



# Protección de datos para OpenShift Virtualization

NetApp Solutions

NetApp  
April 17, 2024

# Tabla de contenidos

- Protección de datos para OpenShift Virtualization ..... 1
  - Protección de datos para máquinas virtuales de OpenShift Virtualization mediante OpenShift API for Data Protection (OADP) ..... 1
  - Instalación del operador de la API de OpenShift para la protección de datos (OADP) ..... 3
  - Crear backups bajo demanda para máquinas virtuales en la virtualización de OpenShift ..... 11
  - Restaurar un equipo virtual desde un backup ..... 14
  - Eliminación de copias de seguridad y restauraciones en el uso de Velero ..... 15

# Protección de datos para OpenShift Virtualization

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

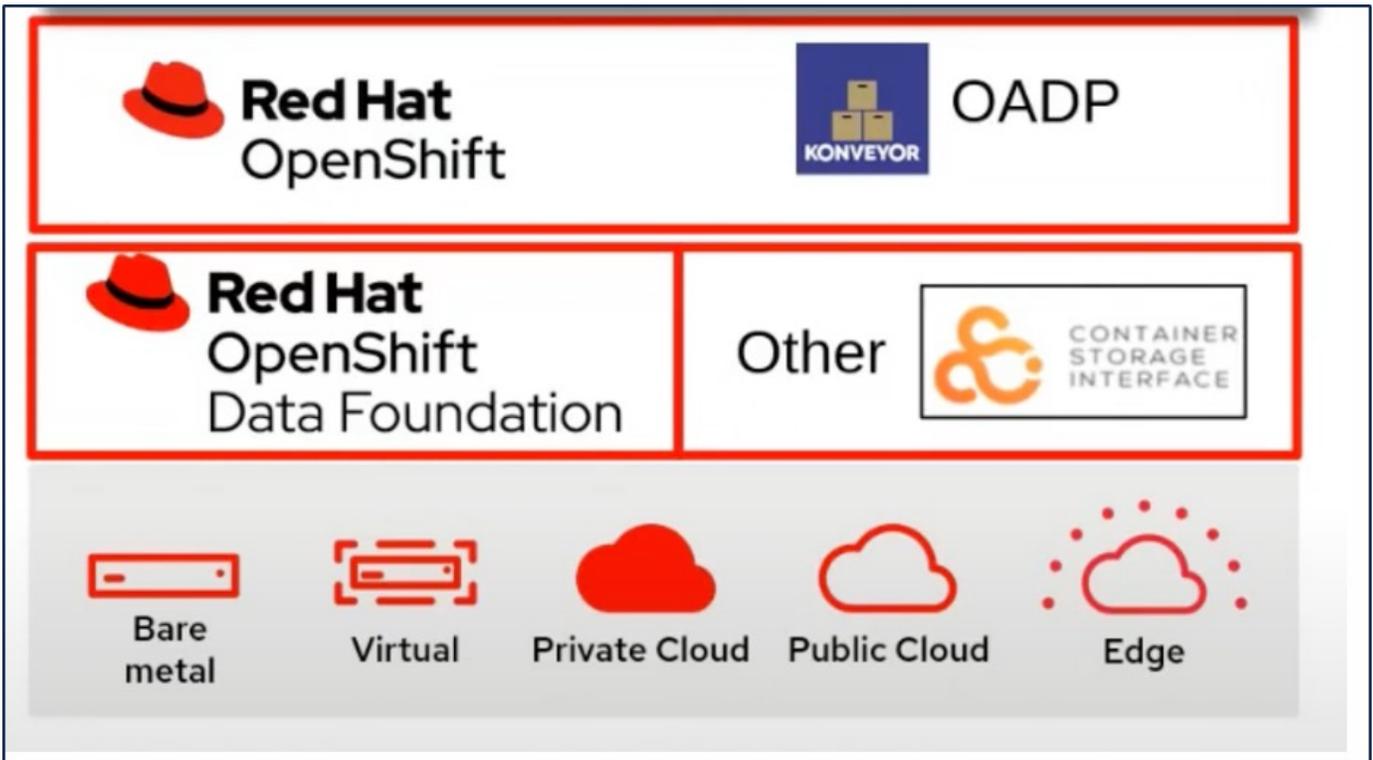
Banu Sundhar, NetApp

Este documento de referencia proporciona detalles para crear backups de máquinas virtuales mediante la API de OpenShift para protección de datos (OADP) con Velero y trasladarla a ONTAP S3. Los backups de las RVP de las máquinas virtuales se crean utilizando CSI Astra Trident Snapshots.

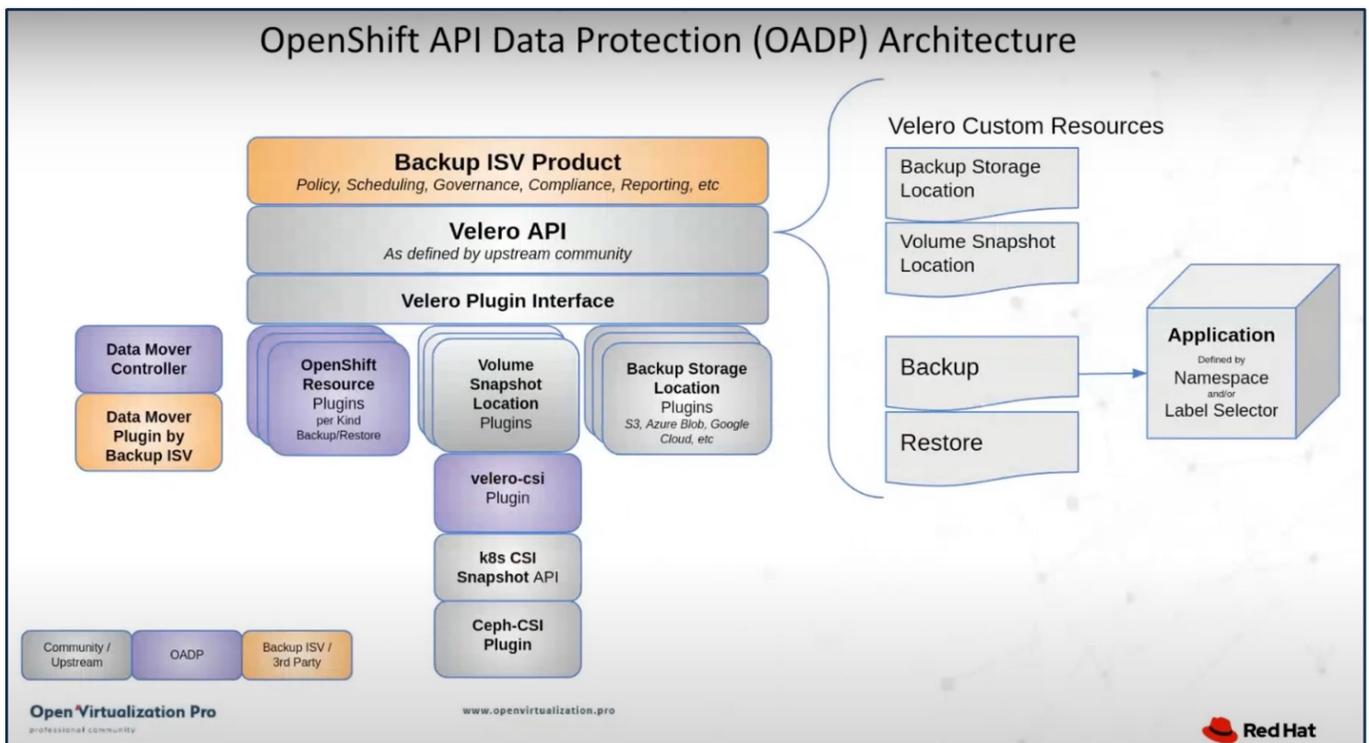
Las máquinas virtuales en el entorno de virtualización de OpenShift son aplicaciones en contenedores que se ejecutan en los nodos de trabajo de la plataforma de contenedores de OpenShift. Es importante proteger los metadatos de la máquina virtual y los discos persistentes de las máquinas virtuales, de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

Los discos persistentes de los equipos virtuales de virtualización OpenShift pueden estar respaldados por el almacenamiento ONTAP integrado en el cluster OpenShift mediante ["CSI de Astra Trident"](#). En esta sección utilizamos ["API de OpenShift para la protección de datos \(OADP\)"](#) Para realizar backup de equipos virtuales, incluidos sus volúmenes de datos en el almacenamiento de objetos de ONTAP. 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 componentes 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
- Astra Trident 24,02
- ONTAP 9,12

## 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 mediante Astra Trident
- Un back-end de Trident configurado con una SVM en un clúster de ONTAP
- Un StorageClass configurado en el clúster OpenShift con Astra Trident como 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 denominado openshift-adp.

**OperatorHub**

Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Marketplace optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the Developer Catalog providing a self-service experience.

All Items

AI/Machine Learning  
Application Runtime  
Big Data  
Cloud Provider  
Database  
Developer Tools  
Development Tools  
Drivers and plugins  
Integration & Delivery  
Logging & Tracing  
Modernization & Migration  
Monitoring

Search: OADP

**Red Hat**  
OADP Operator provided by Red Hat  
OADP (OpenShift API for Data Protection) operator sets up and installs Data Protection...

**Community**  
OADP Operator provided by Red Hat  
OADP (OpenShift API for Data Protection) operator sets up and installs Velero on the OpenShift...

**OADP Operator**  
1.3.0 provided by Red Hat

**Install**

**Channel**  
stable-1.3

**Version**  
1.3.0

**Capability level**

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

**Source**  
Red Hat

**Provider**  
Red Hat

**Infrastructure features**  
Disconnected

**OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.**

Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.

OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.

- [Installing OADP for application backup and restore](#)
- [Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM](#)
- [Frequently Asked Questions](#)

Project: All Projects ▾

## Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#) Operator and ClusterServiceVersion using the [Operator SDK](#).

Name ▾ Search by name... /

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

### Requisitos previos para la configuración de Velero con ONTAP S3 DETALLES:

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) IP 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

- En primer lugar, cree un secreto para las credenciales de usuario de ONTAP S3. 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.

Project: openshift-adp

## Secrets

Filter Name Search by name... Size

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

Create

- Key/value secret
- Image pull secret
- Source secret
- Webhook secret
- From YAML

Project: openshift-adp

## Create key/value secret

Key/value secrets let you inject sensitive data into your application as files or environment variables.

**Secret name \***

Unique name of the new secret.

**Key \***

**Value**

Drag and drop file with your value here or browse to upload it.

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

+ Add key/value

Create Cancel



Para crear el secreto predeterminado con nombres credenciales del cloud desde la CLI, puede usar el siguiente comando. Si las ubicaciones de copia de seguridad y instantáneas utilizan las mismas credenciales, solo tiene que crear el secreto predeterminado como se muestra anteriormente. Para otros escenarios, consulte la documentación de OADP.

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

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 en Operadores, haga clic en Operador OADP y, a continuación, seleccione la pestaña DataProtectionApplication.

Name	Managed Namespaces	Status	Last updated	Provided APIs
 OADP Operator 1.3.0 provided by Red Hat	NS openshift-adp	✔ Succeeded Up to date	🕒 Apr 11, 2024, 10:53 AM	BackupRepository Backup BackupStorageLocation DeleteBackupRequest View II more...

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

Project: openshift-adp

Installed Operators > Operator details

 OADP Operator  
1.3.0 provided by Red Hat

Actions

ServerStatusRequest VolumeSnapshotLocation DataDownload DataUpload CloudStorage DataProtectionApplication

DataProtectionApplications

Create DataProtectionApplication

Ahora vaya a la vista YAML y reemplace la información predeterminada o agregue la información como se muestra en el archivo yaml a continuación.

```

spec:
  backupLocations:
    - velero:
      config:
        insecureSkipTLSVerify: 'true' //use this for https communication
with ONTAP S3
        profile: default
        region: us-east
        s3ForcePathStyle: 'True' //This allows use of IP in s3URL
        s3Url: 'https://10.xx.xx.xx' //Ensure TLS certificate for S3 is
configured
      credential:
        key: cloud
        name: cloud-credentials //previously created secret named cloud-
credentials
        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
      snapshotLocations:
        - velero:
          config:
            profile: default
            region: us-east
            provider: aws

```

El YAML anterior tiene las siguientes secciones en la especificación que deben configurarse adecuadamente de manera similar al ejemplo:

### **BackupLocations**

ONTAP S3 (con sus credenciales y otra información como se muestra en el yaml) está configurado como la

ubicación de copia de seguridad predeterminada para velero.

## SnapshotLocations

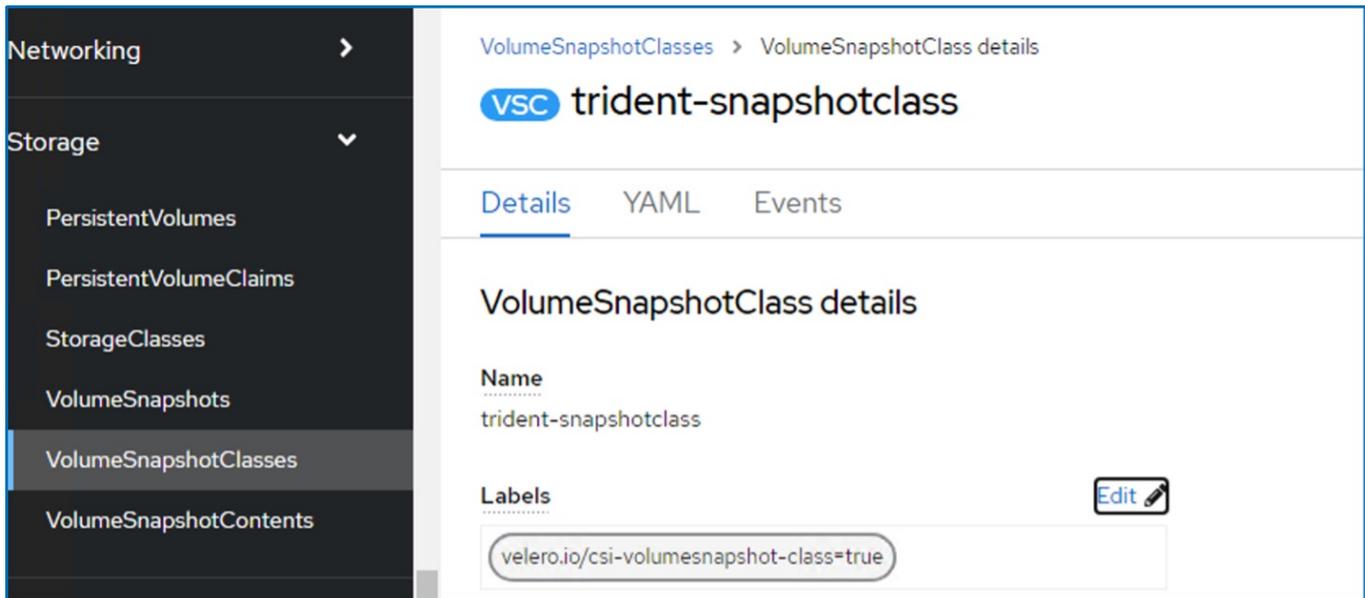
ONTAP S3 está configurado como la ubicación predeterminada para las instantáneas de PVC para Velero.

## Habilitar 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.



The screenshot shows the Kubernetes dashboard interface for a VolumeSnapshotClass. The left sidebar is expanded to 'Storage' > 'VolumeSnapshotClasses'. The main content area shows the details for the 'trident-snapshotclass' VolumeSnapshotClass. The 'Name' is 'trident-snapshotclass'. The 'Labels' section shows a single label: 'velero.io/csi-volumesnapshot-class=true'. There is an 'Edit' button next to the labels.

Asegúrese de que las snapshots puedan persistir incluso si se han eliminado los objetos de VolumeSnapshot. Esto se puede hacer configurando la política de eliminación en 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
```

VolumeSnapshotClasses > VolumeSnapshotClass details

**VSC** trident-snapshotclass

Details | YAML | Events

### VolumeSnapshotClass details

**Name**  
trident-snapshotclass

**Labels** Edit 

velero.io/csi-volumesnapshot-class=true

**Annotations**  
1 annotation 

**Driver**  
csi.trident.netapp.io

**Deletion policy**  
Retain

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

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat Actions 

ServerStatusRequest | VolumeSnapshotLocation | DataDownload | DataUpload | CloudStorage | **DataProtectionApplication**

### DataProtectionApplications

Create DataProtectionApplication

Name  Search by name...

Name 	Kind 	Status 	Labels 
 velero-demo	DataProtectionApplication	Condition: Reconciled	No labels 

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

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat

Actions ▾

Repository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRe

## BackupStorageLocations

Create BackupStorageLocation

Name ▾ Search by name... /

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

## Crear backups bajo demanda para máquinas virtuales en la virtualización de OpenShift

### 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 y se moverá a la ubicación de almacenamiento de objetos proporcionada 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
  ttl: 720h0m0s

```

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

The screenshot shows the OpenShift console interface for the 'openshift-adp' project. It displays the 'Backup' phase of the 'OADP Operator' (version 1.3.0). The 'Backup' tab is selected, and a 'Create Backup' button is visible. Below the navigation bar, there is a search bar and a table of backups. The table has columns for Name, Kind, Status, and Labels. One backup named 'backup1' is listed with a status of 'Completed' and a label 'velero.io/storage-location=velero-demo-1'.

Name	Kind	Status	Labels
backup1	Backup	Phase: <span style="color: green;">✔</span> Completed	velero.io/storage-location=velero-demo-1

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.

The screenshot shows an S3 bucket explorer view for the path '/ demobackup/ backups/ backup1/'. The table lists the following files:

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

## Crear backups programados para máquinas virtuales en la virtualización de OpenShift

Para crear backups según una programación, debe crear un recurso personalizado de programación. La programación es simplemente una expresión Cron que le permite especificar la hora a la que desea crear la copia de seguridad. yml 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 de la hora y frecuencia especificadas.

Una vez creada la programación, se habilita.

Project: openshift-adp ▾

---

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat

---

storageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRestore Restore **Schedule**

---

### Schedules

Name ▾ Search by name... /

Name	Kind	Status	Labels
 schedule1	Schedule	Phase:  Enabled	No labels

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

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat Actions ▾

Events All instances BackupRepository **Backup** BackupStorageLocation DeleteBackupRequest DownloadRequest

**Backups** Create Backup

Name ▾ Search by name... /

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

## Restaurar un equipo virtual 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.

### Pasos para realizar una restauración

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.

Project: openshift-adp ▾

Installed Operators > Operator details

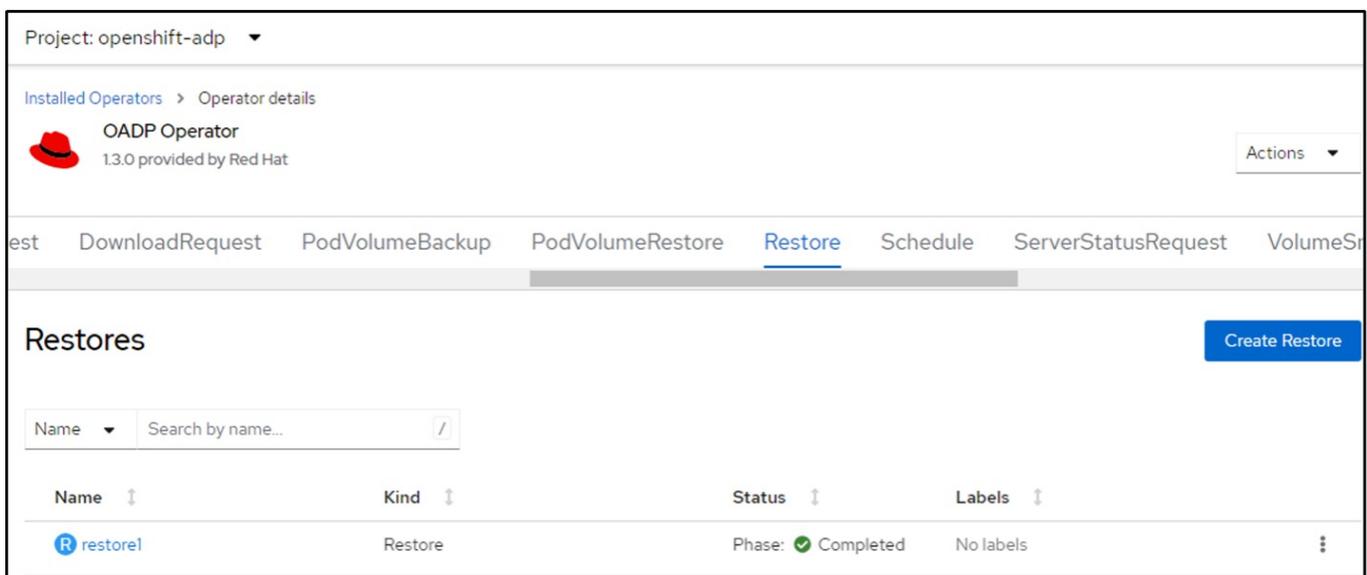
 **OADP Operator**  
1.3.0 provided by Red Hat Actions ▾

est DownloadRequest PodVolumeBackup PodVolumeRestore **Restore** Schedule ServerStatusRequest VolumeSnap

**Restores** Create Restore

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

Cuando la fase muestre Finalizado, verá que las máquinas virtuales se han restaurado al estado en el 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)



Project: openshift-adp

Installed Operators > Operator details

 OADP Operator  
1.3.0 provided by Red Hat

Actions

est DownloadRequest PodVolumeBackup PodVolumeRestore **Restore** Schedule ServerStatusRequest VolumeS

### Restores

Create Restore

Name Search by name...

Name	Kind	Status	Labels
 restore1	Restore	Phase:  Completed	No labels

## Eliminación de copias de seguridad y restauraciones en el uso de 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>
```

También 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

Copyright © 2024 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 INTERRUPTIÓN 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.