Proteger los datos utilizando herramientas de terceros

NetApp virtualization solutions

NetApp
August 18, 2025

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

Tabla de contenidos

Proteger los datos utilizando herramientas de terceros . . . 1
- Obtenga información sobre la protección de datos para máquinas virtuales en Red Hat OpenShift Virtualization mediante OpenShift API for Data Protection (OADP) . . . 1
- Instalar el operador de Red Hat OpenShift API for Data Protection (OADP) . . . 3
  - Prerrequisitos . . . 3
  - Pasos para instalar el operador OADP . . . 4
- Cree copias de seguridad a pedido para máquinas virtuales en Red Hat OpenShift Virtualization con Velero . . . 13
  - Pasos para crear una copia de seguridad de una máquina virtual . . . 13
  - Creación de copias de seguridad programadas para máquinas virtuales en OpenShift Virtualization . . . 15
- Restaurar una máquina virtual a partir de una copia de seguridad en Red Hat OpenShift Virtualization con Velero . . . 16
  - Prerrequisitos . . . 17
- Eliminar una CR de respaldo o restaurar una CR en Red Hat OpenShift Virtualization usando Velero . . . 23
  - Eliminar una copia de seguridad . . . 23
  - Eliminar una restauración . . . 23

Proteger los datos utilizando herramientas de terceros

Obtenga información sobre la protección de datos para máquinas virtuales en Red Hat OpenShift Virtualization mediante OpenShift API for Data Protection (OADP)

OpenShift API for Data Protection (OADP) con Velero proporciona capacidades de respaldo, restauración y recuperación ante desastres para máquinas virtuales en OpenShift Virtualization. Utilice instantáneas Trident CSI para realizar copias de seguridad de volúmenes persistentes y metadatos de máquinas virtuales en NetApp ONTAP S3 o StorageGRID S3. OADP se integra con las API de Velero y los controladores de almacenamiento CSI para administrar las operaciones de protección de datos para máquinas virtuales en contenedores.

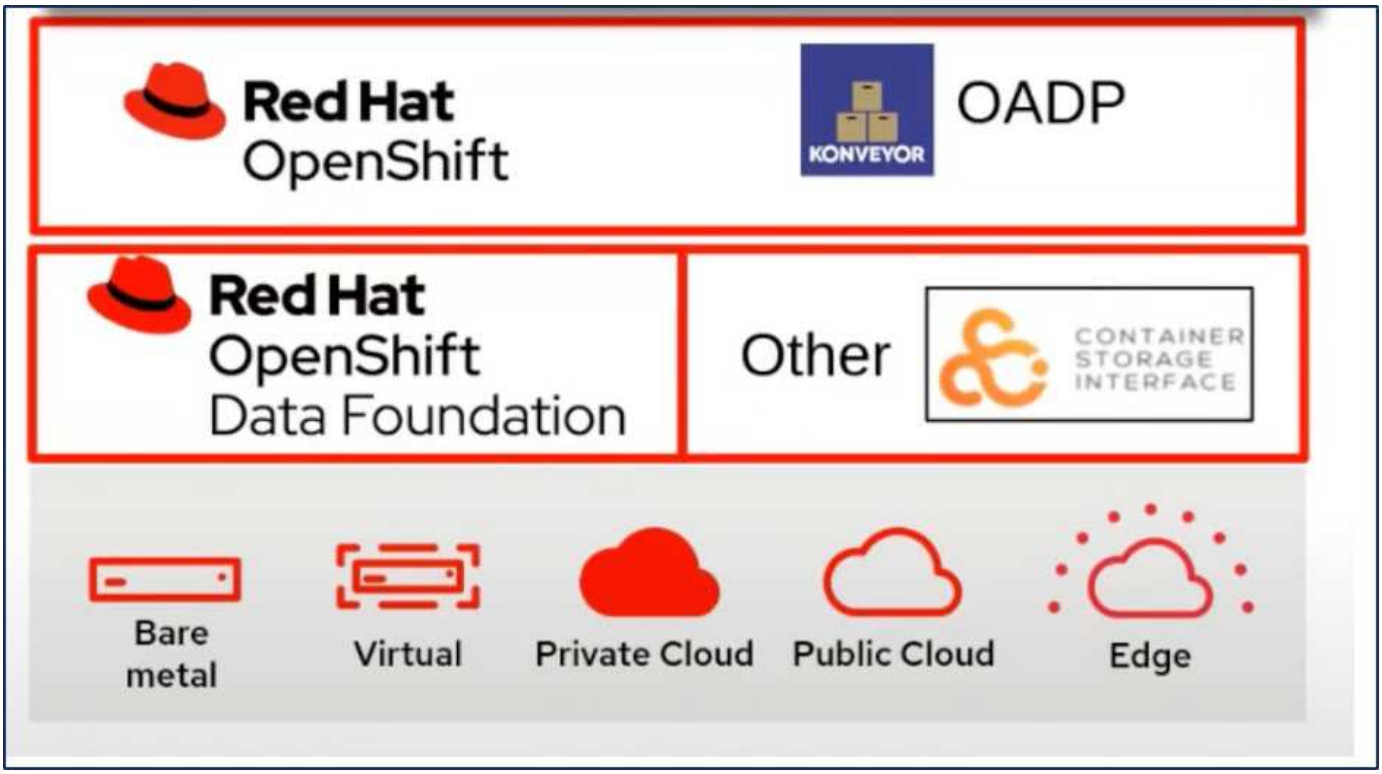
Las máquinas virtuales en el entorno de virtualización OpenShift son aplicaciones en contenedores que se ejecutan en los nodos de trabajo de su plataforma OpenShift Container. Es importante proteger los metadatos de las máquinas virtuales, así como los discos persistentes de las máquinas virtuales, para que cuando se pierdan o se dañen, se puedan recuperar.

Los discos persistentes de las máquinas virtuales de OpenShift Virtualization pueden respaldarse con almacenamiento ONTAP integrado al clúster OpenShift mediante"Trident CSI" . En esta sección utilizamos"API de OpenShift para la protección de datos (OADP)" para realizar copias de seguridad de las máquinas virtuales, incluidos sus volúmenes de datos.

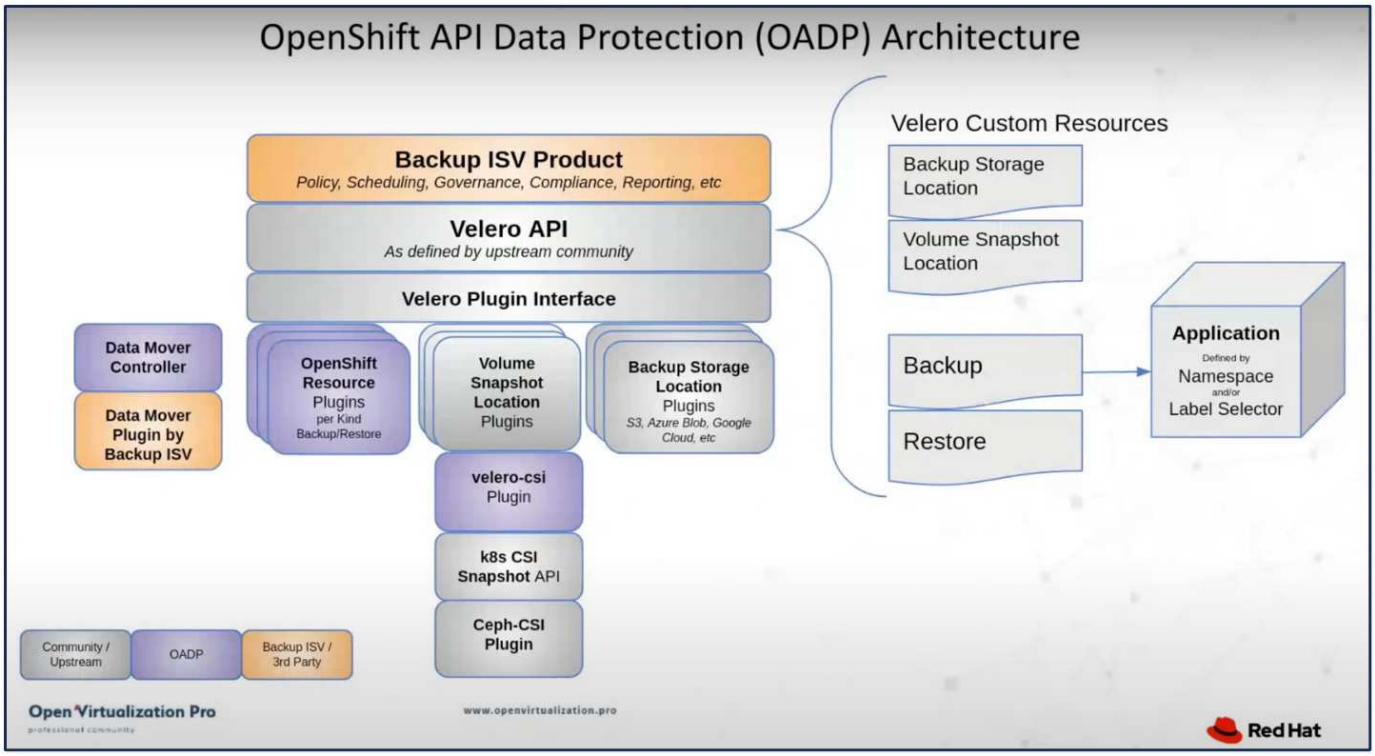
- Almacenamiento de objetos ONTAP
- StorageGrid

Luego restauramos desde la copia de seguridad cuando sea necesario.

OADP permite la copia de seguridad, la restauración y la 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 copias de seguridad y restaurar de forma segura, realizar recuperación ante desastres y migrar recursos de clústeres de Kubernetes y volúmenes persistentes. Para utilizar Velero fácilmente, OpenShift ha desarrollado el operador OADP y el complemento Velero para integrarlo con los controladores de almacenamiento CSI. El núcleo de las API de OADP que se exponen se basan en las API de Velero. Después de instalar el operador OADP y configurarlo, las operaciones de copia de seguridad y restauración que se pueden realizar se basan en las operaciones expuestas por la API de Velero.



OADP 1.3 está disponible en el centro de operadores del clúster OpenShift 4.12 y posteriores. Tiene un Data Mover incorporado que puede mover instantáneas de volumen CSI a un almacén de objetos remoto. Esto proporciona portabilidad y durabilidad al mover instantáneas a una ubicación de almacenamiento de objetos durante la copia de seguridad. Las instantáneas estarán luego disponibles para su restauración después de un desastre.

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

- Clúster OpenShift 4.14
- OpenShift Virtualization instalado a través del operadorOperador de virtualización OpenShift proporcionado por Red Hat
- Operador OADP 1.13 proporcionado por Red Hat
- Velero CLI 1.13 para Linux
- Trident 24.02
- ONTAP 9.12

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

Instalar el operador de Red Hat OpenShift API for Data Protection (OADP)

Instale el operador de API de OpenShift para protección de datos (OADP) para habilitar capacidades de respaldo y restauración para máquinas virtuales en OpenShift Virtualization. Este procedimiento incluye la implementación del operador OADP desde OpenShift Operator Hub, la configuración de Velero para usar NetApp ONTAP S3 o StorageGRID como destino de respaldo y la configuración de los secretos y las ubicaciones de respaldo necesarios.

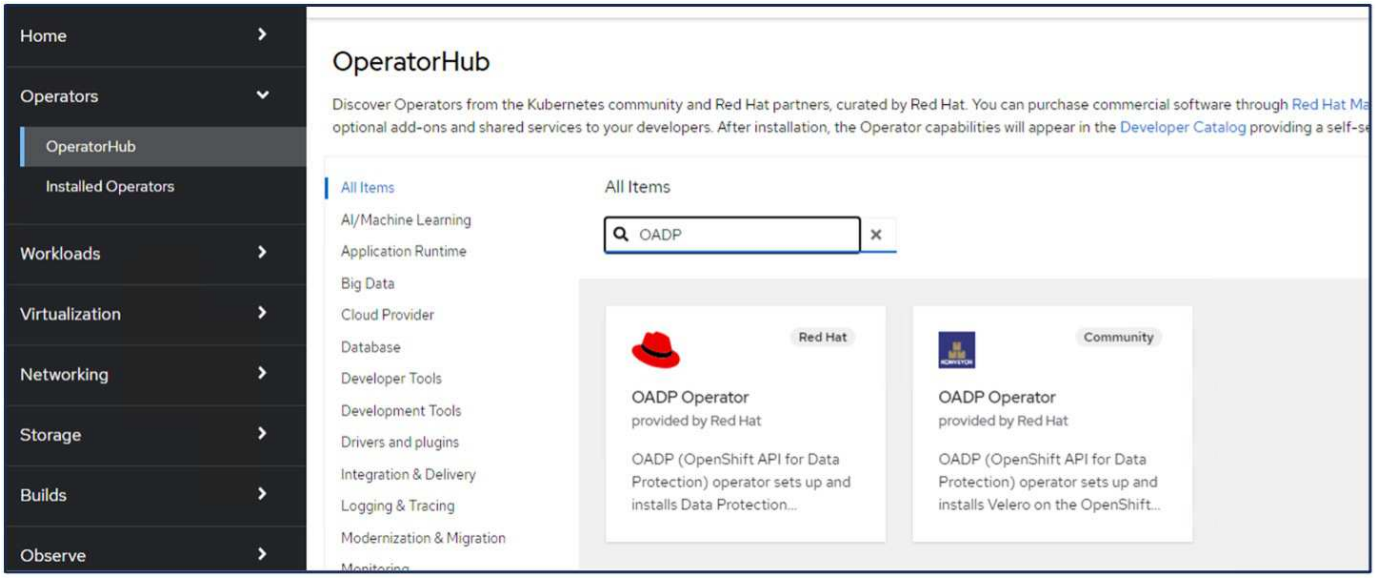
Prerrequisitos

- Un clúster Red Hat OpenShift (posterior a la versión 4.12) instalado en una infraestructura física con nodos de trabajo RHCOS
- Un clúster NetApp ONTAP integrado con el clúster mediante Trident
- Un backend Trident configurado con un SVM en un clúster ONTAP
- Una StorageClass configurada en el clúster OpenShift con Trident como aprovisionador
- Clase Trident Snapshot creada en el clúster
- Acceso de administrador de clúster al clúster Red Hat OpenShift
- Acceso de administrador al clúster NetApp ONTAP
- Operador de virtualización OpenShift instalado y configurado
- Máquinas virtuales implementadas en un espacio de nombres en OpenShift Virtualization
- Una estación de trabajo de administrador con herramientas tridentctl y oc instaladas y agregadas a $PATH

Si desea realizar una copia de seguridad de una máquina virtual cuando está en estado de ejecución, deberá instalar el agente invitado QEMU en esa máquina virtual. Si instala la máquina virtual utilizando una plantilla existente, el agente QEMU se instalará automáticamente. QEMU permite que el agente invitado suspenda los datos en tránsito en el sistema operativo invitado durante el proceso de instantánea y evite 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 el operador OADP

1. Vaya al Centro de operadores del clúster y seleccione el operador Red Hat OADP. En la página Instalar, utilice todas las selecciones predeterminadas y haga clic en instalar. En la página siguiente, utilice nuevamente 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	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

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

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

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

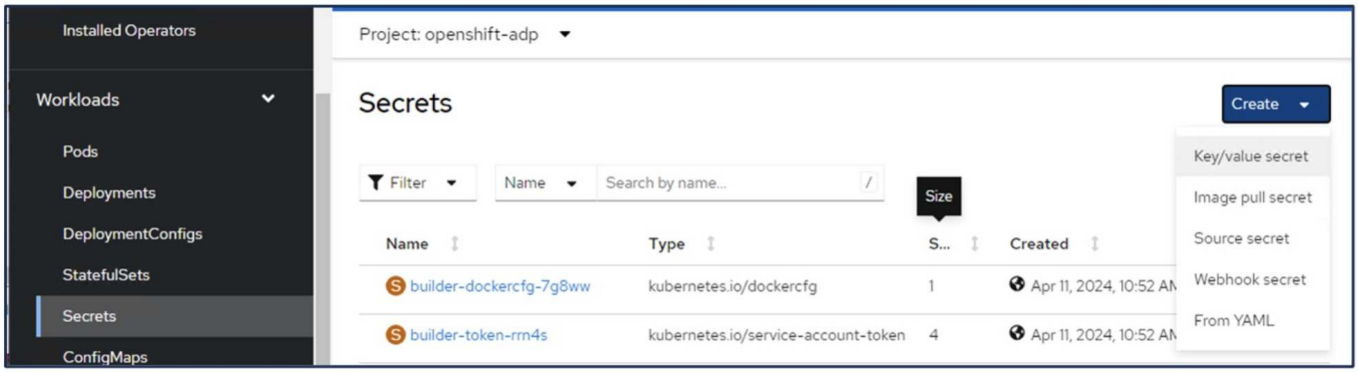
Requisitos previos para la configuración de Velero con detalles de StorageGrid S3

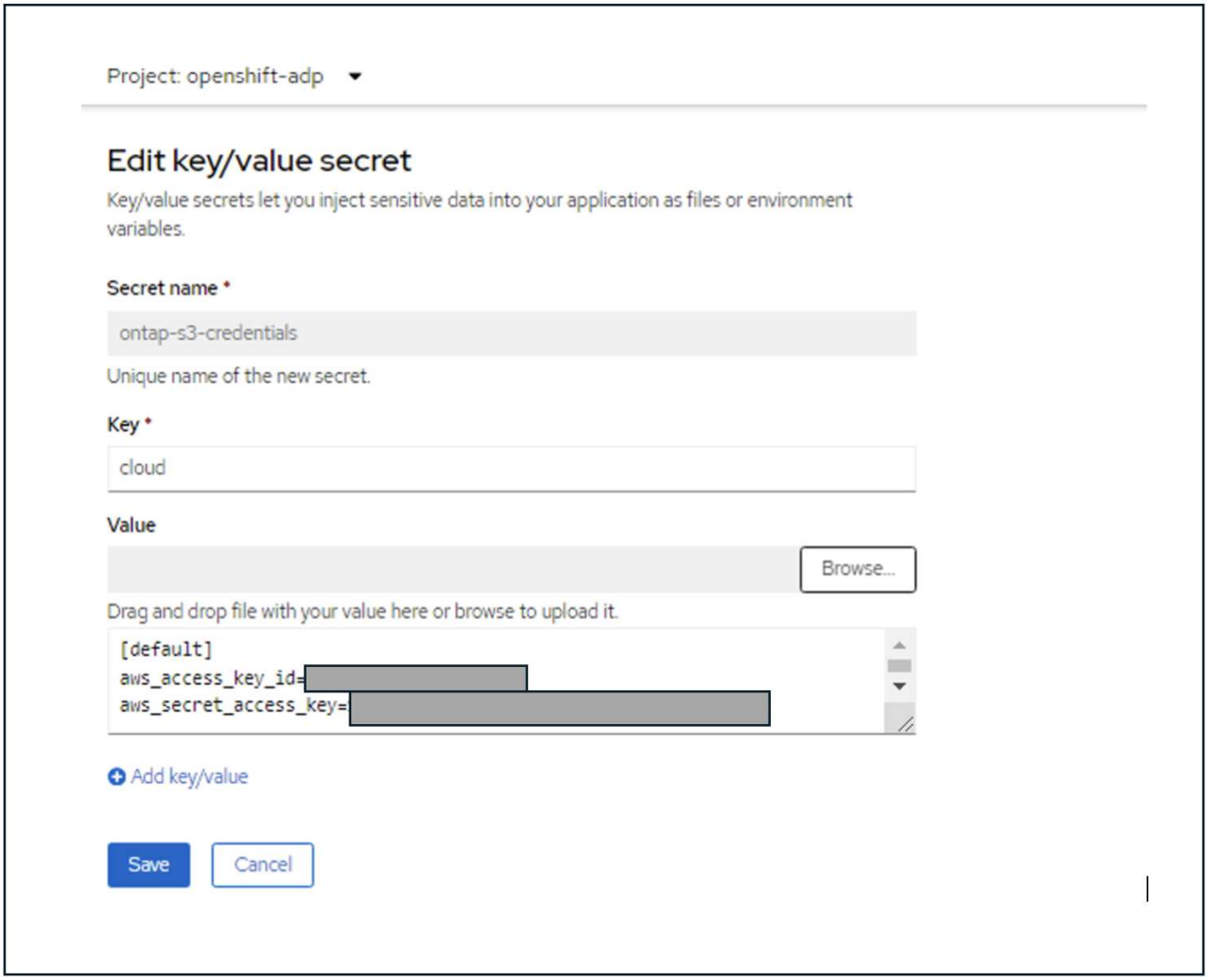
Velero se puede configurar para utilizar almacenamiento de objetos compatible con S3. Puede configurar StorageGrid S3 mediante los procedimientos que se muestran en la"Documentación de StorageGrid" . Necesitará la siguiente información de su configuración de StorageGrid S3 para integrarse con Velero.

- El punto final que se puede utilizar para acceder a S3
- Credenciales de usuario para acceder a S3 que incluyen la clave de acceso y la clave de acceso secreta
- Un nombre de depósito en S3 para copias de seguridad con permisos de acceso para el usuario
- Para obtener un acceso seguro al almacenamiento de objetos, se debe instalar un certificado TLS en el servidor de almacenamiento de objetos.

Pasos para configurar Velero

- Primero, cree un secreto para una credencial de usuario de ONTAP S3 o una credencial de usuario de StorageGrid Tenant. Esto 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 luego haga clic en Secreto de clave/valor. Proporcione los valores para el nombre de la credencial, la clave y el valor como se muestra. Asegúrese de utilizar el Id. de clave de acceso y la clave de acceso secreta de su usuario S3. Nombra el secreto apropiadamente En el siguiente ejemplo, se crea un secreto con credenciales de usuario de ONTAP S3 llamado ontap-s3-credentials.

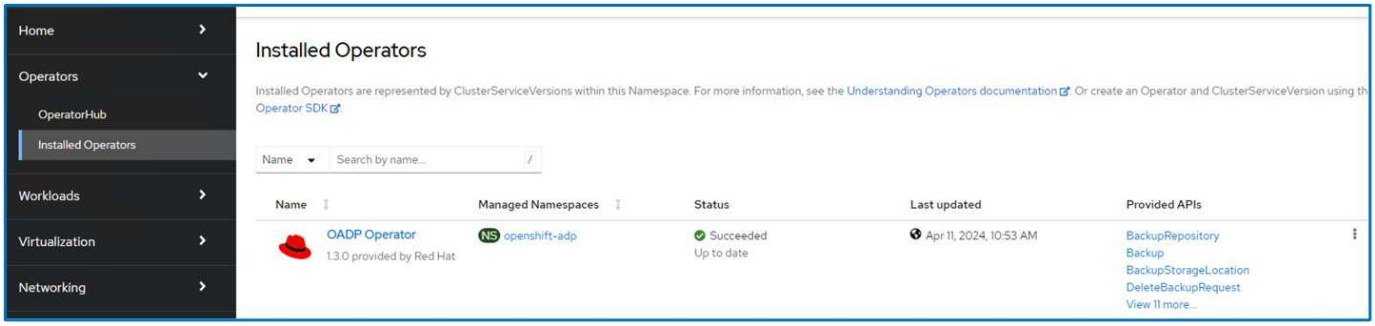




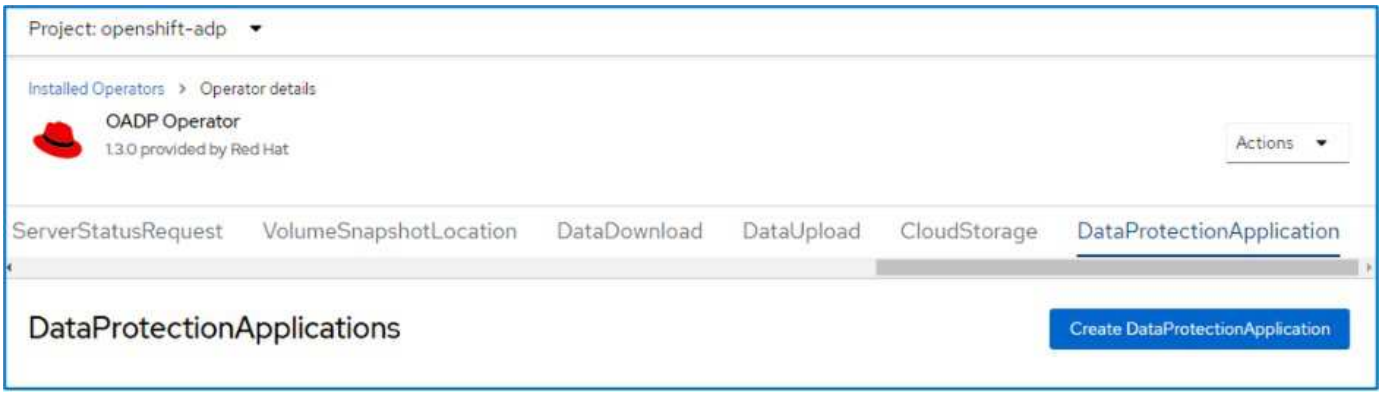
Para crear un secreto llamado sg-s3-credentials desde la CLI, puede utilizar el siguiente comando.

```
# 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 bajo Operadores, haga clic en el operador OADP y luego seleccione la pestaña DataProtectionApplication.



Haga clic en Crear aplicación de protección de datos. En la vista de formulario, proporcione un nombre para la aplicación de protección de datos o utilice el nombre predeterminado.



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

Archivo yaml de muestra para configurar Velero con ONTAP S3 como ubicación de respaldo

```
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
```

Archivo yaml de muestra para configurar Velero con StorageGrid S3 como 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
```

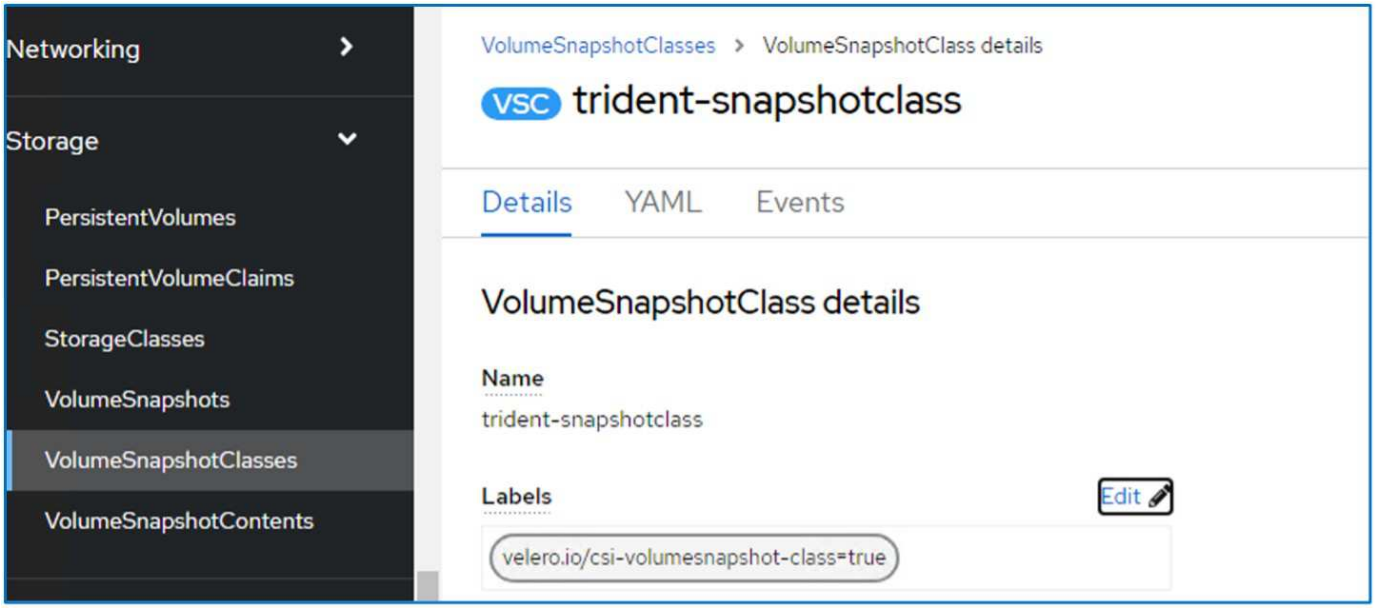
La sección de especificaciones del archivo yaml debe configurarse adecuadamente para los siguientes parámetros, de forma similar al ejemplo anterior.

backupLocations ONTAP S3 o StorageGrid S3 (con sus credenciales y otra información como se muestra en el yaml) está configurado como BackupLocation predeterminado para velero.

snapshotLocations Si usa instantáneas de la Interfaz de almacenamiento de contenedores (CSI), no necesita especificar una ubicación de instantánea porque creará un CR VolumeSnapshotClass para registrar el controlador CSI. En nuestro ejemplo, utiliza Trident CSI y previamente ha creado VolumeSnapShotClass CR utilizando el controlador Trident CSI.

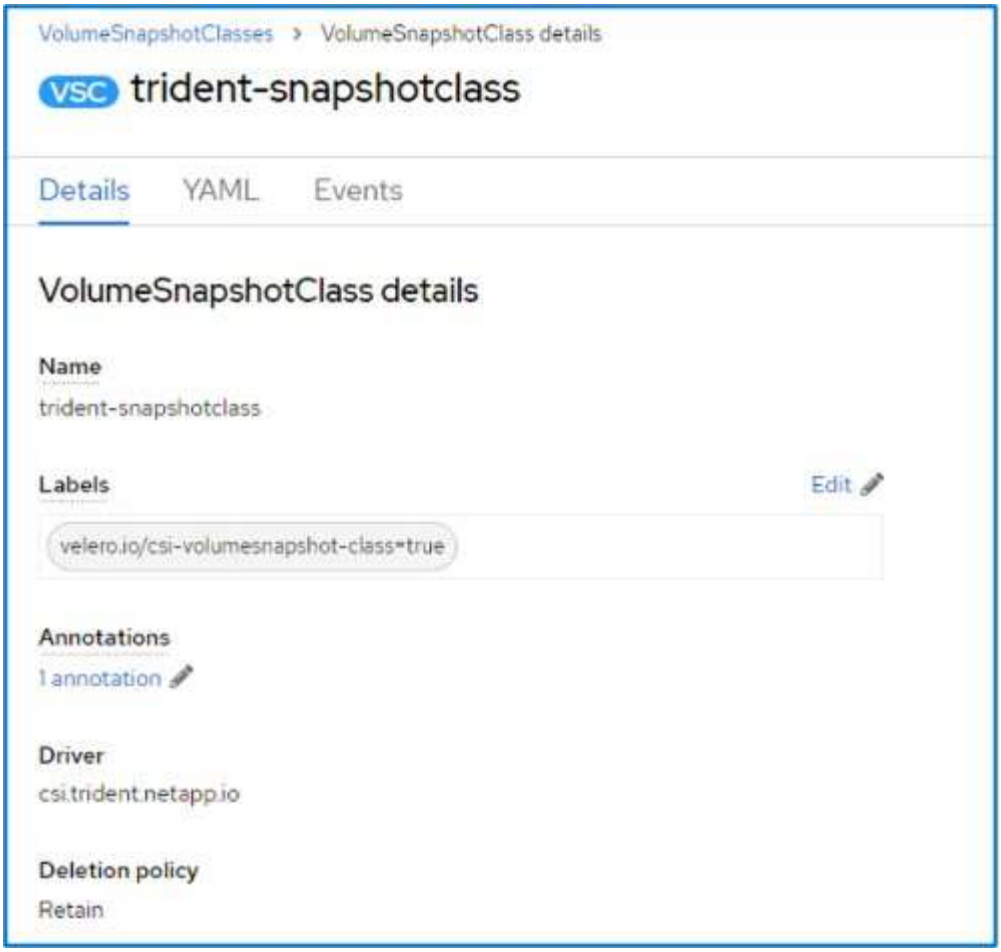
Habilitar complemento CSI Agregue csi a los complementos predeterminados para Velero para realizar copias de seguridad de volúmenes persistentes con instantáneas CSI. Los complementos CSI de Velero, para realizar copias de seguridad de los PVC respaldados por CSI, elegirán VolumeSnapshotClass en el clúster que tenga establecida la etiqueta **velero.io/csi-volumesnapshot-class**. Para esto

- Debe tener creada la clase VolumeSnapshotClass de tridente.
- Edite la etiqueta de trident-snapshotclass y configúrela en **velero.io/csi-volumesnapshot-class=true** como se muestra a continuación.

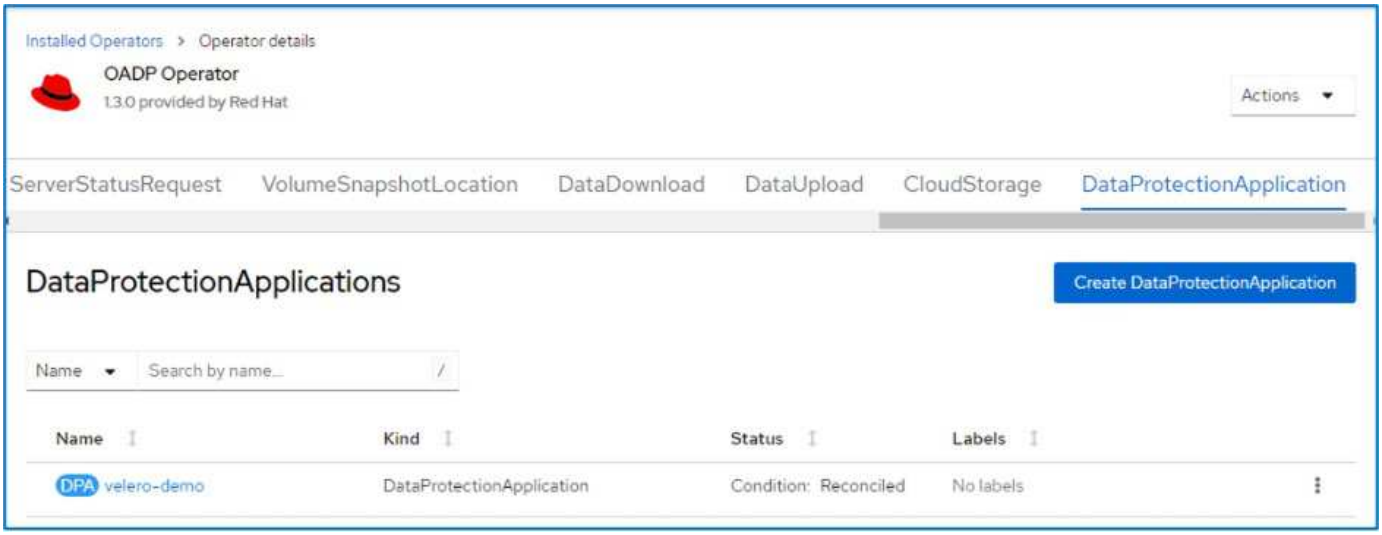


Asegúrese de que las instantáneas puedan persistir incluso si se eliminan los objetos VolumeSnapshot. Esto se puede hacer configurando **deletionPolicy** en Retener. De lo contrario, al eliminar un espacio de nombres se perderán por completo todos los PVC respaldados en él.

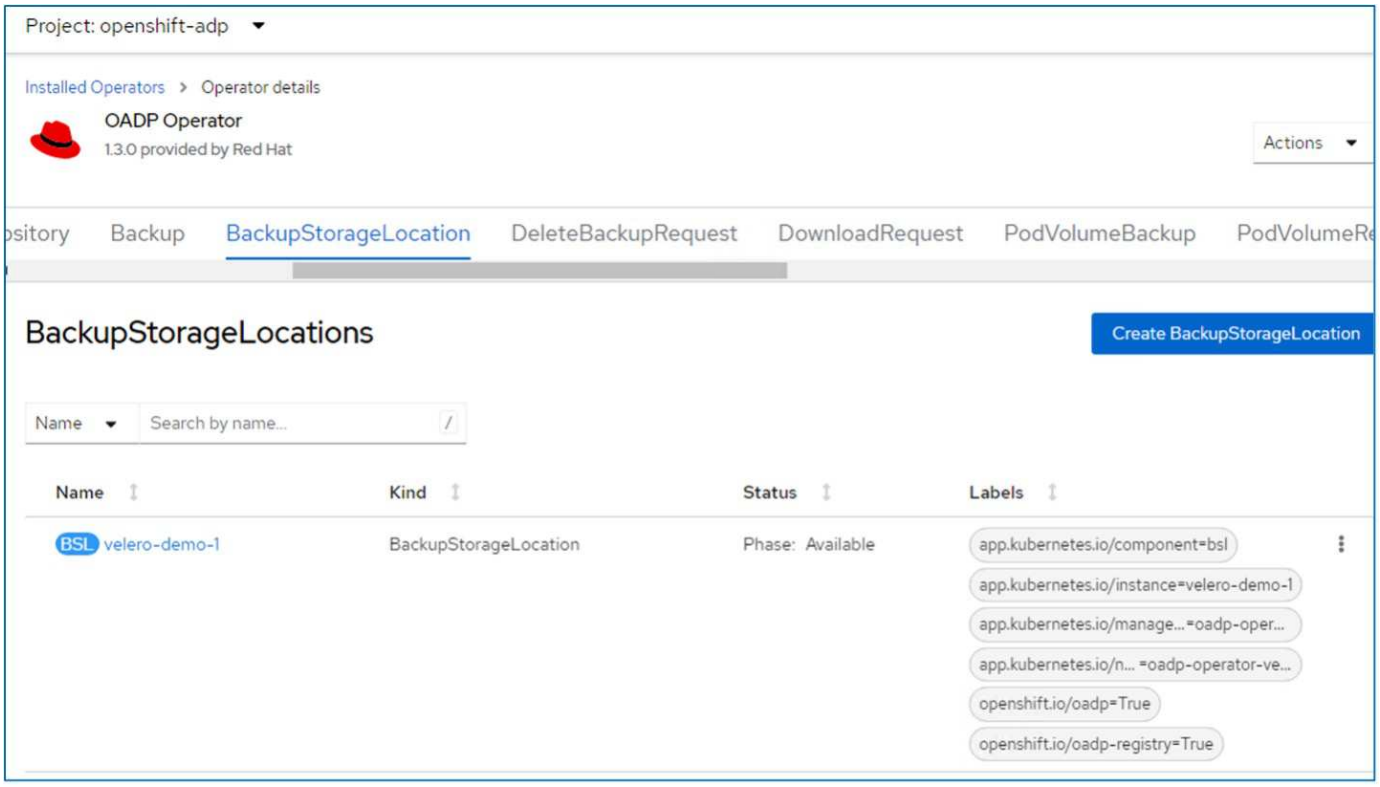
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Asegúrese de que la aplicación DataProtectionApplication se haya creado y esté en condición: Reconciliada.



El operador OADP creará un BackupStorageLocation correspondiente. Este se utilizará al crear una copia de seguridad.



Cree copias de seguridad a pedido para máquinas virtuales en Red Hat OpenShift Virtualization con Velero

Realice copias de seguridad de máquinas virtuales en OpenShift Virtualization utilizando Velero y NetApp ONTAP S3 o StorageGRID. Este procedimiento incluye la creación de recursos de respaldo personalizados (CR) para copias de seguridad a pedido y CR de programación para copias de seguridad programadas. Cada copia de seguridad captura metadatos de la máquina virtual y volúmenes persistentes y los almacena en la ubicación de almacenamiento de objetos especificada para fines de recuperación o cumplimiento.

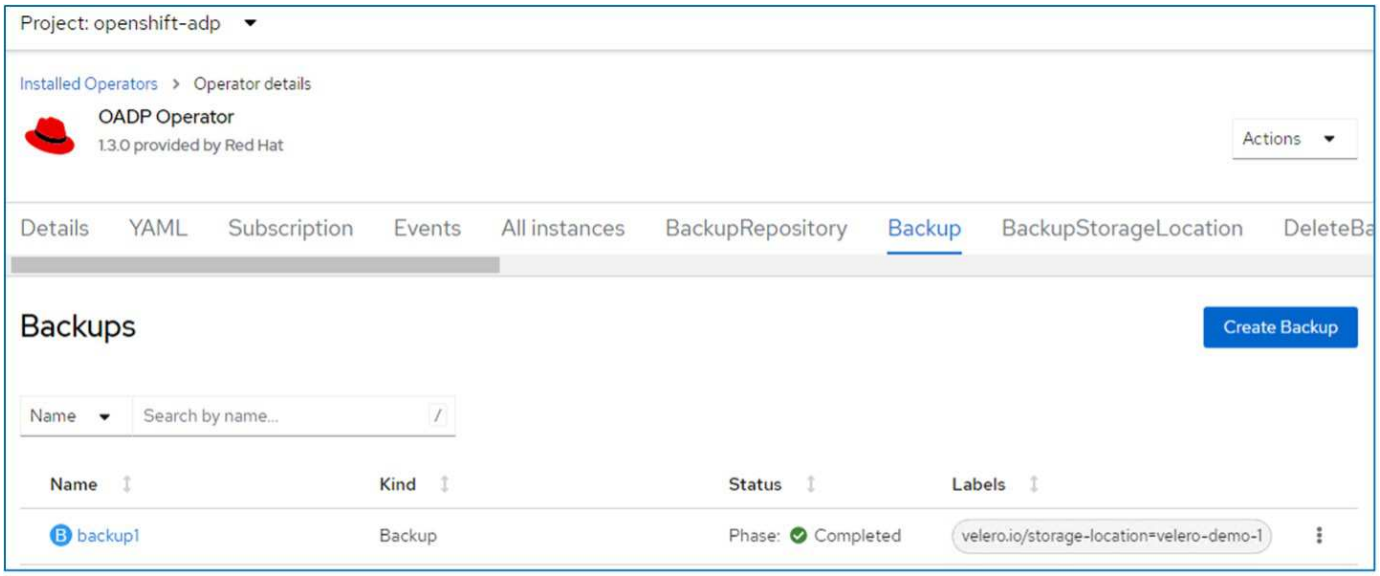
Pasos para crear una copia de seguridad de una máquina virtual

Para crear una copia de seguridad a pedido de toda la VM (metadatos de la VM y discos de la VM), haga clic en la pestaña **Copia de seguridad**. Esto crea un recurso personalizado de respaldo (CR). Se proporciona un yaml de muestra para crear el CR de respaldo. Usando este yaml, se realizará una copia de seguridad de la VM y sus discos en el espacio de nombres especificado. Se pueden configurar parámetros adicionales como se muestra en la"documentación" .

El CSI creará una instantánea de los volúmenes persistentes que respaldan los discos. Se crea una copia de seguridad de la máquina virtual junto con la instantánea de sus discos y se almacena en la ubicación de copia de seguridad especificada en el yaml. La copia de seguridad permanecerá en el sistema durante 30 días según lo especificado 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 navegador S3. La ruta de la copia de seguridad se muestra en el depósito configurado con el nombre de prefijo (velero/demobackup). Puede ver que el contenido de la copia de seguridad incluye las instantáneas de volumen, los registros y otros metadatos de la máquina virtual.

> En StorageGrid, también puede utilizar la consola S3 que está disponible en el Administrador de inquilinos para ver los objetos de respaldo.

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

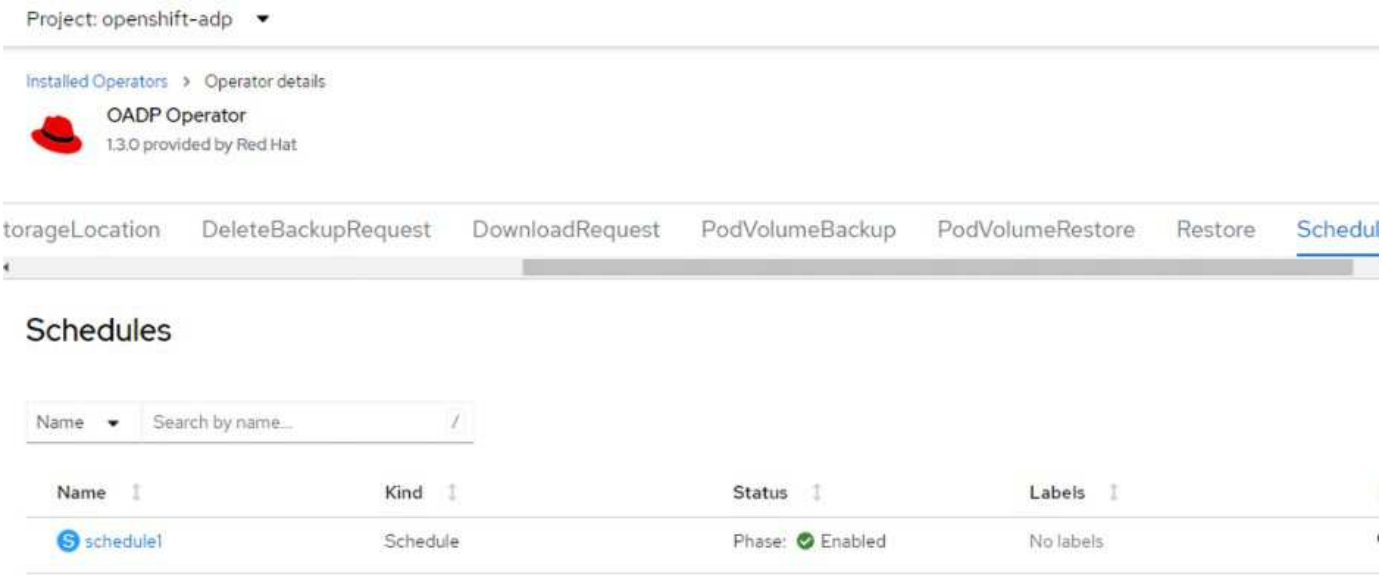
Creación de copias de seguridad programadas para máquinas virtuales en OpenShift Virtualization

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

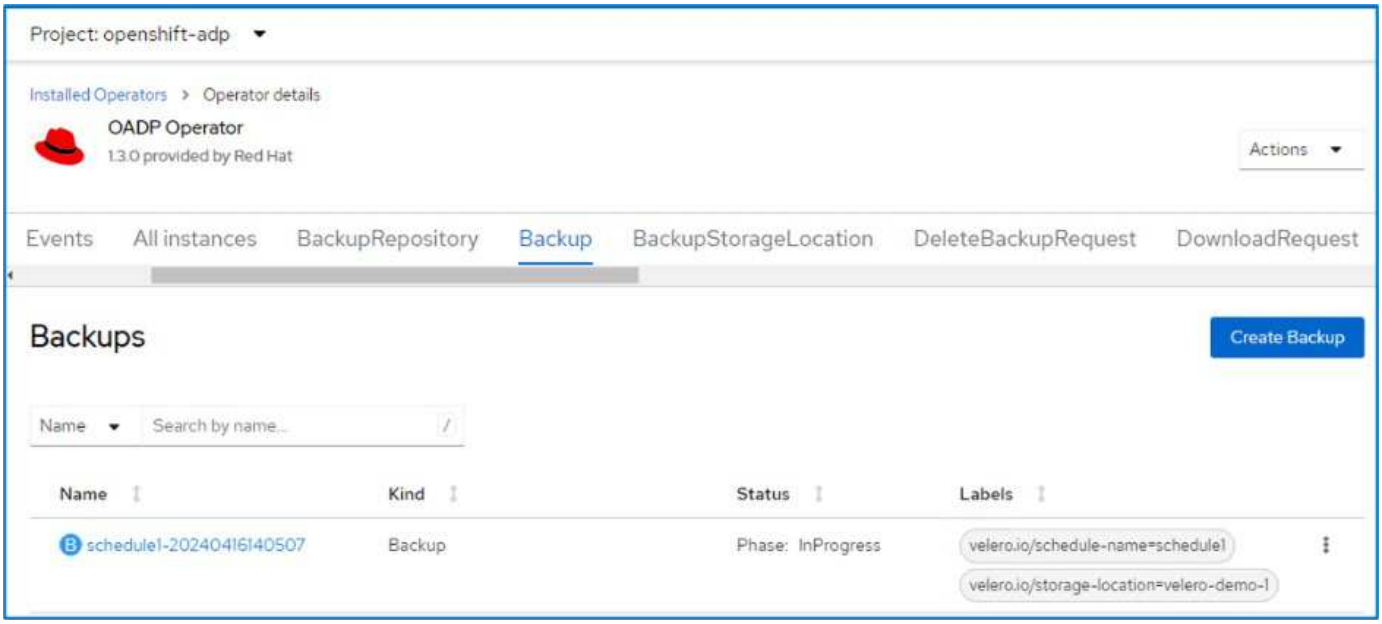
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

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. Entonces, en lugar de una CR de respaldo, se utiliza una CR programada para crear una copia de seguridad en el momento y frecuencia especificados.

Una vez creado el cronograma, se habilitará.



Se crearán copias de seguridad según este cronograma y se podrán ver desde la pestaña Copia de seguridad.



Restaurar una máquina virtual a partir de una copia de seguridad en Red Hat OpenShift Virtualization con Velero

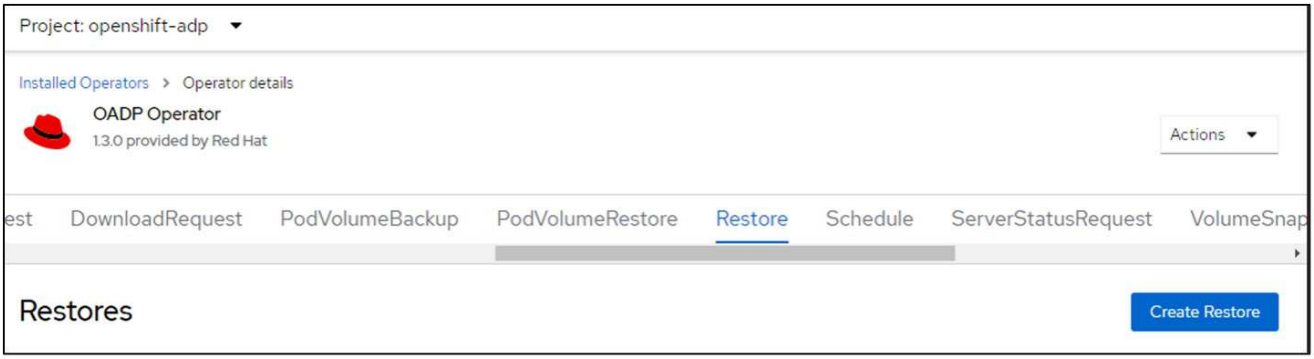
Restaure máquinas virtuales en OpenShift Virtualization utilizando Velero y la API de OpenShift para protección de datos (OADP). Este procedimiento incluye la creación de un recurso personalizado de restauración (CR) para recuperar máquinas virtuales y sus volúmenes persistentes a partir de copias de seguridad, con opciones para restaurar al espacio de nombres original, un espacio de nombres diferente o usar una clase de almacenamiento alternativa.

Prerrequisitos

Para restaurar desde una copia de seguridad, supongamos que el espacio de nombres donde existía la máquina virtual se eliminó accidentalmente.

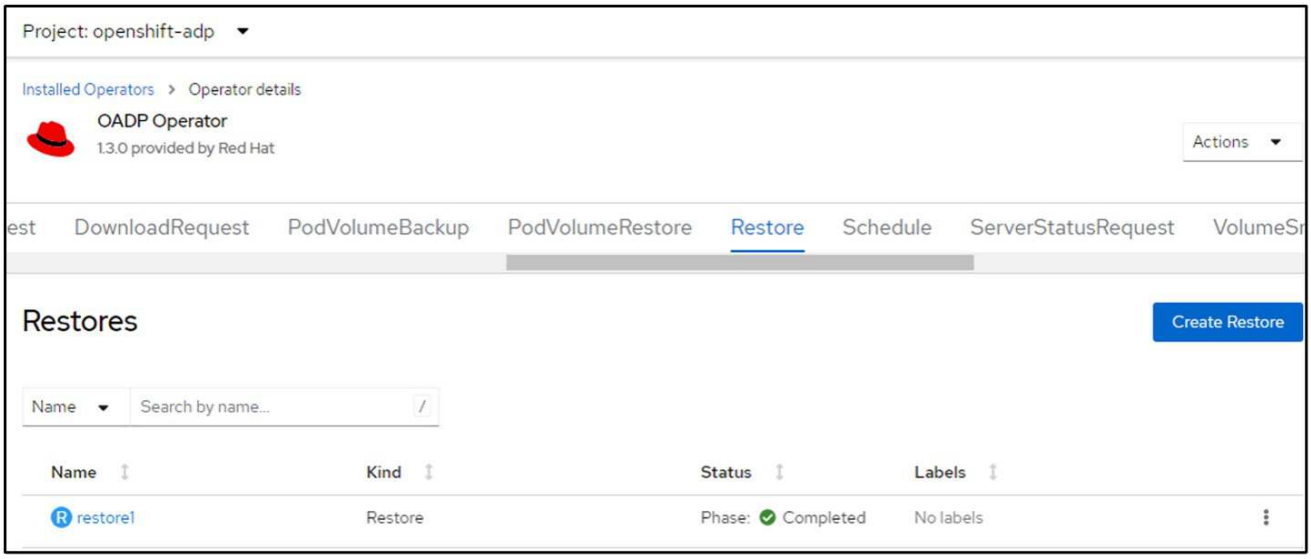
Restaurar al mismo espacio de nombres

Para restaurar desde la copia de seguridad que acabamos de crear, necesitamos crear un recurso de restauración personalizado (CR). Necesitamos proporcionarle un nombre, proporcionar el nombre de la copia de seguridad que queremos restaurar y establecer restorePVs en verdadero. Se pueden configurar parámetros adicionales 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 se muestra completada, puede ver que las máquinas virtuales se han restaurado al estado en el que se tomó la instantánea. (Si la copia de seguridad se creó cuando la VM estaba en ejecución, restaurar la VM desde la copia de seguridad iniciará la VM restaurada y la llevará a un estado de ejecución). La VM se restaura al mismo espacio de nombres.



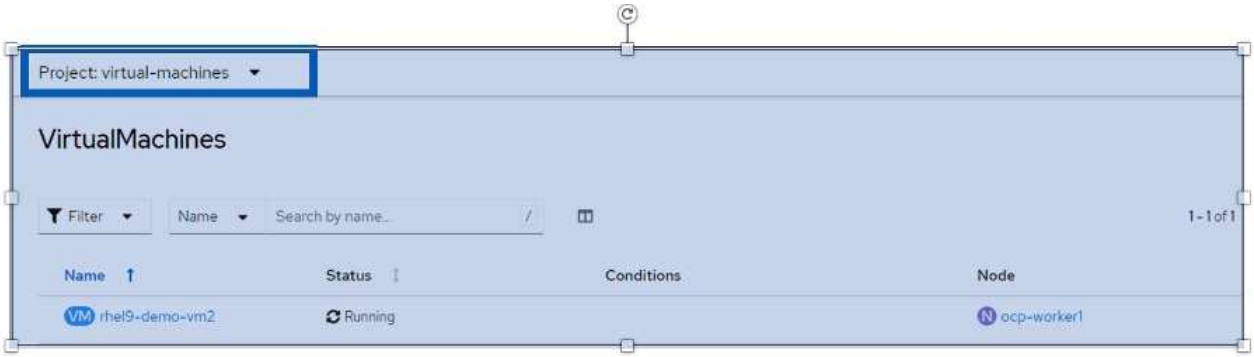
Restaurar a un espacio de nombres diferente

Para restaurar la máquina virtual a un espacio de nombres diferente, puede proporcionar un namespaceMapping en la definición yaml del CR de restauración.

El siguiente archivo yaml de muestra crea una CR de restauración para restaurar una VM y sus discos en el espacio de nombres virtual-machines-demo cuando la copia de seguridad se realizó al espacio de nombres 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
```

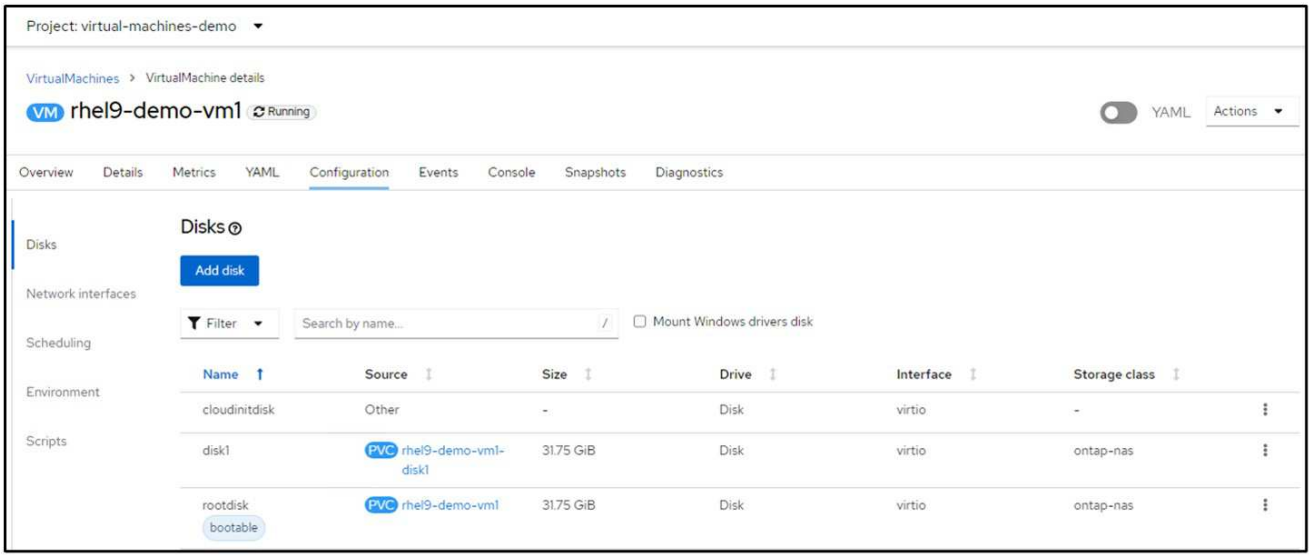
Cuando la fase se muestra completada, puede ver que las máquinas virtuales se han restaurado al estado en el que se tomó la instantánea. (Si la copia de seguridad se creó cuando la VM estaba en ejecución, restaurar la VM desde la copia de seguridad iniciará la VM restaurada y la llevará a un estado de ejecución). La máquina virtual se restaura a un espacio de nombres diferente según lo especificado en el yaml.

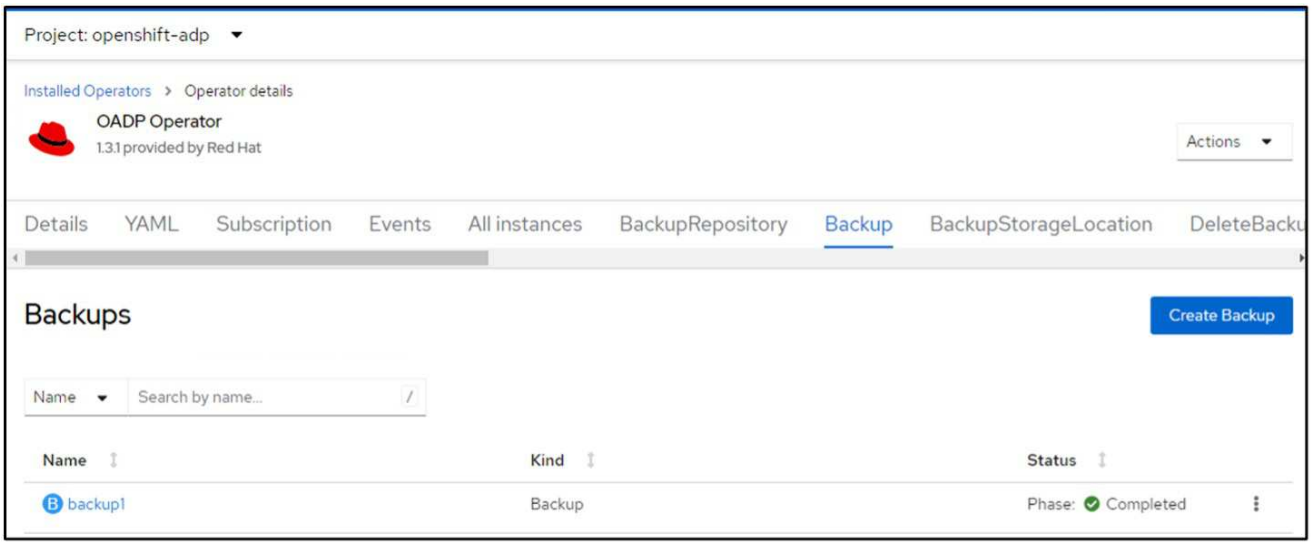


Restaurar a una clase de almacenamiento diferente

Velero proporciona una capacidad genérica para modificar los recursos durante la restauración especificando parches json. Los parches json se aplican a los recursos antes de restaurarlos. Los parches json se especifican en un mapa de configuración y el mapa de configuración se referencia en el comando de restauración. Esta función le permite restaurar utilizando diferentes clases de almacenamiento.

En el siguiente ejemplo, la máquina virtual, durante la creación, utiliza ontap-nas como clase de almacenamiento para sus discos. Se crea una copia de seguridad de la máquina virtual denominada backup1.





Simular una pérdida de la VM eliminándola.

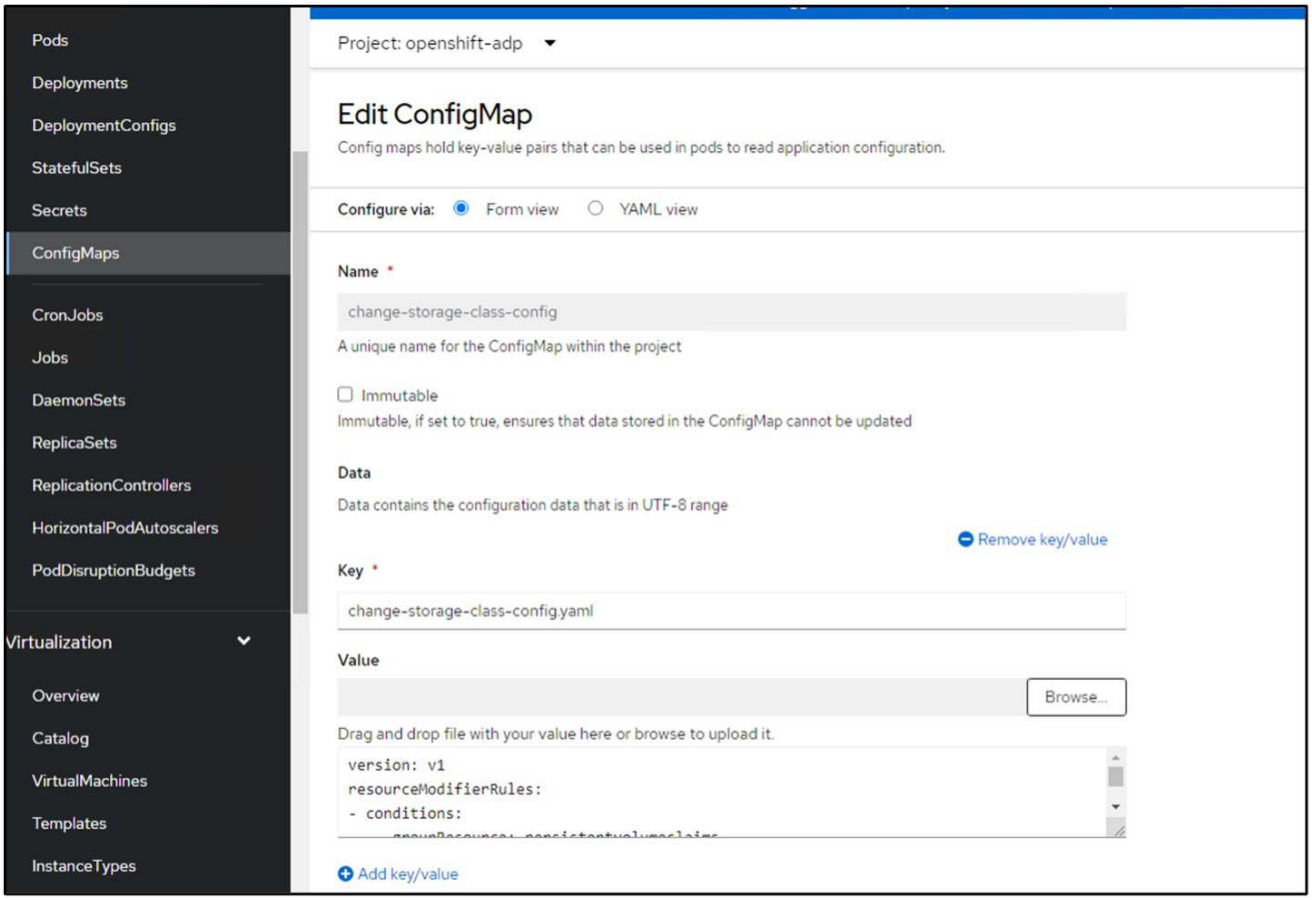
Para restaurar la máquina virtual utilizando una clase de almacenamiento diferente, por ejemplo, la clase de almacenamiento ontap-nas-eco, debe realizar los siguientes dos pasos:

Paso 1

Cree un mapa de configuración (consola) en el espacio de nombres openshift-adp de la siguiente

manera: Complete los detalles como se muestra en la captura de pantalla: Seleccione el 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 debería verse así (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>
```

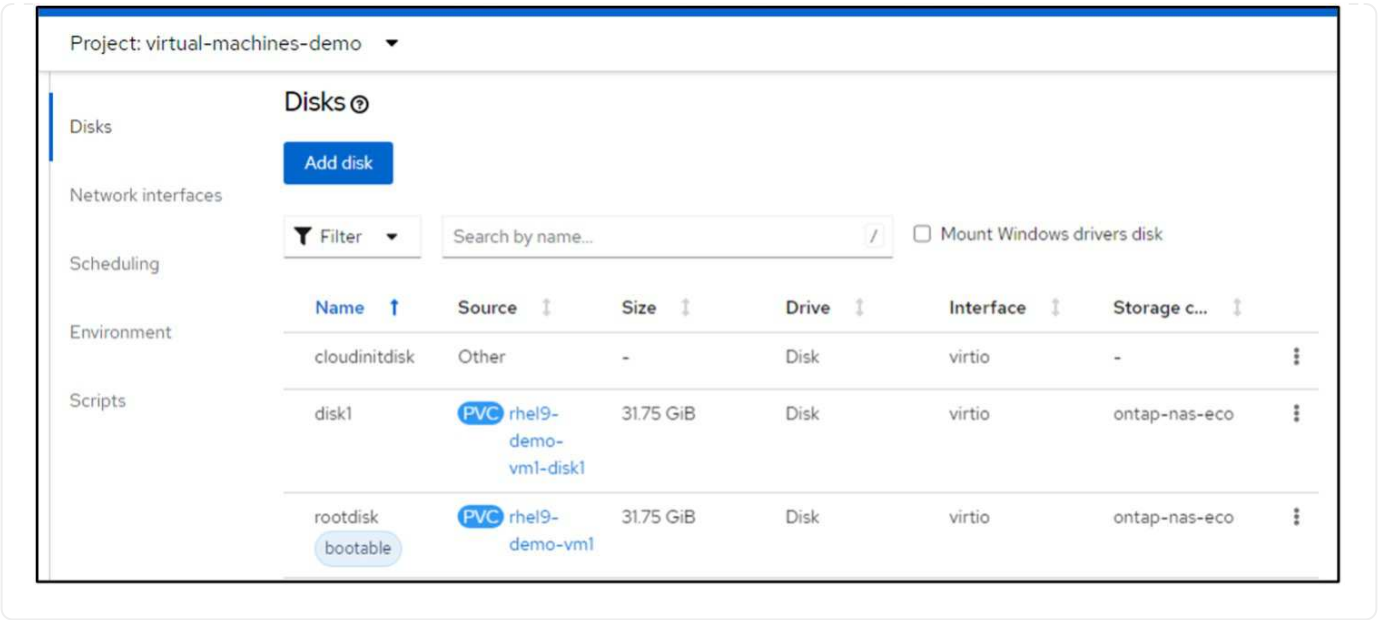
Este mapa de configuración aplicará la regla de modificación de recursos cuando se cree la restauración. Se aplicará un parche para reemplazar el nombre de la clase de almacenamiento a ontap-nas-eco para todos los reclamos de volumen persistente que comiencen con rhel.

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



Eliminar una CR de respaldo o restaurar una CR en Red Hat OpenShift Virtualization usando Velero

Eliminar recursos de copia de seguridad y restauración de máquinas virtuales en OpenShift Virtualization usando Velero. Utilice la CLI de OpenShift para eliminar copias de seguridad y conservar los datos de almacenamiento de objetos, o la CLI de Velero para eliminar tanto el recurso personalizado de copia de seguridad (CR) como los datos de almacenamiento asociados.

Eliminar una copia de seguridad

Puede eliminar un CR de respaldo 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 CR y eliminar los datos de almacenamiento de objetos asociados, puede hacerlo utilizando la herramienta Velero CLI.

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

Ejecute el siguiente comando de eliminación usando la CLI de Velero

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

Eliminar una restauración

Puede eliminar el CR de restauración mediante la CLI de Velero

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

Puede utilizar el comando oc así como la UI para eliminar la CR de restauración

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

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.