



Backup y recuperación de datos de SAP HANA con SnapCenter

NetApp Solutions SAP

NetApp
March 11, 2024

Tabla de contenidos

- Backup y recuperación de datos de SAP HANA con SnapCenter 1
 - TR-4614: Backup y recuperación de datos de SAP HANA con SnapCenter 1
 - Arquitectura SnapCenter 6
 - Solución de backup SAP HANA de SnapCenter 7
 - Conceptos y prácticas recomendadas de SnapCenter 11
 - Configuración de laboratorio utilizada para este informe 31
 - Configuración de SnapCenter 33
 - Configuración inicial de SnapCenter 34
 - Configuración específica de recursos de SnapCenter para backups de base de datos SAP HANA 47
 - Configuración específica de recursos de SnapCenter para backups de volúmenes sin datos 67
 - Backups de bases de datos 71
 - Comprobación de integridad de bloques 80
 - Restauración y recuperación 84
 - Configuración y ajuste avanzados 139
 - Dónde encontrar información adicional e historial de versiones 147

Backup y recuperación de datos de SAP HANA con SnapCenter

TR-4614: Backup y recuperación de datos de SAP HANA con SnapCenter

Nils Bauer: NetApp

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 de datos objeto de backup es cada vez mayor. Por consiguiente, resulta difícil encontrar un momento en el que los backups puedan realizarse 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 el coste y la pérdida de datos para la empresa.

Los puntos siguientes resumen los desafíos a los que se enfrentan los procesos de respaldo y recuperación de SAP:

- **Efectos sobre el rendimiento en los sistemas SAP de producción.** normalmente, las copias de seguridad tradicionales basadas en copias generan un significativo drenaje del rendimiento en los sistemas SAP de producción debido a las pesadas cargas que se encuentran en el servidor de bases de datos, el sistema de almacenamiento y la red de almacenamiento.
- **Reducción de ventanas de copia de seguridad.** las copias de seguridad convencionales sólo se pueden realizar cuando pocas actividades de diálogo o por lotes están en proceso en el sistema SAP. La programación de backups se complica cuando los sistemas SAP se utilizan de forma ininterrumpida.
- **Rápido crecimiento de datos.** el rápido crecimiento de datos y la reducción de los plazos de respaldo requieren una inversión continua en infraestructura de respaldo. En otras palabras, debe adquirir más unidades de cinta, espacio adicional en disco de backup y redes de backup más rápidas. También debe cubrir el gasto continuo en almacenamiento y gestión de estos activos de cinta. Los backups incrementales o diferenciales pueden resolver estos problemas, pero esta disposición da como resultado un proceso de restauración muy lento, engorroso y complejo que es más difícil de verificar. Dichos sistemas suelen aumentar los tiempos de objetivo de tiempo de recuperación (RTO) y objetivo de punto de recuperación (RPO) de formas que no son aceptables para la empresa.
- **Aumento del costo del tiempo de inactividad.** el tiempo de inactividad no planificado de un sistema SAP afecta típicamente a las finanzas del negocio. El requisito de restaurar y recuperar el sistema SAP consume una parte significativa de cualquier tiempo de inactividad no planificado. Por tanto, el objetivo de tiempo de recuperación deseado determina el diseño de la arquitectura de backup y recuperación.
- **Tiempo de copia de seguridad y recuperación para proyectos de actualización SAP.** el plan de proyecto para una actualización SAP incluye al menos tres copias de seguridad de la base de datos SAP. Estos backups reducen significativamente el tiempo disponible para el proceso de actualización. La decisión de proceder suele basarse en el tiempo necesario para restaurar y recuperar la base de datos desde el backup creado previamente. En lugar de simplemente restaurar un sistema a su estado anterior, una restauración rápida ofrece más tiempo para resolver los problemas que pueden ocurrir durante una actualización.

La solución de NetApp

La tecnología Snapshot de NetApp se puede usar 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 porque la tecnología Snapshot de NetApp no mueve ni copia bloques de datos cuando se crea la copia Snapshot o se cambian datos en el sistema de archivos activo. Por tanto, la creación de copias Snapshot puede programarse 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 cuatro horas es habitual. Estos backups de Snapshot suelen conservarse de tres a cinco días en el sistema de almacenamiento principal antes de quitarse.

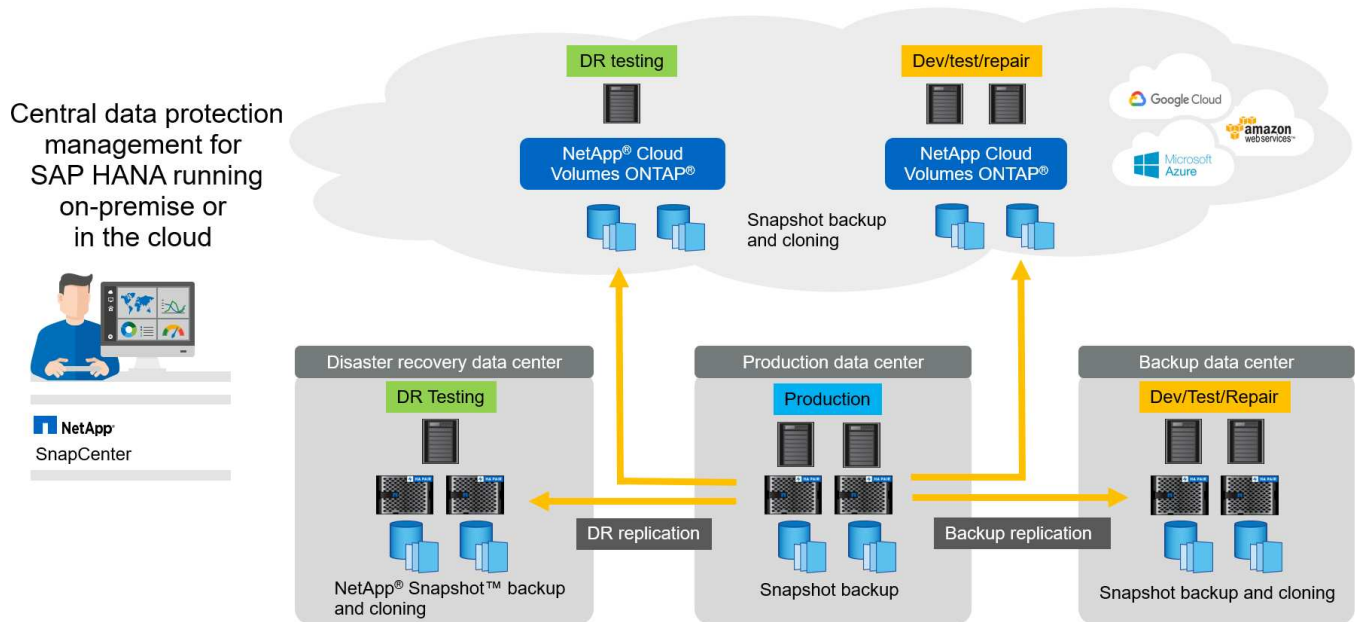
Las copias Snapshot también proporcionan ventajas importantes para las operaciones de recuperación y restauración. El software de recuperación de datos SnapRestore de NetApp permite la restauración de una base de datos completa o, alternativamente, una porción de una base de datos en un momento específico, según las copias Snapshot disponibles. Estos procesos de restauración se completan en cuestión de minutos, independientemente del tamaño de la base de datos. Debido a que se crean varios backups Snapshot online durante el día, el tiempo necesario para el proceso de recuperación se reduce significativamente en comparación con un método de backup tradicional. Dado que una restauración se puede realizar con una copia Snapshot con sólo unas horas de antigüedad (en lugar de hasta 24 horas), deben aplicarse menos registros de transacciones. Por lo tanto, el RTO se reduce a varios minutos en lugar de las varias horas necesarias para los backups en cinta de ciclo único 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 realizan mediante 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. La ubicación secundaria también puede utilizarse si es necesario restaurar un backup que ya no está disponible desde una copia Snapshot: Por ejemplo, un backup final de mes.

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 envía los datos de backup al destino mediante un backup de disco a disco de SnapVault de NetApp.

SnapVault ofrece ventajas significativas en comparación con los backups tradicionales. Después de una transferencia de datos inicial, en la que todos los datos se transfieren del origen al destino, en las copias posteriores sólo se copian 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 destino, un backup completo de la base de datos requiere menos espacio en disco.

La solución también se puede ampliar sin problemas a un modelo de operación de cloud híbrido. La replicación de datos para recuperación ante desastres o los fines de backup externo pueden realizarse desde sistemas ONTAP de NetApp en las instalaciones a instancias Cloud Volumes ONTAP que se ejecuten en el cloud. Puede utilizar SnapCenter como herramienta central para gestionar la protección de datos y la replicación de datos, independientemente de si el sistema SAP HANA se ejecuta en las instalaciones o en el cloud. La siguiente figura muestra información general sobre la solución de backup.



Tiempo de ejecución de backups de Snapshot

La siguiente captura de pantalla muestra HANA Studio de un cliente que ejecuta SAP HANA en almacenamiento de NetApp. El cliente usa copias de Snapshot para realizar backups de la base de datos HANA. La imagen muestra que se puede realizar un backup de la base de datos de HANA (aproximadamente 2,3 TB de tamaño) en 2 minutos y 11 segundos con la tecnología de backup de Snapshot.

La parte más grande del tiempo de ejecución del flujo de trabajo de backup general es el tiempo necesario para ejecutar la operación del punto de guardado del 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.

Backup Catalog

Show Log Backups Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination...
Success	Jun 28, 2017 6:19:11	00h 02m 11s	2.30 TB	Snapshot	SC-PROD_0100_20170628061902
Success	Jun 27, 2017 9:55:57	00h 02m 19s	2.27 TB	Snapshot	SC-PROD_0100_20170627095557
Success	Jun 27, 2017 9:00:11	00h 02m 26s	2.26 TB	Snapshot	SC-PROD_0100_20170627090011
Success	Jun 27, 2017 00:00:00	00h 02m 11s	2.26 TB	Snapshot	SC-PROD_0100_20170627000000
Success	Jun 27, 2017 1:04:16	00h 02m 32s	2.32 TB	Snapshot	SC-PROD_0100_20170627010416
Success	Jun 26, 2017 9:00:10	00h 02m 01s	2.28 TB	Snapshot	SC-PROD_0100_20170626090010
Success	Jun 26, 2017 00:00:00	00h 01m 56s	2.28 TB	Snapshot	SC-PROD_0100_20170626000000
Success	Jun 26, 2017 1:51:50	00h 02m 37s	2.28 TB	Snapshot	SC-PROD_0100_20170626015150
Success	Jun 26, 2017 1:00:00	00h 02m 06s	2.28 TB	Snapshot	SC-PROD_0100_20170626010000
Success	Jun 26, 2017 00:00:00	00h 02m 46s	2.27 TB	Snapshot	SC-PROD_0100_20170626000000
Success	Jun 26, 2017 5:00:11	00h 02m 01s	2.27 TB	Snapshot	SC-PROD_0100_20170626050011
Success	Jun 26, 2017 1:04:21	00h 02m 38s	2.30 TB	Snapshot	SC-PROD_0100_20170626010421
Success	Jun 25, 2017 9:00:11	00h 02m 07s	2.27 TB	Snapshot	SC-PROD_0100_20170625090011
Success	Jun 25, 2017 00:11:11	00h 01m 51s	2.27 TB	Snapshot	SC-PROD_0100_20170625001111
Success	Jun 25, 2017 9:00:00	00h 01m 51s	2.27 TB	Snapshot	SC-PROD_0100_20170625090000
Success	Jun 25, 2017 1:04:13	00h 01m 47s	2.26 TB	Snapshot	SC-PROD_0100_20170625010413
Success	Jun 24, 2017 9:00:00	00h 01m 41s	2.28 TB	Snapshot	SC-PROD_0100_20170624090000
Success	Jun 24, 2017 5:00:00	00h 01m 56s	2.27 TB	Snapshot	SC-PROD_0100_20170624050000
Success	Jun 24, 2017 1:00:00	00h 01m 17s	2.27 TB	Snapshot	SC-PROD_0100_20170624010000
Success	Jun 24, 2017 9:00:12	00h 02m 00s	2.28 TB	Snapshot	SC-PROD_0100_20170624090012
Success	Jun 24, 2017 00:00:00	00h 02m 01s	2.27 TB	Snapshot	SC-PROD_0100_20170624000000
Success	Jun 24, 2017 1:04:35	00h 02m 01s	2.30 TB	Snapshot	SC-PROD_0100_20170624010435
Success	Jun 23, 2017 9:00:09	00h 02m 16s	2.29 TB	Snapshot	SC-PROD_0100_20170623090009
Success	Jun 23, 2017 5:00:11	00h 01m 51s	2.29 TB	Snapshot	SC-PROD_0100_20170623050011

Backup Details

ID: 1498623551457

Status: Successful

Backup Type: Data Backup

Destination Type: Snapshot

Started: Jun 28, 2017 6:19:11 AM (Europe/Berlin)

Finished: Jun 28, 2017 6:21:22 AM (Europe/Berlin)

Duration: 00h 02m 11s

Size: 2.30 TB

Throughput: n.a.

System ID: n.a.

Comment: SC-PROD_0100_20170628061902

Additional Information: <col>

Location:

Host	Service	Size	Name
dsw	nameserver	112.00 MB	hdb000
dsw	indexserver	2.30 TB	hdb000
dsw	xsengine	80.00 MB	hdb000

Comparación de objetivos de tiempo de recuperación

Esta sección proporciona una comparación entre el objetivo de tiempo de recuperación de backups de copias Snapshot basadas en archivos y el almacenamiento. El objetivo de tiempo de recuperación se define por la suma del tiempo necesario para restaurar la base de datos y el tiempo necesario para iniciar y recuperar 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 1 hora y 10 minutos en restaurar una base de datos de 1 TB de tamaño.

Con los backups de copias Snapshot de almacenamiento, el tiempo de restauración es independiente del tamaño de la base de datos y está dentro del intervalo de un par de segundos cuando la restauración puede realizarse desde el almacenamiento principal. Solo es necesario llevar a cabo una restauración a partir del almacenamiento secundario cuando se produzca un desastre cuando el almacenamiento primario ya no esté disponible.

Tiempo necesario para iniciar la base de datos

La hora de inicio de la base de datos depende del tamaño del almacén de filas y columnas. En el almacén de columnas, la hora de inicio también depende de la cantidad de datos precargados durante el inicio de la base de datos. En los siguientes ejemplos asumimos que la hora de inicio es de 30 minutos. La hora de inicio es la misma para una restauración y recuperación basadas en archivos, y una restauración y recuperación basadas en Snapshot.

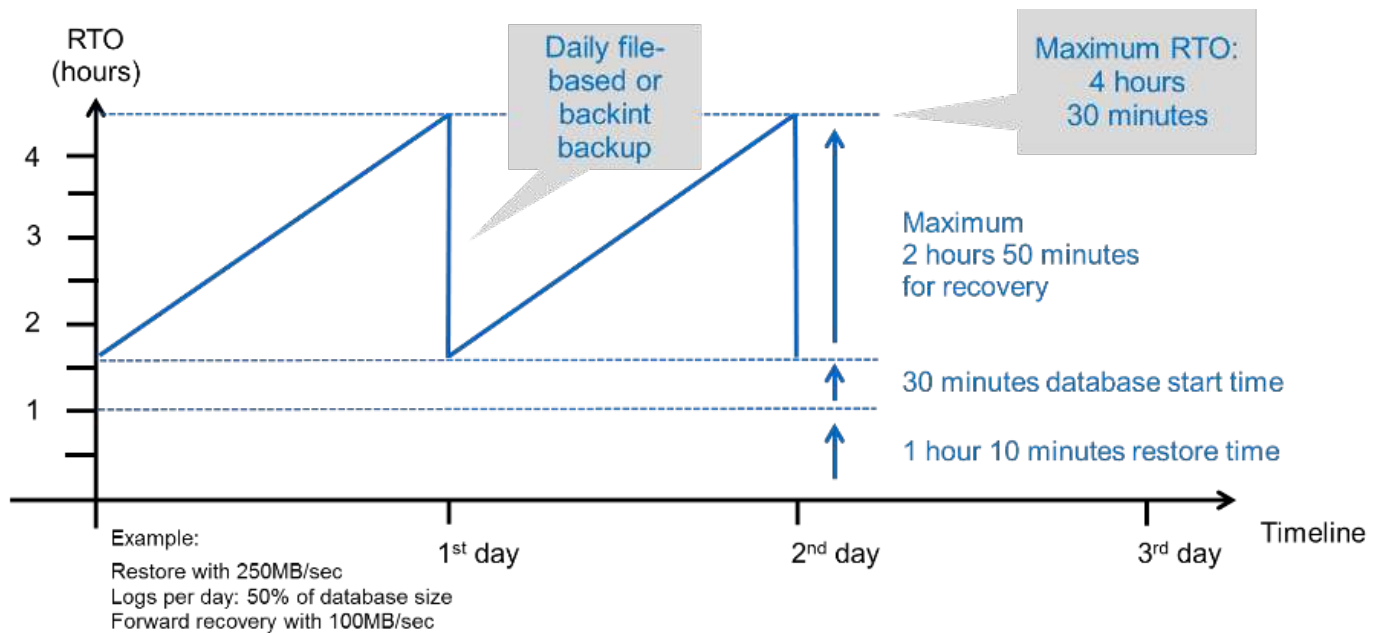
Tiempo necesario para recuperar las bases de datos

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.

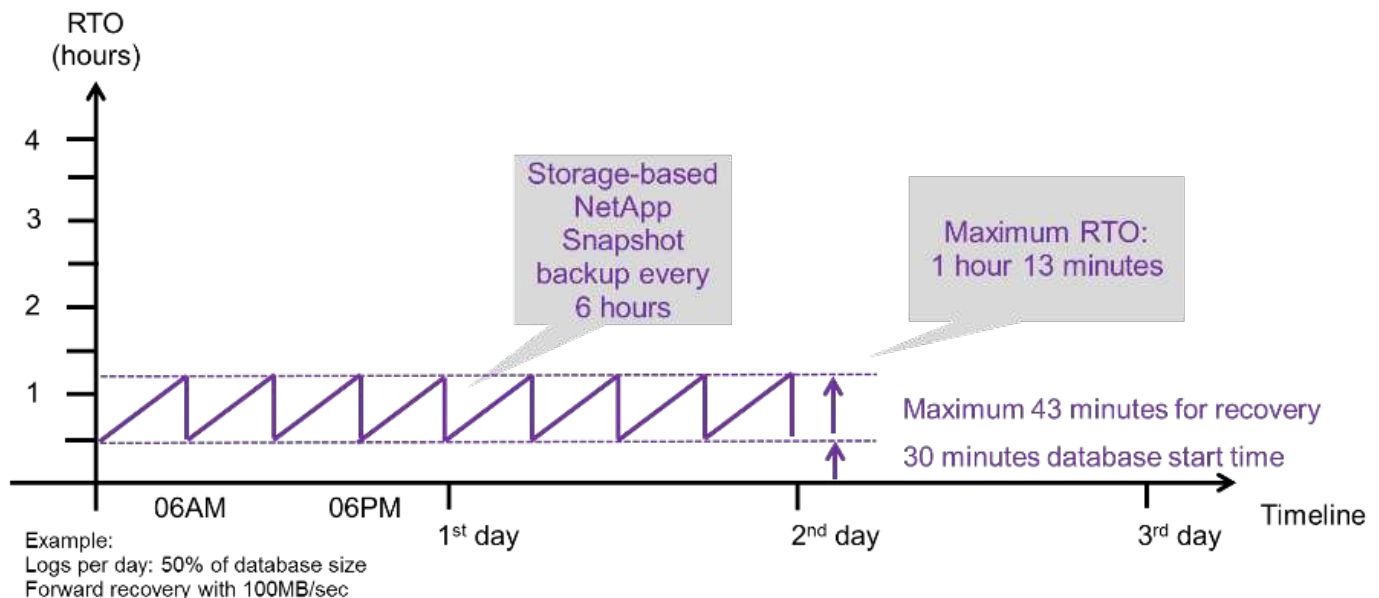
Con los backups de datos basados en archivos, la programación de backup suele ser una vez al día. Por lo general, no es posible aumentar la frecuencia de backup, ya que el backup reduce el rendimiento de producción. Por lo tanto, en el peor de los casos, todos los registros que se escribieron durante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

Los backups de datos de copias de Snapshot de almacenamiento suelen programarse con una frecuencia más alta debido a que no afectan al rendimiento de la base de datos de SAP HANA. Por ejemplo, si los backups de copias 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 ($6 \text{ horas} / 24 \text{ horas} = \frac{1}{4}$).

La siguiente figura muestra un ejemplo de objetivo de tiempo de recuperación para una base de datos de 1 TB cuando se utilizan backups de datos basados en archivos. En este ejemplo, se realiza un backup una vez al día. El objetivo de tiempo de recuperación varía según el momento en que se realizó la restauración y la recuperación. Si las restauraciones y las recuperaciones se llevaron a cabo inmediatamente después de realizar un backup, el RTO se basa principalmente en el tiempo de restauración, que es de 1 hora y 10 minutos en el ejemplo. El tiempo de recuperación se aumentó a 2 horas y 50 minutos cuando se realizaron la restauración y la recuperación inmediatamente antes de que se pudiera realizar el siguiente backup, y el RTO máximo se mostró a 4 horas y 30 minutos.



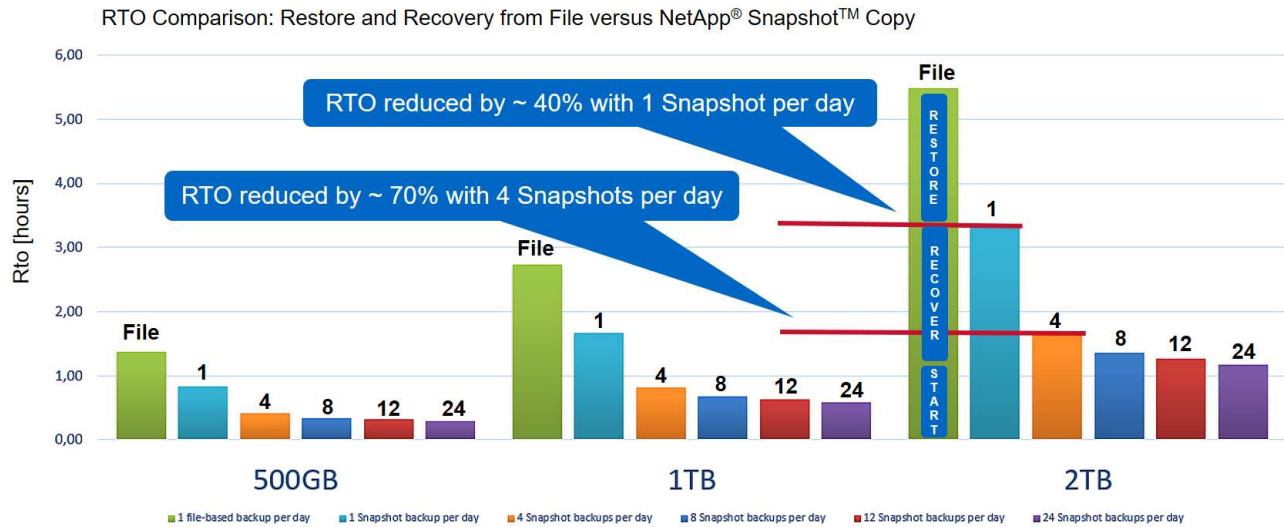
La siguiente figura muestra un ejemplo de objetivo de tiempo de recuperación para una base de datos de 1 TB cuando se utilizan backups Snapshot. En cuanto a los backups de Snapshot basados en almacenamiento, el objetivo de tiempo de recuperación solo depende del tiempo de inicio de la base de datos y del tiempo de recuperación de alcance, ya que la restauración se realiza en unos pocos segundos, independientemente del tamaño de la base de datos. El tiempo de recuperación futura también aumenta en función de cuándo se realicen las restauraciones y las recuperaciones, pero, debido a la mayor frecuencia de backups (cada seis horas en este ejemplo), el tiempo de recuperación futura es, como máximo, de 43 minutos. En este ejemplo, el objetivo de tiempo de recuperación máximo es de 1 hora y 13 minutos.



La siguiente figura muestra una comparación de objetivos de tiempo de recuperación de backups Snapshot basados en archivos y basados en almacenamiento para diferentes tamaños de base de datos y diferentes frecuencias de los backups de Snapshot. La barra verde muestra el backup basado en archivos. Las otras barras muestran los backups de copias de Snapshot con diferentes frecuencias de backup.

Con un único backup de datos de copia Snapshot al día, el objetivo de tiempo de recuperación ya se ha

reducido en un 40 % en comparación con un backup de datos basado en archivos. La reducción aumenta hasta el 70% cuando se realizan cuatro backups Snapshot al día. La figura también muestra que la curva se mantendrá si aumenta la frecuencia de backup de Snapshot a más de cuatro o seis backups de Snapshot al día. Por lo tanto, nuestros clientes suelen configurar de cuatro a seis backups Snapshot al día.



El gráfico muestra el tamaño de la RAM del servidor HANA. El tamaño de la base de datos en la memoria se calcula para ser la mitad del tamaño de la RAM del servidor.



El tiempo de restauración y recuperación se calcula en función de las siguientes suposiciones. La base de datos se puede restaurar a 250 Mbps. La cantidad de archivos de registro por día es del 50% del tamaño de la base de datos. Por ejemplo, una base de datos de 1 TB crea 500 MB de archivos de registro al día. La recuperación se puede realizar a 100 Mbps.

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.

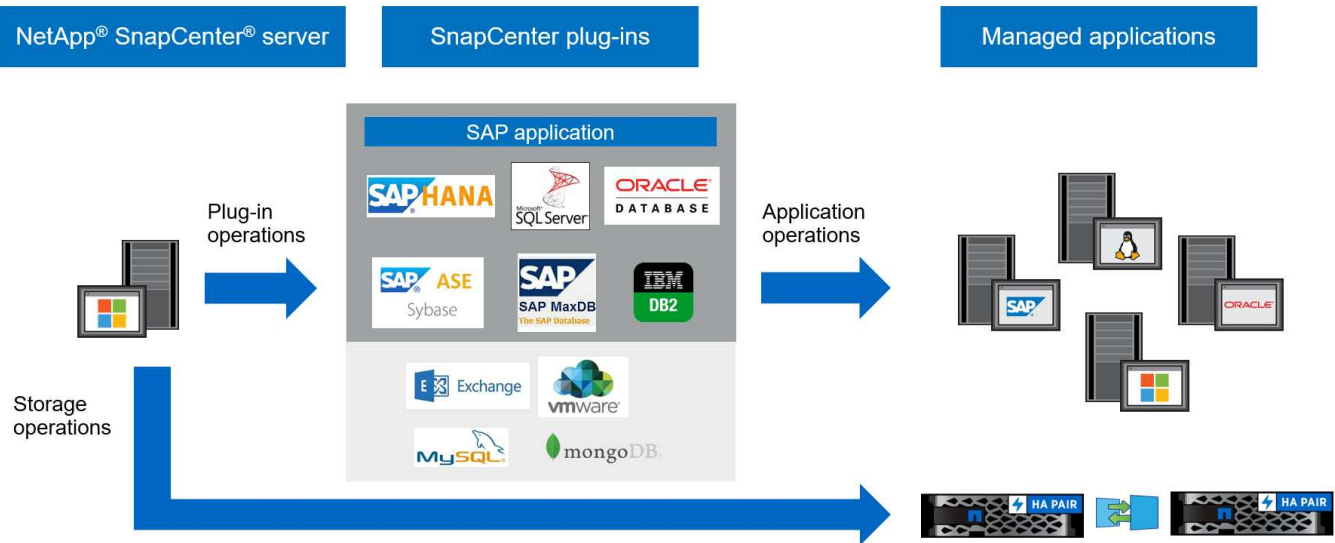
SnapCenter gestiona los datos a través de terminales en el Data Fabric con la tecnología de NetApp. Puede utilizar SnapCenter para replicar datos entre entornos locales, entre entornos locales y el cloud, y entre clouds privados, híbridos o públicos.

Componentes de SnapCenter

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

Los plugins personalizados de SnapCenter permiten crear plugins propios y proteger la aplicación mediante la misma interfaz de SnapCenter.

La siguiente figura muestra los componentes de SnapCenter.



Solución de backup SAP HANA de SnapCenter

En esta sección se enumeran los componentes, las configuraciones y versiones de SAP HANA admitidas y las mejoras de SnapCenter 4.6 que se usan en esta solución.

Componentes de la solución

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

- Backup de datos SAP HANA con copias Snapshot basadas en almacenamiento:
 - Programación de copias de seguridad
 - Gestión de retención
 - Mantenimiento del catálogo de backup de SAP HANA
- Volumen sin datos (por ejemplo, /hana/shared) Backup con copias Snapshot basadas en el almacenamiento:
 - Programación de copias de seguridad
 - Gestión de retención
- Replicación en una ubicación de backup o recuperación ante desastres externa:
 - Backups de las copias Snapshot de datos SAP HANA
 - Volúmenes no en datos
 - Gestión de retención configurada en almacenamiento de backup externo
 - Mantenimiento del catálogo de backup de SAP HANA
- Comprobaciones de integridad de bloques de bases de datos mediante un backup basado en archivos:
 - Programación de copias de seguridad

- Gestión de retención
- Mantenimiento del catálogo de backup de SAP HANA
- Gestión de retención del backup de registros de base de datos de HANA:
 - Gestión de retención basada en la retención de backups de datos
 - Mantenimiento del catálogo de backup de SAP HANA
- Detección automática de las bases de datos HANA
- Restauración y recuperación automatizadas
- Operaciones de restauración de un solo inquilino con sistemas de contenedor de base de datos multitenant (MDC) de SAP HANA

SnapCenter ejecuta los backups de archivos de datos de bases de datos junto con un plugin para SAP HANA. El complemento activa un 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 base de datos consistentes en una ubicación de backup o recuperación ante desastres externa mediante SnapVault o SnapMirror de NetApp. 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 sean de datos mediante el plugin SAP HANA con copias de Snapshot basadas en el almacenamiento. Los volúmenes que no sean de datos pueden programarse de manera independiente del backup de datos de base de datos para habilitar las políticas de retención y protección individuales.

La base de datos SAP HANA ejecuta automáticamente backups de registros. Según los objetivos de punto de recuperación, existen varias opciones para la ubicación de almacenamiento de los backups de registros:

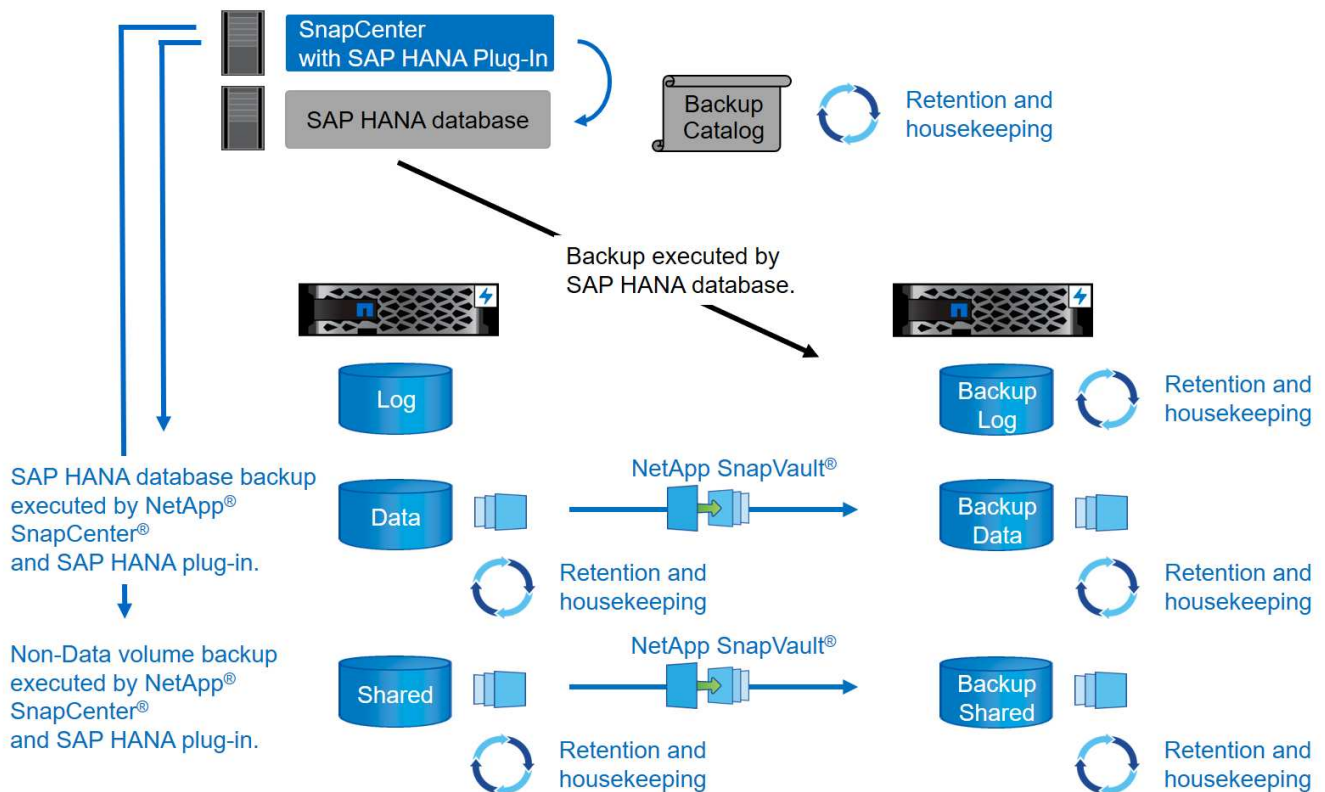
- El backup de registros se escribe en un sistema de almacenamiento que refleja de forma síncrona los datos en una segunda ubicación con el software de almacenamiento de alta disponibilidad (ha) MetroCluster de NetApp y de recuperación ante desastres.
- El destino de los backups de registros se puede configurar en el mismo sistema de almacenamiento primario y, a continuación, se replica de forma síncrona o asíncrona en un almacenamiento secundario con SnapMirror.
- El destino del backup de registros se puede configurar en el mismo almacenamiento de backup externo en el que se replican los backups de base de datos con SnapVault. Con esta configuración, el almacenamiento de backup externo tiene requisitos de disponibilidad como los del almacenamiento principal, de modo que los backups de registros puedan escribirse en el almacenamiento de backup externo.

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. La comprobación de integridad de bloque se puede ejecutar desde SnapCenter. Según sus políticas de retención configurables, SnapCenter gestiona el mantenimiento de backups de archivos de datos en el almacenamiento principal, los backups de archivos de registro y el catálogo de backup de SAP HANA.



SnapCenter se encarga de la retención en el almacenamiento principal, mientras que ONTAP gestiona la retención de backups secundarios.

En la siguiente figura, se muestra información general de la configuración de backup de registros y bases de datos, donde los backups de registros se escriben en un montaje NFS del almacenamiento de backup externo.



Al ejecutar un backup de Snapshot basado en el almacenamiento de volúmenes que no son de datos, SnapCenter realiza las siguientes tareas:

1. Creación de una copia Snapshot de almacenamiento del volumen que no contiene datos.
2. Ejecución de una actualización de SnapVault o SnapMirror para el volumen de datos, si está configurado.
3. Eliminación de copias Snapshot de almacenamiento en el almacenamiento principal a partir de una política de retención definida.

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

1. Creación de un punto de guardado de backup de SAP HANA para crear una imagen consistente en la capa de persistencia.
2. Creación de una copia Snapshot de almacenamiento del volumen de datos.
3. Registro del backup de la snapshot de almacenamiento en el catálogo de backup de SAP HANA.
4. Lanzamiento del punto de guardado de backup de SAP HANA.
5. Ejecución de una actualización de SnapVault o SnapMirror para el volumen de datos, si está configurado.
6. Eliminación de copias Snapshot de almacenamiento en el almacenamiento principal a partir de una política de retención definida.
7. Eliminación de las entradas del catálogo de backup de 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

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.

Versiones y configuraciones de SAP HANA compatibles

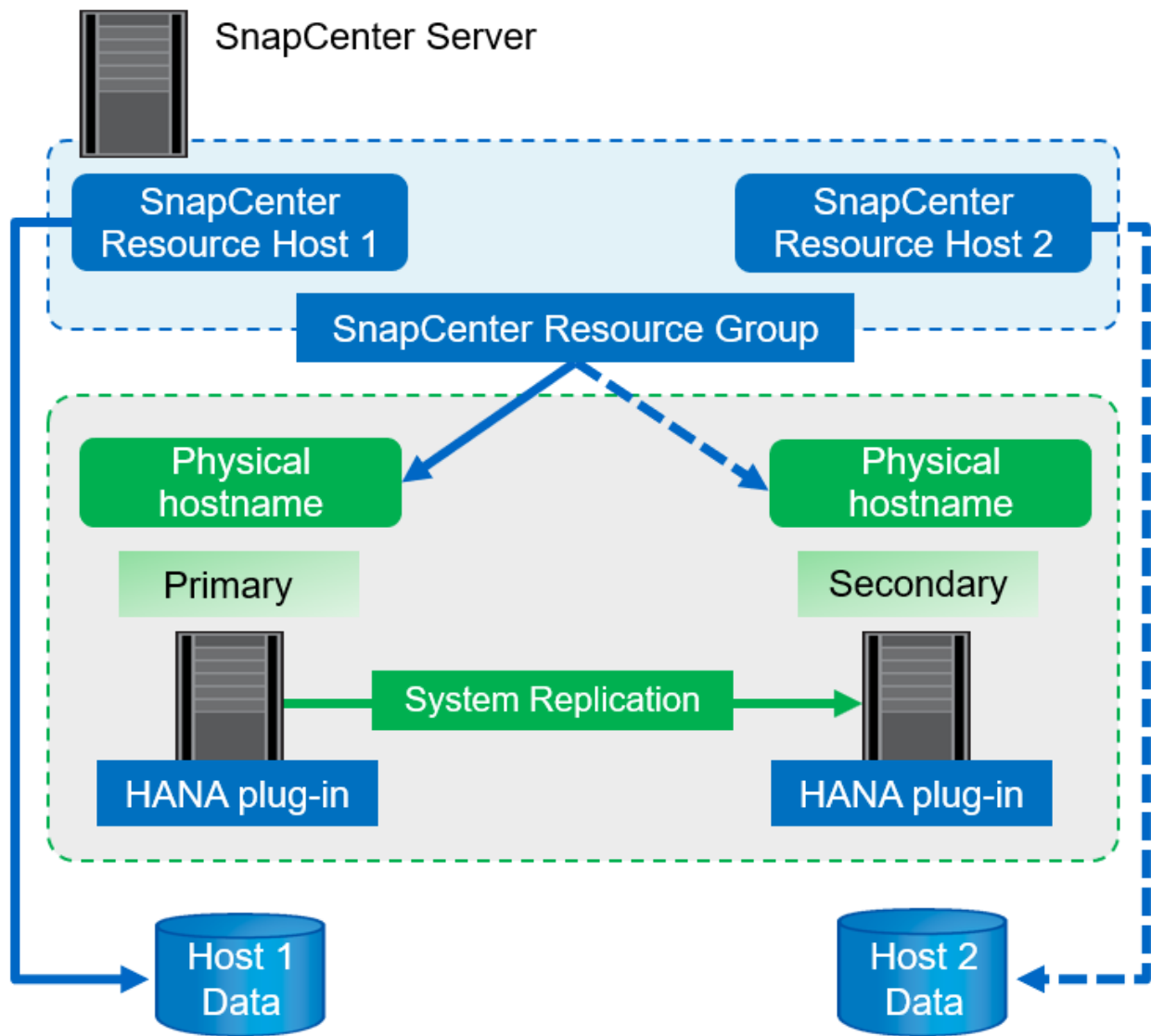
SnapCenter admite configuraciones de un solo host y varios hosts de SAP HANA mediante sistemas de almacenamiento de NetApp conectados a NFS o FC (AFF y FAS), así como sistemas SAP HANA que se ejecutan en Cloud Volumes ONTAP en AWS, Azure, Google Cloud Platform y AWS FSX ONTAP mediante NFS.

SnapCenter es compatible con las siguientes arquitecturas y versiones de SAP HANA:

- Contenedor único de SAP HANA: SAP HANA 1.0 SPS12
- Contenedor de base de datos multitenant (MDC) de SAP HANA: SAP HANA 2.0 SPS3 y versiones posteriores
- Contenedor de base de datos multitenant (MDC) de SAP HANA varios inquilinos: SAP HANA 2.0 SPS4 y versiones posteriores

Mejoras de SnapCenter 4.6

A partir de la versión 4.6, SnapCenter admite la detección automática de sistemas HANA configurados en una relación de replicación del sistema HANA. Cada host se configura usando su dirección IP física (nombre de host) y su volumen de datos individual en la capa de almacenamiento. Los dos recursos de SnapCenter se combinan en un grupo de recursos; SnapCenter identifica automáticamente qué host es primario o secundario y, a continuación, ejecuta las operaciones de backup necesarias según corresponda. La gestión de retención de Snapshot y los backups basados en archivos creados con SnapCenter se realiza en ambos hosts para garantizar que los backups antiguos también se eliminan en el host secundario actual. La siguiente figura muestra una descripción general de alto nivel. Puede encontrar una descripción detallada de la configuración y el funcionamiento de sistemas HANA habilitados para la replicación del sistema HANA en SnapCenter en ["TR-4719 replicación de sistemas SAP HANA, backup y recuperación con SnapCenter"](#).



Conceptos y prácticas recomendadas de SnapCenter

En esta sección se describen los conceptos y las prácticas recomendadas de SnapCenter relacionadas con la configuración y la implementación de recursos SAP HANA.

Opciones y conceptos de configuración de recursos SAP HANA

Con SnapCenter, la configuración de recursos de base de datos SAP HANA puede realizarse con dos enfoques diferentes.

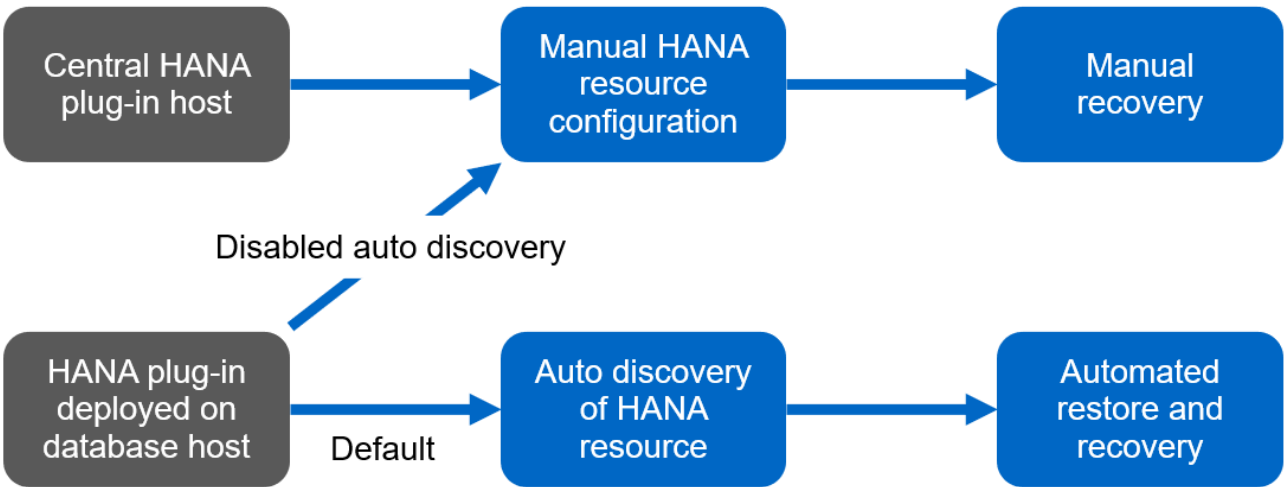
- **Configuración manual de recursos.** la información de recursos y espacio de almacenamiento de HANA se debe proporcionar manualmente.
- **Descubrimiento automático de recursos HANA.** el descubrimiento automático simplifica la configuración de bases de datos HANA en SnapCenter y permite la restauración y recuperación automatizadas.


Es importante entender que solo se habilitan los recursos de bases de datos de HANA en SnapCenter que se detectan automáticamente para realizar restauraciones y recuperaciones automatizadas. Los recursos DE la base de datos DE HANA que se configuran manualmente en SnapCenter deben recuperarse manualmente después de una operación de restauración en SnapCenter.

Por otro lado, la detección automática con SnapCenter no es compatible con todas las arquitecturas de HANA y las configuraciones de infraestructura. Por lo tanto, los entornos HANA pueden requerir un enfoque mixto en el cual algunos sistemas HANA (sistemas de varios hosts HANA) requieren una configuración de recursos manual y todos los demás pueden configurarse mediante detección automática.

La detección automática y las restauraciones y recuperaciones automatizadas dependen de la capacidad para ejecutar comandos del sistema operativo en el host de la base de datos. Algunos ejemplos son la detección de huella de almacenamiento y sistema de archivos, y las operaciones de desmontaje, montaje o detección de LUN. Estas operaciones se ejecutan en el plugin de SnapCenter Linux, que se implementa automáticamente junto con el plugin de HANA. Por lo tanto, es necesario implementar el complemento HANA en el host de la base de datos para permitir la detección automática, así como la restauración y recuperación automatizadas. También es posible deshabilitar la detección automática después de la implementación del plugin de HANA en el host de la base de datos. En este caso, el recurso será un recurso configurado manualmente.

La siguiente figura resume las dependencias. Encontrará más información sobre las opciones de puesta en marcha de HANA en la sección “Opciones de puesta en marcha para el complemento SAP HANA”.



 Los complementos HANA y Linux actualmente, solo están disponibles para sistemas basados en Intel. Si las bases de datos de HANA se ejecutan en IBM Power Systems, se debe utilizar un host de plugin HANA central.

Arquitecturas de HANA compatibles para detección automática y recuperación automatizada

Con SnapCenter, la detección automática, y la restauración y recuperación automatizadas son compatibles con la mayoría de las configuraciones de HANA, con la excepción de que varios sistemas de host de HANA requieren una configuración manual.

La siguiente tabla muestra las configuraciones de HANA compatibles para la detección automática.

Plugin DE HANA instalado en:	Arquitectura DE HANA	Configuración del sistema HANA	De almacenamiento
Host de base de datos HANA	Host único	<ul style="list-style-type: none"> • Contenedor único DE HANA • Contenedores de bases de datos multitenant de SAP HANA (MDC) con uno o varios inquilinos • Replicación de sistemas HANA 	<ul style="list-style-type: none"> • Configuración básica con NFS • Configuración básica con XFS y FC con o sin Linux Logical Volume Manager (LVM) • VMware con montajes NFS de SO directo



Los sistemas MDC DE HANA con varios inquilinos son compatibles para la detección automática, pero no para la restauración y la recuperación automatizadas con la versión de SnapCenter actual.

Arquitecturas HANA compatibles para la configuración manual de recursos de HANA

Es posible configurar manualmente los recursos HANA para todas las arquitecturas HANA; sin embargo, requiere un host de complemento HANA central. El host del plugin central puede ser el propio servidor SnapCenter o un host Linux o Windows independiente.



Cuando el plugin de HANA se implementa en el host de la base de datos HANA, de forma predeterminada, el recurso se detecta automáticamente. Es posible deshabilitar la detección automática para hosts individuales, de modo que el plugin pueda ponerse en marcha; por ejemplo, en un host de base de datos con la replicación del sistema HANA activada y una versión de SnapCenter < 4.6, donde no se admite la detección automática. Para obtener más información, consulte la sección ["Deshabilitar la detección automática en el host del plugin de HANA."](#)

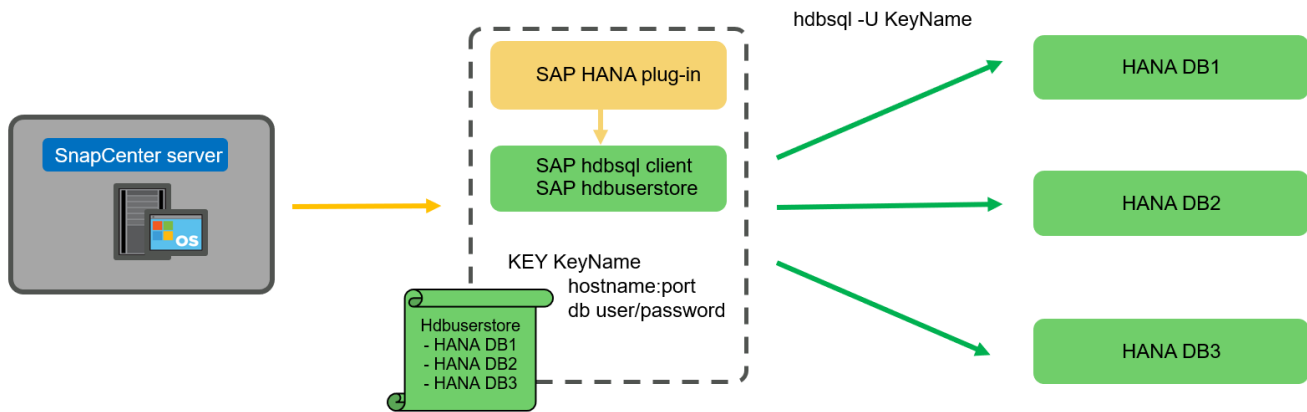
La siguiente tabla muestra las configuraciones de HANA compatibles para la configuración manual de recursos de HANA.

Plugin DE HANA instalado en:	Arquitectura DE HANA	Configuración del sistema HANA	De almacenamiento
Host de plugin central (servidor SnapCenter o host Linux independiente)	Host único o múltiple	<ul style="list-style-type: none"> • Contenedor único DE HANA • MDC DE HANA con uno o varios inquilinos • Replicación de sistemas HANA 	<ul style="list-style-type: none"> • Configuración básica con NFS • Nativo con XFS y FC con o sin Linux LVM • VMware con montajes NFS de SO directo

Opciones de implementación para el complemento SAP HANA

En la siguiente figura, se muestra la vista lógica y la comunicación entre SnapCenter Server y las bases de datos SAP HANA.

El servidor SnapCenter se comunica mediante el plugin de SAP HANA con las bases de datos SAP HANA. El complemento SAP HANA utiliza el software cliente hdbsql de SAP HANA para ejecutar comandos SQL en las bases de datos SAP HANA. El hdbuserstore de SAP HANA se utiliza para proporcionar las credenciales de usuario, el nombre de host y la información del puerto para acceder a las bases de datos SAP HANA.



El complemento SAP HANA y el software cliente SAP hdbsql, que incluye la herramienta de configuración hdbuserstore, deben instalarse conjuntamente en el mismo host.

El host puede ser el servidor de SnapCenter mismo, un host del plugin central independiente o los hosts individuales de bases de datos SAP HANA.

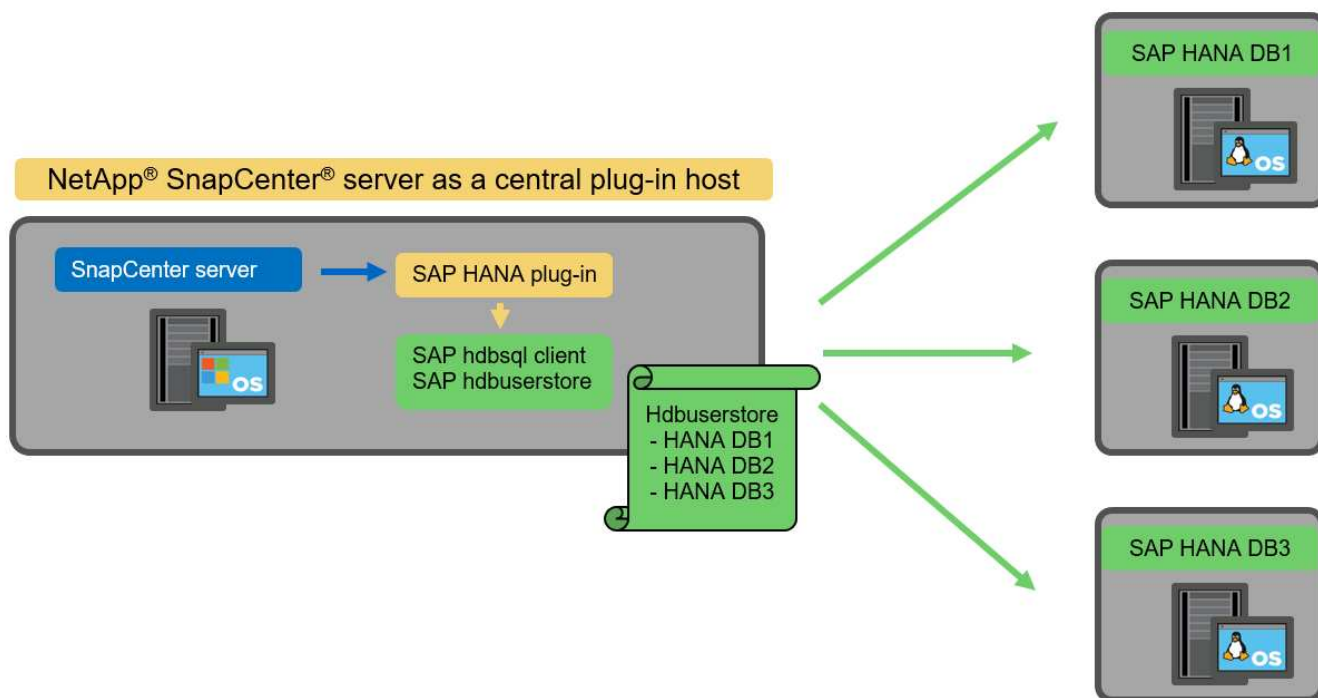
SnapCenter Server de alta disponibilidad

SnapCenter se puede establecer en una configuración de alta disponibilidad de dos nodos. En dicha configuración, se utiliza un equilibrador de carga (por ejemplo, F5) en un modo activo/pasivo utilizando una dirección IP virtual dirigida al host de SnapCenter activo. El repositorio de SnapCenter (la base de datos de MySQL) es replicado por SnapCenter entre los dos hosts para que los datos de SnapCenter estén siempre sincronizados.

La alta disponibilidad del servidor SnapCenter no es compatible si el plugin HANA está instalado en el servidor SnapCenter. Si planea configurar SnapCenter en una configuración de alta disponibilidad, no instale el plugin HANA en el servidor SnapCenter. Puede encontrar más información sobre la alta disponibilidad de SnapCenter en este ["Página de la base de conocimientos de NetApp"](#).

SnapCenter Server como host de plugin de HANA central

La siguiente figura muestra una configuración en la que SnapCenter Server se utiliza como host de plugin central. El complemento SAP HANA y el software de cliente SAP hdbsql se instalan en el servidor SnapCenter.



Dado que el complemento HANA se puede comunicar con las bases de datos HANA gestionadas usando el hdbclient a través de la red, no es necesario instalar ningún componente de SnapCenter en los hosts individuales de la base de datos HANA. SnapCenter puede proteger las bases de datos de HANA mediante un host del complemento de HANA central en el que todas las claves de userstore están configuradas para las bases de datos gestionadas.

Por otro lado, la automatización mejorada del flujo de trabajo para la detección automática, la automatización de la restauración y la recuperación, así como las operaciones de actualización del sistema SAP requieren la instalación de los componentes de SnapCenter en el host de la base de datos. Cuando se utiliza un host de un plugin de HANA central, estas funciones no están disponibles.

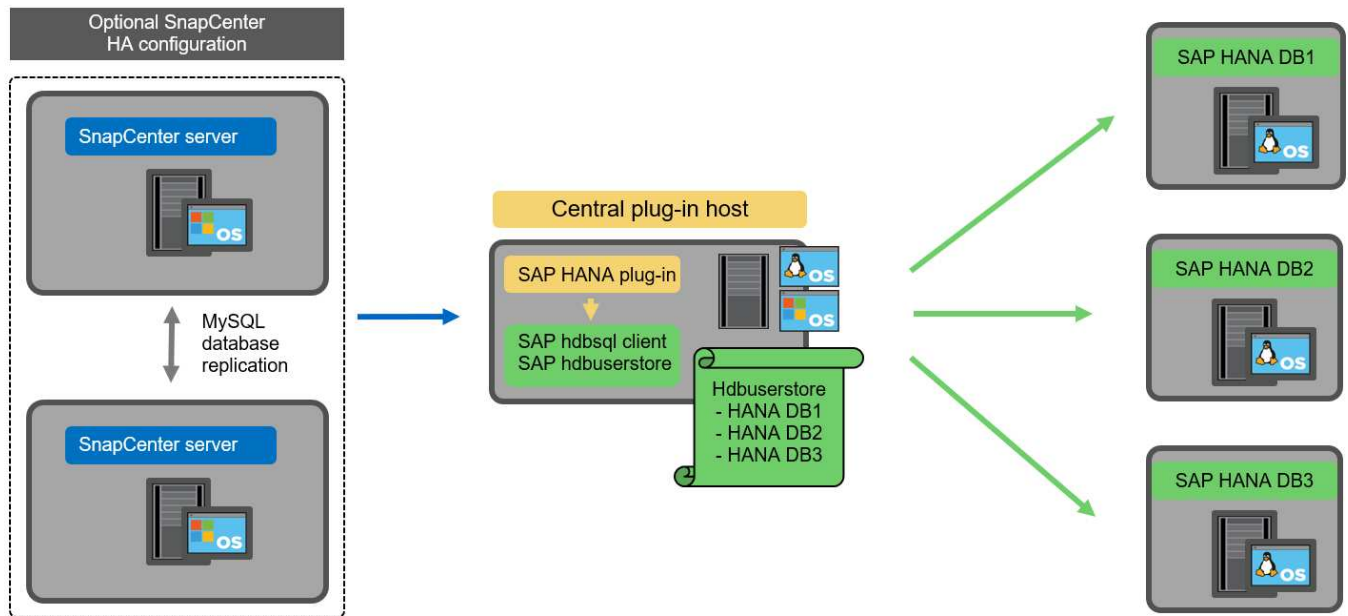
Además, la alta disponibilidad del servidor SnapCenter con la función de alta disponibilidad integrada no se puede usar cuando el complemento HANA está instalado en el servidor SnapCenter. La alta disponibilidad se puede obtener usando VMware ha si el servidor SnapCenter se está ejecutando en un equipo virtual dentro de un clúster de VMware.

Un host separado como host de plugin de HANA central

En la siguiente figura, se muestra una configuración en la que un host Linux separado se usa como host de plugin central. En este caso, el complemento SAP HANA y el software de cliente SAP hdbsql se instalan en el host Linux.



El host separado del plugin central también puede ser un host de Windows.

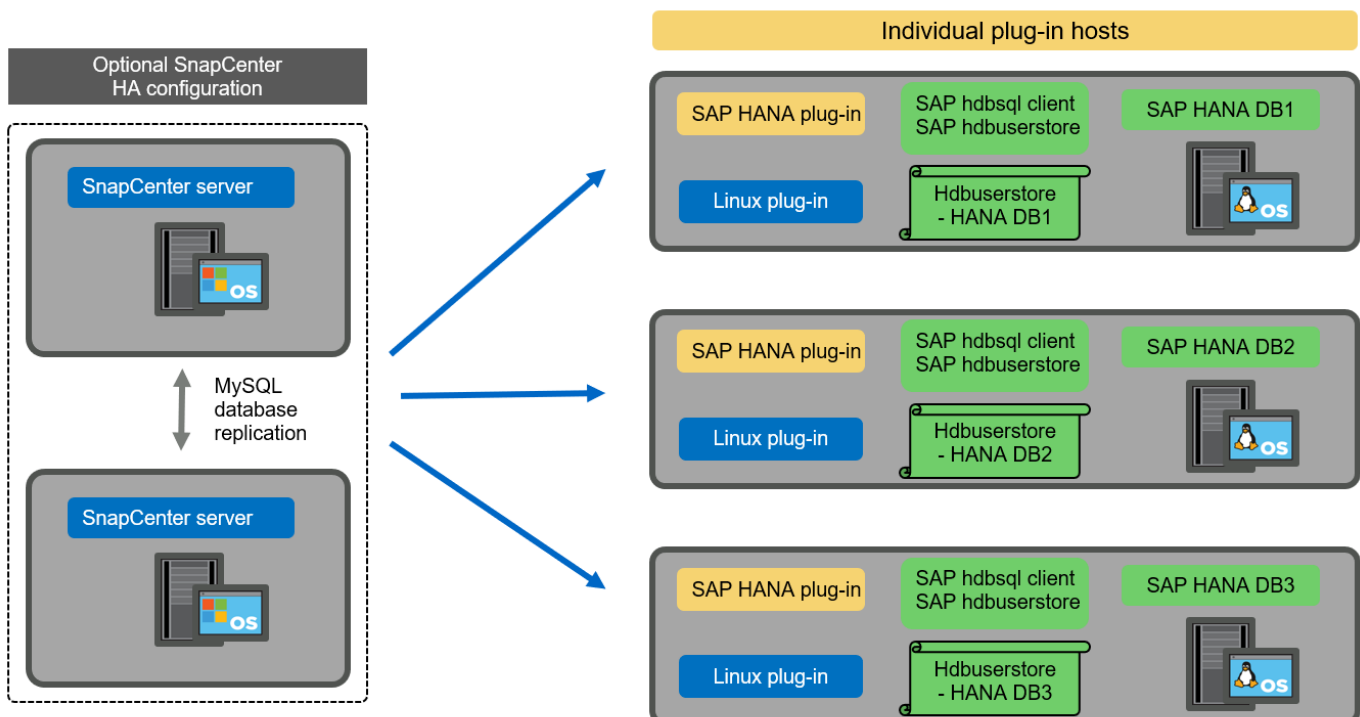


La misma restricción en cuanto a la disponibilidad de funciones descrita en la sección anterior también se aplica a un host de plugin central independiente.

Sin embargo, con esta opción de puesta en marcha, el servidor SnapCenter se puede configurar con la funcionalidad de alta disponibilidad incorporada. El host del plugin central también debe ser ha, por ejemplo, mediante una solución de clúster Linux.

Plugin DE HANA implementado en hosts de base de datos de HANA individuales

La siguiente figura muestra una configuración en la cual el plugin de SAP HANA está instalado en cada host de base de datos SAP HANA.



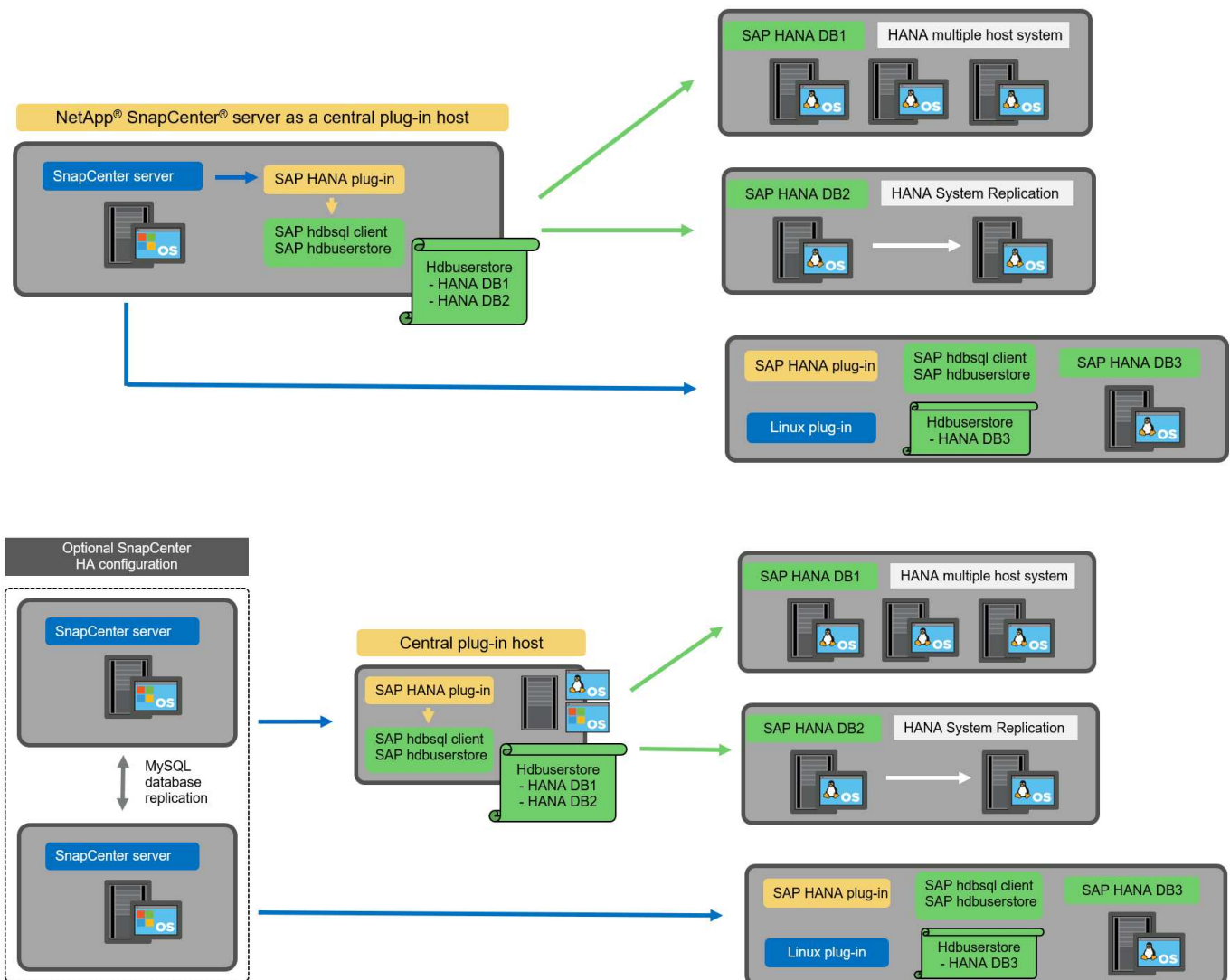
Cuando el complemento HANA se instala en cada host de base de datos HANA individual, todas las funciones, como la detección automática y la restauración y recuperación automatizadas, están disponibles. Además, el servidor SnapCenter puede configurarse en una configuración de alta disponibilidad.

Puesta en marcha mixta del complemento de HANA

Como se explicó al principio de esta sección, algunas configuraciones del sistema HANA, como varios sistemas de host, requieren un host de plugin centralizado. Por lo tanto, la mayoría de las configuraciones de SnapCenter requieren una puesta en marcha mixta del complemento HANA.

NetApp recomienda implementar el plugin de HANA en el host de base de datos de HANA para todas las configuraciones del sistema HANA que se admiten para la detección automática. Otros sistemas HANA, como las configuraciones de varios hosts, deben gestionarse con el host de plugin de HANA central.

Las dos figuras siguientes muestran implementaciones de plugins combinadas con el servidor SnapCenter o con un host Linux independiente como host de plugins centrales. La única diferencia entre estas dos puestas en marcha es la configuración de alta disponibilidad opcional.



Resumen y recomendaciones

En general, NetApp recomienda poner en marcha el complemento HANA en cada host SAP HANA para habilitar todas las funciones disponibles de SnapCenter HANA y mejorar la automatización del flujo de trabajo.



Los complementos HANA y Linux actualmente solo están disponibles para sistemas basados en Intel. Si las bases de datos de HANA se ejecutan en IBM Power Systems, se debe utilizar un host de plugin HANA central.

Para las configuraciones de HANA en las que no se admite la detección automática, como las configuraciones de varios hosts de HANA, se debe configurar un host del plugin de HANA central adicional. El host del complemento central puede ser el servidor de SnapCenter si se puede utilizar ha de VMware para alta disponibilidad de SnapCenter. Si piensa utilizar la funcionalidad de alta disponibilidad incorporada de SnapCenter, utilice un host de plugin de Linux independiente.

En la tabla siguiente se resumen las distintas opciones de implementación.

Opción de implementación	Dependencias
Plugin de host de plugin de HANA central instalado en el servidor SnapCenter	Pros: * Configuración central de almacenamiento de usuario de HDB de complemento único HANA * no se requieren componentes de software SnapCenter en los hosts individuales de bases de datos de HANA * compatibilidad con todas las arquitecturas de HANA: * Configuración manual de recursos * recuperación manual * no se ejecuta soporte para la restauración de un solo inquilino * los pasos previos y posteriores a un script en el host del plugin central * alta disponibilidad de SnapCenter integrada no compatible * la combinación de SID y nombre de inquilino debe ser única en todas las bases de datos HANA gestionadas * Log La gestión de retención de backup está habilitada/deshabilitada para todas las bases de datos HANA gestionadas
Plugin de host de plugin de HANA central instalado en un servidor Linux o Windows independiente	Pros: * Configuración central de almacenamiento de usuario de HDB de complemento único HANA * no se requieren componentes de software SnapCenter en hosts individuales de bases de datos HANA * compatibilidad con todas las arquitecturas HANA * SnapCenter integrada de alta disponibilidad compatible con funciones: * Configuración manual de recursos * recuperación manual * no se ejecuta soporte para la restauración de un solo inquilino * cualquier paso previo y posterior al script en el host del plugin central * la combinación de SID y nombre de inquilino debe ser única en todas las bases de datos HANA gestionadas * la gestión de retención de backup de registro habilitada/deshabilitada para todas las bases de datos gestionadas Bases de datos HANA

Opción de implementación	Dependencias
Plugin de host de plugin de HANA individual instalado en el servidor de bases de datos HANA	Ventajas: * Detección automática de recursos de HANA * restauración y recuperación automatizadas * restauración de un solo inquilino * automatización previa y posterior al script para la actualización del sistema SAP * compatible con alta disponibilidad de SnapCenter integrada * la gestión de la retención de backup de registro se puede habilitar o deshabilitar para cada ubicación de base de datos de HANA individual: * No es compatible con todas las arquitecturas HANA. Se requiere un host de plugin central adicional para varios sistemas host HANA. * El plugin de HANA debe ponerse en marcha en cada host de base de datos HANA

Estrategia de protección de datos

Antes de configurar SnapCenter y el complemento SAP HANA, la estrategia de protección de datos se debe definir de acuerdo con 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.

Los parámetros que deben definirse son:

- ¿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 la producción, desarrollo y prueba del tipo de sistema. 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 4 horas	Cada 4 horas	Cada 4 horas
Retención primaria	2 días	2 días	2 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	PolicyLocalSnap	PolicyLocalSnapAndSnapVault	PolicyBlockIntegrityCheck
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.** Horario cada 4 horas.
- **Prueba.** Horario 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.** programar todos los días.
- **Desarrollo.** Horario todos los días.

La política `BlockIntegrityCheck` se utiliza en los sistemas de producción y desarrollo para cubrir la comprobación de integridad de bloques semanales mediante un backup basado en archivos.

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

- *** Producción.*** Horario cada semana.
- **Desarrollo.** Horario cada semana.

Para cada base de datos SAP HANA individual que utilice la política de backup externa, se 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 nuestro ejemplo, para cada sistema de producción y desarrollo, se define una retención de dos semanas en el almacenamiento de backup externo.



En nuestro 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.

Operaciones de backup

SAP introdujo la compatibilidad de los backups de Snapshot para sistemas de varios inquilinos MDC con HANA 2.0 SPS4. SnapCenter admite operaciones de backup de Snapshot de sistemas MDC de HANA con varios inquilinos. SnapCenter también admite dos operaciones de restauración diferentes de un sistema MDC de HANA. Puede restaurar todo el sistema, la base de datos del sistema y todos los clientes, o bien restaurar un solo usuario. Existen algunos requisitos previos para permitir a SnapCenter ejecutar estas operaciones.

En un sistema MDC, la configuración de tenant no es necesariamente estática. Es posible agregar inquilinos o eliminar inquilinos. SnapCenter no puede confiar en la configuración que se detecta cuando la base de datos HANA se añade a SnapCenter. SnapCenter debe saber qué inquilinos están disponibles en el momento específico en que se ejecuta la operación de backup.

Para habilitar una operación de restauración de un solo usuario, SnapCenter debe saber qué inquilinos se incluyen en cada backup de Snapshot. Además, debe saber qué archivos y directorios pertenecen a cada inquilino incluido en el backup de Snapshot.

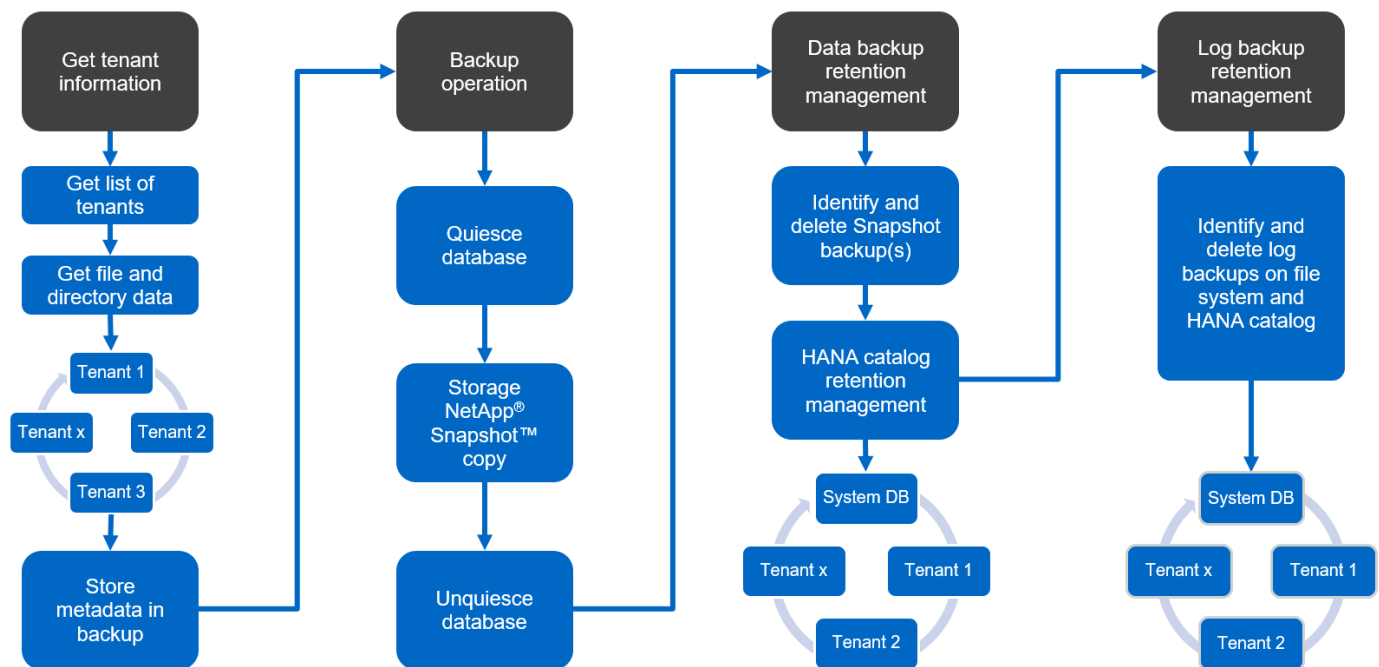
Por lo tanto, con cada operación de backup, el primer paso del flujo de trabajo es obtener la información del inquilino. Esto incluye los nombres de arrendatario y la información de archivo y directorio correspondiente. Estos datos deben almacenarse en los metadatos de backups de Snapshot para poder admitir una única operación de restauración de usuarios. El siguiente paso es la operación de backup de Snapshot. Este paso incluye el comando SQL para activar el punto de guardado de backup de HANA, el backup de snapshot de almacenamiento y el comando SQL para cerrar la operación de Snapshot. Al usar el comando close, la base de datos de HANA actualiza el catálogo de backup de la base de datos del sistema y cada inquilino.



SAP no admite las operaciones de backup de Snapshot para sistemas MDC cuando se detienen uno o varios inquilinos.

Para la gestión de retención de los backups de datos y la gestión del catálogo de backup de HANA, SnapCenter debe ejecutar las operaciones de eliminación de catálogo para la base de datos del sistema y todas las bases de datos de tenant que se identificaron en el primer paso. Del mismo modo para los backups de registros, el flujo de trabajo SnapCenter debe funcionar en cada inquilino que forme parte de la operación de backup.

En la siguiente figura, se muestra información general sobre el flujo de trabajo de backup.



Flujo de trabajo de backup para backups de Snapshot de la base de datos HANA

SnapCenter realiza un backup de la base de datos SAP HANA en el siguiente orden:

1. SnapCenter lee la lista de inquilinos desde la base de datos HANA.
2. SnapCenter lee los archivos y los directorios de cada inquilino desde la base de datos de HANA.
3. La información del inquilino se almacena en los metadatos de SnapCenter para esta operación de backup.
4. SnapCenter activa un punto de guardado de backup sincronizado global de SAP HANA para crear una imagen de base de datos coherente en la capa de persistencia.



Para un sistema tenant único o múltiple de SAP HANA MDC, se crea un punto de guardado de backup global sincronizado para la base de datos del sistema y para cada base de datos de tenant.

5. SnapCenter crea copias Snapshot de almacenamiento para todos los volúmenes de datos configurados para el recurso. En nuestro ejemplo de una base de datos HANA de un único host, solo hay un volumen de datos. Con una base de datos de varios hosts SAP HANA, hay varios volúmenes de datos.
6. SnapCenter registra el backup de Snapshot del almacenamiento en el catálogo de backup de SAP HANA.
7. SnapCenter elimina el punto de guardado de backup de SAP HANA.
8. SnapCenter inicia una actualización de SnapVault o SnapMirror para todos los volúmenes de datos configurados en el recurso.



Este paso solo se ejecuta si la política seleccionada incluye una replicación de SnapVault o SnapMirror.

9. SnapCenter elimina las copias de Snapshot de almacenamiento y las entradas de backup en su base de datos, así como en el catálogo de backup de SAP HANA, según la política de retención definida para los backups en el almacenamiento principal. Las operaciones del catálogo de backup DE HANA se realizan para la base de datos del sistema y todos los inquilinos.



Si el backup sigue disponible en el almacenamiento secundario, no se elimina la entrada de catálogo SAP HANA.

10. SnapCenter elimina todos los backups de registros del sistema de archivos y en el catálogo de backup de SAP HANA más antiguos que el backup de datos más antiguo identificado en el catálogo de backup de SAP HANA. Estas operaciones se realizan para la base de datos del sistema y todos los inquilinos.



Este paso solo se ejecuta si el mantenimiento del backup de registro no está deshabilitado.

Flujo de trabajo de backup para operaciones de comprobación de integridad de bloques

SnapCenter ejecuta la comprobación de integridad de bloques en la siguiente secuencia:

1. SnapCenter lee la lista de inquilinos desde la base de datos HANA.
2. SnapCenter activa una operación de backup basada en archivos para la base de datos del sistema y cada inquilino.
3. SnapCenter elimina los backups basados en archivos de su base de datos, en el sistema de archivos y en el catálogo de backup de SAP HANA en función de la política de retención definida para las operaciones de comprobación de integridad de bloques. La eliminación de backup del sistema de archivos y las operaciones de catálogo de backup de HANA se realizan para la base de datos del sistema y todos los inquilinos.
4. SnapCenter elimina todos los backups de registros del sistema de archivos y en el catálogo de backup de SAP HANA más antiguos que el backup de datos más antiguo identificado en el catálogo de backup de SAP HANA. Estas operaciones se realizan para la base de datos del sistema y todos los inquilinos.



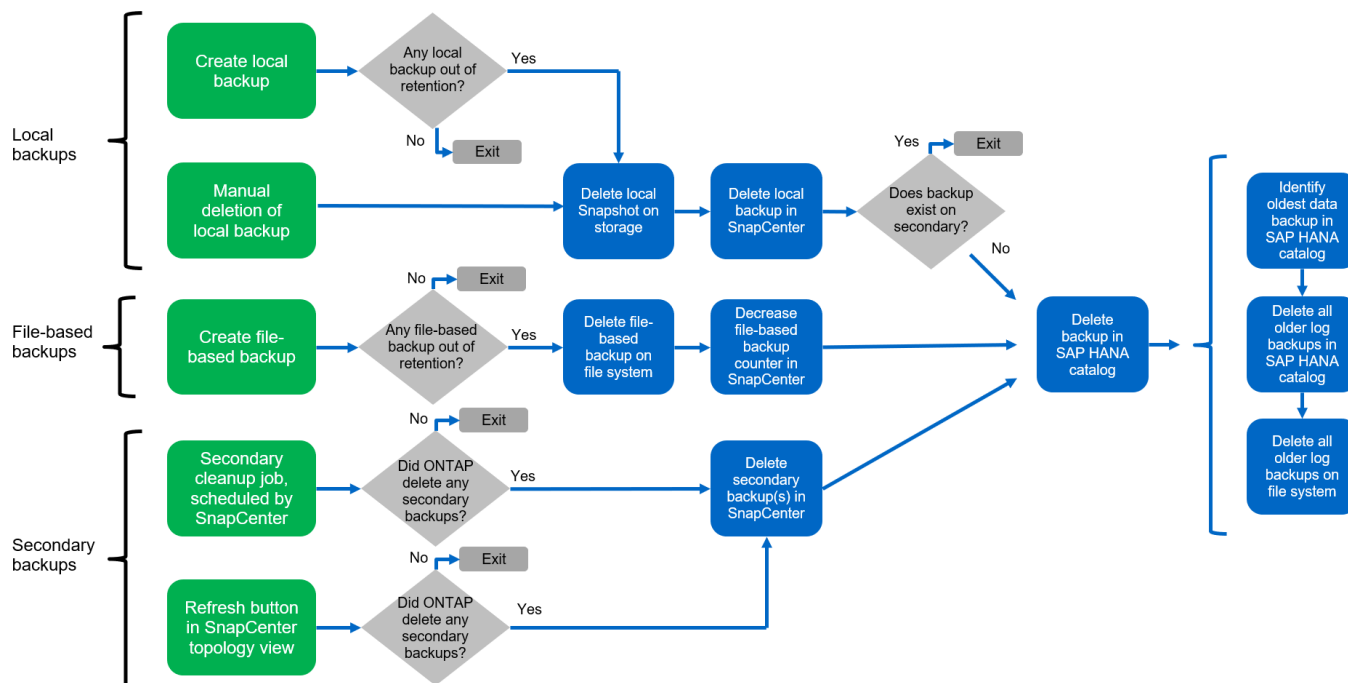
Este paso solo se ejecuta si el mantenimiento del backup de registro no está deshabilitado.

Gestión de retención de backup y mantenimiento de backups de datos y registros

La gestión de la retención de backup de datos y el mantenimiento de los backups de registros se pueden dividir en cinco áreas principales, incluida la gestión de retención de:

- Backups locales en el almacenamiento primario
- Backups basados en archivos
- Backups en el almacenamiento secundario
- Backups de datos en el catálogo de backup de SAP HANA
- Los backups de registro en el catálogo de backup de SAP HANA y el sistema de archivos

En la siguiente figura, se proporciona información general sobre los diferentes flujos de trabajo y las dependencias de cada operación. En las siguientes secciones se describen detalladamente las diferentes operaciones.



Gestión de retención de backups locales en el almacenamiento principal

SnapCenter realiza tareas de mantenimiento de backups de bases de datos SAP HANA y backups de volúmenes sin datos eliminando copias Snapshot en el almacenamiento principal y en el repositorio de SnapCenter según una retención definida en la política de backup de SnapCenter.

La lógica de gestión de retención se ejecuta con cada flujo de trabajo de backup en SnapCenter.



Tenga en cuenta que SnapCenter gestiona la gestión de la retención individualmente tanto para backups programados como bajo demanda.

Los backups locales del almacenamiento primario también se pueden eliminar manualmente en SnapCenter.

Gestión de retención de backups basados en archivos

SnapCenter realiza tareas de mantenimiento de los backups basados en archivos mediante la eliminación de los backups en el sistema de archivos según una retención definida en la política de backup de SnapCenter.

La lógica de gestión de retención se ejecuta con cada flujo de trabajo de backup en SnapCenter.



Tenga en cuenta que SnapCenter gestiona la gestión de la retención individualmente para backups programados o bajo demanda.

Gestión de retención de backups en el almacenamiento secundario

La gestión de retención de backups en el almacenamiento secundario es gestionada por ONTAP de acuerdo con la retención definida en la relación de protección de ONTAP.

Para sincronizar estos cambios en el almacenamiento secundario del repositorio de SnapCenter, SnapCenter utiliza un trabajo de limpieza programado. Esta tarea de limpieza sincroniza todos los backups de almacenamiento secundario con el repositorio de SnapCenter para todos los plugins de SnapCenter y todos los recursos.

De forma predeterminada, el trabajo de limpieza se programa una vez a la semana. Esta programación semanal genera un retraso con la eliminación de backups en SnapCenter y SAP HANA Studio en comparación con los backups que ya se han eliminado en el almacenamiento secundario. Para evitar esta incoherencia, los clientes pueden cambiar la programación por una mayor frecuencia, por ejemplo, una vez al día.



El trabajo de limpieza también se puede activar manualmente para un recurso individual haciendo clic en el botón Refresh de la vista de topología del recurso.

Para obtener información detallada acerca de cómo adaptar la programación del trabajo de limpieza o cómo activar una actualización manual, consulte la sección ["Cambie la frecuencia de programación de la sincronización de copias de seguridad con el almacenamiento de copias de seguridad fuera de las instalaciones".](#)

Gestión de retención de backups de datos dentro del catálogo de backup de SAP HANA

Cuando SnapCenter ha eliminado cualquier backup, snapshot local o basado en archivos, o si ha identificado la eliminación del backup en el almacenamiento secundario, este backup de datos también se elimina en el catálogo de backup de SAP HANA.

Antes de eliminar la entrada del catálogo SAP HANA para un backup de Snapshot local en el almacenamiento principal, SnapCenter comprueba si el backup sigue existiendo en el almacenamiento secundario.

Gestión de retención de backups de registros

La base de datos SAP HANA crea automáticamente backups de registro. Este backup de registro ejecuta crean archivos de backup para cada servicio SAP HANA individual en un directorio de backup configurado en SAP HANA.

Los backups de registros más antiguos del último backup de datos ya no son necesarios para la recuperación futura y, por lo tanto, se pueden eliminar.

SnapCenter realiza tareas de mantenimiento de los backups de archivos de registro en el nivel del sistema de archivos y del catálogo de backup SAP HANA mediante la ejecución de los pasos siguientes:

1. SnapCenter lee el catálogo de backup de SAP HANA para obtener el ID de backup del backup de Snapshot o basado en archivos más antiguo.
2. SnapCenter elimina todos los backups de registros del catálogo SAP HANA y el sistema de archivos antiguos a este ID de backup.



SnapCenter solo gestiona el mantenimiento de los backups creados por SnapCenter. Si se crean backups basados en archivos adicionales fuera de SnapCenter, debe asegurarse de que los backups basados en archivos se eliminen del catálogo de backup. Si un backup de datos de este tipo no se elimina manualmente del catálogo de backups, puede convertirse en el backup de datos más antiguo y los backups de registros más antiguos no se eliminan hasta que este backup basado en archivos se elimina.



Aunque se define una retención para backups bajo demanda en la configuración de políticas, el mantenimiento solo se realiza cuando se ejecuta otro backup bajo demanda. Por lo tanto, los backups bajo demanda suelen eliminarse manualmente en SnapCenter para asegurarse de que estos backups también se eliminan en el catálogo de backup de SAP HANA y que el mantenimiento del backup de registros no se basa en un backup antiguo bajo demanda.

La gestión de retención del backup de registros está habilitada de forma predeterminada. Si es necesario, se puede desactivar tal como se describe en la sección ["Deshabilitar la detección automática en el host del plugin de HANA."](#)

Requisitos de capacidad para backups de Snapshot

Debe tener en cuenta la tasa de cambio de bloque más alta en la capa de almacenamiento en relación con la tasa de cambio con las bases de datos tradicionales. Debido al proceso de combinación de tablas HANA del almacén de columnas, la tabla completa se escribe en el disco, no solo en los bloques modificados.

Los datos de nuestra base de clientes muestran una tasa de cambio diaria entre el 20 % y el 50 % si se realizan varios backups de Snapshot durante el día. En el caso de SnapVault, si la replicación se realiza una sola vez al día, la tasa de cambio diaria normalmente es menor.

Operaciones de restauración y recuperación

Operaciones de restauración con SnapCenter

Desde la perspectiva de la base de datos de HANA, SnapCenter admite dos operaciones de restauración diferentes.

- **Restauración del recurso completo.** todos los datos del sistema HANA se restauran. Si el sistema HANA contiene uno o más inquilinos, se restauran los datos de la base de datos del sistema y los datos de todos los clientes.
- **Restaurar un solo inquilino.** sólo se restauran los datos del arrendatario seleccionado.

Desde la perspectiva del almacenamiento, las operaciones de restauración anteriores deben ejecutarse de una forma diferente en función del protocolo de almacenamiento utilizado (NFS o SAN Fibre Channel), la protección de datos configurada (almacenamiento principal con o sin almacenamiento de backup externo), y el backup seleccionado que se utilizará para la operación de restauración (restauración desde el almacenamiento de backup principal o externo).

Restauración de recursos completos desde el almacenamiento primario

Cuando se restaura el recurso completo desde el almacenamiento primario, SnapCenter admite dos funciones de ONTAP diferentes para ejecutar la operación de restauración. Puede elegir entre las siguientes dos funciones:

- **SnapRestore basado en volumen.** una SnapRestore basada en volumen revierte el contenido del volumen de almacenamiento al estado de la copia de seguridad de instantánea seleccionada.
 - Casilla de comprobación Volume Revert disponible para los recursos detectados automáticamente mediante NFS.
 - Botón de opción Complete Resource para recursos configurados manualmente.
- **SnapRestore basado en archivos.** un SnapRestore basado en archivos, también conocido como Single File SnapRestore, restaura todos los archivos individuales (NFS) o todos los LUN (SAN).
 - Método de restauración predeterminado para recursos detectados automáticamente. Se puede cambiar con la casilla de comprobación Volume revert de NFS.
 - Botón de opción de nivel de archivo para recursos configurados manualmente.

En la siguiente tabla, se proporcionan comparación entre los diferentes métodos de restauración.

	SnapRestore basado en volúmenes	SnapRestore basado en archivos
Velocidad de operación de restauración	Muy rápida, independientemente del tamaño del volumen	Operación de restauración muy rápida, pero utiliza un trabajo de copia en segundo plano en el sistema de almacenamiento, lo cual bloquea la creación de nuevos backups de Snapshot
Historial de copias de seguridad de Snapshot	Restaurar a un backup de Snapshot anterior, elimina todos los backups de Snapshot más recientes.	Sin influencia
Restauración de la estructura de directorio	También se restaura la estructura del directorio	NFS: Solo restaura los archivos individuales, no la estructura de directorios. Si también se pierde la estructura de directorio, se debe crear manualmente antes de ejecutar la operación DE restauración SAN: También se restaura la estructura del directorio
Recurso configurado con replicación al almacenamiento de backup externo	No se puede llevar a cabo una restauración basada en volúmenes en un backup de copia de Snapshot más antiguo que la copia de Snapshot utilizada para la sincronización de SnapVault	Puede seleccionarse cualquier backup de Snapshot

Restauración de recursos completos desde el almacenamiento de backup externo

Una restauración desde el almacenamiento de backup externo siempre se ejecuta mediante una operación de restauración de SnapVault, donde todos los archivos o todos los LUN del volumen de almacenamiento se sobrescriben con el contenido del backup de Snapshot.

Restauración de un único inquilino

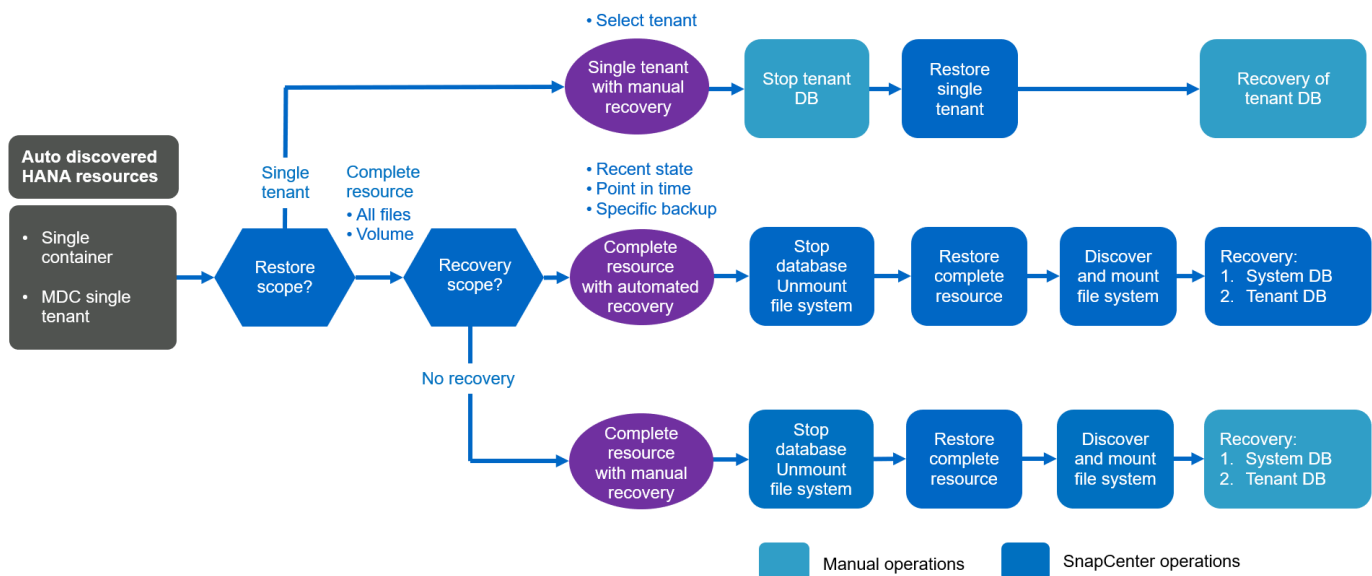
La restauración de un solo inquilino requiere una operación de restauración basada en archivos. Según el protocolo de almacenamiento utilizado, SnapCenter ejecuta diferentes flujos de trabajo de restauración.

- NFS:
 - Almacenamiento primario. Se ejecutan operaciones de SnapRestore basadas en archivos para todos los archivos de la base de datos de tenant.
 - Almacenamiento de backup externo: Se ejecutan las operaciones de restauración de SnapVault para todos los archivos de la base de datos de tenant.
- SAN:
 - Almacenamiento primario. Clonar y conectar el LUN al host de la base de datos y copiar todos los archivos de la base de datos de tenant.
 - Almacenamiento de backup externo. Clonar y conectar el LUN al host de la base de datos y copiar todos los archivos de la base de datos de tenant.

Restauración y recuperación de sistemas de un solo contenedor de HANA detectados automáticamente y de un solo inquilino de MDC

Los sistemas de un solo inquilino de HANA y MDC de HANA que se detectaron automáticamente están habilitados para restaurar y recuperar de forma automatizada con SnapCenter. Para estos sistemas HANA, SnapCenter admite tres flujos de trabajo diferentes de restauración y recuperación, como se muestra en la siguiente figura:

- **Un solo inquilino con recuperación manual.** Si selecciona una operación de restauración de un solo inquilino, SnapCenter enumera todos los arrendatarios que están incluidos en la copia de seguridad de Snapshot seleccionada. Debe detener y recuperar manualmente la base de datos de tenant. La operación de restauración con SnapCenter se realiza con operaciones de SnapRestore de archivos individuales para operaciones de NFS, o clonado, montaje y copia en entornos SAN.
- **Recurso completo con recuperación automatizada.** Si selecciona una operación de restauración de recursos completa y recuperación automatizada, el flujo de trabajo completo se automatiza con SnapCenter. SnapCenter admite hasta estado reciente, un momento específico o operaciones específicas de recuperación de backup. La operación de recuperación seleccionada se utiliza para el sistema y la base de datos de tenant.
- **Recurso completo con recuperación manual.** Si selecciona sin recuperación, SnapCenter detiene la base de datos HANA y ejecuta las operaciones de sistema de archivos necesarias (desmontaje, montaje) y restauración. Debe recuperar el sistema y la base de datos de tenant manualmente.

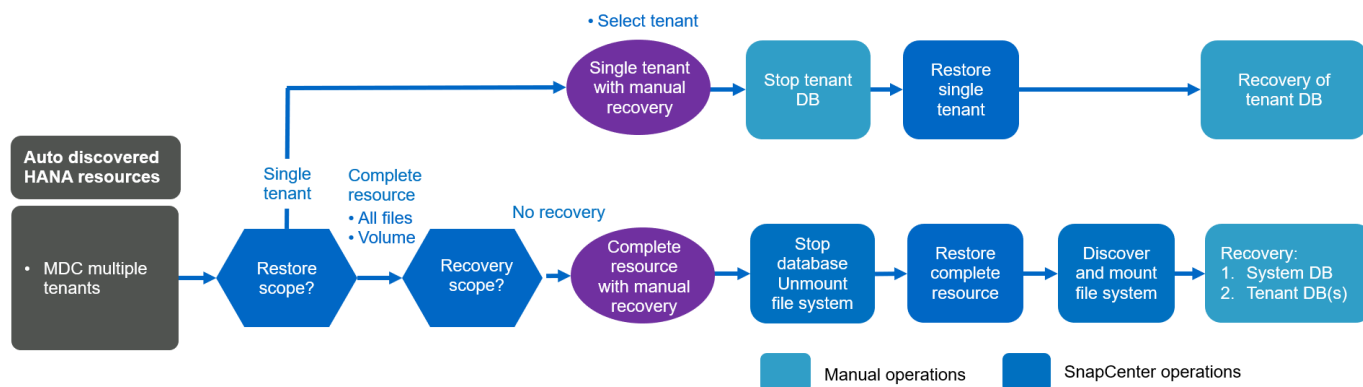


Restauración y recuperación de varios sistemas de tenant descubiertos automáticamente por el MDC de HANA

Aunque los sistemas MDC de HANA con múltiples inquilinos se pueden detectar automáticamente, la restauración y la recuperación automatizadas no son compatibles con la versión actual de SnapCenter. Para los sistemas MDC con múltiples inquilinos, SnapCenter admite dos flujos de trabajo diferentes de restauración y recuperación, como se muestra en la siguiente figura:

- Un solo inquilino con recuperación manual
- Recurso completo con recuperación manual

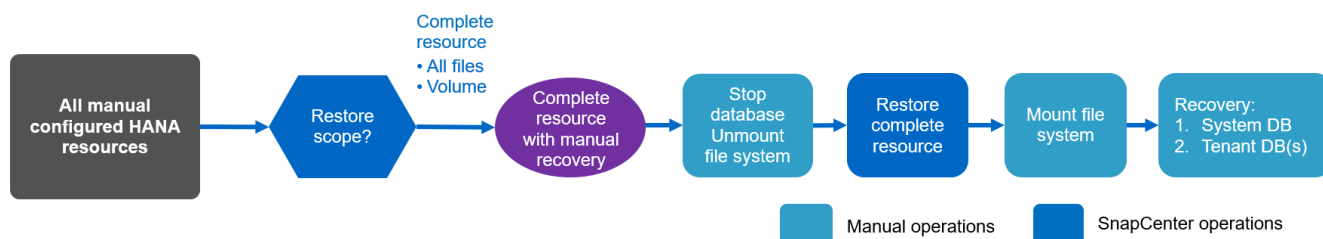
Los flujos de trabajo son los mismos que se describen en la sección anterior.



Restauración y recuperación de recursos HANA configurados manualmente

Los recursos HANA configurados manualmente no están habilitados para la restauración y la recuperación automatizadas. Asimismo, en el caso de sistemas MDC con uno o varios inquilinos, no se admite una operación de restauración de un solo inquilino.

Para los recursos HANA configurados manualmente, SnapCenter solo admite la recuperación manual, como se muestra en la siguiente figura. El flujo de trabajo para la recuperación manual es el mismo que el descrito en las secciones anteriores.



Resumen de las operaciones de restauración y recuperación

La tabla siguiente resume las operaciones de restauración y recuperación en función de la configuración de recursos de HANA en SnapCenter.

Configuración de recursos de SnapCenter	Opciones de restauración y recuperación	Detenga la base de datos HANA	Desmonte antes, monte después de la operación de restauración	Operación de recuperación
Auto descubrió un tenant único de MDC.contenedor único	<ul style="list-style-type: none"> • Recurso completo con cualquiera de los dos • Predeterminado (todos los archivos) • Reversión de volumen (solo NFS a partir del almacenamiento principal) • Recuperación automatizada seleccionada 	Automatizado con SnapCenter	Automatizado con SnapCenter	Automatizado con SnapCenter
	<ul style="list-style-type: none"> • Recurso completo con cualquiera de los dos • Predeterminado (todos los archivos) • Reversión de volumen (solo NFS a partir del almacenamiento principal) • No se ha seleccionado ninguna recuperación 	Automatizado con SnapCenter	Automatizado con SnapCenter	Manual
	<ul style="list-style-type: none"> • Restauración de inquilino 	Manual	No es obligatorio	Manual

Configuración de recursos de SnapCenter	Opciones de restauración y recuperación	Detenga la base de datos HANA	Desmante antes, monte después de la operación de restauración	Operación de recuperación
Auto descubrió múltiples inquilinos MDC	<ul style="list-style-type: none"> • Recurso completo con cualquiera de los dos • Predeterminado (todos los archivos) • Reversión de volumen (solo NFS a partir del almacenamiento principal) • No se admite la recuperación automatizada 	Automatizado con SnapCenter	Automatizado con SnapCenter	Manual
	<ul style="list-style-type: none"> • Restauración de inquilino 	Manual	No es obligatorio	Manual
Todos los recursos configurados manualmente	<ul style="list-style-type: none"> • Completo recurso (= reversión de volumen, disponible solo para NFS y SAN desde el almacenamiento principal) • Nivel de archivo (todos los archivos) • No se admite la recuperación automatizada 	Manual	Manual	Manual

Configuración de laboratorio utilizada para este informe

La configuración de laboratorio utilizada para este informe técnico incluye cinco configuraciones diferentes de SAP HANA:

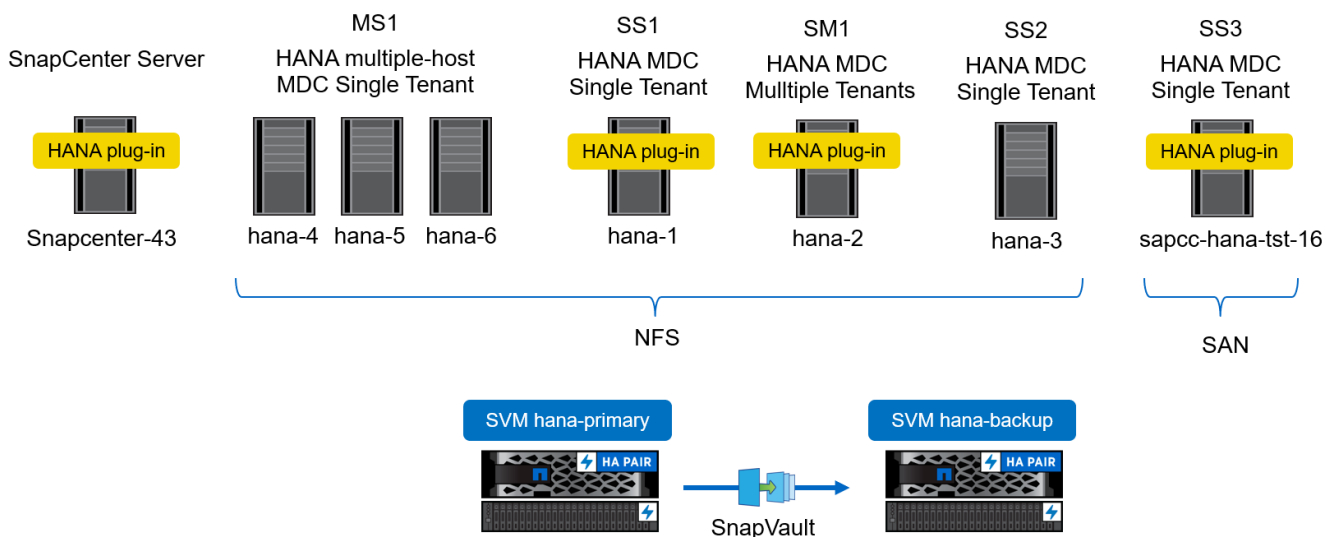
- **MS1.**
 - Sistema de un solo inquilino MDC de varios hosts de SAP HANA
 - Se gestiona con un host de plugin central (servidor SnapCenter).

- Utiliza NFS como protocolo de almacenamiento
- **SS1.**
 - Sistema de un solo inquilino MDC de host único de SAP HANA
 - Detección automática con el plugin de HANA instalado en el host de base de datos HANA
 - Utiliza NFS como protocolo de almacenamiento
- **SM1.**
 - Sistema de varios inquilinos MDC de un solo host SAP HANA
 - Detección automática con el plugin de HANA instalado en el host de base de datos HANA
 - Utiliza NFS como protocolo de almacenamiento
- **SS2.**
 - Sistema de un solo inquilino MDC de host único de SAP HANA
 - Se gestiona con un host de plugin central (servidor SnapCenter).
 - Utiliza NFS como protocolo de almacenamiento
- **SS3.**
 - Sistema de un solo inquilino MDC de host único de SAP HANA
 - Detección automática con el plugin de HANA instalado en el host de base de datos HANA
 - Utiliza SAN Fibre Channel como protocolo de almacenamiento

En las siguientes secciones se describe toda la configuración y los flujos de trabajo de backup, restauración y recuperación. La descripción abarca los backups de Snapshot locales y la replicación en el almacenamiento de backup mediante SnapVault. Las máquinas virtuales de almacenamiento (SVM) son `hana-primary` para el almacenamiento primario y `hana-backup` para el almacenamiento de backup externo.

El servidor SnapCenter se utiliza como host del complemento HANA central para los sistemas HANA MS1 y SS2.

La siguiente figura muestra la configuración del laboratorio.

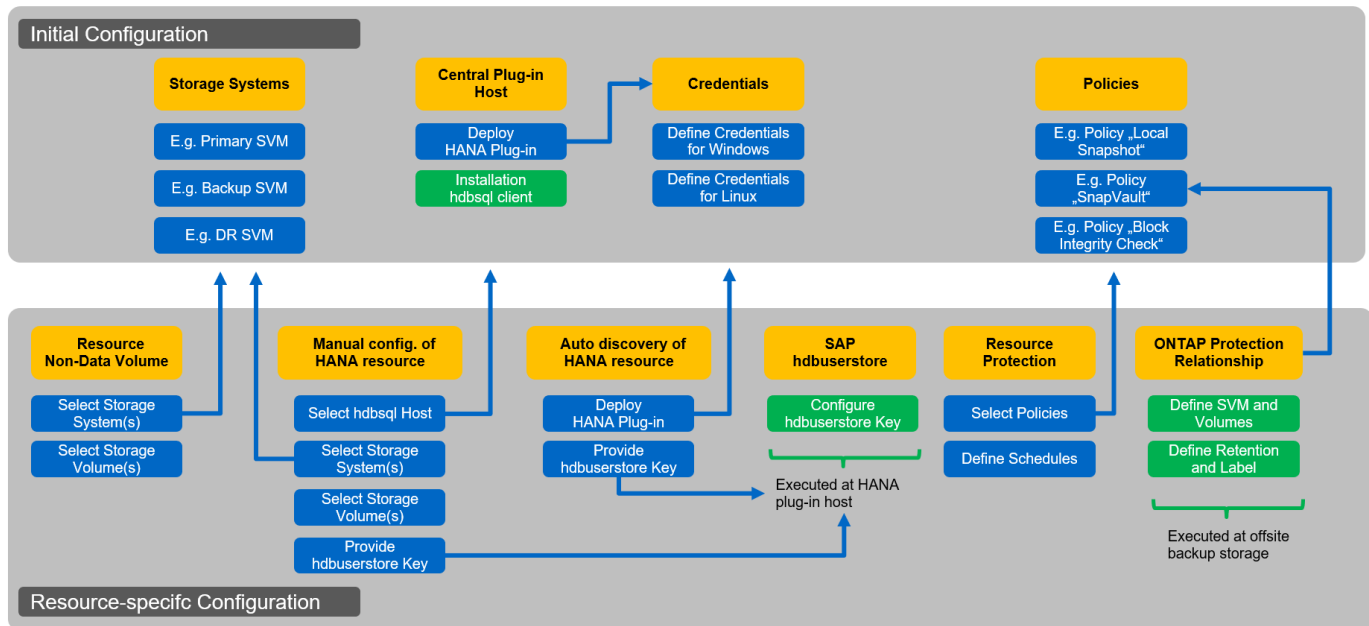


Configuración de SnapCenter

La configuración de SnapCenter se puede separar en dos áreas principales:

- **Configuración inicial.** cubre configuraciones genéricas, independientemente de una base de datos SAP HANA individual. Configuraciones como los sistemas de almacenamiento, los hosts del plugin central de HANA y las políticas, que se seleccionan al ejecutar las configuraciones específicas de un recurso.
- **La configuración específica del recurso.** cubre las configuraciones específicas del sistema SAP HANA y debe realizarse para cada base de datos SAP HANA.

En la siguiente figura, se proporciona información general sobre los componentes de configuración y sus dependencias. Los cuadros verdes muestran los pasos de configuración que deben realizarse fuera de SnapCenter; los cuadros azules muestran los pasos que se realizan mediante la GUI de SnapCenter.



Con la configuración inicial, se instalan y configuran los siguientes componentes:

- **Sistema de almacenamiento.** Configuración de credenciales para todas las SVM que utilizan los sistemas SAP HANA: Normalmente, almacenamiento primario, externo y de recuperación ante desastres.



Las credenciales del clúster de almacenamiento también pueden configurarse en lugar de credenciales de SVM individuales.

- **Credenciales.** Configuración de credenciales utilizada para implementar el complemento SAP HANA en los hosts.
- **Hosts (para hosts de plugins HANA centrales).** implementación del complemento SAP HANA. Instalación del software SAP HANA hdbclient en el host. El software SAP hdbclient debe instalarse manualmente.
- **Directivas.** Configuración del tipo de copia de seguridad, retención y replicación. Normalmente, se necesita al menos una política para las copias Snapshot locales, otra para la replicación de SnapVault y otra para el backup basado en archivos.

La configuración específica del recurso debe realizarse para cada base de datos SAP HANA e incluye las siguientes configuraciones:

- Configuración de recursos de volumen sin datos SAP HANA:
 - De almacenamiento y volúmenes
- Configuración de claves SAP hdbuserstore:
 - La configuración de clave de SAP hdbuserstore para la base de datos de SAP HANA específica debe realizarse en el host del plugin central o en el host de base de datos HANA, según dónde se haya puesto en marcha el plugin de HANA.
- Recursos de base de datos SAP HANA detectados automáticamente:
 - Puesta en marcha del plugin de SAP HANA en el host de la base de datos
 - Proporcione la clave hdbuserstore
- Configuración manual de recursos de base de datos SAP HANA:
 - SID de base de datos de SAP HANA, host del plugin, clave hdbuserstore, sistemas de almacenamiento y volúmenes
- Configuración de protección de recursos:
 - Selección de políticas requeridas
 - Definición de horarios para cada política
- Configuración de protección de datos de ONTAP:
 - Solo es necesario si los backups se deben replicar en un almacenamiento de backup externo.
 - Definición de la relación y la retención.

Configuración inicial de SnapCenter

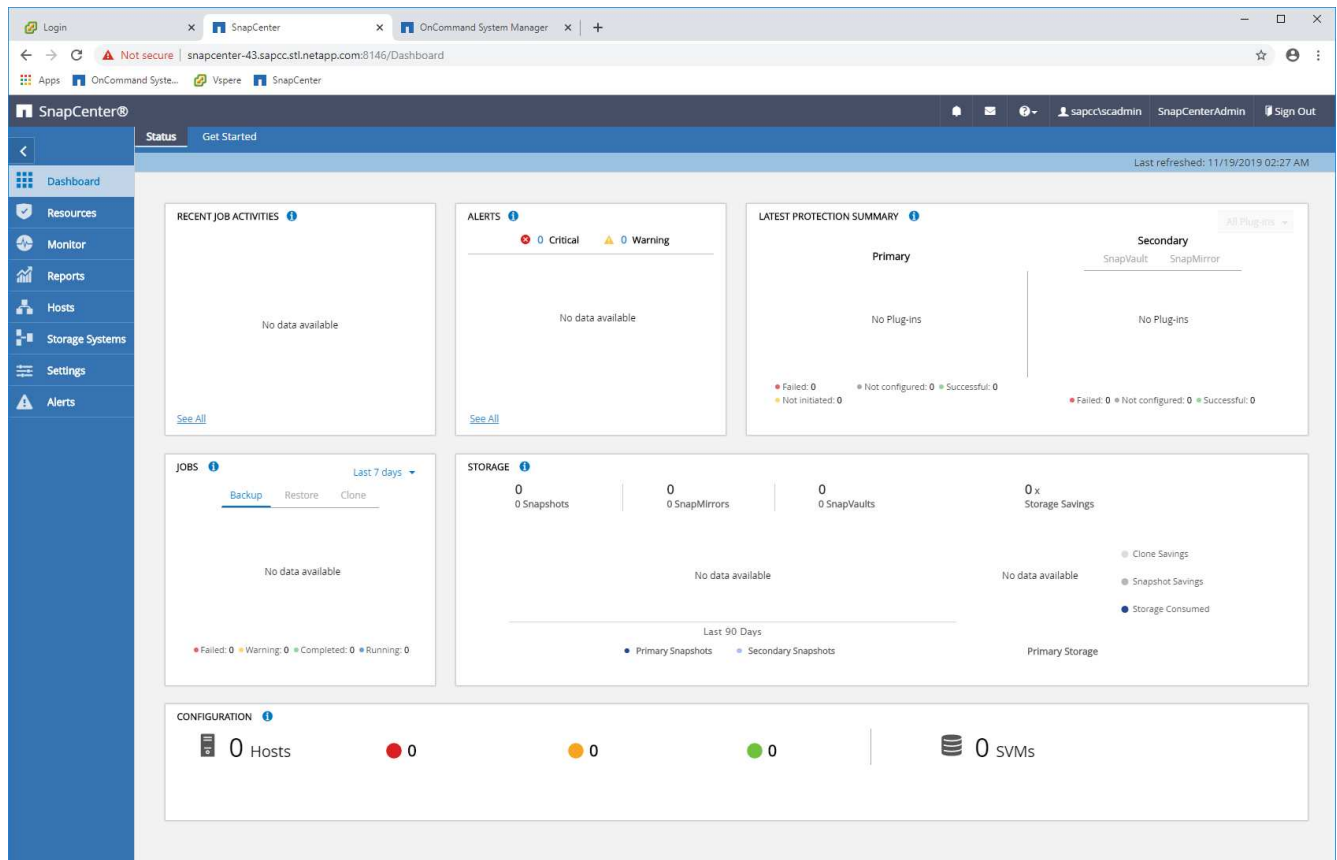
La configuración inicial incluye los siguientes pasos:

1. Configuración del sistema de almacenamiento
2. Configuración de credenciales para la instalación del plugin
3. Para un host de complemento de HANA central:
 - a. Configuración del host y puesta en marcha del plugin de SAP HANA
 - b. Instalación y configuración del software de cliente SAP HANA hdbsql
4. Configuración de políticas

Las siguientes secciones describen los pasos de configuración inicial.

Configuración del sistema de almacenamiento

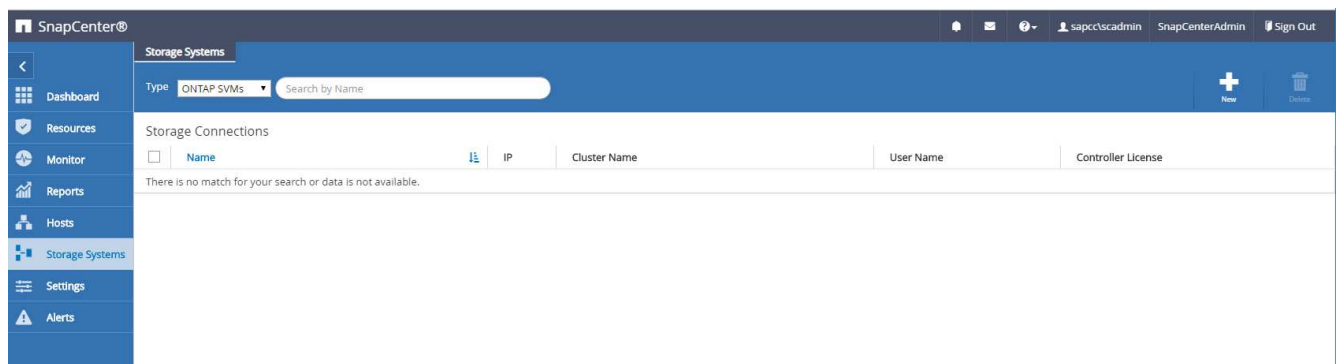
1. Inicie sesión en la interfaz gráfica de usuario del servidor de SnapCenter.



2. Seleccione almacenamiento sistemas.



En la pantalla, puede seleccionar el tipo de sistema de almacenamiento que puede ser ONTAP SVM o ONTAP Clusters. Si configura los sistemas de almacenamiento en el nivel de SVM, debe tener una LIF de gestión configurada para cada SVM. Como alternativa, puede utilizar un acceso de gestión de SnapCenter en el nivel de clúster. La gestión de SVM se utiliza en el siguiente ejemplo.



3. Haga clic en New para añadir un sistema de almacenamiento y proporcionar el nombre de host y las credenciales necesarios.



No se requiere que el usuario de SVM sea el usuario de vsadmin, tal como se muestra en la captura de pantalla. Generalmente, un usuario está configurado en la SVM y asignó los permisos necesarios para ejecutar operaciones de backup y restauración. Puede encontrar más detalles sobre los privilegios necesarios en la ["Guía de instalación de SnapCenter"](#) En la sección titulada "privilegios mínimos de ONTAP requeridos".

- Haga clic en más opciones para configurar la plataforma de almacenamiento.

La plataforma de almacenamiento puede ser FAS, AFF, ONTAP Select o Cloud Volumes ONTAP.



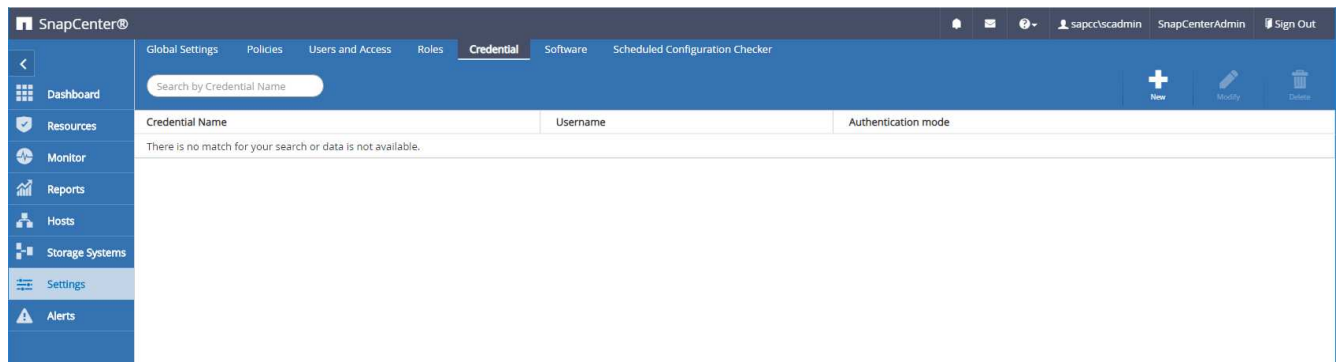
Para los sistemas que se utilizan como destino de SnapVault o SnapMirror, seleccione el icono Secondary.

- Añada sistemas de almacenamiento adicionales según sea necesario. En nuestro ejemplo, se ha añadido un almacenamiento adicional de backup externo y un sistema de almacenamiento de recuperación ante desastres.

Name	IP	Cluster Name	User Name	Controller License
hana-backup.sapcc.sti.netapp.com	10.63.150.45		vsadmin	Not applicable
hana-dr.sapcc.sti.netapp.com	10.63.150.247		vsadmin	Not applicable
hana-primary.sapcc.sti.netapp.com	10.63.150.248		vsadmin	✓

Configuración de credenciales

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



2. Proporcione las credenciales del usuario que se usan para instalaciones de plugins en sistemas Linux.

3. Proporcione las credenciales para el usuario que se usan para instalaciones de plugins en sistemas Windows.

Credential [X]

Provide information for the Credential you want to add

Credential Name:

Username:

Password:

Authentication:

En la siguiente figura se muestran las credenciales configuradas.

Credential Name	Username	Authentication mode
InstallPluginOnLinux	root	Linux
InstallPluginOnWindows	sapcc\scadmin	Windows

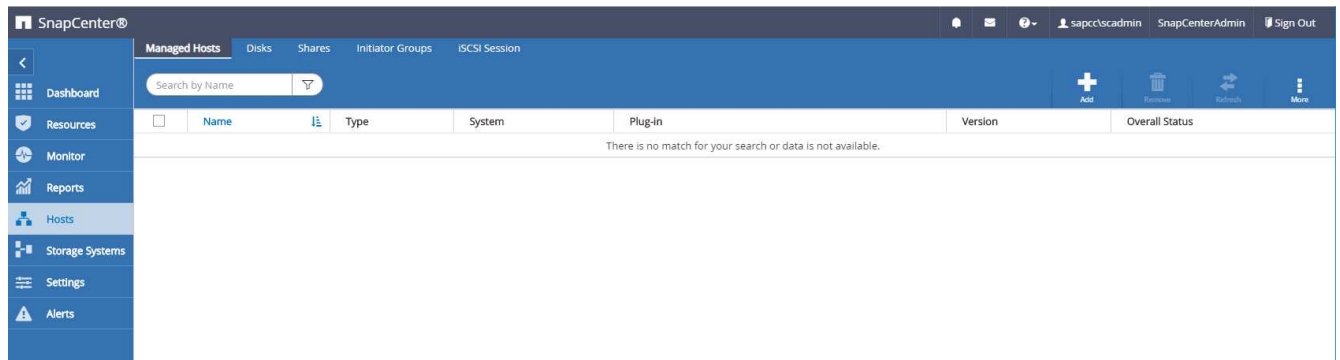
Instalación del plugin de SAP HANA en un host de plugin central

En la configuración de laboratorio, el servidor SnapCenter también se usa como host de complemento HANA central. El host de Windows en el que se ejecuta SnapCenter Server se añade como host y el plugin de SAP HANA se instala en el host de Windows.

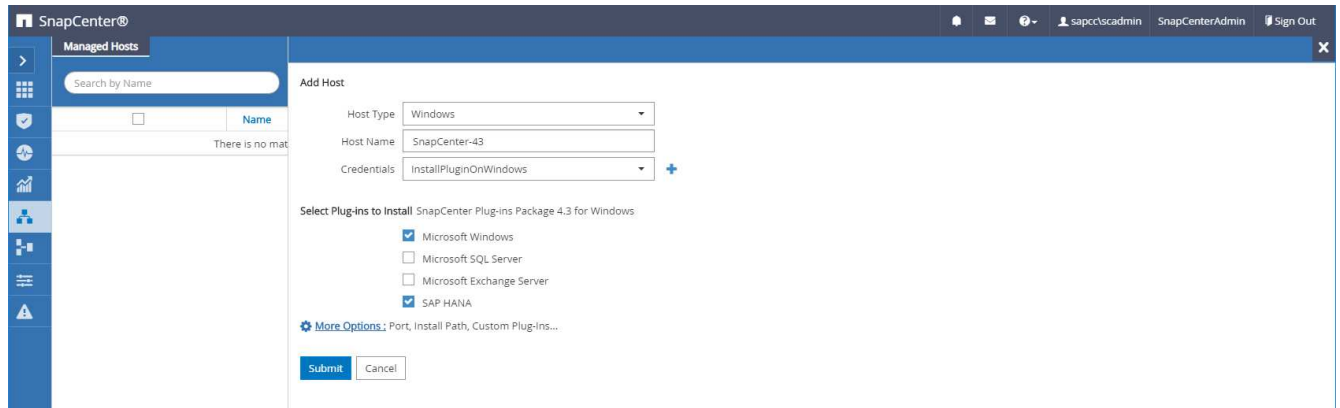


El plugin de SAP HANA requiere Java de 64 bits, versión 1.8. Java se debe instalar en el host antes de que se ponga en marcha el plugin de SAP HANA.

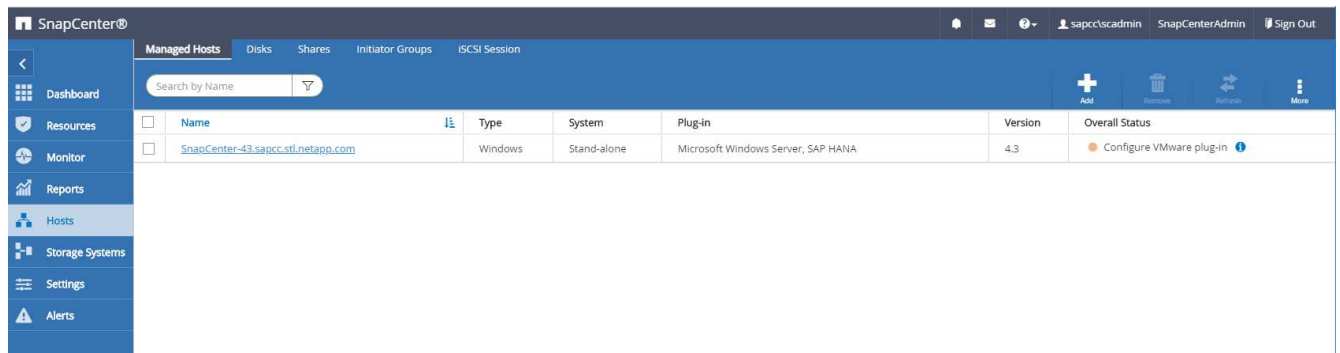
1. Vaya a hosts y haga clic en Add.



2. Proporcione la información del host requerida. Haga clic en Submit.



En la siguiente figura, se muestran todos los hosts configurados una vez que se pone en marcha el plugin para HANA.



Instalación y configuración del software de cliente SAP HANA hdbsql

El software de cliente SAP HANA hdbsql debe estar instalado en el mismo host en el que esté instalado el plugin de SAP HANA. El software puede descargarse del ["Portal de asistencia SAP"](#).

El usuario de sistema operativo de HDBSQL configurado durante la configuración de recursos debe poder ejecutar el ejecutable hdbsql. La ruta al ejecutable hdbsql debe configurarse en `hana.properties` archivo.

- Windows.

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in
Creator\etc\hana.properties
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

- Linux:

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties
HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

Configuración de directivas

Como se explica en la sección ["Estrategia de protección de datos"](#), Las políticas suelen configurarse de manera independiente del recurso y pueden ser usadas por varias bases de datos SAP HANA.

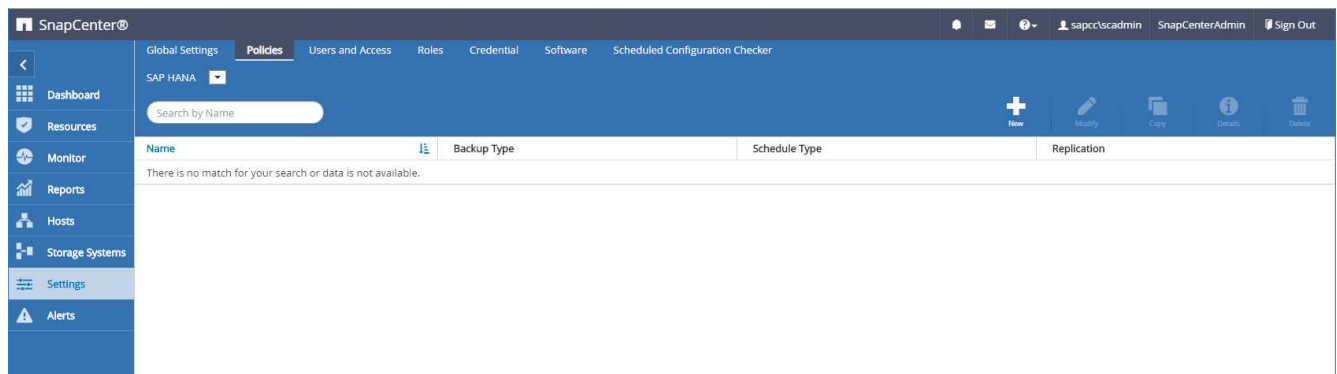
Una configuración mínima típica consiste en las siguientes políticas:

- Política de backups cada hora sin replicación: LocalSnap
- Normativas para backups diarios con replicación SnapVault: LocalSnapAndSnapVault
- 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 tres directivas.

Política de backups de snapshot cada hora

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



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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name

LocalSnap

Description

Snapshot backup at primary storage

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select backup settings

Backup Type

☒ Snapshot Based
 ☐ File-Based

Schedule Frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ None
 ☒ Hourly
 ☐ Daily
 ☐ Weekly
 ☐ Monthly

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Backup retention settings

☒ Total Snapshot copies to keep

☐ Keep Snapshot copies for

days

Hourly retention settings

5. Configurar los ajustes de retención para los backups programados.

New SAP HANA Backup Policy ✕

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Retention settings

On demand backup retention settings ▼

Hourly retention settings ▲

☒ Total Snapshot copies to keep ?

☐ Keep Snapshot copies for days

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

New SAP HANA Backup Policy ✕

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Select secondary replication options ?

☐ Update SnapMirror after creating a local Snapshot copy.
☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label ?

Error retry count ?

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

New SAP HANA Backup Policy ✕

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Summary

Policy name	LocalSnap
Description	Snapshot backup at primary storage
Backup Type	Snapshot Based Backup
Schedule Type	Hourly
On demand backup retention	Total backup copies to retain : 2
Hourly backup retention	Total backup copies to retain : 12
Replication	none

Normativa sobre backups snapshot diarios con replicación SnapVault

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name

LocalSnapAndSnapVault

Description

Local Snapshot backup replicated to backup storage

3. Establezca el tipo de backup en Snapshot Based y la frecuencia de programación en Daily.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select backup settings

Backup Type

☒ Snapshot Based
 ☐ File-Based

Schedule Frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ None
 ☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Backup retention settings

☒ Total Snapshot copies to keep
 ☐ Keep Snapshot copies for

3

14 days

Daily retention settings

5. Configurar los ajustes de retención para los backups programados.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Daily retention settings

Total Snapshot copies to keep

3

Keep Snapshot copies for

14

days

6. Seleccione Actualizar SnapVault después de crear una copia Snapshot local.



La etiqueta de la política secundaria debe ser la misma que la etiqueta de SnapMirror en la configuración de protección de datos en la capa de almacenamiento. Consulte la sección ["Configuración de la protección de datos en almacenamiento de backup externo".](#)

Modify SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

Policy name	LocalSnapAndSnapVault
Description	Local Snapshot backup replicated to backup storage
Backup Type	Snapshot Based Backup
Schedule Type	Daily
On demand backup retention	Total backup copies to retain : 3
Daily backup retention	Total backup copies to retain : 3
Replication	SnapVault enabled , Secondary policy label: Daily , Error retry count: 3

Previous

Finish

Política de Comprobación de integridad de bloque semanal

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name	BlockIntegrityCheck
Description	Block integrity check using file based backup

3. Establezca el tipo de backup en File-based y la frecuencia de programación en Weekly.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Select backup settings

Backup Type

☐ Snapshot Based
☒ File-Based

Schedule Frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ None
☐ Hourly
☐ Daily
☒ Weekly
☐ Monthly

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Retention settings

On demand backup retention settings

Backup retention settings

☒ Total backup copies to keep
☐ Keep backup copies for

1

14 days

Weekly retention settings

5. Configurar los ajustes de retención para los backups programados.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Retention settings

On demand backup retention settings

Backup retention settings

☒ Total backup copies to keep
☐ Keep backup copies for

1

14 days

Weekly retention settings

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

New SAP HANA Backup Policy

1 Name
2 Settings
3 Retention
4 Summary

Summary

Policy name	BlockIntegrityCheck
Description	Block integrity check using file based backup
Backup Type	File-Based Backup
Schedule Type	Weekly
On demand backup retention	Total backup copies to retain : 1
Weekly backup retention	Total backup copies to retain : 1

Previous
Finish

En la siguiente figura, se muestra un resumen de las políticas configuradas.

SnapCenter®				
<div> <div> Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts </div> <div> Global Settings Policies Users and Access Roles Credential Software Scheduled Configuration Checker </div> </div>				
<div> <div>SAP HANA</div> <div>Search by Name</div> <div> + Modify Copy Details Delete </div> </div>				
Name	Backup Type	Schedule Type	Replication	
BlockIntegrityCheck	File Based Backup	Weekly		
LocalSnap	Data Backup	Hourly		
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault	

Configuración específica de recursos de SnapCenter para backups de base de datos SAP HANA

En esta sección se describen los pasos de configuración de dos configuraciones de ejemplo.

- **SS2.**

- Sistema de un solo inquilino SAP HANA MDC de un solo host mediante NFS para el acceso al almacenamiento
- El recurso se configura manualmente en SnapCenter.
- El recurso está configurado para crear backups de Snapshot locales y realizar comprobaciones de integridad de bloques para la base de datos de SAP HANA mediante un backup basado en archivos semanal.

- **SS1.**

- Sistema de un solo inquilino SAP HANA MDC de un solo host mediante NFS para el acceso al almacenamiento
- El recurso se detecta automáticamente con SnapCenter.
- El recurso se configura para crear backups Snapshot locales, replicar a un almacenamiento de backup externo mediante SnapVault y realizar comprobaciones de integridad de bloque para la base de datos SAP HANA mediante un backup semanal basado en archivos.

Las diferencias entre un sistema conectado A SAN, un único contenedor o un sistema de varios hosts se reflejan en los pasos de configuración o flujo de trabajo correspondientes.

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.

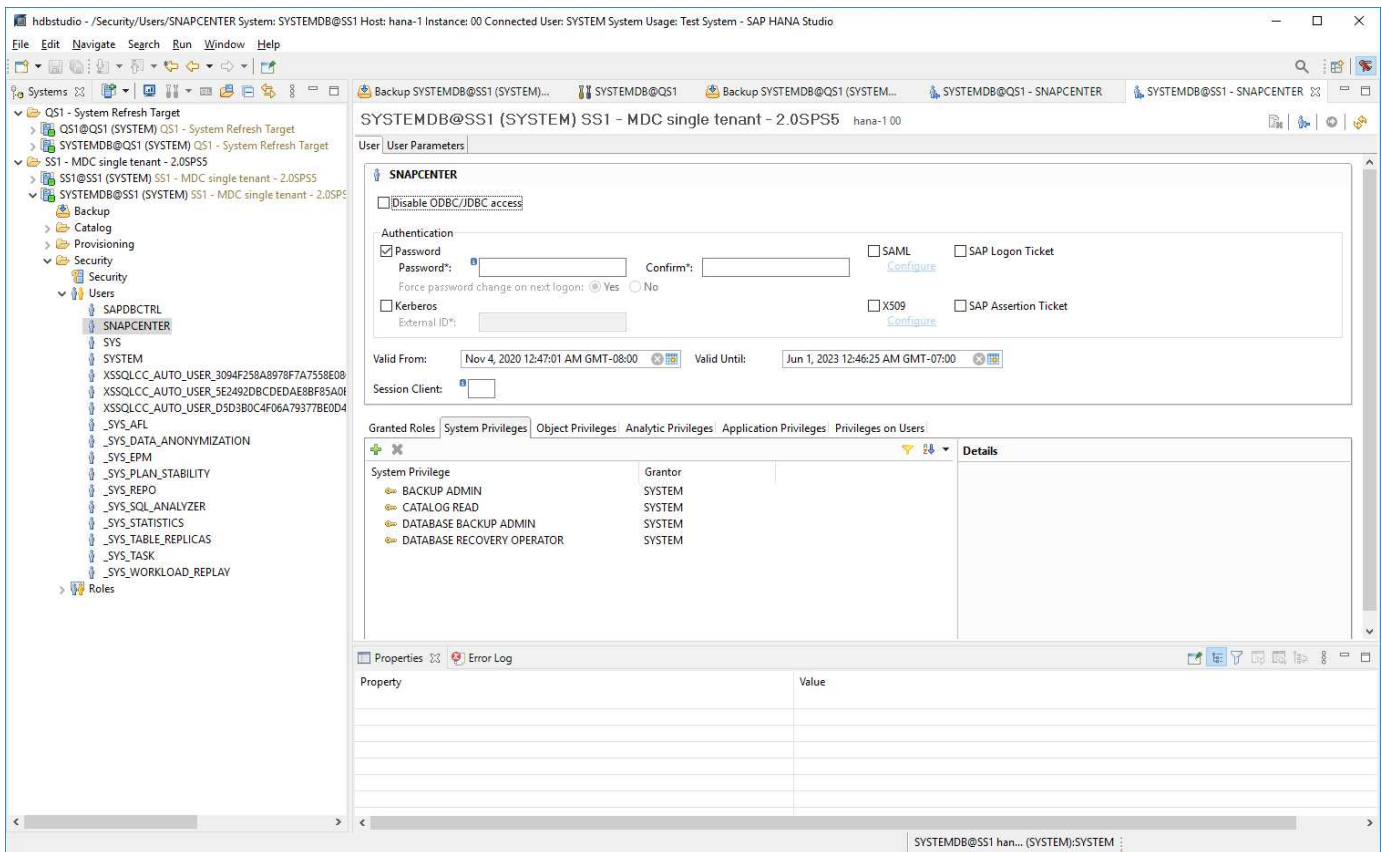
La siguiente figura muestra SAP HANA Studio a través de la cual se puede crear el usuario de backup.



Los privilegios necesarios se modificaron 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, el usuario debe crearse 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.



Debe configurarse una clave de almacén de usuarios en el host del complemento HANA, en el que estén instalados el complemento SAP HANA y el cliente SAP hdbsql.

Configuración del Userstore en el servidor SnapCenter que se utiliza como host de plugin para HANA central

Si el plug-in SAP HANA y el cliente SAP hdbsql están instalados en Windows, el usuario del sistema local ejecuta los comandos hdbsql y está configurado de forma predeterminada en la configuración de recursos. Dado que el usuario del sistema no es un usuario de inicio de sesión, la configuración del almacén de usuario debe realizarse con un usuario diferente y el `-u <User>` opción.

```
hdbuserstore.exe -u SYSTEM set <key> <host>:<port> <database user>
<password>
```



El software SAP HANA hdbclient debe estar instalado primero en el host Windows.

Configuración de Userstore en un host Linux separado que se utiliza como host de plugin para HANA central

Si el complemento SAP HANA y el cliente SAP hdbsql están instalados en un host Linux independiente, se utiliza el siguiente comando para la configuración del almacén de usuarios con el usuario definida en la configuración de recursos:

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



El software SAP HANA hdbclient debe estar instalado primero en el host Linux.

Configuración del Userstore en el host de la base de datos HANA

Si el plugin de SAP HANA se implementa en el host de la base de datos HANA, se utiliza el siguiente comando 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, la clave de almacenamiento de usuario debe configurarse utilizando 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, el hdbclient debe instalarse primero.

Configuración del Userstore en función de la arquitectura del sistema HANA

En una configuración de un solo inquilino 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 contenedor único de SAP HANA, el puerto 3<instanceNo>15 Es el puerto estándar para el acceso SQL al servidor de índices y debe utilizarse en la configuración hdbuserstore.

Para una configuración de varios hosts de SAP HANA, se deben configurar las claves de almacenamiento de usuario de todos los hosts. SnapCenter intenta conectarse a la base de datos utilizando cada una de las claves proporcionadas y, por lo tanto, puede funcionar independientemente de la conmutación al nodo de respaldo de un servicio SAP HANA a un host diferente.

Ejemplos de configuración de Userstore

En la configuración de laboratorio, se utiliza una puesta en marcha mixta de complemento SAP HANA. El plugin de HANA se instala en el servidor de SnapCenter para algunos sistemas HANA y se pone en marcha en servidores de base de datos HANA individuales para otros sistemas.

Sistema SAP HANA SS1, MDC de un solo inquilino, instancia 00

El plugin de HANA se implementó en el host de la base de datos. Por lo tanto, la clave debe configurarse en el host de la base de datos con el usuario ss1adm.


```

hana-1:/ # su - ssladm
ssladm@hana-1:/usr/sap/SS1/HDB00>
ssladm@hana-1:/usr/sap/SS1/HDB00>
ssladm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ssladm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE          : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE           : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ssladm@hana-1:/usr/sap/SS1/HDB00>

```

Sistema SAP HANA MS1, multi-host MDC single tenant, instancia 00

Para HANA de varios sistemas host, se requiere un host de complemento centralizado. En nuestra configuración, utilizamos SnapCenter Server. Por lo tanto, la configuración del almacén de usuario debe realizarse en el servidor SnapCenter.

```

hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE          : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.DAT
KEY FILE           : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
  ENV : hana-4:30013
  USER: SNAPCENTER
KEY MS1KEYHOST2
  ENV : hana-5:30013
  USER: SNAPCENTER
KEY MS1KEYHOST3
  ENV : hana-6:30013
  USER: SNAPCENTER
KEY SS2KEY
  ENV : hana-3:30013
  USER: SNAPCENTER
C:\Program Files\sap\hdbclient>

```

Configuración de la protección de datos para un almacenamiento de backup externo

Para que SnapCenter pueda gestionar las actualizaciones de replicación, es necesario ejecutar la configuración de la relación de protección de datos y la transferencia de datos inicial.

En la siguiente figura, se muestra la relación de protección configurada para el sistema SAP HANA SS1. Con nuestro ejemplo, el volumen de origen SS1_data_mnt00001 En la máquina virtual SVM hana-primary Se replica en la SVM hana-backup y el volumen objetivo SS1_data_mnt00001_dest.



La programación de la relación debe establecerse en ninguna, ya que SnapCenter activa la actualización de SnapVault.

The screenshot shows the OnCommand System Manager interface. The left sidebar contains navigation options: Dashboard, Applications & Tiers, Storage, Network, Protection, Volume Relationships, SVM DR Relationships, Protection Policies, Schedules, Snapshot Policies, Events & Jobs, and Configuration. The main pane is titled 'Volume Relationships' and displays a table with columns: Source Storage Volume, Source Volume, Destination Volume, Destination Storage Volume, Is Healthy, Object, Relationship Type, Lag Time, Policy Name, and Policy Type. A row is highlighted with a blue border, showing 'hana-primary' as the source storage volume, 'SS1_data_mnt00001' as the source volume, 'SS1_data_mnt00001_dest' as the destination volume, 'hana-backup' as the destination storage volume, and 'Yes' for 'Is Healthy'. Below the table, the 'Details' tab is selected, showing configuration details for the relationship. The 'Transfer Schedule' is set to 'None', which is highlighted with a blue border. Other details include 'Source Location: hana-primary:SS1_data_mnt00001', 'Destination Location: hana-backup:SS1_data_mnt00001_dest', 'Source Cluster: a700-marco', 'Destination Cluster: a700-marco', 'Is Healthy: Yes', 'Relationship State: Snapmirrored', 'Network Compression Ratio: Not Applicable', 'Transfer Status: Idle', 'Current Transfer Type: None', 'Current Transfer Error: None', 'Current Transfer Progress: None', 'Last Transfer Error: None', 'Last Transfer Type: Update', 'Latest Snapshot Timestamp: 11/26/2019 11:03:53', and 'Latest Snapshot Copy: SnapCenter_LocalSnapAndSnapVault_Daily_11-26-2019_08.17.01.8979'.

La siguiente figura muestra la política de protección. La política de protección utilizada para la relación de protección define la etiqueta de SnapMirror, así como la retención de backups en el almacenamiento secundario. En nuestro ejemplo, la etiqueta utilizada es `Daily`, y la retención se establece en 5.



La etiqueta de SnapMirror en la política que se va a crear debe coincidir con la etiqueta definida en la configuración de la política de SnapCenter. Para obtener más información, consulte [“Normativa sobre backups snapshot diarios con replicación SnapVault.”](#)



La retención de backups en el almacenamiento de backups fuera de las instalaciones se define en la política y está controlada por ONTAP.

OnCommand System Manager

Type: All Search all Objects

Volume Relationships

Create Edit Delete Operations Refresh

Source Storage Vi...	Source Volume	Destination Volume	Destination Stora...	Is Healthy	Object ...	Rela...	Transf...	Relationship Type	Lag Time	Policy Name	Policy Type
hana-primary	SS1_data_mnt00001	SS1_data_mnt00001_dest	hana-backup	Yes	Volume	Snapmi...	Idle	Asynchronous V...	21 hrs(s)...	SnapCenterVault	Asynchronous Vault

Policy Name: SnapCenterVault

Comments:

Label	Number of Copies	Matching Snapshot copy Schedules in Source Volume
Daily	5	Source does not have any schedules with this label

Details Policy Details Snapshot Copies

Configuración manual de recursos de HANA

Esta sección describe la configuración manual de los recursos SAP HANA SS2 y MS1.

- SS2 es un sistema de un solo inquilino de MDC de un solo host
- MS1 es un sistema de un solo inquilino de MDC de varios hosts.
 - a. En la pestaña Resources, seleccione SAP HANA y haga clic en Add SAP HANA Database.
 - b. Introduzca la información para configurar la base de datos SAP HANA y haga clic en Next.

Seleccione el tipo de recurso en nuestro ejemplo, Multitenant Database Container.



Para un sistema de contenedor único HANA, se debe seleccionar el tipo de recurso Single Container. El resto de pasos de configuración son idénticos.

Para nuestro sistema SAP HANA, el SID es SS2.

El host del plugin de HANA en nuestro ejemplo es el servidor SnapCenter.

La clave hdbuserstore debe coincidir con la clave que se configuró para la base de datos HANA SS2. En nuestro ejemplo es SS2KEY.

Add SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Provide Resource Details

Resource Type
Multitenant Database Container

HANA System Name
SS2 - HANA 20 SPS4 MDC Single Tenant

SID
SS2

Plug-in Host
SnapCenter-43.sapcc.stl.netapp.com

HDB Secure User Store Keys
SS2KEY

HDBSQL OS User
SYSTEM



Para un sistema SAP HANA de varios hosts, debe incluir las claves hdbuserstore para todos los hosts, como se muestra en la siguiente figura. SnapCenter intentará conectarse con la primera clave de la lista y continuará con el otro caso, por si la primera clave no funciona. Esto es necesario para admitir la conmutación por error de HANA en un sistema de varios hosts con hosts de trabajo y en espera.

Modify SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Provide Resource Details

Resource Type
Multitenant Database Container

HANA System Name
MS1 - Multiple Hosts MDC Single Tenant

SID
MS1

Plug-in Host
SnapCenter-43.sapcc.stl.netapp.com

HDB Secure User Store Keys
MS1KEYHOST1,MS1KEYHOST2,MS1KEYHOST3

HDBSQL OS User
SYSTEM

c. Seleccione los datos requeridos para el sistema de almacenamiento (SVM) y el nombre del volumen.

Add SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Provide Storage Footprint Details

Add Storage Footprint

Storage System
hana-primary.sapcc.stl.netapp.com

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name
SS2_data_mnt00001

LUNs or Qtrees
Default is 'None' or type to find

Save



Para obtener una configuración SAN Fibre Channel, también es necesario seleccionar la LUN.



Para un sistema host múltiple SAP HANA, se deben seleccionar todos los volúmenes de datos del sistema SAP HANA, como se muestra en la siguiente figura.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Storage Footprint Details

Add Storage Footprint

Storage System: hana-primary.sapcc.stl.netapp.com

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name	LUNs or Qtrees
MS1_data_mnt00001	Default is 'None' or type to find
MS1_data_mnt00002	Default is 'None' or type to find

Save

Se muestra la pantalla de resumen de la configuración de recursos.

- Haga clic en Finish para añadir la base de datos SAP HANA.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Summary

Resource Type	Multitenant Database Container
HANA System Name	SS2 - HANA 20 SPS4 MDC Single Tenant
SID	SS2
Plug-in Host	SnapCenter-43.sapcc.stl.netapp.com
HDB Secure User Store Keys	SS2KEY
HDBSQL OS User	SYSTEM

Storage Footprint

Storage System	Volume	LUN/Qtree
hana-primary.sapcc.stl.netapp.com	SS2_data_mnt00001	

- Cuando finalice la configuración del recurso, realice la configuración de la protección de recursos como se describe en la sección [“Configuración de protección de recursos.”](#)

Detección automática de las bases de datos HANA

En esta sección se describe la detección automática del recurso SS1 de SAP HANA (sistema de un solo inquilino MDC de host único con NFS). Todos los pasos descritos son idénticos para un único contenedor HANA, sistemas de varios inquilinos MDC de HANA y un sistema HANA que utiliza SAN Fibre Channel.



El plugin de SAP HANA requiere Java de 64 bits, versión 1.8. Java se debe instalar en el host antes de que se ponga en marcha el plugin de SAP HANA.

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.

Managed Hosts

Search by Name

Add Host

Host Type: Linux

Host Name: hana-1

Credentials: InstallPluginOnLinux

Select Plug-ins to Install: SnapCenter Plug-ins Package 4.3 for Linux

☐ Oracle Database

☒ SAP HANA

[More Options](#) : Port, Install Path, Custom Plug-Ins...

3. Confirme la huella.

Confirm Fingerprint

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
hana-1.sapcc.stl.netapp.com	ssh-rsa 2048 6E:80:F0:B7:6E:8F:E4:9A:E5:2E:E8:6A:0C:0A:18:C7	

La instalación del plugin de HANA y el plugin de Linux se inicia de forma automática. Cuando termina la instalación, la columna de estado del host muestra ejecutando. La pantalla también muestra que el plugin de Linux se ha instalado junto con el plugin de HANA.

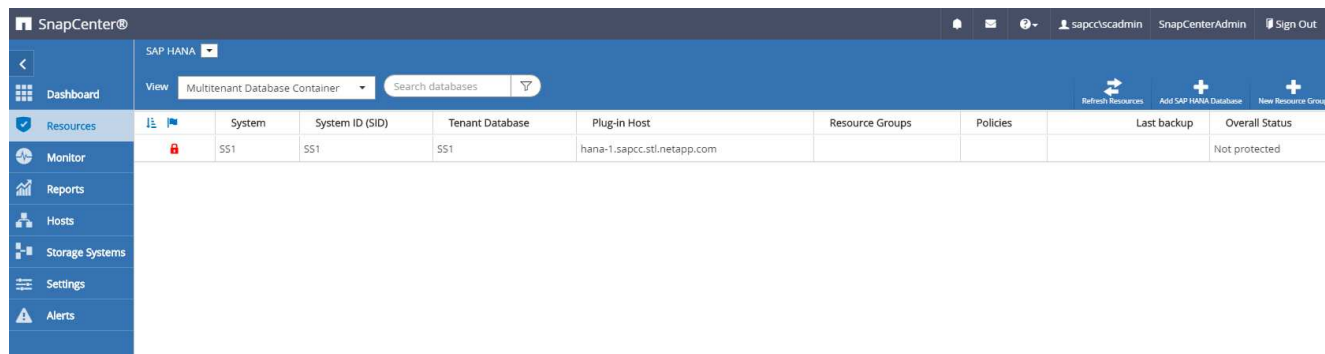
Name	Type	System	Plug-in	Version	Overall Status
hana-1.sapcc.stl.netapp.com	Linux	Stand-alone	UNIX, SAP HANA	4.3	Running
SnapCenter-43.sapcc.stl.netapp.com	Windows	Stand-alone	Microsoft Windows Server, SAP HANA	4.3	Running

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.

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



También es posible activar el proceso de detección automática manualmente en la pantalla Resources, haciendo clic en Refresh Resources.



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

Configure Database

Plug-in host: hana-1.sapcc.stl.netapp.com

HDBSQL OS User: ss1adm

HDB Secure User Store Keys:

Configuring Database...

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.

6. Haga clic en Details para revisar la información de configuración de los recursos HANA en la vista de topología de los recursos.

Manage Copies

Local copies: 17 Backups, 0 Clones

Vault copies: 5 Backups, 0 Clones

Summary Card

- 24 Backups
- 22 Snapshot based backups
- 2 File-Based backups ✓
- 0 Clones

Primary Backup(s)

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_11-27-2019_02.30.01.1788	1	11/27/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_11-26-2019_22.30.01.0413	1	11/26/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_11-26-2019_18.30.01.0738	1	11/26/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_11-26-2019_14.30.01.0340	1	11/26/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_11-26-2019_10.30.01.0649	1	11/26/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-26-2019_08.17.01.8979	1	11/26/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_11-26-2019_06.30.01.0003	1	11/26/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_11-26-2019_02.30.00.9915	1	11/26/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_11-25-2019_22.30.01.0536	1	11/25/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_11-25-2019_18.30.01.0250	1	11/25/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_11-25-2019_14.30.01.0151	1	11/25/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_11-25-2019_10.30.00.9895	1	11/25/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-25-2019_08.17.01.8577	1	11/25/2019 8:17:55 AM
SnapCenter_LocalSnap_Hourly_11-25-2019_06.30.00.9717	1	11/25/2019 6:30:55 AM

Total 4

Activity: The 5 most recent jobs are displayed. 4 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

Resource - Details

Details for selected resource

Type: Multitenant Database Container

HANA System Name: SS1

SID: SS1

Tenant Database: SS1

Plug-in Host: hana-1.sapcc.stl.netapp.com

HDB Secure User Store Keys: SS1KEY

HDBSQL OS User: ss1adm

plug-in name: SAP HANA

Last backup: 11/27/2019 2:30:55 AM (Completed)

Resource Groups: hana-1.sapcc.stl.netapp.com_hana_MDC_SS1

Policy: BlockIntegrityCheck, LocalSnap, LocalSnapAndSnapVault

Discovery Type: Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtrees
hana-primary.sapcc.stl.netapp.com	SS1_data_mnt00001	/SS1_data_mnt00001	

Total 4

Activity: The 5 most recent jobs are displayed. 4 Completed, 0 Warnings, 0 Failed, 0 Canceled, 1 Running, 0 Queued.

Cuando finalice la configuración de los recursos, la configuración de protección de recursos debe ejecutarse tal como se describe en la sección siguiente.

Configuración de protección de recursos

En esta sección se describe la configuración de protección de recursos. La configuración de la protección de recursos es la misma, independientemente de que el recurso se detecte automáticamente o se configure manualmente. También es idéntico para todas las arquitecturas de HANA, hosts únicos o múltiples, sistemas de un solo contenedor o MDC.

1. En la pestaña Resources, haga doble clic en el recurso.
2. Configure un formato de nombre personalizado para la copia de Snapshot.



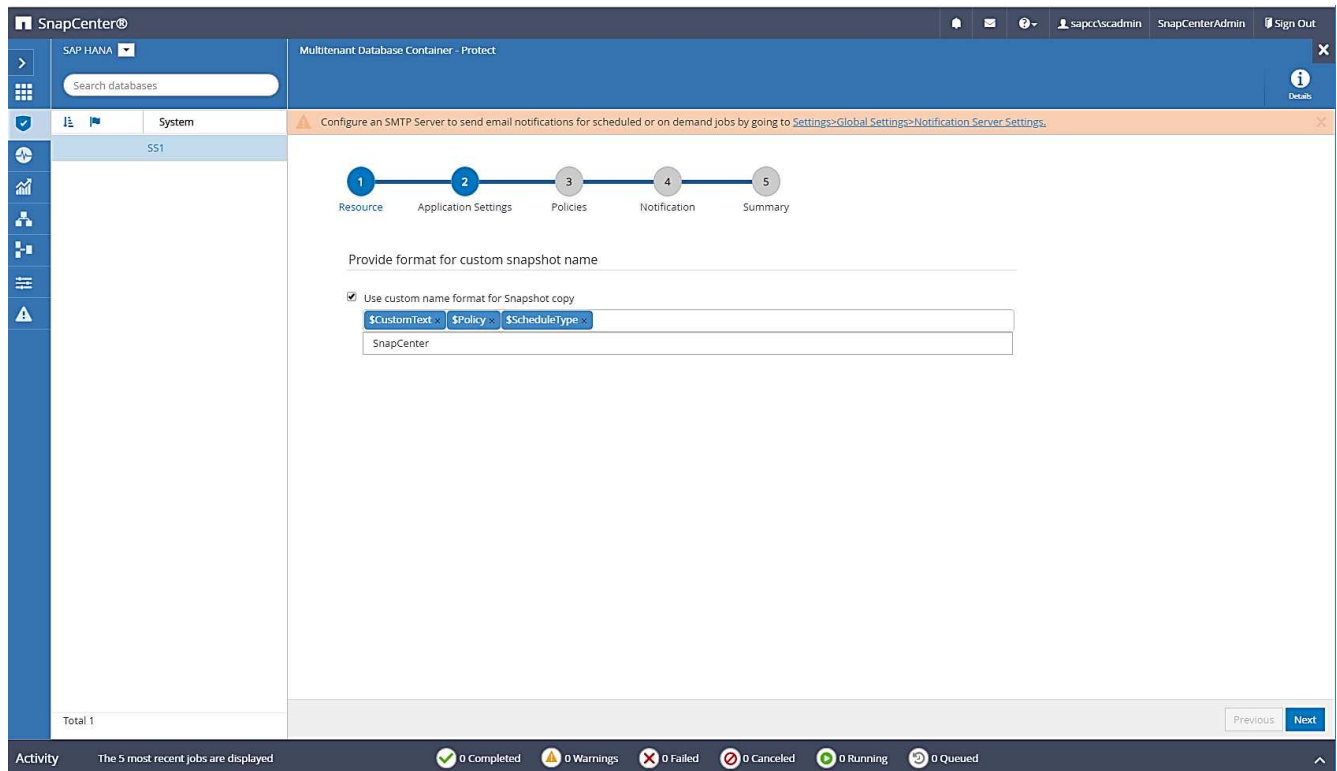
NetApp recomienda utilizar un nombre de copia de Snapshot personalizado para identificar fácilmente qué backups se han creado con qué tipo de normativa y programación. Al añadir el tipo de programación al nombre de la copia de Snapshot, es posible distinguir entre backups programados y bajo demanda. 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.

En la configuración mostrada en la siguiente figura, los nombres de backup y copia Snapshot tienen el siguiente formato:

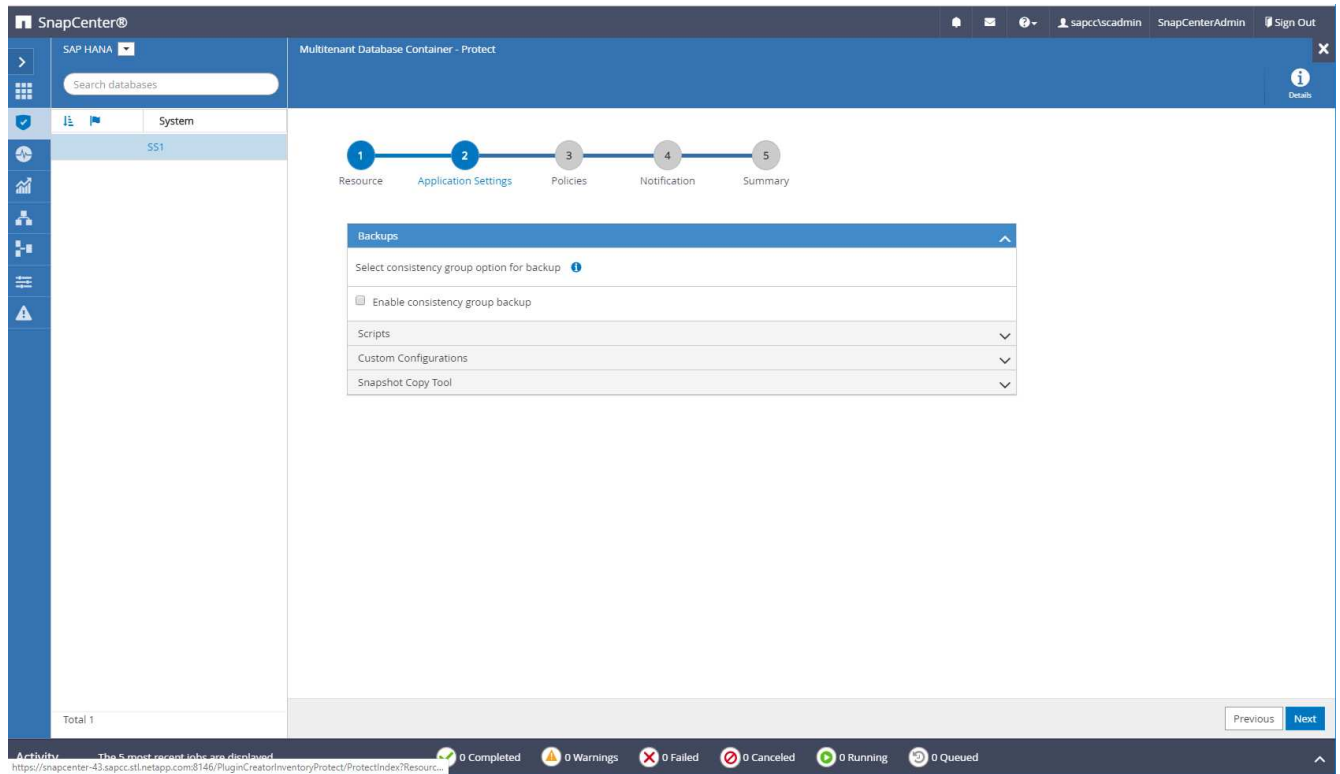
- Backup programado por hora: SnapCenter_LocalSnap_Hourly_<time_stamp>
- Backup diario programado: SnapCenter_LocalSnapAndSnapVault_Daily_<time_stamp>
- Backup por horas bajo demanda: SnapCenter_LocalSnap_<time_stamp>
- Backup diario bajo demanda: SnapCenter_LocalSnapAndSnapVault_<time_stamp>



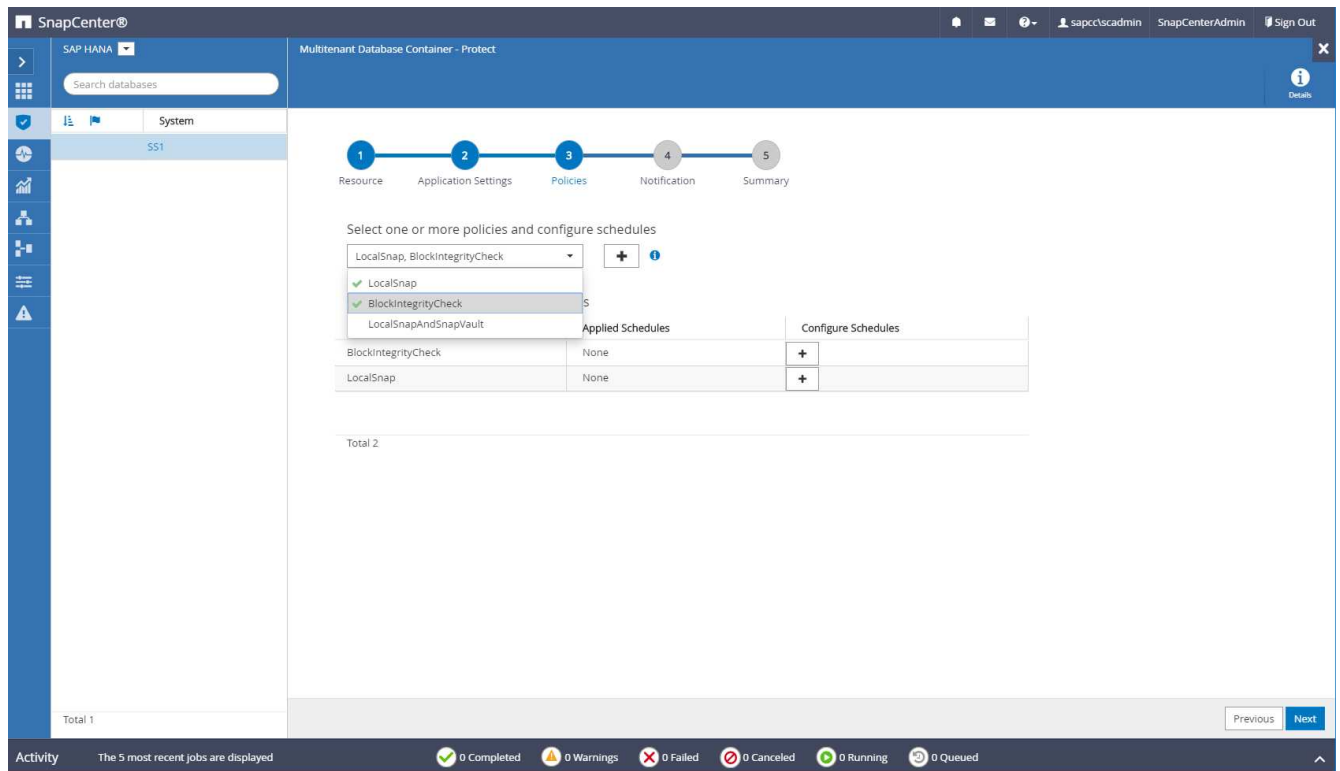
Aunque se define una retención para backups bajo demanda en la configuración de políticas, el mantenimiento solo se realiza cuando se ejecuta otro backup bajo demanda. Por lo tanto, los backups bajo demanda suelen eliminarse manualmente en SnapCenter para asegurarse de que estos backups también se eliminan en el catálogo de backup de SAP HANA y que el mantenimiento del backup de registros no se basa en un backup antiguo bajo demanda.



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



4. Seleccione las políticas que desea añadir al recurso.



5. Defina la programación para la política LocalSnap (en este ejemplo, cada cuatro horas).

Add schedules for policy LocalSnap

Hourly

Start date

11/19/2019 6:30 AM

☐ Expires on

12/19/2019 5:59 AM

Repeat every

4

hours

0

mins

i

The schedules are triggered in the SnapCenter Server time zone.

Cancel

Ok

6. Defina la programación para la política LocalSnapAndSnapVault (en este ejemplo, una vez por día).

Modify schedules for policy LocalSnapAndSnapVault

Daily

Start date

11/19/2019 8:17 AM

☐ Expires on

12/19/2019 8:17 AM

Repeat every

1

days

i

The schedules are triggered in the SnapCenter Server time zone.

Cancel

Ok

- Defina el programa de la política de comprobación de integridad de bloques (en este ejemplo, una vez a la semana).

Add schedules for policy BlockIntegrityCheck

Weekly

Start date

11/19/2019 5:57 AM

☐ Expires on

12/19/2019 5:57 AM

Days

Saturday

Monday

Tuesday

Wednesday

Thursday

Friday

✓ Saturday

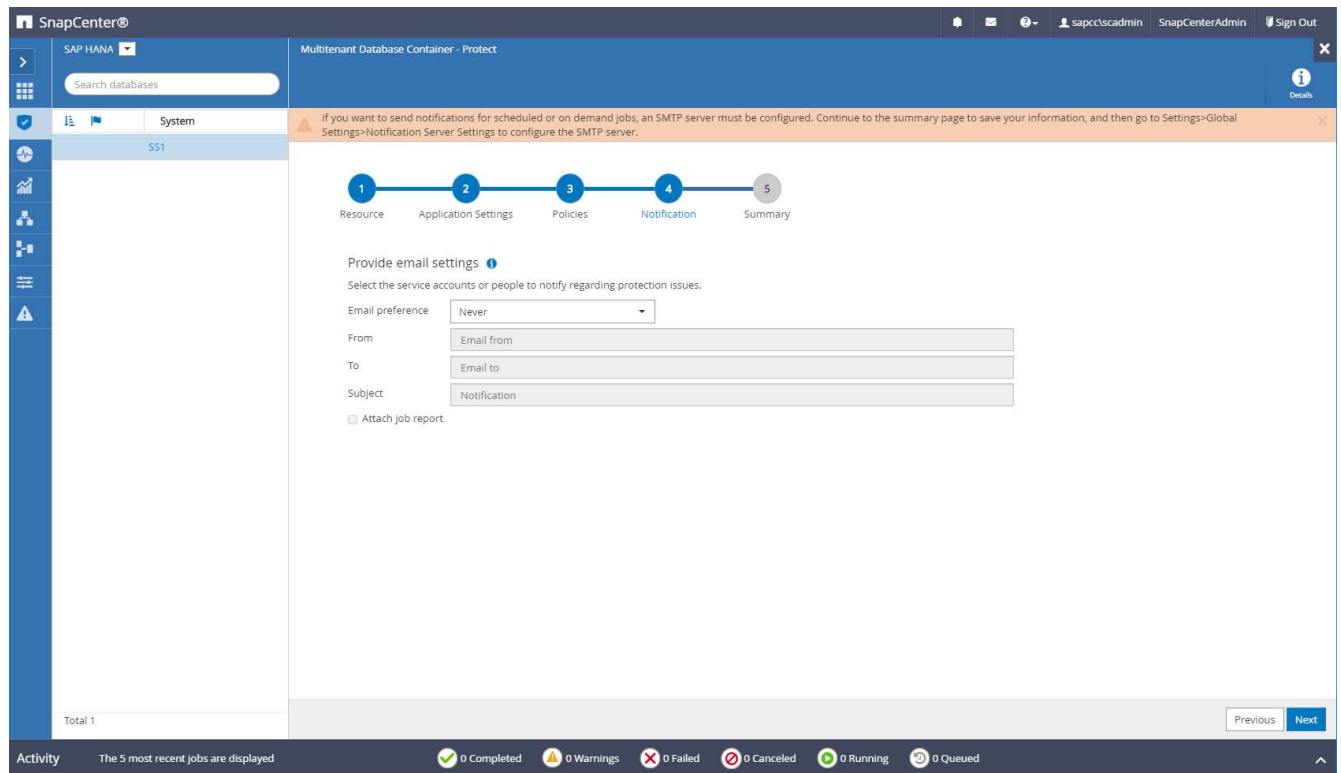
i

The schedules are triggered in the SnapCenter Server time zone.

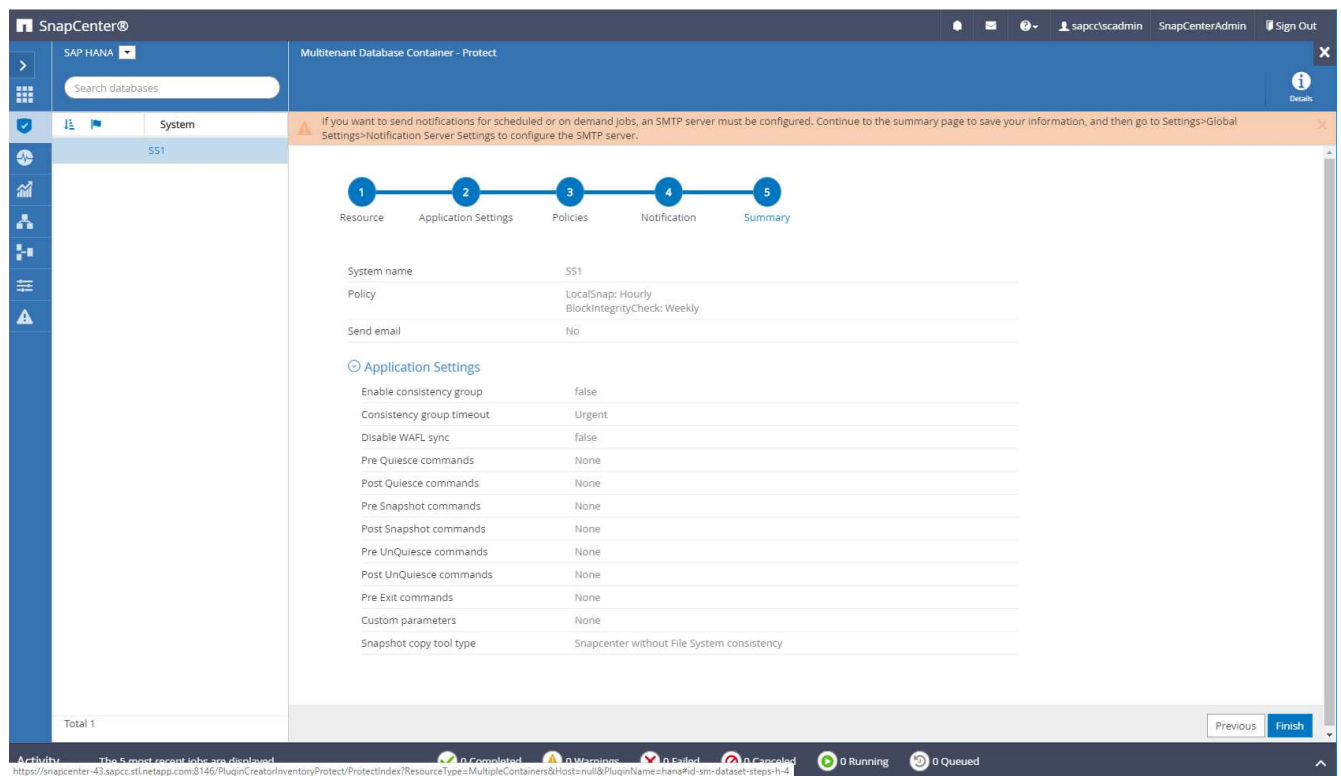
Cancel

Ok

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



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



10. Ahora los backups bajo demanda se pueden crear en la página Topology. Los backups programados se ejecutan según la configuración.

System	System ID (SID)	Tenant Database	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS1	SS1	SS1	hana-1.sapcc.sti.netapp.com		BlockIntegrityCheck LocalSnap LocalSnapAndSnapVault	11/19/2019 6:30:54 AM	Backup succeeded

Total 1

Activity: The 5 most recent jobs are displayed. 2 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

Pasos de configuración adicionales para entornos SAN Fibre Channel

En función de la versión de HANA y la puesta en marcha del complemento HANA, se requieren pasos adicionales de configuración para entornos en los que los sistemas SAP HANA utilizan Fibre Channel y el sistema de archivos XFS.



Estos pasos de configuración adicionales solo son necesarios para recursos HANA, que se configuran manualmente en SnapCenter. También es necesario para las versiones de HANA 1.0 y las versiones de HANA 2.0 hasta SPS2.

Cuando SnapCenter activa un punto de guardado de backup de HANA en SAP HANA, SAP HANA escribe los archivos ID de snapshot para cada cliente y servicio de base de datos como último paso (por ejemplo, /hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1). Estos archivos forman parte del volumen de datos del almacenamiento y, por lo tanto, forman parte de la copia snapshot de almacenamiento. Este archivo es obligatorio cuando se realiza una recuperación en una situación en la que se restaura el backup. Debido al almacenamiento en caché de metadatos con el sistema de archivos XFS en el host Linux, el archivo no es visible inmediatamente en la capa de almacenamiento. La configuración XFS estándar para el almacenamiento en caché de metadatos es de 30 segundos.



Con HANA 2.0 SPS3, SAP cambió la operación de escritura de estos archivos de ID de Snapshot a de forma síncrona para que el almacenamiento en caché de metadatos no surja ningún problema.



Con SnapCenter 4.3, si el plugin de HANA se implementa en el host de base de datos, el plugin de Linux ejecuta una operación de vaciado de sistema de archivos en el host antes de activar la Snapshot de almacenamiento. En este caso, el almacenamiento en caché de metadatos no es un problema.

En SnapCenter, debe configurar un `postquiesce` Comando que espera hasta que la caché de metadatos

XFS se vacía en la capa de disco.

La configuración real del almacenamiento en caché de metadatos se puede comprobar usando el siguiente comando:

```
stlrx300s8-2:/ # sysctl -A | grep xfssyncd_centisecs
fs.xfs.xfssyncd_centisecs = 3000
```

NetApp recomienda utilizar un tiempo de espera que duplique el valor del `fs.xfs.xfssyncd_centisecs` parámetro. Dado que el valor predeterminado es 30 segundos, establezca el comando `sleep` en 60 segundos.

Si el servidor SnapCenter se utiliza como host de complemento HANA central, se puede utilizar un archivo de lotes. El archivo por lotes debe tener el siguiente contenido:

```
@echo off
waitfor AnyThing /t 60 2>NUL
Exit /b 0
```

El archivo por lotes se puede guardar, por ejemplo, como `C:\Program Files\NetApp\Wait60Sec.bat`. En la configuración de protección de recursos, el archivo por lotes debe agregarse como comando Post Quiesce.

Si un host de Linux separado se utiliza como host del plugin de HANA central, debe configurar el comando `/bin/sleep 60` Como el comando Post Quiesce en la interfaz de usuario de SnapCenter.

La siguiente figura muestra el comando Post Quiesce dentro de la pantalla de configuración de protección de recursos.

The screenshot displays the SnapCenter web interface for configuring resource protection. The left sidebar shows the navigation menu with 'System' selected. The main content area is titled 'Multitenant Database Container - Protect' and features a progress bar with five steps: 1. Resource, 2. Application Settings, 3. Policies, 4. Notification, and 5. Summary. The 'Scripts' section is expanded, showing three categories of commands: 'Enter commands to be executed before and after placing the application in consistent operational state', 'Enter commands to be executed before and after creating Snapshot copies', and 'Enter commands to be executed before and after returning the application to normal operational state'. The 'Post Quiesce' field under the first category is highlighted with a red box. The bottom status bar indicates 'Activity' and shows 'The 5 most recent jobs are displayed' with a summary of job statuses: 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, and 0 Queued.

Configuración específica de recursos de SnapCenter para backups de volúmenes sin datos

El backup de volúmenes que no forman parte de datos es una parte integrada 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.

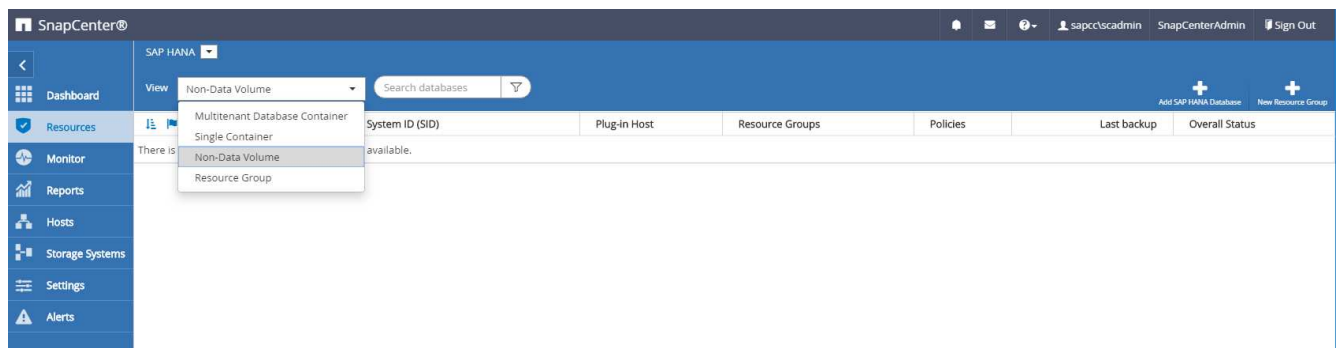
Para la recuperación tras situaciones en las que se deben restaurar otros archivos distintos de datos, NetApp recomienda desarrollar una estrategia de backup adicional para los volúmenes que no sean de datos a fin de aumentar el backup de base de datos SAP HANA. En función de los requisitos específicos, 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.

Configuración de los recursos que no son de volúmenes de datos

En este ejemplo, queremos proteger los volúmenes que no son datos de la base de datos SAP HANA SS1.

1. En la pestaña Resource, seleccione Non-Data-Volume y 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 desea usar para el recurso y, a continuación, haga clic en Next.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

Resource Type

Non-data Volumes

Resource Name

SS1-Shared-Volume

Associated SID

SS1

Plug-in Host

hana-1.sapcc.stl.netapp.com

Previous

Next

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

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Storage Footprint Details

Add Storage Footprint

Storage System

hana-primary.sapcc.stl.netapp.com

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name

SS1_shared

SM1_data_mnt00001

SM1_log_mnt00001

SM1_shared

SS1_data_mnt00001

SS1_log_mnt00001

SS1_shared

SS1_data_mnt00001

LUNs or Qtrees

Default is 'None' or type to find

+

×

Save

Previous

Next

- En el paso de resumen, haga clic en Finish para guardar la configuración.
- Repita estos pasos para todos los volúmenes sin datos requeridos.
- Continúe con la configuración de protección del nuevo recurso.



La protección de datos para recursos de un volumen sin datos es idéntica al flujo de trabajo de los recursos de base de datos SAP HANA y puede definirse en un nivel de recurso individual.

En la siguiente figura, se muestra la lista de los recursos configurados de volúmenes sin datos.

SnapCenter®							
SAP HANA							
View Non-Data Volume Search databases							
<div> <div>Resources</div> <div>Monitor</div> <div>Reports</div> <div>Hosts</div> <div>Storage Systems</div> <div>Settings</div> <div>Alerts</div> </div>							
Name	Associated System ID (SID)	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status	
SS1-Shared-Volume	SS1	hana-1.sapcc.stl.netapp.com		LocalSnap		Backup not run	

Grupos de recursos

Los grupos de recursos son una forma cómoda de definir la protección de varios recursos que requieren las mismas políticas de protección y programaciones. Los recursos individuales que forman parte de un grupo de recursos aún pueden protegerse en un nivel individual.

Los grupos de recursos proporcionan las siguientes funciones:

- Puede añadir uno o varios recursos a un grupo de recursos. Todos los recursos deben pertenecer al mismo plugin de SnapCenter.
- La protección puede definirse en un nivel de grupo de recursos. Todos los recursos del grupo de recursos utilizan la misma política y programación cuando se protegen.
- Todos los backups del repositorio de SnapCenter y las copias de Snapshot de almacenamiento tienen el mismo nombre definido en la protección de recursos.
- Las operaciones de restauración se aplican en un solo nivel de recursos, no como parte de un grupo de recursos.
- Cuando se usa SnapCenter para eliminar el backup de un recurso creado en el nivel de un grupo de recursos, este backup se elimina para todos los recursos del grupo de recursos. Eliminar el backup incluye eliminar el backup del repositorio de SnapCenter y eliminar las copias de Snapshot de almacenamiento.
- El principal caso práctico para los grupos de recursos es cuando un cliente desea utilizar backups creados con SnapCenter para la clonación de sistemas con SAP Landscape Management. Esto se describe en la siguiente sección.

Uso de SnapCenter junto con la gestión de entornos SAP

Con SAP Landscape Management (SAP Lama), los clientes pueden gestionar entornos de sistemas SAP complejos en centros de datos locales y en sistemas que se ejecutan en el cloud. SAP Lama, junto con Storage Services Connector (SSC) de NetApp, puede ejecutar operaciones de almacenamiento como el clonado y la replicación para casos de uso de clonado, copia y actualización del sistema SAP mediante la tecnología Snapshot y FlexClone. Esto le permite automatizar por completo una copia del sistema SAP basada en la tecnología de clonación de almacenamiento y, al mismo tiempo, incluir el postprocesamiento SAP necesario. Para obtener más información sobre las soluciones de NetApp para SAP Lama, consulte ["TR-4018: Integración de los sistemas ONTAP de NetApp con SAP Landscape Management"](#).

SSC de NetApp y SAP Lama pueden crear copias de Snapshot bajo demanda directamente con SSC de NetApp, pero también pueden usar las copias de Snapshot que se han creado mediante SnapCenter. Para utilizar los backups de SnapCenter como base de operaciones de clonado del sistema y copia con SAP Lama, debe cumplir los siguientes requisitos previos:

- SAP Lama requiere que todos los volúmenes estén incluidos en el backup; esto incluye datos de SAP HANA, registros y volúmenes compartidos.
- Todos los nombres de las copias Snapshot de almacenamiento deben ser idénticos.
- Los nombres de las instantáneas de almacenamiento deben comenzar por VCM.



En las operaciones de backup normales, NetApp no recomienda incluir el volumen de registros. Si restaura el volumen de registro desde un backup, sobrescribe los últimos registros de recuperación activos y evita que la recuperación de la base de datos se recupere en el último estado reciente.

Los grupos de recursos SnapCenter satisfacen todos estos requisitos. SnapCenter configura tres recursos: Un recurso cada uno para el volumen de datos, el volumen de registro y el volumen compartido. Los recursos se

colocan en un grupo de recursos y se definen entonces la protección en el nivel del grupo de recursos. En la protección del grupo de recursos, el nombre de Snapshot personalizado debe definirse con VCM al principio.

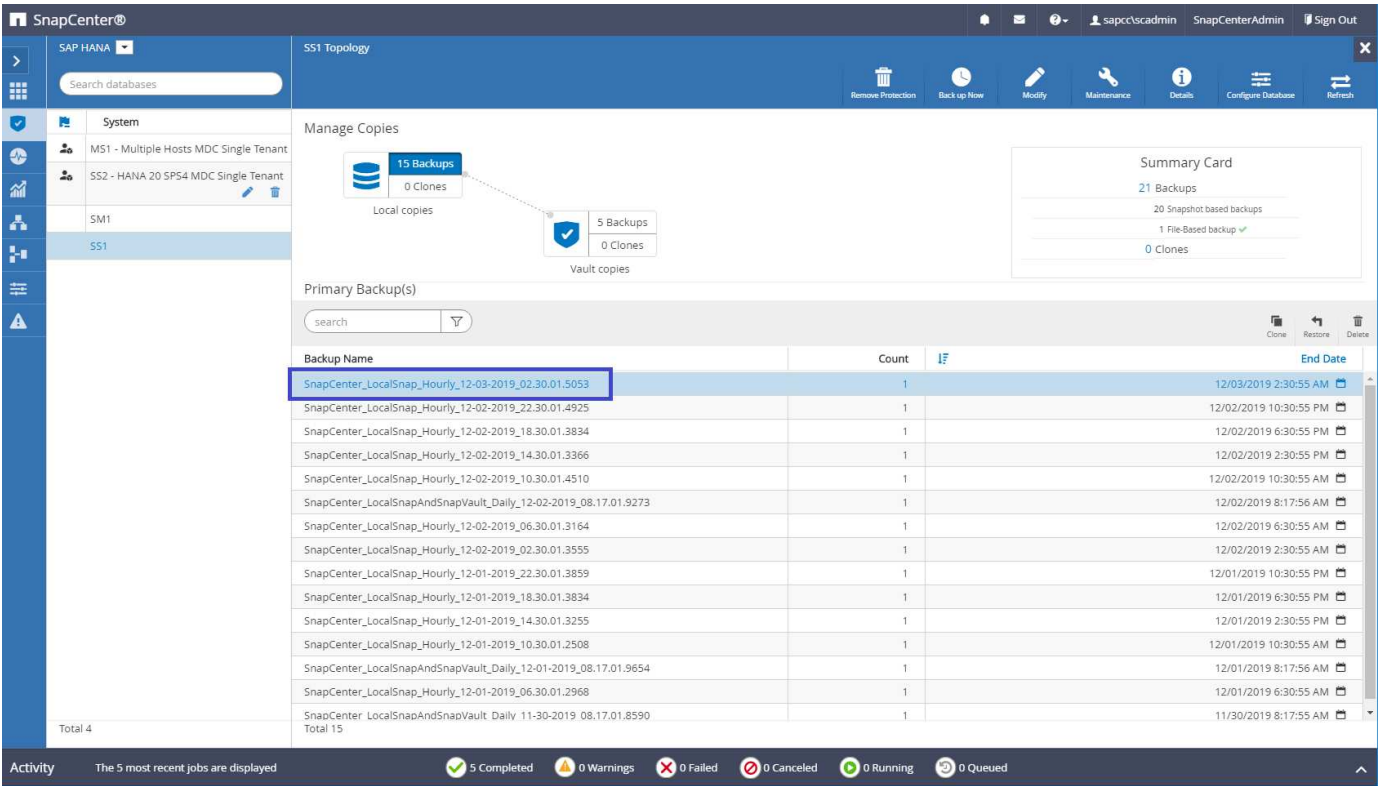
Backups de bases de datos

En SnapCenter, los backups de bases de datos normalmente se ejecutan mediante las programaciones definidas en la configuración de protección de recursos de cada base de datos HANA.

El backup de bases de datos bajo demanda se puede realizar mediante la interfaz gráfica de usuario de SnapCenter, una línea de comandos de PowerShell o las API DE REST.

Identificación de backups de SnapCenter en SAP HANA Studio

La topología de recursos de SnapCenter muestra una lista de los backups creados mediante SnapCenter. En la siguiente figura, se muestran los backups disponibles en el almacenamiento principal y se resalta el backup más reciente.



Cuando se realiza un backup mediante copias de Snapshot de almacenamiento para un sistema SAP HANA MDC, se crea una copia de Snapshot del volumen de datos. Este volumen de datos contiene los datos de la base de datos del sistema, así como los de todas las bases de datos de tenant. Para reflejar esta arquitectura física, SAP HANA lleva a cabo internamente un backup combinado de la base de datos del sistema, así como de todas las bases de datos de tenant siempre que SnapCenter activa un backup de snapshot. Esto da como resultado varias entradas de backup independientes en el catálogo de backup de SAP HANA: Una para la base de datos del sistema y una para cada base de datos de tenant.



Para los sistemas de contenedor único de SAP HANA, el volumen de base de datos solo contiene la única base de datos, y solo hay una entrada en el catálogo de backup de SAP HANA.

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 captura de pantalla de la base de datos del sistema y en la captura de pantalla posterior a la de la base de datos de arrendatarios SS1. Ambas figuras destacan el nombre de la copia de seguridad de SnapCenter almacenada en el campo de comentario y EBID.



El lanzamiento de HANA 2.0 SPS4 (revisiones 40 y 41) muestra siempre un tamaño de backup cero para backups basados en Snapshot. Esto se ha solucionado con la revisión 42. Para obtener más información, consulte la nota de SAP ["https://launchpad.support.sap.com/#/notes/2795010"](https://launchpad.support.sap.com/#/notes/2795010).

The screenshot shows the SAP HANA Studio interface. The main window displays the 'Backup Catalog' for the database 'SYSTEMDB'. The 'Backup Details' panel on the right shows the following information:

- ID: 1575369024442
- Status: Successful
- Backup Type: Data Backup
- Destination Type: Snapshot
- Started: Dec 3, 2019 2:30:24 AM (America/Los Angeles)
- Finished: Dec 3, 2019 2:30:38 AM (America/Los Angeles)
- Duration: 00h 00m 14s
- Size: 0 B
- Throughput: n.a.
- System ID:
- Comment: SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053
- Additional Information: <ok>
- Location: /hana/data/SS1/mnt00001/

Below the 'Backup Details' panel, there is a table showing the backup details:

Host	Service	Name	EBID
hana-1	nameserver	hdb00001	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

The screenshot displays the SAP HANA Studio interface. The main window shows the 'Backup SYSTEMDB@SS1 (SYSTEM) SS1 - HANA20 SPS4 MDC Single Tenant' configuration. The 'Backup Catalog' tab is active, showing a list of backups. The 'Backup Details' panel on the right provides information about the selected backup, including its ID, status, type, and destination. A comment field is highlighted with a blue box, containing the text 'SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053'. Below this, a table lists the backup details for the selected backup.

Host	Service	Name	EBID
hana-1	indexserver	hdb:00003...	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053
hana-1	xsengine	hdb:00002...	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053



SnapCenter solo conoce sus propios backups. Los backups adicionales creados, por ejemplo, con SAP HANA Studio, son visibles en el catálogo SAP HANA pero no en SnapCenter.

Identificación de backups de SnapCenter en los sistemas de almacenamiento

Para ver los backups en la capa de almacenamiento, use OnCommand System Manager de NetApp y seleccione el volumen de la base de datos en la vista SVM—Volume. La ficha inferior copias Snapshot muestra las copias Snapshot del volumen. La siguiente captura de pantalla muestra las copias de seguridad disponibles para el volumen de base de datos SS1_data_mnt00001 en el almacenamiento primario. El backup resaltado es el backup que se muestra en SnapCenter y SAP HANA Studio en las imágenes anteriores y tiene la misma convención de nomenclatura.

Volume: SS1_data_mnt00001

Overview Snapshots Copies Data Protection Storage Efficiency Performance

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	Dec/01/2019 11:03:44	106.27 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_06.30.01.3164	Dec/02/2019 09:16:42	74.76 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	Dec/02/2019 11:03:43	17.21 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_10.30.01.4510	Dec/02/2019 13:16:42	39.11 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_14.30.01.3366	Dec/02/2019 17:16:42	87.53 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3834	Dec/02/2019 21:16:41	95.67 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	Dec/03/2019 01:16:41	29.86 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	Dec/03/2019 05:16:41	43.81 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_06.30.01.4088	Dec/03/2019 09:16:40	49.46 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	Dec/03/2019 11:03:41	77.14 MB	snapmirror
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_10.30.01.4554	Dec/03/2019 13:16:40	42.12 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_14.30.01.3902	Dec/03/2019 17:16:40	57.42 MB	None

La siguiente captura de pantalla muestra las copias de seguridad disponibles para el volumen de destino de replicación hana_SA1_data_mnt00001_dest en el sistema de almacenamiento secundario.

Volume: SS1_data_mnt00001_dest

Overview Snapshots Copies Data Protection Storage Efficiency Performance

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_11-29-2019_08.17.01.8567	Nov/29/2019 11:03:48	113.34 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	Nov/30/2019 11:03:46	87.69 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	Dec/01/2019 11:03:44	108.67 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	Dec/02/2019 11:03:43	102 MB	None
Busy	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	Dec/03/2019 11:03:41	176 KB	busy

Displaying 1 - 5

Backup de bases de datos bajo demanda en el almacenamiento primario

1. En la vista de recursos, seleccione el recurso y haga doble clic en la línea para cambiar a la vista de topología.

La vista de topología de recursos ofrece información general de todos los backups disponibles que se crearon con SnapCenter. En la área 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).

SAP Center SnapCenter

SS1 Topology

Manage Copies

Local copies: 15 Backups, 0 Clones

Vault copies: 5 Backups, 0 Clones

Summary Card

- 21 Backups
- 20 Snapshot based backups
- 1 File-Based backup ✓
- 0 Clones

Primary Backup(s)

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	1	12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	1	12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3834	1	12/02/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_14.30.01.3366	1	12/02/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_10.30.01.4510	1	12/02/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1	12/02/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_06.30.01.3164	1	12/02/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_02.30.01.3555	1	12/02/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_22.30.01.3859	1	12/01/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_18.30.01.3834	1	12/01/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_14.30.01.3255	1	12/01/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_10.30.01.2508	1	12/01/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	1	12/01/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_06.30.01.2968	1	12/01/2019 6:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	1	11/30/2019 8:17:55 AM

Activity: The 5 most recent jobs are displayed. 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

- En la fila superior, seleccione el icono Back up Now para iniciar un backup bajo demanda. En la lista desplegable, seleccione la política de backup LocalSnap Y, a continuación, haga clic en Backup para iniciar el backup bajo demanda.

Backup

Create a backup for the selected resource

Resource Name

SS1

Policy

LocalSnap

Cancel

Backup

Esto inicia el trabajo de copia de seguridad. Se muestra un registro de los cinco trabajos anteriores en el área actividad debajo de la vista de topología. 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 ["Configuración de protección de recursos"](#).



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

Backup Name	Count	End Date
SnapCenter_LocalSnap_12-03-2019_06:37:50.1491	1	12/03/2019 6:38:44 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_06:30:01.4088	1	12/03/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053	1	12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22:30:01.4925	1	12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18:30:01.3834	1	12/02/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_14:30:01.3366	1	12/02/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_10:30:01.4510	1	12/02/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08:17:01.9273	1	12/02/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_06:30:01.3164	1	12/02/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_02:30:01.3555	1	12/02/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_22:30:01.3859	1	12/01/2019 10:30:55 PM

Activity	Job Description	Status
2 minutes ago	Backup of Resource Group 'hana-1_sapcc_stl_netapp_com_hana_MDC_SS1' with policy 'LocalSnap'	Completed
10 minutes ago	Backup of Resource Group 'hana-2_sapcc_stl_netapp_com_hana_MDC_SS1' with policy 'LocalSnap'	Completed
12 minutes ago	Backup of Resource Group 'hana-2_sapcc_stl_netapp_com_hana_MDC_SM1' with policy 'LocalSnap'	Completed
35 minutes ago	Backup of Resource Group 'SnapCenter-43_sapcc_stl_netapp_com_hana_MDC_SS2' with policy 'LocalSnap'	Completed
3 hours ago	Backup of Resource Group 'SnapCenter-43_sapcc_stl_netapp_com_hana_MDC_MS1' with policy 'LocalSnap'	Completed

- 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.

Job Details

Backup of Resource Group 'hana-1_sapcc_stl_netapp_com_hana_MDC_SS1' with policy 'LocalSnap'

▼ Backup of Resource Group 'hana-1_sapcc_stl_netapp_com_hana_MDC_SS1' with policy 'LocalSnap'

▼ hana-1.sapcc.stl.netapp.com

▼ Backup

▶ Validate Dataset Parameters

▶ Validate Plugin Parameters

▶ Complete Application Discovery

▶ Initialize Filesystem Plugin

▶ Discover Filesystem Resources

▶ Validate Retention Settings

▶ Quiesce Application

▶ Quiesce Filesystem

▶ Create Snapshot

▶ UnQuiesce Filesystem

▶ UnQuiesce Application

▶ Get Snapshot Details

▶ Get Filesystem Meta Data

▶ Finalize Filesystem Plugin

▶ Collect Autosupport data

▶ Register Backup and Apply Retention

▶ Register Snapshot attributes

Task Name: Backup Start Time: 12/03/2019 6:37:51 AM End Time: 12/03/2019 6:39:03 AM

View Logs

Cancel Job

Close

- En SAP HANA Studio, el nuevo backup se puede ver en el catálogo de backup. El mismo nombre de backup en SnapCenter también se utiliza en el campo comment y EBID del catálogo de backups.

Backups de bases de datos bajo demanda con replicación SnapVault

- En la vista de recursos, seleccione el recurso y haga doble clic en la línea para cambiar a la vista de topología.
- En la fila superior, seleccione el icono Backup Now para iniciar un backup bajo demanda. En la lista desplegable, seleccione la política de backup LocalSnapAndSnapVault, A continuación, haga clic en copia de seguridad para iniciar la copia de seguridad bajo demanda.

77

Backup

×

Create a backup for the selected resource

Resource Name

SS1

Policy

LocalSnapAndSnapVault

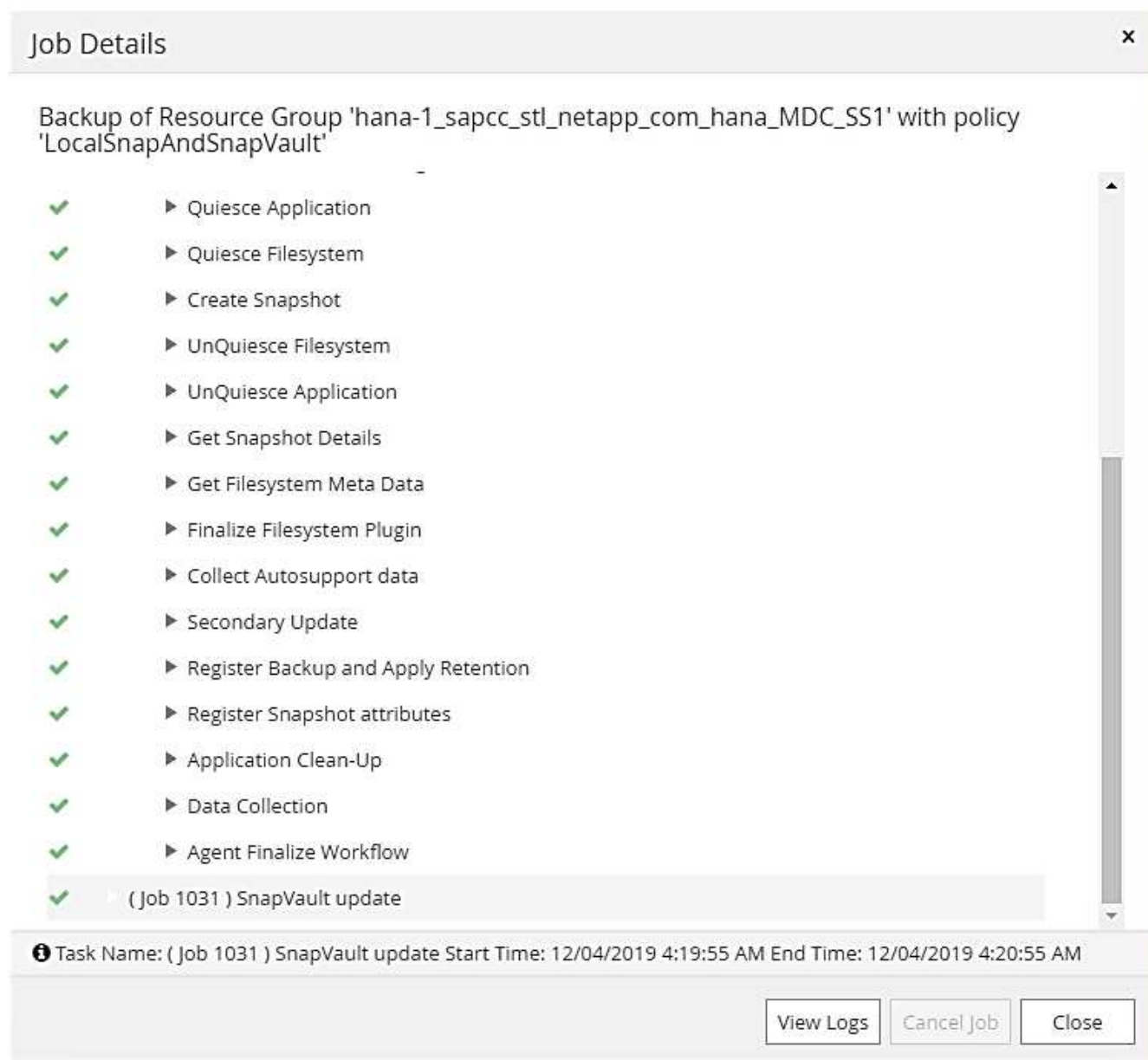
▼

i

Cancel

Backup

3. Los detalles del trabajo se muestran al hacer clic en la línea de actividad del trabajo en el área actividad.



4. 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 ["Configuración de protección de recursos"](#).



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

Manage Copies

Local copies: 16 Backups, 0 Clones

Vault copies: 6 Backups, 0 Clones

Primary Backup(s)

Backup Name	Count	IF	End Date
SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527	1		12/04/2019 4:19:52 AM
SnapCenter_LocalSnap_Hourly_12-04-2019_02.30.01.4636	1		12/04/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_22.30.01.4836	1		12/03/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-03-2019_18.30.01.4818	1		12/03/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-03-2019_14.30.01.3902	1		12/03/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-03-2019_10.30.01.4554	1		12/03/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	1		12/03/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_06.30.01.4088	1		12/03/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	1		12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	1		12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3934	1		12/02/2019 6:30:55 PM
Total 16			

Secondary Vault Backup(s)

Backup Name	Count	IF	End Date
SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527	1		12/04/2019 4:19:52 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	1		12/03/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1		12/02/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	1		12/01/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	1		11/30/2019 8:17:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-29-2019_08.17.01.8567	1		11/29/2019 8:17:56 AM
Total 6			

Summary Card

- 23 Backups
- 22 Snapshot based backups
- 1 File-Based backup ✓
- 0 Clones

Activity The 5 most recent jobs are displayed

5 Completed 0 Warnings 0 Failed 0 Canceled 0 Running 0 Queued

- Al seleccionar copias de almacén, se muestran los backups en el almacenamiento secundario. El nombre del backup replicado es idéntico al nombre de la copia de seguridad en el almacenamiento principal.

Manage Copies

Local copies: 16 Backups, 0 Clones

Vault copies: 6 Backups, 0 Clones

Secondary Vault Backup(s)

Backup Name	Count	IF	End Date
SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527	1		12/04/2019 4:19:52 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	1		12/03/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1		12/02/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	1		12/01/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	1		11/30/2019 8:17:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-29-2019_08.17.01.8567	1		11/29/2019 8:17:56 AM
Total 6			

Summary Card

- 23 Backups
- 22 Snapshot based backups
- 1 File-Based backup ✓
- 0 Clones

Activity The 5 most recent jobs are displayed

5 Completed 0 Warnings 0 Failed 0 Canceled 0 Running 0 Queued

- En SAP HANA Studio, el nuevo backup se puede ver en el catálogo de backup. El mismo nombre de backup en SnapCenter también se utiliza en el campo comment y EBID del catálogo de backups.

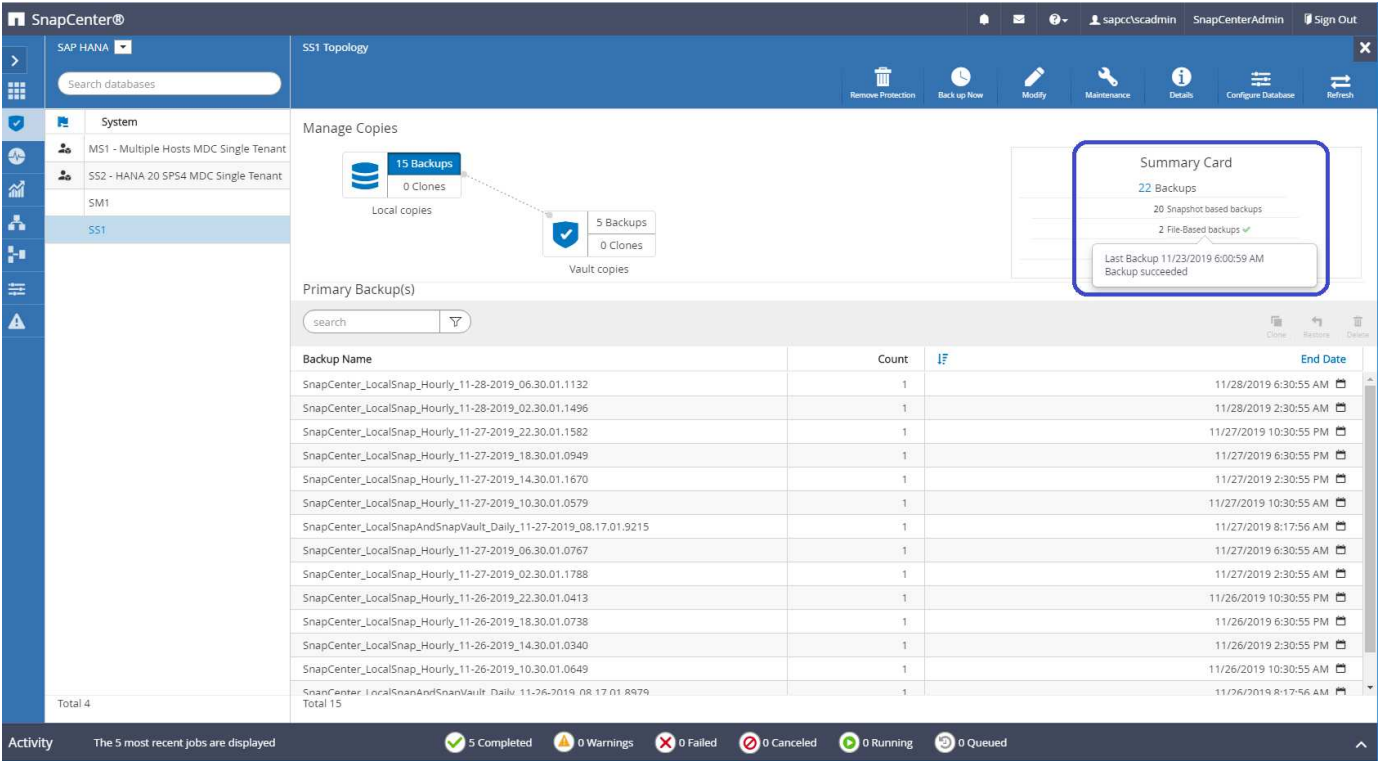
Comprobación de integridad de bloques

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. SnapCenter permite ejecutar una comprobación de integridad de bloque mediante una política en la que se selecciona el backup basado en archivos como tipo

de backup.

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.

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.



No se puede eliminar un backup de comprobación de integridad del bloque con la interfaz de usuario de SnapCenter, pero se puede eliminar mediante comandos de PowerShell.

```

PS C:\Users\scadmin> Get-SmBackupReport -Resource SS1
SmBackupId           : 9
SmJobId              : 42
StartDateTime        : 11/19/2019 8:26:32 AM
EndDateTime          : 11/19/2019 8:27:33 AM
Duration             : 00:01:00.7652030
CreatedDateTime       : 11/19/2019 8:27:24 AM
Status               : Completed
ProtectionGroupName  : hana-1_sapcc_stl_netapp_com_hana_MDC_SS1
SmProtectionGroupId  : 1
PolicyName           : BlockIntegrityCheck
SmPolicyId           : 5
BackupName           : SnapCenter_BlockIntegrityCheck_11-19-
2019_08.26.33.2913
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError            :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : hana
JobTypeId            : 0
JobHost              :

PS C:\Users\scadmin> Remove-SmBackup -BackupIds 9

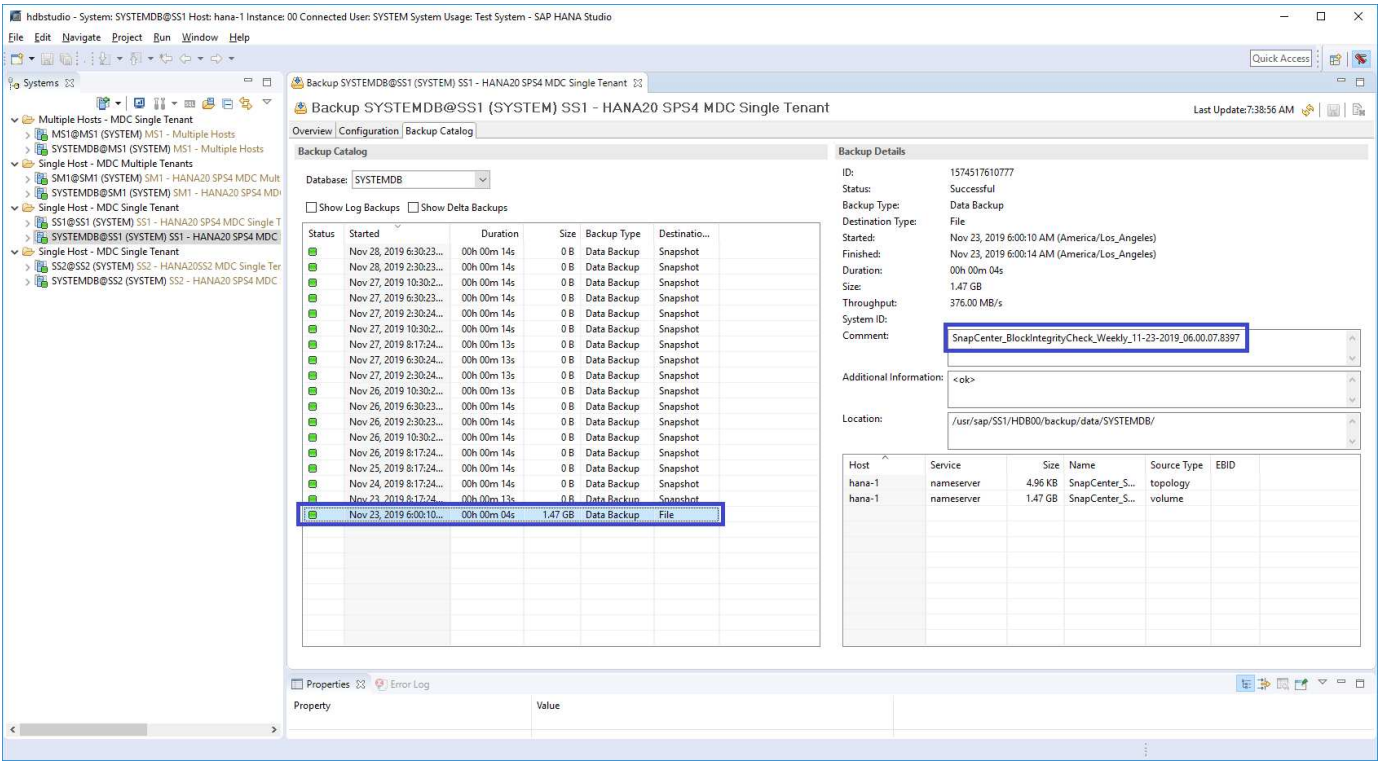
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): y

BackupResult : {}
Result       : SMCoreContracts.SMResult
TotalCount   : 0
DisplayCount : 0
Context      :
Job          : SMCoreContracts.SmJob

PS C:\Users\scadmin>

```


El catálogo de backup de SAP HANA muestra entradas tanto para las bases de datos del sistema como para las de tenant. En la siguiente figura se muestra una comprobación de integridad de bloques de SnapCenter en el catálogo de backup de la base de datos del sistema.



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

```
hana-1:/usr/sap/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 1710840
drwxr-xr-- 2 ssladm sapsys      4096 Nov 28 10:25 .
drwxr-xr-- 4 ssladm sapsys      4096 Nov 19 05:11 ..
-rw-r----- 1 ssladm sapsys    155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ssladm sapsys    83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ssladm sapsys 1660952576 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_3_1
SYSTEMDB:
total 1546340
drwxr-xr-- 2 ssladm sapsys      4096 Nov 28 10:24 .
drwxr-xr-- 4 ssladm sapsys      4096 Nov 19 05:11 ..
-rw-r----- 1 ssladm sapsys    159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ssladm sapsys 1577066496 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_1_1
```

Restauración y recuperación

Las siguientes secciones describen los flujos de trabajo de restauración y recuperación de tres situaciones diferentes y configuraciones de ejemplo.

- Restauración y recuperación automatizadas:
 - Sistema HANA detectado automáticamente SS1
 - Host único de SAP HANA, sistema de tenant único de MDC mediante NFS
- Restauración y recuperación de un solo inquilino:
 - Sistema HANA detectado automáticamente SM1
 - Un solo host de SAP HANA, MDC.sistema de varios inquilinos mediante NFS
- Restauración con recuperación manual:
 - Sistema HANA configurado manualmente SS2
 - Un solo host de SAP HANA, MDC.sistema de varios inquilinos mediante NFS

En las siguientes secciones, se destacan las diferencias entre un solo host de SAP HANA y varios hosts y los sistemas HANA conectados a SAN Fibre Channel.

Los ejemplos muestran SAP HANA Studio como una herramienta para ejecutar la recuperación manual.

También puede usar declaraciones SQL de SAP HANA Cockpit o HANA.

Restauración y recuperación automatizadas

Con SnapCenter 4.3, las operaciones de restauración y recuperación automatizadas son compatibles con los sistemas de un solo inquilino de MDC.o contenedores únicos de HANA que SnapCenter ha detectado automáticamente.

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. El backup se puede seleccionar de entre las siguientes opciones de almacenamiento:
 - Almacenamiento primario
 - Almacenamiento de backup externo (destino SnapVault)
2. Seleccione el tipo de restauración. Seleccione completar restauración con reversión de volumen o sin reversión de volumen.



La opción Volume Revert solo está disponible para las operaciones de restauración del almacenamiento primario y si la base de datos HANA utiliza NFS como protocolo de almacenamiento.

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 y el protocolo de almacenamiento utilizado, se ejecutan diferentes operaciones.

- Si se seleccionan NFS y Volume Revert, entonces SnapCenter desmonta el volumen, restaura el volumen mediante SnapRestore basado en volúmenes en la capa de almacenamiento y monta el volumen.
- Si se selecciona NFS y no se selecciona Volume Revert, SnapCenter restaura todos los archivos mediante las operaciones de SnapRestore de archivos individuales en la capa de almacenamiento.
- Si está seleccionada LA opción SAN de Fibre Channel, SnapCenter desmonta los LUN, restaura los LUN mediante las operaciones de SnapRestore de archivo único en la capa de almacenamiento y detecta y monta los LUN.

3. Recupera la base de datos:

- Recupera la base de datos del sistema.
- Recupera la base de datos de tenant.

O bien, en los sistemas de contenedor único de HANA, la recuperación se ejecuta en un solo paso:

- Inicia la base de datos HANA.



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

En esta sección se proporcionan los pasos para la operación de restauración y recuperación automatizada del sistema HANA detectado automáticamente SS1 (host único de SAP HANA, sistema de un solo inquilino de MDC mediante NFS).

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



Puede seleccionar la opción de restauración desde el almacenamiento de backup principal o desde un almacenamiento de backup externo.

The screenshot displays the SnapCenter web interface for managing SAP HANA backups. The left sidebar contains navigation icons for System, Users, Backups, Reports, and Alerts. The top navigation bar shows the user 'sapcc/scadmin' and various action buttons like 'Remove Protection', 'Back up Now', 'Modify', 'Maintenance', 'Details', 'Configure Database', and 'Refresh'. The main content area is titled 'Manage Copies' and shows a hierarchy of backups: '16 Backups' (0 Clones) under 'Local copies' and '6 Backups' (0 Clones) under 'Vault copies'. A 'Summary Card' on the right indicates '23 Backups', with '22 Snapshot based backups' and '1 File-based backup'. Below this, the 'Primary Backup(s)' section features a search bar and a table of backup entries.

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_12-05-2019_22:30:01.5385	1	12/05/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_18:30:01.5244	1	12/05/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_14:30:01.6022	1	12/05/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_10:30:01.5450	1	12/05/2019 10:30:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08:17:02.0191	1	12/05/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_06:30:01.5487	1	12/05/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_02:30:01.5470	1	12/05/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-04-2019_22:30:01.5182	1	12/04/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_18:30:01.5249	1	12/04/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_14:30:01.5069	1	12/04/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_10:30:01.5200	1	12/04/2019 10:30:55 AM
Total 16		

The bottom status bar shows the activity of the restore job: '5 Completed', '0 Warnings', '0 Failed', '0 Canceled', '0 Running', and '0 Queued'.

SAP HANA

Search databases

SS1 Topology

Remove Protection

Back up Now

Modify

Maintenance

Details

Configure Database

Refresh

System

MS1 - Multiple Hosts MDC Single Tenant

SS2 - HANA 20 SP54 MDC Single Tenant

SM1

SS1

Manage Copies

16 Backups

0 Clones

Local copies

5 Backups

0 Clones

Vault copies

Summary Card

22 Backups

21 Snapshot based backups

1 File-Based backup

0 Clones

Secondary Vault Backup(s)

search

Restore

Clone

Restore

Backup Name	Count	IF	End Date
SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08.17.02.0191	1		12/05/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-04-2019_08.17.01.9976	1		12/04/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527	1		12/04/2019 4:19:52 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	1		12/03/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1		12/02/2019 8:17:56 AM

Total 4

Total 5

5 Completed

0 Warnings

0 Failed

0 Canceled

0 Running

0 Queued

2. Seleccione el ámbito y el tipo de restauración.

Las tres capturas de pantalla siguientes muestran las opciones de restauración para restaurar desde el principal con NFS, restauración desde el secundario con NFS y restauración desde el principal con San Fibre Channel.

Las opciones de tipo de restauración para restaurar desde el almacenamiento principal.



La opción Volume Revert solo está disponible para las operaciones de restauración desde el almacenamiento primario con NFS.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ⓘ

☒ Volume Revert

☐ Tenant Database

⚠ As part of Complete Resource restore, if a resource contains volumes as Storage Footprint, then the latest Snapshot copies on such volumes will be deleted permanently. Also, if there are other resources hosted on the same volumes, then it will result in data loss for such resources.

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

Las opciones de tipo de restauración para restaurar desde el almacenamiento de backup externo.

Restore from SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08.17.02.0191

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ⓘ

☐ Tenant Database

Choose archive location

hana-primary.sapcc.stf.netapp.com:SS1_data_mnt00001

hana-backup.sapcc.stf.netapp.com:SS1_data ▾

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

Las opciones de tipo de restauración para restaurar desde un almacenamiento principal con Fibre Channel SAN.

Restore from SnapCenter_LocalSnap_Hourly_12-16-2019_22.35.01.3065

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ⓘ
 ☐ Tenant Database

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous

Next

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.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☒ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☐ No recovery

Specify log backup locations

Add

/mnt/log-backup

Specify backup catalog location

/mnt/log-backup

Recovery options are applicable to both system database and tenant database.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

4. Introduzca los comandos prerestore opcionales.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run before performing a restore operation

Pre restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

5. Introduzca los comandos posteriores a la restauración opcionales.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run after performing a restore operation

Post restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

6. Introduzca la configuración de correo electrónico opcional.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Provide email settings ⓘ

Email preference

Never

From

Email from

To

Email to

Subject

Notification

☐ Attach Job Report

⚠

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

×

Previous

Next

7. Para iniciar la operación de restauración, haga clic en Finalizar.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup Name	SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385
Backup date	12/05/2019 10:30:55 PM
Restore scope	Complete Resource with Volume Revert
Recovery scope	Recover to most recent state
Log backup locations	/mnt/log-backup
Backup catalog location	/mnt/log-backup
Pre restore command	
Post restore command	
Send email	No

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish

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

Restore 'hana-1.sapcc.stl.netapp.com\hana\MDC\SS1'

- ✓ ▼ Restore 'hana-1.sapcc.stl.netapp.com\hana\MDC\SS1'
- ✓ ▼ hana-1.sapcc.stl.netapp.com
- ✓ ▼ Restore
- ✓ ▼ Validate Plugin Parameters
- ✓ ▼ Pre Restore Application
 - ▶ Stopping HANA instance
- ✓ ▼ Filesystem Pre Restore
 - ▶ Determining the restore mechanism
 - ▶ Deporting file systems and associated entities
- ✓ ▶ Restore Filesystem
- ✓ ▼ Filesystem Post Restore
 - ▶ Building file systems and associated entities
- ✓ ▼ Recover Application
- ✓ ▶ Recovering system database
- ✓ ▶ Checking HDB services status
- ✓ ▶ Recovering tenant database 'SS1'
- ✓ ▶ Starting HANA instance
- ✓ ▶ Clear Catalog on Server
- ✓ ▶ Application Clean-Up
- ✓ ▶ Data Collection
- ✓ ▶ Agent Finalize Workflow

i Task Name: Recover Application Start Time: 12/06/2019 7:26:11 AM End Time: 12/06/2019 7:28:46 AM

[View Logs](#)[Cancel Job](#)[Close](#)

Operaciones de restauración y recuperación de un solo inquilino

Con SnapCenter 4.3, las operaciones de restauración de un solo inquilino son compatibles con los sistemas MDC de HANA con un único inquilino o con varios inquilinos que SnapCenter ha detectado automáticamente.

Puede realizar una operación de restauración y recuperación de un solo usuario con los pasos siguientes:

1. Detener el inquilino a restaurar y recuperar.
2. Restaure el inquilino con SnapCenter.
 - Para una restauración desde el almacenamiento primario, SnapCenter ejecuta las siguientes operaciones:
 - **NFS.** almacenamiento de operaciones SnapRestore de archivo único para todos los archivos de la base de datos de arrendatario.
 - **SAN.** Clone y conecte el LUN al host de la base de datos, y copie todos los archivos de la base de datos del arrendatario.
 - Para una restauración desde el almacenamiento secundario, SnapCenter ejecuta las siguientes operaciones:
 - **NFS.** Operaciones de Restaurar SnapVault de almacenamiento para todos los archivos de la base de datos de arrendatario
 - **SAN.** Clone y conecte el LUN al host de la base de datos, y copie todos los archivos de la base de datos del arrendatario
3. Recupere el inquilino con HANA Studio, Cockpit o declaración SQL.

En esta sección se proporcionan los pasos para la operación de restauración y recuperación desde el almacenamiento principal del sistema HANA SM1 autodetectado (sistema SAP HANA single-host, MDC Multiple-tenant Using NFS). Desde la perspectiva de la entrada del usuario, los flujos de trabajo son idénticos para realizar una restauración desde sistema secundario o una restauración en una configuración DE SAN Fibre Channel.

1. Detenga la base de datos de tenant.

```
smladm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql SYSTEMDB=>
```

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

SnapCenter®

SAP HANA

Search databases

SM1 Topology

Manage Copies

12 Backups

0 Clones

Local copies

Summary Card

13 Backups

12 Snapshot based backups

1 File Based backup ✓

0 Clones

Primary Backup(s)

search

Backup Name	Count	IF	End Date
SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445	1		12/05/2019 10:28:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_18.28.01.1350	1		12/05/2019 6:28:56 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_14.28.01.2553	1		12/05/2019 2:28:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_10.28.01.2412	1		12/05/2019 10:28:55 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_06.28.01.1628	1		12/05/2019 6:28:55 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_02.28.01.1081	1		12/05/2019 2:28:55 AM
SnapCenter_LocalSnap_Hourly_12-04-2019_22.28.01.1106	1		12/04/2019 10:28:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_18.28.01.0470	1		12/04/2019 6:28:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_14.28.01.1969	1		12/04/2019 2:28:56 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_10.28.01.0201	1		12/04/2019 10:28:55 AM
SnapCenter_LocalSnap_Hourly_12-04-2019_06.28.01.0858	1		12/04/2019 6:28:55 AM
Total 4	Total 12		

5 Completed 0 Warnings 0 Failed 0 Canceled 0 Running 0 Queued

3. Seleccione el arrendatario que desea restaurar.



SnapCenter muestra una lista con todos los inquilinos que se incluyen en el backup seleccionado.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☐ Complete Resource

☒ Tenant Database

Select tenant database

Select tenant database

SM1

TENANT2

Stop the tenant before performing the tenant restore operation.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

SnapCenter 4.3 no admite la recuperación de un solo inquilino. No hay ninguna recuperación

preseleccionada y no se puede cambiar.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☐ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☒ No recovery

Recovery of an multitenant database container with multiple tenants is not supported

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

4. Introduzca los comandos prerestore opcionales.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run before performing a restore operation

Pre restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

5. Introduzca los comandos posteriores a la restauración opcionales.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run after performing a restore operation

Post restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous

Next

6. Introduzca la configuración de correo electrónico opcional.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Provide email settings ⓘ

Email preference

Never

From

Email from

To

Email to

Subject

Notification

☐ Attach Job Report

⚠

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

7. Para iniciar la operación de restauración, haga clic en Finalizar.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup Name	SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445
Backup date	12/05/2019 10:28:55 PM
Restore scope	Restore tenant database 'TENANT2'
Recovery scope	No recovery
Pre restore command	
Post restore command	
Send email	No

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish

SnapCenter ejecuta la operación de restauración. Este ejemplo muestra los detalles del trabajo de restauración.

Restore 'hana-2.sapcc.stl.netapp.com\hana\MDC\SM1'

✓ ▼ Restore 'hana-2.sapcc.stl.netapp.com\hana\MDC\SM1'

✓ ▼ hana-2.sapcc.stl.netapp.com

✓ ▼ Restore

✓ ▶ Validate Plugin Parameters

✓ ▶ Pre Restore Application

✓ ▶ Filesystem Pre Restore

✓ ▶ Restore Filesystem

✓ ▶ Filesystem Post Restore

✓ ▶ Recover Application

✓ ▶ Application Clean-Up

✓ ▶ Data Collection

✓ ▶ Agent Finalize Workflow

i Task Name: Restore Start Time: 12/06/2019 1:10:40 AM End Time: 12/06/2019 1:12:04 AM

View Logs

Cancel Job

Close



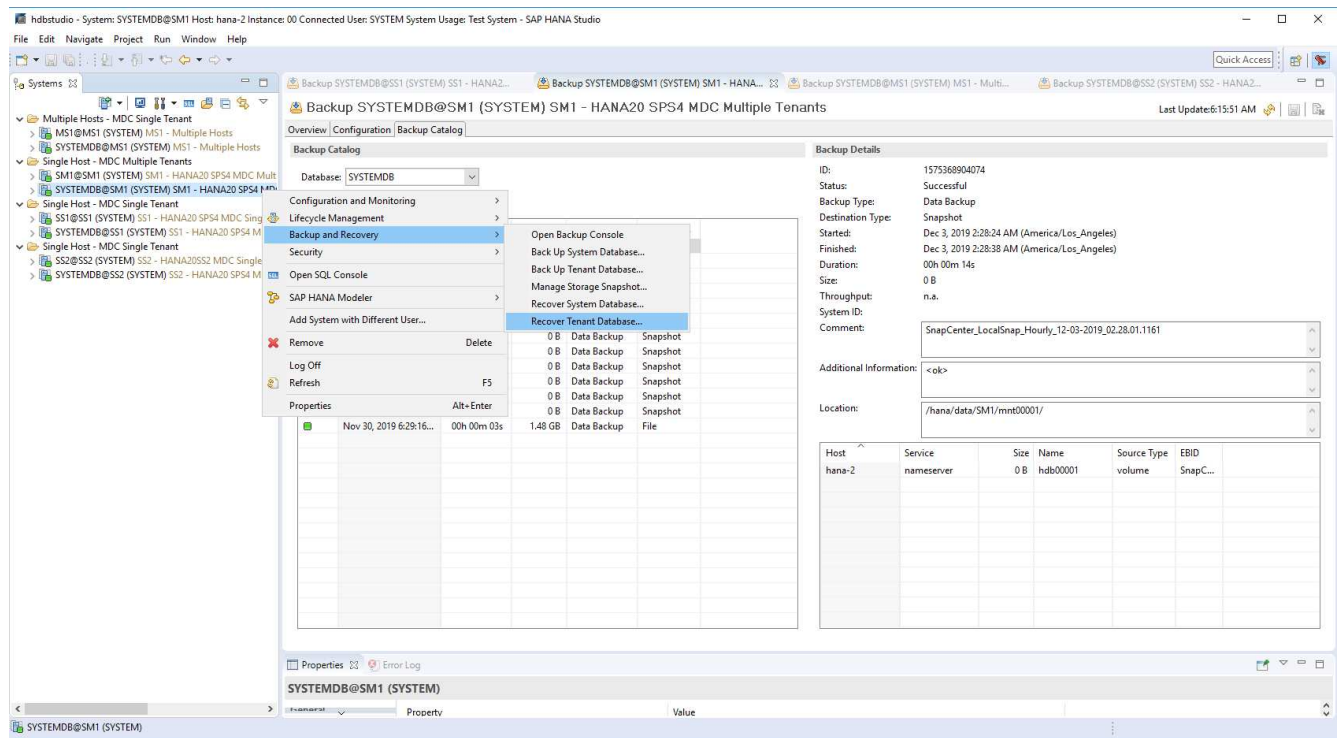
Cuando finaliza la operación de restauración de inquilinos, solo se restauran los datos relevantes del inquilino. En el sistema de archivos del host de la base de datos HANA, el archivo de datos restaurado y el archivo de ID de backup de Snapshot del inquilino están disponibles.

```

smladm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 smladm sapsys 17 Dec 6 04:01
/hana/data/SM1/mnt00001/nameserver.lck
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 smladm sapsys 4096 Dec 6 01:14 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r----- 1 smladm sapsys 3758096384 Dec 6 03:59 datavolume_0000.dat
-rw-r----- 1 smladm sapsys 0 Nov 20 08:36
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 smladm sapsys 36 Nov 20 08:37 landscape.id
/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 smladm sapsys 4096 Nov 20 08:37 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 201441280 Dec 6 03:59 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 smladm sapsys 4096 Dec 6 03:57 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 3758096384 Dec 6 01:14 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 09:35
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 smladm sapsys 155648 Dec 6 01:14
snapshot_databackup_0_1
/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 smladm sapsys 4096 Dec 6 01:14 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 3758096384 Dec 6 03:59 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
smladm@hana-2:/usr/sap/SM1/HDB00>

```

8. Inicie la recuperación con HANA Studio.



9. Seleccione el inquilino.

Recovery of Tenant Database in SM1

Specify tenant database

ipe filter text

☐ SM1

☒ TENANT2

? < Back Next > Finish Cancel

10. Seleccione el tipo de recuperación.


Recovery of Tenant Database in SM1


Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state ⁱ

☐ Recover the database to the following point in time ⁱ


Date: 2019-12-06  Time: 01:18:31

Select Time Zone: (GMT-08:00) Pacific Standard Time 

ⁱ System Time Used (GMT): 2019-12-06 09:18:31

☐ Recover the database to a specific data backup ⁱ

Advanced >>

 < Back Next > Finish Cancel

11. Proporcione la ubicación del catálogo de copias de seguridad.

Recovery of Tenant Database in SM1

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only


Backup Catalog Location:

☐ Recover without the backup catalog


Backint System Copy

☐ Backint System Copy

Source System:



Stop Database TENANT2@SM1

 The database must be offline before recovery can start; the database will be stopped now

Dentro del catálogo de backup, el backup restaurado se resalta con un icono verde. El ID de backup externo muestra el nombre de backup que se seleccionó anteriormente en SnapCenter.

12. Seleccione la entrada con el icono verde y haga clic en Siguiente.

Recovery of Tenant Database in SM1

Select a Backup

Select a backup to recover the SAP HANA database

Selected Point in Time

Database will be recovered to its most recent state.

Backups

The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	A...
2019-12-05 22:28:24	/hana/data/SM1	SNAPSHOT	●
2019-12-05 18:28:24	/hana/data/SM1	SNAPSHOT	⊗
2019-12-05 14:28:23	/hana/data/SM1	SNAPSHOT	⊗
2019-12-05 10:28:24	/hana/data/SM1	SNAPSHOT	⊗
2019-12-05 06:28:23	/hana/data/SM1	SNAPSHOT	⊗
2019-12-05 02:28:23	/hana/data/SM1	SNAPSHOT	⊗
2019-12-04 22:28:24	/hana/data/SM1	SNAPSHOT	⊗
2019-12-04 18:28:23	/hana/data/SM1	SNAPSHOT	⊗
2019-12-04 14:28:25	/hana/data/SM1	SNAPSHOT	⊗
2019-12-04 10:28:24	/hana/data/SM1	SNAPSHOT	⊗

Refresh

Show More

Details of Selected Item

Start Time:

2019-12-05 22:28:24

Destination Type:

SNAPSHOT

Source System:

TENANT2@SM1

Size:

0 B

Backup ID:

1575613704345

External Backup ID:

SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

Backup Name:

/hana/data/SM1

Alternative Location:

Check Availability

?

< Back

Next >

Finish

Cancel

13. Proporcionar la ubicación del backup de registros.

Recovery of Tenant Database in SM1

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

i Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

14. Seleccione los ajustes restantes según sea necesario.

Recovery of Tenant Database in SM1

Other Settings

Check Availability of Delta and Log Backups
You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.
Check the availability of delta and log backups:

☒ File System ^S
☐ Third-Party Backup Tool (Backint)

Initialize Log Area
If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.


☐ Initialize Log Area ^S

Use Delta Backups
Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.

☒ Use Delta Backups (Recommended)

Install New License Key
If you recover the database from a different system, the old license key will no longer be valid
You can:
- Select a new license key to install now
- Install a new license key manually after the database has been recovered

☐ Install New License Key



15. Inicie la operación de recuperación de inquilinos.

Recovery of Tenant Database in SM1

Review Recovery Settings

Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.

Database Information

Database:

TENANT2@SM1

Host:

hana-2

Version:

2.00.040.00.1553674765

Recovery Definition

Recovery Type:

Snapshot (Point-in-Time Recovery (Until Now))

Configuration File Handling

⚠ Caution

To recover customer-specific configuration changes, you may need to make the changes manually in the target system.
More Information: SAP HANA Administration Guide

Show SQL Statement

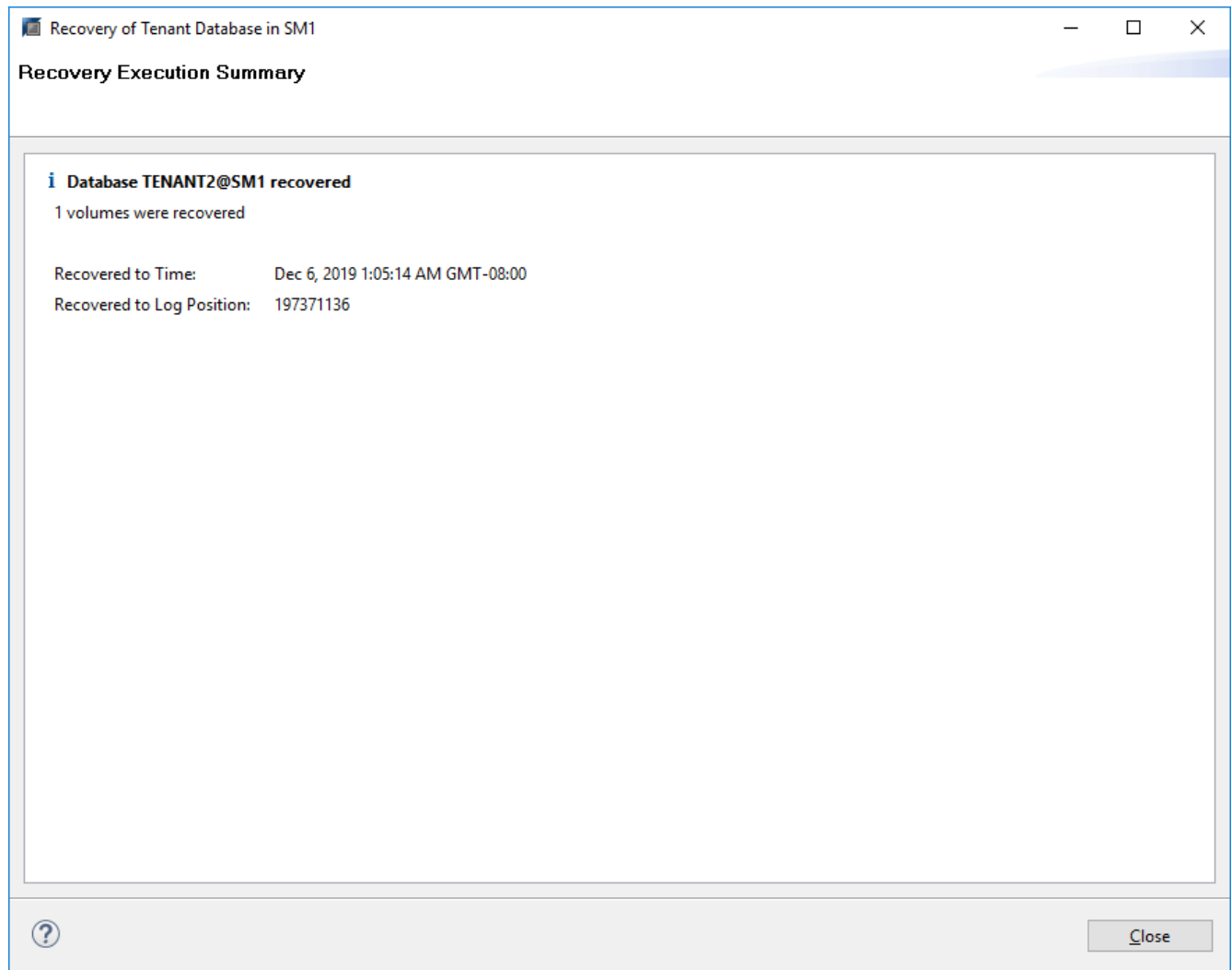
?

< Back

Next >

Finish

Cancel



Restauración con recuperación manual

Para restaurar y recuperar un sistema de un solo inquilino de SAP HANA MDC mediante SAP HANA Studio y SnapCenter, realice los siguientes pasos:

1. Prepare el proceso de restauración y recuperación con SAP HANA Studio:
 - a. Seleccione Recover System Database y confirme el apagado del sistema SAP HANA.
 - b. Seleccione el tipo de recuperación y la ubicación del backup de registro.
 - c. Se muestra la lista de backups de datos. Seleccione copia de seguridad para ver el ID de copia de seguridad externa.
2. Lleve a cabo el proceso de restauración con SnapCenter:
 - a. En la vista de topología del recurso, seleccione copias locales para restaurar desde el almacenamiento principal o copias de almacén si desea restaurar desde un almacenamiento de backup externo.
 - b. Seleccione el backup de SnapCenter que coincida con el campo External backup ID o comment de SAP HANA Studio.
 - c. Inicie el proceso de restauración.



Si se elige una restauración basada en volumen desde el almacenamiento principal, los volúmenes de datos deben desmontarse de todos los hosts de bases de datos SAP HANA antes de la restauración y montarse de nuevo una vez que haya finalizado el proceso de restauración.



En una configuración de varios hosts de SAP HANA con FC, el servidor de nombres SAP HANA ejecuta las operaciones de desmontaje y montaje como parte del proceso de apagado e inicio de la base de datos.

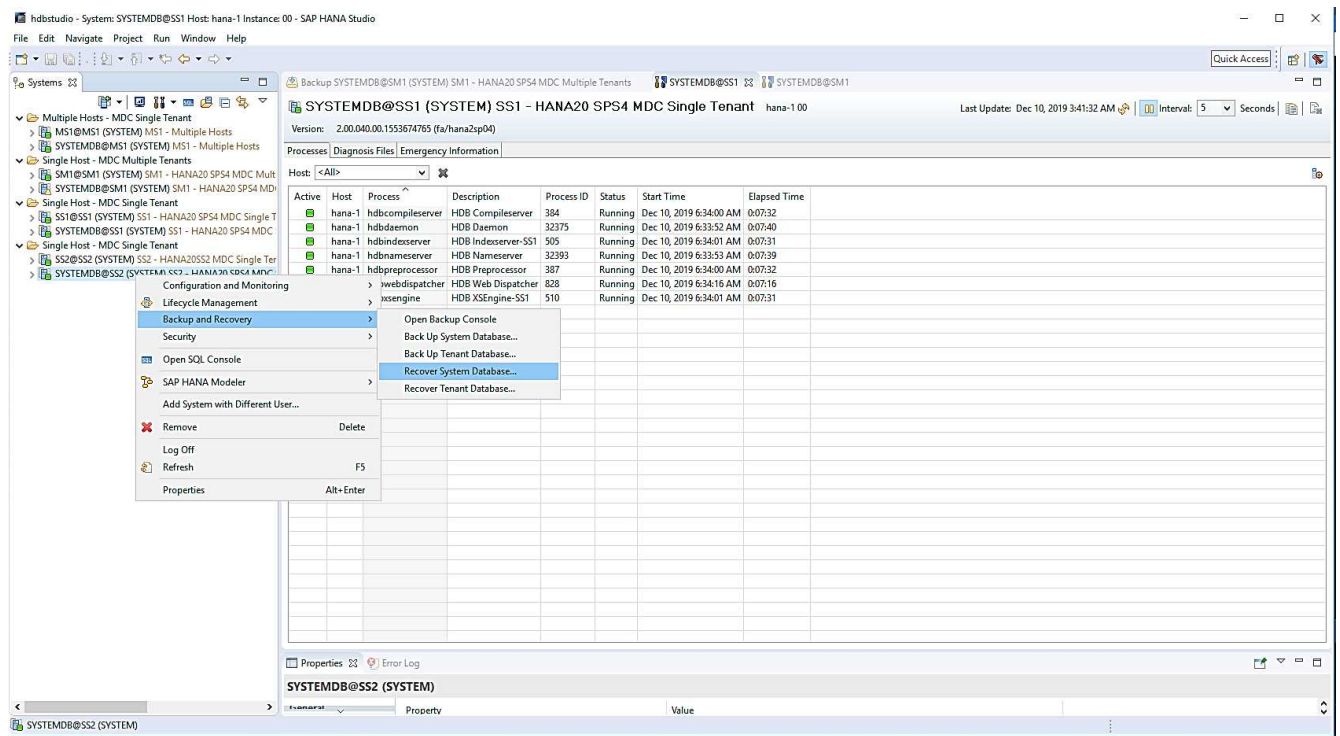
3. Ejecute el proceso de recuperación de la base de datos del sistema con SAP HANA Studio:
 - a. Haga clic en Refresh en la lista de copias de seguridad y seleccione el backup disponible para la recuperación (se indica con un icono verde).
 - b. Inicie el proceso de recuperación. Una vez finalizado el proceso de recuperación, se inicia la base de datos del sistema.
4. Ejecute el proceso de recuperación de la base de datos de tenant con SAP HANA Studio:
 - a. Seleccione Recover Tenant Database y seleccione el inquilino que se va a recuperar.
 - b. Seleccione el tipo de recuperación y la ubicación del backup de registro.

Se muestra una lista de backups de datos. Dado que el volumen de datos ya se ha restaurado, el backup de inquilinos se indica como disponible (en verde).

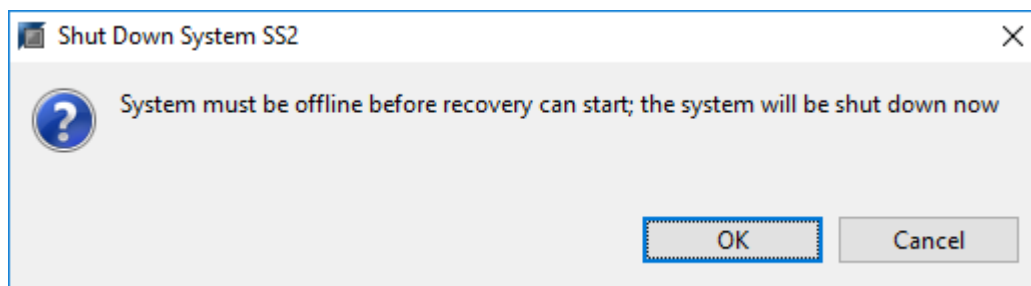
- c. Seleccione este backup e inicie el proceso de recuperación. Una vez que finaliza el proceso de recuperación, la base de datos de tenant se inicia automáticamente.

En la siguiente sección se describen los pasos de las operaciones de restauración y recuperación del sistema HANA configurado manualmente SS2 (un solo host de SAP HANA, sistema de varios inquilinos de MDC mediante NFS).

1. En SAP HANA Studio, seleccione la opción recover System Database para iniciar la recuperación de la base de datos del sistema.



2. Haga clic en OK para apagar la base de datos SAP HANA.



El sistema SAP HANA se apaga y se inicia el asistente de recuperación.

3. Seleccione el tipo de recuperación y haga clic en Next.


Recovery of SYSTEMDB@SS2


Specify Recovery Type


Select a recovery type.

☒ Recover the database to its most recent state ¹

☐ Recover the database to the following point in time ¹


Date: 2019-12-10  Time: 03:43:03

Select Time Zone: (GMT-08:00) Pacific Standard Time 

 System Time Used (GMT): 2019-12-10 11:43:03

☐ Recover the database to a specific data backup ¹

Advanced >>

 < Back **Next >** Finish Cancel

4. Proporcione la ubicación del catálogo de copias de seguridad y haga clic en Siguiente.

Recovery of SYSTEMDB@SS2

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only


Backup Catalog Location:

☐ Recover without the backup catalog

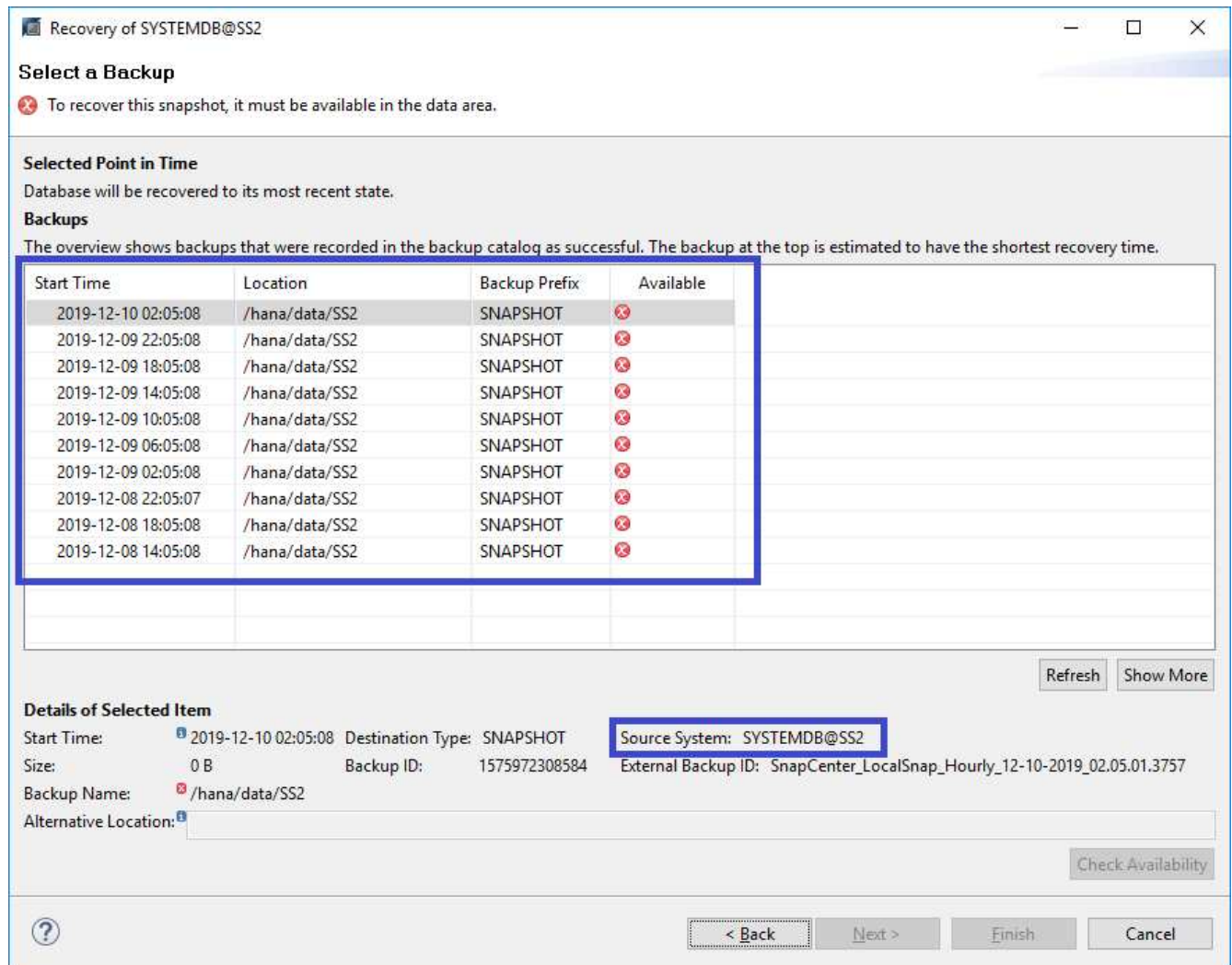
Backint System Copy

☐ Backint System Copy

Source System:



5. Se muestra una lista de backups disponibles en función del contenido del catálogo de backup. Elija la copia de seguridad necesaria y anote el ID de copia de seguridad externa: En nuestro ejemplo, la copia de seguridad más reciente.



6. Desmonte todos los volúmenes de datos.

```
umount /hana/data/SS2/mnt00001
```



Para un sistema host SAP HANA con NFS, se deben desmontar todos los volúmenes de datos de cada host.



En una configuración de varios hosts de SAP HANA con FC, la operación de desmontaje se ejecuta mediante el servidor de nombres de SAP HANA como parte del proceso de apagado.

7. Desde la interfaz gráfica de usuario de SnapCenter, seleccione la vista de topología de recursos y seleccione el backup que debe restaurarse; en nuestro ejemplo, el backup principal más reciente. Haga clic en el icono Restaurar para iniciar la restauración.

SnapCenter®

SAP HANA | SS2 - HANA 20 SP54 MDC Single Tenant Topology

Search databases

System

MS1 - Multiple Hosts MDC Single Tenant

SS2 - HANA 20 SP54 MDC Single Tenant

SM1

SS1

Manage Copies

12 Backups

0 Clones

Local copies

Summary Card

14 Backups

12 Snapshot based backups

2 File-Based backups ✓

0 Clones

Primary Backup(s)

search

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757	1	12/10/2019 2:05:23 AM
SnapCenter_LocalSnap_Hourly_12-09-2019_22.05.01.3848	1	12/09/2019 10:05:23 PM
SnapCenter_LocalSnap_Hourly_12-09-2019_18.05.01.2909	1	12/09/2019 6:05:23 PM
SnapCenter_LocalSnap_Hourly_12-09-2019_14.05.01.3300	1	12/09/2019 2:05:23 PM
SnapCenter_LocalSnap_Hourly_12-09-2019_10.05.01.3143	1	12/09/2019 10:05:23 AM
SnapCenter_LocalSnap_Hourly_12-09-2019_06.05.01.6648	1	12/09/2019 6:05:23 AM
SnapCenter_LocalSnap_Hourly_12-09-2019_02.05.01.2792	1	12/09/2019 2:05:22 AM
SnapCenter_LocalSnap_Hourly_12-08-2019_22.05.01.1815	1	12/08/2019 10:05:22 PM
SnapCenter_LocalSnap_Hourly_12-08-2019_18.05.01.2784	1	12/08/2019 6:05:23 PM
SnapCenter_LocalSnap_Hourly_12-08-2019_14.05.01.2938	1	12/08/2019 2:05:23 PM
Total 4		
Total 12		

Activities

5 Completed 0 Warnings 0 Failed 0 Canceled 0 Running 0 Queued

Se iniciará el asistente SnapCenter restore.

8. Seleccione el tipo de restauración Complete Resource o File Level.

Seleccione Complete Resource para utilizar una restauración basada en volúmenes.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

☒ Complete Resource

☐ File Level

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous Next

9. Seleccione nivel de archivo y todo para utilizar una operación SnapRestore de archivo único para todos los archivos.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

☐ Complete Resource

☒ File Level

Select files to restore

Volume/Qtree	All	File Path
<input checked="" type="checkbox"/> hana-primary.sapcc.stl.netapp.com:/vol/SS...	<input checked="" type="checkbox"/>	<div>Provide one or more file paths separated by comma</div>

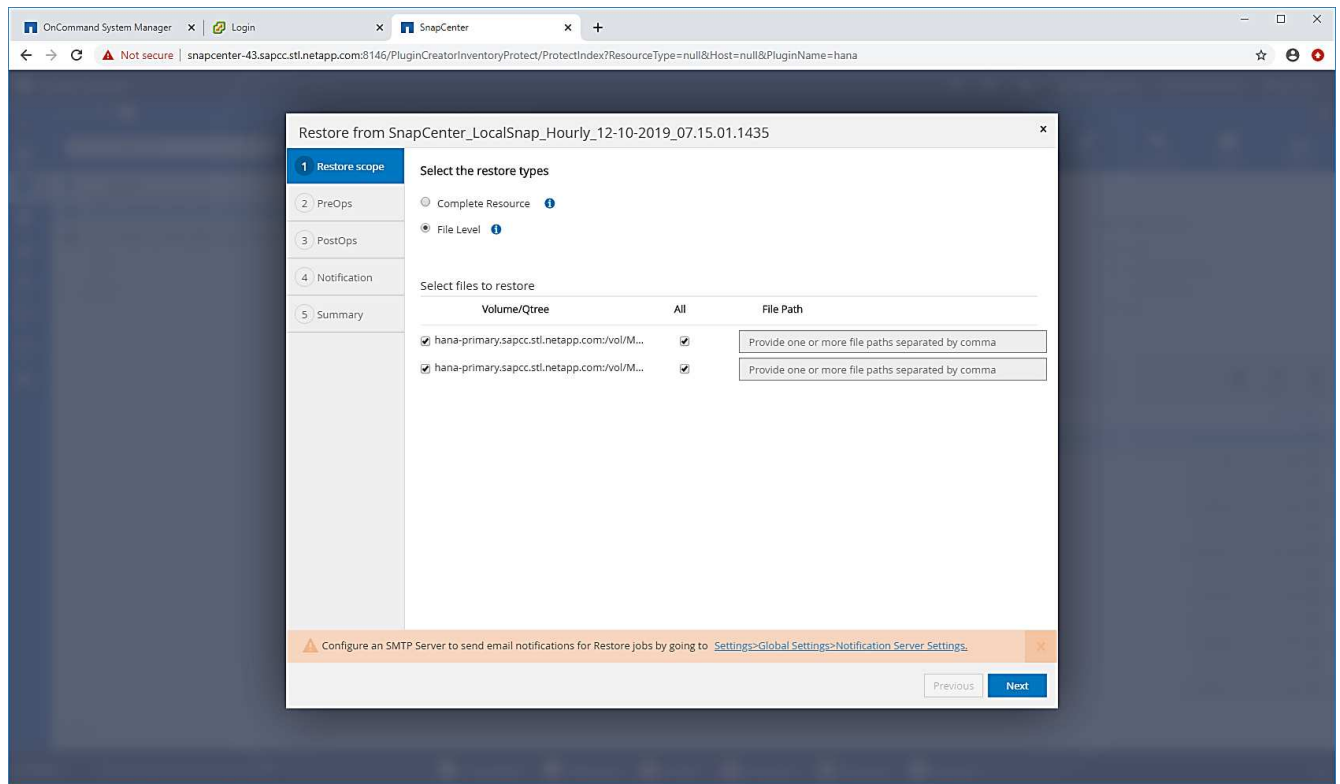
Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next



Para una restauración a nivel de archivo de un sistema host SAP HANA varios, seleccione todos los volúmenes.



10. (Opcional) especifique los comandos que se deben ejecutar desde el plugin de SAP HANA que se ejecuta en el host del plugin de HANA central. Haga clic en Siguiente.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Enter optional commands to run before performing a restore operation

Pre restore command

Unmount command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

11. Especifique los comandos opcionales y haga clic en Next.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Enter optional commands to run after performing a restore operation

Mount command

Post restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

12. Especifique la configuración de notificación para que SnapCenter pueda enviar un correo electrónico de estado y un registro de trabajos. Haga clic en Siguiente.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

Email from

To

Email to

Subject

Notification

☐ Attach Job Report

⚠ If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

13. Revise el resumen y haga clic en Finish para iniciar la restauración.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Summary

Backup Name	SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757
Backup date	12/10/2019 2:05:23 AM
Restore scope	Complete Resource
Pre restore command	
Unmount command	
Mount command	
Post restore command	
Send email	No

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish

14. Se inicia el trabajo de restauración y el registro de trabajos se puede mostrar haciendo doble clic en la línea de registro del panel de actividades.

Job Details

×

Restore 'SnapCenter-43.sapcc.stl.netapp.com\hana\MDC\SS2'

✓ ▼ Restore 'SnapCenter-43.sapcc.stl.netapp.com\hana\MDC\SS2'

✓ ▼ SnapCenter-43.sapcc.stl.netapp.com

✓ ▼ Restore

✓ ▶ Validate Plugin Parameters

✓ ▶ Pre Restore Application

✓ ▶ File or Volume Restore

✓ ▶ Recover Application

✓ ▶ Clear Catalog on Server

✓ ▶ Application Clean-Up

✓ ▶ Data Collection

✓ ▼ Agent Finalize Workflow

Task Name: Agent Finalize Workflow Start Time: 12/10/2019 3:47:30 AM End Time: 12/10/2019 3:47:35 AM

View Logs

Cancel Job

Close

15. Espere hasta que finalice el proceso de restauración. En cada host de base de datos, monte todos los volúmenes de datos. En nuestro ejemplo, solo se debe volver a montar un volumen en el host de la base de datos.

```
mount /hana/data/SP1/mnt00001
```

16. Vaya a SAP HANA Studio y haga clic en Refresh para actualizar la lista de backups disponibles. El backup que se restauró con SnapCenter se muestra con un icono verde en la lista de backups. Seleccione el backup y haga clic en Next.

125

Recovery of SYSTEMDB@SS2

Select a Backup

Select a backup to recover the SAP HANA database

Selected Point in Time

Database will be recovered to its most recent state.

Backups

The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	Available
2019-12-10 02:05:08	/hana/data/SS2	SNAPSHOT	●
2019-12-09 22:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 18:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 14:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 10:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 06:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 02:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 22:05:07	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 18:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 14:05:08	/hana/data/SS2	SNAPSHOT	✗

Refresh
Show More

Details of Selected Item

Start Time:
2019-12-10 02:05:08

Destination Type:
SNAPSHOT

Source System:
SYSTEMDB@SS2

Size:
0 B

Backup ID:
1575972308584

External Backup ID:
SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

Backup Name:
/hana/data/SS2

Alternative Location:

Check Availability

?

< Back
Next >
Finish
Cancel

17. Proporcionar la ubicación de los backups de registros. Haga clic en Siguiente.

Recovery of SYSTEMDB@SS2

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

i Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

18. Seleccione otros ajustes según sea necesario. Asegúrese de que no esté seleccionada la opción utilizar copias de seguridad delta. Haga clic en Siguiente.

Recovery of SYSTEMDB@SS2

Other Settings

Check Availability of Delta and Log Backups

You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.

Check the availability of delta and log backups:

☒ File System [?]

☐ Third-Party Backup Tool (Backint)

Initialize Log Area

If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.

☐ Initialize Log Area [?]

Use Delta Backups

Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.

☐ Use Delta Backups (Recommended)


Install New License Key

If you recover the database from a different system, the old license key will no longer be valid

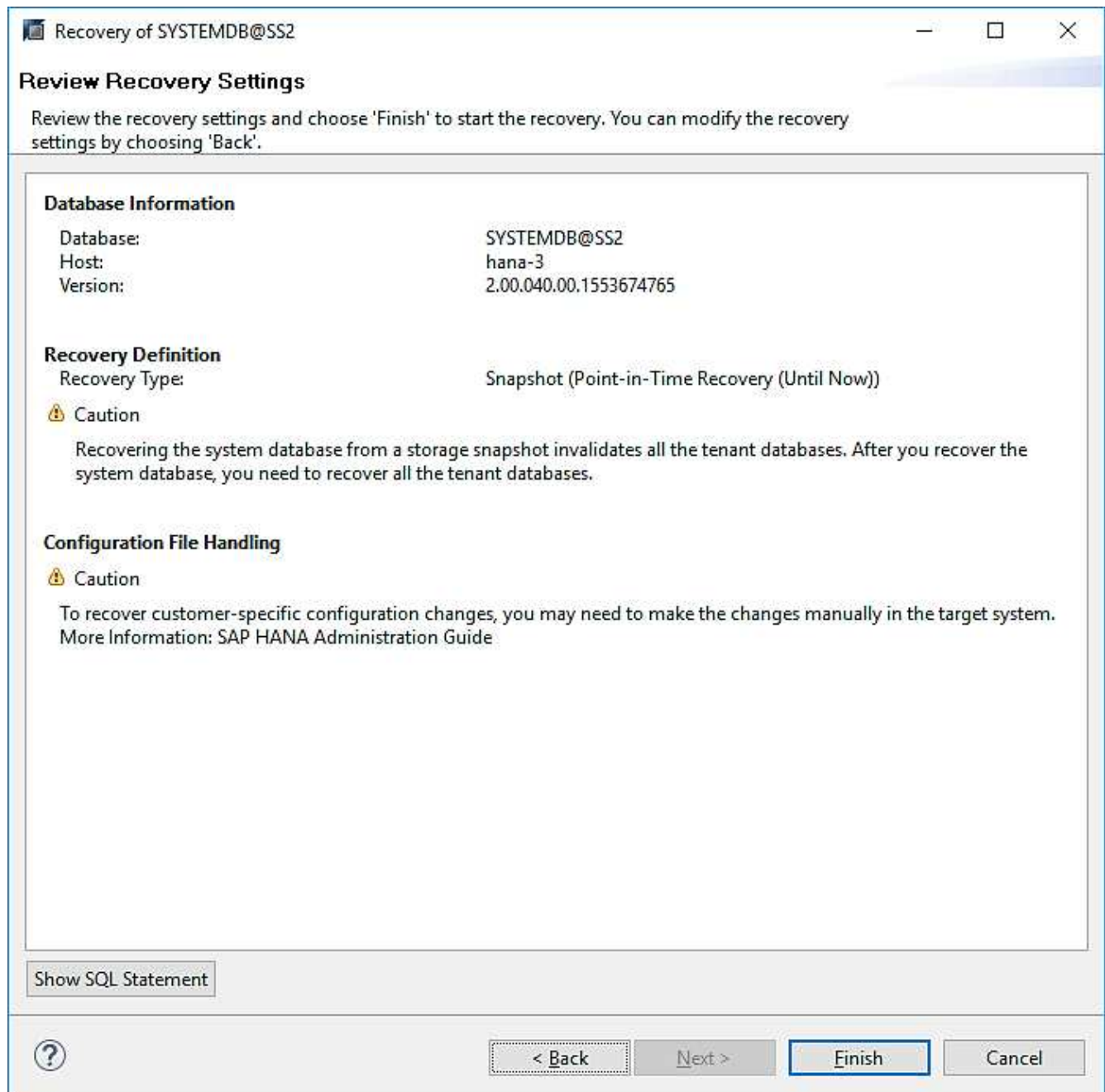
You can:

- Select a new license key to install now
- Install a new license key manually after the database has been recovered

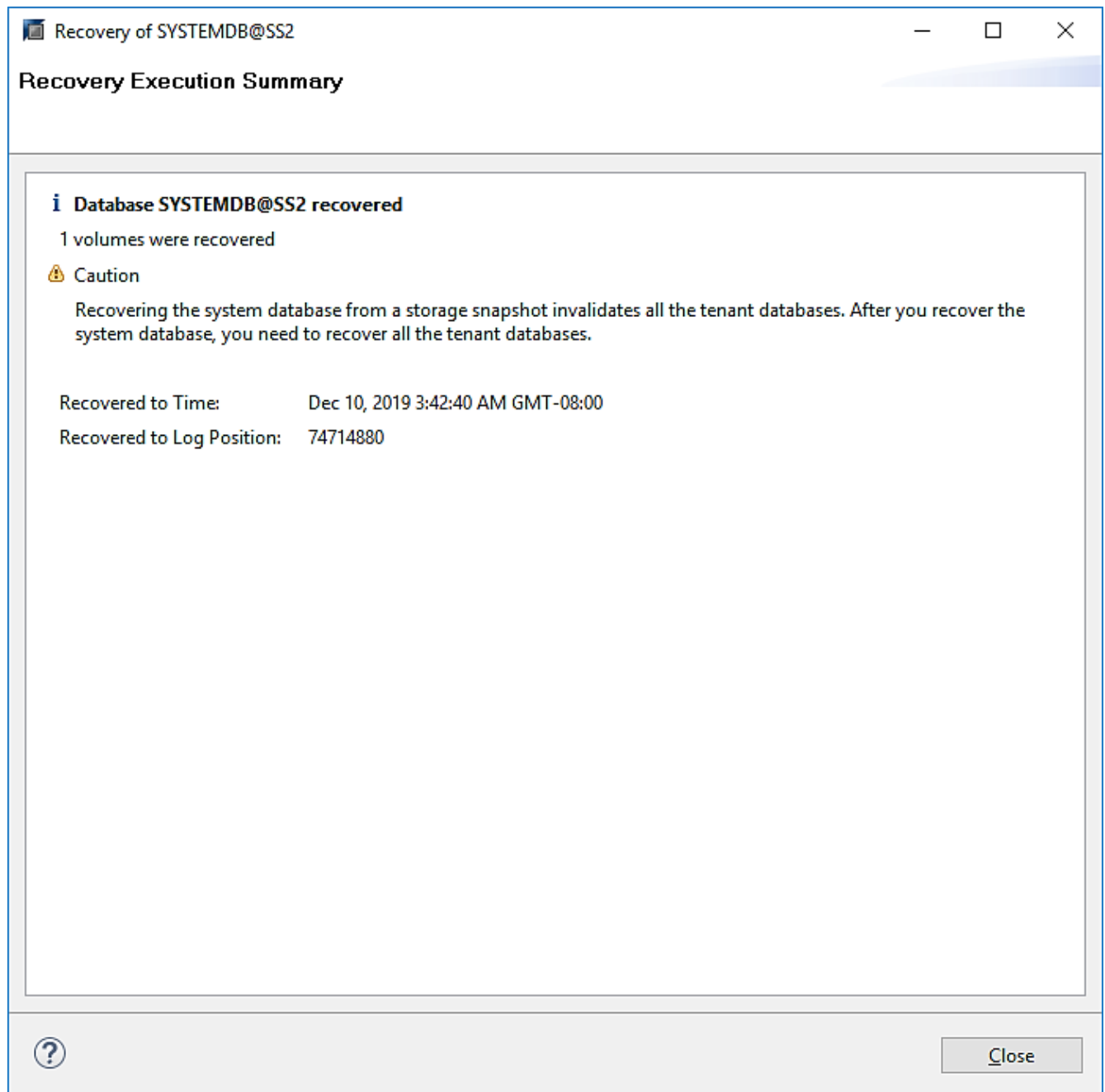
☐ Install New License Key



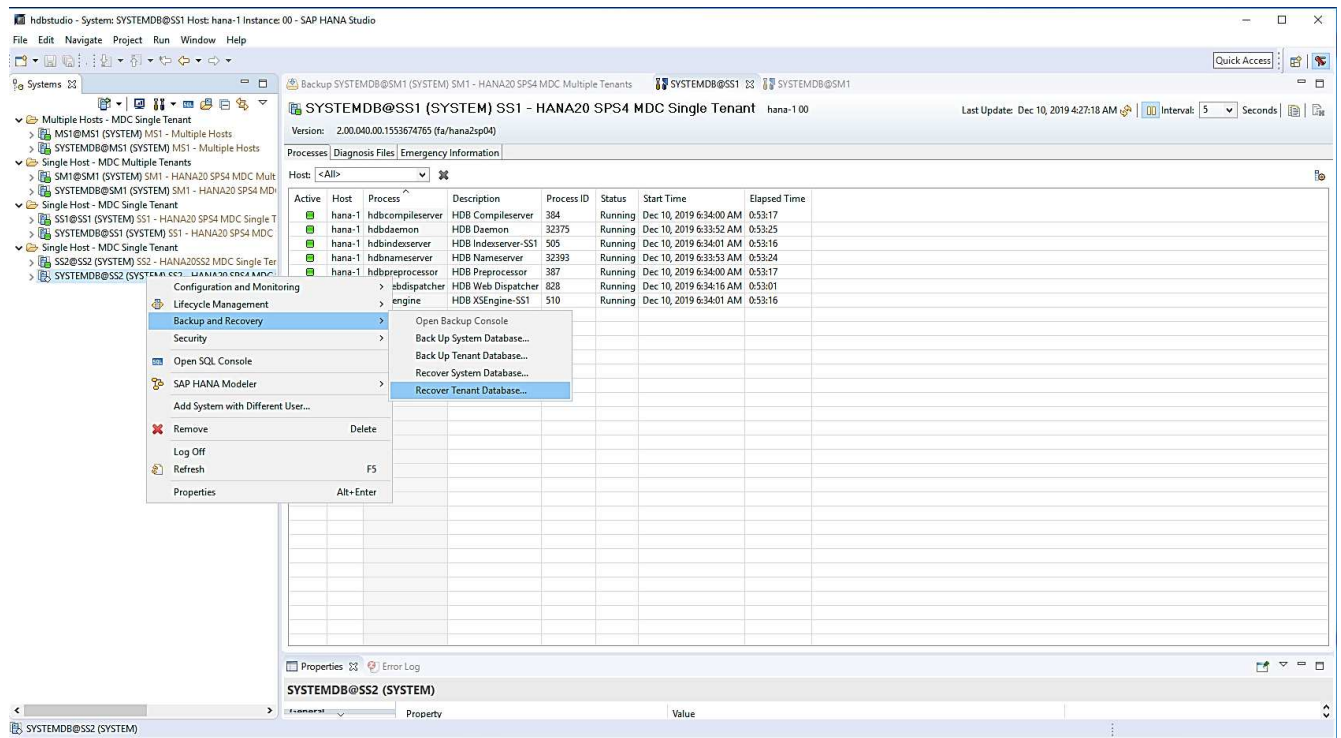
19. Revise la configuración de recuperación y haga clic en Finish.



20. Se inicia el proceso de recuperación. Espere hasta que finalice la recuperación de la base de datos del sistema.



21. En SAP HANA Studio, seleccione la entrada de la base de datos del sistema e inicie Backup Recovery - recover tenant Database.



22. Seleccione el inquilino que desea recuperar y haga clic en Siguiente.

Recovery of Tenant Database in SS2

Specify tenant database

ipe filter text

☒ SS2

? < Back Next > Finish Cancel

23. Especifique el tipo de recuperación y haga clic en Next.


Recovery of Tenant Database in SS2


Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state ⁱ

☐ Recover the database to the following point in time ⁱ


Date: 2019-12-10  Time: 04:27:22

Select Time Zone: (GMT-08:00) Pacific Standard Time 

ⁱ System Time Used (GMT): 2019-12-10 12:27:22

☐ Recover the database to a specific data backup ⁱ

Advanced >>

 < Back Next > Finish Cancel

24. Confirme la ubicación del catálogo de backup y haga clic en Next.

Recovery of Tenant Database in SS2

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only

Backup Catalog Location:

☐ Recover without the backup catalog

Backint System Copy

☐ Backint System Copy

Source System:

25. Confirme que la base de datos de tenant está sin conexión. Haga clic en OK para continuar.

Stop Database SS2@SS2

The database must be offline before recovery can start; the database will be stopped now

26. Como la restauración del volumen de datos se ha producido antes de la recuperación de la base de datos del sistema, el backup de inquilino está disponible de inmediato. Seleccione el backup resaltado en verde

y haga clic en Next.

Recovery of Tenant Database in SS2

Select a Backup

Select a backup to recover the SAP HANA database

Selected Point in Time

Database will be recovered to its most recent state.

Backups

The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	Available
2019-12-10 02:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 22:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 18:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 14:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 10:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 06:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 02:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-08 22:05:07	/hana/data/SS2	SNAPSHOT	
2019-12-08 18:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-08 14:05:08	/hana/data/SS2	SNAPSHOT	

Refresh

Show More

Details of Selected Item

Start Time: 2019-12-10 02:05:08

Destination Type: SNAPSHOT

Source System: SS2@SS2

Size: 0 B

Backup ID: 1575972308585

External Backup ID: SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

Backup Name: /hana/data/SS2

Alternative Location:

Check Availability

< Back

Next >

Finish

Cancel

27. Confirme la ubicación del backup de registros y haga clic en Next.

Recovery of Tenant Database in SS2

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

i Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

28. Seleccione otros ajustes según sea necesario. Asegúrese de que no esté seleccionada la opción utilizar copias de seguridad delta. Haga clic en Siguiente.

Recovery of Tenant Database in SS2

Other Settings

Check Availability of Delta and Log Backups

You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.

Check the availability of delta and log backups:

☒ File System ⁱ

☐ Third-Party Backup Tool (Backint)

Initialize Log Area

If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.

☐ Initialize Log Area ⁱ

Use Delta Backups

Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.

☐ Use Delta Backups (Recommended) ⁱ

Install New License Key

If you recover the database from a different system, the old license key will no longer be valid

You can:

- Select a new license key to install now
- Install a new license key manually after the database has been recovered

☐ Install New License Key

Browse

? < Back Next > Finish Cancel

29. Revise la configuración de recuperación e inicie el proceso de recuperación de la base de datos de tenant haciendo clic en Finish.

Recovery of Tenant Database in SS2

Review Recovery Settings

Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.

Database Information

Database:

SS2@SS2

Host:

hana-3

Version:

2.00.040.00.1553674765

Recovery Definition

Recovery Type:

Snapshot (Point-in-Time Recovery (Until Now))

Configuration File Handling

⚠ Caution

To recover customer-specific configuration changes, you may need to make the changes manually in the target system.

More Information: SAP HANA Administration Guide

Show SQL Statement

?

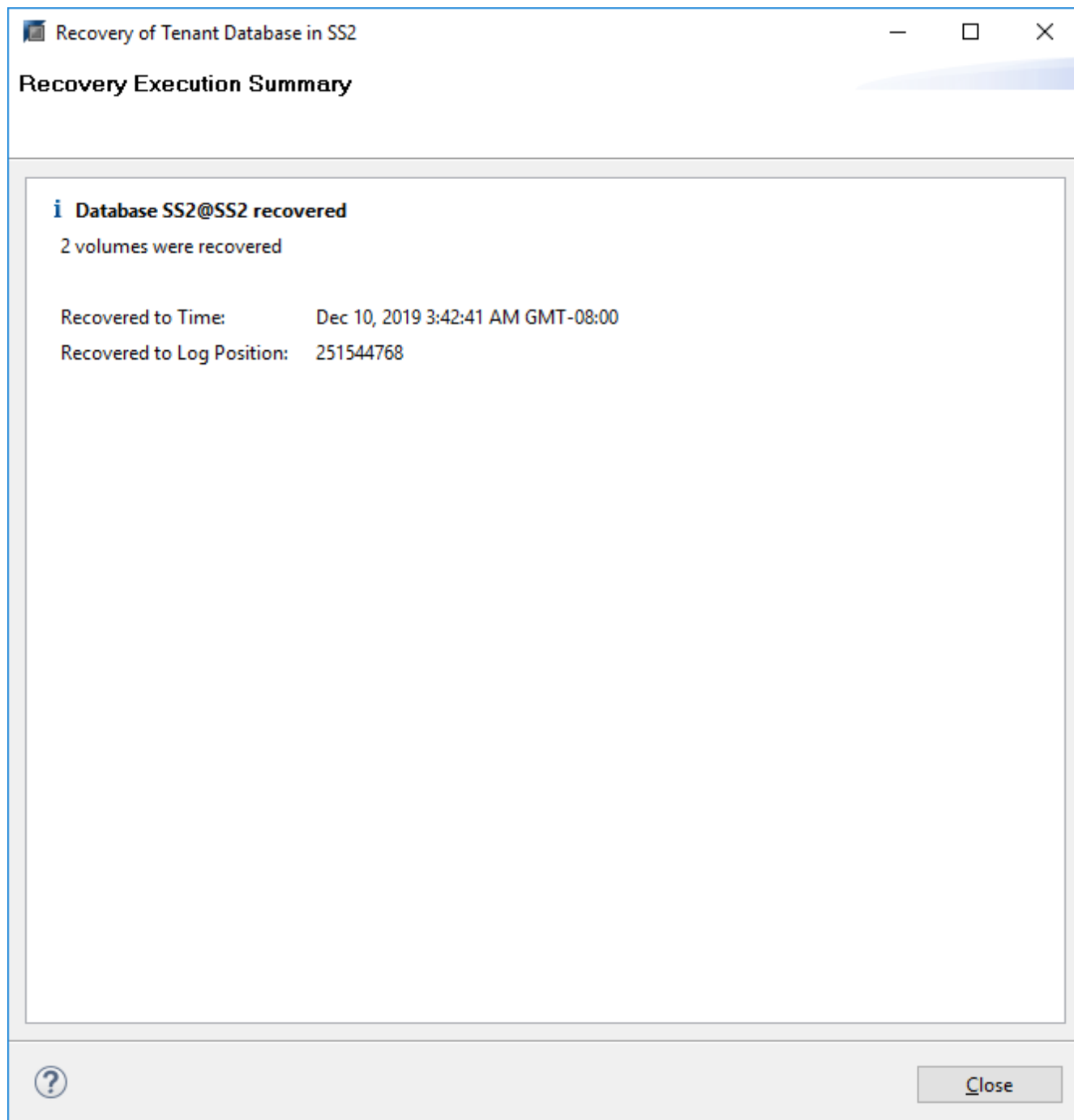
< Back

Next >

Finish

Cancel

30. Espere hasta que termine la recuperación y se inicie la base de datos de tenant.



El sistema SAP HANA está listo para funcionar.



Para un sistema MDC de SAP HANA con varios inquilinos, debe repetir los pasos 20–29 para cada inquilino.

Configuración y ajuste avanzados

En esta sección se describen las opciones de configuración y ajuste que los clientes pueden usar para adaptar la configuración de SnapCenter a sus necesidades específicas. Es posible que no todas las configuraciones se apliquen a todos los escenarios de clientes.

Habilite la comunicación segura con la base de datos de HANA

Si las bases de datos de HANA están configuradas con comunicación segura, el `hdbsql` El comando que ejecuta SnapCenter debe utilizar opciones adicionales de la línea de comandos. Esto se puede lograr usando un script contenedor que llama `hdbsql` con las opciones necesarias.



Existen varias opciones para configurar la comunicación SSL. En los siguientes ejemplos, la configuración de cliente más simple se describe utilizando la opción de línea de comandos, donde no se realiza ninguna validación de certificado de servidor. Si se requiere la validación de certificados en el servidor o en el cliente, se necesitan diferentes opciones de línea de comandos `hdbsql` y debe configurar el entorno PSE de acuerdo con lo descrito en la Guía de seguridad de SAP HANA.

En lugar de configurar el `hdbsql` ejecutable en la `hana.properties` archivos, se agrega el script contenedor.

Para un host de plugin de HANA central en el servidor de Windows de SnapCenter, debe añadir el siguiente contenido en `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\hana.properties`.

```
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql-ssl.cmd
```

La secuencia de comandos contenedora `hdbsql-ssl.cmd` llamadas `hdbsql.exe` con las opciones de línea de comandos necesarias.

```
@echo off
"C:\Program Files\sap\hdbclient\hdbsql.exe" -e -ssltrustcert %*
```



La `-e - ssltrustcert` La opción de línea de comandos `hdbsql` también funciona con sistemas HANA en los que SSL no está habilitado. Por lo tanto, esta opción también se puede usar con un host del complemento HANA central, donde no todos los sistemas HANA tienen SSL habilitado o deshabilitado.

Si el plugin de HANA se pone en marcha en hosts de base de datos HANA individuales, la configuración se debe realizar en cada host Linux de forma acorde.

```
HANA_HDBSQL_CMD = /usr/sap/SM1/HDB12/exe/hdbsqls
```

La secuencia de comandos contenedora `hdbsqls` llamadas `hdbsql` con las opciones de línea de comandos necesarias.

```
#!/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql -e -ssltrustcert $*
```

Deshabilite la detección automática en el host del plugin de HANA

Para deshabilitar la detección automática en el host del plugin de HANA, complete los siguientes pasos:

1. En el servidor de SnapCenter, abra PowerShell. Conéctese al servidor SnapCenter ejecutando el `Open-SmConnection` y especifique el nombre de usuario y la contraseña en la ventana de inicio de sesión de apertura.
2. Para deshabilitar la detección automática, ejecute el `Set-SmConfigSettings` comando.

Para un host HANA hana-2, el mandato es el siguiente:

```
PS C:\Users\administrator.SAPCC> Set-SmConfigSettings -Agent -Hostname
hana-2 -configSettings @{"DISABLE_AUTO_DISCOVERY"="true"}
Name                               Value
----                               -
DISABLE_AUTO_DISCOVERY            true
PS C:\Users\administrator.SAPCC>
```

3. Verifique la configuración ejecutando el `Get-SmConfigSettings` comando.

```
PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname
hana-2 -key all
Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC           Value: 3600000
Details: Plug-in API operation Timeout
Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC  Value: 1800
Details: Web Service API Timeout
Key: CUSTOMPLUGINS_ALLOWED_CMDS                       Value: *;
Details: Allowed Host OS Commands
Key: DISABLE_AUTO_DISCOVERY                           Value: true
Details:
Key: PORT                                               Value: 8145
Details: Port for server communication
PS C:\Users\administrator.SAPCC>
```

La configuración se escribe en el archivo de configuración del agente en el host y sigue disponible después de una actualización de plugin con SnapCenter.

```
hana-2:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/agent.properties | grep DISCOVERY
DISABLE_AUTO_DISCOVERY = true
hana-2:/opt/NetApp/snapcenter/scc/etc #
```

Desactivar el mantenimiento automático de los backups de registros

El mantenimiento del backup de registros está habilitado de forma predeterminada y se puede deshabilitar en el nivel de host del plugin de HANA. Hay dos opciones para cambiar esta configuración.

Edite el archivo hana.property

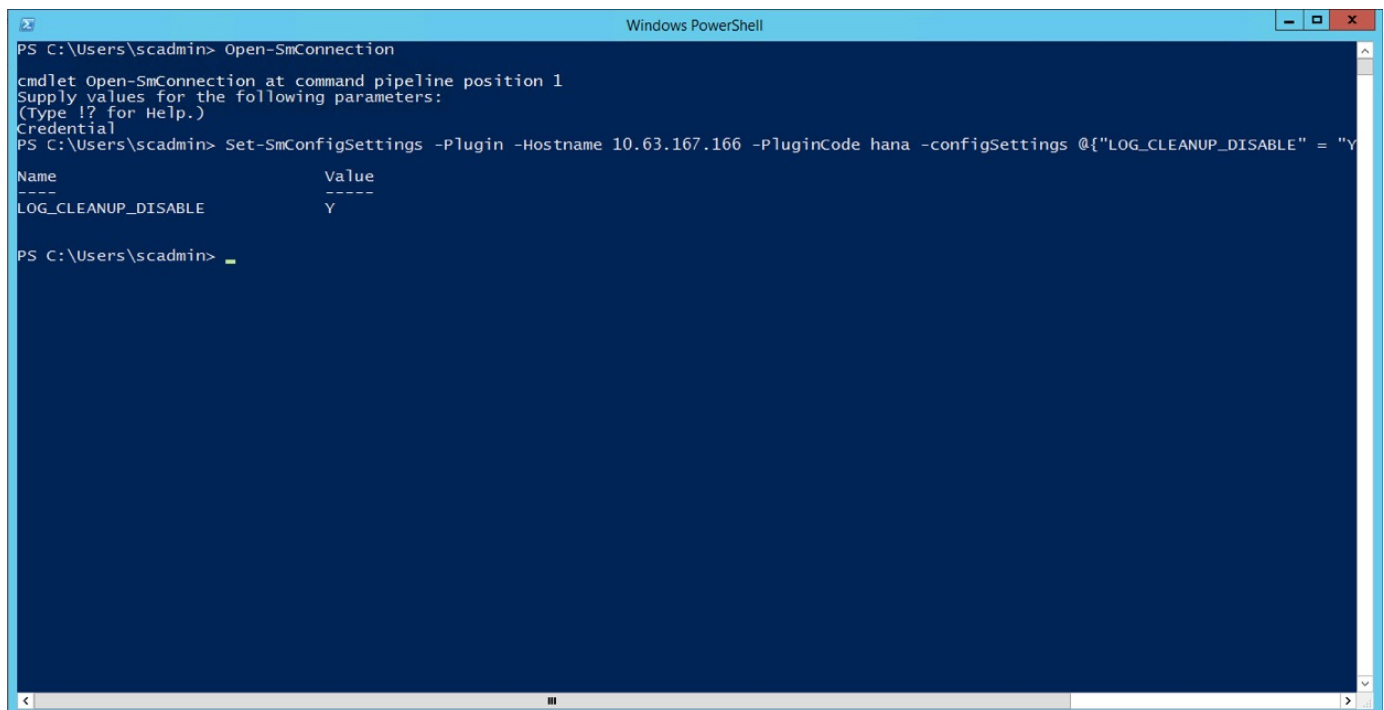
Incluido el parámetro `LOG_CLEANUP_DISABLE = Y` en la `hana.property` El archivo de configuración deshabilita el mantenimiento del backup de registros de todos los recursos mediante este host del plugin de SAP HANA como host de comunicación:

- Para el host de comunicación Hdbsql en Windows, la `hana.property` el archivo está ubicado en `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc.`
- Para el host de comunicación Hdbsql en Linux, la `hana.property` el archivo está ubicado en `/opt/NetApp/snapcenter/scc/etc.`

Utilice el comando PowerShell

Una segunda opción para configurar estas opciones es usar un comando de PowerShell de SnapCenter.

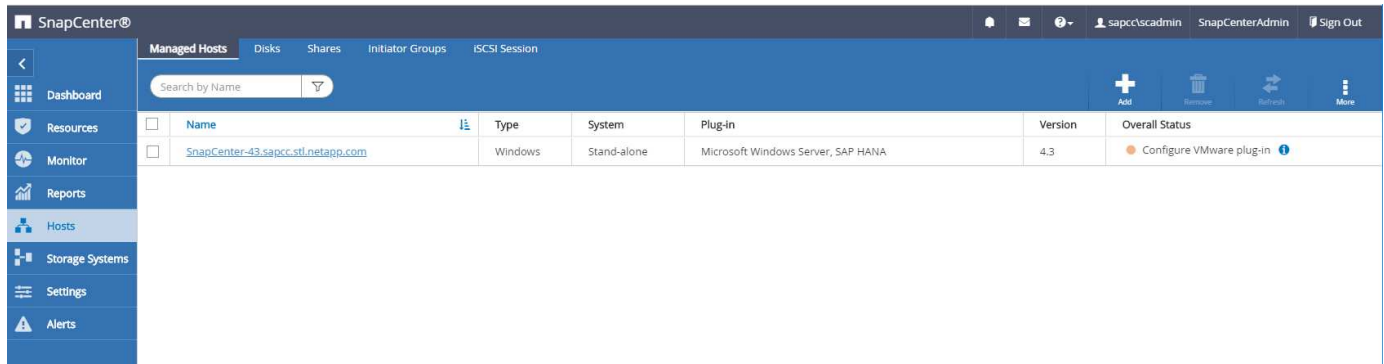
1. En el servidor SnapCenter, abra un PowerShell. Conéctese al servidor SnapCenter mediante el comando `Open-SmConnection` y especifique el nombre de usuario y la contraseña en la ventana de inicio de sesión abierta.
2. Con el comando `Set-SmConfigSettings -Plugin -HostName <pluginhostname> -PluginCode hana -configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}`, Los cambios se configuran para el host del plug-in SAP HANA <pluginhostname> Especificado por la IP o el nombre de host (consulte la siguiente figura).



```
Windows PowerShell
PS C:\Users\scadmin> Open-SmConnection
cmdlet Open-SmConnection at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Credential
PS C:\Users\scadmin> Set-SmConfigSettings -Plugin -HostName 10.63.167.166 -PluginCode hana -configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}
Name Value
----
LOG_CLEANUP_DISABLE Y
PS C:\Users\scadmin>
```

Deshabilite la advertencia cuando ejecute el plugin de SAP HANA en un entorno virtual

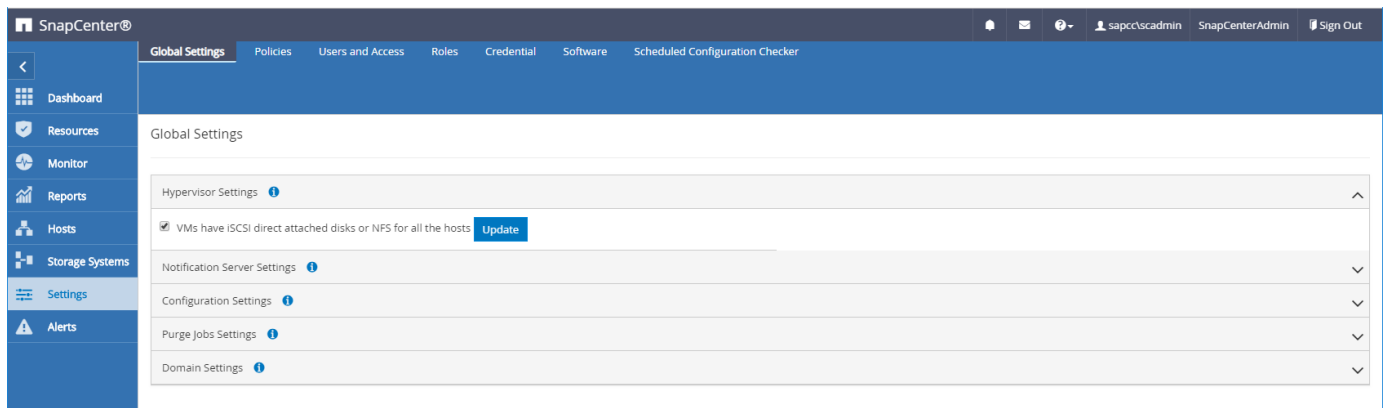
SnapCenter detecta si el plugin de SAP HANA está instalado en un entorno virtualizado. Podría ser un entorno VMware o una instalación de SnapCenter en un proveedor de cloud público. En este caso, SnapCenter muestra una advertencia para configurar el hipervisor, como se muestra en la siguiente figura.



Es posible suprimir esta advertencia globalmente. En este caso, SnapCenter no conoce los entornos virtualizados y, por lo tanto, no muestra estas advertencias.

Para configurar SnapCenter para suprimir esta advertencia, se debe aplicar la siguiente configuración:

1. En la pestaña Configuración, seleccione Configuración global.
2. Para la configuración del hipervisor, seleccione VMs have iSCSI Direct Attached Disks or NFS for All the hosts y actualice la configuración.



Cambie la frecuencia de programación de la sincronización de los backups con el almacenamiento de backup externo

Como se describe en la sección ["Gestión de retención de backups en el almacenamiento secundario"](#), La gestión de retención de backups de datos en un almacenamiento de backup externo es gestionada por ONTAP. SnapCenter comprueba periódicamente si ONTAP ha eliminado los backups del almacenamiento de backup externo ejecutando un trabajo de limpieza con una programación predeterminada semanal.

El trabajo de limpieza de SnapCenter elimina los backups del repositorio de SnapCenter, así como en el catálogo de backups de SAP HANA si se han identificado algunos backups eliminados en el almacenamiento de backup externo.

La tarea de limpieza también ejecuta el mantenimiento de los backups de registros de SAP HANA.

Hasta que esta limpieza programada haya finalizado, SAP HANA y SnapCenter pueden seguir mostrando backups que ya se han eliminado del almacenamiento de backup externo.

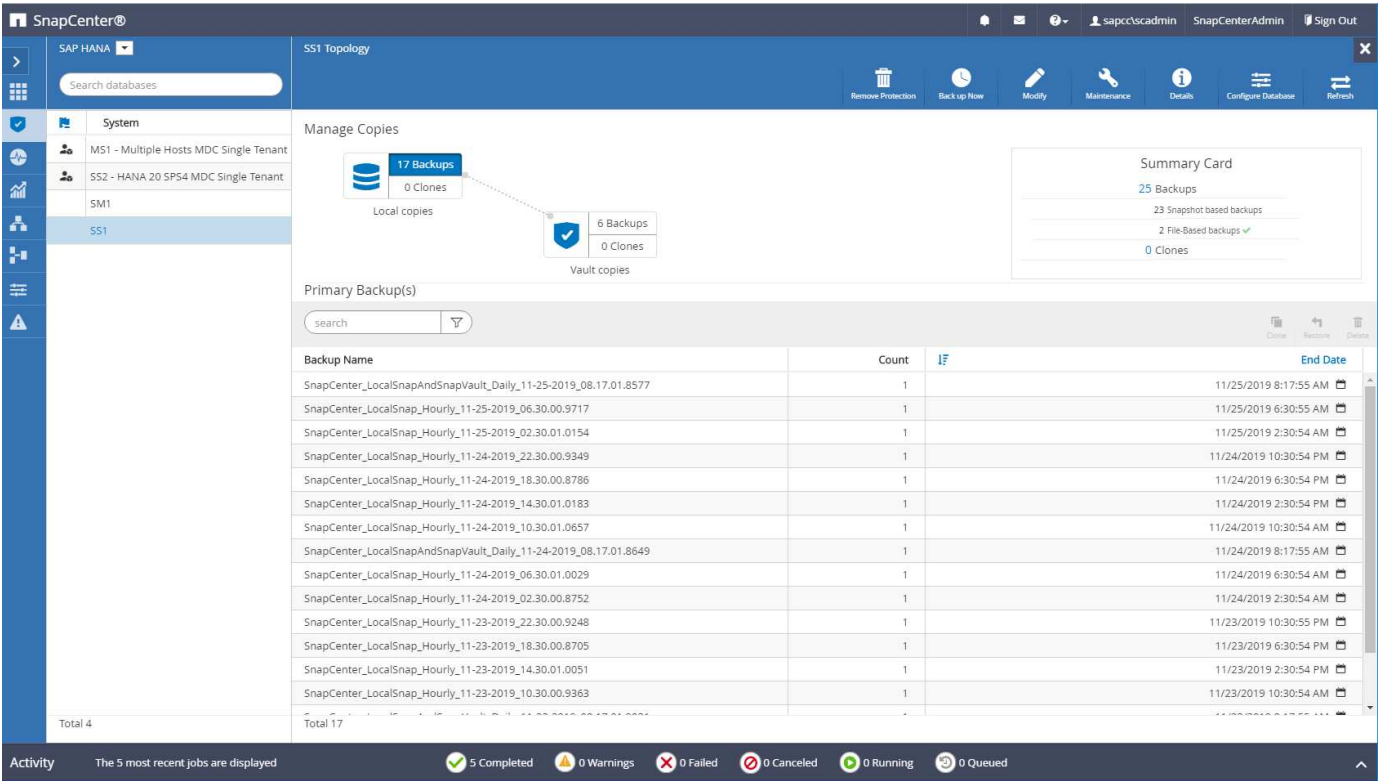


Esto puede generar backups de registros adicionales, incluso si ya se han eliminado los backups Snapshot basados en almacenamiento correspondientes en el almacenamiento de backup externo.

En las siguientes secciones se describen dos formas de evitar esta discrepancia temporal.

Actualización manual a nivel de recursos

En la vista de topología de un recurso, SnapCenter muestra los backups en el almacenamiento de backup externo al seleccionar los backups secundarios, como se muestra en la siguiente captura de pantalla. SnapCenter ejecuta una operación de limpieza con el icono Refresh para sincronizar los backups de este recurso.



Cambie la frecuencia del trabajo de limpieza de SnapCenter

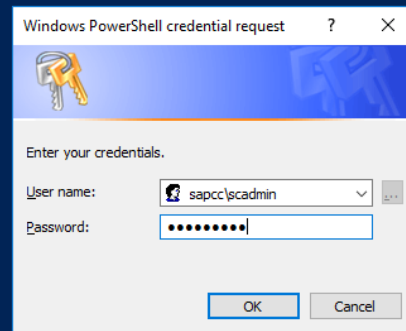
SnapCenter ejecuta el trabajo de limpieza `SnapCenter_RemoveSecondaryBackup` De forma predeterminada, para todos los recursos semanalmente mediante el mecanismo de programación de tareas de Windows. Esto se puede modificar con un cmdlet de PowerShell de SnapCenter.

1. Inicie una ventana de comandos de PowerShell en el servidor SnapCenter.
2. Abra la conexión con SnapCenter Server e introduzca las credenciales de administrador de SnapCenter en la ventana de inicio de sesión.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\scadmin> Open-SmConnection

cmdlet Open-SmConnection at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Credential
```



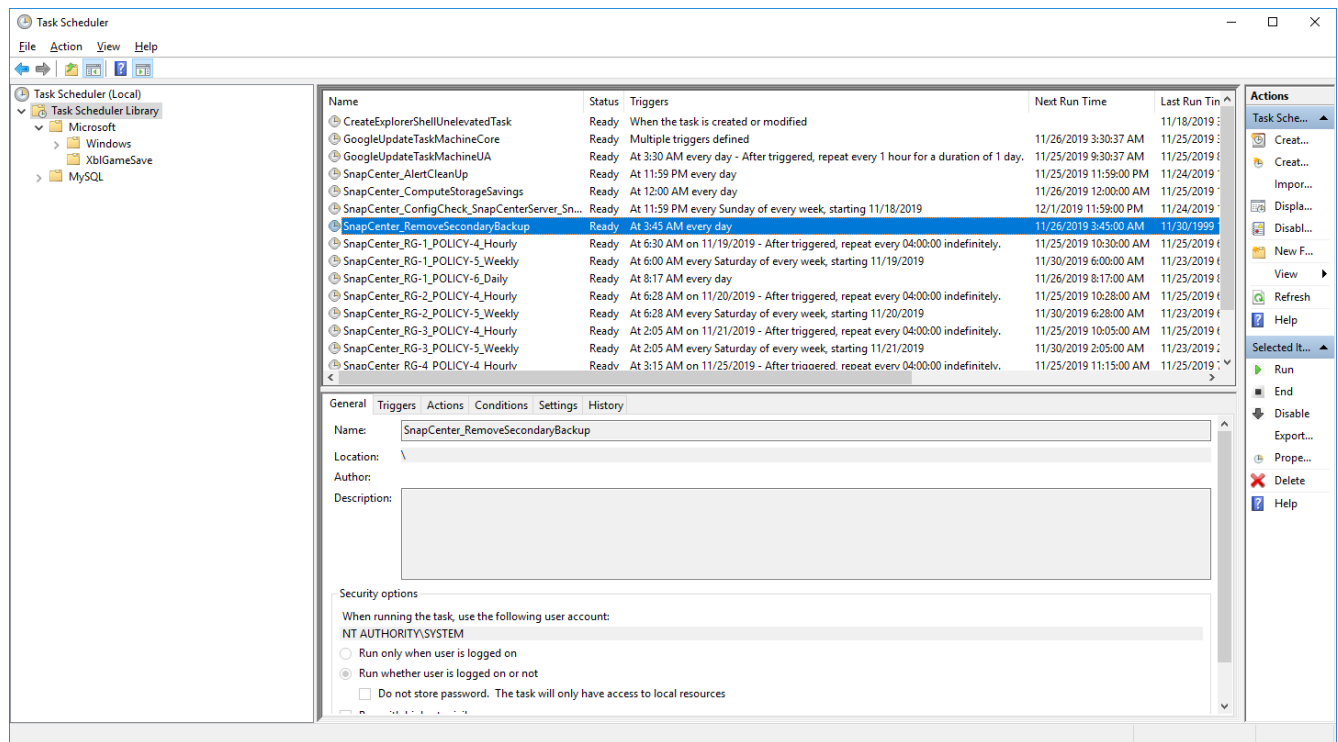
3. Para cambiar la programación de manera semanal a diaria, use el cmdlet `Set-SmSchedule`.

```

PS C:\Users\scadmin> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"=
"1"} -TaskName SnapCenter_RemoveSecondaryBackup
TaskName                : SnapCenter_RemoveSecondaryBackup
Hosts                    : {}
StartTime                : 11/25/2019 3:45:00 AM
DaysOfTheMonth           :
MonthsOfTheYear          :
DaysInterval             : 1
DaysOfTheWeek            :
AllowDefaults            : False
ReplaceJobIfExist        : False
UserName                 :
Password                 :
SchedulerType            : Daily
RepeatTask_Every_Hour    :
IntervalDuration         :
EndTime                  :
LocalScheduler           : False
AppType                  : False
AuthMode                 :
SchedulerSQLInstance     : SMCoreContracts.SmObject
MonthlyFrequency         :
Hour                     : 0
Minute                   : 0
NodeName                 :
ScheduleID               : 0
RepeatTask_Every_Mins    :
CronExpression           :
CronOffsetInMinutes      :
StrStartTime             :
StrEndTime               :
PS C:\Users\scadmin> Check the configuration using the Windows Task
Scheduler.

```

4. Puede comprobar las propiedades del trabajo en el programador de tareas de Windows.



Dónde encontrar información adicional e historial de versiones

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

- Página de recursos de SnapCenter

["https://www.netapp.com/us/documentation/snapcenter-software.aspx"](https://www.netapp.com/us/documentation/snapcenter-software.aspx)

- Documentación del software SnapCenter

["https://docs.netapp.com/us-en/snapcenter/index.html"](https://docs.netapp.com/us-en/snapcenter/index.html)

- TR-4667: Automatización de copias del sistema SAP mediante SnapCenter

<https://www.netapp.com/pdf.html?item=/media/17111-tr4667pdf.pdf>

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

<https://www.netapp.com/pdf.html?item=/media/17030-tr4719pdf.pdf>

- TR-4018: Integración de los sistemas ONTAP de NetApp con SAP Landscape Management

<https://www.netapp.com/pdf.html?item=/media/17195-tr4018pdf.pdf>

- TR-4646: Recuperación ante desastres de SAP HANA con replicación de almacenamiento

<https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf>

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Julio de 2017	<ul style="list-style-type: none"> • Versión inicial.
Versión 1.1	Septiembre de 2017	<ul style="list-style-type: none"> • Se añadió la sección “Configuración y ajuste avanzados”. • Correcciones menores.
Versión 2.0	Marzo de 2018	<ul style="list-style-type: none"> • Actualizaciones de Cover SnapCenter 4,0: Nuevo recurso de volumen de datos Funcionamiento de Single File SnapRestore mejorado
Versión 3.0	A enero de 2020	<ul style="list-style-type: none"> • Añadió la sección “conceptos y mejores prácticas de SnapCenter”. • Actualizaciones de Cover SnapCenter 4,3: Detección automática Restauración y recuperación automatizadas Compatibilidad con varios inquilinos de HANA MDC Operación de restauración de un solo inquilino
Versión 3.1	Julio de 2020	<ul style="list-style-type: none"> • Actualizaciones y correcciones menores: Compatibilidad de NFSv4 con SnapCenter 4.3.1 Configuración de la comunicación SSL Implementación de plug-in central para Linux en IBM Power
Versión 3.2	Noviembre de 2020	<ul style="list-style-type: none"> • Se añadieron los privilegios de usuario de la base de datos necesarios para HANA 2.0 SPS5.

Versión	Fecha	Historial de versiones del documento
Versión 3.3	Mayo de 2021	<ul style="list-style-type: none"> • Se ha actualizado la sección de configuración de SSL hdbsql. • Se añadió el soporte LVM de Linux.
Versión 3.4	Agosto de 2021	<ul style="list-style-type: none"> • Se añadió la descripción de la configuración Deshabilitar la detección automática.
Versión 3.5	Febrero de 2022	<ul style="list-style-type: none"> • Actualizaciones menores para cubrir SnapCenter 4.6 y la compatibilidad con la detección automática para sistemas HANA con replicación de sistemas HANA.

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.