



# **Proteja los datos de las aplicaciones en las instalaciones**

## **Cloud Backup**

NetApp  
February 20, 2023

# Tabla de Contenido

- Proteja los datos de las aplicaciones en las instalaciones. . . . . 1
  - Proteja los datos de las aplicaciones locales. . . . . 1
  - Registre el servidor SnapCenter . . . . . 2
  - Crear una política para realizar backups de aplicaciones . . . . . 4
  - Realice backup de los datos de las aplicaciones en las instalaciones en Amazon Web Services . . . . . 5
  - Realice backups de los datos de las aplicaciones en las instalaciones en Microsoft Azure . . . . . 6
  - Realice backups de los datos de las aplicaciones en las instalaciones en Google Cloud Platform . . . . . 7
  - Realice backups de los datos de las aplicaciones en las instalaciones en StorageGRID. . . . . 7
  - Gestione la protección de aplicaciones . . . . . 8
  - Restaura los datos de las aplicaciones en las instalaciones . . . . . 11
  - Montar backups de aplicaciones . . . . . 15

# Proteja los datos de las aplicaciones en las instalaciones

## Proteja los datos de las aplicaciones locales

Puede integrar Cloud Backup para aplicaciones con BlueXP (anteriormente Cloud Manager) y SnapCenter en las instalaciones para realizar backups de las copias Snapshot consistentes con la aplicación desde ONTAP en las instalaciones al cloud. Cuando sea necesario, puede restaurar desde el cloud a un servidor de SnapCenter en las instalaciones.

Puede realizar backups de datos de aplicaciones de Oracle, Microsoft SQL y SAP HANA desde sistemas ONTAP en las instalaciones a Amazon Web Services, Microsoft Azure, Google Cloud Platform y StorageGRID.



Debe utilizar el software SnapCenter 4.6 o una versión posterior.

Para obtener más información sobre el backup en el cloud para las aplicaciones, consulte:

- ["Backup para aplicaciones con Cloud Backup y SnapCenter"](#)
- ["Podcast sobre Cloud Backup para aplicaciones"](#)

## Requisitos

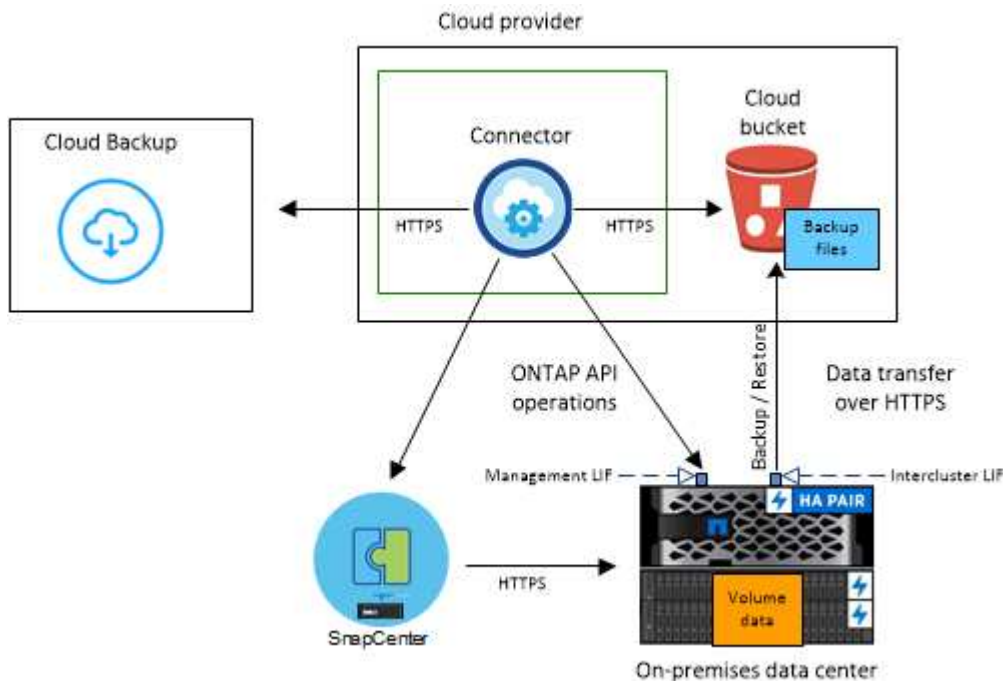
Lea los siguientes requisitos para asegurarse de tener una configuración compatible antes de empezar a realizar el backup de datos de aplicación en los servicios de cloud.

- ONTAP 9.8 o posterior
- BlueXP 3.9
- SnapCenter Server 4.6 o posterior debe utilizar SnapCenter Server 4.7 si desea utilizar las siguientes características:
  - proteja los backups del almacenamiento secundario en las instalaciones
  - Proteja aplicaciones SAP HANA
  - Protección de aplicaciones de Oracle y SQL que se encuentran en un entorno de VMware
  - montar backups
  - desactivar las copias de seguridad
  - Cancele el registro del servidor SnapCenter
- Debe haber al menos un backup por aplicación disponible en SnapCenter Server
- Al menos una política diaria, semanal o mensual en SnapCenter sin etiqueta ni etiqueta de la política de backup en cloud para aplicaciones en BlueXP.



Cloud Backup para aplicaciones no admite la protección de aplicaciones que se encuentran en las SVM que se añadieron mediante FQDN o dirección IP.

En la siguiente imagen se muestra cada componente al realizar backups en cloud y las conexiones que necesita preparar entre ellos:



En la siguiente imagen se muestra cada componente al realizar un backup en StorageGRID y las conexiones que necesita preparar entre ellos:



## Registre el servidor SnapCenter

Solo un usuario con el rol de administrador de SnapCenter puede registrar el host en el que se ejecuta SnapCenter Server 4.6 o una versión posterior. Es posible registrar varios hosts de SnapCenter Server.

- Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. En el menú desplegable **Configuración**, haga clic en **servidores SnapCenter**.
3. Haga clic en **Registrar servidor SnapCenter**.
4. Especifique los siguientes detalles:
  - a. En el campo servidor SnapCenter, especifique el FQDN o la dirección IP del host SnapCenter Server.
  - b. En el campo Puerto, especifique el número de puerto en el que se está ejecutando el servidor SnapCenter.  
  
Debe asegurarse de que el puerto esté abierto para que se produzca la comunicación entre SnapCenter Server y el backup en el cloud para las aplicaciones.
  - c. En el campo Etiquetas, especifique un nombre de sitio, un nombre de ciudad o cualquier nombre personalizado con el que desee etiquetar el servidor SnapCenter.  
  
Las etiquetas están separadas por comas.
  - d. En el campo Username and Password, especifique las credenciales del usuario con el rol SnapCenterAdmin.
5. Haga clic en **Registrar**.

## Después de terminar

Haga clic en **copia de seguridad y restauración > aplicaciones** para ver todas las aplicaciones protegidas con el host de servidor SnapCenter registrado.

De forma predeterminada, las aplicaciones se detectan automáticamente cada día, a medianoche. Puede configurar la programación para detectar las aplicaciones.



En las bases de datos de SQL Server, la columna Nombre de aplicación muestra el nombre en formato *Application\_name (nombre de instancia)*.

Las aplicaciones admitidas y sus configuraciones son:

- Base de datos de Oracle:
  - Backups completos (datos + registro) creados con al menos una programación diaria, semanal o mensual
  - SAN, NFS, VMDK-SAN, VMDK-NFS Y RDM
- Base de datos Microsoft SQL Server:
  - Independientes, instancias de clústeres de conmutación por error y grupos de disponibilidad
  - Backups completos creados con al menos un programa diario, semanal o mensual
  - SAN, VMDK-SAN, VMDK-NFS Y RDM
- Base de datos SAP HANA:
  - Contenedor único 1.x
  - Contenedor de base de datos múltiple 2.x.
  - Replicación de sistemas HANA (HSR)

Debe tener al menos un backup en las ubicaciones primaria y secundaria. Puede decidir realizar un error proactivo o una conmutación por error diferida al secundario.

- Recursos de volúmenes sin datos (NDV), como los binarios de HANA, el volumen de registro de archivos de HANA, el volumen compartido de HANA, etc.

No se mostrarán las siguientes bases de datos:

- Bases de datos que no tienen backups
- Bases de datos que solo tienen políticas bajo demanda o por hora
- Bases de datos de Oracle que residen en NVMe

## Crear una política para realizar backups de aplicaciones

Puede usar una de las políticas preparadas previamente o crear una política personalizada para realizar el backup de los datos de la aplicación en el cloud. Puede crear directivas si no desea editar las directivas preparadas previamente.

Las políticas predefinidas son:

| Nombre de la directiva     | Etiqueta       | Valor de retención |
|----------------------------|----------------|--------------------|
| 1 año diario LTR           | Todos los días | 366                |
| 5 años diarios             | Todos los días | 1830               |
| 7 años de SERVICIO semanal | Semanal        | 370                |
| 10 años cada mes LTR       | Mensual        | 120                |

- Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. En el menú desplegable Configuración, haga clic en **Directivas > Crear directiva**.
3. En la sección Policy Details, especifique el nombre de la política.
4. En la sección Retention, seleccione uno de los tipos de retención y especifique la cantidad de backups que desea retener.
5. Seleccione Primary o Secondary como origen de almacenamiento de backup.
6. (Opcional) Si desea mover copias de seguridad del almacén de objetos al almacenamiento de archivado después de un determinado número de días para la optimización de costes, seleccione la casilla de verificación **copias de seguridad de nivel a archivado**.

Es posible mover backups de un almacén de objetos a un almacenamiento de archivado solo si utiliza ONTAP 9.10.1 o una versión posterior, y Amazon Web Services o Azure como proveedor de cloud. Debe configurar el nivel de acceso de archivado para cada proveedor de cloud.

7. Haga clic en **Crear**.

Puede editar, copiar y eliminar las políticas personalizadas.



No se puede editar ni eliminar una directiva asociada a una aplicación.

## Realice backup de los datos de las aplicaciones en las instalaciones en Amazon Web Services

Puede realizar backups de los datos de aplicaciones de ONTAP en Amazon Web Services integrando Cloud Backup para aplicaciones con BlueXP y SnapCenter en las instalaciones.

Puede proteger una o más aplicaciones simultáneamente al cloud mediante una única política.



Sólo puede proteger una aplicación a la vez si utiliza la GUI de BlueXP. Sin embargo, si utiliza API DE REST, puede proteger varias aplicaciones en simultáneo.

### • Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **...** Corresponde a la aplicación y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configure el clúster de ONTAP que aloja la SVM en la que se ejecuta la aplicación. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

- a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.
- b. En el asistente Agregar entorno de trabajo:
  - i. Especifique la dirección IP del clúster de ONTAP.
  - ii. Especifique las credenciales de administración.

Cloud Backup para aplicaciones solo admite administradores de clústeres.

- c. Haga clic en **Agregar entorno de trabajo**.

5. Seleccione **Amazon Web Services** como proveedor de la nube.
  - a. Especifique la cuenta de AWS.
  - b. En el campo AWS Access Key, especifique la clave.
  - c. En el campo AWS Secret Key, especifique la contraseña.
  - d. Seleccione la región en la que desea crear los backups.
  - e. Especifique el espacio de IP.
  - f. Seleccione el nivel de archivado.

Se recomienda configurar el nivel de archivado porque se trata de una actividad única y no se le permitirá configurarla más adelante.

6. Revise los detalles y haga clic en **Activar copia de seguridad**.

## Realice backups de los datos de las aplicaciones en las instalaciones en Microsoft Azure

Puede realizar backups de los datos de aplicaciones de ONTAP en Microsoft Azure mediante la integración de Cloud Backup para aplicaciones con BlueXP y SnapCenter en las instalaciones.

Puede proteger una o más aplicaciones simultáneamente al cloud mediante una única política.



Sólo puede proteger una aplicación a la vez si utiliza la GUI de BlueXP. Sin embargo, si utiliza API DE REST, puede proteger varias aplicaciones en simultáneo.

### • Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **...** Corresponde a la aplicación y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configure el clúster de ONTAP que aloja la SVM en la que se ejecuta la aplicación. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

- a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.
- b. En el asistente Agregar entorno de trabajo:
  - i. Especifique la dirección IP del clúster de ONTAP.
  - ii. Especifique las credenciales de administración.

Cloud Backup para aplicaciones solo admite administradores de clústeres.

- c. Haga clic en **Agregar entorno de trabajo**.

5. Seleccione **Microsoft Azure** como proveedor de cloud.

- a. Especifique el ID de suscripción de Azure.
- b. Seleccione la región en la que desea crear los backups.
- c. Cree un grupo de recursos nuevo o utilice un grupo de recursos existente.
- d. Especifique el espacio de IP.
- e. Seleccione el nivel de archivado.

Se recomienda configurar el nivel de archivado porque se trata de una actividad única y no se le permitirá configurarla más adelante.

6. Revise los detalles y haga clic en **Activar copia de seguridad**.



# Realice backups de los datos de las aplicaciones en las instalaciones en Google Cloud Platform

Puede realizar backups de los datos de aplicaciones de ONTAP a Google Cloud Platform integrando Cloud Backup para aplicaciones con Cloud Manager y SnapCenter en las instalaciones.

Puede proteger una o más aplicaciones simultáneamente al cloud mediante una única política.



Sólo puede proteger una aplicación a la vez si utiliza la GUI de BlueXP. Sin embargo, si utiliza API DE REST, puede proteger varias aplicaciones en simultáneo.

## • Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **...** Corresponde a la aplicación y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configure el clúster de ONTAP que aloja la SVM en la que se ejecuta la aplicación. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

- a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.
- b. En el asistente Agregar entorno de trabajo:
  - i. Especifique la dirección IP del clúster de ONTAP.
  - ii. Especifique las credenciales de administración.

Cloud Backup para aplicaciones solo admite administradores de clústeres.

- c. Haga clic en **Agregar entorno de trabajo**.
5. Seleccione **Google Cloud Platform** como proveedor de cloud.
    - a. Seleccione Google Cloud Project en el que desea que se cree el bloque de Google Cloud Storage para realizar backups.
    - b. En el campo Google Cloud Access Key, especifique la clave.
    - c. En el campo Google Cloud Secret Key, especifique la contraseña.
    - d. Seleccione la región en la que desea crear los backups.
    - e. Especifique el espacio de IP.
  6. Revise los detalles y haga clic en **Activar copia de seguridad**.

# Realice backups de los datos de las aplicaciones en las instalaciones en StorageGRID

Puede realizar backups de los datos de aplicaciones de ONTAP en StorageGRID integrando Cloud Backup para aplicaciones con BlueXP y SnapCenter en las

instalaciones.

Puede proteger una o varias aplicaciones simultáneamente a StorageGRID mediante una sola política.



Sólo puede proteger una aplicación a la vez si utiliza la GUI de BlueXP. Sin embargo, si utiliza API DE REST, puede proteger varias aplicaciones en simultáneo.

## Lo que necesitará

Al realizar una copia de seguridad de datos en StorageGRID, debe haber un conector disponible en las instalaciones. Tendrá que instalar un conector nuevo o asegurarse de que el conector seleccionado actualmente reside en las instalaciones. El conector se puede instalar en un sitio con o sin acceso a Internet.

Para obtener más información, consulte ["Crear conectores para StorageGRID"](#).

### • Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **...** Corresponde a la aplicación y haga clic en **Activar copia de seguridad**.
3. En la página asignar directiva, seleccione la directiva y haga clic en **Siguiente**.
4. Agregue el entorno de trabajo.

Configure el clúster de ONTAP que aloja la SVM en la que se ejecuta la aplicación. Tras agregar el entorno de trabajo para una de las aplicaciones, se puede reutilizar para todas las demás aplicaciones que residen en el mismo clúster de ONTAP.

a. Seleccione la SVM y haga clic en **Agregar entorno de trabajo**.

b. En el asistente Agregar entorno de trabajo:

- i. Especifique la dirección IP del clúster de ONTAP.
- ii. Especifique las credenciales de administración.

Cloud Backup para aplicaciones solo admite administradores de clústeres.

c. Haga clic en **Agregar entorno de trabajo**.

### 5. Seleccione **StorageGRID**.

- a. Especifique el FQDN del servidor StorageGRID y el puerto en el que se está ejecutando el servidor StorageGRID.

Introduzca los detalles en el formato FQDN:PORT.

b. En el campo Access Key, especifique la clave.

c. En el campo Secret Key, especifique la contraseña.

d. Especifique el espacio de IP.

### 6. Revise los detalles y haga clic en **Activar copia de seguridad**.

## Gestione la protección de aplicaciones

Puede gestionar la protección de aplicaciones realizando diferentes operaciones desde

la interfaz de usuario de BlueXP.

## Ver políticas

Puede ver todas las políticas. Para cada una de estas políticas, al ver los detalles, se muestran todas las aplicaciones asociadas.

1. Haga clic en **copia de seguridad y recuperación > aplicaciones**.
2. En el menú desplegable **Configuración**, haga clic en **Directivas**.
3. Haga clic en **Ver detalles** correspondiente a la directiva cuyos detalles desea ver.

Se muestran las aplicaciones asociadas.



No se puede editar ni eliminar una directiva asociada a una aplicación.

También puede ver políticas de SnapCenter ampliadas para la nube, ejecutando el `Get-SmResources` Cmdlet SnapCenter. La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help nombre_comando`. Como alternativa, también puede consultar el ["Guía de referencia de cmdlets de SnapCenter Software"](#).

## Ver backups en el cloud

Puede ver los backups en la nube en la interfaz de usuario de BlueXP.

1. Haga clic en **copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **...** Corresponde a la aplicación y haga clic en **Ver detalles**.



El tiempo que se tarda en enumerar los backups depende del programa de replicación predeterminado de ONTAP (máximo de 1 hora) y BlueXP (máximo de 6 horas).

- Para las bases de datos de Oracle, tanto los backups de datos como los de registros, se muestra el número SCN de cada backup, la fecha de finalización de cada backup. Puede seleccionar solo el backup de datos y restaurar la base de datos en el servidor de SnapCenter en las instalaciones.
- Para las bases de datos de Microsoft SQL Server, solo se muestran los backups completos y la fecha de finalización de cada backup. Puede seleccionar el backup y restaurar la base de datos en el servidor de SnapCenter en las instalaciones.
- Para la instancia de Microsoft SQL Server, los backups no se enumeran en su lugar solo las bases de datos incluidas en esa instancia.
- Para las bases de datos SAP HANA, solo se muestran los backups de datos y la fecha de finalización de cada backup. Puede seleccionar el backup y realizar una operación de montaje.



Los backups creados antes de habilitar la protección cloud no se enumeran para la restauración.

También puede ver estos backups ejecutando el `Get-SmBackup` Cmdlet SnapCenter. La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help nombre_comando`. Como alternativa, también puede consultar el ["Guía de referencia de cmdlets de SnapCenter Software"](#).

## Cambio del diseño de la base de datos

Cuando se añaden volúmenes a la base de datos, el servidor SnapCenter etiqueta automáticamente las copias de Snapshot en los nuevos volúmenes según la política y la programación. Estos volúmenes nuevos no tendrán el extremo de almacén de objetos y debe actualizar mediante la ejecución de los siguientes pasos:

1. Haga clic en **copia de seguridad y recuperación > aplicaciones**.
2. En el menú desplegable **Configuración**, haga clic en **servidores SnapCenter**.
3. Haga clic en **...** Corresponde al servidor SnapCenter que aloja la aplicación y haga clic en **Actualizar**.

Se detectan los volúmenes nuevos.

4. Haga clic en **...** Correspondiente a la aplicación y haga clic en **Actualizar protección** para activar la protección en nube para el nuevo volumen.

Si un volumen de almacenamiento se elimina de la aplicación después de configurar el servicio en cloud, para los backups nuevos, SnapCenter Server solo etiquetará las snapshots en las que reside la aplicación. Si el volumen eliminado no lo utiliza ninguna otra aplicación, debe eliminar manualmente la relación de almacén de objetos. Si actualiza el inventario de aplicaciones, este contendrá la distribución de almacenamiento actual de la aplicación.

## Cambio de política o grupo de recursos

Si existe un cambio en la política o el grupo de recursos de SnapCenter, se debe actualizar la protección.

1. Haga clic en **copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **...** Corresponde a la aplicación y haga clic en **Actualizar protección**.

## Cancele el registro del servidor SnapCenter

1. Haga clic en **copia de seguridad y recuperación > aplicaciones**.
2. En el menú desplegable **Configuración**, haga clic en **servidores SnapCenter**.
3. Haga clic en **...** Corresponde al servidor SnapCenter y haga clic en **Unregister**.

## Supervisar trabajos

Se crean trabajos para todas las operaciones de backup en el cloud. Puede supervisar todos los trabajos y todas las subtareas que se realizan como parte de cada tarea.

1. Haga clic en **copia de seguridad y recuperación > Supervisión de trabajos**.

Al iniciar una operación, aparece una ventana que indica que el trabajo se ha iniciado. Puede hacer clic en el enlace para supervisar el trabajo.

2. Haga clic en la tarea principal para ver las subtareas y el estado de cada una de estas subtareas.

## Establecer el espacio IP del entorno de trabajo principal

Si desea restaurar o montar un backup que se haya movido a almacén de objetos desde un almacenamiento secundario, debe añadir los detalles del entorno de trabajo principal y establecer el espacio de IP.

- Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **almacenamiento > Canvas > Mis entornos de trabajo > Agregar entorno de trabajo**.
2. Especifique los detalles del entorno de trabajo principal y haga clic en **Agregar**.
3. Haga clic en **copia de seguridad y recuperación > volúmenes**.
4. Haga clic en **...** Corresponde a cualquiera de los volúmenes y haga clic en **Detalles**.
5. Haga clic en **...** Corresponde a la copia de seguridad y haga clic en **Restaurar**.
6. En el asistente, seleccione el entorno de trabajo principal recién añadido como destino.
7. Especifique el espacio de IP.

## Configurar los certificados de CA

Si tiene certificados de CA, debe copiar manualmente los certificados de CA raíz en el equipo conector.

Sin embargo, si no tiene certificados de CA, puede continuar sin configurar los certificados de CA.

### • Pasos\*

1. Copie el certificado en el volumen al que se puede acceder desde el agente docker.

- `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_certs`
- `chmod 777 sc_certs`

2. Copie los archivos de certificado de RootCA en la carpeta anterior de la máquina del conector.

```
cp <path on connector>/<filename>
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs
```

3. Copie el archivo CRL en el volumen al que se puede acceder desde el agente docker.

- `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_crl`
- `chmod 777 sc_crl`

4. Copie los archivos CRL en la carpeta anterior del equipo del conector.

```
cp <path on connector>/<filename>
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_crl
```

5. Después de copiar los certificados y los archivos CRL, reinicie el servicio copia de seguridad en la nube para aplicaciones.

- `sudo docker exec cloudmanager_snapcenter sed -i 's/skipSCCertValidation: true/skipSCCertValidation: false/g' /opt/netapp/cloudmanager-snapcenter-agent/config/config.yml`
- `sudo docker restart cloudmanager_snapcenter`

## Restaurar los datos de las aplicaciones en las instalaciones

## Restaurar base de datos de Oracle

Solo puede restaurar la base de datos de Oracle en el mismo host de servidor de SnapCenter, la misma SVM o en el mismo host de base de datos. Para una base de datos de RAC, los datos se restauran en el nodo local donde se creó el backup.



Se admite la restauración de backups secundarios mediante el almacenamiento primario.

Solo es compatible una base de datos completa con restauración de archivos de control. Si los registros de archivo no están presentes en el AFS, debe especificar la ubicación que contiene los registros de archivo necesarios para la recuperación.



No se admite la restauración de archivos individuales (SFR).

### Lo que necesitará

Si desea restaurar una copia de seguridad que se haya movido a almacén de objetos desde almacenamiento secundario, debe añadir los detalles del entorno de trabajo principal y establecer el espacio de IP. Para obtener más información, consulte ["Establecer el espacio IP del entorno de trabajo principal"](#).

#### • Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. En el campo **filtro por**, seleccione el filtro **Tipo** y, en la lista desplegable, seleccione **Oracle**.
3. Haga clic en **Ver detalles** correspondiente a la base de datos que desea restaurar y haga clic en **Restaurar**.
4. En la página Restore Type, realice las siguientes acciones:
  - a. Seleccione **Estado de la base de datos** si desea cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.

Los distintos estados de una base de datos, del más alto al más bajo, son open, mounted, started y shutdown. Debe seleccionar esta casilla de comprobación si la base de datos está en un estado más alto, pero el estado debe cambiarse a un estado más bajo para realizar una operación de restauración. Si la base de datos está en un estado más bajo, pero el estado debe cambiarse a uno más alto para realizar la operación de restauración, el estado de la base de datos se modifica automáticamente aunque no seleccione la casilla de comprobación.

Si una base de datos está en el estado open y, para restaurarla, la base de datos necesita que esté en el estado mounted, el estado de la base de datos se modifica únicamente si selecciona esta casilla de comprobación.

- a. Seleccione **Archivos de control** si desea restaurar el archivo de control junto con la base de datos completa.
- b. Si la instantánea se encuentra en el almacenamiento de archivado, especifique la prioridad de restauración de los datos desde el almacenamiento de archivado.
  1. En la página Recovery Scope, realice las siguientes acciones:
- c. Especifique el alcance de recuperación.

| Si...   | Realice lo siguiente...  |
|---|--|
| Desea recuperar la última transacción                                   | Seleccione <b>todos los registros</b> .  |
| Desea recuperar a un número de cambio de sistema (SCN) específico       | Seleccione <b>Until SCN (System Change Number)</b> .   |
| Desea recuperar a una fecha y una hora específicas                      | Seleccione <b>Fecha y hora</b> .<br><br>Debe especificar la fecha y la hora de la zona horaria del host de la base de datos.                                   |
| No desea recuperar  | Seleccione <b>sin recuperación</b> .   |
| Desea especificar cualquier ubicación de registros de archivos externos | Si los registros de archivo no están presentes en el AFS, debe especificar la ubicación que contiene los registros de archivo necesarios para la recuperación. |

- d. Seleccione la casilla de comprobación si desea abrir la base de datos después de la recuperación.

En una configuración de RAC, solo la instancia de RAC que se usa para la recuperación se abre después de esta.

1. Revise los detalles y haga clic en **Restaurar**.

## Restaurar base de datos de SQL Server

Es posible restaurar la base de datos de SQL Server en el mismo host o en el host alternativo. No se admiten la recuperación de backups de registros ni la propagación de grupos de disponibilidad.



**IMPORTANTE:** Se admite la restauración de backups secundarios mediante el almacenamiento primario.



No se admite la restauración de archivos individuales (SFR).


### Lo que necesitará

Si desea restaurar una copia de seguridad que se haya movido a almacén de objetos desde almacenamiento secundario, debe añadir los detalles del entorno de trabajo principal y establecer el espacio de IP. Para obtener más información, consulte ["Establecer el espacio IP del entorno de trabajo principal"](#).

#### • Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. En el campo **filtro por**, seleccione el filtro **Tipo** y, en la lista desplegable, seleccione **SQL**.
3. Haga clic en **Ver detalles** para ver todas las copias de seguridad disponibles.

4. Seleccione la copia de seguridad y haga clic en **Restaurar**.
5. Seleccione la ubicación en la que desea restaurar los archivos de la base de datos.

| Opción  | Descripción   |
|---|---|
| Restablezca la base de datos en el mismo host en el que se creó el backup | Seleccione esta opción si desea restaurar la base de datos en la misma instancia de SQL Server donde se realizan los backups.   |
| Restaurar la base de datos en un host alternativo                         | <p>Seleccione esta opción si desea que la base de datos se restaure en un servidor SQL diferente en el mismo host o diferente donde se realizan los backups.</p> <p>Seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración.</p> <div style="display: flex; align-items: center;">  <div> <p>La extensión de archivo proporcionada en la ruta alternativa debe ser la misma que la del archivo de base de datos original.</p> </div> </div> <p>Si la opción <b>Restaurar la base de datos a un host alternativo</b> no aparece en la página Restaurar ámbito, borre la memoria caché del explorador.</p> |

6. Si la instantánea se encuentra en el almacenamiento de archivado, especifique la prioridad de restauración de los datos desde el almacenamiento de archivado.
7. En la página **Opciones previas a la restauración**, seleccione una de las siguientes opciones:
  - Seleccione **Sobrescribir la base de datos con el mismo nombre durante la restauración** para restaurar la base de datos con el mismo nombre.
  - Seleccione **mantener la configuración de replicación de bases de datos SQL** para restaurar la base de datos y mantener la configuración de replicación existente.
8. En la página **Opciones de posrestauración**, para especificar el estado de la base de datos para restaurar registros transaccionales adicionales, seleccione una de las siguientes opciones:
  - Seleccione **operativo, pero no disponible** si está restaurando todas las copias de seguridad necesarias ahora.
 

Este es el comportamiento predeterminado, que deja la base de datos preparada para su uso revirtiendo las transacciones no comprometidas. No podrá restaurar registros de transacciones adicionales hasta que cree un backup.
  - Seleccione **no operativo, pero disponible** para dejar la base de datos no operativa sin revertir las transacciones no comprometidas.
 

Pueden restaurarse registros de transacciones adicionales. No podrá utilizar la base de datos hasta que esta se recupere.



- Seleccione **modo de sólo lectura y disponible** para dejar la base de datos en modo de sólo lectura.

Esta opción deshace las transacciones no comprometidas, pero guarda las acciones deshechas en un archivo en espera para que puedan revertirse los efectos de recuperación.

Si se habilita la opción Undo directory, se restauran más registros de transacciones. Si la operación de restauración para el registro de transacciones no se realiza correctamente, pueden revertirse los cambios. La documentación de SQL Server contiene más información.

1. Revise los detalles y haga clic en **Restaurar**.

## Montar backups de aplicaciones

SnapCenter no admite la restauración de backups de Oracle y HANA en un host alternativo. Así, el backup en cloud para aplicaciones le permite montar los backups de Oracle y HANA en el host determinado.

### Lo que necesitará

Si desea montar una copia de seguridad que se haya movido a almacén de objetos desde un almacenamiento secundario, debe añadir los detalles del entorno de trabajo principal y establecer el espacio de IP. Para obtener más información, consulte ["Establecer el espacio IP del entorno de trabajo principal"](#).

- Pasos\*

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. En el campo Filter by (filtro por), seleccione **Type** (Tipo) y, en la lista desplegable, seleccione **SAP HANA** o **Oracle**.
3. Haga clic en **...** Corresponde a la aplicación protegida y selecciona **Ver detalles**.
4. Haga clic en **...** Corresponde a la copia de seguridad y selecciona **Mount**.
  - a. Especifique una de las siguientes opciones:
    - i. Para el entorno NAS, especifique el FQDN o la dirección IP del host al cual se van a exportar los volúmenes alternativos restaurados a partir del almacén de objetos.
    - ii. Para el entorno SAN, especifique los iniciadores del host al cual se asignarán las LUN de un volumen alternativo restaurado en el almacén de objetos.
  - b. Especifique el sufijo que se añadirá al nombre del volumen alternativo.
  - c. Si la instantánea se encuentra en el almacenamiento de archivado, especifique la prioridad para recuperar los datos del almacenamiento de archivado.
  - d. Haga clic en **Mount**.

Esta operación monta solo el almacenamiento en el host especificado. Debe montar manualmente el sistema de archivos y activar la base de datos. Después de utilizar el volumen alternativo, el administrador de almacenamiento puede eliminar el volumen del clúster de ONTAP.

Para obtener información sobre cómo preparar la base de datos SAP HANA, consulte ["TR-4667: Automatización de las operaciones de copia y clonado del sistema SAP HANA con SnapCenter"](#).

## Información de copyright

Copyright © 2023 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.