



# **Proteja los datos de aplicaciones nativas en el cloud**

## **Cloud Backup**

NetApp  
March 06, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-backup-restore/azure/concept-protect-cloud-app-data-to-cloud.html> on March 06, 2023. Always check docs.netapp.com for the latest.

# Tabla de Contenido

- Proteja los datos de aplicaciones nativas en el cloud ..... 1
  - Proteja los datos de aplicaciones nativas del cloud..... 1
  - Realice backups de datos de aplicaciones nativas en el cloud ..... 5
  - Restaure los datos de aplicaciones nativas en el cloud..... 20
  - Clone datos de aplicaciones nativas en el cloud ..... 23
  - Gestione la protección de datos de aplicaciones nativas en el cloud ..... 31

# Proteja los datos de aplicaciones nativas en el cloud

## Proteja los datos de aplicaciones nativas del cloud

Cloud Backup para aplicaciones es un servicio basado en SaaS que proporciona funcionalidades de protección de datos para aplicaciones que se ejecutan en el almacenamiento en cloud de NetApp. Cloud Backup para aplicaciones habilitado en BlueXP (anteriormente Cloud Manager) ofrece protección eficiente, coherente con las aplicaciones y basada en políticas de las siguientes aplicaciones:

- Bases de datos de Oracle que residen en Amazon FSX para ONTAP y Cloud Volumes ONTAP de NetApp
- Sistemas SAP HANA que residen en Azure NetApp Files

### Arquitectura

La arquitectura Cloud Backup para aplicaciones incluye los siguientes componentes.

- Cloud Backup para aplicaciones es un conjunto de servicios de protección de datos alojados en NetApp como servicio SaaS y se basa en la plataforma SaaS de BlueXP.

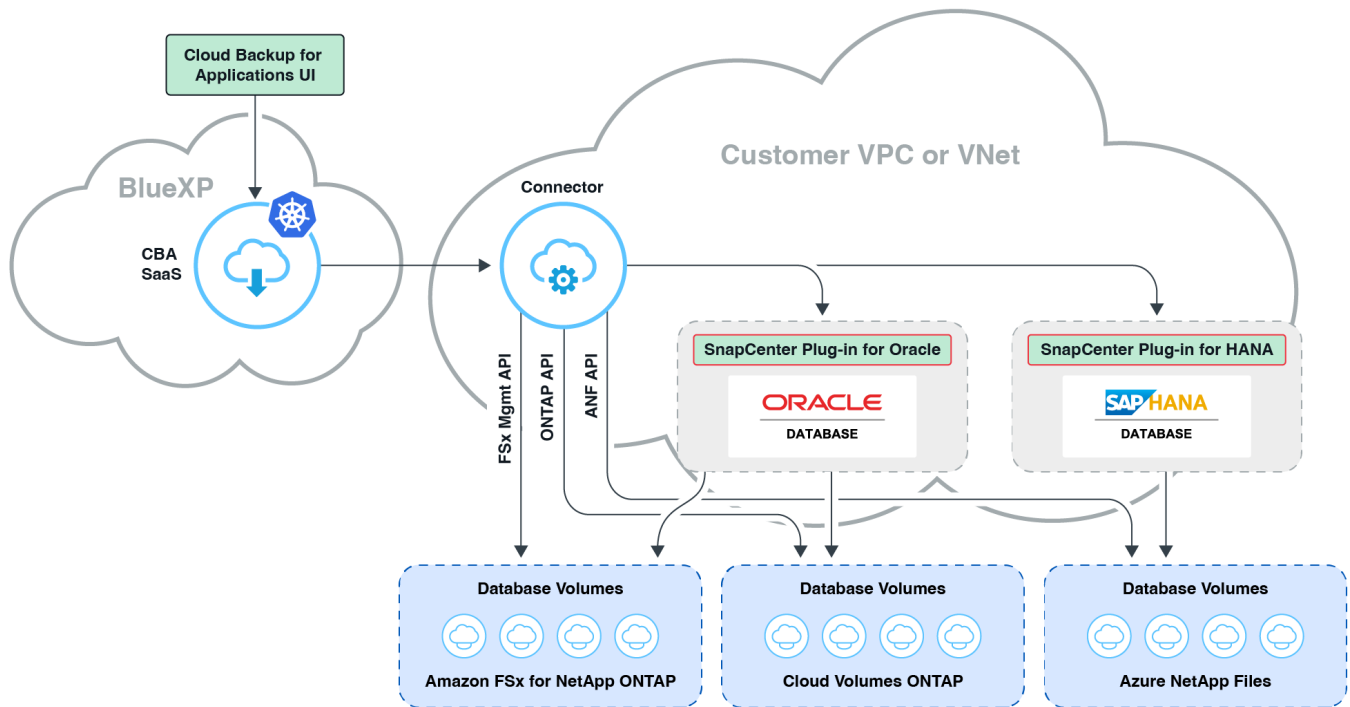
Organiza los flujos de trabajo de protección de datos para aplicaciones que residen en el almacenamiento en cloud de NetApp.

- Se puede acceder a la interfaz de usuario de Cloud Backup para aplicaciones desde la interfaz de usuario de BlueXP.

La interfaz de usuario de Cloud Backup para aplicaciones ofrece funcionalidades de protección de datos para aplicaciones.

- BlueXP Connector es un componente que se ejecuta en la red en nube del usuario e interactúa con los sistemas de almacenamiento y los complementos específicos de aplicaciones.
- El plugin específico de la aplicación es un componente que se ejecuta en cada host de la aplicación e interactúa con las bases de datos que se ejecutan en el host mientras se ejecutan operaciones de protección de datos.

La siguiente imagen muestra cada componente y las conexiones que necesita preparar entre ellos:



Para cualquier solicitud iniciada por el usuario, la interfaz de usuario de Cloud Backup para aplicaciones se comunica con el SaaS BlueXP, que al validar los procesos de solicitud son los mismos. Si se solicita que se ejecute un flujo de trabajo como un backup, una restauración o un clon, el servicio SaaS inicia el flujo de trabajo y, cuando sea necesario, reenvía la llamada al conector BlueXP. A continuación, el conector se comunica con el sistema de almacenamiento y el complemento específico de la aplicación como parte de la ejecución de las tareas del flujo de trabajo.

El conector puede ponerse en marcha en el mismo VPC o vnet que las de las aplicaciones, o en uno diferente. Si el conector y las aplicaciones están en una red diferente, debe establecer una conectividad de red entre ellos.



Un único conector BlueXP puede comunicarse con varios sistemas de almacenamiento y múltiples complementos de aplicaciones. Necesitará un único conector para gestionar sus aplicaciones siempre que haya conectividad entre el conector y los hosts de aplicaciones.



La infraestructura de Cloud Backup para aplicaciones SaaS es resiliente a fallos de zonas de disponibilidad dentro de una región. Soporta fallos regionales al conmutar por error a una región nueva y esta conmutación por error implica un tiempo de inactividad de unas 2 horas.

## Proteja la base de datos de Oracle

### Configuraciones admitidas

- Sistema operativo:
  - RHEL 7.5 o posterior y 8.x
  - OL 7.5 o posterior y 8.x.
- Sistema de almacenamiento:
  - Amazon FSX para ONTAP

- Cloud Volumes ONTAP
- Distribución de almacenamiento:
  - NFS v3 y v4.1 (incluido dNFS)
  - iSCSI con ASM (ASMFD, ASMLib y ASMUdev)
- Distribución de bases de datos: Oracle Standard y Oracle Enterprise Standalone (CDB heredado y multitenant y PDB)
- Versiones de base de datos: 12cR2, 18c, 19c y 21c

## Funciones

- Añada el host y ponga en marcha el plugin

Es posible poner en marcha el plugin de forma manual, mediante script o de forma automática.

- Detección automática de las bases de datos Oracle
- Realizar backups de bases de datos de Oracle
  - Backup completo (datos + control + archivos de registro de archivo)
  - Backup bajo demanda
  - Backup programado basado en las políticas definidas por el sistema o personalizadas

Puede especificar diferentes frecuencias de programación, como por ejemplo, cada hora, día, semana o mes en la política.

- Retención de backups según la política
- Restaurar una base de datos de Oracle completa (archivos de datos + archivo de control) desde la copia de seguridad especificada
- Restaurar únicamente los archivos de datos y los archivos de control desde el backup especificado
- Recuperación de la base de datos de Oracle con Until SCN, Until Time, todos los registros disponibles y las opciones de recuperación no
- Clonado de bases de datos de Oracle en hosts de origen o destino alternativo
  - Clon básico con un solo clic
  - Clonado avanzado usando el archivo de especificación del clon personalizado
  - El nombre de las entidades clonadas puede generarse automáticamente o ser idéntico al origen
  - Ver la jerarquía de clones
  - Eliminación de bases de datos clonadas
- Supervisar backups, restauraciones, clones y otros trabajos
- Mostrar el resumen de protección en el tablero de a bordo
- Enviar alertas por correo electrónico

## Limitaciones

- No es compatible con Oracle 11g
- No admite las operaciones de montaje, catálogo y verificación en backups
- No es compatible con Oracle en RAC y Data Guard

- Para alta disponibilidad de Cloud Volumes ONTAP, solo se utiliza una de las IP de interfaz de red. Si la conectividad de la IP se desactiva o si no puede acceder a la IP, se produce un error en las operaciones.
- Las direcciones IP de la interfaz de red de Amazon FSX para ONTAP de NetApp o Cloud Volumes ONTAP deben ser únicas en la cuenta y región de BlueXP.

## Proteja la base de datos SAP HANA

### Configuraciones admitidas

- Sistema operativo:
  - RHEL 7.5 o posterior, plataformas 8.x certificadas por SAP HANA
  - SLES 12 SP5 o posteriores y 15 plataformas SPX certificadas por SAP HANA
- Sistema de almacenamiento: Azure NetApp Files
- Disposiciones de almacenamiento: Para datos y registros, Azure solo admite NFSv4.1.
- Diseños de base de datos:
  - Contenedor único versión 1.0SPS12
  - Contenedor de bases de datos multitenant (MDC) SAP HANA 2.0SPS4, 2.0SPS5, 2.0SPS6 con uno o varios inquilinos
  - Sistema host único SAP HANA, varios sistemas host SAP HANA (sin un host en espera), replicación de sistemas HANA
- Plugin de SAP HANA en el host de la base de datos

### Funciones

- Añada manualmente sistemas SAP HANA
- Realizar un backup de las bases de datos SAP HANA
  - Backup bajo demanda (basado en ficheros y en copias Snapshot)
  - Backup programado basado en las políticas definidas por el sistema o personalizadas

Puede especificar diferentes frecuencias de programación, como por ejemplo, cada hora, día, semana o mes en la política.

  - Detección de la replicación de sistemas HANA (HSR)
- Retención de backups según la política
- Restaure toda la base de datos SAP HANA desde el backup especificado
- Realizar backups y restaurar volúmenes no Data de HANA y volúmenes no Data globales
- Compatibilidad con scripts previos y posteriores mediante variables del entorno para las operaciones de backup y restauración
- Creación de un plan de acción para situaciones de error mediante la opción pre-exit

### Limitaciones

- Para la configuración de HSR, solo se admite HSR de 2 nodos (1 principal y 1 secundario)
- La retención no se activará si el script posterior falla durante la operación de restauración

# Realice backups de datos de aplicaciones nativas en el cloud

## Realice backup de bases de datos de Oracle nativas en el cloud

### Acceda a BlueXP

Usted debe ["Regístrese en la página web de NetApp BlueXP"](#), ["Inicie sesión en BlueXP"](#) y, a continuación, configure un ["Cuenta de NetApp"](#).

### Configure FSX para ONTAP

Debe crear el entorno de trabajo FSX para ONTAP y el conector.

#### Crear un entorno de trabajo FSX para ONTAP

Debe crear los entornos de trabajo de Amazon FSX para ONTAP donde se alojan las bases de datos. Para obtener más información, consulte ["Comience a utilizar Amazon FSX para ONTAP"](#) y.. ["Crear y gestionar un entorno de trabajo de Amazon FSX para ONTAP"](#).

Puede crear FSX de NetApp con BlueXP o AWS. Si ha creado utilizando AWS, debe descubrir el FSX para sistemas ONTAP en BlueXP.

#### Cree un conector

Un administrador de cuentas tiene que poner en marcha un conector en AWS que permita a BlueXP gestionar recursos y procesos dentro de su entorno de cloud público.

Para obtener más información, consulte ["Creación de un conector en AWS desde BlueXP"](#).

- Debe utilizar el mismo conector para administrar tanto el entorno de trabajo FSX como las bases de datos Oracle.
- Si tiene el entorno de trabajo FSX y las bases de datos de Oracle en el mismo VPC, puede implementar el conector en el mismo VPC.
- Si tiene el entorno de trabajo FSX y las bases de datos Oracle en distintos equipos virtuales:
  - Si tiene cargas de trabajo NAS (NFS) configuradas en FSX, puede crear el conector en cualquiera de los VPC.
  - Si solo tiene configuradas las cargas de trabajo SAN y no tiene previsto utilizar ninguna carga de trabajo NAS (NFS), debe crear el conector en el VPC donde se crea el sistema FSX.



Para usar las cargas de trabajo NAS (NFS), debe tener una pasarela de tránsito entre el VPC de la base de datos de Oracle y FSX VPC. A la dirección IP de NFS, que es una dirección IP flotante, se puede acceder desde otro VPC, solo mediante una puerta de enlace de tránsito. No podemos acceder a las direcciones IP flotantes mediante la asociación de las VPC.

Después de crear el conector, haga clic en **almacenamiento > Canvas > Mis entornos de trabajo > Agregar entorno de trabajo** y siga las indicaciones para agregar el entorno de trabajo. Asegúrese de que existe conectividad entre el conector y los hosts de la base de datos Oracle y el entorno de trabajo FSX. El conector debe poder conectarse a la dirección IP de administración del clúster del entorno de trabajo FSX.



Después de crear el conector, haga clic en **conector > gestionar conectores**; seleccione el nombre del conector y copie el ID del conector.

## Configure Cloud Volumes ONTAP

Debe crear el entorno de trabajo de Cloud Volumes ONTAP y el conector.

### Crear el entorno de trabajo de Cloud Volumes ONTAP

Puede descubrir y agregar sistemas Cloud Volumes ONTAP existentes a BlueXP. Para obtener más información, consulte ["Adición de sistemas Cloud Volumes ONTAP existentes a BlueXP"](#).

### Cree un conector

Puede empezar a usar Cloud Volumes ONTAP para su entorno de cloud en unos pasos. Para obtener información, consulte una de las siguientes indicaciones:

- ["Inicio rápido para Cloud Volumes ONTAP en AWS"](#)
- ["Inicio rápido para Cloud Volumes ONTAP en Azure"](#)
- ["Inicio rápido de Cloud Volumes ONTAP en Google Cloud"](#)

Debe utilizar el mismo conector para gestionar tanto el entorno de trabajo CVO como las bases de datos Oracle.

- Si tiene el entorno de trabajo de CVO y las bases de datos de Oracle en el mismo VPC o vnet, puede implementar el conector en el mismo VPC o vnet.
- Si tiene el entorno de trabajo de CVO y las bases de datos de Oracle en distintos equipos virtuales o Nets, asegúrese de que los equipos VPC o VNets tienen una relación entre iguales.

## Ponga en marcha el plugin de SnapCenter para Oracle y añada hosts de base de datos

Es necesario implementar el plugin de SnapCenter para Oracle en cada uno de los hosts de la base de datos Oracle, añadir los hosts de la base de datos y detectar las bases de datos en el host para asignar políticas y crear backups.

- Si SSH está habilitado para el host de base de datos, es posible implementar el plugin mediante uno de los métodos:
  - Implemente el plugin y añada el host de la interfaz de usuario mediante la opción SSH. [Leer más.](#)
  - Ponga en marcha el plugin mediante script y añada el host desde la interfaz de usuario mediante la opción manual. [Leer más.](#)
- Si SSH está deshabilitado, implemente el plugin manualmente y añada el host desde la interfaz de usuario mediante la opción manual. [Leer más.](#)

### Requisitos previos

Antes de añadir el host, debe asegurarse de que se cumplan los requisitos previos.

- Debe haber creado el entorno de trabajo y el conector.
- Asegúrese de que el conector tiene conectividad con el entorno de trabajo y los hosts de bases de datos Oracle.



- Asegúrese de que el usuario de BlueXP tiene la función “Administrador de cuentas”.
- Asegúrese de que Java 11 (64 bits) Oracle Java u OpenJDK estén instalados en cada uno de los hosts de la base de datos de Oracle y QUE LA variable JAVA\_HOME esté configurada correctamente.
- Debe haber creado el usuario de SnapCenter y configurado sudo para el usuario de SnapCenter. Para obtener más información, consulte [Configure sudo para el usuario de SnapCenter](#).
- Asegúrese de que el conector tiene activada la comunicación al puerto SSH (valor predeterminado: 22) si se utiliza la implementación basada en SSH.
- Asegúrese de que el conector tiene la comunicación habilitada para el puerto del plug-in (valor predeterminado: 8145) para que funcionen las operaciones.

## Configure sudo para el usuario de SnapCenter

Debe crear un usuario de SnapCenter y configurar sudo para el usuario.

### • Pasos\*

1. Inicie sesión en el conector VM.
2. Descargue el binario del plugin del host Linux de SnapCenter.  

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Obtenga la ruta de montaje base.  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```
4. Copie las líneas 1 a 16 del archivo **oracle\_checksum\_scs.txt** ubicado en **base\_Mount\_path/version/sc-linux-host-plugin/**.
5. Inicie sesión en el host de la base de datos Oracle y realice los siguientes pasos:
  - a. Cree la cuenta de usuario de SnapCenter, el par de claves privadas y asigne los permisos. Para obtener más información, consulte ["Cree una cuenta de usuario"](#).
  - b. Pegue las líneas copiadas en el paso 4 al archivo **/etc/sudoers** mediante la función visudo de Linux.

En las líneas anteriores, reemplace <LINUXUSER> por el usuario de SnapCenter que ha creado y guarde el archivo en la función visudo.

## Implemente el plugin y añada el host desde la interfaz de usuario mediante la opción SSH

1. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en detectar aplicaciones.
3. Seleccione **nativo de la nube** y haga clic en **Siguiente**.

Se crea una cuenta de servicio con el rol *SnapCenter System* para realizar operaciones de protección de datos programadas para todos los usuarios de esta cuenta.

- Haga clic en **cuenta > Administrar cuenta > Miembros** para ver la cuenta de servicio.



La cuenta de servicio (*SnapCenter-account-**<accountid>***) se utiliza para ejecutar las operaciones de backup programadas. Nunca debe eliminar la cuenta de servicio.

4. En la página Add Host, realice lo siguiente:

- a. Seleccione **usando SSH**.
- b. Especifique el FQDN o la dirección IP del host en el que desea instalar el plugin.
- c. Especifique el nombre de usuario (**Usuario sudo SnapCenter**) mediante el cual se copiará el paquete de plugins en el host.
- d. Especifique el SSH y el puerto del plugin.

El puerto SSH predeterminado es 22 y el puerto del plugin es 8145.

Puede cerrar el puerto SSH en el host de la aplicación después de instalar el plugin. El puerto SSH no es necesario para ninguna otra operación de plugin.

- a. Seleccione el conector.
- b. (Opcional) Si la autenticación sin clave no está habilitada entre el conector y el host, debe especificar la clave privada SSH que se usará para comunicarse con el host.



La clave privada SSH no se almacena en ningún lugar de la aplicación y no se usará en ninguna otra operación.

c. Haga clic en **Siguiente**.

- Muestra todas las bases de datos en el host. Si la autenticación del sistema operativo está desactivada para la base de datos, debe configurar la autenticación de la base de datos haciendo clic en **Configurar**. Para obtener más información, consulte [Configurar las credenciales de la base de datos de Oracle](#).
- Haga clic en **Configuración** y seleccione **hosts** para ver todos los hosts. Haga clic en **Eliminar** para eliminar un host de base de datos.



El filtro para ver un host específico no funciona. Cuando se especifica un nombre de host en el filtro, se muestran todos los hosts.

- Haga clic en **Configuración** y seleccione **Directivas** para ver las directivas preparadas previamente. Revise las directivas predefinidas y, si desea, puede editarlas para cumplir sus requisitos o crear una nueva directiva.

#### Ponga en marcha el plugin mediante script y añada el host desde la interfaz de usuario mediante la opción manual

Si la autenticación basada en claves SSH está habilitada en el host de Oracle para el usuario de SnapCenter, puede realizar los siguientes pasos para implementar el plugin. Antes de realizar los pasos, asegúrese de que la conexión SSH al conector está activada.

##### • Pasos\*

1. Inicie sesión en el conector VM.

2. Obtenga la ruta de montaje base.

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```

3. Despliegue el complemento mediante el script de ayuda incluido en el conector.

```
sudo <base_mount_path>/scripts/oracle_plugin_copy_and_install.sh --host  
<host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port>
```

```
--pluginport <plugin_port> --installdir <install_dir>
```

- Nombre\_host es el nombre del host de Oracle y éste es un parámetro obligatorio.
- ssh\_key\_file es la clave SSH del usuario SnapCenter y se utiliza para conectarse al host Oracle. Este es un parámetro obligatorio.
- User\_name: Usuario de SnapCenter con privilegios SSH en el host de Oracle y este es un parámetro opcional. El valor predeterminado es ec2-user.
- ssh\_Port: Puerto SSH en el host de Oracle y este es un parámetro opcional. El valor predeterminado es 22
- Plugin\_Port: Puerto que utiliza el plugin y este es un parámetro opcional. El valor predeterminado es 8145
- Directorio\_de\_instalación: Directorio donde se va a implementar el complemento y éste es un parámetro opcional. El valor predeterminado es /opt.

Por ejemplo:

```
sudo /var/lib/docker/volumes/service-manager-  
2_cloudmanager_scs_cloud_volume/_data/scripts/oracle_plugin_copy_and_inst  
all.sh --host xxx.xx.x.x --sshkey /keys/netapp-ssh.ppk
```

4. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
5. Haga clic en detectar aplicaciones.
6. Seleccione **nativo de la nube** y haga clic en **Siguiente**.

Se crea una cuenta de servicio con el rol *SnapCenter System* para realizar operaciones de protección de datos programadas para todos los usuarios de esta cuenta.

- Haga clic en **cuenta > Administrar cuenta > Miembros** para ver la cuenta de servicio.



La cuenta de servicio (*SnapCenter-account-<accountid>*) se utiliza para ejecutar las operaciones de backup programadas. Nunca debe eliminar la cuenta de servicio.

7. En la página Add Host, realice lo siguiente:

- a. Seleccione **Manual**.
- b. Especifique el FQDN o la dirección IP del host donde se implementó el plugin.

Asegúrese de que con el FQDN o la dirección IP, el conector puede comunicarse con el host de la base de datos.

- c. Especifique el puerto del plugin.

El puerto predeterminado es 8145.

- d. Seleccione el conector.
- e. Seleccione la casilla de comprobación para confirmar que el plugin está instalado en el host
- f. Haga clic en **detectar aplicaciones**.
  - Muestra todas las bases de datos en el host. Si la autenticación del sistema operativo está desactivada para la base de datos, debe configurar la autenticación de la base de datos haciendo clic en **Configurar**. Para obtener más información, consulte [Configurar las](#)

credenciales de la base de datos de Oracle.

- Haga clic en **Configuración** y seleccione **hosts** para ver todos los hosts. Haga clic en **Eliminar** para eliminar un host de base de datos.



El filtro para ver un host específico no funciona. Cuando se especifica un nombre de host en el filtro, se muestran todos los hosts.

- Haga clic en **Configuración** y seleccione **Directivas** para ver las directivas preparadas previamente. Revise las directivas predefinidas y, si desea, puede editarlas para cumplir sus requisitos o crear una nueva directiva.

#### Implemente el plugin manualmente y añada el host desde la interfaz de usuario mediante la opción manual

Si la autenticación basada en claves SSH no está habilitada en el host de la base de datos de Oracle, debe realizar los siguientes pasos manuales para poner en marcha el plugin y luego añadir el host desde la interfaz de usuario con la opción manual.

##### • Pasos\*

1. Inicie sesión en el conector VM.

2. Descargue el binario del plugin del host Linux de SnapCenter.

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET  
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

3. Obtenga la ruta de montaje base.

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```

4. Obtenga la ruta binaria del plug-in descargado.

```
sudo ls <base_mount_path> $(sudo docker ps|grep -Po  
"cloudmanager_scs_cloud:.*? "|sed -e 's/ *$//'|cut -f2 -d":")/sc-linux-host  
-plugin/snapcenter_linux_host_plugin_scs.bin
```

5. Copie *snapcenter\_linux\_host\_plugin\_scs.bin* a cada uno de los hosts de la base de datos Oracle con *scp* u otros métodos alternativos.

El *snapcenter\_linux\_host\_plugin\_scs.bin* debe copiarse a una ubicación a la que el usuario de SnapCenter puede acceder.

6. Inicie sesión en el host de la base de datos Oracle utilizando la cuenta de usuario de SnapCenter y ejecute el siguiente comando para habilitar los permisos de ejecución para el archivo binario.

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```

7. Implemente el plugin de Oracle como usuario sudo SnapCenter.

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<snapcenter  
-user>
```

8. Copie *certificate.p12* de *<base\_mount\_path>/client/certificate/* la ruta del conector VM a */var/opt/snapcenter/spl/etc/* en el host del plugin.

9. Desplácese hasta */var/opt/snapcenter/spl/etc* y ejecute el comando *keytool* para importar el certificado.

```
keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12  
-destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter  
-deststorepass snapcenter -srccalias agentcert -destalias agentcert -noprompt
```

10. Reinicie SPL: `systemctl restart spl`

11. Valide que es posible acceder al plugin desde el conector ejecutando el comando siguiente desde el conector.  

```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the  
plug-in host>:<plug-in port>/getVersion --cert  
/config/client/certificate/certificate.pem --key  
/config/client/certificate/key.pem
```
12. En la interfaz de usuario de BlueXP, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
13. Haga clic en detectar aplicaciones.
14. Seleccione **nativo de la nube** y haga clic en **Siguiente**.

Se crea una cuenta de servicio con el rol *SnapCenter System* para realizar operaciones de protección de datos programadas para todos los usuarios de esta cuenta.

- Haga clic en **cuenta > Administrar cuenta > Miembros** para ver la cuenta de servicio.



La cuenta de servicio (*SnapCenter-account-<accountid>*) se utiliza para ejecutar las operaciones de backup programadas. Nunca debe eliminar la cuenta de servicio.

15. En la página Add Host, realice lo siguiente:

- a. Seleccione **Manual**.
- b. Especifique el FQDN o la dirección IP del host donde se implementó el plugin.

Asegúrese de que con el FQDN o la dirección IP, el conector puede comunicarse con el host de la base de datos.

- c. Especifique el puerto del plugin.

El puerto predeterminado es 8145.

- d. Seleccione el conector.
- e. Seleccione la casilla de comprobación para confirmar que el plugin está instalado en el host
- f. Haga clic en **detectar aplicaciones**.

- Muestra todas las bases de datos en el host. Si la autenticación del sistema operativo está desactivada para la base de datos, debe configurar la autenticación de la base de datos haciendo clic en **Configurar**. Para obtener más información, consulte [Configurar las credenciales de la base de datos de Oracle](#).
- Haga clic en **Configuración** y seleccione **hosts** para ver todos los hosts. Haga clic en **Eliminar** para eliminar un host de base de datos.



El filtro para ver un host específico no funciona. Cuando se especifica un nombre de host en el filtro, se muestran todos los hosts.

- Haga clic en **Configuración** y seleccione **Directivas** para ver las directivas preparadas previamente. Revise las directivas predefinidas y, si desea, puede editarlas para cumplir sus requisitos o crear una nueva directiva.

## Configurar las credenciales de la base de datos de Oracle

Es necesario configurar las credenciales que se usan para realizar operaciones de protección de datos en bases de datos de Oracle.

- Pasos\*

1. Si la autenticación del sistema operativo está desactivada para la base de datos, debe configurar la autenticación de la base de datos haciendo clic en **Configurar**.
2. Especifique el nombre de usuario, la contraseña y los detalles del puerto.

Si la base de datos reside en ASM, también debe configurar los ajustes de ASM.

El usuario de Oracle debe tener privilegios sysdba y el usuario de ASM debe tener privilegios sysasm.

1. Haga clic en **Configurar**.

## Realice backup de bases de datos de Oracle nativas en el cloud

Debe asignar una política predefinida o la que creó y, a continuación, realizar una copia de seguridad.

### Crear una política para proteger una base de datos de Oracle

Puede crear directivas si no desea editar las directivas preparadas previamente.

- Pasos\*

1. En la página aplicaciones, en la lista desplegable Configuración, seleccione **Directivas**.
2. Haga clic en **Crear directiva**.
3. Escriba el nombre de una política.
4. (Opcional) edite el formato del nombre de la copia de seguridad.
5. Especifique los detalles de programación y retención.
6. Haga clic en **Crear**.

### Cree un backup de la base de datos Oracle

Puede asignar una directiva predefinida o crear una directiva y, a continuación, asignarla a la base de datos. Una vez asignada la política, los backups se crean según la programación definida en la política.



Para Oracle, al crear grupos de discos ASM, asegúrese de que no haya volúmenes comunes entre grupos de discos. Cada grupo de discos debe tener volúmenes dedicados.

- Pasos\*

1. En la página aplicaciones, si la base de datos no está protegida mediante ninguna directiva, haga clic en **asignar directiva**.

Si la base de datos se protege mediante una o más políticas, puede asignar más políticas haciendo clic en **...** > **asignar directiva**.

2. Seleccione la directiva y haga clic en **asignar**.

Los backups se crearán según el programa que se defina en la política.



La cuenta de servicio (*SnapCenter-account- $\langle$ account\_id $\rangle$* ) se utiliza para ejecutar las operaciones de backup programadas.

### Cree un backup bajo demanda de la base de datos de Oracle

Después de asignar la política, puede crear un backup bajo demanda de la aplicación.

- Pasos\*

1. En la página aplicaciones, haga clic en **...** Corresponde a la aplicación y haga clic en **On-Demand Backup**.
2. Si se asignan varias directivas a la aplicación, seleccione la directiva, el valor de retención y, a continuación, haga clic en **Crear copia de seguridad**.

### Más información

Después de restaurar una base de datos grande (250 GB o más), si se ejecuta un backup completo en línea en la misma base de datos, la operación puede fallar y generar el siguiente error:

```
failed with status code 500, error
{"error":{"code":"app_internal_error","message":"Failed to create
snapshot. Reason: Snapshot operation not allowed due to clones backed by
snapshots. Try again after sometime.
```

Para obtener información sobre cómo solucionar este problema, consulte: ["No se permite la operación de Snapshot debido a clones realizados por copias de Snapshot"](#).

### Limitaciones

- No admite backups de datos en línea ni solo backups de registros
- No admite backups sin conexión
- No admite la copia de seguridad de la base de datos Oracle que reside en puntos de montaje recursivos
- No admite snapshots de grupos de consistencia para bases de datos de Oracle que residen en varios grupos de discos de ASM con superposición de volúmenes FSX
- Si las bases de datos de Oracle se configuran en ASM, asegúrese de que los nombres de SVM sean únicos en los sistemas FSX. Si tiene el mismo nombre de SVM en sistemas FSX, no se admite el backup de las bases de datos de Oracle que residen en dichas SVM.

## Realice backup de la base de datos SAP HANA nativa del cloud

### Acceda a BlueXP

Usted debe ["Regístrese en la página web de NetApp BlueXP"](#), ["Inicie sesión en BlueXP"](#)y, a continuación, configure un ["Cuenta de NetApp"](#).

### Configure Azure NetApp Files

Debe crear el entorno de trabajo de Azure NetApp Files y el conector.

## Crear el entorno de trabajo de Azure NetApp Files

Debe crear entornos de trabajo de Azure NetApp Files en los que se alojan las bases de datos. Para obtener más información, consulte ["Más información sobre Azure NetApp Files"](#) y.. ["Crear un entorno de trabajo de Azure NetApp Files"](#).

### Cree un conector

Un administrador de cuentas debe poner en marcha un conector en Azure NetApp Files que permita a BlueXP gestionar recursos y procesos dentro de su entorno de nube pública.



No puede actualizar el nuevo Connector\_id desde la interfaz de usuario.

Para obtener más información, consulte ["Cree un conector en Azure desde BlueXP"](#).

## Ponga en marcha el plugin de SnapCenter para SAP HANA y añada hosts de base de datos

Debe implementar el plugin de SnapCenter para SAP HANA en cada uno de los hosts de bases de datos SAP HANA. Según si el host SAP HANA tiene una autenticación basada en clave SSH habilitada, puede seguir uno de los métodos para implementar el plugin.

### Requisitos previos

- Compruebe que Oracle Java 11 (64 bits) u OpenJDK estén instalados en cada uno de los hosts de bases de datos SAP HANA.
- Debe haber agregado el entorno de trabajo y creado el conector.
- Asegúrese de que el conector tiene conectividad con el entorno de trabajo
- Asegúrese de que el usuario de BlueXP tiene la función "Administrador de cuentas".
- Debe haber creado el usuario de SnapCenter y configurado sudo para el usuario de SnapCenter. Para obtener más información, consulte ["Configure sudo para el usuario de SnapCenter."](#)
- Debe haber implementado el plugin de SnapCenter para SAP HANA antes de añadir el host de base de datos.
- Al añadir los hosts de la base de datos SAP HANA, debe añadir las claves de almacenamiento de usuario HDB. La clave de almacenamiento de usuario seguro HDB se utiliza para almacenar la información de conexión de los hosts de la base de datos SAP HANA de forma segura en el cliente, y el cliente HDBSQL utiliza la clave de almacenamiento de usuario segura para conectarse con el host de la base de datos SAP HANA.
- Para la replicación de sistemas HANA (HSR), para proteger los sistemas HANA, debe registrar manualmente los sistemas HANA primarios y secundarios.
- El conector debe tener activada la comunicación al puerto SSH (predeterminado: 22) si se utiliza la implementación basada en SSH.
- El conector debe tener la comunicación activada al puerto del plug-in (valor predeterminado: 8145) para que funcionen las operaciones.

### Configure sudo para el usuario de SnapCenter

Debe crear un usuario de SnapCenter para implementar el plugin.

- Pasos\*



1. Inicie sesión en el conector VM.
2. Descargue el binario del plugin del host Linux.  

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Obtenga la ruta de montaje base.  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```
4. Copie las líneas 1 a 16 de la `oracle_checksum_scs.txt` archivo ubicado en `base_mount_path/version/sc-linux-host-plugin/`
5. Inicie sesión en el host de la base de datos SAP HANA y realice los pasos siguientes:
  - a. Cree la cuenta de usuario de SnapCenter, el par de claves privadas y asigne los permisos.
  - b. Pegue las líneas copiadas en el paso 4 en el `/etc/sudoers` Archivo mediante la función `visudo` Linux.

En las líneas anteriores, reemplace `<LINUXUSER>` por el usuario de SnapCenter que ha creado y guardado en la función `visudo`.

#### Implemente el plugin mediante autenticación basada en clave SSH

Si la autenticación basada en clave SSH está habilitada en el host HANA, puede realizar los siguientes pasos para implementar el plugin. Antes de realizar los pasos, asegúrese de que la conexión SSH al conector está activada.

##### • Pasos\*

1. Inicie sesión en el conector VM.
2. Obtenga la ruta de montaje base.  

```
# sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```
3. Implemente el plugin.  

```
# sudo <base_mount_path>/scripts/hana_plugin_copy_and_install.sh --host  
<host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port>  
--pluginport <plugin_port> --installdir <install_dir>
```

  - `Host_name` es el nombre del host HANA y es un parámetro obligatorio.
  - `ssh_key_file` es la clave SSH que se utiliza para conectarse al host de HANA, y este es un parámetro obligatorio.
  - `User_name`: Usuario con privilegios de SSH en el host HANA, y este es un parámetro opcional. El valor predeterminado es `azureuser`.
  - `ssh_Port`: Puerto SSH en el host HANA, y este es un parámetro opcional. El valor predeterminado es 22.
  - `Plugin_Port`: Puerto que utiliza el plugin, y este es un parámetro opcional. El valor predeterminado es 8145.
  - `Directorio_de_instalación`: Directorio en el que se va a implementar el complemento y éste es un parámetro opcional. El valor predeterminado es `/opt`.

Después de implementar el plugin, debe añadir el ["Hosts de bases de datos SAP HANA."](#)

## Implemente el plugin manualmente

Si la autenticación basada en clave SSH no está habilitada en el host HANA, debe realizar los siguientes pasos manuales para implementar el plugin.

- Pasos\*

1. Inicie sesión en el conector VM.

2. Descargue el binario del plugin del host Linux.

```
# sudo docker exec -it cloudmanager_scs_cloud curl -X GET  
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

3. Obtenga la ruta de montaje base.

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```

4. Obtenga la ruta binaria del plug-in descargado.

```
sudo ls <base_mount_path> $(sudo docker ps|grep -Po  
"cloudmanager_scs_cloud:.*? " | sed -e 's/ *$//' | cut -f2 -d":")/sc-linux-host  
-plugin/snapcenter_linux_host_plugin_scs.bin
```

5. Copiar snapcenter\_linux\_host\_plugin\_scs.bin A cada uno de los hosts de la base de datos SAP HANA mediante scp u otros métodos alternativos.

6. En el host de la base de datos SAP HANA, ejecute el comando siguiente para habilitar permisos de ejecución para el binario.

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```

7. Implemente el complemento SAP HANA como usuario sudo SnapCenter.

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root-user>
```

8. Copiar certificate.p12 de <base\_mount\_path>/client/certificate/ Ruta del conector VM a. /var/opt/snapcenter/spl/etc/ en el host del plugin.

- a. Vaya a. /var/opt/snapcenter/spl/etc y ejecute el comando keytool para importar el certificado.

```
keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype  
PKCS12 -destkeystore keystore.jks -deststoretype JKS -srcstorepass  
snapcenter -deststorepass snapcenter -srcalias agentcert -destalias  
agentcert -noprompt
```

- b. Reinicie SPL: `systemctl restart spl`

9. Valide que es posible acceder al plugin desde el conector ejecutando el comando siguiente desde el conector:

```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the  
plug-in host>:<plug-in port>/getVersion --cert  
/config/client/certificate/certificate.pem --key  
/config/client/certificate/key.pem
```

## Añada hosts de base de datos SAP HANA

Debe añadir manualmente hosts de base de datos SAP HANA para asignar políticas y crear backups. No se admite la detección automática del host de la base de datos SAP HANA.

- Pasos\*

1. En la interfaz de usuario de **BlueXP**, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **detectar aplicaciones**.
3. Seleccione **Cloud Native > SAP HANA** y haga clic en **Siguiente**.
4. En la página **aplicaciones**, haga clic en **Agregar sistema**.
5. En la página **Detalles del sistema**, realice las siguientes acciones:
  - a. Seleccione el Tipo de sistema como contenedor de base de datos multi-tenant o contenedor único.
  - b. Introduzca el nombre del sistema SAP HANA.
  - c. Especifique el SID del sistema SAP HANA.
  - d. (Opcional) especifique el usuario de sistema operativo de HDBSQL.
  - e. Seleccione el host del plugin. (Opcional) Si el host no está agregado o si desea agregar varios hosts, haga clic en **Agregar host del plugin**.
  - f. Si el sistema HANA está configurado con la replicación del sistema HANA, habilite **sistema de replicación del sistema HANA (HSR)**.
  - g. Haga clic en el cuadro de texto **HDB Secure User Store Keys** para agregar los detalles de las claves de almacenamiento de usuario.

Especifique el nombre de la clave, los detalles del sistema, el nombre de usuario y la contraseña y haga clic en **Agregar clave**.

Puede eliminar o modificar las claves de almacenamiento de usuario.

1. Haga clic en **Siguiente**.
2. En la página **Storage Footprint**, haga clic en **Add Storage** y realice lo siguiente:
  - a. Seleccione el entorno de trabajo y especifique la cuenta de NetApp.  
  
Vaya a la página **Canvas** para añadir un nuevo entorno de trabajo
  - b. Seleccione los volúmenes requeridos.
  - c. Haga clic en **Agregar almacenamiento**.
3. Revise todos los detalles y haga clic en **Agregar sistema**.



El filtro para ver un host específico no funciona. Cuando se especifica un nombre de host en el filtro, se muestran todos los hosts

Puede modificar y quitar los sistemas SAP HANA mediante la API DE REST. Antes de quitar el sistema HANA, debe eliminar todos los backups asociados y quitar la protección.

### Añada volúmenes no Data

Después de añadir el contenedor de base de datos multitenant o el sistema SAP HANA de un solo tipo de contenedor, puede añadir los volúmenes que no son de datos del sistema HANA.

#### • Pasos\*

1. En la interfaz de usuario de **BlueXP**, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.

2. Haga clic en **detectar aplicaciones**.
3. Seleccione **Cloud Native > SAP HANA** y haga clic en **Siguiente**.
4. En la página **aplicaciones**, haga clic en **...** Corresponde al sistema para el que desea agregar los volúmenes no Data y seleccione **gestionar sistema > volumen no Data**.

### Añada volúmenes no Data globales

Después de añadir el contenedor de base de datos multitenant o el sistema SAP HANA de un solo contenedor, puede añadir los volúmenes globales de Non-Data del sistema HANA.

- Pasos\*

1. En la interfaz de usuario de **BlueXP**, haga clic en **Protección > copia de seguridad y recuperación > aplicaciones**.
2. Haga clic en **detectar aplicaciones**.
3. Seleccione **Cloud Native > SAP HANA** y haga clic en **Siguiente**.
4. En la página **aplicaciones**, haga clic en **Agregar sistema**.
5. En la página **Detalles del sistema**, realice las siguientes acciones:
  - a. En el menú desplegable Tipo de sistema, seleccione **volumen no Data global**.
  - b. Introduzca el nombre del sistema SAP HANA.
  - c. Especifique el SIDS asociado del sistema SAP HANA.
  - d. Seleccione el host del plugin  
  
(Opcional) para agregar varios hosts, haga clic en **Agregar host Plug-in** y especifique el nombre de host y el puerto y haga clic en **Agregar host**.
  - e. Haga clic en **Siguiente**.
  - f. Revise todos los detalles y haga clic en **Agregar sistema**.

### Realice backup de la base de datos SAP HANA nativa del cloud

Antes de crear un backup de la base de datos SAP HANA, debe añadir los hosts de la base de datos SAP HANA y asignar una política predefinida o la que ha creado.

#### Cree una política para proteger la base de datos SAP HANA

Puede crear directivas si no desea utilizar o editar las directivas preparadas previamente.

1. En la página **aplicaciones**, en la lista desplegable Configuración, seleccione **políticas**.
2. Haga clic en **Crear directiva**.
3. Escriba el nombre de una política.
4. (Opcional) edite el formato del nombre de la copia Snapshot.
5. Seleccione el tipo de política.
6. Especifique los detalles de programación y retención.
7. (Opcional) especifique los scripts. "[Leer más](#)."
8. Haga clic en **Crear**.

## Scripts previos y posteriores

Es posible proporcionar scripts previos, posteriores y de salida mientras se crea una política. Estos scripts se ejecutan en el host HANA durante la operación de protección de datos.

El formato admitido para scripts es .sh, script python, script perl, etc.

El script previo y el script posterior deben ser registrados por el administrador del host en `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` archivo.

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

## Variables ambientales

Para el flujo de trabajo de backup, las siguientes variables de entorno están disponibles como parte del script previo y posterior.

Variable ambiental	Descripción
SID	El identificador del sistema de la base de datos HANA elegido para restaurar
Nombre de copia de seguridad	Nombre de backup elegido para la operación de restauración
UserStoreKeyNames	Se ha configurado la clave de almacenamiento de usuario para la base de datos HANA
OSDBUser	Se configuró OSDBUser para la base de datos HANA
PolicyName	Solo para copia de seguridad programada
schedule_type	Solo para copia de seguridad programada

## Cree un backup de la base de datos SAP HANA

Puede asignar una directiva predefinida o crear una directiva y, a continuación, asignarla a la base de datos. Una vez asignada la política, los backups se crean según la programación definida en la política.

## Acerca de esta tarea

Para la replicación de sistemas HANA (HSR), el trabajo de backup programado solo se activará para el sistema HANA principal y si el sistema conmuta por error al sistema HANA secundario, las programaciones existentes activarán un backup en el sistema HANA principal actual. Si no se asigna la política a ambos sistemas HANA, después de la conmutación al respaldo, se producirá un error en las programaciones.

Si se asignan diferentes políticas a los sistemas HSR, se activa el backup programado para ambos sistemas y no se puede realizar el backup para el sistema HANA secundario.

- Pasos\*

1. En la página aplicaciones, si la base de datos no está protegida mediante ninguna directiva, haga clic en **asignar directiva**.

Si la base de datos se protege mediante una o más políticas, puede asignar más políticas haciendo clic en **...** > **asignar directiva**.

2. Seleccione la directiva y haga clic en **asignar**.

Los backups se crearán según el programa que se defina en la política.



La cuenta de servicio (*SnapCenter-account-`<account_id>`*) se utiliza para ejecutar las operaciones de backup programadas.

### Cree un backup bajo demanda de la base de datos SAP HANA

Después de asignar la política, puede crear un backup bajo demanda de la aplicación.

- Pasos\*

1. En la página **aplicaciones**, haga clic en **...** Corresponde a la aplicación y haga clic en **On-Demand Backup**.
2. Seleccione el tipo de backup bajo demanda.
3. Para copias de seguridad basadas en directivas, seleccione la directiva, el nivel de retención y, a continuación, haga clic en **Crear copia de seguridad**.
4. Por una vez, seleccione Snapshot copy based o File based realice los siguientes pasos:
  - a. Seleccione el valor de retención y especifique el nombre del backup.
  - b. (Opcional) especifique los scripts y la ruta de acceso de los scripts.

Para obtener más información, consulte ["Scripts previos y posteriores"](#)

- c. Haga clic en **Crear copia de seguridad**.

## Restaurar los datos de aplicaciones nativas en el cloud

### Restaurar base de datos de Oracle nativa en cloud

En caso de pérdida de datos, puede restaurar los archivos de datos, los archivos de control o ambos y recuperar la base de datos.

#### Lo que necesitará

Si la base de datos de Oracle 21c está EN estado INICIADO, se produce un error en la operación de restauración. Debe ejecutar lo siguiente para restaurar la base de datos correctamente.

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar  
/opt/NetApp/snapcenter/spl/plugins/sco/lib ojdbc8-8.jar
```

- Pasos\*

1. Haga clic en **...** Corresponde a la base de datos que desea restaurar y haga clic en **Ver detalles**.

- Haga clic en **...** Corresponde a la copia de seguridad de datos que desea utilizar para restaurar y haga clic en **Restaurar**.
- En la sección Restore Scope, realice las siguientes acciones:

Si...	Realice lo siguiente...
Desea restaurar únicamente los archivos de datos	Seleccione <b>todos los archivos de datos</b> .
Desea restaurar únicamente los archivos de control	Seleccione <b>Archivos de control</b>
Desea restaurar tanto archivos de datos como archivos de control	Seleccione <b>todos los archivos de datos y Archivos de control</b> .



No se admiten la restauración de archivos de datos con archivos de control o solo archivos de control para iSCSI en el diseño de ASM.

También puede seleccionar la casilla de verificación **Forzar restauración in situ**.

En la distribución DE SAN, si el plugin de SnapCenter para Oracle encuentra cualquier archivo externo distinto a los archivos de datos de Oracle en el grupo de discos de ASM, se realiza el método de restauración de conexión y copia. Los archivos externos pueden ser uno o varios de los siguientes tipos:

- Parámetro
- Contraseña
- registro de archivo
- registro en línea
- Archivo de parámetros de ASM.

La opción **Forzar restauración in situ** reemplaza los archivos externos de tipo parámetro, contraseña y registro de archivo. Debe utilizar la última copia de seguridad cuando se seleccione la opción **Forzar restauración in situ**.

- En la sección Recovery Scope, realice las siguientes acciones:

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 System Change Number</b> y especifique el SCN.
Desea recuperar a una fecha y hora específicas	Seleccione <b>Fecha y hora</b> .
No desea recuperar	Seleccione <b>sin recuperación</b> .

Para el ámbito de recuperación seleccionado, en el campo **Ubicaciones de archivos de registro de archivo** puede especificar opcionalmente la ubicación que contiene los registros de archivo necesarios para la recuperación.

Seleccione la casilla de comprobación si desea abrir la base de datos en modo DE LECTURA/ESCRITURA después de la recuperación.

1. Haga clic en **Siguiente** y revise los detalles.
2. Haga clic en **Restaurar**.

### Limitaciones

- No admite restauraciones granulares, por ejemplo, la restauración de espacios de tablas y PDB
- Se utilizan métodos de restauración sin movimiento y de conexión y copia si algunos de los grupos de discos contienen archivos externos. Sin embargo, no se admite el uso de ambos métodos a la vez para realizar la restauración y se produce un error en la operación de restauración. La base de datos se quedará en estado montado y es necesario que la base de datos se abra manualmente.

El mensaje de error debido a la presencia de archivos externos no se muestra en la página de trabajo de la interfaz de usuario debido a un problema conocido. Compruebe si hay un fallo durante la fase DE restauración previa DE SAN en los registros del conector para conocer la causa del problema.

## Restaura la base de datos SAP HANA nativa del cloud

En caso de pérdida de datos, es posible restaurar los datos y los archivos que no son de datos, para luego recuperar la base de datos.

### Restaura la base de datos SAP HANA nativa del cloud

#### Lo que necesita

1. El sistema SAP HANA debe estar en estado detenido.
2. Puede proporcionar un script previo para detener el sistema SAP HANA.
  - Pasos\*
3. Haga clic en **...** Corresponde a la base de datos que desea restaurar y haga clic en **Ver detalles**.
4. Haga clic en **...** Corresponde a la copia de seguridad de datos que desea utilizar para restaurar y haga clic en **Restaurar**.
5. En la página **Restore System**, introduzca los scripts. "[Leer más.](#)"

Para el flujo de trabajo de restauración, las siguientes variables de entorno están disponibles como parte del script previo y posterior.

Variable ambiental	Descripción
SID	El identificador del sistema de la base de datos HANA elegido para restaurar
Nombre de copia de seguridad	Nombre de backup elegido para la operación de restauración



Variable ambiental	Descripción
UserStoreKeyNames	Se ha configurado la clave de almacenamiento de usuario para la base de datos HANA
OSDBUser	Se configuró OSDBUser para la base de datos HANA

6. Haga clic en **Restaurar**.

### Después de terminar

- Una vez realizada la restauración, recupere manualmente el sistema SAP HANA o proporcione un script posterior, que realiza la recuperación del sistema SAP HANA.

### Restaurar volumen no almacenado en datos

1. En la página **aplicaciones**, seleccione volumen sin datos en el cuadro desplegable.
2. Haga clic en **...** Corresponde a la copia de seguridad que desea restaurar y haga clic en **Restaurar**.

### Restaurar volumen no Data global

- Pasos\*
  1. En la página **aplicaciones**, haga clic en el volumen global que no es de datos que desea restaurar.
  2. Haga clic en **...** Corresponde al volumen Global no Data que desea restaurar y haga clic en **Restaurar**.

## Clone datos de aplicaciones nativas en el cloud

### Clone la base de datos de Oracle nativa en el cloud

#### Conceptos y requisitos de los clones

Es posible clonar una base de datos de Oracle con el backup de la base de datos en el host de la base de datos de origen o en un host alternativo. Puede clonar el backup de sistemas de almacenamiento primarios.

Antes de clonar la base de datos, debe comprender los conceptos de clon y asegurarse de que se cumplen todos los requisitos.

#### Requisitos para clonar una base de datos de Oracle

Antes de clonar una base de datos de Oracle, debe asegurarse de que se hayan completado los requisitos previos.

- Debe tener creado un backup de la base de datos. Debe haber creado correctamente el backup en línea y del registro para que la operación de clonado se complete correctamente.
- En el parámetro `asm_diskstring`, debe configurar `AFD:*` si está utilizando ASMFD o configurar `ORCL:*` si está utilizando ASMLIB.

- Si crea el clon en un host alternativo, este host debe cumplir los siguientes requisitos:
  - El plugin debe estar instalado en el host alternativo.
  - El host del clon debe poder detectar LUN del almacenamiento si se clona una base de datos que resida en un almacenamiento SAN iSCSI. Si clona en un host alternativo, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento y el host alternativo.
  - Si la base de datos de origen es una base de datos ASM:
    - La instancia de ASM debe estar activa y en ejecución en el host donde se realizará el clon.
    - El grupo de discos de ASM debe aprovisionarse antes de la operación de clonado si desea colocar los archivos de registro de archivos de la base de datos clonada en un grupo de discos de ASM dedicado.
    - Puede configurarse el nombre del grupo de discos de datos, pero asegúrese de que ningún otro grupo de discos ASM use el nombre en el host donde se realizará la clonación.
    - Los archivos de datos que residen en el grupo de discos de ASM se aprovisionan como parte del flujo de trabajo del clon.

### Limitaciones de clones

- No se admiten los clones programados (gestión del ciclo de vida de clones).
- No se admite la clonación de una base de datos clonada.
- No se admite la clonación de bases de datos que residen en Qtree.
- No se admite la clonación de backups de registros de archivos.
- No se admite el backup de una base de datos clonada.

### Métodos de clonado

Puede crear un clon con el método básico o con el archivo de especificación del clon.

#### Clonación mediante un método básico

Puede crear el clon con las configuraciones predeterminadas según la base de datos de origen y el backup seleccionado.

- Los parámetros de la base de datos, el usuario inicial y el usuario de sistema operativo se establecen de forma predeterminada en la base de datos de origen.
- Las rutas de acceso al archivo de datos se nombran según el esquema de nomenclatura seleccionado.
- No se pueden especificar las sentencias pre-script, post-script y SQL.
- La opción de recuperación es de forma predeterminada **hasta cancelar** y utiliza la copia de seguridad de registro asociada con la copia de seguridad de datos para la recuperación

#### Clonar utilizando archivo de especificación

Puede definir las configuraciones en el archivo de especificación del clon y usarlas para clonar la base de datos. Puede descargar el archivo de especificación, modificarlo según sus necesidades y, a continuación, cargar el archivo. ["Leer más"](#).

Los diferentes parámetros definidos en el archivo de especificación y que se pueden modificar son los siguientes:

Parámetro	Descripción
archivos_control	<p>Ubicación de los archivos de control de la base de datos del clon.</p> <p>La cantidad de archivos de control será la misma que la de la base de datos de origen. Si desea anular la ruta de acceso del archivo de control, puede proporcionar otra ruta de acceso al archivo de control. El sistema de archivos o el grupo de discos ASM deben existir en el host.</p>
redo_logs	<p>Ubicación, tamaño, número de redo logs del grupo de redo logs.</p> <p>Se requiere un mínimo de dos grupos de registros de recuperación para clonar la base de datos. Si desea anular la ruta de acceso del archivo de registro de recuperación, puede personalizarla en otro sistema de archivos que no sea el de la base de datos de origen. el sistema de archivos o el grupo de discos ASM deben existir en el host.</p>
versión_de_oracle	La versión de Oracle en el host de destino.
oracle_home	Directorio raíz de Oracle en el host de destino.
enable_archive_log_mode	Controla el modo de registro de archivos para la base de datos clonada
parámetros_base_datos	Parámetros de la base de datos clonada
sentencias sql	Las sentencias SQL que se ejecutarán en la base de datos después del clonado
detalles_usuario_so	Usuario del sistema operativo Oracle en la base de datos del clon de destino
puerto_base_datos	Puerto que se utiliza para comunicarse con la base de datos si la autenticación del sistema operativo está deshabilitada en el host.
asm_port	Puerto que se utiliza para comunicarse con la base de datos de ASM si las credenciales se proporcionan en la entrada de creación de clon.
saltar_recuperación	No realiza la operación de recuperación.
until_scn	Recupera la base de datos hasta el scn especificado.

Parámetro	Descripción
hasta_hora	<p>Recupera la base de datos hasta la fecha y la hora especificadas.</p> <p>El formato aceptado es <i>mm/dd/yyyy hh:mm:ss</i>.</p>
until_cancel	<p>Recupera mediante el montaje del backup de registros asociado con el backup de datos que se seleccionó para la clonación.</p> <p>La base de datos clonada se recupera hasta el archivo de registro faltante o dañado.</p>
rutas_log	Ubicaciones adicionales de las rutas de acceso de registros de archivos que se usarán para recuperar la base de datos clonada.
ubicación_origen	Ubicación del grupo de discos o punto de montaje en el host de la base de datos de origen.
ubicación_del_clon	Ubicación del grupo de discos o punto de montaje que se debe crear en el host de destino correspondiente a la ubicación de origen.
tipo_ubicación	<p>Puede ser ASM_Diskgroup o mountpoint.</p> <p>Los valores se completan automáticamente en el momento de descargar el archivo. No debe editar este parámetro.</p>
script previo	El script que se ejecutará en el host de destino antes de crear el clon.
post_script	El script que se ejecutará en el host de destino después de crear el clon.
ruta	<p>Ruta absoluta del script en el host del clon.</p> <p>Debe almacenar el script en <i>/var/opt/snapcenter/spl/scripts</i> o en cualquier carpeta dentro de esta ruta de acceso.</p>
tiempo de espera	El tiempo de espera especificado para el script que se ejecuta en el host de destino.
argumentos	Argumentos especificados para los scripts.

## Esquema de nomenclatura de los clones

El esquema de nomenclatura de los clones define la ubicación de los puntos de montaje y el nombre de los grupos de discos de la base de datos clonada. Puede seleccionar **idéntico** o **generado automáticamente**.

### Esquema de nomenclatura idéntico

Si selecciona el esquema de nomenclatura de clones como **idéntico**, la ubicación de los puntos de montaje y el nombre de los grupos de discos de la base de datos clonada serán los mismos que la base de datos de origen.

Por ejemplo, si el punto de montaje de la base de datos de origen es `/netapp_sourcedb/data_1`, `+DATA1_DG`, en la base de datos clonada, el punto de montaje permanece igual tanto para NFS como para ASM en SAN.

- Las configuraciones como el número y la ruta de acceso de los archivos de control y los archivos de recuperación serán las mismas que las del origen.



Si los registros de recuperación o las rutas de los archivos de control se encuentran en los volúmenes que no son de datos, el usuario debería haber aprovisionado el grupo de discos ASM o el punto de montaje en el host de destino.

- El usuario de Oracle OS y la versión de Oracle serán los mismos que la base de datos de origen.
- El nombre del volumen de almacenamiento del clon tendrá el siguiente formato `sourceVolNameSCS_Clone_CurrentTimeStampNumber`.

Por ejemplo, si el nombre del volumen en la base de datos de origen es `sourceVolName`, el nombre del volumen clonado será `sourceVolNameSCS_Clone_1661420020304608825`.



El `CurrentTimeStampNumber` proporciona la singularidad en el nombre del volumen.

### Esquema de nomenclatura generado automáticamente

Si selecciona el esquema de clonación como **generado automáticamente**, la ubicación de los puntos de montaje y el nombre de los grupos de discos de la base de datos clonada se adjuntarán con un sufijo. \* Si ha seleccionado el método básico de clonación, el sufijo será el **SID de clon**. \* Si ha seleccionado el método de archivo de especificación, el sufijo será el **sufijo** que se especificó al descargar el archivo de especificación del clon.

Por ejemplo, si el punto de montaje de la base de datos de origen es `/netapp_sourcedb/data_1` y el **SID de clon** o el **sufijo** es `HR`, el punto de montaje de la base de datos clonada será `/netapp_sourcedb/data_1_HR`.

- La cantidad de archivos de control y los archivos de registro de recuperación serán los mismos que el origen.
- Todos los archivos de registro de recuperación y los archivos de control se ubicarán en uno de los puntos de montaje de datos clonados o los grupos de discos ASM de datos.
- El nombre del volumen de almacenamiento del clon tendrá el siguiente formato `sourceVolNameSCS_Clone_CurrentTimeStampNumber`.

Por ejemplo, si el nombre del volumen en la base de datos de origen es `sourceVolName`, el nombre del volumen clonado será `sourceVolNameSCS_Clone_1661420020304608825`.



El `CurrentTimeStampNumber` proporciona la singularidad en el nombre del volumen.

- El formato del punto de montaje NAS será *SourceNASMountPoint\_suffix*.
- El formato del grupo de discos de ASM será *SourceDiskgroup\_suffix*.



Si el número de caracteres del grupo de discos del clon es mayor que 25, tendrá *SC\_hashCode\_suffix*.

#### Parámetros de la base de datos

El valor de los siguientes parámetros de la base de datos será el mismo que el de la base de datos de origen, independientemente del esquema de nomenclatura de los clones.

- `formato_archivo_registro`
- `pista_auditoría`
- `procesos`
- `pga_aggregate_target`
- `remote_login_passwordfile`
- `deshacer_tablespace`
- `open_cursors`
- `sga_target`
- `db_block_size`

El valor de los siguientes parámetros de la base de datos se añadirá con un sufijo basado en el SID del clon.

- `audit_file_dest = {sourcedatabase_parametervalue}_suffix`
- `log_archive_dest_1 = {sourcedatabase_oraclehome}_suffix`

#### Variables de entorno predefinidas compatibles para el script previo y script posterior específicos de clon

Puede utilizar las variables de entorno predefinidas compatibles al ejecutar el script previo y el script posterior mientras se clona una base de datos.

- `SC_ORIGINAL_SID` especifica el SID de la base de datos de origen. Este parámetro se rellenará para los volúmenes de aplicaciones. Ejemplo: NFSB32
- `SC_ORIGINAL_HOST` especifica el nombre del host de origen. Este parámetro se rellenará para los volúmenes de aplicaciones. Ejemplo: asmrac1.gdl.englab.netapp.com
- `SC_ORACLE_HOME` especifica la ruta de acceso del directorio inicial de Oracle de la base de datos de destino. Ejemplo: /Ora01/app/oracle/product/18.1.0/dB\_1
- `SC_BACKUP_NAME` especifica el nombre del backup. Este parámetro se rellenará para los volúmenes de aplicaciones. Ejemplos:
  - Si la base de datos no se está ejecutando en modo ARCHIVELOG:  
`DATA@RG2_sspr2417819002_07-20- 2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1`
  - Si la base de datos se está ejecutando en modo ARCHIVELOG: `DATA@RG2_sspr2417819002_07-20- 2021_12.16.48.9267_0|LOG@RG2_sspr24819002_07-20-2021_12.16.48.9267_1, RG2_sspr2417819002_07-21-2021_12.16.48.9267_07_22_2021_sspr241_12.16.48.9267R17819002_R172242-__R172242`

- SC\_ORIGINAL\_OS\_USER especifica el propietario del sistema operativo de la base de datos de origen. Ejemplo: oracle
- SC\_ORIGINAL\_OS\_GROUP especifica el grupo de sistemas operativos de la base de datos de origen. Ejemplo: Oinstall
- SC\_TARGET\_SID" especifica el SID de la base de datos clonada. Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido. Este parámetro se rellenará para los volúmenes de aplicaciones. Ejemplo: Clonedb
- SC\_TARGET\_HOST especifica el nombre del host donde se clonará la base de datos. Este parámetro se rellenará para los volúmenes de aplicaciones. Ejemplo: asmrac1.gdl.englab.netapp.com
- SC\_TARGET\_OS\_USER especifica el propietario del sistema operativo de la base de datos clonada. Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido. Ejemplo: oracle
- SC\_TARGET\_OS\_GROUP especifica el grupo del sistema operativo de la base de datos clonada. Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido. Ejemplo: Oinstall
- SC\_TARGET\_DB\_PORT especifica el puerto de la base de datos de la base de datos clonada. Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido. Ejemplo: 1521

### Delimitadores compatibles

- @ se utiliza para separar los datos de su nombre de base de datos y separar el valor de su clave. Ejemplo: DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- | se utiliza para separar los datos entre dos entidades diferentes para el parámetro SC\_BACKUP\_NAME. Ejemplo: DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- , se utiliza para separar el conjunto de variables para la misma clave. Ejemplo: DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1, RG2\_scspr2417819002\_07-21-2021\_12.16.48.9267\_07, RG2\_scspr2417819002\_12.16.48.9267\_22-2021\_-

### Clone la base de datos de Oracle nativa en el cloud

Es posible clonar una base de datos de Oracle con el backup de la base de datos en el host de la base de datos de origen o en un host alternativo.

Pueden clonarse bases de datos por los siguientes motivos:

- Para poner a prueba una funcionalidad que debe implementarse con la estructura y el contenido de la base de datos actual durante ciclos de desarrollo de aplicaciones.
- Para completar almacenes de datos con herramientas de extracción y manipulación de datos.
- Para recuperar datos que se eliminaron o se modificaron por error.

### Lo que necesitará

Antes de clonar la base de datos, debe comprender los conceptos de clon y asegurarse de que se cumplen todos los requisitos. "[Leer más](#)".

- Pasos\*

1. Haga clic en [...](#) Corresponde a la base de datos que desea clonar y haga clic en **Ver detalles**.

2. Haga clic en **...** Corresponde a la copia de seguridad de los datos y haga clic en **Clonar**.
3. En la página Clone Details, seleccione una de las opciones de clonado.
4. En función de la opción seleccionada, realice las siguientes acciones:

Si seleccionó...	Realice lo siguiente...
<b>Básico</b>	<p>a. Seleccione el host del clon.</p> <p>Si desea crear el clon en un host alternativo, seleccione el host que tiene la misma versión de Oracle y del sistema operativo que el host de la base de datos de origen.</p> <p>b. Especifique el SID del clon.</p> <p>c. Seleccione el esquema de nomenclatura de los clones.</p> <p>Si la base de datos se clona en el host de origen, el esquema de nomenclatura de los clones se generará automáticamente. Si la base de datos se clona en un host alternativo, el esquema de nomenclatura de los clones será idéntico.</p> <p>d. Especifique la ruta de acceso de inicio de Oracle.</p> <p>e. (Opcional) especifique las credenciales de la base de datos.</p> <ul style="list-style-type: none"> <li>◦ Credencial de base de datos: Si la autenticación de usuario de sistema operativo está deshabilitada, debe proporcionar una contraseña para que el usuario sys la defina en el host de destino.</li> <li>◦ Credencial ASM: Si la autenticación del usuario del sistema operativo está deshabilitada en el host de destino, debe proporcionar credenciales de usuario con privilegios sysasm para conectarse a la instancia de ASM en el host de destino.</li> </ul> <p>f. Haga clic en <b>Siguiente</b>.</p> <p>g. Haga clic en <b>Clonar</b>.</p>



Si seleccionó...	Realice lo siguiente...
Archivo de especificación	<p>a. Haga clic en <b>Descargar archivo</b> para descargar el archivo de especificación.</p> <p>b. Seleccione el esquema de nomenclatura de los clones.</p> <p>Si selecciona <b>generado automáticamente</b>, debe especificar el sufijo.</p> <p>c. Edite el archivo de especificación según los requisitos y cárguelo haciendo clic en el botón <b>examinar</b>.</p> <p>d. Seleccione el host del clon.</p> <p>Si desea crear el clon en un host alternativo, seleccione el host que tiene la misma versión de Oracle y del sistema operativo que el host de la base de datos de origen.</p> <p>e. Especifique el SID del clon.</p> <p>f. (Opcional) especifique las credenciales de la base de datos.</p> <ul style="list-style-type: none"> <li>◦ Credencial de base de datos: Si la autenticación de usuario de sistema operativo está deshabilitada, debe proporcionar una contraseña para que el usuario sys la defina en el host de destino.</li> <li>◦ Credencial ASM: Si la autenticación del usuario del sistema operativo está deshabilitada en el host de destino, debe proporcionar credenciales de usuario con privilegios sysasm para conectarse a la instancia de ASM en el host de destino.</li> </ul> <p>g. Haga clic en <b>Siguiente</b>.</p> <p>h. Haga clic en <b>Clonar</b>.</p>

5. Haga clic en  Junto a **Filter by** y seleccione **Clone options > Clones** para ver los clones.

## Gestione la protección de datos de aplicaciones nativas en el cloud

### Supervisar trabajos

Es posible supervisar el estado de los trabajos que se han iniciado en los entornos de trabajo. Esto permite ver los trabajos que se completaron correctamente, los que están en curso en ese momento y los que han fallado para poder diagnosticar y corregir cualquier problema.

Es posible ver una lista de todas las operaciones y su estado. Cada operación, o trabajo, tiene un ID exclusivo y un estado. El estado puede ser:

- Exitoso
- En curso
- En cola
- Advertencia
- Error
- Pasos\*

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

Puede hacer clic en el nombre de un trabajo para ver los detalles que corresponden a esa operación. Si está buscando un trabajo específico, puede:

- utilice el selector de tiempo situado en la parte superior de la página para ver los trabajos de un determinado intervalo de tiempo
- Introduzca una parte del nombre del trabajo en el campo Buscar
- ordene los resultados mediante el filtro de cada encabezado de columna

## Datos de auditoría

Cuando ejecuta una API directamente o utiliza la interfaz de usuario para realizar llamadas a la API a cualquiera de las API expuestas externamente de Cloud Backup para aplicaciones, los detalles de la solicitud como encabezados, rol, cuerpo de la solicitud, Y la información de API se registrará en la línea de tiempo de BlueXP y las entradas de auditoría se conservarán siempre en la línea de tiempo. El estado y la respuesta de error de la llamada API también se auditan tras la finalización de la operación. En el caso de respuestas asíncronas de la API como los trabajos, el ID de trabajo también se registra como parte de la respuesta.

Cloud Backup para aplicaciones registra las entradas como IP de host, cuerpo de solicitud, nombre de operación, que se activan, algunos encabezados, Y el estado de funcionamiento de la API.

## Ver detalles de backup

Es posible ver la cantidad total de backups creados, las políticas que se usan para crear backups, la versión de la base de datos y el ID de agente.





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 ID de agente está asociado al conector. Si ya no existe un conector que se utilizó durante el registro del host SAP HANA, se producirá un error en las copias de seguridad subsiguientes de esa aplicación porque el ID de agente del nuevo conector es diferente. Debe modificar el id del conector en el host.

## Eliminar clon

Es posible eliminar un clon si ya no se necesita.

1. Haga clic en  Junto a **Filter by** y seleccione **Clone options > Clone parents**.
2. Haga clic en  Corresponde a la aplicación y haga clic en **Ver detalles**.
3. En la página Database Details, haga clic en  Junto a **Filter by** y seleccione **Clone**.
4. Haga clic en  Correspondiente al clon que desea eliminar y haga clic en **Eliminar**.
5. (Opcional) Active la casilla de verificación **forzar eliminación**.

## Actualice los detalles del conector para el host de la base de datos SAP HANA

Si el conector que se utilizó durante el registro del host de la aplicación ya no existe o está dañado, debe implementar un nuevo conector. Después de implementar el nuevo conector, debe ejecutar la **API Connector-update** para actualizar los detalles del conector para todos los hosts registrados utilizando el conector antiguo.

```
curl --location --request PATCH
'https://snapcenter.cloudmanager.cloud.netapp.com/api/saphana/hosts/connector/update' \
--header 'x-account-id: <CM account-id>' \
--header 'Authorization: Bearer token' \
--header 'Content-Type: application/json' \
--data-raw '{
"old_connector_id": "Old connector id that no longer exists",
"new_connector_id": "New connector Id"
}'
```

Los detalles del conector se actualizarán correctamente si todos los hosts tienen el servicio del plugin de SnapCenter para SAP HANA instalado y en ejecución, y también si se puede acceder a todos desde el nuevo conector.

## Configure el certificado firmado de CA

Es posible configurar un certificado firmado de CA si se desea incluir la seguridad adicional en el entorno.

### Configure el certificado de CA firmado para la autenticación de certificado de cliente

El conector utiliza un certificado autofirmado para comunicarse con el plug-in. El certificado autofirmado se importa al almacén de claves mediante el script de instalación. Puede realizar los siguientes pasos para reemplazar el certificado autofirmado con el certificado firmado de CA.

#### Lo que necesitará

Puede ejecutar el siguiente comando para obtener el `<base_mount_path>`:

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

- Pasos\*

1. Inicie sesión en el conector.

2. Elimine todos los archivos existentes ubicados en `<base_mount_path>/client/certificate` en la máquina virtual conector.
3. Copie el certificado firmado de CA y el archivo de claves en el `<base_mount_path>/client/certificate` de la máquina virtual conector.

El nombre del archivo debe ser `certificate.pem` y `key.pem`. El `certificate.pem` debe tener toda la cadena de certificados como la CA intermedia y la CA raíz.

4. Cree el formato PKCS12 del certificado con el nombre `certificate.p12` y conserve en `<base_mount_path>/client/certificate`.
5. Copie el certificado.p12 y los certificados de toda la CA intermedia y la CA raíz en el host del plugin, en `/var/opt/snapcenter/spl/etc/`.
6. Inicie sesión en el host del plugin.
7. Desplácese hasta `/var/opt/snapcenter/spl/etc` y ejecute el comando `keytool` para importar el archivo `certificate.p12`.  

```
keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter -deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt
```
8. Importe la CA raíz y los certificados intermedios.  

```
keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter -alias trustedca -file <certificate.crt>
```



Certfile.crt hace referencia a los certificados de la CA raíz así como a la CA intermedia.

9. Reinicie SPL: `systemctl restart spl`

## Configure el certificado firmado de CA para el certificado de servidor del plugin

El certificado de CA debe tener el nombre exacto del host del plugin con el que se comunica la máquina virtual conector.

### Lo que necesitará

Puede ejecutar el siguiente comando para obtener el `<base_mount_path>`:

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
```

#### • Pasos\*

1. Realice los siguientes pasos en el host del plugin:
  - a. Desplácese hasta la carpeta que contiene el almacén de claves `/var/opt/snapcenter/spl/etc` del SPL.
  - b. Cree el formato PKCS12 del certificado que tiene tanto el certificado como la clave con alias `splkeystore`.
  - c. Añada el certificado de CA.  

```
keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore -destalias splkeystore -noprompt
```
  - d. Verifique los certificados.

```
keytool -list -v -keystore keystore.jks
```

e. Reinicie SPL: `systemctl restart spl`

2. Lleve a cabo los siguientes pasos en el conector:

a. Inicie sesión en el conector como usuario no raíz.

b. Copie la cadena completa de certificados de CA en el volumen persistente ubicado en `<base_mount_path>/Server`.

Cree la carpeta de servidor si no existe.

c. Conéctese a `cloudManager_scs_Cloud` y modifique **enableCACert** in `config.yml` a **true**.

```
sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert:
false/enableCACert: true/g' /opt/netapp/cloudmanager-scs-
cloud/config/config.yml
```

d. Reinicie el contenedor `cloudManager_scs_Cloud`.

```
sudo docker restart cloudmanager_scs_cloud
```

## Acceda a las API de REST

Hay disponibles las API REST para proteger las aplicaciones en el cloud ["aquí"](#).

Debe obtener el token de usuario con autenticación federada para acceder a las API DE REST. Para obtener información sobre cómo obtener el token de usuario, consulte ["Cree un token de usuario con autenticación federada"](#).

## 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 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.