SAP HANA en Amazon FSX para ONTAP de NetApp: Backup y recuperación con SnapCenter

NetApp Solutions SAP

NetApp
March 11, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions-sap/backup/amazon-fsx-overview.html on March 11, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

SAP HANA en Amazon FSX para ONTAP de NetApp: Backup y recuperación con SnapCenter 1
TR-4926: SAP HANA en Amazon FSX para ONTAP de NetApp: Backup y recuperación de datos con SnapCenter 1
Backup y recuperación de datos mediante Amazon FSX para ONTAP 1
Arquitectura SnapCenter 6
Configuración de SnapCenter 12
Operaciones de backup de SnapCenter 28
Backup de volúmenes que no sean de datos 38
Replicación de backups con SnapVault 53
Dónde encontrar información adicional 67

SAP HANA en Amazon FSX para ONTAP de NetApp: Backup y recuperación con SnapCenter

TR-4926: SAP HANA en Amazon FSX para ONTAP de NetApp: Backup y recuperación de datos con SnapCenter

Nils Bauer: NetApp

Este informe técnico proporciona las mejores prácticas para la protección de datos de SAP HANA en Amazon FSX para ONTAP de NetApp y SnapCenter de NetApp. Este documento abarca conceptos de SnapCenter, recomendaciones de configuración y flujos de trabajo de operaciones, incluidos la configuración, las operaciones de backup y operaciones de restauración y recuperación.

Las empresas requieren hoy en día una disponibilidad continua e ininterrumpida para sus aplicaciones SAP. Esperan niveles de rendimiento constantes frente al creciente volumen de datos, así como la necesidad de realizar tareas de mantenimiento rutinarias, como los backups del sistema. La realización de backups de bases de datos SAP es una tarea crucial y puede tener un efecto significativo en el rendimiento del sistema SAP de producción.

Los períodos definidos para los procesos de backup se reducen, mientras que la cantidad total de datos objeto de backup es cada vez mayor. Por lo tanto, es difícil encontrar una hora en la que se pueden realizar backups con un efecto mínimo en los procesos empresariales. El tiempo necesario para restaurar y recuperar los sistemas SAP es una preocupación, ya que deben minimizarse el tiempo de inactividad para la producción SAP y los sistemas que no son de producción para reducir los costes empresariales.

Backup y recuperación de datos mediante Amazon FSX para ONTAP

Es posible utilizar la tecnología Snapshot de NetApp para crear backups de bases de datos en cuestión de minutos.

El tiempo necesario para crear una copia Snapshot es independiente del tamaño de la base de datos porque la copia Snapshot no mueve bloques de datos físicos en la plataforma de almacenamiento. Además, el uso de la tecnología Snapshot no afecta al rendimiento del sistema SAP en vivo. Por tanto, puede programar la creación de copias Snapshot sin tener en cuenta los períodos de actividad en lote o con picos de carga. SAP y los clientes de NetApp suelen programar varios backups Snapshot en línea durante el día; por ejemplo, cada seis horas es habitual. Estos backups Snapshot suelen conservarse de tres a cinco días en el sistema de almacenamiento primario antes de quitarse o organizar en niveles el almacenamiento más barato para retenerlos a largo plazo.

Las copias Snapshot también proporcionan ventajas importantes para las operaciones de recuperación y restauración. La tecnología SnapRestore de NetApp permite la restauración de una base de datos completa o, como alternativa, solo una parte de una base de datos a un momento específico, según las copias Snapshot disponibles actualmente. Estos procesos de restauración se completan en pocos segundos, independientemente del tamaño de la base de datos. Debido a que pueden crearse varios backups Snapshot online durante el día, el tiempo necesario para el proceso de recuperación se reduce significativamente en comparación con el método de backup tradicional una vez al día. Dado que puede realizar una restauración con una copia Snapshot que tenga como máximo unas pocas horas de antigüedad (en lugar de hasta 24 horas), deben aplicarse menos registros de transacciones durante la recuperación futura. Por lo tanto, el RTO se reduce a varios minutos en lugar de las varias horas necesarias para los backups por streaming

convencionales.

Los backups de copias snapshot se almacenan en el mismo sistema de disco que los datos activos en línea. Por ello, NetApp recomienda utilizar los backups de copias snapshot como suplemento en lugar de como sustituto para los backups en una ubicación secundaria. La mayoría de las acciones de restauración y recuperación se gestionan usando SnapRestore en el sistema de almacenamiento principal. Solo son necesarias las restauraciones desde una ubicación secundaria si el sistema de almacenamiento primario que contiene las copias snapshot está dañado. También puede usar la ubicación secundaria si es necesario restaurar un backup que ya no esté disponible en la ubicación principal.

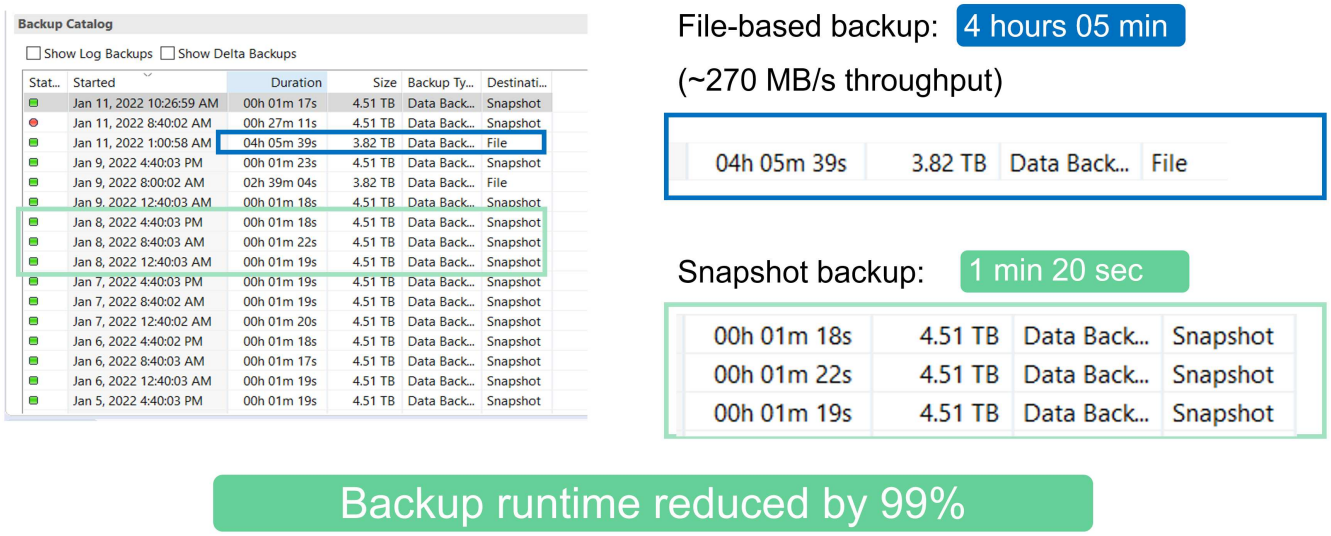
Un backup en una ubicación secundaria se basa en las copias Snapshot creadas en el almacenamiento principal. Por tanto, los datos se leen directamente desde el sistema de almacenamiento primario sin generar carga en el servidor de bases de datos SAP. El almacenamiento primario se comunica directamente con el almacenamiento secundario y replica los datos de backup en el destino mediante la función SnapVault de NetApp.

SnapVault ofrece ventajas significativas en comparación con los backups tradicionales. Tras una transferencia de datos inicial, en la que se transfieren todos los datos del origen al destino, en las copias posteriores de solo se mueven los bloques modificados al almacenamiento secundario. Por tanto, se reduce significativamente la carga del sistema de almacenamiento primario y el tiempo necesario para un backup completo. Como SnapVault almacena solo los bloques modificados en el destino, todos los backups adicionales de bases de datos completas consumen mucho menos espacio en disco.

Tiempo de ejecución de las operaciones de backup y restauración de Snapshot

La siguiente figura muestra HANA Studio de un cliente mediante operaciones de backup de Snapshot. La imagen muestra que se realiza un backup de la base de datos de HANA (con un tamaño aproximado de 4 TB) en 1 minuto y 20 segundos con la tecnología de backup de Snapshot y más de 4 horas con una operación de backup basada en archivos.

La parte más grande del tiempo de ejecución general del flujo de trabajo de backup es el tiempo necesario para ejecutar la operación de punto de guardado de backup de HANA, y este paso depende de la carga de la base de datos de HANA. El propio backup de los snapshots de almacenamiento siempre finaliza en un par de segundos.



Comparación de objetivos de tiempo de recuperación

Esta sección proporciona una comparación de objetivos de tiempo de recuperación (RTO) de backups de Snapshot basados en archivos y en almacenamiento. El objetivo de tiempo de recuperación se define con la suma del tiempo necesario para restaurar, recuperar e iniciar la base de datos.

Tiempo necesario para restaurar las bases de datos

Con un backup basado en archivos, el tiempo de restauración depende del tamaño de la infraestructura de backup y base de datos, que define la velocidad de restauración en megabytes por segundo. Por ejemplo, si la infraestructura admite una operación de restauración a una velocidad de 250 Mbps, se tarda aproximadamente 4.5 horas en restaurar una base de datos de 4 TB de tamaño en la persistencia.

Con los backups de copias de Snapshot de almacenamiento, el tiempo de restauración es independiente del tamaño de la base de datos y siempre está dentro del rango de un par de segundos.

Tiempo necesario para iniciar la base de datos

El tiempo de inicio de la base de datos depende del tamaño de la base de datos y del tiempo necesario para cargar los datos en la memoria. En los siguientes ejemplos, se supone que los datos se pueden cargar con 1000 Mbps. Cargar 4 TB en la memoria tarda aproximadamente 1 hora y 10 minutos. La hora de inicio es la misma para las operaciones de recuperación y restauración basadas en archivos y de Snapshot.

Tiempo necesario para recuperar las bases de datos

El tiempo de recuperación depende de la cantidad de registros que se deben aplicar después de la restauración. Este número viene determinado por la frecuencia con la que se realizan backups de datos.

Con los backups de datos basados en archivos, la programación de backup suele ser una vez al día. Por lo general, no es posible aumentar la frecuencia de backup, ya que el backup reduce el rendimiento de producción. Por lo tanto, en el peor de los casos, todos los registros que se escribieron durante el día deben aplicarse durante la recuperación de avance.

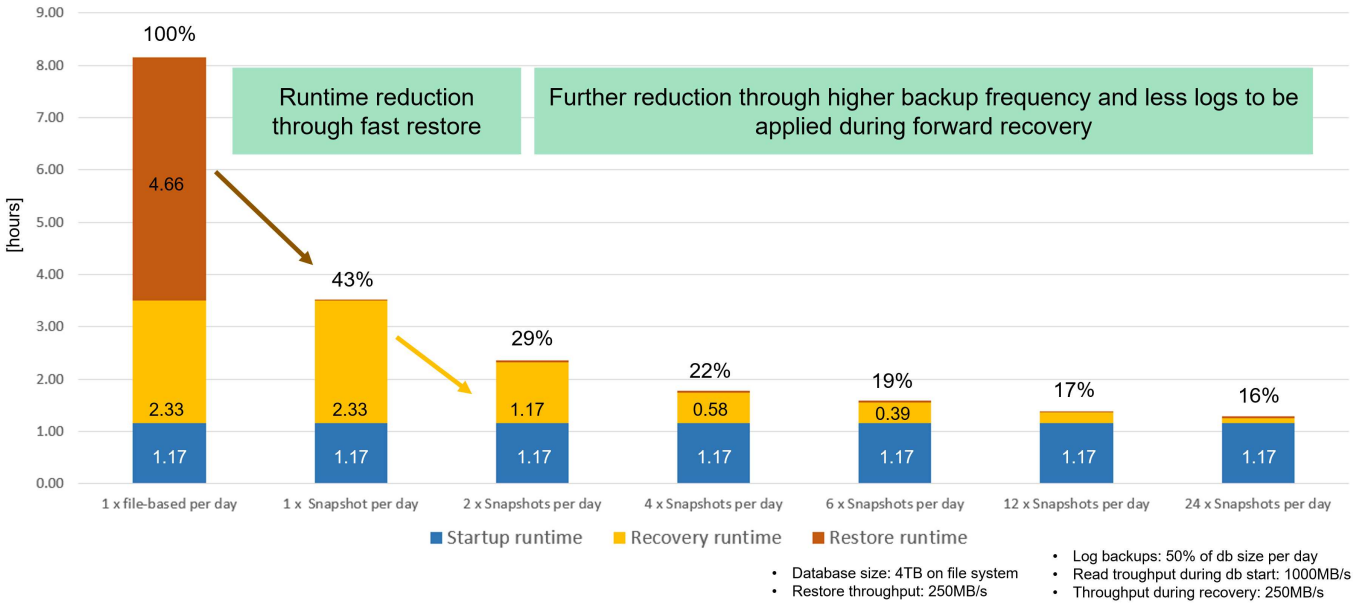
Los backups de snapshots normalmente se programan con una mayor frecuencia debido a que no influyen en el rendimiento de la base de datos de SAP HANA. Por ejemplo, si los backups de Snapshot se programan cada seis horas, el tiempo de recuperación sería, en el peor de los casos, la cuarta parte del tiempo de recuperación de un backup basado en archivos (6 horas / 24 horas = 25).

La siguiente figura muestra una comparación de las operaciones de restauración y recuperación con un backup diario basado en archivos y backups de Snapshot con diferentes programaciones.

Las dos primeras barras muestran que, incluso con un único backup de Snapshot al día, la restauración y la recuperación se reducen al 43% debido a la velocidad de la operación de restauración desde un backup de Snapshot. Si se crean varios backups Snapshot diarios, es posible reducir más el tiempo de ejecución, ya que es necesario aplicar menos registros durante la recuperación futura.

La siguiente figura también muestra que tiene más sentido realizar entre cuatro y seis backups Snapshot al día, ya que una mayor frecuencia ya no tiene una gran influencia en el tiempo de ejecución general.

Restore and Recovery of a 4TB HANA Database (8TB RAM)



Casos de uso y valores de operaciones de backup y clonado aceleradas

La ejecución de backups es una parte fundamental de cualquier estrategia de protección de datos. Las copias de seguridad se programan regularmente para garantizar que puede recuperarse de fallos del sistema. Este es el caso de uso más obvio, pero también hay otras tareas de gestión del ciclo de vida de SAP, en las que acelerar las operaciones de backup y recuperación es decisivo.

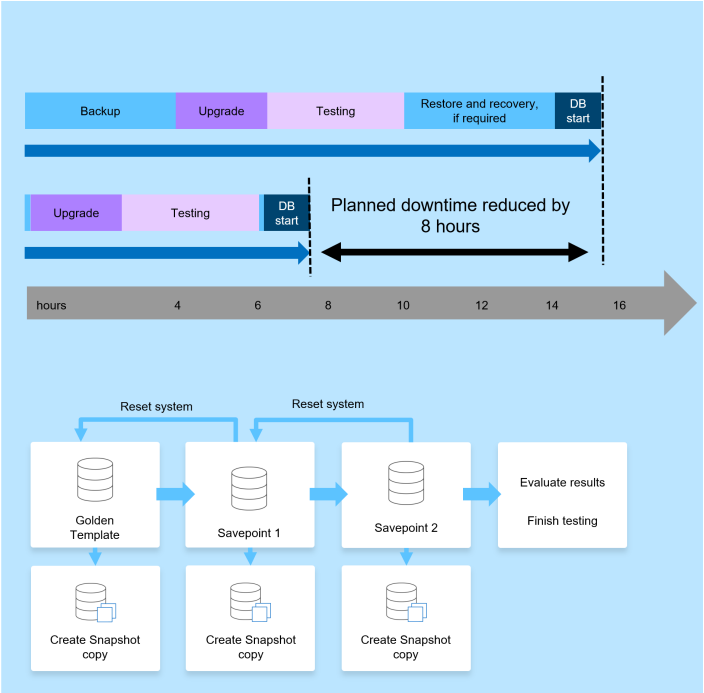
La actualización del sistema SAP HANA es un ejemplo de dónde un backup bajo demanda antes de la actualización y una posible operación de restauración si falla la actualización tiene un impacto significativo en el tiempo de inactividad general planificado. Con el ejemplo de una base de datos de 4 TB, es posible reducir el tiempo de inactividad planificado en 8 horas gracias a las operaciones de backup y restauración basadas en Snapshot.

Otro ejemplo de caso de uso sería un ciclo de prueba típico, en el que las pruebas deben realizarse en varias iteraciones con conjuntos de datos o parámetros diferentes. Al aprovechar las operaciones rápidas de backup y restauración, se pueden crear fácilmente puntos de guardado en el ciclo de pruebas y restablecer el sistema a cualquiera de estos puntos de guardado anteriores si falla una prueba o es necesario repetirla. Esto permite que las pruebas finalicen antes o permite realizar más pruebas al mismo tiempo y mejorar los resultados de las pruebas.

Use Cases for Backup and Recovery Operations

- Accelerate HANA system upgrade operations
  - Fast on-demand backup before HANA system upgrade
  - Fast restore operation in case of an upgrade failure
  - Reduction of planned downtime

- Acclerate test cycles
  - Fast creation of savepoints after a successful step
  - Fast reset of system to any savepoint
  - Repeat step until successful



Cuando se han implementado backups de Snapshot, pueden utilizarse para abordar varios otros casos prácticos, los cuales requieren copias de una base de datos HANA. Con FSX para ONTAP, puede crear un volumen nuevo basado en el contenido de cualquier backup de Snapshot disponible. El tiempo de ejecución de esta operación es de unos segundos, independientemente del tamaño del volumen.

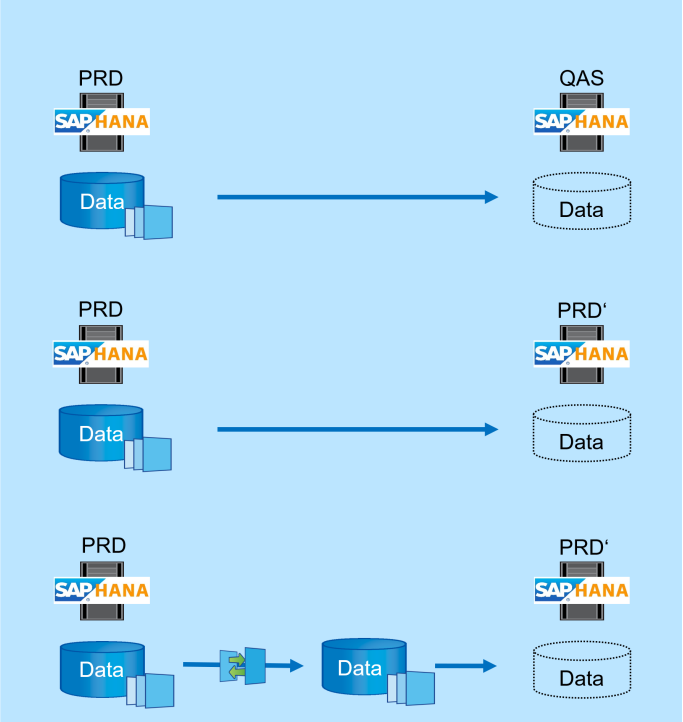
El caso de uso más popular es la actualización de sistemas SAP, donde los datos del sistema de producción deben copiarse al sistema de prueba o control de calidad. Al aprovechar la función de clonación de FSX para ONTAP, puede aprovisionar el volumen para el sistema de prueba desde cualquier copia Snapshot del sistema de producción en cuestión de segundos. A continuación, el volumen nuevo se debe asociar al sistema de prueba y la base de datos HANA recuperada.

El segundo caso de uso es la creación de un sistema de reparación, que se utiliza para abordar un daño lógico en el sistema de producción. En este caso, se utiliza un backup de Snapshot anterior del sistema de producción para iniciar un sistema de reparación, que es un clon idéntico del sistema de producción con los datos antes de que se produjera el daño. El sistema de reparación se utiliza para analizar el problema y exportar los datos necesarios antes de que se dañara.

El último caso de uso es la capacidad de ejecutar una prueba de conmutación al nodo de respaldo de recuperación ante desastres sin detener la replicación y, por lo tanto, sin influir en el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación del ajuste de recuperación ante desastres. Cuando se usa FSX para la replicación de SnapMirror de NetApp de ONTAP para replicar los datos en el centro de recuperación ante desastres, los backups Snapshot de producción están disponibles también en el centro de recuperación ante desastres y se pueden usar para crear un nuevo volumen para la prueba de la recuperación ante desastres.

Use Cases for Cloning Operations

- SAP System Refresh
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the test system and recover HANA database with SID change
- Repair System creation to address logical corruption
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the repair system and recover HANA database w/o SID change
- Disaster Recovery testing
  - Combined with SnapMirror Replication
  - Attach storage clone from a replicated production Snapshot backup to a DR test system



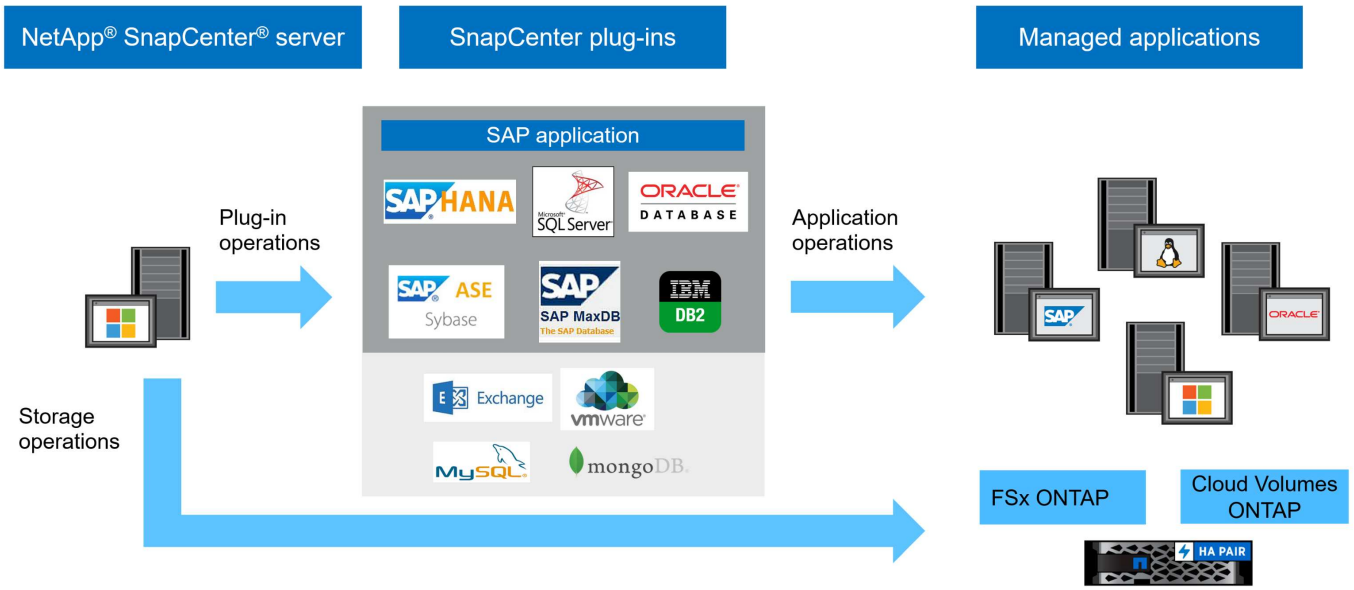
Arquitectura SnapCenter

SnapCenter es una plataforma unificada y escalable destinada a la protección de datos coherente con las aplicaciones. SnapCenter proporciona control y supervisión centralizados, a la vez que delega la capacidad para que los usuarios gestionen trabajos de backup, restauración y clonado específicos de aplicaciones. Con SnapCenter, los administradores de bases de datos y almacenamiento conocen una única herramienta para gestionar los backups, las restauraciones de datos y las operaciones de clonado para diferentes aplicaciones y bases de datos.

SnapCenter gestiona los datos a través de terminales en el Data Fabric con la tecnología de NetApp. Puede utilizar SnapCenter para replicar datos entre entornos locales, entre entornos locales y el cloud y entre clouds privados, híbridos o públicos.

Componentes de SnapCenter

SnapCenter incluye el servidor SnapCenter, el paquete de plugins de SnapCenter para Windows y el paquete de plugins de SnapCenter para Linux. Cada paquete contiene complementos de SnapCenter para diferentes aplicaciones y componentes de la infraestructura.



Solución de backup SAP HANA de SnapCenter

La solución de backup SnapCenter para SAP HANA cubre las siguientes áreas:

- Gestión de las operaciones de backup, programación y retención
  - Backup de datos de SAP HANA con copias de SnapVault basadas en almacenamiento
  - Backup de volúmenes sin datos con copias Snapshot basadas en el almacenamiento (por ejemplo, `/hana/shared`)
  - Comprobaciones de integridad de bloques de bases de datos mediante un backup basado en archivos
  - Replicación en una ubicación de backup o recuperación ante desastres externa
- Mantenimiento del catálogo de backup de SAP HANA
  - Para backups de datos de HANA (Snapshot y basados en archivos)
  - Para backups de registros de HANA
- Operaciones de restauración y recuperación
  - Restauración y recuperación automatizadas
  - Operaciones de restauración de un solo inquilino para sistemas SAP HANA (MDC)

SnapCenter ejecuta los backups de archivos de datos de bases de datos junto con un plugin para SAP HANA. El complemento activa el punto de guardado de backup de base de datos SAP HANA, de forma que las copias Snapshot, que se crean en el sistema de almacenamiento principal, se basen en una imagen consistente de la base de datos SAP HANA.

SnapCenter permite la replicación de imágenes de bases de datos consistentes en una ubicación de backup o recuperación ante desastres externa mediante SnapVault o la función SnapMirror. Normalmente, las distintas políticas de retención se definen para backups en el almacenamiento principal y en el almacenamiento de backup externo. SnapCenter se ocupa de la retención en el almacenamiento principal y ONTAP se ocupa de la retención en el almacenamiento de backup externo.

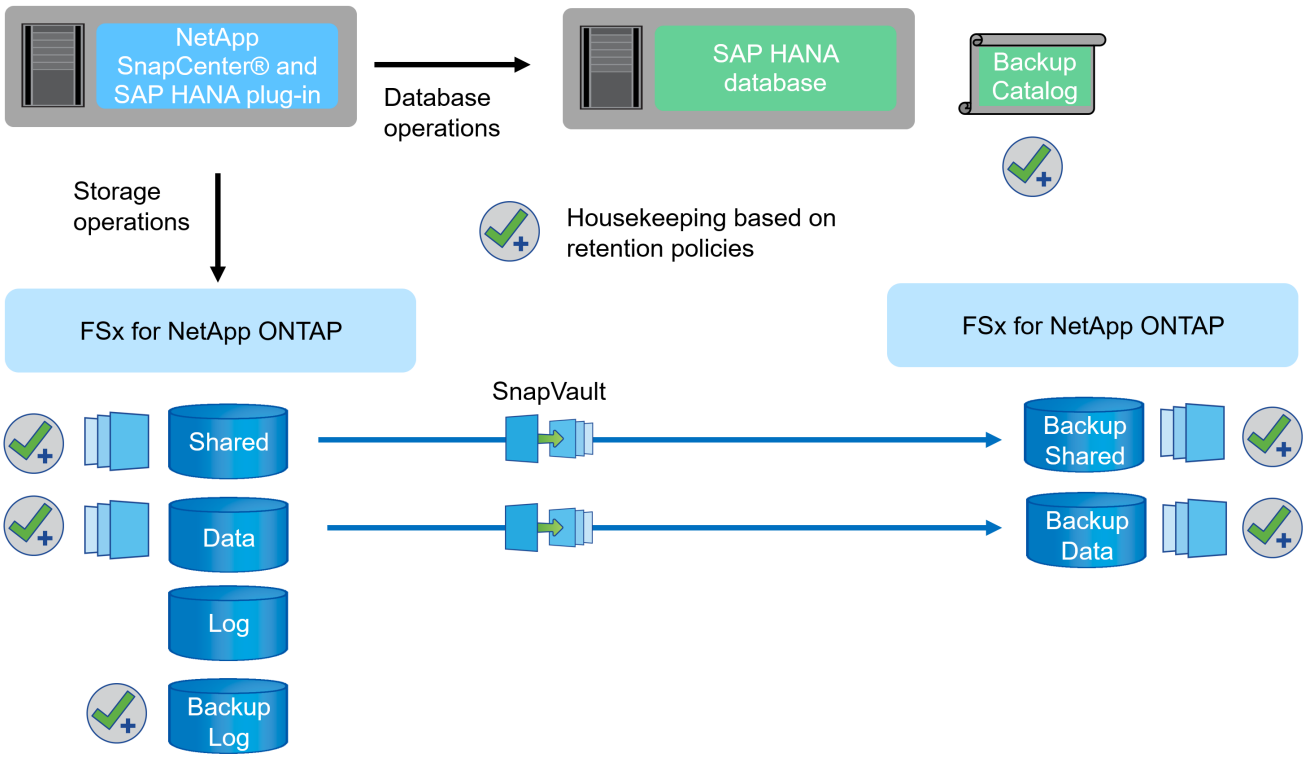
Para permitir un backup completo de todos los recursos relacionados con SAP HANA, SnapCenter también le permite realizar un backup de todos los volúmenes que no son datos mediante el plugin de SAP HANA con copias de Snapshot basadas en el almacenamiento. Puede programar volúmenes que no sean de datos

independientemente del backup de datos de la base de datos para habilitar políticas de retención y protección individuales.

SAP recomienda combinar backups de SnapVault basados en almacenamiento con un backup basado en archivos semanal para ejecutar una comprobación de la integridad de los bloques. Puede ejecutar la comprobación de integridad de bloques desde SnapCenter. Según las políticas de retención configuradas, SnapCenter gestiona el mantenimiento de los backups de archivos de datos en el almacenamiento principal, los backups de archivos de registro y el catálogo de backup SAP HANA.

SnapCenter se encarga de la retención en el almacenamiento principal, mientras que FSX para ONTAP gestiona la retención de backup secundario.

En la siguiente figura, se muestra una descripción general de las operaciones de gestión de backup y retención de SnapCenter.



Al ejecutar un backup de Snapshot basado en el almacenamiento de la base de datos SAP HANA, SnapCenter realiza las siguientes tareas:

1. Crea un punto de guardado de copia de seguridad de SAP HANA para crear una imagen consistente en la capa de persistencia.
2. Crea una copia de Snapshot basada en el almacenamiento del volumen de datos.
3. Registra el backup de Snapshot basado en el almacenamiento en el catálogo de backup de SAP HANA.
4. Lanza el punto de guardado de backup de SAP HANA.
5. Ejecuta una actualización de SnapVault o SnapMirror para el volumen de datos, si se ha configurado.
6. Elimina las copias snapshot de almacenamiento en el almacenamiento principal en función de las políticas de retención definidas.
7. Elimina las entradas del catálogo de backup SAP HANA si los backups ya no existen en el almacenamiento de backup principal o externo.

8. Cada vez que se elimina un backup en función de la política de retención o de forma manual, SnapCenter también elimina todos los backups de registros más antiguos que el backup de datos más antiguo. Los backups de registros se eliminan en el sistema de archivos y en el catálogo de backup SAP HANA.

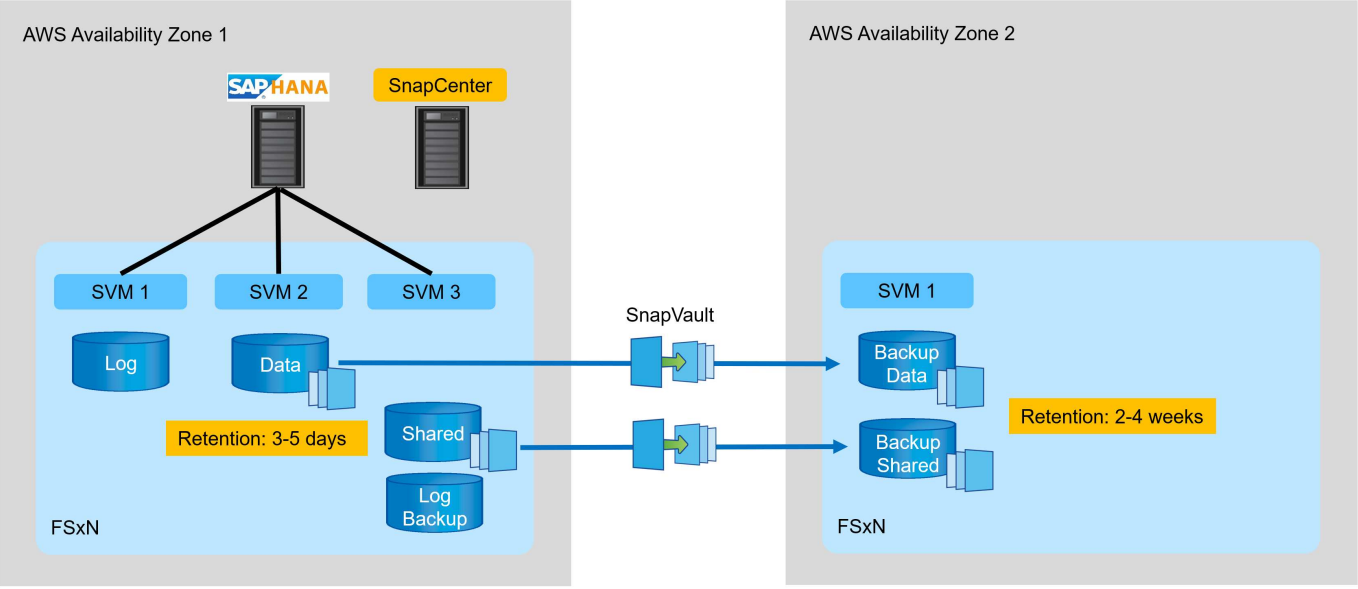
Alcance de este documento

Este documento describe la opción de configuración de SnapCenter más común para un sistema de host único de SAP HANA MDC con un único inquilino en FSX para ONTAP. En algunos casos, se pueden utilizar otras opciones de configuración como las necesarias para sistemas SAP HANA específicos, por ejemplo, para un sistema host múltiple. Para obtener una descripción detallada de otras opciones de configuración, consulte "Conceptos y prácticas recomendadas de SnapCenter (netapp.com)".

En este documento, utilizamos la consola de Amazon Web Services (AWS) y la interfaz de línea de comandos FSX para ONTAP para ejecutar los pasos de configuración necesarios en la capa de almacenamiento. También puede utilizar Cloud Manager de NetApp para gestionar FSX para ONTAP, pero este documento no está dentro del alcance. Para obtener información sobre el uso de Cloud Manager de NetApp para FSX para ONTAP, consulte "Más información acerca de Amazon FSX para ONTAP (netapp.com)".

Estrategia de protección de datos

La siguiente figura muestra una arquitectura de backup típica para SAP HANA en FSX para ONTAP. El sistema HANA se encuentra en la zona de disponibilidad 1 de AWS y utiliza un FSX para el sistema de archivos ONTAP dentro de la misma zona de disponibilidad. Se ejecutan las operaciones de backup de Snapshot para los datos y el volumen compartido de la base de datos de HANA. Además de los backups de Snapshot locales, que se conservan durante 3-5 días, los backups también se replican en un almacenamiento externo para su retención a largo plazo. El almacenamiento de backup externo es un segundo FSX para el sistema de archivos ONTAP ubicado en una zona de disponibilidad de AWS diferente. Los backups de los datos de HANA y el volumen compartido se replican con SnapVault al segundo FSX para el sistema de archivos ONTAP y se mantienen durante 2-3 semanas.



Antes de configurar SnapCenter, debe definirse la estrategia de protección de datos en función de los requisitos de objetivo de tiempo de recuperación y objetivo de punto de recuperación de los distintos sistemas SAP.

Un enfoque común es definir tipos de sistemas como sistemas de producción, desarrollo, pruebas o entornos de pruebas. Normalmente, todos los sistemas SAP del mismo tipo tienen los mismos parámetros de

protección de datos.

Deben definirse los siguientes parámetros:

- ¿Con qué frecuencia se debería ejecutar un backup de Snapshot?
- ¿Cuánto tiempo se deberían conservar los backups de copias snapshot en el sistema de almacenamiento principal?
- ¿Con qué frecuencia se debe ejecutar una comprobación de integridad de bloque?
- ¿Deberían replicarse los principales backups en una ubicación de backup externa?
- ¿Cuánto tiempo deberían guardarse los backups en el almacenamiento de backups externo?

En la siguiente tabla se muestra un ejemplo de parámetros de protección de datos para los tipos del sistema: Producción, desarrollo y pruebas. Para el sistema de producción se ha definido una alta frecuencia de backups, y los backups se replican en un centro de backup externo una vez al día. Los sistemas de prueba tienen menos requisitos y no tienen replicación de backups.

Parámetros	Sistemas de producción	Sistemas de desarrollo	Pruebas de sistemas
Frecuencia de backup	Cada 6 horas	Cada 6 horas	Cada 6 horas
Retención primaria	3 días	3 días	3 días
Comprobación de integridad de bloques	Una vez a la semana	Una vez a la semana	No
Replicación en centro de backup externo	Una vez al día	Una vez al día	No
Retención de backups fuera de las instalaciones	2 semanas	2 semanas	No aplicable

En la siguiente tabla, se muestran las políticas que deben configurarse para los parámetros de protección de datos.

Parámetros	Policy LocalSnap	Policy LocalSnapAndSnapVault	Política BlockIntegrityCheck
Tipo de backup	Basado en Snapshot	Basado en Snapshot	Basado en archivos
Frecuencia de programación	Cada hora	Todos los días	Semanal
Retención primaria	Recuento = 12	Recuento = 3	Recuento = 1
Replicación SnapVault	No	Sí	No aplicable

La política `LocalSnapshot` Se usa para los sistemas de producción, desarrollo y prueba para cubrir los backups locales de Snapshot con una retención de dos días.

En la configuración de protección de recursos, la programación se define de forma diferente para los tipos de sistema:

- Producción: Horario cada 4 horas.
- Desarrollo: Programación cada 4 horas.

- Prueba: Programe cada 4 horas.

La política `LocalSnapAndSnapVault` se utiliza en los sistemas de producción y desarrollo para cubrir la replicación diaria al almacenamiento de backup externo.

En la configuración de protección de recursos, la programación se define para producción y desarrollo:

- Producción: Programa todos los días.
- Desarrollo: Programa todos los días.la política `BlockIntegrityCheck` se utiliza para los sistemas de producción y desarrollo a fin de abarcar la comprobación semanal de la integridad de los bloques mediante un backup basado en archivos.

En la configuración de protección de recursos, la programación se define para producción y desarrollo:

- Producción: Programa cada semana.
- Desarrollo: Programa cada semana.

Para cada base de datos SAP HANA individual que utilice la política de backup externa, debe configurar una relación de protección en la capa de almacenamiento. La relación de protección define qué volúmenes se replican y la retención de los backups en el almacenamiento de backup externo.

Con el siguiente ejemplo, para cada sistema de producción y desarrollo, se define una retención de dos semanas en el almacenamiento de backup externo.

En este ejemplo, las políticas de protección y la retención para los recursos de la base de datos SAP HANA y los recursos de volúmenes sin datos no son diferentes.

Configuración de ejemplo de laboratorio

La siguiente configuración de laboratorio se utilizó como configuración de ejemplo para el resto de este documento.

PFX de sistema HANA:

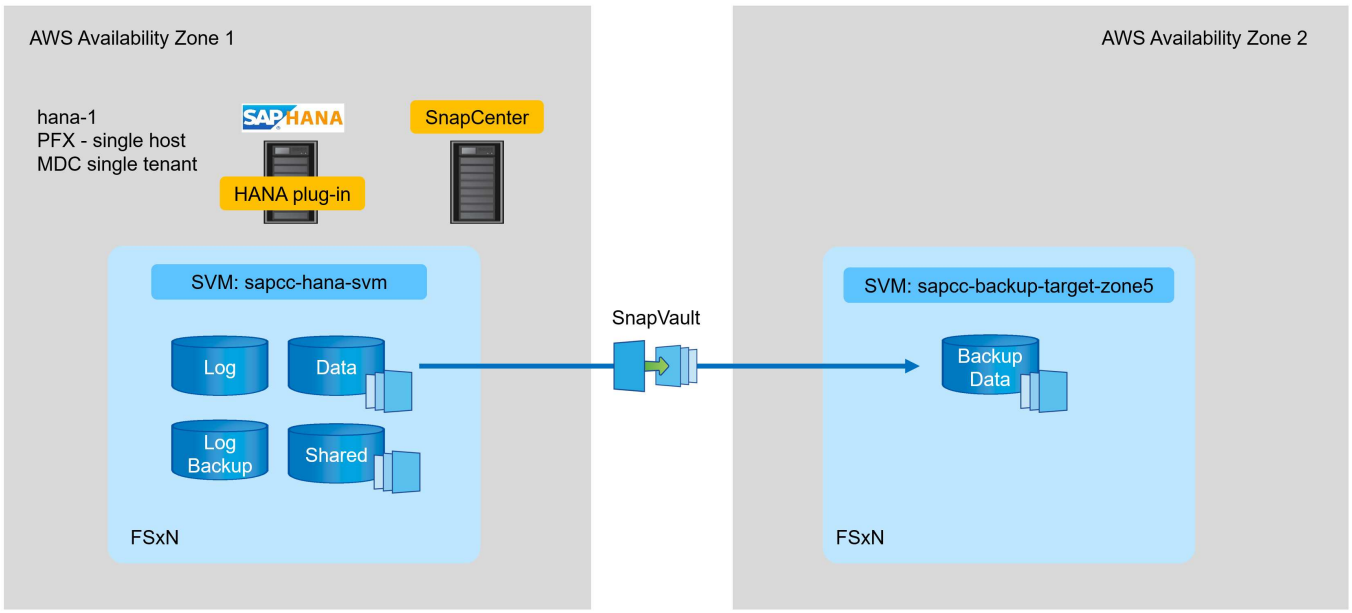
- Sistema MDC de host único con un único inquilino
- HANA 2.0 SPS 6 revisión 60
- SLES PARA SAP 15SP3

SnapCenter.:

- Versión 4.6
- HANA y el plugin de Linux implementados en un host de base de datos HANA

FSX para sistemas de archivos ONTAP:

- Dos FSX para sistemas de archivos ONTAP con una única máquina virtual de almacenamiento (SVM)
- Cada FSX para el sistema ONTAP en una zona de disponibilidad de AWS diferente
- Volumen de datos DE HANA replicado en el segundo FSX para el sistema de archivos ONTAP



Configuración de SnapCenter

Debe realizar los pasos de esta sección para establecer la configuración de SnapCenter base y la protección del recurso HANA.

Descripción general de los pasos de configuración

Debe realizar los siguientes pasos para la configuración base de SnapCenter y la protección del recurso HANA. Cada paso se describe detalladamente en los siguientes capítulos.

1. Configure el usuario de backup de SAP HANA y la clave hdbuserstore. Se utiliza para acceder a la base de datos HANA con el cliente hdbsql.
2. Configurar el almacenamiento en SnapCenter. Credenciales para acceder al FSX para las SVM de ONTAP desde SnapCenter
3. Configure credenciales para la implementación de plugins. Se utiliza para poner en marcha e instalar automáticamente los plugins de SnapCenter necesarios en el host de la base de datos de HANA.
4. Añada el host HANA a SnapCenter. Pone en marcha e instala los complementos de SnapCenter necesarios.
5. Configurar políticas. Define el tipo de operación de backup (Snapshot, archivo), retentions, así como la replicación de backup de Snapshot opcional.
6. Configure la protección de recursos de HANA. Proporcione la clave hdbuserstore y adjunte políticas y programaciones al recurso HANA.

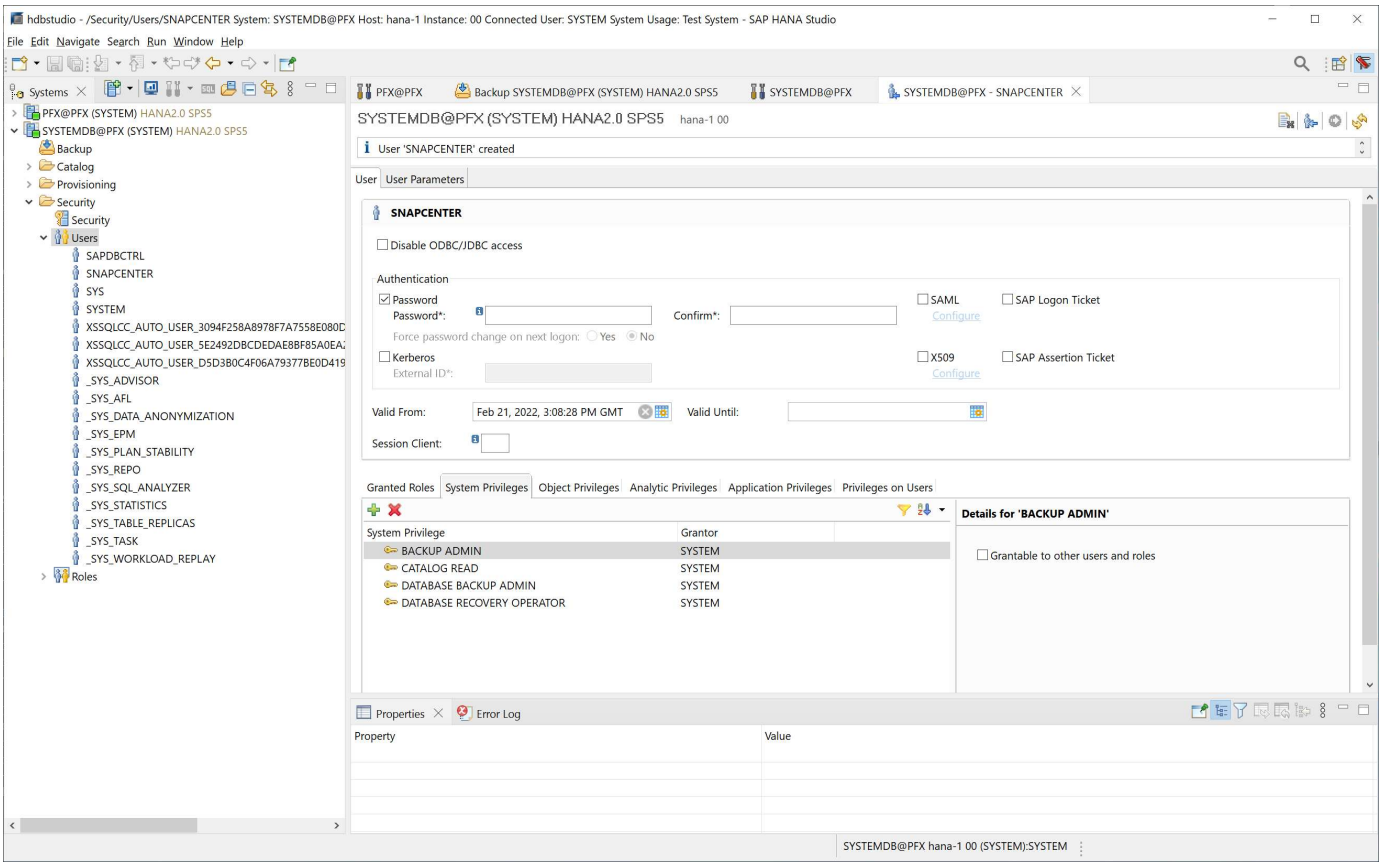
Usuario de backup de SAP HANA y configuración de hdbuserstore

NetApp recomienda configurar un usuario de base de datos dedicado en la base de datos de HANA para ejecutar las operaciones de backup con SnapCenter. En el segundo paso, hay una clave de almacenamiento de usuario SAP HANA configurada para este usuario de backup, y esta clave de almacenamiento de usuario se usa en la configuración del plugin SAP HANA de SnapCenter.

La figura siguiente muestra SAP HANA Studio a través del cual puede crear el usuario de backup

Los privilegios necesarios se cambian con la versión HANA 2.0 SPS5: Administrador de backup, lectura de catálogo, administrador de backup de bases de datos y operador de recuperación de bases de datos. En versiones anteriores, el administrador de backup y la lectura de catálogo son suficientes.

Para un sistema MDC de SAP HANA, debe crear el usuario en la base de datos del sistema porque todos los comandos de backup para el sistema y las bases de datos de tenant se ejecutan mediante la base de datos del sistema.



El siguiente comando se utiliza para la configuración del almacén de usuarios con el `<sid>adm` usuario:

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

SnapCenter utiliza la `<sid>adm` Usuario para comunicarse con la base de datos HANA. Por lo tanto, debe configurar la clave de almacenamiento de usuario mediante el usuario <smid>adm' del host de la base de datos. Normalmente, el software cliente hdbsql de SAP HANA se instala junto con la instalación del servidor de bases de datos. Si este no es el caso, primero debe instalar hdbclient.

En una configuración de SAP HANA MDC, Puerto `3<instanceNo>13` Es el puerto estándar para el acceso SQL a la base de datos del sistema y debe utilizarse en la configuración hdbuserstore.

Para una configuración de varios hosts de SAP HANA, debe configurar claves de almacenamiento de usuario para todos los hosts. SnapCenter intenta conectarse a la base de datos usando cada una de las claves proporcionadas y, por lo tanto, puede funcionar independientemente de la conmutación por error de un servicio SAP HANA a un host diferente. En nuestra configuración de laboratorio, configuramos una clave de almacenamiento de usuario para el usuario `pfxadm` Para nuestro sistema PFX, que es un solo sistema MDC de HANA host con un solo inquilino.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore set PFXKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore list
DATA FILE       : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.KEY
ACTIVE RECORDS  : 7
DELETED RECORDS : 0
KEY PFXKEY
  ENV : hana-1:30013
  USER: SNAPCENTER
KEY PFXSAPDBCTRL
  ENV : hana-1:30013
  USER: SAPDBCTRL
Operation succeed.
```

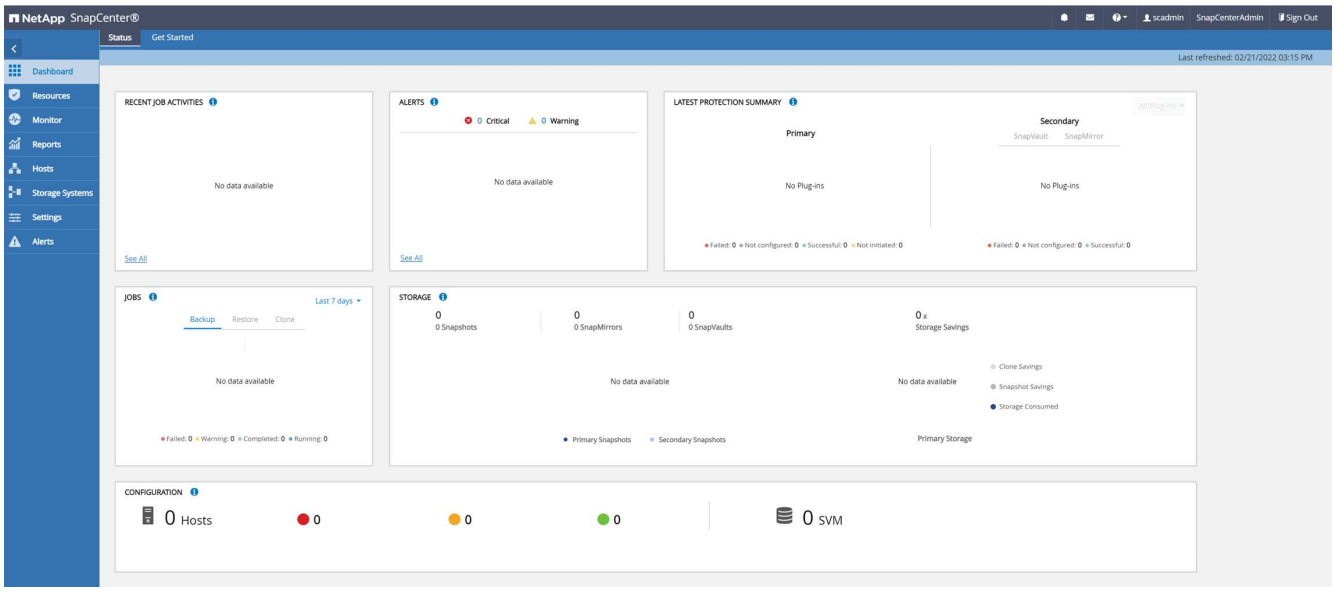
Puede comprobar el acceso a la base de datos del sistema HANA que utiliza la clave con el `hdbsql` comando.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbsql -U PFXKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=>
```

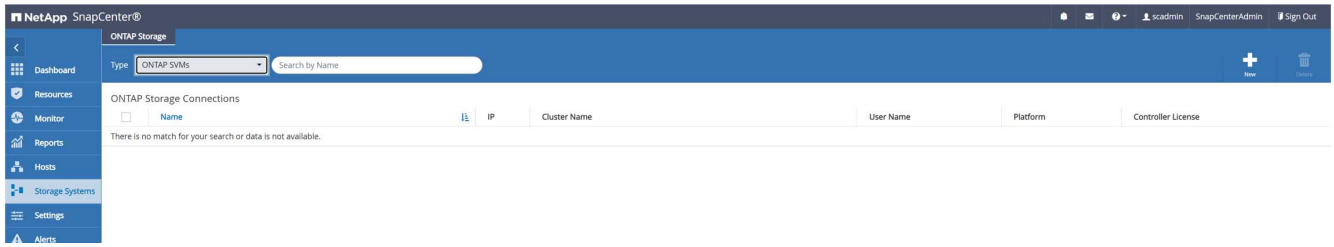
Configurar el almacenamiento

Siga estos pasos para configurar el almacenamiento en SnapCenter.

1. En la interfaz de usuario de SnapCenter, seleccione Storage Systems.

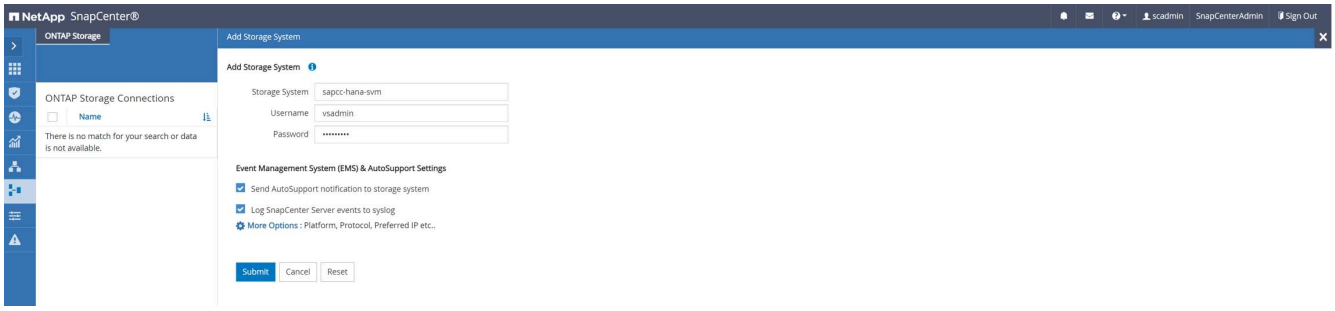


Puede seleccionar el tipo de sistema de almacenamiento que puede ser ONTAP SVM o ONTAP Clusters. En el ejemplo siguiente, se selecciona la gestión de SVM.

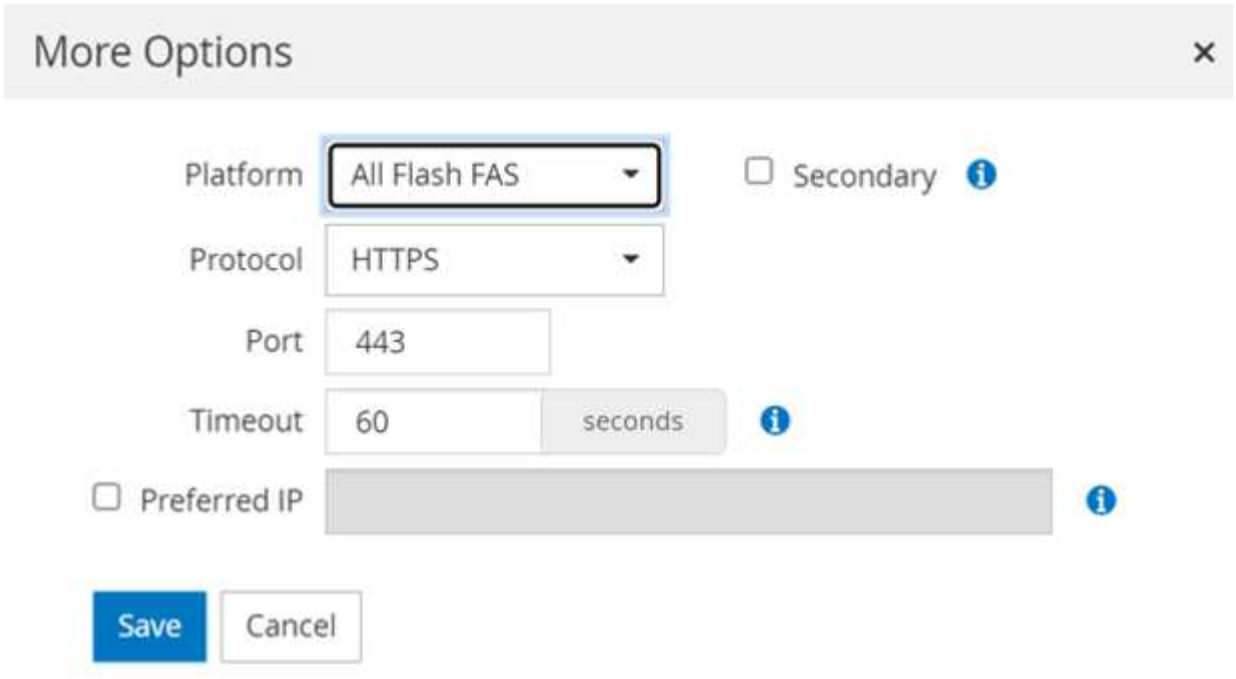


2. Para añadir un sistema de almacenamiento y proporcionar el nombre de host y las credenciales necesarios, haga clic en New.

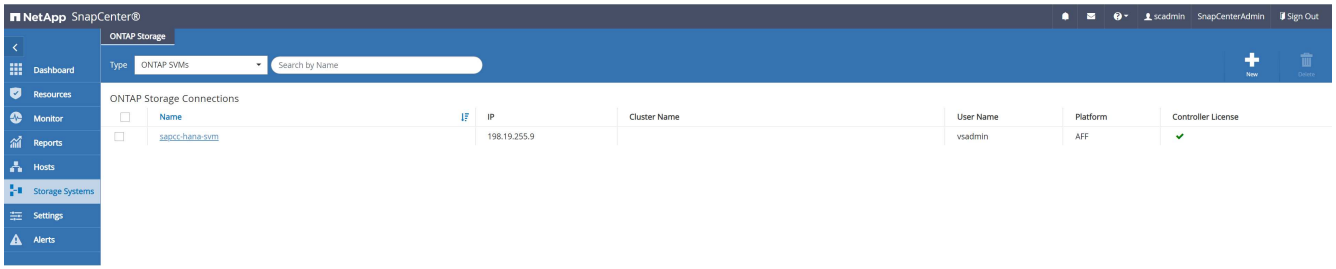
   No se requiere que el usuario de SVM sea el usuario de vsadmin, como se muestra en la siguiente figura. Generalmente, un usuario está configurado en la SVM y asignó los permisos necesarios para ejecutar operaciones de backup y restauración. Para obtener información sobre los privilegios necesarios, consulte "Guía de instalación de SnapCenter" En la sección titulada “privilegios mínimos de ONTAP requeridos”.



3. Para configurar la plataforma de almacenamiento, haga clic en más opciones.
4. Seleccione All Flash FAS como el sistema de almacenamiento para garantizar que la licencia, que forma parte de FSX para ONTAP, esté disponible para SnapCenter.



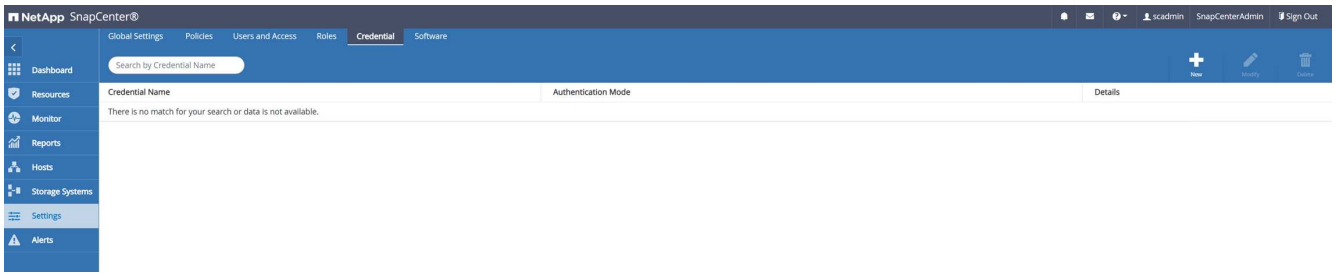
La SVM `sapcc-hana-svm` Ahora está configurado en SnapCenter.



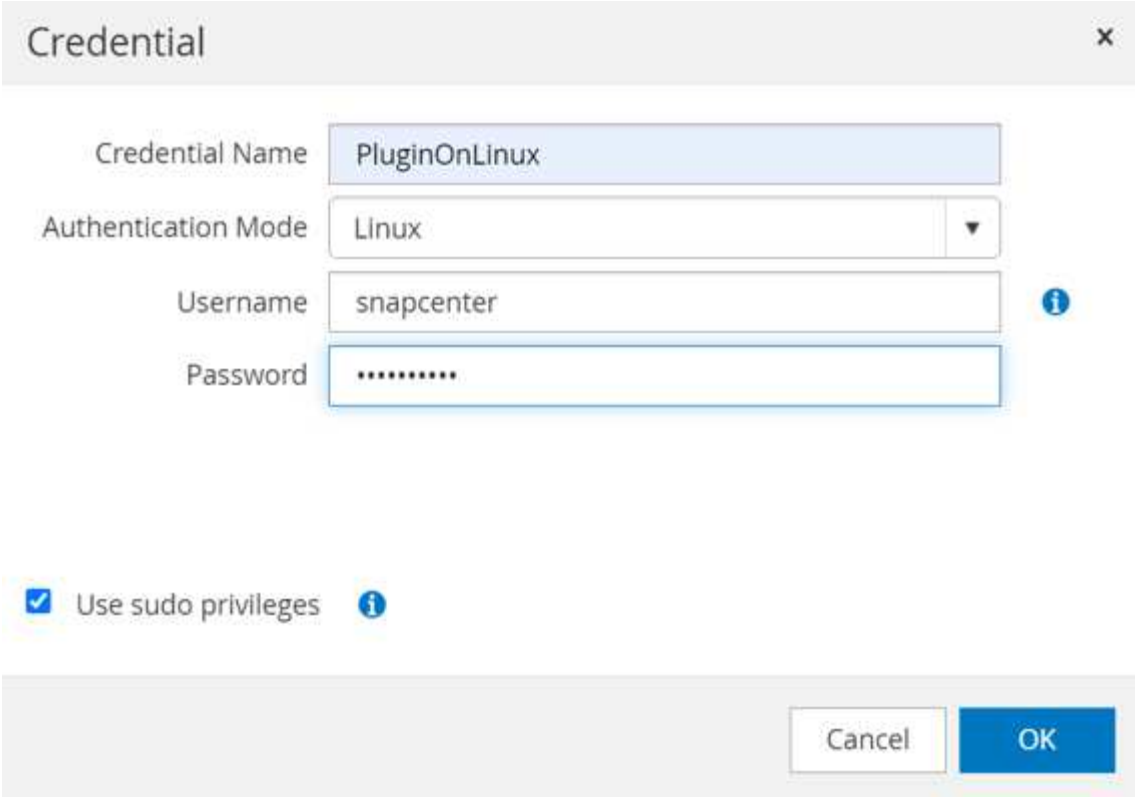
Crear credenciales para la implementación del plugin

Para habilitar SnapCenter a fin de implementar los plugins necesarios en los hosts de HANA, debe configurar las credenciales de usuario.

1. Vaya a Configuración, seleccione credenciales y haga clic en New.



2. En la configuración de laboratorio, configuramos un nuevo usuario, `snapcenter`, En el host HANA que se utiliza para la implementación del plugin. Debe habilitar sudo prvileges, como se muestra en la siguiente figura.




```
hana-1:/etc/sudoers.d # cat /etc/sudoers.d/90-cloud-init-users
# Created by cloud-init v. 20.2-8.48.1 on Mon, 14 Feb 2022 10:36:40 +0000
# User rules for ec2-user
ec2-user ALL=(ALL) NOPASSWD:ALL
# User rules for snapcenter user
snapcenter ALL=(ALL) NOPASSWD:ALL
hana-1:/etc/sudoers.d #
```

Añada un host SAP HANA

Cuando se añade un host de SAP HANA, SnapCenter implementa los plugins necesarios en el host de la base de datos y ejecuta las operaciones de detección automática.

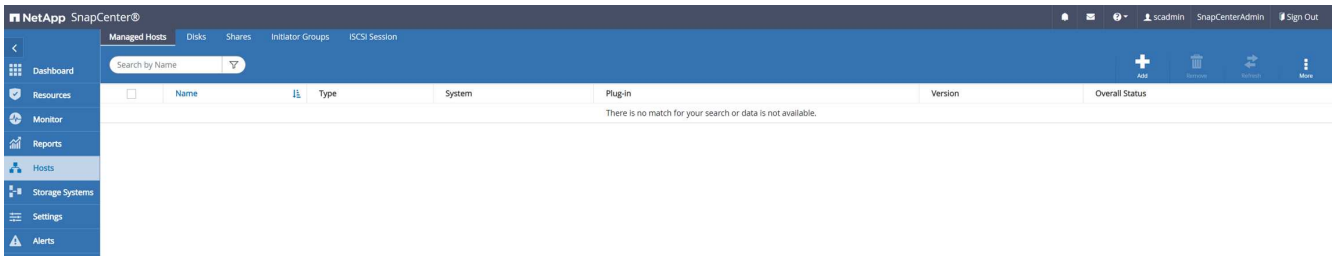
El plugin de SAP HANA requiere Java de 64 bits, versión 1.8. Debe instalarse Java en el host antes de que el host se añada a SnapCenter.

```
hana-1:/etc/ssh # java -version
openjdk version "1.8.0_312"
OpenJDK Runtime Environment (IcedTea 3.21.0) (build 1.8.0_312-b07 suse-
3.61.3-x86_64)
OpenJDK 64-Bit Server VM (build 25.312-b07, mixed mode)
hana-1:/etc/ssh #
```

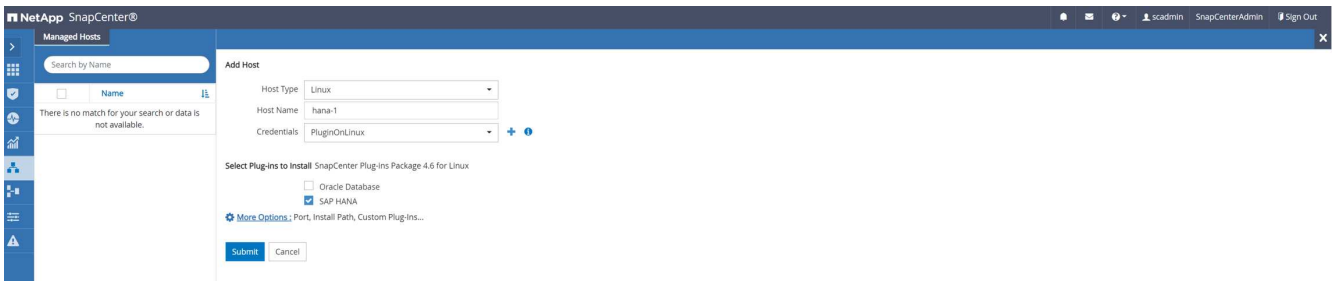
SnapCenter admite OpenJDK u Oracle Java.

Para añadir el host SAP HANA, siga estos pasos:

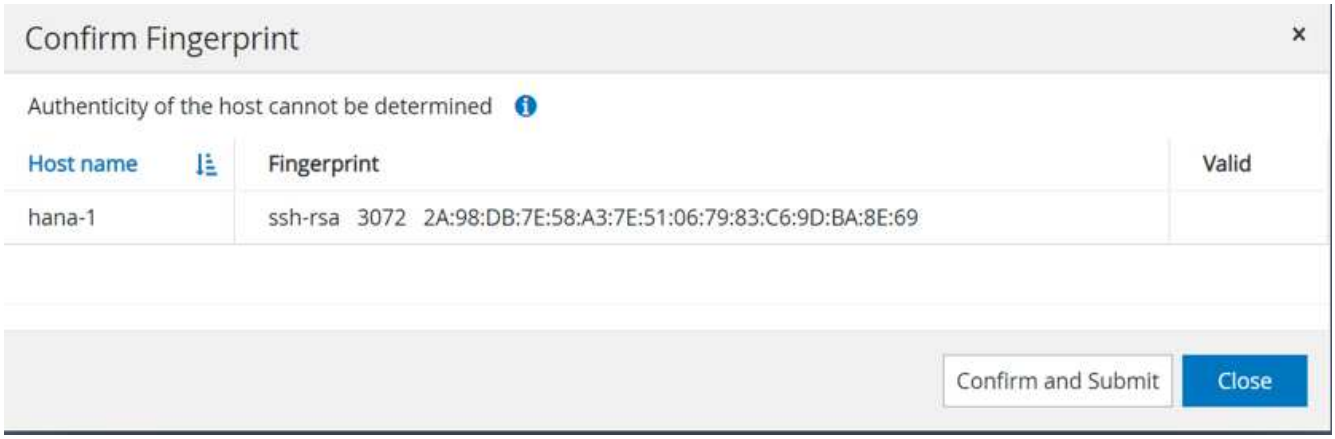
1. En la pestaña del host, haga clic en Add.



2. Proporcione información del host y seleccione el plugin de SAP HANA que se va a instalar. Haga clic en Submit.

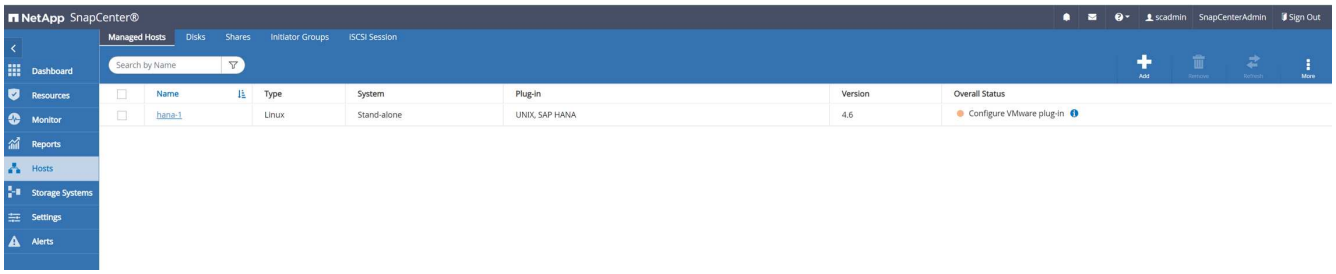


3. Confirme la huella.



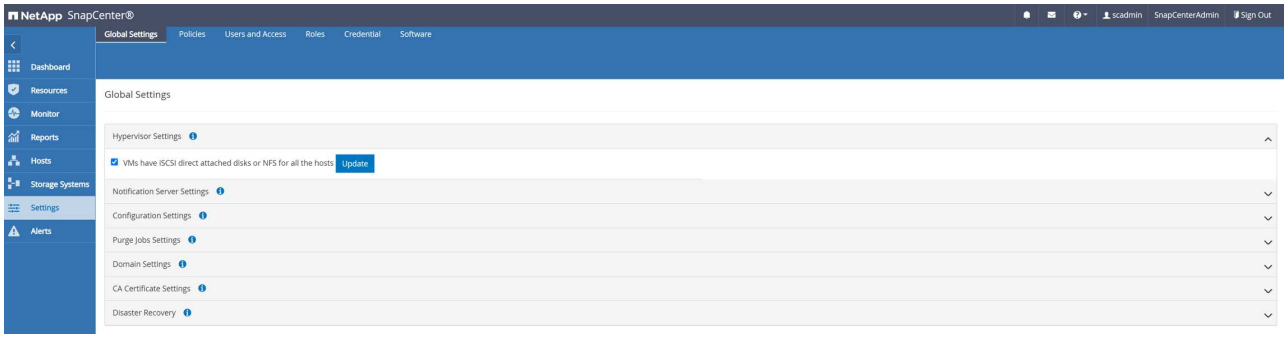
La instalación de HANA y el plugin de Linux se inicia automáticamente. Cuando termina la instalación, la columna de estado del host muestra Configure VMware Plug-in. SnapCenter detecta si el plugin de SAP HANA está instalado en un entorno virtualizado. Puede ser un entorno de VMware o un entorno de un proveedor de cloud público. En este caso, SnapCenter muestra una advertencia para configurar el hipervisor.

Puede eliminar el mensaje de advertencia mediante los pasos siguientes.

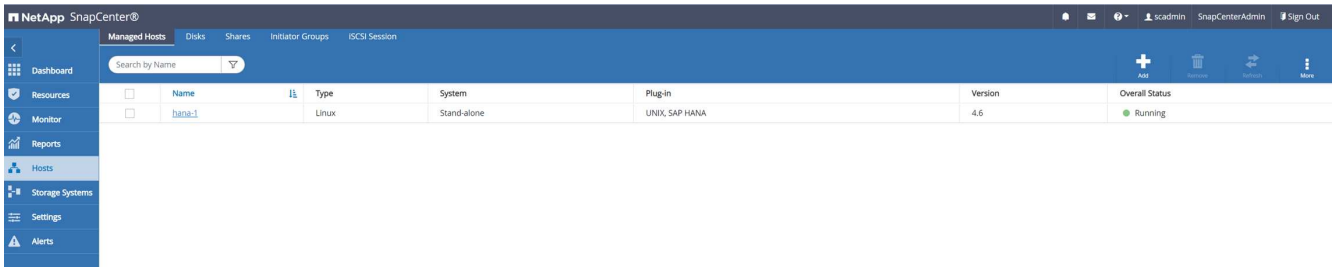


a. En la pestaña Configuración, seleccione Configuración global.

b. Para la configuración del hipervisor, seleccione VMs have iSCSI Direct Attached Disks or NFS for All the hosts y actualice la configuración.



La pantalla ahora muestra el plugin de Linux y el plugin de HANA con el estado ejecutando.



Configurar políticas

Las políticas suelen configurarse de manera independiente del recurso y pueden ser usadas por varias bases de datos SAP HANA.

Una configuración mínima típica consiste en las siguientes políticas:

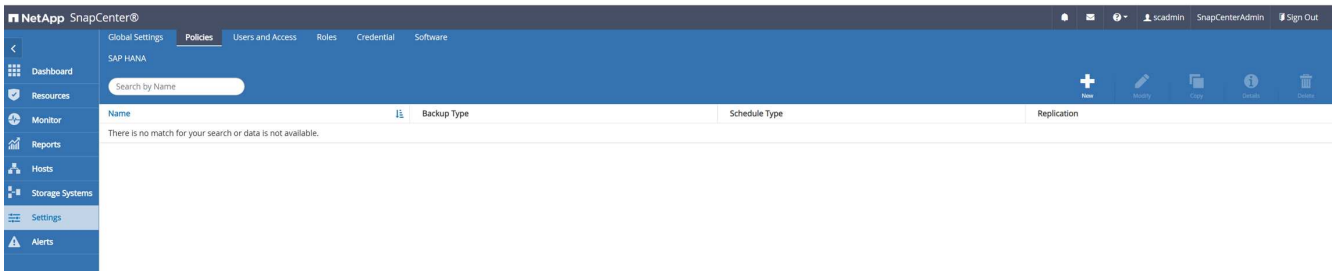
- Política de backups cada hora sin replicación: `LocalSnap`.
- Política para la comprobación semanal de la integridad de los bloques mediante un backup basado en archivos: `BlockIntegrityCheck`.

En las siguientes secciones se describe la configuración de estas directivas.

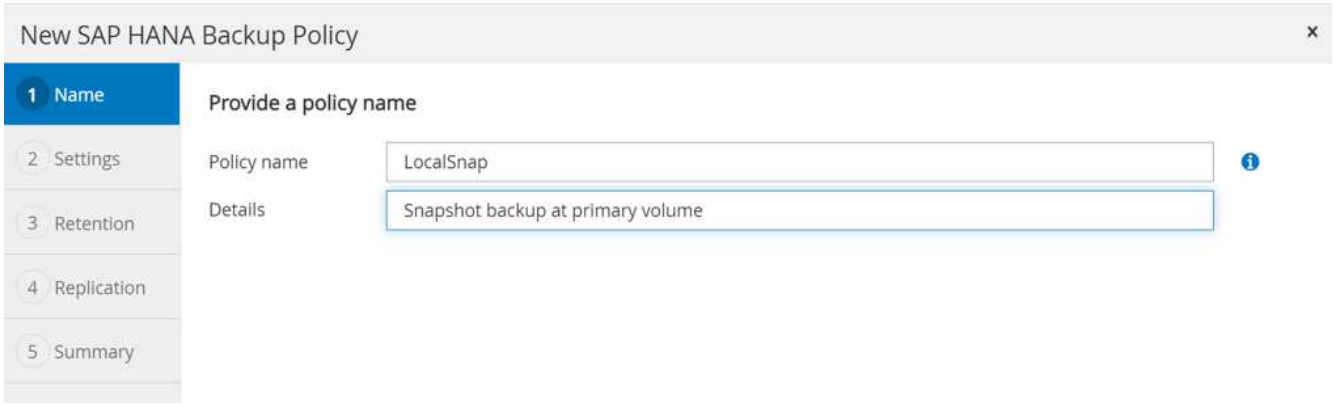
Política para backups de Snapshot

Siga estos pasos para configurar las políticas de backup de Snapshot.

1. Vaya a Configuración > Directivas y haga clic en Nuevo.

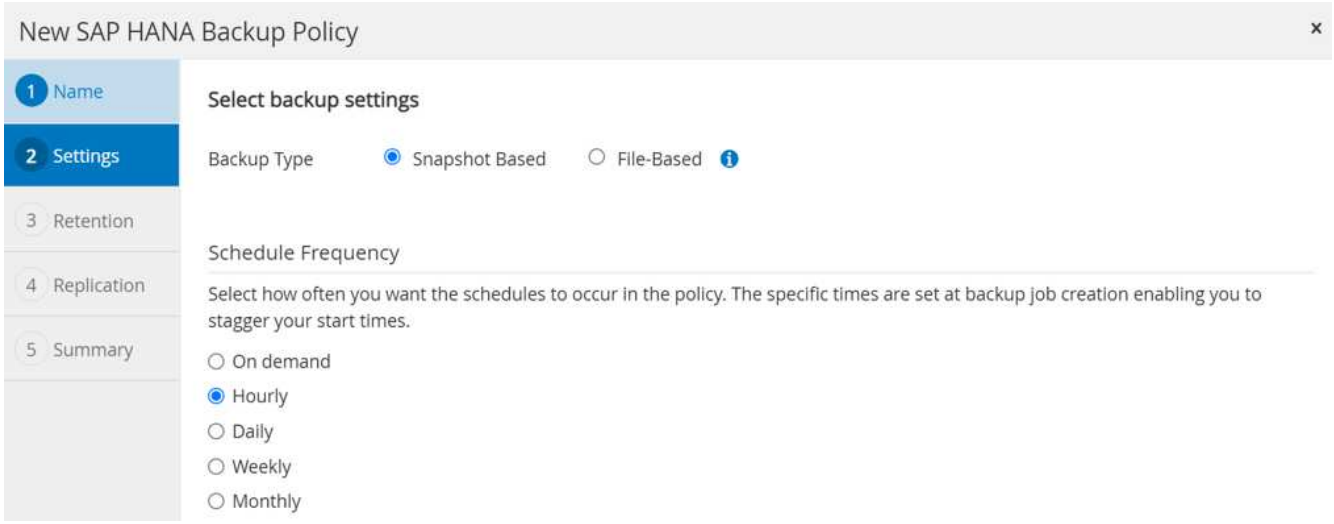


2. Escriba el nombre de la política y una descripción. Haga clic en Siguiente.

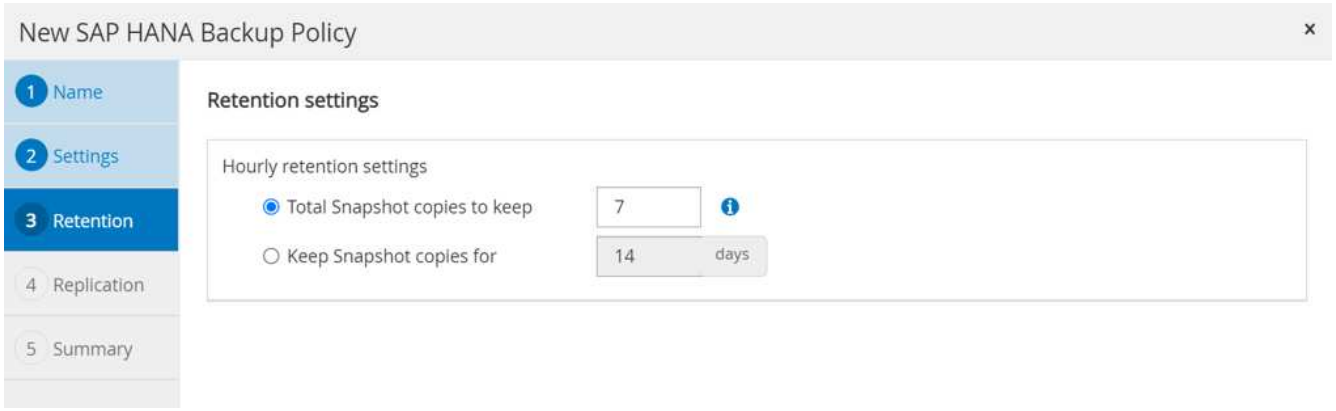


3. Seleccione el tipo de backup as Snapshot Based y seleccione Hourly for schedule frequency.

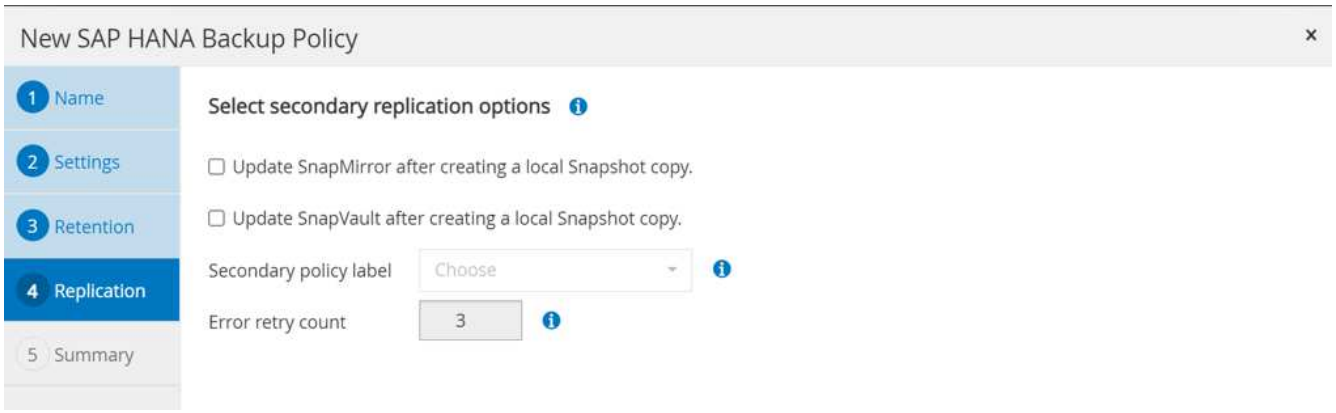
   La programación se configura más adelante con la configuración de protección de recursos HANA.

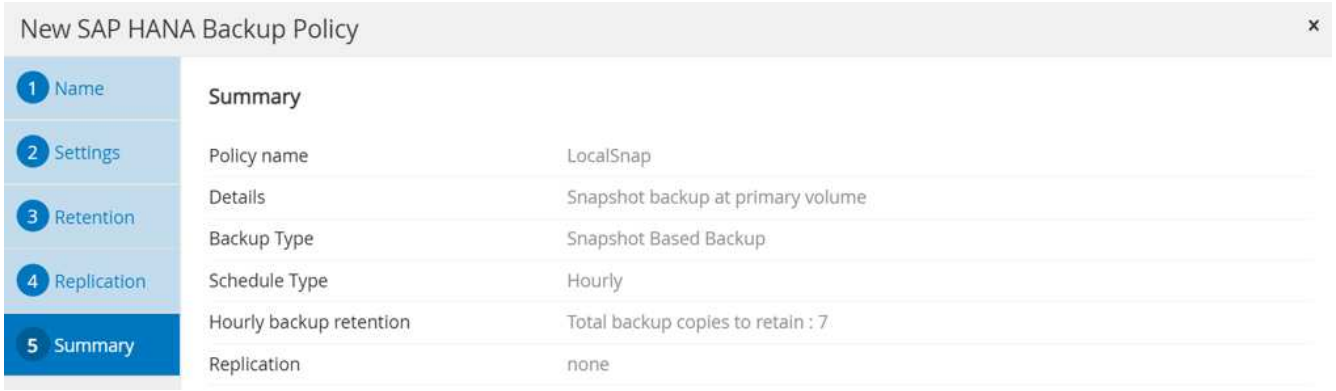


4. Configurar las opciones de retención para backups bajo demanda.

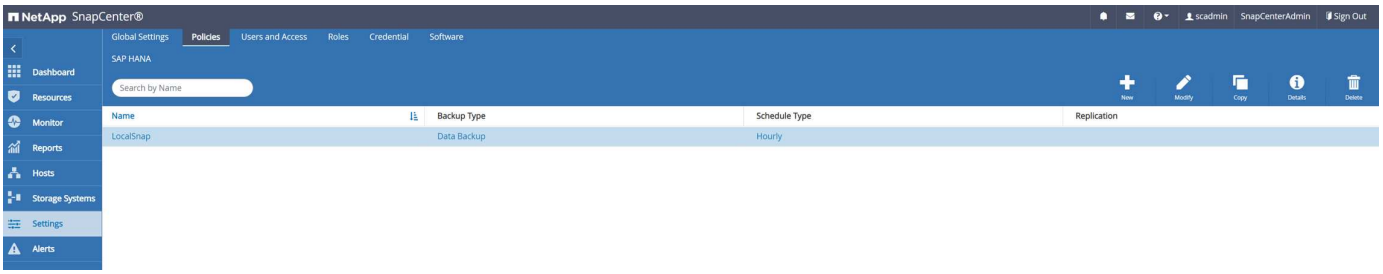


5. Configure las opciones de replicación. En este caso, no se ha seleccionado ninguna actualización de SnapVault o SnapMirror.





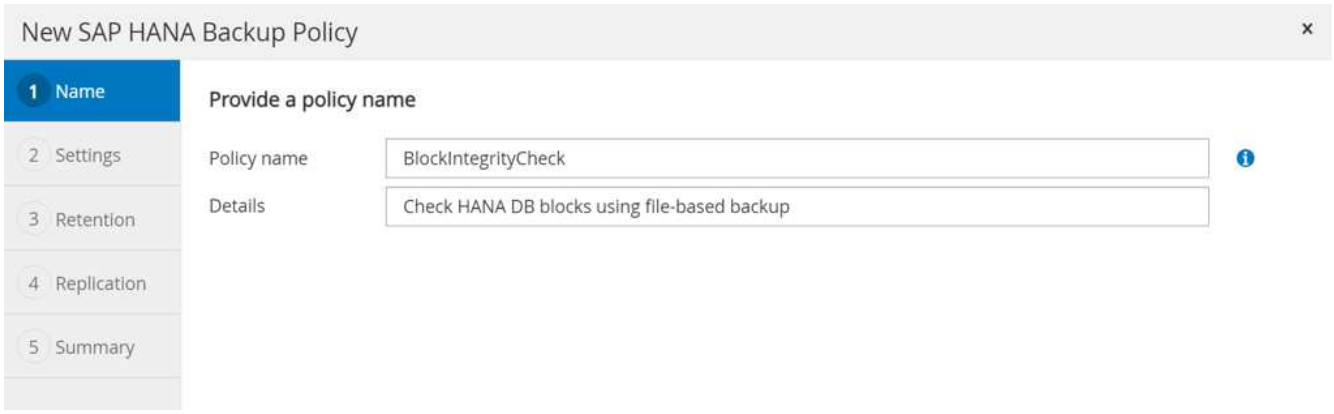
La nueva directiva está configurada ahora.



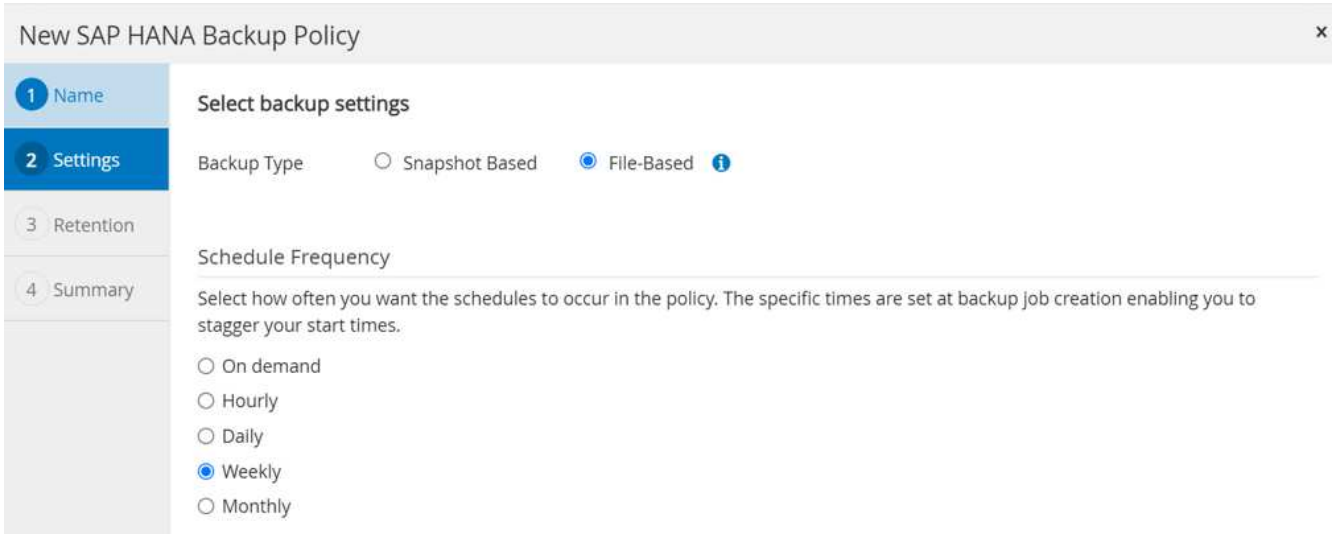
Política para la comprobación de integridad de bloques

Siga estos pasos para configurar la directiva de comprobación de integridad de bloques.

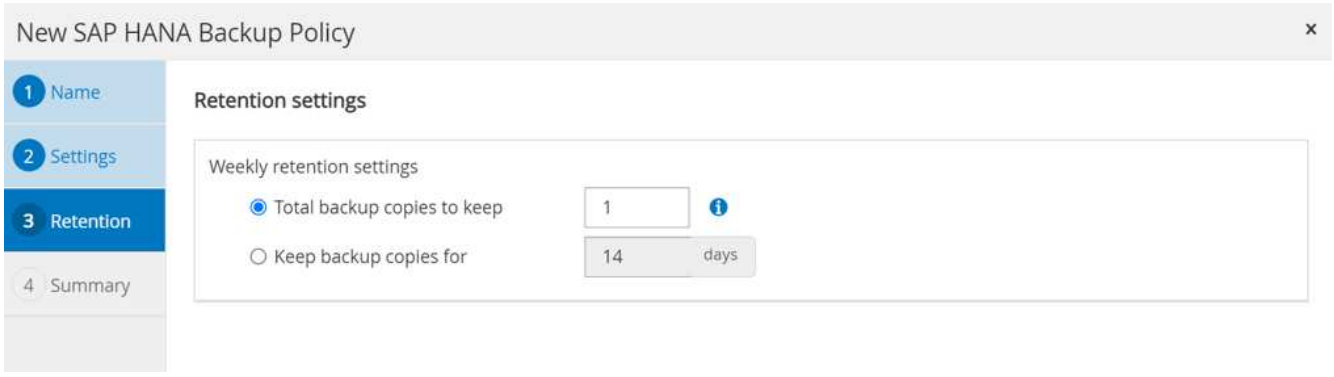
1. Vaya a Configuración > Directivas y haga clic en Nuevo.
2. Escriba el nombre de la política y una descripción. Haga clic en Siguiente.



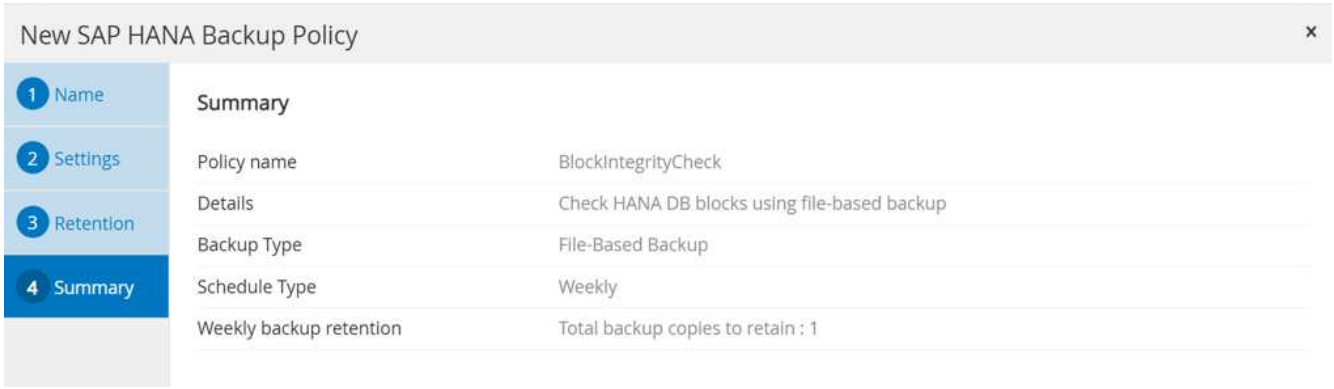
3. Establezca el tipo de backup en File-based y la frecuencia de programación en Weekly. La programación se configura más adelante con la configuración de protección de recursos HANA.

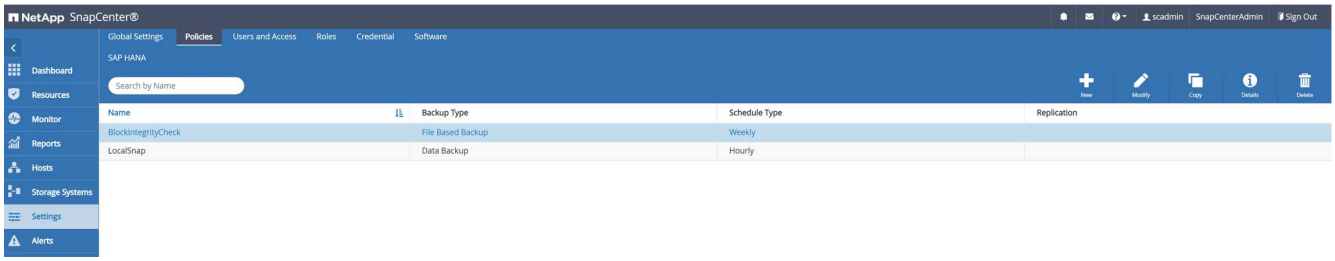


4. Configurar las opciones de retención para backups bajo demanda.



5. En la página Summary, haga clic en Finish.



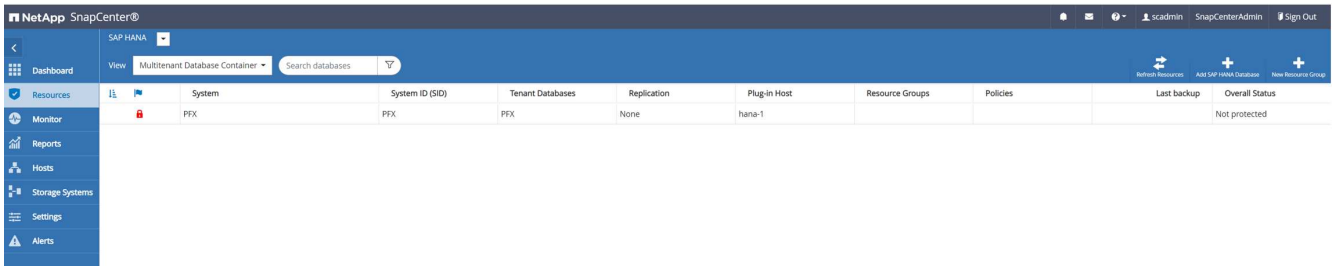


Configure y proteja un recurso de HANA

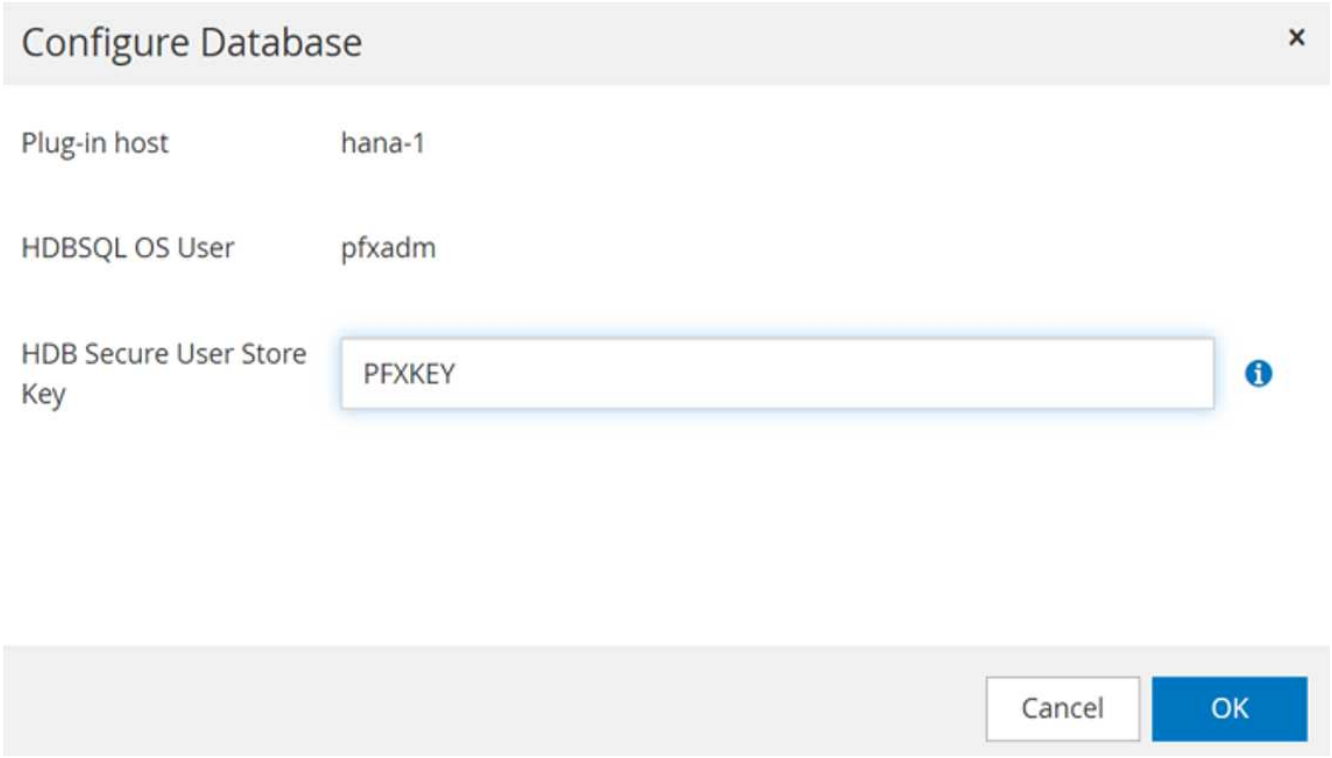
Después de la instalación del plugin, el proceso de detección automática del recurso HANA se inicia de forma automática. En la pantalla Recursos, se crea un recurso nuevo, que se Marca como bloqueado con el icono de candado rojo. Para configurar y proteger el nuevo recurso HANA, siga estos pasos:

1. Seleccione y haga clic en el recurso para continuar con la configuración.

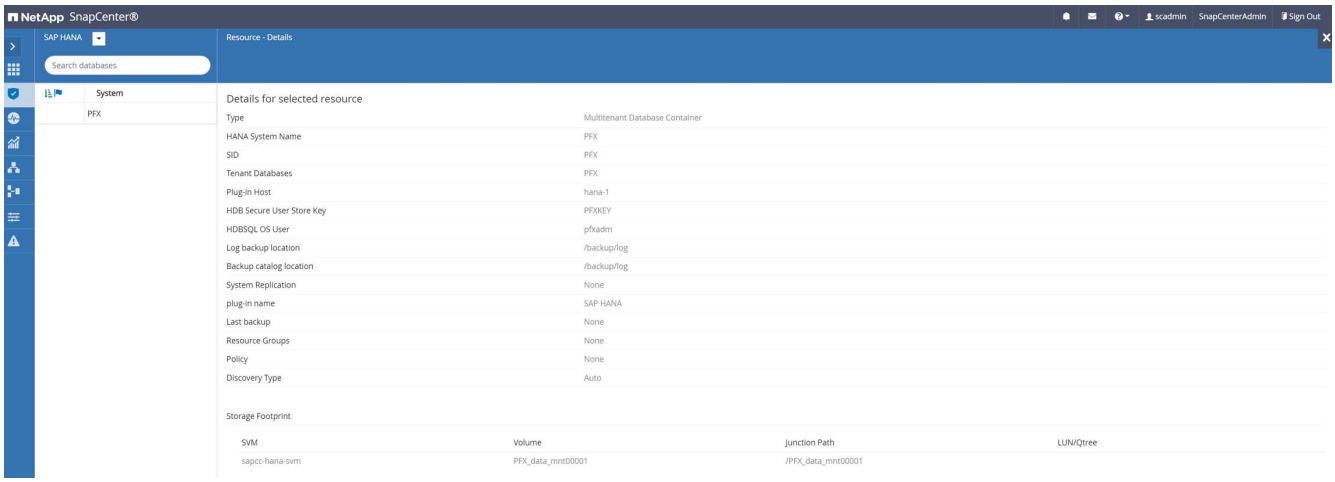
   También es posible activar el proceso de detección automática manualmente dentro de la pantalla Recursos. Para ello, haga clic en Refresh Resources.



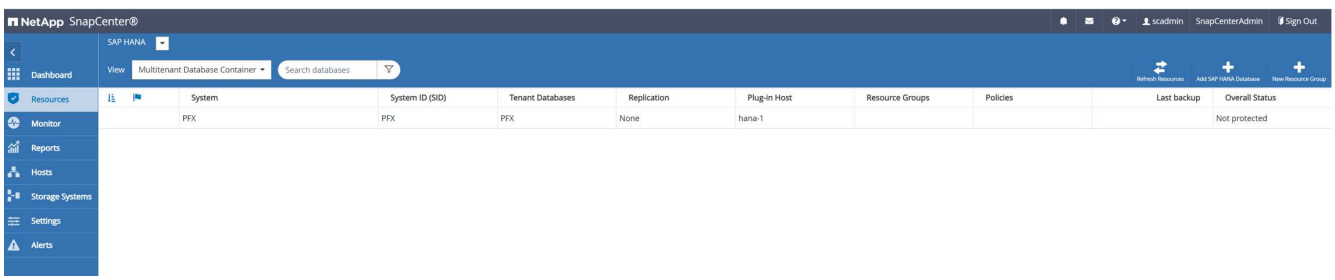
2. Proporcione la clave de almacenamiento de usuarios para la base de datos HANA.



El proceso de detección automática de segundo nivel comienza en el cual se detectan los datos de inquilinos y la información sobre la huella de almacenamiento.



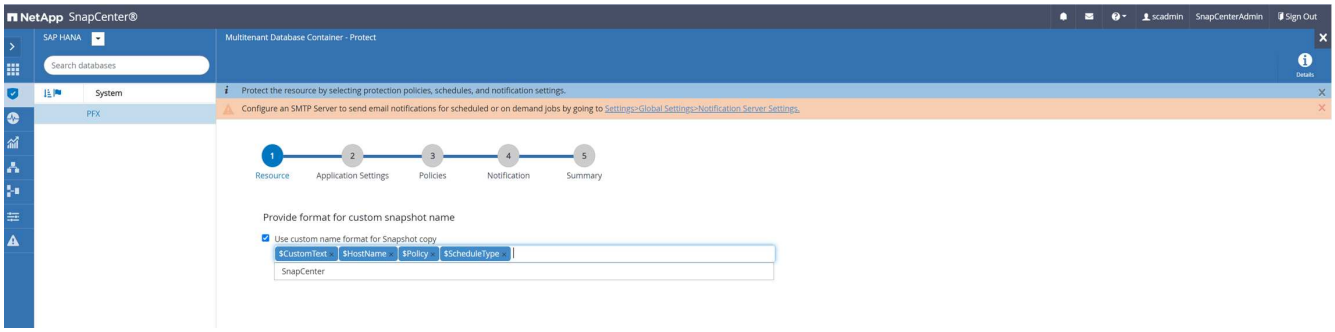
3. En la pestaña Resources, haga doble clic en el recurso para configurar la protección de recursos.



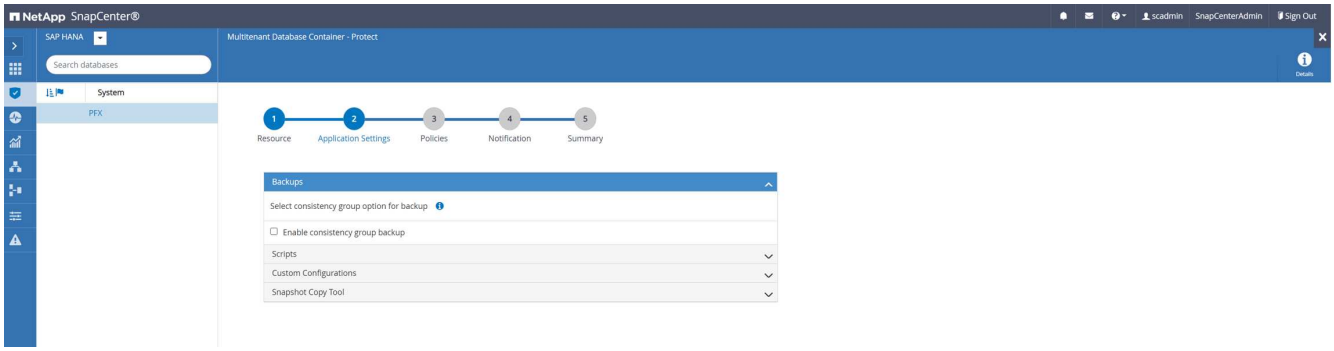
4. Configure un formato de nombre personalizado para la copia de Snapshot.

   NetApp recomienda utilizar un nombre de copia de Snapshot personalizado para identificar fácilmente qué

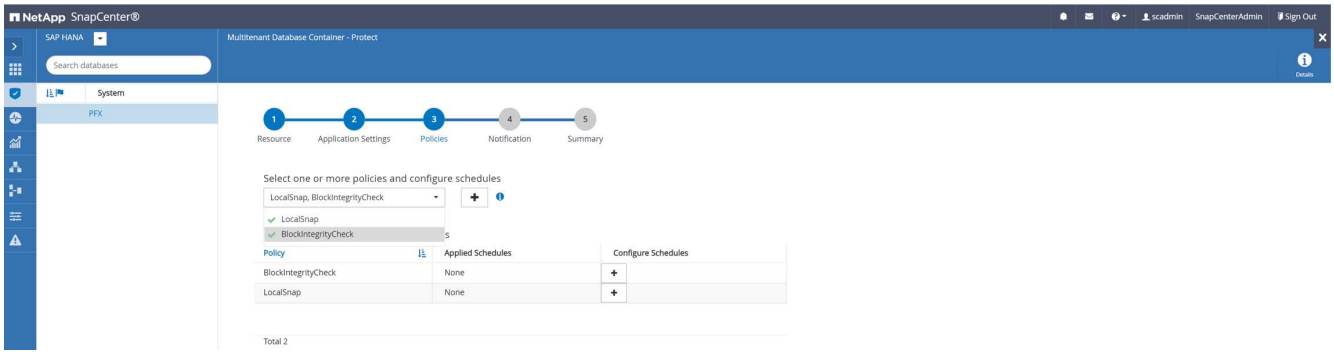
backups se han creado con qué tipo de normativa y programación. Al añadir el tipo de programación al nombre de la copia de Snapshot, es posible distinguir entre backups programados y bajo demanda. La `schedule name` la cadena de backups bajo demanda está vacía, mientras que las copias de seguridad programadas incluyen la cadena `Hourly`, `Daily`, `or Weekly`.



5. No es necesario realizar ningún ajuste específico en la página Configuración de la aplicación. Haga clic en Siguiente.

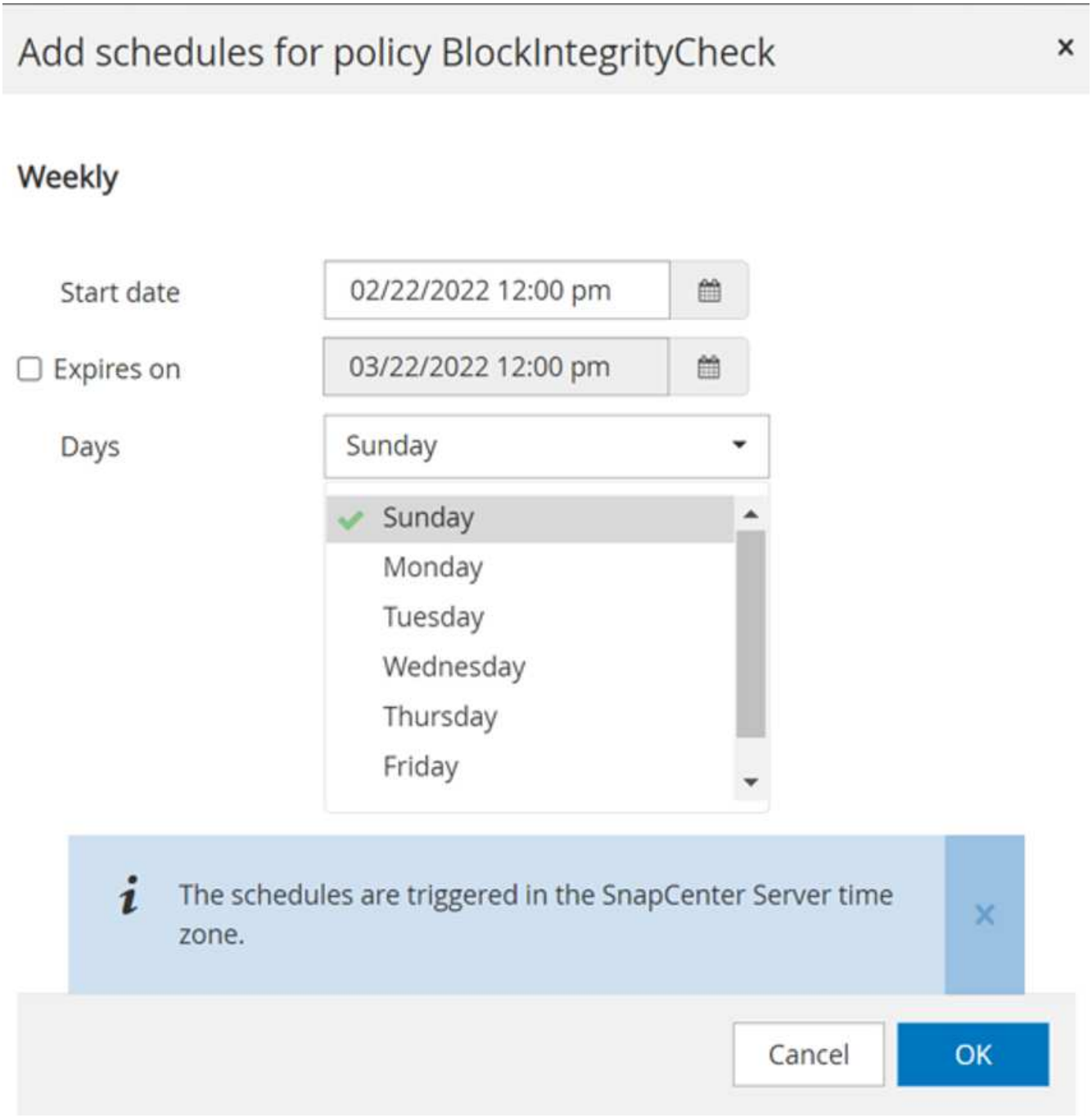


6. Seleccione las políticas que desea añadir al recurso.



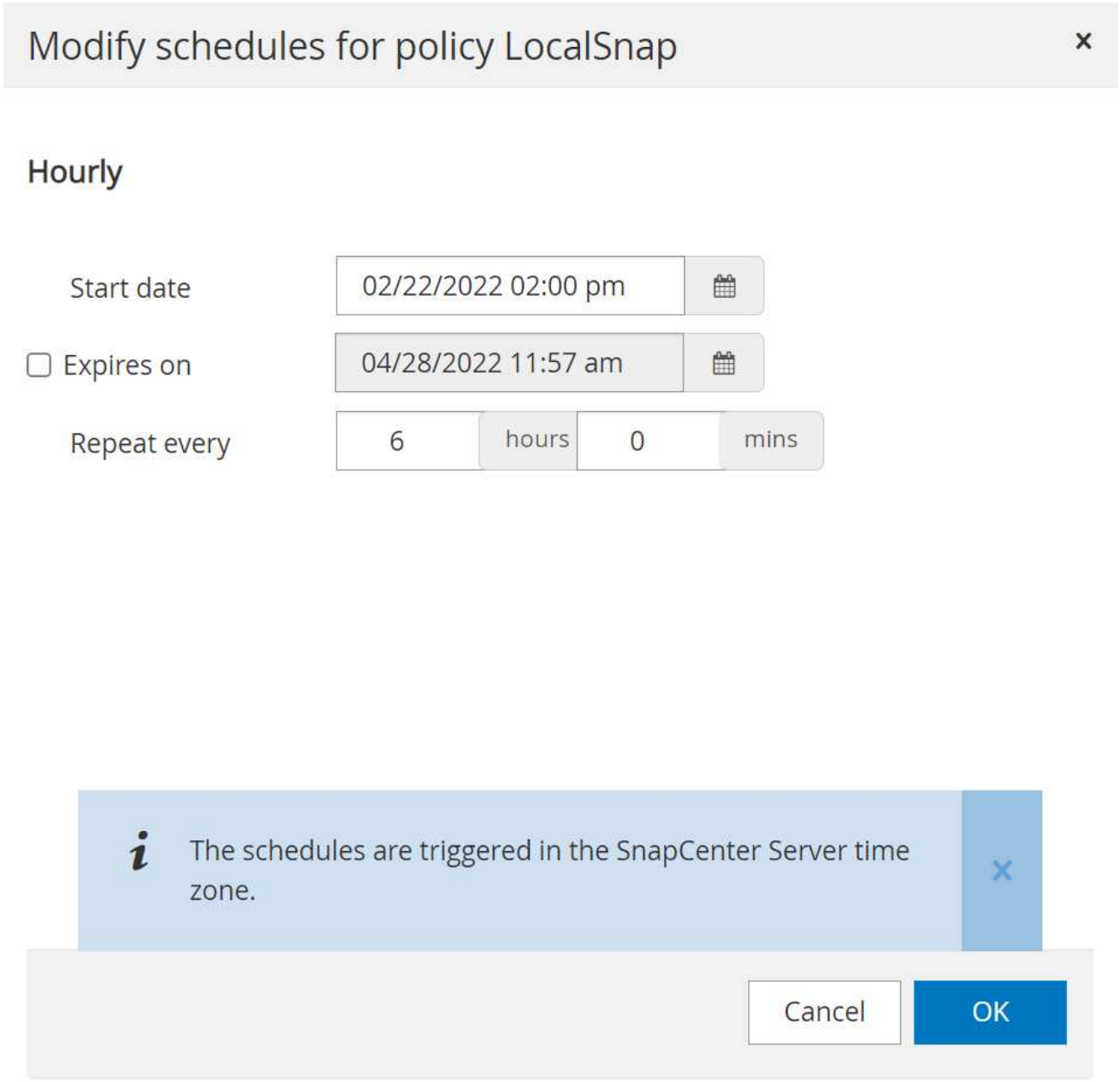
7. Defina la programación de la política de comprobación de integridad de bloques.

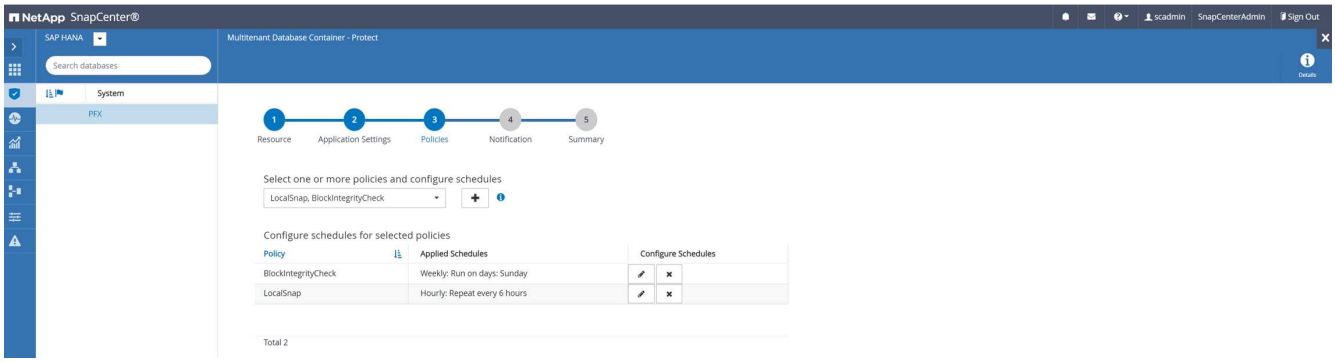
   En este ejemplo, se establece una vez por semana.



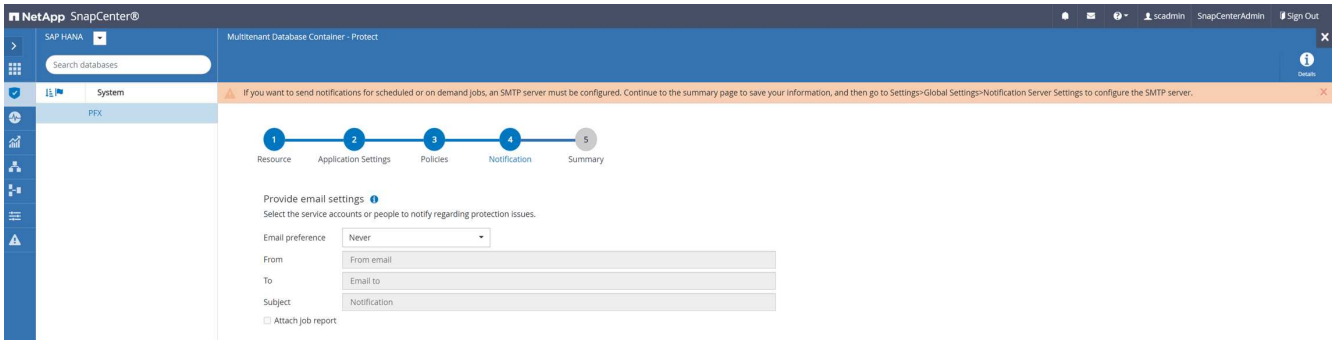
8. Defina la programación para la política de Snapshot local.

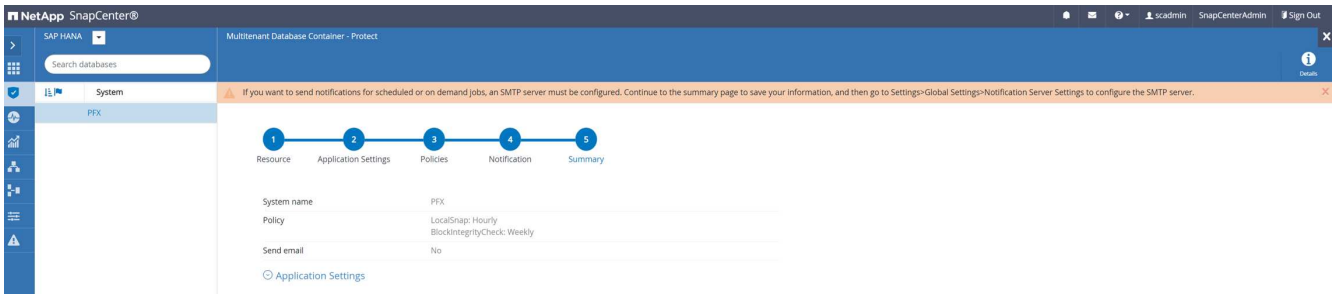
   En este ejemplo, se establece para cada 6 horas.



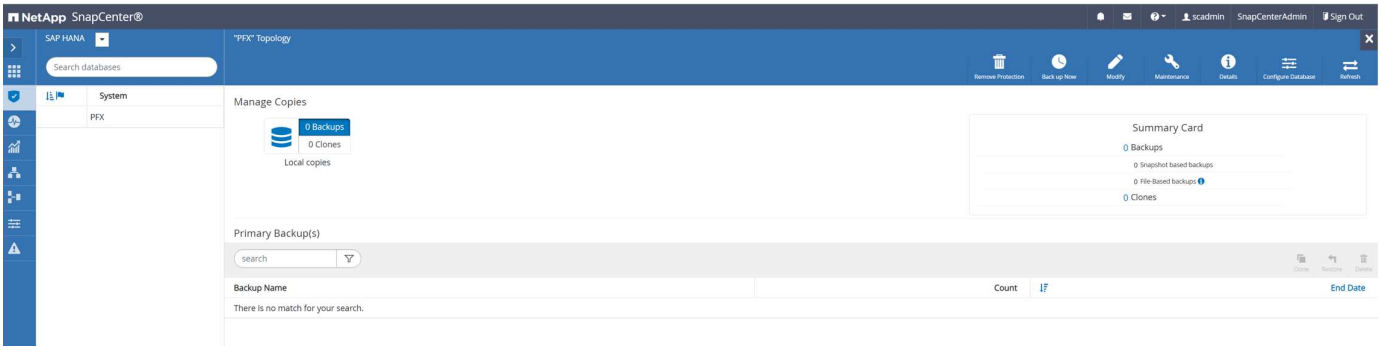


9. Proporcione información acerca de las notificaciones por correo electrónico.





La configuración de recursos HANA ahora se completa y puede ejecutar backups.



Operaciones de backup de SnapCenter

Puede crear un backup de Snapshot bajo demanda y una operación de comprobación de integridad de bloques bajo demanda.

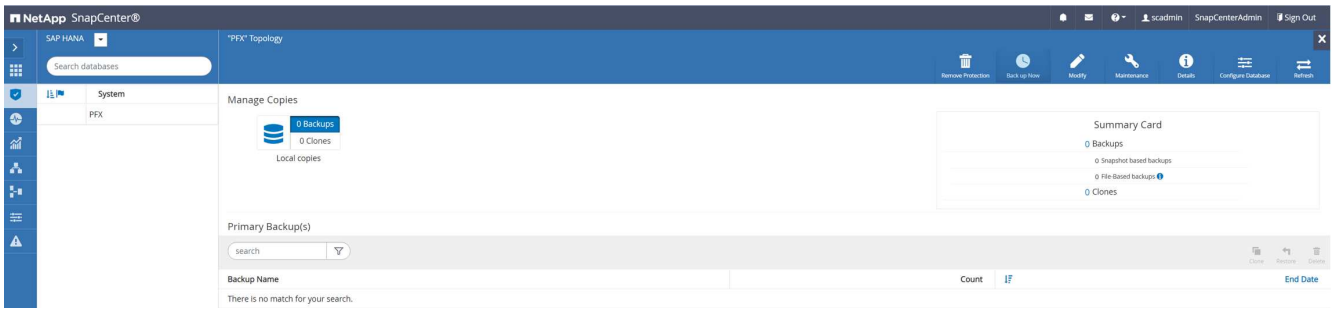
Crear un backup de Snapshot bajo demanda

Siga estos pasos para crear backups de Snapshot bajo demanda.

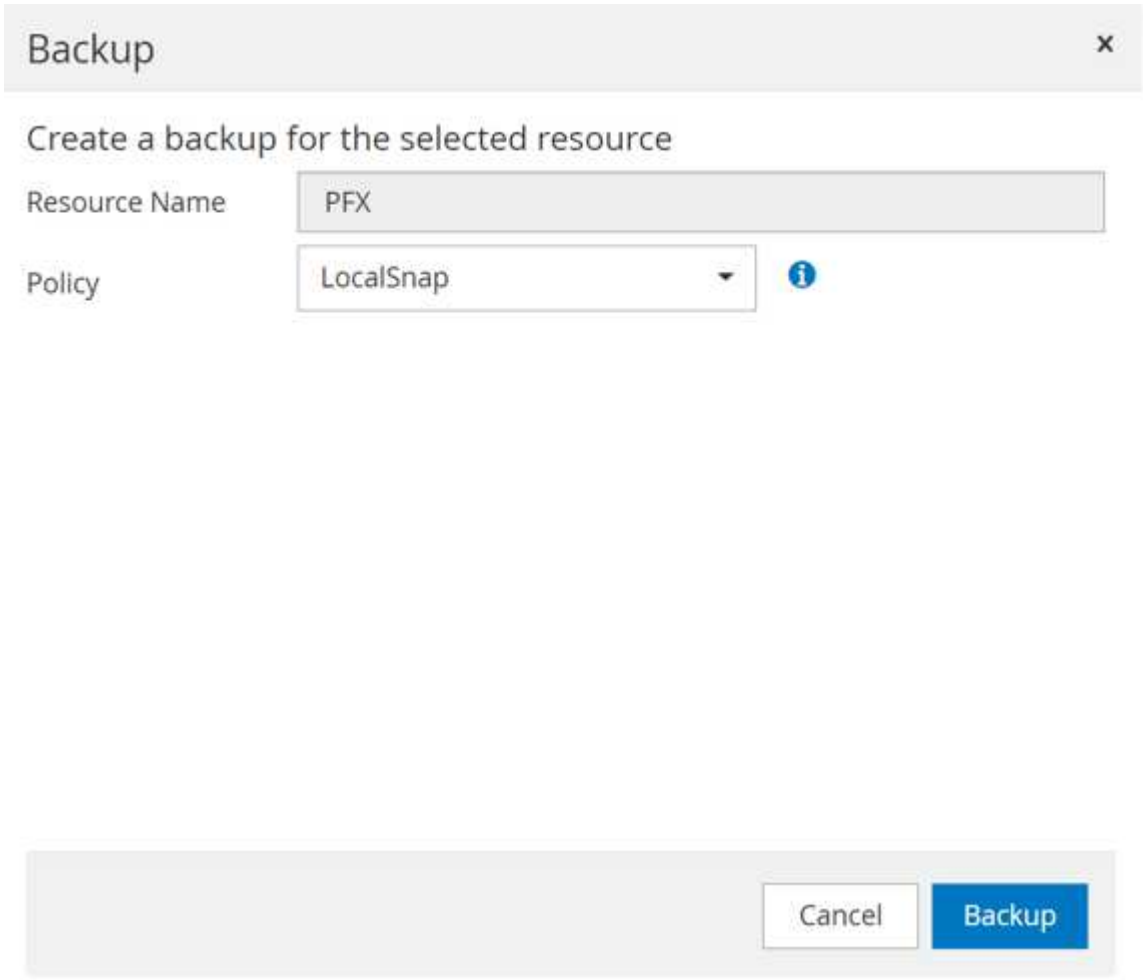
1. En la vista Recursos, seleccione el recurso y haga doble clic en la línea para cambiar a la vista Topología.

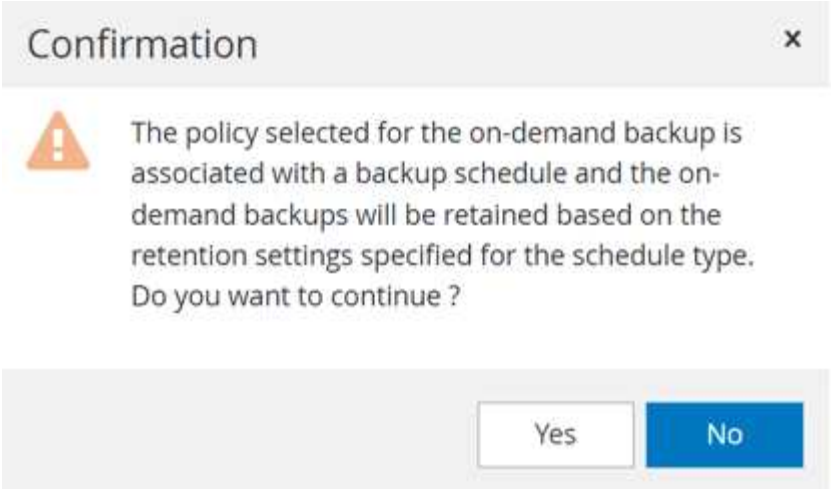
   La vista de topología de recursos proporciona información general de todos los backups disponibles que se han creado con SnapCenter. En la zona superior de esta vista se muestra la topología de backup que muestra los backups en el almacenamiento principal (copias locales) y, si están disponibles, en el almacenamiento de backup externo (copias vault).

2. En la fila superior, seleccione el icono Back up Now para iniciar un backup bajo demanda.



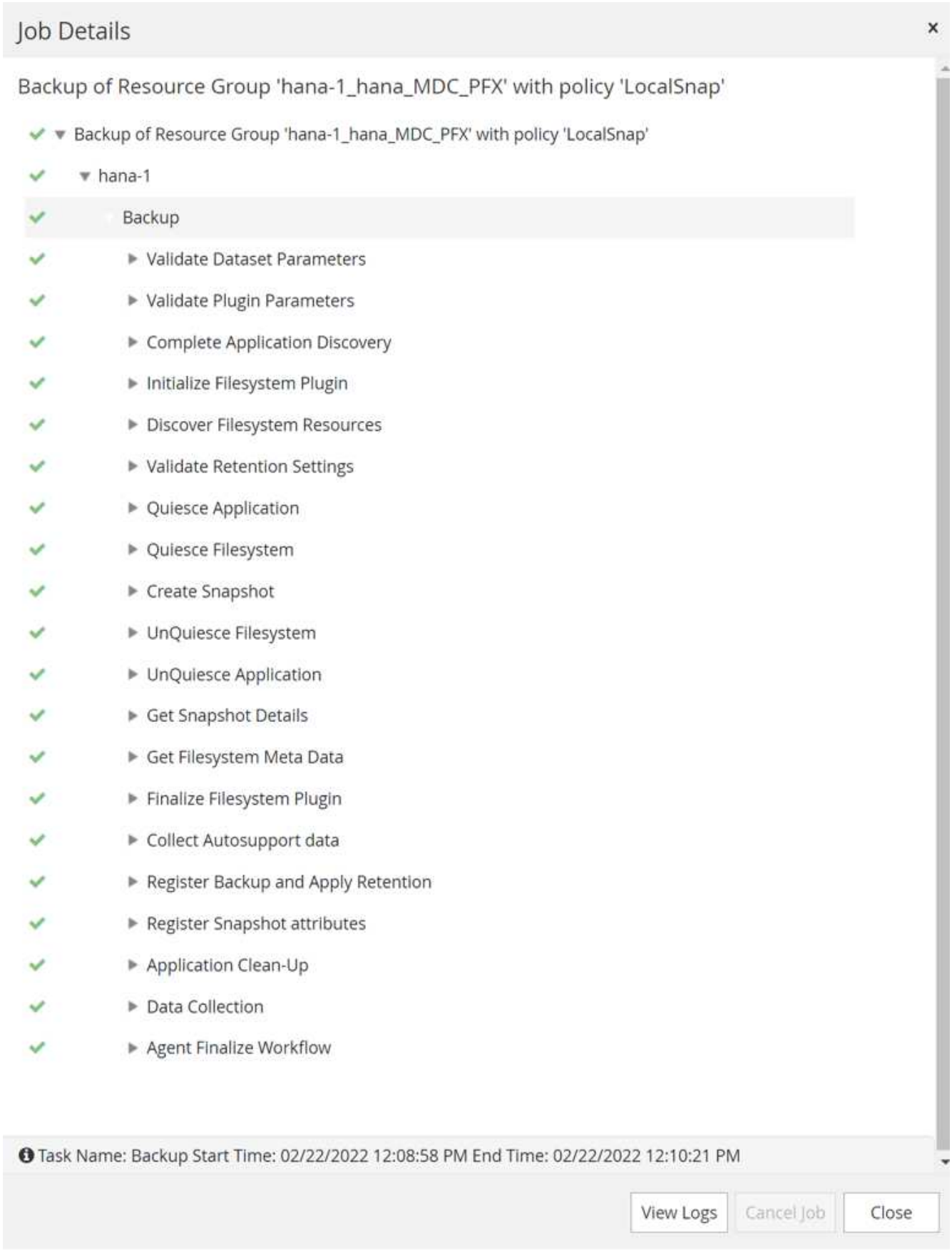
3. En la lista desplegable, seleccione la política de backup `LocalSnap`Y, a continuación, haga clic en copia de seguridad para iniciar la copia de seguridad bajo demanda.





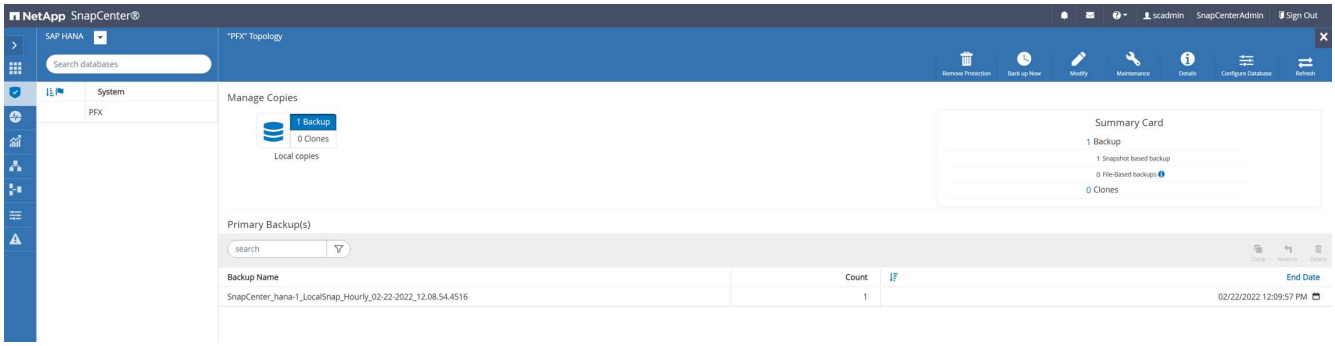
Se muestra un registro de los cinco trabajos anteriores en el área actividad en la parte inferior de la vista de topología.

4. Los detalles del trabajo se muestran al hacer clic en la línea de actividad del trabajo en el área actividad. Es posible abrir un registro de trabajos detallado si se hace clic en View Logs

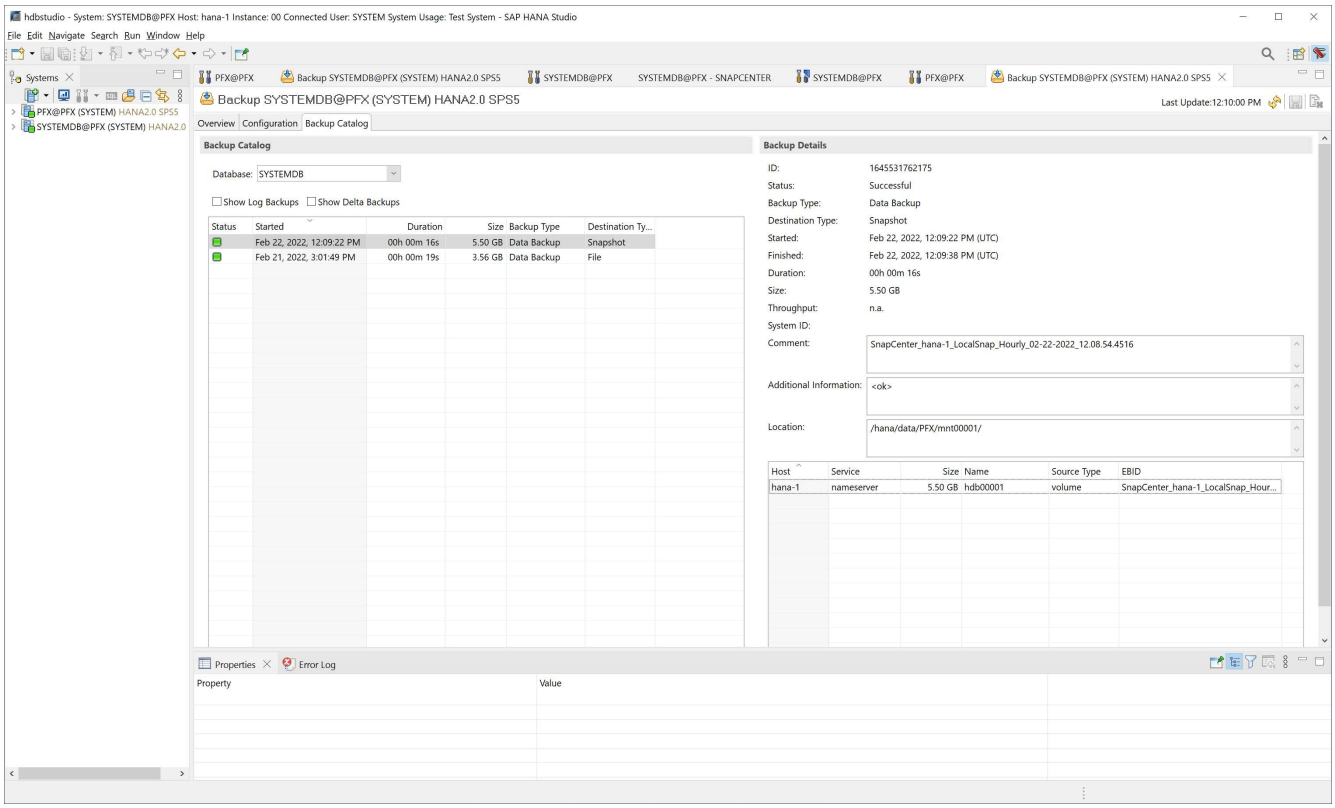


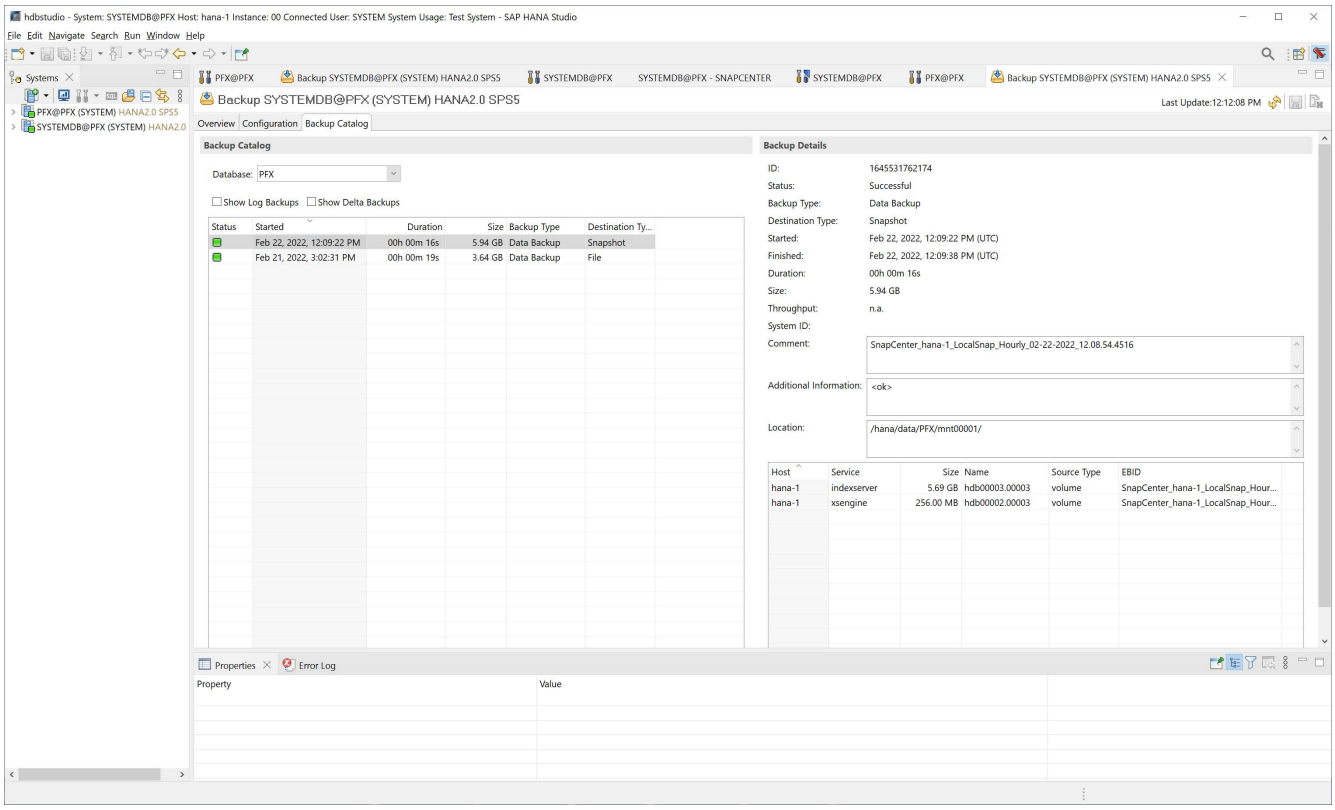
Cuando termina el backup, se muestra una entrada nueva en la vista de topología. Los nombres de los backups siguen la misma convención de nomenclatura que el nombre de Snapshot definido en la sección ""“Configurar y proteger un recurso HANA”."

Debe cerrar y volver a abrir la vista de topología para ver la lista de backups actualizada.



En el catálogo de backup de SAP HANA, el nombre del backup de SnapCenter se almacena como un `Comment` también campo `External Backup ID (EBID)`. Esto se muestra en la siguiente figura para la base de datos del sistema y en la siguiente figura para la base de datos de tenant PFX.



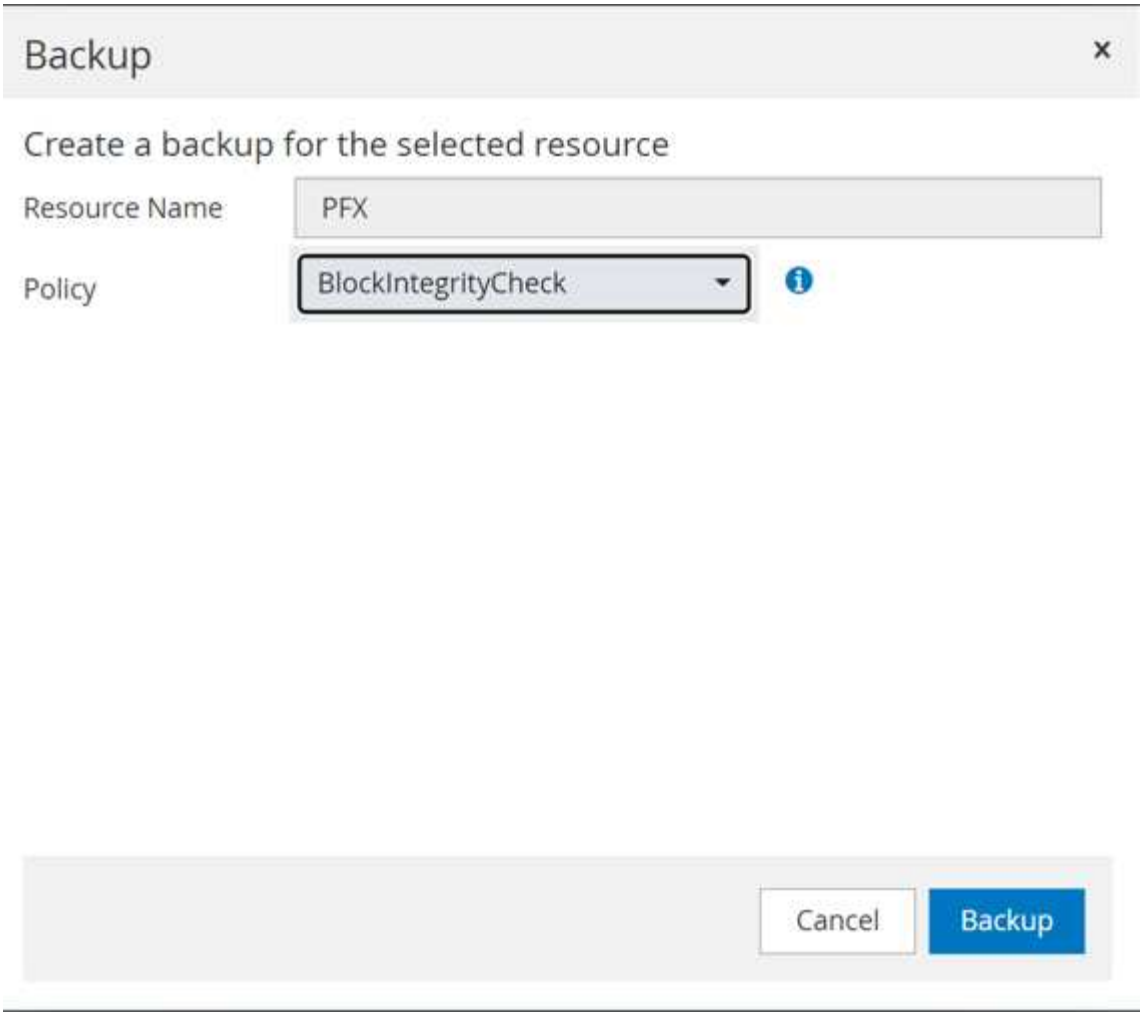


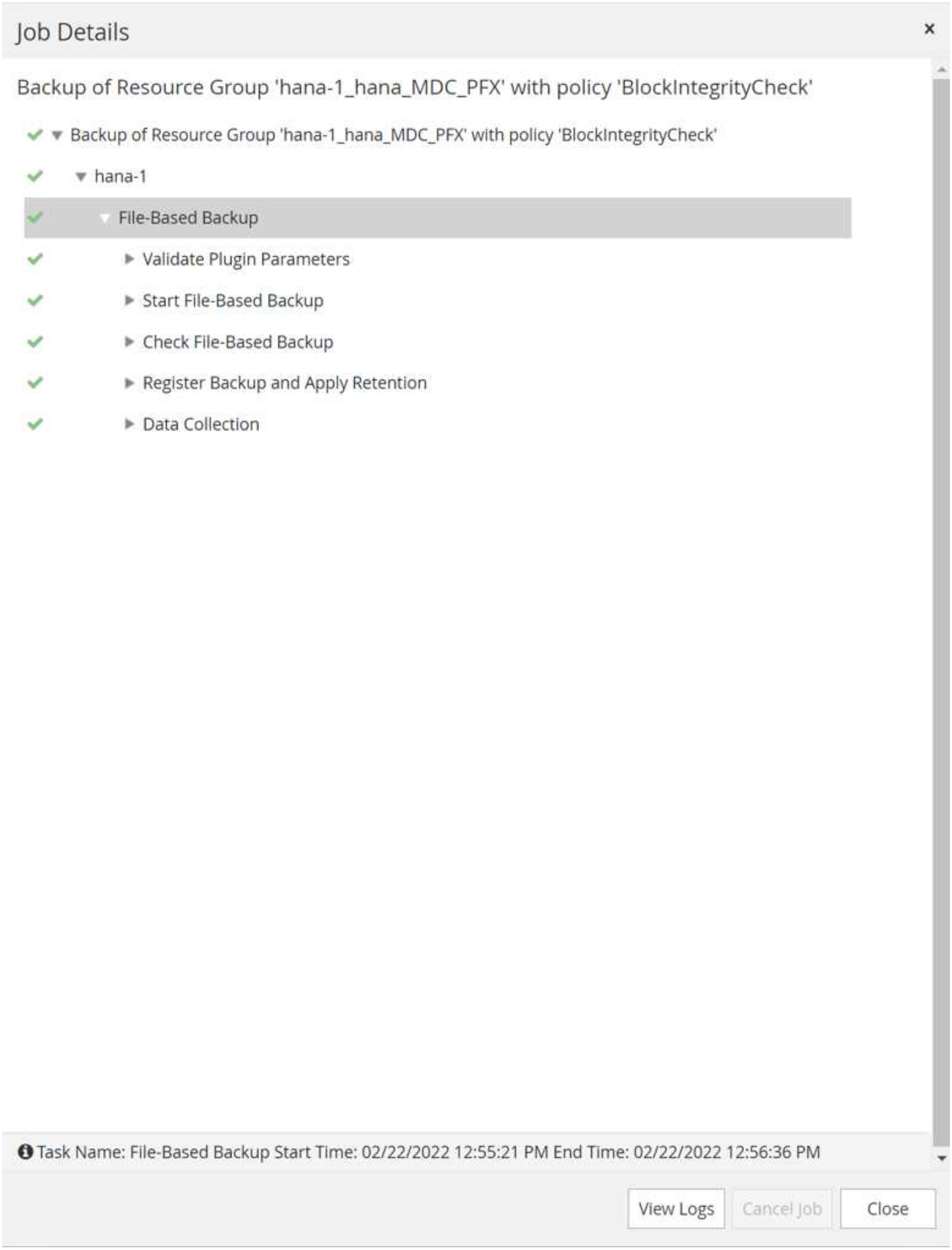
En el FSX para el sistema de archivos ONTAP, puede mostrar los backups de Snapshot conectando a la consola de la SVM.

```
sapcc-hana-svm::> snapshot show -volume PFX_data_mnt00001
---Blocks---
Vserver  Volume   Snapshot                                  Size Total%
Used%
-------- -------- ------------------------------------ -------- ------
-----
sapcc-hana-svm
         PFX_data_mnt00001
                  SnapCenter_hana-1_LocalSnap_Hourly_02-22-
2022_12.08.54.4516
                                                       126.6MB     0%
2%
sapcc-hana-svm::>
```

Cree una operación de comprobación de integridad de bloques bajo demanda

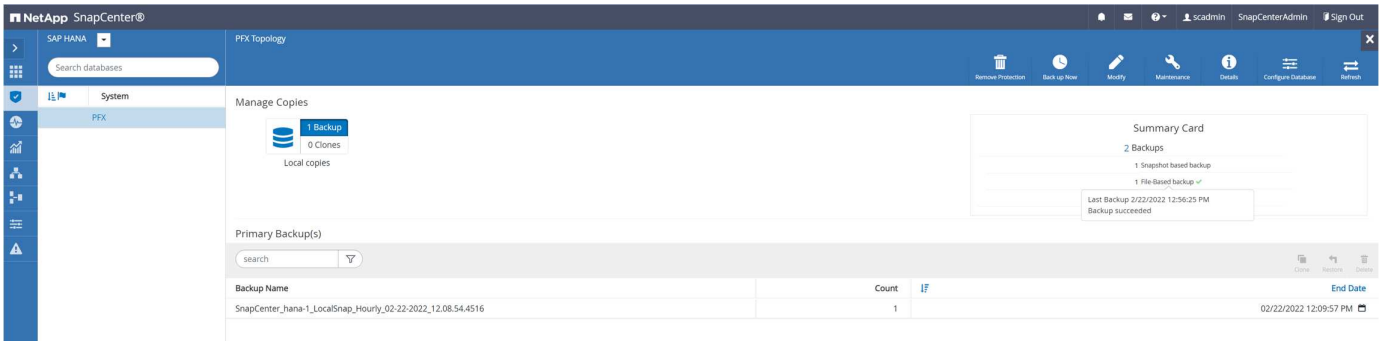
Una operación de comprobación de integridad de bloque bajo demanda se ejecuta de la misma manera que una tarea de backup de Snapshot. Para ello, se selecciona la política BlockIntegrityCheck. Al programar backups con esta política, SnapCenter crea un backup de archivos SAP HANA estándar para las bases de datos del sistema y del inquilino.


Backup
Create a backup for the selected resource
Resource Name
PFX
Policy
BlockIntegrityCheck
Cancel
Backup

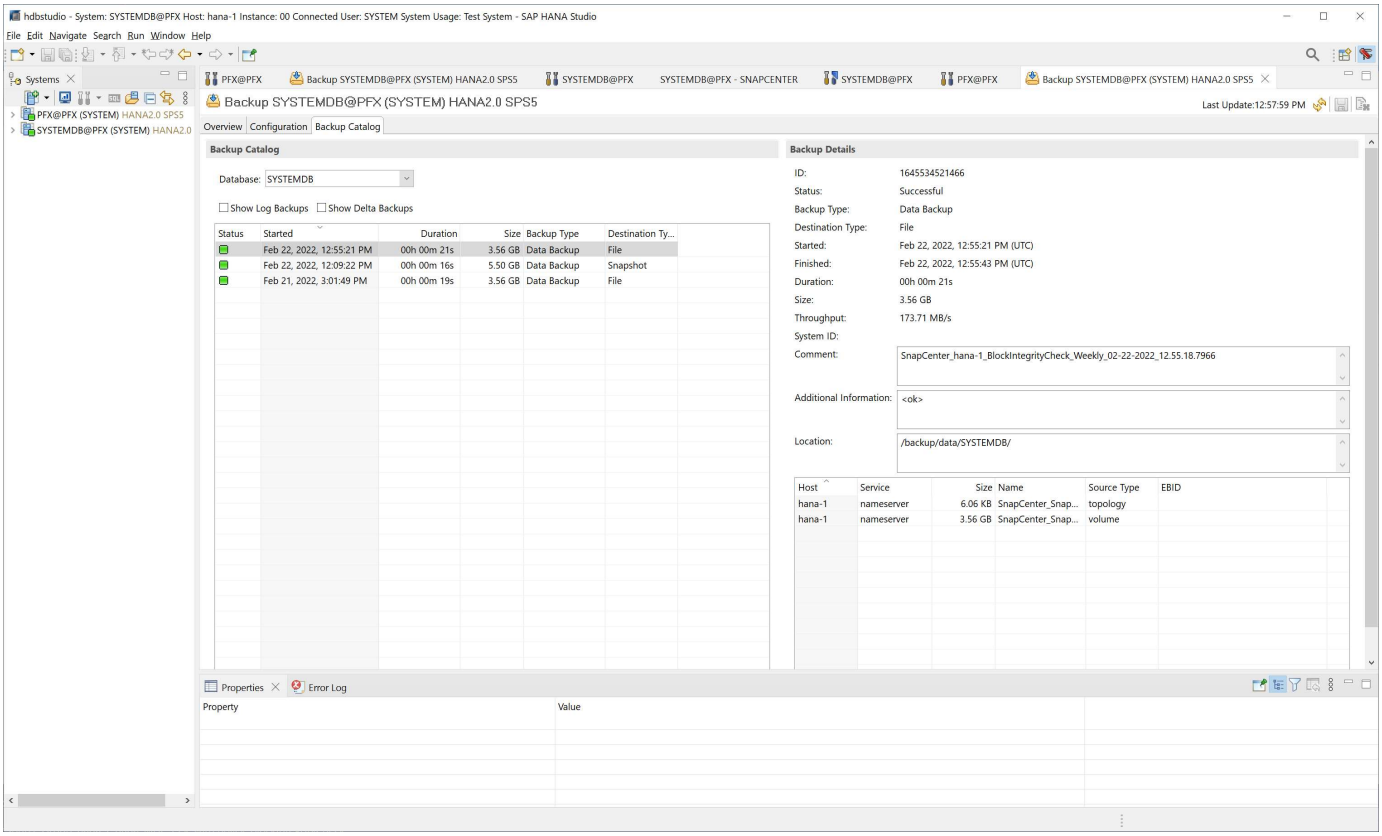


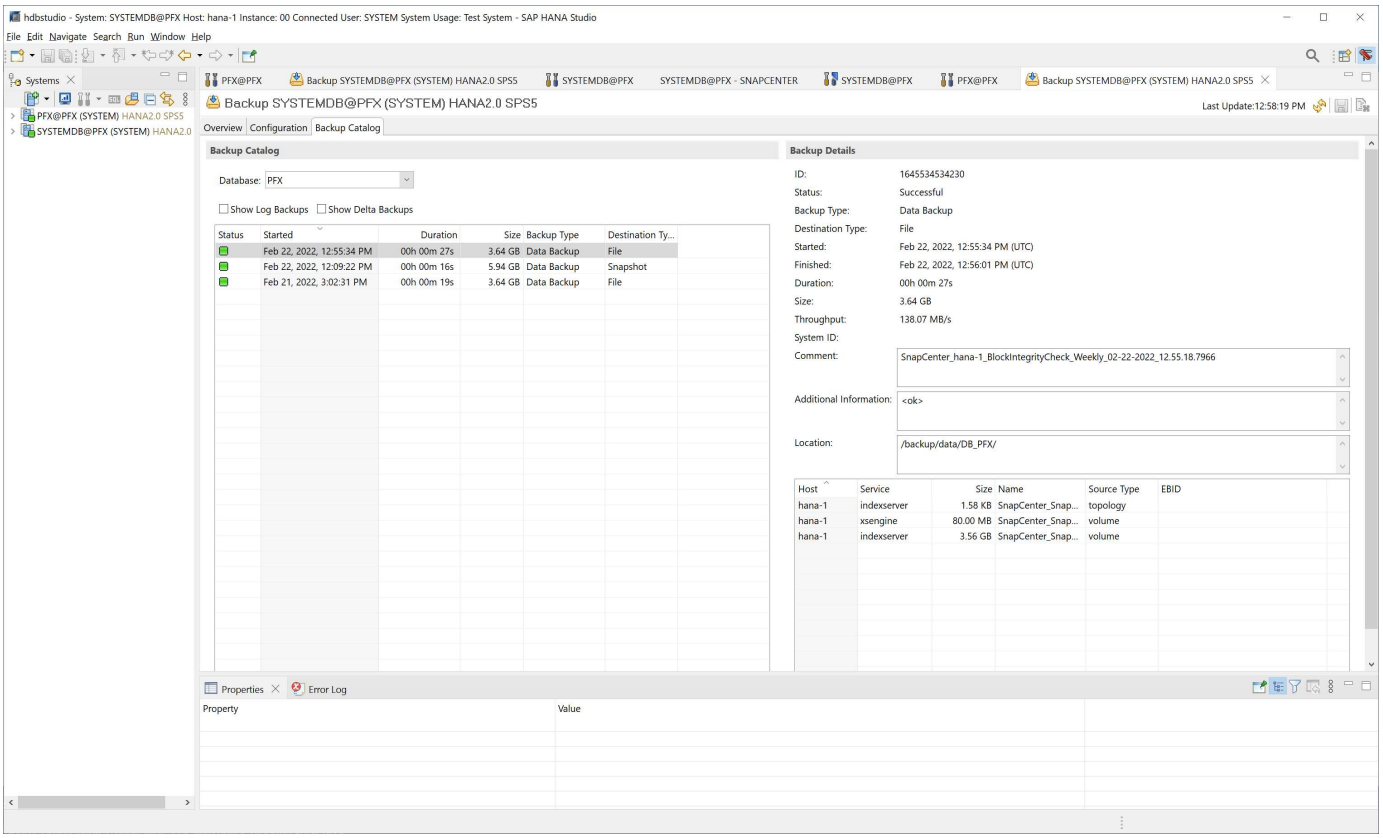
SnapCenter no muestra la comprobación de integridad de bloques del mismo modo que los backups basados

en copias de Snapshot. En su lugar, la tarjeta de resumen muestra la cantidad de backups basados en archivos y el estado del backup anterior.



El catálogo de backup de SAP HANA muestra entradas tanto para las bases de datos del sistema como para las de tenant. Las siguientes figuras muestran la comprobación de integridad de bloques SnapCenter en el catálogo de copias de seguridad del sistema y de la base de datos de inquilinos.





Una comprobación correcta de integridad de bloque crea archivos de backup de datos SAP HANA estándar. SnapCenter usa la ruta de backup que se ha configurado con la base de datos HANA para las operaciones de backup de datos basadas en archivos.

```
hana-1:~ # ls -al /backup/data/*
/backup/data/DB_PFX:
total 7665384
drwxr-xr-- 2 pfxadm sapsys       4096 Feb 22 12:56 .
drwxr-xr-x 4 pfxadm sapsys       4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys     155648 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys   83894272 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_3_1
-rw-r----- 1 pfxadm sapsys     155648 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys   83894272 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:56
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_3_1
/backup/data/SYSTEMDB:
total 7500880
drwxr-xr-- 2 pfxadm sapsys       4096 Feb 22 12:55 .
drwxr-xr-x 4 pfxadm sapsys       4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys     159744 Feb 21 15:01
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_1_1
-rw-r----- 1 pfxadm sapsys     159744 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_1_1
hana-1:~ #
```

Backup de volúmenes que no sean de datos

El backup de volúmenes que no sean de datos es una parte integrada de SnapCenter y del complemento SAP HANA.

Proteger el volumen de datos de la base de datos es suficiente para restaurar y recuperar la base de datos SAP HANA en un momento determinado, siempre y cuando los recursos de instalación de la base de datos y los registros requeridos sigan estando disponibles.

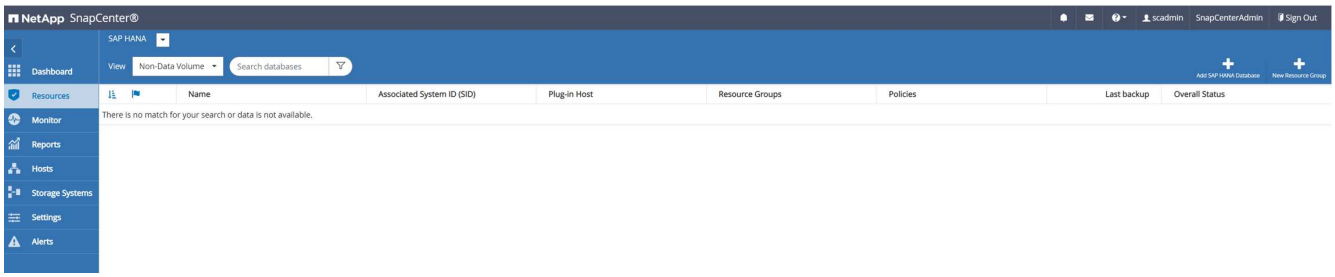
Para la recuperación tras situaciones en las que se deben restaurar otros archivos distintos de datos, NetApp recomienda desarrollar una estrategia de backup adicional para los volúmenes que no sean de datos a fin de aumentar el backup de base de datos SAP HANA. En función de los requisitos específicos, el backup de volúmenes que no pertenecen a datos puede diferir en la configuración de frecuencia de programación y retención, por lo que debe tenerse en cuenta la frecuencia con la que se modifican los archivos que no son de datos. Por ejemplo, el volumen HANA `/hana/shared` Contiene ejecutables, pero también archivos de seguimiento SAP HANA. Aunque los ejecutables solo cambian cuando se actualiza la base de datos SAP HANA, es posible que los archivos de seguimiento de SAP HANA necesiten una frecuencia de backup mayor para permitir el análisis de situaciones problemáticas con SAP HANA.

El backup de volúmenes que no son de datos de SnapCenter permite crear copias Snapshot de todos los volúmenes relevantes en solo unos segundos, con la misma eficiencia de espacio que los backups de bases de datos de SAP HANA. La diferencia es que no se requiere ninguna comunicación de SQL con la base de datos SAP HANA.

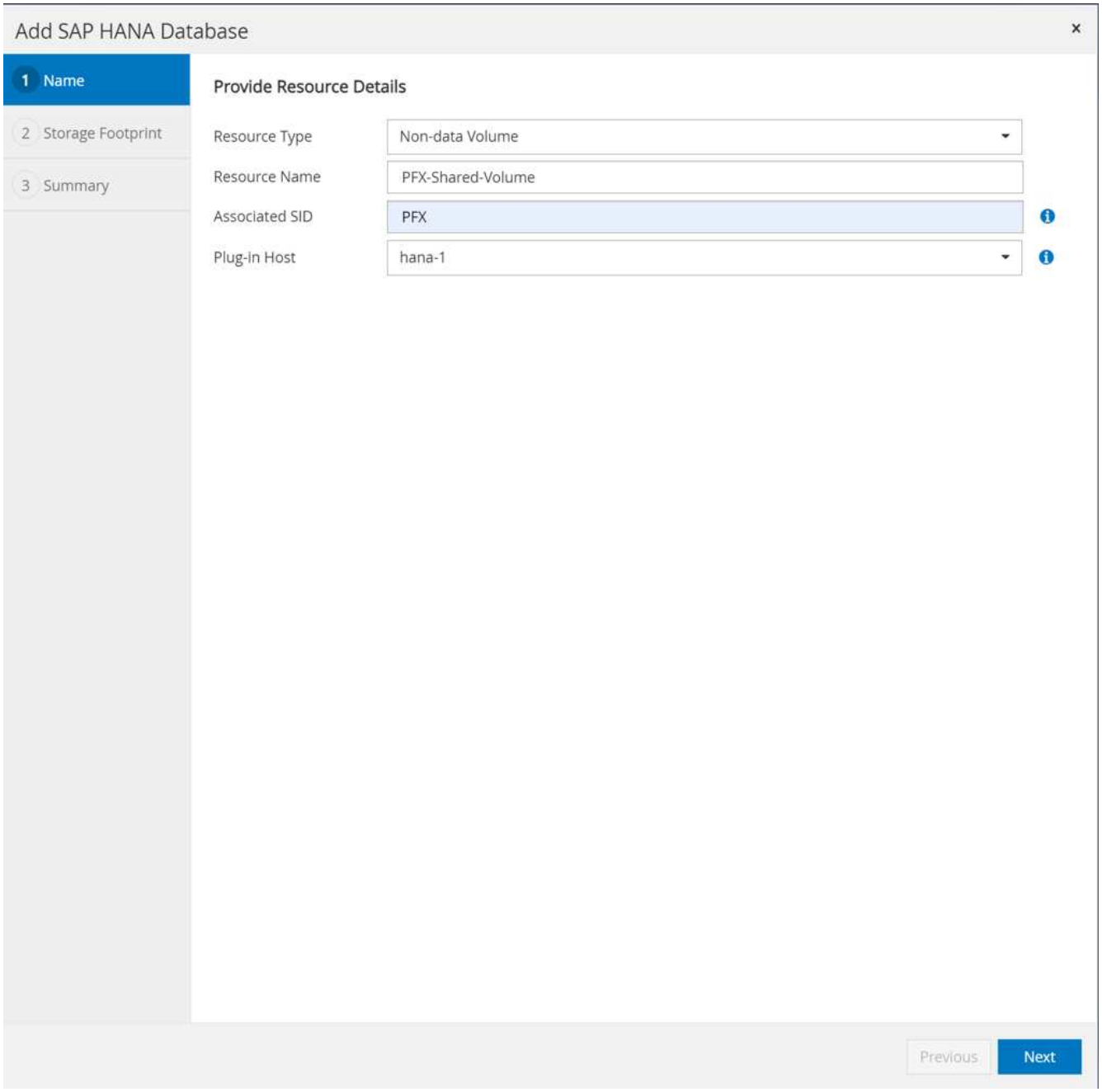
Configure los recursos que no sean de volúmenes en datos

Siga estos pasos para configurar recursos de volúmenes sin datos:

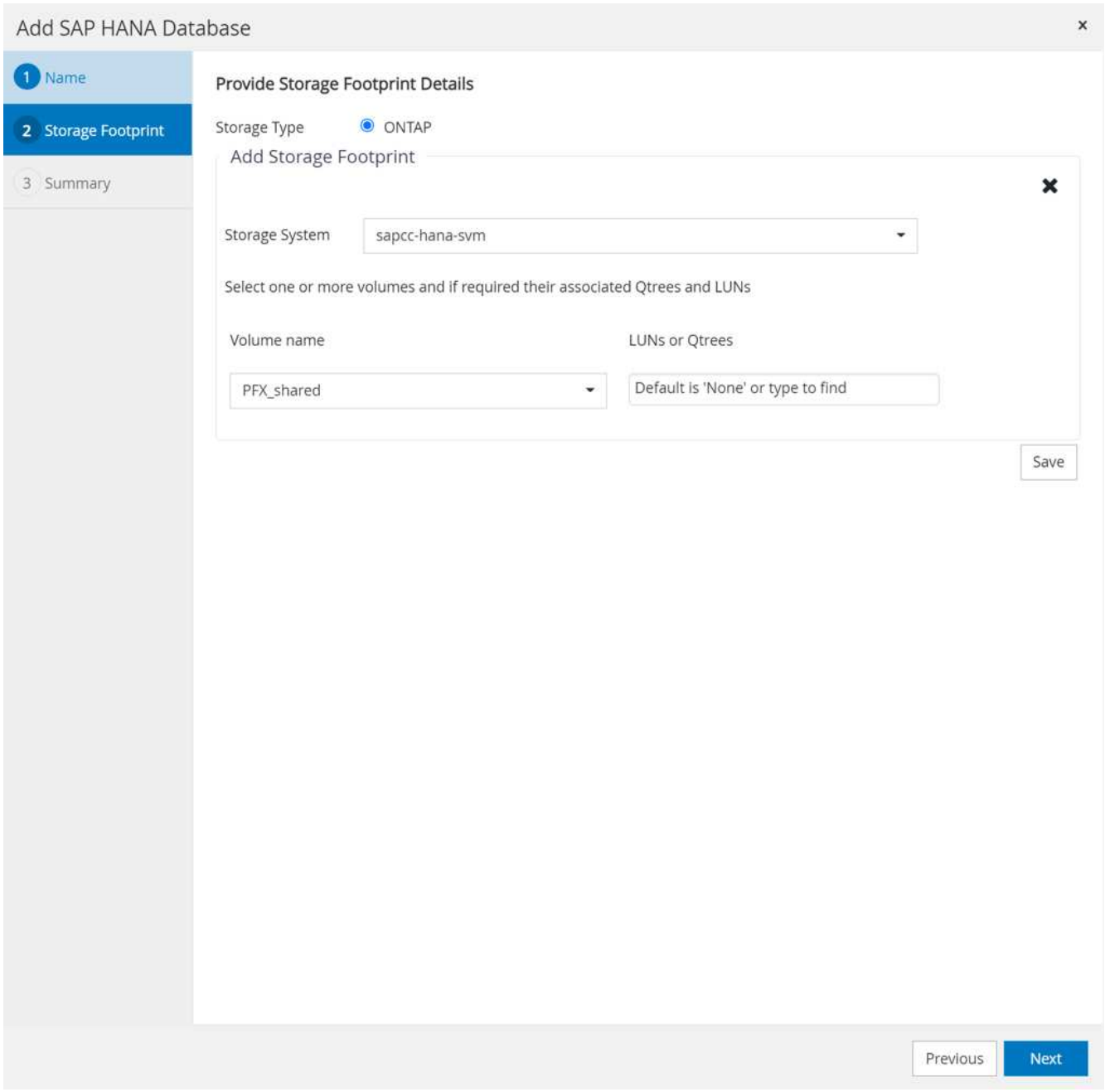
1. En la pestaña Resources, seleccione Non-Data-Volume y, a continuación, haga clic en Add SAP HANA Database.



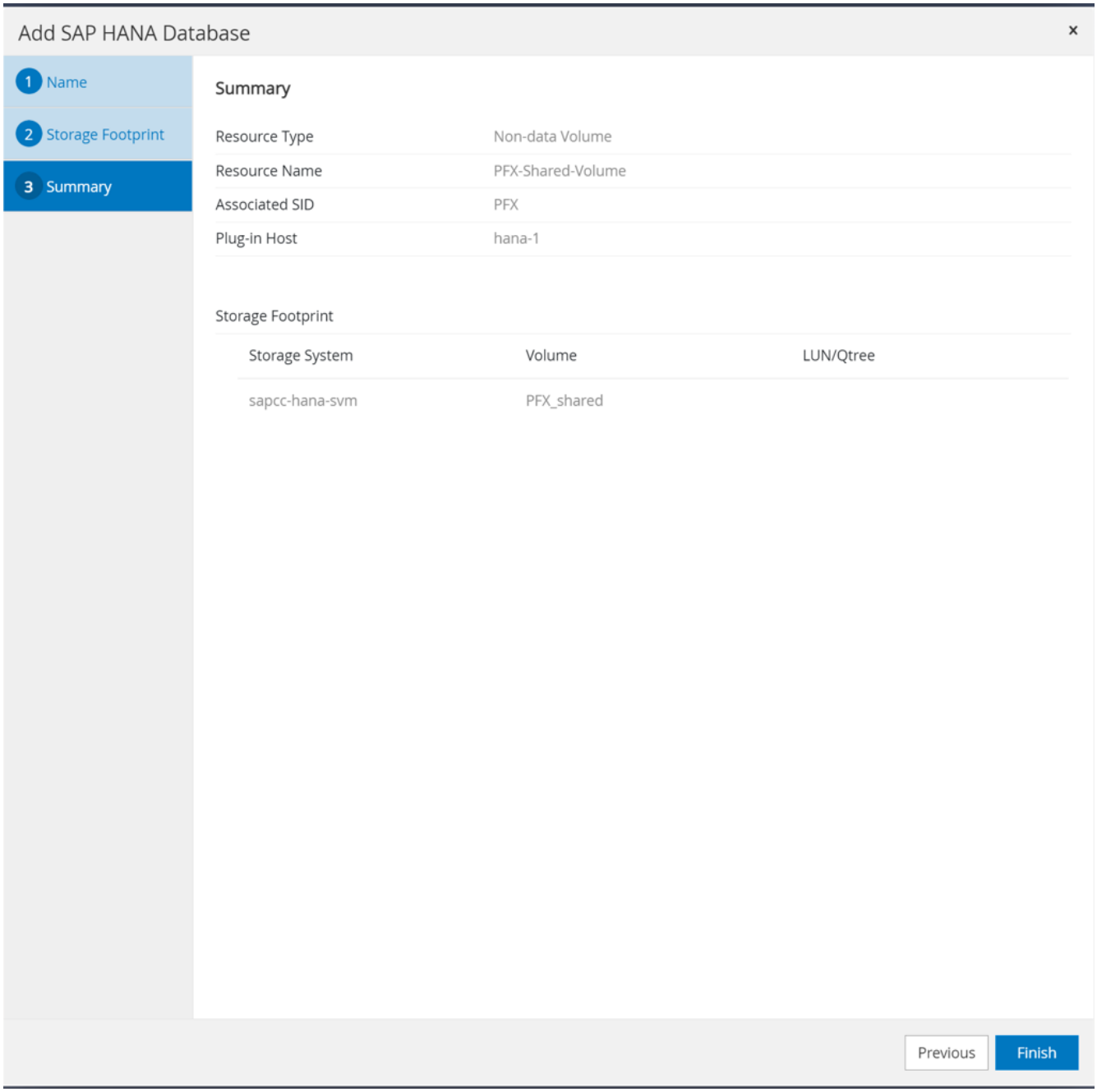
2. En el paso uno del cuadro de diálogo Add SAP HANA Database, en la lista Resource Type, seleccione Non-data Volumes. Especifique un nombre para el recurso y el SID asociado y el host del plugin de SAP HANA que desee usar para el recurso y, a continuación, haga clic en Next.



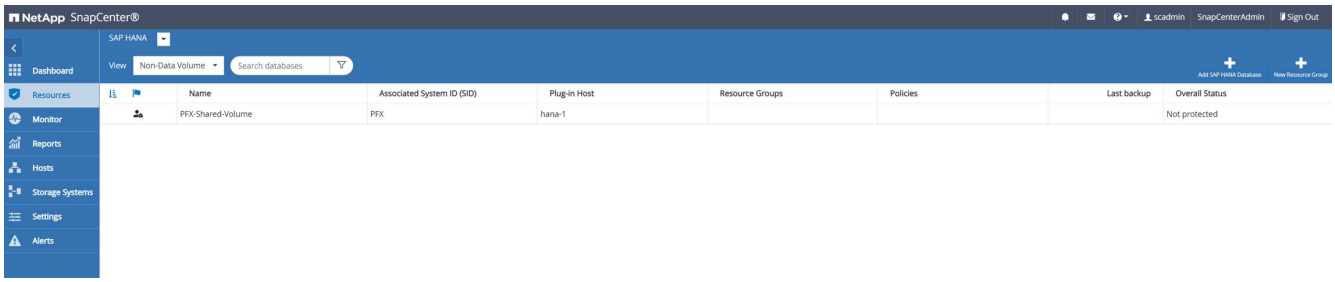
3. Añada la SVM y el volumen de almacenamiento como espacio físico de almacenamiento y, a continuación, haga clic en Next.



4. Para guardar la configuración, en el paso de resumen, haga clic en Finalizar.



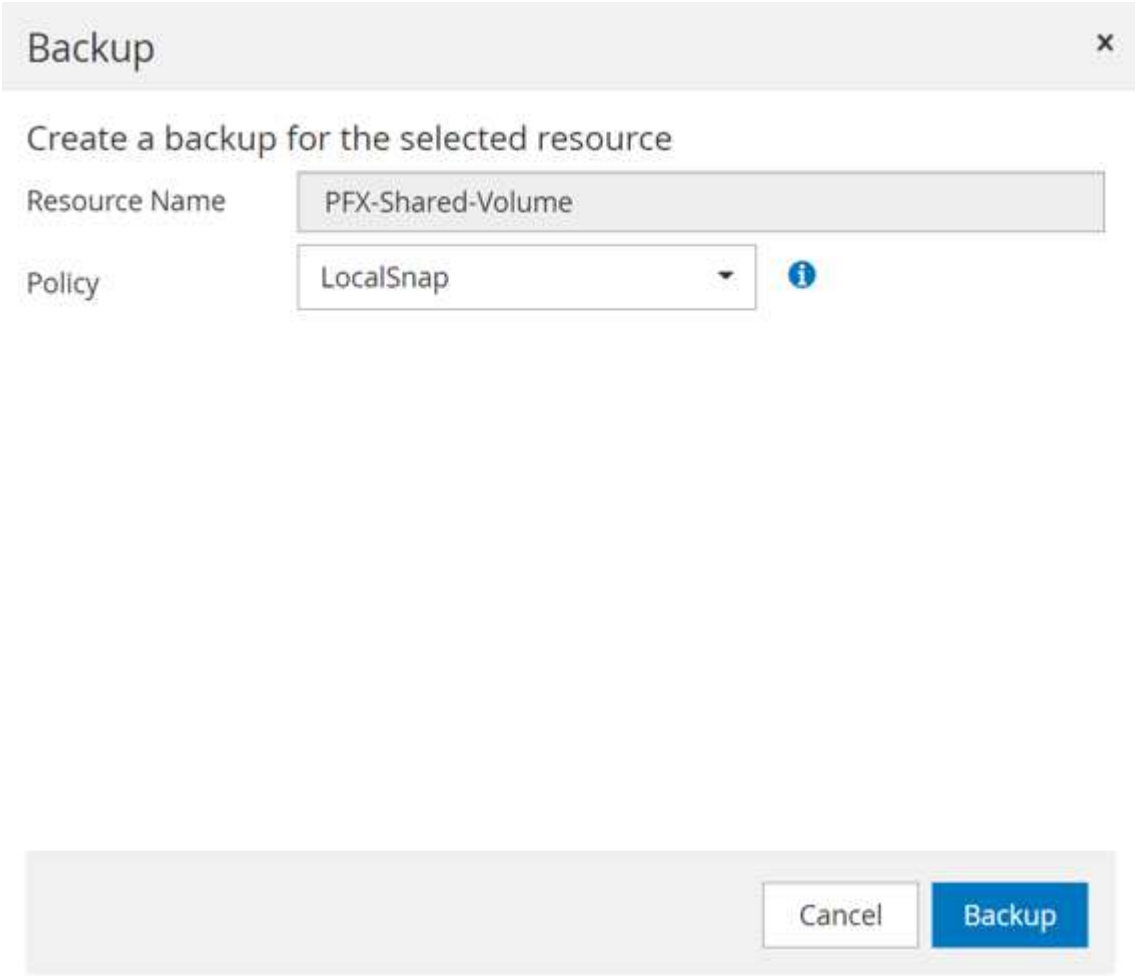
El nuevo volumen sin datos se añade a SnapCenter. Haga doble clic en el nuevo recurso para ejecutar la protección de recursos.



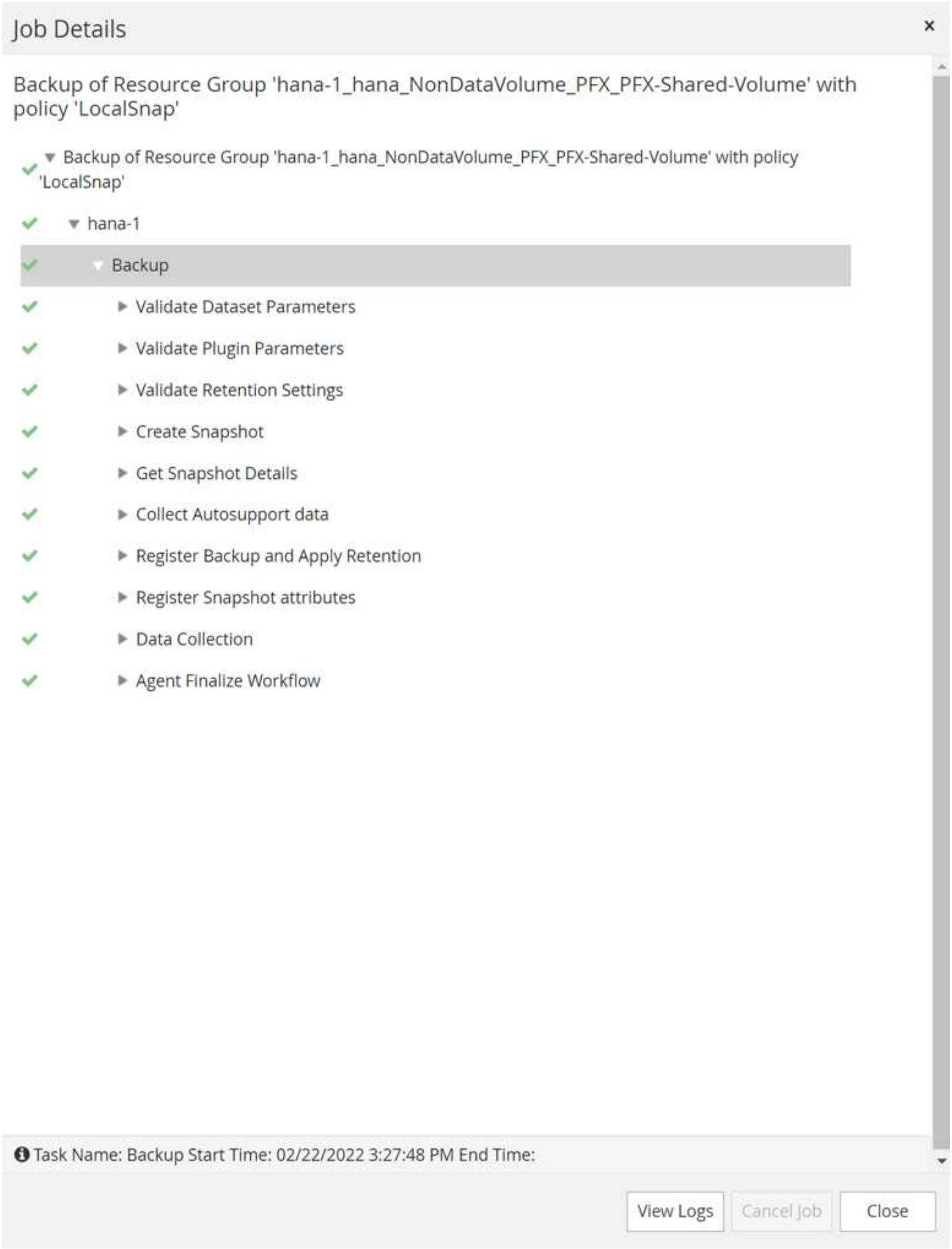
La protección de recursos se realiza del mismo modo que se describe antes con un recurso de base de datos HANA.

5. Ahora puede ejecutar una copia de seguridad haciendo clic en Backup Now.

6. Seleccione la política e inicie la operación de backup.

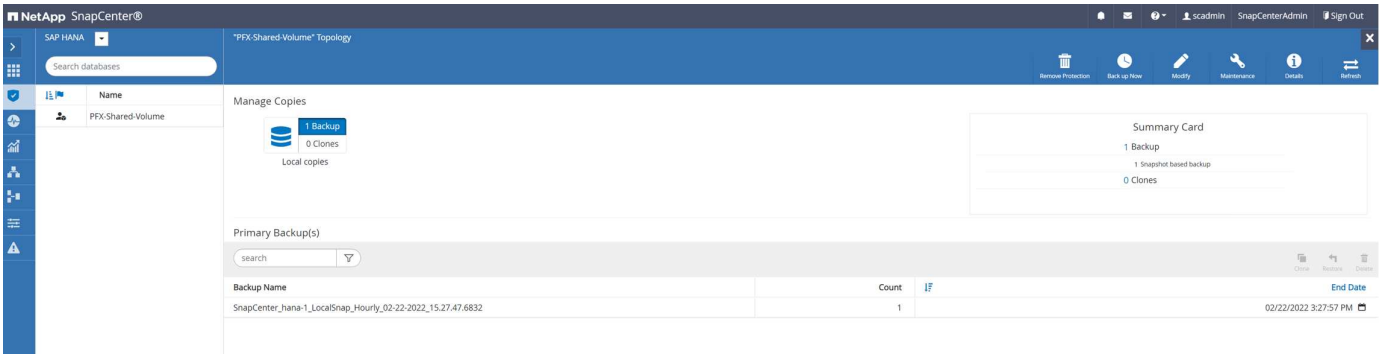


El registro de trabajos de SnapCenter muestra los pasos del flujo de trabajo individual.



El nuevo backup ahora se puede ver en la vista de recursos del recurso del volumen no relacionado con

datos.



Restaurar y recuperar

Con SnapCenter, las operaciones automatizadas de restauración y recuperación son compatibles con los sistemas MDC de host único de HANA con un solo inquilino. Para los sistemas de varios hosts o MDC con varios inquilinos, SnapCenter solo ejecuta la operación de restauración y se debe ejecutar la recuperación manualmente.

Puede ejecutar una operación de restauración y recuperación automatizada con los siguientes pasos:

1. Seleccione el backup que se usará para la operación de restauración.
2. Seleccione el tipo de restauración. Seleccione completar restauración con reversión de volumen o sin reversión de volumen.
3. Seleccione el tipo de recuperación de las siguientes opciones:
   - Al estado más reciente
   - Momento específico
   - A backups de datos específicos
   - Sin recuperación

     El tipo de recuperación seleccionado se utiliza para la recuperación del sistema y la base de datos de tenant.

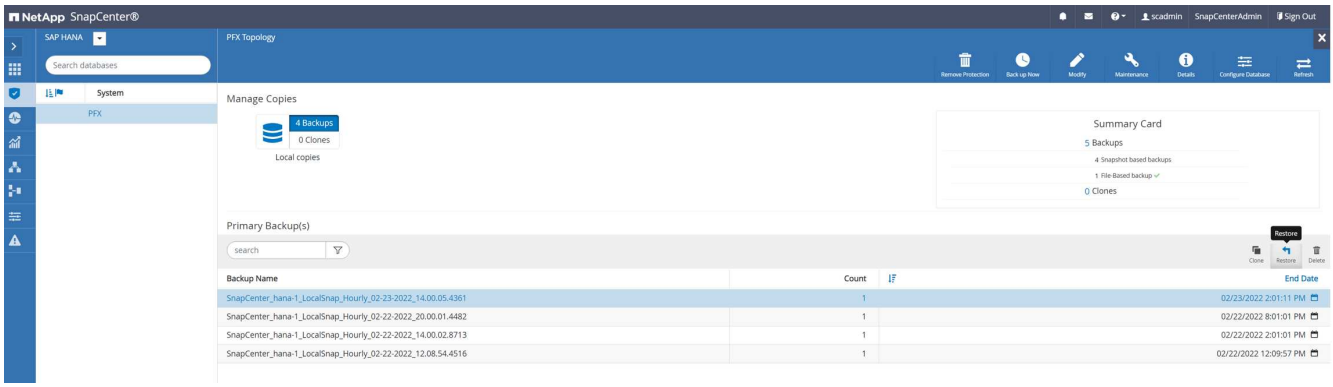
A continuación, SnapCenter realiza las siguientes operaciones:

1. Detiene la base de datos HANA.
2. Restaura la base de datos. Según el tipo de restauración seleccionado, se ejecutan diferentes operaciones.
   - Si se selecciona Volume Revert, entonces SnapCenter desmonta el volumen, restaura el volumen mediante el uso de SnapRestore basado en volumen en la capa de almacenamiento y monta el volumen.
   - Si no se selecciona Volume Revert, SnapCenter restaura todos los archivos mediante operaciones de SnapRestore de archivos individuales en la capa de almacenamiento.
3. Recupera la base de datos:
   a. Recuperando la base de datos del sistema
   b. recuperar la base de datos de tenant
   c. Iniciar la base de datos HANA

Si no se selecciona ninguna recuperación, se cerrará SnapCenter y deberá realizar la operación de restauración del sistema y la base de datos de tenant manualmente.

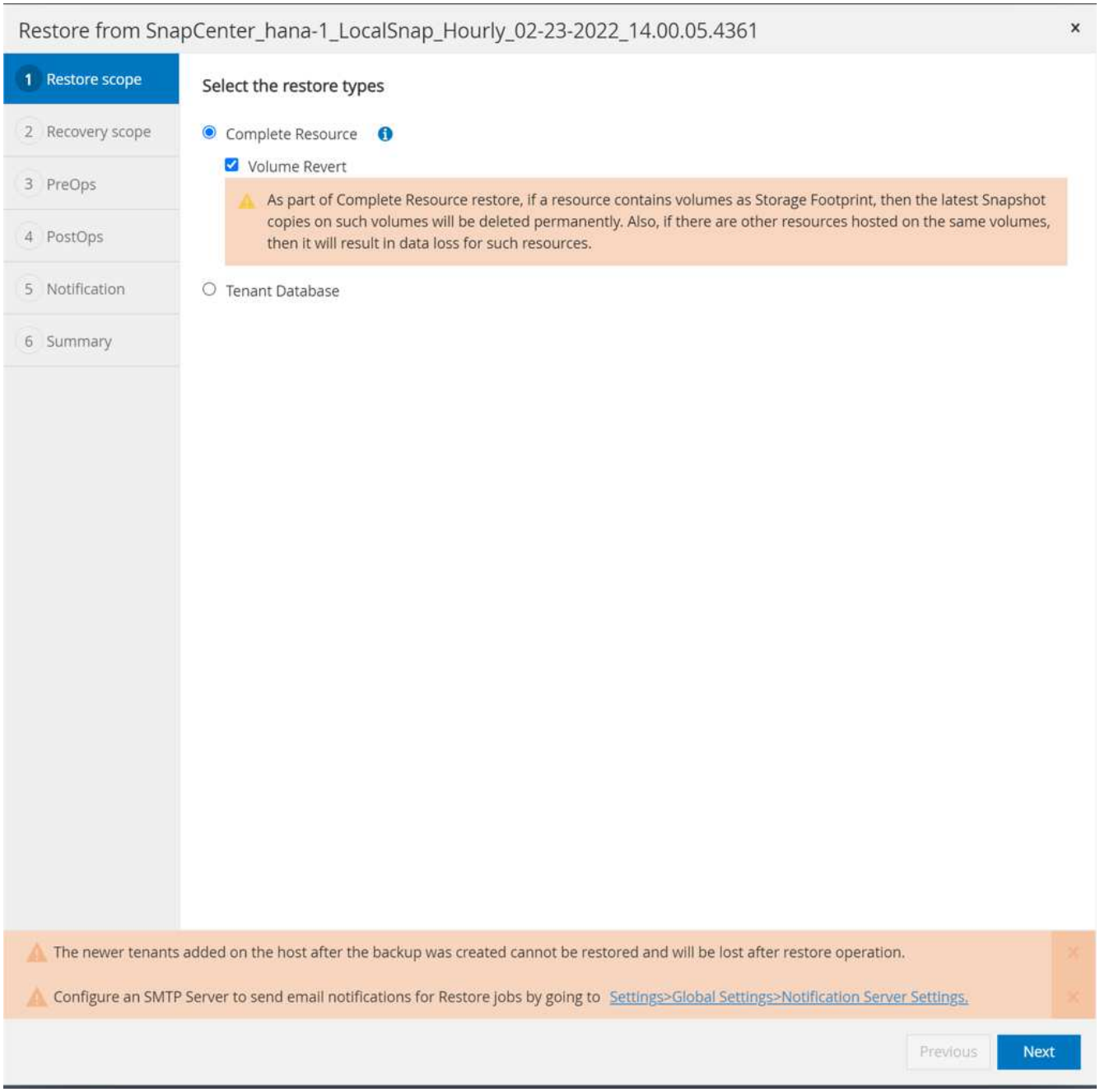
Para realizar una operación de restauración manual, siga estos pasos:

1. Seleccione un backup en SnapCenter que se usará para la operación de restauración.



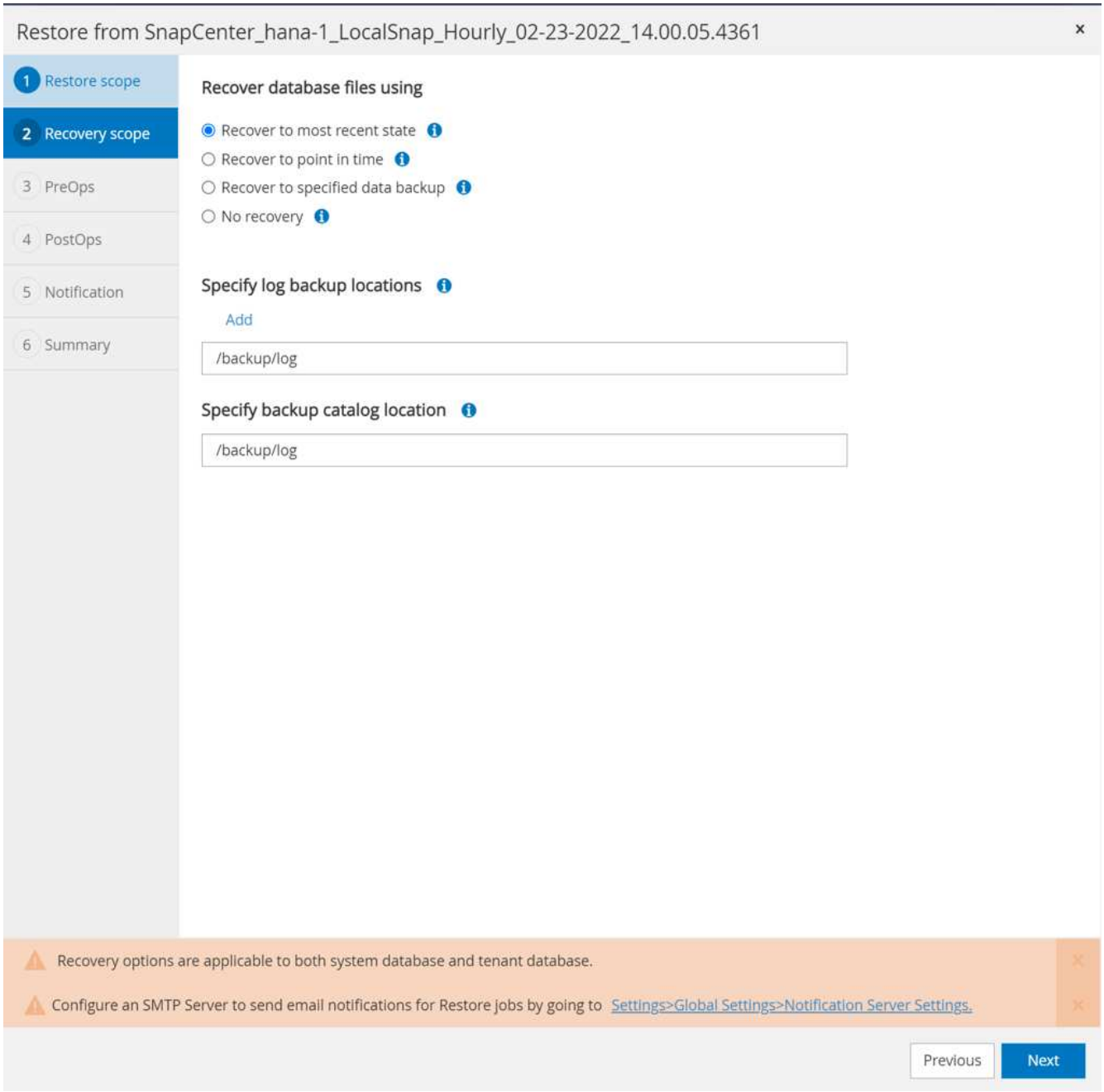
2. Seleccione el ámbito y el tipo de restauración.

   El escenario estándar para los sistemas de un solo inquilino MDC de HANA es utilizar un recurso completo con reversión de volumen. Para un sistema MDC de HANA con varios inquilinos, puede que desee restaurar solo un tenant. Para obtener más información sobre la restauración de un solo inquilino, consulte "Restauración y recuperación (netapp.com)".

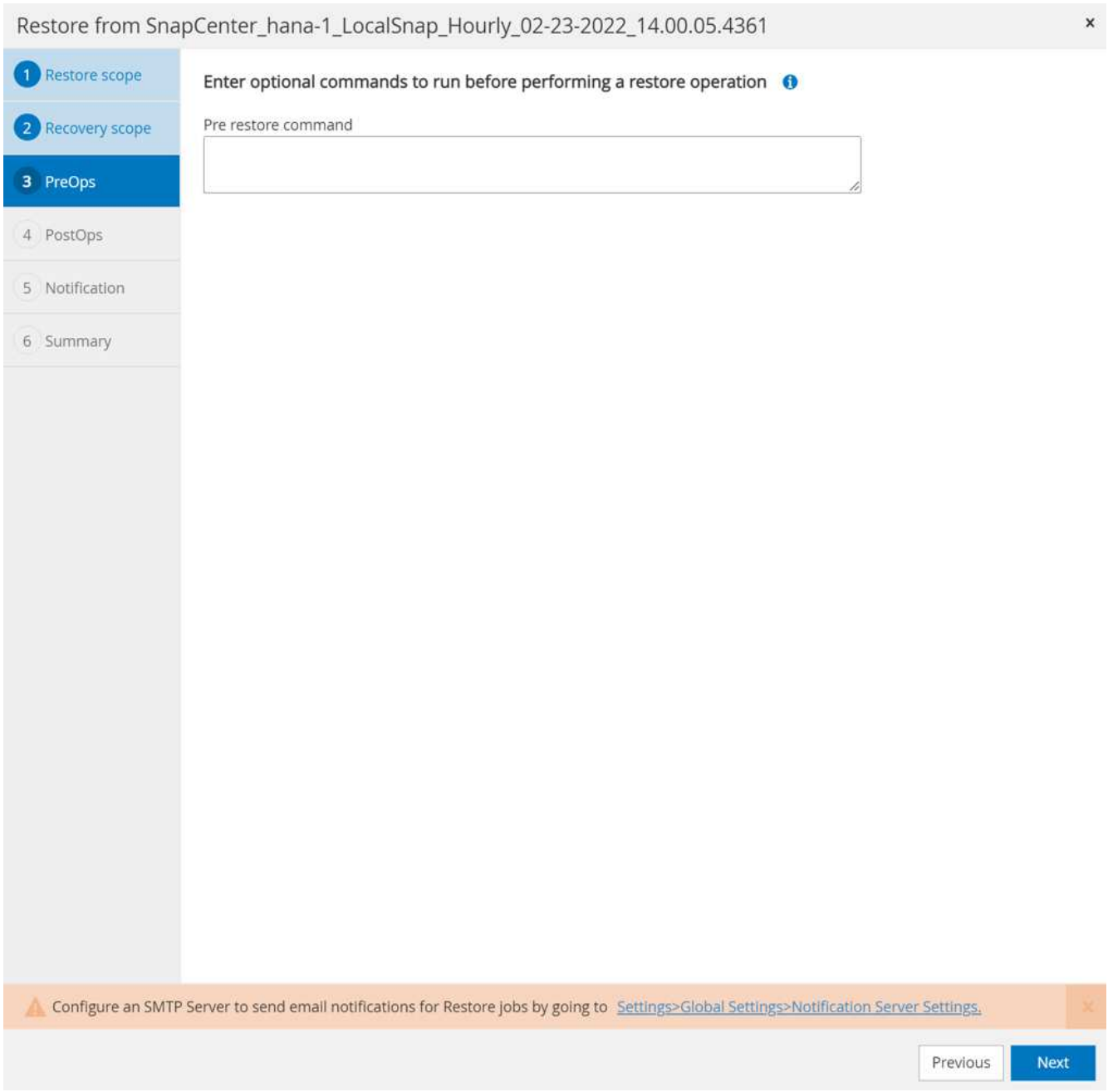


3. Seleccione Recovery Scope y proporcione la ubicación para backup de registros y backup de catálogo.

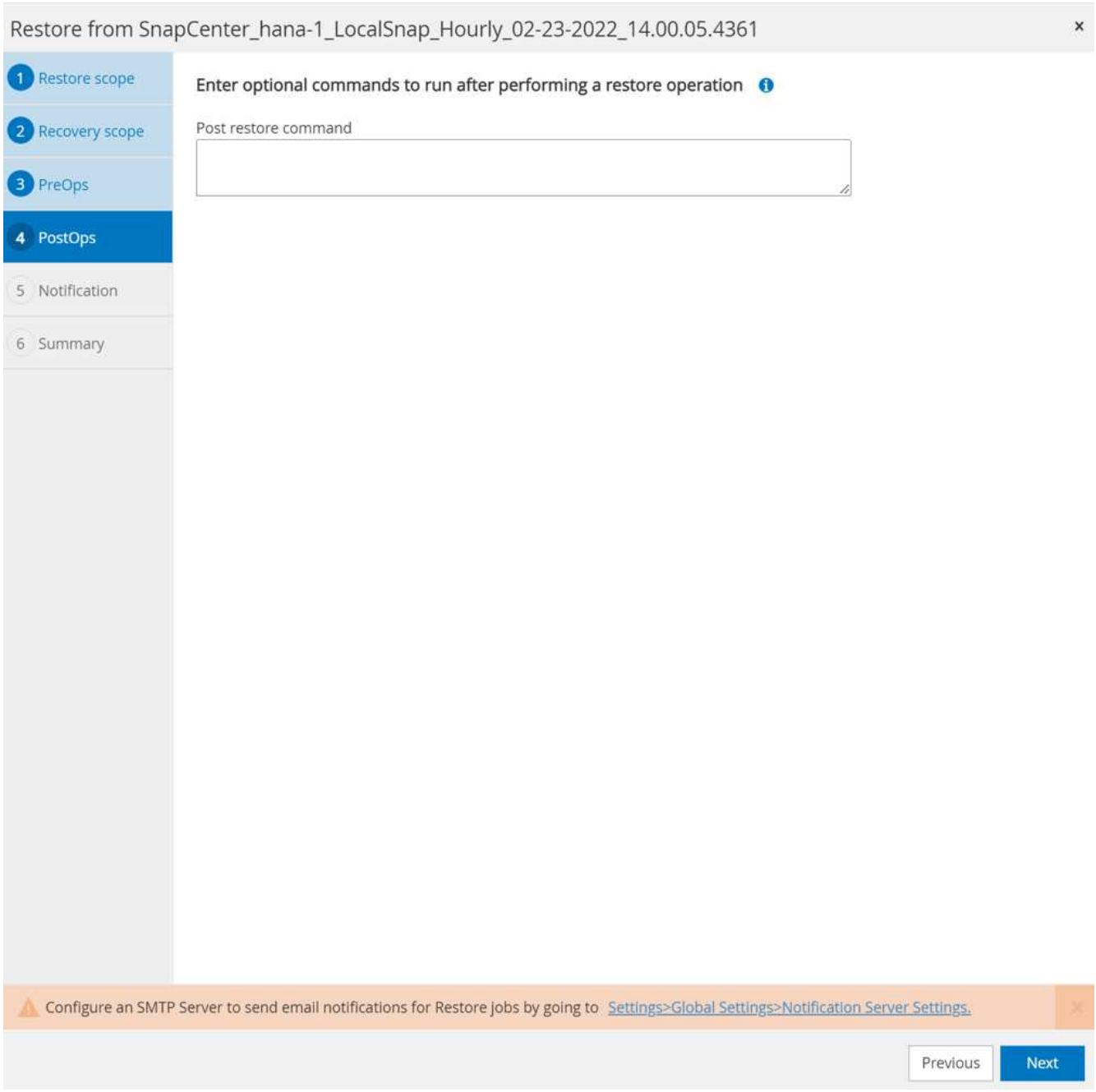
   SnapCenter utiliza la ruta predeterminada o las rutas modificadas en el archivo HANA global.ini para rellenar previamente las ubicaciones de backup de registros y catálogos.



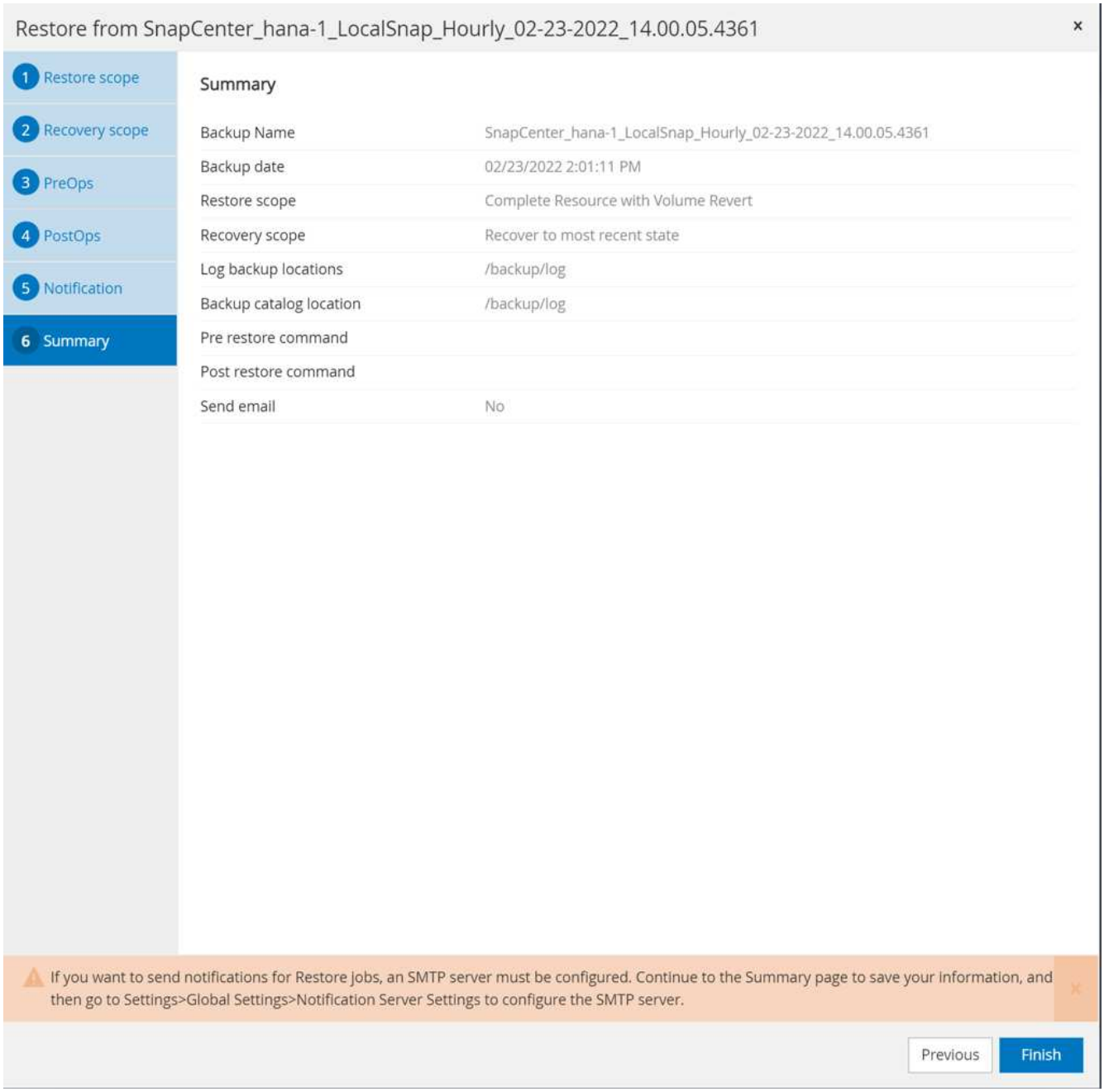
4. Introduzca los comandos previos a la restauración opcionales.



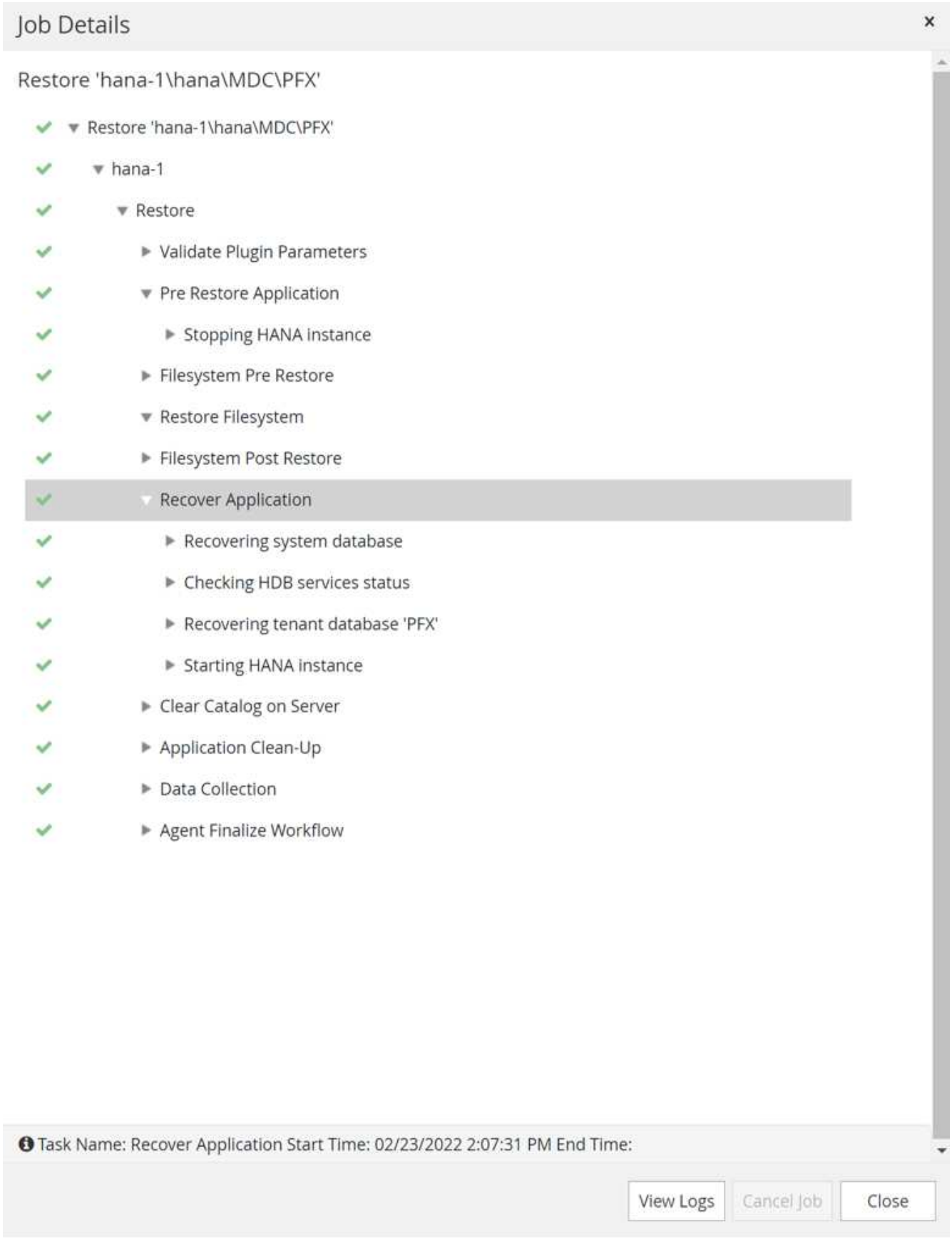
5. Introduzca los comandos posteriores a la restauración opcionales.



6. Para iniciar la operación de restauración y recuperación, haga clic en Finish.



SnapCenter ejecuta la operación de restauración y recuperación. Este ejemplo muestra los detalles de la tarea de restauración y recuperación.

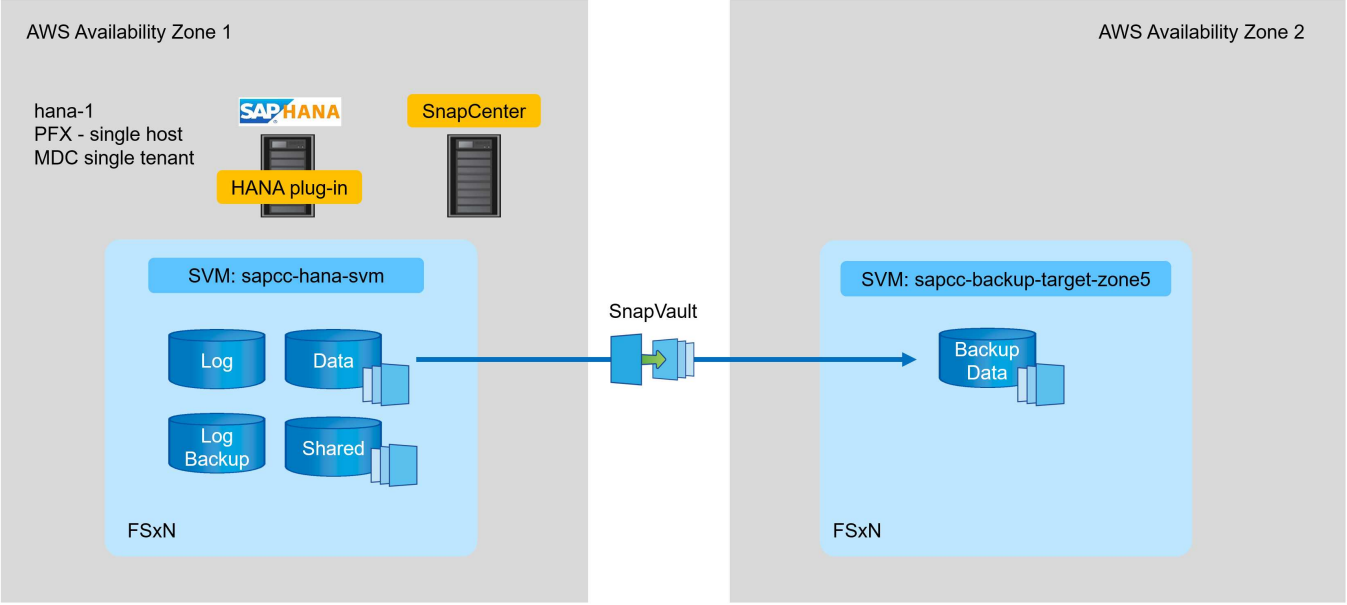

Job Details
Restore 'hana-1\hana\MDC\PFX'
Restore 'hana-1\hana\MDC\PFX'
hana-1
Restore
Validate Plugin Parameters
Pre Restore Application
Stopping HANA instance
Filesystem Pre Restore
Restore Filesystem
Filesystem Post Restore
Recover Application
Recovering system database
Checking HDB services status
Recovering tenant database 'PFX'
Starting HANA instance
Clear Catalog on Server
Application Clean-Up
Data Collection
Agent Finalize Workflow
Task Name: Recover Application Start Time: 02/23/2022 2:07:31 PM End Time:
View Logs
Cancel Job
Close

Replicación de backups con SnapVault

Descripción general: Replicación de backup con SnapVault

En nuestra configuración de laboratorio, utilizamos un segundo FSX para el sistema de archivos ONTAP en una segunda zona de disponibilidad de AWS para mostrar la replicación de backup del volumen de datos de HANA.

Como se explica en el capítulo ""Estrategia de protección de datos"", El destino de replicación debe ser un segundo FSX para que el sistema de archivos ONTAP de otra zona de disponibilidad esté protegido de un fallo del FSX primario para el sistema de archivos ONTAP. Además, el volumen compartido de HANA se debe replicar en el FSX secundario para el sistema de archivos ONTAP.



Descripción general de los pasos de configuración

Hay un par de pasos de configuración que debe ejecutar en la capa FSX para ONTAP. Puede hacerlo con Cloud Manager de NetApp o con la línea de comandos FSX para ONTAP.

1. FSX de paridad para sistemas de archivos ONTAP. Los FSX para sistemas de archivos ONTAP deben tener una relación entre iguales para permitir la replicación entre sí.
2. SVM de paridad. Las instancias de SVM deben tener una relación entre iguales para permitir la replicación entre sí.
3. Cree un volumen de destino. Cree un volumen en la SVM de destino con el tipo de volumen `DP`. Tipo `DP` se debe utilizar como volumen de destino de replicación.
4. Cree una política de SnapMirror. Esto se utiliza para crear una política para la replicación con el tipo `vault`.
   a. Agregar una regla a la directiva. La regla contiene la etiqueta de SnapMirror y la retención para backups en el sitio secundario. Debe configurar la misma etiqueta de SnapMirror más adelante en la política de SnapCenter para que SnapCenter cree backups de Snapshot en el volumen de origen que contiene esta etiqueta.
5. Crear una relación de SnapMirror. Define la relación de replicación entre el volumen de origen y el de

destino, y adjunta una política.

6. Inicializar SnapMirror. Esto inicia la replicación inicial en la que se transfieren los datos de origen completos al volumen objetivo.

Cuando la configuración de replicación de volúmenes se completa, es necesario configurar la replicación de backup en SnapCenter de la siguiente manera:

1. Añada la SVM de destino a SnapCenter.
2. Cree una nueva política de SnapCenter para backup de Snapshot y replicación de SnapVault.
3. Añada la política a la protección de recursos HANA.
4. Ahora puede ejecutar backups con la nueva normativa.

Los siguientes capítulos describen los pasos individuales con más detalle.

Configurar las relaciones de replicación en FSX para los sistemas de archivos ONTAP

Puede encontrar información adicional sobre las opciones de configuración de SnapMirror en la documentación de ONTAP en "Flujo de trabajo de replicación de SnapMirror (netapp.com)".

- FSX de origen para el sistema de archivos ONTAP: `FsxId00fa9e3c784b6abbb`
- SVM de origen: `sapcc-hana-svm`
- FSX de destino para el sistema de archivos ONTAP: `FsxId05f7f00af49dc7a3e`
- SVM de destino: `sapcc-backup-target-zone5`

FSX de paridad para sistemas de archivos ONTAP

```
FsxId00fa9e3c784b6abbb::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId00fa9e3c784b6abbb
            inter_1      up/up    10.1.1.57/24
FsxId00fa9e3c784b6abbb-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.7/24
FsxId00fa9e3c784b6abbb-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId05f7f00af49dc7a3e
            inter_1      up/up    10.1.2.144/24
FsxId05f7f00af49dc7a3e-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.69/24
FsxId05f7f00af49dc7a3e-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> cluster peer create -address-family ipv4 -peer
-addrs 10.1.1.57, 10.1.2.7
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command
in the other cluster.
```

`peer-addrs` Son las IP de clúster del clúster de destino.

```
FsxId00fa9e3c784b6abbb::>  cluster peer create -address-family ipv4 -peer
-addrs  10.1.2.144, 10.1.2.69
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
        phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
FsxId00fa9e3c784b6abbb::>
FsxId00fa9e3c784b6abbb::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
FsxId05f7f00af49dc7a3e    1-80-000011           Available      ok
```

SVM de paridad

```
FsxId05f7f00af49dc7a3e::> vserver peer create -vserver sapcc-backup-
target-zone5 -peer-vserver sapcc-hana-svm -peer-cluster
FsxId00fa9e3c784b6abbb -applications snapmirror
Info: [Job 41] 'vserver peer create' job queued
```

```
FsxId00fa9e3c784b6abbb::> vserver peer accept -vserver sapcc-hana-svm
-peer-vserver sapcc-backup-target-zone5
Info: [Job 960] 'vserver peer accept' job queued
```

```
FsxId05f7f00af49dc7a3e::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
sapcc-backup-target-zone5
            peer-source-cluster
                        peered       FsxId00fa9e3c784b6abbb
                                                       snapmirror
sapcc-hana-svm
```

Cree un volumen de destino

Debe crear el volumen objetivo con el tipo `DP` para marcarla como un destino de replicación.

```
FsxId05f7f00af49dc7a3e::> volume create -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -aggregate aggr1 -size 100GB -state online
-policy default -type DP -autosize-mode grow_shrink -snapshot-policy none
-foreground true -tiering-policy all -anti-ransomware-state disabled
[Job 42] Job succeeded: Successful
```

Cree una política de SnapMirror

La política de SnapMirror y la regla añadida definen la retención y la etiqueta de SnapMirror para identificar los Snapshots que deben replicarse. Al crear la política de SnapCenter más adelante, debe usar la misma etiqueta.

```
FsxId05f7f00af49dc7a3e::> snapmirror policy create -policy snapcenter-
policy -tries 8 -transfer-priority normal -ignore-atime false -restart
always -type vault -vserver sapcc-backup-target-zone5
```

```
FsxId05f7f00af49dc7a3e::> snapmirror policy add-rule -vserver sapcc-
backup-target-zone5  -policy snapcenter-policy -snapmirror-label
snapcenter -keep 14
```

```
FsxId00fa9e3c784b6abbb::> snapmirror policy showVserver Policy
Policy Number         Transfer
Name    Name               Type   Of Rules Tries Priority Comment
------- ------------------ ------ -------- ----- -------- ----------
FsxId00fa9e3c784b6abbb
        snapcenter-policy  vault         1     8  normal  -
  SnapMirror Label: snapcenter                          Keep:      14
                                                  Total Keep:      14
```

Crear una relación de SnapMirror

Ahora se define la relación entre el volumen de origen y el de destino, así como el tipo XDP y la política que hemos creado anteriormente.

```
FsxId05f7f00af49dc7a3e::> snapmirror create -source-path sapcc-hana-
svm:PFX_data_mnt00001 -destination-path sapcc-backup-target-
zone5:PFX_data_mnt00001 -vserver sapcc-backup-target-zone5 -throttle
unlimited -identity-preserve false -type XDP -policy snapcenter-policy
Operation succeeded: snapmirror create for the relationship with
destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

Inicializar SnapMirror

Con este comando, se inicia la replicación inicial. Esta es una transferencia completa de todos los datos del volumen de origen al volumen objetivo.

```
FsxId05f7f00af49dc7a3e::> snapmirror initialize -destination-path sapcc-
backup-target-zone5:PFX_data_mnt00001 -source-path sapcc-hana-
svm:PFX_data_mnt00001
Operation is queued: snapmirror initialize of destination "sapcc-backup-
target-zone5:PFX_data_mnt00001".
```

Puede comprobar el estado de la replicación con el `snapmirror show` comando.

```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
sapcc-hana-svm:PFX_data_mnt00001
            XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                              Uninitialized
                                      Transferring   1009MB    true
02/24 12:34:28
```

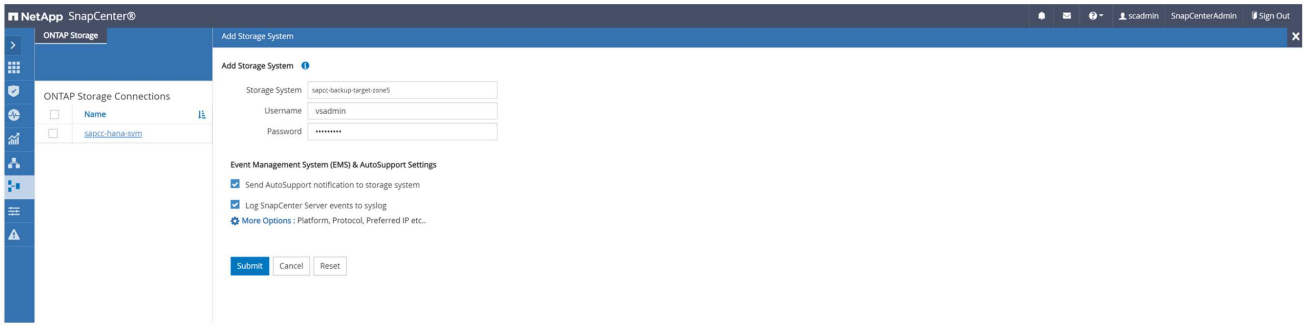
```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source             Destination Mirror  Relationship   Total
Last
Path         Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
sapcc-hana-svm:PFX_data_mnt00001
            XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                              Snapmirrored
                                      Idle           -         true    -
```

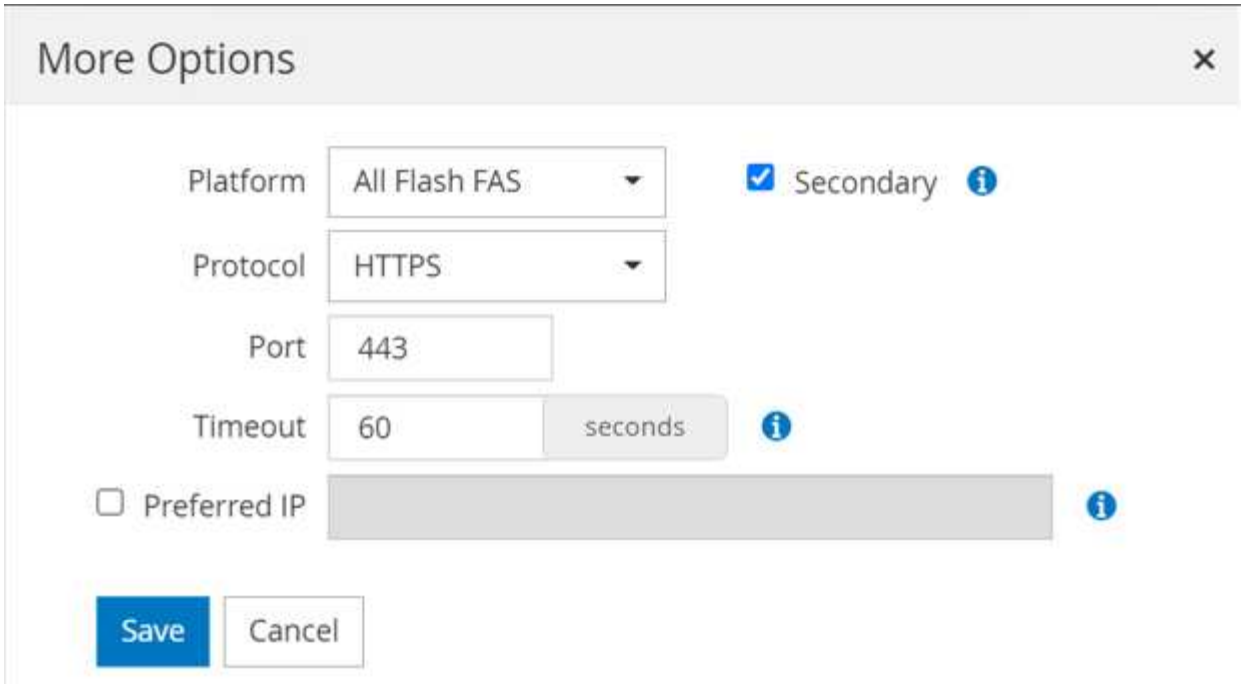
Añada una SVM de backup a SnapCenter

Para añadir una SVM de backup a SnapCenter, siga estos pasos:

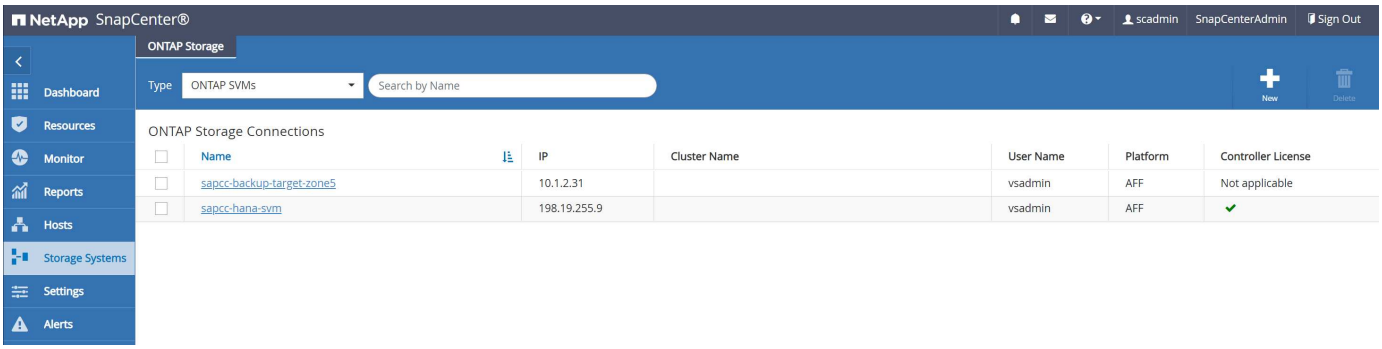
1. Configure la SVM donde el volumen de destino de SnapVault se encuentra en SnapCenter.



2. En la ventana More Options, seleccione All Flash FAS como la plataforma y seleccione Secondary.



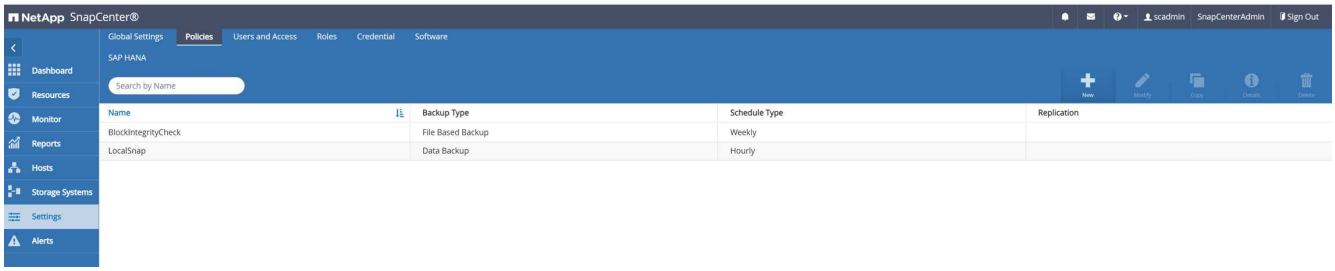
La SVM ya está disponible en SnapCenter.



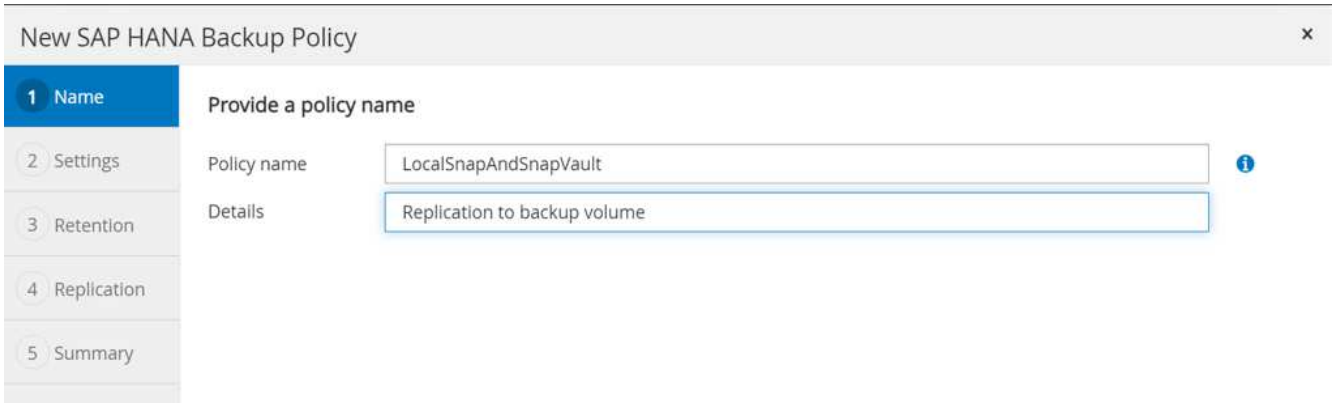
Cree una nueva política de SnapCenter para la replicación de backups

Debe configurar una política para la replicación de backups de la siguiente manera:

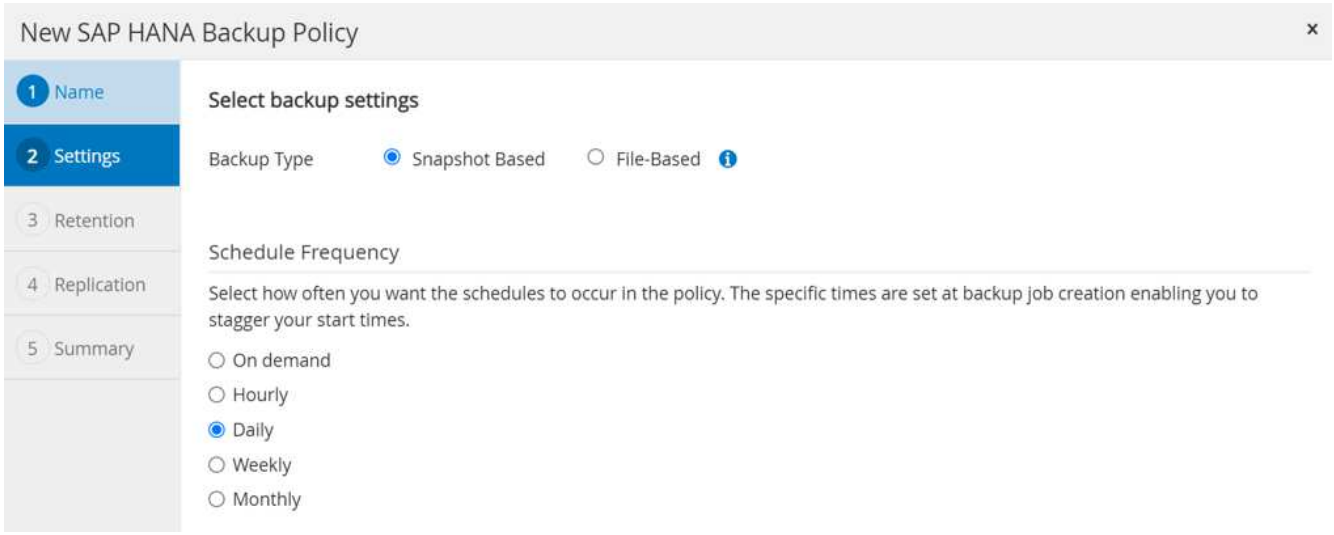
1. Escriba un nombre para la política.



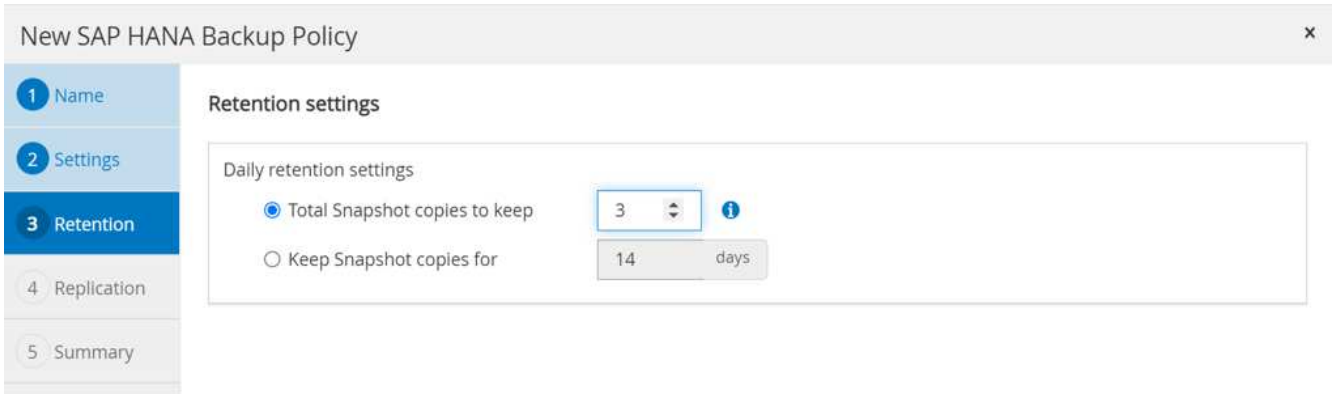
2. Seleccione Snapshot backup and a schedule frequency. Normalmente se utiliza diariamente para la replicación de backup.



3. Seleccione la retención para los backups de Snapshot.

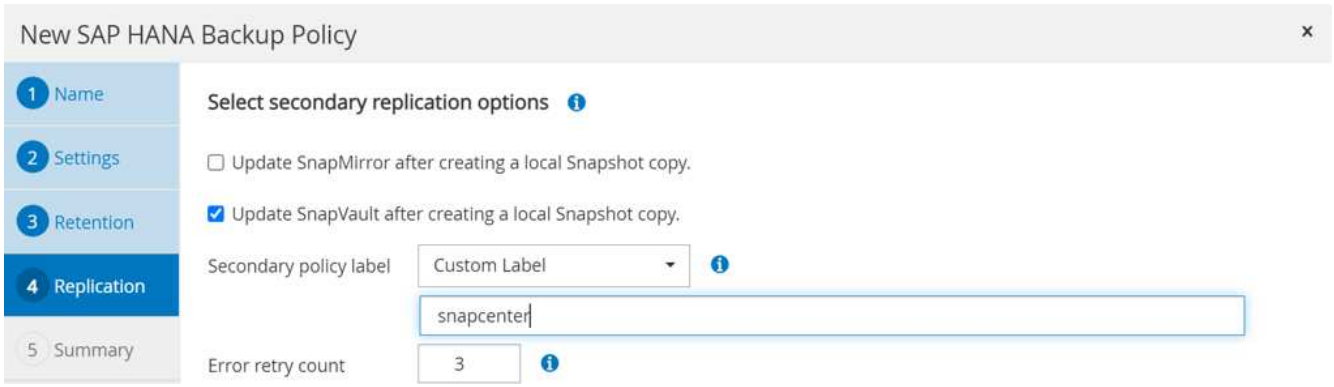


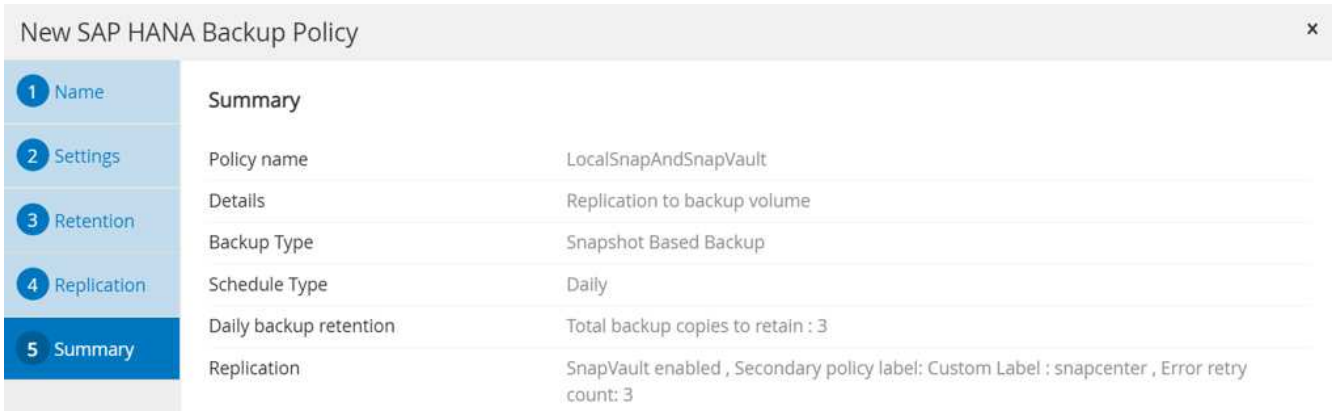
Esta es la retención de los backups de Snapshot diarios que se realizan en el almacenamiento primario. La retención de backups secundarios en el destino de SnapVault ya se ha configurado previamente mediante el comando add rule en el nivel ONTAP. Consulte “Configurar relaciones de replicación en FSX para sistemas de archivos ONTAP” (xref).



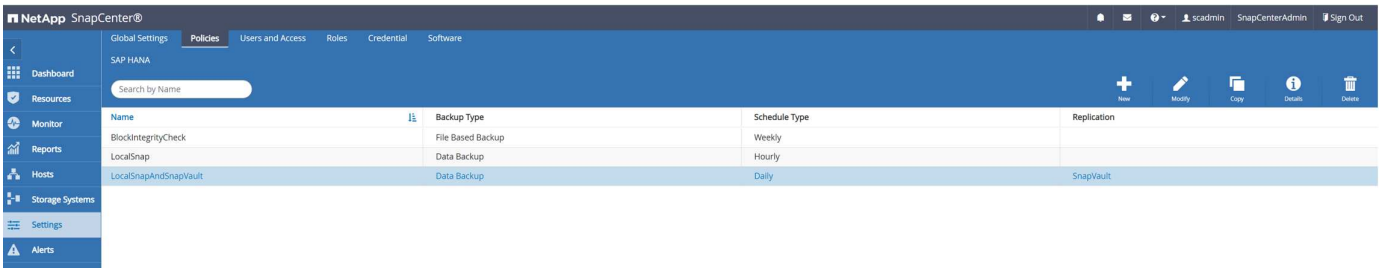
4. Seleccione el campo Update SnapVault y proporcione una etiqueta personalizada.

Esta etiqueta debe coincidir con la etiqueta de SnapMirror que se proporciona en la `add rule` Comando a nivel de ONTAP.



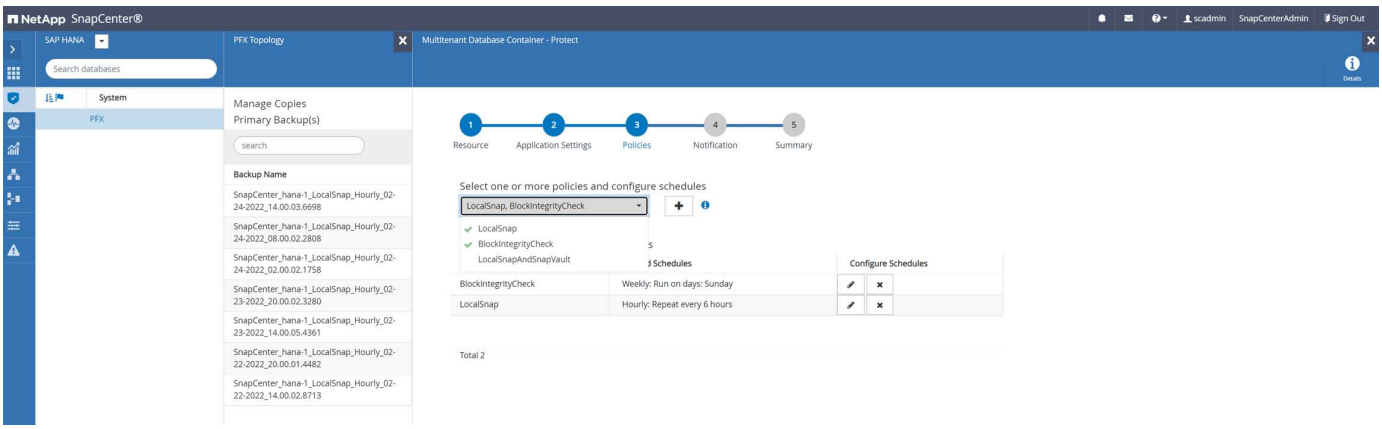


Se ha configurado la nueva política de SnapCenter.

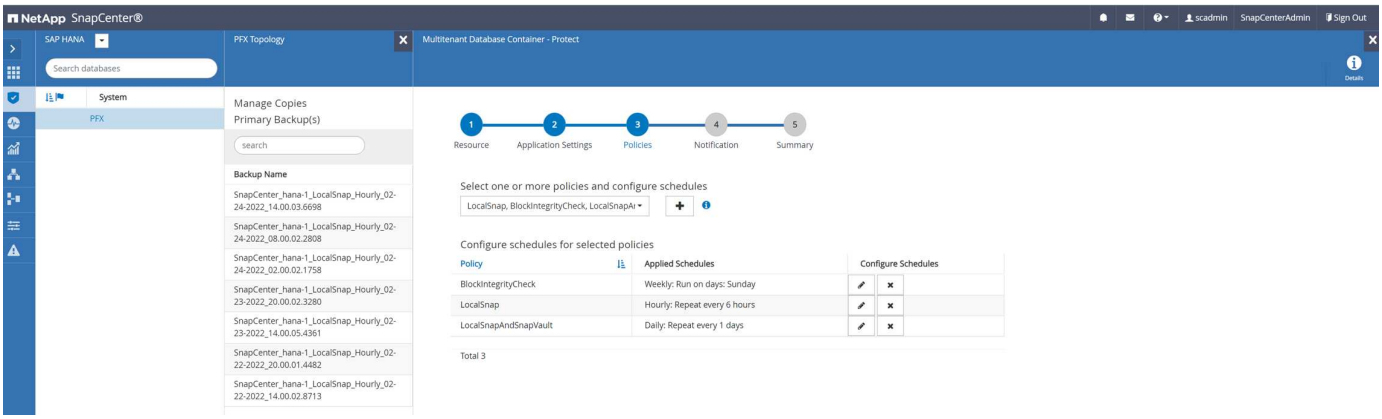


Añadir una política a la protección de recursos

Debe añadir la nueva política a la configuración de protección de recursos de HANA, como se muestra en la siguiente figura.



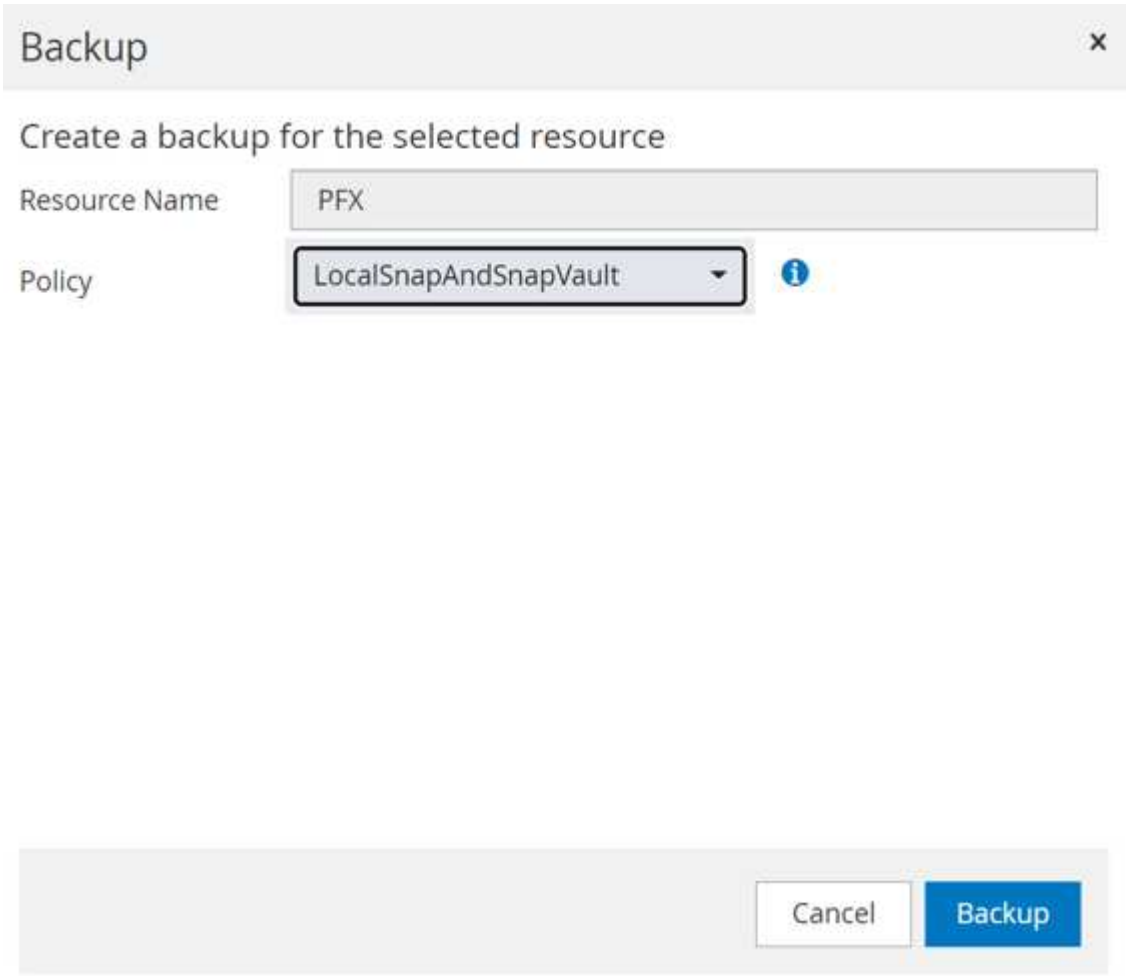
En nuestra configuración se define un programa diario.



Cree un backup con la replicación

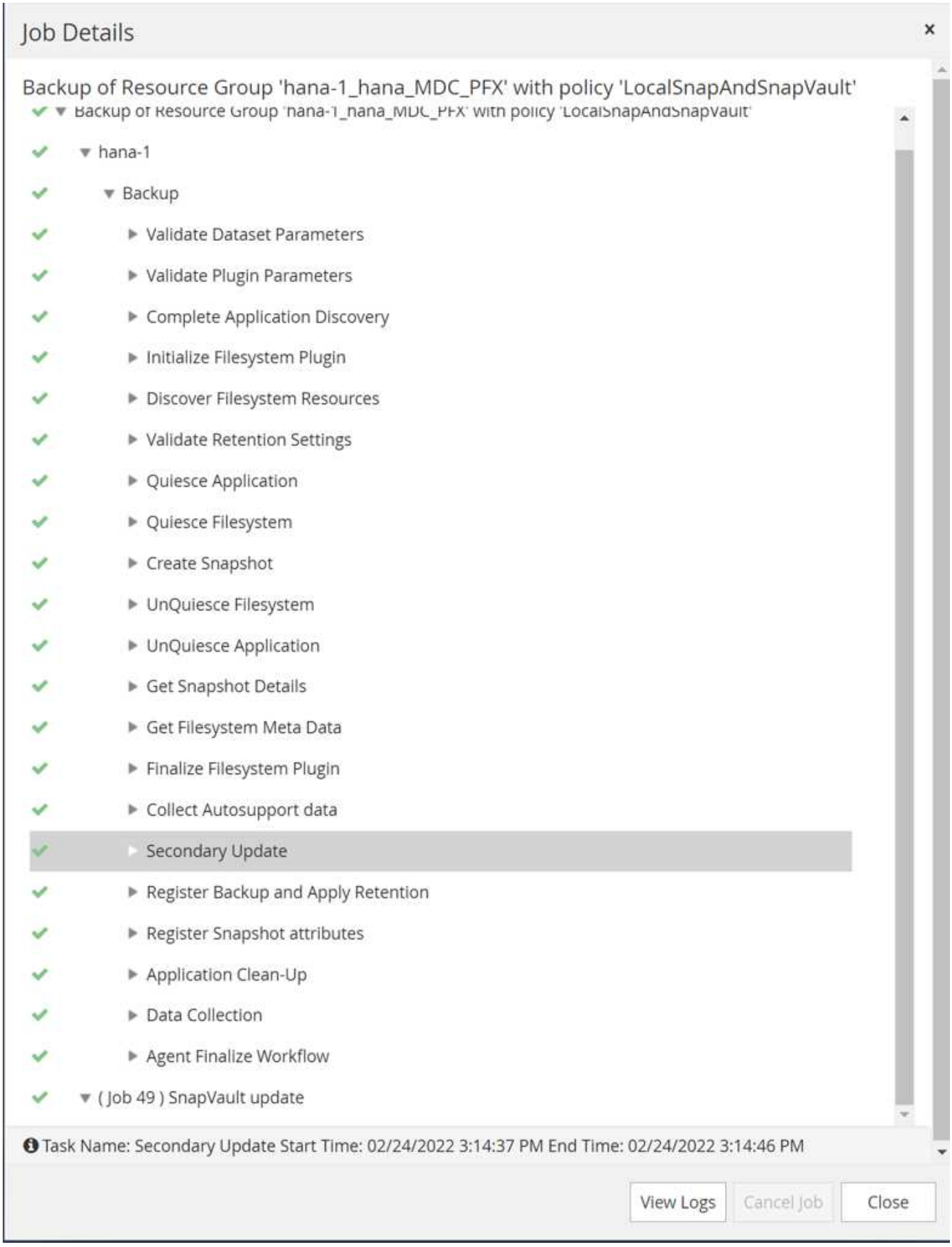
Se crea un backup del mismo modo que con una copia Snapshot local.

Para crear un backup con replicación, seleccione la política que incluye la replicación de backup y haga clic en Backup.



Dentro del registro de trabajos de SnapCenter, puede ver el paso actualización secundaria, que inicia una operación de actualización de SnapVault. Los bloques modificados de replicación del volumen de origen al

volumen objetivo.



En el FSX para el sistema de archivos ONTAP, se crea una copia Snapshot del volumen de origen con la etiqueta SnapMirror, `snapcenter`, Según se configuró en la directiva SnapCenter.

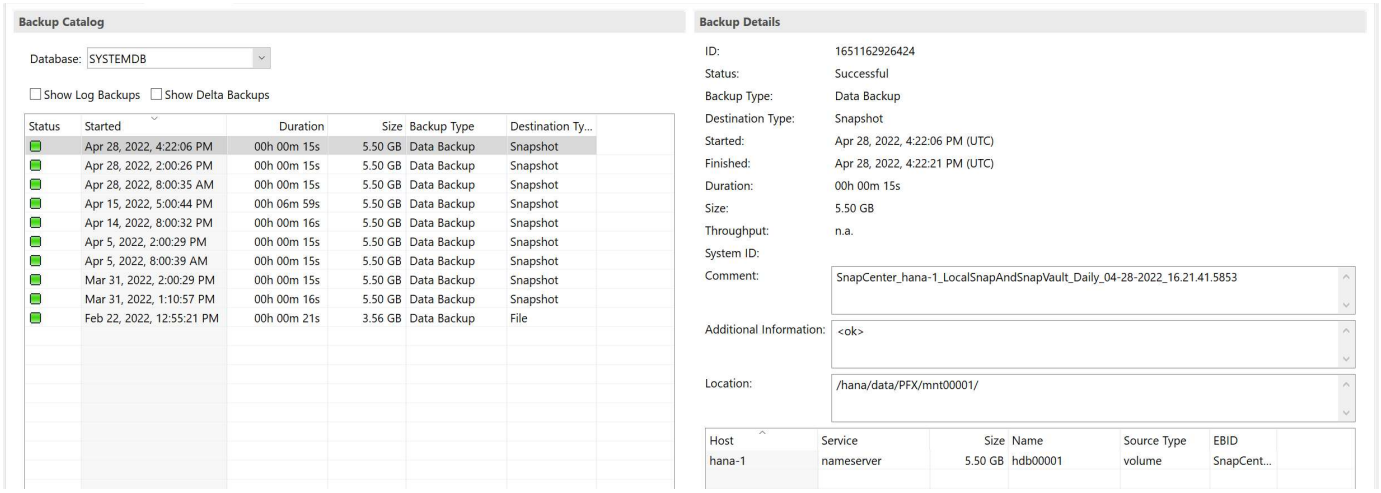
```
FsxId00fa9e3c784b6abbb::> snapshot show -vserver sapcc-hana-svm -volume
PFX_data_mnt00001 -fields snapmirror-label
vserver        volume            snapshot
snapmirror-label
-------------- -----------------
---------------------------------------------------------
----------------
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_13.10.26.5482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_14.00.05.2023 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_08.00.06.3380 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_14.00.01.6482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-14-
2022_20.00.05.0316 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_08.00.06.3629 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_14.00.01.7275 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853

snapcenter
8 entries were displayed.
```

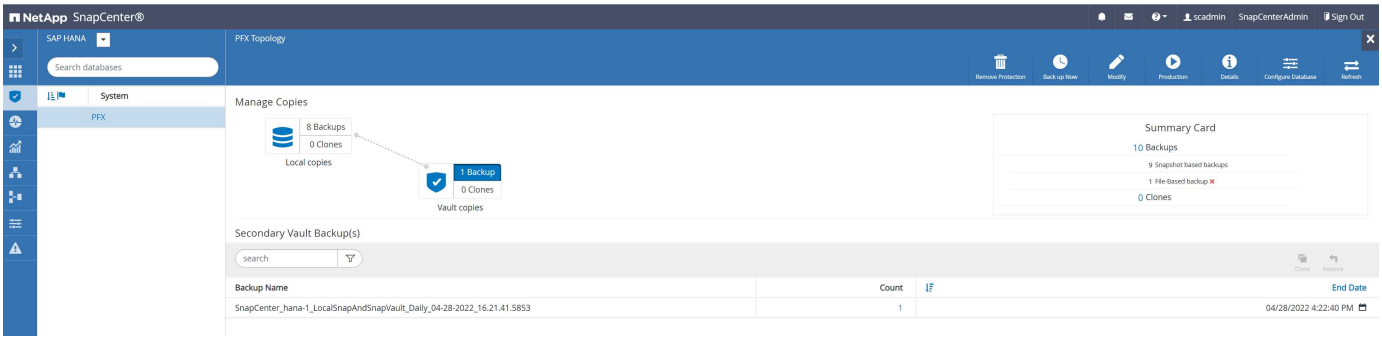
En el volumen objetivo, se crea una copia Snapshot con el mismo nombre.

```
FsxId05f7f00af49dc7a3e::> snapshot show -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -fields snapmirror-label
vserver                  volume            snapshot
snapmirror-label
------------------------ -----------------
---------------------------------------------------------------------
----------------
sapcc-backup-target-zone5 PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853 snapcenter
FsxId05f7f00af49dc7a3e::>
```

El nuevo backup de Snapshot también se incluye en el catálogo de backup de HANA.



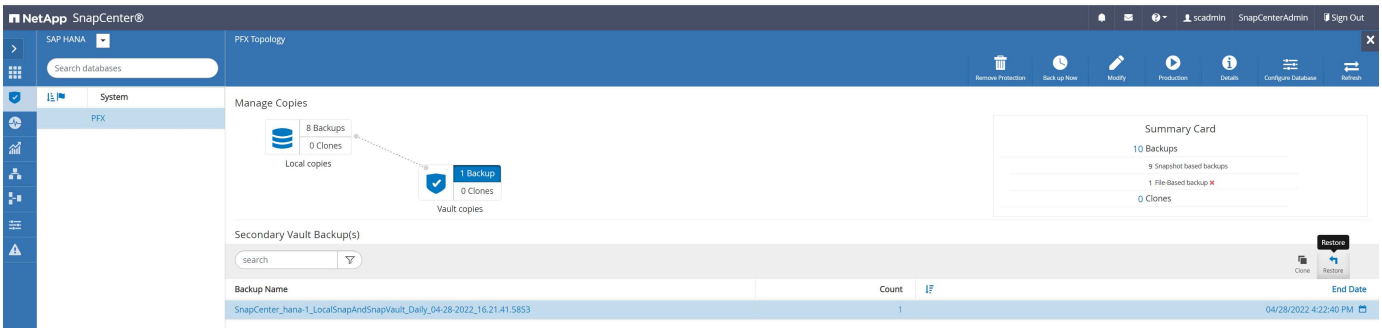
En SnapCenter, puede ver una lista de los backups replicados haciendo clic en Vault copies en la vista de topología.



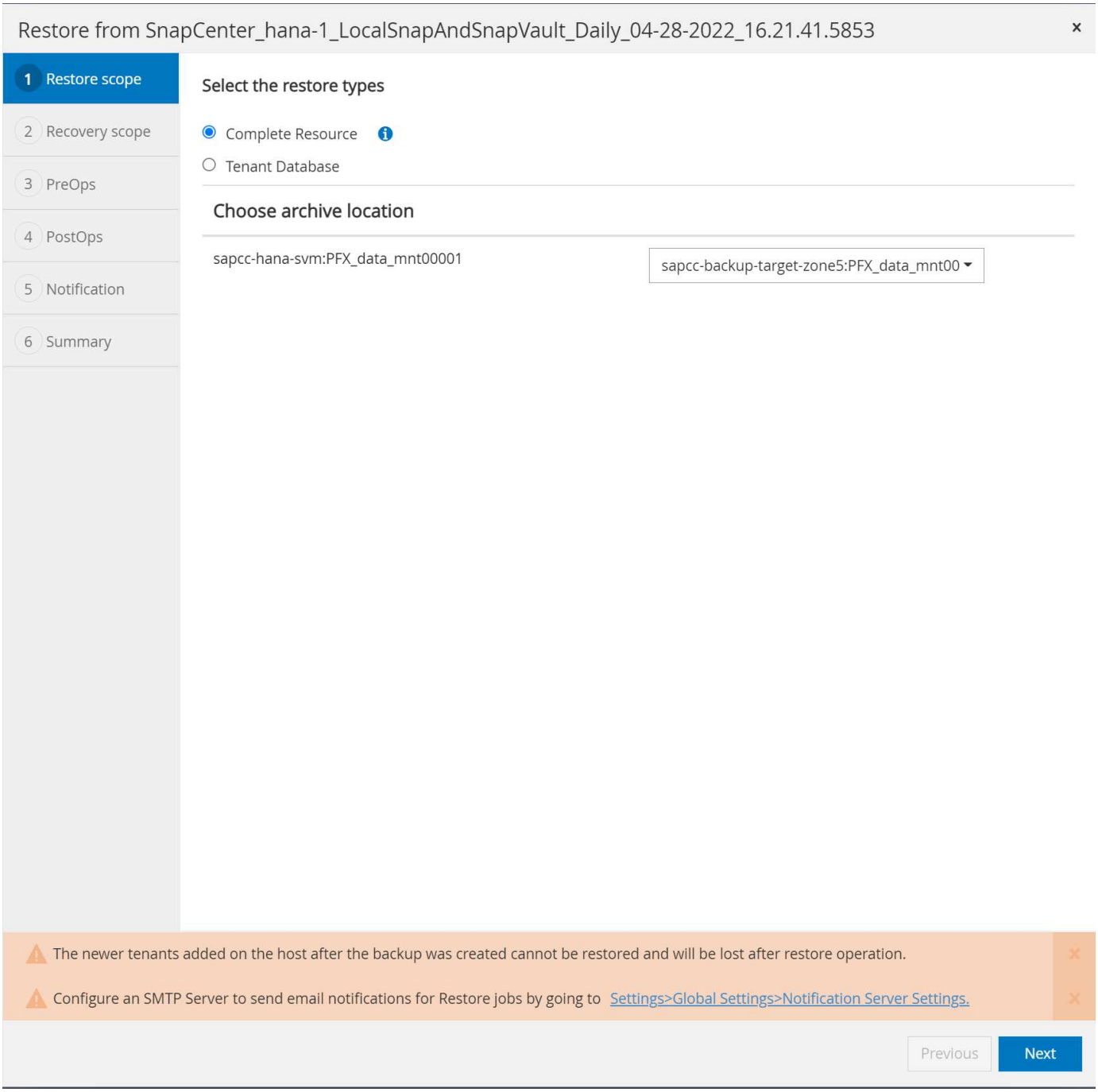
Restauración y recuperación desde el almacenamiento secundario

Para restaurar y recuperar el sistema desde el almacenamiento secundario, siga estos pasos:

Para recuperar la lista de todos los backups del almacenamiento secundario, en la vista SnapCenter Topology, haga clic en Vault copies, seleccione un backup y haga clic en Restore.



El cuadro de diálogo de restauración muestra las ubicaciones secundarias.



Otros pasos para la restauración y recuperación son idénticos a los que se encontraban previamente para un backup con Snapshot en el almacenamiento primario.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Guía de usuario de FSX para ONTAP de NetApp: ¿Qué es Amazon FSX para ONTAP de NetApp?

  https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html

- Página de recursos de SnapCenter

"https://www.netapp.com/us/documentation/snapcenter-software.aspx"

- Documentación sobre el software SnapCenter

  "https://docs.netapp.com/us-en/snapcenter/index.html"

- TR-4667: Automatización de las operaciones de copia y clonado del sistema SAP HANA con SnapCenter

  https://www.netapp.com/pdf.html?item=/media/17111-tr4667.pdf

- TR-4719: Replicación de sistemas SAP HANA: Backup y recuperación de datos con SnapCenter

  "https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-sr-scs-sap-hana-system-replication-overview.html"

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Mayo de 2022	Versión inicial.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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