Protección de la configuración y ejecución de backups

SnapManager for SAP

NetApp
April 19, 2024

Tabla de contenidos

Protección de la configuración y ejecución de backups

Es necesario configurar SnapManager y Protection Manager para admitir backups de bases de datos en el almacenamiento secundario. El administrador de la base de datos y el administrador de almacenamiento deben coordinar las acciones correspondientes.

Utilice SnapManager para SAP para crear el perfil de base de datos para un backup local

Los administradores de bases de datos utilizan SnapManager para crear un perfil de base de datos que se utilizará para iniciar una copia de seguridad en el almacenamiento local en un sistema de almacenamiento primario. Los procesos de creación de perfiles y de creación de backups se realizan por completo en SnapManager; no implican Protection Manager.

Acerca de esta tarea

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para las copias de seguridad. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos, en su lugar sólo se proporciona el nombre del perfil. Un perfil sólo puede hacer referencia a una base de datos. Se puede hacer referencia a esa misma base de datos por más de un perfil.

Pasos

1. Acceda al cliente de SnapManager para SAP.
2. En el árbol repositorios SnapManager, haga clic con el botón secundario del ratón en el host que desee asociar a este perfil y seleccione **Crear perfil**.
3. En la página Información de configuración del perfil, introduzca la siguiente información y haga clic en **Siguiente**.
   - Nombre del perfil: Payroll_prod
   - Contraseña de perfil: Payroll123
   - Comentario: Base de datos de nóminas de producción
4. En la página Database Configuration Information (Información de configuración de la base de datos), introduzca la siguiente información y haga clic en **Next** (Siguiente).
   - Nombre de la base de datos: PAYDB
   - SID de base de datos: Payroldb
   - Host de la base de datos: Acepte el valor predeterminado

     Debido a que está creando un perfil a partir de un host en el árbol de repositorios, SnapManager muestra el nombre de host.
5. En la segunda página Información de configuración de la base de datos, acepte la siguiente información de la base de datos y haga clic en **Siguiente**:
   - Cuenta de host, que representa la cuenta de usuario de Oracle (para orWindows <sid>): Orapayroldb

◦ Host Group, que representa al grupo Oracle: dba

6. En la página Información de conexión a la base de datos, seleccione **utilizar autenticación de base de datos** para permitir que los usuarios se autentiquen mediante la información de la base de datos.

   Para este ejemplo, introduzca la siguiente información y haga clic en **Siguiente**.

   ◦ SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
   ◦ Contraseña (contraseña SYSDBA): oracle
   ◦ Puerto para conectarse al host de la base de datos: 1527

7. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables. La única variable que se requiere es la variable **smid**, que crea un identificador de instantánea único.

   Para este ejemplo, haga lo siguiente:

   a. En la lista símbolo de variable, seleccione la variable **{usertext}** y haga clic en **Agregar**.
   b. Introduzca "prod01.sample.com_" como nombre de host y haga clic en **Aceptar**.
   c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de "smSAP" en el cuadro Formato .
   d. Haga clic en **Siguiente**.

   La convención de nomenclatura Snapshot de *`smsap_hostname_smsapprofile_dbsid_scope_mode_smid`* Se convierte en "smsap_prpd01.sample.com_P01_BACKUP_P01_f_a_x" (donde "f" indica una copia de seguridad completa, la "a" indica el modo automático y la "x" representa el SMID único).

8. En la página realizar operación, compruebe la información y haga clic en **Crear**.
9. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.

Use Protection Manager para configurar un pool de recursos secundario

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para organizar los sistemas de almacenamiento secundario habilitados con la licencia secundaria de SnapVault en un conjunto de recursos para los backups.

Lo que necesitará

Lo ideal es que los sistemas de almacenamiento de un conjunto de recursos sean intercambiables en cuanto a su aceptación como destinos para los backups. Por ejemplo, al desarrollar la estrategia de protección para la base de datos de nóminas, como administrador de almacenamiento, identificó los sistemas de almacenamiento secundarios con niveles de servicio y rendimiento similares que serían miembros adecuados del mismo conjunto de recursos.

Ya creó agregados de espacio no utilizado en sistemas de almacenamiento que piensa asignar a pools de recursos. De este modo se garantiza que haya espacio adecuado para contener las copias de seguridad.

Pasos

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos** > **grupos de recursos**.

   Aparecerá la ventana Pools de recursos.

3. Haga clic en **Agregar**.

   Se iniciará el asistente Add Resource Pool.

4. Complete los pasos del asistente para crear el pool de recursos **paydb_backup_resource**.

   Utilice los siguientes ajustes:

   - Nombre: Use **paydb-backup_resource**
   - Umbrales de espacio (utilice los valores predeterminados):
     - Umbrales de utilización del espacio: Activado
     - Umbral casi completo (para el conjunto de recursos): 80%
     - Umbral completo (para el conjunto de recursos): 90%

Use Protection Manager para configurar las programaciones de backups secundarios

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para configurar una programación de backups.

Lo que necesitará

Antes de configurar la programación para las copias de seguridad secundarias, el administrador de almacenamiento consulta al partner DBA la siguiente información:

- La programación que el administrador de bases de datos desea que se sigan los backups secundarios.

  En este caso, los backups únicos diarios se realizan a las 7 p. m. Y los backups una vez semanales se realizan el sábado a las 1:00

Pasos

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **políticas** > **Protección** > **programas**.

   Se muestra la pestaña Schedules de la ventana Protection Policies.

3. Seleccione el horario diario **Diario a las 8:00 PM** en la lista de horarios.
4. Haga clic en **Copiar**.

   En la lista se muestra un nuevo horario diario, **copia del diario a las 8:00 PM**. Ya está seleccionado.

5. Haga clic en **Editar**.

La hoja de propiedades Editar horario diario se abre a la ficha Programación.

6. Cambie el nombre del programa a **nómina diaria a las 7 PM**, actualice la descripción y, a continuación, haga clic en **aplicar**.

   Se guardan los cambios.

7. Haga clic en la ficha **Eventos diarios**.

   La hora actual de copia de seguridad diaria de la programación es de 8:00 p.m. aparece en pantalla.

8. Haga clic en **Agregar** e introduzca **7:00 PM** en el nuevo campo Hora y, a continuación, haga clic en **aplicar**.

   La hora actual de copia de seguridad diaria del programa es ahora a las 7:00 p.m.

9. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

   Su nuevo horario diario, **Payroll Daily a las 7 PM**, se muestra en la lista de horarios.

10. Seleccione el horario semanal **Domingo a las 8:00 PM más diariamente** en la lista de horarios.
11. Haga clic en **Copiar**.

    En la lista se muestra un nuevo horario semanal, **copia del domingo a las 8:00 PM más diario**. Ya está seleccionado.

12. Haga clic en **Editar**.

    La hoja de propiedades Editar horario semanal se abre a la ficha Programación.

13. Cambie el nombre del programa a **Payroll Saturday a la 1 AM PLUS Daily a las 7 PM** y actualice la descripción.
14. En la lista desplegable **Horario diario**, seleccione el horario diario que acaba de crear, **Payroll Daily a las 7 PM**.

    Seleccionar **nómina diaria a las 7 PM** significa que este programa define cuándo se producen las operaciones diarias cuando se aplica a una política el programa **nómina de sábado a la 1 AM más diario a las 7 PM**.

15. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

    Su nuevo horario semanal, **Payroll Saturday a la 1 AM más diariamente a las 7 PM**, se muestra en la lista de horarios.

Use Protection Manager para configurar una política de protección de backups secundarios

Después de configurar la programación de backup, el administrador de almacenamiento configura una normativa de almacenamiento de backup protegido en la que se incluirá dicha programación.

Lo que necesitará

Antes de configurar la normativa de protección, el administrador de almacenamiento le ofrece al partner DBA la siguiente información:

- Duración de retención que se debe especificar para el almacenamiento secundario
- Tipo de protección del almacenamiento secundario requerida

Acerca de esta tarea

La política de protección que se crea, puede figurar en SnapManager para SAP por el partner de administrador de bases de datos y asignarse a un perfil de base de datos para la protección de los datos.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **políticas** > **Protección** > **Descripción general**.

   Se muestra la pestaña Overview de la ventana Protection Policies.

3. Haga clic en **Agregar directiva** para iniciar el asistente **Agregar directiva de protección**.
4. Complete el asistente con los siguientes pasos:

   a. Especifique un nombre de política descriptivo.

      Para este ejemplo, introduzca **TechCo Payroll Data: Copia de seguridad** y una descripción y, a continuación, haga clic en **Siguiente**.

   b. Seleccione una política base.

      Para este ejemplo, seleccione **copia de seguridad** y haga clic en **Siguiente**.

   c. En la hoja de propiedades de la directiva del nodo **datos primarios**, acepte la configuración predeterminada y haga clic en **Siguiente**.

      

      En este ejemplo, se aplica la programación de backup local configurada en SnapManager. Se ignora cualquier programación de backup local especificada con este método.

   d. En la hoja de propiedades de la conexión **datos primarios a copia de seguridad**, seleccione un programa de copia de seguridad.

      Para este ejemplo, seleccione **Payroll Saturday a la 1 AM más diariamente a las 7 PM** como su programa de copia de seguridad y, a continuación, haga clic en **Next**.

      En este ejemplo, la programación seleccionada incluye tanto las programaciones semanales como diarias que se configuraron anteriormente.

   e. En la hoja de propiedades **Política de copia de seguridad**, especifique el nombre del nodo de copia de seguridad y los tiempos de retención de copias de seguridad diarias, semanales o mensuales.

      Para este ejemplo, especifique una retención de backup diaria de 10 días y una retención de backup semanal de 52 semanas. Después de completar cada hoja de propiedades, haga clic en **Siguiente**.

   Una vez completadas todas las hojas de propiedades, el asistente para agregar directivas de protección muestra una hoja de resumen de la directiva de protección que desea crear.

5. Haga clic en **Finalizar** para guardar los cambios.

resultado

La política de protección de **TechCo Payroll Data: Backup** se incluye entre las demás políticas configuradas para Protection Manager.

Después de terminar

El partner de DBA puede ahora usar SnapManager para SAP para enumerar y asignar esta normativa al crear el perfil de base de datos para proteger los datos.

Utilice SnapManager para SAP para crear el perfil de base de datos y asignar una normativa de protección

Debe crear un perfil en SnapManager para SAP, habilitar la protección en el perfil y asignar una política de protección para crear un backup protegido.

Acerca de esta tarea

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para backups. Después de crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación. Un perfil sólo puede hacer referencia a una base de datos, pero es posible hacer referencia a esa misma base de datos mediante más de un perfil.

Pasos

1. Acceda al cliente de SnapManager para SAP.
2. En el árbol repositorios, haga clic con el botón secundario del ratón en el host y seleccione **Crear perfil**.
3. En la página **Información de configuración del perfil**, introduzca los detalles del perfil y haga clic en **Siguiente**.

   ejemplo

   Puede introducir la siguiente información:

   - Nombre del perfil: P01_BACKUP
   - Contraseña de perfil: Payroll123
   - Comentario: Base de datos de nóminas de producción
4. En las páginas **Información de configuración de la base de datos**, introduzca los detalles de la base de datos y haga clic en **Siguiente**.

   ejemplo

   Puede introducir la siguiente información:

   - Nombre de la base de datos: P01
   - SID de base de datos: P01
   - Host de la base de datos: Acepte el valor predeterminado. Debido a que está creando un perfil a partir de un host en el árbol de repositorios, SnapManager muestra el nombre de host.

- Cuenta de host, que representa la cuenta de usuario de Oracle (para orWindows <sid>): Orapayroldb
- Host Group, que representa al grupo Oracle: dba

5. En la página **Información de conexión a la base de datos**, haga clic en **usar autenticación de base de datos** para permitir que los usuarios autentiquen mediante información de la base de datos.
6. Introduzca los detalles de conexión de la base de datos y haga clic en **Siguiente**.

   ejemplo

   Puede introducir la siguiente información:

   - SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
   - Contraseña (contraseña SYSDBA): oracle
   - Puerto para conectarse al host de la base de datos: 1527
7. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables.

   La *`smid`* la variable crea un identificador snapshot único.

   Realice lo siguiente:

   a. En la lista **símbolo de variable**, seleccione *`usertext`* Y haga clic en **Agregar**.
   b. Introduzca *`prod01.sample.com_`* Como nombre de host y haga clic en **Aceptar**.
   c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de smsap en el cuadro Formato .
   d. Haga clic en **Siguiente**.

   La convención de nomenclatura Snapshot de *`smsap_hostname_smsapprofile_dbsid_scope_mode_smid`* Se convierte en "smsap_prpd01.sample.com_P01_BACKUP_P01_f_a_x" (donde "f" indica una copia de seguridad completa, "a" indica el modo automático y "x" representa el SMID único).
8. Seleccione **Directiva de protección de Protection Manager**.

   La normativa de protección de Protection Manager le permite seleccionar una directiva de protección configurada mediante la Consola de gestión de NetApp.
9. Seleccione **TechCo Payroll Data: Backup** como política de protección de las políticas de protección recuperadas de NetApp Management Console y haga clic en **Siguiente**.
10. En la página **realizar operación**, compruebe la información y haga clic en **Crear**.
11. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.

resultado

- La asignación de una normativa de protección de NetApp Management Console al perfil de base de datos crea automáticamente un conjunto de datos no conforme, visible para el operador de la Consola de gestión de NetApp, con el nombre convención smSAP_<hostname>_<profilename> o en este ejemplo: smsap_prod01.sample.com_P01_BACKUP.

- Si el perfil no es apto para la restauración de volumen (también llamado "restauración rápida"), se produce lo siguiente:
  - La ficha **resultados** indica que la creación del perfil se ha realizado correctamente y que se han producido advertencias durante la operación.
  - La ficha **Detalles de operación** incluye un registro DE ADVERTENCIA, que indica que el perfil no es elegible para una restauración rápida y explica por qué.

Utilice Protection Manager para aprovisionar el nuevo conjunto de datos

Una vez creado el conjunto de datos smsap_paydb, el administrador de almacenamiento utiliza Protection Manager para asignar recursos del sistema de almacenamiento a fin de aprovisionar el nodo Backup del conjunto de datos.

Lo que necesitará

Antes de aprovisionar el conjunto de datos recién creado, el administrador de almacenamiento consulta al partner DBA el nombre del conjunto de datos especificado en el perfil.

En este caso, el nombre del conjunto de datos es smsap_prod01.sample.com_P01.

Pasos

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos** > **conjuntos de datos** > **Descripción general**.

   La pestaña Datasets de la ventana Datasets muestra una lista de conjuntos de datos que incluye el conjunto de datos que acaba de crear mediante SnapManager.

3. Localice y seleccione el conjunto de datos **smsap_prod01.sample.com_p01**.

   Al seleccionar este conjunto de datos, el área del gráfico muestra el conjunto de datos smSAP_p01 sin aprovisionar con su nodo de backup. Su estado de conformidad se Marca como no conforme.

4. Con el conjunto de datos smsap_p01 todavía resaltado, haga clic en **Editar**.

   La consola de gestión de NetApp de Protection Manager muestra la ventana Editar conjunto de datos para el conjunto de datos **smsap_prod01.sample.com_p01**. El panel de navegación de la ventana muestra las opciones de configuración del nodo principal del conjunto de datos, la conexión de backup y el nodo de backup.

5. En el panel de navegación, busque las opciones del nodo de copia de seguridad del conjunto de datos y seleccione **agrupaciones de aprovisionamiento/recursos**.

   La ventana Edit Dataset muestra una configuración de la política de aprovisionamiento predeterminada y una lista de pools de recursos disponibles.

6. Para este ejemplo, seleccione el pool de recursos **p01_backup_resource** y haga clic en **>**.

   El pool de recursos seleccionado aparece en el campo "Pools de recursos para este nodo".

7. Haga clic en **Finalizar** para guardar los cambios.

resultado

Protection Manager aprovisiona automáticamente el nodo de copia de seguridad secundario con recursos del pool de recursos paydb_backup_resource.

Use SnapManager para SAP para crear un backup protegido

Al crear un backup para este ejemplo, el administrador de bases de datos selecciona la creación de un backup completo, define las opciones de backup y selecciona la protección para el almacenamiento secundario. Si bien el backup se realiza inicialmente en el almacenamiento local, ya que este backup se basa en un perfil con protección habilitada, el backup se transfiere luego al almacenamiento secundario según la programación de la política de protección definida en Protection Manager.

Pasos

1. Acceda al cliente de SnapManager para SAP.
2. En el árbol del repositorio de SnapManager, 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**.

   Se iniciará el Asistente para copia de seguridad de SnapManager para SAP.

3. Introduzca

   `Production_payroll`

   como etiqueta.

4. Introduzca

   `Production payroll Jan 19 backup`

   como comentario.

5. Seleccione **Auto** como el tipo de copia de seguridad que desea crear.

   Esto permite a SnapManager determinar si se debe realizar un backup en línea o sin conexión.

6. Seleccione **Diario** o **Semanal** como la frecuencia de la copia de seguridad.
7. Para confirmar que la copia de seguridad tiene un formato válido para Oracle, marque la casilla junto a **verificar copia de seguridad**.

   Esta operación utiliza Oracle DBVerify para comprobar el formato de bloque y la estructura.

8. Para forzar el estado de la base de datos al modo apropiado (por ejemplo, de abierto a montado), seleccione **permitir inicio o cierre de la base de datos, si es necesario**, y haga clic en **Siguiente**.
9. En la página Database, Tablespaces o Datafiles to Backup, seleccione **Full Backup** y haga clic en **Next**.
10. Para proteger la copia de seguridad en almacenamiento secundario, seleccione **proteger la copia de seguridad** y haga clic en **Siguiente**.

11. En la página realizar operación, compruebe la información suministrada y haga clic en **copia de seguridad**.
12. En la página Progress, consulte el progreso y los resultados de la creación de backup.
13. Para ver los detalles de la operación, haga clic en **Detalles de la operación**.

Utilice SnapManager para SAP para confirmar la protección del backup

Con SnapManager para SAP, se puede ver una lista de backups asociados a un perfil, determinar si los backups estaban habilitados para la protección y ver la clase de retención (diaria o semanal, en este ejemplo).

Acerca de esta tarea

Al principio, el nuevo backup en este ejemplo se muestra como programado para la protección, pero no está protegido aún (en la interfaz gráfica de usuario de SnapManager y en el resultado del comando backup show). Una vez que el administrador de almacenamiento garantiza que el backup se haya copiado al almacenamiento secundario, SnapManager cambia el estado de protección de backup de "no protegido" a "protegido" en la interfaz gráfica de usuario y con el comando backup list.

1. Acceda al cliente de SnapManager para SAP.
2. En el árbol del repositorio de SnapManager, expanda el perfil para mostrar sus copias de seguridad.
3. Haga clic en la ficha **copias de seguridad/clones**.
4. En el panel Informes, seleccione **Detalles de copia de seguridad**.
5. Consulte la columna Protection y asegúrese de que el estado sea "Protected".