Realice backups de bases de datos de Oracle

SnapCenter Software 4.5

NetApp
January 18, 2024

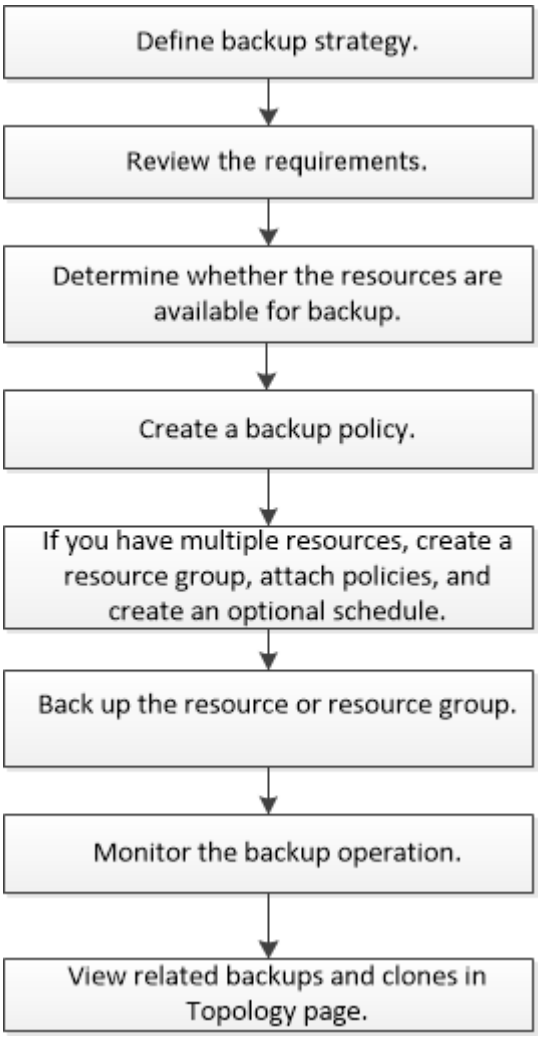
Tabla de contenidos

Realice backups de bases de datos de Oracle

Flujo de trabajo de backup

Es posible crear un backup de un recurso (base de datos) o un grupo de recursos. El flujo de trabajo de backup incluye planificación, identificación de los recursos para el backup, creación de políticas de backup, creación de grupos de recursos y vinculación de políticas, creación de backups y supervisión de las operaciones.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de backup:



Al crear un backup para bases de datos de Oracle, se crea un archivo de bloqueo operativo (.sm_lock_dbsid) en el host de la base de datos de Oracle, en el directorio *$ORACLE_HOME/DBS*, para evitar que se ejecuten varias operaciones en la base de datos. Después de realizar el backup de la base de datos, se elimina automáticamente el archivo de bloqueo operativo.

Sin embargo, si la copia de seguridad anterior se completó con una advertencia, es posible que el archivo de bloqueo operativo no se elimine y la próxima operación de copia de seguridad entra en la cola de espera. Es posible que finalmente se cancele si el archivo **.sm_lock_dbsid** no se elimina. En este caso, debe eliminar manualmente el archivo de bloqueo operativo siguiendo estos pasos:

1. En la línea de comandos, desplácese hasta $ORACLE_HOME/DBS.
2. Elimine el bloqueo operativo:`rm -rf .sm_lock_dbsid.`

Definir una estrategia de backup para bases de datos de Oracle

Definir una estrategia de backup antes de crear las tareas de backup garantiza que se cuente con todos los backups necesarios para restaurar o clonar correctamente las bases de datos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el RPO ayudan a establecer una estrategia de protección de datos.

Configuraciones de bases de datos de Oracle para backups admitidas

SnapCenter admite el backup de diferentes configuraciones de bases de datos de Oracle.

- Oracle independiente
- Real Application Clusters (RAC) de Oracle
- Oracle Standalone Legacy
- Base de datos de contenedores independiente de Oracle (CDB)
- Oracle Data Guard en espera

  Solo se pueden crear backups sin conexión montados de bases de datos en espera de Data Guard. No se admiten el backup sin conexión apagado, el backup de solo registro de archivos y el backup completo.

- Oracle Active Data Guard en espera

  Solo pueden crearse backups en línea de bases de datos en espera de Active Data Guard. No se admiten el backup solo de registro de archivo y el backup completo.

  > Antes de crear un backup de una base de datos en espera de Data Guard o Active Data Guard, se detiene el proceso de recuperación gestionado (MRP) y, una vez que se crea el backup, se inicia MRP.

- Gestión automática del almacenamiento (ASM)
  - ASM independiente y ASM RAC en disco de máquina virtual (VMDK)

    > Entre todos los métodos de restauración compatibles con las bases de datos de Oracle, solo se puede ejecutar la restauración por conexión y copia de bases de datos de ASM RAC en VMDK.

  - ASM independiente y ASM RAC en asignación de dispositivos sin formato (RDM) es posible realizar

operaciones de backup, restauración y clonado en bases de datos de Oracle en ASM, con o sin ASMLib.

- Controlador de filtro de Oracle ASM (ASMFD)

  No se admiten las operaciones de migración de PDB y clonado de PDB.

- Oracle Flex ASM

Para obtener la información más reciente sobre las versiones de Oracle admitidas, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Tipos de backup compatibles con las bases de datos de Oracle

El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite los tipos backup en línea y sin conexión para bases de datos de Oracle.

Backup en línea

Un backup que se crea cuando la base de datos está en estado en línea se denomina backup en línea. También denominado backup dinámico, un backup en línea permite crear un backup de la base de datos sin apagarlo.

Como parte del backup en línea, es posible crear un backup de los siguientes archivos:

- Solo archivos de datos y archivos de control
- Solo archivos del registro de archivos (en este escenario, la base de datos no se coloca en modo de backup)
- Base de datos completa, que incluye archivos de datos, archivos de control y archivos del registro de archivos

Backup sin conexión

Un backup creado cuando la base de datos está en estado montado o apagado se denomina backup sin conexión. Este tipo de backup también se denomina backup en frío. Es posible incluir solo archivos de datos y archivos de control en los backups sin conexión. Puede crear un backup sin conexión montado o apagado sin conexión.

- Cuando se crea un backup sin conexión montado, la base de datos debe estar en estado montado.

  Si está en cualquier otro estado, la operación de backup generará errores.

- Al crear un backup sin conexión apagado, la base de datos puede estar en cualquier estado.

  El estado de la base de datos se modifica para alcanzar el estado deseado y poder crear el backup. Después de crear el backup, el estado de la base de datos se revierte a su estado original.

Cómo detecta SnapCenter las bases de datos de Oracle

"Resources" son las bases de datos de Oracle en el host que mantiene SnapCenter. Es posible añadir estas bases de datos a grupos de recursos para realizar operaciones de protección de datos después de detectar las bases de datos disponibles. Debe tener en cuenta el proceso que sigue SnapCenter para detectar diferentes tipos y versiones de las bases de datos de Oracle.

Para las versiones de Oracle 11*g* a 12*c*R1	Para las versiones de Oracle 12*c*R2 a 18*c*_
Base de datos RAC: Las bases de datos RAC se detectan sólo sobre la base de entradas /etc/oratab. Deben tener las entradas de la base de datos en el archivo /etc/oratab.	**Base de datos RAC**: Las bases de datos RAC se detectan con el comando srvctl config.
Standalone: Las bases de datos independientes se detectan sólo sobre la base de entradas /etc/oratab. Deben tener las entradas de la base de datos en el archivo /etc/oratab.	**Standalone**: Las bases de datos independientes se detectan según las entradas del archivo /etc/oratab y la salida del comando srvctl config.
ASM: La entrada de instancia ASM debería estar disponible en el archivo /etc/oratab.	**ASM**: No es necesario que la entrada de instancia ASM esté en el archivo /etc/oratab.

Para las versiones de Oracle 11*g* a 12*c*R1	Para las versiones de Oracle 12*c*R2 a 18*c*_
RAC One Node: Las bases de datos RAC One Node se detectan sólo sobre la base de entradas /etc/oratab. Las bases de datos deben estar en el estado *nomount*, *Mount* o *open*. Deben tener las entradas de la base de datos en el archivo /etc/oratab. El estado de la base de datos de RAC One Node se marcará como cambiado de nombre o se eliminará si la base de datos ya se detecta y los backups se asocian a la base de datos. Si se reubica la base de datos, debe realizar los siguientes pasos: 1. Añada manualmente la entrada de la base de datos reubicada en el archivo /etc/oratab en el nodo RAC con error. 2. Actualice manualmente los recursos. 3. Seleccione la base de datos RAC One Node de la página de recursos y, a continuación, haga clic en **Configuración de base de datos**. 4. Configure la base de datos para establecer los nodos de clúster preferidos en el nodo de RAC que aloja actualmente la base de datos. 5. Ejecute las operaciones de SnapCenter. Si se recolocó una base de datos de un nodo a otro y si la entrada oratab del nodo anterior no se elimina, se debe eliminar manualmente la entrada oratab para evitar que la misma base de datos se muestre dos veces.	**RAC One Node**: Las bases de datos RAC One Node se detectan sólo con el comando srvctl config . Las bases de datos deben estar en el estado *nomount*, *Mount* o *open*. El estado de la base de datos de RAC One Node se marcará como cambiado de nombre o se eliminará si la base de datos ya se detecta y los backups se asocian a la base de datos. Si se reubica la base de datos, debe realizar los siguientes pasos: 1. Actualice manualmente los recursos. 2. Seleccione la base de datos RAC One Node en la página de recursos y, a continuación, haga clic en **Configuración de base de datos**. 3. Configure la base de datos para establecer los nodos de clúster preferidos en el nodo de RAC que aloja actualmente la base de datos. 4. Ejecute las operaciones de SnapCenter.

Si hay alguna entrada de base de datos de Oracle 12*c*R2 y 18*c* en el archivo /etc/oratab y la misma base de datos se registra con el comando srvctl config, SnapCenter eliminará las entradas de base de datos duplicadas. Si hay entradas obsoletas de la base de datos, la base de datos se descubrirá, pero no se podrá acceder a la base de datos y el estado será sin conexión.

Nodos preferidos en la configuración de RAC

En una configuración de Real Application Clusters (RAC) de Oracle, es posible especificar los nodos preferidos para ejecutar la operación de backup. Si no se especifica un nodo preferido, SnapCenter asigna automáticamente un nodo como preferido y lo usa para crear el backup.

Los nodos preferidos pueden ser uno o varios de los nodos del clúster donde se encuentran las instancias de la base de datos de RAC. La operación de backup se activa únicamente en esos nodos preferidos en el orden

de preferencia indicado.

Ejemplo: La base de datos de RAC cdbrac tiene tres instancias: Cdbrac1 en el nodo 1, cdbrac2 en el nodo 2 y cdbrac3 en el nodo 3. Las instancias 1 y 2 están configuradas como preferidos, con el nodo 2 en el primer lugar de preferencia y el nodo 1 en el segundo. Cuando se ejecuta una operación de backup, primero se intenta en el nodo 2, ya que es el primero en preferencia. Si el nodo 2 no tiene un estado adecuado para el backup, lo cual puede deberse a diversos motivos, por ejemplo, que el agente del plugin no esté en ejecución en el host, la instancia de la base de datos del host no tiene el estado requerido para el tipo de backup especificado, O la instancia de base de datos del nodo 2 en una configuración de FlexASM no sirve a la instancia de ASM local; luego se intenta ejecutar la operación en el nodo 1. El nodo 3 no se usará para el backup, ya que no es parte de la lista de nodos preferidos.

En una configuración de Flex ASM, los nodos de hoja no se mostrarán como nodos preferidos si la cardinalidad es inferior al número de nodos del clúster de RAC. Si hay algún cambio en las funciones del nodo del clúster de ASM de Flex, debe detectar manualmente para que se actualicen los nodos preferidos.

Estado de la base de datos necesario

Las instancias de base de datos de RAC de los nodos preferidos deben tener el estado necesario para que el backup se ejecute correctamente:

- Una de las instancias de base de datos de RAC de los nodos preferidos configurados debe tener el estado abierto para que se pueda crear un backup en línea.
- Una de las instancias de base de datos de RAC de los nodos preferidos configurados debe tener el estado de montaje y las demás instancias, incluidos los demás nodos preferidos, deben tener el estado de montaje o un valor inferior para crear un backup de montaje sin conexión.
- Las instancias de base de datos de RAC pueden tener cualquier estado, pero es necesario especificar los nodos preferidos para poder crear un backup de apagado sin conexión.

Cómo catalogar backups con Oracle Recovery Manager

Es posible catalogar los backups de bases de datos de Oracle con Oracle RMAN para almacenar la información de backups en el repositorio de Oracle RMAN.

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. Cuando no se necesitan estos backups catalogados, es posible quitar la información de catálogo.

La base de datos debe estar en un estado montado o superior para la catalogación. Es posible realizar la catalogación en backups de datos, backups de registros de archivo y backups completos. Si se habilita la catalogación para un backup de un grupo de recursos que contiene varias bases de datos, se realiza la catalogación en cada base de datos. Para las bases de datos de Oracle RAC, la catalogación se realiza en el nodo preferido donde la base de datos se encuentra al menos en estado montado.

> Si desea catalogar backups de una base de datos de RAC, asegúrese de que no exista otro trabajo en ejecución para esa base de datos. Si existe otro trabajo en ejecución, la operación de catalogación genera un error se interrumpe tras generar un error y no se colocar en cola.

De forma predeterminada, se utiliza el archivo de control de la base de datos de destino para la catalogación. Si desea añadir una base de datos de catálogo externo, puede especificar la credencial y el nombre de sustrato de red transparente (TNS) para el catálogo externo en el asistente Database Settings de la interfaz gráfica de usuario (GUI) de SnapCenter para configurar esa base de datos. También es posible ejecutar el comando Configure-SmOracleDatabase con las opciones -OracleRmanCatalogCredentialName y

-OracleRmanCatalogTnsName para configurar la base de datos de catálogo externo desde la interfaz de línea de comandos.

Si habilitó la opción de catalogación durante la creación de una política de backup de Oracle desde la interfaz gráfica de usuario de SnapCenter, los backups se catalogan mediante Oracle RMAN como parte de la operación de backup. También puede ejecutar el comando Catalog-SmBackupWithOracleRMAN para realizar una catalogación diferida de backups. Después de catalogar los backups, puede ejecutar el comando Get-SmBackupDetails para obtener la información de backups catalogados, como las ubicaciones de los registros de archivo, la etiqueta para los archivos de datos catalogados y la ruta de catálogo para el archivo de control.

Si el nombre del grupo de discos de ASM contiene 16 caracteres o más, en SnapCenter 3.0, el formato de nomenclatura que se utiliza para el backup es SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. Sin embargo, si el nombre del grupo de discos tiene menos de 16 caracteres, el formato de nomenclatura utilizado para la copia de seguridad es DISKGROUPNAME_DBSID_BACKUPID, que es el mismo formato utilizado en SnapCenter 2.0.

> HASHCODEofDISKGROUP es un número generado automáticamente (de 2 a 10 dígitos) que es exclusivo de cada grupo de discos de ASM.

Es posible realizar verificaciones cruzadas para actualizar la información obsoleta en el repositorio de RMAN sobre los backups con registros de repositorio que no coinciden con su estado físico. Por ejemplo, si un usuario quita registros archivados del disco con un comando del sistema operativo, se seguirá indicando en el archivo de control que los registros están en el disco, cuando realmente no lo están. La operación de verificación cruzada permite actualizar el archivo de control con la información. Para habilitar la verificación cruzada, puede ejecutar el comando Set-SmConfigSettings y asignar el valor TRUE al parámetro ENABLE_CROSSCHECK. De forma predeterminada, el valor se establece en FALSE.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Para quitar la información de catálogo, puede ejecutar el comando Uncatalog-SmBackupWithOracleRMAN. No se puede quitar la información de catálogo mediante la interfaz gráfica de usuario de SnapCenter. Sin embargo, la información de un backup catalogado se quita mientras se elimina el backup o mientras se eliminan la retención y el grupo de recursos asociado a ese backup catalogado.

> Cuando se fuerza la eliminación de un host de SnapCenter, no se quita la información de los backups catalogados asociados a ese host. Es necesario quitar la información de todos los backups catalogados de ese host para poder forzar la eliminación del host.

Si se produce un error de catalogación y descatalogación porque el tiempo de la operación superó el valor especificado de tiempo de espera en el parámetro ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT, debe modificar el valor del parámetro ejecutando el siguiente comando:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Después de modificar el valor del parámetro, reinicie SnapCenter el servicio del SPL con el siguiente comando:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help nombre_comando. Como alternativa, también puede consultar la "Guía de

referencia de comandos del software SnapCenter".

Programaciones de backup

La frecuencia de los backups (tipo de programación) se especifica en las políticas; la programación de los backups se especifica en la configuración del grupo de recursos. El factor más crítico para determinar la frecuencia o la programación de los backups es la tasa de cambio del recurso y la importancia de los datos. Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores son la importancia del recurso para la organización, el SLA y el RPO.

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso en el caso de un recurso utilizado intensivamente, no existe el requisito de ejecutar un backup completo más de una o dos veces al día. Por ejemplo, es posible que sea suficiente realizar backups regulares de registros de transacciones para garantizar los backups necesarios Cuanto mayor sea la frecuencia con que realiza backups de las bases de datos, menos registros de transacciones deberá utilizar SnapCenter en el momento de la restauración, lo que puede dar como resultado operaciones más rápidas.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

  La frecuencia de los backups (cada cuánto tiempo deben realizarse los backups), denominada *schedule type* para algunos plugins, forma parte de la configuración de una política. Se puede seleccionar una frecuencia de backups por hora, por día, por semana o por mes para la política. Si no selecciona ninguna de estas frecuencias, la política creada es de sólo bajo demanda. Puede acceder a las directivas haciendo clic en **Configuración** > **Directivas**.

- Programaciones de backup

  Las programaciones de los backups (el momento exacto en que se realizan los backups) forman parte de una configuración de grupo de recursos. Por ejemplo, si tiene un grupo de recursos que posee una política configurada para backups semanales, quizás sea conveniente configurar la programación para que realice backups todos los jueves a las 00:10. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos** > **grupos de recursos**.

Convenciones de nomenclatura de backups

Es posible usar la convención de nomenclatura de copia Snapshot predeterminada o usar una convención de nomenclatura personalizada. La convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de las copias de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La copia Snapshot usa la siguiente convención de nomenclatura predeterminada:

```
resourcegroupname_hostname_timestamp
```

Es necesario asignar un nombre a los grupos de recursos de backup de forma lógica, como en el ejemplo siguiente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de la sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre de host.
- *03-12-2015_23.17.26* es la fecha y la marca de hora.

Como alternativa, puede especificar el formato de nombre de la copia Snapshot mientras protege los recursos o grupos de recursos seleccionando **usar formato de nombre personalizado para copia Snapshot**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la copia de Snapshot.

Opciones de retención de backups

Es posible elegir la cantidad de días durante los cuales se retendrán las copias de backup o especificar la cantidad de copias de backup que se desean retener, con un máximo de 255 copias en ONTAP. Por ejemplo, una organización puede necesitar retener 10 días de copias de backup o 130 copias de backup.

Al crear una política, es posible especificar las opciones de retención para cada tipo y programación de backup.

Si se configura la replicación de SnapMirror, la política de retención se refleja en el volumen de destino.

SnapCenter elimina los backups previos que tengan etiquetas de retención que coincidan con el tipo de programación. Si se modifica el tipo de programación para el recurso o el grupo de recursos, los backups con la etiqueta del tipo de programación anterior podrían conservarse en el sistema.

> Para la retención a largo plazo de copias de backup, es conveniente usar el backup de SnapVault.

Verifique la copia de backup con un volumen de almacenamiento primario o secundario

Es posible verificar las copias de backups en el volumen de almacenamiento principal o en el volumen de almacenamiento secundario de SnapMirror y SnapVault. La verificación con un volumen de almacenamiento secundario reduce la carga para el volumen de almacenamiento principal.

Cuando se verifica un backup que se encuentra en el volumen de almacenamiento primario o secundario, todas las copias de Snapshot primarias y secundarias se marcan como verificadas.

Se necesita una licencia de SnapRestore para verificar copias de backup en un volumen de almacenamiento secundario de SnapMirror o SnapVault.

Determinar si las bases de datos de Oracle están disponibles para backup

Los recursos son bases de datos de Oracle en el host gestionado por SnapCenter. Es posible añadir estas bases de datos a grupos de recursos para realizar operaciones de

protección de datos después de detectar las bases de datos disponibles.

Lo que necesitará

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir hosts, crear conexiones con el sistema de almacenamiento y añadir credenciales.
- Si las bases de datos residen en un disco de máquina virtual (VMDK) o una asignación de dispositivo sin formato (RDM), es necesario implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter.

  Para obtener más información, consulte "Ponga en marcha el plugin de SnapCenter para VMware vSphere".

- Si las bases de datos residen en un sistema de archivos VMDK, debe haber iniciado sesión en vCenter y navegado hasta **VM options** > **Advanced** > **Edit Configuration** para configurar el valor de *disk.enableUUID* en true para la máquina virtual.
- Debe haber revisado el proceso que sigue SnapCenter para detectar diferentes tipos y versiones de las bases de datos de Oracle.

Acerca de esta tarea

Después de instalar el plugin, todas las bases de datos en ese host se detectan de forma automática y se muestran en la página Resources.

Las bases de datos deben estar en estado montado o superior para que la detección de la base de datos sea exitosa. En un entorno Oracle RAC, la instancia de la base de datos de RAC en el host donde se realiza la detección, debe estar en estado montado o superior para que la detección de la instancia de la base de datos sea exitosa. Solo las bases de datos que se detecten exitosamente pueden añadirse a los grupos de recursos.

Si eliminó una base de datos de Oracle en el host, el servidor de SnapCenter no tendrá conocimiento y enumerará la base de datos eliminada. Debe actualizar manualmente los recursos para actualizar la lista de recursos de SnapCenter.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Database** en la lista **View**.

     Haga clic en y, a continuación, seleccione el nombre de host y el tipo de base de datos para filtrar los recursos. A continuación, haga clic en el para cerrar el panel de filtros.

  3. Haga clic en **Actualizar recursos**.

     En un escenario de RAC One Node, la base de datos se detecta como la base de datos de RAC en el nodo en el que está alojado actualmente.

Resultados

Las bases de datos se muestran junto con información como el tipo de base de datos, el nombre del clúster o host, las políticas y los grupos de recursos asociados, y el estado.

- Si la base de datos está en un sistema de almacenamiento de terceros, la interfaz de usuario muestra el mensaje Not available for backup en la columna Overall Status.

No es posible realizar operaciones de protección de datos en una base de datos que está en un sistema de almacenamiento de terceros.

- Si la base de datos está en un sistema de almacenamiento de NetApp y no está protegida, la interfaz de usuario muestra un mensaje Not protected en la columna Overall Status.
- Si la base de datos está en un sistema de almacenamiento de NetApp y está protegida, la interfaz de usuario muestra un mensaje Available for backup en la columna Overall Status.

> Si habilitó una autenticación de base de datos de Oracle, se muestra un icono de candado rojo en la vista de recursos. Es necesario configurar las credenciales de la base de datos para poder proteger la base de datos, o bien añadirla al grupo de recursos para realizar operaciones de protección de datos.

Crear políticas de backup para bases de datos de Oracle

Antes de usar SnapCenter para realizar backups de recursos de base de datos de Oracle, debe crear una política de backup para el recurso o el grupo de recursos que se respaltendrá. Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups. También puede especificar la configuración de replicación, script y tipo de backup. Crear una política permite ahorrar tiempo cuando se desea volver a utilizar esa política en otro recurso o grupo de recursos.

Lo que necesitará

- Debe tener definida una estrategia de backup.
- En el marco de los preparativos para la protección de datos, completó tareas como instalar SnapCenter, añadir hosts, detectar bases de datos y crear conexiones del sistema de almacenamiento.
- Si desea replicar copias de Snapshot en un almacenamiento secundario con SnapMirror o SnapVault, el administrador de SnapCenter debe haberle asignado las SVM de los volúmenes de origen y de destino.
- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Directivas**.
  3. Seleccione **Oracle Database** en la lista desplegable.
  4. Haga clic en **Nuevo**.
  5. En la página Name, escriba el nombre de la política y una descripción.
  6. En la página Backup Type, realice los siguientes pasos:

     - Si desea **crear una copia de seguridad en línea**, seleccione **copia de seguridad en línea**.

       Debe especificar si desea realizar un backup de todos los archivos de datos, los archivos de control y los archivos de registro de archivos, solo de los archivos de datos y los archivos de control, o solo de los archivos de registro de archivos.

     - Si desea **crear una copia de seguridad sin conexión**, seleccione **copia de seguridad sin conexión** y, a continuación, seleccione una de las siguientes opciones:

       - Si desea crear una copia de seguridad sin conexión cuando la base de datos está en estado montado, seleccione **Mount**.

- Si desea crear una copia de seguridad de apagado sin conexión cambiando el estado de la base de datos a apagado, seleccione **Apagar**.

  Si tiene bases de datos conectables (PDB) y desea guardar el estado de las PDB antes de crear el backup, debe seleccionar **Guardar estado de PDB**. Esto permite que las PDB regresen a su estado original después de la creación del backup.

- Especifique la frecuencia de programación seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.

  Es posible especificar la programación (fecha de inicio y fecha de finalización) para la operación de backup mientras se crea un grupo de recursos. De este modo, puede crear grupos de recursos que compartan la misma política y la misma frecuencia de backup, pero también asignar diferentes programaciones de backup a cada política.

  Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

- Si desea catalogar la copia de seguridad con Oracle Recovery Manager (RMAN), seleccione **Catalog backup with Oracle Recovery Manager (RMAN)**.

  Puede realizar una catalogación diferida de un backup a la vez con la interfaz gráfica de usuario o con el comando Catalog-SmBackupWithOracleRMAN de la CLI de SnapCenter.

  Si desea catalogar backups de una base de datos de RAC, asegúrese de que no exista otro trabajo en ejecución para esa base de datos. Si existe otro trabajo en ejecución, la operación de catalogación genera un error se interrumpe tras generar un error y no se colocar en cola.

- Si desea reducir los registros de archivos después de la copia de seguridad, seleccione **Prune archive logs after backup**.

  Se omitirá la eliminación de registros de archivo desde el destino del registro de archivos que no esté configurado en la base de datos.

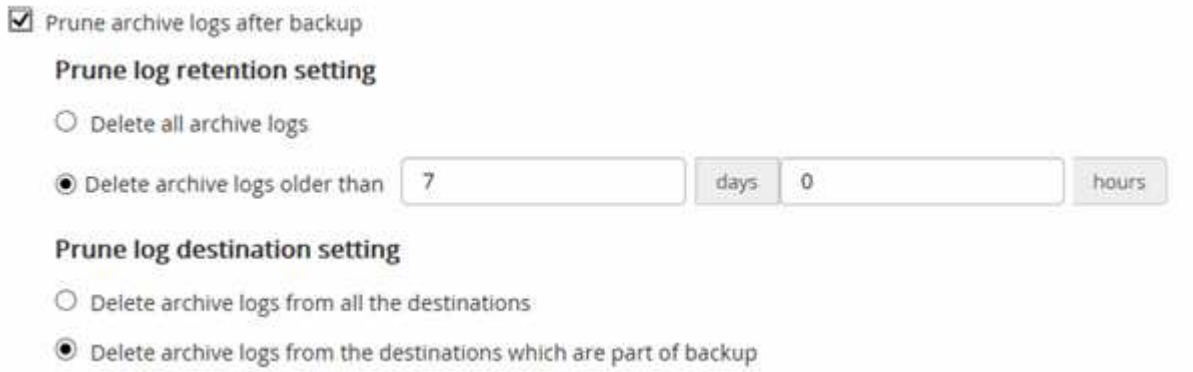
  Si está utilizando Oracle Standard Edition, puede utilizar los parámetros LOG_ARCHIVE_DEST y LOG_ARCHIVE_DUPLEX_DEST al realizar una copia de seguridad del registro de archivos.

- Puede eliminar los registros de archivos únicamente si seleccionó los archivos de registro de archivos como parte del backup.

  Debe asegurarse de que todos los nodos en el entorno RAC puedan acceder a todas las ubicaciones del registro de archivos para que la operación de eliminación se complete correctamente.

Si desea…	Realice lo siguiente…
Elimine todos los registros de archivos	Seleccione **Eliminar todos los registros de archivo**.

Si desea…	Realice lo siguiente…
Elimine los registros de archivos antiguos	Seleccione **Eliminar registros de archivo de más de** y, a continuación, especifique la antigüedad de los registros de archivo que se eliminarán en días y horas.
Elimine los registros de archivos en todos los destinos	Seleccione **Eliminar registros de archivo de todos los destinos**.
Eliminar los registros de archivos de los destinos de registro que forman parte del backup	Seleccione **Eliminar registros de archivo de los destinos que forman parte de copia de seguridad**.



+

7. En la página Retention, especifique la configuración de retención para el tipo de backup y el tipo de programación seleccionados en la página Backup Type:

Si desea…	Realice lo siguiente…

Conservar una cierta cantidad de copias de Snapshot	Seleccione **total Snapshot copies to keep** y, a continuación, especifique el número de copias Snapshot que desea conservar. Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas. El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente. Debe establecer el número de retención en 2 o un valor más alto si tiene pensado habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino.
Conserve las copias de Snapshot por una cierta cantidad de días	Seleccione **mantener copias Snapshot para** y, a continuación, especifique el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas.

Puede retener los backups de registros de archivos únicamente si seleccionó los archivos de registro de archivos como parte del backup.

8. En la página Replication, especifique la configuración de replicación:

Para este campo…	Realice lo siguiente…
Actualizar SnapMirror tras crear una copia Snapshot local	Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror).
Actualizar SnapVault después de crear una copia Snapshot local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault).

Para este campo…	Realice lo siguiente…
Etiqueta de la política secundaria	Seleccione una etiqueta de Snapshot. Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta. Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria.
Número de reintentos con error	Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga.

Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar alcanzar el límite máximo de copias de Snapshot en el almacenamiento secundario.

9. En la página Script, introduzca la ruta y los argumentos del script previo o script posterior que desea ejecutar antes o después de la operación de backup, según corresponda.

   Debe almacenar los scripts previos y los scripts posteriores en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar los scripts, debe especificar esas carpetas en la ruta.

   También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60 segundos.

10. En la página Verification, realice los siguientes pasos:

    a. Seleccione la programación de backups donde desea realizar la operación de verificación.

    b. En la sección Verification script, introduzca la ruta de acceso y los argumentos del script previo o el script posterior que desea ejecutar antes o después de la operación de verificación, respectivamente.

       Debe almacenar los scripts previos y los scripts posteriores en */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de esta ruta de acceso. De forma predeterminada, se completa la ruta de acceso */var/opt/snapcenter/spl/scripts*. Si creó cualquier carpeta dentro de esta ruta de acceso para almacenar los scripts, debe especificar esas carpetas en la ruta.

También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60

segundos.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Crear grupos de recursos y vincular políticas para bases de datos de Oracle

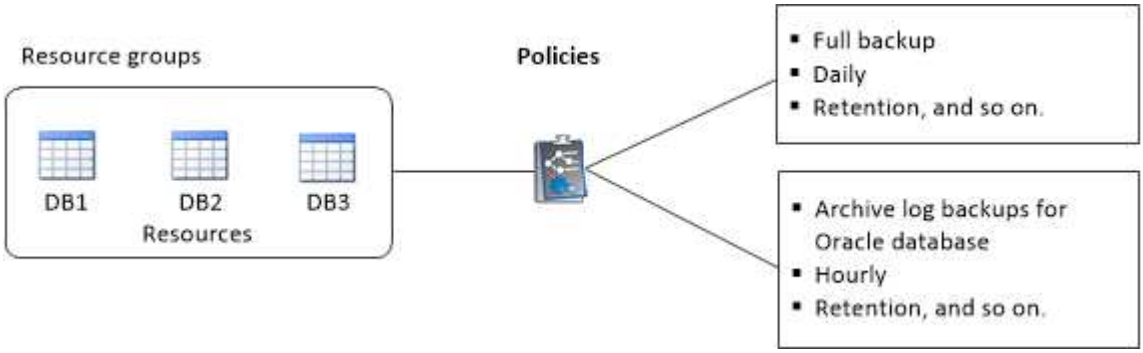
Un grupo de recursos es el contenedor al que debe añadir los recursos que desea proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación.

Acerca de esta tarea

Debe asegurarse de que la base de datos que tiene archivos en los grupos de discos ASM debe estar en estado "MOUNT" o "OPEN" para verificar sus copias de seguridad con la utilidad Oracle DBVERIFY.

Debe añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para las bases de datos:



- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. El nombre del grupo de recursos no debe superar los 250 caracteres.

Para este campo…	Realice lo siguiente…
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos. Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.
Utilice un formato de nombre personalizado para la copia de Snapshot	Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.
Excluir destinos de registro de archivos de la copia de seguridad	Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

4. En la página Resources, seleccione un nombre de host de la base de datos Oracle en la lista desplegable **Host**.

   Los recursos aparecen en la sección Available Resources solo si se detectan correctamente. Si agregó recursos recientemente, aparecerán en la lista de recursos disponibles únicamente después de actualizar la lista de recursos.

5. Seleccione los recursos de la sección Available Resources y muévalos a la sección Selected Resources.

   Puede agregar bases de datos desde hosts Linux y AIX en un solo grupo de recursos.

6. En la página Policies, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

      También puede crear una política haciendo clic en + .

      En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   b. Haga clic en + En la columna Configurar programaciones de la directiva para la que desea configurar una programación.

   c. En la ventana Add schedules for policy *policy_name*, configure la programación y haga clic en **OK**.

Donde, *policy_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

7. En la página Verification, realice los siguientes pasos:
   a. Haga clic en **Load locators** para cargar los volúmenes de SnapMirror o SnapVault y realizar la verificación en el almacenamiento secundario.
   b. Haga clic en + En la columna Configure Schedules para configurar la programación de verificación de todos los tipos de programación de la política.
   c. En el cuadro de diálogo Add Verification Schedules *policy_name*, realice las siguientes acciones:

Si desea…	Realice lo siguiente…
Ejecutar la verificación después del backup	Seleccione **Ejecutar verificación después de la copia de seguridad**.
Programar una verificación	Seleccione **Ejecutar verificación programada** y, a continuación, seleccione el tipo de programa en la lista desplegable.

   d. Seleccione **verificar en la ubicación secundaria** para verificar las copias de seguridad en el sistema de almacenamiento secundario.
   e. Haga clic en **Aceptar**.

      Las programaciones de verificación configuradas aparecerán en la columna Applied Schedules.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

   > Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Requisitos para realizar backups de una base de datos de Oracle

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

- Debe tener creado un grupo de recursos con una política anexada.

- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Asignó el agregado que utiliza la operación de backup a la SVM que utiliza la base de datos.
- Verificó que todos los volúmenes de datos y los volúmenes de registros de archivos que pertenecen a la base de datos están protegidos si la protección secundaria está habilitada para esa base de datos.
- Debe haber comprobado que la base de datos que contiene archivos en los grupos de discos ASM debe estar en el estado "DESMONTAR" o "ABIERTO" para verificar sus copias de seguridad con la utilidad Oracle DBVERIFY.
- Debe haber verificado que la longitud del punto de montaje del volumen no supera los 240 caracteres.
- Aumente el valor de RESTTimeout a 86400000 segundos en *C:\Program Files\NetApp \SMCore\SMCoreServiceHost.exe.config* en el host de SnapCenter Server, si la base de datos de la que se realiza el backup es grande (tamaño en TB).

  Mientras se modifican los valores, se garantiza que no haya trabajos en ejecución y se reinicia el servicio SnapCenter SMCore después de aumentar el valor.

Realice backup de recursos de Oracle

Si un recurso no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Database** en la lista **View**.
  3. Haga clic en y luego seleccione el nombre de host y el tipo de base de datos para filtrar los recursos.

     A continuación, puede hacer clic en para cerrar el panel de filtros.
  4. Seleccione la base de datos de la que desea realizar el backup.

     Aparece la página Database-Protect.
  5. En la página Resource, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Utilice un formato de nombre personalizado para la copia de Snapshot	Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot. Por ejemplo, customtext__policy_hostname o resource_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.
Excluir destinos de registro de archivos de la copia de seguridad	Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

6. En la página Policies, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

   > También puede crear una directiva haciendo clic en + .

   En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   b. Haga clic en + En la columna Configure Schedules correspondiente a la política para la cual se desea configurar una programación.

   c. En la ventana Add schedules for policy *policy_name*, configure la programación y haga clic en **OK**.

   policy_name es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

7. En la página Verification, realice los siguientes pasos:

   a. Haga clic en **Load locators** para cargar los volúmenes de SnapMirror o SnapVault y realizar la verificación en el almacenamiento secundario.

   b. Haga clic en + En la columna Configure Schedules, a fin de configurar la programación de verificación de todos los tipos de programación de la política.

   c. En el cuadro de diálogo Add Verification Schedules *policy_name*, realice las siguientes acciones:

Si desea…	Realice lo siguiente…
Ejecutar la verificación después del backup	Seleccione **Ejecutar verificación después de la copia de seguridad**.

Si desea…	Realice lo siguiente…
Programar una verificación	Seleccione **Ejecutar verificación programada** y, a continuación, seleccione el tipo de programa en la lista desplegable. En una configuración de Flex ASM, no puede realizar la operación de verificación en los nodos Leaf si la cardinalidad es menor que el número de nodos del clúster RAC.

d. Seleccione **verificar en la ubicación secundaria** para verificar las copias de seguridad en el almacenamiento secundario.

e. Haga clic en **Aceptar**.

Las programaciones de verificación configuradas aparecerán en la columna Applied Schedules.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea asociar el informe de la operación de backup ejecutada en el recurso y, a continuación, seleccione **Attach Job Report**.

   Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Se muestra la página de topología de la base de datos.

2. Haga clic en **copia de seguridad ahora**.
3. En la página Backup, realice los siguientes pasos:

   a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

   Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.

4. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Después de terminar

- En la configuración de AIX, puede utilizar el mandato lkdev para bloquear y el mandato rendev para cambiar el nombre de los discos en los que reside la base de datos de la que se ha realizado la copia de seguridad.

El bloqueo o cambio de nombre de los dispositivos no afectará a la operación de restauración al restaurar mediante esa copia de seguridad.

- Si se produce un error en la operación de backup porque el tiempo de ejecución de la consulta de base de datos superó el valor de tiempo de espera, debe cambiar el valor de los parámetros ORACLE_SQL_QUERY_TIMEOUT Y ORACLE_PLUGIN_SQL_QUERY_TIMEOUT con el cmdlet Set-SmConfigSettings:

  Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si no se puede acceder al archivo y el punto de montaje no está disponible durante el proceso de verificación, puede que se produzca un error en la operación con el código de error DBV-00100 specified file. Debe modificar los valores de los parámetros VERIFICATION_DELAY y VERIFICATION_RETRY_COUNT en sco.properties.

  Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.
- Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup.

  Para aumentar el tamaño de pila de Java, busque el archivo de script */opt/netapp/init_scripts/svservice*. En ese script, la `do_start method` Command inicia el servicio de plugin de VMware de SnapCenter. Actualice este comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

Más información

- "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"
- "Se omite la base de datos de Oracle RAC One Node para ejecutar operaciones de SnapCenter"
- "Se produjo un error al cambiar el estado de una base de datos de ASM de Oracle 12c"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

Realice backups de grupos de recursos de bases de datos de Oracle

Un grupo de recursos es una agrupacion de recursos en un host o un clúster. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.

2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Puede buscar el grupo de recursos escribiendo el nombre en el cuadro de búsqueda o haciendo clic en y, a continuación, seleccionar la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. En la página Resource Groups, seleccione el grupo de recursos que desea incluir en un backup y, a continuación, haga clic en **Back up Now**.

   > Si posee un grupo de recursos federado con dos bases de datos y una de ellas tiene el archivo de datos en un almacenamiento de terceros, se cancelará la operación de backup aunque la otra base de datos esté en almacenamiento de NetApp.

4. En la página Backup, realice los siguientes pasos:
   a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

      Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

   b. Haga clic en **copia de seguridad**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Después de terminar

- En la configuración de AIX, puede utilizar el mandato lkdev para bloquear y el mandato rendev para cambiar el nombre de los discos en los que reside la base de datos de la que se ha realizado la copia de seguridad.

  El bloqueo o cambio de nombre de los dispositivos no afectará a la operación de restauración al restaurar mediante esa copia de seguridad.

- Si se produce un error en la operación de backup porque el tiempo de ejecución de la consulta de base de datos superó el valor de tiempo de espera, debe cambiar el valor de los parámetros ORACLE_SQL_QUERY_TIMEOUT Y ORACLE_PLUGIN_SQL_QUERY_TIMEOUT con el cmdlet Set-SmConfigSettings:

  Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si no se puede acceder al archivo y el punto de montaje no está disponible durante el proceso de verificación, puede que se produzca un error en la operación con el código de error DBV-00100 specified file. Debe modificar los valores de los parámetros VERIFICATION_DELAY y VERIFICATION_RETRY_COUNT en sco.properties.

  Después de modificar el valor de los parámetros, reinicie SnapCenter el servicio del SPL con el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

Backups de bases de datos de Oracle con comandos de UNIX

El flujo de trabajo de backup incluye planificación, identificación de los recursos para el backup, creación de políticas de backup, creación de grupos de recursos y vinculación de políticas, creación de backups y supervisión de las operaciones.

Lo que necesitará

- Debe haber agregado las conexiones del sistema de almacenamiento y creado la credencial con los comandos *Add-SmStorageConnection* y *Add-SmCredential*.
- Estableció la sesión de conexión con el servidor SnapCenter mediante el comando *Open-SmConnection*.

  Solo puede tener una sesión iniciada con una cuenta de SnapCenter, y el token se almacena en el directorio inicial del usuario.

  > La sesión de conexión solo es válida por 24 horas. Sin embargo, puede crear un token con la opción TokenNeverExpires que no caduque nunca para que la sesión sea válida siempre.

Acerca de esta tarea

Debe ejecutar los siguientes comandos para establecer la conexión con SnapCenter Server, detectar las instancias de la base de datos de Oracle, añadir políticas y grupos de recursos, realizar el backup y verificarlo.

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help *command_name*. Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter".

- Pasos*
  1. Inicie una sesión de conexión con el servidor SnapCenter para el usuario especificado: *Open-SmConnection*
  2. Realizar la operación de detección de recursos del host: *Get-SmResources*
  3. Configure las credenciales y los nodos preferidos de la base de datos de Oracle para la operación de backup de una base de datos de RAC: *Configure-SmOracleDatabase*
  4. Cree una política de backup: *Add-SmPolicy*
  5. Recupere la información acerca de la ubicación de almacenamiento secundaria (SnapVault o SnapMirror) : *Get-SmSecondaryDetails*

     Este comando recupera los detalles de asignación de almacenamiento principal a secundario de un recurso especificado. Es posible utilizar los detalles de asignación para configurar las opciones de verificación secundaria mientras se crea un grupo de recursos de backup.
  6. Añada un grupo de recursos a SnapCenter: *Add-SmResourceGroup*
  7. Cree una copia de seguridad: *New-SmBackup*

     Puede sondear el trabajo con la opción WaitForCompletion. Si se especifica esta opción, el comando sigue sondeando el servidor hasta la finalización del trabajo de backup.
  8. Recupere los registros de SnapCenter: *Get-SmLogs*

Supervisar las operaciones de backup de bases de datos de Oracle

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página Monitor, haga clic en **Jobs**.
  3. En la página Jobs, realice los siguientes pasos:
     a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
     b. Especifique las fechas de inicio y finalización.
     c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
     d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
     e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
  4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

     > Aunque el estado del trabajo de backup indique , al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

  5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

     El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Supervise las operaciones de protección de datos en el panel Activity

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup

programado. Si utiliza el plugin para SQL Server o el plugin para Exchange Server, el panel Activity también muestra información sobre la operación de propagación.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. Haga clic en En el panel Activity para ver las cinco operaciones más recientes.

     Al hacer clic en una de las operaciones, se muestran sus detalles en la página Job Details.

Cancelar las operaciones de backup de las bases de datos de Oracle

Es posible cancelar las operaciones de backup que se estén ejecutando, en cola o no respondan.

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de backup.

Acerca de esta tarea

Cuando se cancela una operación de backup, el servidor de SnapCenter detiene la operación y quita todas las copias de Snapshot del almacenamiento si el backup creado no se registra en SnapCenter Server. Si el backup ya está registrado en el servidor SnapCenter, no retrocederá la copia de Snapshot ya creada incluso después de que se active la cancelación.

- Solo es posible cancelar la operación de registro o backup completo que se encuentra en cola o en ejecución.
- No se puede cancelar la operación una vez iniciada la verificación.

  Si cancela la operación antes de verificarlo, se cancelará la operación y no realizará la operación de verificación.

- No se puede cancelar la operación de backup una vez que se iniciaron las operaciones de catálogo.
- Es posible cancelar una operación de backup desde la página Monitor o el panel Activity.
- Además de usar la interfaz gráfica de usuario de SnapCenter, es posible usar los comandos de la CLI para cancelar las operaciones.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.

Paso

Ejecute una de las siguientes acciones:

Del…	Acción
Página Monitor	1. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**. 2. Seleccione la operación y haga clic en **Cancelar trabajo**.
Panel de actividades	1. Después de iniciar el trabajo de backup, haga clic en En el panel Activity para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**.

Resultados

La operación se cancela y el recurso se revierte a su estado original.

Si la operación que canceló no responde en el estado de cancelación o ejecución, debe ejecutar la operación Cancel-SmJob -JobID <int> -Force para detener la operación de backup enérgicamente.

Consulte los backups y los clones de las bases de datos de Oracle en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede resultar útil ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario.

Acerca de esta tarea

En la página Topology, es posible ver todos los backups y clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

Puede consultar los siguientes iconos de la vista gestionar copias para determinar si los backups o clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).

- muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
- Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.
- Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario. Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.

> Los clones de un backup de un reflejo con versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejo no incluye el backup con versión flexible.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

   Si el recurso está protegido, se muestra la página Topology del recurso seleccionado.

4. Consulte Summary Card para ver un resumen de la cantidad de backups y clones disponibles en el almacenamiento principal y secundario.

   La sección Summary Card muestra la cantidad total de backups y clones, y la cantidad total de backups de registros.

   Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

5. En la vista Administrar copias, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

   Estos detalles se muestran en forma de tabla.

6. Seleccione el backup en la tabla y haga clic en los iconos de protección de datos para realizar restauración, clonado, montaje, desmontaje, cambio de nombre, operaciones de catalogación, descatalogación y eliminación.

   > Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

   - Si seleccionó un backup de registros, solo es posible realizar un cambio de nombre, montaje, desmontaje, catálogo, descatalogar, y eliminar operaciones.
   - Si catalogó el backup con Oracle RMAN, no puede cambiar el nombre de esos backups catalogados.

7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en 🗑.

Si el valor asignado a SnapmirrorStatusUpdateWaitTime es menor, las copias de backup de reflejo y almacén no se enumeran en la página de topología aunque los volúmenes de registros y datos estén protegidos correctamente. Debe aumentar el valor asignado a SnapmirrorStatusUpdateWaitTime con el cmdlet *Set-SmConfigSettings* PowerShell.

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando Get-Help *command_name*.

Como alternativa, también puede consultar la "Guía de referencia de comandos del software SnapCenter" o. "Guía de referencia de cmdlets de SnapCenter Software".