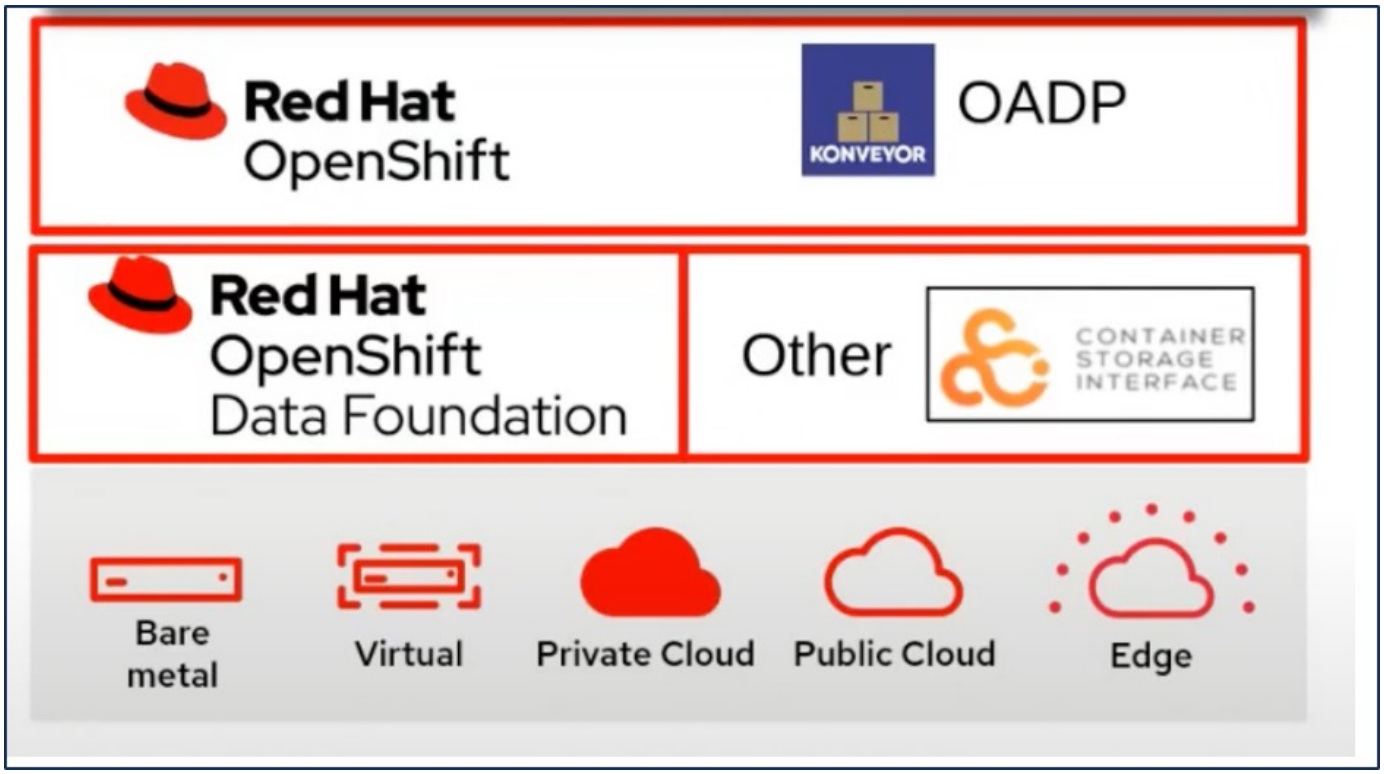
Las máquinas virtuales en el entorno de virtualización de OpenShift son aplicaciones en contenedores que se ejecutan en los nodos de trabajo de la plataforma de contenedores de OpenShift. Es importante proteger los metadatos de la máquina virtual y los discos persistentes de las máquinas virtuales, de forma que, cuando se pierden o están dañados, se puedan recuperar.

Los discos persistentes de las máquinas virtuales de virtualización de OpenShift pueden ser respaldados por el almacenamiento ONTAP integrado en el cluster de OpenShift usando "CSI de Trident". En esta sección, utilizaremos "API de OpenShift para la protección de datos (OADP)" para realizar backup de equipos virtuales, incluidos sus volúmenes de datos en

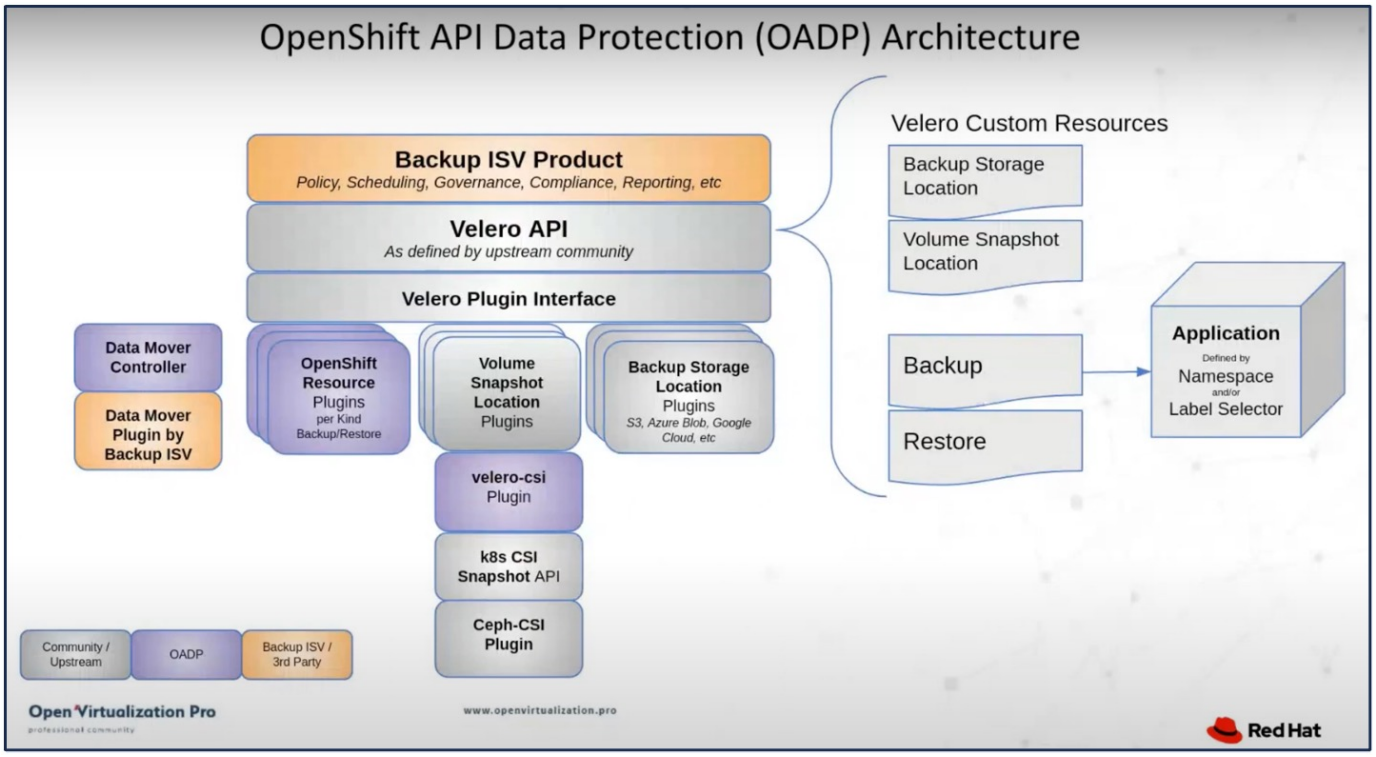
- Almacenamiento de objetos ONTAP
- StorageGRID

Después, restauramos desde el backup cuando sea necesario.

OADP permite realizar copias de seguridad, restauraciones y recuperación ante desastres de aplicaciones en un clúster OpenShift. Los datos que se pueden proteger con OADP incluyen objetos de recursos de Kubernetes, volúmenes persistentes e imágenes internas.



Red Hat OpenShift ha aprovechado las soluciones desarrolladas por las comunidades OpenSource para la protección de datos. "Velero" Es una herramienta de código abierto para realizar backups y restauraciones seguras, llevar a cabo la recuperación de desastres y migrar los recursos de clústeres de Kubernetes y volúmenes persistentes. Para usar Velero fácilmente, OpenShift ha desarrollado el operador OADP y el plugin Velero para integrarse con los controladores de almacenamiento CSI. El núcleo de las API de OADP que se exponen se basa en las API de Velero. Después de instalar el operador OADP y configurarlo, las operaciones de copia de seguridad/restauración que se pueden realizar se basan en las operaciones expuestas por la API de Velero.



OADP 1,3 está disponible desde el concentrador de operadores del cluster OpenShift 4,12 y versiones posteriores. Tiene un Data Mover integrado que puede mover instantáneas de volumen CSI a un almacén de objetos remoto. De este modo, se proporciona portabilidad y durabilidad al mover snapshots a una ubicación de almacenamiento de objetos durante el backup. A continuación, las instantáneas están disponibles para la restauración después de un desastre.

Las siguientes son las versiones de los diversos componentes utilizados para los ejemplos de esta sección

- Cluster OpenShift 4,14
- OpenShift Virtualization instalado a través de OperatorOpenShift Virtualization Operator proporcionado por Red Hat
- Operador OADP 1,13 proporcionado por Red Hat
- Velero CLI 1,13 para Linux
- Trident 24,02
- ONTAP 9,12

"CSI de Trident" "API de OpenShift para la protección de datos (OADP)" "Velero"

Instalación del operador de la API de OpenShift para la protección de datos (OADP)

En esta sección se describe la instalación del operador de la API de OpenShift para la protección de datos (OADP).

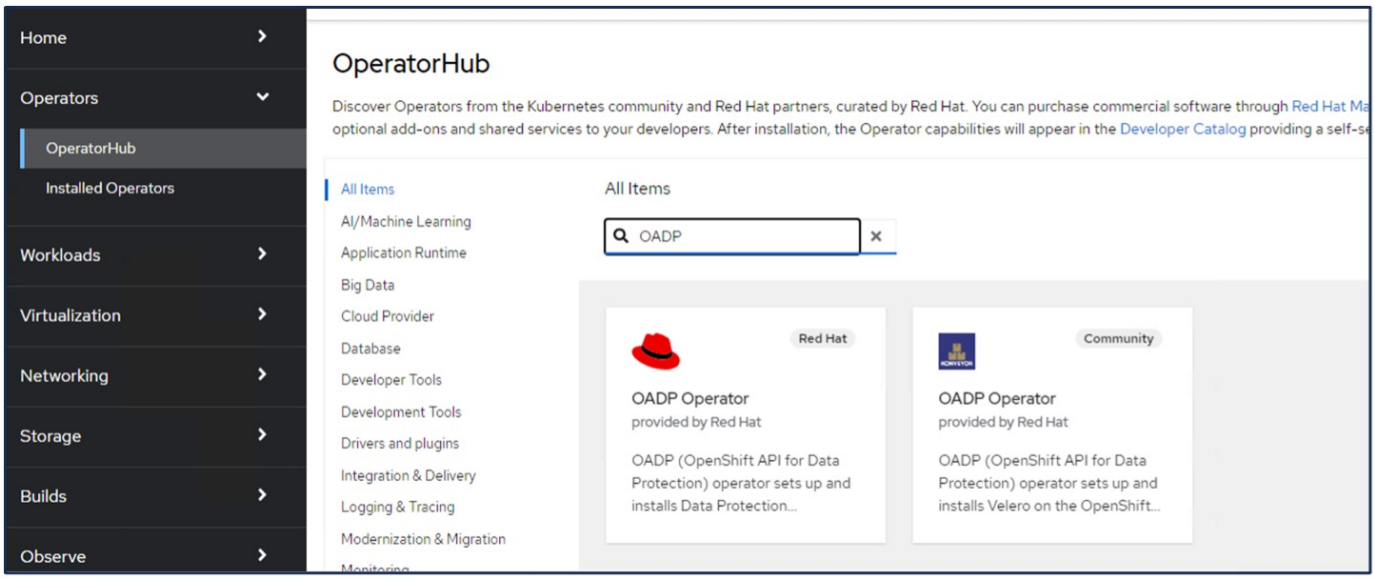
Requisitos previos

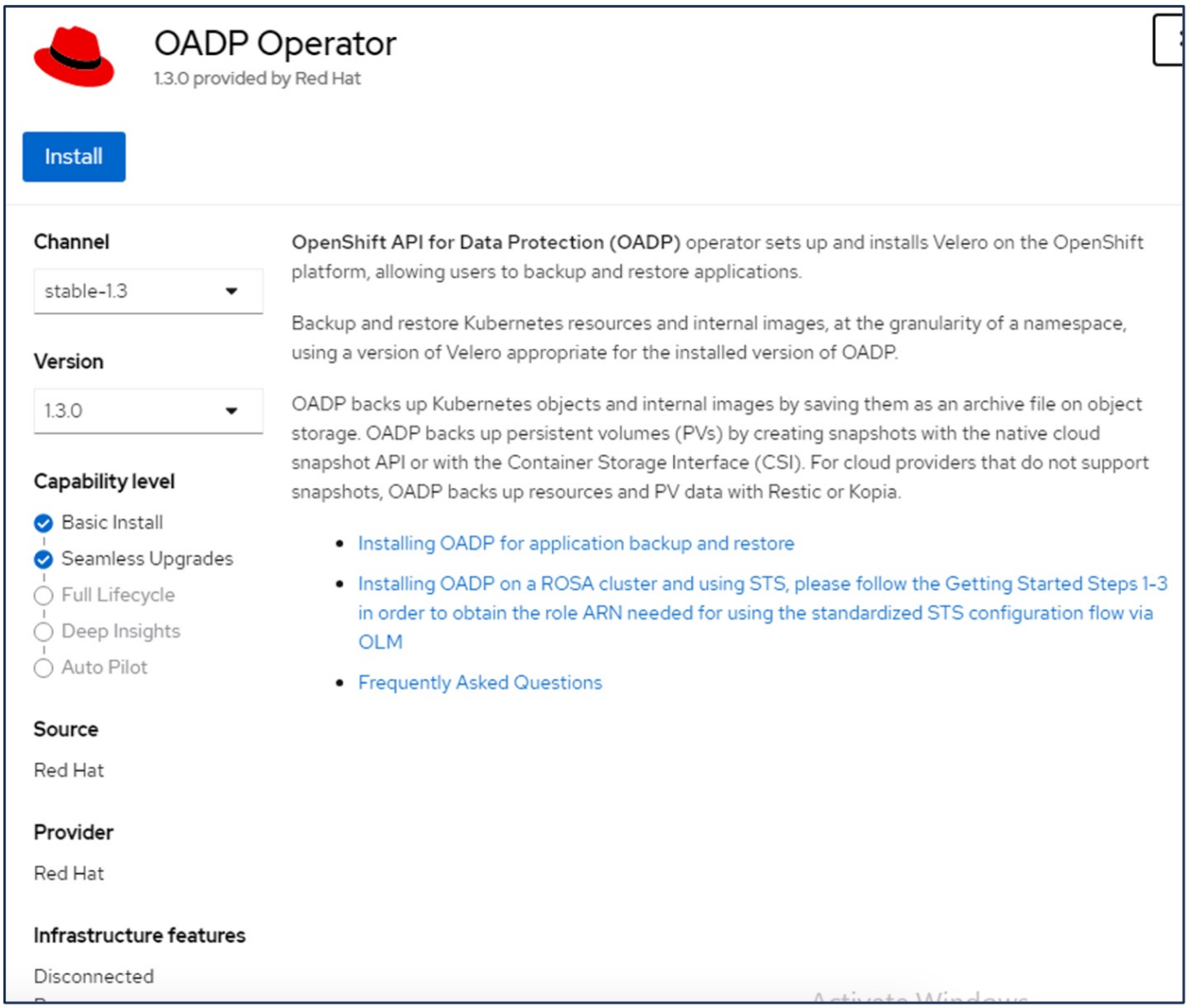
- Un clúster Red Hat OpenShift (posterior a la versión 4,12) instalado en una infraestructura básica con nodos de trabajo RHCOS
- Un clúster de NetApp ONTAP integrado con el clúster de mediante Trident
- Un back-end de Trident configurado con una SVM en un clúster de ONTAP
- Un StorageClass configurado en el clúster OpenShift con Trident como el aprovisionador
- La clase Snapshot de Trident creada en el clúster
- Acceso de administrador de clúster al clúster de Red Hat OpenShift
- Acceso de administrador al clúster de ONTAP de NetApp
- Operador de virtualización de OpenShift instalado y configurado
- Equipos virtuales implementados en un espacio de nombres en la virtualización OpenShift
- Una estación de trabajo de administración con herramientas trimentctl y oc instaladas y agregadas a $PATH

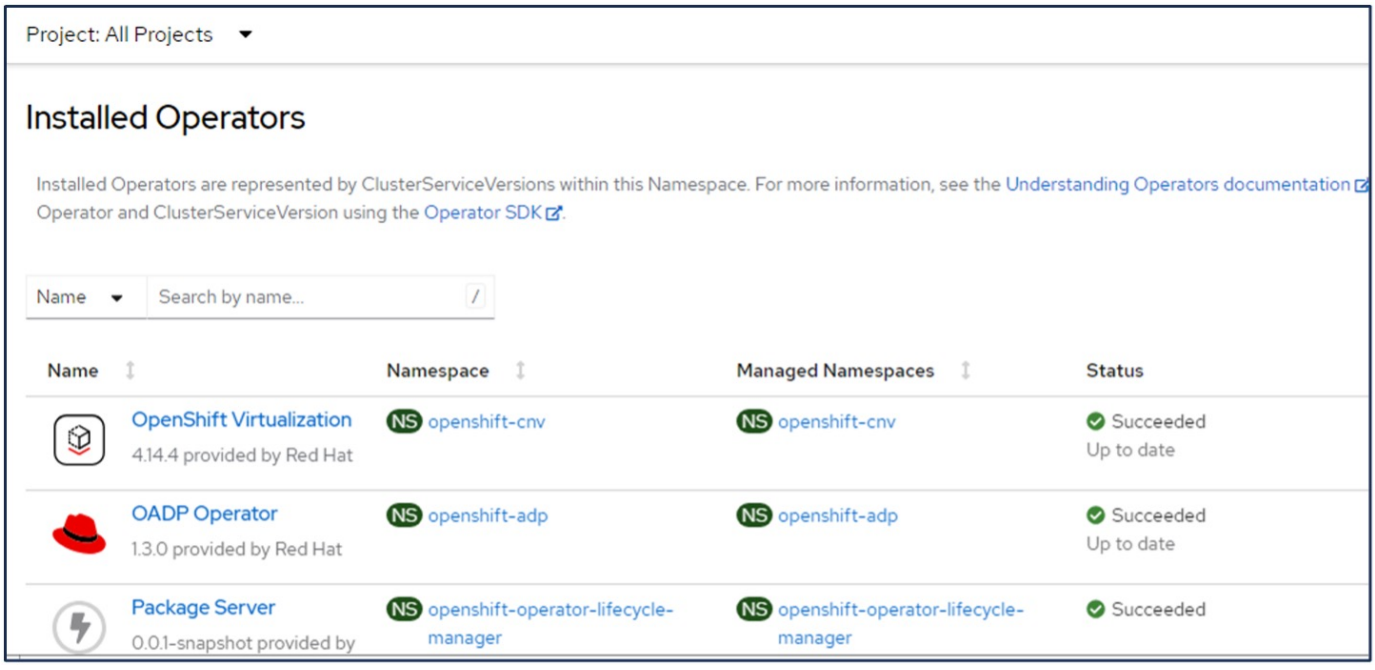
Si desea realizar una copia de seguridad de una máquina virtual cuando se encuentra en estado de ejecución, debe instalar el agente invitado QEMU en esa máquina virtual. Si instala la máquina virtual con una plantilla existente, el agente QEMU se instala automáticamente. QEMU permite al agente invitado detener los datos en tránsito en el SO invitado durante el proceso de instantánea y evitar posibles daños en los datos. Si no tiene QEMU instalado, puede detener la máquina virtual antes de realizar una copia de seguridad.

Pasos para instalar OADP Operator

1. Vaya al Centro del operador del clúster y seleccione Operador OADP de Red Hat. En la página Install, utilice todas las selecciones predeterminadas y haga clic en install. En la página siguiente, vuelva a utilizar todos los valores predeterminados y haga clic en Instalar. El operador OADP se instalará en el espacio de nombres 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

Requisitos previos para la configuración de Velero con detalles de ONTAP S3

Una vez que la instalación del operador tenga éxito, configure la instancia de Velero.
Velero se puede configurar para utilizar el almacenamiento de objetos compatible con S3. Configure ONTAP S3 utilizando los procedimientos que se muestran en la "Sección Gestión de almacenamiento de objetos de la documentación de ONTAP". Necesitará la siguiente información de su configuración de ONTAP S3 para integrarla con Velero.

- Una interfaz lógica (LIF) que puede usarse para acceder a S3
- Credenciales de usuario para acceder a S3 que incluye la clave de acceso y la clave de acceso secreta
- Un nombre de bloque en S3 para backups con permisos de acceso para el usuario
- Para obtener un acceso seguro al almacenamiento de objetos, el certificado TLS se debe instalar en el servidor de almacenamiento de objetos.

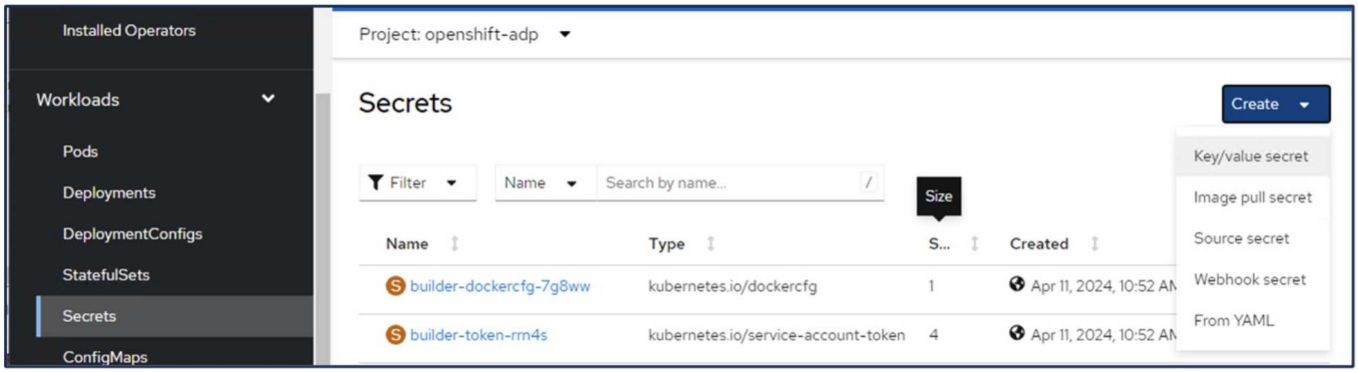
Requisitos previos para la configuración de Velero con detalles de StorageGRID S3

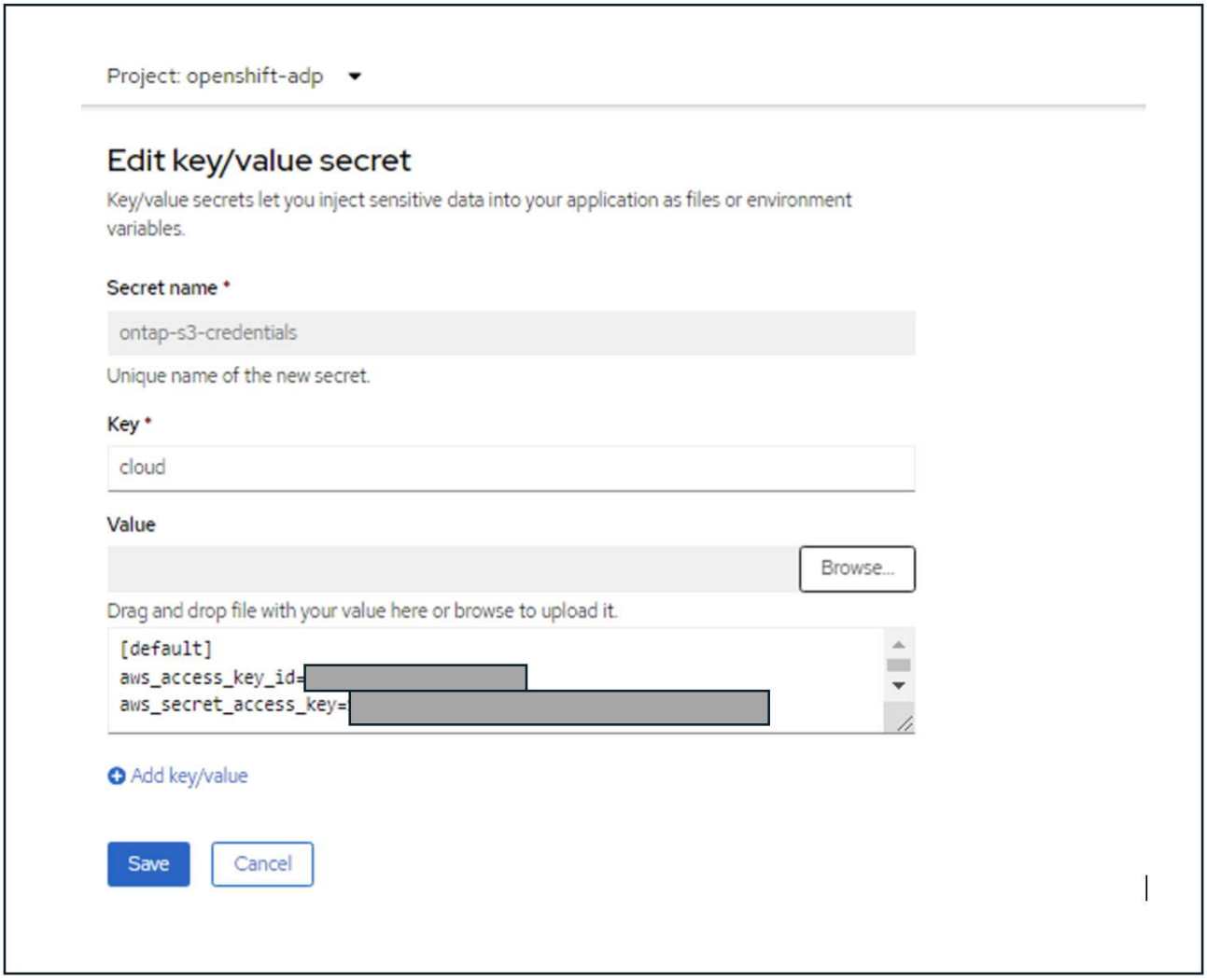
Velero se puede configurar para utilizar el almacenamiento de objetos compatible con S3. Puede configurar StorageGRID S3 con los procedimientos que se muestran en la "Documentación de StorageGRID". Necesitará la siguiente información de su configuración de StorageGRID S3 para integrarla con Velero.

- Punto final que se puede utilizar para acceder a S3
- Credenciales de usuario para acceder a S3 que incluye la clave de acceso y la clave de acceso secreta
- Un nombre de bloque en S3 para backups con permisos de acceso para el usuario
- Para obtener un acceso seguro al almacenamiento de objetos, el certificado TLS se debe instalar en el servidor de almacenamiento de objetos.

Pasos para configurar Velero

- Primero, cree un secreto para una credencial de usuario de ONTAP S3 o credenciales de usuario inquilino de StorageGRID. Se utilizará para configurar Velero más adelante. Puede crear un secreto desde la CLI o desde la consola web.
  Para crear un secreto desde la consola web, seleccione Secretos y, a continuación, haga clic en Clave/Valor Secreto. Proporcione los valores para el nombre de la credencial, la clave y el valor que se muestra. Asegúrese de utilizar el ID de clave de acceso y la clave de acceso secreta de su usuario de S3. Asigne el nombre apropiado al secreto. En el siguiente ejemplo, se crea un secreto con las credenciales de usuario de ONTAP S3 llamado ontap-S3-credentials.

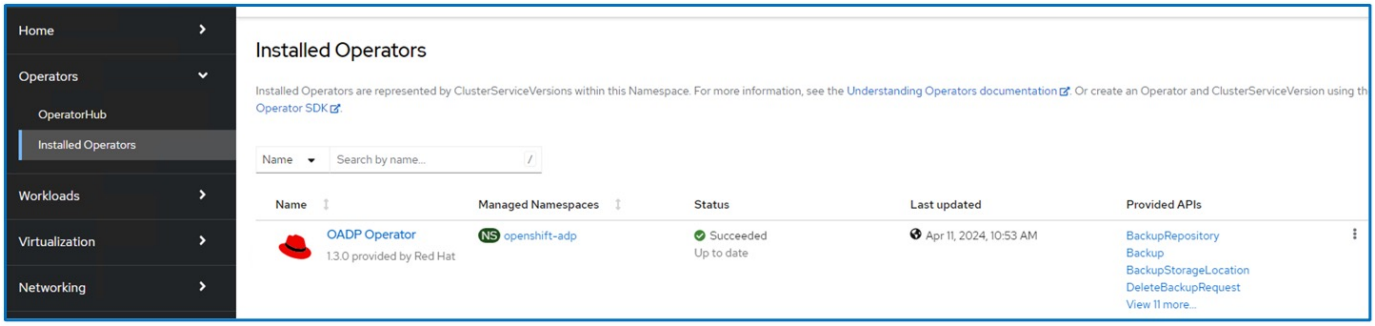




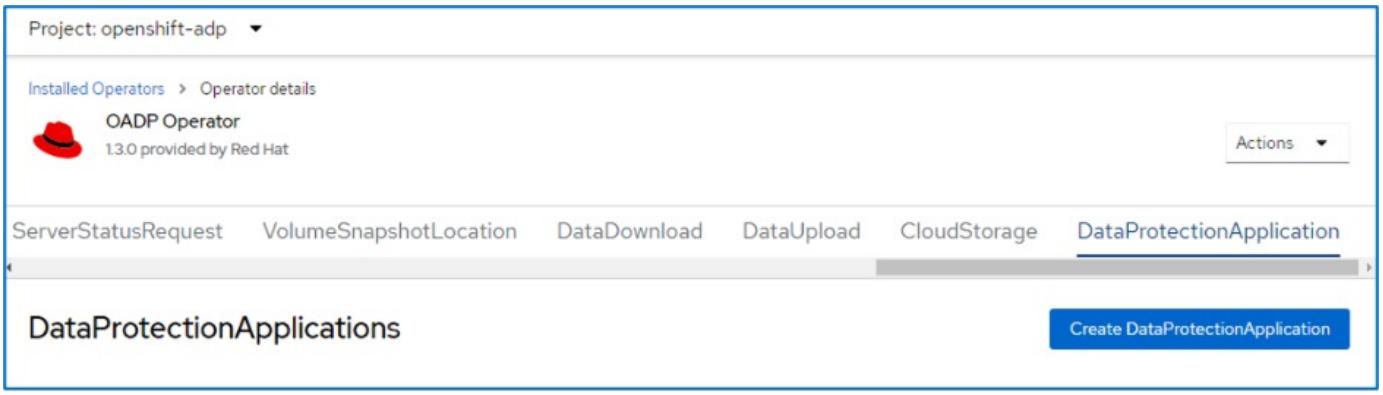
Para crear un secreto llamado sg-S3-credentials desde la CLI, puede usar el siguiente comando.

```
# 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>
```

- A continuación, para configurar Velero, seleccione Operadores instalados en el elemento de menú de Operadores, haga clic en Operador OADP y, a continuación, seleccione la pestaña DataProtectionApplication.



Haga clic en Create DataProtectionApplication. En la vista Formulario, proporcione un nombre para la aplicación DataProtection o utilice el nombre predeterminado.



Ahora vaya a la vista YAML y reemplace la información de especificaciones como se muestra en los ejemplos de archivos yaml a continuación.

Muestra de archivo yaml para configurar Velero con ONTAP S3 como el 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
```

Muestra de archivo yaml para configurar Velero con StorageGRID S3 como el backupLocation y 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 sección SPEC del archivo yaml debe configurarse adecuadamente para los siguientes parámetros similares al ejemplo anterior

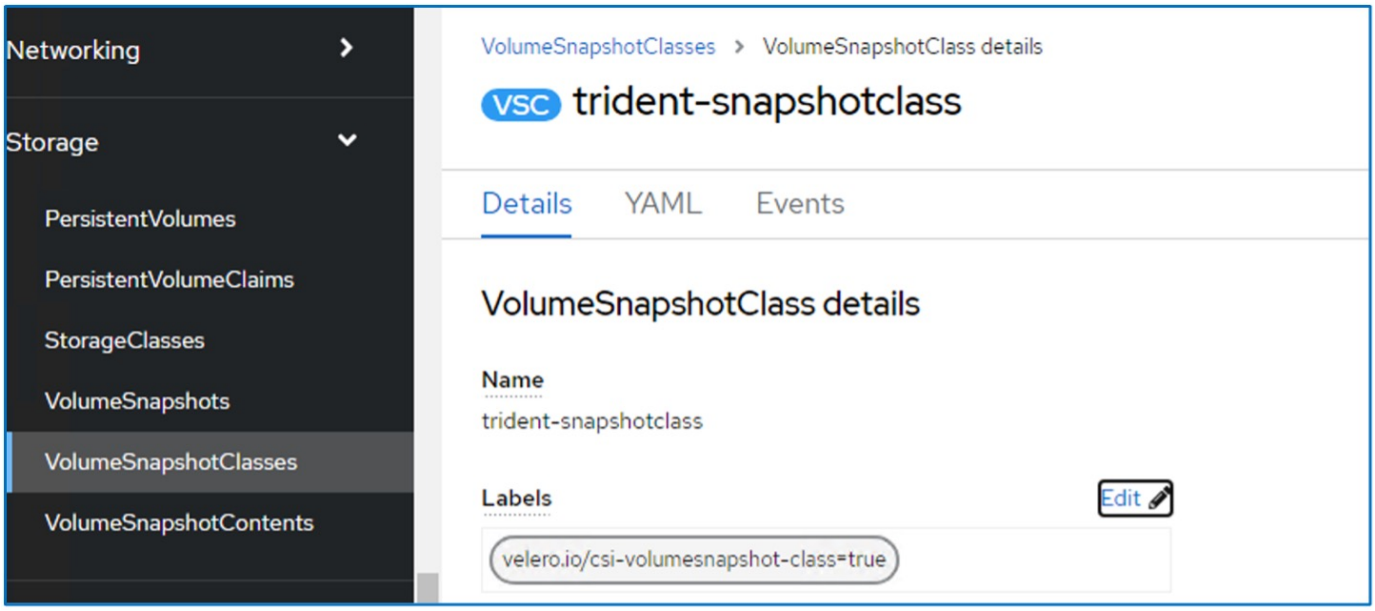
BackupLocations
ONTAP S3 o StorageGRID S3 (con sus credenciales y otra información como se muestra en el yaml) se configura como la ubicación de copia de seguridad predeterminada para velero.

SnapshotLocations Si utiliza instantáneas de Container Storage Interface (CSI), no es necesario especificar una ubicación de instantánea porque creará un VolumeSnapshotClass CR para registrar el controlador CSI. En nuestro ejemplo, utilizaría CSI de Trident y ya había creado anteriormente VolumeSnapShotClass CR mediante el controlador CSI de Trident.

Habilitar plugin CSI
Agregue csi a los defaultPlugins para Velero para realizar copias de seguridad de volúmenes persistentes con snapshots CSI.
Los plugins de Velero CSI, para respaldar los PVCs respaldados por CSI, elegirán el VolumeSnapshotClass en el clúster que tiene la etiqueta **velero.io/csi-volumesnapshot-class** establecida en él. Para esto

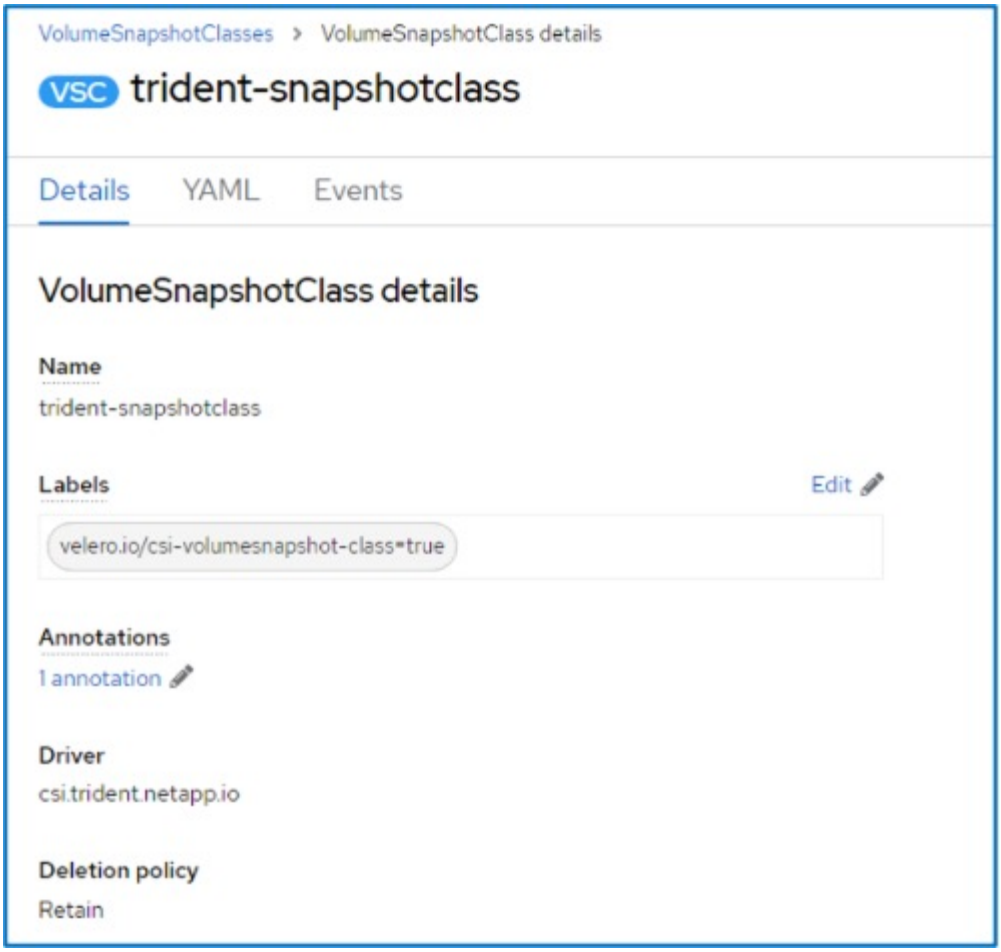
- Debe tener creado el trident VolumeSnapshotClass.

- Edite la etiqueta de la clase trident-snapshotclass y establézcala en **velero.io/csi-volumesnapshot-class=true** como se muestra a continuación.

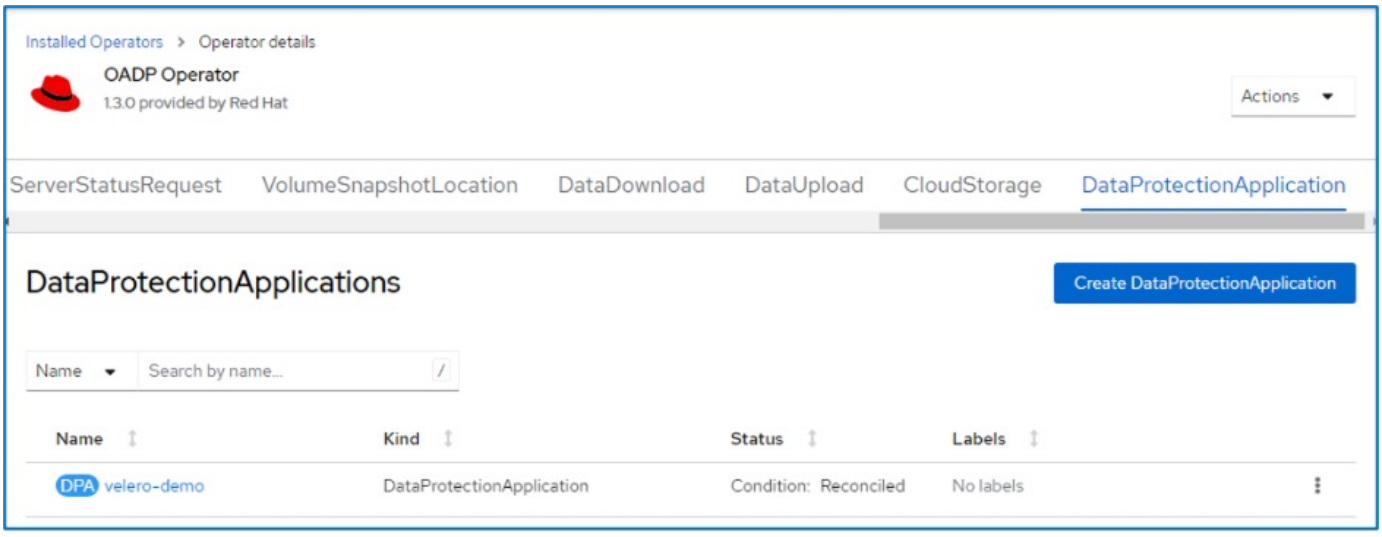


Asegúrese de que las snapshots puedan persistir incluso si se han eliminado los objetos de VolumeSnapshot. Esto se puede hacer configurando la **deletionPolicy** para retener. De lo contrario, al eliminar un espacio de nombres se perderán por completo todas las RVP de las que se haya realizado un backup.

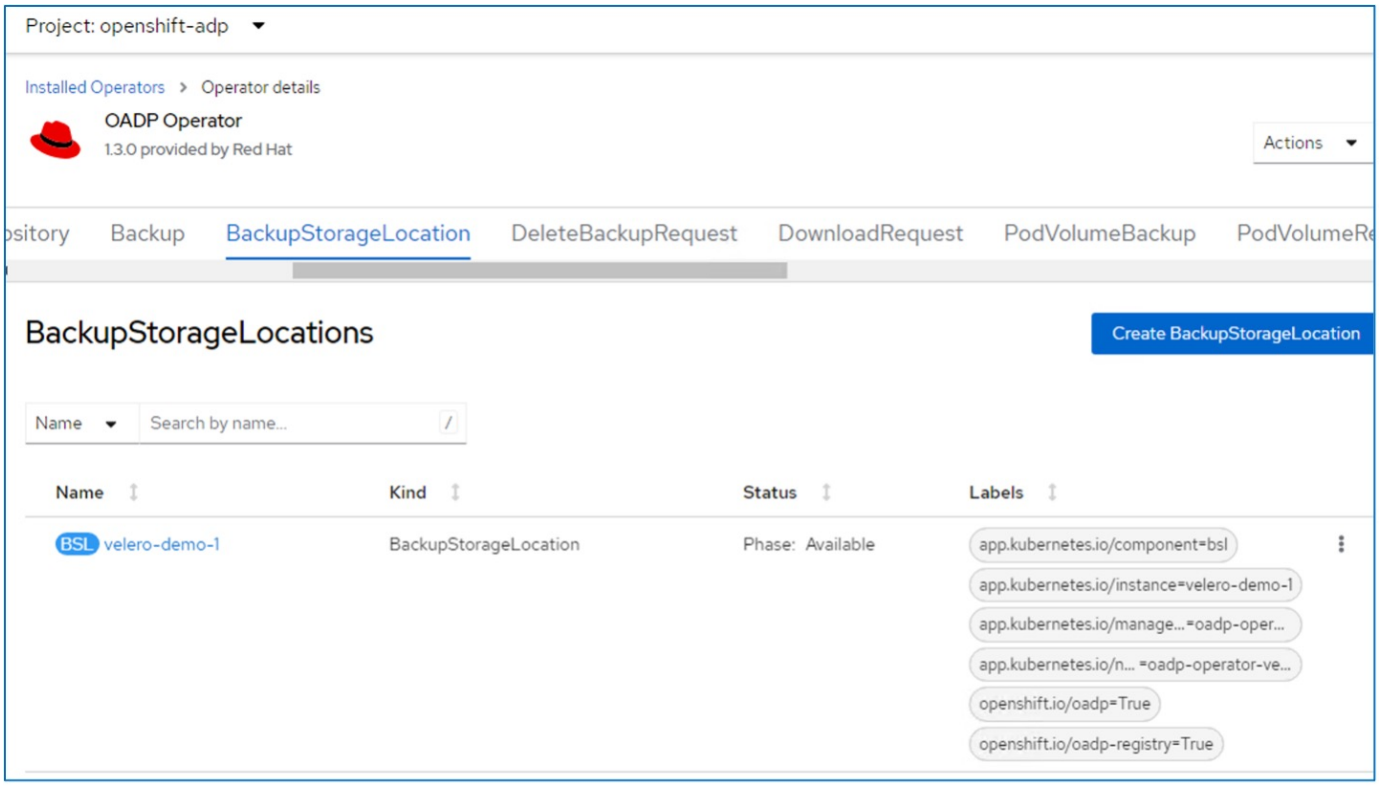
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Asegúrese de que se ha creado la aplicación DataProtectionApplication y que se encuentra en Condición:Reconciliada.



El operador OADP creará una BackupStorageLocation correspondiente. Se utilizará al crear una copia de seguridad.



Crear backups bajo demanda para equipos virtuales en OpenShift Virtualization

Esta sección describe cómo crear copias de seguridad bajo demanda para máquinas virtuales en OpenShift Virtualization.

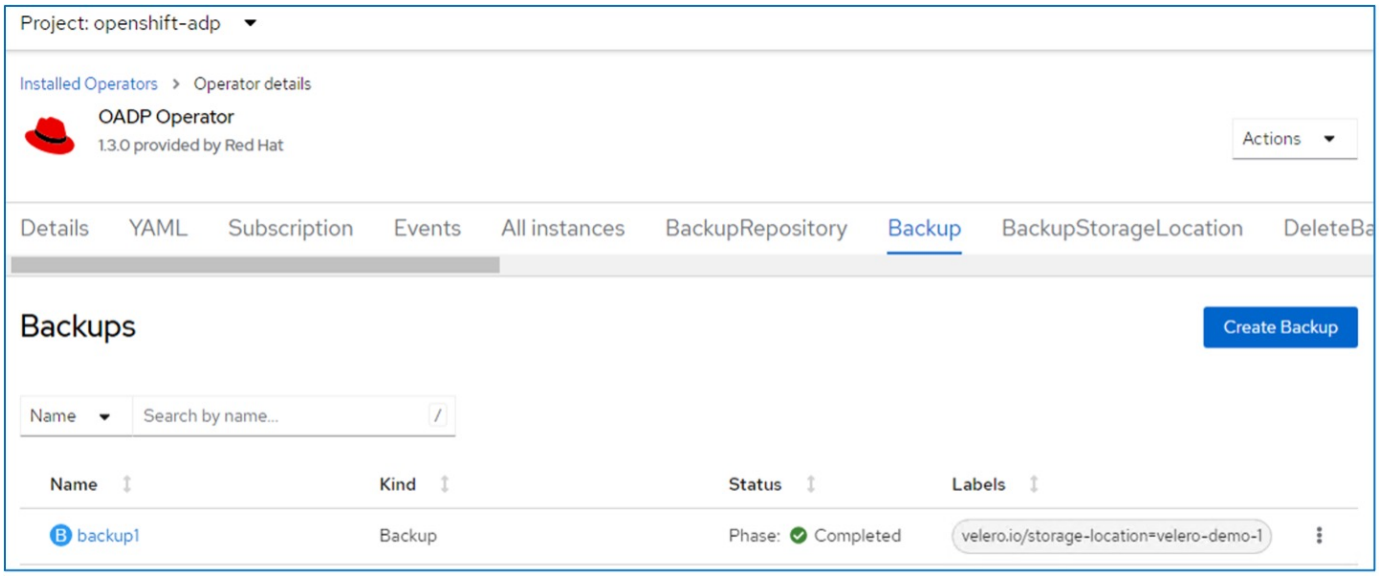
Pasos para crear un backup de una máquina virtual

Para crear una copia de seguridad bajo demanda de toda la VM (metadatos de VM y discos de VM), haga clic en la pestaña **Backup**. Esto crea un recurso personalizado de copia de seguridad (CR). Se proporciona un yaml de ejemplo para crear el CR de copia de seguridad. Mediante este yaml se realizará una copia de seguridad de la máquina virtual y sus discos en el espacio de nombre especificado. Los parámetros adicionales se pueden establecer como se muestra en la "documentación".

El CSI creará una instantánea de los volúmenes persistentes que respalden los discos. Se crea un backup del equipo virtual junto con la snapshot de sus discos, y se almacena en la ubicación de backup especificada en yaml. La copia de seguridad permanecerá en el sistema durante 30 días, tal y como se especifica en el ttl.

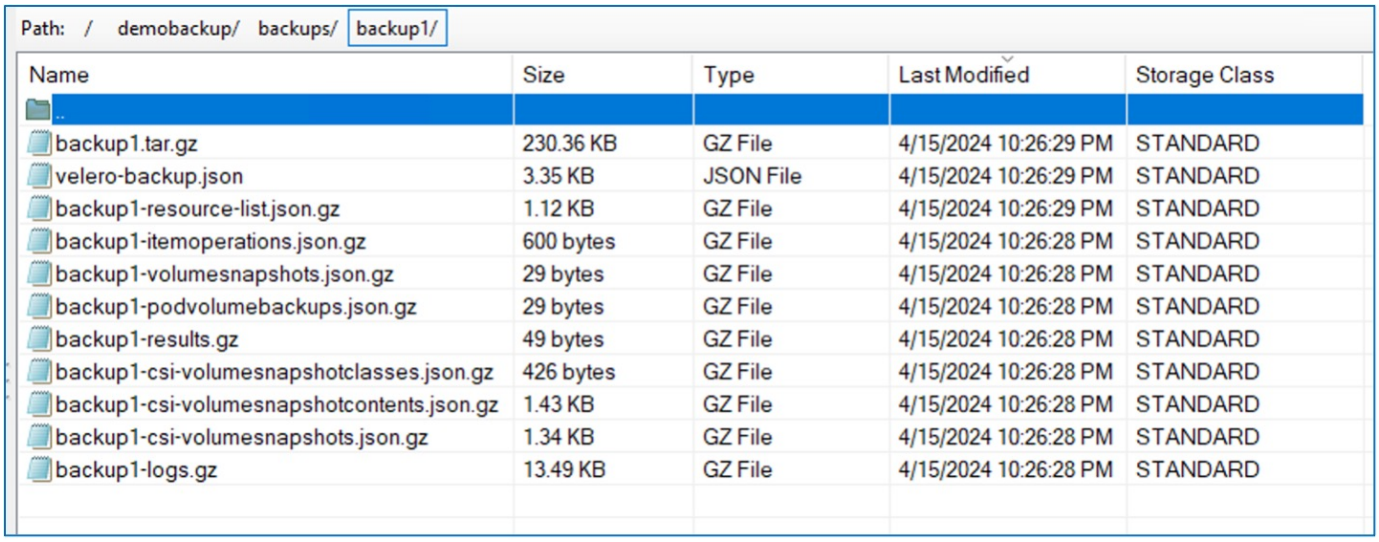
```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
previously created
                                    when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

Una vez que se complete la copia de seguridad, su Fase se mostrará como completada.



Puede inspeccionar la copia de seguridad en el almacenamiento de objetos con la ayuda de una aplicación de explorador S3. La ruta de acceso del backup aparece en el bucket configurado con el prefijo name (velero/demobackup). Es posible ver el contenido del backup incluidos las copias de Snapshot de volúmenes, los registros y otros metadatos de la máquina virtual.

En StorageGRID, también puede utilizar la consola S3 que está disponible desde el Administrador de inquilinos para ver los objetos de backup.



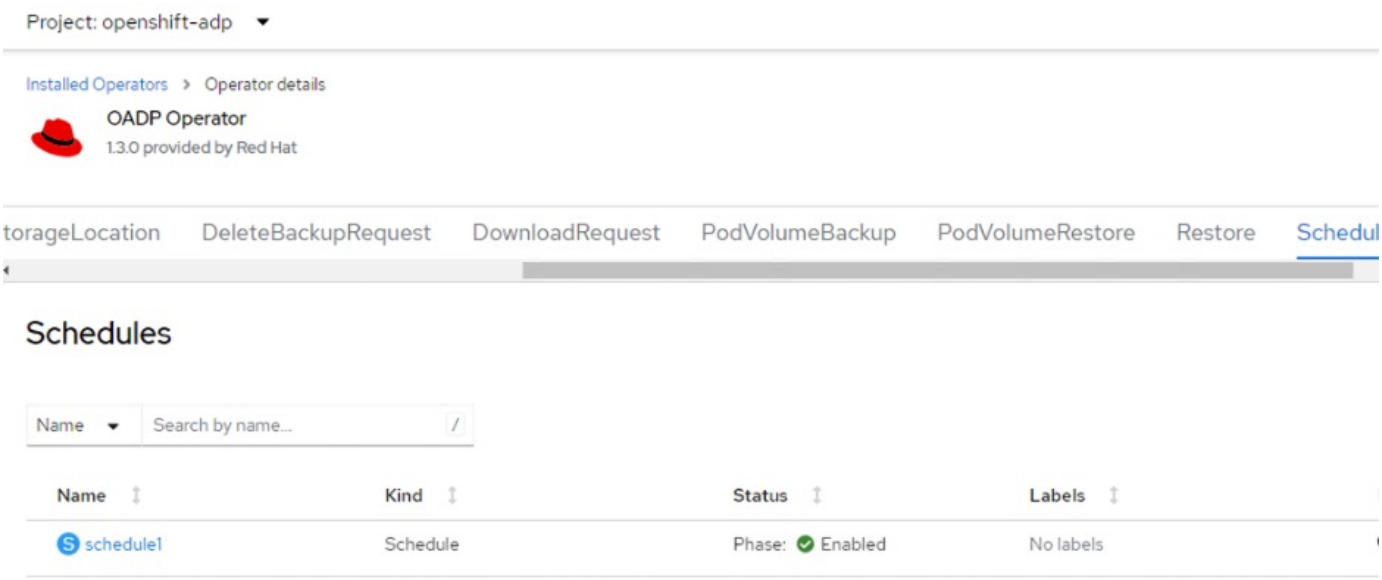
Creación de backups programados para máquinas virtuales en OpenShift Virtualization

Para crear copias de seguridad en un programa, debe crear un CR de programa.
La programación es simplemente una expresión Cron que le permite especificar la hora a la que desea crear la copia de seguridad. yaml de ejemplo para crear un CR de programa.

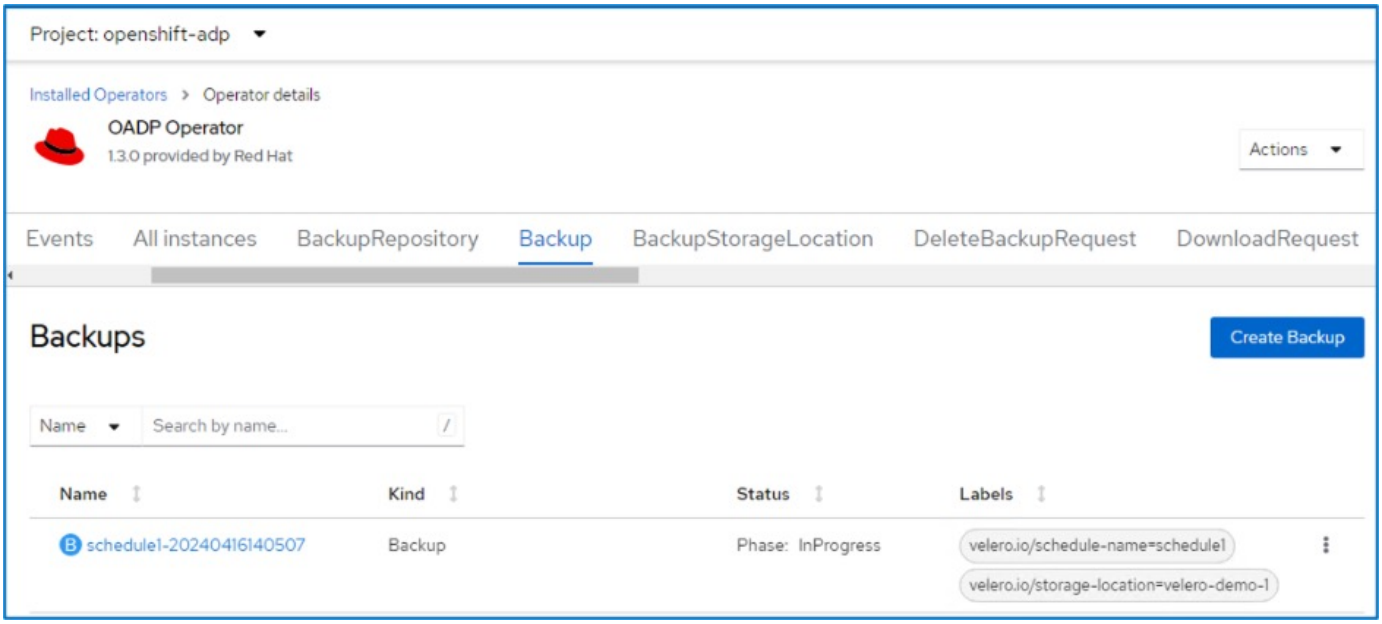
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

La expresión Cron 0 7 * * * significa que se creará una copia de seguridad a las 7:00 todos los días.
También se especifican los espacios de nombres que se incluirán en la copia de seguridad y la ubicación de almacenamiento para la copia de seguridad. Por lo tanto, en lugar de un CR de copia de seguridad, el CR de programa se utiliza para crear una copia de seguridad a la hora y frecuencia especificadas.

Una vez creada la programación, se habilita.



Las copias de seguridad se crearán de acuerdo con esta programación y se podrán ver desde la pestaña Copia de seguridad.



Restaurar un equipo virtual desde un backup

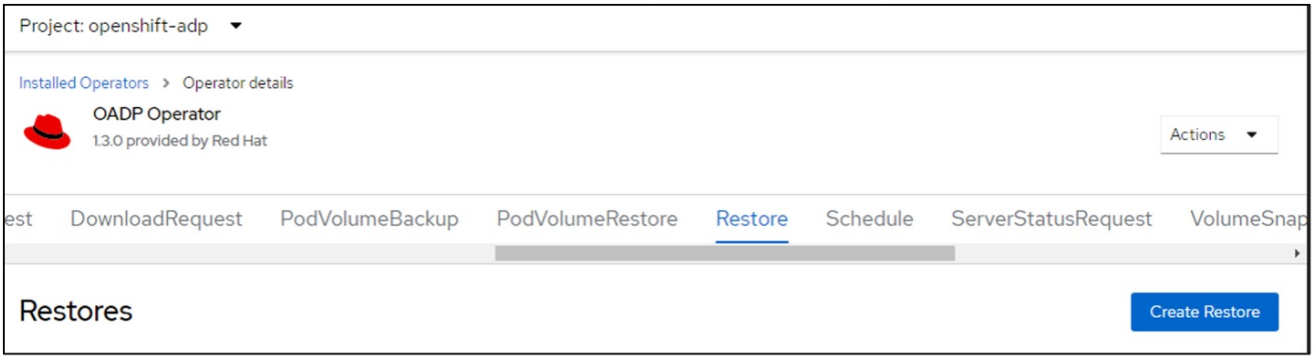
En esta sección se describe cómo restaurar máquinas virtuales desde un backup.

Requisitos previos

Para restaurar desde un backup, asumimos que el espacio de nombres donde existía la máquina virtual se eliminó por accidente.

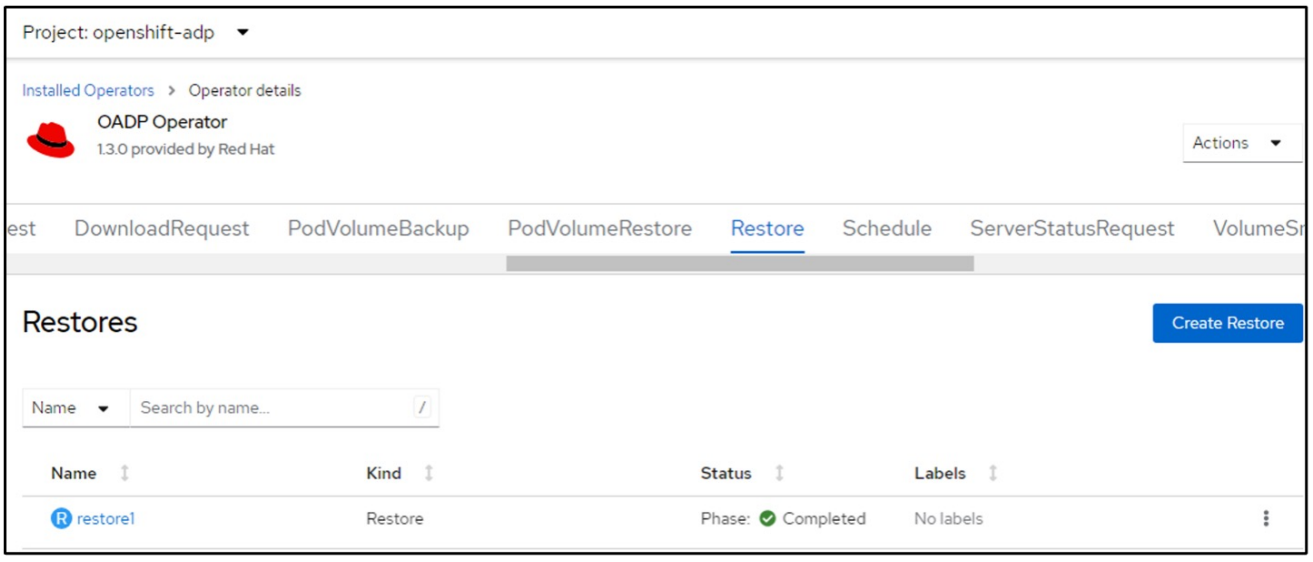
Restaure el mismo espacio de nombres

Para restaurar desde el backup que acabamos de crear, necesitamos crear un Restore Custom Resource (CR). Necesitamos darle un nombre, proporcionar el nombre del backup del que queremos restaurar y establecer restorePVs en true. Los parámetros adicionales se pueden establecer como se muestra en la "documentación". Haga clic en el botón Crear.




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

Cuando la fase muestra Completado, puede ver que las máquinas virtuales se han restaurado al estado en que se tomó la instantánea. (Si el backup se creó cuando la máquina virtual se estaba ejecutando, al restaurar la máquina virtual desde el backup se iniciará la máquina virtual restaurada y se llevará a un estado en ejecución). La máquina virtual se restaura en el mismo espacio de nombres.



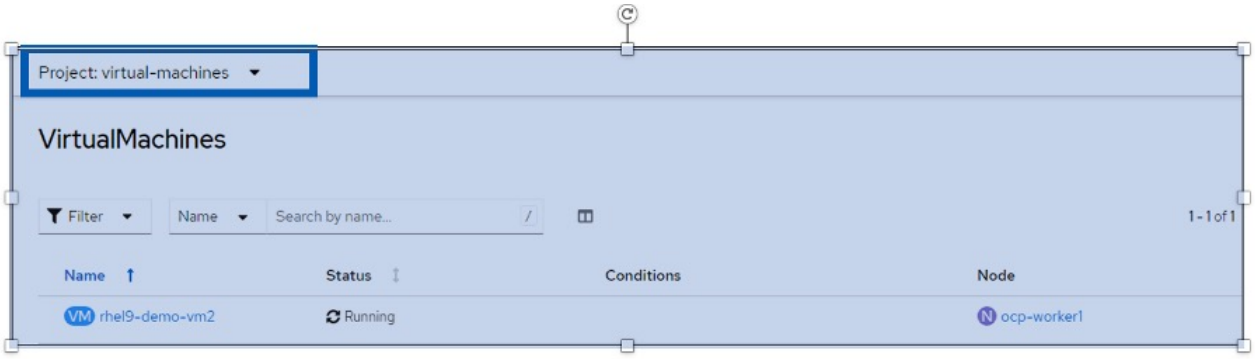
Restaure un espacio de nombres diferente

Para restaurar el equipo virtual en un espacio de nombres diferente, puede proporcionar un namespaceMapping en la definición yaml del Restore CR.

El siguiente ejemplo de archivo yaml crea un Restore CR para restaurar un equipo virtual y sus discos en el espacio de nombres virtual-machines-demo cuando el backup se realizó en el espacio de nombres de equipos virtuales.

```
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
```

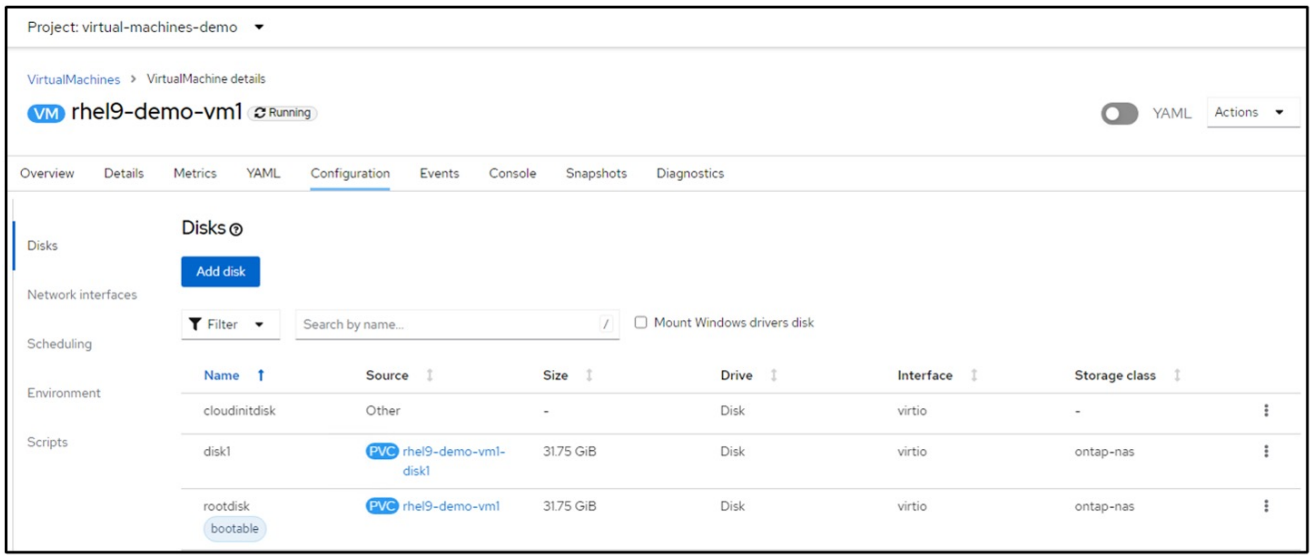
Cuando la fase muestra Completado, puede ver que las máquinas virtuales se han restaurado al estado en que se tomó la instantánea. (Si el backup se creó cuando la máquina virtual se estaba ejecutando, al restaurar la máquina virtual desde el backup se iniciará la máquina virtual restaurada y se llevará a un estado en ejecución). La máquina virtual se restaura en un espacio de nombres diferente como se especifica en la yaml.

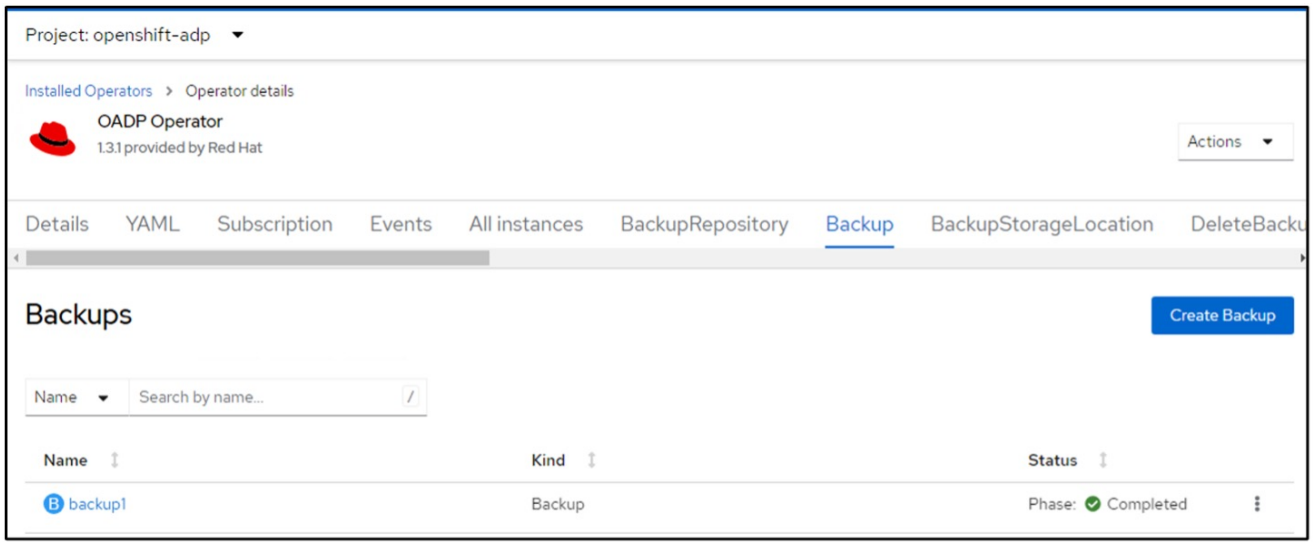


Restaure a otra clase de almacenamiento

Velero proporciona una capacidad genérica para modificar los recursos durante la restauración mediante la especificación de parches json. Los parches json se aplican a los recursos antes de restaurarlos. Los parches json se especifican en un configmap y se hace referencia al configmap en el comando restore. Esta función le permite restaurar utilizando una clase de almacenamiento diferente.

En el siguiente ejemplo, la máquina virtual, durante su creación utiliza ontap-nas como clase de almacenamiento de sus discos. Se crea un backup de la máquina virtual llamada backup1.





Simule una pérdida de la máquina virtual eliminando la máquina virtual.

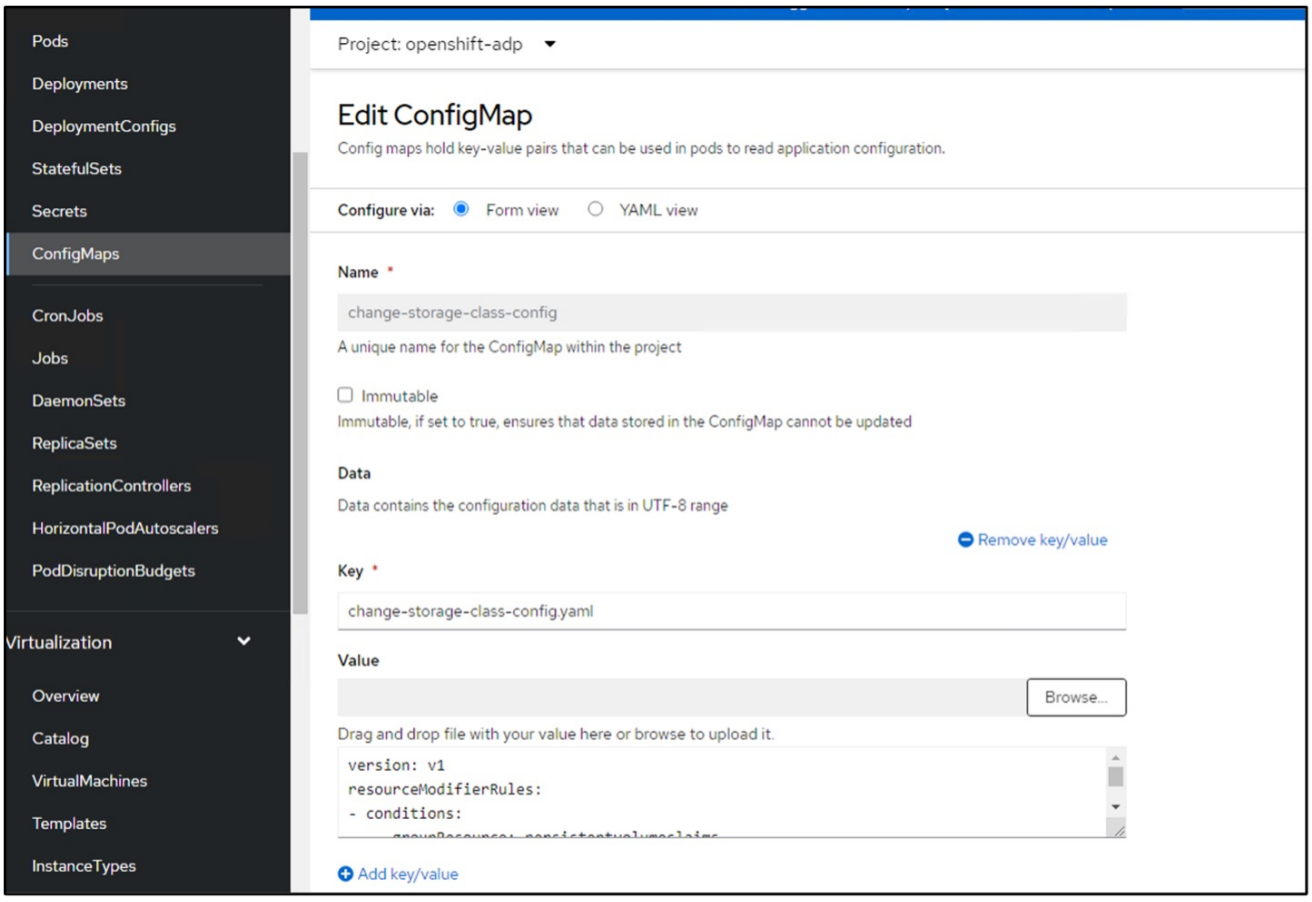
Para restaurar la máquina virtual con un tipo de almacenamiento diferente (por ejemplo, ontap-nas-eco storage class, tiene que seguir estos dos pasos:

Paso 1

Cree un mapa de configuración (consola) en el espacio de nombres openshift-adp de la siguiente manera:
Rellene los detalles como se muestra en la captura de pantalla:

Seleccionar espacio de nombres : openshift-adp
Nombre: Change-storage-class-config (puede ser cualquier nombre)
Clave: Change-storage-class-config.yaml:
Valor:

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



El objeto de mapa de configuración resultante debe tener el siguiente aspecto (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>
```

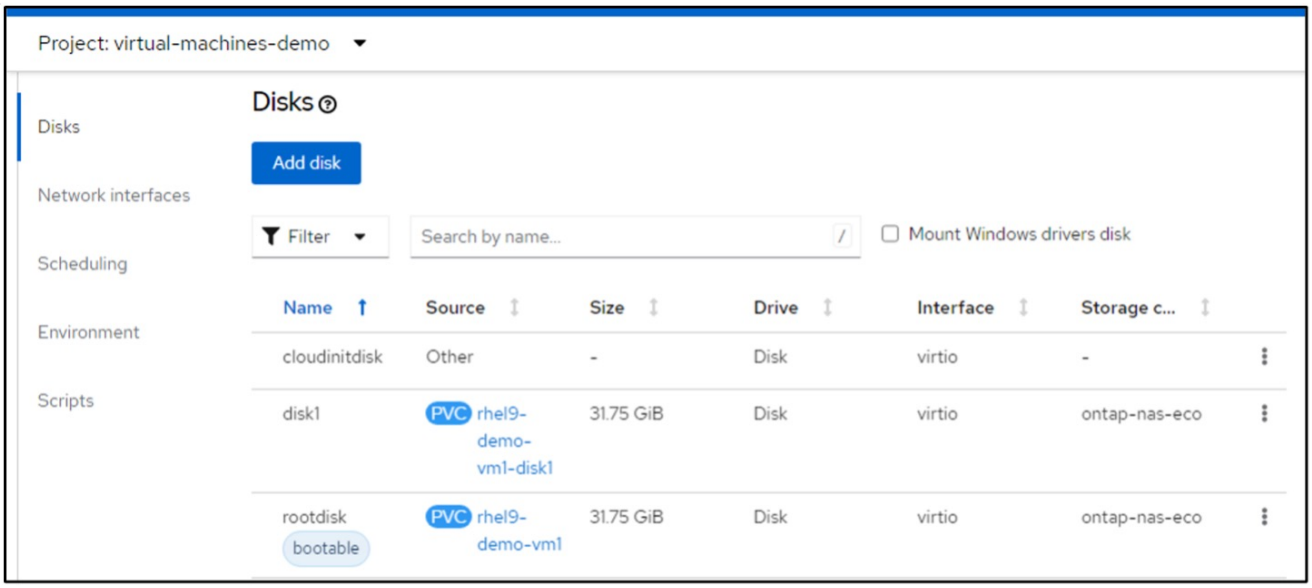
Esta asignación de configuración aplicará la regla de modificador de recursos cuando se cree la restauración. Se aplicará una revisión para sustituir el nombre de clase de almacenamiento a ontap-nas-eco para todas las solicitudes de volumen persistentes que comiencen por rhel.

Paso 2

Para restaurar la máquina virtual, utilice el siguiente comando desde la CLI de Velero:

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

La máquina virtual se restaura en el mismo espacio de nombres con los discos creados utilizando ontap-nas-eco para la clase de almacenamiento.



Eliminación de copias de seguridad y restauraciones en el uso de Velero

Esta sección describe cómo eliminar copias de seguridad y restauraciones de máquinas virtuales en OpenShift Virtualization Using Velero.

Eliminar un backup

Puede eliminar una copia de seguridad de CR sin eliminar los datos de almacenamiento de objetos mediante la herramienta CLI de OC.

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

Si desea eliminar la copia de seguridad de CR y eliminar los datos de almacenamiento de objetos asociados, puede hacerlo mediante la herramienta CLI de Velero.

Descargue la CLI como se indica en las instrucciones de "Documentación de velero".

Ejecute el siguiente comando delete mediante la CLI de Velero

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

Eliminación de una restauración

Puede eliminar Restore CR mediante la CLI de Velero

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

Puede utilizar el comando oc, así como la interfaz de usuario para suprimir el CR de restauración

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

Información de copyright

Información de la marca comercial