Proteger bases de datos de Oracle

SnapCenter Software 4.7

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-47/protect-sco/concept_what_you_can_do_with_the_snapcenter_plug_in_for_oracle_database.html on September 26, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Proteger bases de datos de Oracle . . . 1
Información general del plugin de SnapCenter para base de datos de Oracle . . . 1
Qué puede hacer con el plugin para base de datos de Oracle . . . 1
Funciones del plugin para base de datos de Oracle . . . 1
Tipos de almacenamiento compatibles con el plugin para bases de datos de Oracle . . . 3
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para Oracle . . . 4
Privilegios mínimos requeridos de ONTAP para el plugin para Oracle . . . 5
Instale el plugin de SnapCenter para base de datos de Oracle . . . 8
Flujo de trabajo de instalación del plugin de SnapCenter para base de datos de Oracle . . . 8
Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux o AIX . . . 8
Añada hosts e instale el paquete de plugins para Linux o AIX mediante la interfaz gráfica de usuario . . . 17
Formas alternativas de instalar el paquete de plugins para Linux o AIX . . . 21
Configure el servicio de cargador de plugins de SnapCenter . . . 24
Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux . . . 27
Habilite certificados de CA para plugins . . . 30
Importe datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter . . . 31
Instale el plugin de SnapCenter para VMware vSphere . . . 37
Implemente el certificado de CA . . . 37
Configure el archivo CRL . . . 37
Preparar la protección de bases de datos de Oracle . . . 37
Realice backups de bases de datos de Oracle . . . 39
Flujo de trabajo de backup . . . 39
Definir una estrategia de backup para bases de datos de Oracle . . . 40
Variables de entorno predefinidas para scripts previos y posteriores específicos para backup . . . 47
Determinar si las bases de datos de Oracle están disponibles para backup . . . 52
Crear políticas de backup para bases de datos de Oracle . . . 55
Crear grupos de recursos y vincular políticas para bases de datos de Oracle . . . 60
Requisitos para realizar backups de una base de datos de Oracle . . . 62
Realice backup de recursos de Oracle . . . 63
Realice backups de grupos de recursos de bases de datos de Oracle . . . 66
Backups de bases de datos de Oracle con comandos de UNIX . . . 67
Supervisar las operaciones de backup de bases de datos de Oracle . . . 68
Cancelar las operaciones de backup de las bases de datos de Oracle . . . 69
Consulte los backups y los clones de las bases de datos de Oracle en la página Topology . . . 70
Montar y desmontar backups de bases de datos . . . 72
Montar un backup de base de datos . . . 72
Desmontar un backup de base de datos . . . 74
Restaurar y recuperar bases de datos de Oracle . . . 74
Restaure el flujo de trabajo . . . 74
Definir una estrategia de restauración y recuperación para bases de datos de Oracle . . . 75
Variables de entorno predefinidas para restaurar scripts previos y posteriores específicos . . . 80

Requisitos para restaurar una base de datos de Oracle . . . 81
Restaurar y recuperar bases de datos de Oracle . . . 82
Restauración y recuperación de espacios de tablas mediante la recuperación de un momento específico . . . 87
Restaure y recupere una base de datos conectable mediante la recuperación de un momento específico . . . 89
Restaure y recupere bases de datos de Oracle con comandos de UNIX . . . 91
Supervisar las operaciones de restauración de bases de datos de Oracle . . . 92
Cancelar operaciones de restauración de bases de datos de Oracle . . . 93
Clone la base de datos de Oracle . . . 93
Flujo de trabajo de clonado . . . 93
Defina una estrategia de clonado para bases de datos de Oracle . . . 94
Variables de entorno predefinidas para el script previo y script posterior específicos de clon . . . 95
Requisitos para clonar una base de datos de Oracle . . . 97
Clonar el backup de una base de datos de Oracle . . . 99
Clonar una base de datos conectable . . . 108
Clonar backups de bases de datos de Oracle con comandos UNIX . . . 113
Divida el clon de una base de datos de Oracle . . . 113
Clon dividido de una base de datos conectable . . . 114
Supervise las operaciones de clonado de las bases de datos de Oracle . . . 115
Actualizar un clon . . . 116
Eliminar el clon de una base de datos conectables . . . 117
Gestione los volúmenes de aplicaciones . . . 117
Añada volúmenes de la aplicación . . . 117
Aplicación de backup para volúmenes . . . 118
Clone el backup de volumen de la aplicación . . . 121

Proteger bases de datos de Oracle

Información general del plugin de SnapCenter para base de datos de Oracle

Qué puede hacer con el plugin para base de datos de Oracle

El plugin de SnapCenter para bases de datos de Oracle es un compenente de NetApp SnapCenter Software que se instala en los hosts de Oracle que permite la gestión de protección de datos para aplicaciones de bases de datos de Oracle.

El plugin para bases de datos de Oracle automatiza las operaciones de backup, catalogación y descatalogación con Oracle Recovery Manager (RMAN), verificación, montaje, desmontaje, restauración, Recuperación y clonado de bases de datos de Oracle en el entorno de SnapCenter. El plugin para bases de datos de Oracle instala el plugin de SnapCenter para UNIX para realizar todas las operaciones de protección de datos.

Es posible utilizar el plugin para bases de datos de Oracle para gestionar backups de bases de datos de Oracle que ejecutan aplicaciones SAP. Sin embargo, no se admite la integración con BR*Tools de SAP.

- Realizar backup de archivos de datos, archivos de control y archivos de registro de archivo.

  El backup solo puede usarse en el nivel de la base de datos del contenedor (CDB).

- Restaurar y recuperar bases de datos, bases de datos de contenedor y bases de datos conectables (PDB).

  No se admite la recuperación incompleta de bases de datos conectables.

- Crear clones de bases de datos de producción hasta un momento específico.

  La clonado solo puede usarse en el nivel de la base de datos de contenedor.

- Verificar backups de inmediato.
- Montaje y desmontaje de datos y backups de registro para la operación de recuperación.
- Programar operaciones de backup y verificación.
- Supervisar todas las operaciones.
- Ver informes para operaciones de backup, restauración y clonado.

Funciones del plugin para base de datos de Oracle

El plugin para bases de datos de Oracle se integra con la base de datos de Oracle en el host Linux o AIX y con las tecnologías de NetApp en el sistema de almacenamiento.

- Interfaz gráfica de usuario unificada

  La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar operaciones de backup, restauración, recuperación y clonado consistentes entre plugins, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins.

- Administración central automatizada

  Es posible programar operaciones de backup y clonado, configurar retención de backup basado en políticas y realizar operaciones de restauración. También es posible supervisar de manera proactiva el entorno configurando SnapCenter para que envíe alertas por correo electrónico.

- Tecnología de copia de Snapshot de NetApp no disruptiva

  SnapCenter utiliza la tecnología de copia de Snapshot de NetApp con el plugin para bases de datos de Oracle y el plugin para UNIX con el fin de realizar backups de bases de datos. Las copias de Snapshot consumen un espacio de almacenamiento mínimo.

El plugin para bases de datos de Oracle también ofrece los siguientes beneficios:

- Compatibilidad con backup, restauración, clonado, montaje, desmontaje y flujos de trabajo de verificación
- Detección automática de las bases de datos de Oracle configuradas en el host
- Compatibilidad para catalogar y descatalogar con Oracle RMAN
- Seguridad compatible con RBAC y delegación de roles centralizada

  También es posible configurar las credenciales para que los usuarios de SnapCenter autorizados tengan permisos en el nivel de las aplicaciones.

- Compatibilidad con la gestión de registros de archivo (ALM) para operaciones de restauración y clonado
- Creación de copias de bases de datos de producción con gestión eficiente del espacio y en un momento específico con fines de prueba o de extracción de datos con la tecnología FlexClone de NetApp

  Se requiere una licencia de FlexClone en el sistema de almacenamiento donde desea crear el clon.

- Compatibilidad con la función del grupo de consistencia (CG) de ONTAP como parte de la creación de backups en entornos DE SAN y ASM
- Verificación de backups no disruptiva y automatizada
- Capacidad para ejecutar varios backups de forma simultánea entre varios hosts de bases de datos

  En una sola operación se consolidan copias de Snapshot cuando las bases de datos en un solo host comparten el mismo volumen.

- Compatibilidad con infraestructuras físicas y virtualizadas
- Compatibilidad con NFS, iSCSI, Fibre Channel (FC), RDM, VMDK sobre NFS y VMFS, y ASM sobre NFS, SAN, RDM y VMDK
- Compatibilidad con la función de asignación de LUN selectiva (SLM) de ONTAP

  Habilitada de forma predeterminada, la función SLM detecta periódicamente los LUN que no poseen rutas optimizadas y los corrige. Puede configurar SLM mediante la modificación de los parámetros del archivo scu.properties ubicado en /var/opt/snapcenter/scu/etc.

  - Para deshabilitar esto, debe configurarse el valor del parámetro ENABLE_LUNPATH_MONITORING como false.
  - Es posible especificar la frecuencia en la cual se corrigen automáticamente las rutas de LUN mediante la asignación del valor (en horas) como el parámetro LUNPATH_MONITORING_INTERVAL. Para obtener más información sobre SLM, consulte "Guía de administración de SAN de ONTAP 9".

- Compatibilidad con memoria no volátil exprés (NVMe) en Linux
  - La utilidad NVMe debe estar instalada en el host.

    Debe instalar NVMe util para clonar o montar en un host alternativo.

  - Backup, restauración, clonado, montaje, desmontaje, Se admiten las operaciones de catalogación, descatalogación y verificación en el hardware de NVMe, excepto en los entornos virtualizados como VMDK y RDM.

    Las operaciones anteriores se admiten en dispositivos sin particiones o con una sola partición.

Puede configurar una solución multivía para dispositivos NVMe estableciendo la opción multivía nativa del kernel. No se admite la función multivía de Device Mapper (DM).

+ para obtener la información más reciente acerca de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Tipos de almacenamiento compatibles con el plugin para bases de datos de Oracle

SnapCenter admite una amplia variedad de tipos de almacenamiento en máquinas físicas y virtuales. Debe comprobar la compatibilidad de su tipo de almacenamiento antes de instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX.

SnapCenter no es compatible con el aprovisionamiento de almacenamiento para Linux y AIX.

Tipos de almacenamiento compatibles con Linux

En la siguiente tabla, se enumeran los tipos de almacenamiento admitidos en Linux.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • Volúmenes conectados en NFS

Máquina	Tipo de almacenamiento
VMware ESXi	• Los LUN de RDM conectados por un HBAScanning de adaptadores de bus de host (HBA) FC o iSCSI pueden tardar mucho en completarse debido a que SnapCenter analiza todos los adaptadores de bus de host presentes en el host. Puede editar el archivo **LinuxConfig.pm** ubicado en */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* para establecer el valor del parámetro **SCSI_HOSTS_OPTIMIZED_RESCAN** en 1 para volver a analizar sólo los HBA que aparecen en HBA_DRIVER_NAMES. • LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI • VMDK en almacenes de datos VMFS o NFS • Volúmenes NFS conectados directamente con el Guest VM

Tipos de almacenamiento compatibles con AIX

En la siguiente tabla se enumeran los tipos de almacenamiento admitidos en AIX.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC e iSCSI. En un entorno SAN, se admiten los sistemas de archivos ASM, LVM y SAN. No se admite NFS en AIX y sistema de archivos. • Sistema de archivos con diario mejorado (JFS2) Admite el registro en línea en sistemas DE archivos SAN y el diseño de LVM.

La "Herramienta de matriz de interoperabilidad de NetApp" contiene la información más reciente acerca de las versiones con puerto.

Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para Oracle

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la

tecnología ONTAP SnapVault para realizar replicaciones de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

SnapCenter realiza actualizaciones en SnapMirror y SnapVault después de completar la operación de copia de Snapshot. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter; no cree una programación de ONTAP aparte.

Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.

SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary** > **Mirror** > **Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "Documentación de ONTAP".

SnapCenter no admite replicación **SYNC_mirror**.

Privilegios mínimos requeridos de ONTAP para el plugin para Oracle

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores
• event generate-autosupport-log
• se muestra el historial del trabajo • detención de trabajo

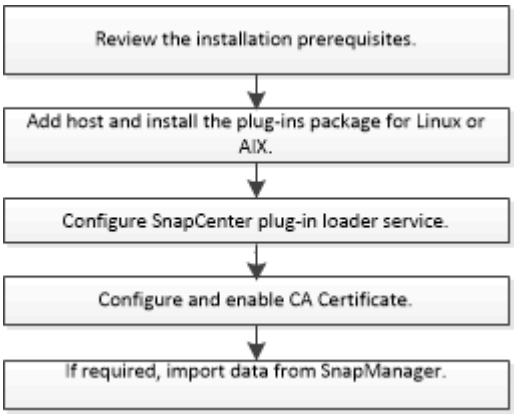
Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores
• lun • se muestra el atributo de lun • lun create • eliminación de lun • geometría de lun • igroup de lun añadido • crear lun igroup • lun igroup eliminado • cambio de nombre de lun igroup • lun igroup show • asignación de lun de nodos adicionales • se crea la asignación de lun • se elimina la asignación de lun • asignación de lun quitar nodos de generación de informes • se muestra el mapa de lun • modificación de lun • movimiento de lun en volumen • lun desconectada • lun conectada • reserva persistente de lun clara • cambio de tamaño de lun • serie de lun • muestra de lun
• regla adicional de la política de snapmirror • regla de modificación de la política de snapmirror • regla de eliminación de la política de snapmirror • la política de snapmirror • restauración de snapmirror • de snapmirror • historial de snapmirror • actualización de snapmirror • conjunto de actualizaciones de snapmirror • destinos de listas de snapmirror
• versión

Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores
• crear el clon de volumen • show de clon de volumen • inicio de división de clon de volumen • detención de división de clon de volumen • cree el volumen • destrucción del volumen • crear el archivo de volumen • uso show-disk del archivo de volumen • volumen sin conexión • volumen en línea • modificación del volumen • crear el qtree de volúmenes • eliminación de qtree de volumen • modificación del qtree del volumen • se muestra volume qtree • restricción de volumen • visualización de volumen • crear snapshots de volumen • eliminación de snapshots de volumen • modificación de las copias de snapshot de volumen • cambio de nombre de copias de snapshot de volumen • restauración de copias snapshot de volumen • archivo de restauración de snapshots de volumen • visualización de copias de snapshot de volumen • desmonte el volumen
• vserver • vserver cifs • se muestra vserver shadowcopy • se muestra vserver
• interfaz de red • se muestra la interfaz de red
• MetroCluster show

Instale el plugin de SnapCenter para base de datos de Oracle

Flujo de trabajo de instalación del plugin de SnapCenter para base de datos de Oracle

Debe instalar y configurar el plugin de SnapCenter para base de datos de Oracle si desea proteger las bases de datos Oracle.



Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux o AIX

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.

  El plugin de SnapCenter para base de datos Oracle puede ser instalado por un usuario no raíz. Sin embargo, debe configurar los privilegios sudo para el usuario no raíz para instalar e iniciar el proceso del plugin. Después de instalar el plugin, los procesos se ejecutan como un usuario raíz eficaz.

- Si va a instalar el paquete de plugins de SnapCenter para AIX en el host AIX, debe haber resuelto manualmente los enlaces simbólicos del nivel de directorio.

  El paquete de plugins de SnapCenter para AIX resuelve automáticamente el enlace simbólico del nivel de archivo, pero no los enlaces simbólicos del nivel de directorio para obtener la ruta absoluta DE JAVA_HOME.

- Cree credenciales con el modo de autenticación como Linux o AIX para el usuario de instalación.
- Debe haber instalado Java 1.8.x de 64 bits en el host Linux o AIX.

  Para obtener información sobre CÓMO descargar JAVA, consulte:

  - "Descargas de Java para todos los sistemas operativos"
  - "IBM Java para AIX"

- Para bases de datos Oracle que se ejecuten en un host Linux o AIX, debe instalar tanto el plugin de SnapCenter para base de datos Oracle como el plugin de SnapCenter para UNIX.

También es posible utilizar el plugin para bases de datos de Oracle para gestionar bases de datos de Oracle para SAP. Sin embargo, no se admite la integración con BR*Tools de SAP.

- Si utiliza la base de datos Oracle 11.2.0.3 o posterior, debe instalar la revisión 13366202 de Oracle.

SnapCenter no admite la asignación de UUID en el archivo /etc/fstab.

Requisitos del host Linux

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de plugins de SnapCenter para Linux.

Elemento	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux Si utiliza la base de datos de Oracle en LVM en sistemas operativos Oracle Linux o Red Hat Enterprise Linux 6.6 o 7.0, tiene que instalar la versión más reciente del administrador de volúmenes lógicos (LVM). • SUSE Linux Enterprise Server (SLES)
RAM mínima para el plugin de SnapCenter en el host	1 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.
Paquetes de software obligatorios	Tipos Java 1.8.x (64 bits)Oracle Java y OpenJDK Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta.

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

Configure privilegios sudo para usuarios que no son raíz para el host Linux

SnapCenter 2.0 y versiones posteriores permiten que un usuario no raíz instale el paquete de plugins de SnapCenter para Linux e inicie el proceso del plugin. Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas.

Lo que necesitará

- Versión sudo entre 1.8.7 y 1.8.19P2.
- Asegúrese de que el usuario que no sea raíz forma parte del grupo de instalación de Oracle.
- Edite el archivo */etc/ssh/sshd_config* para configurar los algoritmos de código de autenticación de mensajes: Macs hmac-sha2-256 y MACs hmac-sha2-512.

  Reinicie el servicio sshd después de actualizar el archivo de configuración.

  Ejemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Acerca de esta tarea

Tiene que configurar los privilegios sudo para usuarios que no son raíz con el fin de ofrecer acceso a las rutas siguientes:

- /Home/*SUDO_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl

> Si gestiona una configuración de RAC, el usuario que no sea raíz debe ser un usuario de Oracle y no puede ser un usuario de sistema operativo que no sea raíz.

- Pasos*

  1. Inicie sesión en el host Linux en el que desee instalar el paquete de plugins de SnapCenter para Linux.
  2. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de Linux.

```
Cmnd_Alias SCCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/Linux_Prechecks.sh
SUDO_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: SUDO_USER env_keep=JAVA_HOME
Defaults: SUDO_USER !visiblepw
Defaults: SUDO_USER !requiretty
```

SUDO_USER es el nombre del usuario no raíz que ha creado.

Puede obtener el valor de suma de comprobación en el archivo **oracle_checksum.txt**, que se encuentra en *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Si ha especificado una ubicación personalizada, esta será *custom_path\NetApp\SnapCenter\Package Repository*.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

Mejor práctica: por razones de seguridad, debe eliminar la entrada sudo después de completar cada instalación o actualización.

Requisitos del host AIX

Debe asegurarse de que el host cumpla los requisitos antes de instalar el paquete de plugins de SnapCenter para AIX.

El plugin de SnapCenter para UNIX que forma parte del paquete de plugins de SnapCenter para AIX, no admite grupos de volúmenes concurrentes.

Elemento	Requisitos
Sistemas operativos	AIX 6.1 o posterior
RAM mínima para el plugin de SnapCenter en el host	4 GB

Elemento	Requisitos
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	1 GB Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.
Paquetes de software obligatorios	Java 1.8.x (64 bits)IBM Java Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta.

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

Configure privilegios sudo para usuarios que no son raíz para el host AIX

SnapCenter 4.4 y versiones posteriores permiten que un usuario no raíz instale el paquete de plugins de SnapCenter para AIX e inicie el proceso del plugin. Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas.

Lo que necesitará

- Versión sudo entre 1.8.7 y 1.8.19P2.
- Asegúrese de que el usuario que no sea raíz forma parte del grupo de instalación de Oracle.
- Edite el archivo */etc/ssh/sshd_config* para configurar los algoritmos de código de autenticación de mensajes: Macs hmac-sha2-256 y MACs hmac-sha2-512.

  Reinicie el servicio sshd después de actualizar el archivo de configuración.

  Ejemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Acerca de esta tarea

Tiene que configurar los privilegios sudo para usuarios que no son raíz con el fin de ofrecer acceso a las rutas siguientes:

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Si gestiona una configuración de RAC, el usuario que no sea raíz debe ser un usuario de Oracle y no puede ser un usuario de sistema operativo que no sea raíz.

- Pasos*

1. Inicie sesión en el host AIX en el que desee instalar el paquete de plugins de SnapCenter para AIX.
2. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de Linux.

```
Cmnd_Alias SCCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
AIX_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

AIX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el valor de suma de comprobación en el archivo **oracle_checksum.txt**, que se encuentra en *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Si ha especificado una ubicación personalizada, esta será *custom_path\NetApp\SnapCenter\Package Repository*.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

Mejor práctica: por razones de seguridad, debe eliminar la entrada sudo después de completar cada instalación o actualización.

Configure las credenciales

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar el paquete de plugins en hosts Linux o AIX.

Acerca de esta tarea

Las credenciales se crean para el usuario raíz o para un usuario que no es raíz que tiene privilegios sudo para instalar e iniciar el proceso del plugin.

Para obtener más información, consulte: Configure privilegios sudo para usuarios que no son raíz para el host Linux o. Configure privilegios sudo para usuarios que no son raíz para el host AIX

Práctica recomendada: aunque se le permite crear credenciales después de implementar hosts e instalar plugins, la práctica recomendada es crear credenciales después de añadir SVM, antes de implementar hosts e instalar plugins.

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Settings, haga clic en **Credential**.
  3. Haga clic en **Nuevo**.
  4. En la página Credential, introduzca la información de la credencial:

Para este campo…	Realice lo siguiente…
Nombre de credencial	Introduzca un nombre para las credenciales.

Para este campo…	Realice lo siguiente…
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • Administrador del dominio Especifique el administrador de dominio en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son: ◦ *NetBIOS\Username* ◦ *Domain FQDN\Username* • Administrador local (sólo para grupos de trabajo) Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: *Username*
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar. Según el sistema operativo del host del plugin, seleccione Linux o AIX.
Use privilegios sudo	Seleccione la casilla de verificación **Use sudo Privileges** si va a crear credenciales para usuarios que no son raíz.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, puede que desee asignar mantenimiento de credenciales a un usuario o grupo de usuarios en la página **Usuario y acceso**.

Configurar credenciales para una base de datos Oracle

Es necesario configurar las credenciales que se usan para realizar operaciones de protección de datos en bases de datos de Oracle.

Acerca de esta tarea

Debe revisar los diferentes métodos de autenticación compatibles con las bases de datos de Oracle. Para

obtener más información, consulte"Métodos de autenticación para las credenciales".

Si se configuran credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, el nombre de usuario debe tener al menos privilegios de grupo de recursos y backup.

Si habilitó la 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.

Si especifica detalles incorrectos al crear una credencial, se muestra un mensaje de error. Debe hacer clic en **Cancelar** y luego volver a intentarlo.

- 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, 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 y, a continuación, haga clic en **Configuración de base de datos** > **Configurar base de datos**.
5. En la sección Configure database settings, en la lista desplegable **Use existing Credential**, seleccione la credencial que debe utilizarse para realizar trabajos de protección de datos en la base de datos Oracle.

   El usuario de Oracle debe tener privilegios sysdba.

   También se puede crear una credencial si se hace clic en .

6. En la sección Configure ASM settings, en la lista desplegable **Use existing Credential**, seleccione la credencial que debe utilizarse para realizar trabajos de protección de datos en la instancia de ASM.

   El usuario de ASM debe tener privilegios sysasm.

   También se puede crear una credencial si se hace clic en .

7. En la sección Configurar los ajustes del catálogo RMAN, en la lista desplegable **utilizar credencial existente**, seleccione la credencial que debe utilizarse para realizar trabajos de protección de datos en la base de datos del catálogo de Oracle Recovery Manager (RMAN).

   También se puede crear una credencial si se hace clic en .

   En el campo **TNSName**, introduzca el nombre de archivo de sustrato de red transparente (TNS) que utilizará el servidor SnapCenter para comunicarse con la base de datos.

8. En el campo **nodos de RAC preferidos**, especifique los nodos de Real Application Cluster (RAC) preferidos para la copia de seguridad.

Estos nodos preferidos pueden ser uno o todos los nodos del clúster donde hay instancias de bases de datos de RAC presentes. La operación de backup se activa solo en estos nodos preferidos y en el orden indicado.

En RAC One Node, sólo un nodo aparece en los nodos preferidos y este nodo preferido es el nodo en el que la base de datos está alojada actualmente.

Después de la conmutación por error o la reubicación de la base de datos de RAC One Node, la actualización de recursos en la página Recursos de SnapCenter eliminará el host de la lista **nodos de RAC preferidos** donde se alojó la base de datos anteriormente. El nodo RAC en el que se reubica la base de datos aparecerá en **nodos RAC** y deberá configurarse manualmente como el nodo RAC preferido.

Para obtener más información, consulte "Nodos preferidos en la configuración de RAC".

1. Haga clic en **Aceptar**.

Añada hosts e instale el paquete de plugins para Linux o AIX mediante la interfaz gráfica de usuario

Puede utilizar la página Add Host para añadir hosts y, a continuación, instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX. Los plugins se instalan automáticamente en hosts remotos.

Acerca de esta tarea

Puede añadir un host e instalar paquetes de plugins para un host individual o para un clúster. Si instala el plugin en un clúster (Oracle RAC), el plugin se instala en todos los nodos del clúster. Para Oracle RAC One Node, debe instalar el plugin en nodos activos y pasivos.

Debe asignarse a un rol que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.

No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione **Linux** o **AIX** como tipo de host. El servidor de SnapCenter añade el host y, a continuación, instala el plugin para base de datos de Oracle y el plugin para UNIX si los plugins no están todavía instalados en el host.

Para este campo…	Realice lo siguiente…
Nombre de host	Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN. Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • Cualquier nodo en el entorno de Oracle Real Application Clusters (RAC) El nodo VIP o IP de exploración no es compatible Si va a añadir un host mediante SnapCenter y el host forma parte de un subdominio, debe proporcionar el FQDN.
Credenciales	Seleccione el nombre de credencial que ha creado o cree nuevas credenciales. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales. Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host.

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) haga clic en **más opciones**.

Para este campo…	Realice lo siguiente…
Puerto	Conserve el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado. Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error.
Ruta de instalación	La ruta predeterminada es */opt/NetApp/snapcenter*. Opcionalmente, puede personalizar la ruta.
Añada todos los hosts en Oracle RAC	Seleccione esta casilla de comprobación para añadir todos los nodos del clúster en un Oracle RAC. En una configuración de Flex ASM, se agregarán todos los nodos, independientemente de si se trata de un nodo Hub o Leaf.
Omitir comprobaciones previas a la instalación	Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin.

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación Skip prechecks, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin.

   La secuencia de comandos comprobaciones previas no valida el estado del firewall del puerto del plugin si se especifica en las reglas de rechazo del firewall.

   Si no se cumplen los requisitos mínimos, se muestran los mensajes de error o advertencia pertinentes. Si el error está relacionado con el espacio en disco o RAM, es posible actualizar el archivo web.config ubicado en *C:\Program Files\NetApp\SnapCenter WebApp* para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero tendrá que solucionar el problema.

   En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Compruebe la huella y, a continuación, haga clic en **Confirmar y enviar**.

   En una configuración de clúster, debe comprobar la huella de cada uno de los nodos del clúster.

   SnapCenter no admite el algoritmo ECDSA.

   La verificación de huellas digitales es obligatoria aunque se haya añadido anteriormente el mismo host a SnapCenter y se haya confirmado la huella.

1. Supervise el progreso de la instalación.

   Los archivos de registro específicos de la instalación están en */custom_location/snapcenter/logs*.

Después de terminar

Todas las bases de datos en el host se detectan automáticamente y se muestran en la página Resources. Si no aparece nada, haga clic en **Actualizar recursos**.

Supervise el estado de la instalación

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- 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, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de plugins, proceda como sigue:
     a. Haga clic en **filtro**.
     b. Opcional: Indique las fechas de inicio y finalización.
     c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
     d. En el menú desplegable de estado, seleccione el estado de instalación.
     e. Haga clic en **aplicar**.
  4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Formas alternativas de instalar el paquete de plugins para Linux o AIX

Instale en varios hosts remotos mediante cmdlets

Debe utilizar el cmdlet de PowerShell *Install-SmHostPackage* para instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX en varios hosts.

Lo que necesitará

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador en cada host en el que desee instalar el paquete de plugins.

- Pasos*

1. Inicie PowerShell.
2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet _Open-SmConnection y, a continuación, introduzca sus credenciales.
3. Instale el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX mediante el cmdlet *Install-SmHostPackage* y los parámetros necesarios.

   Puede utilizar la opción *-skipprecheck* cuando ya haya instalado los plugins manualmente y no desee validar si el host cumple los requisitos para instalar el plugin.

   La secuencia de comandos comprobaciones previas no valida el estado del firewall del puerto del plugin si se especifica en las reglas de rechazo del firewall.

1. Introduzca sus credenciales para la instalación remota.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Instale en el host del clúster

Debe instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX en los dos nodos del host del clúster.

Cada uno de los nodos del host del clúster tiene dos IP. Una de las IP será la IP pública de los nodos correspondientes y la segunda IP será la IP de clúster que se compartirá entre ambos nodos.

- Pasos*

1. Instale el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX en los dos nodos del host del clúster.
2. Valide que los valores correctos de los parámetros SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT y SPL_ENABLED_PLUGINS se especifiquen en el archivo spl.properties ubicado en */var/opt/snapcenter/spl/etc/*.

   Si SPL_ENABLED_PLUGINS no se especifica en spl.properties, puede agregarla y asignar el valor SCO,SCU.

3. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet _Open-SmConnection y, a continuación, introduzca sus credenciales.

4. En cada uno de los nodos, establezca las IP preferidas del nodo mediante el comando *Set-PreferredHostIPsInStorageExportPolicy* sccli y los parámetros requeridos.
5. En el host del servidor SnapCenter, agregue una entrada para la IP del clúster y el nombre DNS correspondiente en *C:\Windows\System32\drivers\etc\hosts*.
6. Añada el nodo al servidor SnapCenter mediante el cmdlet *Add-SmHost* especificando la IP del clúster para el nombre de host.

Descubra la base de datos Oracle en el nodo 1 (suponiendo que la IP del clúster esté alojada en el nodo 1) y cree una copia de seguridad de la base de datos. Si se produce una conmutación por error, puede usar la copia de seguridad creada en el nodo 1 para restaurar la base de datos en el nodo 2. También puede usar el backup creado en el nodo 1 para crear un clon en el nodo 2.

Habrá volúmenes, directorios y archivos de bloqueo obsoletos si se produce la conmutación por error mientras se ejecuta cualquier otra operación de SnapCenter.

Instale el paquete de plugins para Linux en modo silencioso o modo de consola

Puede instalar el paquete de plugins de SnapCenter para Linux en el modo consola o en el modo silencioso mediante la interfaz de la línea de comandos (CLI).

Lo que necesitará

- Debe revisar los requisitos previos para instalar el paquete de plugins.
- Debe asegurarse de que la variable de entorno DISPLAY no esté configurada.

  Si se establece la variable de entorno DISPLAY, se debe ejecutar unset DISPLAY y, a continuación, intentar instalar manualmente el plugin.

Acerca de esta tarea

Debe proporcionar la información de instalación necesaria mientras instala en el modo consola, mientras que en la instalación en modo silencioso no tiene que proporcionar ninguna información de instalación.

- Pasos*
  1. Descargue el paquete de plugins de SnapCenter para Linux desde la ubicación de instalación del servidor SnapCenter.

     La ruta de instalación predeterminada es *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.
  2. Desde el símbolo del sistema, desplácese hasta el directorio en el que ha descargado el archivo de instalación.
  3. En función del modo de instalación que prefiera, lleve a cabo uno de los pasos siguientes.

Modo de instalación	Pasos
Modo de consola	a. Ejecución: `./SnapCenter_linux_host_plugin.bin -i console` b. Siga las instrucciones en pantalla para completar la instalación.
Modo silencioso	Ejecución: `./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-DUSER_INSTALL_DIR==/opt/custom_path`

4. Edite el archivo spl.properties ubicado en */var/opt/snapcenter/spl/etc/* para añadir SPL_ENABLED_PLUGINS=SCO,SCU y, a continuación, reinicie el servicio de cargador de plugins de SnapCenter.

> La instalación del paquete de plugins registra los plugins en el host y no en SnapCenter Server. Para registrar los plugins de SnapCenter Server, debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Al añadir el host, seleccione “Ninguno” como credencial. Una vez añadido el host, los plugins instalados se detectan de forma automática.

Instale el paquete de plugins para AIX en modo silencioso

Puede instalar el paquete de plugins de SnapCenter para AIX en modo silencioso mediante la interfaz de línea de comandos (CLI).

Lo que necesitará

- Debe revisar los requisitos previos para instalar el paquete de plugins.
- Debe asegurarse de que la variable de entorno DISPLAY no esté configurada.

  Si se establece la variable de entorno DISPLAY, se debe ejecutar unset DISPLAY y, a continuación, intentar instalar manualmente el plugin.

- Pasos*
  1. Descargue el paquete de plugins de SnapCenter para AIX desde la ubicación de instalación del servidor SnapCenter.

     La ruta de instalación predeterminada es *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.

  2. Desde el símbolo del sistema, desplácese hasta el directorio en el que ha descargado el archivo de instalación.

3. Ejecución

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR==/opt/custom_path-
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. Edite el archivo spl.properties ubicado en */var/opt/snapcenter/spl/etc/* para añadir SPL_ENABLED_PLUGINS=SCO,SCU y, a continuación, reinicie el servicio de cargador de plugins de SnapCenter.

> La instalación del paquete de plugins registra los plugins en el host y no en SnapCenter Server. Para registrar los plugins de SnapCenter Server, debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Al añadir el host, seleccione “Ninguno” como credencial. Una vez añadido el host, los plugins instalados se detectan de forma automática.

Configure el servicio de cargador de plugins de SnapCenter

El servicio de cargador de plugins de SnapCenter carga el paquete del plugin para Linux o AIX para interactuar con el servidor SnapCenter. El servicio de cargador de plugins de SnapCenter se instala cuando lo hace el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX.

Acerca de esta tarea

Después de instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX, el servicio de cargador de plugins de SnapCenter se inicia de forma automática. Si el servicio de cargador de plugins de SnapCenter no se inicia de forma automática, tendrá que:

- Asegúrese de que no se haya eliminado el directorio donde está funcionando el plugin
- Aumente el espacio de la memoria asignado a la máquina virtual Java

El archivo spl.properties, que se encuentra en */custom_location/NetApp/snapcenter/spl/etc/*, contiene los parámetros siguientes. Los valores predeterminados se asignan a estos parámetros.

Nombre del parámetro	Descripción
NIVEL_REGISTRO	Muestra los niveles de los registros que se admiten. Los posibles valores son INFO, DEBUG, TRACE, ERROR, FATAL, Y ADVIERTA.
SPL_PROTOCOL	Muestra el protocolo que admite el cargador del plugin de SnapCenter. Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.

Nombre del parámetro	Descripción
SNAPCENTER_SERVER_PROTOCOL	Muestra el protocolo compatible con SnapCenter Server. Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.
SKIP_JAVAHOME_UPDATE	De forma predeterminada, el servicio SPL detecta la ruta de Java y el parámetro update JAVA_HOME. Por lo tanto, el valor predeterminado se establece en FALSE. Puede establecer EN TRUE si desea deshabilitar el comportamiento predeterminado y corregir manualmente la ruta de acceso java.
SPL_KEYSTORE_PASS	Muestra la contraseña del archivo keystore. Puede cambiar este valor solo si cambia la contraseña o crea un nuevo archivo keystore.
SPL_PORT	Muestra el número de puerto en el que se está ejecutando el cargador del plugin de SnapCenter. Puede agregar el valor si falta el valor predeterminado. No debe cambiar el valor después de instalar los plugins.
SNAPCENTER_SERVER_HOST	Muestra la dirección IP o el nombre de host del servidor SnapCenter.
SPL_KEYSTORE_RUTA	Muestra la ruta absoluta del archivo keystore.
SNAPCENTER_SERVER_PORT	Muestra el número de puerto en el que se está ejecutando el servidor SnapCenter.

Nombre del parámetro	Descripción
LOGS_MAX_COUNT	Muestra el número de archivos de registro del cargador del plugin de SnapCenter que se conservan en la carpeta */custom_location/snapcenter/spl/logs*. El valor predefinido se establece en 5000. Si la cantidad es superior al valor especificado, se conservan los 5000 últimos archivos modificados. La comprobación del número de archivos se realiza de forma automática cada 24 horas desde el momento en que se inicia el servicio de cargador de plugins de SnapCenter. Si elimina manualmente el archivo spl.properties, el número de archivos que se desea conservar se establece en 9999.
JAVA_HOME	Muestra la ruta del directorio absoluto DE JAVA_HOME que se utiliza para iniciar el servicio SPL. Esta ruta se determina durante la instalación y como parte del SPL de inicio.
LOG_MAX_SIZE	Muestra el tamaño máximo del archivo de registro de trabajos. Una vez alcanzado el tamaño máximo, el archivo de registro se comprime y los registros se escriben en el nuevo archivo de ese trabajo.
RETAIN_LOGS_OF_LAST_DAYS	Muestra el número de días hasta los que se conservan los registros.
ENABLE_CERTIFICATE_VALIDATION	Muestra TRUE cuando la validación de certificados de CA está habilitada para el host. Puede habilitar o deshabilitar este parámetro editando la versión spl.properties o bien mediante la interfaz gráfica de usuario o el cmdlet de SnapCenter.

Si cualquiera de estos parámetros no se asignan al valor predeterminado, o si desea asignar o cambiar el valor, puede modificar el archivo spl.properties. También puede verificar el archivo spl.properties y editarlo para solucionar los problemas relacionados con los valores que se asignan a los parámetros. Después de modificar el archivo spl.properties, tendrá que reiniciar el servicio de cargador de plugins de SnapCenter.

- Pasos*
  1. Ejecute una de las siguientes acciones, según sea necesario:

- Inicie el servicio de cargador de plugins de SnapCenter como usuario raíz:

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl start`
** Detenga el servicio de cargador de plugins de SnapCenter:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
```

Puede utilizar la opción -force con el comando stop para detener el servicio de cargador de plugins de SnapCenter enérgicamente. Sin embargo, debe ser cauteloso antes de hacerlo, ya que también termina las operaciones existentes.

- Reinicie el servicio de cargador de plugins de SnapCenter:

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
** Busque el estado del servicio de cargador de plugins de
SnapCenter:
```

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl status`
** Busque el cambio en el servicio de cargador de plugins de
SnapCenter:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
```

Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux

Debe gestionar la contraseña del almacén de claves de SPL y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de SPL y configurar la pareja de claves firmadas de CA para el almacén de confianza de SPL con el servicio de cargador de plugins de SnapCenter para activar el certificado digital instalado.

SPL utiliza el archivo 'keystore.jks', que se encuentra en '/var/opt/snapcenter/spl/etc' tanto como su almacén de confianza como su almacén de claves.

Gestione la contraseña para el almacén de claves SPL y el alias de la pareja de claves firmada de CA en uso

- Pasos*

1. Puede recuperar la contraseña predeterminada del almacén de claves del SPL desde el archivo de propiedades del SPL.

Es el valor correspondiente a la clave 'PL_KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

```
 keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña para todos los alias de las entradas de clave
privada en el almacén de claves por la misma contraseña utilizada
para el almacén de claves:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Actualice lo mismo para la clave SPL_KEYSTORE_PASS en el archivo spl.properties.1.

3. Reinicie el servicio después de cambiar la contraseña.

La contraseña para el almacén de claves SPL y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

Configure los certificados intermedios o de raíz para el almacén de confianza SPL

Debe configurar los certificados intermedios o de raíz sin la clave privada en el almacén de confianza de SPL.

- Pasos*
  1. Desplácese hasta la carpeta que contiene el almacén de claves SPL: */var/opt/snapcenter/spl/etc*.
  2. Busque el archivo 'keystore.jks'.
  3. Enumere los certificados añadidos al almacén de claves:

```
 keytool -list -v -keystore keystore.jks
. Añada un certificado raíz o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath>
-keystore keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza de SPL.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configure la pareja de claves firmados de CA para el almacén de confianza SPL

Debe configurar la pareja de claves firmada de CA en el almacén de confianza del SPL.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves /var/opt/snapcenter/spl/etc. de SPL
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
 keytool -list -v -keystore keystore.jks
. Agregue el certificado de CA con clave pública y privada.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Enumere los certificados añadidos al almacén de claves.
```

```
 keytool -list -v -keystore keystore.jks
. Compruebe que el almacén de claves contiene el alias
correspondiente al nuevo certificado de CA, que se añadió al almacén
de claves.
. Cambie la contraseña de clave privada añadida para el certificado
de CA a la contraseña del almacén de claves.
```

La contraseña predeterminada del almacén de claves SPL es el valor de la clave SPL_KEYSTORE_PASS en el archivo spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>"
-keystore keystore.jks
. Si el nombre del alias del certificado de CA es largo y contiene
espacio o caracteres especiales ("*",","), cambie el nombre del alias
por un nombre simple:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure el nombre de alias del almacén de claves ubicado en el
archivo spl.propertiesI.
```

Actualice este valor contra la clave SPL_CERTIFICATE_ALIAS.

4. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza SPL.

Configurar la lista de revocación de certificados (CRL) para SPL

Debe configurar la CRL para SPL

Acerca de esta tarea

- SPL buscará los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de SPL es */var/opt/snapcenter/spl/etc/crl*.
- Pasos*
  1. Puede modificar y actualizar el directorio predeterminado del archivo spl.properties con respecto a la CLAVE SPL_CRL_PATH.
  2. Puede colocar más de un archivo CRL en este directorio.

     Los certificados entrantes se verificarán en cada CRL.

Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

Lo que necesitará

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.
  4. Haga clic en **más opciones**.
  5. Seleccione **Activar validación de certificados**.

Después de terminar

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- * * Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- * * Indica que el certificado CA se ha validado correctamente.
- * * Indica que el certificado CA no se pudo validar.
- * * indica que no se ha podido recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

Importe datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter

Importar datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter le permite continuar usando sus datos de las versiones anteriores.

Puede importar datos desde SnapManager para Oracle y SnapManager para SAP a SnapCenter ejecutando la herramienta de importación desde la interfaz de línea de comandos (CLI de host Linux).

La herramienta de importación crea políticas y grupos de recursos en SnapCenter. Las políticas y los grupos de recursos creados en SnapCenter se corresponden con los perfiles y las operaciones realizadas mediante dichos perfiles en SnapManager para Oracle y SnapManager para SAP. La herramienta de importación de SnapCenter interactúa con las bases de datos del repositorio de SnapManager para Oracle y SnapManager para SAP, así como la base de datos que desee importar.

- Recupera todos los perfiles, las programaciones y las operaciones realizadas mediante los perfiles.
- Crea una política de backup de SnapCenter para cada operación única y cada programación adjunta a un perfil.
- Crea un grupo de recursos para cada base de datos de destino.

Puede ejecutar la herramienta de importación ejecutando el script sc-migrate ubicado en */opt/NetApp/snapcenter/spl/bin*. Al instalar el paquete de plugins de SnapCenter para Linux en el host de la base de datos que desea importar, el script sc-migrate se copia en */opt/NetApp/snapcenter/spl/bin*.

No es posible importar datos desde la interfaz gráfica de usuario (GUI) de SnapCenter.

SnapCenter no es compatible con Data ONTAP operando en 7-Mode. Puede utilizar la 7-Mode Transition Tool para migrar datos y configuraciones que se almacenan en un sistema que ejecuta Data ONTAP operando en 7-Mode a un sistema ONTAP.

Configuraciones compatibles para la importación de datos

Antes de importar datos desde SnapManager 3.4.x para Oracle y SnapManager 3.4.x para SAP hacia SnapCenter, debe tener en cuenta cuáles son las configuraciones compatibles con el plugin de SnapCenter para base de datos de Oracle.

Las configuraciones compatibles con el plugin de SnapCenter para base de datos de Oracle se enumeran en la "Herramienta de matriz de interoperabilidad de NetApp".

Qué elementos se importan en SnapCenter

Es posible usar los perfiles para importar perfiles, programas y operaciones ejecutados.

De SnapManager para Oracle y SnapManager para SAP	A SnapCenter
Perfiles sin operaciones ni programas	Se crea una política con las opciones de tipo de backup Online y de alcance de backup Full.

De SnapManager para Oracle y SnapManager para SAP	A SnapCenter
Perfiles con una o más operaciones	Se crean múltiples políticas de acuerdo con una combinación única de un perfil y las operaciones ejecutadas por medio de ese perfil. Las políticas que se crean en SnapCenter contienen los detalles de retención y de eliminación de registros de archivo que se recuperan del perfil y de las operaciones correspondientes.
Configurar perfiles con Oracle Recovery Manager (RMAN)	Las directivas se crean con la opción **Catalog backup with Oracle Recovery Manager** activada. Si se utilizó la catalogación externa de RMAN en SnapManager, debe configurar los ajustes del catálogo de RMAN en SnapCenter. Puede seleccionar la credencial existente o crear una nueva credencial. Si se configuró RMAN a través del archivo de control en SnapManager, no será necesario configurar RMAN en SnapCenter.
Programa conectado a un perfil	Se crea una política específica y exclusiva para el programa.
Base de datos	Se crea un grupo de recursos para cada base de datos que se importa. En una configuración de Real Application Clusters (RAC), el nodo en el que se ejecuta la herramienta de importación se convierte en el nodo preferido tras la importación y se crea el grupo de recursos para ese nodo.

Cuando se importa un perfil, se crea una política de verificación junto con la política de backups.

Si se importan en SnapCenter los perfiles, las programaciones y cualquier operación de SnapManager para Oracle y SnapManager para SAP, también se importan los distintos valores de los parámetros.

Parámetros y valores de SnapManager para Oracle y SnapManager para SAP	Parámetros y valores de SnapCenter	Notas
Alcance de backup • Lleno • SQL Server • Registro	Alcance de backup • Lleno • SQL Server • Registro	
Modo de backup • Automático • En línea • Sin conexión	Tipo de backup • En línea • Apagado sin conexión	Si el modo de backup es Auto, la herramienta de importación verifica cuál era el estado de la base de datos cuando se ejecutó la operación y define, según corresponda, el tipo de backup como Online u Offline Shutdown.
Retención • Días • Recuentos	Retención • Días • Recuentos	SnapManager para Oracle y SnapManager para SAP utiliza tanto días como números para determinar la retención. En SnapCenter, hay días *O* recuentos. Por lo tanto, la retención se define con respecto a los días, porque se prefieren los días antes que los números en SnapManager para Oracle y SnapManager para SAP.
Eliminar para programaciones • Todo • Número de cambio de sistema (SCN) • Fecha • Registros creados antes de horas, días, semanas y meses específicos	Eliminar para programaciones • Todo • Registros creados antes de horas y días específicos	SnapCenter no admite la eliminación basada en SCN, Fecha, semanas y meses.

Parámetros y valores de SnapManager para Oracle y SnapManager para SAP	Parámetros y valores de SnapCenter	Notas
Notificación • Solo se envían mensajes de correo electrónico sobre operaciones desarrolladas correctamente • Solo se envían mensajes de correo electrónico sobre operaciones con errores • Se envían mensajes de correo electrónico sobre operaciones desarrolladas correctamente y operaciones con errores	Notificación • Siempre • En caso de fallo • Advertencia • Error	Las notificaciones por correo electrónico se importan. Sin embargo, debe actualizar manualmente el servidor SMTP con la interfaz gráfica de usuario de SnapCenter. El asunto del correo electrónico está en blanco para que usted lo configure.

Qué elementos no se importan en SnapCenter

La herramienta de importación no importa todos los elementos en SnapCenter.

Los siguientes elementos no se pueden importar en SnapCenter:

- Metadatos de backups
- Backups parciales
- Backups relacionados con Virtual Storage Console (VSC) y asignación de dispositivos sin formato (RDM)
- Roles o cualquier tipo de credenciales disponibles en el repositorio de SnapManager para SAP y SnapManager para Oracle
- Datos relacionados con operaciones de verificación, restauración y clonado
- Eliminar para operaciones
- Detalles de replicación especificados en el perfil de SnapManager para Oracle y el perfil de SnapManager para SAP

  Después de la importación, debe editar manualmente la política correspondiente creada en SnapCenter para incluir los detalles de la replicación.

- Información de backups catalogados

Prepare la importación de datos

Antes de importar datos en SnapCenter, debe ejecutar determinadas tareas para ejecutar la operación de importación con éxito.

- Pasos*

  1. Identifique la base de datos que desea importar.
  2. Utilice SnapCenter para añadir el host de la base de datos e instalar el paquete de plugins de SnapCenter para Linux.

3. Utilice SnapCenter para configurar las conexiones de las máquinas virtuales de almacenamiento (SVM) que utilizan las bases de datos en el host.
4. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
5. En la página Resources, asegúrese de que se determina y se muestra la base de datos que deba importarse.

   Cuando desee ejecutar la herramienta de importación, la base de datos deberá estar accesible o se producirá un error al crear el grupo de recursos.

Si la base de datos cuenta con credenciales configuradas, deberá crear la credencial correspondiente en SnapCenter, asignar la credencial a la base de datos y, después, ejecutar de nuevo el descubrimiento de la base de datos. Si la base de datos se encuentra en Automatic Storage Management (ASM), deberá crear credenciales para la instancia de ASM y asignar la credencial a la base de datos.

1. Asegúrese de que el usuario que ejecute la herramienta de importación tenga derechos suficientes para ejecutar SnapManager para Oracle o SnapManager para comandos de la CLI de SAP (como el comando de suspender programaciones) desde SnapManager para Oracle o SnapManager para el host de SAP.
2. Ejecute los siguientes comandos en el host de SnapManager para Oracle o SnapManager para SAP a fin de suspender las programaciones:
   a. Si desea suspender las programaciones en el host de SnapManager para Oracle, ejecute:
      - `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smo credential set -profile -name profile_name`

        Debe ejecutar el comando smo credential set para cada perfil del host.

   b. Si desea suspender las programaciones en el host de SnapManager para SAP, ejecute:
      - `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smsap credential set -profile -name profile_name`

        Debe ejecutar el comando smsap credential set para cada perfil del host.
3. Asegúrese de que se muestre un nombre de dominio completo (FQDN) del host de la base de datos cuando ejecute hostname -f

   Si no se muestra un FQDN, debe modificar /etc/hosts para indicar el FQDN del host.

Importar datos

Puede importar datos ejecutando la herramienta de importación desde el host de la base de datos.

Acerca de esta tarea

Las políticas de backup de SnapCenter que se crean después de importar tienen diferentes formatos de nomenclatura:

- Las políticas creadas para los perfiles sin operaciones ni programaciones tienen el formato SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED.

  Cuando no se realicen operaciones mediante un perfil, la política correspondiente se creará con el tipo de backup predeterminado como en línea y el ámbito del backup como completo.

- Las políticas creadas para los perfiles con una o más operaciones tienen el formato SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- Las políticas creadas para las programaciones adjuntas a los perfiles tienen el formato SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- Pasos*
  1. Inicie sesión en el host de la base de datos que desee importar.
  2. Ejecute la herramienta de importación ejecutando el script sc-migrate ubicado en */opt/NetApp/snapcenter/spl/bin*.
  3. Introduzca el nombre de usuario y la contraseña del servidor SnapCenter.

     Después de validar las credenciales, se establecerá una conexión con SnapCenter.

  4. Especifique los detalles de la base de datos del repositorio de SnapManager para Oracle o SnapManager para SAP.

     La base de datos del repositorio incluye las bases de datos que están disponibles en el host.

  5. Especifique los detalles de la base datos de destino.

     Si desea importar toda la base de datos en el host, especifique all.

  6. Si desea generar un registro del sistema o enviar mensajes ASUP por operaciones con errores, tendrá que habilitarlos ejecutando los comandos *Add-SmStorageConnection* o *Set-SmStorageConnection*.

Si desea cancelar una operación de importación, ya sea al ejecutar la herramienta de importación o después de la importación, debe eliminar manualmente las políticas de SnapCenter, las credenciales y los grupos de recursos creados como parte de la operación de importación.

Resultados

Las políticas de backup de SnapCenter se crean para perfiles, programaciones y operaciones realizadas mediante los perfiles. Los grupos de recursos también se crean para cada base de datos de destino.

Después de importar los datos correctamente, las programaciones asociadas con la base de datos importada se suspenden en SnapManager para Oracle y SnapManager para SAP.

Después de importar, tiene que gestionar la base de datos importada o el sistema de archivos usando SnapCenter.

Los registros de cada ejecución de la herramienta de importación se almacenan en el directorio */var/opt/snapcenter/spl/logs* con el nombre spl_migration_timestamp.log. Puede consultar este registro para revisar los errores de importación y solucionar sus problemas.

Instale el plugin de SnapCenter para VMware vSphere

Si la base de datos está almacenada en máquinas virtuales (VM) o si desea proteger máquinas virtuales y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte "Visión General de la implementación".

Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte "Crear o importar certificado SSL".

Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es */opt/netapp/config/crl*.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

Preparar la protección de bases de datos de Oracle

Antes de ejecutar una operación de protección de datos, como un backup, un clon o una restauración, debe definir una estrategia y configurar el entorno. También debe configurar SnapCenter Server para que use las tecnologías SnapMirror y SnapVault.

Para aprovechar las ventajas de las tecnologías SnapVault y SnapMirror, debe configurar e inicializar una relación de protección de datos entre el volumen de origen y el volumen de destino en el dispositivo de almacenamiento. Puede usar NetApp System Manager o la línea de comandos de la consola de almacenamiento para ejecutar estas tareas.

Antes de usar el plugin para base de datos de Oracle, el administrador de SnapCenter debe instalar y configurar el servidor de SnapCenter y llevar a cabo las tareas de los requisitos previos.

- Instalar y configurar SnapCenter Server. "Leer más"
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento. "Leer más"

SnapCenter no admite varias SVM con el mismo nombre en clústeres diferentes. Cada SVM registrada en SnapCenter con registro de SVM o de clúster debe ser única.

- Cree credenciales con el modo de autenticación como Linux o AIX para el usuario de instalación. "Leer más"
- Añada hosts, instale los plugins y detecte los recursos.
- Si va a utilizar SnapCenter Server para proteger las bases de datos de Oracle que residen en LUN o VMDK de VMware RDM, debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter.
- Instale Java en el host Linux o AIX.

  Consulte "Requisitos del host Linux" o. "Requisitos del host AIX" si quiere más información.

- Debe configurar el tiempo de espera del firewall de la aplicación con un valor de 3 horas o más.
- Si tiene bases de datos de Oracle en entornos NFS, debe haber configurado al menos una LIF de datos NFS para almacenamiento principal o secundario a fin de realizar operaciones de montaje, clonado, verificación y restauración.
- Si tiene varias rutas de datos (LIF) o una configuración de dNFS, puede realizar lo siguiente mediante la CLI de SnapCenter en el host de la base de datos:
  - De forma predeterminada, todas las direcciones IP del host de la base de datos se añaden a la directiva de exportación de almacenamiento de NFS en la máquina virtual de almacenamiento (SVM) para los volúmenes clonados. Si desea contar con una dirección IP específica o restringir a una subred de direcciones IP, ejecute la CLI de Set-PreferredHostIPsInStorageExportPolicy.
  - Si tiene varias LIF en la SVM, SnapCenter elije la ruta de LIF correspondiente para montar el volumen clonado de NFS. No obstante, si desea especificar una determinada ruta de LIF, debe ejecutar la CLI de Set-SvmPreferredDataPath. La guía de referencia de comandos tiene más información.
- Si tiene bases de datos de Oracle en entornos SAN, asegúrese de que el entorno SAN esté configurado según las recomendaciones mencionadas en las siguientes guías:
  - "Configuración del host recomendada para Linux Unified Host Utilities"
  - "Uso de hosts Linux con almacenamiento de ONTAP"
  - "Configuración del host afectada por AIX Host Utilities"
- Si tiene bases de datos de Oracle en LVM en sistemas operativos Oracle Linux o RHEL, instale la versión más reciente de Logical Volume Management (LVM).
- Si utiliza SnapManager para Oracle y desea migrar al plugin de SnapCenter para base de datos de Oracle, puede migrar los perfiles a políticas y grupos de recursos de SnapCenter usando el comando sccli sc-Migrate.
- Configure SnapMirror y SnapVault en ONTAP si quiere realizar una replicación de backup

Para los usuarios de SnapCenter 4.1.1, la documentación del plugin de SnapCenter para VMware vSphere 4.1.1 tiene información sobre la protección de las bases de datos y los sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, la documentación de NetApp Data Broker 1.0 y 1.0.1 ofrece información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el plugin de SnapCenter para VMware vSphere que proporciona el dispositivo virtual de agente de datos de NetApp basado en Linux (formato de dispositivo virtual abierto). Para los usuarios de SnapCenter 4.3.x, la documentación del plugin de SnapCenter para VMware vSphere 4.3 tiene información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual del plugin de SnapCenter para VMware vSphere basado en Linux (formato de dispositivo virtual abierto).

Más información

- "Herramienta de matriz de interoperabilidad"

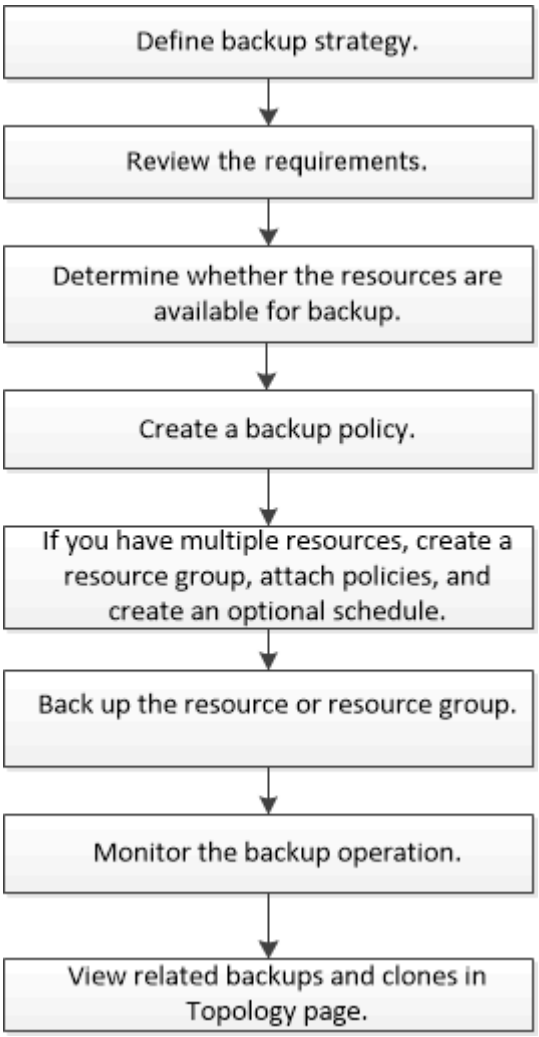
- "Documentación del plugin de SnapCenter para VMware vSphere"
- "Error en la operación de protección de datos en un entorno no multivía en RHEL 7 y versiones posteriores"

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.

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.*207*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-B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2BS123-B2B2BS123-B2B2B2B2B2B2B2B2B2B2BS123-B2B2BS123-B2B2B2B2B2B2BS123-B2BS

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, 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.

Cómo evitar que SnapCenter descubra entradas que no pertenecen a la 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.

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.

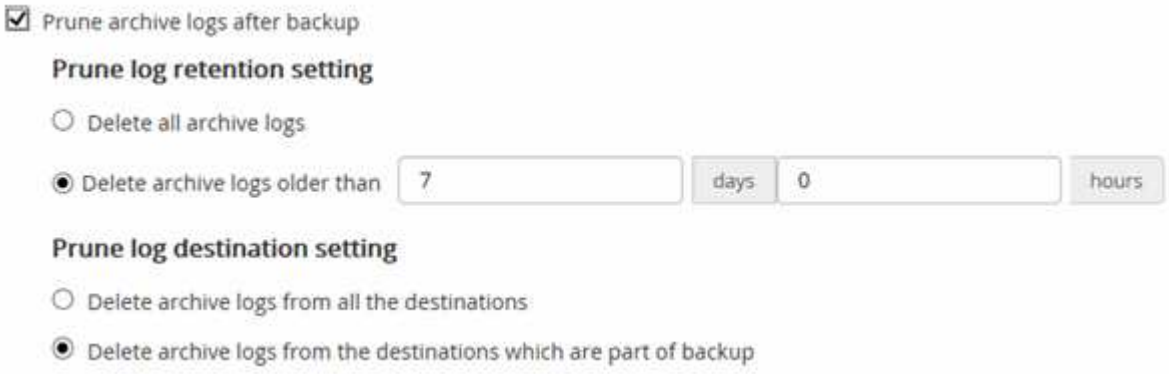
  Si desea catalogar backups de una base de datos de RAC, asegúrese de que no exista otro trabajo en ejecución para esa base de datos. Si existe otro trabajo en ejecución, la operación de catalogación genera un error se interrumpe tras generar un error y no se colocar en cola.
- Si desea reducir los registros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

   SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y 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

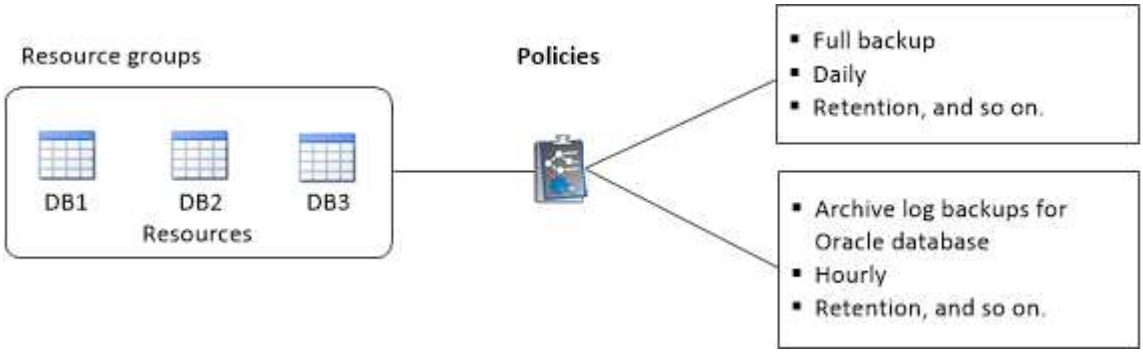
Un grupo de recursos es el contenedor al que debe añadir los recursos que desea proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación.

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 los siguientes pasos:

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 Configure Schedules correspondiente a la política para la cual 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 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.

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, 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 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.

Para este campo…	Realice lo siguiente…
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 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**.

      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 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. 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**.

     Se puede buscar el grupo de recursos ingresando su nombre en el cuadro de búsqueda o haciendo clic en * **y, luego, 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 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 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*.

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

Montar y desmontar backups de bases de datos

Si desea acceder a los archivos en el backup, puede montar uno o varios backups de solo datos y registros. Se puede montar el backup en el mismo host donde se creó el backup o en uno remoto con el mismo tipo de configuración de host y de Oracle. Si montó manualmente los backups, debe desmontarlos manualmente después de completar la operación. En cualquier instancia determinada, se puede montar un backup de una base de datos en cualquier host. Mientras realiza una operación, puede montar un solo backup.

En una configuración de Flex ASM, no puede realizar la operación de montaje en los nodos Leaf si la cardinalidad es menor que el número de nodos del clúster RAC.

Montar un backup de base de datos

Si desea acceder a los archivos en el backup, debe montar manualmente un backup de base de datos.

Lo que necesitará

- Si tiene una instancia de base de datos de Automatic Storage Management (ASM) en un entorno NFS y desea montar las copias de seguridad de ASM, debe haber agregado la ruta de acceso a los discos ASM */var/opt/snapcenter/sco/backup*/*/**/*_* en la ruta de acceso existente definida en el parámetro asm_diskstring.
- Si tiene una instancia de base de datos de ASM en un entorno NFS y desea montar los backups de registros de ASM como parte de una operación de recuperación, debe haber agregado la ruta de acceso al disco ASM */var/opt/snapcenter/scu/clones/*/** en la ruta de acceso existente definida en el parámetro

asm_diskstring.

- En el parámetro asm_diskstring, debe configurar *AFD:** si está utilizando ASMFD o configurar *ORCL:** si está utilizando ASMLIB.

> Para obtener información sobre cómo editar el parámetro asm_diskstring, consulte "Cómo agregar las rutas de acceso al disco a asm_diskstring".

- Deben configurar las credenciales de ASM y el puerto ASM si difiere del host de la base de datos de origen mientras se monta el backup.
- Si desea montar en un host alternativo, debe verificar que este host cumpla los siguientes requisitos:
  - El mismo UID y GID que el host original
  - La misma versión de Oracle que el host original
  - La misma distribución de sistema operativo que el host original
  - En NVMe, se debe instalar NVMe util
- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup compuesto por protocolos mixtos iSCSI y FC. Para obtener más información, consulte "Error en la operación porque no puede detectar el dispositivo para la LUN".
- 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** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

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

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en el sistema de almacenamiento principal o secundario (reflejado o replicado).
5. Seleccione el backup en la tabla y haga clic en .
6. En la página Mount backups, seleccione el host en el que desea montar la copia de seguridad en la lista desplegable **Elija el host para montar la copia de seguridad**.

   Aparece la ruta de acceso de montaje */var/opt/snapcenter/sco/backup_Mount/backup_name/database_name*.

Si va a montar el backup de una base de datos de ASM, aparece la ruta de acceso de montaje +diskgroupname_SID_backupid.

1. Haga clic en **Mount**.

Después de terminar

- Es posible ejecutar el siguiente comando para recuperar la información relacionada con el backup montado:

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- Si montó una base de datos de ASM, puede ejecutar el siguiente comando para recuperar la información relacionada con el backup montado:

  ```
  ./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
  ```

- Para recuperar el ID de backup, ejecute el siguiente comando:

  ```
  ./sccli Get-Smbackup-BackupNamebackup_name
  ```

  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".

Desmontar un backup de base de datos

Es posible desmontar manualmente un backup de base de datos montado si ya no se desea acceder a los archivos en el backup.

- 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** o **Resource Group** en la lista **View**.
  3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

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

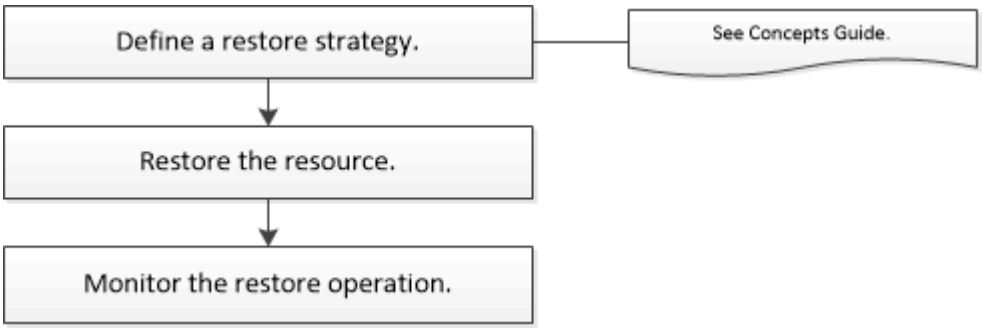
  4. Seleccione el backup que está montado y haga clic en .
  5. Haga clic en **Aceptar**.

Restaurar y recuperar bases de datos de Oracle

Restaure el flujo de trabajo

El flujo de trabajo de restauración incluye la planificación, la realización de operaciones de restauración y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de restauración:



Definir una estrategia de restauración y recuperación para bases de datos de Oracle

Para poder ejecutar operaciones de restauración y recuperación correctamente, es necesario definir una estrategia antes de restaurar y recuperar una base de datos.

Tipos de backups compatibles con las operaciones de restauración y recuperación

SnapCenter admite la restauración y recuperación de diferentes tipos de backups de bases de datos de Oracle.

- Backups de datos en línea
- Backups de datos sin conexión apagados
- Backups de datos sin conexión montados

> Si va a restaurar un backup de datos sin conexión apagado o sin conexión montado, SnapCenter deja la base de datos en estado sin conexión. Es necesario recuperar manualmente la base de datos y restablecer los registros.

- Backup completo
- Backups sin conexión montados de bases de datos en espera de Data Guard
- Backups en línea solo de datos de bases de datos en espera de Active Data Guard

> No se pueden realizar operaciones de recuperación de bases de datos en espera de Active Data Guard.

- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración RAC
- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración ASM

Tipos de métodos de restauración compatibles con las bases de datos de Oracle

SnapCenter es compatible con operaciones de conexión y copia y de restauración sin movimiento de bases de datos de Oracle. Durante una operación de restauración, SnapCenter determina el método de restauración adecuado del sistema de archivos que se usará para restaurar sin pérdida de datos.

> SnapCenter no es compatible con SnapRestore basado en volúmenes.

Restauración por conexión y copia

Si el diseño de la base de datos difiere del backup o si se agregan archivos nuevos después de la creación del backup, se ejecuta una restauración por conexión y copia. En el método de restauración por conexión y copia, se ejecutan las siguientes tareas:

- Pasos*
  1. Se clona el volumen a partir de la copia de Snapshot, y se construye la pila del sistema de archivos en el host con los LUN o volúmenes clonados.
  2. Se copian los archivos de los sistemas de archivos clonados en los sistemas de archivos originales.

3. Los sistemas de archivos clonados luego se desmontan del host, y se eliminan los volúmenes clonados de ONTAP.

> Para una configuración de Flex ASM (donde la cardinalidad es inferior al número de nodos del clúster de RAC) o bases de datos de RAC de ASM en VMDK o RDM, solo se admite el método de restauración por conexión y copia.

Aunque se haya habilitado una restauración sin movimiento forzada, SnapCenter ejecuta la restauración por conexión y copia en las siguientes situaciones:

- Restauración desde el sistema de almacenamiento secundario, si Data ONTAP corresponde a una versión anterior a 8.3
- Restauración de grupos de discos de ASM en nodos de una configuración de Oracle RAC en la cual no está configurada la instancia de base de datos
- En una configuración de Oracle RAC, en cualquiera de los nodos del mismo nivel si la instancia de ASM o del clúster no están en ejecución o si el nodo del mismo nivel está inactivo
- Restauración de los archivos de control únicamente
- Restauración de un subconjunto de espacios de tablas que residen en un grupo de discos de ASM
- Grupo de discos compartido entre archivos de datos, archivo sp y archivo de contraseñas
- Servicio de SnapCenter Plug-in Loader (SPL) no instalado o sin ejecución en el nodo remoto de un entorno RAC
- Adición de nuevos nodos a Oracle RAC sin que SnapCenter Server reciba información sobre los nuevos nodos agregados

Restauración sin movimiento

Si el diseño de la base de datos es similar al backup y no hubo ningún cambio de configuración en el almacenamiento ni en la pila de base de datos, se ejecuta una restauración sin movimiento, en la cual se restauran el archivo o el LUN en ONTAP. SnapCenter es compatible únicamente con SnapRestore de archivo único (SFSR) como parte del método de restauración sin movimiento.

> Data ONTAP 8.3 o y versiones posteriores son compatibles con la restauración sin movimiento desde una ubicación secundaria.

Si se desea ejecutar una restauración sin movimiento en la base de datos, es necesario confirmar que solo haya archivos de datos en el grupo de discos de ASM. Se debe crear un backup cada vez que se hacen cambios en el grupo de discos de ASM o en la estructura física de la base de datos. Después de ejecutar una restauración sin movimiento, el grupo de discos contendrá la misma cantidad de archivos de datos que había en el momento del backup.

La restauración sin movimiento se aplica automáticamente cuando el grupo de discos o el punto de montaje cumple los siguientes criterios:

- No se agregan nuevos archivos de datos después del backup (control de archivos externo).
- No se agregan, eliminan ni recrean discos de ASM o LUN después del backup (control de cambios estructurales del grupo de discos de ASM).
- No se agregan, eliminan ni recrean LUN en el grupo de discos de LVM (control de cambios estructurales del grupo de discos de LVM).

También es posible habilitar una restauración sin movimiento forzada desde la interfaz gráfica de usuario, desde la interfaz de línea de comandos de SnapCenter o desde el cmdlet de PowerShell para anular el control de archivos externo y el control de cambios estructurales del grupo de discos de LVM.

Restauración sin movimiento en RAC de ASM

En SnapCenter, el nodo en el que se ejecuta la restauración se denomina nodo primario, y los demás nodos de RAC donde reside el grupo de discos de ASM se denominan nodos del mismo nivel. SnapCenter cambia el estado del grupo de discos de ASM a desmontaje en todos los nodos donde el grupo de discos de ASM tiene estado de montaje antes de ejecutar la operación de restauración de almacenamiento. Una vez que se termina de restaurar el almacenamiento, SnapCenter cambia el estado del grupo de discos de ASM al que tenía antes de la operación de restauración.

En los entornos DE SAN, SnapCenter quita los dispositivos de todos los nodos del mismo nivel y ejecuta la operación de anulación de asignación de LUN antes de la operación de restauración de almacenamiento. Después de la operación de restauración de almacenamiento, SnapCenter ejecuta una operación de asignación de LUN y construye los dispositivos en todos los nodos del mismo nivel. En un entorno DE SAN, si el diseño de ASM de Oracle RAC reside en LUN, durante la restauración SnapCenter ejecuta operaciones para desasignar LUN, restaurar LUN y asignar LUN en todos los nodos del clúster de RAC donde reside el grupo de discos de ASM. En la restauración, incluso si no todos los iniciadores de los nodos de RAC se usaban para los LUN, después de restaurar, SnapCenter crea un iGroup nuevo con todos los iniciadores de todos los nodos de RAC.

- Si hay algún fallo durante la actividad previa a la restauración en los nodos del mismo nivel, SnapCenter revierte automáticamente el estado del grupo de discos de ASM al usado antes de restaurar en los nodos del mismo nivel donde la operación previa a la restauración se ejecutó correctamente. No es posible revertir el nodo primario y el nodo del mismo nivel en los que falló la operación. Antes de intentar otra restauración, se debe reparar manualmente el problema en el nodo del mismo nivel y colocar el grupo de discos de ASM del nodo primario nuevamente en el estado de montaje.
- Si hay algún fallo durante la actividad de restauración, la operación de restauración falla y no se ejecuta la reversión. Antes de intentar otra restauración, se debe reparar manualmente el problema de restauración del almacenamiento y colocar el grupo de discos de ASM del nodo primario nuevamente en el estado de montaje.
- Si hay algún fallo durante la actividad posterior a la restauración en cualquiera de los nodos del mismo nivel, SnapCenter avanza con la operación de restauración en los demás nodos del mismo nivel. Es necesario reparar manualmente el problema posterior a la restauración en el nodo del mismo nivel.

Tipos de operaciones de restauración compatibles con las bases de datos de Oracle

SnapCenter permite ejecutar diferentes tipos de operaciones de restauración para las bases de datos de Oracle.

Antes de restaurar la base de datos, se validan los backups para identificar si faltan archivos al compararlos con los archivos de la base de datos real.

Restauración completa

- Solo restaura los archivos de datos
- Solo restaura los archivos de control
- Restaura los archivos de datos y los archivos de control

- Restaura archivos de datos, archivos de control y archivos de registro de recuperación en las bases de datos en espera de Data Guard y Active Data Guard

Restauración parcial

- Restaura solo los espacios de tablas seleccionados
- Restaura solo las bases de datos conectables (PDB) seleccionadas
- Restaura solo los espacios de tablas seleccionados de una PDB

Tipos de operaciones de recuperación compatibles con las bases de datos de Oracle

SnapCenter permite ejecutar diferentes tipos de operaciones de recuperación para las bases de datos de Oracle.

- La base de datos hasta la última transacción (todos los registros)
- La base de datos hasta un número de cambio de sistema específico (SCN)
- La base de datos hasta una fecha y hora específicas

  La fecha y la hora de la recuperación deben especificarse según la zona horaria del host de la base de datos.

  SnapCenter también incluye la opción no recovery para las bases de datos de Oracle.

> El plugin para la base de datos de Oracle no es compatible con la recuperación si se hizo una restauración con un backup creado con el rol de base de datos en espera. Para las bases de datos físicas en espera, siempre se debe usar la recuperación manual.

Limitaciones de la restauración y la recuperación de bases de datos de Oracle

Antes de ejecutar operaciones de restauración y recuperación, es necesario conocer las limitaciones.

Si está utilizando cualquier versión de Oracle de 11.2.0.4 a 12.1.0.1, la operación de restauración estará en estado de bloqueo cuando ejecute el comando *renamedg* . Puede aplicar el parche de Oracle 19544733 para solucionar este problema.

No se admiten las siguientes operaciones de restauración y recuperación:

- Restauración y recuperación de espacios de tablas en la base de datos del CDB raíz
- Restauración de espacios de tablas temporales y asociados con PDB
- Restauración y recuperación de espacios de tablas de varios PDB simultáneamente
- Restauración de backups de registros
- Restauración de backups en otra ubicación
- Restauración de archivos de registro de recuperación en cualquier configuración, excepto bases de datos en espera de Data Guard o de Active Data Guard
- Restauración de archivos SPFILE y Password
- Cuando se ejecuta una operación de restauración en una base de datos que se volvió a crear con el nombre de base de datos preexistente en el mismo host, fue gestionado por SnapCenter y tenía backups válidos, la operación de restauración sobrescribe los archivos de base de datos recién creados aunque los DBID sean diferentes.

Esto se puede evitar realizando una de las siguientes acciones:

- Detectar los recursos de SnapCenter después de volver a crear la base de datos
- Cree una copia de seguridad de la base de datos que se ha vuelto a crear

Limitaciones relacionadas con la recuperación de espacios de tablas en un momento específico

- No se admite la recuperación puntual (PITR) de los tablespaces SYSTEM, SYSAUX y UNDO
- No se pueden realizar PITR de tablespaces junto con otros tipos de restauraciones
- Si se cambia el nombre de un tablespace y se desea recuperarlo a un punto antes de cambiar su nombre, debe especificar el nombre anterior del tablespace
- Si las restricciones de las tablas de un tablespace se encuentran en otro tablespace, debe recuperar los dos tablespaces
- Si una tabla y sus índices se almacenan en tablespaces diferentes, los índices se deben eliminar antes de ejecutar PITR
- PITR no se puede utilizar para recuperar el tablespace por defecto actual
- PITR no se puede utilizar para recuperar tablespaces que contengan cualquiera de los siguientes objetos:
  - Objetos con objetos subyacentes (como vistas materializadas) o objetos contenidos (como tablas particionadas) a menos que todos los objetos subyacentes o contenidos estén en el conjunto de recuperación

    Además, si las particiones de una tabla con particiones se almacenan en distintos tablespaces, debe eliminar la tabla antes de realizar PITR o mover todas las particiones al mismo tablespace antes de realizar PITR.

  - Deshacer o revertir segmentos
  - Colas avanzadas compatibles con Oracle 8 con varios destinatarios
  - Objetos propiedad del usuario SYS

    Ejemplos de estos tipos de objetos son PL/SQL, clases Java, programas de llamada, vistas, sinónimos, usuarios, privilegios, dimensiones, directorios y secuencias.

Orígenes y destinos para restaurar bases de datos de Oracle

Es posible restaurar una base de datos de Oracle desde una copia de backup en el almacenamiento primario o el almacenamiento secundario. Las bases de datos se pueden restaurar únicamente en la misma ubicación y en la misma instancia de base de datos. Sin embargo, en la configuración de RAC, se pueden restaurar bases de datos a otros nodos.

Orígenes para operaciones de restauración

Es posible restaurar bases de datos desde un backup en el almacenamiento primario o el almacenamiento secundario. Si desea restaurar desde un backup en el almacenamiento secundario en una configuración de reflejos múltiples, puede seleccionar el reflejo de almacenamiento secundario como origen.

Destinos para operaciones de restauración

Las bases de datos se pueden restaurar únicamente en la misma ubicación y en la misma instancia de base de datos.

En una configuración de RAC, se pueden restaurar bases de datos de RAC desde cualquier nodo en el clúster.

Variables de entorno predefinidas para restaurar scripts previos y posteriores específicos

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y el script posterior mientras se restaura una base de datos.

Variables de entorno predefinidas admitidas para restaurar una base de datos

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

  Ejemplo: 257

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

  Si la operación implica varias bases de datos, esto contendrá nombres de bases de datos separados por tuberías.

  Ejemplo: NFSB31

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

  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.

  Ejemplo: oracle

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

  Ejemplo: Oinstall

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

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplos:

  - Si la base de datos no se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Si la base de datos se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1,RG2_scspr2417819002_07-21-2021_12.16.48.9267_1,RG2_sspr2417819002_07-22-2021_12.16.48.9267_1

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

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplos:

- Si la base de datos no se está ejecutando en modo ARCHIVELOG: DATA@203|LOG@205
- Si la base de datos se está ejecutando en modo ARCHIVELOG: DATA@203|LOG@205,206,207

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

  Ejemplo: RG1

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

  Ejemplo: /Ora01/app/oracle/product/18.1.0/dB_1

- **SC_RECOVERY_TYPE** especifica los archivos que se recuperan y también el ámbito de recuperación.

  Ejemplo: RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Para obtener más información acerca de los delimitadores, consulte "Delimitadores compatibles".

Requisitos para restaurar una base de datos de Oracle

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

- Definió la estrategia de restauración y recuperación.
- El administrador de SnapCenter asignó SVM para los volúmenes de origen y los volúmenes de destino si va a replicar copias de Snapshot a un reflejo o un almacén.
- Si se reducen los archivos de registro como parte del backup, debe haber montado manualmente los backups de los archivos de registro requeridos.
- Si desea restaurar bases de datos de Oracle que residen en un VMDK, debe asegurarse de que la máquina invitada tenga la cantidad requerida de ranuras libres para asignar los VMDK clonados.
- Se aseguró de que todos los volúmenes de datos y los volúmenes de registros de archivos que pertenecen a la base de datos estén protegidos si la protección secundaria está habilitada para esa base de datos.
- Debe asegurarse de que la base de datos RAC One Node se encuentra en estado "nomount" para realizar una restauración completa de archivos de control o de bases de datos.
- Si tiene una instancia de base de datos de ASM en el entorno NFS, debe añadir la ruta de acceso al disco de ASM */var/opt/snapcenter/scu/clones/*/** a la ruta de acceso existente definida en el parámetro asm_diskstring de modo que pueda montar correctamente los backups de registro de ASM como parte de la operación de recuperación.
- En el parámetro asm_diskstring, debe configurar *AFD:** si está utilizando ASMFD o configurar *ORCL:** si está utilizando ASMLIB.

  Para obtener información sobre cómo editar el parámetro asm_diskstring, consulte "Cómo agregar las rutas de acceso al disco a asm_diskstring"

- Debe configurar el listener estático en el archivo **listener.ora** disponible en *$ORACLE_HOME/network/admin* para bases de datos que no son de ASM y *$GRID_HOME/network/admin* para bases de datos de ASM si ha deshabilitado la autenticación del sistema operativo y ha habilitado la autenticación de base de datos de Oracle para una base de datos de

Oracle, y desea restaurar los archivos de datos y archivos de control de esa base de datos.

- Debe aumentar el valor del parámetro SCORestoreTimeout. Para hacerlo, ejecute el comando Set-SmConfigSettings si el tamaño de la base de datos está en terabytes (TB).
- Asegúrese de que todas las licencias requeridas para vCenter estén instaladas y actualizadas.

  Si las licencias no están instaladas o actualizadas, aparecerá un mensaje de advertencia. Si ignora la advertencia y continúa, se produce un error en la restauración desde RDM.

- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup compuesto por protocolos mixtos iSCSI y FC. Para obtener más información, consulte "Error en la operación porque no puede detectar el dispositivo para la LUN".

Restaurar y recuperar bases de datos de Oracle

En caso de pérdida de datos, es posible usar SnapCenter para restaurar datos desde uno o más backups en el sistema de archivos activo para luego recuperar la base de datos.

Acerca de esta tarea

La recuperación se lleva a cabo con los registros de archivos disponibles en la ubicación del registro de archivos configurado. Si la base de datos se está ejecutando en modo ARCHIVELOG, Oracle Database guarda los grupos rellenados de archivos redo log en uno o más destinos sin conexión, conocidos conjuntamente como redo log archivado. SnapCenter identifica y monta la cantidad óptima de backups de registros según el SCN especificado, la fecha y la hora seleccionadas o la opción All logs. Si los registros de archivos requeridos para la recuperación no están disponibles en la ubicación configurada, debe montar la copia Snapshot que contiene los registros y especificar la ruta como registros de archivo externos.

Si se migra la base de datos de ASM de ASMLIB a ASMFD, los backups creados con ASMLIB no se pueden utilizar para restaurar la base de datos. Es necesario crear backups en la configuración de ASMFD y utilizar esos backups para restaurar. De forma similar, si se migra la base de datos de ASM de ASMFD a ASMLIB, es necesario crear backups en la configuración de ASMLIB para restaurar.

Cuando restaura una base de datos, 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 restaurar la base de datos, se elimina automáticamente el archivo de bloqueo operativo.

No se admite la restauración de archivos SPFILE y Password.

- 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** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

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

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principal o secundario (reflejado o replicado).

5. Seleccione el backup en la tabla y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
   a. Si seleccionó un backup de una base de datos en un entorno RAC, seleccione el nodo de RAC.
   b. Al seleccionar un datos reflejados o de almacén:
      - si no hay backup de registros en el reflejo o el almacén, no se selecciona nada y los localizadores están vacíos.
      - si existen backups de registros en el reflejo o almacén, se selecciona el último backup de registros y se muestra el localizador correspondiente.

      Si el backup de registro seleccionado existe en la ubicación de reflejo y almacén, se muestran ambos localizadores.

   c. Realice las siguientes acciones:

Si desea restaurar…	Realice lo siguiente…
Todos los archivos de datos de la base de datos	Seleccione **todos los archivos de datos**. Solo se restauran los archivos de datos de la base de datos. No se restauran los archivos de control, los registros de archivos ni los archivos de registro de recuperación.
Espacios de tabla	Seleccione **Tablespaces**. Se pueden especificar los espacios de tabla que se desean restaurar.
Archivos de control	Seleccione **Archivos de control**. Al restaurar los archivos de control, asegúrese de que la estructura de directorio existe o se debe crear con las propiedades de usuario y grupo correctas, si las hay, para permitir que los archivos se copien a la ubicación de destino mediante el proceso de restauración. Si no existe el directorio, se producirá un error en el trabajo de restauración.

Si desea restaurar…	Realice lo siguiente…
Archivos de registro de recuperación	Seleccione **Redo log files**. Esta opción está disponible solo para bases de datos Data Guard en espera o Active Data Guard en espera. No se realiza un backup de los archivos de registro de recuperación para bases de datos que no son de Data Guard. Para bases de datos que no son de Data Guard, la recuperación se realiza con registros de archivos.
Bases de datos conectables (PDB)	Seleccione **Pluggable databases** y, a continuación, especifique las PDB que desea restaurar.
Espacios de tabla de bases de datos conectables (PDB)	Seleccione * tablespaces de base de datos conectables (PDB)* y, a continuación, especifique la PDB y los tablespaces de esa PDB que desea restaurar. Esta opción está disponible solo si seleccionó una PDB para restaurar.

d. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.

   Los distintos estados de una base de datos, del más alto al más bajo, son open, mounted, started y shutdown. Debe seleccionar esta casilla de comprobación si la base de datos está en un estado más alto, pero el estado debe cambiarse a un estado más bajo para realizar una operación de restauración. Si la base de datos está en un estado más bajo, pero el estado debe cambiarse a uno más alto para realizar la operación de restauración, el estado de la base de datos se modifica automáticamente aunque no seleccione la casilla de comprobación.

Si una base de datos está en el estado open y, para restaurarla, la base de datos necesita que esté en el estado mounted, el estado de la base de datos se modifica únicamente si selecciona esta casilla de comprobación.

a. Seleccione **Force in place restore** si desea realizar restauraciones in situ en los escenarios en los que se agregan nuevos archivos de datos después de la copia de seguridad o cuando se agregan, eliminan o recrean LUN en un grupo de discos de LVM.

7. En la página Recovery Scope, realice las siguientes acciones:

Si…	Realice lo siguiente…
Desea recuperar la última transacción	Seleccione **todos los registros**.
Desea recuperar a un número de cambio de sistema (SCN) específico	Seleccione **Until SCN (System Change Number)**.
Desea recuperar a una fecha y una hora específicas	Seleccione **Fecha y hora**. Debe especificar la fecha y la hora de la zona horaria del host de la base de datos.
No desea recuperar	Seleccione **sin recuperación**.
Desea especificar cualquier ubicación de registros de archivos externos	Si la base de datos se ejecuta en modo ARCHIVELOG, SnapCenter identifica y monta el número óptimo de backups de registros según el SCN especificado, la fecha y la hora seleccionadas o la opción All logs. Si aún desea especificar la ubicación de los archivos de registro de archivos externos, seleccione **especificar ubicaciones de registro de archivos externos**. Si se reducen los registros de archivos como parte del backup y se montaron manualmente los backups de los registros de archivo requeridos, debe especificar la ruta de acceso del backup montado como ubicación de registro de archivo externo para la recuperación. Debe verificar la ruta y el contenido de la ruta de montaje antes de enumerarla como ubicación de registro externo. • "Protección de datos de Oracle con ONTAP" • "Se produce un error en el funcionamiento con ORA-00308"

No se pueden realizar restauraciones con recuperación de backups secundarios si los volúmenes de registros de archivos no están protegidos y los volúmenes de datos sí lo están. Sólo puede restaurar seleccionando **sin recuperación**.

Si se va a recuperar una base de datos de RAC con la opción de base de datos abierta seleccionada, solo la instancia de RAC en la que se inició la operación de recuperación vuelve a estar en estado abierto.

No se admite la recuperación para bases de datos Data Guard en espera y Active Data Guard en espera.

8. En la página PreOps, introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de restauración.

   Debe almacenar los scripts previos en la ruta de acceso */var/opt/snapcenter/spl/scripts* o en cualquier carpeta dentro de ella. 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 usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

9. En la página PostOps, siga estos pasos:

   a. Introduzca la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de restauración.

      Debe almacenar 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.

      Si se produce un error en la operación de restauración, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

   b. Seleccione la casilla de comprobación si desea abrir la base de datos después de la recuperación.

      Después de restaurar una base de datos de contenedor (CDB) con o sin archivos de control, o después de restaurar solo los archivos de control de la CDB, si especifica que se abre la base de datos después de la recuperación, solo se abre la CDB y no las bases de datos conectables (PDB) de esa CDB.

      En una configuración de RAC, solo la instancia de RAC que se usa para la recuperación se abre después de esta.

      Después de restaurar un espacio de tabla de usuario con archivos de control, un espacio de tabla del sistema con o sin archivos de control o una PDB con o sin archivos de control, solo el estado de la PDB relacionada con la operación de restauración vuelve a su estado original. El estado de las demás PDB que no se usaron para la restauración no vuelven a su estado original, ya que el estado de esas PDB no se guardó. Debe modificar manualmente el estado de las PDB que no se usaron para la restauración.

10. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.

    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 de restauración realizada, debe seleccionar **Adjuntar informe de trabajo**.

Para la notificación por correo electrónico, debe haber especificado los detalles del servidor SMTP a través de la interfaz gráfica de usuario o el comando Set-SmSmtpServer de PowerShell.

1. Revise el resumen y, a continuación, haga clic en **Finalizar**.
2. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Para más información

- "Se omite la base de datos de Oracle RAC One Node para ejecutar operaciones de SnapCenter"
- "Error al restaurar desde una ubicación de SnapMirror o SnapVault secundaria"
- "Se ha producido un error al restaurar desde un backup de una encarnación huérfana"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

Restauración y recuperación de espacios de tablas mediante la recuperación de un momento específico

Se puede restaurar un subconjunto de espacios de tablas que se han dañado o eliminado sin afectar a los otros espacios de tablas de la base de datos. SnapCenter utiliza RMAN para realizar una recuperación puntual (PITR) de los tablespaces.

Lo que necesitará

Los backups necesarios para ejecutar PITR de espacios de tablas deben catalogarse y montarse.

Acerca de esta tarea

Durante la operación PITR, RMAN crea una instancia auxiliar en el destino auxiliar especificado. El destino auxiliar puede ser un punto de montaje o un grupo de discos ASM. Si hay suficiente espacio en la ubicación montada, puede reutilizar una de las ubicaciones montadas en lugar de un punto de montaje dedicado.

Debe especificar la fecha y hora o SCN y el espacio de tabla se restaurará en la base de datos de origen.

Se pueden seleccionar y restaurar varios espacios de tablas que residen en entornos ASM, NFS y SAN. Por ejemplo, si los espacios de tablas TS2 y TS3 residen en NFS y TS4 en SAN, puede realizar una única operación PITR para restaurar todos los espacios de tablas.

En una configuración de RAC, puede realizar PITR de tablespaces desde cualquier nodo del RAC.

- 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** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos del tipo de instancia única (Multitenant) ya sea en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

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

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principal o secundario (reflejado o replicado).

   Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione el backup catalogado y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
   a. Si seleccionó un backup de una base de datos en un entorno RAC, seleccione el nodo de RAC.
   b. Seleccione **Tablespaces** y, a continuación, especifique los tablespaces que desea restaurar.

      No puede realizar PITR en tablespaces SYSAUX, SYSTEM y UNDO.

   c. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.
7. En la página Recovery Scope, realice una de las siguientes acciones:
   - Si desea recuperar un número de cambio de sistema (SCN) específico, seleccione **hasta SCN** y especifique el SCN y el destino auxiliar.
   - Si desea recuperar una fecha y hora específicas, seleccione **Fecha y hora** y especifique la fecha y hora y el destino auxiliar.

     SnapCenter identifica y, a continuación, monta y cataloga la cantidad óptima de backups de datos y registros necesarios para realizar PITR según el SCN especificado o la fecha y hora seleccionadas.

8. En la página PreOps, introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de restauración.

   Debe almacenar los scripts previos en la ruta de acceso /var/opt/snapcenter/spl/scripts o en cualquier carpeta dentro de ella. 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 usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

1. En la página PostOps, siga estos pasos:
   a. Introduzca la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de restauración.

      Si se produce un error en la operación de restauración, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

   b. Seleccione la casilla de comprobación si desea abrir la base de datos después de la recuperación.
2. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los

que desea enviar las notificaciones por correo electrónico.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.
4. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Restaure y recupere una base de datos conectable mediante la recuperación de un momento específico

Puede restaurar y recuperar una base de datos conectables (PDB) que se dañó o se borró sin afectar a las otras PDB de la base de datos de contenedores (CDB). SnapCenter utiliza RMAN para realizar una recuperación de un momento específico (PITR) de la PDB.

Lo que necesitará

Los backups necesarios para ejecutar PITR de una PDB deben catalogarse y montarse.

En una configuración de RAC, debe cerrar manualmente la PDB (cambiando el estado a MONTADO) en todos los nodos de la configuración de RAC.

Acerca de esta tarea

Durante la operación PITR, RMAN crea una instancia auxiliar en el destino auxiliar especificado. El destino auxiliar puede ser un punto de montaje o un grupo de discos ASM. Si hay suficiente espacio en la ubicación montada, puede reutilizar una de las ubicaciones montadas en lugar de un punto de montaje dedicado.

Debe especificar la fecha y hora o SCN para ejecutar PITR de la PDB. RMAN puede recuperar PDB de LECTURA, SOLO LECTURA o PDB borrada, incluidos archivos de datos.

Solo puede restaurar y recuperar:

- Una PDB a la vez
- Un tablespace en una PDB
- Varios espacios de tablas de la misma PDB

En una configuración de RAC, puede realizar PITR de tablespaces desde cualquier nodo del RAC.

- 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** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos del tipo de instancia única (Multitenant) ya sea en la vista de detalles de la base de datos o en la vista de detalles del grupo de recursos.

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

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principal o secundario (reflejado o replicado).

Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione el backup catalogado y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
   a. Si seleccionó un backup de una base de datos en un entorno RAC, seleccione el nodo de RAC.
   b. Según si desea restaurar la PDB o los espacios de tablas en una PDB, realice una de las acciones:

Si desea…	Pasos…
Restaurar una PDB	i. Seleccione **bases de datos conectables (PDB)**. ii. Especifique la PDB que desea restaurar. No se puede ejecutar PITR en la base de datos PDB$SEED.
Restaurar espacios de tablas en una PDB	i. Seleccione **tablespaces de base de datos conectables (PDB)**. ii. Especifique la PDB. iii. Especifique un único espacio de tabla o varios espacios de tablas que desee restaurar. No puede realizar PITR en tablespaces SYSAUX, SYSTEM y UNDO.

   c. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.
7. En la página Recovery Scope, realice una de las siguientes acciones:
   - Si desea recuperar un número de cambio de sistema (SCN) específico, seleccione **hasta SCN** y especifique el SCN y el destino auxiliar.
   - Si desea recuperar una fecha y hora específicas, seleccione **Fecha y hora** y especifique la fecha y hora y el destino auxiliar.

     SnapCenter identifica y, a continuación, monta y cataloga la cantidad óptima de backups de datos y registros necesarios para realizar PITR según el SCN especificado o la fecha y hora seleccionadas.
8. En la página PreOps, introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de restauración.

Debe almacenar los scripts previos en la ruta de acceso /var/opt/snapcenter/spl/scripts o en cualquier carpeta dentro de ella. 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 usar las variables de entorno predefinidas al ejecutar el script previo y script posterior. "Leer más"

1. En la página PostOps, siga estos pasos:
   a. Introduzca la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de restauración.

      Si se produce un error en la operación de restauración, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

   b. Seleccione la casilla de comprobación si desea abrir la base de datos después de la recuperación.

      En una configuración de RAC, la PDB solo se abre en el nodo donde se recuperó la base de datos. Debe abrir manualmente la PDB recuperada en todos los demás nodos de la configuración de RAC.
2. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.
3. Revise el resumen y, a continuación, haga clic en **Finalizar**.
4. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Restaure y recupere bases de datos de Oracle con comandos de UNIX

El flujo de trabajo de restauración y recuperación incluye la planificación, la realización de operaciones de restauración y recuperación, y la supervisión de las operaciones.

Acerca de esta tarea

Debe ejecutar los siguientes comandos para establecer la conexión con SnapCenter Server, enumerar los backups y recuperar su información, y restaurar el backup.

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. Recupere la información sobre los backups que desea restaurar: *Get-SmBackup*
  3. Recupere la información detallada acerca del backup especificado: *Get-SmBackupDetails*

     Este comando recupera la información detallada sobre el backup de un recurso especificado con un determinado ID de backup. La información incluye nombre de la base de datos, versión, inicio, SCN de

inicio y de finalización, espacios de tabla, bases de datos conectables y sus espacios de tabla.

4. Restaure los datos del backup: *Restore-SmBackup*

Supervisar las operaciones de restauración de bases de datos de Oracle

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

Acerca de esta tarea

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- 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 figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

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

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

Cancelar operaciones de restauración de bases de datos de Oracle

Es posible cancelar los trabajos de restauración que se encuentran en cola.

Inició sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.

Acerca de esta tarea

- Puede cancelar una operación de restauración en cola desde la página **Monitor** o desde el panel **actividad**.
- No se puede cancelar una operación de restauración en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está desactivado para operaciones de restauración 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 restauración 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 el trabajo y haga clic en **Cancelar trabajo**.
Panel de actividades	1. Después de iniciar la operación de restauración, 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**.

Clone la base de datos de Oracle

Flujo de trabajo de clonado

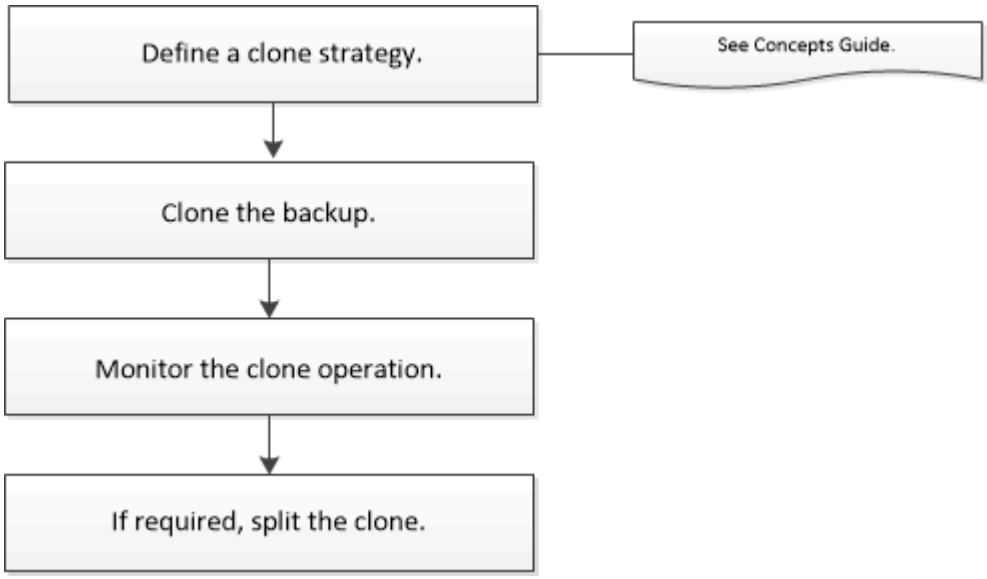
El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

Pueden clonarse bases de datos por los siguientes motivos:

- Para poner a prueba una funcionalidad que debe implementarse con la estructura y el contenido de la base de datos actual durante ciclos de desarrollo de aplicaciones.

- Para completar almacenes de datos con herramientas de extracción y manipulación de datos.
- Para recuperar datos que se eliminaron o se modificaron por error.

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



Defina una estrategia de clonado para bases de datos de Oracle

Definir una estrategia antes de clonar una base de datos permite garantizar que la operación se ejecute correctamente.

Tipos de backups compatibles con la clonado

SnapCenter permite clonar diversos tipos de backup de las bases de datos de Oracle.

- Backups de datos en línea
- Backup completo en línea
- Backups de montaje sin conexión
- Backups de apagado sin conexión
- Backups de bases de datos en espera de Data Guard y bases de datos en espera de Active Data Guard
- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración RAC
- Backups de datos en línea, backups completos en línea, backups de montaje sin conexión y backups de apagado sin conexión en una configuración ASM

> Las configuraciones DE SAN no son compatibles si la opción USER_Friendly_Names del archivo de configuración multivía está establecida en yes.

> No se admite la clonado de backups de registros de archivos.

Tipos de clonado compatibles con las bases de datos de Oracle

En un entorno de bases de datos de Oracle, SnapCenter admite la clonado de un backup de base de datos. Puede clonar el backup de sistemas de almacenamiento primarios y secundarios.

El servidor SnapCenter utiliza la tecnología FlexClone de NetApp para clonar backups.

Puede actualizar un clon ejecutando el comando "Refresh-SmClone". Este comando crea un backup de la base de datos, elimina el clon existente y crea un clon con el mismo nombre.

La operación de actualización de clones solo puede realizarse con los comandos UNIX.

Convenciones de nomenclatura de los clones para las bases de datos de Oracle

A partir de SnapCenter 3.0, la convención de nomenclatura utilizada para los clones de sistemas de archivos es diferente de la aplicada a los clones de grupos de discos de ASM.

- La convención de nomenclatura para los sistemas de archivos SAN o NFS es FileSystemNameofsourcedatabase_CLONESID.
- La convención de nomenclatura para los grupos de discos de ASM es SC_HASHCODEofDISKGROUP_CLONESID.

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

Limitaciones de la clonado de bases de datos de Oracle

Antes de clonar las bases de datos, es necesario tener en cuenta las limitaciones de las operaciones de clonado.

- Si utiliza una versión de Oracle de 11.2.0.4 a 12.1.0.1, la operación de clonado estará en estado colgado al ejecutar el comando *renamedg* . Puede aplicar el parche de Oracle 19544733 para solucionar este problema.
- No se admite la clonado de bases de datos de un LUN conectado directamente a un host (por ejemplo, usando el iniciador de iSCSI de Microsoft en un host de Windows) a un VMDK o un LUN de RDM en el mismo host de Windows, ni en otro host de Windows, o viceversa.
- El directorio raíz del punto de montaje del volumen no puede ser un directorio compartido.
- Si se mueve un LUN que contiene un clon de un volumen nuevo, no es posible eliminar el clon.

Variables de entorno predefinidas para el script previo y script posterior específicos de clon

SnapCenter permite usar las variables de entorno predefinidas al ejecutar el script previo y el script posterior mientras se clona una base de datos.

Variables de entorno predefinidas admitidas para clonar una base de datos

- **SC_ORIGINAL_SID** especifica el SID de la base de datos de origen.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: NFSB32

- **SC_ORIGINAL_HOST** especifica el nombre del host de origen.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** especifica la ruta de acceso del directorio raíz de Oracle de la base de datos de destino.

  Ejemplo: /Ora01/app/oracle/product/18.1.0/dB_1

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

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplos:

  - Si la base de datos no se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Si la base de datos se está ejecutando en modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG:RG2_sscspr2417819002_07-20-2021_12.16.48.9267_1,RG2_sspr2417819002_07-21-2021_12.16.48.9267_1,RG2_sspr2417819002_07-22-2021_12.16.48.9267_1

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

  Ejemplo: AV1|AV2

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

  Ejemplo: oracle

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

  Ejemplo: Oinstall

- **SC_TARGET_SID**" especifica el SID de la base de datos clonada.

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: Clonedb

- **SC_TARGET_HOST** especifica el nombre del host donde se clonará la base de datos.

  Este parámetro se rellenará para los volúmenes de aplicaciones.

  Ejemplo: asmrac1.gdl.englab.netapp.com

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

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Ejemplo: oracle

- **SC_TARGET_OS_GROUP** especifica el grupo del sistema operativo de la base de datos clonada.

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Ejemplo: Oinstall

- **SC_TARGET_DB_PORT** especifica el puerto de base de datos de la base de datos clonada.

  Para el flujo de trabajo de clonado de PDB, el valor de este parámetro no estará predefinido.

  Ejemplo: 1521

Para obtener más información acerca de los delimitadores, consulte "Delimitadores compatibles".

Requisitos para clonar una base de datos de Oracle

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

- Creó un backup de la base de datos con SnapCenter.

  Debe haber creado correctamente backups del registro y de datos en línea, o backups sin conexión (montados o apagados) para que la operación de clonado se complete correctamente.

- Si desea personalizar las rutas de acceso del archivo de control o el archivo de registro de recuperación, debe haber aprovisionado previamente el sistema de archivos requerido o el grupo de discos de Automatic Storage Management (ASM).

  De forma predeterminada, los archivos de registro de recuperación y de control de la base de datos clonada se crean en el grupo de discos de ASM o el sistema de archivos aprovisionado por SnapCenter para los archivos de datos de la base de datos del clon.

- Si está usando ASM sobre NFS, debe agregar */var/opt/snapcenter/scu/clones///** a la ruta de acceso existente definida en el parámetro asm_diskstring.
- En el parámetro asm_diskstring, debe configurar *AFD:** si está utilizando ASMFD o configurar *ORCL:** si está utilizando ASMLIB.

  Para obtener información sobre cómo editar el parámetro asm_diskstring, consulte "Cómo agregar las rutas de acceso al disco a asm_diskstring".

- Si crea el clon en un host alternativo, este host debe cumplir los siguientes requisitos:
  - El plugin de SnapCenter para base de datos de Oracle debe estar instalado en el host alternativo.
  - El host del clon debe poder detectar LUN de almacenamiento principal o secundario.
    - Si clona un almacenamiento principal o secundario (almacén o reflejo) en un host alternativo, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento secundario y el host alternativo, o una zona adecuada para Fibre Channel (FC).
    - Si clona un almacén o un reflejo en el mismo host, asegúrese de que se establezca una sesión iSCSI entre el almacén o reflejo y el host, o una zona adecuada para FC.
    - Si clona en un entorno virtualizado, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento principal o secundario y el servidor ESX que aloja al host alternativo, o una zona adecuada para FC.

Para obtener más información, consulte "documentación de utilidades de host".

- Si la base de datos de origen es una base de datos ASM:
  - La instancia de ASM debe estar activa y en ejecución en el host donde se realizará el clon.
  - El grupo de discos ASM debe aprovisionarse antes de la operación de clonado si desea colocar archivos de registro de archivos de la base de datos clonada en un grupo de discos de ASM dedicado.
  - Que el nombre del grupo de discos de datos pueda configurarse y, a la vez, que ningún otro grupo de discos ASM use el nombre en el host donde se realizará la clonado.

    Los archivos de datos que residen en el grupo de discos ASM se aprovisionan como parte del flujo de trabajo del clon de SnapCenter.
- En NVMe, se debe instalar NVMe util

- El tipo de protección del LUN de datos y el LUN de registro, como reflejo, almacén o reflejo-almacén, debe ser el mismo para detectar localizadores secundarios durante la clonado en un host alternativo que use backups de registros.
- Configuró el valor de exclude_seed_cdb_view como FALSE en el archivo de parámetros de la base de datos de origen con el fin de recuperar información relacionada con la PDB de inicialización para la clonado de una base de datos de 12_c_.

  La PDB de inicialización es una plantilla proporcionada por el sistema que la CDB puede utilizar para crear PDB. La PDB de inicialización se denomina PDB$SEED. Para obtener información sobre PDB$SEED, consulte el ID de documento de Oracle 1940806.1.

  Debe configurar el valor antes de realizar el backup de la base de datos 12_c_.

- SnapCenter admite copia de seguridad de sistemas de archivos administrados por el subsistema autofs. Si va a clonar la base de datos, asegúrese de que los puntos de montaje de datos no están bajo la raíz del punto de montaje de autofs porque el usuario raíz del host del plugin no tiene permiso para crear directorios bajo la raíz del punto de montaje de autofs.

  Si los archivos de control y de registro de recuperación se encuentran en el punto de montaje de datos, debe modificar la ruta de acceso del archivo de control y, a continuación, la ruta de acceso del archivo de registro de recuperación según corresponda.

  Puede registrar manualmente los nuevos puntos de montaje clonados con el subsistema autofs. Los puntos de montaje nuevos no se registrarán automáticamente.

- Si tiene un TDE (inicio de sesión automático) y desea clonar la base de datos en el mismo host o en otro alternativo, debe copiar la cartera (archivos de clave) en */etc/ORACLE/WALLET/$ORACLE_SID* desde la base de datos de origen a la base de datos clonada.
- Debe configurar el valor de use_lvmetad = 0 en */etc/lvm/lvm.conf* y detener el servicio lvm2-lvmetad para realizar correctamente la clonado en entornos de red de área de almacenamiento (SAN) en Oracle Linux 7 o posteriores, o Red Hat Enterprise Linux (RHEL) 7 o posteriores.
- Debe instalar el parche de Oracle 13366202 si utiliza la base de datos Oracle 11.2.0.3 o posterior y el identificador de la base de datos para la instancia auxiliar se cambia con un script NID.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- Para NVMe, si debe excluir un puerto de destino de la conexión, debe añadir el nombre del nodo de

destino y el nombre del puerto en el archivo /var/opt/snapcenter/scu/etc/nvme.conf.

Si el archivo no existe, debe crearlo como se muestra en el siguiente ejemplo:

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup compuesto por protocolos mixtos iSCSI y FC. Para obtener más información, consulte "Error en la operación porque no puede detectar el dispositivo para la LUN".

Clonar el backup de una base de datos de Oracle

Es posible utilizar SnapCenter para clonar una base de datos de Oracle con el backup de esa base de datos.

Acerca de esta tarea

La operación de clonado crea una copia de los archivos de datos de la base de datos y, luego, crea nuevos archivos de registro de recuperación en línea y archivos de control. La base de datos puede recuperarse opcionalmente a una hora específica, según las opciones de recuperación especificadas.

Se produce un error en la clonado si intenta clonar un backup que se creó en un host Linux en un host AIX o viceversa.

SnapCenter crea una base de datos independiente cuando se clona desde un backup de base de datos de Oracle RAC. SnapCenter admite la creación de un clon desde el backup de bases de datos Data Guard en espera y Active Data Guard en espera.

Durante la clonado, SnapCenter monta la cantidad óptima de backups de registros basados en SCN o dat y el tiempo para las operaciones de recuperación. Después de la recuperación, el backup de registros se desasocia. Todos estos clones están montados en */var/opt/snapcenter/scu/Clones/*. Si está usando ASM sobre NFS, debe agregar */var/opt/snapcenter/scu/clones///** a la ruta de acceso existente definida en el parámetro asm_diskstring.

Mientras se clona un backup de una base de datos ASM en un entorno SAN, se crean reglas udev para el host clonado en */etc/udev/rules.d/999-scu-netapp.rules*. Estas reglas udev asociadas con los dispositivos host clonados se eliminan cuando se elimina el clon.

En una configuración de Flex ASM, no puede realizar la operación de clonado en nodos Leaf si la cardinalidad es menor que el número de nodos del clúster RAC.

- 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** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos en la vista de detalles de la base de datos o en la vista de detalles del

grupo de recursos.

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

4. En la vista Manage Copies, seleccione los backups desde local copies (primary), Mirror copies (secondary) o Vault copies (secondary).
5. Seleccione el backup de datos en la tabla y haga clic en .
6. En la página Name, realice una de las siguientes acciones:

Si desea…	Pasos…
Clonar una base de datos (CDB o no CDB)	a. Especifique el SID del clon. El SID del clon no está disponible de manera predeterminada, y la longitud máxima del SID es de 8 caracteres. Debe asegurarse de que no exista otra base de datos con el mismo SID en el host donde se creará el clon.
Clonar una base de datos conectables (PDB)	a. Seleccione **PDB Clone**. b. Especifique la PDB que desea clonar. c. Especifique el nombre de la PDB clonada. Para ver los pasos detallados para clonar una PDB, consulte "Clonar una base de datos conectable".

Al seleccionar un datos reflejados o de almacén:

- si no hay backup de registros en el reflejo o el almacén, no se selecciona nada y los localizadores están vacíos.
- si existen backups de registros en el reflejo o almacén, se selecciona el último backup de registros y se muestra el localizador correspondiente.

Si el backup de registro seleccionado existe en la ubicación de reflejo y almacén, se muestran ambos localizadores.

7. En la página Locations, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el host	De forma predeterminada, se completa el host de la base de datos de origen. Si desea crear el clon en un host alternativo, seleccione el host que tiene la misma versión de Oracle y del sistema operativo que el host de la base de datos de origen.
Ubicaciones de los almacenes de datos	De forma predeterminada, se completa la ubicación del archivo de datos. La convención de nomenclatura predeterminada de SnapCenter para sistemas de archivos SAN o NFS es FileSystemNameofsourcedatabase_CLONESID. La convención de nomenclatura predeterminada de SnapCenter para grupos de discos ASM es SC_HASHCODEofDISKGROUP_CLONESID. El HASHCODEofDISKGROUP es un número generado automáticamente (entre 2 y 10 dígitos) que es único para cada grupo de discos ASM. Si personaliza el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre respete el límite admitido por Oracle. Si desea especificar otra ruta de acceso, debe introducir los puntos de montaje del archivo de datos o los nombres de los grupos de discos ASM para la base de datos del clon. Cuando personaliza la ruta de acceso del archivo de datos, también debe cambiar los nombres de los grupos de discos ASM del archivo de control y el archivo de registro de recuperación para que tengan el mismo nombre utilizado en los archivos de datos o cambiar el sistema de archivos a un grupo de discos ASM o sistema de archivos existente.

Para este campo…	Realice lo siguiente…
Archivos de control	De forma predeterminada, se completa la ruta de acceso al archivo de control. Los archivos de control se ubican en el mismo grupo de discos ASM o sistema de archivos que los archivos de datos. Si desea anular la ruta de acceso del archivo de control, puede proporcionar otra ruta de acceso al archivo de control. El sistema de archivos o el grupo de discos ASM deben existir en el host. De forma predeterminada, la cantidad de archivos de control será la misma que la de la base de datos de origen. Es posible modificar la cantidad de archivos de control, pero se requiere un mínimo de un archivo de control para clonar la base de datos. Puede personalizar la ruta de acceso del archivo de control a otro sistema de archivos (existente) distinto del de la base de datos de origen.

Para este campo…	Realice lo siguiente…
Rehacer registros	De forma predeterminada, se completan el grupo de archivos, la ruta de acceso y el tamaño de los archivos de registro de recuperación. Los registros de recuperación se ubican en el mismo grupo de discos ASM o sistema de archivos que los archivos de datos de la base de datos clonada. Si desea anular la ruta de acceso del archivo de registro de recuperación, puede personalizarla en otro sistema de archivos que no sea el de la base de datos de origen. El nuevo sistema de archivos o el grupo de discos ASM deben existir en el host. De forma predeterminada, la cantidad de grupos de registros de recuperación, los archivos de registro de recuperación y sus tamaños serán los mismos que los de la base de datos de origen. Puede modificar los siguientes parámetros: • Cantidad de grupos de registros de recuperación Se requiere un mínimo de dos grupos de registros de recuperación para clonar la base de datos. • Los archivos de registro de recuperación en cada grupo y su ruta de acceso Puede personalizar la ruta de acceso del archivo de registro de recuperación a otro sistema de archivos (existente) distinto del de la base de datos de origen. Se requiere un mínimo de un archivo de registro de recuperación en el grupo de registros de recuperación para clonar la base de datos. • Tamaños del archivo del registro de recuperación

8. En la página Credentials, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre de credencial del usuario sys	Seleccione la credencial que se usará para definir la contraseña de usuario sys de la base de datos clonada. Si SQLNET.AUTHENTICATION_SERVICES está configurado como NONE en el archivo sqlnet.ora del host de destino, no debe seleccionar **Ninguno** como la credencial en la interfaz gráfica de usuario de SnapCenter.
Nombre de credencial de la instancia de ASM	Seleccione **Ninguno** si está activada la autenticación del SO para conectarse a la instancia de ASM en el host del clon. De lo contrario, seleccione la credencial de Oracle ASM configurada con el usuario "stys" o un usuario con el privilegio "sasma" aplicable al host del clon.

El inicio, el nombre de usuario y los detalles de grupo de Oracle se completan automáticamente desde la base de datos de origen. Es posible cambiar los valores según el entorno de Oracle del host donde se creará el clon.

9. En la página PreOps, siga estos pasos:

   a. Introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de clonado.

      Debe almacenar el script previo 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 colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script.

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

   b. En la sección Database Parameter settings, modifique los valores de los parámetros de la base de datos completados automáticamente que se utilizan para inicializar la base de datos.

      Puede agregar parámetros adicionales haciendo clic en + .

      Si está utilizando Oracle Standard Edition y la base de datos se está ejecutando en el modo de registro de archivo o desea restaurar una base de datos del redo log de archivo, agregue los parámetros y especifique la ruta de acceso.

      - ARCHIVO_DE_REGISTRO_DEST
      - LOG_ARCHIVE_DUPLEX_DEST

El área de recuperación rápida (FRA) no se define en los parámetros de la base de datos completados automáticamente. Para configurar la FRA, añada los parámetros relacionados.

El valor predeterminado de log_archive_dest_1 es $ORACLE_HOME/clone_sid, y los registros de archivos de la base de datos clonada se crearán en esta ubicación. Si eliminó el parámetro log_archive_dest_1, Oracle determina la ubicación del registro de archivos. Para definir una nueva ubicación para el registro de archivos, debe editar log_archive_dest_1, pero asegúrese de que el sistema de archivos o el grupo de discos existan y estén disponible en el host.

a. Haga clic en **Restablecer** para obtener la configuración predeterminada de los parámetros de la base de datos.

10. En la página PostOps, **Recover database** y **Until Cancel** se seleccionan de forma predeterminada para realizar la recuperación de la base de datos clonada.

    SnapCenter realiza la recuperación mediante el montaje del backup de registro más reciente que posee la secuencia ininterrumpida de archivos de registro después del backup de datos que se seleccionó para la clonado. El registro y el backup de datos deben estar en el almacenamiento principal para realizar la clonado en el almacenamiento principal y en el almacenamiento secundario para realizar la clonado en el almacenamiento secundario.

    Las opciones **recuperar base de datos** y **hasta Cancelar** no se seleccionan si SnapCenter no encuentra las copias de seguridad de registro adecuadas. Puede proporcionar la ubicación del archivo de registro externo si la copia de seguridad del registro no está disponible en **especificar ubicaciones de archivo de registro externo**. Se pueden especificar varias ubicaciones del registro.

    Si desea clonar una base de datos de origen configurada para admitir FRA y Oracle Managed Files (OMF), el destino del registro para la recuperación también debe respetar la estructura de directorios de OMF.

    La página PostOps no se muestra si la base de datos de origen es una base de datos Data Guard en espera o Active Data Guard en espera. Para bases de datos Data Guard en espera o Active Data Guard en espera, SnapCenter no ofrece la opción de seleccionar el tipo de recuperación en la interfaz gráfica de usuario de SnapCenter, pero la base de datos se recupera con el tipo de recuperación Until Cancel sin aplicar ningún registro.

Nombre del campo	Descripción
Hasta Cancelar	SnapCenter realiza la recuperación mediante el montaje del backup de registro más reciente con la secuencia ininterrumpida de archivos de registro después de ese backup de datos que se seleccionó para la clonado. La base de datos clonada se recupera hasta el archivo de registro faltante o dañado.

Nombre del campo	Descripción
Fecha y hora	SnapCenter recupera la base de datos hasta la fecha y la hora especificadas. El formato aceptado es mm/dd/yyyy hh:mm:ss La hora puede especificarse en formato de 24 horas.
Until SCN (número de cambio de sistema)	SnapCenter recupera la base de datos hasta un SCN especificado.
Especifique las ubicaciones de los registros de archivos externos	Si la base de datos se ejecuta en modo ARCHIVELOG, SnapCenter identifica y monta el número óptimo de backups de registros según el SCN especificado o la fecha y hora seleccionadas. También es posible especificar la ubicación del registro de archivos externo. SnapCenter no identifica ni monta automáticamente los backups de registros si seleccionó hasta Cancel.
Crear nuevo DBID	De forma predeterminada **la casilla de verificación Crear nuevo DBID** está activada para generar un número único (DBID) para la base de datos clonada que lo diferencia de la base de datos de origen. Desactive la casilla de comprobación si desea asignar el DBID de la base de datos de origen a la base de datos clonada. En esta situación, si desea registrar la base de datos clonada en el catálogo de RMAN externo donde la base de datos de origen ya está registrada, se produce un error en la operación.
Crear archivo temporal para tablespace temporal	Seleccione la casilla de comprobación si desea crear un archivo tempfile para el espacio de tabla temporal predeterminado de la base de datos clonada. Si no está seleccionada la casilla de comprobación, se creará el clon de la base de datos sin el archivo tempfile.

Nombre del campo	Descripción
Introduzca las entradas de sql que se van a aplicar al crear el clon	Agregue las entradas sql que desee aplicar al crear el clon.
Introduzca los scripts que se ejecutarán después de la operación de clonado	Especifique la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de clonado. Debe almacenar el script posterior 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 colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script. Si se produce un error en la operación de clonado, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

11. 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 de clonado realizada, 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**.

    Al realizar una recuperación como parte de la operación de creación de un clon, incluso si se producen errores en la recuperación, el clon se crea con una advertencia. Es posible realizar una recuperación manual de este clon para que la base de datos del clon pase a un estado consistente.

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

resultado

Después de clonar la base de datos, es posible actualizar la página de recursos para que enumere la base de datos clonada como uno de los recursos disponibles para realizar backups. La base de datos clonada puede protegerse como cualquier otra base de datos con el flujo de trabajo de backup estándar, o bien puede incluirse en un grupo de recursos (recientemente creado o existente). La base de datos clonada puede volver

a clonarse (clon de clones).

Después de clonar, no debe cambiar nunca el nombre de la base de datos clonada.

> Si no realizó la recuperación durante la clonado, se pueden producir errores en el backup de la base de datos clonada debido a una recuperación incorrecta, y es posible que deba realizar una recuperación manual. También se pueden producir errores en el backup de registro si la ubicación predeterminada que se completó para los registros de archivos es un almacenamiento de terceros o si el sistema de almacenamiento no está configurado con SnapCenter.

En la instalación de AIX, puede utilizar el mandato lkdev para bloquear y el mandato rendev para cambiar el nombre de los discos en los que residió la base de datos clonada.

El bloqueo o cambio de nombre de dispositivos no afectará a la operación de eliminación de clones. En el caso de diseños LVM de AIX construidos en dispositivos SAN, el cambio de nombre de dispositivos no será compatible con los dispositivos SAN clonados.

Más información

- "La restauración o el clonado producen errores con el mensaje de error ORA-00308"
- "Error al recuperar una base de datos clonada"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

Clonar una base de datos conectable

Es posible clonar una base de datos conectables (PDB) en una base de datos diferente o la misma CDB objetivo en el mismo host o alternativo. También es posible recuperar la PDB clonada en un SCN o la fecha y la hora que desee.

- 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** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos del tipo de instancia única (Multitenant) desde la vista de detalles de la base de datos o desde la vista de detalles del grupo de recursos.

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

4. En la vista Manage Copies, seleccione los backups desde local copies (primary), Mirror copies (secondary) o Vault copies (secondary).
5. Seleccione el backup en la tabla y haga clic en .
6. En la página Name, realice los siguientes pasos:
   a. Seleccione **PDB Clone**.
   b. Especifique la PDB que desea clonar.

      Solo es posible clonar una PDB a la vez.

c. Especifique el nombre de la PDB del clon.

7. En la página Locations, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el host	De forma predeterminada, se completa el host de la base de datos de origen. Si desea crear el clon en un host alternativo, seleccione el host que tiene la misma versión de Oracle y del sistema operativo que el host de la base de datos de origen.
CDB de destino	Seleccione la CDB en el que desea incluir la PDB clonada. Debe asegurarse de que la CDB de destino esté en ejecución.
Estado de la base de datos	Active la casilla de verificación **Abrir la PDB clonada en modo DE LECTURA y ESCRITURA** si desea abrir la PDB en modo DE LECTURA Y ESCRITURA.
Ubicaciones de los almacenes de datos	De forma predeterminada, se completa la ubicación del archivo de datos. La convención de nomenclatura predeterminada de SnapCenter para sistemas DE archivos SAN o NFS es FileSystemNameofsourcedatabase_SCJOBID. La convención de nomenclatura predeterminada de SnapCenter para grupos de discos ASM es SC_HASHCODEofDISKGROUP_SCJOBID. El HASHCODEofDISKGROUP es un número generado automáticamente (entre 2 y 10 dígitos) que es único para cada grupo de discos ASM. Si personaliza el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre respete el límite admitido por Oracle. Si desea especificar otra ruta de acceso, debe introducir los puntos de montaje del archivo de datos o los nombres de los grupos de discos ASM para la base de datos del clon.

El inicio, el nombre de usuario y los detalles de grupo de Oracle se completan automáticamente desde la base de datos de origen. Es posible cambiar los valores según el entorno de Oracle del host donde se creará el clon.

8. En la página PreOps, siga estos pasos:

   a. Introduzca la ruta de acceso y los argumentos del script previo que desea ejecutar antes de la operación de clonado.

      Debe almacenar el script previo 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 colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script.

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

   a. En la sección Configuración de parámetros de la base de datos del clon auxiliar de la CDB, modifique los valores de los parámetros de la base de datos completados automáticamente que se utilizan para inicializar la base de datos.

9. Haga clic en **Restablecer** para obtener la configuración predeterminada de los parámetros de la base de datos.
10. En la página PostOps, **hasta que se selecciona Cancelar** de forma predeterminada para realizar la recuperación de la base de datos clonada.

    La opción **Until Cancel** no está seleccionada si SnapCenter no encuentra las copias de seguridad de registro adecuadas. Puede proporcionar la ubicación del archivo de registro externo si la copia de seguridad del registro no está disponible en **especificar ubicaciones de archivo de registro externo**. Se pueden especificar varias ubicaciones del registro.

    Si desea clonar una base de datos de origen configurada para admitir FRA y Oracle Managed Files (OMF), el destino del registro para la recuperación también debe respetar la estructura de directorios de OMF.

Nombre del campo	Descripción
Hasta Cancelar	SnapCenter realiza la recuperación mediante el montaje del backup de registro más reciente con la secuencia ininterrumpida de archivos de registro después de ese backup de datos que se seleccionó para la clonado. El registro y el backup de datos deben estar en el almacenamiento principal para realizar la clonado en el almacenamiento principal y en el almacenamiento secundario para realizar la clonado en el almacenamiento secundario. La base de datos clonada se recupera hasta el archivo de registro faltante o dañado.

Nombre del campo	Descripción
Fecha y hora	SnapCenter recupera la base de datos hasta la fecha y la hora especificadas. La hora puede especificarse en formato de 24 horas.
Until SCN (número de cambio de sistema)	SnapCenter recupera la base de datos hasta un SCN especificado.
Especifique las ubicaciones de los registros de archivos externos	Especifique la ubicación del registro de archivos externo.
Crear nuevo DBID	De forma predeterminada **la casilla de verificación Crear nuevo DBID** no está seleccionada para la base de datos auxiliar de clones. Marque la casilla de comprobación si desea generar un número único (DBID) para la base de datos clonada auxiliar que la diferencia entre la base de datos de origen.
Crear archivo temporal para tablespace temporal	Seleccione la casilla de comprobación si desea crear un archivo tempfile para el espacio de tabla temporal predeterminado de la base de datos clonada. Si no está seleccionada la casilla de comprobación, se creará el clon de la base de datos sin el archivo tempfile.
Introduzca las entradas de sql que se van a aplicar al crear el clon	Agregue las entradas sql que desee aplicar al crear el clon.

Nombre del campo	Descripción
Introduzca los scripts que se ejecutarán después de la operación de clonado	Especifique la ruta de acceso y los argumentos del script posterior que desea ejecutar después de la operación de clonado. Debe almacenar el script posterior 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 colocó el script en cualquier carpeta dentro de esta ruta de acceso, debe proporcionar la ruta de acceso completa hasta la carpeta donde está ubicado el script. Si se produce un error en la operación de clonado, los scripts posteriores no se ejecutarán y las actividades de limpieza se desencadenarán directamente.

11. 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 de clonado realizada, 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**.
2. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Después de terminar

Si desea crear un backup de la PDB clonada, debe realizar un backup de la CDB de destino donde se clona la PDB porque no es posible realizar un backup de la PDB clonada. Debe crear una relación secundaria para la base de datos de destino para si desea crear el backup con la relación secundaria.

En una configuración de RAC, el almacenamiento para la PDB clonada solo se asocia al nodo donde se ejecutó el clon de la PDB. Las PDB de los otros nodos del RAC se encuentran en estado DE MONTAJE. Si desea que la PDB clonada sea accesible desde los otros nodos, debe asociar manualmente el almacenamiento a los otros nodos.

Más información

- "La restauración o el clonado producen errores con el mensaje de error ORA-00308"
- "Parámetros personalizables para operaciones de backup, restauración y clonado en sistemas AIX"

Clonar backups de bases de datos de Oracle con comandos UNIX

El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

Acerca de esta tarea

Debe ejecutar los siguientes comandos para crear el archivo de especificación del clon de la base de datos de Oracle e iniciar la operación de clonado.

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. Cree una especificación de clon de base de datos de Oracle a partir de una copia de seguridad especificada: *New-SmOracleCloneSpecification*

   Si la política de protección de datos secundaria es mirror-vault unificado, especifique solo -IncludeSecondaryDetails. No es necesario especificar -SecondaryStorageType.

   Este comando crea automáticamente un archivo de especificación de clon de base de datos de Oracle para la base de datos de origen especificada y su backup. Además debe proporcionar un SID de base de datos del clon para que el archivo de especificación creado tenga los valores generados automáticamente para la base de datos del clon que creará.

   El archivo de especificación del clon se crea en */var/opt/snapcenter/sco/clone_specs*.

2. Inicie una operación de clonado desde un grupo de recursos de clon o un backup existente: *New-SmClone*

   Este comando inicia una operación de clonado. También debe proporcionar una ruta de acceso al archivo de especificación del clon de Oracle para la operación de clonado. Además, puede especificar las opciones de recuperación, el host donde se realizará la operación de clonado, scripts previos, scripts posteriores y otros detalles.

De forma predeterminada, el archivo de destino del registro de archivos para la base de datos del clon se completa automáticamente en *$ORACLE_HOME/CLONE_SIDS*.

Divida el clon de una base de datos de Oracle

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

Acerca de esta tarea

- No se puede ejecutar la operación de división de clones en un clon intermedio.

  Por ejemplo, después de crear el clon 1 a partir de un backup de la base de datos, puede realizar un backup del clon 1 y luego clonar este backup (que sería el clon 2). Una vez creado el clon 2, el clon 1 se convierte en un clon intermedio y la operación de división de clones puede hacerse con el clon 1. No obstante, esta operación también puede ejecutarse con el clon 2.

Después de dividir el clon 2, puede ejecutar la operación de división de clones con el clon 1, ya que este deja de ser el clon intermedio.

- Cuando divide un clon, se eliminan las copias del backup del clon.
- Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
- Asegúrese de que el volumen o el agregado del sistema de almacenamiento estén en línea.
- 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. Seleccione el recurso clonado (por ejemplo, la base de datos o el LUN) y haga clic en .
4. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

   La operación de división de clones se detiene si se reinicia el servicio SMCore y las bases de datos en las que se ejecutó la operación de división de clones aparecen como clones en la página Resources. Debe ejecutar el cmdlet *Stop-SmJob* para detener la operación de división de clones y luego volver a intentar la operación de división de clones.

   Si necesita más o menos tiempo de sondeo para comprobar si el clon está dividido o no, puede cambiar el valor del parámetro CloneSplitStatusCheckPollTime en el archivo SMCoreServiceHost.exe.config. De este modo, se establece un intervalo para que SMCore sondee el estado de la operación de división de clones. El valor se registra en milisegundos; el predeterminado son 5 minutos.

   Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

Se produce un error en la operación de inicio de división de clones si hay un backup, una restauración o una división de clones en curso. Solo debe reiniciar la operación de división de clones una vez que hayan finalizado las operaciones en ejecución.

Clon dividido de una base de datos conectable

Es posible utilizar SnapCenter para dividir una base de datos conectables (PDB) clonada.

Acerca de esta tarea

Si creó un backup de la CDB de destino donde se clona la PDB, al dividir la PDB, la PDB clonada también se quita de todos los backups de la CDB de destino que contiene la PDB clonada.

Los clones de las PDB no se muestran en la vista de inventario o recursos.

- 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. Seleccione la base de datos del contenedor de origen (CDB) en la vista del recurso o grupo de recursos.
  3. En la vista Manage Copies (Administrar copias), seleccione **Clones** ya sea en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
  4. Seleccione el clon de PDB (targetCDB:PDBClone) y, a continuación, haga clic en .
  5. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
  6. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Supervise las operaciones de clonado de las bases de datos de Oracle

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- 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 figuren las operaciones de clonado.
     b. Especifique las fechas de inicio y finalización.
     c. En la lista desplegable **Tipo**, seleccione **Clonar**.
     d. En la lista desplegable **Estado**, seleccione el estado del clon.
     e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
  4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Actualizar un clon

Para actualizar el clon, puede ejecutar el comando *Refresh-SmClone*. Este comando crea un backup de la base de datos, elimina el clon existente y crea un clon con el mismo nombre.

No se puede actualizar un clon de una PDB.

Lo que necesitará

- Cree un backup completo en línea o una política de backup de datos sin conexión sin conexión sin backups programados habilitados.
- Configure la notificación por correo electrónico en la directiva sólo para los fallos de copia de seguridad.
- Defina el número de retención de los backups bajo demanda correctamente para garantizar que no haya backups no deseados.
- Asegúrese de que solo exista asociada una política de backup completo en línea o de backup de datos sin conexión a un grupo de recursos identificado para la operación de actualización de clonado.
- Cree un grupo de recursos con solo una base de datos.
- Si se crea un trabajo de cron para el comando clone Refresh, asegúrese de que las programaciones de SnapCenter y de cron no se superpongan para el grupo de recursos de la base de datos.

  Para un trabajo de cron creado para el comando clone Refresh, asegúrese de ejecutar Open-SmConnection cada 24 horas.

- Asegúrese de que el SID del clon sea único para un host.

  Si diversas operaciones de clonado de actualización utilizan el mismo archivo de especificación de clon o utilizan el archivo de especificación de clon con el mismo SID de clon, se eliminará el clon existente con el SID del host y, a continuación, se creará el clon.

- Asegúrese de que la política de backup esté habilitada con protección secundaria y que el archivo de especificación del clon se cree con "'-IncludeSecondaryDetails" para crear los clones con backups secundarios.
  - Si se especifica el archivo de especificación del clon principal pero la política tiene seleccionada la opción de actualización secundaria, se creará el backup y la actualización se transferirá al secundario. Sin embargo, el clon se creará a partir del backup primario.
  - Si se especifica el archivo de especificación del clon principal y la política no tiene seleccionada la opción de actualización secundaria, se creará el backup en la ubicación principal y se creará el clon a partir de la ubicación principal.
- Pasos*

1. Inicie una sesión de conexión con el servidor SnapCenter para el usuario especificado: *Open-SmConnection*
2. Cree una especificación de clon de base de datos de Oracle a partir de una copia de seguridad especificada: *New-SmOracleCloneSpecification*

   Si la política de protección de datos secundaria es mirror-vault unificado, especifique solo -IncludeSecondaryDetails. No es necesario especificar -SecondaryStorageType.

Este comando crea automáticamente un archivo de especificación de clon de base de datos de Oracle para la base de datos de origen especificada y su backup. Además debe proporcionar un SID de base de datos del clon para que el archivo de especificación creado tenga los valores generados automáticamente para la base de datos del clon que creará.

> El archivo de especificación del clon se crea en */var/opt/snapcenter/sco/clone_specs*.

3. Ejecute *Refresh-SmClone*.

   Si la operación falla con los mensajes de error "PL-SCO-20032: CanExecute operación falló con el error: PL-SCO-30031: Redo log file +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log exists", especifique un valor superior para *-WaitToTriggerClone*.

Para obtener información detallada sobre comandos UNIX, consulte "Guía de referencia de comandos del software SnapCenter".

Eliminar el clon de una base de datos conectables

Es posible eliminar el clon de una base de datos conectables (PDB) si ya no se necesita.

Si creó un backup de la CDB de destino donde se clona la PDB, al eliminar la clonado de la PDB, la PDB clonada también se quita del backup de la CDB de destino.

> Los clones de las PDB no se muestran en la vista de inventario o recursos.

- 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. Seleccione la base de datos del contenedor de origen (CDB) en la vista del recurso o grupo de recursos.
  3. En la vista Manage Copies (Administrar copias), seleccione **Clones** ya sea en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
  4. Seleccione el clon de PDB (targetCDB:PDBClone) y, a continuación, haga clic en .
  5. Haga clic en **Aceptar**.

Gestione los volúmenes de aplicaciones

Añada volúmenes de la aplicación

SnapCenter permite realizar backups y clonado de volúmenes de aplicaciones de bases de datos de Oracle. Debe añadir manualmente los volúmenes de la aplicación. No se admite la detección automática de volúmenes de aplicaciones.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. Haga clic en **Agregar volumen de aplicación**.

3. En la página Name, realice los siguientes pasos:
   - En el campo Name, introduzca el nombre del volumen de la aplicación.
   - En el campo Host Name, introduzca el nombre del host.
4. En la página Storage Footprint, introduzca el nombre del sistema de almacenamiento, seleccione uno o volúmenes y especifique los LUN o qtree asociados.

   Puede añadir varios sistemas de almacenamiento.

5. Revise el resumen y, a continuación, haga clic en **Finalizar**.
6. En la página Resources, seleccione **volumen de aplicación** en la lista **View** para ver todos los volúmenes de aplicación que ha agregado.

Modifique el volumen de la aplicación

Es posible modificar todos los valores especificados al añadir el volumen de aplicaciones si no se crean backups. Si se crea el backup, solo puede modificar los detalles del sistema de almacenamiento.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
  3. Haga clic en para modificar los valores.

Elimine el volumen de la aplicación

Cuando se elimina un volumen de aplicaciones, si hay backups asociados con el volumen de la aplicación, el volumen se pondrá en modo de mantenimiento y no se crearán backups nuevos y no se conservarán backups anteriores. Si no hay backups asociados, se eliminan todos los metadatos.

Si es necesario, SnapCenter permite deshacer la operación de eliminación.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
  3. Haga clic en para modificar los valores.

Aplicación de backup para volúmenes

Realice un backup del volumen de la aplicación

Si el volumen de la aplicación no forma parte de ningún grupo de recursos, es posible realizar backups del volumen de la aplicación desde la página Resources.

Acerca de esta tarea

De manera predeterminada, se crean backups de grupo de consistencia (CG). Si desea crear copias de seguridad basadas en volúmenes, debe establecer el valor de **EnableOracleNdvVolumeBasedBackup** en

true en el archivo *web.config*.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
2. En la página Resources, seleccione **volumen de aplicación** 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 el volumen de la aplicación del que desea realizar un backup.

   Aparece la página Application volume-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 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**.

      policy_name es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

7. 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 del volumen de la aplicación.

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

Realice un backup del grupo de recursos de volúmenes de aplicaciones

Es posible realizar un backup del grupo de recursos que solo contenga volúmenes de aplicación o una combinación de volúmenes de aplicaciones y bases de datos. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

Si el grupo de recursos tiene varios volúmenes de aplicaciones, todos los volúmenes de aplicaciones deben tener una política de replicación de SnapMirror o SnapVault.

Acerca de esta tarea

De manera predeterminada, se crean backups de grupo de consistencia (CG). Si desea crear copias de seguridad basadas en volúmenes, debe establecer el valor de **EnableOracleNdvVolumeBasedBackup** en true en el archivo *web.config*.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Se puede buscar el grupo de recursos ingresando su nombre en el cuadro de búsqueda o haciendo clic en * **y, luego, 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**.
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**.

Se realizará la operación de verificación solo para las bases de datos y no para los volúmenes de aplicaciones.

Clone el backup de volumen de la aplicación

Es posible utilizar SnapCenter para clonar los backups de volumen de aplicaciones.

- Pasos*

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
3. Seleccione el volumen de la aplicación en la vista de detalles del volumen de la aplicación o en la vista de detalles del grupo de recursos.

   Se muestra la página de topología del volumen de la aplicación.

4. En la vista Manage Copies, seleccione los backups desde local copies (primary), Mirror copies (secondary) o Vault copies (secondary).
5. Seleccione el backup en la tabla y haga clic en .
6. En la página Location, lleve a cabo las siguientes acciones:

Para este campo…	Realice lo siguiente…
Host de plugin	Seleccione el host donde desea crear el clon.
Nombre del recurso de destino	Especifique el nombre del recurso.

7. En la página Scripts, especifique los nombres de los scripts que se van a ejecutar antes de la clonación, comandos para montar un sistema de archivos y nombres de los scripts que se van a ejecutar después de la clonación.
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 de clonado realizada, 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**.

Divida un clon de volumen de aplicación

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
  3. Seleccione el recurso clonado y haga clic en .
  4. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
  5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Eliminar un clon de volumen de aplicaciones

Puede eliminar clones si ya no le resultan necesarios. No puede eliminar clones que actúan como origen para otros clones.

- Pasos*
  1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Oracle Database en la lista.
  2. En la página Resources, seleccione **volumen de aplicación** en la lista **View**.
  3. Seleccione el recurso o el grupo de recursos de la lista.

     Se muestra la página con el resumen o grupo de recursos.

  4. En la vista Manage Copies (Administrar copias), seleccione **Clones** ya sea en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
  5. Seleccione el clon y, a continuación, haga clic en .
  6. En la página Delete Clone, lleve a cabo las acciones siguientes:
     a. En el campo **Pre clone delete**, introduzca los nombres de las secuencias de comandos que se van a ejecutar antes de eliminar el clon.
     b. En el campo **Unmount**, introduzca los comandos para desmontar el clon antes de eliminarlo.
  7. Haga clic en **Aceptar**.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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