Recuperación ante desastres de SAP HANA con Azure NetApp Files

NetApp Solutions SAP

NetApp
September 11, 2024

Tabla de contenidos

Recuperación ante desastres de SAP HANA con Azure NetApp Files

TR-4891: Recuperación ante desastres de SAP HANA con Azure NetApp Files

Nils Bauer, NetApp Ralf Klahr, Microsoft

Estudios han demostrado que el tiempo de inactividad de las aplicaciones empresariales tiene un impacto negativo significativo en el negocio de las empresas. Además del impacto financiero, el tiempo de inactividad también puede dañar la reputación de la empresa, la moral del personal y la lealtad del cliente. Sorprendentemente, no todas las empresas cuentan con una normativa completa de recuperación ante desastres.

Al ejecutar SAP HANA en Azure NetApp Files (ANF), los clientes acceden a funciones adicionales que amplían y mejoran las funcionalidades integradas de protección de datos y recuperación ante desastres de SAP HANA. En esta sección de descripción general se explican estas opciones para ayudar a los clientes a seleccionar opciones que respalden sus necesidades empresariales.

Para desarrollar una normativa completa de recuperación ante desastres, los clientes deben comprender los requisitos de las aplicaciones empresariales y las capacidades técnicas que necesitan para la protección de datos y la recuperación ante desastres. En la figura siguiente se ofrece información general sobre la protección de datos.

[saphana dr y image2] | *saphana-dr-anf_image2.png*

Requisitos de las aplicaciones empresariales

Existen dos indicadores clave para las aplicaciones de negocio:

- El objetivo de punto de recuperación (RPO) o la pérdida máxima de datos tolerable
- El objetivo de tiempo de recuperación o el tiempo de inactividad máximo tolerable de las aplicaciones empresariales

Estos requisitos se definen por el tipo de aplicación utilizada y la naturaleza de los datos de su negocio. El objetivo de punto de recuperación y el objetivo de tiempo de recuperación pueden diferir si se protege contra fallos en una única región de Azure. También pueden diferir si se están preparando para desastres catastróficos como la pérdida de una región completa de Azure. Es importante evaluar los requisitos comerciales que definen los objetivos de tiempo y de puntos de recuperación, ya que estos requisitos tienen un impacto significativo en las opciones técnicas disponibles.

Alta disponibilidad

La infraestructura para SAP HANA, como máquinas virtuales, redes y almacenamiento, debe tener componentes redundantes para garantizar de que no exista un único punto de error. MS Azure ofrece redundancia para los diferentes componentes de la infraestructura.

Para proporcionar una alta disponibilidad en el lado de los recursos informáticos y las aplicaciones, los hosts SAP HANA en espera se pueden configurar para alta disponibilidad incorporada con un sistema host múltiple SAP HANA. Si se produce un error en un servidor o un servicio SAP HANA, el servicio SAP HANA conmuta al host de espera, lo que provoca un tiempo de inactividad de la aplicación.

Si no se aceptan tiempos de inactividad de las aplicaciones en caso de un fallo del servidor o de la aplicación, también puede utilizar la replicación del sistema SAP HANA como una solución de alta disponibilidad que permita la conmutación por error en un plazo muy breve. Los clientes de SAP utilizan la replicación de sistemas HANA no solo para gestionar la alta disponibilidad ante fallos no planificados, sino también para minimizar el tiempo de inactividad para operaciones planificadas, como actualizaciones de software HANA.

Daño lógico

La corrupción lógica puede deberse a errores de software, errores humanos o sabotaje. Desgraciadamente, la corrupción lógica no se puede hacer frente a menudo con soluciones estándares de alta disponibilidad y de recuperación ante desastres. Como resultado, dependiendo de la capa, la aplicación, el sistema de archivos o el almacenamiento donde se produjo el daño lógico, a veces no se pueden satisfacer los requisitos de objetivo de tiempo de recuperación y objetivo de punto de recuperación.

El peor de los casos es un daño lógico en una aplicación SAP. Las aplicaciones SAP suelen funcionar en un entorno en el que diferentes aplicaciones se comunican entre sí y intercambian datos. Por lo tanto, el enfoque recomendado no es restaurar ni recuperar un sistema SAP en el que se ha producido un daño lógico. Cuando se restaura el sistema a un momento específico antes de que se dañara, se perderán los datos, de modo que el objetivo de punto de recuperación será mayor que cero. Además, el entorno SAP ya no estaría sincronizado y necesitaría un postprocesamiento adicional.

En lugar de restaurar el sistema SAP, el mejor método consiste en intentar solucionar el error lógico dentro del sistema mediante el análisis del problema en un sistema de reparación independiente. El análisis de la causa raíz requiere la participación del proceso empresarial y el propietario de la aplicación. En esta situación, puede crear un sistema de reparación (un clon del sistema de producción) basado en los datos almacenados antes de que se produjera el daño lógico. Dentro del sistema de reparación, los datos necesarios se pueden exportar e importar al sistema de producción. Con este enfoque, no es necesario detener el sistema productivo y, en el mejor de los casos, no se pierden datos ni sólo una pequeña fracción de los datos.

> Los pasos necesarios para configurar un sistema de reparación son idénticos a los escenarios de prueba de recuperación ante desastres descritos en este documento. Por lo tanto, la solución de recuperación ante desastres descrita también puede ampliarse con facilidad para abordar el daño lógico.

Completos

Los backups se crean para habilitar la restauración y recuperación de diferentes conjuntos de datos de un momento específico. Normalmente, estos backups se guardan durante un par de días a unas semanas.

En función del tipo de daños, la restauración y la recuperación se pueden realizar con o sin pérdida de datos. Si el objetivo de punto de recuperación debe ser cero, incluso cuando se pierde el almacenamiento primario y de backup, el backup debe combinarse con la replicación de datos síncrona.

El objetivo de tiempo de recuperación para la restauración y la recuperación se define por el tiempo de restauración necesario, el tiempo de recuperación (incluido el inicio de la base de datos) y la carga de datos en la memoria. En el caso de bases de datos de gran tamaño y enfoques de backup tradicionales, el objetivo de tiempo de recuperación puede ser fácilmente de varias horas, lo cual puede que no sea aceptable. Para lograr un objetivo de tiempo de recuperación muy bajo, se debe combinar una copia de seguridad con una solución en espera en activo, que incluye la precarga de datos en la memoria.

Por el contrario, una solución de backup debe hacer frente a un daño lógico, ya que las soluciones de replicación de datos no pueden cubrir todo tipo de daños lógicos.

Replicación de datos síncrona o asíncrona

El RPO determina principalmente el método de replicación de datos que se debe usar. Si el RPO debe ser cero, incluso cuando se pierde el almacenamiento primario y backup, los datos se deben replicar de forma síncrona. Sin embargo, existen limitaciones técnicas para la replicación síncrona como la distancia entre dos regiones de Azure. En la mayoría de los casos, la replicación síncrona no es adecuada para distancias superiores a 100 km debido a la latencia, por lo que esto no es una opción para la replicación de datos entre regiones de Azure.

Si se admite un objetivo de punto de recuperación de mayor tamaño, es posible usar la replicación asíncrona a grandes distancias. En este caso, el RPO se define mediante la frecuencia de replicación.

Replicación del sistema HANA con o sin precarga de datos

El tiempo de inicio de una base de datos SAP HANA es mucho más largo que el de las bases de datos tradicionales, ya que debe cargarse una gran cantidad de datos en la memoria antes de que la base de datos pueda proporcionar el rendimiento esperado. Por lo tanto, una parte significativa del objetivo de tiempo de recuperación es el tiempo necesario para iniciar la base de datos. Con cualquier replicación basada en almacenamiento y con la replicación del sistema HANA sin carga previa de los datos, se debe iniciar la base de datos de SAP HANA en caso de conmutación al nodo de respaldo en el sitio de recuperación ante desastres.

La replicación del sistema SAP HANA ofrece un modo de operación en el que los datos se cargan de manera previa y se actualizan de manera continua en el host secundario. Este modo habilita unos valores de objetivo de tiempo de recuperación muy bajos, pero también requiere un servidor dedicado que solo se utilice para recibir los datos de replicación del sistema de origen.

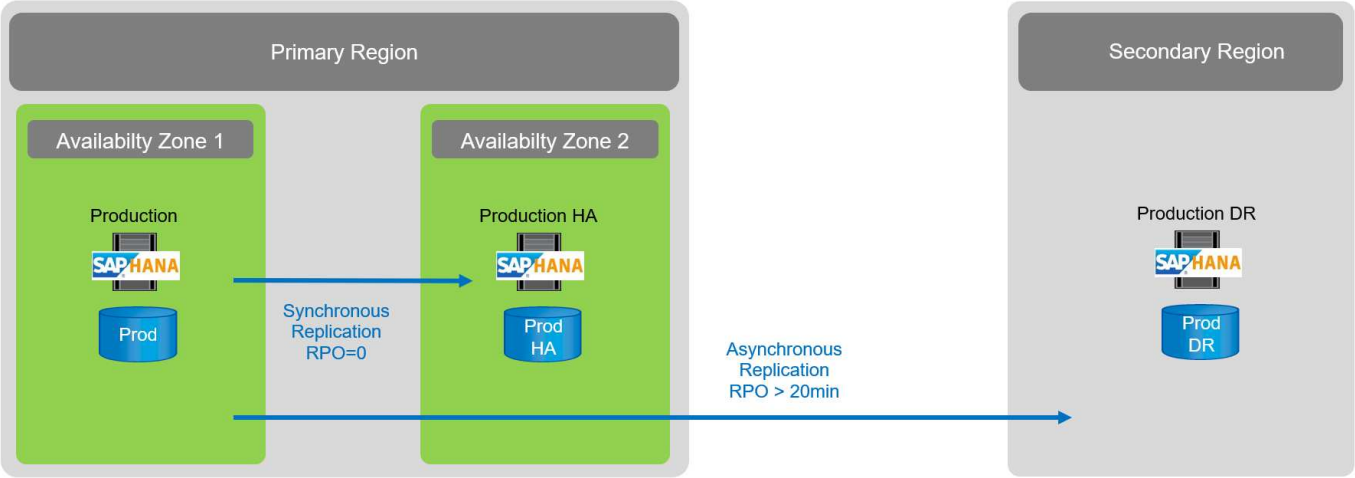
Comparación de soluciones de recuperación tras siniestros

Una completa solución de recuperación ante desastres debe permitir a los clientes recuperarse de un fallo completo del sitio principal. Por lo tanto, los datos deben transferirse a un sitio secundario y es necesario contar con una infraestructura completa para ejecutar los sistemas SAP HANA de producción necesarios en caso de un fallo en el sitio. En función de los requisitos de disponibilidad de la aplicación y del tipo de desastre del que se desea proteger, debe considerarse una solución de recuperación tras desastres de dos o tres instalaciones.

La figura siguiente muestra una configuración típica en la que los datos se replican de forma síncrona dentro de la misma región de Azure en una segunda zona de disponibilidad. La corta distancia le permite replicar los datos de forma síncrona para lograr un objetivo de punto de recuperación de cero (normalmente se utiliza para proporcionar alta disponibilidad).

Además, los datos también se replican de forma asíncrona en una región secundaria para protegerse frente a desastres, cuando la región primaria resulta afectada. El objetivo de punto de recuperación mínimo factible depende de la frecuencia de replicación de datos, limitada por el ancho de banda disponible entre la región primaria y la secundaria. Un objetivo de punto de recuperación típico mínimo es de 20 minutos a varias horas.

En este documento se tratan las distintas opciones de implantación de una solución de recuperación ante desastres en dos regiones.



Replicación de sistemas SAP HANA

La replicación de sistemas SAP HANA funciona en la capa de bases de datos. La solución se basa en un sistema SAP HANA adicional del sitio de recuperación ante desastres al que recibe los cambios del sistema principal. Este sistema secundario debe ser idéntico al sistema primario.

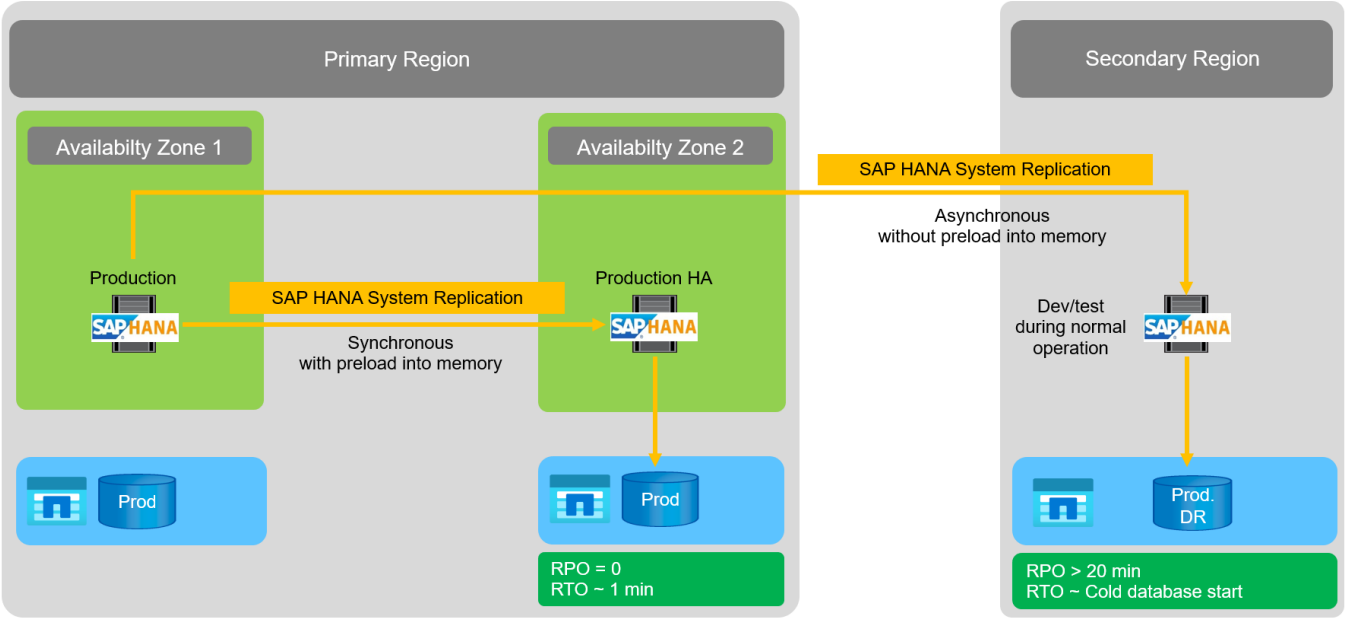
La replicación de sistemas SAP HANA se puede utilizar en uno de estos dos modos:

- Con carga previa de los datos en la memoria y un servidor dedicado en el sitio de recuperación de desastres:
  - El servidor se usa exclusivamente como host secundario SAP HANA System Replication.
  - Se pueden obtener valores de objetivo de tiempo de recuperación muy bajos porque los datos ya están cargados en la memoria y no se requiere inicio de la base de datos en caso de recuperación tras fallos.
- Sin carga previa de los datos en la memoria y en un servidor compartido en el sitio de recuperación ante desastres:
  - El servidor se comparte como secundario de replicación de sistemas SAP HANA y como sistema de desarrollo y pruebas.
  - El objetivo de tiempo de recuperación depende principalmente del tiempo necesario para iniciar la base de datos y cargar los datos en la memoria.

Para obtener una descripción completa de todas las opciones de configuración y escenarios de replicación, consulte "Guía de administración de SAP HANA".

La siguiente figura muestra la configuración de una solución de recuperación ante desastres a dos regiones con la replicación del sistema SAP HANA. La replicación síncrona con datos precargados en la memoria se utiliza para la alta disponibilidad local en la misma región de Azure, pero en diferentes zonas de disponibilidad. La replicación asíncrona sin carga previa de datos está configurada para la región de recuperación ante desastres remota.

La figura siguiente muestra la replicación del sistema SAP HANA.



Replicación de sistemas SAP HANA con carga previa de los datos en la memoria

Los valores de objetivo de tiempo de recuperación muy bajos en SAP HANA solo se pueden lograr con la replicación de sistemas SAP HANA con carga previa de los datos en la memoria. La operación de la replicación de sistemas SAP HANA con un servidor secundario dedicado en el sitio de recuperación de desastres permite obtener un valor de objetivo de tiempo de recuperación de aproximadamente 1 minuto o menos. Los datos replicados se reciben y precargados en la memoria del sistema secundario. Debido a este reducido tiempo de conmutación al nodo de respaldo, la replicación de sistemas SAP HANA también se suele utilizar en operaciones de mantenimiento que prácticamente no producen tiempos de inactividad, como actualizaciones de software HANA.

Normalmente, la replicación de sistemas SAP HANA está configurada para replicarse de forma síncrona cuando se elige la precarga de datos. La distancia máxima admitida para la replicación síncrona es de 100 km.

Replicación de sistemas SAP sin carga previa de los datos en la memoria

Para cumplir los requisitos de objetivo de tiempo de recuperación menos estrictos, puede usar la replicación de sistemas SAP HANA sin tener que preinstalada la carga de datos. En este modo operativo, los datos de la región de recuperación ante desastres no se cargan en la memoria. El servidor de la región de recuperación ante desastres se sigue utilizando para procesar la replicación del sistema SAP HANA que ejecuta todos los procesos SAP HANA necesarios. Sin embargo, la mayor parte de la memoria del servidor está disponible para ejecutar otros servicios, como los sistemas SAP HANA dev/test.

En caso de desastre, el sistema de prueba/desarrollo debe estar apagado, se debe iniciar la conmutación por error y los datos deben cargarse en la memoria. El objetivo de tiempo de recuperación de este enfoque de reserva en frío depende del tamaño de la base de datos y del rendimiento de lectura durante la carga del almacén de filas y columnas. Suponiendo que se leen los datos con un rendimiento de 1000 Mbps, la carga de 1 TB de datos debería tardar aproximadamente 18 minutos.

Recuperación ante desastres de SAP HANA con replicación entre regiones de ANF

LA replicación entre regiones DE ANF está integrada en ANF como solución de recuperación ante desastres mediante replicación de datos asíncrona. ANF Cross-Region Replication se configura mediante una relación de protección de datos entre dos volúmenes ANF en una región de Azure primaria y secundaria. ANF Cross-

Region Replication actualiza el volumen secundario mediante replicaciones delta por bloques eficientes. Las programaciones de actualización pueden definirse durante la configuración de replicación.

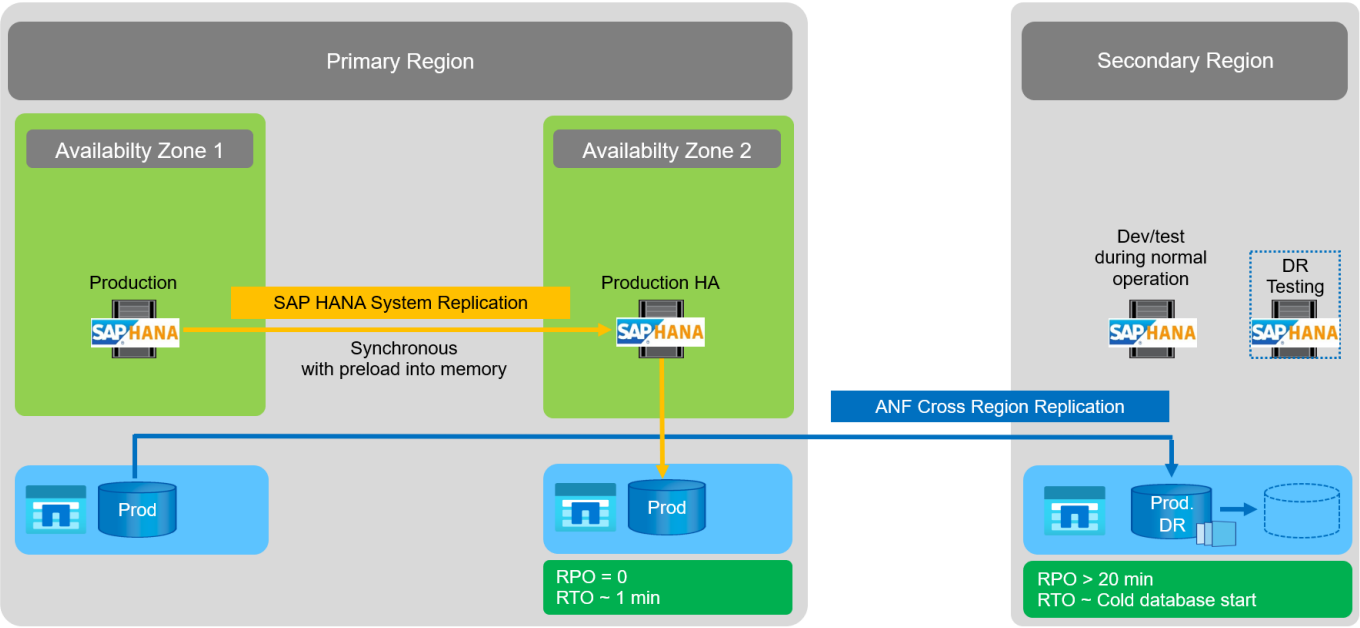
En la siguiente figura se muestra un ejemplo de solución de recuperación ante desastres en dos regiones mediante la replicación entre regiones de ANF. En este ejemplo, el sistema HANA está protegido con la replicación de sistema HANA en la región principal, como se explica en el capítulo anterior. La replicación a una región secundaria se realiza mediante la replicación de regiones cruzadas ANF. El RPO está definido por las opciones de programación y replicación.

El objetivo de tiempo de recuperación depende principalmente del tiempo necesario para iniciar la base de datos HANA en el sitio de recuperación ante desastres y cargar los datos en la memoria. Suponiendo que se leen los datos con una velocidad de transferencia de 1000 MB/s, la carga de 1 TB de datos llevaría aproximadamente 18 minutos. Dependiendo de la configuración de la replicación, es necesaria también la recuperación futura y se añadirá al valor de RTO total.

En el capítulo encontrará más información sobre las distintas opciones de configuración "Opciones de configuración para la replicación entre regiones con SAP HANA".

Los servidores en los sitios de recuperación de desastres pueden usarse como sistemas de prueba/desarrollo durante el funcionamiento normal. En caso de desastre, los sistemas de desarrollo y pruebas deben cerrarse y iniciarse como servidores de producción de recuperación ante desastres.

ANF Cross-Region Replication le permite probar el flujo de trabajo de recuperación ante desastres sin que ello afecte al RPO ni al RTO. Esto se logra mediante la creación de clones de volúmenes y la conexión de estos al servidor de pruebas de recuperación ante desastres.



Resumen de soluciones de recuperación tras siniestros

En la siguiente tabla se comparan las soluciones de recuperación ante desastres tratadas en esta sección y se destacan los indicadores más importantes.

Las principales conclusiones son las siguientes:

- Si se requiere un objetivo de tiempo de recuperación muy bajo, la única opción es la replicación de sistemas SAP HANA con precarga en memoria.

    - Se necesita un servidor dedicado en el centro de recuperación ante desastres para recibir los datos replicados y cargar los datos en la memoria.
- Además, la replicación del almacenamiento es necesaria para los datos que residen fuera de la base de datos (por ejemplo, archivos compartidos, interfaces, etc.).
- Si los requisitos de objetivo de tiempo de recuperación y objetivo de punto de recuperación son menos estrictos, la replicación entre regiones de ANF también se puede utilizar para:
    - Combine la replicación de datos que no sea de base de datos y de base de datos
    - Cubra otros casos de uso, como las pruebas de recuperación ante desastres y las actualizaciones de prueba y desarrollo.
    - Con la replicación de almacenamiento, el servidor del centro de recuperación ante desastres se puede usar como sistema de control de calidad o de prueba durante el funcionamiento normal.
- Es lógico que una combinación de la replicación de sistemas de SAP HANA como una solución de alta disponibilidad con RPO=0 y la replicación de almacenamiento a larga distancia aborde los diferentes requisitos.

La tabla siguiente muestra una comparación entre las soluciones de recuperación ante desastres.

	Replicación del almacenamiento	**Replicación de sistemas SAP HANA**	
	Replicación entre regiones	**Con precarga de datos**	**Sin precarga de datos**
RTO	De bajo a medio, en función del tiempo de inicio y la recuperación futura de la base de datos	Muy bajo	De bajo a medio, en función del tiempo de inicio de la base de datos
OBJETIVO DE PUNTO DE RECUPERACIÓN	Replicación asíncrona de RPO > 20 minutos	RPO > 20 minutos de replicación asíncrona RPO=0 replicación síncrona	RPO > 20 minutos de replicación asíncrona RPO=0 replicación síncrona
Los servidores del sitio de DR pueden usarse para desarrollo y pruebas	Sí	No	Sí
Replicación de datos que no forman parte de ninguna base de datos	Sí	No	No
Los datos de DR pueden usarse para actualizaciones o desarrollo y pruebas de sistemas	Sí	No	No
Pruebas de DR sin que ello afecte ni al RTO ni al RPO	Sí	No	No

Replicación entre regiones ANF con SAP HANA

Replicación entre regiones ANF con SAP HANA

La información de la aplicación independiente sobre la replicación entre regiones se puede encontrar en "Documentación de Azure NetApp Files | Microsoft Docs" en las secciones conceptos y procedimientos.

Opciones de configuración para replicación entre regiones con SAP HANA

La siguiente figura muestra las relaciones de replicación de volúmenes para un sistema SAP HANA mediante la replicación entre regiones de ANF. Con la replicación entre regiones de ANF, los datos HANA y el volumen compartido de HANA se deben replicar. Si solo se replica el volumen de datos de HANA, los valores típicos de RPO se encuentran en el intervalo de un día. Si se requieren valores de RPO menores, los backups de registros de HANA también se deben replicar para la recuperación futura.

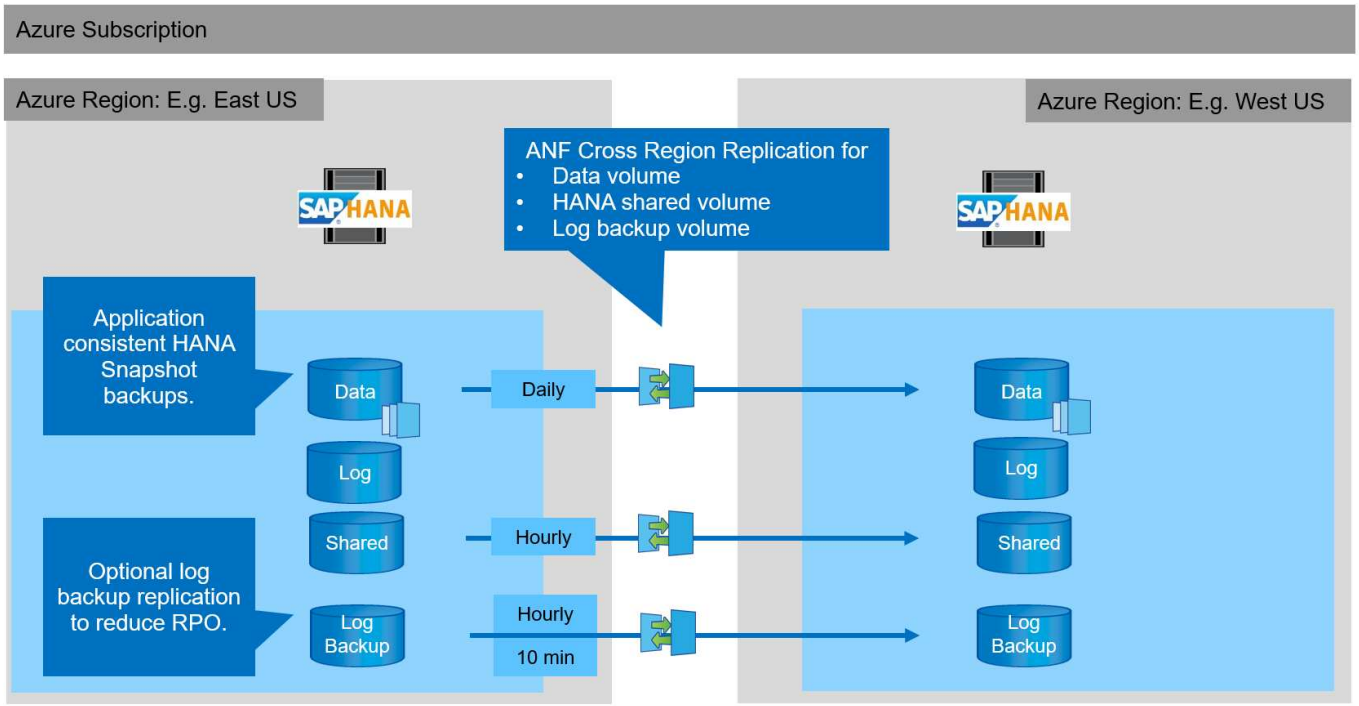
> El término «backup de registros» que se utiliza en este documento incluye el backup de registros y el backup de catálogo de backup de HANA. Se necesita el catálogo de backup de HANA para ejecutar operaciones de recuperación de reenvío.

> La siguiente descripción y la configuración del laboratorio se centran en la base de datos HANA. Otros archivos compartidos, por ejemplo, el directorio de transporte SAP se protegería y replicaría del mismo modo que el volumen compartido HANA.

Para permitir la recuperación de punto de guardado de HANA o una recuperación posterior mediante los backups de registros, es necesario crear backups de Snapshot de datos coherentes con las aplicaciones en el sitio principal para el volumen de datos de HANA. Esto se puede realizar, por ejemplo, con la herramienta de copia de seguridad ANF AzAcSnap (consulte también "Qué es una herramienta Snapshot coherente con las aplicaciones de Azure para Azure NetApp Files | Microsoft Docs"). Los backups de Snapshot creados en el sitio principal se replican a continuación en el site de recuperación ante desastres.

En caso de conmutación por error ante desastres, la relación de replicación debe estar rota, los volúmenes deben montarse en el servidor de producción de DR, y se debe recuperar la base de datos HANA, ya sea en el último punto de guardado de HANA o con recuperación directa mediante los backups de registro replicados. El capítulo "Recuperación tras fallos", describe los pasos necesarios.

La siguiente figura muestra las opciones de configuración de HANA para la replicación entre regiones.



Con la versión actual de la replicación entre regiones, sólo se pueden seleccionar programaciones fijas y el usuario no puede definir el tiempo real de actualización de la replicación. Los horarios disponibles son diarios, cada hora y cada 10 minutos. Con estas opciones de programación, tiene sentido usar dos configuraciones diferentes según los requisitos del objetivo de punto de recuperación: La replicación de volúmenes de datos sin la replicación de backup de registros y el backup de registros con programaciones diferentes, cada hora o cada 10 minutos. El objetivo de punto de recuperación más bajo posible es de unos 20 minutos. En la tabla siguiente se resumen las opciones de configuración y los valores resultantes de RPO y RTO.

	Replicación de volúmenes de datos	**Replicación de volumen de backup de datos y registros**	**Replicación de volumen de backup de datos y registros**
Volumen de datos de programación de CRR	Todos los días	Todos los días	Todos los días
Volumen de copia de seguridad del registro de programación de CRR	n.a.	Cada hora	10 min
Objetivo de punto de recuperación máximo	24 horas + programación Snapshot (p. ej., 6 horas)	1 hora	2 x 10 min
Objetivo de tiempo de recuperación máximo	Definido principalmente por el tiempo de inicio de HANA	tiempo de inicio de HANA + tiempo de recuperación	tiempo de inicio de HANA + tiempo de recuperación
Recuperación de avance	NA	Logs de las últimas 24 horas + programación Snapshot (por ejemplo, 6 horas)	Logs de las últimas 24 horas + programación Snapshot (por ejemplo, 6 horas)

Requisitos y prácticas recomendadas

Microsoft Azure no garantiza la disponibilidad de un tipo de máquina virtual específico tras la creación o al iniciar una máquina virtual no escrita En concreto, en caso de fallo de la región, muchos clientes pueden necesitar equipos virtuales adicionales en la región de recuperación ante desastres. Por lo tanto, se recomienda utilizar activamente una máquina virtual con el tamaño necesario para la conmutación por error ante desastres como un sistema de prueba o control de calidad en la región de recuperación ante desastres para asignar el tipo de equipo virtual necesario.

Para la optimización de los costes, es conveniente usar un pool de capacidad ANF con un nivel de rendimiento menor durante el funcionamiento normal. La replicación de datos no requiere alto rendimiento y, por consiguiente, podría utilizar un pool de capacidad con un nivel de rendimiento estándar. Para realizar pruebas de recuperación ante desastres o para realizar una conmutación al nodo de respaldo en caso de desastre, los volúmenes se deben mover a un pool de capacidad con un nivel de alto rendimiento.

Si un segundo pool de capacidad no es una opción, los volúmenes de destino de replicación deben configurarse en función de los requisitos de capacidad y no de los requisitos de rendimiento durante las operaciones normales. La cuota o el rendimiento (para calidad de servicio manual) pueden entonces adaptarse para las pruebas de recuperación ante desastres en caso de conmutación por error.

Para obtener más información, consulte "Requisitos y consideraciones sobre el uso de la replicación entre regiones de volumen de Azure NetApp Files | Microsoft Docs".

Configuración de laboratorio

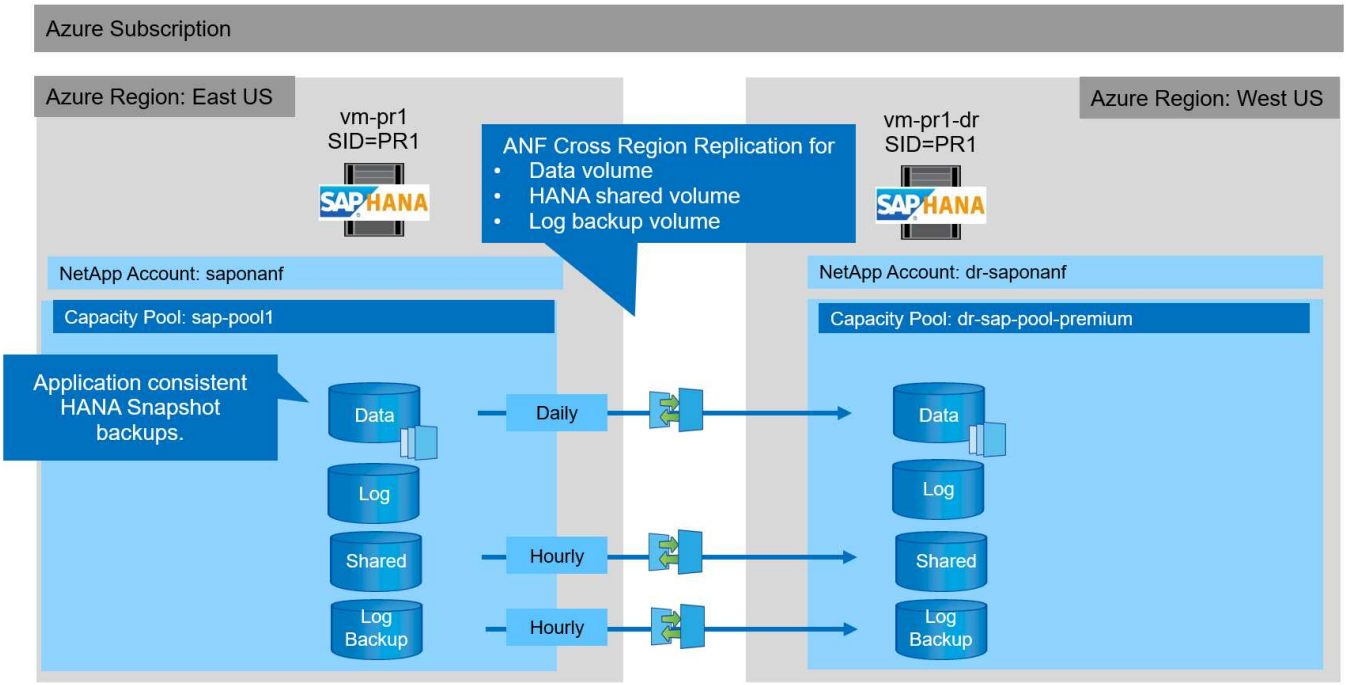
La validación de la solución se ha realizado con un sistema SAP HANA de un solo host. La herramienta de backup Microsoft AzAcSnap Snapshot para ANF se ha utilizado para configurar los backups de Snapshot coherentes con las aplicaciones de HANA. Se configuraron todos un volumen de datos diario, un backup de registros cada hora y una replicación de volúmenes compartidos. Las pruebas de recuperación ante desastres y la conmutación por error se validaron con un punto de guardado y con operaciones de recuperación adelante.

En la configuración de laboratorio se han utilizado las siguientes versiones de software:

- Sistema SAP HANA 2.0 SPS5 de host único con un solo cliente
- SUSE SLES PARA SAP 15 SP1
- AzAcSnap 5.0

Se ha configurado un pool de capacidad único con calidad de servicio manual en el sitio de recuperación ante desastres.

La siguiente figura muestra la configuración de laboratorio.

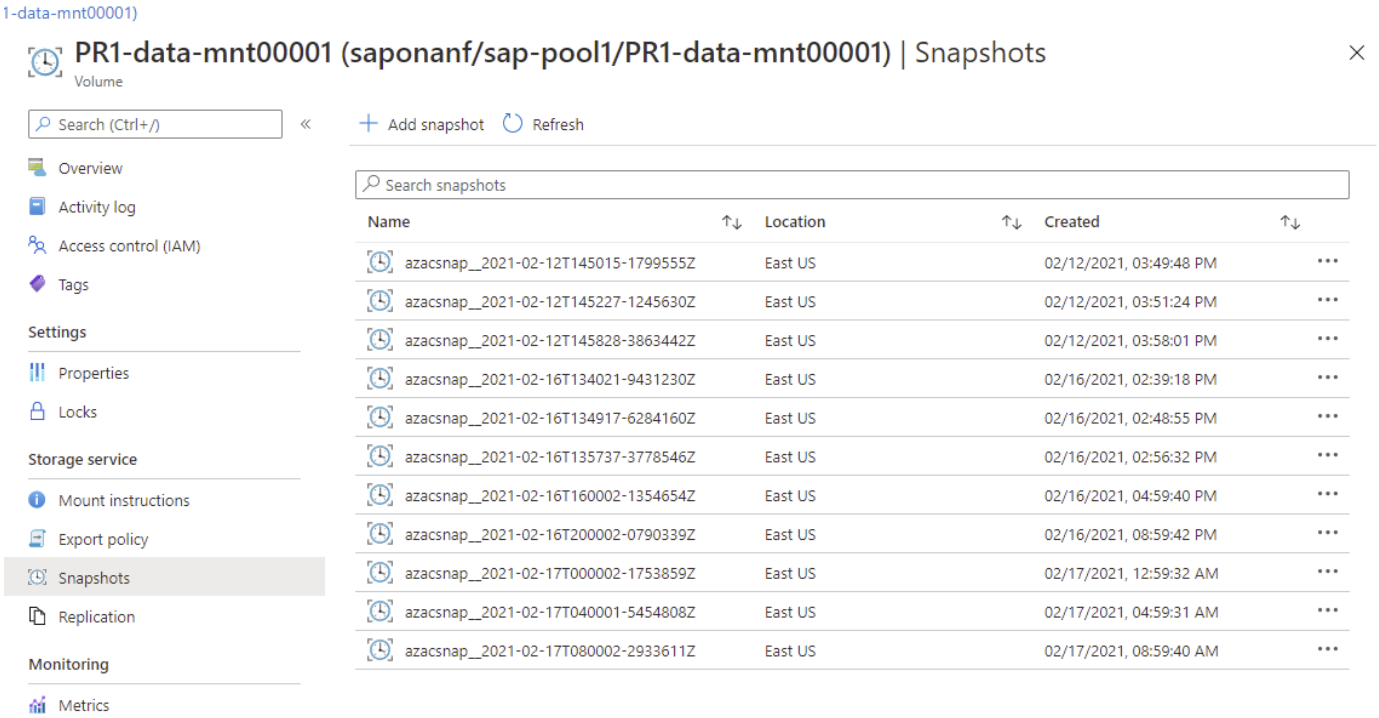


Configuración de backup de Snapshot con AzAcSnap

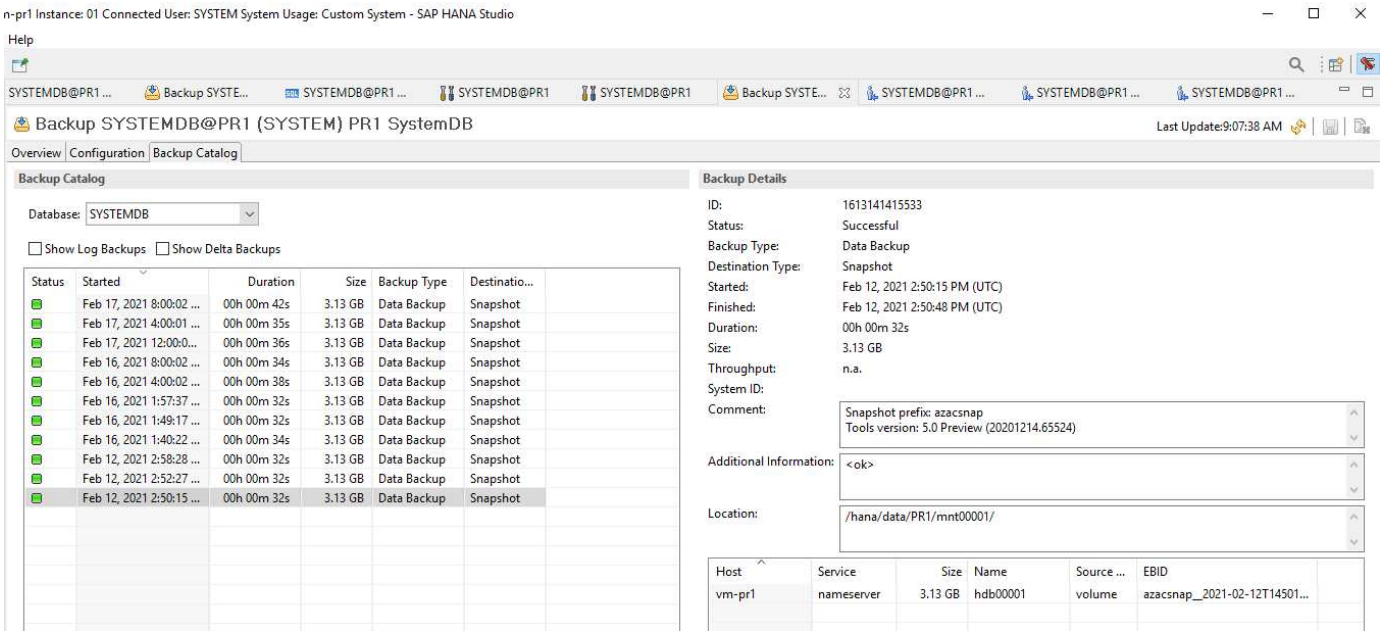
En el centro principal, AzAcSnap se configuró para crear backups snapshot coherentes con las aplicaciones del sistema HANA PR1. Estos backups Snapshot están disponibles en el volumen de datos ANF del sistema PR1 HANA y también están registrados en el catálogo de backup SAP HANA, tal y como se muestra en las dos figuras siguientes. Se programaron backups de Snapshot cada 4 horas.

Con la replicación del volumen de datos mediante la replicación entre regiones de ANF, estos backups de Snapshot se replican en el sitio de recuperación de desastres y se pueden usar para recuperar la base de datos de HANA.

La siguiente figura muestra los backups Snapshot del volumen de datos HANA.



La siguiente figura muestra el catálogo de backup de SAP HANA.



Pasos de configuración para la replicación entre regiones ANF

Para poder configurar la replicación de volúmenes, es necesario realizar algunos pasos de preparación en el centro de recuperación ante desastres.

- Una cuenta de NetApp debe estar disponible y configurada con la misma suscripción de Azure que el origen.
- Un pool de capacidad debe estar disponible y configurado con la cuenta de NetApp anterior.
- Debe haber una red virtual disponible y configurada.

- Dentro de la red virtual, debe haber una subred delegada disponible y configurada para utilizarse con ANF.

Los volúmenes de protección ahora se pueden crear para los datos de HANA, HANA compartido y el volumen de backup de registros de HANA. La siguiente tabla muestra los volúmenes de destino configurados en nuestra configuración de laboratorio.

> Para lograr la mejor latencia, los volúmenes se deben colocar cerca de las máquinas virtuales que ejecutan SAP HANA en caso de conmutación por error de desastre. Por lo tanto, es necesario el mismo proceso de fijación para los volúmenes de recuperación ante desastres que para cualquier otro sistema de producción de SAP HANA.

Volumen HANA	Origen	Destino	Programa de replicación
Volumen de datos HANA	PR1-data-mnt00001	PR1-data-mnt00001-sm-dest	Todos los días
Volumen compartido DE HANA	PR1-compartido	PR1-shared-sm-dest	Cada hora
Volumen de backup de catálogo/registro DE HANA	ahorackup	el más extraño	Cada hora

Para cada volumen, deben realizarse los siguientes pasos:

1. Cree un nuevo volumen de protección en el sitio de recuperación ante desastres:
   a. Proporcione el nombre del volumen, el pool de capacidad, la cuota y la información de red.
   b. Proporcione la información de acceso de volúmenes y del protocolo.
   c. Proporcione el ID del volumen de origen y una programación de replicación.
   d. Cree un volumen de destino.
2. Autorice la replicación en el volumen de origen.
   - Proporcione el ID del volumen objetivo.

Las siguientes capturas de pantalla muestran detalladamente los pasos de la configuración.

En el sitio de recuperación ante desastres, se crea un nuevo volumen de protección seleccionando Volumes y haciendo clic en Add Data Replication. En la pestaña Fundamentos, debe proporcionar la información sobre el nombre del volumen, el pool de capacidad y la red.

> La cuota del volumen se puede establecer en función de los requisitos de capacidad, ya que el rendimiento del volumen no afecta al proceso de replicación. En caso de conmutación por error de recuperación ante desastres, es necesario ajustar la cuota para cumplir los requisitos de rendimiento reales.

> Si el pool de capacidad se configuró con calidad de servicio manual, se puede configurar el rendimiento además de los requisitos de capacidad. Igual que lo anterior, puede configurar el rendimiento con un valor bajo durante el funcionamiento normal y aumentarlo en caso de recuperación ante desastres en caso de fallo.

Create a new protection volume

Basics | Protocol | Replication | Tags | Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. Learn more about Azure NetApp Files

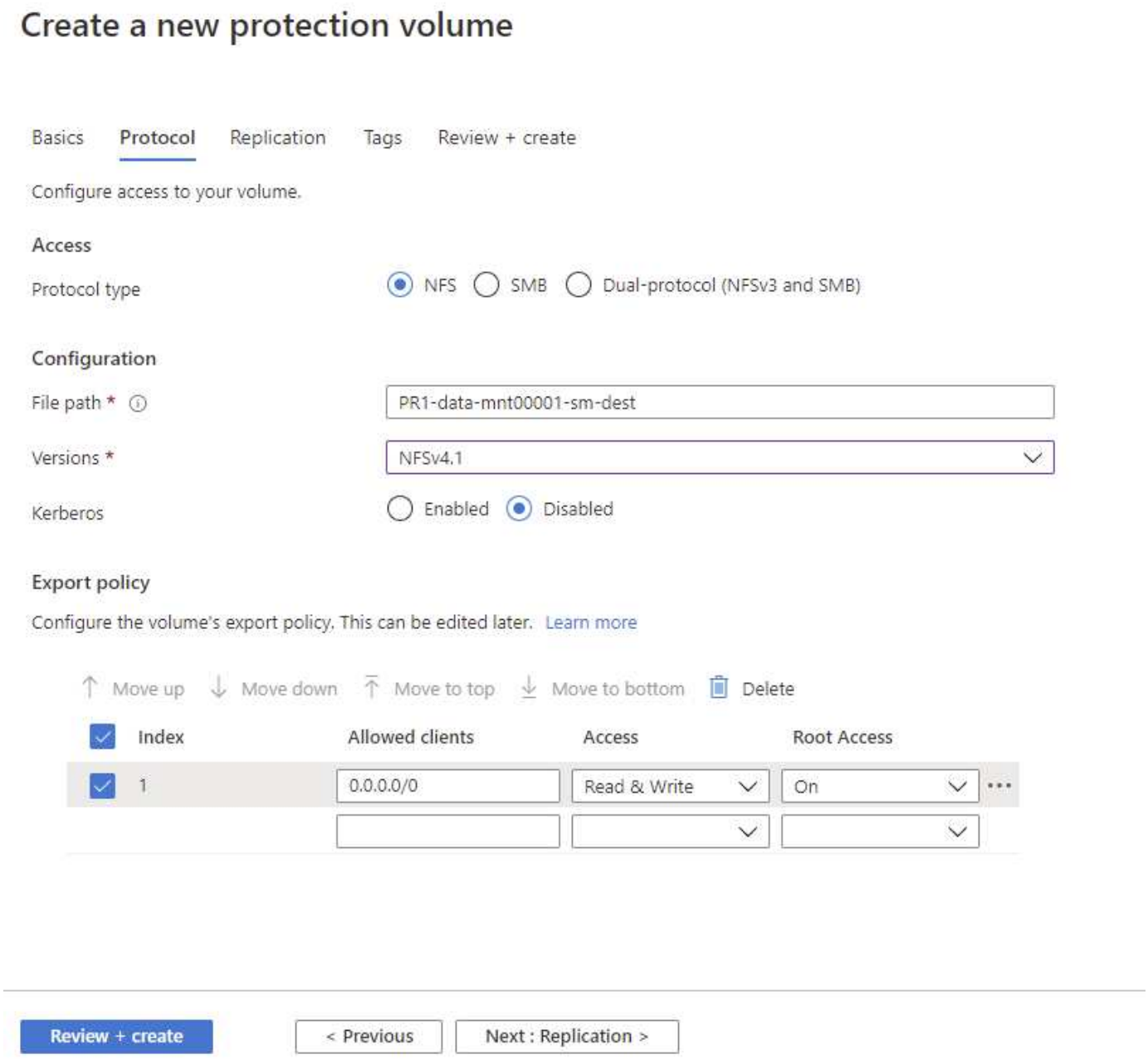
Volume details

Volume name *	PR1-data-mnt00001-sm-dest
Capacity pool *	dr-sap-pool1
Available quota (GiB)	4096 4 TiB
Quota (GiB) *	500 500 GiB
Virtual network *	dr-vnet (10.2.0.0/16,10.0.2.0/24) Create new
Delegated subnet *	default (10.0.2.0/28) Create new
Show advanced section	☐

Review + create | < Previous | Next : Protocol >

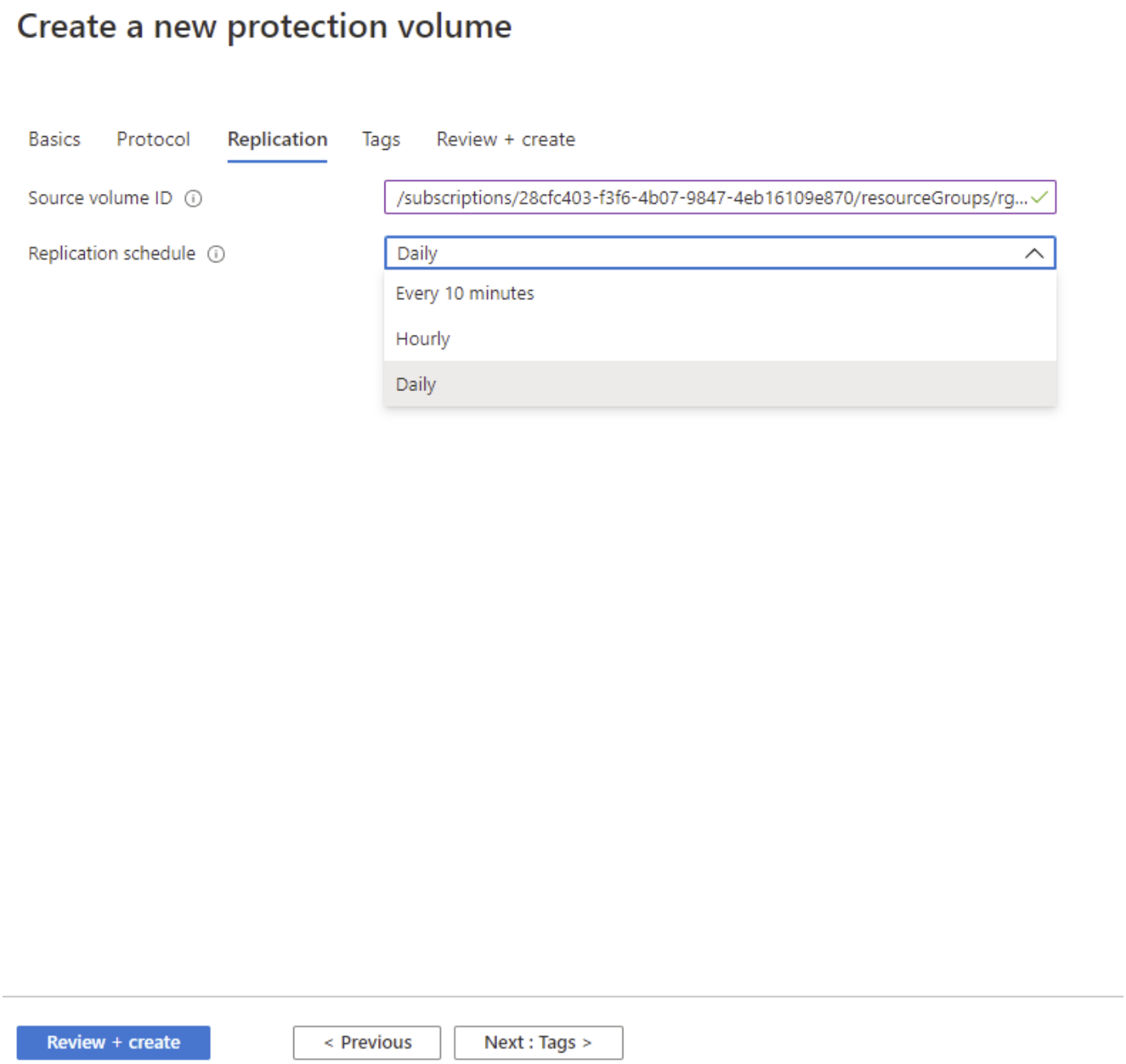
En la pestaña Protocol, debe proporcionar el protocolo de red, la ruta de red y la política de exportación.

> El protocolo debe ser el mismo que el protocolo utilizado para el volumen de origen.



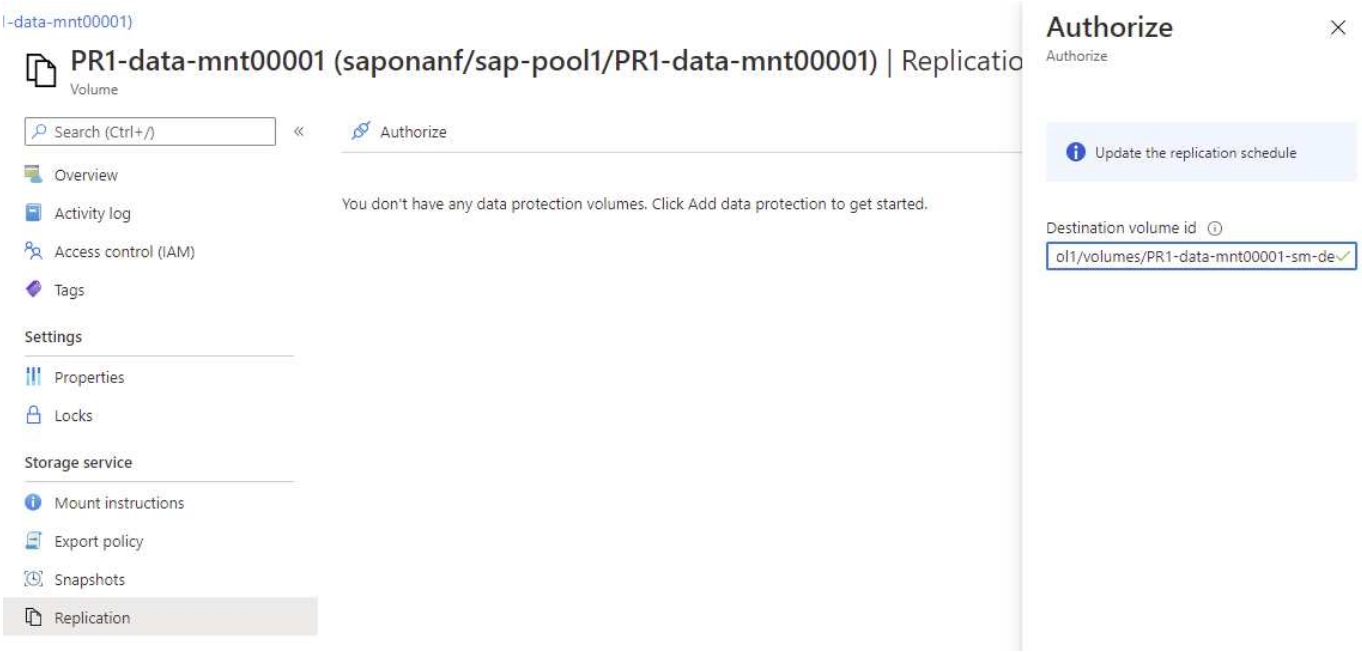
En la pestaña Replication, debe configurar el ID del volumen de origen y la programación de replicación. Para la replicación del volumen de datos, configuramos un programa de replicación diario para nuestra configuración de laboratorio.

> El ID del volumen de origen se puede copiar desde la pantalla Propiedades del volumen de origen.



Como paso final, se debe autorizar la replicación en el volumen de origen mediante el ID del volumen de destino.

> El ID del volumen de destino se puede copiar desde la pantalla Propiedades del volumen de destino.



Se deben realizar los mismos pasos para el volumen de backup compartido de HANA y de registros.

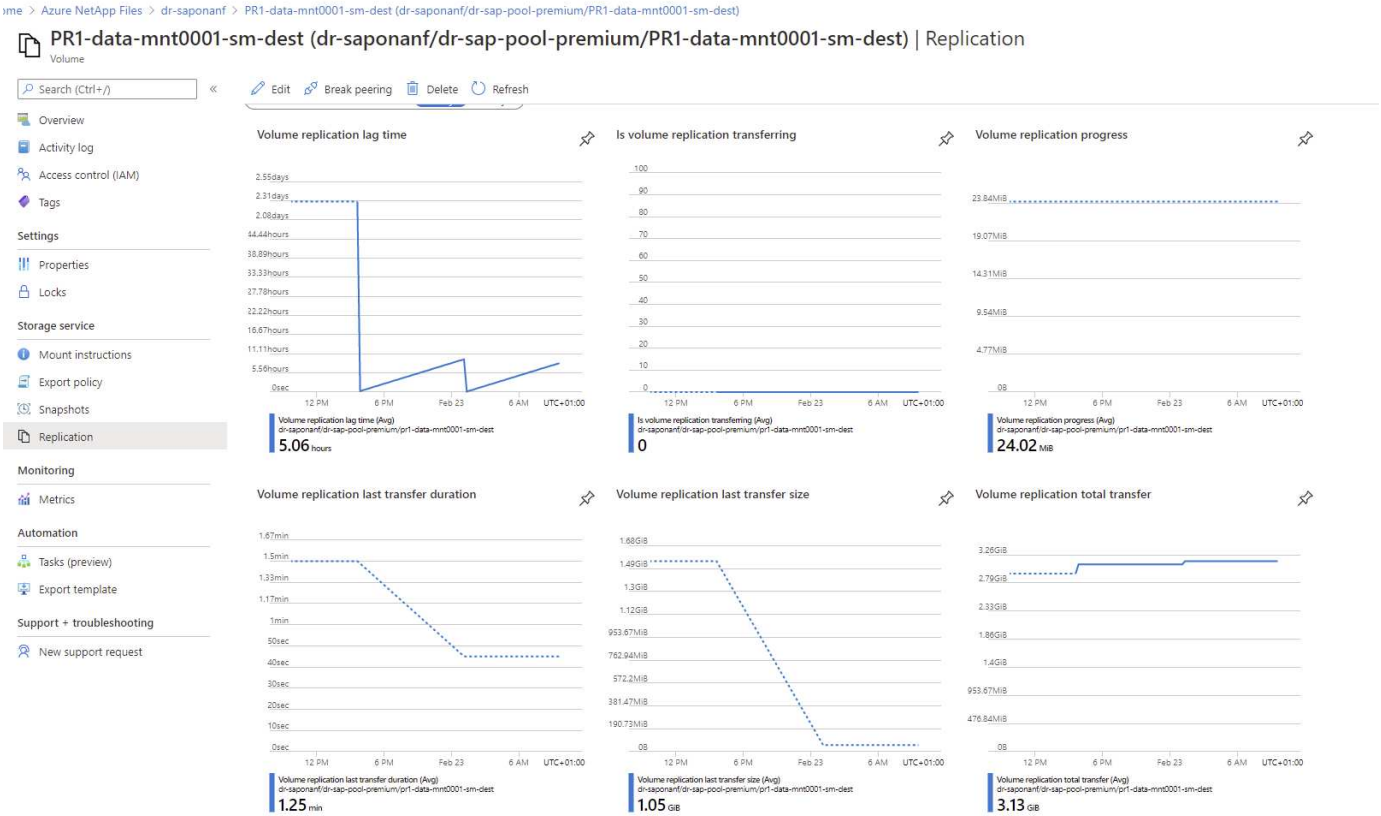
Monitorización de la replicación entre regiones de ANF

Las tres siguientes capturas de pantalla muestran el estado de replicación de los datos, el backup de registros y los volúmenes compartidos.

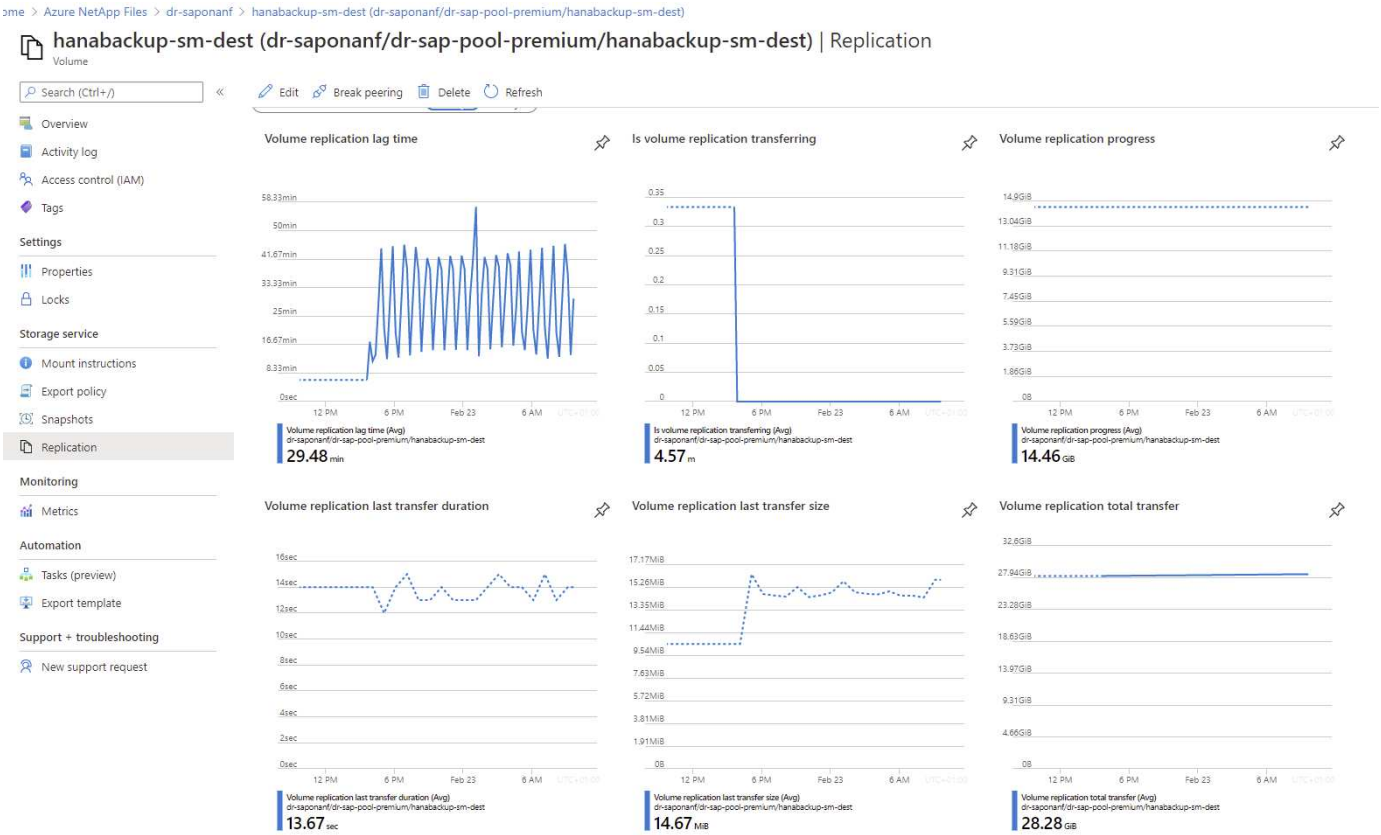
El tiempo de retraso de replicación de volúmenes es un valor útil para entender las expectativas de RPO. Por ejemplo, la replicación del volumen de backup de registros muestra un tiempo de demora máximo de 58 minutos, lo que significa que el objetivo de punto de recuperación máximo tiene el mismo valor.

La duración de la transferencia y el tamaño de la transferencia proporcionan información valiosa sobre los requisitos de ancho de banda y cambian la tasa del volumen replicado.

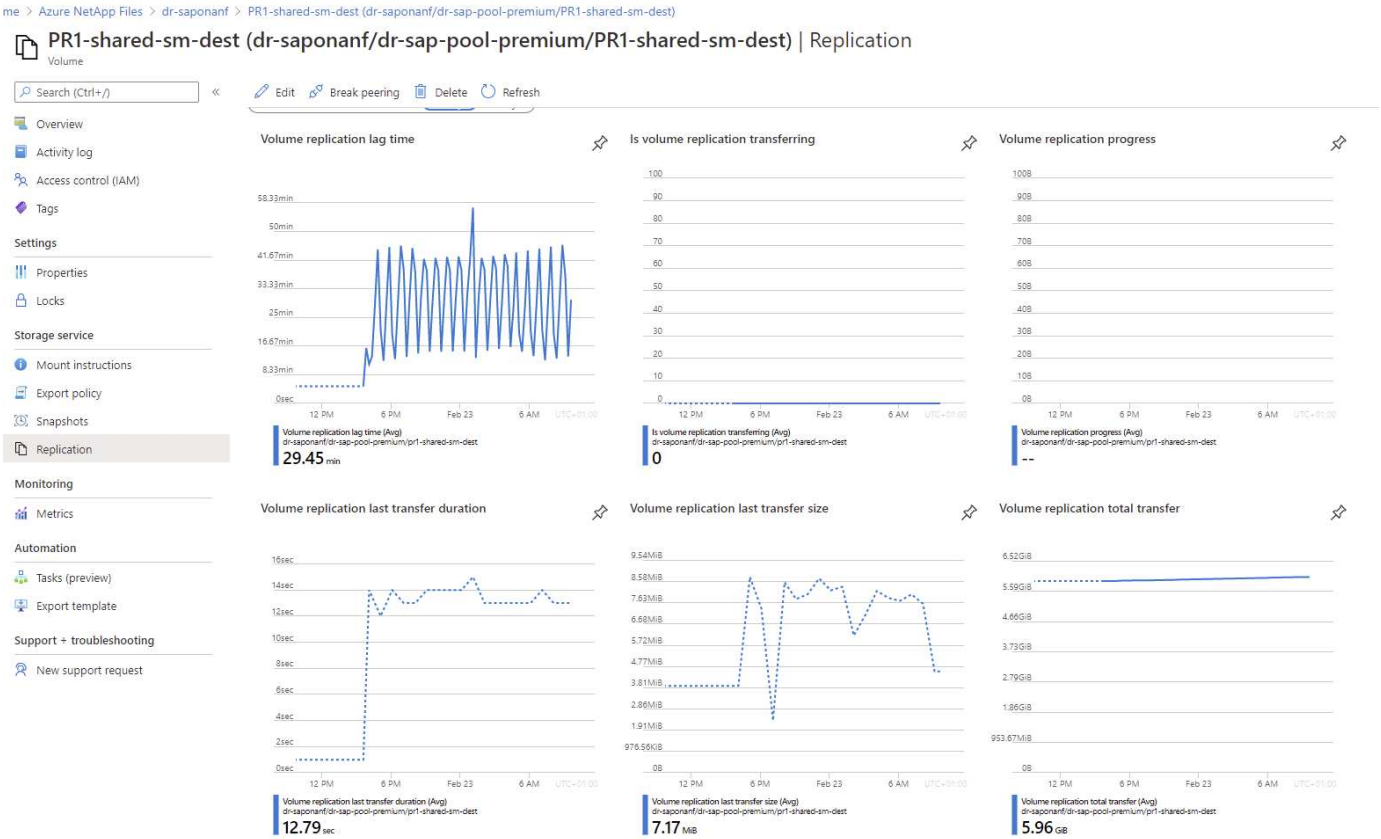
La siguiente captura de pantalla muestra el estado de replicación del volumen de datos HANA.



La siguiente captura de pantalla muestra el estado de replicación del volumen de backup de registros de HANA.



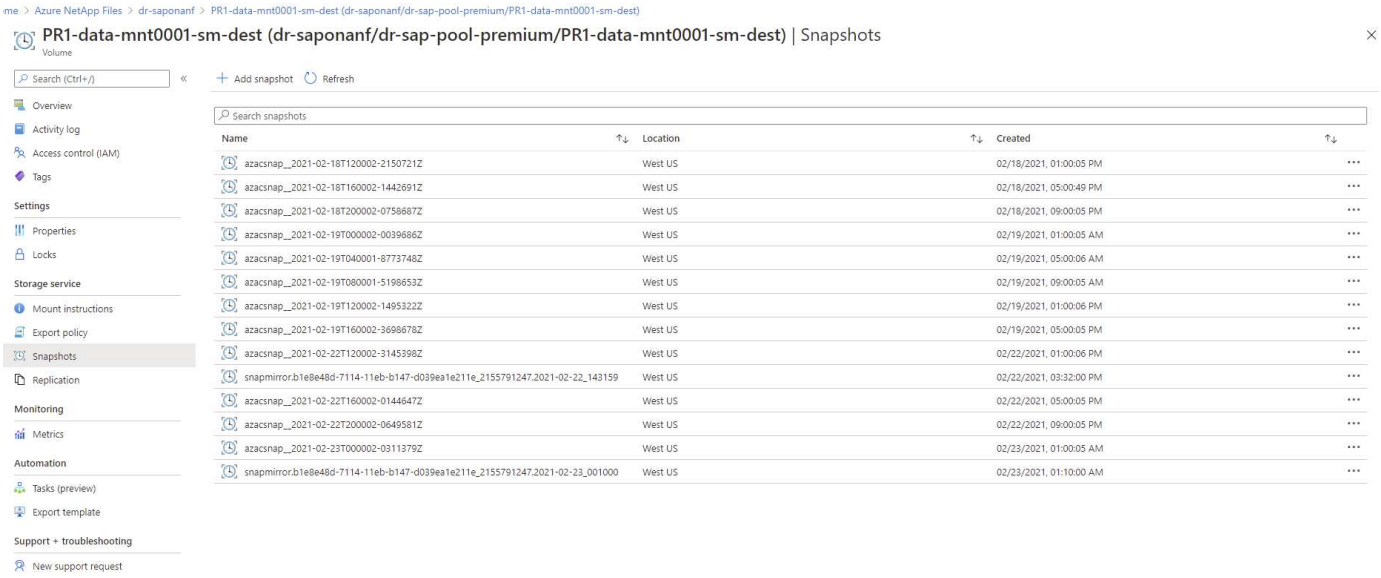
La siguiente captura de pantalla muestra el estado de replicación del volumen compartido de HANA.



Backups Snapshot replicados

Con cada actualización de replicación del volumen de origen al de destino, todos los cambios de bloques que ocurrieron entre la última actualización y la actual se replican en el volumen de destino. También incluye las copias de Snapshot, que se crearon en el volumen de origen. La siguiente captura de pantalla muestra las instantáneas disponibles en el volumen de destino. Como ya hemos visto, cada una de las copias Snapshot creadas por la herramienta AzAcSnap son imágenes consistentes con las aplicaciones de la base de datos HANA que se pueden utilizar para ejecutar un punto de guardado o una recuperación futura.

> En el volumen de origen y destino, también se crean copias Snapshot de SnapMirror, que se utilizan para realizar operaciones de actualización de sincronización y replicación. Estas copias Snapshot no son coherentes con las aplicaciones desde el punto de vista de la base de datos de HANA; solo se pueden utilizar las copias snapshot coherentes con las aplicaciones creadas a través de AzaCSnap para las operaciones de recuperación de HANA.



Pruebas de recuperación ante desastres

Pruebas de recuperación ante desastres

Para implementar una estrategia de recuperación ante desastres eficaz, es necesario probar el flujo de trabajo requerido. Las pruebas demuestran si la estrategia funciona y si la documentación interna es suficiente, y también permiten a los administradores entrenar sobre los procedimientos necesarios.

ANF Cross-Region Replication permite realizar pruebas de recuperación ante desastres sin poner en riesgo el objetivo de tiempo de recuperación ni el objetivo de punto de recuperación. Es posible realizar pruebas de recuperación ante desastres sin interrumpir la replicación de datos.

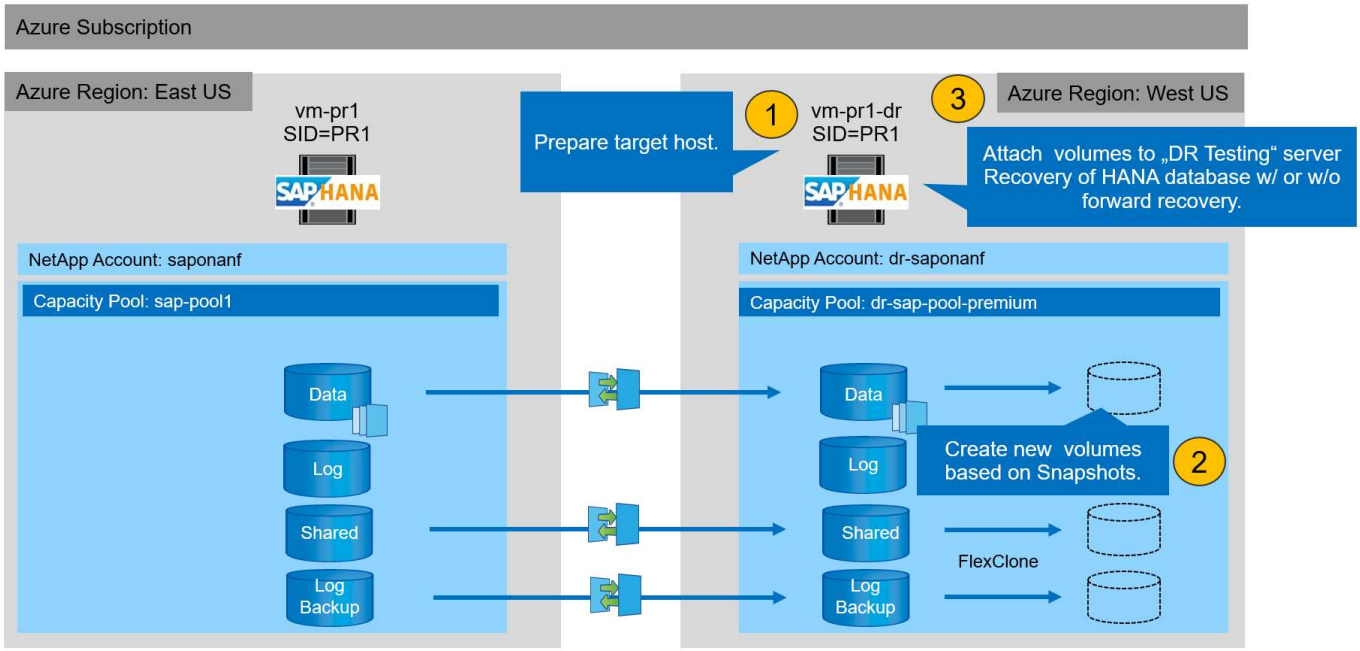
El flujo de trabajo de pruebas de recuperación ante desastres aprovecha el conjunto de funciones de ANF para crear nuevos volúmenes basados en backups de Snapshot existentes en el destino de recuperación ante desastres. Consulte "Cómo funcionan las copias Snapshot de Azure NetApp Files | Microsoft Docs".

Dependiendo de si la replicación de backup de registros forma parte o no de la configuración de recuperación ante desastres, los pasos para la recuperación ante desastres son ligeramente diferentes. En esta sección se describen las pruebas de recuperación ante desastres para la replicación solo de backup de datos y para la replicación de volúmenes de datos combinada con la replicación de volúmenes de backup de registros.

Para realizar pruebas de recuperación ante desastres, complete los siguientes pasos:

1. Prepare el host de destino.
2. Crear nuevos volúmenes basados en backups de Snapshot en el centro de recuperación ante desastres.
3. Monte los nuevos volúmenes en el host de destino.
4. Recupere la base de datos HANA.
    - Únicamente recuperación del volumen de datos.
    - Recuperación posterior mediante backups de registros replicados.

Las siguientes subsecciones describen estos pasos con detalle.



Prepare el host de destino

En esta sección se describen los pasos de preparación necesarios en el servidor que se usa para la prueba de conmutación al nodo de respaldo de recuperación ante desastres.

Durante el funcionamiento normal, el host de destino se suele utilizar para otros fines, por ejemplo, como un sistema de prueba o control de calidad de HANA. Por lo tanto, la mayoría de estos pasos deben ejecutarse cuando se realicen las pruebas de conmutación al nodo de respaldo de desastre. Por otro lado, los archivos de configuración pertinentes, como `/etc/fstab` y.. `/usr/sap/sapservices`, puede prepararse y luego ponerse en producción simplemente copiando el archivo de configuración. El procedimiento de pruebas de recuperación ante desastres garantiza que los archivos de configuración pertinentes preparados estén configurados correctamente.

La preparación del host de destino también incluye apagar el sistema de prueba o control de calidad de HANA, así como detener todos los servicios que usen `systemctl stop sapinit`.

El nombre de host y la dirección IP del servidor de destino

El nombre de host del servidor de destino debe ser idéntico al nombre de host del sistema de origen. La dirección IP puede ser diferente.

> Se debe establecer una correcta delimitación del servidor de destino para que no pueda comunicarse con otros sistemas. Si no se cuenta con una delimitación adecuada, el sistema de producción clonado puede intercambiar datos con otros sistemas de producción, lo que puede dar lugar a datos dañados lógicamente.

Instale el software necesario

El software del agente de host SAP debe instalarse en el servidor de destino. Para obtener más información, consulte "Agente host SAP" En el portal de ayuda de SAP.

Si el host se usa como sistema de control de calidad o prueba de HANA, el software del agente de host SAP ya está instalado.

Configurar usuarios, puertos y servicios SAP

Los usuarios y los grupos requeridos para la base de datos SAP HANA deben estar disponibles en el servidor de destino. Normalmente, se utiliza la gestión central de usuarios; por lo tanto, no es necesario realizar ningún paso de configuración en el servidor de destino. Los puertos necesarios para la base de datos HANA deben configurarse en los hosts objetivo. La configuración se puede copiar desde el sistema de origen copiando el `/etc/services` archivo al servidor de destino.

Las entradas de servicios SAP necesarias deben estar disponibles en el host de destino. La configuración se puede copiar desde el sistema de origen copiando el `/usr/sap/sapservices` archivo al servidor de destino. El siguiente resultado muestra las entradas necesarias para la base de datos SAP HANA que se utilizan en la configuración de laboratorio.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

Prepare el volumen de registro de HANA

Debido a que el volumen de registro de HANA no forma parte de la replicación, debe existir un volumen de registro vacío en el host de destino. El volumen de registro debe incluir los mismos subdirectorios que el sistema HANA de origen.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Preparar el volumen de backup de registros

Dado que el sistema de origen está configurado con un volumen separado para los backups de registros de HANA, debe haber un volumen de backup de registros también disponible en el host de destino. Es necesario configurar y montar un volumen para los backups de registros en el host objetivo.

Si la replicación de volúmenes de backup de registros forma parte de la configuración de recuperación ante desastres, un nuevo volumen basado en una snapshot se monta en el host de destino y no es necesario preparar un volumen de backup de registros adicional.

Preparar los montajes del sistema de archivos

En la siguiente tabla se muestran las convenciones de nomenclatura utilizadas en la configuración del laboratorio. Los nombres de los volúmenes nuevos del sitio de recuperación ante desastres se incluyen en `/etc/fstab`. Estos nombres de volúmenes se utilizan en el paso de creación de volúmenes en la siguiente sección.

Volúmenes PR1 HANA	Nuevos volúmenes y subdirectorios en el centro de recuperación ante desastres	Punto de montaje en el host de destino
Volumen de datos	PR1-data-mnt00001-sm-dest-clone	/hana/data/PR1/mnt00001
Volumen compartido	PR1-shared-sm-dest-clone/shared-sm-dest-clone/usr-SAP-PR1	/hana/shared /usr/SAP/PR1
Volumen de backup de registros	clon más extraño del hanabackup-sm-dest	/hanabackup

Los puntos de montaje indicados en esta tabla deben crearse en el host objetivo.

Aquí están los requisitos `/etc/fstab` entradas.

```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest-clone    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

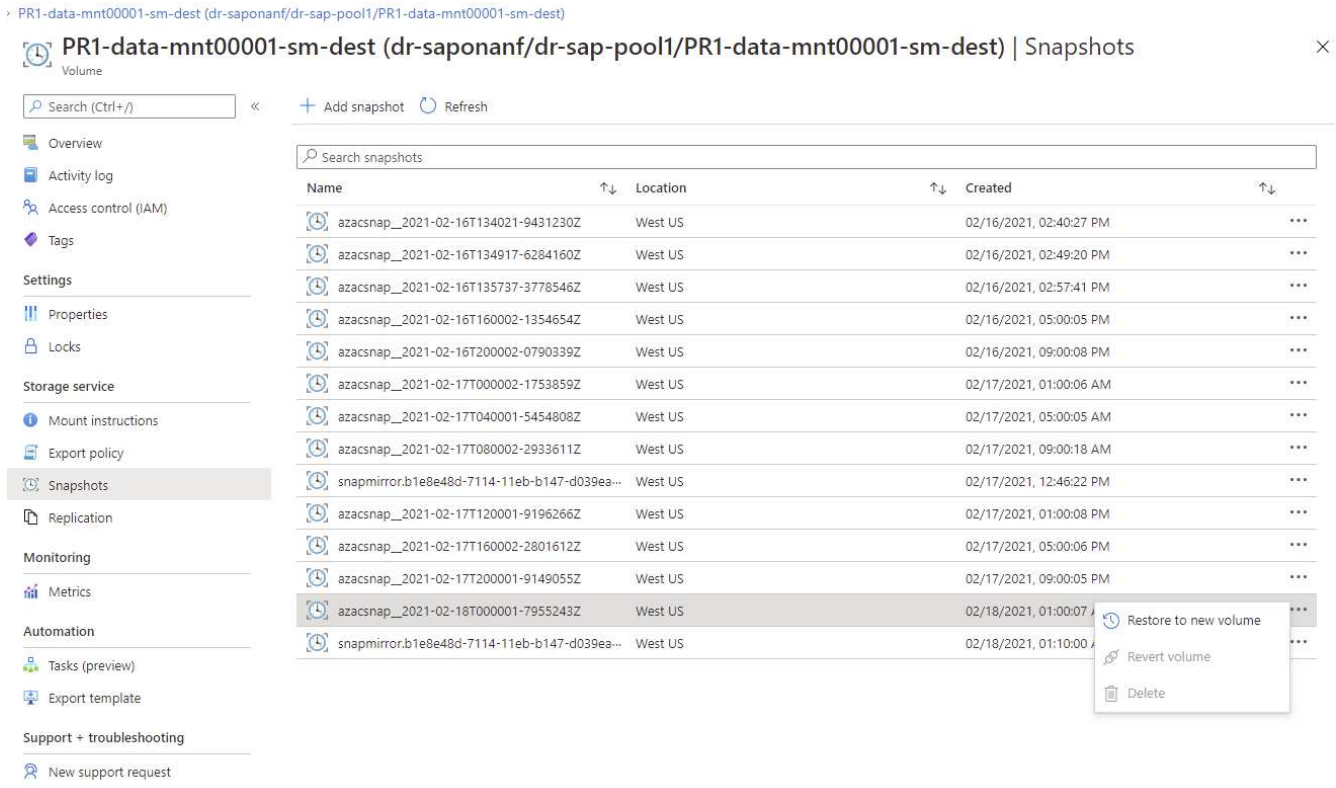
Crear nuevos volúmenes basados en backups de snapshots en el centro de recuperación ante desastres

Según la configuración de recuperación ante desastres (con o sin replicación de backup de registros), deben crearse dos o tres volúmenes nuevos basados en backups de snapshots. En ambos casos, se debe crear un nuevo volumen de datos y el volumen

compartido de HANA.

Es necesario crear un nuevo volumen del volumen de backup de registros si también se replican los datos del backup de registros. En nuestro ejemplo, el volumen de backup de datos y registros se ha replicado en el centro de recuperación ante desastres. Los siguientes pasos utilizan el Portal de Azure.

1. Se selecciona uno de los backups de snapshot consistentes con las aplicaciones como origen del nuevo volumen del volumen de datos de HANA. La opción Restore to New Volume está seleccionada para crear un nuevo volumen según el backup de snapshot.



2. El nuevo nombre de volumen y la cuota se deben proporcionar en la interfaz de usuario de.

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (d

Create a volume

Basics | Protocol | Tags | Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. Learn more about Azure NetApp Files

Volume details

Volume name *	PR1-data-mnt00001-sm-dest-clone
Restoring from snapshot	azacsnap__2021-02-18T000001-7955243Z
Available quota (GiB)	2096 2.05 TiB
Quota (GiB) *	500 500 GiB
Virtual network	dr-vnet (10.2.0.0/16,10.0.2.0/24)
Delegated subnet	default (10.0.2.0/28)
Show advanced section	☐

3. En la ficha de protocolo, se configuran la ruta de acceso y la directiva de exportación del archivo.

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (d

Create a volume

Basics | **Protocol** | Tags | Review + create

Configure access to your volume.

Access

Protocol type: (•) NFS ( ) SMB ( ) Dual-protocol (NFSv3 and SMB)

Configuration

File path * ⓘ: PR1-data-mnt00001-sm-dest-clone

Versions: NFSv4.1

Kerberos: ( ) Enabled (•) Disabled

Export policy

Configure the volume's export policy. This can be edited later. Learn more

Move up | Move down | Move to top | Move to bottom | Delete

Index	Allowed clients	Access	Root Access
1	0.0.0.0/0	Read & Write	On

4. La pantalla Crear y revisar resume la configuración.

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (dr-sapon

Create a volume

Validation passed

Basics Protocol Tags **Review + create**

Basics

Subscription	Pay-As-You-Go
Resource group	dr-rg-sap
Region	West US
Volume name	PR1-data-mnt00001-sm-dest-clone
Capacity pool	dr-sap-pool1
Service level	Standard
Quota	500 GiB

Networking

Virtual network	dr-vnet (10.2.0.0/16,10.0.2.0/24)
Delegated subnet	default (10.0.2.0/28)

Protocol

Protocol	NFSv4.1
File path	PR1-data-mnt00001-sm-dest-clone

5. Ahora se ha creado un nuevo volumen según el backup de snapshot de HANA.

dr-saponanf | Volumes
NetApp account

Search (Ctrl+/)

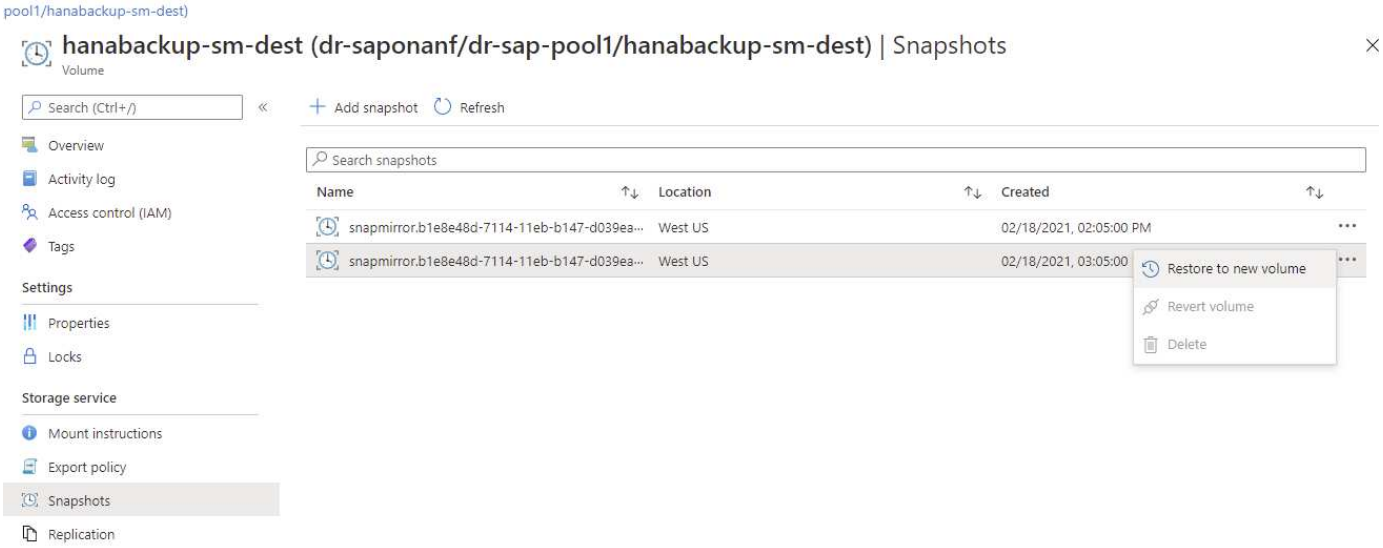
Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Azure NetApp Files
Active Directory connections
Storage service
Capacity pools
Volumes
Data protection
Snapshot policies
Automation
Tasks (preview)
Export template
Support + troubleshooting
New support request

Add volume | Add data replication | Refresh

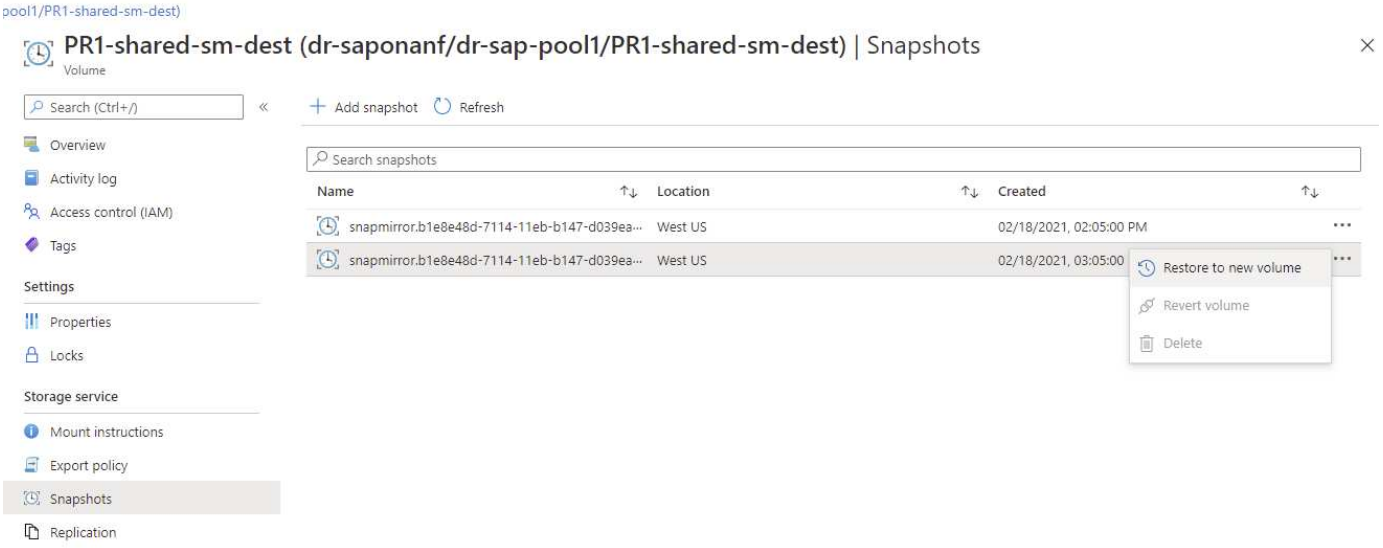
Search volumes

Name	Quota	Protocol type	Mount path	Service level	Capacity pool
hanabackup-sm-dest	1000 GiB	NFSv3	10.0.2.4:/hanabackup-sm-dest	Standard	dr-sap-pool1
PR1-data-mnt00001-sm-dest	500 GiB	NFSv4.1	10.0.2.4:/PR1-data-mnt00001-s	Standard	dr-sap-pool1
PR1-data-mnt00001-sm-dest-clone	500 GiB	NFSv4.1	10.0.2.4:/PR1-data-mnt00001-s	Standard	dr-sap-pool1
PR1-log-mnt00001-dr	250 GiB	NFSv4.1	10.0.2.4:/PR1-log-mnt00001-dr	Standard	dr-sap-pool1
PR1-shared-sm-dest	250 GiB	NFSv4.1	10.0.2.4:/PR1-shared-sm-dest	Standard	dr-sap-pool1

Ahora deben realizarse los mismos pasos para el volumen de backup compartido de HANA y de registros, como se muestra en las siguientes dos capturas de pantalla. Como no se han creado otras copias de Snapshot para el volumen de backup compartido y de registros de HANA, se debe seleccionar la copia de Snapshot de SnapMirror más reciente como origen del nuevo volumen. Se trata de datos no estructurados, y la copia Snapshot de SnapMirror puede utilizarse para este caso práctico.



La siguiente captura de pantalla muestra el volumen compartido de HANA restaurado en el nuevo volumen.



Si se utiliza un pool de capacidad con un nivel de bajo rendimiento, los volúmenes se deben mover ahora a un pool de capacidad que ofrezca el rendimiento requerido.

Ahora están disponibles los tres volúmenes nuevos y se pueden montar en el host de destino.

Monte los nuevos volúmenes en el host de destino

Los nuevos volúmenes ahora pueden montarse en el host de destino, según el `/etc/fstab` archivo creado anteriormente.

```
vm-pr1:~ # mount -a
```

El siguiente resultado muestra los sistemas de archivos necesarios.

```
vm-pr1:/hana/data/PR1/mnt00001/hdb00001 # df
Filesystem                                          1K-blocks     Used
Available Use% Mounted on
devtmpfs                                              8190344        8
8190336   1% /dev
tmpfs                                                12313116        0
12313116   0% /dev/shm
tmpfs                                                 8208744    17292
8191452   1% /run
tmpfs                                                 8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                            29866736  2438052
27428684   9% /
/dev/sda3                                             1038336   101520
936816  10% /boot
/dev/sda2                                              524008     1072
522936   1% /boot/efi
/dev/sdb1                                            32894736    49176
31151560   1% /mnt
tmpfs                                                 1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-log-mnt00001-dr                  107374182400      256
107374182144   1% /hana/log/PR1/mnt00001
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone      107377026560  6672640
107370353920   1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096
107365844224   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096
107365844224   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone             107379429120 35293440
107344135680   1% /hanabackup
```

Recuperación de base de datos de HANA

A continuación se muestran los pasos para la recuperación de la base de datos HANA

Inicie los servicios SAP necesarios.

```
vm-pr1:~ # systemctl start sapinit
```

El siguiente resultado muestra los procesos necesarios.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

Los siguientes subapartados describen el proceso de recuperación con y sin recuperación futura mediante los backups de registros replicados. La recuperación se ejecuta mediante el script de recuperación de HANA para la base de datos del sistema y los comandos hdbsql para la base de datos del arrendatario.

Recuperación en el último punto de guardado de backup de volumen de datos de HANA

La recuperación del último punto de guardado de la copia de seguridad se ejecuta con los siguientes comandos como usuario pr1adm:

- Base de datos del sistema

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- Base de datos de tenant

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

También puede usar HANA Studio o Cockpit para ejecutar la recuperación del sistema y la base de datos de inquilinos.

El siguiente resultado del comando muestra la ejecución de la recuperación.

Recuperación de la base de datos del sistema

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Recuperación de bases de datos de tenant

Si no se ha creado una clave de almacenamiento de usuario para el usuario pr1adm en el sistema de origen, debe crearse una clave en el sistema de destino. El usuario de la base de datos configurado en la clave debe tener privilegios para ejecutar operaciones de recuperación de inquilinos.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

La recuperación de arrendatarios se ejecuta ahora con hdbsql.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

La base de datos HANA ahora está en funcionamiento y el flujo de trabajo de recuperación ante desastres de la base de datos de HANA se ha probado.

Recuperación con recuperación de reenvío mediante backups de registros/catálogos

Los backups de registros y el catálogo de backup de HANA se están replicando desde el sistema de origen.

La recuperación mediante todas las copias de seguridad de registro disponibles se ejecuta con los siguientes comandos como usuario pr1adm:

- Base de datos del sistema

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Base de datos de tenant

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

> Para recuperar utilizando todos los registros disponibles, puede utilizar en cualquier momento en el futuro como Marca de tiempo en la sentencia Recovery.

También puede usar HANA Studio o Cockpit para ejecutar la recuperación del sistema y la base de datos de inquilinos.

El siguiente resultado del comando muestra la ejecución de la recuperación.

Recuperación de la base de datos del sistema

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

Recuperación de bases de datos de tenant

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

La base de datos HANA ahora está en funcionamiento y el flujo de trabajo de recuperación ante desastres de la base de datos de HANA se ha probado.

Comprobar la coherencia de los backups de registros más recientes

Debido a que la replicación del volumen de backup de registros se realiza de forma independiente del proceso de backup de registros ejecutado por la base de datos SAP HANA, puede haber archivos de backup de registros abiertos e incoherentes en el sitio de recuperación ante desastres. Sólo es posible que los archivos de backup de registro más recientes no sean consistentes y se deben comprobar dichos archivos antes de que se realice una recuperación Reenviar en el sitio de recuperación ante desastres mediante el `hdbbackupcheck` herramienta.

Si la `hdbbackupcheck` la herramienta informa de un error acerca de los backups de registros más recientes, es necesario eliminar o eliminar el último conjunto de backups de registros.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

La comprobación debe ejecutarse para los archivos de backup de registro más recientes del sistema y la base de datos de tenant.

Si la `hdbbackupcheck` la herramienta informa de un error acerca de los backups de registros más recientes, es necesario eliminar o eliminar el último conjunto de backups de registros.

Recuperación tras fallos

Recuperación tras fallos

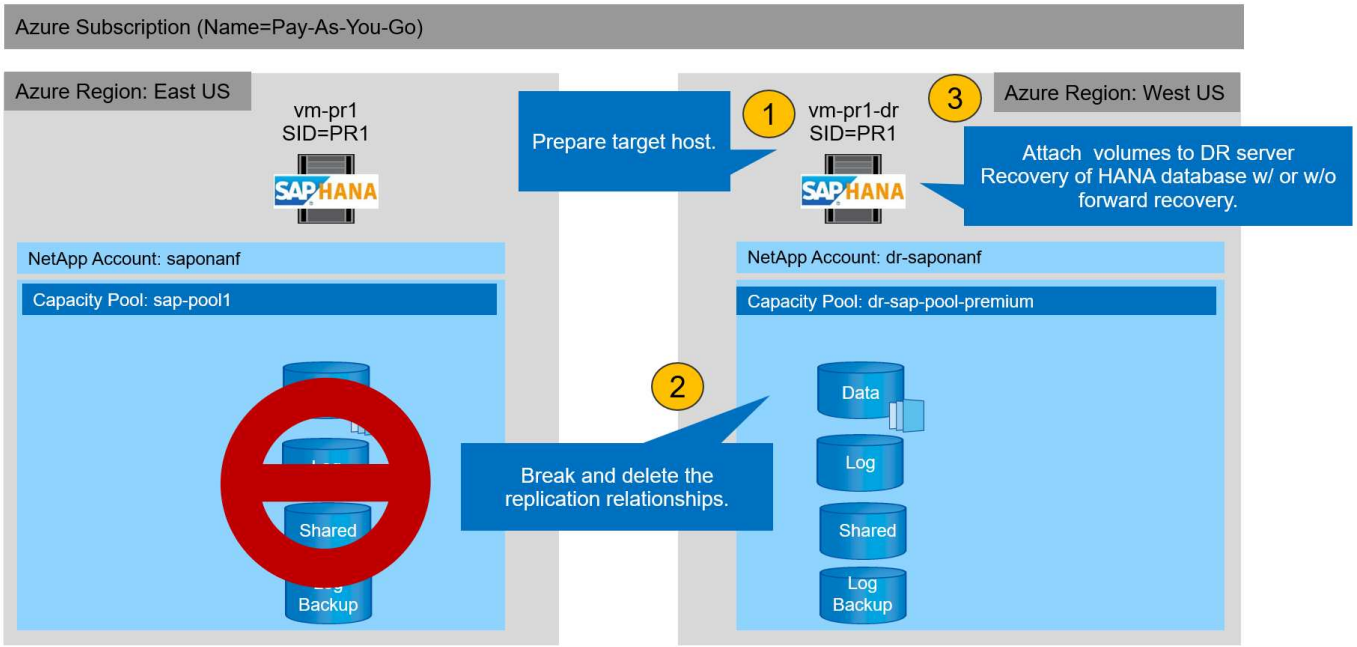
Dependiendo de si la replicación de backup de registros forma parte de la configuración de recuperación ante desastres, los pasos para la recuperación ante desastres son ligeramente diferentes. En esta sección se describe la conmutación al nodo de respaldo de recuperación ante desastres para la replicación solo de backup de datos y para la replicación del volumen de datos combinada con la replicación de volumen de backup de registros.

Para ejecutar la recuperación tras fallos, lleve a cabo los siguientes pasos:

1. Prepare el host de destino.
2. Rompa y elimine las relaciones de replicación.
3. Restaure el volumen de datos al backup de Snapshot más reciente coherente con las aplicaciones.
4. Monte los volúmenes en el host de destino.
5. Recupere la base de datos HANA.
    - Únicamente recuperación del volumen de datos.

- Recuperación posterior mediante backups de registros replicados.

En las siguientes subsecciones se describen estos pasos con detalle, y la siguiente figura describe las pruebas de recuperación tras fallos en caso de desastre.



Prepare el host de destino

En esta sección se describen los pasos de preparación necesarios en el servidor que se usa para la conmutación al nodo de respaldo de recuperación ante desastres.

Durante el funcionamiento normal, el host de destino se suele utilizar para otros fines, por ejemplo, como un sistema de garantía de calidad o prueba de HANA. Por lo tanto, la mayoría de los pasos descritos deben ejecutarse al ejecutar las pruebas de recuperación tras fallos de desastres. Por otro lado, los archivos de configuración pertinentes, como `/etc/fstab` y.. `/usr/sap/sapservices`, puede prepararse y luego ponerse en producción simplemente copiando el archivo de configuración. El procedimiento de conmutación por error de recuperación ante desastres garantiza que los archivos de configuración pertinentes preparados estén configurados correctamente.

La preparación del host de destino también incluye apagar el sistema de prueba o control de calidad de HANA, así como detener todos los servicios que utilizan `systemctl stop sapinit`.

El nombre de host y la dirección IP del servidor de destino

El nombre de host del servidor de destino debe ser idéntico al nombre de host del sistema de origen. La dirección IP puede ser diferente.

> Se debe establecer una correcta delimitación del servidor de destino para que no pueda comunicarse con otros sistemas. Si no se cuenta con una delimitación adecuada, el sistema de producción clonado puede intercambiar datos con otros sistemas de producción, lo que puede dar lugar a datos dañados lógicamente.

Instale el software necesario

El software del agente de host SAP debe instalarse en el servidor de destino. Para obtener toda la información, consulte "Agente host SAP" En el portal de ayuda de SAP.

> Si el host se usa como sistema de control de calidad o prueba de HANA, el software del agente de host SAP ya está instalado.

Configurar usuarios, puertos y servicios SAP

Los usuarios y los grupos requeridos para la base de datos SAP HANA deben estar disponibles en el servidor de destino. Normalmente, se utiliza la gestión central de usuarios; por lo tanto, no es necesario realizar ningún paso de configuración en el servidor de destino. Los puertos necesarios para la base de datos HANA deben configurarse en los hosts objetivo. La configuración se puede copiar desde el sistema de origen copiando el `/etc/services` archivo al servidor de destino.

Las entradas de servicios SAP necesarias deben estar disponibles en el host de destino. La configuración se puede copiar desde el sistema de origen copiando el `/usr/sap/sapservices` archivo al servidor de destino. El siguiente resultado muestra las entradas necesarias para la base de datos SAP HANA que se utilizan en la configuración de laboratorio.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

Prepare el volumen de registro de HANA

Debido a que el volumen de registro de HANA no forma parte de la replicación, debe existir un volumen de registro vacío en el host de destino. El volumen de registro debe incluir los mismos subdirectorios que el sistema HANA de origen.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Preparar el volumen de backup de registros

Dado que el sistema de origen está configurado con un volumen separado para los backups de registros de HANA, debe haber un volumen de backup de registros también disponible en el host de destino. Es necesario configurar y montar un volumen para los backups de registros en el host objetivo.

Si la replicación de volumen de backup de registros forma parte de la configuración de recuperación ante desastres, el volumen de backup de registros replicado se monta en el host de destino y no es necesario preparar un volumen de backup de registros adicional.

Preparar los montajes del sistema de archivos

En la siguiente tabla se muestran las convenciones de nomenclatura utilizadas en la configuración del laboratorio. Los nombres de los volúmenes en el sitio de recuperación de desastres se incluyen en `/etc/fstab`.

Volúmenes PR1 HANA	Volumen y subdirectorios en el centro de recuperación ante desastres	Punto de montaje en el host de destino
Volumen de datos	PR1-data-mnt00001-sm-dest	/hana/data/PR1/mnt00001
Volumen compartido	PR1-shared-sm-dest/shared-sm-dest/usr-SAP-PR1	/hana/shared /usr/SAP/PR1
Volumen de backup de registros	el más extraño	/hanabackup

Los puntos de montaje de esta tabla deben crearse en el host objetivo.

Aquí están los requisitos `/etc/fstab` entradas.

```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

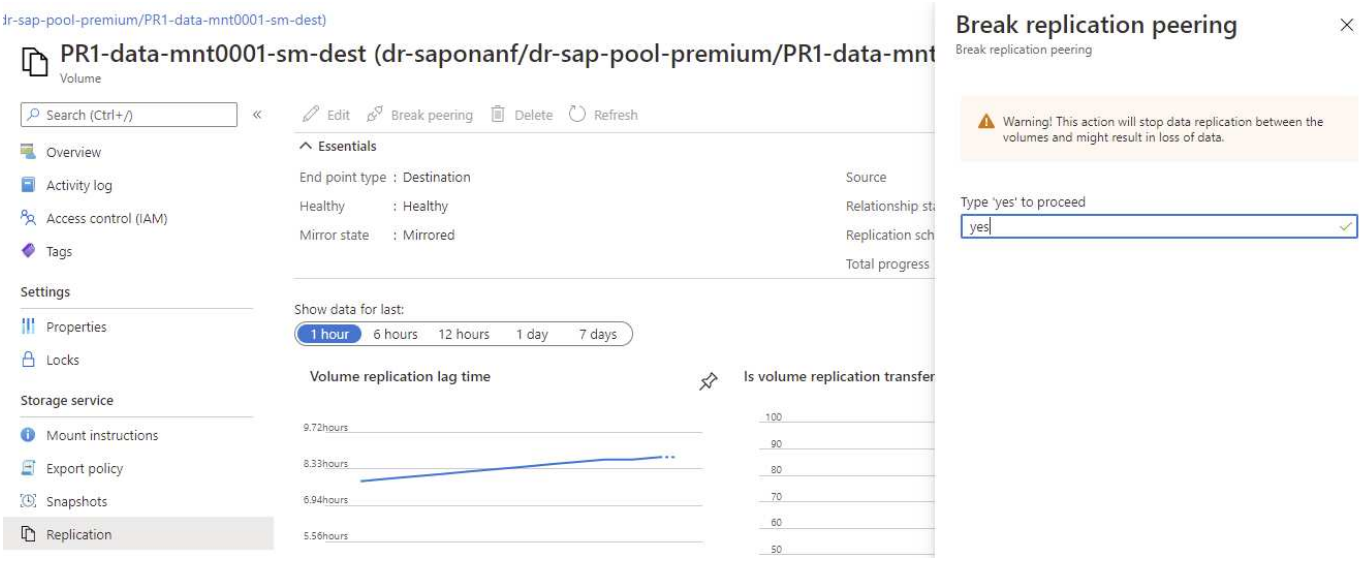
Rompa y elimine la paridad de replicación

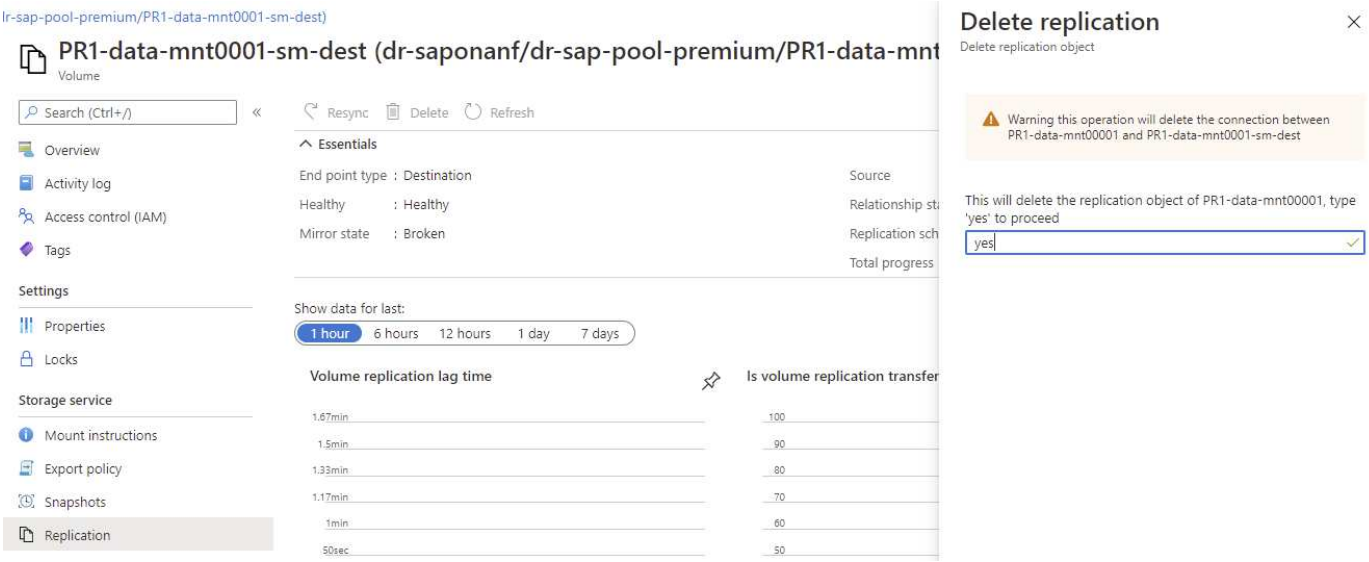
En caso de conmutación al nodo de respaldo ante desastres, es necesario desactivar los volúmenes objetivo para que el host objetivo pueda montar los volúmenes para

operaciones de lectura y escritura.

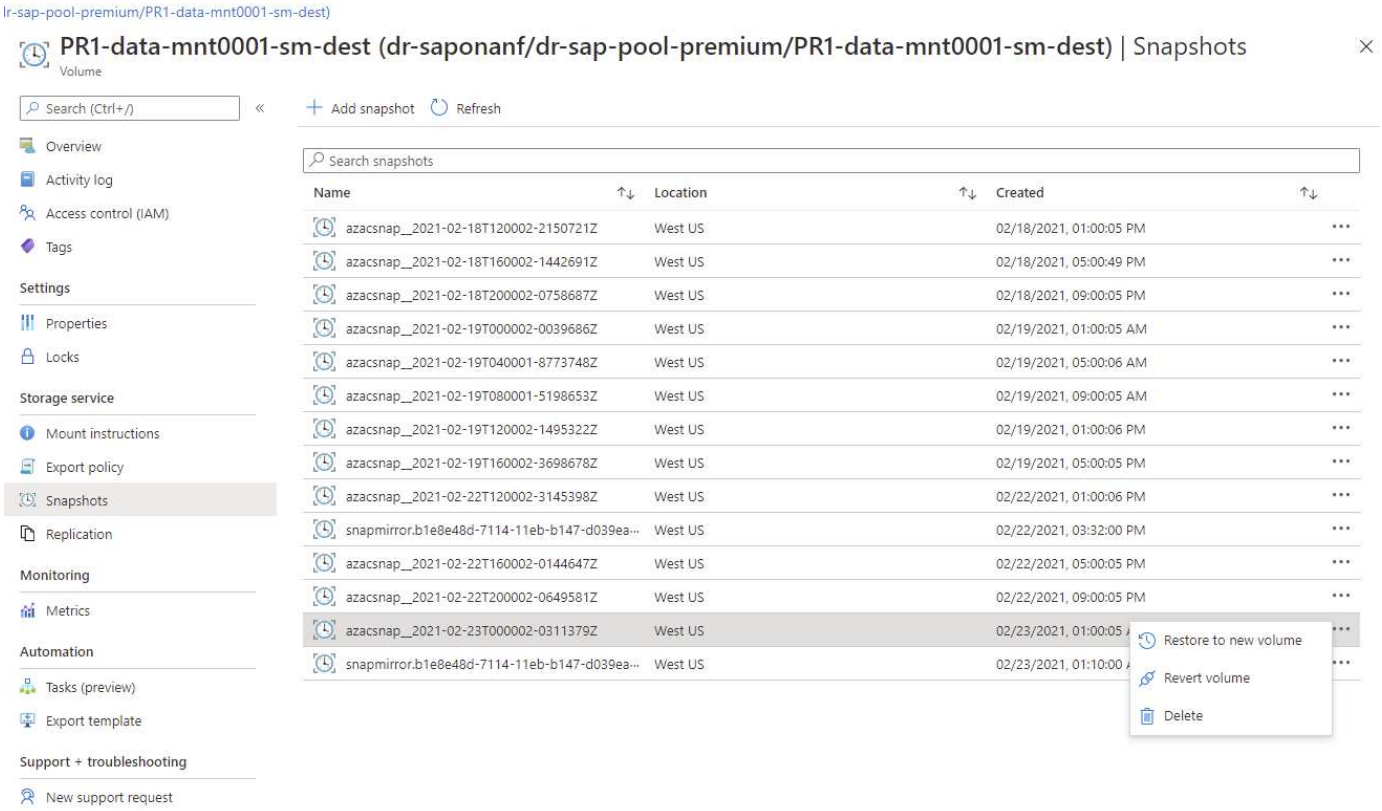
> Para el volumen de datos de HANA, debe restaurar el volumen al backup de snapshot de HANA más reciente creado con AzAcSnap. Esta operación de reversión de volumen no es posible si la snapshot de replicación más reciente se Marca como ocupada debido a la paridad de replicación. Por lo tanto, también debe eliminar la relación de paridad de replicación.

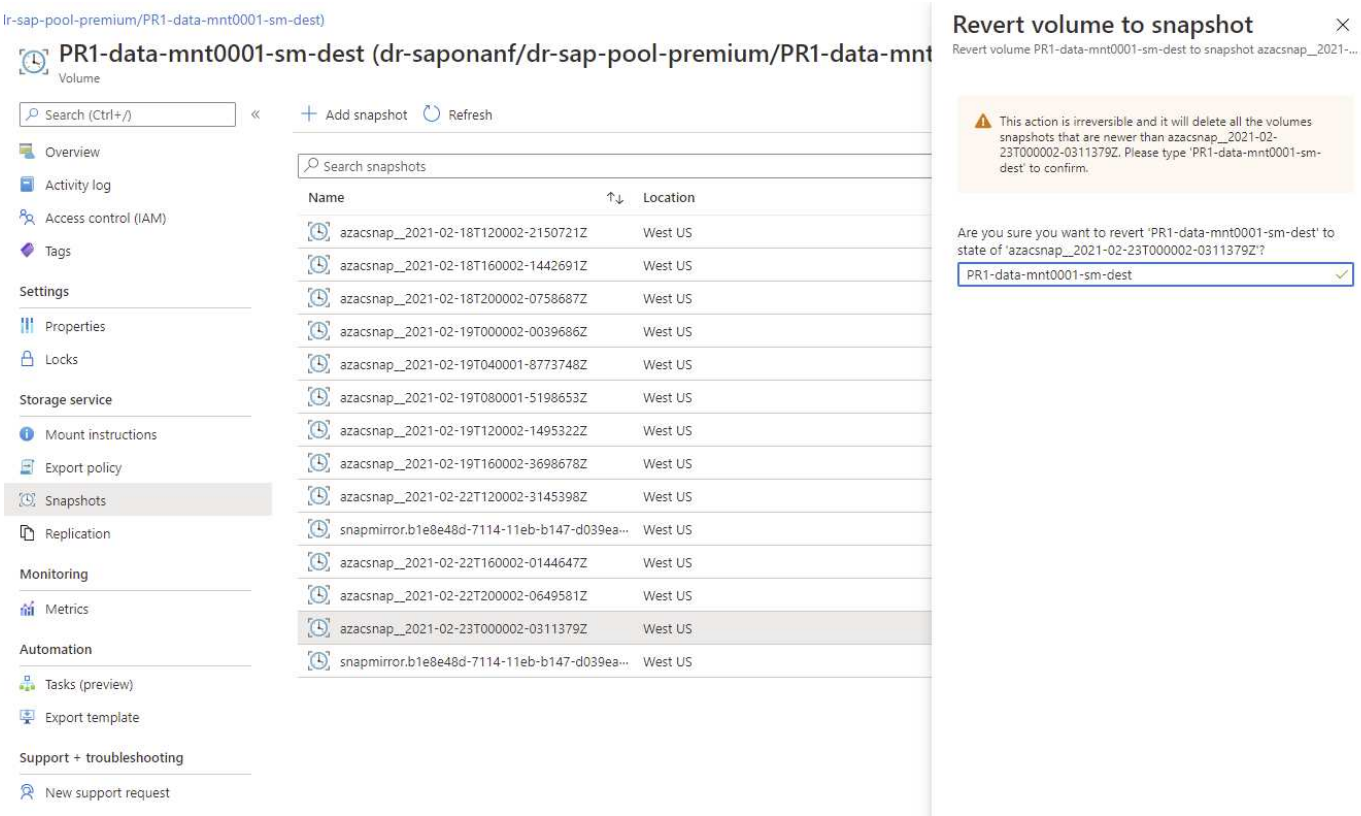
Las siguientes dos capturas de pantalla muestran la operación de pausa y eliminación de paridad para el volumen de datos de HANA. Deben realizarse las mismas operaciones para el backup de registros y el volumen compartido de HANA.





Como se eliminó el paridad de replicación, es posible revertir el volumen al último backup de snapshot de HANA. Si no se elimina la relación de paridad, la selección de revertir volumen se atenúa y no se puede seleccionar. Las dos siguientes capturas de pantalla muestran la operación de reversión de volumen.





Después de la operación de reversión de volumen, el volumen de datos se basa en el backup de snapshot consistente de HANA y ahora puede utilizarse para ejecutar operaciones de recuperación de reenvío.

Si se utiliza un pool de capacidad con un nivel de bajo rendimiento, los volúmenes ahora deben moverse a un pool de capacidad que pueda proporcionar el rendimiento requerido.

Monte los volúmenes en el host de destino

Los volúmenes ahora pueden montarse en el host de destino, según el `/etc/fstab` archivo creado anteriormente.

```
vm-pr1:~ # mount -a
```

El siguiente resultado muestra los sistemas de archivos necesarios.

```
vm-pr1:~ # df
Filesystem                                     1K-blocks     Used
Available Use% Mounted on
devtmpfs                                         8201112        0
8201112   0% /dev
tmpfs                                           12313116        0
12313116   0% /dev/shm
tmpfs                                            8208744     9096
8199648   1% /run
tmpfs                                            8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                       29866736  2543948
27322788   9% /
/dev/sda3                                        1038336    79984
958352   8% /boot
/dev/sda2                                         524008     1072
522936   1% /boot/efi
/dev/sdb1                                       32894736    49180
31151556   1% /mnt
10.0.2.4:/PR1-log-mnt00001-dr            107374182400     6400
107374176000   1% /hana/log/PR1/mnt00001
tmpfs                                            1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-shared-sm-dest/hana-shared 107377178368 11317248
107365861120   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 107377178368 11317248
107365861120   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest             107379678976 35249408
107344429568   1% /hanabackup
10.0.2.4:/PR1-data-mnt0001-sm-dest       107376511232  6696960
107369814272   1% /hana/data/PR1/mnt00001
vm-pr1:~ #
```

Recuperación de base de datos de HANA

Los siguientes son pasos para la recuperación de la base de datos de HANA.

Inicie los servicios SAP necesarios.

```
vm-pr1:~ # systemctl start sapinit
```

El siguiente resultado muestra los procesos necesarios.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

Los siguientes subapartados describen el proceso de recuperación con recuperación futura mediante los backups de registros replicados. La recuperación se ejecuta mediante el script de recuperación de HANA para la base de datos del sistema y los comandos hdbsql para la base de datos del arrendatario.

Los comandos para ejecutar una recuperación del último punto de guardado de datos se describen en el capítulo "Recuperación en el último punto de guardado de Data Volume Backup de HANA".

Recuperación con recuperación futura con backups de registros

La recuperación mediante todas las copias de seguridad de registro disponibles se ejecuta con los siguientes comandos como usuario pr1adm:

- Base de datos del sistema

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Base de datos de tenant

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

Para recuperar utilizando todos los registros disponibles, puede utilizar en cualquier momento en el futuro como Marca de tiempo de la sentencia Recovery.

También puede usar HANA Studio o Cockpit para ejecutar la recuperación del sistema y la base de datos de inquilinos.

El siguiente resultado del comando muestra la ejecución de la recuperación.

Recuperación de la base de datos del sistema

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-24 00:00:00' CLEAR LOG USING
SNAPSHOT"
[139792805873472, 0.008] >> starting recoverSys (at Tue Feb 23 12:05:16
2021)
[139792805873472, 0.008] args: ()
[139792805873472, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-24 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-23 12:05:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-23 12:05:17
stopped system: 2021-02-23 12:05:18
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-23 12:05:23
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-23T12:07:53+00:00  P0012969      177cec93d51 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
23T09:03:11+00:00, reached log position 43123520
recoverSys finished successfully: 2021-02-23 12:07:54
[139792805873472, 157.466] 0
[139792805873472, 157.466] << ending recoverSys, rc = 0 (RC_TEST_OK),
after 157.458 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Recuperación de bases de datos de tenant

Si no se ha creado una clave de almacenamiento de usuario para el usuario pr1adm en el sistema de origen, debe crearse una clave en el sistema de destino. El usuario de la base de datos configurado en la clave debe tener privilegios para ejecutar operaciones de recuperación de inquilinos.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-24
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 98.740038 sec; server time 98.737788 sec)
hdbsql SYSTEMDB=>
```

Comprobar la coherencia de los backups de registros más recientes

Debido a que la replicación del volumen de backup de registros se realiza de forma independiente del proceso de backup de registros ejecutado por la base de datos SAP HANA, puede haber archivos de backup de registros abiertos e incoherentes en el sitio de recuperación ante desastres. Sólo es posible que los archivos de backup de registro más recientes no sean consistentes y se deben comprobar dichos archivos antes de que se realice una recuperación Reenviar en el sitio de recuperación ante desastres mediante el `hdbbackupcheck` herramienta.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

La comprobación debe ejecutarse para los archivos de backup de registros más recientes del sistema y la base de datos de tenant.

Si la `hdbbackupcheck` la herramienta informa de un error acerca de los backups de registros más recientes, es necesario eliminar o eliminar el último conjunto de backups de registros.

Actualizar historial

Desde su publicación original se han realizado los siguientes cambios técnicos en esta solución.

Versión	Fecha	Actualizar el resumen
Versión 1.0	Abril de 2021	Versión inicial