Proteja los datos de las aplicaciones

Cloud Backup

NetApp
February 20, 2023

Tabla de Contenido

Proteja los datos de las aplicaciones

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"

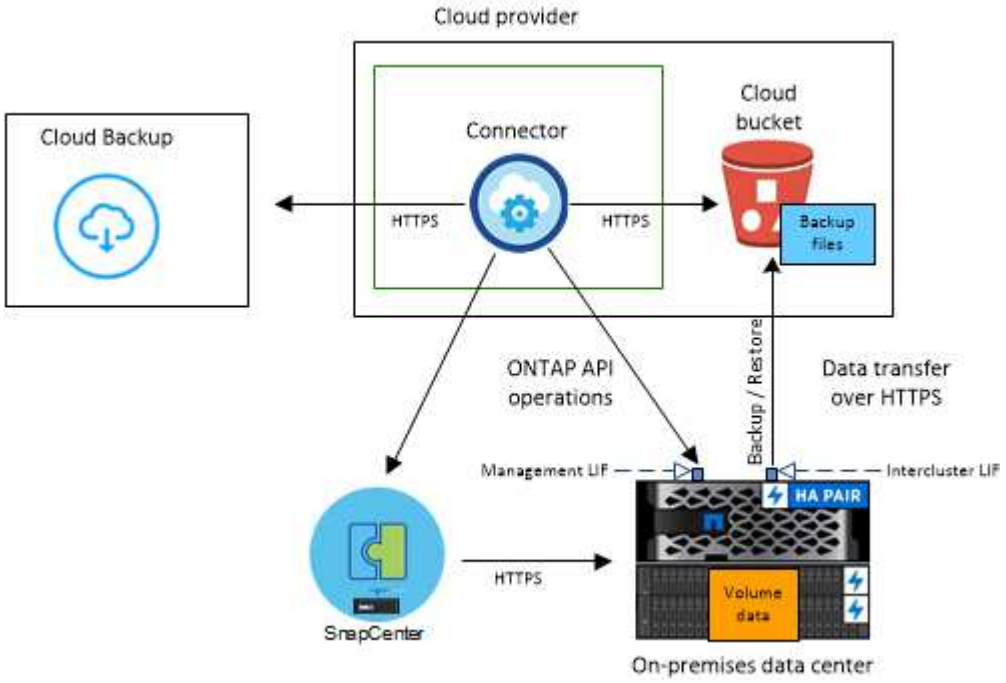
Requisitos

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.

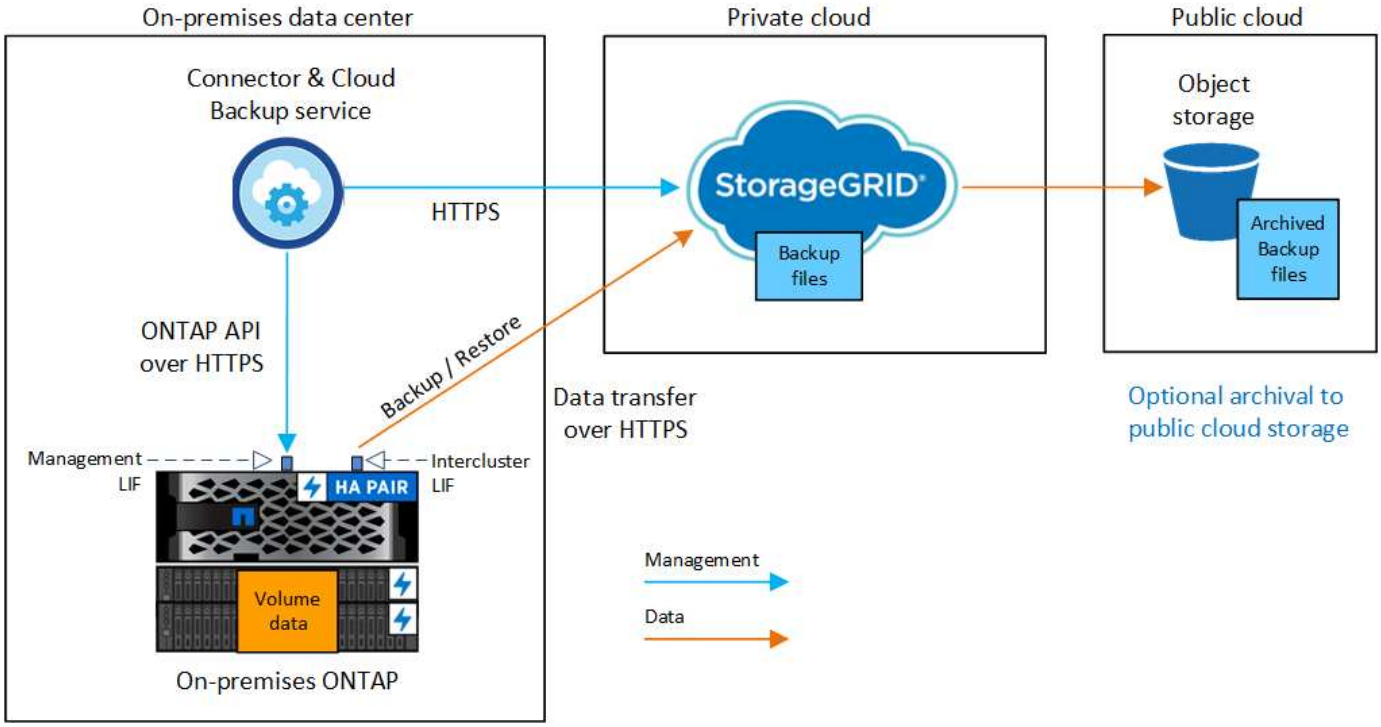
- ONTAP 9.8 o posterior
- BlueXP 3.9
- SnapCenter Server 4.6 o posterior debe utilizar SnapCenter Server 4.7 si desea utilizar las siguientes características:
  - proteja los backups del almacenamiento secundario en las instalaciones
  - Proteja aplicaciones SAP HANA
  - Protección de aplicaciones de 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 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 etiquete 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`

Restaure 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 **todos los registros**.
Desea recuperar a un número de cambio de sistema (SCN) específico	Seleccione **Until SCN (System Change Number)**.
Desea recuperar a una fecha y una hora específicas	Seleccione **Fecha y hora**. Debe especificar la fecha y la hora de la zona horaria del host de la base de datos.
No desea recuperar	Seleccione **sin recuperación**.
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
Restaure 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	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. Seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración. La extensión de archivo proporcionada en la ruta alternativa debe ser la misma que la del archivo de base de datos original. Si la opción **Restaurar la base de datos a un host alternativo** no aparece en la página Restaurar ámbito, borre la memoria caché del explorador.

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".

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 (ANF).

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.

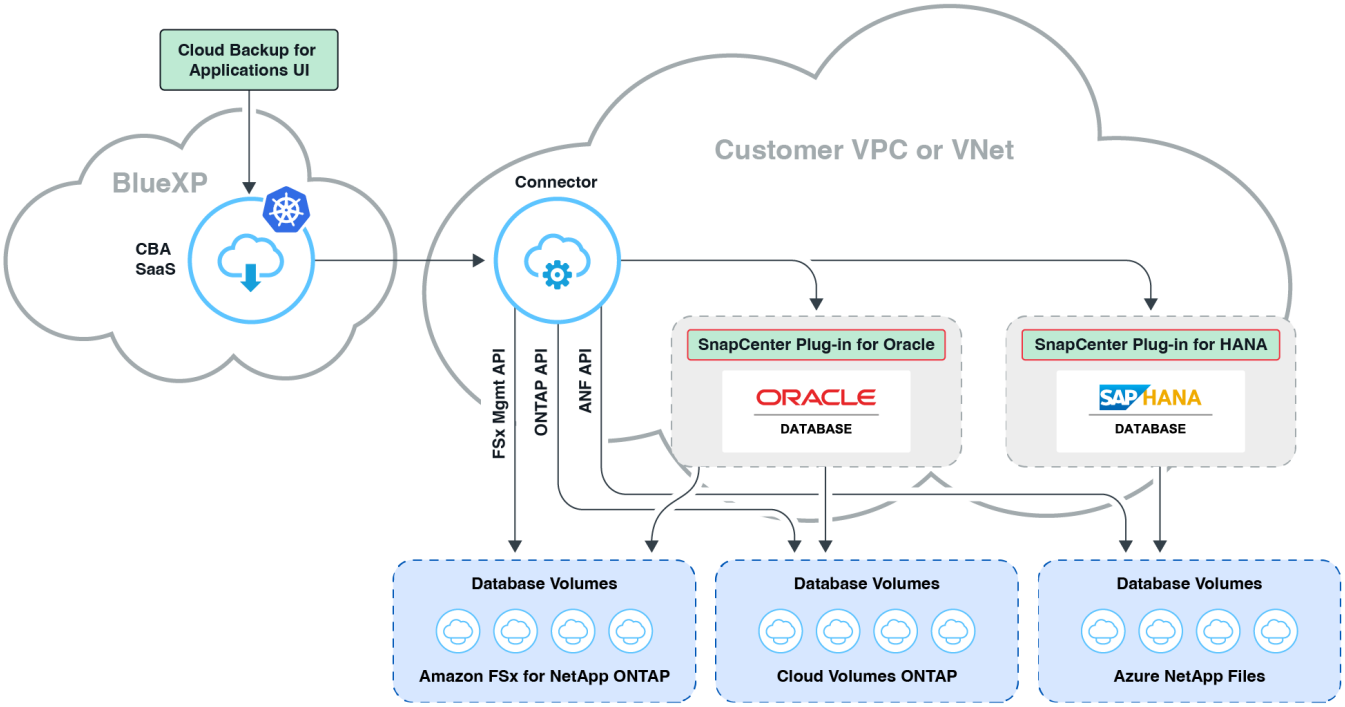
  Organiza los flujos de trabajo de protección de datos para aplicaciones que residen en el almacenamiento en cloud de NetApp.

- 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 (ANF)
- 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.

Añadir host y detectar bases de datos de Oracle

Debe añadir el host y detectar las bases de datos en el host para asignar políticas y crear backups. Es posible añadir el host manualmente cuando ya ha implementado el plugin o añadir el host mediante SSH.

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 que no es raíz. Para obtener más información, consulte Configurar un usuario que no sea raíz.
- Si desea añadir el host manualmente, primero debe implementar el plugin. Puede implementar el plugin manualmente o. con el script.

Debe implementar el plugin en cada uno de los hosts de las bases de datos de Oracle.

Configurar un usuario que no sea raíz

Debe configurar un usuario que no sea raíz para implementar el plugin.

- 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 que no sea raíz, 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 el <LINUXUSER> por el usuario no raíz que ha creado y guarde el archivo en la función visudo.

Implemente el plugin mediante script

Si la autenticación basada en claves SSH está habilitada en el host de Oracle para el usuario no raíz, 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 no raíz y se usa para conectarse al host Oracle. Este es un parámetro obligatorio.
     - User_name: Usuario no raíz con privilegios SSH en el host 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_install.sh
--host xxx.xx.x.x --sshkey /keys/netapp-ssh.ppk
```

Implemente el plugin manualmente

Si la autenticación basada en claves SSH no está habilitada en el host de Oracle, 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 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 que no sea raíz puede acceder.
6. Inicie sesión en el host de la base de datos Oracle utilizando la cuenta de usuario no raíz y ejecute el comando siguiente para habilitar los permisos de ejecución para el binario.
   ```
   chmod +x snapcenter_linux_host_plugin_scs.bin
   ```
7. Implemente el plugin de Oracle como usuario sudo que no sea raíz.
   ```
   ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root-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 -srcalias agentcert -destalias agentcert -noprompt
   ```
10. Reinicie SPL: `systemctl restart spl`

Añadir host

Debe añadir el host y detectar las bases de datos de Oracle.

- 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 **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 una de las siguientes acciones:

Si…	Realice lo siguiente…
Ya haya implementado el plugin manualmente o. con el script	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**.

Si…	Realice lo siguiente…
Desea poner en marcha el plugin de forma automática	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 no raíz) 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. e. Seleccione el conector. f. (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. g. 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.

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-<account_id>*) 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.

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

Si…	Realice lo siguiente…
Desea restaurar únicamente los archivos de datos	Seleccione **todos los archivos de datos**.
Desea restaurar únicamente los archivos de control	Seleccione **Archivos de control**
Desea restaurar tanto archivos de datos como archivos de control	Seleccione **todos los archivos de datos** y **Archivos de control**.

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**.

4. En la sección Recovery Scope, realice las siguientes acciones:

Si…	Realice lo siguiente…
Desea recuperar la última transacción	Seleccione **todos los registros**.
Desea recuperar a un número de cambio de sistema (SCN) específico	Seleccione **Until System Change Number** y especifique el SCN.
Desea recuperar a una fecha y hora específicas	Seleccione **Fecha y hora**.

Si…	Realice lo siguiente…
No desea recuperar	Seleccione **sin recuperación**.

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.

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 clonado.
  - 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 clonado de una base de datos clonada.
- No se admite la clonado de bases de datos que residen en Qtree.
- No se admite la clonado 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	Ubicación de los archivos de control de la base de datos del clon. 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.
redo_logs	Ubicación, tamaño, número de redo logs del grupo de redo logs. 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.
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	Recupera la base de datos hasta la fecha y la hora especificadas. El formato aceptado es *mm/dd/yyyy hh:mm:ss*.
until_cancel	Recupera mediante el montaje del backup de registros asociado con el backup de datos que se seleccionó para la clonación. La base de datos clonada se recupera hasta el archivo de registro faltante o dañado.
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	Puede ser ASM_Diskgroup o mountpoint. Los valores se completan automáticamente en el momento de descargar el archivo. No debe editar este parámetro.
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	Ruta absoluta del script en el host del clon. Debe almacenar el script en /var/opt/snapcenter/spl/scripts o en cualquier carpeta dentro de esta ruta de acceso.
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_16614200203046088825*.

  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_16614200203046088825*.

  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_12.16.48.9267*R17819002*_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…
Básico	a. Seleccione el host del clon. 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. b. Especifique el SID del clon. c. Seleccione el esquema de nomenclatura de los clones. 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. d. Especifique la ruta de acceso de inicio de Oracle. e. (Opcional) especifique las credenciales de la base de datos. ◦ 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. ◦ 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. f. Haga clic en **Siguiente**. g. Haga clic en **Clonar**.

Si seleccionó…	Realice lo siguiente…
Archivo de especificación	a. Haga clic en **Descargar archivo** para descargar el archivo de especificación. b. Seleccione el esquema de nomenclatura de los clones. Si selecciona **generado automáticamente**, debe especificar el sufijo. c. Edite el archivo de especificación según los requisitos y cárguelo haciendo clic en el botón **examinar**. d. Seleccione el host del clon. 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. e. Especifique el SID del clon. f. (Opcional) especifique las credenciales de la base de datos. ◦ 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. ◦ 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. g. Haga clic en **Siguiente**. h. Haga clic en **Clonar**.

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 asincrónicas 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/connec
tor/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

Información de la marca comercial