



Realice backups de datos de aplicaciones nativas en el cloud

Cloud Backup

NetApp
February 20, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-backup-restore/aws/reference-access-bluexp.html> on February 20, 2023. Always check docs.netapp.com for the latest.

Tabla de Contenido

Realice backups de datos de aplicaciones nativas en el cloud	1
Realice backup de bases de datos de Oracle nativas en el cloud.....	1

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	<ol style="list-style-type: none">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 hostf. Haga clic en detectar aplicaciones.

Si...	Realice lo siguiente...
Desea poner en marcha el plugin de forma automática	<p>a. Seleccione usando SSH.</p> <p>b. Especifique el FQDN o la dirección IP del host en el que desea instalar el plugin.</p> <p>c. Especifique el nombre de usuario (usuario no raíz) mediante el cual se copiará el paquete de plugins en el host.</p> <p>d. Especifique el SSH y el puerto del plugin.</p> <p>El puerto SSH predeterminado es 22 y el puerto del plugin es 8145.</p> <p>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.</p> <p>e. Seleccione el conector.</p> <p>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.</p> <div>  <p>La clave privada SSH no se almacena en ningún lugar de la aplicación y no se usará en ninguna otra operación.</p> </div> <p>g. Haga clic en Siguiente.</p>

- 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.

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.