Realizar backups de bases de datos de Oracle nativas en el cloud

BlueXP backup and recovery

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/es-es/bluexp-backup-recovery/task-quick-start-oracle.html on April 18, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Realizar backups de bases de datos de Oracle nativas en el cloud . . . 1
Inicio rápido . . . 1
Configure FSX para ONTAP . . . 2
Configure Cloud Volumes ONTAP . . . 3
Configure Azure NetApp Files . . . 3
Instale el plugin de SnapCenter para Oracle y añada hosts de base de datos . . . 4
Realizar backups de bases de datos de Oracle nativas en el cloud . . . 11

Realizar backups de bases de datos de Oracle nativas en el cloud

Inicio rápido

Comience rápidamente siguiendo estos pasos.

1 Verifique la compatibilidad con la configuración

- Sistema operativo:
  - RHEL 7.5 o posterior y 8.x
  - OL 7.5 o posterior y 8.x.
  - SLES 15 SP4
- Almacenamiento en cloud de NetApp:
  - Amazon FSX para ONTAP de NetApp
  - Cloud Volumes ONTAP
  - Azure NetApp Files
- Distribución de almacenamiento:
  - NFS v3 y v4.1 (incluido dNFS)
  - ISCSI con ASM (ASMFD, ASMLib y ASMUdev)

    Azure NetApp Files no es compatible con entornos SAN.

- Distribución de bases de datos: Oracle Standard y Oracle Enterprise Standalone (CDB heredado y multitenant y PDB)
- Versiones de base de datos: 19C y 21c

2 Regístrese en BlueXP

BlueXP es accesible desde una consola basada en Web. Cuando comience a utilizar BlueXP, su primer paso consiste en registrarse con sus credenciales actuales del sitio de soporte de NetApp o mediante la creación de un inicio de sesión en cloud de NetApp. Para obtener más información, consulte "Regístrese en BlueXP".

3 Inicia sesión en BlueXP

Después de registrarse en BlueXP, puede iniciar sesión desde la consola basada en Web. Para obtener más información, consulte "Inicia sesión en BlueXP".

4 Administre su cuenta de BlueXP

Puede administrar su cuenta gestionando usuarios, cuentas de servicio, áreas de trabajo y conectores. Para obtener más información, consulte "Administre su cuenta de BlueXP".

Configure FSX para ONTAP

Con BlueXP, deberías crear un entorno de trabajo FSx para ONTAP para añadir y gestionar volúmenes y servicios de datos adicionales. También debes crear un conector en AWS que permita a BlueXP gestionar los recursos y procesos dentro de tu entorno de nube pública.

Crear un entorno de trabajo FSX para ONTAP

Debes crear los entornos de trabajo de FSx para ONTAP en los que estén alojadas 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".

Puedes crear el entorno de trabajo de FSx para ONTAP mediante BlueXP o AWS. Si ha creado utilizando AWS, debe descubrir el FSX para sistemas ONTAP en BlueXP.

Cree un conector

Un administrador de cuenta debe crear un conector en AWS que permita a BlueXP gestionar recursos y procesos dentro de tu entorno de nube pública.

Para obtener más información, consulte "Creación de un conector en AWS desde BlueXP".

- Deberías utilizar el mismo conector para gestionar tanto el entorno de trabajo como las bases de datos de FSx for ONTAP.
- Si tiene el entorno de trabajo de FSx para ONTAP y las bases de datos en el mismo cloud privado virtual (VPC), puede poner en marcha el conector en la misma VPC.
- Si tienes el entorno de trabajo de FSx para ONTAP y las bases de datos en distintos PC:
  - Si tiene cargas de trabajo NAS (NFS) configuradas en FSx para ONTAP, puede crear el conector en cualquiera de los PC virtuales.
  - Si solo tiene cargas de trabajo SAN configuradas y no planea usar ninguna carga de trabajo NAS (NFS), debe crear el conector en la VPC donde se crea el sistema FSx para ONTAP.

> Para usar cargas de trabajo NAS (NFS), debe tener una pasarela de tránsito entre el VPC de la base de datos y Amazon 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** > **Lienzo** > **Mis entornos de trabajo** > **Agregar entorno de trabajo** y siga las indicaciones para agregar el entorno de trabajo. Asegúrese de que existe conectividad desde el conector a los hosts de la base de datos Oracle y el entorno de trabajo de FSx. El conector debe poder conectarse a la dirección IP de administración del clúster del entorno de trabajo de FSx.

- Agregue el entorno de trabajo haciendo clic en **Almacenamiento** > **Lienzo** > **Mis entornos de trabajo** > **Agregar entorno de trabajo**.

  Asegúrese de que haya conectividad entre el conector y los hosts de la base de datos y el entorno de trabajo de FSx para ONTAP. El conector debe conectarse a la dirección IP de gestión del clúster del entorno de trabajo de FSx para ONTAP.

- Copie el ID del conector haciendo clic en **Conector > Administrar conectores** y seleccionando el nombre del conector.

Configure Cloud Volumes ONTAP

Con BlueXP, deberías crear un entorno de trabajo de Cloud Volumes ONTAP para añadir y gestionar volúmenes y servicios de datos adicionales. También debes crear un conector para tu entorno de nube que permita a BlueXP gestionar los recursos y procesos dentro de tu entorno de nube pública.

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 más información, consulte una de las siguientes secciones:

- "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 de Cloud Volumes ONTAP como las bases de datos.

- Si tiene el entorno de trabajo de Cloud Volumes ONTAP y las bases de datos en el mismo cloud privado virtual (VPC) o vnet, puede poner en marcha el conector en la misma VPC o vnet.
- Si dispone del entorno de trabajo de Cloud Volumes ONTAP y de las bases de datos en distintos VPC o VNets, asegúrese de que los VPC o VNets están interconectados.

Configure Azure NetApp Files

Con BlueXP, deberías crear un entorno de trabajo de Azure NetApp Files para añadir y gestionar volúmenes y servicios de datos adicionales. También debes crear un conector en Azure que permita a BlueXP gestionar los recursos y procesos dentro de tu entorno de nube pública.

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 cuenta de BlueXP debería poner en marcha un conector en Azure que permita a BlueXP gestionar recursos y procesos dentro de tu entorno de nube pública.

Para obtener más información, consulte "Cree un conector en Azure desde BlueXP".

- Asegúrese de que existe conectividad entre el conector y los hosts de la base de datos.
- Si tiene el entorno de trabajo de Azure NetApp Files y las bases de datos en la misma red virtual (vnet), puede implementar el conector en el mismo vnet.
- Si tiene el entorno de trabajo y las bases de datos de Azure NetApp Files en distintas VNets y tiene cargas de trabajo NAS (NFS) configuradas en Azure NetApp Files, puede crear el conector en cualquiera de las VNets.

Después de crear el conector, agregue el entorno de trabajo haciendo clic en **Almacenamiento** > **Lienzo** > **Mis entornos de trabajo** > **Agregar entorno de trabajo**.

Instale el plugin de SnapCenter para Oracle y añada hosts de base de datos

Debe instalar el plugin de SnapCenter para Oracle en cada host de la base de datos de 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 la base de datos, puede instalar el plugin mediante uno de los métodos:
  - Instale el plugin y añada el host desde la interfaz de usuario mediante la opción SSH. Leer más.
  - Instale el plugin mediante un script y añada el host desde la interfaz de usuario mediante la opción manual. Leer más.
- Si SSH está deshabilitado, instale el plugin manualmente y añada el host desde la interfaz de usuario con 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 Connector tiene conectividad con los hosts de la base de datos Oracle.

  Para obtener información sobre cómo resolver el problema de conectividad, consulte "No se pudo validar la conectividad desde el host del conector de BlueXP al host de la base de datos de la aplicación".

  Cuando se pierde el conector o se ha creado un nuevo conector, debe asociar el conector a los recursos de la aplicación existentes. Para obtener instrucciones para actualizar el conector, consulte "Actualice los detalles del conector".

- Asegúrese de que el usuario de BlueXP tiene la función “Administrador de cuentas”.
- Asegúrese de que haya una cuenta no raíz (sudo) en el host de la aplicación para operaciones de protección de datos.
- 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.
- Asegúrese de que el conector tiene la comunicación habilitada al puerto SSH (predeterminado: 22) si se realiza una instalación basada en SSH.

- Asegúrese de que el conector tiene la comunicación habilitada para el puerto de conexión (valor predeterminado: 8145) para que las operaciones de protección de datos funcionen.
- Compruebe que tenga instalada la versión más reciente del plugin. Para actualizar el plugin, consulte Actualice el plugin de SnapCenter para base de datos de Oracle.

Añada el host desde la interfaz de usuario mediante la opción SSH

Pasos

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

   Si ya ha agregado un host y desea agregar otro host, haga clic en **Aplicaciones** > **Administrar bases de datos** > **Agregar** y, a continuación, continúe con el paso 5.

2. Haga clic en **detectar aplicaciones**.
3. Seleccione **nativo de la nube** y haga clic en **Siguiente**.

   Se crea una cuenta de servicio (*SnapCenter-account-<accountid>*) con el rol *SnapCenter System* para realizar operaciones de protección de datos programadas para todos los usuarios de esta cuenta. La cuenta de servicio (*SnapCenter-account-<accountid>*) se usa para ejecutar las operaciones de backup programadas. Nunca debe eliminar la cuenta de servicio. Puede ver la cuenta de servicio haciendo clic en **Cuenta** > **Administrar cuenta** > **Miembros**.

4. Seleccione Oracle como tipo de aplicación.
5. En la página de detalles 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.

      Asegúrese de que el conector se puede comunicar con el host de la base de datos mediante el FQDN o la dirección IP.

   c. Especifique el usuario no raíz(sudo) mediante el cual se copiará el paquete de plugins en el host.

      No se admite el usuario raíz.

   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 operación de protección de datos.

   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 usa para ninguna otra operación.

   c. Haga clic en **Siguiente**.

6. En la página Configuration, realice lo siguiente:
   a. Configure el acceso sudo para el usuario de SnapCenter en el host de la base de datos de Oracle iniciando sesión en la máquina Linux que ejecuta la base de datos de Oracle.
   b. Copia el texto que aparece en la interfaz de usuario de BlueXP.
   c. Cree el archivo */etc/sudoers.d/snapcenter* en la máquina Linux y pegue el texto copiado.
   d. En la interfaz de usuario de BlueXP, selecciona la casilla de verificación y haz clic en **Siguiente**.
7. Revise los detalles y haga clic en **Discover Applications**.
   - Una vez instalado el plugin, se inicia la operación de detección.
   - Después de completar la operación de detección, se muestran todas las bases de datos del host. Si la autenticación del sistema operativo está desactivada para la base de datos, haga clic en **Configurar** para habilitar la autenticación de la base de datos. 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 **Configuración** y seleccione **Directivas** para ver las directivas preparadas previamente. Revise las políticas predefinidas y puede editarlas para satisfacer sus requisitos o crear una nueva política.

Añada el host desde la interfaz de usuario con la opción manual e instale el plugin mediante script

Configure la autenticación basada en clave SSH para la cuenta de usuario no raíz del host de Oracle y realice los siguientes pasos para instalar el plugin.

Antes de empezar

Asegúrese de que la conexión SSH al conector está activada.

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 (*SnapCenter-account-<accountid>*) con el rol *SnapCenter System* para realizar operaciones de protección de datos programadas para todos los usuarios de esta cuenta. La cuenta de servicio (*SnapCenter-account-<accountid>*) se usa para ejecutar las operaciones de backup programadas. Nunca debe eliminar la cuenta de servicio. Puede ver la cuenta de servicio haciendo clic en **Cuenta** > **Administrar cuenta** > **Miembros**.
4. Seleccione Oracle como tipo de aplicación.
5. En la página de detalles Host, realice lo siguiente:
   a. Seleccione **Manual**.
   b. Especifique la dirección IP o FQDN del host donde se instaló el plugin.

      Asegúrese de que el conector se puede comunicar con el host de la base de datos mediante el FQDN o la dirección IP.

   c. Especifique el puerto del plugin.

El puerto predeterminado es 8145.

d. Especifique el usuario no raíz (sudo) mediante el cual se copiará el paquete de plugins en el host.
e. Seleccione el conector.
f. Seleccione la casilla de comprobación para confirmar que el plugin está instalado en el host.
g. Haga clic en **Siguiente**.

6. En la página Configuration, realice lo siguiente:
   a. Configure el acceso sudo para el usuario de SnapCenter en el host de la base de datos de Oracle iniciando sesión en la máquina Linux que ejecuta la base de datos de Oracle.
   b. Copia el texto que aparece en la interfaz de usuario de BlueXP.
   c. Cree el archivo */etc/sudoers.d/snapcenter* en la máquina Linux y pegue el texto copiado.
   d. En la interfaz de usuario de BlueXP, selecciona la casilla de verificación y haz clic en **Siguiente**.
7. Inicie sesión en el conector VM.
8. Instale el plugin mediante el script proporcionado en el conector.

```
sudo /var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

   Si está utilizando un conector antiguo, ejecute el siguiente comando para instalar el plugin.

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

Nombre	Descripción	Obligatorio	Predeterminado
host_plugin	Especifica el host de Oracle	Sí	-
nombre_usuario_host	Especifica el usuario SnapCenter con privilegios SSH en el host de Oracle	Sí	-
host_ssh_key	Especifica la clave SSH del usuario de SnapCenter y se utiliza para conectarse al host de Oracle	Sí	-
puerto_plugin	Especifica el puerto que utiliza el plugin	No	8145
puerto_ssh_host	Especifica el puerto SSH en el host de Oracle	No	22

Por ejemplo:

- `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`
- `sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

9. En la interfaz de usuario de BlueXP, revisa los detalles y haz clic en **Descubrir aplicaciones**.
   - Después de completar la operación de detección, se muestran todas las bases de datos del host. Si la autenticación del sistema operativo está desactivada para la base de datos, haga clic en **Configurar** para habilitar la autenticación de la base de datos. 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 **Configuración** y seleccione **Directivas** para ver las directivas preparadas previamente. Revise las políticas predefinidas y puede editarlas para satisfacer sus requisitos o crear una nueva política.

Añada el host desde la interfaz de usuario con la opción manual e instale el plugin manualmente

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

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 (*SnapCenter-account-<accountid>*) con el rol *SnapCenter System* para realizar operaciones de protección de datos programadas para todos los usuarios de esta cuenta. La cuenta de servicio (*SnapCenter-account-<accountid>*) se usa para ejecutar las operaciones de backup programadas. Nunca debe eliminar la cuenta de servicio. Puede ver la cuenta de servicio haciendo clic en **Cuenta** > **Administrar cuenta** > **Miembros**.

4. Seleccione Oracle como tipo de aplicación.
5. En la página **Detalles del host**, realice lo siguiente:
   a. Seleccione **Manual**.
   b. Especifique la dirección IP o FQDN del host donde se instaló 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. Especifique el usuario sudo no raíz (sudo) mediante la cual se copiará el paquete de plugins en el host.

e. Seleccione el conector.

f. Seleccione la casilla de comprobación para confirmar que el plugin está instalado en el host.

g. Haga clic en **Siguiente**.

6. En la página Configuration, realice lo siguiente:

   a. Configure el acceso sudo para el usuario de SnapCenter en el host de la base de datos de Oracle iniciando sesión en la máquina Linux que ejecuta la base de datos de Oracle.

   b. Copia el texto que aparece en la interfaz de usuario de BlueXP.

   c. Cree el archivo */etc/sudoers.d/snapcenter* en la máquina Linux y pegue el texto copiado.

   d. En la interfaz de usuario de BlueXP, selecciona la casilla de verificación y haz clic en **Siguiente**.

7. Inicie sesión en el conector VM.

8. 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'
   ```

   El binario del plugin está disponible en: *cd /var/lib/docker/volumes/service-manager[1]-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -Po «cloudmanager_scs_cloud:.*?«|sed -e's/ *$/'|cut -f2 -d»:)/sc-linux-host-plugin*

9. Copie *snapcenter_linux_host_plugin_scs.bin* de la ruta anterior a */home/<non root user (sudo)>/.sc_netapp* ruta de acceso para cada uno de los hosts de base de datos de Oracle ya sea usando scp u otros métodos alternativos.

10. Inicie sesión en el host de la base de datos Oracle con la cuenta no raíz (sudo).

11. Cambie el directorio a */home/<non root user>/.sc_netapp/* y ejecute el siguiente comando para habilitar los permisos de ejecución para el binario.
    ```
    chmod +x snapcenter_linux_host_plugin_scs.bin
    ```

12. Instale el plugin de Oracle como usuario sudo SnapCenter.
    ```
    ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
    ```

13. Copie la ruta de acceso *certificate.pem* from *<base_mount_path>/client/certificate/* de la máquina virtual de conector a */var/opt/snapcenter/spl/etc/* en el host del plugin.

14. Desplácese hasta */var/opt/snapcenter/spl/etc* y ejecute el comando keytool para importar el archivo certificate.pem.
    ```
    keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
    -deststorepass snapcenter -noprompt
    ```

15. Reinicie SPL: `systemctl restart spl`

16. 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>/PluginService/Version --cert
    /config/client/certificate/certificate.pem --key
    /config/client/certificate/key.pem
    ```

17. En la interfaz de usuario de BlueXP, revisa los detalles y haz clic en **Descubrir aplicaciones**.

    - Después de completar la operación de detección, se muestran todas las bases de datos del host. Si la autenticación del sistema operativo está desactivada para la base de datos, haga clic en **Configurar**

para habilitar la autenticación de la base de datos. 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 **Configuración** y seleccione **Directivas** para ver las directivas preparadas previamente. Revise las políticas predefinidas y puede editarlas para satisfacer sus requisitos o crear una nueva política.

Configurar las credenciales de la base de datos de Oracle

Es necesario configurar las credenciales de bases de datos 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, haga clic en **Configurar** para modificar la autenticación de la base de datos.
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.

3. Haga clic en **Configurar**.

Actualice el plugin de SnapCenter para base de datos de Oracle

Debe actualizar el plugin de SnapCenter para Oracle para obtener acceso a las nuevas funciones y mejoras más recientes. Puede realizar una actualización desde la interfaz de usuario de BlueXP o mediante la línea de comandos.

Antes de empezar

- Asegúrese de que no existan operaciones en ejecución en el host.

Pasos

1. Haga clic en **Copia de seguridad y recuperación** > **Aplicaciones** > **Hosts**.
2. Compruebe si la actualización de plugins está disponible para cualquiera de los hosts mediante la comprobación de la columna Overall Status.
3. Actualice el plugin desde la interfaz de usuario o mediante la línea de comandos.

Actualice mediante la IU	Actualice mediante la línea de comandos

a. Haga clic en ••• Correspondiente al host y haga clic en **Upgrade Plug-in**.
b. En la página Configuration, realice lo siguiente:
i. Configure el acceso sudo para el usuario de SnapCenter en el host de la base de datos de Oracle iniciando sesión en la máquina Linux que ejecuta la base de datos de Oracle.
ii. Copia el texto que aparece en la interfaz de usuario de BlueXP.
iii. Edite el archivo */etc/sudoers.d/snapcenter* en el equipo Linux y pegue el texto copiado.
iv. En la interfaz de usuario de BlueXP, selecciona la casilla de verificación y haz clic en **Actualizar**.
	a. Inicie sesión en Connector VM.
	b. Ejecute el siguiente script.
	`sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`
	
	Si utiliza un conector antiguo, ejecute el siguiente comando para actualizar el plugin.
	`sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`

Realizar backups de bases de datos de Oracle nativas en el cloud

Puede crear backups programados o bajo demanda mediante la asignación de una política predeterminada o la política que se haya creado.

También puede catalogar los backups de la base de datos de Oracle con Oracle Recovery Manager (RMAN) si habilitó la catalogación al crear una política. Solo se admite la catalogación (RMAN) para las bases de datos que se encuentran en Azure NetApp Files. Posteriormente, se pueden utilizar los backups catalogados para operaciones de restauración a nivel de bloque o de recuperación de un momento específico en el espacio de tabla. La base de datos debe estar en un estado montado o superior para la catalogación.

Cree una política para proteger la 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. Si ha seleccionado *DAILY* y *SEMANAL* como programa y desea activar la catalogación de RMAN, seleccione **Catalog backup with Oracle Recovery Manager (RMAN)**.
7. (Opcional) Introduzca la ruta de acceso posterior al script y el valor de tiempo de espera para el script posterior que se ejecutará después del backup correcto, como copiar la snapshot en el almacenamiento secundario.

   Opcionalmente, también puede especificar los argumentos.

   Debe conservar los scripts posteriores en la ruta */var/opt/snapcenter/spl/scripts*.

   El script POST soporta un conjunto de variables de entorno.

Variable ambiental	Descripción
SC_ORACLE_SID	Especifica el SID de la base de datos Oracle.
SC_HOST	Especifica el nombre de host de la base de datos
SC_BACKUP_NAME	Especifica el nombre del backup. El nombre de backup de datos y el nombre de backup de registros se concatenan mediante delimitadores.
SC_BACKUP_POLICY_NAME	Especifica el nombre de la política utilizada para crear el backup.
SC_PRIMARY_DATA_VOLUME_FULL_PATH	Especifica las rutas del volumen de datos concatenadas mediante el delimitador. Para volúmenes Azure NetApp Files, la información se concatena mediante «/» _ /Subscriptions/{subscription_id}/ResourceGroups/{resource_group}/providers/{provider}/netAppAccounts/{anfaccount}/capacityPools/{capacity_pool}/volumes/{volumename}_
SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH	Especifica las rutas de acceso del volumen de registros de archivos concatenadas mediante «,» como delimitador. Para volúmenes Azure NetApp Files, la información de la muestra concatenada usando «/» _ /Subscriptions/{subscription_id}/ResourceGroups/{resource_group}/providers/{provider}/netAppAccounts/{anfaccount}/capacityPools/{capacity_pool}/volumes/{volumename}_

1. Haga clic en **Crear**.

Configure el repositorio del catálogo de RMAN

Puede configurar la base de datos del catálogo de recuperación como repositorio de catálogos de RMAN. Si no configura el repositorio, por defecto, el archivo de control de la base de datos destino se convierte en el repositorio del catálogo de RMAN.

Antes de empezar

Debe registrar manualmente la base de datos de destino en la base de datos del catálogo RMAN.

Pasos

1. En la página aplicaciones, haga clic en ••• > **Ver detalles**.
2. En la sección Database details, haga clic en Para configurar el repositorio del catálogo de RMAN.
3. Especifique las credenciales para catalogar los backups con RMAN y el nombre de sustrato de red transparente (TNS) de la base de datos de recuperación de catálogos.
4. Haga clic en **Configurar**.

Cree un backup de la base de datos Oracle

Puede asignar una política predefinida o crear una política 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.

> Al crear grupos de discos de ASM en Amazon FSx para NetApp ONTAP o Cloud Volumes ONTAP, asegúrese de que no haya volúmenes comunes entre los 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. Si habilitó el catálogo de RMAN en la política, el backup al final del flujo de trabajo iniciará la operación de catalogación como un trabajo independiente. El progreso de la catalogación se puede ver en el Monitor de trabajos. Una vez realizada la catalogación, **Backup Details** mostrará el estado del catálogo para cada copia de seguridad.

   > La cuenta de servicio (*SnapCenter-account-<account_id>*) se usa 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 políticas a la aplicación, seleccione la política, el nivel de retención y, a continuación, haga clic en **Crear copia de seguridad**.

   Si habilitó el catálogo de RMAN en la política, el backup al final del flujo de trabajo iniciará la operación de catalogación como un trabajo independiente. El progreso de la catalogación se puede ver en el Monitor de trabajos. Una vez realizada la catalogación, **Backup Details** mostrará el estado del catálogo para cada copia de seguridad.

Limitaciones

- 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 tus bases de datos de Oracle se encuentran en Amazon FSx para ONTAP de NetApp o Cloud Volumes ONTAP y están configuradas en ASM, asegúrate de que los nombres de tus SVM sean únicos en todos 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.
- 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".

Información de copyright

Copyright © 2024 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.