Reprise après incident de SAP HANA avec Azure NetApp Files

NetApp Solutions SAP

NetApp
March 11, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions-sap/backup/saphana-dr-anf_data_protection_overview_overview.html on March 11, 2024. Always check docs.netapp.com for the latest.

Sommaire

Reprise après incident de SAP HANA avec Azure NetApp Files

Tr-4891 : reprise après incident de SAP HANA avec Azure NetApp Files

Nils Bauer, NetApp Ralf Klahr, Microsoft

Des études ont montré que les temps d'indisponibilité des applications d'entreprise ont un impact négatif considérable sur le business des entreprises. En plus de l'impact financier, les temps d'arrêt peuvent également nuire à la réputation de l'entreprise, au moral du personnel et à la fidélité des clients. Il est surprenant que toutes les entreprises ne disposent pas d'une politique globale de reprise après incident.

L'exécution de SAP HANA sur Azure NetApp Files (ANF) permet aux clients d'accéder à des fonctionnalités supplémentaires qui étendent et améliorent la protection des données intégrée et les fonctionnalités de reprise après incident de SAP HANA. Cette section de présentation explique ces options afin d'aider les clients à sélectionner les options qui répondent à leurs besoins.

Pour développer une stratégie complète de reprise sur incident, les clients doivent comprendre les exigences des applications métier et les fonctionnalités techniques dont ils ont besoin pour la protection des données et la reprise sur incident. La figure suivante fournit une présentation de la protection des données.

[Erreur : image graphique manquante]

Aux exigences des applications d'entreprise

Il existe deux indicateurs clés pour les applications d'entreprise :

- L'objectif de point de récupération (RPO) ou la perte de données maximale tolérable
- L'objectif de durée de restauration (RTO) ou l'interruption maximale tolérable des applications d'entreprise

Ces besoins sont définis par le type d'application utilisé et la nature de vos données d'entreprise. L'objectif RPO et l'objectif RTO peuvent différer si vous protégez-vous contre les défaillances dans une seule région Azure. Elles peuvent également différer si vous préparez des incidents catastrophiques, tels que la perte d'une région Azure complète. Il est important d'évaluer les exigences de l'entreprise qui définissent le RPO et RTO, car ces exigences ont un impact significatif sur les options techniques disponibles.

Haute disponibilité

L'infrastructure pour SAP HANA, telles que les machines virtuelles, le réseau et le stockage, doit disposer de composants redondants pour s'assurer qu'il n'y a pas de point de défaillance unique. MS Azure assure la redondance des différents composants de l'infrastructure.

Pour assurer une haute disponibilité côté applications et calcul, les hôtes SAP HANA en attente peuvent être configurés pour une haute disponibilité intégrée avec un système multihôte SAP HANA. En cas de panne d'un serveur ou d'un service SAP HANA, le service SAP HANA bascule vers l'hôte de secours, ce qui entraîne les interruptions des applications.

Si vous ne pouvez pas profiter de la continuité de l'activité de vos applications ou de vos serveurs, vous pouvez également utiliser la réplication du système SAP HANA comme solution haute disponibilité qui permet un basculement dans des délais très courts. Les clients SAP utilisent la réplication système HANA pour traiter

la haute disponibilité en cas de défaillance non planifiée et réduire au maximum les interruptions pour les opérations planifiées, telles que les mises à niveau logicielles HANA.

Corruption logique

Une corruption logique peut être provoquée par des erreurs logicielles, des erreurs humaines ou du sabotage. Malheureusement, la corruption logique ne peut souvent pas être abordée avec les solutions standard de haute disponibilité et de reprise après incident. Par conséquent, selon la couche, l'application, le système de fichiers ou le stockage où la corruption logique s'est produite, les exigences RTO et RPO ne peuvent parfois pas être satisfaites.

Le pire cas étant la corruption logique d'une application SAP. Les applications SAP fonctionnent souvent dans un environnement dans lequel les différentes applications communiquent entre elles et échangent des données. Par conséquent, la restauration et la récupération d'un système SAP dans lequel une corruption logique s'est produite n'est pas l'approche recommandée. La restauration du système à un point dans le temps avant l'altération entraîne une perte de données. L'objectif de point de récupération dépasse ainsi zéro. Par ailleurs, le paysage SAP ne serait plus synchronisé et devrait nécessiter un post-traitement supplémentaire.

Au lieu de restaurer le système SAP, la meilleure approche consiste à essayer de corriger l'erreur logique dans le système, en analysant le problème dans un système de réparation distinct. L'analyse de la cause première nécessite la participation du processus métier et du propriétaire des applications. Dans ce cas, vous créez un système de réparation (clone du système de production) basé sur les données stockées avant l'altération logique. Dans le système de réparation, les données requises peuvent être exportées et importées dans le système de production. Avec cette approche, le système productif n'a pas besoin d'être arrêté et, dans le meilleur des cas, aucune donnée ou seulement une petite fraction des données n'est perdue.

> Les étapes requises pour configurer un système de réparation sont identiques à celles d'un scénario de test de reprise après incident décrit dans ce document. La solution de reprise sur incident décrite peut donc facilement être étendue pour gérer la corruption logique.

Sauvegardes

Des sauvegardes sont créées pour permettre la restauration et la restauration à partir de différents jeux de données ponctuelles. Ces sauvegardes sont généralement conservées pendant quelques jours à quelques semaines.

Selon le type de corruption, il est possible d'effectuer des restaurations et des restaurations avec ou sans perte de données. Si le RPO doit être nul, même en cas de perte du stockage primaire et de sauvegarde, la sauvegarde doit être combinée avec la réplication synchrone des données.

Le RTO pour la restauration et la récupération est défini par le temps de restauration requis, le temps de restauration (démarrage de base de données inclus) et le chargement des données dans la mémoire. Pour les bases de données volumineuses et les approches de sauvegarde classiques, l'RTO peut facilement prendre plusieurs heures, ce qui n'est pas acceptable. Pour atteindre de très faibles valeurs RTO, une sauvegarde doit être combinée à une solution de secours, qui comprend le préchargement des données dans la mémoire.

En revanche, une solution de sauvegarde doit traiter la corruption logique, car les solutions de réplication des données ne peuvent pas couvrir tous les types de corruption logique.

La réplication des données synchrone ou asynchrone

L'objectif RPO détermine principalement la méthode de réplication des données que vous devez utiliser. Si le RPO doit être nul, même en cas de perte du stockage principal et de sauvegarde, les données doivent être répliquées de manière synchrone. Cependant, la réplication synchrone est limitée de manière technique,

comme la distance entre deux régions Azure. Dans la plupart des cas, la réplication synchrone n'est pas adaptée aux distances supérieures à 100 km en raison de la latence. Il ne s'agit donc pas d'une option de réplication des données entre les régions Azure.

Si un RPO plus important est acceptable, la réplication asynchrone peut être utilisée sur de grandes distances. L'objectif RPO dans ce cas est défini par la fréquence de réplication.

Réplication du système HANA avec ou sans préchargement des données

La durée de démarrage d'une base de données SAP HANA est bien plus longue que celle des bases de données classiques, car une quantité importante de données doit être chargée dans la mémoire avant que la base de données puisse fournir les performances attendues. Par conséquent, une partie importante du RTO est le temps nécessaire au démarrage de la base de données. Avec une réplication basée sur le stockage et la réplication système HANA sans précharger les données, la base de données SAP HANA doit être démarrée en cas de basculement vers le site de reprise d'activité.

La réplication du système SAP HANA offre un mode de fonctionnement dans lequel les données sont préchargées et mises à jour en continu sur l'hôte secondaire. Ce mode assure des valeurs RTO très faibles, mais il requiert également un serveur dédié qui n'est utilisé que pour recevoir les données de réplication du système source.

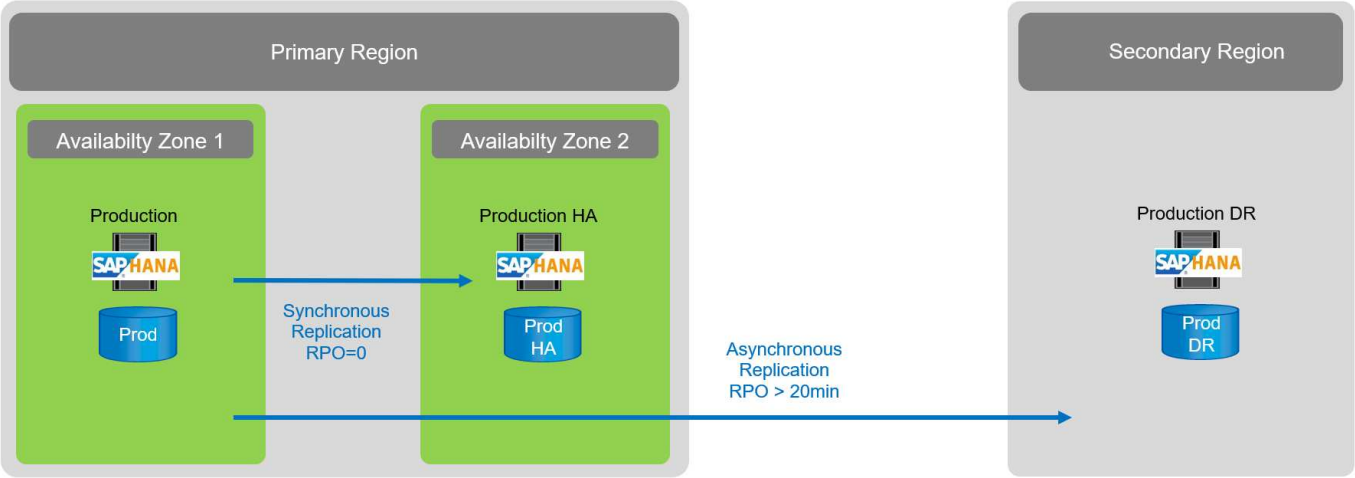
Comparaison des solutions de reprise d'activité

Une solution complète de reprise sur incident doit permettre aux clients de récupérer après une panne complète du site primaire. Par conséquent, les données doivent être transférées vers un site secondaire et une infrastructure complète est nécessaire pour exécuter les systèmes SAP HANA de production requis en cas de panne sur un site. Selon les exigences de disponibilité de l'application et le type d'incident à protéger, une solution de reprise sur incident sur deux ou trois sites doit être envisagée.

La figure suivante montre une configuration standard dans laquelle les données sont répliquées de manière synchrone au sein de la même région Azure vers une seconde zone de disponibilité. La distance courte permet de répliquer les données de manière synchrone pour atteindre un RPO de zéro (généralement utilisé pour fournir la haute disponibilité).

Les données sont également répliquées de manière asynchrone vers une région secondaire pour être protégée contre les incidents lorsque la région primaire est affectée. L'objectif RPO minimal possible dépend de la fréquence de réplication des données, qui est limitée par la bande passante disponible entre la région primaire et la région secondaire. Un RPO minimal type est généralement compris entre 20 minutes et plusieurs heures.

Ce document présente différentes options d'implémentation d'une solution de reprise après incident de deux régions.



Réplication système SAP HANA

La réplication système SAP HANA fonctionne au niveau de la couche base de données. La solution repose sur un système SAP HANA supplémentaire sur le site de reprise d'activité, qui reçoit les modifications du système principal. Ce système secondaire doit être identique au système principal.

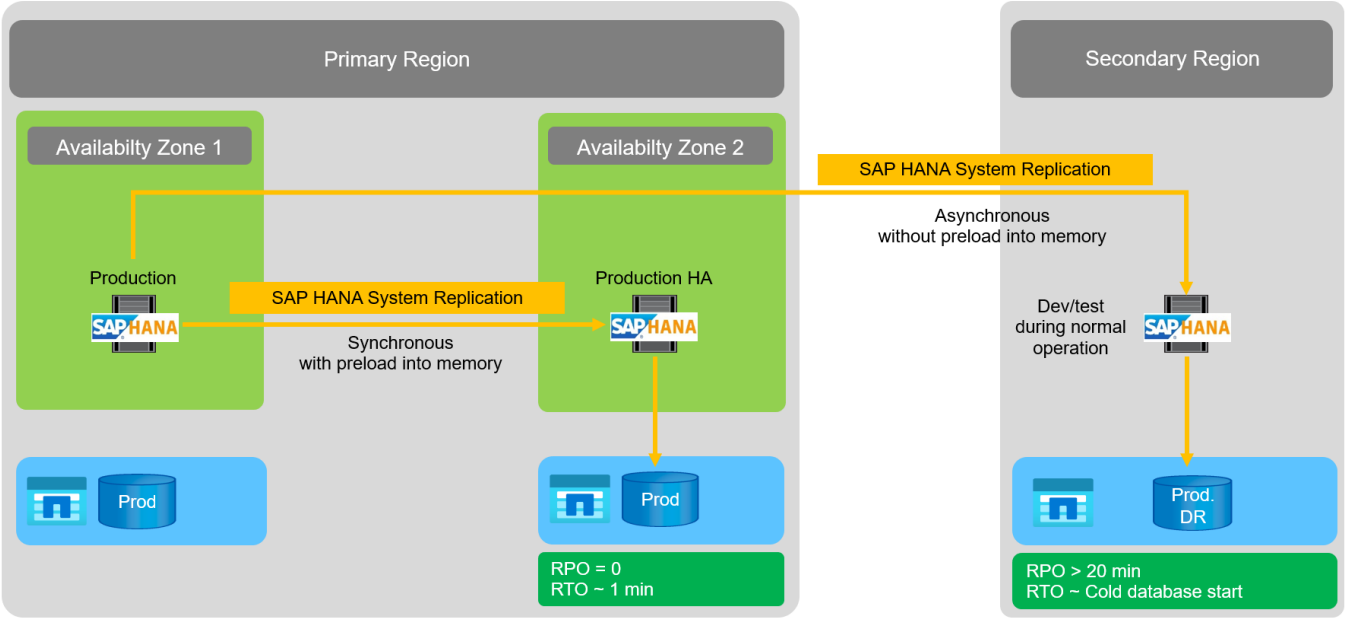
La réplication système SAP HANA peut être exploitée selon l'un des deux modes suivants :

- Avec des données préchargées dans la mémoire et un serveur dédié sur le site de reprise d'activité :
  - Le serveur est utilisé exclusivement en tant qu'hôte secondaire de réplication système SAP HANA.
  - Des valeurs RTO très faibles peuvent être obtenues car les données sont déjà chargées en mémoire et aucune base de données de démarrage n'est nécessaire en cas de basculement.
- Sans données préchargées dans la mémoire et sans serveur partagé sur le site de reprise d'activité :
  - Le serveur est partagé en tant que système secondaire de réplication système SAP HANA et en tant que système de test et de développement.
  - Le RTO dépend principalement du temps nécessaire au démarrage de la base de données et à la charge des données dans la mémoire.

Pour une description complète de toutes les options de configuration et de tous les scénarios de réplication, reportez-vous à la "Guide d'administration de SAP HANA".

La figure suivante montre la configuration d'une solution de reprise après incident à deux régions avec la réplication système SAP HANA. La réplication synchrone avec données préchargées dans la mémoire est utilisée pour la haute disponibilité locale dans la même région Azure, mais dans des zones de disponibilité différentes. La réplication asynchrone sans données préchargées est configurée pour la région de reprise d'activité distante.

La figure suivante représente la réplication système SAP HANA.



Réplication système SAP HANA avec données préchargées dans la mémoire

De très faibles valeurs RTO avec SAP HANA ne peuvent être obtenues qu'avec la réplication système SAP HANA avec des données préchargées dans la mémoire. La réplication système SAP HANA avec un serveur secondaire dédié sur le site de reprise d'activité permet d'obtenir une valeur RTO d'environ 1 minute au maximum. Les données répliquées sont reçues et préchargées dans la mémoire du système secondaire. Du fait de ce faible temps de basculement, la réplication système SAP HANA est également souvent utilisée pour les opérations de maintenance sans interruption quasi-nul, telles que les mises à niveau du logiciel HANA.

Généralement, la réplication système SAP HANA est configurée de façon synchrone pour effectuer une réplication synchrone lors de l'opération de préchargement des données. La distance maximale prise en charge pour la réplication synchrone se situe dans une plage de 100 km.

Réplication système SAP sans données préchargées dans la mémoire

Pour les exigences RTO moins strictes, vous pouvez utiliser la réplication système SAP HANA sans données préchargées. Dans ce mode opérationnel, les données de la région de reprise après sinistre ne sont pas chargées en mémoire. Le serveur de la région de reprise après incident est toujours utilisé pour traiter la réplication système SAP HANA exécutant tous les processus SAP HANA requis. Cependant, la majeure partie de la mémoire du serveur est disponible pour exécuter d'autres services, tels que les systèmes de développement/test SAP HANA.

En cas d'incident, le système de développement/test doit être arrêté, le basculement doit être lancé et les données doivent être chargées dans la mémoire. L'objectif RTO de cette approche de veille à froid dépend de la taille de la base de données et du débit de lecture pendant la charge du magasin de lignes et de colonnes. L'hypothèse selon laquelle le débit de lecture des données est de 1 000 Mbit/s devrait prendre environ 18 minutes pour charger 1 To de données.

Reprise après incident SAP HANA avec la réplication inter-région ANF

La réplication inter-régions ANF est intégrée à ANF comme une solution de reprise après incident grâce à la réplication asynchrone des données. La réplication inter-région ANF est configurée par le biais d'une relation de protection des données entre deux volumes ANF sur une région Azure primaire et secondaire. La réplication inter-région ANF permet de mettre à jour le volume secondaire grâce à des réplications différentielles de bloc efficaces. Des planifications de mise à jour peuvent être définies au cours de la

configuration de la réplication.

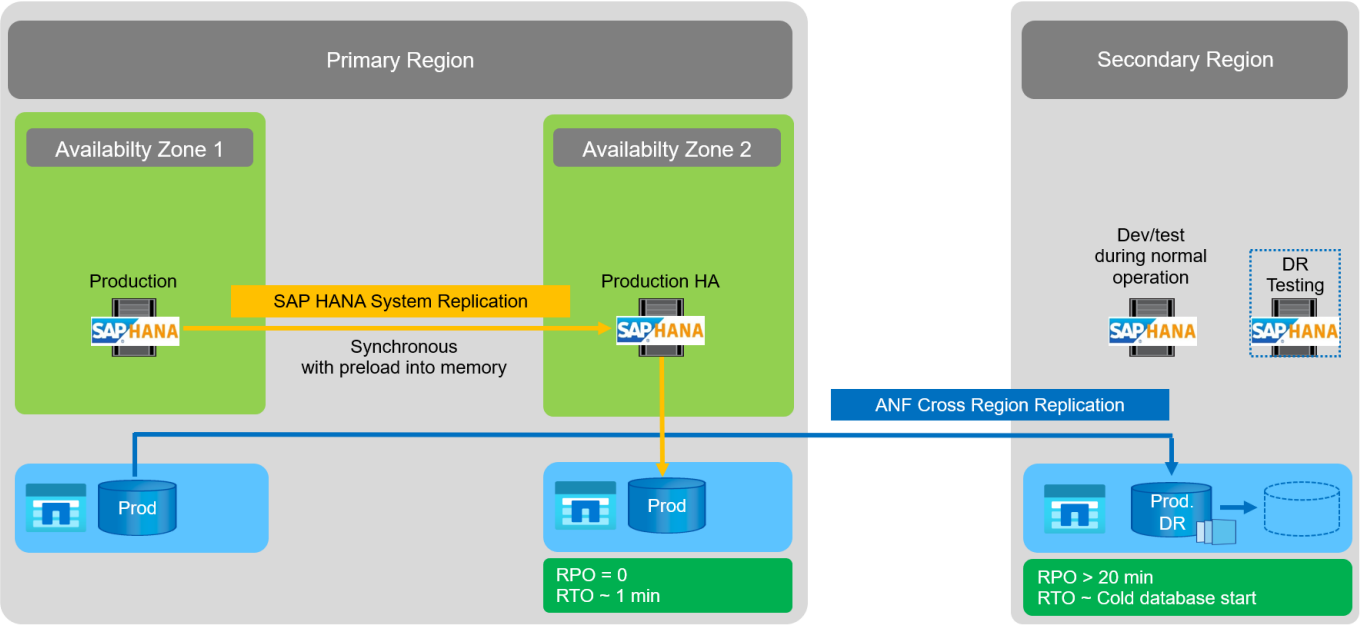
La figure suivante présente un exemple de solution de reprise après incident dans deux régions avec la réplication ANF Cross- Region. Dans cet exemple, le système HANA est protégé avec la réplication système HANA dans la région primaire, comme indiqué au chapitre précédent. La réplication vers une région secondaire s'effectue à l'aide de la réplication ANF inter-région. Le RPO est défini par la planification de réplication et les options de réplication.

Le RTO dépend principalement du temps nécessaire pour démarrer la base de données HANA sur le site de reprise d'activité et pour charger les données dans la mémoire. En supposant que les données sont lues avec un débit de 1000 Mo/s, le chargement de 1 To de données prendra environ 18 minutes. En fonction de la configuration de la réplication, la restauration par transfert est également requise et ajoute à la valeur RTO totale.

Le chapitre fournit plus de détails sur les différentes options de configuration "Options de configuration pour la réplication inter-région avec SAP HANA".

Les serveurs des sites de reprise d'activité peuvent être utilisés en tant que systèmes de développement/test pendant le fonctionnement normal. En cas d'incident, les systèmes de dév/test doivent être arrêtés et démarrés est en tant que serveurs de production de reprise sur incident.

La réplication inter-région d'ANF vous permet de tester le workflow de reprise après incident sans incidence sur les objectifs RPO et RTO. Pour ce faire, il est possible de créer des clones de volume et de les relier au serveur de test de la reprise après incident.



Récapitulatif des solutions de reprise sur incident

Le tableau suivant compare les solutions de reprise sur incident abordées dans cette section et met en évidence les indicateurs les plus importants.

Les principales conclusions sont les suivantes :

- Si un RTO très faible est nécessaire, la réplication système SAP HANA avec un préchargement en mémoire est la seule option.

    - Un serveur dédié est nécessaire sur le site de reprise après incident pour recevoir les données répliquées et charger les données dans la mémoire.
- De plus, la réplication du stockage est nécessaire pour les données résidant en dehors de la base de données (par exemple, les fichiers partagés, les interfaces, etc.).
- Si les exigences RTO/RPO sont moins strictes, la réplication ANF multi-région peut également être utilisée pour :
    - Combiner la réplication de données sans base de données et autres applications
    - Couvrez davantage d'utilisations, telles que les tests de reprise après incident et la mise à jour de développement/test.
    - Avec la réplication du stockage, le serveur du site de DR peut être utilisé comme système d'assurance qualité ou de test pendant le fonctionnement normal.
- Une combinaison de la réplication système SAP HANA en tant que solution haute disponibilité avec RPO=0 et la réplication du stockage sur longue distance est judicieux pour répondre aux différentes exigences.

Le tableau suivant compare les solutions de reprise d'activité.

	Réplication du stockage	**Réplication du système SAP HANA**	
	Réplication inter-région	**Avec préchargement des données**	**Sans préchargement de données**
LE RTO	Faible à moyen, selon le délai de démarrage de la base de données et la restauration avant	Très faible	Faible à moyen, selon le délai de démarrage de la base de données
RPO	Réplication asynchrone > 20 min	Réplication asynchrone RPO > 20 min RPO=0 réplication synchrone	Réplication asynchrone RPO > 20 min RPO=0 réplication synchrone
Les serveurs du site de reprise d'activité peuvent être utilisés pour les activités de développement/test	Oui.	Non	Oui.
Réplication de données ne provenant pas d'une base de données	Oui.	Non	Non
Les données de reprise d'activité peuvent être utilisées pour actualiser les systèmes de développement/tests	Oui.	Non	Non
Tests de reprise d'activité sans incidence sur le RTO et le RPO	Oui.	Non	Non

Réplication ANF entre les régions avec SAP HANA

Réplication ANF entre les régions avec SAP HANA

Des informations indépendantes des applications sur la réplication inter-région sont disponibles à l'adresse "Documentation Azure NetApp Files | Microsoft Docs" dans les sections concepts et mode d'emploi.

Options de configuration pour la réplication inter-région avec SAP HANA

La figure suivante montre les relations de réplication de volume pour un système SAP HANA utilisant la réplication inter-région ANF. Avec la réplication inter-région ANF, les données HANA et le volume partagé HANA doivent être répliqués. Si seul le volume de données HANA est répliqué, les valeurs RPO typiques sont comprises dans la plage d'une journée. Si des valeurs RPO plus faibles sont requises, les sauvegardes du journal HANA doivent également être répliquées pour une restauration par progression.

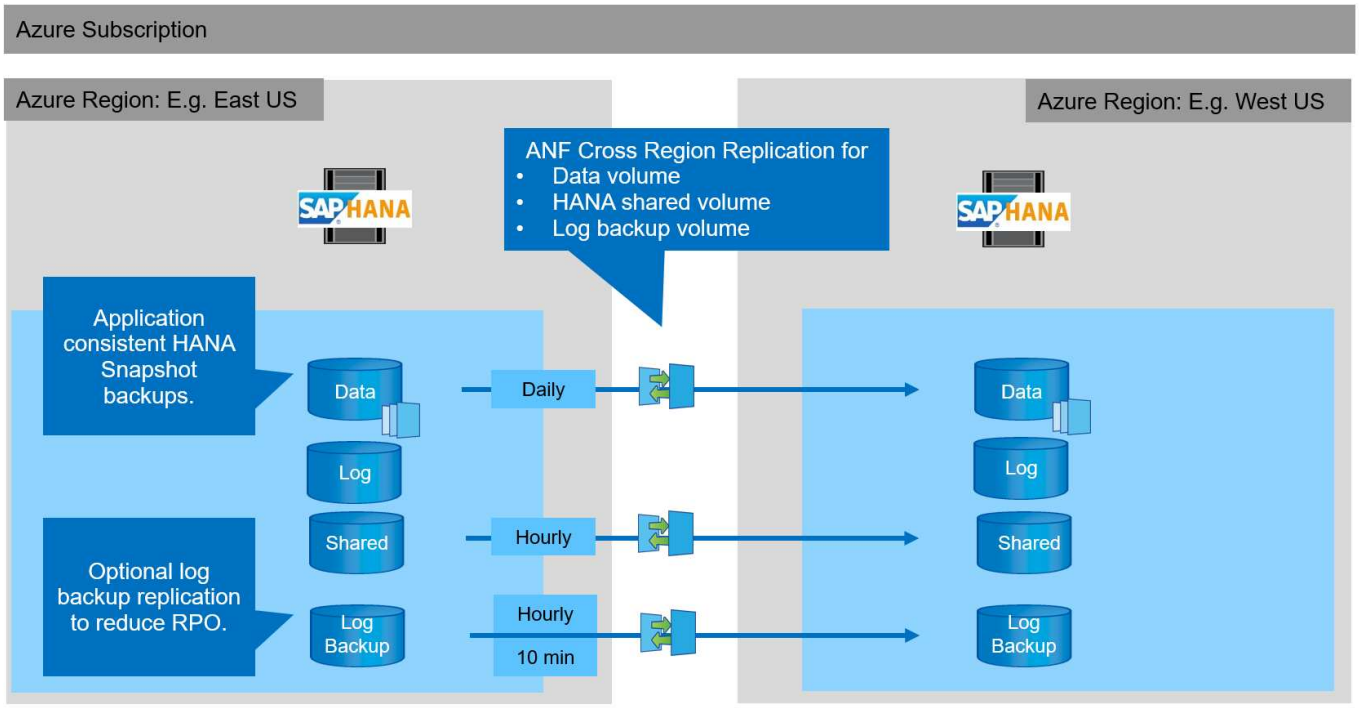
> Le terme « sauvegarde du journal » utilisé dans ce document inclut la sauvegarde du journal et la sauvegarde du catalogue de sauvegardes HANA. Le catalogue de sauvegardes HANA est nécessaire pour exécuter les opérations de récupération par transfert.

> Les descriptions suivantes ainsi que la configuration de laboratoire sont axées sur la base de données HANA. D'autres fichiers partagés, par exemple le répertoire de transport SAP est protégé et répliqué de la même manière que le volume partagé HANA.

Pour permettre la restauration HANA des points de sauvegarde ou la restauration suivante à l'aide des sauvegardes de journaux, des sauvegardes Snapshot de données cohérentes au niveau des applications doivent être créées sur le site principal pour le volume de données HANA. Cela peut être fait par exemple avec l'outil de sauvegarde ANF AzAcSnap (voir aussi "Qu'est-ce que l'outil Snapshot Azure application cohérent pour Azure NetApp Files | Microsoft Docs"). Les sauvegardes Snapshot créées sur le site primaire sont ensuite répliquées sur le site de reprise sur incident.

Dans le cas d'un basculement, la relation de réplication doit être rompue, les volumes doivent être montés sur le serveur de production de reprise après incident et la base de données HANA doit être récupérée, soit vers le dernier point de sauvegarde HANA, soit avec récupération via les sauvegardes de journaux répliquées. Le chapitre "Basculement de reprise d'activité", décrit les étapes requises.

La figure suivante décrit les options de configuration HANA pour la réplication inter-région.



Avec la version actuelle de la réplication inter-région, seules les planifications fixes peuvent être sélectionnées et l'heure de mise à jour de la réplication réelle ne peut pas être définie par l'utilisateur. Les horaires disponibles sont tous les jours, toutes les heures et toutes les 10 minutes. Utilisez ces options de planification, deux configurations différentes selon les exigences RPO : la réplication de volume de données sans journalisation de la réplication des sauvegardes et la réplication des sauvegardes de journaux avec des planifications différentes, toutes les heures ou toutes les 10 minutes. Le RPO le plus faible possible est d'environ 20 minutes. Le tableau suivant récapitule les options de configuration et les valeurs RPO et RTO qui en résultent.

	Réplication du volume de données	**Réplication du volume de sauvegarde des données et des journaux**	**Réplication du volume de sauvegarde des données et des journaux**
Volume de données de planification CRR	Tous les jours	Tous les jours	Tous les jours
Volume de sauvegarde du journal CRR schedule	s/o	Horaire	10 min
RPO max	24 heures + planning Snapshot (par ex. 6 heures)	1 heure	2 x 10 min
RTO max	Principalement défini par l'heure de démarrage HANA	temps de démarrage HANA + temps de restauration	temps de démarrage HANA + temps de restauration
Vers l'avant la reprise	NA	journaux des dernières 24 heures + calendrier Snapshot (par ex. 6 heures)	journaux des dernières 24 heures + calendrier Snapshot (par ex. 6 heures)

Exigences et bonnes pratiques

Microsoft Azure ne garantit pas la disponibilité d'un type de machine virtuelle spécifique lors de sa création ou lors du lancement d'une machine virtuelle désallocation. Plus précisément, en cas de défaillance d'une région, de nombreux clients peuvent avoir besoin de serveurs virtuels supplémentaires dans la région de reprise sur incident. Il est donc recommandé d'utiliser activement une machine virtuelle avec la taille requise pour le basculement après incident en tant que système de test ou d'assurance qualité dans la région de reprise après incident pour allouer le type de machine virtuelle requis.

Pour optimiser les coûts, il est logique d'utiliser un pool de capacité ANF avec un Tier de performance inférieur pendant le fonctionnement normal. La réplication des données ne nécessite pas de hautes performances et peut donc utiliser un pool de capacité avec un niveau de performances standard. Pour les tests de reprise d'activité ou, si un basculement est nécessaire, les volumes doivent être déplacés vers un pool de capacité disposant d'un niveau hautes performances.

Lorsqu'un second pool de capacité n'est pas une option, les volumes cibles de réplication doivent être configurés en fonction des besoins en capacité et non pas des exigences de performances pendant les opérations normales. Le quota ou le débit (pour QoS manuelle) peut ensuite être adapté pour tester la reprise après incident dans le cas d'un basculement de incident.

Vous trouverez des renseignements supplémentaires à l'adresse "Conditions requises et considérations relatives à l'utilisation de la réplication multi-région du volume Azure NetApp Files | Microsoft Docs".

Configuration de laboratoire

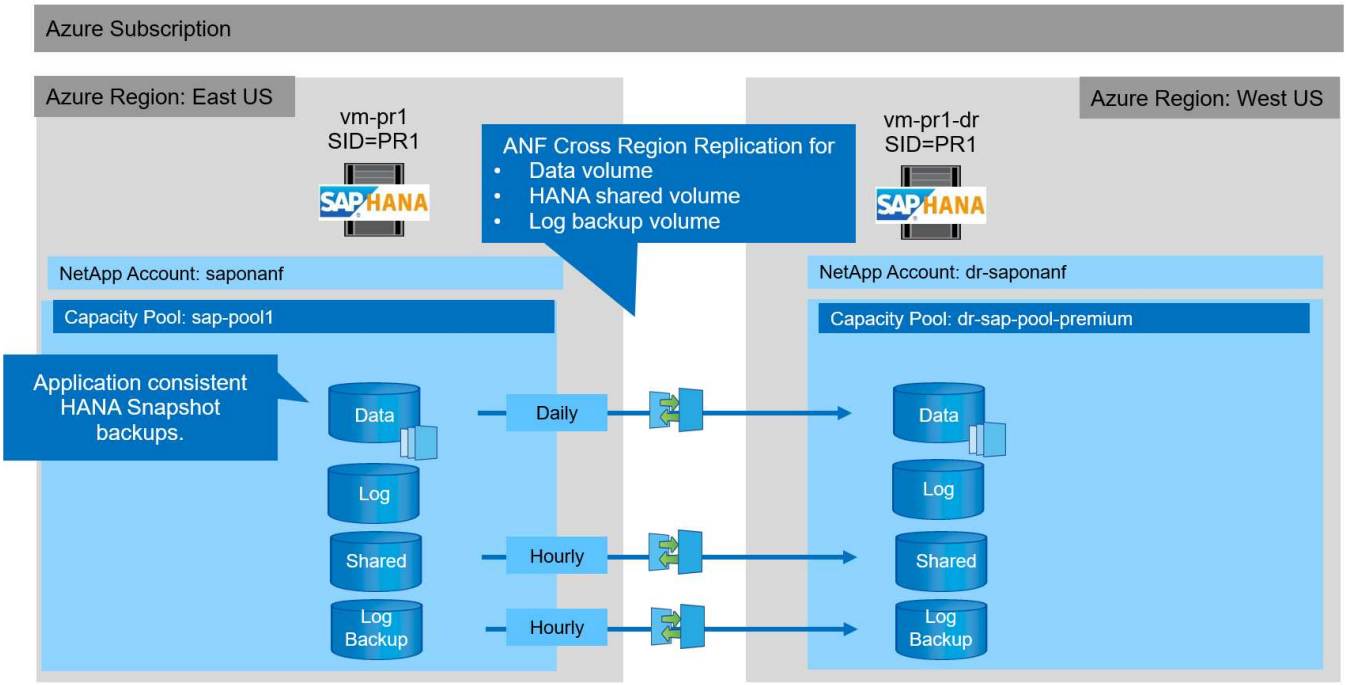
La validation de la solution a été réalisée avec un système hôte unique SAP HANA. L'outil de sauvegarde Microsoft AzAcSnap Snapshot pour ANF a été utilisé pour configurer des sauvegardes Snapshot HANA cohérentes avec les applications. Les volumes de données quotidiens, les sauvegardes de journaux horaires et la réplication de volume partagé sont tous configurés. Le basculement et les tests de reprise après incident ont été validés avec un point de sauvegarde ainsi que pour les opérations de reprise après incident.

Les versions logicielles suivantes ont été utilisées dans la configuration du laboratoire :

- Un seul hôte système SAP HANA 2.0 SPS5 avec un seul locataire
- SUSE SLES POUR SAP 15 SP1
- AzAcSnap 5.0

Un pool de capacité unique avec QoS manuelle a été configuré sur le site de reprise après incident.

La figure suivante illustre la configuration du laboratoire.

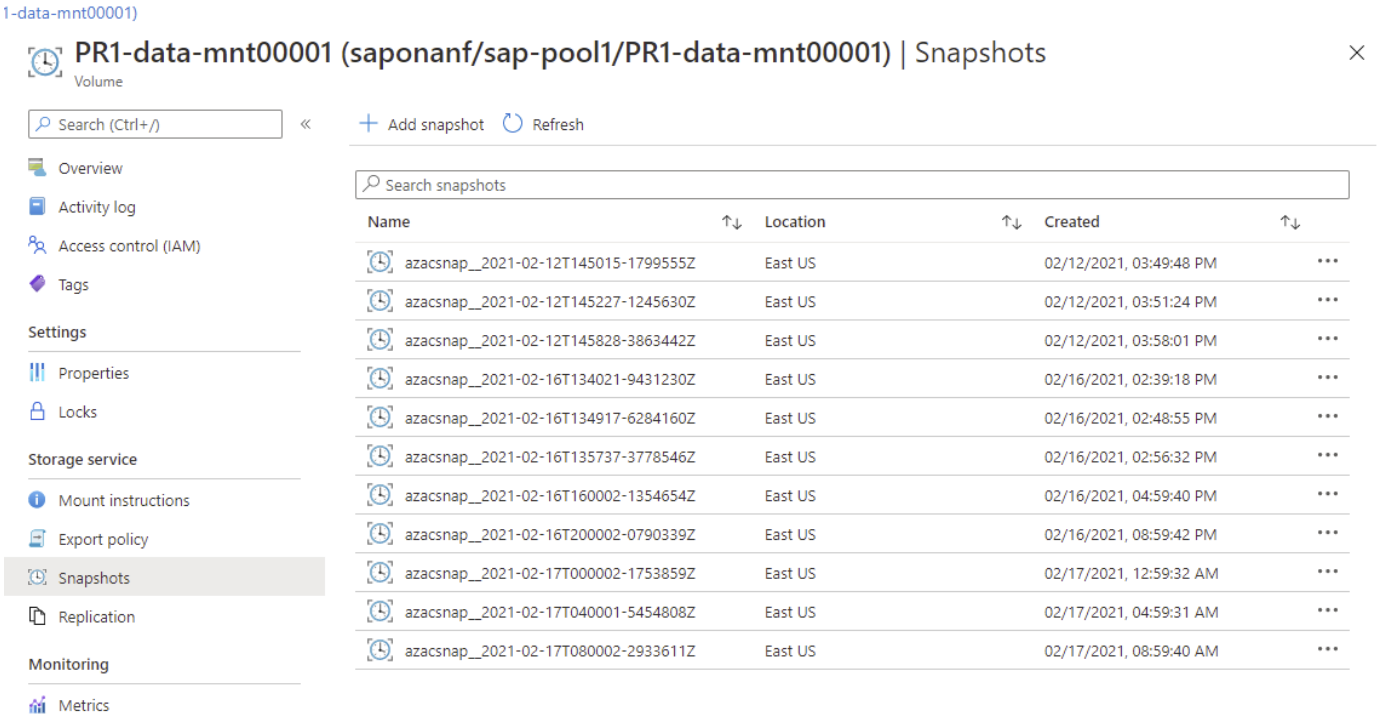


Configuration de sauvegarde Snapshot avec AzAcSnap

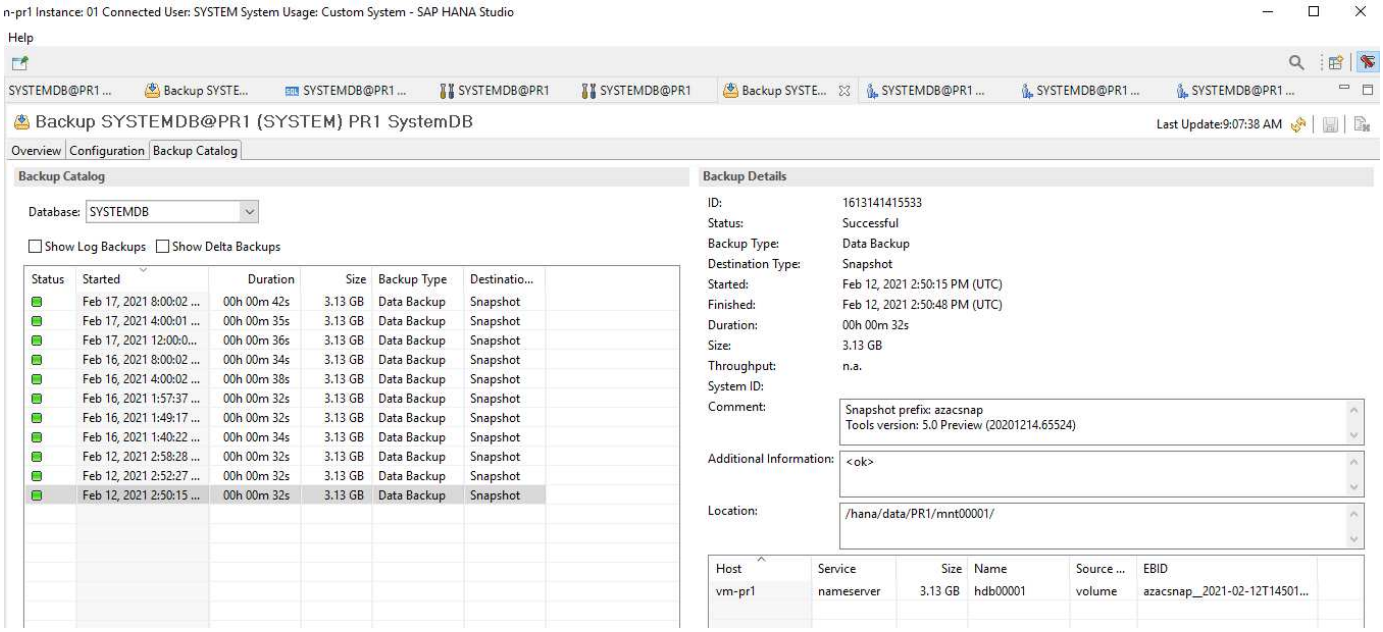
Sur le site principal, AzAcSnap a été configuré pour créer des sauvegardes Snapshot cohérentes au niveau des applications du système HANA PR1. Ces sauvegardes Snapshot sont disponibles au niveau du volume de données ANF du système PR1 HANA et sont également enregistrées dans le catalogue des sauvegardes SAP HANA, comme illustré dans les deux figures suivantes. Des sauvegardes Snapshot ont été planifiées toutes les 4 heures.

Avec la réplication du volume de données à l'aide de la réplication ANF Cross-Region, ces sauvegardes Snapshot sont répliquées sur le site de reprise d'activité et peuvent être utilisées pour restaurer la base de données HANA.

La figure suivante présente les sauvegardes Snapshot du volume de données HANA.



La figure suivante présente le catalogue des sauvegardes SAP HANA.



Étapes de configuration pour la réplication ANF inter-région

Quelques étapes de préparation doivent être effectuées sur le site de reprise d'activité pour que la réplication de volume puisse être configurée.

- Un compte NetApp doit être disponible et configuré avec le même abonnement Azure que la source.
- Un pool de capacité doit être disponible et configuré à l'aide du compte NetApp ci-dessus.
- Un réseau virtuel doit être disponible et configuré.
- Au sein du réseau virtuel, un sous-réseau délégué doit être disponible et configuré pour une utilisation

avec ANF.

Des volumes de protection peuvent désormais être créés pour les données HANA, le partage HANA et le volume de sauvegarde du journal HANA. Le tableau suivant présente les volumes de destination configurés dans notre configuration de laboratoire.

> Pour optimiser la latence, les volumes doivent être placés près des machines virtuelles qui exécutent SAP HANA en cas de basculement. Par conséquent, le même processus de épinglage est requis pour les volumes de reprise après incident et pour tout autre système de production SAP HANA.

Volume HANA	Source	Destination	Planification de la réplication
Volume de données HANA	PR1-data-mnt00001	PR1-data-mnt00001-sm-dest	Tous les jours
Volume partagé HANA	PR1-partagé	PR1-shared-sm-dest	Horaire
Volume de sauvegarde de log/Catalog HANA	hanabackup	hanabackup-sm-dest	Horaire

Pour chaque volume, les étapes suivantes doivent être effectuées :

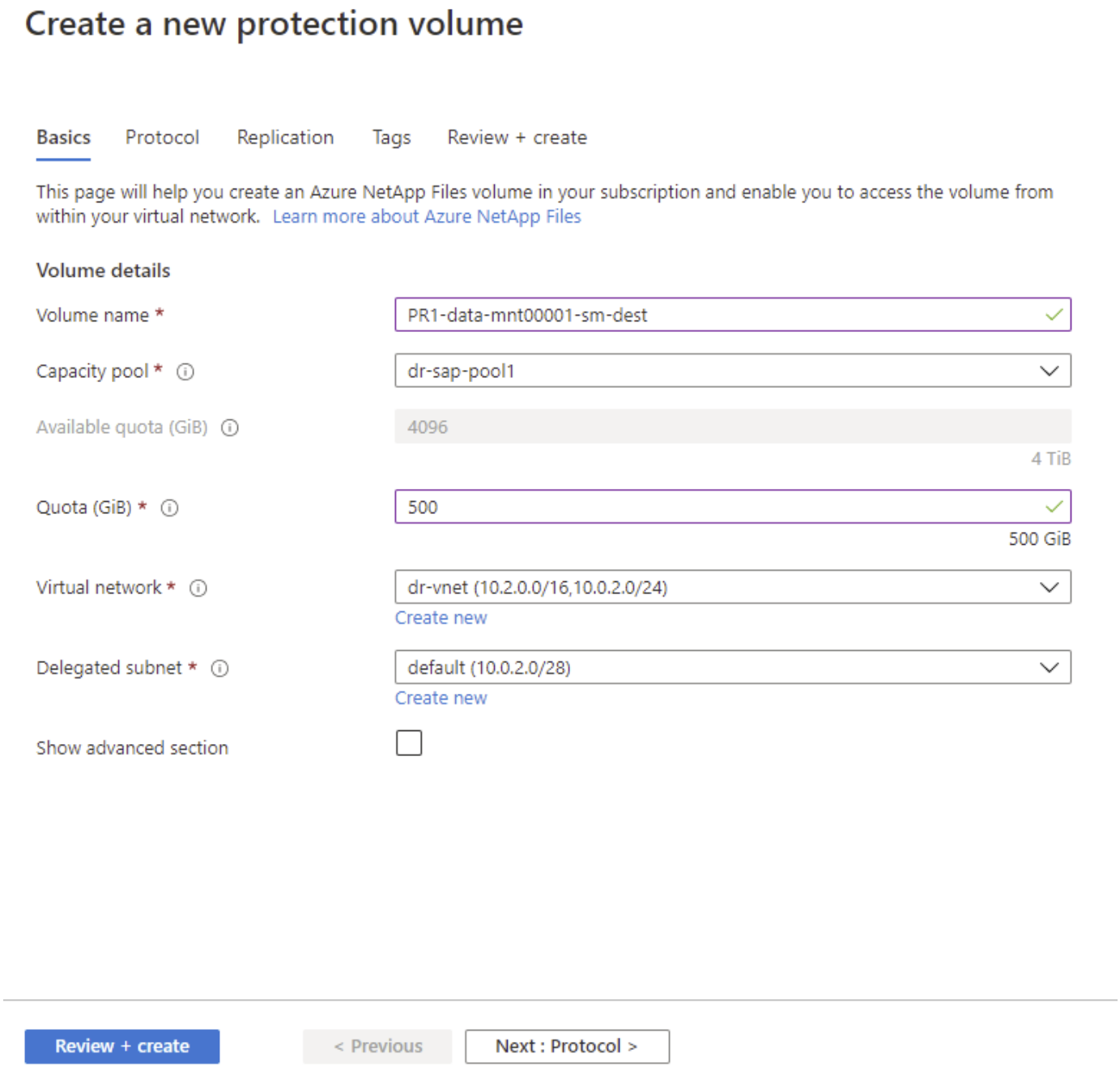
1. Créez un nouveau volume de protection sur le site de reprise après incident :
   a. Indiquez le nom du volume, le pool de capacité, le quota et les informations réseau.
   b. Fournissez le protocole et les informations d'accès aux volumes.
   c. Indiquez l'ID du volume source et la planification de la réplication.
   d. Créer un volume cible.
2. Autoriser la réplication sur le volume source.
   - Indiquez l'ID du volume cible.

Les captures d'écran suivantes montrent en détail les étapes de configuration.

Sur le site de reprise après incident, un nouveau volume de protection est créé en sélectionnant volumes et en cliquant sur Ajouter une réplication des données. Dans l'onglet Basics, vous devez fournir le nom du volume, le pool de capacité et les informations sur le réseau.

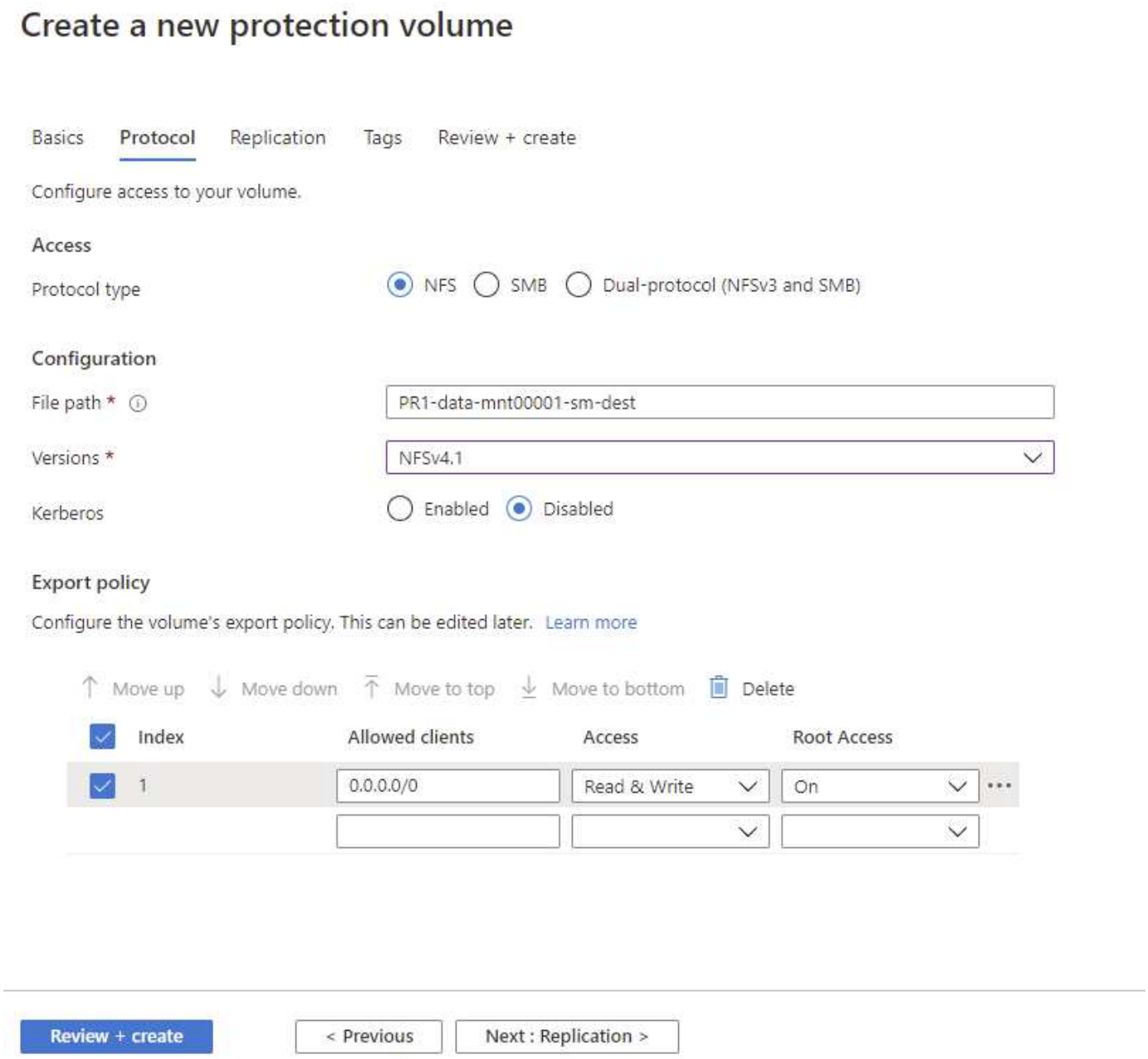
> Le quota du volume peut être défini en fonction des exigences de capacité, car les performances du volume n'ont aucun impact sur le processus de réplication. Dans le cas d'un basculement de reprise après incident, le quota doit être ajusté pour répondre aux exigences de performances réelles.

> Si le pool de capacité a été configuré avec une QoS manuelle, vous pouvez configurer le débit en plus des besoins de capacité. Comme ci-dessus, vous pouvez configurer le débit avec une valeur faible en fonctionnement normal et l'augmenter en cas de basculement de reprise après incident.



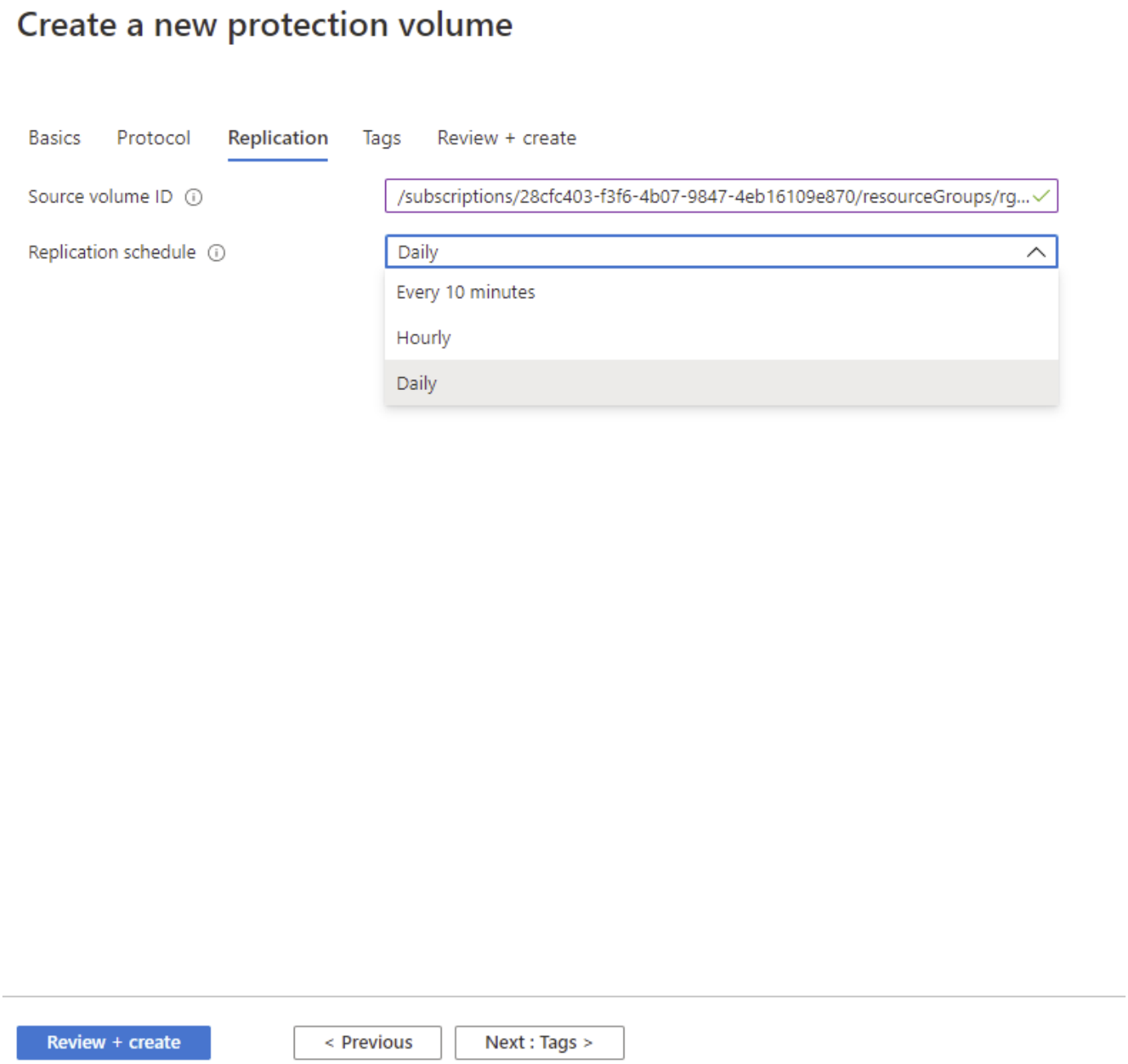
Dans l’onglet Protocol, vous devez fournir le protocole réseau, le chemin du réseau et la export policy.

> Le protocole doit être identique au protocole utilisé pour le volume source.



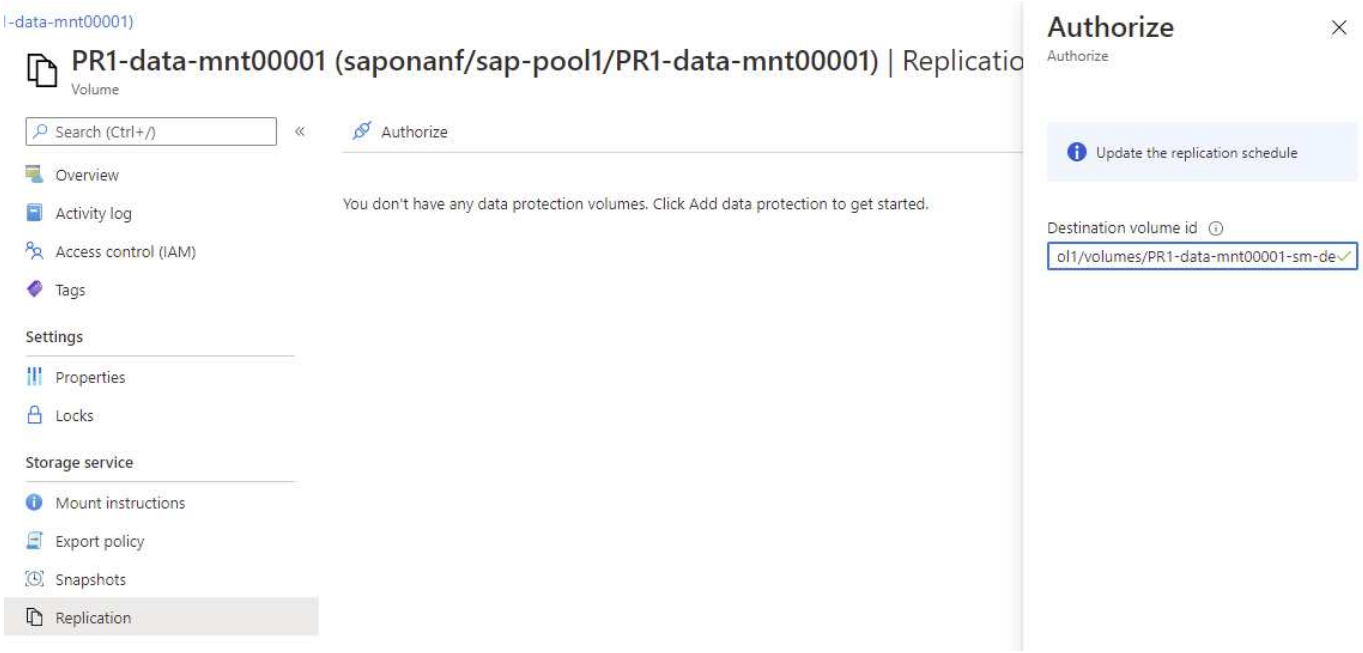
Dans l'onglet réplication, vous devez configurer l'ID du volume source et la planification de réplication. Pour la réplication du volume de données, nous avons configuré une planification de réplication quotidienne pour notre configuration de laboratoire.

L'ID du volume source peut être copié à partir de l'écran Propriétés du volume source.



En dernier lieu, vous devez autoriser la réplication sur le volume source en fournissant l'ID du volume cible.

> Vous pouvez copier l'ID du volume de destination à partir de l'écran Propriétés du volume de destination.



Les mêmes étapes doivent être réalisées pour les systèmes HANA partagés et le volume de sauvegarde du journal.

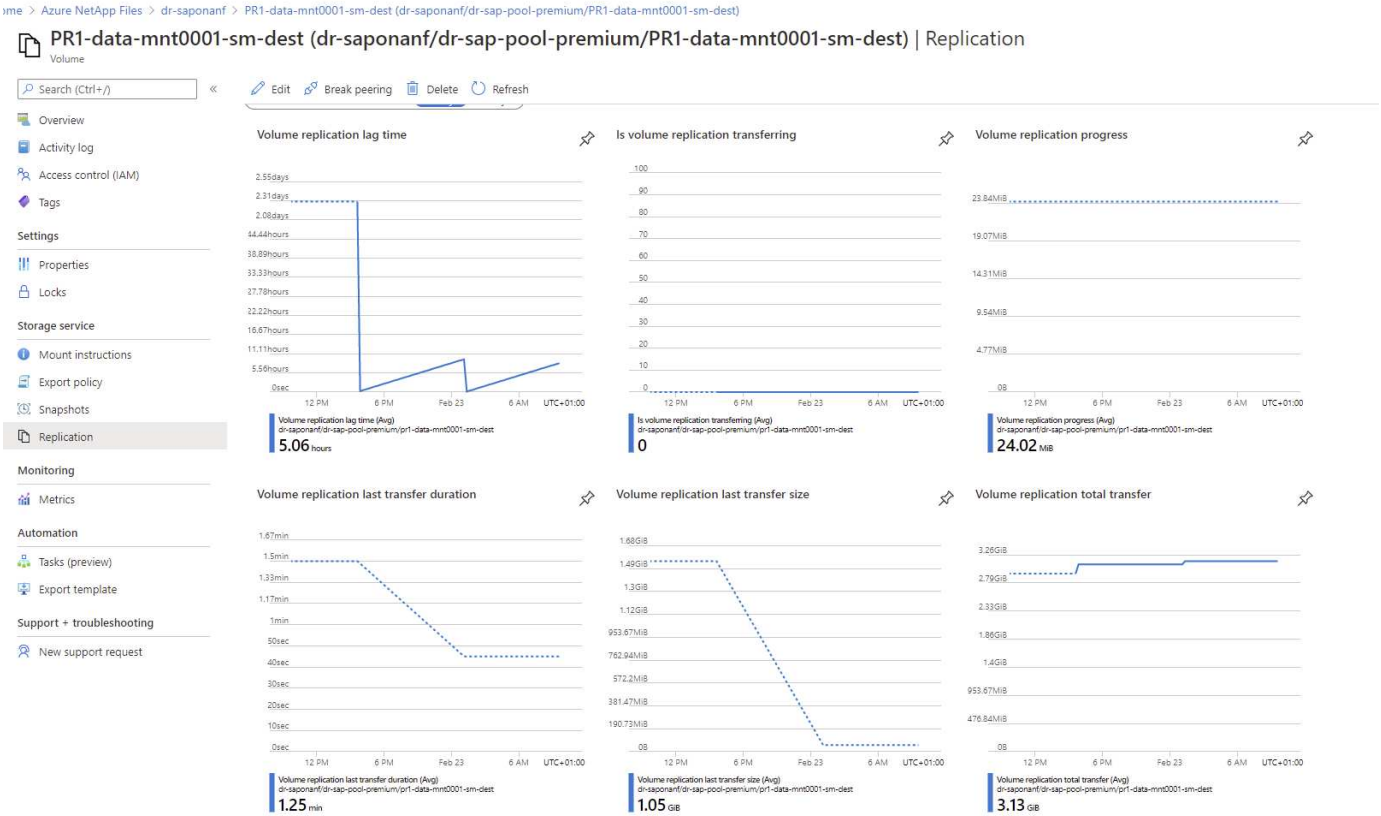
Surveillance de la réplication inter-région ANF

Les trois captures d'écran suivantes indiquent l'état de la réplication pour les données, la sauvegarde du journal et les volumes partagés.

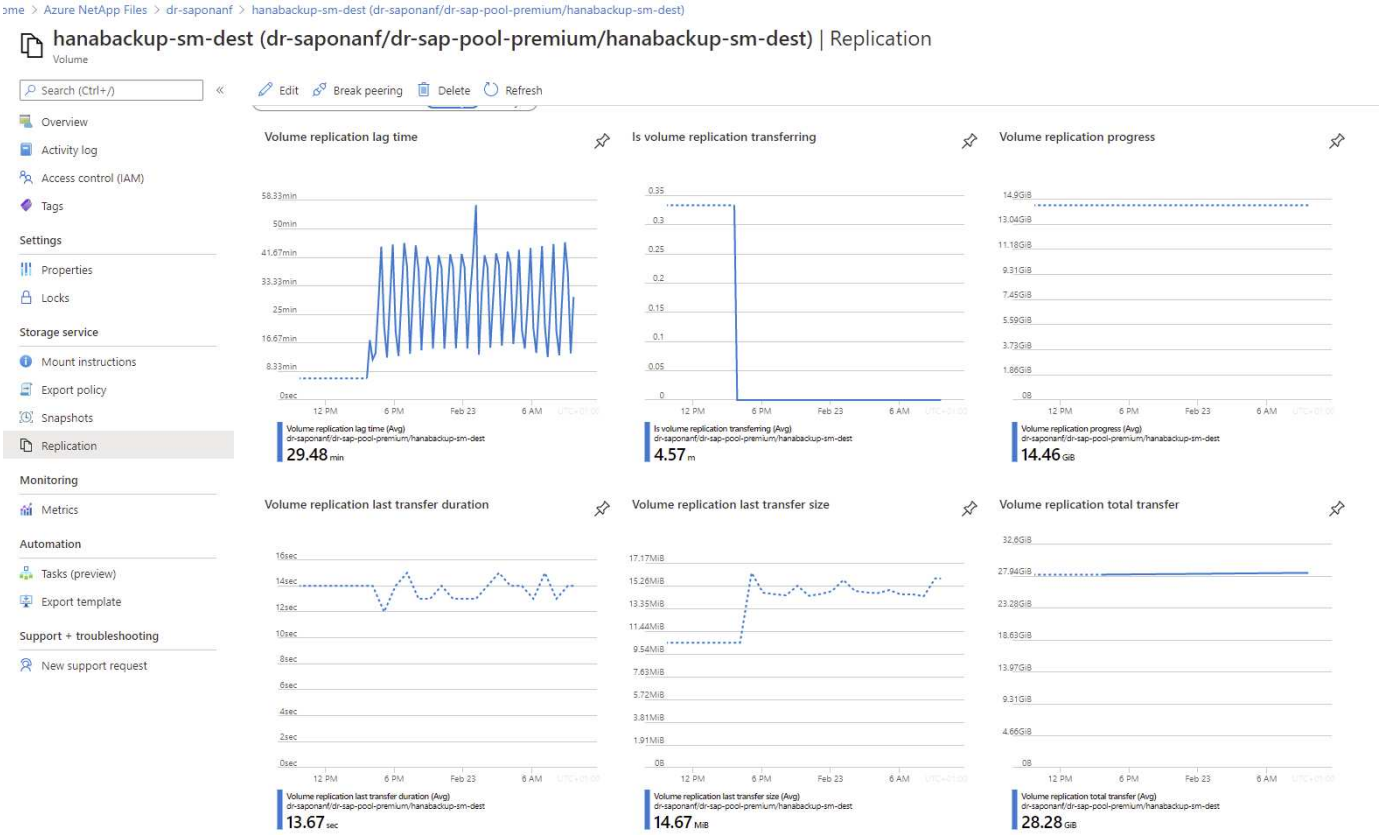
Le délai de réplication du volume est une valeur utile pour comprendre les attentes en matière de RPO. Par exemple, la réplication du volume de sauvegarde des journaux affiche un temps de décalage maximal de 58 minutes, ce qui signifie que l'RPO maximal a la même valeur.

La durée du transfert et la taille du transfert fournissent des informations précieuses sur les besoins en bande passante et modifient le taux du volume répliqué.

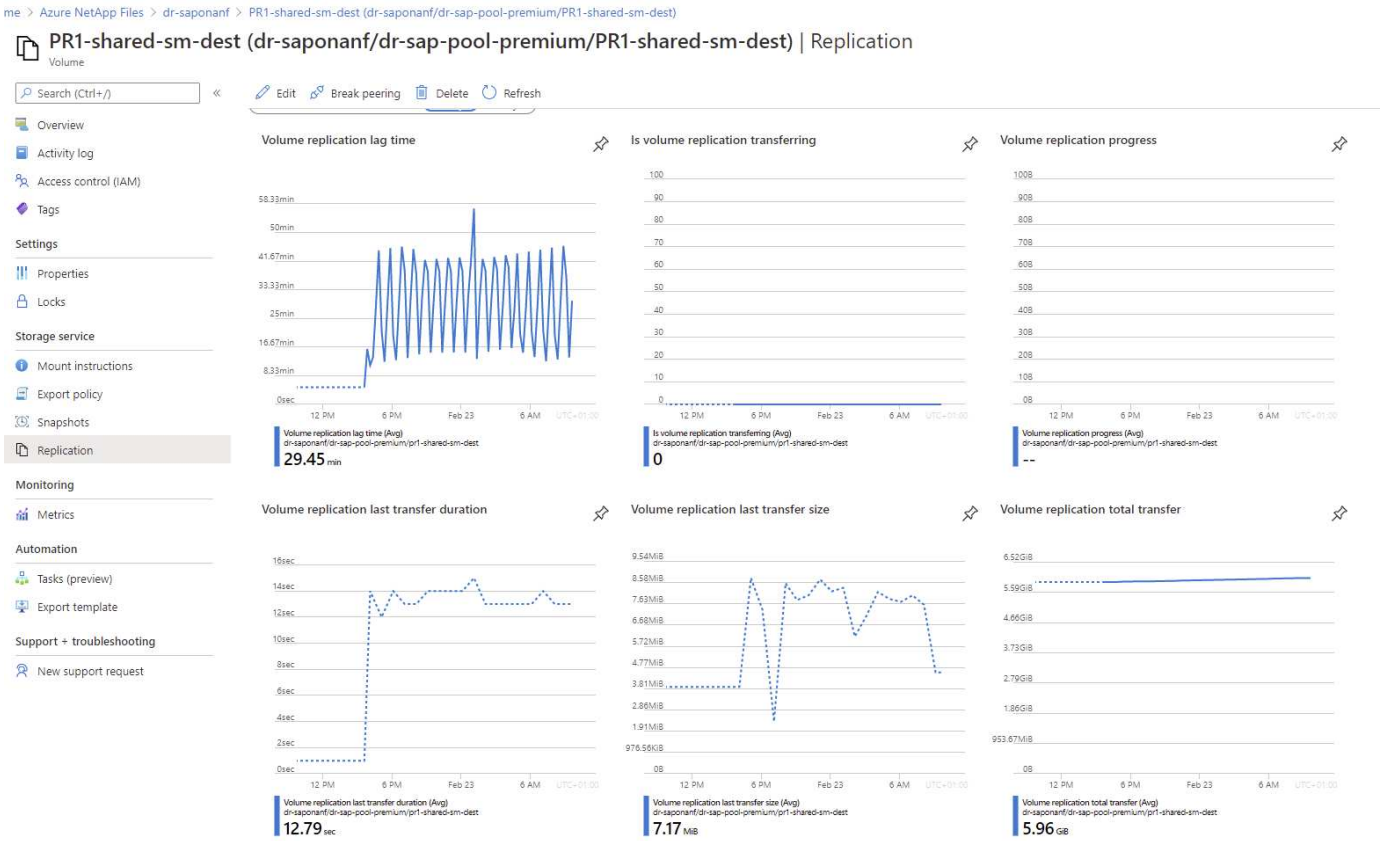
La capture d'écran suivante montre l'état de réplication du volume de données HANA.



La capture d’écran suivante montre l’état de réplication du volume de sauvegarde du journal HANA.



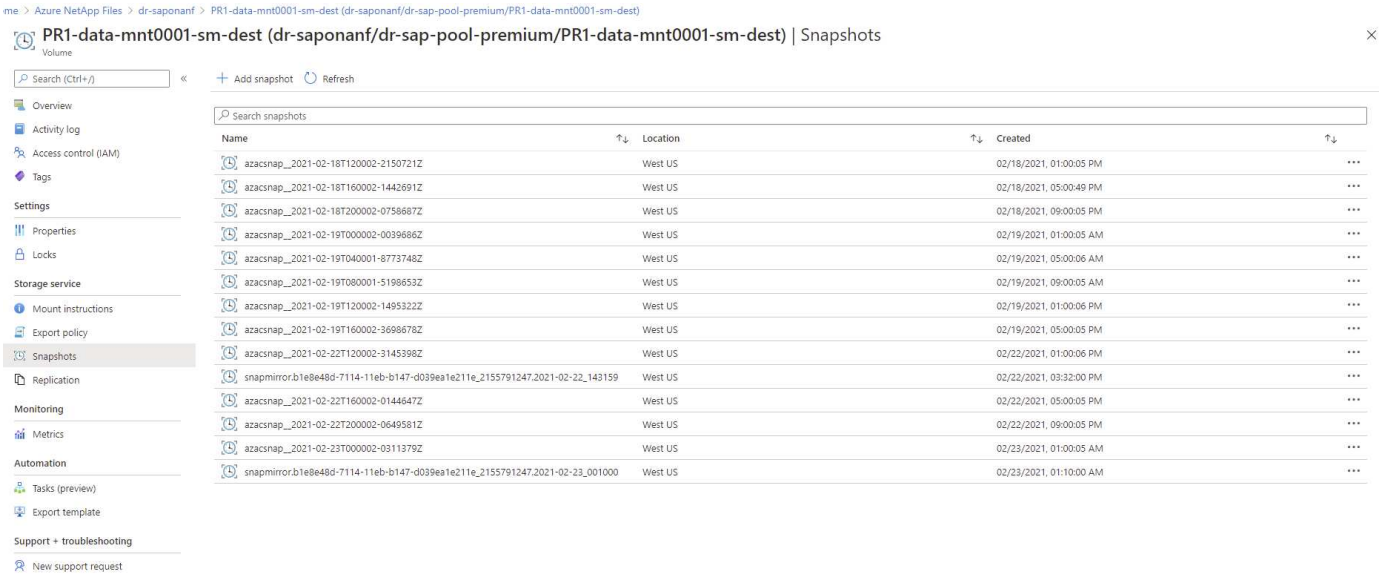
La capture d’écran suivante montre l’état de réplication du volume partagé HANA.



Sauvegardes Snapshot répliquées

À chaque mise à jour de réplication du volume source vers le volume cible, toutes les modifications de bloc effectuées entre le dernier et la mise à jour actuelle sont répliquées vers le volume cible. Les snapshots, qui ont été créés au niveau du volume source, sont également inclus. La capture d'écran suivante montre les snapshots disponibles sur le volume cible. Comme mentionné précédemment, chacun des snapshots créés par l'outil AzAcSnap est des images cohérentes avec les applications de la base de données HANA qui peuvent être utilisées pour exécuter un point de sauvegarde ou une restauration avant.

> Au sein du volume source et du volume cible, des copies Snapshot SnapMirror sont également créées pour les opérations de resynchronisation et de mise à jour de réplication. Ces copies Snapshot ne sont pas cohérentes au niveau de l'application du point de vue de la base de données HANA ; seuls les snapshots cohérents au niveau des applications créés via AzaCSNAP peuvent être utilisés pour les opérations de restauration HANA.



Test de reprise après incident

Test de reprise après incident

Pour mettre en œuvre une stratégie de reprise après incident efficace, vous devez tester le workflow requis. Les tests montrent si la stratégie fonctionne et si la documentation interne est suffisante, et ils permettent également aux administrateurs de suivre les procédures requises.

La réplication interrégion d'ANF permet de tester la reprise après incident sans mettre en péril le RTO et le RPO. Des tests de reprise après incident sont possibles sans interrompre la réplication des données.

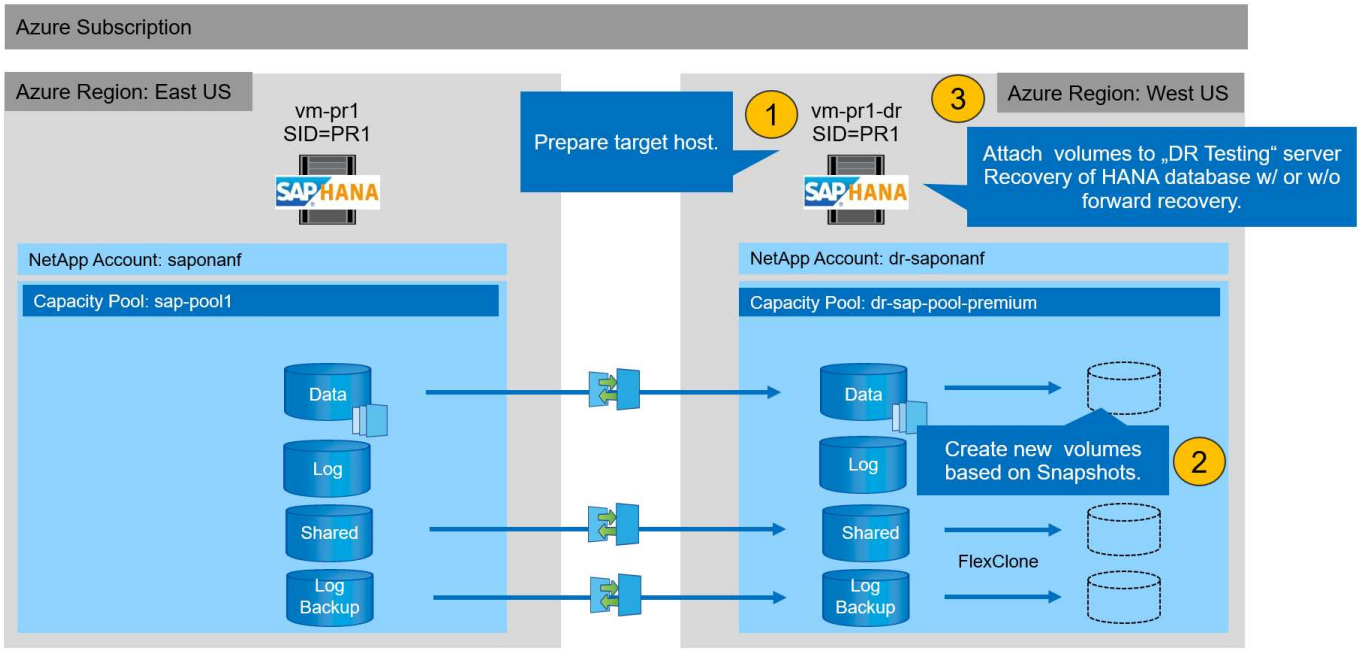
Le workflow de test de reprise d'activité utilise l'ensemble de fonctionnalités ANF pour créer des volumes basés sur des sauvegardes Snapshot existantes à la cible de reprise d'activité. Voir "Fonctionnement des snapshots Azure NetApp Files | Microsoft Docs".

Selon que la réplication des sauvegardes de journaux fait partie de la configuration de la reprise sur incident ou non, les étapes de la reprise sur incident sont légèrement différentes. Cette section décrit les tests de reprise après incident pour la réplication de données uniquement à des fins de sauvegarde, ainsi que pour la réplication de volume de données associée à la réplication de volume de sauvegarde des journaux.

Pour tester la reprise après incident, procédez comme suit :

1. Préparez l'hôte cible.
2. Créer de nouveaux volumes basés sur des sauvegardes Snapshot sur le site de reprise d'activité
3. Montez les nouveaux volumes sur l'hôte cible.
4. Restaurez la base de données HANA.
    - Restauration du volume de données uniquement.
    - Restauration par transfert à l'aide de sauvegardes des journaux répliqués.

Les sous-sections suivantes décrivent ces étapes en détail.



Préparez l’hôte cible

Cette section décrit les étapes de préparation requises au niveau du serveur utilisé pour le test de reprise après incident.

En fonctionnement normal, l’hôte cible est généralement utilisé à d’autres fins, par exemple comme système d’assurance qualité ou de test HANA. Par conséquent, la plupart de ces étapes doivent être effectuées lors d’un test de basculement de reprise d’activité. D’autre part, les fichiers de configuration appropriés, comme `/etc/fstab` et `/usr/sap/sapservices`, peut être préparé puis mis en production en copiant simplement le fichier de configuration. La procédure de test de reprise après sinistre garantit que les fichiers de configuration préparés appropriés sont correctement configurés.

La préparation de l’hôte cible comprend également l’arrêt du système d’assurance qualité ou de test HANA, ainsi que l’arrêt de tous les services à l’aide de `systemctl stop sapinit`.

Nom d’hôte et adresse IP du serveur cible

Le nom d’hôte du serveur cible doit être identique au nom d’hôte du système source. L’adresse IP peut être différente.

> Une clôture correcte du serveur cible doit être établie de sorte qu’il ne puisse pas communiquer avec d’autres systèmes. Si une clôture correcte n’est pas en place, le système de production cloné peut échanger des données avec d’autres systèmes de production, ce qui entraîne une corruption logique des données.

Installez le logiciel requis

Le logiciel de l’agent hôte SAP doit être installé sur le serveur cible. Pour plus d’informations, reportez-vous à la section "Agent hôte SAP" Sur le portail d’aide SAP.

> Si l’hôte est utilisé comme système d’assurance qualité ou de test HANA, le logiciel de l’agent hôte SAP est déjà installé.

Configuration des utilisateurs, des ports et des services SAP

Les utilisateurs et groupes requis pour la base de données SAP HANA doivent être disponibles sur le serveur cible. En général, la gestion centralisée des utilisateurs est utilisée ; aucune étape de configuration n'est donc nécessaire sur le serveur cible. Les ports requis pour la base de données HANA doivent être configurés sur les hôtes cibles. La configuration peut être copiée à partir du système source en copiant `/etc/services` vers le serveur cible.

Les entrées de services SAP requises doivent être disponibles sur l'hôte cible. La configuration peut être copiée à partir du système source en copiant `/usr/sap/sapservices` vers le serveur cible. Le résultat suivant montre les entrées requises pour la base de données SAP HANA utilisée dans la configuration de laboratoire.

```
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
```

Préparez le volume du journal HANA

Comme le volume de journal HANA ne fait pas partie de la réplication, un volume de journal vide doit exister sur l'hôte cible. Le volume de journalisation doit inclure les mêmes sous-répertoires que le système HANA source.

```
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:~ #
```

Préparez le volume de sauvegarde des journaux

Comme le système source est configuré avec un volume distinct pour les sauvegardes de journaux HANA, un volume de sauvegarde de journal doit également être disponible au niveau de l'hôte cible. Un volume pour les sauvegardes des journaux doit être configuré et monté sur l'hôte cible.

Si la réplication du volume de sauvegarde des journaux fait partie de la configuration de reprise d'activité, un nouveau volume basé sur un snapshot est monté sur l'hôte cible, et il n'est pas nécessaire de préparer un volume de sauvegarde supplémentaire des journaux.

Préparer les montages du système de fichiers

Le tableau suivant présente les conventions de nommage utilisées dans la configuration du laboratoire. Les noms de volume des nouveaux volumes du site de reprise d'activité sont inclus dans `/etc/fstab`. Ces noms

de volume sont utilisés à l'étape de création du volume de la section suivante.

Volumes HANA PR1	Nouveau volume et sous-répertoires sur le site de reprise après incident	Point de montage sur l'hôte cible
Volume de données	PR1-data-mnt00001-sm-dest-clone	/hana/data/PR1/mnt00001
Volume partagé	PR1-shared-sm-dest-clone/shared PR1-shared-sm-dest-clone/usr-sap-PR1	/hana/shared /usr/sap/PR1
Volume de sauvegarde du journal	hanabackup-sm-dest-clone	/hanabackup

Les points de montage répertoriés dans ce tableau doivent être créés sur l'hôte cible.

Voici les informations requises `/etc/fstab` entrées.

```
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
```

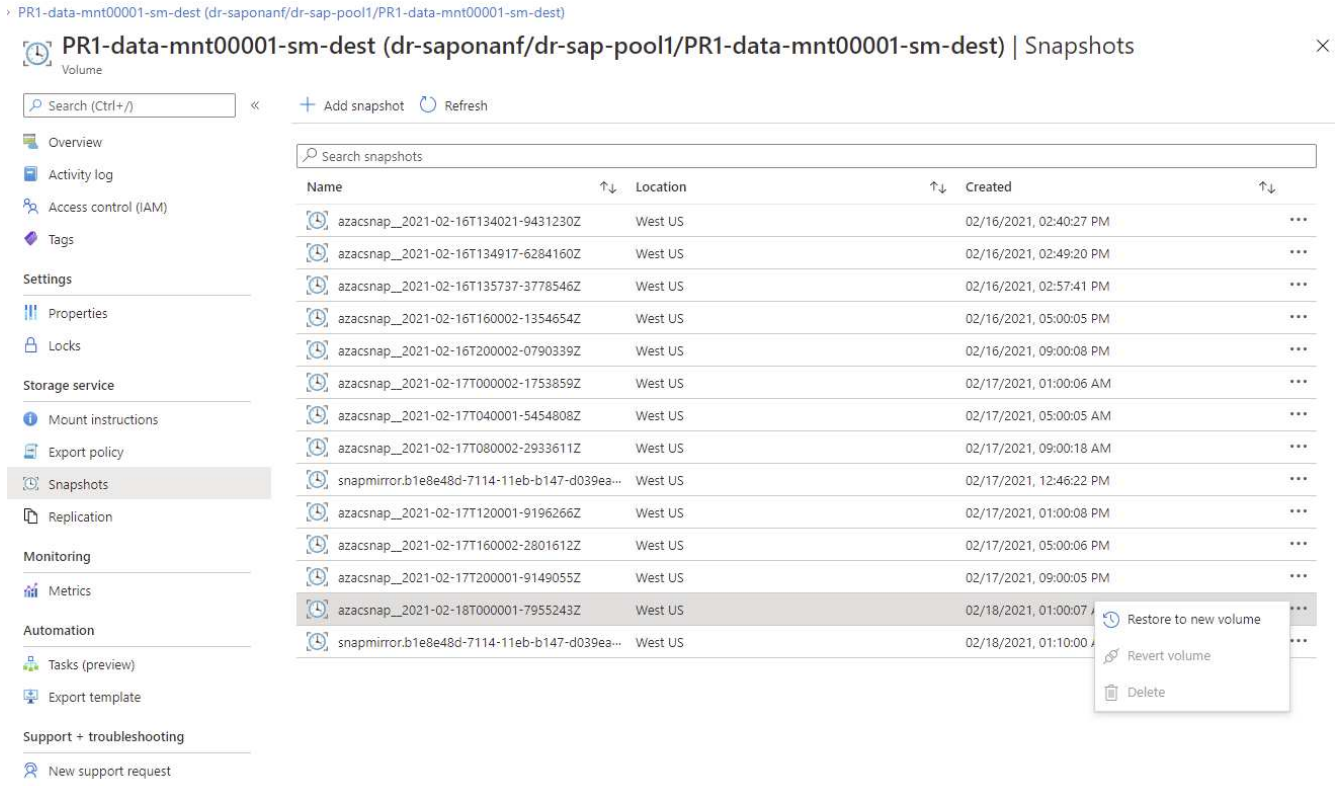
Créer de nouveaux volumes basés sur des sauvegardes Snapshot sur le site de reprise d'activité

Selon la configuration de reprise après incident (avec ou sans réplication de sauvegarde des journaux), il faut créer deux ou trois nouveaux volumes basés sur des sauvegardes Snapshot. Dans les deux cas, un nouveau volume de données et le volume partagé HANA doivent être créés.

Un nouveau volume du volume de sauvegarde des journaux doit être créé si les données de sauvegarde des journaux sont également répliquées. Dans notre exemple, le volume de sauvegarde des données et des

journaux a été répliqué sur le site de reprise sur incident. Voici la procédure à suivre pour utiliser Azure Portal.

1. L'une des sauvegardes Snapshot cohérentes au niveau des applications est sélectionnée comme source pour le nouveau volume du volume de données HANA. L'option Restaurer vers un nouveau volume est sélectionnée pour créer un nouveau volume basé sur la sauvegarde snapshot.



2. Le nouveau nom de volume et quota doivent être fournis dans l'interface utilisateur.

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. Le chemin des fichiers et l’export policy sont configurés dans l’onglet Protocol.

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. L'écran Créer et revoir résume la configuration.

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

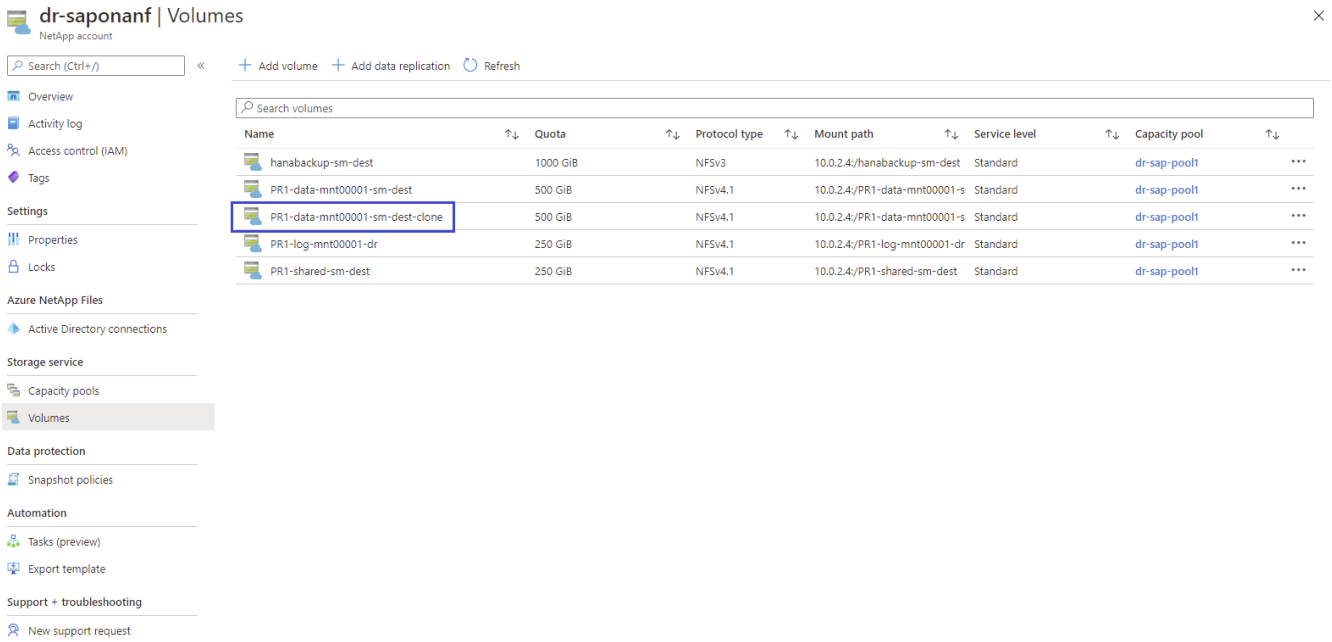
Networking

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

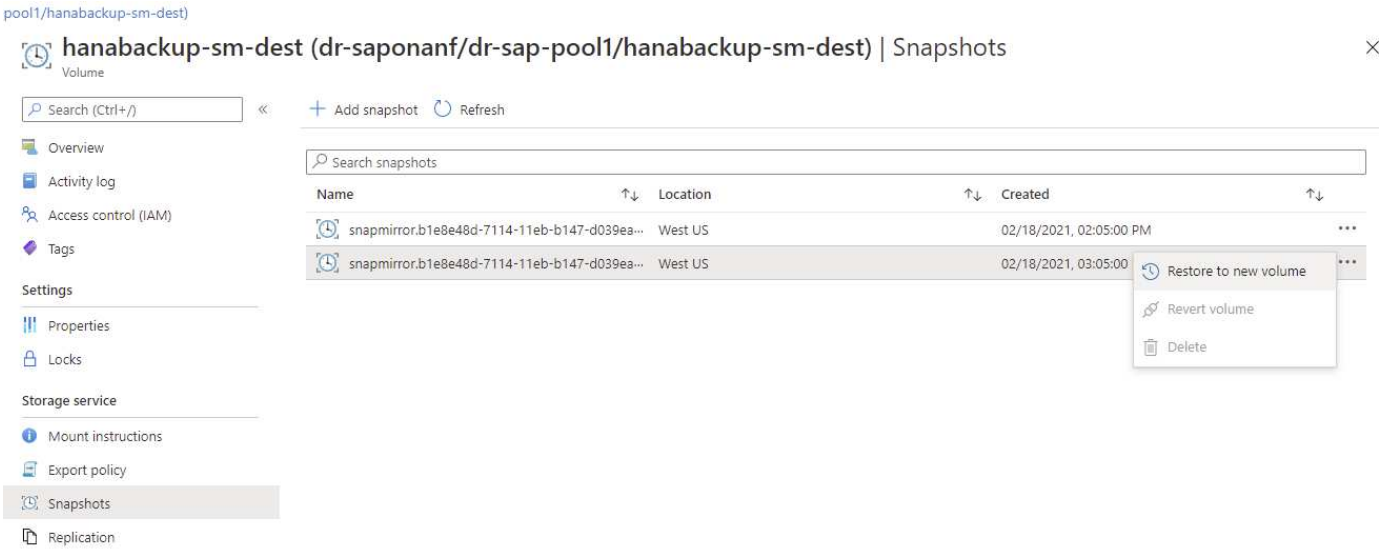
Protocol

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

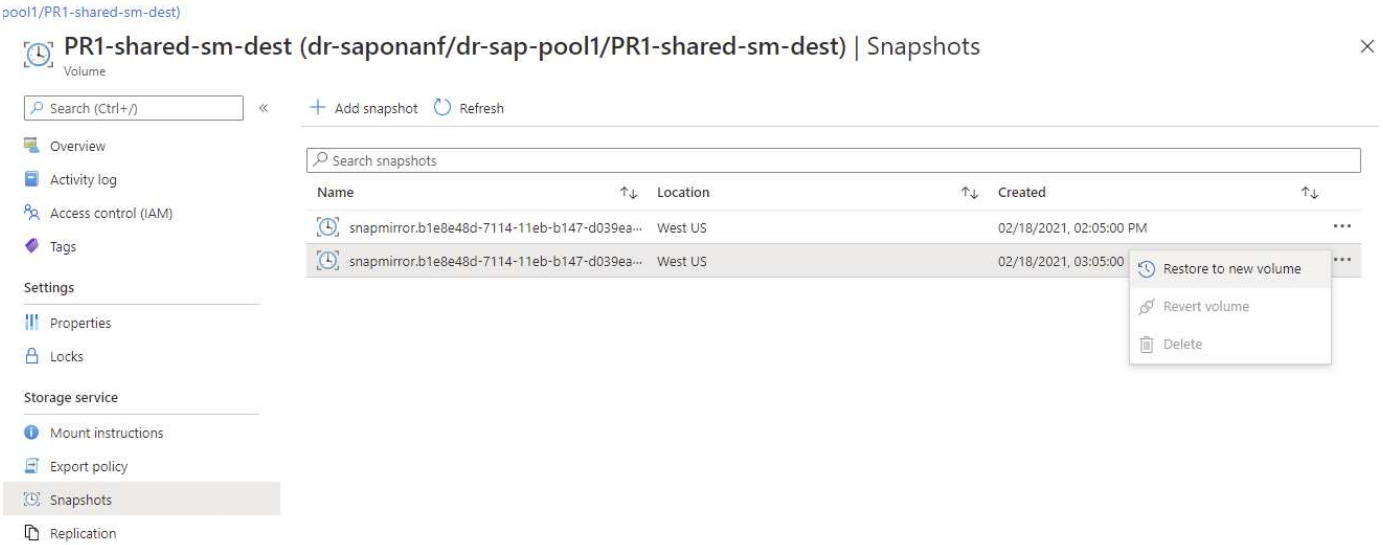
5. Un nouveau volume a été créé à partir de la sauvegarde snapshot HANA.



Il faut maintenant effectuer les mêmes étapes pour les volumes HANA partagés et de sauvegarde des journaux, comme indiqué dans les deux captures d'écran suivantes. Étant donné qu'aucun snapshot supplémentaire n'a été créé pour le volume de sauvegarde de journaux et partagé HANA, la copie Snapshot SnapMirror la plus récente doit être sélectionnée comme source pour le nouveau volume. Il s'agit de données non structurées et la copie Snapshot de SnapMirror peut être utilisée dans ce cas d'utilisation.



La capture d'écran suivante montre le volume partagé HANA restauré vers le nouveau volume.



Lorsqu'un pool de capacité doté d'un niveau de performance faible a été utilisé, les volumes doivent à présent être déplacés vers un pool de capacité qui fournit les performances requises.

Les trois nouveaux volumes sont désormais disponibles et peuvent être montés sur l'hôte cible.

Montez les nouveaux volumes sur l'hôte cible

Les nouveaux volumes peuvent désormais être montés sur l'hôte cible, basé sur le `/etc/fstab` fichier créé précédemment.

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

Le résultat suivant indique les systèmes de fichiers requis.

```
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
```

Restauration des bases de données HANA

Les étapes de la restauration de bases de données HANA sont décrites ci-dessous

Démarrez les services SAP requis.

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

Le résultat suivant indique les processus requis.

```
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
```

Les sous-sections suivantes décrivent le processus de restauration avec et sans récupération à l'aide des sauvegardes des journaux répliqués. La restauration est exécutée à l'aide du script de restauration HANA pour la base de données système et des commandes hdbsql pour la base de données des locataires.

Restauration vers le point de sauvegarde du volume de données HANA le plus récent

La restauration vers le point de sauvegarde le plus récent est exécutée avec les commandes suivantes en tant qu'utilisateur pr1adm :

- Base de données du système

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

- Base de données des locataires

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

Vous pouvez également utiliser HANA Studio ou Cockpit pour exécuter la restauration du système et de la base de données des locataires.

Le résultat de la commande suivante affiche l'exécution de la restauration.

Restauration des bases de données du système

```
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>
```

Restauration des bases de données des locataires

Si aucune clé de magasin utilisateur n’a été créée pour l’utilisateur pr1adm sur le système source, une clé doit être créée sur le système cible. L’utilisateur de base de données configuré dans la clé doit disposer des privilèges nécessaires pour exécuter les opérations de récupération du locataire.

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

La restauration du locataire est maintenant exécutée avec 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 données HANA est à présent opérationnelle, et le workflow de reprise d'activité pour la base de données HANA a été testé.

Restauration par transfert à l'aide des sauvegardes de journaux/catalogues

Les sauvegardes du journal et le catalogue de sauvegardes HANA sont répliquées à partir du système source.

La récupération à l'aide de toutes les sauvegardes de journaux disponibles est exécutée avec les commandes suivantes en tant qu'utilisateur pr1adm :

- Base de données du système

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

- Base de données des locataires

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

> Pour effectuer une restauration à l'aide de tous les journaux disponibles, vous pouvez utiliser à tout moment comme horodatage dans l'instruction de récupération.

Vous pouvez également utiliser HANA Studio ou Cockpit pour exécuter la restauration du système et de la base de données des locataires.

Le résultat de la commande suivante affiche l'exécution de la restauration.

Restauration des bases de données du système

```
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
```

Restauration des bases de données des locataires

```
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 données HANA est à présent opérationnelle, et le workflow de reprise d'activité pour la base de données HANA a été testé.

Vérifier la cohérence des dernières sauvegardes des journaux

La réplication du volume de sauvegarde des journaux étant effectuée indépendamment du processus de sauvegarde des journaux exécuté par la base de données SAP HANA, il peut y avoir des fichiers de sauvegarde des journaux ouverts et incohérents sur le site de reprise d'activité. Seuls les fichiers de sauvegarde des journaux les plus récents peuvent être incohérents, et ces fichiers doivent être vérifiés avant qu'une restauration par transfert ne soit effectuée sur le site de reprise d'activité à l'aide de l' `hdbbackupcheck` outil.

Si le `hdbbackupcheck` l'outil signale une erreur pour les dernières sauvegardes de journaux, le dernier ensemble de sauvegardes de journaux doit être supprimé ou supprimé.

```
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 vérification doit être exécutée pour les fichiers de sauvegarde des journaux les plus récents du système et de la base de données des locataires.

Si le `hdbbackupcheck` l'outil signale une erreur pour les dernières sauvegardes de journaux, le dernier ensemble de sauvegardes de journaux doit être supprimé ou supprimé.

Basculement de reprise d'activité

Basculement de reprise d'activité

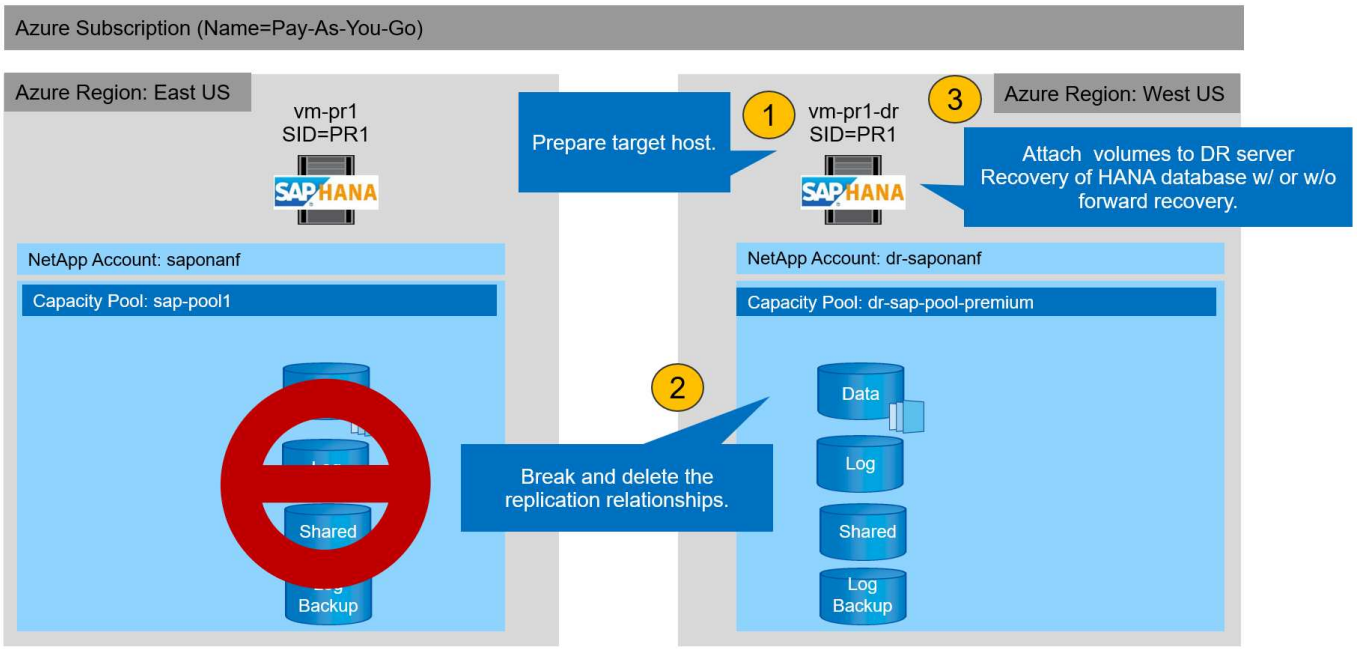
Selon que la réplication de sauvegarde des journaux fait partie de la configuration de reprise sur incident, les étapes de la reprise sur incident sont légèrement différentes. Cette section décrit le basculement de reprise après incident pour la réplication de données uniquement à des fins de sauvegarde, ainsi que pour la réplication de volume de données associée à la réplication de volume de sauvegarde des journaux.

Pour exécuter le basculement de reprise après incident, procédez comme suit :

1. Préparez l'hôte cible.
2. Rompre et supprimer les relations de réplication.
3. Restauration du volume de données vers la dernière sauvegarde Snapshot cohérente avec les applications
4. Montez les volumes sur l'hôte cible.
5. Restaurez la base de données HANA.
    - Restauration du volume de données uniquement.

- Restauration par transfert à l'aide de sauvegardes des journaux répliqués.

Les sous-sections suivantes décrivent ces étapes de manière détaillée, ainsi que la figure suivante décrit les tests de basculement en cas de reprise après incident.



Préparez l'hôte cible

Cette section décrit les étapes de préparation requises au niveau du serveur utilisé pour le basculement de reprise après sinistre.

En fonctionnement normal, l'hôte cible est généralement utilisé à d'autres fins, par exemple comme système d'assurance qualité ou de test HANA. Par conséquent, la plupart des étapes décrites doivent être effectuées lors de l'exécution du test de basculement. D'autre part, les fichiers de configuration appropriés, comme `/etc/fstab` et `/usr/sap/sapservices`, peut être préparé puis mis en production en copiant simplement le fichier de configuration. La procédure de basculement de reprise après sinistre garantit que les fichiers de configuration préparés appropriés sont correctement configurés.

La préparation de l'hôte cible comprend également l'arrêt du système d'assurance qualité ou de test HANA, ainsi que l'arrêt de tous les services à l'aide de `systemctl stop sapinit`.

Nom d'hôte et adresse IP du serveur cible

Le nom d'hôte du serveur cible doit être identique au nom d'hôte du système source. L'adresse IP peut être différente.

> Une clôture correcte du serveur cible doit être établie de sorte qu'il ne puisse pas communiquer avec d'autres systèmes. Si une clôture correcte n'est pas en place, le système de production cloné peut échanger des données avec d'autres systèmes de production, ce qui entraîne une corruption logique des données.

Installez le logiciel requis

Le logiciel de l'agent hôte SAP doit être installé sur le serveur cible. Pour plus d'informations, reportez-vous à la section "Agent hôte SAP" Sur le portail d'aide SAP.

> Si l'hôte est utilisé comme système d'assurance qualité ou de test HANA, le logiciel de l'agent hôte SAP est déjà installé.

Configuration des utilisateurs, des ports et des services SAP

Les utilisateurs et groupes requis pour la base de données SAP HANA doivent être disponibles sur le serveur cible. En général, la gestion centralisée des utilisateurs est utilisée ; aucune étape de configuration n'est donc nécessaire sur le serveur cible. Les ports requis pour la base de données HANA doivent être configurés sur les hôtes cibles. La configuration peut être copiée à partir du système source en copiant `/etc/services` vers le serveur cible.

Les entrées de services SAP requises doivent être disponibles sur l'hôte cible. La configuration peut être copiée à partir du système source en copiant `/usr/sap/sapservices` vers le serveur cible. Le résultat suivant montre les entrées requises pour la base de données SAP HANA utilisée dans la configuration de laboratoire.

```
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
```

Préparez le volume du journal HANA

Comme le volume de journal HANA ne fait pas partie de la réplication, un volume de journal vide doit exister sur l'hôte cible. Le volume de journalisation doit inclure les mêmes sous-répertoires que le système HANA source.

```
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:~ #
```

Préparez le volume de sauvegarde des journaux

Comme le système source est configuré avec un volume distinct pour les sauvegardes de journaux HANA, un volume de sauvegarde de journal doit également être disponible au niveau de l'hôte cible. Un volume pour les sauvegardes des journaux doit être configuré et monté sur l'hôte cible.

Si la réplication du volume de sauvegarde des journaux fait partie de la configuration de reprise après incident, le volume de sauvegarde des journaux répliqués est monté sur l'hôte cible, et il n'est pas nécessaire de préparer un volume de sauvegarde de journaux supplémentaire.

Préparer les montages du système de fichiers

Le tableau suivant présente les conventions de nommage utilisées dans la configuration du laboratoire. Les noms des volumes du site de reprise d'activité sont inclus dans la `/etc/fstab`.

Volumes HANA PR1	Volume et sous-répertoires du site de reprise après incident	Point de montage sur l'hôte cible
Volume de données	PR1-data-mnt00001-sm-dest	/hana/data/PR1/mnt00001
Volume partagé	PR1-shared-sm-dest/shared PR1-shared-sm-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Volume de sauvegarde du journal	hanabackup-sm-dest	/hanabackup

Les points de montage de cette table doivent être créés sur l'hôte cible.

Voici les informations requises `/etc/fstab` entrées.

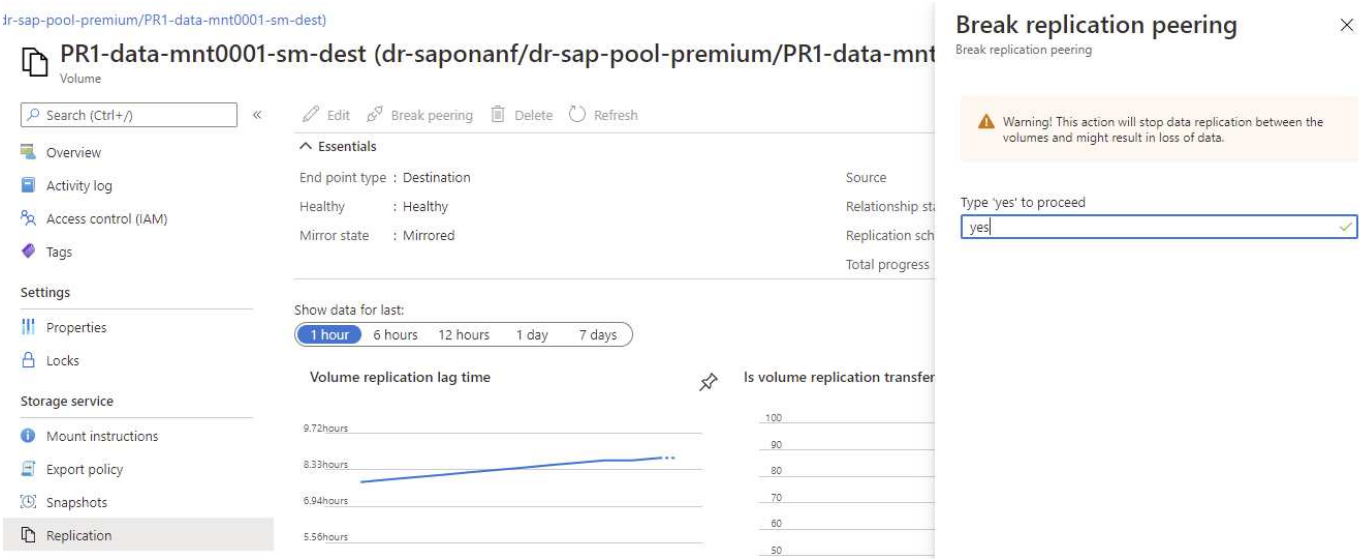
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
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
```

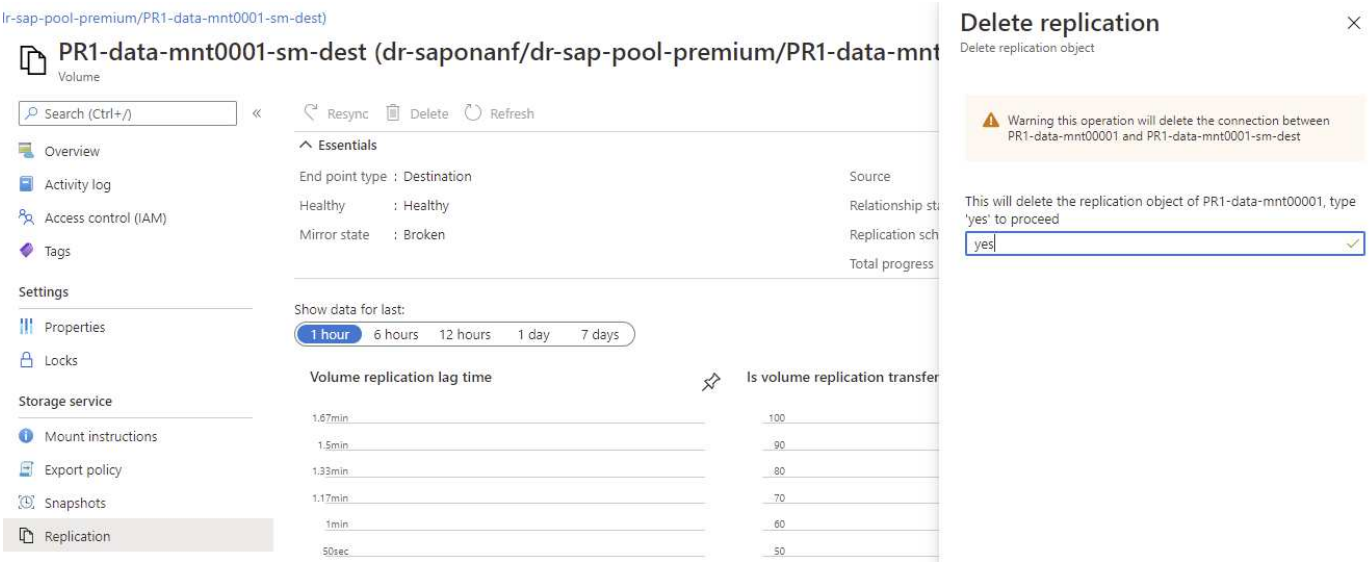
Interrompre et supprimer le peering de réplication

En cas de basculement après incident, les volumes cibles doivent être désactivés afin que l'hôte cible puisse monter les volumes pour les opérations de lecture et d'écriture.

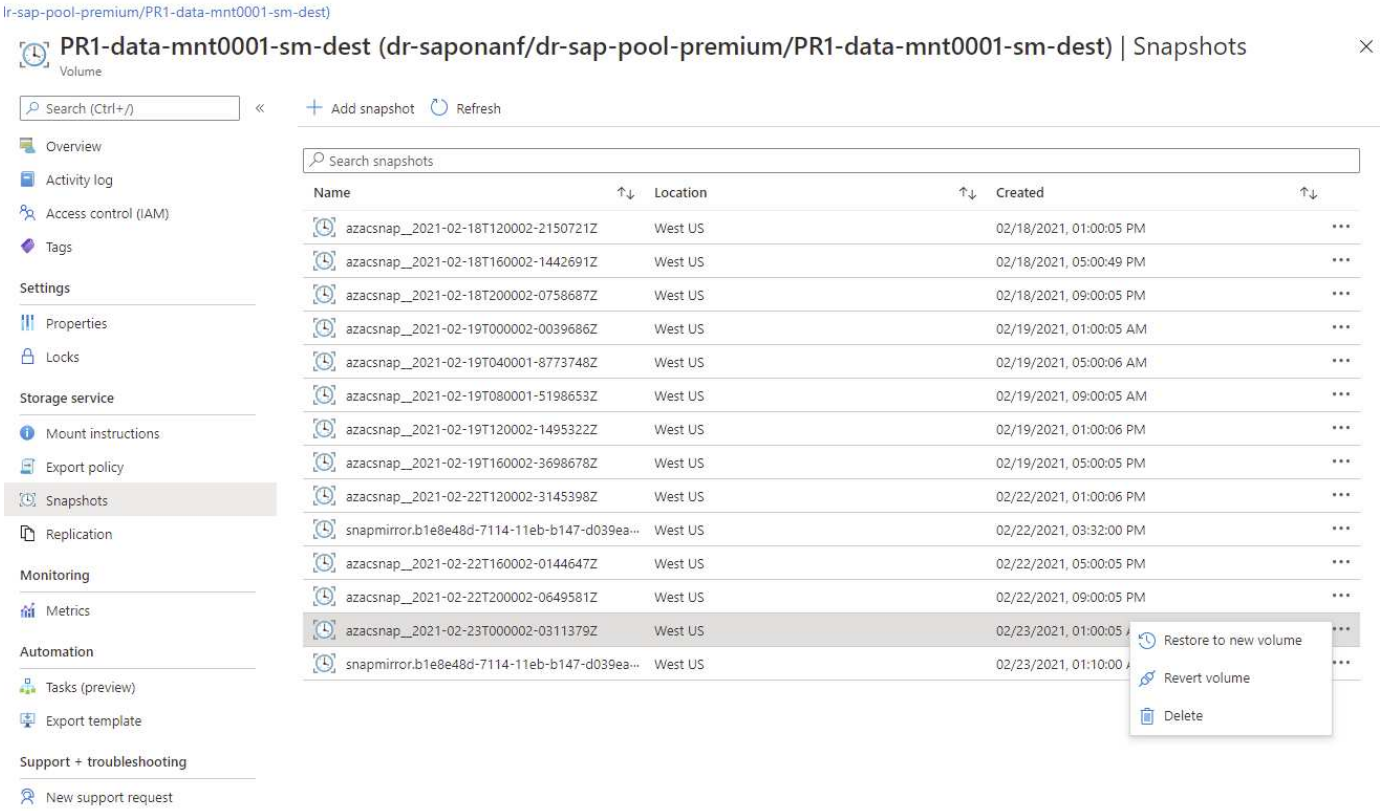
Pour le volume de données HANA, vous devez restaurer le volume vers la dernière sauvegarde Snapshot HANA créée avec AzAcSnap. Cette opération de restauration de volume n'est pas possible si le snapshot de réplication le plus récent est marqué comme étant occupé en raison du peering de réplication. Par conséquent, vous devez également supprimer le peering de réplication.

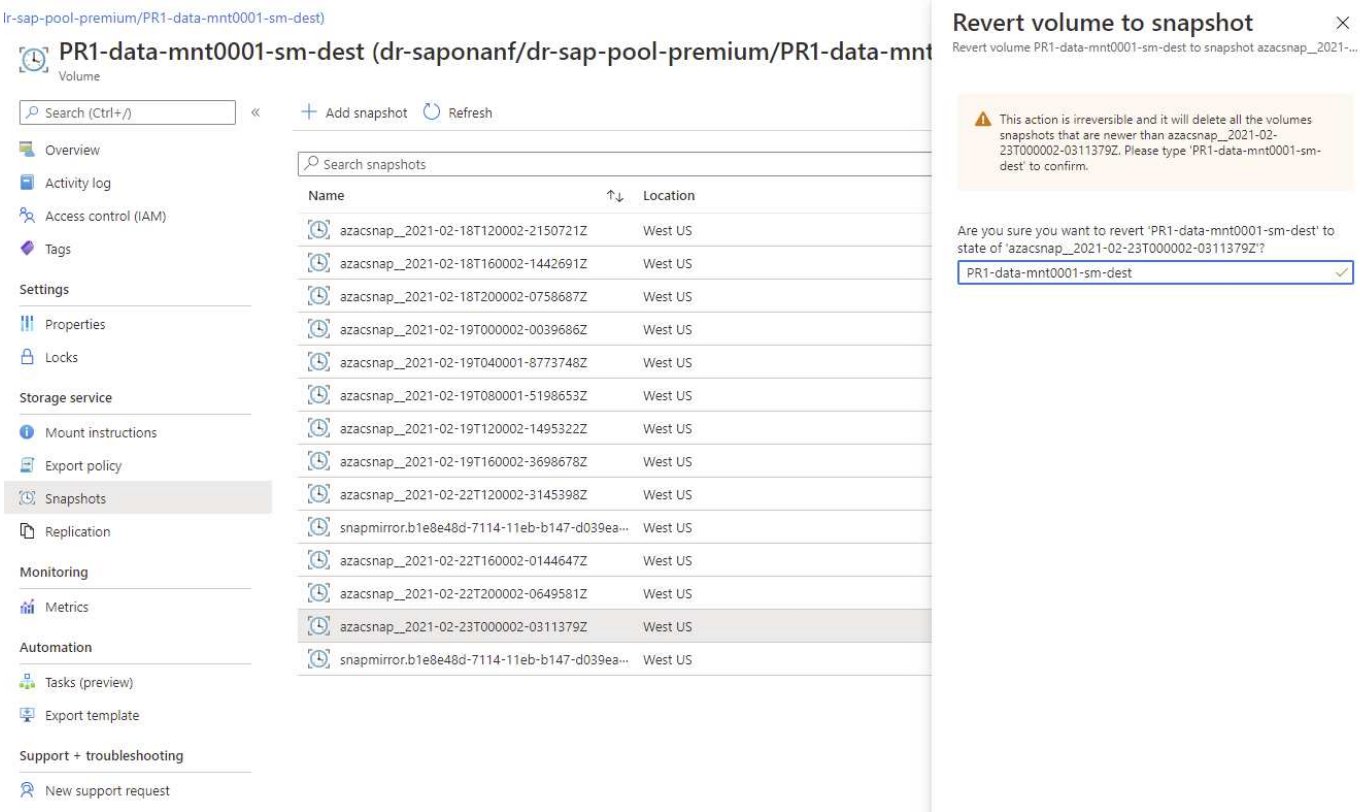
Les deux captures d'écran suivantes montrent l'opération de peering et de suppression pour le volume de données HANA. Les mêmes opérations doivent être effectuées pour la sauvegarde du journal et le volume partagé HANA.





Le peering de réplication ayant été supprimé, il est possible de restaurer le volume vers la dernière sauvegarde Snapshot HANA. Si le peering n'est pas supprimé, la sélection du volume revert est grisée et ne peut pas être sélectionnée. Les deux captures d'écran suivantes montrent l'opération de restauration du volume.





Une fois le volume revert, le volume de données repose sur la sauvegarde Snapshot HANA cohérente et peut maintenant être utilisé pour exécuter les opérations de restauration par progression.

Lorsqu'un pool de capacité doté d'un niveau de performance faible a été utilisé, les volumes doivent à présent être déplacés vers un pool de capacité capable d'assurer les performances requises.

Montez les volumes sur l'hôte cible

Les volumes peuvent désormais être montés sur l'hôte cible, basé sur `/etc/fstab` fichier créé précédemment.

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

Le résultat suivant indique les systèmes de fichiers requis.

```
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:~ #
```

Restauration des bases de données HANA

Les étapes suivantes sont décrites pour la restauration de bases de données HANA.

Démarrez les services SAP requis.

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

Le résultat suivant indique les processus requis.

```
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
```

Les sous-sections suivantes décrivent le processus de restauration avec récupération avant à l'aide des sauvegardes des journaux répliqués. La restauration est exécutée à l'aide du script de restauration HANA pour la base de données système et des commandes hdbsql pour la base de données des locataires.

Les commandes permettant d'exécuter une restauration vers le dernier point de sauvegarde de données sont décrites au chapitre "Restauration vers le point de sauvegarde du volume de données HANA le plus récent".

Récupération avec récupération par transfert à l'aide de sauvegardes de journaux

La récupération à l'aide de toutes les sauvegardes de journaux disponibles est exécutée avec les commandes suivantes en tant qu'utilisateur pr1adm :

- Base de données du système

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

- Base de données des locataires

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

> Pour effectuer une restauration à l'aide de tous les journaux disponibles, vous pouvez utiliser à tout moment comme horodatage dans l'instruction de récupération.

Vous pouvez également utiliser HANA Studio ou Cockpit pour exécuter la restauration du système et de la base de données des locataires.

Le résultat de la commande suivante affiche l'exécution de la restauration.

Restauration des bases de données du système

```
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>
```

Restauration des bases de données des locataires

Si aucune clé de magasin utilisateur n’a été créée pour l’utilisateur pr1adm sur le système source, une clé doit être créée sur le système cible. L’utilisateur de base de données configuré dans la clé doit disposer des privilèges nécessaires pour exécuter les opérations de récupération du locataire.

```
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=>
```

Vérifier la cohérence des dernières sauvegardes des journaux

La réplication du volume de sauvegarde des journaux étant effectuée indépendamment du processus de sauvegarde des journaux exécuté par la base de données SAP HANA, il peut y avoir des fichiers de sauvegarde des journaux ouverts et incohérents sur le site de reprise d'activité. Seuls les fichiers de sauvegarde des journaux les plus récents peuvent être incohérents, et ces fichiers doivent être vérifiés avant qu'une restauration par transfert ne soit effectuée sur le site de reprise d'activité à l'aide de l' `hdbbackupcheck` outil.

```
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 vérification doit être exécutée pour les fichiers de sauvegarde des journaux les plus récents du système et de la base de données des locataires.

Si le `hdbbackupcheck` l'outil signale une erreur pour les dernières sauvegardes de journaux, le dernier ensemble de sauvegardes de journaux doit être supprimé ou supprimé.

Historique des mises à jour

Les modifications techniques suivantes ont été apportées à cette solution depuis sa publication initiale.

Version	Date	Mettre à jour le résumé
Version 1.0	Avril 2021	Version initiale

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.