Instalación y configuración de UNIX para 7-mode

SnapManager for SAP

NetApp
April 19, 2024

Tabla de contenidos

Instalación y configuración de UNIX para 7-mode

Información general del producto

SnapManager para SAP automatiza y simplifica los procesos manuales asociados a operaciones como el backup, la recuperación y el clonado de bases de datos, tareas de gran complejidad y que requieren mucho tiempo. Puede usar SnapManager con la tecnología SnapMirror de ONTAP para crear copias de backups en otro volumen, y también con la tecnología ONTAP SnapVault para archivar backups de forma eficiente a disco.

SnapManager proporciona las herramientas necesarias, como Unified Manager de OnCommand e integración con BR* Tools de SAP, para realizar la administración de datos basada en normativas, programar y crear backups regulares de bases de datos, así como restaurar datos de estos backups en caso de pérdida o desastre.

SnapManager también se integra con tecnologías nativas de Oracle, como Real Application Clusters (Oracle RAC) y Oracle Recovery Manager (RMAN) para conservar la información de backup. Posteriormente, se pueden utilizar estos backups en operaciones de restauración a nivel de bloque o de recuperación de un momento específico en el espacio de tabla.

Aspectos destacados de SnapManager

SnapManager integra perfectamente con bases de datos en el host UNIX y con las tecnologías de Snapshot, SnapRestore y FlexClone en back-end Ofrece una interfaz de usuario (UI) fácil de usar y una interfaz de línea de comandos (CLI) para funciones administrativas.

SnapManager permite realizar las siguientes operaciones de base de datos y gestionar los datos de forma eficiente:

- Creación de backups con gestión eficiente del espacio en almacenamiento primario o secundario

  SnapManager permite realizar backups de los archivos de datos y los archivos de registro de archivos por separado.

- Programación de backups
- Restauración de bases de datos completas o parciales mediante una operación de restauración basada en archivos o volúmenes
- Recuperación de bases de datos mediante la detección, el montaje y la aplicación de archivos de registro de archivos a partir de backups
- Eliminar archivos de registro de archivos de destinos de registro de archivos cuando se crean backups solo de los registros de archivos
- Si se conserva un número mínimo de backups de registros de archivos automáticamente, solo se deben retener los backups que contienen archivos únicos de registro de archivos
- Realizar un seguimiento de los detalles de las operaciones y generar informes
- Verificación de copias de seguridad para garantizar que las copias de seguridad tienen un formato de bloque válido y que ninguno de los archivos de copia de seguridad está dañado
- Mantener un historial de operaciones realizadas en el perfil de base de datos

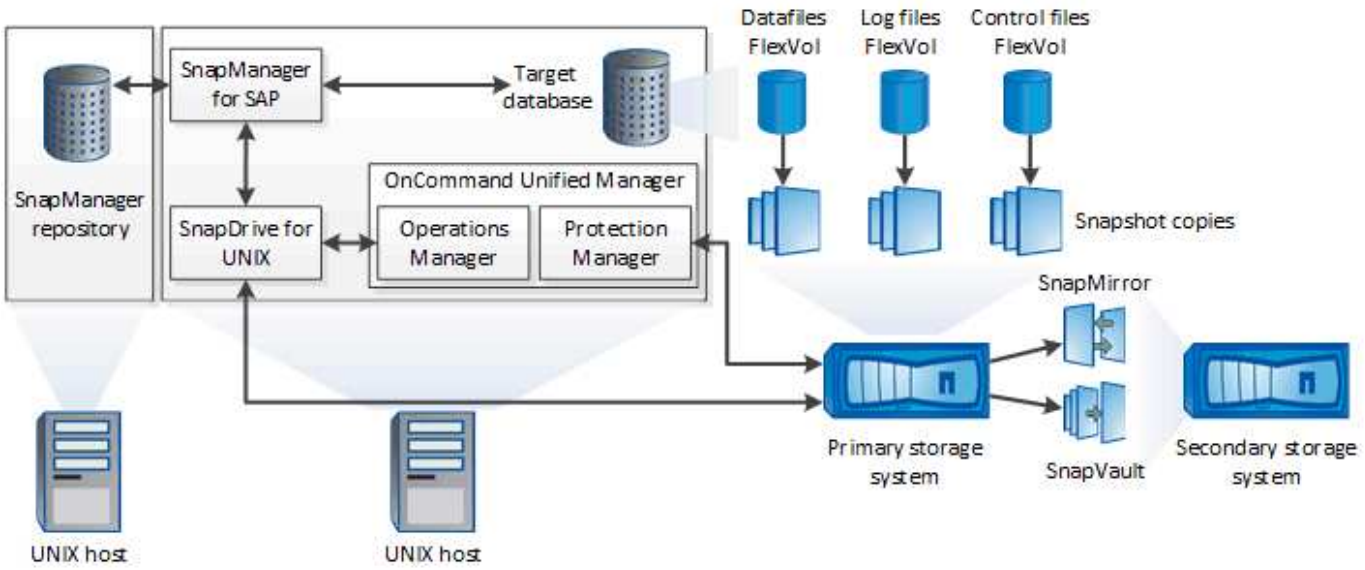
Un perfil contiene información acerca de la base de datos que va a gestionar SnapManager.

- Protección de backups en sistemas de almacenamiento secundario y terciario.
- Crear clones de backups con gestión eficiente del espacio en el almacenamiento principal o secundario

  SnapManager permite dividir el clon de una base de datos.

Arquitectura SnapManager

SnapManager para SAP incluye componentes que trabajan conjuntamente para proporcionar una solución completa y potente de backup, restauración, recuperación y clonación para bases de datos Oracle.



SnapDrive para UNIX

SnapManager requiere que SnapDrive establezca la conexión con el sistema de almacenamiento. Debe instalar SnapDrive para UNIX en cada host de la base de datos de destino antes de instalar SnapManager.

SnapManager para SAP

Debe instalar SnapManager para SAP en cada host de la base de datos de destino.

Puede usar la interfaz de línea de comandos (CLI) o la interfaz de usuario desde el host de base de datos donde se ha instalado SnapManager para SAP. También puede usar la interfaz de usuario de SnapManager de forma remota mediante un explorador web desde cualquier sistema que se ejecute en un sistema operativo compatible con SnapManager.

La versión de JRE compatible es 1.8.

Base de datos de destino

La base de datos de destino es una base de datos de Oracle que se desea gestionar mediante SnapManager para realizar operaciones de backup, restauración, recuperación y clonado.

La base de datos de destino puede ser independiente, Real Application Clusters (RAC) o residir en volúmenes de Oracle Automatic Storage Management (ASM). Para obtener detalles sobre las versiones, las configuraciones, los sistemas operativos y los protocolos de la base de datos de Oracle admitidos, consulte la herramienta de matriz de interoperabilidad de NetApp.

Repositorio de SnapManager

El repositorio de SnapManager reside en una base de datos de Oracle y almacena metadatos sobre perfiles, backups, restauración, recuperación y clonado. Un único repositorio puede contener información sobre las operaciones realizadas en varios perfiles de base de datos.

El repositorio de SnapManager no puede residir en la base de datos de destino. La base de datos del repositorio de SnapManager y la base de datos de destino deben estar en línea antes de ejecutar operaciones de SnapManager.

Paquete Core de OnCommand Unified Manager

El paquete principal de OnCommand Unified Manager integra las funcionalidades de Operations Manager, Protection Manager y Provisioning Manager. Centraliza las normativas de aprovisionamiento, clonado, backup y recuperación de datos, así como las de recuperación tras siniestros (DR). Integrar todas estas funciones hace que sea posible realizar muchas funciones de gestión desde una única herramienta.

Operations Manager

Operations Manager es la interfaz de usuario web del paquete principal de OnCommand Unified Manager. Se utiliza para la supervisión diaria del almacenamiento, las alertas de problemas y la generación de informes sobre la infraestructura del sistema de almacenamiento y el sistema de almacenamiento. La integración de SnapManager aprovecha las funcionalidades RBAC de Operations Manager.

Protection Manager

Protection Manager brinda a los administradores una consola de gestión fácil de usar que permite configurar y controlar rápidamente todas las operaciones de SnapMirror y SnapVault. La aplicación permite que los administradores apliquen políticas de protección de datos sistemáticas, automaticen procesos complejos de protección de datos y agrupen los recursos de respaldo y replicación para lograr una mejor utilización.

La interfaz de Protection Manager es la consola de gestión de NetApp, la plataforma de cliente para las aplicaciones de software de gestión de NetApp. La consola de gestión de NetApp se ejecuta en un sistema Windows o Linux diferente al servidor en el que se ha instalado el OnCommand Server. Permite a los administradores de almacenamiento, aplicaciones y servidores realizar tareas diarias sin tener que cambiar entre diferentes IU. Las aplicaciones que se ejecutan en la consola de gestión de NetApp son Protection Manager, Provisioning Manager y Performance Advisor.

Sistema de almacenamiento primario

SnapManager realiza un backup de las bases de datos objetivo en el sistema de almacenamiento primario de NetApp.

Sistema de almacenamiento secundario

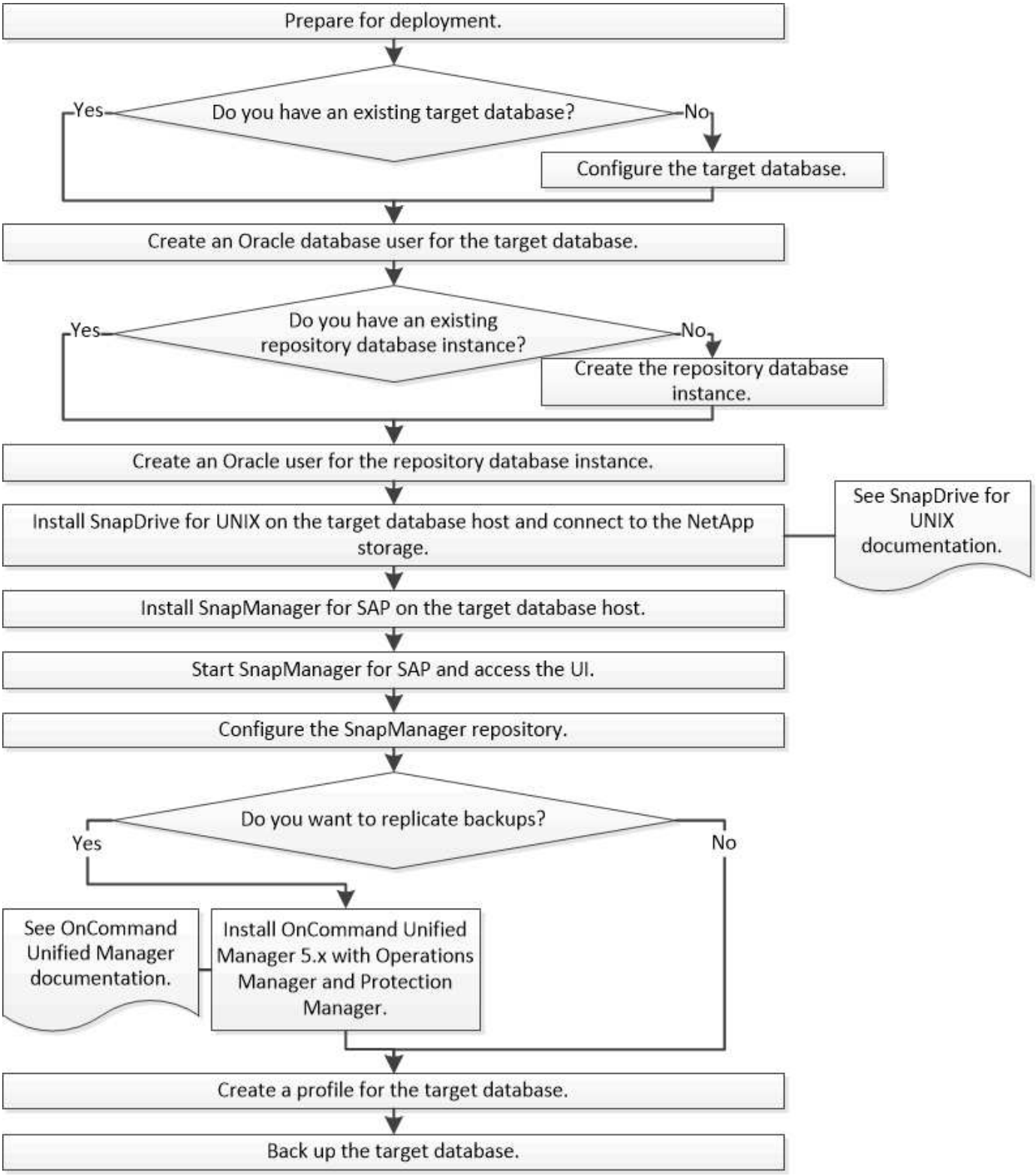
Cuando se habilita la protección de datos en un perfil de base de datos, los backups creados en el sistema de almacenamiento principal por SnapManager se replican en un sistema de almacenamiento secundario de NetApp mediante las tecnologías SnapVault y SnapMirror.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Flujo de trabajo de implementación

Antes de poder crear backups con SnapManager, primero debe instalar SnapDrive para UNIX y, a continuación, instalar SnapManager para SAP.



Prepárese para la puesta en marcha

Antes de implementar SnapManager, debe asegurarse de que el sistema de almacenamiento y los hosts UNIX cumplen con los requisitos mínimos de recursos.

Pasos

1. Compruebe que tiene las licencias necesarias.
2. Compruebe las configuraciones admitidas.
3. Compruebe los tipos de almacenamiento admitidos.
4. Verificar que los hosts UNIX cumplen los requisitos de SnapManager.

Licencias de SnapManager

Se requieren una licencia de SnapManager y varias licencias de sistema de almacenamiento para habilitar las operaciones de SnapManager. La licencia de SnapManager está disponible en dos modelos de licencia: *Por servidor y licencia*, en los que reside la licencia de SnapManager en cada host de bases de datos; y *por sistema de almacenamiento, licencia*, en los que reside la licencia de SnapManager en el sistema de almacenamiento.

Los requisitos de licencia de SnapManager son los siguientes:

Licencia	Descripción	Donde se la requiere
SnapManager por servidor	Una licencia del lado del host para un host de base de datos específico.las licencias solo se requieren para los hosts de base de datos en los que se ha instalado SnapManager. No se requiere ninguna licencia de SnapManager para el sistema de almacenamiento.	En el host SnapManager. No se requiere una licencia de SnapManager en los sistemas de almacenamiento primarios y secundarios al usar la licencia por servidor.
SnapManager por sistema de almacenamiento	Una licencia del almacenamiento compatible con cualquier número de hosts de base de datos. Es obligatorio solo si no utiliza una licencia por servidor en el host de la base de datos.	En sistemas de almacenamiento principales y secundarios
SnapRestore	Una licencia requerida que permite a SnapManager restaurar bases de datos.	En sistemas de almacenamiento principales y secundarios Requerida en sistemas de destino de SnapVault para restaurar un archivo a partir de un backup

Licencia	Descripción	Donde se la requiere
FlexClone	Una licencia opcional para clonar bases de datos.	En sistemas de almacenamiento principal y secundario.requerida en sistemas de destino de SnapVault al crear clones a partir de un backup.
SnapMirror	Una licencia opcional para reflejar backups en un sistema de almacenamiento de destino.	En sistemas de almacenamiento principales y secundarios
SnapVault	Una licencia opcional para archivar backups en un sistema de almacenamiento de destino.	En sistemas de almacenamiento principales y secundarios
Protocolos	Se requieren licencias de NFS, iSCSI o FC en función del protocolo utilizado.	En sistemas de almacenamiento principales y secundarios Requerida en sistemas de destino de SnapMirror para suministrar datos si un volumen de origen no se encuentra disponible

Configuraciones admitidas

Los hosts en los que está instalando SnapManager deben cumplir con los requisitos especificados de software, explorador, base de datos y sistema operativo. Debe verificar la compatibilidad de la configuración antes de instalar o actualizar SnapManager.

Para obtener información acerca de las configuraciones admitidas, consulte "Herramienta de matriz de interoperabilidad".

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Tipos de almacenamiento admitidos

SnapManager admite una amplia variedad de tipos de almacenamiento en máquinas físicas y virtuales. Es necesario verificar la compatibilidad de su tipo de almacenamiento antes de instalar o actualizar SnapManager.

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

Máquina	Tipo de almacenamiento
ESX de VMware	• Volúmenes NFS conectados directamente con el Guest VM • LUN de RDM en el sistema operativo invitado

Requisitos del host UNIX

Debe instalar SnapManager para SAP en cada host donde esté alojada la base de datos de la que desea realizar el backup. Debe asegurarse de que los hosts cumplan con los requisitos mínimos de la configuración de SnapManager.

- Debe instalar SnapDrive en el host de la base de datos antes de instalar SnapManager.
- Puede instalar SnapManager en equipos físicos o virtuales.
- Debe instalar la misma versión de SnapManager en todos los hosts que compartan el mismo repositorio.
- Debe instalar el parche de Oracle `13366202` Si utiliza bases de datos de Oracle 11.2.0.2 o 11.2.0.3.

  Si usa DNFS, también debe instalar los parches enumerados en el informe My Oracle Support (MOS) `1495104.1` para un rendimiento y estabilidad máximos.

Para utilizar la interfaz gráfica de usuario (GUI) de SnapManager, debe tener un host ejecutándose en una de las siguientes plataformas. La GUI también requiere que Java Runtime Environment (JRE) 1.8 esté instalado en el host.

- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- SUSE Enterprise Linux
- Solaris SPARC, x86 y x86_64
- IBM AIX

SnapManager también funciona en el entorno virtualizado de VMware ESX.

Configurar las bases de datos

Debe configurar al menos dos bases de datos: Una base de datos de destino en la que se desea realizar backup con SnapManager y una base de datos de repositorio para almacenar los metadatos de la base de datos de destino. La base de datos de destino y la base de datos del repositorio de SnapManager deben estar configuradas y en línea antes de ejecutar operaciones de SnapManager.

Configurar la base de datos de destino

La base de datos de destino es una base de datos de Oracle que se puede configurar como independiente, Real Application Clusters (RAC), Automatic Storage Management (ASM) o cualquier otra combinación compatible.

Paso

1. Configure la base de datos de destino en *Informe técnico de NetApp 3633: Prácticas recomendadas para las bases de datos de Oracle en el almacenamiento de NetApp*.

Información relacionada

"Informe técnico de NetApp 3633: Mejores prácticas para las bases de datos de Oracle en el almacenamiento de NetApp"

Cree un usuario de base de datos Oracle para la base de datos de destino

Se necesita un usuario de la base de datos de Oracle para iniciar sesión en la base de datos y ejecutar operaciones de SnapManager. Debe crear este usuario con el privilegio *sysdba* si no existe un usuario con el privilegio *sysdba* para la base de datos de destino.

Acerca de esta tarea

SnapManager puede utilizar cualquier usuario de Oracle con el privilegio *sysdba* que existe para la base de datos de destino. Por ejemplo, SnapManager puede utilizar el usuario predeterminado *sys*. Sin embargo, incluso si el usuario existe, puede crear un nuevo usuario para la base de datos de destino y asignar el privilegio *sysdba*.

También puede usar el método de autenticación del SO en donde el sistema operativo (SO) permite que la base de datos Oracle utilice las credenciales que mantiene el sistema operativo para autenticar a los usuarios para iniciar sesión en la base de datos y ejecutar operaciones de SnapManager. Si el sistema operativo autentica, puede conectarse a la base de datos de Oracle sin especificar un nombre de usuario o una contraseña.

Pasos

1. Iniciar sesión en SQL *Plus:

   ```
   sqlplus '/ as sysdba'
   ```

2. Cree un nuevo usuario con una contraseña de administrador:

   ```
   create user user_name identified by admin_password;
   ```

   `user_name` es el nombre del usuario que va a crear y. *`admin_password`* es la contraseña que desea asignar al usuario.

3. Asigne el privilegio sysdba al nuevo usuario de Oracle:

   ```
   grant sysdba to user_name;
   ```

Cree la instancia de la base de datos del repositorio

La instancia de la base de datos del repositorio es una base de datos de Oracle en la que se crea el repositorio de SnapManager. La instancia de la base de datos del repositorio debe ser una base de datos independiente y no puede ser la base de datos de destino.

Debe tener una base de datos de Oracle y una cuenta de usuario para acceder a la base de datos.

1. Iniciar sesión en SQL *Plus: `sqlplus '/ as sysdba'`
2. Crear un nuevo espacio de tabla para el repositorio de SnapManager: `create tablespacetablespace_name datafile '/u01/app/oracle/oradata/datafile/tablespace_name.dbf' size 100M autoextend on;`

   tablespace_name es el nombre del tablespace.
3. Compruebe el tamaño de bloque del tablespace: `select tablespace_name, block_size from dba_tablespaces;`

   SnapManager requiere un tamaño de bloque mínimo de 4 K para el espacio de tabla.

Información relacionada

"Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

Cree un usuario de Oracle para la instancia de la base de datos del repositorio

Se necesita un usuario de Oracle para iniciar sesión en la instancia de la base de datos del repositorio y acceder a ella. Debe crear este usuario con privilegios *connect* y *resource*.

1. Iniciar sesión en SQL *Plus:

   `sqlplus '/ as sysdba'`
2. Cree un nuevo usuario y asigne una contraseña de administrador a dicho usuario:

   `create user user_name identified by admin_password default tablespace tablespace_name quota unlimited on tablespace_name;`

   - *`user_name`* es el nombre del usuario que se está creando para la base de datos del repositorio.
   - *`admin_password`* es la contraseña que desea asignar al usuario.
   - *`tablespace_name`* es el nombre del tablespace creado para la base de datos del repositorio.
3. Asigne los privilegios *connect* y *resource* al nuevo usuario de Oracle:

   `grant connect, resource to user_name;`

Verifique la configuración del listener de Oracle

El listener es un proceso que escucha las solicitudes de conexión de cliente. Recibe solicitudes entrantes de conexión de cliente y administra el tráfico de estas solicitudes a la base de datos. Antes de conectarse a una base de datos de destino o a una instancia de base de datos de repositorio, puede utilizar `STATUS` comando para verificar la configuración del listener.

Acerca de esta tarea

La `STATUS` el comando muestra información básica sobre el estado de un listener específico, incluido un resumen de la configuración del listener, las direcciones del protocolo de escucha y un resumen de los servicios registrados con ese listener.

1. Introduzca el siguiente comando en el símbolo del sistema: **`lsnrctl STATUS`**

   El valor predeterminado asignado al puerto de escucha es 1521.

Instale SnapManager

Debe instalar SnapManager en cada host donde se ejecute la base de datos de la que desea realizar el backup.

Lo que necesitará

Debe haber instalado SnapDrive para UNIX en el host de la base de datos y establecer una conexión con el sistema de almacenamiento.

Para obtener información sobre cómo instalar SnapDrive y establecer una conexión con el sistema de almacenamiento, consulte la documentación de SnapDrive para UNIX.

Acerca de esta tarea

Debe instalar una instancia de SnapManager por cada host de bases de datos. Si usa una base de datos de RAC y desea realizar un backup de la base de datos de RAC, debe instalar SnapManager en todos los hosts de la base de datos de RAC.

1. Descargue el paquete de instalación de SnapManager para SAP para UNIX desde el sitio de soporte de NetApp y cópielo al sistema host.

   "Descargas de NetApp: Software"

2. Inicie sesión en el host de la base de datos como usuario root.
3. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el paquete de instalación.
4. Haga ejecutable el paquete de instalación:

   `chmod 755 *install_package.bin*`

5. Instalar SnapManager:

   `*./install_package.bin*`

6. Pulse `Enter` para continuar.
7. Siga estos pasos:

   a. Cambie el valor predeterminado del usuario del sistema operativo a. **`ora`** *`sid`*, donde *`sid`* es el identificador del sistema de la base de datos.

   b. Pulse `Enter` aceptar el valor predeterminado para el grupo de sistemas operativos.

      El valor predeterminado para el grupo es *dba*.

c. Pulse `Enter` aceptar el valor predeterminado para el tipo de inicio.

Se muestra el resumen de la configuración.

8. Revise el resumen de configuración y pulse `Enter` para continuar.

   SnapManager para SAP y el entorno de ejecución de Java (JRE) necesarios están instalados y el `smsap_setup` el script se ejecuta automáticamente.

   SnapManager para SAP se instala en `/opt/NetApp/smsap`.

Después de terminar

Para verificar si la instalación se realizó correctamente, siga estos pasos:

1. Inicie el para el servidor SnapManager ejecutando el siguiente comando:

   `smsap_server start`

   Aparece un mensaje que indica que el para el servidor SnapManager se está ejecutando.

2. Compruebe que el sistema SnapManager para SAP está funcionando correctamente introduciendo el comando siguiente:

   `smsap system verify`

   Aparece el siguiente mensaje: Número de ID de operación correcto.

   Número es el número de identificación de la operación.

Información relacionada

"Documentación de NetApp: SnapDrive para UNIX"

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Integración con SAP BR* Tools

Las herramientas SAP BR* que contienen herramientas SAP para la administración de bases de datos Oracle, por ejemplo, BRARCHIVE, BRBACKUP, BRCONNECT, BRRECOVER, BRRESTORE, BRSPACE y BRTOOLS utilizan la interfaz BACKINT proporcionada por SnapManager for SAP. Para integrar SAP BR* Tools, debe crear un vínculo desde el directorio BR* Tools hasta `/opt/NetApp/smsap/bin/`, Donde se instala el archivo BACKINT.

Lo que necesitará

- Debe asegurarse de que ha instalado SAP BR* Tools.

Pasos

1. Cree un vínculo desde el directorio BR*Tools hasta `/opt/NetApp/smsap/bin/backint` Archivo para cada instancia de SAP.

Debe usar el vínculo en lugar de copiar el archivo de modo que cuando instale una nueva versión de SnapManager, el vínculo señale la nueva versión de la interfaz BACKINT.

2. Defina las credenciales para el usuario que ejecuta los comandos BR*Tools.

   El usuario del sistema operativo necesita las credenciales del repositorio, el perfil y el servidor de SnapManager para SAP a fin de admitir el backup y la restauración de la instancia de SAP.

3. Especifique un nombre de perfil diferente.

   De forma predeterminada, SnapManager utiliza el perfil con el mismo nombre que el identificador del sistema SAP al procesar comandos de BR*Tools. Si este identificador de sistema no es único en su entorno, modifique el `initSID.utl` Archivo de inicialización SAP y cree un parámetro para especificar el perfil correcto. La `initSID.utl` el archivo está ubicado en `%ORACLE_HOME%\database`.

   ejemplo

   Una muestra `initSID.utl` el archivo es el siguiente:

```
# Backup Retention policy.
# Specifies the retention / lifecycle of backups on the filer.
#
----------------------------------------------------------------------
----------
# Default Value: daily
# Valid Values: unlimited/hourly/daily/weekly/monthly
# retain = daily
# Enabling Fast Restore.
#
----------------------------------------------------------------------
----------
# Default Value: fallback
# Valid Values: require/fallback/off
#
# fast = fallback
# Data Protection.
#
----------------------------------------------------------------------
----------
# Default Value: empty
# Valid Values: empty/yes/no
# protect =
# profile_name = SID_BRTOOLS
```

El nombre del parámetro siempre está en minúsculas y los comentarios deben tener un signo de número (#).

4. Edite el `initSID.sap` Archivo de configuración BR*Tools realizando los siguientes pasos:

   a. Abra el `initSID.sap` archivo.

   b. Busque la sección que contiene la información del archivo de parámetros de la utilidad de backup.

      ejemplo

      ```
      # backup utility parameter file
      # default: no parameter file
      # util_par_file =
      ```

   c. Edite la última línea para incluir la `initSID.utl` archivo.

      ejemplo

```
# backup utility parameter file
# default: no parameter file
# util_par_file = initSID.utl
```

Después de terminar

Registre la interfaz BACKINT en el Directorio de entorno del sistema (SLD) ejecutando `backint register-sld` comando.

Configure SnapManager

Puede iniciar SnapManager y acceder a ella mediante la interfaz de usuario (UI) o desde la interfaz de línea de comandos (CLI). Después de acceder a SnapManager, debe crear el repositorio de SnapManager antes de realizar cualquier operación de SnapManager.

Inicie el servidor SnapManager

Debe iniciar el servidor SnapManager desde el host de la base de datos de destino.

Paso

1. Inicie sesión en el host de la base de datos de destino e inicie el servidor SnapManager:

   `smsap_server start`

   Se muestra el siguiente mensaje: `SnapManager Server started on secure port` *`port_number with PID PID_number`*.

   El puerto predeterminado es *27214*.

Después de terminar

Puede verificar que SnapManager funciona correctamente:

`smsap_server verify`

Se muestra el siguiente mensaje: `Operation Id operation_ID_number succeeded`.

Acceda a la interfaz de usuario de SnapManager

Puede acceder a la interfaz de usuario de SnapManager de forma remota mediante un explorador web desde cualquier sistema que se ejecute en un sistema operativo compatible con SnapManager. También puede acceder a la interfaz de usuario de SnapManager desde el host de la base de datos de destino ejecutando el `smsapgui` comando.

Lo que necesitará

- Debe asegurarse de que SnapManager esté en ejecución.
- Debe asegurarse de que el sistema operativo y Java compatibles estén instalados en el sistema donde desea acceder a la interfaz de usuario de SnapManager.

  Para obtener información sobre el sistema operativo compatible y Java, consulte herramienta matriz de interoperabilidad.

Pasos

1. En la ventana del navegador web, introduzca lo siguiente:

   `https://server_name.domain.com:port_number`

   - *`server_name`* Es el nombre del host de la base de datos de destino donde se instala SnapManager.

     También puede introducir la dirección IP del host de la base de datos de destino.

   - *`port_number`* Es el puerto en el que se ejecuta SnapManager.

     El valor predeterminado es 27214.

2. Haga clic en el enlace **Iniciar SnapManager para SAP**.

   Aparecerá la interfaz de usuario de SnapManager for SAP.

Configurar el repositorio de SnapManager

Debe configurar el repositorio de SnapManager en la instancia de la base de datos del repositorio. La base de datos del repositorio almacena metadatos para las bases de datos gestionadas por SnapManager.

Lo que necesitará

- Debe haber creado la instancia de la base de datos del repositorio.
- Debe haber creado el usuario de Oracle para la instancia de la base de datos del repositorio con los

privilegios correspondientes.

- Debe haber incluido los detalles de la instancia de la base de datos del repositorio en `tnsnames.ora` archivo.

Acerca de esta tarea

Es posible configurar el repositorio de SnapManager desde la interfaz de usuario de SnapManager o desde la interfaz de línea de comandos (CLI). Estos pasos muestran cómo crear un repositorio con la interfaz de usuario de SnapManager. También puede utilizar la CLI si lo prefiere.

Para obtener información acerca de cómo crear el repositorio mediante la CLI, consulte la guía de administración de *SnapManager para SAP para UNIX*.

1. En el panel izquierdo de la interfaz de usuario de SnapManager, haga clic con el botón derecho del ratón en **repositorios**.
2. Seleccione **Crear nuevo repositorio** y haga clic en **Siguiente**.
3. En la ventana **Información de configuración de la base de datos del repositorio**, introduzca la siguiente información:

En este campo…	Realice lo siguiente…
Nombre de usuario	Introduzca el nombre del usuario creado para la instancia de la base de datos del repositorio.
Contraseña	Introduzca la contraseña.
Host	Introduzca la dirección IP del host donde se crea la instancia de la base de datos del repositorio.
Puerto	Introduzca el puerto utilizado para conectarse a la instancia de la base de datos del repositorio. El puerto predeterminado es 1521.
Nombre del servicio	Introduzca el nombre que utiliza SnapManager para conectarse a la instancia de la base de datos del repositorio. Según los detalles incluidos en la `tnsnames.ora` archivo, puede ser el nombre corto del servicio o el nombre completo del servicio.

4. En la ventana **Perform Repository Add Operation**, revise el resumen de configuración y haga clic en **Add**.

   Si la operación falla, haga clic en la pestaña **Detalles de operación** para ver qué causó el error de la operación. Los detalles del error también se capturan en el registro de operaciones ubicado en /var/log/smSAP.

5. Haga clic en **Finalizar**.

   El repositorio aparece en el panel izquierdo bajo el árbol **repositorios**. Si no ve el repositorio, haga clic con el botón derecho del ratón en **repositorios** y haga clic en **Actualizar**.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4.1 para SAP"

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault

Es posible utilizar SnapManager con la tecnología SnapMirror de ONTAP para crear copias reflejadas 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 *data-protection* entre los volúmenes de origen y destino y *initialize* la relación.

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.

Comprender las diferencias entre SnapMirror y SnapVault

SnapMirror es la tecnología de recuperación ante desastres diseñada para la conmutación del almacenamiento principal al almacenamiento secundario en un sitio geográficamente remoto. SnapVault es una tecnología de replicación de backup disco a disco diseñada para el cumplimiento de normativas y otros fines relacionados con la regulación.

Estos objetivos tienen en cuenta el diferente equilibrio que ocurre cada tecnología entre los objetivos de la moneda de backup y la retención de backup:

- SnapMirror almacena *only* las copias Snapshot que residen en el almacenamiento principal porque, en caso de desastre, necesita poder realizar una conmutación al respaldo a la versión más reciente de los datos primarios que sabe que son buenos.

  Por ejemplo, la organización puede duplicar las copias de los datos de producción por hora en un plazo de diez días. Como se indica en el caso de uso de la conmutación por error, el equipo del sistema secundario debe ser equivalente o casi equivalente al equipo del sistema primario para servir datos de forma eficiente desde el almacenamiento reflejado.

- Por el contrario, SnapVault almacena las copias snapshot _independientemente de que residan en el almacenamiento principal, ya que, en caso de auditoría, es probable que el acceso a los datos históricos sea tan importante como el acceso a los datos actuales.

  Es posible que desee conservar copias Snapshot mensuales de sus datos en un plazo de 20 años, por ejemplo, para cumplir con las normativas de contabilidad gubernamental de su empresa. Al no haber ningún requisito para servir datos desde el almacenamiento secundario, puede utilizar discos más lentos y menos costosos en el sistema vault.

Los diferentes pesos que aportan SnapMirror y SnapVault a la moneda de backup y la retención de backup se derivan finalmente del límite de 255 copias Snapshot por volumen. Aunque SnapMirror conserva las copias más recientes, SnapVault conserva las copias realizadas durante el período más prolongado.

Preparar los sistemas de almacenamiento para la replicación de SnapMirror

Antes de poder utilizar la tecnología SnapMirror integrada de SnapManager para reflejar copias Snapshot, debe configurar e inicializar una relación de protección de datos entre los volúmenes de origen y de destino. Durante la inicialización, SnapMirror realiza una copia Snapshot del volumen de origen, a continuación transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino. También transfiere cualquier otra copia Snapshot menos reciente del volumen de origen al volumen de destino.

Acerca de esta tarea

Es posible usar la CLI de ONTAP o OnCommand System Manager para ejecutar estas tareas. El siguiente procedimiento se basa en el supuesto de que está utilizando la CLI. Para obtener más información, consulte "Guía de recuperación y backup en línea de protección de datos de Data ONTAP 8.2 para 7-Mode".

> No se puede utilizar SnapManager para reflejar qtrees. SnapManager admite solo mirroring de volúmenes.

No se puede usar SnapManager para el mirroring síncrono. SnapManager solo admite mirroring asíncrono.

> Si va a almacenar archivos de base de datos y registros de transacciones en diferentes volúmenes, debe crear relaciones entre los volúmenes de origen y de destino para los archivos de base de datos y entre los volúmenes de origen y de destino para los registros de transacciones.

1. En la consola del sistema de origen, utilice `options snapmirror.access` comando para especificar los nombres de host de los sistemas con permiso para copiar datos directamente desde el sistema de origen.

   ejemplo

   La entrada siguiente permite la replicación a Destination_systemB:

   ```
   options snapmirror.access host=destination_systemB
   ```

2. En el sistema de destino, cree o edite el `/etc/snapmirror.conf` archivo para especificar el volumen que se va a copiar.

   ejemplo

   La siguiente entrada especifica la replicación de vol0 de source_Systema a vol2 de Destination_systemB:

   ```
   source_systemA:vol0 destination_systemB:vol2
   ```

3. En las consolas del sistema de origen y de destino, utilice `snapmirror on` Comando para habilitar SnapMirror.

   ejemplo

El siguiente comando habilita SnapMirror:

```
snapmirror on
```

4. En la consola del sistema de destino, utilice `vol create` Comando para crear un volumen de destino de SnapMirror con un tamaño igual o superior que el volumen de origen.

   ejemplo

   El siguiente comando crea un volumen de destino de 2 GB denominado vol2 en el agregado aggr1:

   ```
   vol create vol2 aggr1 2g
   ```

5. En la consola del sistema de destino, utilice el comando vol restrict para marcar el volumen de destino como restringido.

   ejemplo

   El siguiente comando Marca el volumen de destino vol2 como restringido:

   ```
   vol restrict vol2
   ```

6. En la consola del sistema de origen, utilice `snap sched` comando para deshabilitar cualquier transferencia programada.

   ejemplo

   Debe deshabilitar las transferencias programadas para evitar que se produzcan conflictos de programación con SnapDrive.

   El siguiente comando deshabilita las transferencias programadas:

   ```
   snap sched vol1 -----
   ```

7. En la consola del sistema de destino, utilice `snapmirror initialize` comando para crear una relación entre los volúmenes de origen y de destino, e inicializar la relación.

   El proceso de inicialización realiza una *transferencia basal* al volumen de destino. SnapMirror realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino. También transfiere cualquier otra copia Snapshot del volumen de origen al volumen de destino.

   ejemplo

   El siguiente comando crea una relación de SnapMirror entre el volumen de origen vol0 en source_Systema y el volumen de destino vol2 en Destination_systemB, e inicializa la relación:

```
snapmirror initialize -S source_systemA:vol0 destination_systemB:vol2
```

Preparar los sistemas de almacenamiento para la replicación SnapVault

Antes de poder utilizar la tecnología SnapVault integrada de SnapManager para archivar copias Snapshot en disco, debe configurar e inicializar una relación de protección de datos entre los volúmenes de origen y de destino. Durante la inicialización, SnapVault realiza una copia Snapshot del volumen de origen, a continuación transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino.

Lo que necesitará

- Debe haber configurado un conjunto de datos para la ubicación de almacenamiento principal en el asistente de configuración de SnapManager.
- Todas las LUN deben estar en qtrees, con una LUN por qtree.

> Si va a almacenar archivos de base de datos y registros de transacciones en diferentes volúmenes, debe crear relaciones entre los volúmenes de origen y de destino para los archivos de base de datos y entre los volúmenes de origen y de destino para los registros de transacciones.

Pasos

1. En las consolas del sistema de origen y de destino, active SnapVault:

   ejemplo

   ```
   options snapvault.enable on
   ```

2. En la consola del sistema de origen, utilice `options snapvault.access` comando para especificar los nombres de host de los sistemas con permiso para copiar datos directamente desde el sistema de origen.

   ejemplo

   El comando siguiente permite la replicación a Destination_systemB:

   ```
   options snapvault.access host=destination_systemB
   ```

3. En la consola del sistema de destino, utilice `options snapvault.access` comando para especificar los nombres de host de los sistemas a los que se pueden restaurar los datos copiados.

   ejemplo

   El siguiente comando permite restaurar los datos copiados en source_Systema:

```
options snapvault.access host=destination_systemA
```

4. En la consola del sistema de origen, utilice `ndmpd on` Comando para habilitar NDMP.

   ejemplo

   El siguiente comando habilita NDMP:

   ```
   ndmpd on
   ```

5. En la consola del sistema de destino, utilice `vol create` Comando para crear un volumen de destino de SnapMirror con un tamaño igual o superior que el volumen de origen.

   ejemplo

   El siguiente comando crea un volumen de destino de 2 GB denominado vol2 en el agregado aggr1:

   ```
   vol create vol2 aggr1 2g
   ```

6. En la consola de gestión de NetApp de OnCommand Unified Manager (UM), añada el pool de recursos para el volumen de destino:
   a. Haga clic en **datos** > **grupos de recursos** para abrir la página **grupos de recursos**.
   b. En la página Pools de recursos, haga clic en **Agregar** para iniciar el asistente **Agregar grupo de recursos**.
   c. Siga las instrucciones del asistente para especificar el agregado del volumen de destino.
   d. Haga clic en **Finalizar** para salir del asistente.
7. En la consola de gestión de UM de NetApp, asigne el pool de recursos al conjunto de datos que haya creado en el asistente de configuración de SnapManager:
   a. Haga clic en **Data** > **Datasets** para abrir la página Datasets.
   b. En la página **Datasets**, seleccione el conjunto de datos que ha creado y haga clic en **Editar**.
   c. En la página **Editar conjunto de datos**, haga clic en **copia de seguridad** > **grupos de aprovisionamiento/recursos** para abrir el asistente **Configurar nodo de conjunto de datos**.
   d. Siga las instrucciones del asistente para asignar el pool de recursos al conjunto de datos.

      La asignación de pool de recursos especifica la relación de protección de datos entre los volúmenes de origen y destino.

   e. Haga clic en **Finalizar** para salir del asistente e inicializar la relación de protección de datos.

      El proceso de inicialización realiza una *transferencia basal* al volumen de destino. SnapVault realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino.

Realizar backup y verificación de las bases de datos

Después de instalar SnapManager, puede crear una copia de seguridad básica de la base de datos y comprobar que la copia de seguridad no contiene ningún archivo dañado.

Información general sobre backup de SnapManager

SnapManager utiliza la tecnología Snapshot de NetApp para crear backups de bases de datos. Puede utilizar la utilidad DBVERIFY o SnapManager para verificar la integridad de las copias de seguridad.

SnapManager realiza un backup de una base de datos mediante la creación de copias Snapshot de los volúmenes que contienen archivos de datos, archivos de control y archivos de registro de archivos. Juntas, estas copias Snapshot incluyen un conjunto de respaldos que SnapManager puede usar para restaurar una base de datos.

Definición de una estrategia de backup

Definir una estrategia de backup antes de crear backups garantiza que se cuente con todos los backups para restaurar correctamente las bases de datos. SnapManager ofrece un programa de backup granular y flexible para cumplir con el acuerdo de nivel de servicio.

Para obtener información sobre las prácticas recomendadas de SnapManager, consulte *TR 3761*.

¿Qué modo de backup de SnapManager necesita?

SnapManager admite dos modos de backup:

Modo de backup	Descripción
Backup en línea	Crea un backup de la base de datos cuando la base de datos está en estado en línea. Este modo de backup también se denomina backup dinámico.
Backup sin conexión	Crea un backup de la base de datos cuando la base de datos está en estado montado o apagado. Este modo de backup también se denomina backup en frío.

¿Qué tipo de backup de SnapManager necesita?

SnapManager admite tres tipos de backups:

Tipo de backup	Descripción
Backup completo	Crea un backup de la base de datos completa, que incluye todos los archivos de datos, los archivos de control y los archivos de registro de archivos.

Tipo de backup	Descripción
Copia de seguridad parcial	Crea un backup de archivos de datos, archivos de control, espacios de tabla y archivos de registro de archivos seleccionados
Backup de solo registro de archivo	Crea una copia de seguridad sólo de los archivos de registro de archivo.debe seleccionar **copia de seguridad de archivos por separado** mientras crea el perfil.

¿Qué tipo de perfil de base de datos necesita?

SnapManager crea backups según si el perfil de la base de datos separa los backups de los registros de archivo de los backups del archivo de datos.

Tipo de perfil	Descripción
Un único perfil de base de datos para el backup combinado de archivos de datos y registros de archivos	Permite crear: • Backup completo que contiene todos los archivos de datos, los archivos de registro del archivo y los archivos de control • Backup parcial con los archivos de datos, espacios de tabla, archivos de registro de archivo y archivos de control seleccionados
Perfiles de base de datos separados para backups de registros de archivo y backups de archivos de datos	Permite crear: • Backup combinado con distintas etiquetas para backup de archivos de datos y backup de registros de archivo • Backup de solo archivos de datos de todos los archivos de datos junto con los archivos de control • Backup parcial de solo archivos de datos de los archivos de datos o espacios de tablas seleccionados junto con los archivos de control • Backup de solo registros de archivo

¿Qué convenciones de nomenclatura se deben utilizar para las copias Snapshot?

Las copias Snapshot creadas por los backups pueden seguir una convención de nomenclatura personalizada. El texto personalizado o las variables integradas, como el nombre del perfil, el nombre de la base de datos y el SID de la base de datos proporcionado por SnapManager, se pueden utilizar para crear la convención de nomenclatura. Puede crear la convención de nomenclatura mientras crea la política.

Debe incluir la variable smid en el formato de nomenclatura. La variable smid crea un identificador de instantánea único.

La convención de nomenclatura de las copias Snapshot se puede cambiar durante o después de la creación de un perfil. El patrón actualizado se aplica solo a las copias Snapshot que todavía no se han creado; las copias Snapshot existentes conservan el patrón anterior.

¿Cuánto tiempo desea retener las copias de backup en el sistema de almacenamiento primario y en el sistema de almacenamiento secundario?

Una política de retención de backup especifica la cantidad de backups correctos que se retendrán. Puede especificar la política de retención mientras crea la política.

Puede seleccionar cada hora, día, semana, mensual o ilimitado como clase de retención. Para cada clase de retención, puede especificar el recuento de retención y la duración de la retención, ya sea de forma conjunta o individual.

- El recuento de retenciones determina la cantidad mínima de backups de una clase de retención determinada que se deben retener.

  Por ejemplo, si la programación de backup es *Daily* y el recuento de retenciones es *10*, se conservan 10 backups diarios.

  > El número máximo de copias de Snapshot que Data ONTAP permite retener es de 255. Cuando alcance el límite máximo, se producirá un error al crear nuevas copias Snapshot de forma predeterminada. Sin embargo, puede configurar la política de rotación en Data ONTAP para eliminar copias Snapshot más antiguas.

- La duración de la retención determina la cantidad mínima de días durante los cuales se debe conservar el backup.

  Por ejemplo, si la programación de la copia de seguridad es *Daily* y la duración de la retención es *10*, se retienen 10 días de los backups diarios.

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

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

¿Desea verificar las copias de backup con el volumen de origen o un volumen de destino?

Si usa SnapMirror o SnapVault, puede verificar las copias de backups con la copia de Snapshot en el volumen de destino de SnapMirror o SnapVault, en lugar de la copia de Snapshot en el sistema de almacenamiento principal. Al utilizar un volumen de destino para verificar, se reduce la carga para el sistema de almacenamiento principal.

Información relacionada

"Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

Cree un perfil para la base de datos

Debe crear un perfil para que la base de datos pueda realizar cualquier operación en esa base de datos. El perfil contiene información acerca de la base de datos y sólo puede hacer referencia a una base de datos; sin embargo, varios perfiles pueden hacer referencia a una base de datos. No es posible acceder a una copia de seguridad creada con un perfil desde otro perfil, incluso si ambos perfiles están asociados con la misma base de datos.

Lo que necesitará

Debe asegurarse de que los detalles de la base de datos de destino se incluyan en el `/etc/oratab` archivo.

Acerca de esta tarea

Estos pasos muestran cómo crear un perfil para la base de datos con la interfaz de usuario de SnapManager. También puede utilizar la CLI si lo prefiere.

Para obtener información acerca de cómo crear perfiles mediante la CLI, consulte la guía de administración de *SnapManager para SAP para UNIX*.

Pasos

1. En el árbol repositorios, haga clic con el botón secundario del ratón en el repositorio o en el host y seleccione **Crear perfil**.
2. En la página **Información de configuración del perfil**, introduzca el nombre y la contraseña personalizados del perfil.
3. En la página **Información de configuración de la base de datos**, introduzca la siguiente información:

En este campo…	Realice lo siguiente…
Nombre de la base de datos	Introduzca el nombre de la base de datos de la que desea realizar backup.
SID de base de datos	Introduzca el ID seguro (SID) de la base de datos. El nombre de la base de datos y el SID de la base de datos pueden ser iguales.
Host	Introduzca la dirección IP del host en el que reside la base de datos de destino. También puede especificar el nombre de host si el nombre de host se especifica en el sistema de nombres de dominio (DNS).
Cuenta de host	Introduzca el nombre de usuario de Oracle de la base de datos de destino. el valor predeterminado para el usuario es oracle.
Grupo de hosts	Introduzca el nombre del grupo de usuarios de Oracle. El valor predeterminado es dba.

4. En la página Database Connection Information, seleccione una de las siguientes opciones:

Elija esto…	Si desea…
Usar autenticación de o/S	Utilice las credenciales que mantiene el sistema operativo para autenticar a los usuarios que acceden a la base de datos.

Elija esto…	Si desea…
Usar autenticación de base de datos	Permitir que Oracle autentique un usuario administrativo mediante la autenticación del archivo de contraseña. Introduzca la información de conexión de la base de datos adecuada. • En el campo **SYSDBA Privileged User Name**, introduzca el nombre del administrador de la base de datos con privilegios administrativos. • En el campo **Contraseña**, introduzca la contraseña del administrador de la base de datos. • En el campo **Puerto**, introduzca el número de puerto utilizado para conectarse al host en el que reside la base de datos. El valor predeterminado es 1527.
Usar autenticación de instancia de ASM	Permitir que la instancia de la base de datos de Automatic Storage Management (ASM) autentique un usuario administrativo. Introduzca la información de autenticación de la instancia de ASM correspondiente. • En el campo **SYSDBA/SYSASM Privileged User Name**, introduzca el nombre de usuario del administrador de la instancia de ASM con privilegios administrativos. • En el campo **Contraseña**, introduzca la contraseña del administrador.

Puede seleccionar el modo de autenticación ASM solo si tiene una instancia de ASM en el host de la base de datos.

1. En la página Información de configuración de RMAN, seleccione una de las siguientes opciones:

Elija esto…	Si…
No utilice RMAN	No se utiliza RMAN para gestionar las operaciones de backup y restauración.
Usar RMAN a través del archivo de control	Se gestiona el repositorio de RMAN mediante archivos de control.
Usar RMAN a través del Catálogo de recuperación	Se gestiona el repositorio de RMAN mediante la base de datos de catálogo de recuperación. Introduzca el nombre de usuario que tiene acceso a la base de datos del catálogo de recuperación, la contraseña y el nombre del servicio de red de Oracle de la base de datos que gestiona la conexión de sustrato de red transparente (TNS).

2. En la página **Información de nomenclatura de instantánea**, seleccione las variables para especificar un formato de nomenclatura para la copia Snapshot.

   Debe incluir el `smid` variable en el formato de nomenclatura. La `smid` La variable crea un identificador

Snapshot único.

3. En la página **Configuración de directivas**, realice lo siguiente:
   a. Introduzca el recuento y la duración de la retención para cada clase de retención.
   b. En la lista desplegable **Directiva de protección**, seleccione la directiva de Protection Manager.
   c. Si desea realizar una copia de seguridad de los registros de archivos por separado, active la casilla de verificación **copia de seguridad de archivos por separado**, especifique la retención y seleccione la política de protección.

      Puede seleccionar una política que sea diferente de la asociada para los archivos de datos. Por ejemplo, si seleccionó una de la política de Protection Manager para archivos de datos, puede seleccionar una política diferente de Protection Manager para los registros de archivos.
4. En la página **Configurar ajustes de notificación**, especifique la configuración de notificación por correo electrónico.
5. En la página **Información de configuración del historial**, seleccione una de las opciones para mantener el historial de operaciones de SnapManager.
6. En la página **Perform Profile Create Operation**, compruebe la información y haga clic en **Crear**.
7. Haga clic en **Finalizar** para cerrar el asistente.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4.1 para SAP"

Realice una copia de seguridad de la base de datos

Después de crear un perfil, debe realizar un backup de la base de datos. Se pueden programar backups recurrentes después del backup y la verificación iniciales.

Acerca de esta tarea

Estos pasos muestran cómo crear un backup de la base de datos con la interfaz de usuario de SnapManager. También puede usar la interfaz de línea de comandos (CLI) si lo prefiere.

Para obtener información acerca de cómo crear copias de seguridad mediante la CLI o SAP BR* Tools, consulte la guía de administración de *SnapManager para SAP para UNIX*.

Pasos

1. En el árbol repositorios, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos de la que desea realizar la copia de seguridad y seleccione **copia de seguridad**.
2. En **Label**, introduzca un nombre personalizado para la copia de seguridad.

   No debe incluir espacios ni caracteres especiales en el nombre. Si no se especifica un nombre, SnapManager crea automáticamente una etiqueta de backup.

   En SnapManager 3.4, es posible modificar la etiqueta de backup creada automáticamente por SnapManager. Puede editar el `override.default.backup.pattern` y.. `new.default.backup.pattern` variables de configuración para crear su propio patrón de etiqueta de backup predeterminado.

3. Seleccione **permitir inicio o cierre de la base de datos, si es necesario** para modificar el estado de la base de datos, si es necesario.

   Esta opción garantiza que si la base de datos no está en el estado requerido para crear un backup, SnapManager automáticamente llevará la base de datos al estado deseado a fin de completar la operación.

4. En la página **base de datos, Tablespaces o Datafiles to Backup**, realice lo siguiente:
   a. Seleccione **copia de seguridad de archivos de datos** para realizar una copia de seguridad de la base de datos completa, los archivos de datos seleccionados o los tablespaces seleccionados.
   b. Seleccione **copia de seguridad Archivelogs** para realizar una copia de seguridad de los archivos de registro de archivos por separado.
   c. Seleccione **Prune Archivelogs** si desea eliminar los archivos de registro de archivos del sistema de archivos activo del que ya se ha realizado una copia de seguridad.

      Si está habilitado el área de recuperación de flash (FRA) para los archivos de registro de archivos, SnapManager no puede depurar los archivos de registro de archivos.

   d. Seleccione **proteger la copia de seguridad** si desea activar la protección de copia de seguridad.

      Esta opción sólo está activada si se ha seleccionado la directiva de protección al crear el perfil.

   e. Seleccione **proteger ahora** si desea proteger la copia de seguridad inmediatamente en el almacenamiento secundario reemplazando el programa de protección de Protection Manager.
   f. En la lista desplegable **Tipo**, seleccione el tipo de copia de seguridad (sin conexión o en línea) que desea crear.

      Si selecciona *Auto*, SnapManager crea una copia de seguridad basada en el estado actual de la base de datos.

   g. En la lista desplegable **clase de retención**, seleccione la clase de retención.
   h. Active la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** si desea asegurarse de que los archivos de copia de seguridad no están dañados.
5. En la página **activación de tareas**, especifique si desea realizar tareas antes y después de finalizar las operaciones de copia de seguridad.
6. En la página **realizar la operación de copia de seguridad**, compruebe la información y haga clic en **copia de seguridad**.
7. Haga clic en **Finalizar** para cerrar el asistente.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4.1 para SAP"

Verificar los backups de la base de datos

Puede verificar la copia de seguridad de la base de datos para asegurarse de que los archivos de los que se ha realizado una copia de seguridad no estén dañados.

Acerca de esta tarea

Si no ha seleccionado la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** al crear una copia de seguridad, debe realizar estos pasos manualmente para verificar la copia de seguridad. Sin embargo, si seleccionó esta casilla de comprobación, SnapManager verifica automáticamente el backup.

Pasos

1. En el árbol **repositorios**, seleccione el perfil.
2. Haga clic con el botón derecho del ratón en la copia de seguridad que desee verificar y seleccione **verificar**.
3. Haga clic en **Finalizar**.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

   En el árbol **repositorio**, haga clic con el botón secundario del ratón en la copia de seguridad y, a continuación, haga clic en **Propiedades** para ver los resultados de la operación de verificación.

Después de terminar

Es posible usar archivos de backup para realizar operaciones de restauración. Para obtener información acerca de cómo realizar operaciones de restauración con la interfaz de usuario de SnapManager, consulte *Ayuda en línea*. Si desea utilizar la interfaz de línea de comandos (CLI) para realizar operaciones de restauración, consulte la guía de administración de *SnapManager for SAP para UNIX*.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4.1 para SAP"

Programar copias de seguridad periódicas

Es posible programar operaciones de backup para que los backups se inicien automáticamente a intervalos regulares. SnapManager permite programar backups por hora, día, semana, mes o una sola vez.

Acerca de esta tarea

Es posible asignar varias programaciones de backup para una sola base de datos. Sin embargo, cuando se programen varios backups para la misma base de datos, se debe asegurarse de que no se hayan programado al mismo tiempo.

Estos pasos muestran cómo crear una programación de backups para la base de datos con la interfaz de usuario de SnapManager. También puede usar la interfaz de línea de comandos (CLI) si lo prefiere. Para obtener información acerca de cómo programar copias de seguridad mediante la CLI, consulte la guía de administración de *SnapManager para SAP para UNIX*.

1. En el árbol repositorios, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos para la que desea crear una programación de copia de seguridad y seleccione **copia de seguridad programada**.
2. En **Label**, introduzca un nombre personalizado para la copia de seguridad.

   No debe incluir espacios ni caracteres especiales en el nombre. Si no se especifica un nombre,

SnapManager crea automáticamente una etiqueta de backup.

En SnapManager 3.4, es posible modificar la etiqueta de backup creada automáticamente por SnapManager. Puede editar el `override.default.backup.pattern` y.. `new.default.backup.pattern` variables de configuración para crear su propio patrón de etiqueta de backup predeterminado.

3. Seleccione **permitir inicio o cierre de la base de datos, si es necesario** para modificar el estado de la base de datos, si es necesario.

   Esta opción garantiza que si la base de datos no está en el estado requerido para crear un backup, SnapManager automáticamente llevará la base de datos al estado deseado a fin de completar la operación.

4. En la página **Database, Tablespaces o Datafiles to Backup**, realice lo siguiente:
   a. Seleccione **copia de seguridad de archivos de datos** para realizar una copia de seguridad de la base de datos completa, los archivos de datos seleccionados o los tablespaces seleccionados.
   b. Seleccione **copia de seguridad Archivelogs** para realizar una copia de seguridad de los archivos de registro de archivos por separado.
   c. Seleccione **Prune Archivelogs** si desea eliminar los archivos de registro de archivos del sistema de archivos activo del que ya se ha realizado una copia de seguridad.

      Si está habilitado el área de recuperación de flash (FRA) para los archivos de registro de archivos, SnapManager no puede depurar los archivos de registro de archivos.

   d. Seleccione **proteger la copia de seguridad** si desea activar la protección de copia de seguridad.

      Esta opción sólo está activada si se ha seleccionado la directiva de protección al crear el perfil.

   e. Seleccione **proteger ahora** si desea proteger la copia de seguridad inmediatamente en el almacenamiento secundario reemplazando el programa de protección de Protection Manager.
   f. En la lista desplegable **Tipo**, seleccione el tipo de copia de seguridad (sin conexión o en línea) que desea crear.

      Si selecciona *Auto*, SnapManager crea una copia de seguridad basada en el estado actual de la base de datos.

   g. En la lista desplegable **clase de retención**, seleccione la clase de retención.
   h. Active la casilla de verificación **verificar copia de seguridad con la utilidad Oracle DBVERIFY** si desea asegurarse de que los archivos de copia de seguridad no están dañados.
5. En el campo **Nombre de programa**, introduzca un nombre personalizado de la programación.

   No debe incluir espacios en el nombre.

6. En la página **Configurar programa de copia de seguridad**, realice lo siguiente:
   a. En la lista desplegable **Perform this operation**, seleccione la frecuencia de la programación de copia de seguridad.
   b. En el campo **Fecha de inicio**, especifique la fecha en la que desea iniciar el programa de copia de seguridad.
   c. En el campo **Hora de inicio**, especifique la hora a la que desea iniciar el programa de copia de seguridad.

d. Especifique el intervalo en el que se crearán los backups.

   Por ejemplo, si ha seleccionado la frecuencia por hora y especifica el intervalo como 2, los backups se programarán cada 2 horas.

7. En la página **activación de tareas**, especifique si desea realizar tareas antes y después de finalizar las operaciones de copia de seguridad.
8. En la página **realizar operación de programación de copia de seguridad**, compruebe la información y haga clic en **programar**.
9. Haga clic en **Finalizar** para cerrar el asistente.

   Si la operación falla, haga clic en **Detalles de operación** para ver qué causó el fallo de la operación.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4.1 para SAP"

Desinstale el software desde un host UNIX

Si ya no necesita el software SnapManager, puede desinstalarlo desde el servidor host.

Pasos

1. Inicie sesión como root.
2. Para detener el servidor, escriba el siguiente comando: **`smsap_server stop`**
3. Para quitar el software SnapManager, introduzca el siguiente comando:

   `UninstallSmsap`

4. Después del texto de introducción, pulse **Intro** para continuar.

   Se completa la desinstalación.

Actualizar SnapManager

Puede actualizar a la última versión de SnapManager para SAP desde cualquiera de las versiones anteriores. Es posible actualizar todos los hosts SnapManager a la vez o realizar una actualización gradual, lo que permite actualizar los hosts de forma escalonada de host por host.

Preparando la actualización de SnapManager

El entorno en el que desea actualizar SnapManager debe cumplir con los requisitos específicos de software, hardware, explorador, base de datos y sistema operativo. Para obtener la información más reciente sobre los requisitos, consulte "Matriz de interoperabilidad".

Antes de la actualización, debe asegurarse de realizar las siguientes tareas:

- Complete las tareas de preinstalación necesarias.
- Descargue el último paquete de instalación de SnapManager para SAP.
- Instalar y configurar la versión adecuada de SnapDrive para UNIX en todos los hosts de destino.
- Crear un backup de la base de datos del repositorio de SnapManager para SAP.

Información relacionada

"Matriz de interoperabilidad"

Actualice los hosts SnapManager

Es posible actualizar todos los hosts existentes para utilizar la versión más reciente de SnapManager. Todos los hosts se actualizan de forma simultánea. Sin embargo, esto puede provocar un tiempo de inactividad de todos los hosts SnapManager y las operaciones programadas durante ese tiempo.

Pasos

1. Inicie sesión en el sistema host como usuario raíz.
2. Desde la interfaz de línea de comandos (CLI), desplácese hasta la ubicación donde ha descargado el archivo de instalación.
3. Si el archivo no es ejecutable, cambie los permisos: **`chmod 544 netapp.smsap`***
4. Detenga el servidor SnapManager:

   `smsap_server stop`

5. En función del host UNIX, instale SnapManager:

Si el sistema operativo es…	A continuación, ejecute…
Solaris (SPARC64)	**`# ./netapp.smsap.sunos-sparc64-version_number.bin`**
Solaris (x86_64)	**`# ./netapp.smsap.sunos-x64-version_number.bin`**
AIX (PPC64)	**`# ./netapp.smsap.aix-ppc64-version_number.bin`**
Linux x86	**`# ./netapp.smsap.linux-x86-version_number.bin`**
Linux x64	**`# ./netapp.smsap.linux-x64-version_number.bin`**

6. En la página **Introducción**, pulse **Intro** para continuar.

   Se muestra el siguiente mensaje: `Existing SnapManager For SAP Detected`.

7. Pulse **Intro**.
8. En el símbolo del sistema, realice lo siguiente:

a. Cambie el valor predeterminado del usuario del sistema operativo a. **ora** *sid*.

   sid Es el identificador del sistema de la base de datos SAP.

b. Introduzca el valor correcto para el grupo de sistemas operativos o pulse **Intro** para aceptar el valor predeterminado.

c. Introduzca el valor correcto para el tipo de inicio del servidor o pulse **Intro** para aceptar el valor predeterminado.

Se muestra el resumen de la configuración.

9. Pulse **Intro** para continuar.

   Se muestra el siguiente mensaje: `Uninstall of Existing SnapManager For SAP has started.`

   La desinstalación ha finalizado y la versión más reciente de SnapManager se ha instalado.

Tareas posteriores a la actualización

Después de actualizar a una versión posterior de SnapManager, es necesario actualizar el repositorio existente. También es posible que desee modificar la clase de retención de backup asignada a la copia de seguridad existente e identificar qué proceso de restauración se puede utilizar.

> Después de actualizar a SnapManager 3.3 o una versión posterior, debe configurar *sqlnet.authentication_services* para **NONE** Si desea utilizar la autenticación de base de datos (DB) como único método de autenticación. Esta función no es compatible con las bases de datos RAC.

Actualice el repositorio existente

No es necesario actualizar el repositorio existente si va a actualizar de SnapManager 3.3.x a SnapManager 3.4 o posterior pero para el resto de las rutas de actualización debe actualizar el repositorio existente para poder acceder a él después de la actualización.

Lo que necesitará

- El servidor SnapManager actualizado debe haberse iniciado y verificado.
- Debe existir un backup del repositorio existente.

Acerca de esta tarea

- Si va a actualizar desde cualquier versión anterior a SnapManager 3.1 a SnapManager 3.3 o posterior, primero debe actualizar a SnapManager 3.2.

  Después de actualizar a SnapManager 3.2, puede actualizar a SnapManager 3.3 o una versión posterior.

- Después de actualizar el repositorio, no se puede utilizar el repositorio con una versión anterior de SnapManager.

Paso

1. Actualice el repositorio existente:

   `smsap repository update -repository -dbname repository_service_name -host repository_host_name -login -username repository_user_name -port repository_port`

   - El nombre de usuario del repositorio, el nombre de servicio del repositorio y el nombre de host del repositorio pueden consistir en caracteres alfanuméricos, un signo menos, un guión bajo y un punto.
   - El puerto del repositorio puede ser cualquier número de puerto válido. Las demás opciones utilizadas durante la actualización del repositorio existente son las siguientes:
   - La `force` opción
   - La `noprompt` opción
   - La `quiet` opción
   - La `verbose` opción

     ejemplo

   ```
   smsap repository update -repository -dbname HR1
   -host server1 -login -username admin -port 1521
   ```

Después de terminar

Reinicie el servidor SnapManager para reiniciar todas las programaciones asociadas.

Modifique la clase de retención de la copia de seguridad

Después de la actualización, SnapManager asigna la clase de retención de backup predeterminada a los backups existentes. Puede modificar los valores predeterminados de la clase de retención para cumplir sus requisitos de copia de seguridad.

Acerca de esta tarea

La clase de retención de copias de seguridad predeterminada asignada a las copias de seguridad existentes es la siguiente:

Tipo de backup	Asignación de clase de retención después de la actualización
Los backups se retienen siempre	Ilimitada
Otros backups	Todos los días

Puede eliminar los backups que se conservan eternamente sin cambiar la clase de retención.

Si actualiza a SnapManager 3.0 o posterior, el valor mayor de los siguientes dos valores se asignará a los

perfiles existentes:

- Recuento de retención anterior para el perfil
- Valores predeterminados para el número de retención y la duración de los backups diarios, tal como se especifica en la `smsap.config` archivo

Paso

1. Modifique los valores asignados a. `retain.hourly.count` y.. `retain.hourly.duration` en la `smsap.config` archivo.

   La `smsap.config` el archivo está ubicado en *`default installation location`*`/properties/smsap.config`.

   Puede introducir los siguientes valores:

   - retain.hourly.count = **`12`**
   - retain.hourly.duration = **`2`**

Restaurar tipos de proceso

Todas las versiones de SnapManager para SAP no admiten todos los procesos de restauración. Después de actualizar SnapManager, debe tener en cuenta el proceso de restauración que puede usar para restaurar un backup.

Los backups creados con SnapManager 3.0 o versiones posteriores pueden restaurarse utilizando procesos rápidos de restauración y restauración basada en archivos. Sin embargo, los backups creados con una versión anterior a SnapManager 3.0 se pueden restaurar utilizando únicamente el proceso de restauración basada en archivos.

Puede determinar la versión de SnapManager utilizada para crear el backup mediante la ejecución del comando -backup show.

Actualizar hosts de SnapManager mediante actualización gradual

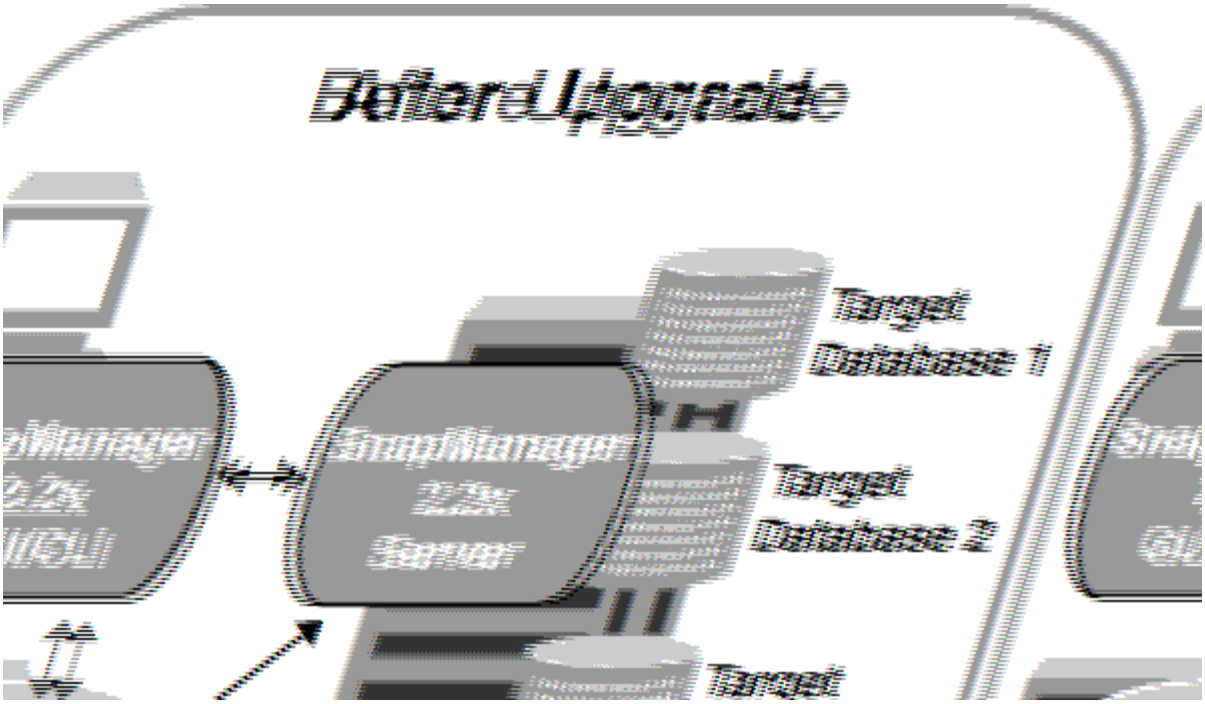
El enfoque de actualización gradual que permite actualizar los hosts de forma escalonada y host por host se admite desde SnapManager 3.1.

SnapManager 3.0 o versiones anteriores solo permitió actualizar todos los hosts al mismo tiempo. Esto provocó un tiempo de inactividad de todos los hosts SnapManager y las operaciones programadas durante la operación de actualización.

La actualización gradual ofrece las siguientes ventajas:

- Se ha mejorado el rendimiento de SnapManager porque solo se actualiza un host a la vez.
- Capacidad para probar las nuevas funciones en un host de servidor SnapManager antes de actualizar los otros hosts.

Solo se puede realizar la actualización gradual mediante la interfaz de línea de comandos (CLI).



Después de completar correctamente la actualización, los hosts de SnapManager, los perfiles, las programaciones, las backups, Además, los clones asociados con los perfiles de las bases de datos de destino se migran de la base de datos del repositorio de la versión de SnapManager anterior a la base de datos del repositorio de la nueva versión. Los detalles sobre las operaciones realizadas mediante los perfiles, las programaciones, los backups y los clones que se crearon con la versión anterior de SnapManager ahora están disponibles en la base de datos del repositorio de la nueva versión. Puede iniciar la GUI utilizando los valores de configuración predeterminados del archivo user.config. No se consideran los valores configurados en el archivo user.config de la versión anterior de SnapManager.

El servidor SnapManager actualizado ahora puede comunicarse con la base de datos del repositorio actualizada. Los hosts que no se actualizaron pueden gestionar sus bases de datos de destino mediante el repositorio de la versión anterior de SnapManager y, por lo tanto, pueden utilizar las funciones disponibles en la versión anterior.

Antes de realizar la actualización gradual, debe asegurarse de que todos los hosts de la base de datos del repositorio puedan resolverse. Para obtener información acerca de cómo resolver los hosts, consulte la sección de solución de problemas en *SnapManager for SAP Administration Guide for UNIX*.

Información relacionada

"Guía de administración para UNIX de SnapManager 3.4.1 para SAP"

Requisitos previos para realizar actualizaciones sucesivas

Antes de realizar una actualización gradual, debe asegurarse de que el entorno cumpla con ciertos requisitos.

- Si utiliza cualquier versión anterior a SnapManager 3.1 y desea realizar una actualización gradual a SnapManager 3.3 o posterior, primero debe actualizar a la versión 3.2 y, después, a la última.

  Puede actualizar directamente de SnapManager 3.2 a SnapManager 3.3 o posterior.

- Deben realizarse backups de los scripts externos que se usan para realizar cualquier protección de datos externa o retención de datos.
- Debe instalarse la versión de SnapManager a la que desea actualizar.

> Si va a actualizar desde cualquier versión anterior a SnapManager 3.1 a SnapManager 3.3 o posterior, primero debe instalar SnapManager 3.2 y realizar una actualización gradual. Después de actualizar a la versión 3.2, puede instalar SnapManager 3.3 o posterior y realizar otra actualización gradual a SnapManager 3.3 o posterior.

- Debe instalarse la versión de SnapDrive para UNIX compatible con la versión de SnapManager a la que desea actualizar.

  La documentación de SnapDrive contiene detalles sobre la instalación de SnapDrive.

- Debe realizarse un backup de la base de datos del repositorio.
- La cantidad de utilización de repositorio de SnapManager debe ser mínima.
- Si el host que se va a actualizar utiliza un repositorio, no deben realizarse operaciones de SnapManager en los demás hosts que utilizan el mismo repositorio.

  Las operaciones que están programadas o en ejecución en los otros hosts esperan a que finalice la actualización gradual.

> Se recomienda realizar una actualización gradual cuando el repositorio esté menos ocupado, como durante el fin de semana o cuando las operaciones no estén programadas.

- Los perfiles que apuntan a la misma base de datos de repositorio deben crearse con nombres diferentes en los hosts de servidor SnapManager.

  Si utiliza perfiles con el mismo nombre, la actualización gradual que implica esa base de datos del repositorio falla sin previo aviso.

- No deben realizarse operaciones de SnapManager en el host que se está actualizando.

> La actualización gradual se ejecuta durante más tiempo a medida que aumenta el número de backups de los hosts que se van actualizando conjuntamente. La duración de la actualización puede variar según la cantidad de perfiles y backups asociados con un host determinado.

Información relacionada

"Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"

Realice la actualización gradual en un único host o en varios

Puede realizar la actualización gradual en un único o varios hosts de servidor SnapManager mediante la interfaz de línea de comandos (CLI). El host del servidor SnapManager actualizado se gestiona únicamente con la versión posterior de SnapManager.

Lo que necesitará

Debe asegurarse de que se hayan completado todos los requisitos previos para realizar la actualización

gradual.

Pasos

1. Para realizar una actualización gradual en un solo host, introduzca el siguiente comando:

   smsap repository rollingupgrade-repository-dbname *repo_service_name* -host *repo_host* -login-username *repo_username* -port *repo_port* -upgradehost *host_with_target_database* -force [-quiet | -verbose]

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino montadas en Hosta y una base de datos de repositorio denominada REPOA ubicada en repo_host:

   ```
   smsap repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA
   ```

2. Para realizar una actualización gradual en varios hosts, introduzca el siguiente comando: `smsaprepository rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_port-upgradehosthost_with_target_database1,host_with_target_database2-force [-quiet | -verbose]`

   > Para varios hosts, introduzca los nombres de hosts separados por una coma y asegúrese de no incluir espacio entre la coma y el siguiente nombre de host.Si utiliza una configuración RAC, debe actualizar manualmente todos los hosts asociados con RAC. Puede utilizar -allhosts para realizar la actualización gradual de todos los hosts.

   El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino montadas en los hosts, Hosta y HostB y una base de datos de repositorio denominada REPOA ubicada en repo_host:

   ```
   smsap repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA,hostB
   ```

3. Para realizar una actualización gradual en todos los hosts de una base de datos de repositorio, introduzca el siguiente comando: `smsaprepository rollingupgrade-repository-`

```
dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-
portrepo_port-allhosts-force [-quiet | -verbose]
```

Después de actualizar correctamente la base de datos de repositorio, puede realizar todas las operaciones de SnapManager en la base de datos de destino.

El siguiente comando realiza la actualización sucesiva de todas las bases de datos de destino disponibles en una base de datos de repositorio denominada REPOA ubicada en repo_host:

```
smsap repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
      -allhosts
```

- Si el servidor SnapManager se inicia automáticamente, debe reiniciar el servidor para garantizar que pueda ver las programaciones.
- Si actualiza uno de los dos hosts relacionados, debe actualizar el segundo host después de actualizar el primero.

  Por ejemplo, si ha creado un clon del host A al host B o montado un backup del host A al host B, los hosts A y B están relacionados entre sí. Cuando se actualiza el host A, aparece un mensaje de advertencia en el que se le solicita actualizar el host B poco después de actualizar el host A.

> Los mensajes de advertencia se muestran aunque el clon se elimina o el backup se desasocia del host B durante la actualización gradual del host A. Esto se debe a que existen metadatos en el repositorio para las operaciones realizadas en el host remoto.

Qué es una reversión

La operación de reversión permite revertir a una versión anterior de SnapManager después de realizar una actualización gradual.

> Antes de realizar una reversión, debe asegurarse de que todos los hosts en la base de datos del repositorio puedan resolverse.

Al realizar una reversión, se revierte lo siguiente:

- Los backups creados, liberados y eliminados mediante la versión de SnapManager desde la que se está revirtiendo
- Los clones creados a partir de un backup que se creó mediante la versión de SnapManager a partir de la cual se va a revertir
- Las credenciales de perfil modificadas por medio de la versión de SnapManager de la que se va a revertir
- Estado de protección del backup modificado mediante la versión de SnapManager de la cual se va a revertir

No se admiten las funciones disponibles en la versión de SnapManager que utilizaba, pero no están disponibles en la versión en la que se está revirtiendo. Por ejemplo, cuando realiza una reversión desde SnapManager 3.3 o posterior a SnapManager 3.1, la configuración de historial establecida para perfiles en SnapManager 3.3 o posterior no se revierte a los perfiles en SnapManager 3.1. Esto se debe a que la característica de configuración del historial no estaba disponible en SnapManager 3.1.

Limitaciones en la ejecución de una reversión

Debe conocer cuáles son las situaciones en las que no se puede ejecutar una reversión. No obstante, en algunas de estas situaciones es posible ejecutar algunas tareas adicionales antes de realizar la reversión.

Los casos en los que no se puede ejecutar la reversión o se debe realizar las tareas adicionales son los siguientes:

- Si realiza una de las siguientes operaciones después de realizar una actualización gradual:
  - Cree un nuevo perfil.
  - Divida un clon.
  - Cambie el estado de protección del perfil.
  - Asigne una política de protección, una clase de retención o las relaciones de SnapVault y SnapMirror.

    En esta situación, después de ejecutar una reversión, debe quitar manualmente la política de protección, la clase de retención o las relaciones SnapVault y SnapMirror asignadas.
  - Cambie el estado de montaje del backup.

    En este caso, primero debe cambiar el estado de montaje a su estado original y, a continuación, ejecutar una reversión.
  - Restaurar un backup.
  - Cambie el modo de autenticación de la autenticación de la base de datos a la autenticación del sistema operativo (SO).

    En esta situación, después de realizar una reversión, debe cambiar manualmente el modo de autenticación de sistema operativo a base de datos.
- Si se cambia el nombre de host del perfil
- Si se separan perfiles para crear backups de registros de archivo

  En este caso, no puede volver a una versión anterior a SnapManager 3.2.

Requisitos previos para ejecutar una reversión

Antes de realizar una reversión, debe asegurarse de que el entorno cumpla con ciertos requisitos.

- Si utiliza SnapManager 3.3 o una versión posterior y desea revertir a una versión anterior a SnapManager 3.1, tendrá que volver a la versión 3.2 y, a continuación, a la versión deseada.
- Deben realizarse backups de los scripts externos que se usan para realizar cualquier protección de datos externa o retención de datos.

- Debe instalarse la versión de SnapManager a la que desea revertir.

  Si desea realizar una reversión de SnapManager 3.3 o posterior a una versión anterior a SnapManager 3.1, primero debe instalar SnapManager 3.2 y realizar una reversión. Después de revertir a 3.2, puede instalar SnapManager 3.1 o una versión anterior y realizar otra reversión a esa versión.

- Debe instalarse la versión de SnapDrive para UNIX compatible con la versión de SnapManager a la que desea revertir.

  Para obtener información sobre la instalación de SnapDrive, consulte el conjunto de documentación de SnapDrive.

- Debe realizarse un backup de la base de datos del repositorio.
- Si el host que se va a revertir utiliza un repositorio, no debe realizarse operaciones de SnapManager en los demás hosts que utilizan el mismo repositorio.

  Las operaciones que están programadas o en ejecución en los otros hosts esperan a que se complete la reversión.

- Los perfiles que apuntan a la misma base de datos del repositorio deben crearse con nombres diferentes en los hosts del servidor SnapManager.

  Si se utilizan perfiles con el mismo nombre, la operación de reversión que implica la base de datos del repositorio generará un error sin previo aviso.

- No se deben realizar operaciones de SnapManager en el host al que se desea revertir.

  Si existe una operación en ejecución, debe esperar hasta que se complete esa operación y antes de continuar con la reversión.

La operación de reversión se ejecuta durante más tiempo a medida que aumenta la cantidad acumulativa de backups de los hosts que se están revertir juntos. La duración de la reversión puede variar según la cantidad de perfiles y backups asociados con un host determinado.

Información relacionada

"Documentación en el sitio de soporte de NetApp"

Ejecute una reversión en un solo host o varios hosts

Puede realizar una reversión en una sola o varios hosts de servidor SnapManager con la interfaz de línea de comandos (CLI).

Lo que necesitará

Se debe asegurarse de que se hayan completado todos los requisitos previos para realizar una reversión.

Pasos

1. Para realizar una reversión en un solo host, introduzca el siguiente comando:

   ```
   smsaprepository rollback-repository-dbname repo_service_name -host repo_host
   -login -username repo_username -port repo_port -rollbackhost
   ```

host_with_target_database

ejemplo

En el ejemplo siguiente se muestra el comando para revertir todas las bases de datos de destino montadas en Hosta y una base de datos de repositorio denominada REPOA ubicada en el host de repositorio, repo_host:

```
smsap repository rollback
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -rollbackhost hostA
```

2. Para realizar una reversión en varios hosts, introduzca el siguiente comando:

smsaprepository rollback-repository-dbname *repo_service_name* -host *repo_host* -login-username *repo_username* -port *repo_port* -rollback *hosthost_with_target_database1,host_with_target_database2*

> Si desea introducir varios hosts, introduzca los nombres de host separados por una coma y asegúrese de que no haya espacio entre la coma y el siguiente nombre de host.

Si utiliza una configuración de RAC, debe revertir manualmente todos los hosts asociados de RAC. Es posible utilizar -allhosts para realizar una reversión de todos los hosts.

ejemplo

En el ejemplo siguiente se muestra el comando para revertir todas las bases de datos de destino montadas en los hosts, Hosta, HostB y una base de datos de repositorio denominada REPOA ubicada en el host de repositorios, repo_host:

```
smsap repository rollback
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -rollbackhost hostA,hostB
```

Los hosts, los perfiles, las programaciones, los backups y los clones que están asociados con los perfiles de las bases de datos de destino para el host se revierten al repositorio anterior.

Tareas posteriores a la reversión

Es necesario realizar algunos pasos adicionales después de revertir una base de datos de repositorio y degradar el host de SnapManager de SnapManager 3.2 a SnapManager 3.0, para ver las programaciones creadas en la versión anterior de la base de datos del repositorio.

1. Vaya a. `cd /opt/NetApp/smsap/repositories`.

   La `repositories` el directorio puede contener dos archivos para cada repositorio. El nombre de archivo con el signo de número (#) se crea utilizando SnapManager 3.1 o posterior y el nombre de archivo con el guión (-) se crea utilizando SnapManager 3.0.

   ejemplo

   Los nombres de los archivos pueden ser los siguientes:

   - `repository#SMSAP300a#SMSAPREPO1#10.72.197.141#1521`
   - `repository-smsap300a-smsaprepo1-10.72.197.141-1521`

2. Reemplace el signo de número (#) en el nombre de archivo por el guión (-).

   ejemplo

   El nombre de archivo que tenía el signo de número (#), ahora contiene un guión (-): `repository-SMSAP300a-SMSAPREPO1-10.72.197.141-1521.`

A continuación, ¿dónde ir

Después de instalar SnapManager y crear correctamente un backup, puede utilizar SnapManager para realizar operaciones de restauración, recuperación y clonado. Además, se recomienda buscar información sobre otras funciones de SnapManager, como la programación, la gestión de operaciones de SnapManager y el mantenimiento del historial de operaciones.

Es posible encontrar más información sobre estas funciones, así como información específica de la versión de SnapManager, en la siguiente documentación, toda la cual está disponible en "Soporte de NetApp".

- "Guía de administración para UNIX de SnapManager 3.4.1 para SAP"

  Describe cómo configurar Administrar SnapManager para SAP. Los temas incluyen cómo configurar, realizar backup, restaurar y clonar bases de datos, realizar una protección secundaria, Además de una explicación de los comandos de la CLI.

- "Notas de la versión de SnapManager 3.4 para SAP"

  Describe nuevas funciones, problemas solucionados, precauciones importantes, problemas conocidos y limitaciones de SnapManager para SAP.

- *Ayuda en línea de SnapManager para SAP*

  Describe los procedimientos paso a paso para realizar diferentes operaciones de SnapManager mediante

la interfaz de usuario de SnapManager.

> El *Ayuda en línea* se integra con la interfaz de usuario de SnapManager y no está disponible en el sitio de soporte.

- "Informe técnico de NetApp 3761: SnapManager para Oracle: Prácticas recomendadas"

  Describe las prácticas recomendadas de SnapManager para Oracle.

- "Informe técnico de NetApp 3633: Mejores prácticas para las bases de datos de Oracle en el almacenamiento de NetApp"

  Describe las prácticas recomendadas para configurar las bases de datos de Oracle en el sistema de almacenamiento de NetApp.

- "Informe técnico de NetApp 3442: SAP con Oracle en sistemas de almacenamiento UNIX y NFS y NetApp"

  Describe las prácticas recomendadas para poner en marcha el almacenamiento de NetApp para dar soporte a las soluciones de SAP.

Información relacionada

"Soporte de NetApp"

"Documentación de NetApp: Biblioteca de productos A-Z"