Realice backups de bases de datos de Oracle

SnapCenter Software 5.0

NetApp
July 18, 2024

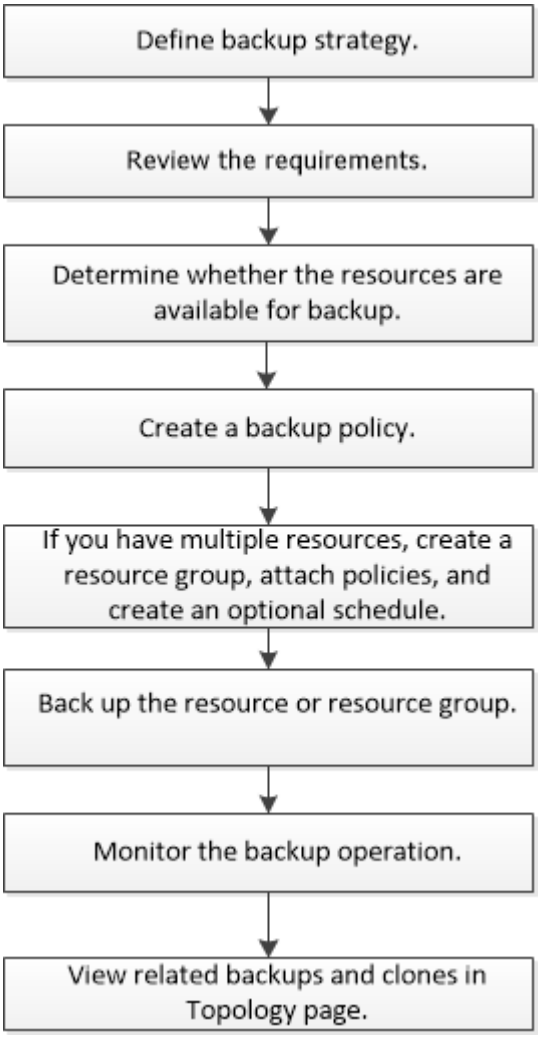
Tabla de contenidos

Realice backups de bases de datos de Oracle

Descripción general del procedimiento de copia de seguridad

Es posible crear un backup de un recurso (base de datos) o un grupo de recursos. El procedimiento de backup incluye planificar, identificar los recursos para el backup, crear políticas de backup, crear grupos de recursos y añadir políticas, crear backups y supervisar 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 */var/opt/snapcenter/sco/lock*, 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 tal situación, debe eliminar

manualmente el archivo de bloqueo operativo mediante los siguientes pasos:

1. Desde el símbolo del sistema, desplácese hasta */var/opt/snapcenter/sco/lock*.
2. Elimine el bloqueo operativo:`rm -rf .sm_lock_dbsid.`

Información de configuración de backup

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 soportadas, consulte la "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

Los recursos son 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.

En las siguientes secciones se describe el proceso que utiliza SnapCenter para detectar diferentes tipos y versiones de bases de datos Oracle.

Para las versiones de Oracle 11*g* a 12*c*R1

Base de datos RAC

Las bases de datos RAC solo se detectan sobre la base de /etc/oratab`entries. Deben tener las entradas de la base de datos en el archivo /etc/oratab.

Independiente

Las bases de datos autónomas se detectan sólo sobre la base de las entradas /etc/oratab.

ASM

La entrada de instancia de ASM debe estar disponible en el archivo /etc/oratab.

RAC One Node

Las bases de datos RAC One Node sólo se detectan en función de las entradas /etc/oratab. Las bases de datos deben estar en 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 en la página de recursos y, a continuación, haga clic en Database Settings.
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.
6. Si ha reubicado una base de datos de un nodo a otro y no se ha suprimido la entrada oratab del nodo anterior, suprima manualmente la entrada oratab para evitar que se muestre la misma base de datos dos veces.

Para las versiones de Oracle 12cR2 a 18c

Base de datos RAC

Las bases de datos de RAC se detectan mediante el comando srvctl config. Deben tener las entradas de la base de datos en el archivo /etc/oratab.

Independiente

Las bases de datos independientes se detectan según las entradas en el archivo /etc/oratab y la salida del comando srvctl config.

ASM

La entrada de la instancia de ASM no debe estar en el archivo /etc/oratab.

RAC One Node

Las bases de datos RAC One Node se detectan únicamente mediante el comando srvctl config. Las bases de datos deben estar en 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.

Debe realizar los siguientes pasos si se reubica la base de datos: . Actualice manualmente los recursos. . Seleccione la base de datos RAC One Node en la página de recursos y, a continuación, haga clic en Database Settings. . Configure la base de datos para establecer los nodos de clúster preferidos en el nodo de RAC que aloja actualmente la base de datos. . 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 que utiliza SnapCenter 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 solo en estos nodos preferidos y en el orden de preferencia indicado.

Ejemplo

La base de datos de RAC cdbrac tiene tres instancias: cdbrac1 en el nodo node1, cdbrac2 en el nodo node2 y cdbrac3 en el nodo node3.

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.

Configuración de ASM Flex

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.

Base de datos de catálogo externo

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.

Comando RMAN

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 para realizar una catalogación diferida de backups `Catalog-SmBackupWithOracleRMAN`.

Después de catalogar los backups, puede ejecutar `Get-SmBackupDetails` el comando para obtener la información de backups catalogados, como la etiqueta para los archivos de datos catalogados, la ruta de catálogo para el archivo de control y las ubicaciones de los registros de archivo catalogados.

Formato de nomenclatura

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.

Operaciones de verificación cruzada

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"
```

Eliminar información de catálogo

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. Alternativamente, puede consultar la "Guía de referencia de comandos del software SnapCenter".

Variables de entorno predefinidas para scripts previos y posteriores específicos para backup

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y el script posterior al crear políticas de backup. Esta funcionalidad es compatible con todas las configuraciones de Oracle excepto VMDK.

SnapCenter predefine los valores de los parámetros a los que se podrá acceder directamente en el entorno en el que se ejecutan los scripts de shell. No es necesario especificar manualmente los valores de estos parámetros al ejecutar los scripts.

Variables de entorno predefinidas compatibles para crear una política de backup

- **SC_JOB_ID** especifica el ID de trabajo de la operación.

  Ejemplo: 256

- **SC_ORACLE_SID** especifica el identificador del sistema de la base de datos.

  Si la operación implica varias bases de datos, el parámetro contendrá nombres de base de datos separados por tubería.

Este parámetro se rellenará para los volúmenes de aplicaciones.

Ejemplo: NFSB32|NFSB31

- **SC_HOST** especifica el nombre de host de la base de datos.

  Para RAC, el nombre de host será el nombre del host donde se realiza el backup.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** especifica el propietario del sistema operativo de la base de datos.

  Los datos se formatearán como <db1>@<osuser1>|<db2>@<osuser2>.

  Ejemplo: NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** especifica el grupo de sistemas operativos de la base de datos.

  Los datos se formatearán como <db1>@<osgroup1>|<db2>@<osgroup2>.

  Ejemplo: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE"** especifica el tipo de copia de seguridad (en línea completa, datos en línea, registro en línea, apagado sin conexión, montaje sin conexión)

  Ejemplos:

  - Para una copia de seguridad completa: ONLINEFULL
  - Backup exclusivo de los datos: ONLINEDATA
  - Para copia de seguridad únicamente de registro: ONLINELOG

- **SC_BACKUP_NAME** especifica el nombre de la copia de seguridad.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- **SC_BACKUP_ID** especifica el ID de copia de seguridad.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  EJEMPLO: DATA@203|LOG@205|AV@207

- **SC_ORACLE_HOME** especifica la ruta de acceso del directorio principal de Oracle.

  Ejemplo: NFSB32@/ora01/app/oracle/product/18.1.0/dB_1|NFSB31@/ora01/app/oracle/product/18.1.0/dB_1

- **SC_BACKUP_RETENTION** especifica el período de retención definido en la directiva.

  Ejemplos:

- Para el backup completo: Hourly|DATA@DAYS:3|LOG@COUNT:4
- Para backup solo de datos bajo demanda: OnDemand|DATA@COUNT:2
- Para backup solo de registros bajo demanda: OnDemand|LOG@COUNT:2

- **SC_RESOURCE_GROUP_NAME** especifica el nombre del grupo de recursos.

  Ejemplo: RG1

- **SC_BACKUP_POLICY_NAME** especifica el nombre de la política de copia de seguridad.

  Ejemplo: Backup_policy

- **SC_AV_NAME** especifica los nombres de los volúmenes de la aplicación.

  Ejemplo: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** especifica la asignación de almacenamiento de SVM al volumen para el directorio de archivos de datos. Será el nombre del volumen principal para las lun y qtrees.

  Los datos se formatearán como <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2>.

  Ejemplos:

  - Para 2 bases de datos en el mismo grupo de recursos: NFS32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA|NFS31@buck:/vol/sspr2417819002_NFS_CDB_NFSB31_DATA
  - Para una única base de datos con archivos de datos dispersos por varios volúmenes: buck:/vol/sspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/sspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** especifica la asignación de almacenamiento de SVM al volumen para el directorio de archivos de registros. Será el nombre del volumen principal para las lun y qtrees.

  Ejemplos:

  - Para una instancia de base de datos: buck:/vol/sspr2417819002_NFS_CDB_NFSB31_REDO
  - Para varias instancias de bases de datos: NFS31@buck:/vol/sscspr2417819002_NFS_CDB_NFS31_REDO|NFS32@buck:/vol/sspr2417819002_NFS_CDB_NFS32_REDO

- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** especifica la lista de instantáneas que contienen el nombre del sistema de almacenamiento y el nombre del volumen.

  Ejemplos:

  - Para una única base de datos: buck:/vol/sspr2417819002_NFS_NFSB32_DATA/RG2_sspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/sspr2417819002_NFS_NFSB32_REDO/RCDB_sspr24819002_07_21_2021-02.28.26.3973--
  - Para varias instancias de bases de datos: NFS32@buck:/vol/sspr2417819002_NFS_CDB_NFS32_DATA/RG2_sspr2417819002_07-21_2021_02.28.26.3973,buck:/vol/sspr241781900_NFS_21_SCADE1900_07_2021_SCS0-B2173-B212_SCR212_02.28.26.3973_07_02.28.26.3973_SCRNFS0-B217312003-B.2_21_2021_2021_SCRNFS01.0-BC0-B.2_21_SCS01.0-B.B.2_SCR2B.B2B2B.2*07*SCRSCS0-

B2B2B.B.B2B2B.B.B.B.B.B.2_02.28.26.3973___

- **SC_PRIMARY_SNAPSHOT_NAMES** especifica los nombres de las instantáneas primarias creadas durante la copia de seguridad.

  Ejemplos:

  - Para una sola base de datos: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_sspr2417819002_07-21-2021_02.28.26.3973_1
  - Para varias instancias de bases de datos: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_sspr2417819002_07-21-2021_02.28.26.3973_1
  - Para instantáneas de grupo de consistencia que implican 2 volúmenes: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350

- **SC_PRIMARY_MOUNT_POINTS** especifica los detalles del punto de montaje que forman parte de la copia de seguridad.

  Los detalles incluyen el directorio en el que se montan los volúmenes, y no el primario inmediato del archivo en backup. Para una configuración de ASM, es el nombre del grupo de discos.

  Los datos se formatearán como <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>.

  Ejemplos:

  - Para una única instancia de base de datos: /Mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
  - Para varias instancias de bases de datos: NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/dbnfs32_log,/mnt/nfsdb32_data1
  - PARA ASM: +DATA2DG,+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** especifica los nombres de las instantáneas creadas durante la copia de seguridad de cada uno de los puntos de montaje.

  Ejemplos:

  - Para una única base de datos: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
  - Para varias instancias de bases de datos: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_data,RG2_scspr2417819002_07 02.28.26.3973-21-2021_mnt

- **SC_ARCHIVELOGS_LOCATIONS** especifica la ubicación del directorio de registros de archivo.

  Los nombres de directorio serán el primario inmediato de los archivos de registro de archivos. Si los registros de archivos se colocan en más de una ubicación, se capturarán todas las ubicaciones. Esto también incluye los escenarios de FRA. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

    - Para una única base de datos en NFS: /Mnt/nfsdb2_log
    - Para varias bases de datos en NFS y para los registros de archivo de base de datos NFSB31 que se colocan en dos ubicaciones diferentes: NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
    - PARA ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15
- **SC_REDO_LOGS_LOCATIONS** especifica la ubicación del directorio redo logs.

  Los nombres de directorio serán el primario inmediato de los archivos redo log. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

    - Para una base de datos única en NFS: /Mnt/nfsdb2_data/newdb1
    - Para varias bases de datos en NFS: NFS31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
    - PARA ASM: +LOG2DG/ASMDB2/ONLINELOG
- **SC_CONTROL_FILES_LOCATION** especifica la ubicación del directorio de archivos de control.

  Los nombres de directorio serán el primario inmediato de los archivos de control. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

    - Para bases de datos únicas en NFS: /Mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
    - Para varias bases de datos en NFS: NFB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFB32@/mnt/nfsdb32_data/fra/dbnew32,/mnt/dbnfs32_data/newdb32
    - PARA ASM: +LOG2DG/ASMDB2/CONTROLFILE
- **SC_DATA_FILES_LOCATIONS**" especifica la ubicación del directorio de archivos de datos.

  Los nombres de directorio serán el primario inmediato de los archivos de datos. Si se utilizan enlaces Softplink para el directorio, se rellenará lo mismo.

  Ejemplos:

    - Para una única base de datos en NFS: /Mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/DataFile
    - Para varias bases de datos en NFS: NFB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/DataFile|NFB32@/mnt/nfsdb32_data1,/mnt/dbnfs32_data/NEWDB32/DataFile
    - PARA ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE
- **SC_SNAPSHOT_LABEL** especifica el nombre de las etiquetas secundarias.

  Ejemplos: Etiqueta Hourly, Daily, Weekly, Monthly o custom.

Delimitadores compatibles

- **:** se utiliza para separar el nombre de SVM y el nombre de volumen

  Ejemplo: buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sspr2417819002_07-21-

2021_02.28.26.3973_0,buck:/vol/sspr2417819002_NFS_CDB_NFSB32_REDO/RG2_sspr2417819002_07_21_2021_02.28.26.3973--

- **@** se utiliza para separar los datos de su nombre de base de datos y separar el valor de su clave.

  Ejemplos:

  - NFSB32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/sspr2417819002_NFS_sspr24B32_REDO/RCDB_sc2417875_07_21_2021_07_SCRNFS212002BS_21_02.28.26.3973_2021_02.28.26.3973_2021_07_SCNG2B2B2B2B2B2B2B2B2BV_*21*02.28.26.3973SCR2BV_SCR2B2BV_SCR2BV_SCR2BSSCR24B2B2B2B2B2B2BV_—
  - NFSB31@oracle|NFSB32@oracle

- **|** se utiliza para separar los datos entre dos bases de datos diferentes y para separar los datos entre dos entidades diferentes para los parámetros SC_BACKUP_ID, SC_BACKUP_RETENTION y SC_BACKUP_NAME.

  Ejemplos:

  - DATA@203|LOG@205
  - HOURLY|DATA@DAYS:3|LOG@COUNT:4
  - DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **/** se utiliza para separar el nombre del volumen de su Snapshot para SC_PRIMARY_SNAPSHOT_NAMES y los parámetros SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG.

  Ejemplo: NFSB32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sscspr2417819002_07-21_2021_02.28.26.3973,buck:/vol/sspr2417819002_NFS_NFSB32_REDO/RCDB_sc2417819002_07-21_2021-02.28.26.3973--

- **,** se utiliza para separar el conjunto de variables para la misma DB.

  Ejemplo: NFSB32@buck:/vol/sspr2417819002_NFS_CDB_NFSB32_DATA/RG2_sspr2417819002_07-21_2021_02.28.26.3973,buck:/vol/sspr2417819002_NFS_2021_SSPR242172B_07_21_07_SCS0122B002S_21 07 02.28.26.3973_02.28.26.3973 2021 21_02.28.26.3973 2021_SCS0-B003-B003-B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2BS123-B2B2BS123-B2B2B2B2B2B2B2B2B2B2BS123-B2B2BS123-B2B2B2B2B2B2BS123-B2BS

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.

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 22:10:00. 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 Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La 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, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la Snapshot.

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 ms 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.

Detectar las bases de datos de Oracle 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.

Paso 1: Evitar que SnapCenter detecte entradas que no son de base de datos

Es posible evitar que SnapCenter descubra entradas que no forman parte de una base de datos añadidas en el archivo oratab.

- Pasos*

  1. Después de instalar el plugin para Oracle, el usuario raíz debe crear el archivo **sc_oratab.config** en el directorio */var/opt/snapcenter/sco/etc/*.

     Conceda el permiso de escritura al propietario y grupo binario de Oracle para que el archivo pueda mantenerse en el futuro.

  2. El administrador de la base de datos debe añadir las entradas que no pertenecen a la base de datos en el archivo **sc_oratab.config**.

     Se recomienda mantener el mismo formato definido para las entradas que no son de base de datos en el archivo */etc/oratab* o el usuario puede añadir la cadena de entidad que no pertenece a la base de datos.

     La cadena distingue mayúsculas de minúsculas. Cualquier texto con # en el principio se trata como un comentario. El comentario se puede agregar después del nombre que no sea de la base de datos.

```
For example:
-----------------------------------------
# Sample entries
# Each line can have only one non-database name
# These are non-database name
oratar  # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N
-----------------------------------------------
```

1. Detectar los recursos.

   Las entradas que no sean de base de datos añadidas en **sc_oratab.config** no se mostrarán en la página Resources.

Siempre se recomienda realizar un backup del archivo sc_oratab.config antes de actualizar el plugin de SnapCenter.

Paso 2: Descubrir recursos

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, puede hacer clic en el icono 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.

Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

- 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.

Antes de empezar

- 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 snapshots 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.
- Si instaló el plugin como usuario no raíz, debe asignar manualmente los permisos de ejecución a los directorios de scripts previos y posteriores.
- Para conocer los requisitos previos y las limitaciones de Continuidad del Negocio con SnapMirror (SM-BC), consulte "Límites de objetos para la continuidad del negocio de SnapMirror".

Acerca de esta tarea

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.

    Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta

que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.

Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

ⓘ La configuración principal de SnapLock se gestiona en la política de backup de SnapCenter y la configuración secundaria de SnapLock se gestiona mediante ONTAP.

- 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**.

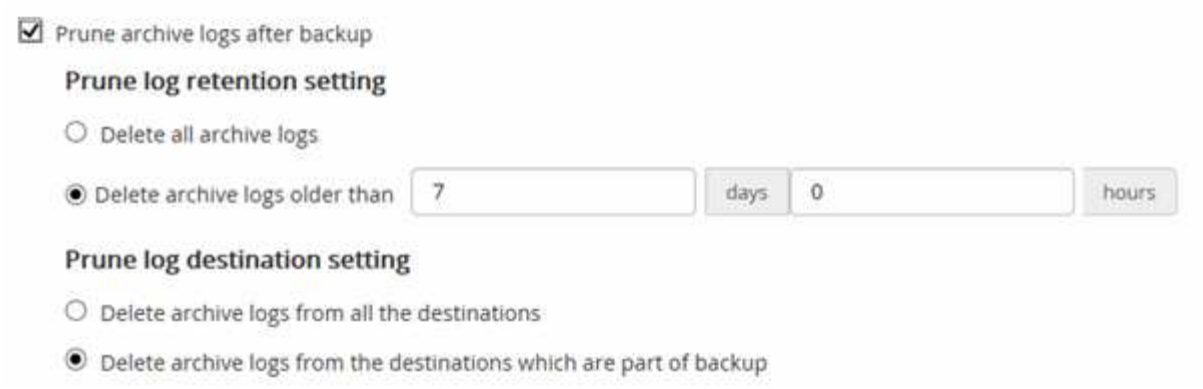
> Se omitirá la eliminación de registros de archivo desde el destino del registro de archivos que no esté configurado en la base de datos.

> 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**.
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…
Mantenga un cierto número de Snapshots	Seleccione **Total Snapshot copies to keep** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de snapshots supera el número especificado, las snapshots 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 Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino.
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione **Mantener copias snapshot para** y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.

Período de bloqueo de instantánea	Seleccione Snapshot copy locking period y seleccione días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

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…**
Actualice SnapMirror después de crear una instantánea local	Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror). Esta opción debe estar habilitada para SnapMirror Business Continuity (SM-BC). Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.
Actualizar SnapVault después de crear una instantánea local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre el Almacén SnapLock, consulte "Confirmar copias Snapshot a WORM en un destino de almacén" Consulte "Consulte los backups y los clones de las bases de datos de Oracle en la página Topology".

Para este campo…	Realice lo siguiente…
Etiqueta de la política secundaria	Seleccione una etiqueta de Snapshot. Según la etiqueta de Snapshot que seleccione, ONTAP aplicará la política de retención de Snapshot secundaria 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 que se alcance el límite máximo de Snapshots 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.

   SnapCenter permite utilizar las variables de entorno predefinidas al ejecutar el script previo y el script posterior. "Leer más"

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

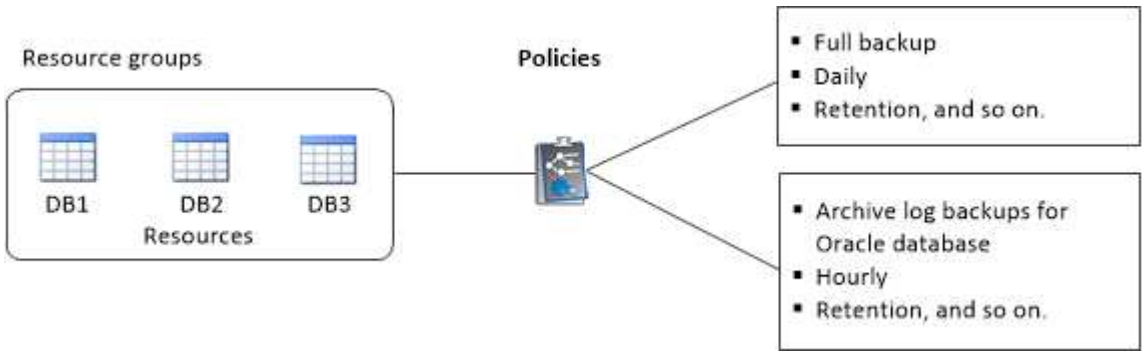
Un grupo de recursos es un contenedor donde se añaden recursos que se quieren proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación.

Acerca de esta tarea

- Una base de datos con archivos en grupos de discos de ASM debe tener el estado «MOUNT» o «OPEN» para verificar sus backups mediante la utilidad Oracle DBVERIFY.

  Añada 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:



- Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se permite añadir bases de datos nuevas sin SM-BC a un grupo de recursos existente que contiene recursos con SM-BC.
- No se admite la adición de bases de datos nuevas a un grupo de recursos existente en modo de conmutación al nodo de respaldo de SM-BC. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

a. Escriba un nombre para el grupo de recursos en el campo Name.

   El nombre del grupo de recursos no debe superar los 250 caracteres.

b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

   Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre 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 Snapshot.

d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.

   Debe utilizar exactamente el mismo destino que se estableció en Oracle, incluido el prefijo, si es necesario.

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. Se debe hacer clic en + en la columna Configure Schedules para la política cuya programación se desea configurar.

   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.

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

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, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, seleccione **Database** en la lista View.
3. Haga clic en y, a continuación, 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 Resources, puede realizar los siguientes pasos:
   a. Marque la casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

      Por ejemplo, `customtext_policy_hostname` o `resource_hostname`. De forma predeterminada, se añade una fecha/hora al nombre de Snapshot.

   b. 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.

      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 Configure Schedules para configurar una programación para la política que desea.
   c. En la ventana Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione `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 **Cargar localizadores** para cargar los volúmenes de SnapMirror o SnapVault para verificar 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. + En el cuadro de diálogo Add Verification Schedules *policy_name*, puede realizar los siguientes pasos:
   c. Seleccione **Ejecutar verificación después de la copia de seguridad**.
   d. Seleccione **Ejecutar verificación programada** y seleccione el tipo de programación 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.

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

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

8. En la página Notificación, seleccione los escenarios en los que desea enviar los correos electrónicos desde la lista desplegable **Preferencias de correo electrónico**.

   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, seleccione **Attach Job Report**.

   Para la notificación por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando PowerShell `Set-SmSmtpServer`.

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

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

10. Haga clic en **copia de seguridad ahora**.
11. En la página Backup, realice los siguientes pasos:
    a. Si aplicó varias políticas al recurso, en la lista desplegable Policy seleccione la política que desea usar para el backup.

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

Después de terminar

- En la configuración de AIX, puede utilizar `lkdev` el comando para bloquear y el `rendev` comando para cambiar el nombre de los discos en los que residía la base de datos de la que se hizo el backup.

  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 debido a que 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 mediante la ejecución del `Set-SmConfigSettings` cmdlet:

  Después de modificar el valor de los parámetros, reinicie el SnapCenter 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 el SnapCenter 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, el `do_start method` comando inicia el servicio del plugin de VMware de SnapCenter. Actualice ese comando a lo siguiente `Java -jar -Xmx8192M -Xms4096M:` .

Obtenga 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" (Requiere inicio de sesión)

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. La operación de backup se realiza con todos los recursos definidos en el grupo de recursos.

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

Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. Escriba el nombre del grupo de recursos en el cuadro de búsqueda o haga clic en y seleccione la etiqueta.

   Haga clic en para cerrar el panel de filtros.

4. En la página Resource Group, seleccione el grupo de recursos que desea incluir en un backup.

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

5. En la página Backup, realice los siguientes pasos:
   a. Si tiene varias políticas asociadas con el grupo de recursos, seleccione la política de copia de seguridad que desea usar en la lista desplegable **Política**.

      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. Seleccione **copia de seguridad**.
6. Controla el progreso seleccionando **Monitor > Trabajos**.

Después de terminar

- En la configuración de AIX, puede utilizar `lkdev` el comando para bloquear y el `rendev` comando para cambiar el nombre de los discos en los que residía la base de datos de la que se hizo el backup.

  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 debido a que 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 mediante la ejecución del `Set-SmConfigSettings` cmdlet:

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

Supervisar la copia de seguridad de Oracle Database

Descubra cómo supervisar el progreso de las operaciones de backup y las operaciones de protección de datos.

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
- Con errores
- 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 se muestra el estado del trabajo de copia de seguridad ✔ , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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.

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, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Otras operaciones de backup

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*. Alternativamente, 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*

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 snapshots del almacenamiento si el backup creado no se registró en el servidor de SnapCenter. Si la copia de seguridad ya está registrada en el servidor de SnapCenter, no revertirá la copia 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 la tarea 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 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.

Si tiene una relación secundaria como Continuidad empresarial de SnapMirror (SM-BC), verá los siguientes iconos adicionales:

-  implica que el sitio de réplica está activo.
-  implica que el sitio de réplica está caído.
-  implica que no se restableció la relación de reflejo o almacén secundario.
- 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.

Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

Para la continuidad del negocio con SnapMirror (SM-BC), al hacer clic en el botón **Actualizar**, se actualiza el inventario de backup de SnapCenter consultando ONTAP tanto para los sitios primarios como de réplica. Una programación semanal también realiza esta actividad para todas las bases de datos que contienen una relación SM-BC.

- Para las relaciones SM-BC, Mirror asíncrono, Vault o MirrorVault con el nuevo destino primario se deben configurar manualmente después de la conmutación al nodo de respaldo.
- Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya creado una copia de seguridad.

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*.

Alternativamente, también puede consultar el "Guía de referencia de comandos del software SnapCenter" o "Guía de referencia de cmdlets de SnapCenter Software".