Realice backups de datos de aplicaciones nativas en el cloud

Cloud Backup

NetApp
March 06, 2023

Tabla de Contenido

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 -srcalias 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-<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.

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 visuod.

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

Variable ambiental	Descripción
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**.

Información de copyright

Información de la marca comercial