Sauvegarde, restauration et reprise après incident

NetApp Solutions SAP

NetApp
June 27, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions-sap/backup/amazon-fsx-overview.html on June 27, 2024. Always check docs.netapp.com for the latest.

Sommaire

Sauvegarde, restauration et reprise après incident

SAP HANA sur Amazon FSX pour NetApp ONTAP - sauvegarde et restauration avec SnapCenter

Tr-4926 : SAP HANA sur Amazon FSX pour NetApp ONTAP - sauvegarde et restauration avec SnapCenter

Nils Bauer, NetApp

Dans ce rapport technique, vous bénéficiez des meilleures pratiques en matière de protection des données SAP HANA sur Amazon FSX pour NetApp ONTAP et NetApp SnapCenter. Ce document présente les concepts relatifs à SnapCenter, les recommandations sur la configuration et les workflows d'exploitation, y compris la configuration, les opérations de sauvegarde et les opérations de restauration et de reprise.

Les entreprises ont besoin aujourd'hui d'une disponibilité continue et sans interruption pour leurs applications SAP. Elles espèrent obtenir des niveaux de performance prévisibles dans un contexte où les volumes de données ne cessent d'augmenter et nécessitent des tâches de maintenance de routine, comme les sauvegardes système. Le fait d'effectuer des sauvegardes de bases de données SAP est une tâche critique qui peut avoir un impact significatif sur les performances du système SAP de production.

Les fenêtres de sauvegarde diminuent alors que le volume des données à sauvegarder augmente. Par conséquent, il est difficile de trouver un moment où vous pouvez effectuer des sauvegardes avec un impact minimal sur les processus de l'entreprise. Le temps nécessaire à la restauration et à la restauration des systèmes SAP pose problème, car les temps d'indisponibilité des systèmes de production et hors production SAP doivent être réduits de manière à réduire les coûts pour l'entreprise.

Sauvegarde et restauration avec Amazon FSX pour ONTAP

Vous pouvez utiliser la technologie Snapshot de NetApp pour créer des sauvegardes de bases de données en quelques minutes.

Le temps nécessaire à la création d'une copie Snapshot ne dépend pas de la taille de la base de données, car cette copie ne déplace aucun bloc de données sur la plateforme de stockage. De plus, cette technologie n'a aucune incidence sur les performances du système SAP en direct. Par conséquent, vous pouvez planifier la création de copies Snapshot sans tenir compte des périodes de pointe de dialogue ou d'activité de lots. Les clients de SAP et de NetApp programraient généralement plusieurs sauvegardes Snapshot en ligne pendant la journée, par exemple, toutes les six heures sont fréquentes. Ces sauvegardes Snapshot sont généralement conservées pendant trois à cinq jours sur le système de stockage principal avant d'être supprimées ou hiérarchisées vers un stockage moins coûteux pour une conservation à long terme.

Les copies Snapshot offrent également des avantages clés pour les opérations de restauration et de reprise. La technologie NetApp SnapRestore permet de restaurer l'ensemble d'une base de données ou, alternativement, une partie d'une base de données à un point dans le temps, en fonction des copies Snapshot actuellement disponibles. Ce processus ne dure que quelques secondes, quelle que soit la taille de la base de données. Comme plusieurs sauvegardes Snapshot en ligne peuvent être créées chaque jour, le délai nécessaire pour le processus de restauration est considérablement réduit par rapport à une sauvegarde traditionnelle une fois par jour. Comme vous pouvez effectuer une restauration à l'aide d'une copie Snapshot datant au plus de quelques heures (au lieu de 24 heures), il faut moins d'journaux de transaction lors de la restauration par transfert. L'objectif RTO est donc réduit à plusieurs minutes, au lieu de plusieurs heures

requises pour les sauvegardes de streaming conventionnelles.

Les sauvegardes de copie Snapshot sont stockées sur le même système de disque que les données en ligne actives. Par conséquent, NetApp recommande d'utiliser les sauvegardes de copies Snapshot comme supplément plutôt que comme remplacement des sauvegardes sur un emplacement secondaire. La plupart des actions de restauration et de récupération sont gérées à l'aide de SnapRestore sur le système de stockage primaire. Les restaurations depuis un emplacement secondaire sont uniquement nécessaires si le système de stockage primaire contenant les copies Snapshot est endommagé. Vous pouvez également utiliser l'emplacement secondaire s'il est nécessaire de restaurer une sauvegarde qui n'est plus disponible sur l'emplacement principal.

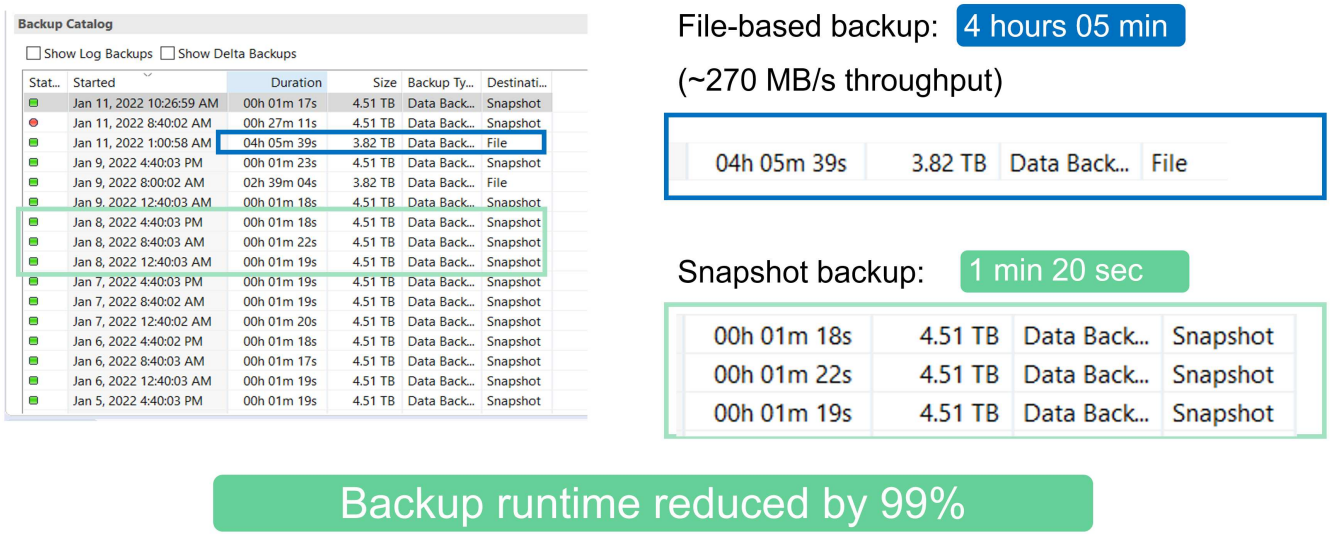
Une sauvegarde vers un emplacement secondaire repose sur des copies Snapshot créées sur le système de stockage primaire. Par conséquent, les données sont lues directement depuis le système de stockage primaire sans générer de charge sur le serveur de base de données SAP. Le stockage primaire communique directement avec le stockage secondaire et réplique les données de sauvegarde vers la destination via la fonction NetApp SnapVault.

SnapVault offre des avantages significatifs par rapport aux sauvegardes traditionnelles. Après le transfert initial des données, dans lequel toutes les données ont été transférées de la source vers la destination, toutes les sauvegardes ultérieures copient uniquement les blocs modifiés vers le stockage secondaire. Par conséquent, la charge sur le système de stockage primaire et le temps nécessaire à une sauvegarde complète sont considérablement réduits. Étant donné que SnapVault stocke uniquement les blocs modifiés au niveau de la destination, toute sauvegarde de bases de données complètes supplémentaire consomme beaucoup moins d'espace disque.

Exécution des opérations de sauvegarde et de restauration Snapshot

La figure suivante illustre HANA Studio d'un client utilisant des opérations de sauvegarde Snapshot. L'image montre que la base de données HANA (environ 4 To de taille) est sauvegardée en 1 minute et 20 secondes à l'aide de la technologie de sauvegarde Snapshot, et plus de 4 heures avec une opération de sauvegarde basée sur des fichiers.

La majeure partie du temps d'exécution du workflow de sauvegarde est le temps nécessaire pour exécuter l'opération de point de sauvegarde de la sauvegarde HANA, et cette étape dépend de la charge exercée sur la base de données HANA. La sauvegarde Snapshot de stockage elle-même s'effectue toujours en quelques secondes.



Comparaison des objectifs de délai de restauration (RTO)

Cette section compare les objectifs de durée de restauration (RTO) des sauvegardes Snapshot basées sur les fichiers et le stockage. Le RTO est défini par la somme du temps nécessaire à la restauration, à la restauration, puis au démarrage de la base de données.

Temps nécessaire pour restaurer la base de données

Avec une sauvegarde basée sur des fichiers, le temps de restauration dépend de la taille de l'infrastructure de base de données et de sauvegarde, qui définit la vitesse de restauration en mégaoctets par seconde. Par exemple, si l'infrastructure prend en charge une opération de restauration à une vitesse de 250 Mbit/s, il faut environ 4.5 heures pour restaurer une base de données de 4 To sur la persistance.

Avec les sauvegardes de stockage Snapshot, la durée de restauration ne dépend pas de la taille de la base de données, et reste toujours de l'ordre de quelques secondes.

Temps nécessaire au démarrage de la base de données

L'heure de démarrage de la base de données dépend de la taille de la base de données et du temps nécessaire pour charger les données dans la mémoire. Dans les exemples suivants, on suppose que les données peuvent être chargées avec 1 000 Mbit/s. Le chargement de 4 To en mémoire prend environ 1 heure et 10 minutes. L'heure de début est la même pour les opérations de restauration et de restaurations basées sur des fichiers et des snapshots.

Temps nécessaire pour restaurer la base de données

La durée de restauration dépend du nombre de journaux qui doivent être appliqués après la restauration. Ce nombre est déterminé par la fréquence à laquelle les sauvegardes de données sont effectuées.

Avec les sauvegardes de données basées sur des fichiers, la planification des sauvegardes est généralement une fois par jour. Étant donné que la sauvegarde dégrade les performances en termes de production, une fréquence de sauvegarde plus élevée est généralement impossible. Par conséquent, dans le pire des cas, tous les journaux qui ont été écrits pendant la journée doivent être appliqués lors de la récupération avant.

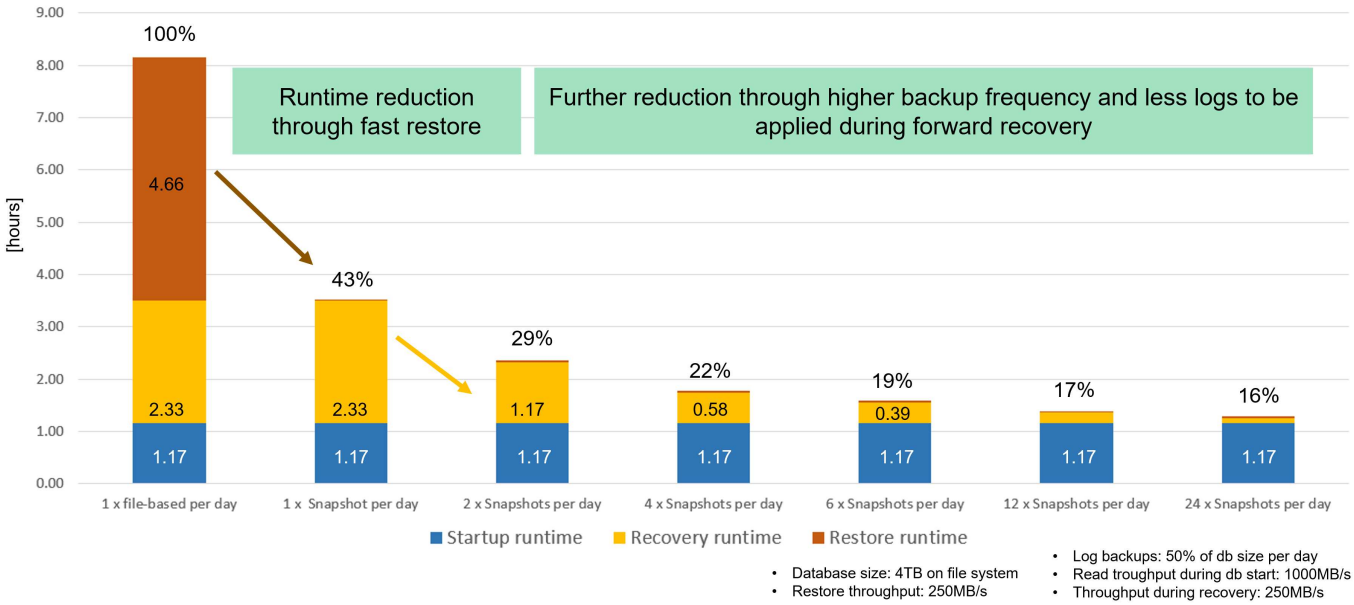
Les sauvegardes Snapshot sont généralement planifiées à une fréquence plus élevée, car elles n'influencent pas les performances de la base de données SAP HANA. Par exemple, si des sauvegardes Snapshot sont planifiées toutes les six heures, la durée de restauration serait, dans le pire des cas, d'un quart de la durée de restauration d'une sauvegarde basée sur des fichiers (6 heures / 24 heures = 25).

La figure suivante montre une comparaison des opérations de restauration et de restauration avec une sauvegarde quotidienne basée sur des fichiers et des sauvegardes Snapshot avec des calendriers différents.

Les deux premières barres indiquent que, même avec une seule sauvegarde Snapshot par jour, la restauration et la restauration sont réduites à 43 % en raison de la vitesse de restauration à partir d'une sauvegarde Snapshot. Si plusieurs sauvegardes Snapshot par jour sont créées, l'exécution peut être réduite encore davantage, car moins de journaux doivent être appliqués lors de la restauration avant transfert.

La figure suivante montre également que quatre à six sauvegardes Snapshot par jour sont les plus utiles, car la fréquence plus élevée n'a plus d'influence sur le temps d'exécution global.

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



Cas d'utilisation et valeurs d'opérations de sauvegarde et de clonage accélérées

L'exécution des sauvegardes est un élément essentiel de toute stratégie de protection des données. Les sauvegardes sont planifiées régulièrement pour vous assurer qu'elles peuvent être restaurées en cas de panne système. Il s'agit là du cas d'utilisation le plus évident, mais d'autres tâches de gestion du cycle de vie SAP jouent un rôle crucial dans l'accélération des opérations de sauvegarde et de restauration.

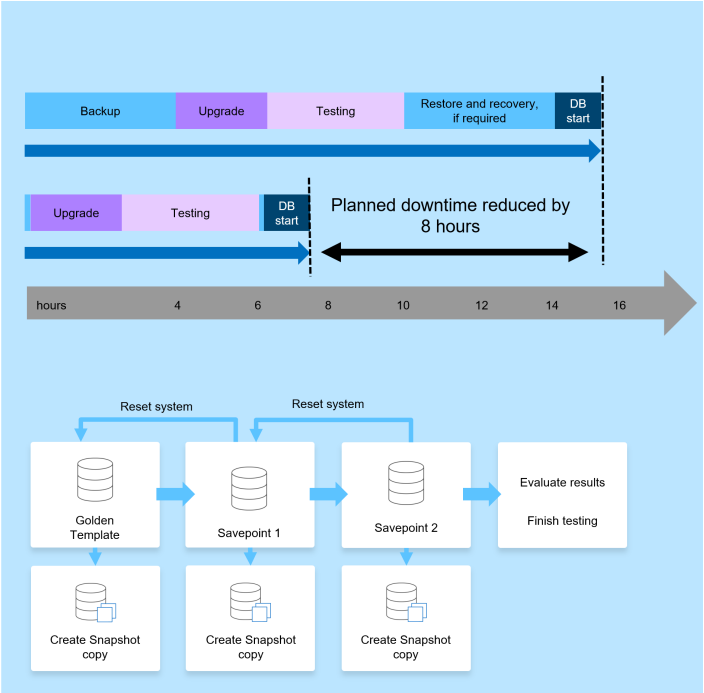
La mise à niveau du système SAP HANA est un exemple : une sauvegarde à la demande avant la mise à niveau et une opération de restauration possible en cas d'échec de la mise à niveau a un impact significatif sur le temps d'indisponibilité planifié global. Dans l'exemple d'une base de données de 4 To, vous pouvez réduire les temps d'indisponibilité planifiés de 8 heures en utilisant les opérations de sauvegarde et de restauration basées sur Snapshot.

Il s'agit également d'un cycle de test standard, où les tests doivent être réalisés sur plusieurs itérations avec différents jeux de données ou paramètres. Lorsque vous utilisez les opérations de sauvegarde et de restauration rapides, vous pouvez facilement créer des points de sauvegarde au cours de votre cycle de test et réinitialiser le système à l'un de ces points de sauvegarde précédents en cas d'échec ou de répétition d'un test. Cela permet de terminer les tests plus tôt ou d'effectuer davantage de tests simultanément et améliore les résultats des tests.

Use Cases for Backup and Recovery Operations

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

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



Lorsque des sauvegardes Snapshot ont été implémentées, elles peuvent être utilisées pour traiter plusieurs autres cas d'utilisation qui requièrent des copies d'une base de données HANA. FSX pour ONTAP vous permet de créer un nouveau volume basé sur le contenu de toute sauvegarde Snapshot disponible. L'exécution de cette opération est de quelques secondes, indépendamment de la taille du volume.

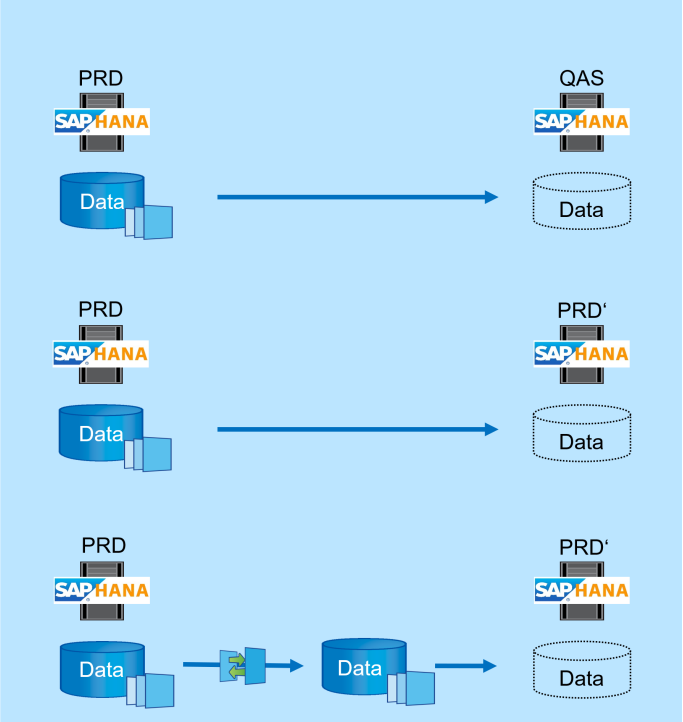
L'utilisation la plus courante est la mise à jour du système SAP, où les données du système de production doivent être copiées sur le système de test ou d'assurance qualité. La fonction de clonage FSX pour ONTAP vous permet de provisionner le volume du système de test à partir de n'importe quelle copie Snapshot du système de production en quelques secondes. Le nouveau volume doit alors être relié au système de test et la base de données HANA récupérée.

Le deuxième cas d'utilisation est la création d'un système de réparation, qui est utilisé pour résoudre une corruption logique dans le système de production. Dans ce cas, une ancienne sauvegarde Snapshot du système de production est utilisée pour démarrer un système de réparation, qui est un clone identique du système de production avec les données avant que la corruption ne se produise. Le système de réparation est alors utilisé pour analyser le problème et exporter les données requises avant d'être corrompu.

Notre dernier cas d'utilisation est la possibilité d'exécuter un test de basculement de reprise d'activité sans arrêter la réplication et sans affecter l'objectif RTO et RPO (Recovery point objective) de la configuration de la reprise d'activité. Lorsque la réplication FSX pour ONTAP NetApp SnapMirror est utilisée pour répliquer les données sur le site de reprise après incident, les sauvegardes Snapshot de production sont également disponibles sur le site de reprise après incident et peuvent ensuite être utilisées pour créer un nouveau volume pour le test de reprise après incident.

Use Cases for Cloning Operations

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



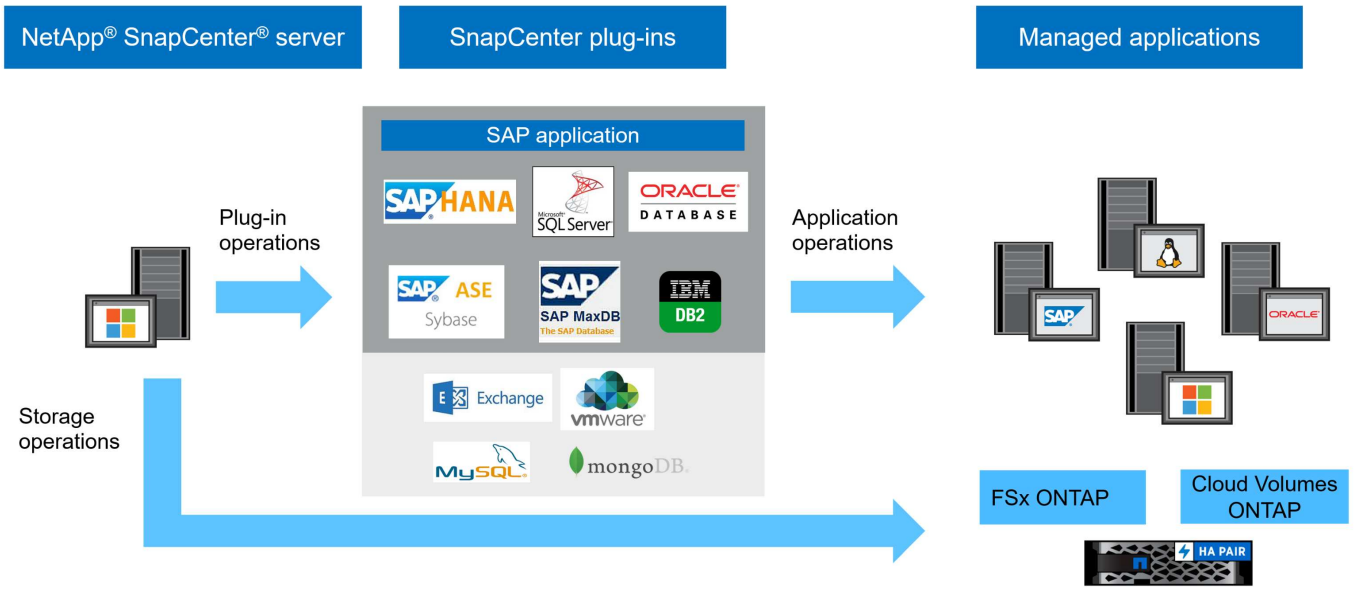
Architecture SnapCenter

SnapCenter est une plateforme unifiée et évolutive qui assure la cohérence de la protection des données au niveau des applications. SnapCenter offre un contrôle et une surveillance centralisés, tout en déléguant aux utilisateurs la possibilité de gérer les tâches de sauvegarde, de restauration et de clonage spécifiques aux applications. Avec SnapCenter, les administrateurs de bases de données et de stockage apprennent à utiliser un seul outil pour gérer les opérations de sauvegarde, de restauration et de clonage des différentes applications et bases de données.

SnapCenter gère les données dans les différents terminaux de la Data Fabric optimisée par NetApp. Vous pouvez utiliser SnapCenter pour répliquer des données entre les environnements sur site, entre les environnements sur site et le cloud, et entre les clouds privés, hybrides et publics.

Composants de SnapCenter

SnapCenter inclut le serveur SnapCenter, le module de plug-in SnapCenter pour Windows et le module de plug-in SnapCenter pour Linux. Chaque offre comprend des plug-ins à SnapCenter pour divers composants d’infrastructure et d’applications.



Solution de sauvegarde SnapCenter SAP HANA

La solution de sauvegarde SnapCenter pour SAP HANA couvre les domaines suivants :

- Opérations de sauvegarde, planification et gestion de la conservation
  - Sauvegarde des données SAP HANA avec copies Snapshot basées sur le stockage
  - Sauvegarde de volumes sans données avec copies Snapshot basées sur le stockage (par exemple, `/hana/shared`)
  - Contrôle de l'intégrité des blocs de base de données à l'aide d'une sauvegarde basée sur des fichiers
  - La réplication vers un emplacement de sauvegarde hors site ou de reprise après incident
- Gestion du catalogue des sauvegardes SAP HANA
  - Pour les sauvegardes de données HANA (basées sur des copies Snapshot et des fichiers)
  - Pour les sauvegardes de journaux HANA
- Les opérations de restauration et de reprise
  - Restauration et reprise automatisées
  - Opérations de restauration d'un seul locataire pour les systèmes SAP HANA (MDC)

SnapCenter exécute également des sauvegardes de fichiers de données de bases de données en association avec le plug-in pour SAP HANA. Le plug-in définit le point de sauvegarde de la base de données SAP HANA pour que les copies Snapshot, qui sont créées sur le système de stockage principal, soient basées sur une image cohérente de la base de données SAP HANA.

SnapCenter permet la réplication d'images cohérentes de bases de données vers un emplacement de sauvegarde ou de reprise après incident hors site à l'aide de SnapVault ou de la fonctionnalité SnapMirror. Généralement, différentes règles de conservation sont définies selon l'emplacement des sauvegardes sur le stockage primaire et sur le stockage de sauvegarde hors site. SnapCenter gère la conservation au niveau du stockage primaire, et ONTAP gère la conservation au niveau du stockage de sauvegarde hors site.

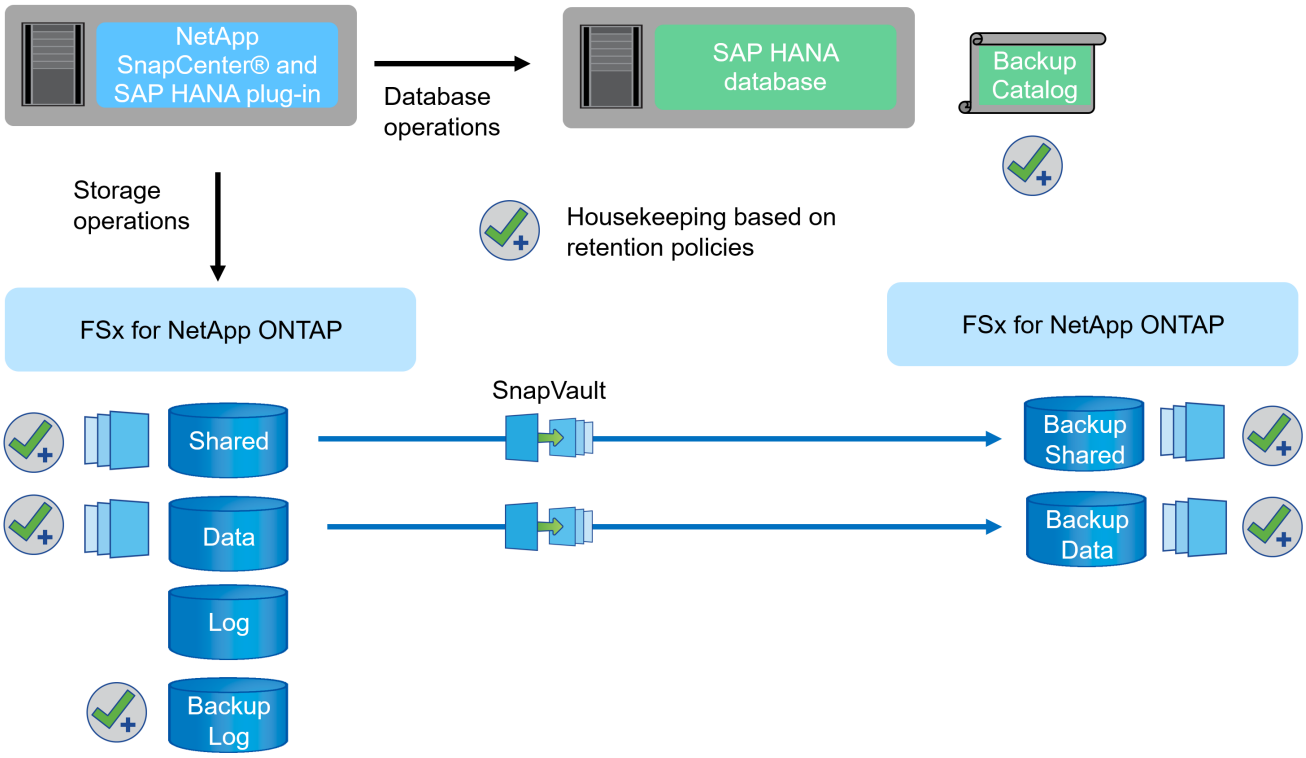
Pour permettre une sauvegarde complète de toutes les ressources SAP HANA, SnapCenter vous permet également de sauvegarder tous les volumes non-data à l'aide du plug-in SAP HANA avec des copies Snapshot basées sur le stockage. Vous pouvez planifier des volumes autres que des volumes de données

indépendamment de la sauvegarde de la base de données afin de mettre en place des règles de conservation et de protection individuelles.

SAP recommande de combiner des sauvegardes Snapshot basées sur le stockage et une sauvegarde hebdomadaire basée sur des fichiers pour exécuter une vérification de l'intégrité des blocs. Vous pouvez exécuter la vérification d'intégrité des blocs depuis SnapCenter. En fonction des règles de conservation que vous avez configurées, SnapCenter gère le nettoyage des sauvegardes de fichiers de données dans le système de stockage primaire, les sauvegardes de fichiers journaux et le catalogue de sauvegardes SAP HANA.

SnapCenter gère la conservation au niveau du stockage primaire, tandis que FSX pour ONTAP gère la conservation des sauvegardes secondaires.

La figure suivante présente une vue d'ensemble des opérations de gestion des sauvegardes et des conservation de SnapCenter.



Lors de l'exécution d'une sauvegarde Snapshot basée sur le stockage de la base de données SAP HANA, SnapCenter effectue les tâches suivantes :

1. Crée un point de sauvegarde SAP HANA pour créer une image cohérente sur la couche de persistance.
2. Crée une copie Snapshot du volume de données basée sur le stockage.
3. Enregistre la sauvegarde Snapshot basée sur le stockage dans le catalogue de sauvegardes SAP HANA.
4. Libère le point de sauvegarde de SAP HANA.
5. Exécute une mise à jour SnapVault ou SnapMirror pour le volume de données, s'il est configuré.
6. Supprime les copies Snapshot de stockage au niveau du stockage primaire selon les règles de conservation définies.
7. Supprime les entrées du catalogue de sauvegardes SAP HANA si les sauvegardes n'existent plus sur le stockage de sauvegarde primaire ou hors site.

8. Lorsqu'une sauvegarde a été supprimée en fonction de la stratégie de conservation ou manuellement, SnapCenter supprime également toutes les sauvegardes de journaux antérieures à la sauvegarde de données la plus ancienne. Les sauvegardes des journaux sont supprimées dans le système de fichiers et dans le catalogue de sauvegardes SAP HANA.

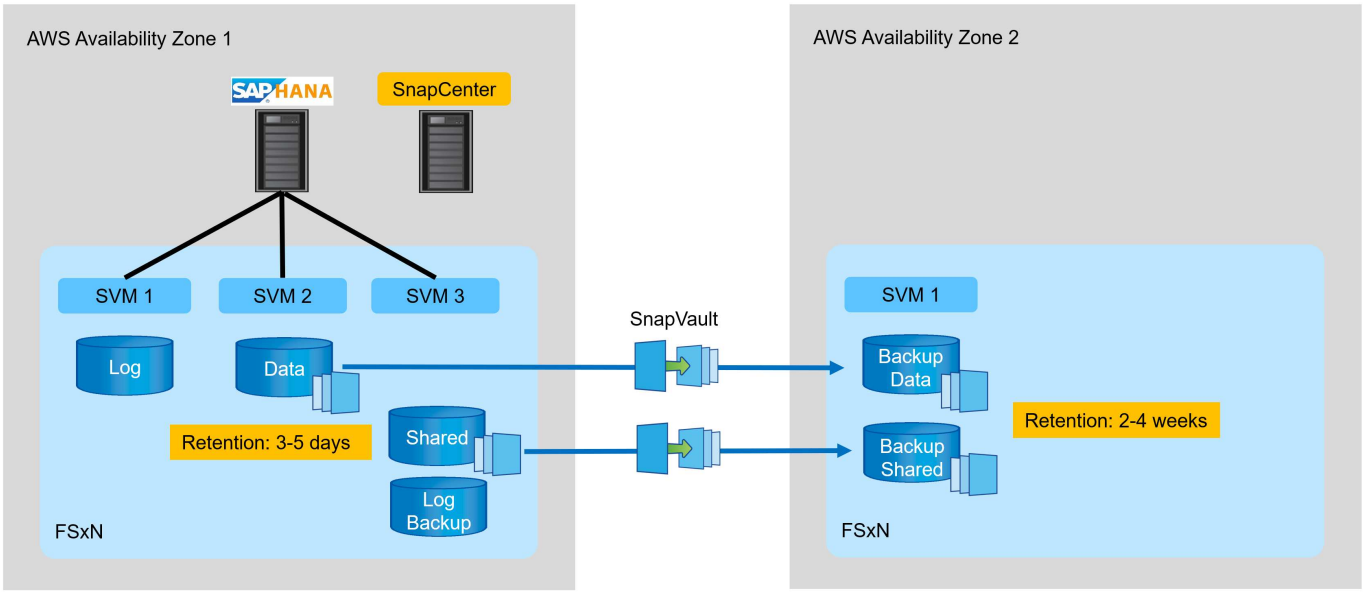
Portée de ce document

Ce document décrit l'option de configuration SnapCenter la plus courante pour un système hôte unique MDC SAP HANA avec un seul locataire sur FSX pour ONTAP. D'autres options de configuration sont possibles et, dans certains cas, requises pour des systèmes SAP HANA spécifiques, par exemple, pour un système hôte multiple. Pour une description détaillée des autres options de configuration, voir "Concepts et bonnes pratiques SnapCenter (netapp.com)".

Dans ce document, nous utilisons la console Amazon Web Services (AWS) et l'interface de ligne de commande FSX pour ONTAP pour exécuter les étapes de configuration requises au niveau de la couche de stockage. Vous pouvez également utiliser NetApp Cloud Manager pour gérer FSX pour ONTAP, mais ce document n'est pas périmètre. Pour plus d'informations sur l'utilisation de NetApp Cloud Manager pour FSX pour ONTAP, consultez la page "En savoir plus sur Amazon FSX pour ONTAP (netapp.com)".

Stratégie de protection des données

La figure suivante montre une architecture de sauvegarde type pour SAP HANA sur FSX pour ONTAP. Le système HANA se trouve dans la zone de disponibilité AWS 1 et utilise un système de fichiers FSX pour ONTAP au sein de la même zone de disponibilité. Les opérations de sauvegarde Snapshot sont exécutées pour les données et le volume partagé de la base de données HANA. Outre les sauvegardes Snapshot locales, conservées pendant 3-5 jours, les sauvegardes sont également répliquées vers un stockage hors site pour une conservation à long terme. Le stockage de sauvegarde hors site est un second système de fichiers FSX pour ONTAP, situé dans une zone de disponibilité AWS différente. Les sauvegardes des données HANA et des volumes partagés sont répliquées avec SnapVault sur le deuxième système de fichiers FSX pour ONTAP, et conservées pendant 2-3 semaines.



Avant de configurer le SnapCenter, la stratégie de protection des données doit être définie en fonction des exigences RTO et RPO des divers systèmes SAP.

Une approche commune consiste à définir des types de systèmes tels que la production, le développement, les tests ou les systèmes sandbox. Tous les systèmes SAP d'un même type de système ont généralement les

mêmes paramètres de protection des données.

Les paramètres suivants doivent être définis :

- À quelle fréquence une sauvegarde Snapshot doit-elle être exécutée ?
- Combien de temps les sauvegardes de copies Snapshot doivent-elles être conservées sur le système de stockage primaire ?
- À quelle fréquence un contrôle d'intégrité des blocs doit-il être exécuté ?
- Les sauvegardes primaires doivent-elles être répliquées sur un site de sauvegarde hors site ?
- Combien de temps les sauvegardes doivent-elles être conservées sur le stockage de sauvegarde hors site ?

Le tableau suivant présente un exemple de paramètres de protection des données pour les types de système : production, développement et test. Pour le système de production, une fréquence de sauvegarde élevée a été définie et les sauvegardes sont répliquées sur un site de sauvegarde hors site une fois par jour. Les systèmes de test présentent des exigences moindres, et aucune réplication des sauvegardes n'est possible.

Paramètres	Systèmes de production	Systèmes de développement	Systèmes de test
Fréquence des sauvegardes	Toutes les 6 heures	Toutes les 6 heures	Toutes les 6 heures
Conservation primaire	3 jours	3 jours	3 jours
Vérification de l'intégrité des blocs	Une fois par semaine	Une fois par semaine	Non
La réplication vers un site de sauvegarde hors site	Une fois par jour	Une fois par jour	Non
Conservation des sauvegardes hors site	2 semaines	2 semaines	Sans objet

Le tableau suivant présente les règles à configurer pour les paramètres de protection des données.

Paramètres	Policy LocalSnap	Via la gestion locale SnapAndSnapVault	Vérification de l'Integratédu bloc de règles
Type de sauvegarde	Basé sur Snapshot	Basé sur Snapshot	Basée sur un fichier
Fréquence de programmation	Horaire	Tous les jours	Hebdomadaire
Conservation primaire	Nombre = 12	Nombre = 3	Nombre = 1
Réplication SnapVault	Non	Oui.	Sans objet

La politique `LocalSnapshot` Utilisé dans les systèmes de production, de développement et de test pour couvrir les sauvegardes Snapshot locales avec une durée de conservation de deux jours.

Dans la configuration de la protection des ressources, le planning est défini différemment pour les types de système :

- Production : planifier toutes les 4 heures.

- Développement : programmez toutes les 4 heures.
- Test : programmez toutes les 4 heures.

La politique `LocalSnapAndSnapVault` utilisé pour les systèmes de production et de développement afin de couvrir la réplication quotidienne vers le stockage de sauvegarde hors site.

Dans la configuration de la protection des ressources, le planning est défini pour la production et le développement :

- Production : planifier tous les jours.
- Développement : planifiez tous les jours.la politique `BlockIntegrityCheck` utilisé par les systèmes de production et de développement pour couvrir le contrôle hebdomadaire de l'intégrité des blocs à l'aide d'une sauvegarde basée sur des fichiers.

Dans la configuration de la protection des ressources, le planning est défini pour la production et le développement :

- Production : horaire chaque semaine.
- Développement : planifier chaque semaine.

Pour chaque base de données SAP HANA individuelle qui utilise la règle de sauvegarde hors site, vous devez configurer une relation de protection sur la couche de stockage. La relation de protection définit quels volumes sont répliqués et la conservation de sauvegardes sur le stockage de sauvegarde hors site.

Dans l'exemple suivant, pour chaque système de production et de développement, une durée de conservation de deux semaines est définie sur le stockage de sauvegarde hors site.

Dans cet exemple, les règles de protection et la conservation des ressources de bases de données SAP HANA et de volumes autres que de données ne sont pas différentes.

Exemple de configuration de laboratoire

La configuration de laboratoire suivante a été utilisée comme exemple de configuration pour le reste de ce document.

Système HANA PFX :

- Système MDC hôte unique avec un seul locataire
- HANA 2.0 SPS 6 révision 60
- SLES POUR SAP 15SP3

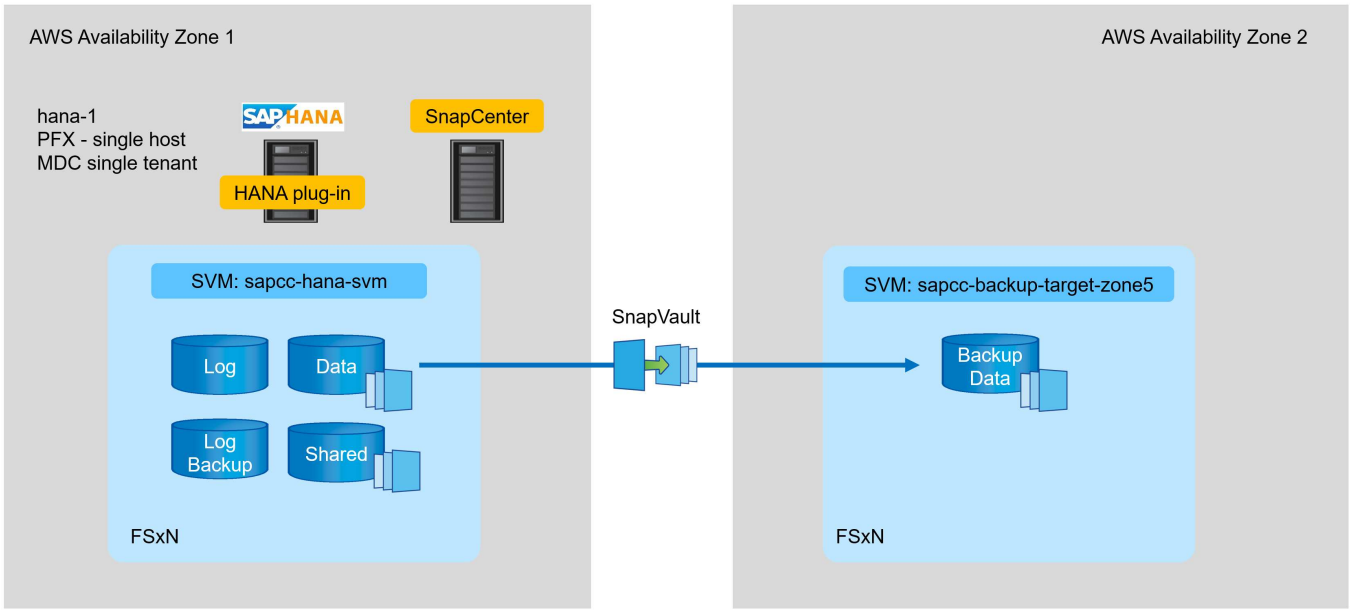
SnapCenter :

- Version 4.6
- Le plug-in HANA et Linux est déployé sur un hôte de base de données HANA

FSX pour systèmes de fichiers ONTAP :

- Deux systèmes FSX pour systèmes de fichiers ONTAP avec une seule machine virtuelle de stockage (SVM)
- Chaque système FSX pour ONTAP dans une zone de disponibilité AWS différente

- Le volume de données HANA est répliqué sur le second FSX pour le système de fichiers ONTAP



Configuration SnapCenter

Vous devez effectuer les étapes de cette section pour la configuration SnapCenter de base et la protection de la ressource HANA.

Présentation des étapes de configuration

Pour la configuration SnapCenter de base et la protection de la ressource HANA, vous devez effectuer les étapes suivantes. Chaque étape est décrite en détail dans les chapitres suivants.

1. Configurer l'utilisateur de sauvegarde SAP HANA et la clé de magasin hdbuserStore. Permet d'accéder à la base de données HANA avec le client hdbsql.
2. Configurer le stockage dans SnapCenter Identifiants pour accéder au FSX pour les SVM ONTAP à partir de SnapCenter
3. Configurer les identifiants pour le déploiement du plug-in Permet de déployer et d'installer automatiquement les plug-ins SnapCenter requis sur l'hôte de la base de données HANA.
4. Ajoutez l'hôte HANA à SnapCenter. Déploie et installe les plug-ins SnapCenter requis
5. Configurez des règles. Définit le type d'opération de sauvegarde (Snapshot, fichier), les retentions, ainsi qu'une réplication de sauvegarde Snapshot facultative.
6. Configurez la protection des ressources HANA. Fournir une clé hdbuserstore et connecter des règles et des planifications à la ressource HANA.

L'utilisateur de sauvegarde SAP HANA et la configuration du hdbuserstore

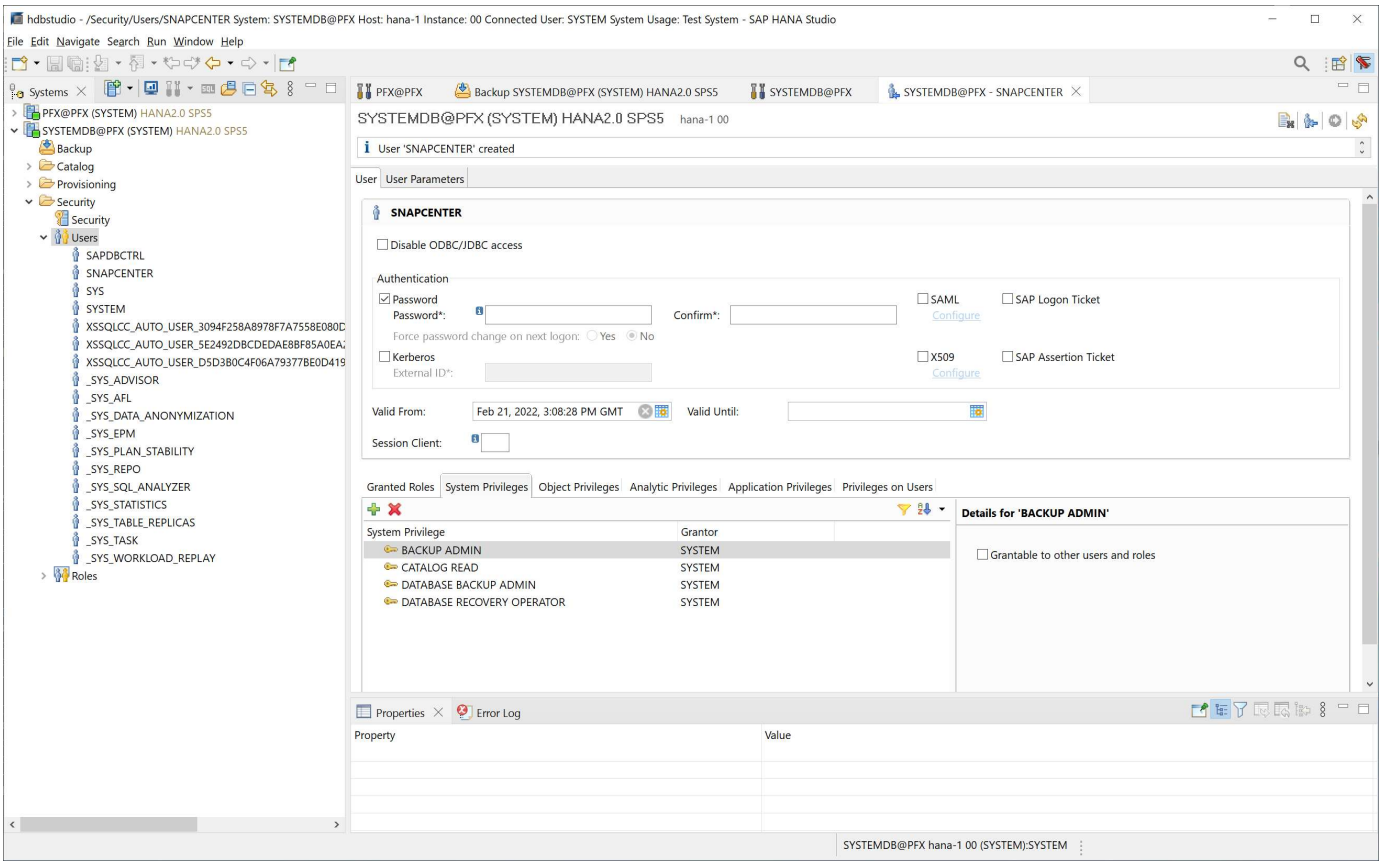
NetApp recommande de configurer un utilisateur de base de données dédiée sur la base de données HANA pour exécuter les opérations de sauvegarde avec SnapCenter. Dans la deuxième étape, une clé de magasin utilisateur SAP HANA est configurée pour cet utilisateur de sauvegarde, et cette clé de magasin utilisateur est utilisée dans la configuration du plug-in SnapCenter SAP HANA.

La figure suivante montre SAP HANA Studio par l'intermédiaire de lequel vous pouvez créer l'utilisateur de

sauvegarde

Les privilèges requis sont modifiés avec la version HANA 2.0 SPS5 : administrateur des sauvegardes, lecture du catalogue, administrateur des sauvegardes de bases de données et opérateur de récupération de bases de données. Pour les versions antérieures, l'administrateur des sauvegardes et la lecture du catalogue suffisent.

Pour un système MDC SAP HANA, vous devez créer l'utilisateur dans la base de données du système car toutes les commandes de sauvegarde pour le système et les bases de données des locataires sont exécutées à l'aide de la base de données du système.



La commande suivante est utilisée pour la configuration du magasin utilisateur avec le `<sid>adm` utilisateur :

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

SnapCenter utilise le `<sid>adm` L'utilisateur doit communiquer avec la base de données HANA. Par conséquent, vous devez configurer la clé de stockage des utilisateurs en utilisant l'utilisateur <sID> adm sur l'hôte de la base de données. En général, le logiciel client SAP HANA hdbsql est installé avec l'installation du serveur de base de données. Si ce n'est pas le cas, vous devez d'abord installer hdbclient.

Dans une configuration MDC SAP HANA, port `3<instanceNo>13` Est le port standard pour l'accès SQL à la base de données système et doit être utilisé dans la configuration hdbuserstore.

Dans le cas d'une configuration SAP HANA à plusieurs hôtes, vous devez configurer les clés de magasin utilisateur pour tous les hôtes. SnapCenter tente de se connecter à la base de données à l'aide de chacune des clés fournies et peut donc opérer indépendamment d'un basculement d'un service SAP HANA vers un autre hôte. Dans notre configuration de laboratoire, nous avons configuré une clé de magasin utilisateur pour l'utilisateur `pfxadm` Pour notre système PFX, qui est un système MDC HANA hôte unique avec un seul

locataire.

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

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

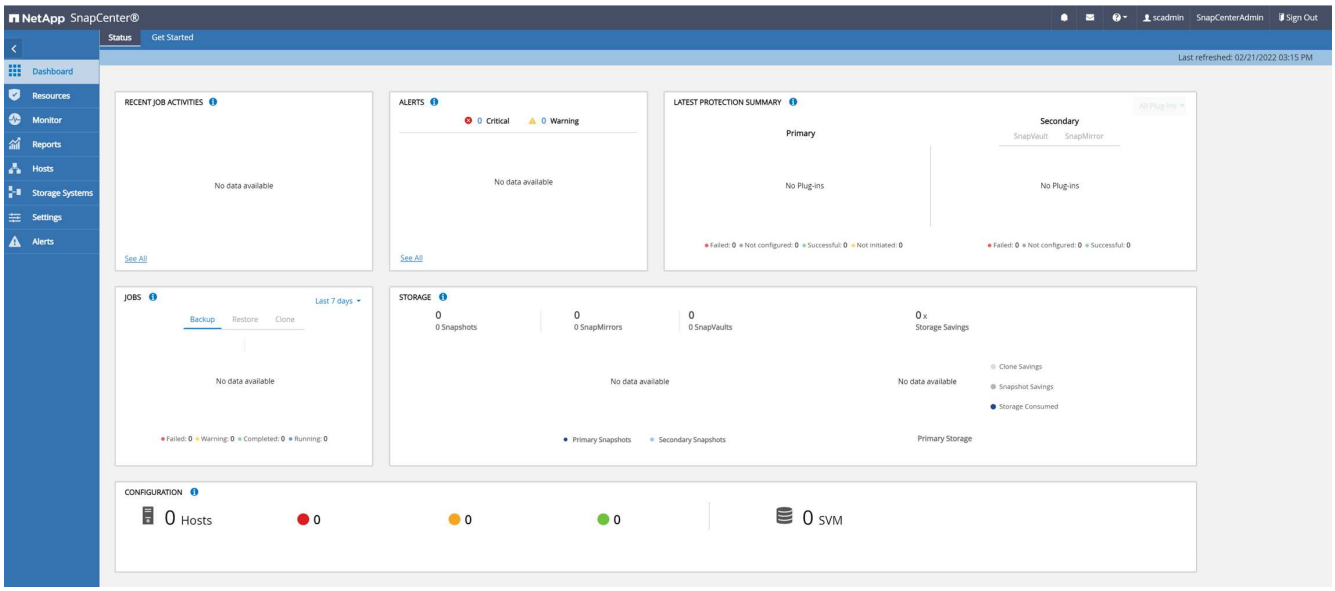
Vous pouvez vérifier l'accès à la base de données système HANA qui utilise la clé avec le `hdbsql` commande.

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

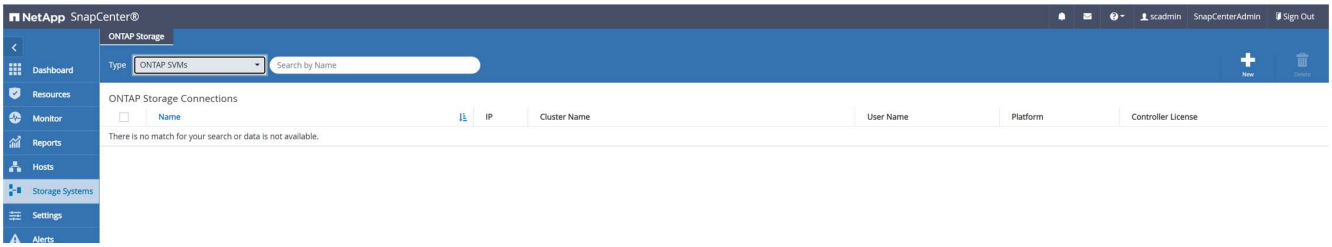
Configurer le stockage

Procédez comme suit pour configurer le stockage dans SnapCenter.

1. Dans l'interface utilisateur SnapCenter, sélectionnez systèmes de stockage.

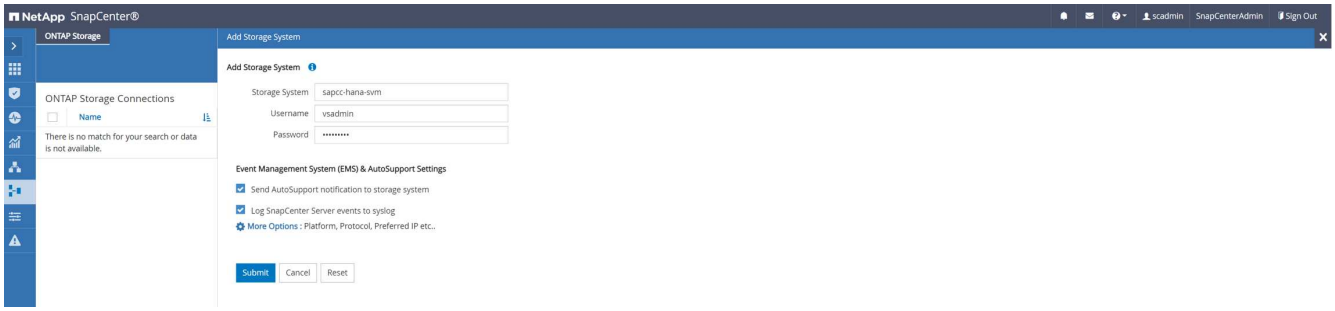


Vous pouvez sélectionner le type de système de stockage, qui peut être SVM ONTAP ou clusters ONTAP. Dans l'exemple suivant, la gestion SVM est sélectionnée.

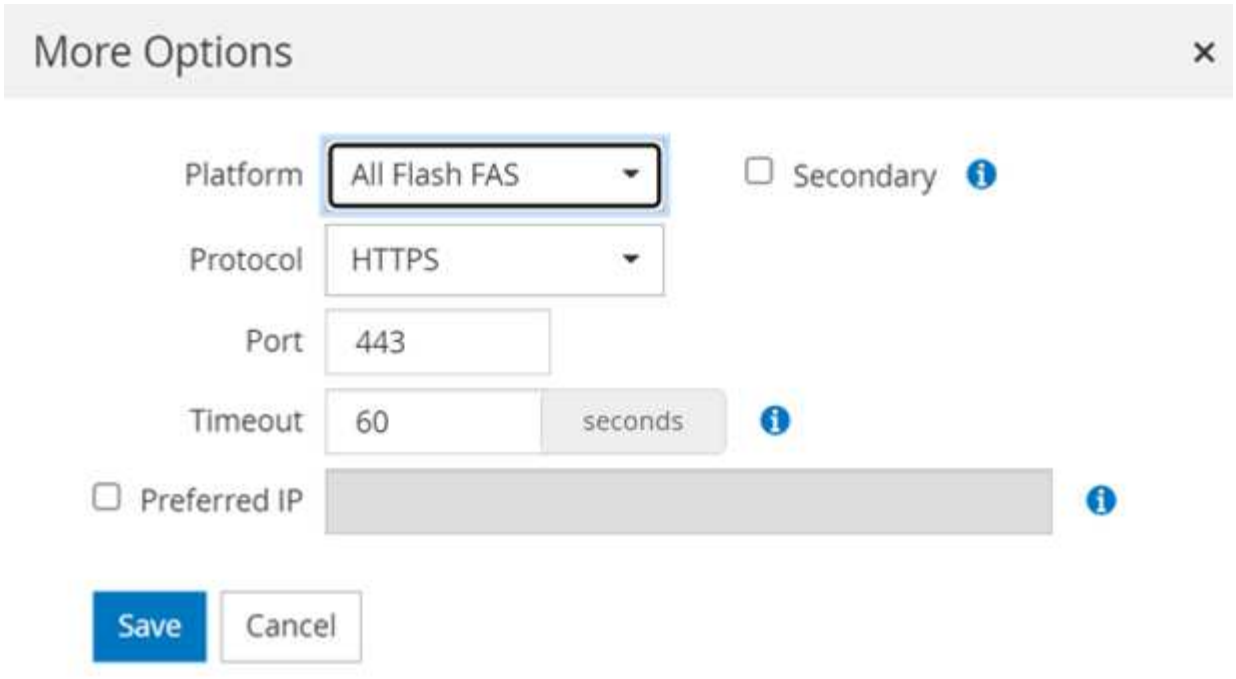


2. Pour ajouter un système de stockage et fournir le nom d'hôte et les informations d'identification requis, cliquez sur Nouveau.

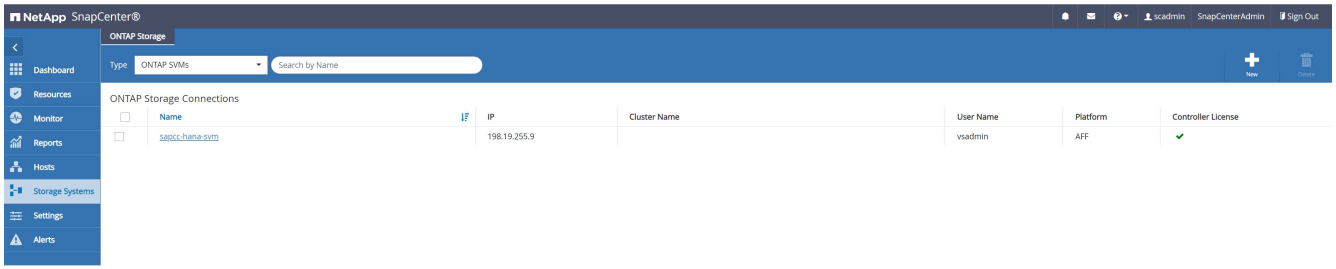
   L'utilisateur SVM n'est pas requis pour être l'utilisateur vsadmin, comme illustré dans la figure suivante. En général, un utilisateur est configuré sur le SVM et se voit attribuer les autorisations requises pour exécuter les opérations de sauvegarde et de restauration. Pour plus d'informations sur les privilèges requis, reportez-vous à la section "Guide d'installation de SnapCenter" Dans la section intitulée « privilèges minimum de ONTAP requis ».



3. Pour configurer la plate-forme de stockage, cliquez sur autres options.
4. Sélectionnez All Flash FAS comme système de stockage pour vous assurer que la licence, qui fait partie de FSX pour ONTAP, est disponible pour SnapCenter.



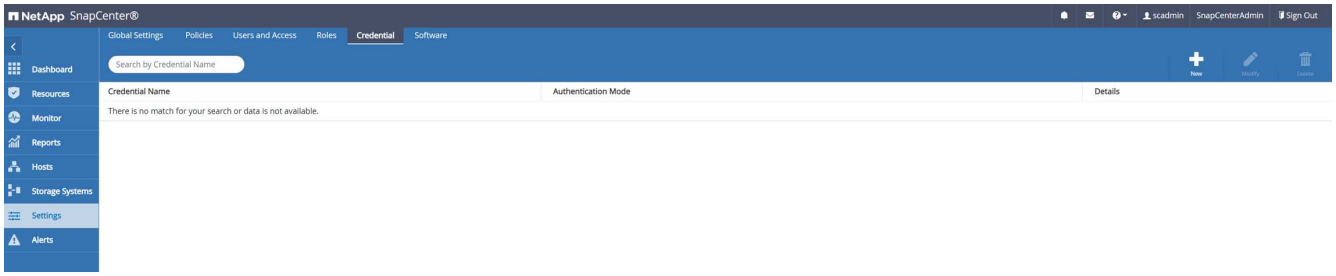
SVM `sapcc-hana-svm` Est désormais configuré dans SnapCenter.



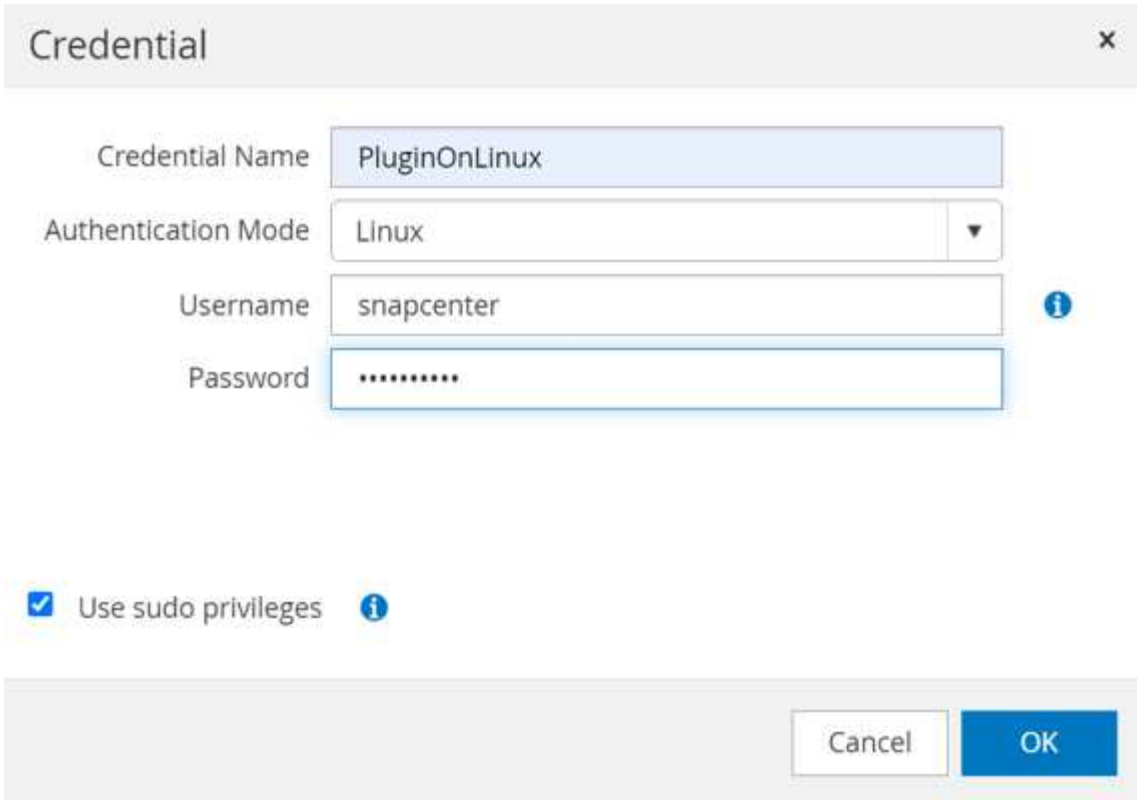
Créez des informations d'identification pour le déploiement du plug-in

Pour que SnapCenter puisse déployer les plug-ins requis sur les hôtes HANA, vous devez configurer les identifiants utilisateur.

1. Accédez à Paramètres, sélectionnez informations d'identification, puis cliquez sur Nouveau.



2. Dans la configuration de laboratoire, nous avons configuré un nouvel utilisateur, `snapcenter`, Sur l'hôte HANA utilisé pour le déploiement du plug-in. Vous devez activer les pivges de sudo, comme indiqué dans la figure suivante.




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

Ajoutez un hôte SAP HANA

Lors de l'ajout d'un hôte SAP HANA, SnapCenter déploie les plug-ins requis sur l'hôte de base de données et exécute les opérations de détection automatique.

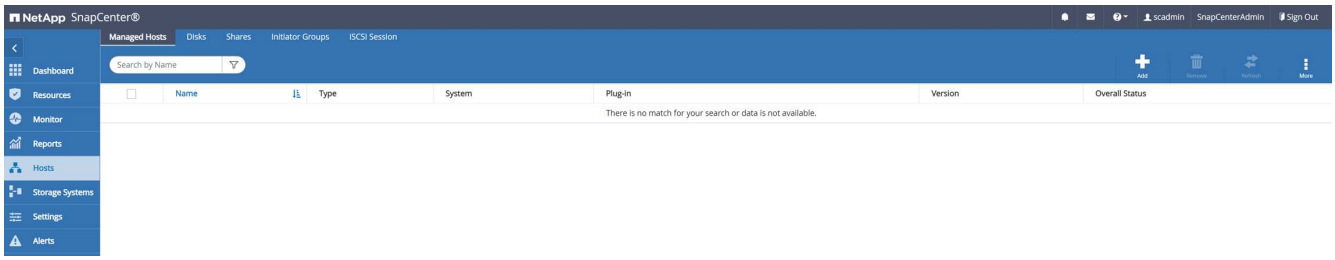
Le plug-in SAP HANA requiert Java 64 bits version 1.8. Java doit être installé sur l'hôte avant d'ajouter l'hôte à SnapCenter.

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

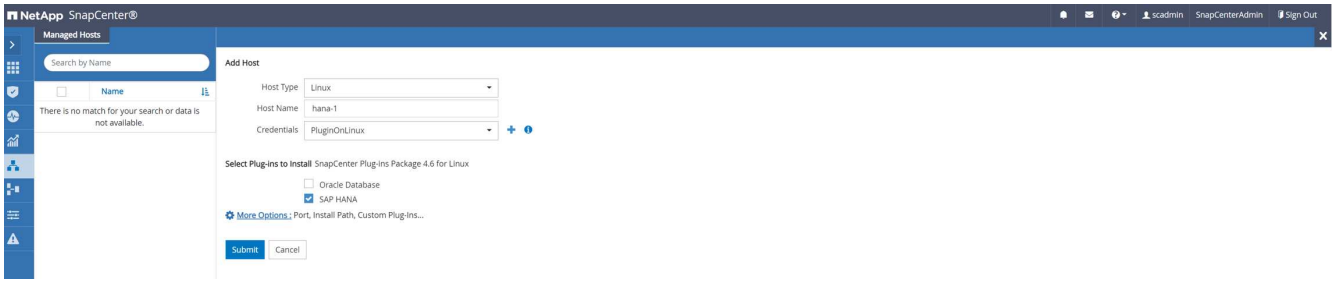
OpenJDK ou Oracle Java est pris en charge avec SnapCenter.

Pour ajouter l'hôte SAP HANA, procédez comme suit :

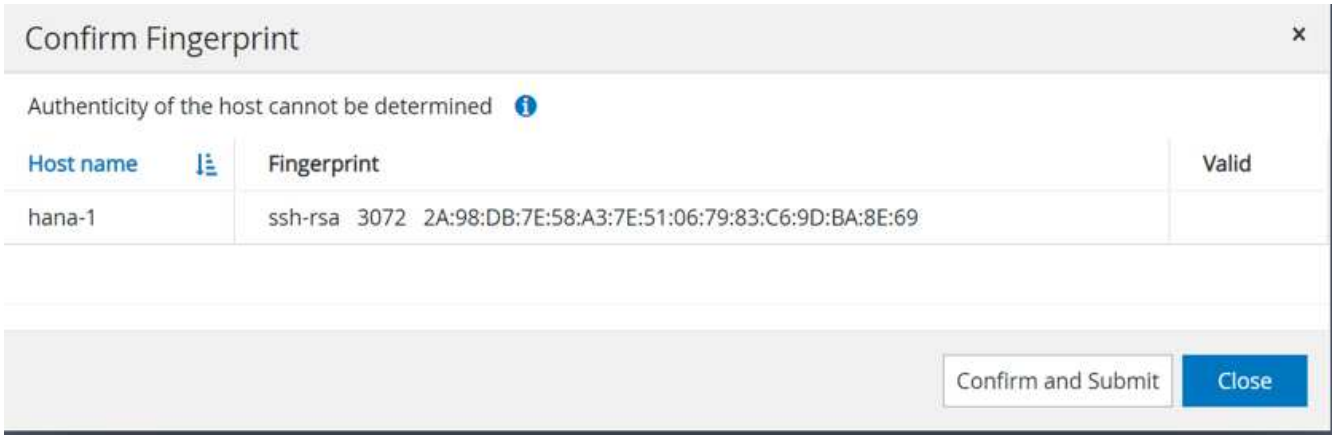
1. Dans l'onglet hôte, cliquez sur Ajouter.



2. Fournissez des informations sur l'hôte et sélectionnez le plug-in SAP HANA à installer. Cliquez sur soumettre.

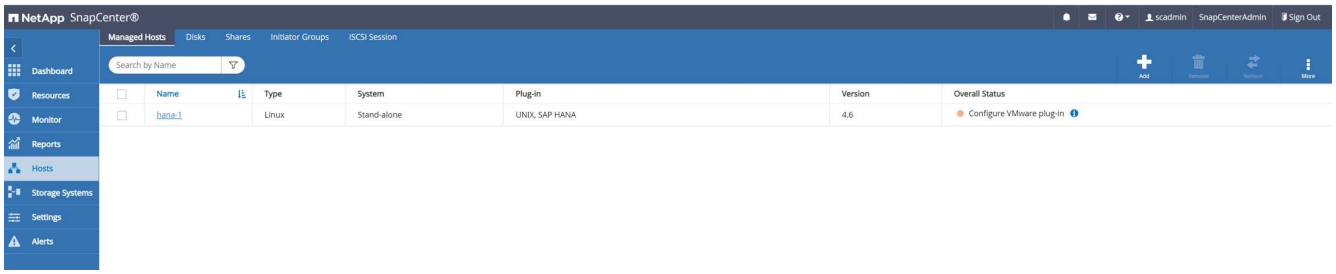


3. Confirmez l'empreinte digitale.



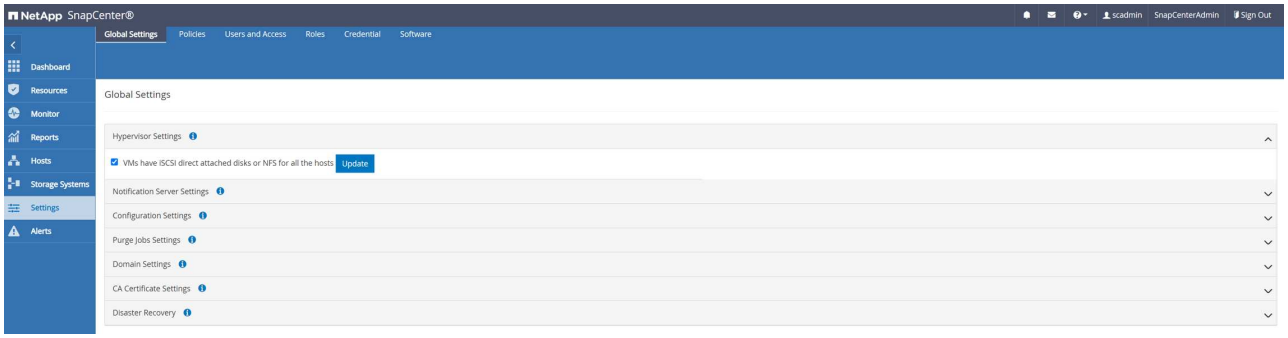
L'installation de HANA et du plug-in Linux démarre automatiquement. Une fois l'installation terminée, la colonne d'état de l'hôte indique configurer le plug-in VMware. SnapCenter détecte si le plug-in SAP HANA est installé dans un environnement virtualisé. Il peut s'agir d'un environnement VMware ou d'un environnement proposé par un fournisseur de cloud public. Dans ce cas, SnapCenter affiche un avertissement pour configurer l'hyperviseur.

Vous pouvez supprimer le message d'avertissement en procédant comme suit.

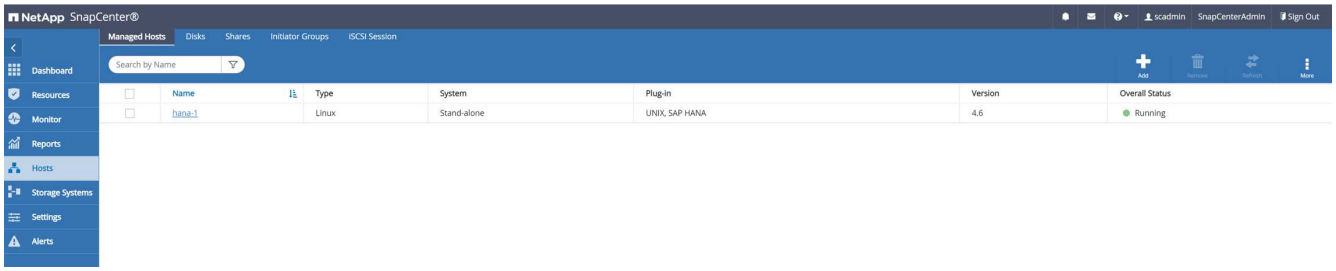


a. Dans l'onglet Paramètres, sélectionnez Paramètres globaux.

b. Pour les paramètres de l'hyperviseur, sélectionnez les machines virtuelles disposent de disques iSCSI à connexion directe ou de NFS pour tous les hôtes et mettez à jour les paramètres.



L'écran affiche désormais le plug-in Linux et le plug-in HANA lorsque l'état est en cours d'exécution.



Configurez des règles

Les règles sont généralement configurées indépendamment des ressources et peuvent être utilisées par plusieurs bases de données SAP HANA.

Une configuration minimale typique comprend les règles suivantes :

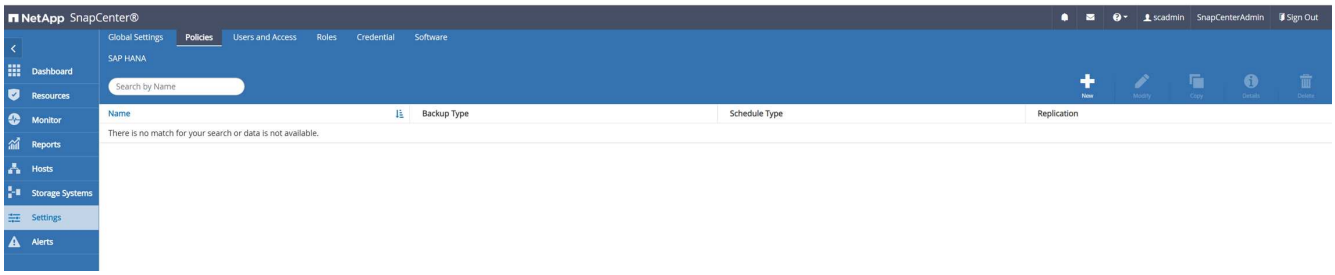
- Règle pour les sauvegardes horaires sans réplication : `LocalSnap`.
- Règles pour une vérification hebdomadaire de l'intégrité des blocs à l'aide d'une sauvegarde basée sur des fichiers : `BlockIntegrityCheck`.

Les sections suivantes décrivent la configuration de ces règles.

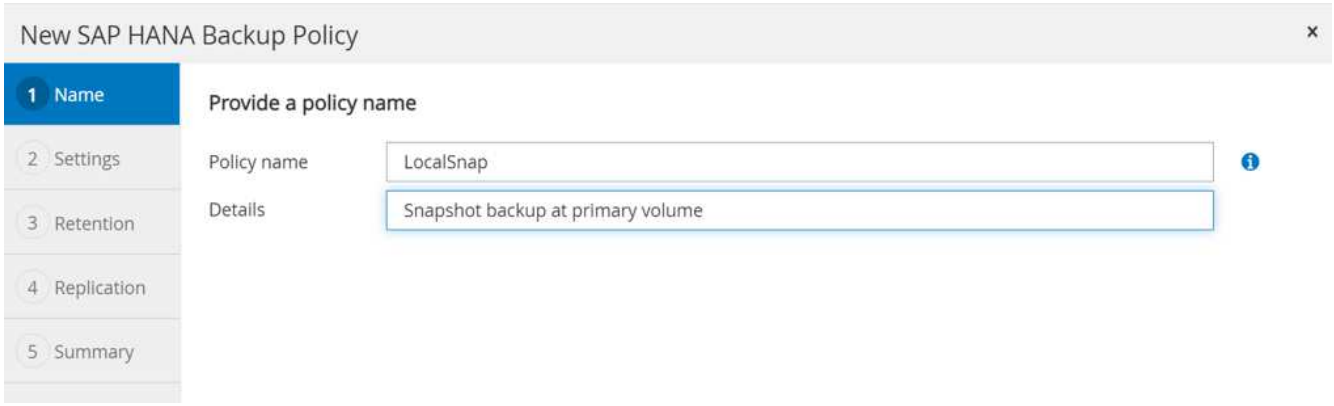
Règle pour les sauvegardes Snapshot

Procédez comme suit pour configurer les règles de sauvegarde Snapshot.

1. Accédez à Paramètres > stratégies et cliquez sur Nouveau.

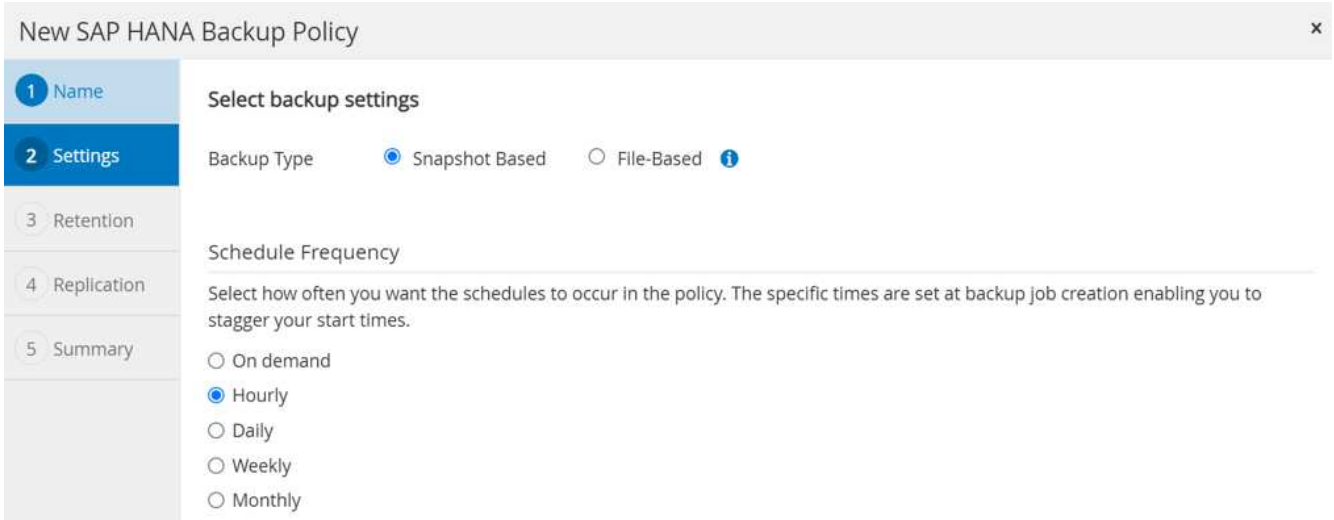


2. Entrez le nom et la description de la stratégie. Cliquez sur Suivant.

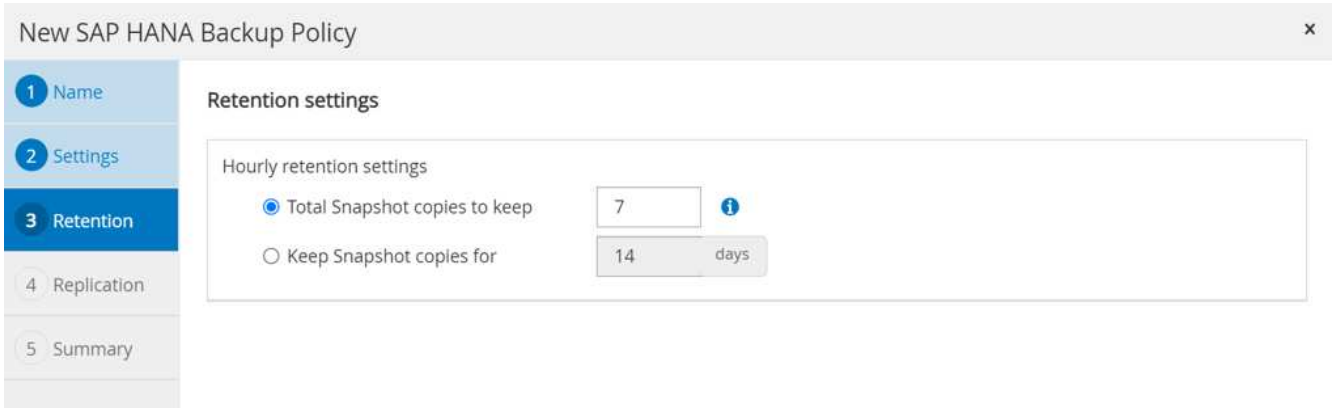


3. Sélectionnez le type de sauvegarde comme basé sur Snapshot et sélectionnez horaire pour la fréquence d'horaire.

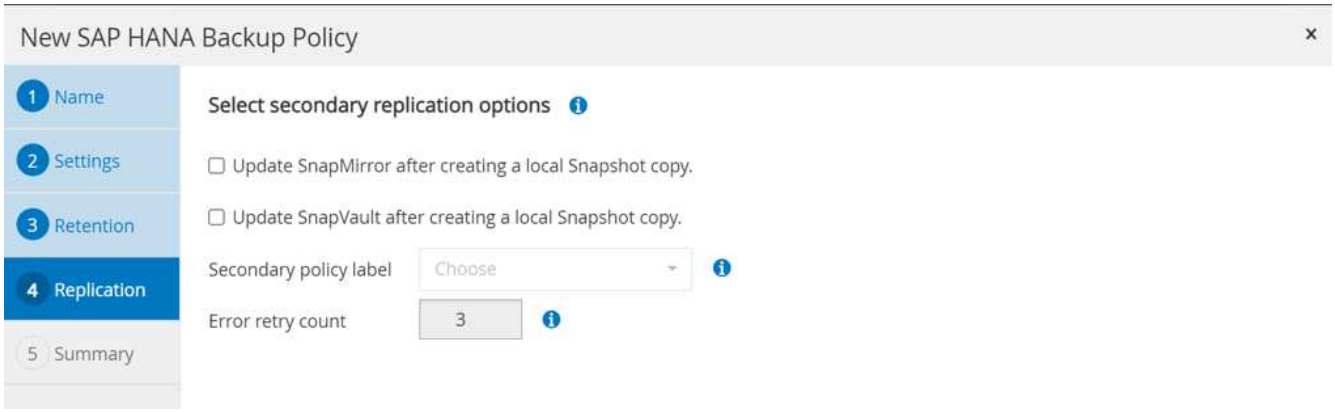
   La planification elle-même est configurée ultérieurement avec la configuration de protection des ressources HANA.

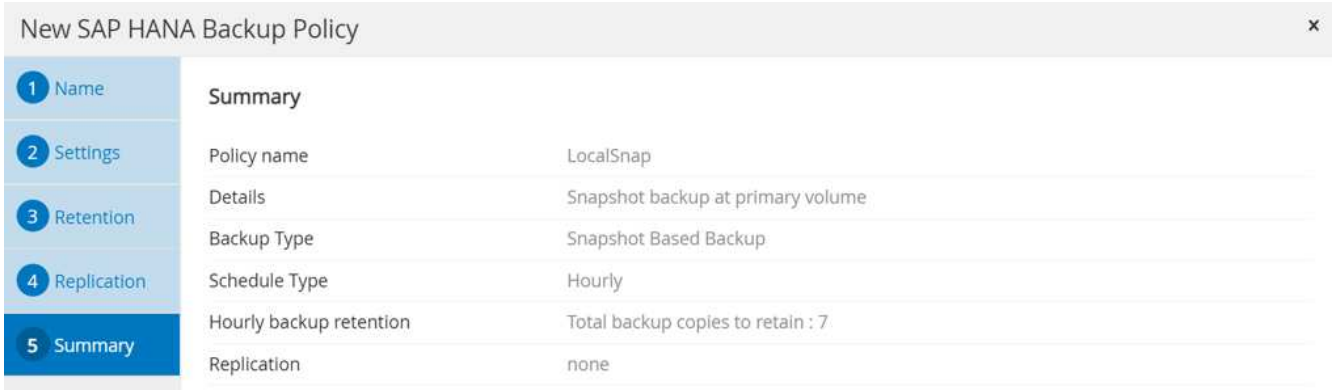


4. Configurez les paramètres de conservation pour les sauvegardes à la demande.

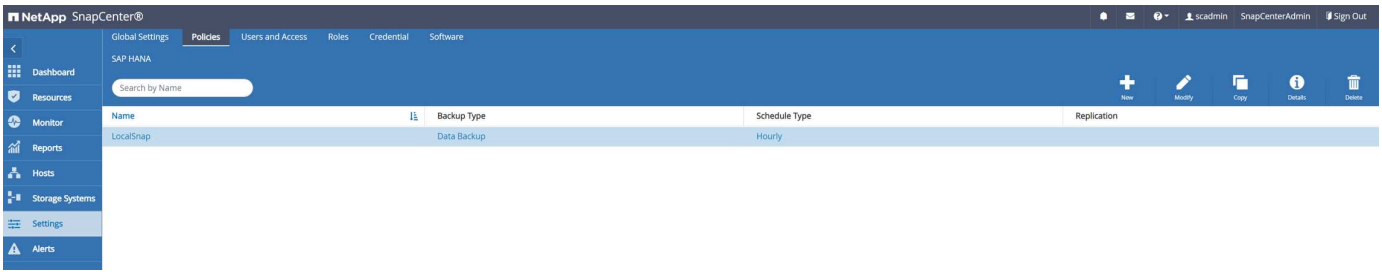


5. Configurez les options de réplication. Dans ce cas, aucune mise à jour de SnapVault ou de SnapMirror n'est sélectionnée.





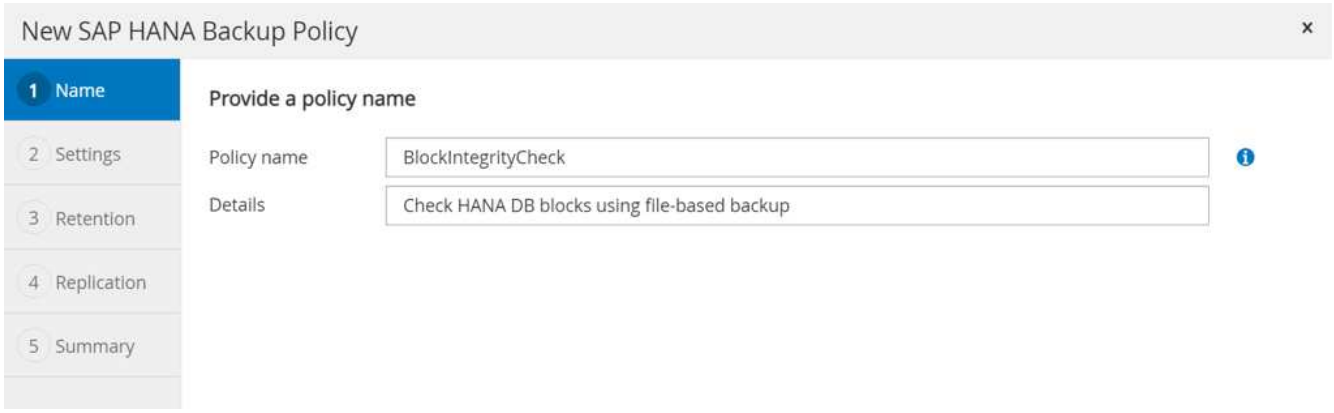
La nouvelle règle est maintenant configurée.



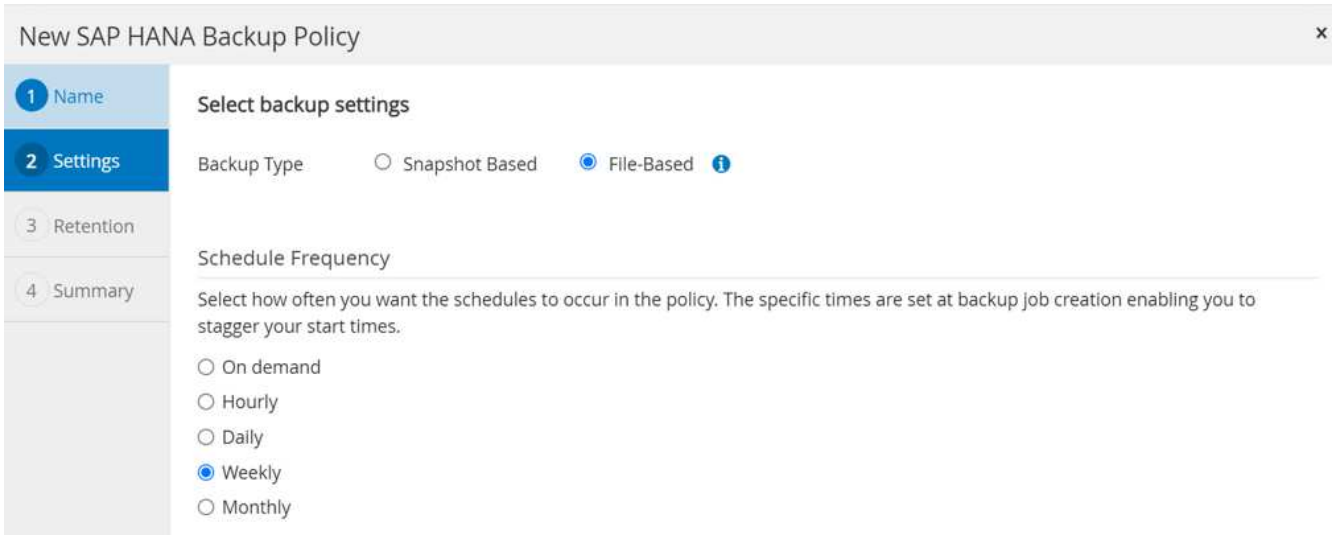
Règle de vérification de l'intégrité des blocs

Procédez comme suit pour configurer la stratégie de vérification de l'intégrité des blocs.

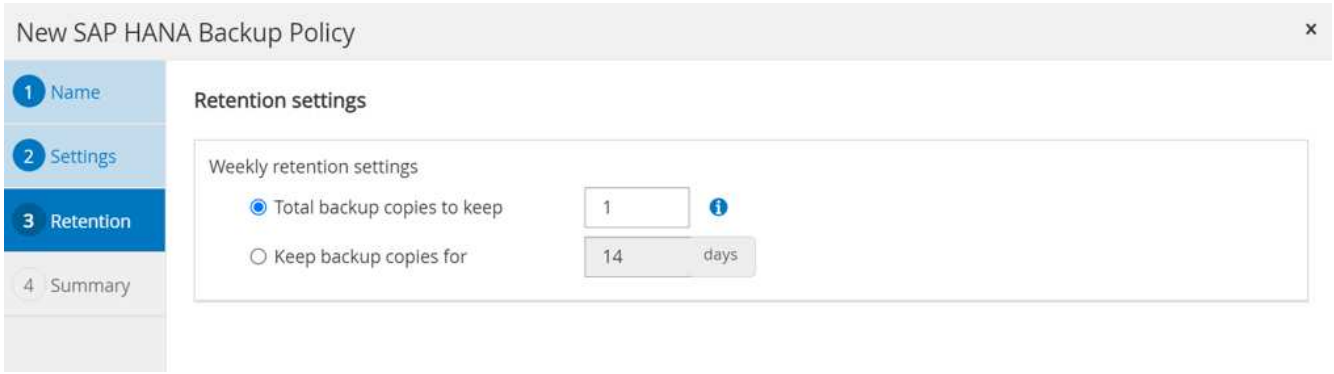
1. Accédez à Paramètres > stratégies et cliquez sur Nouveau.
2. Entrez le nom et la description de la stratégie. Cliquez sur Suivant.



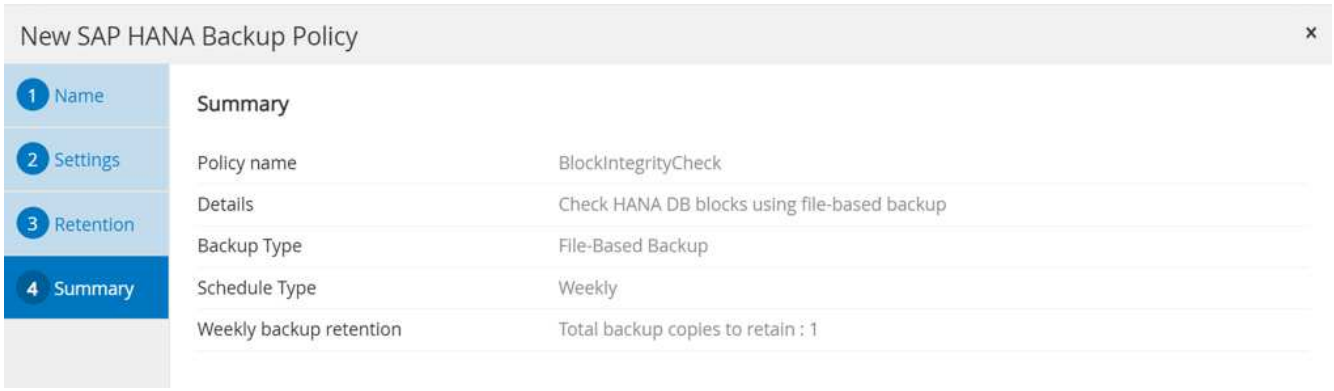
3. Définissez le type de sauvegarde sur fichier et fréquence de planification sur hebdomadaire. La planification elle-même est configurée ultérieurement avec la configuration de protection des ressources HANA.

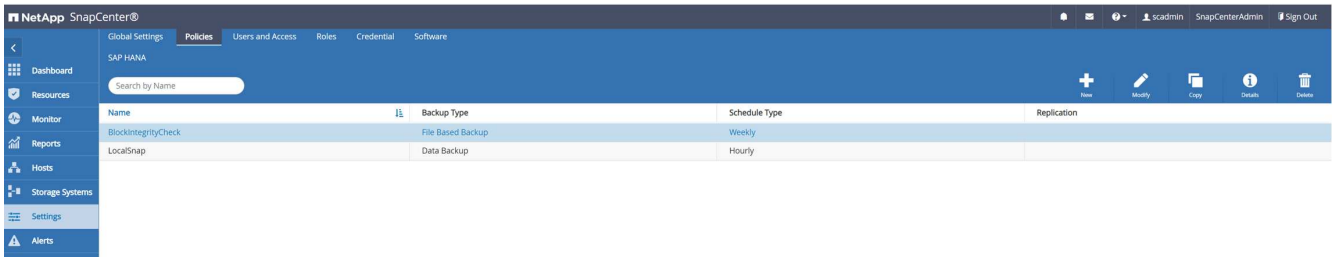


4. Configurez les paramètres de conservation pour les sauvegardes à la demande.



5. Sur la page Récapitulatif, cliquez sur Terminer.



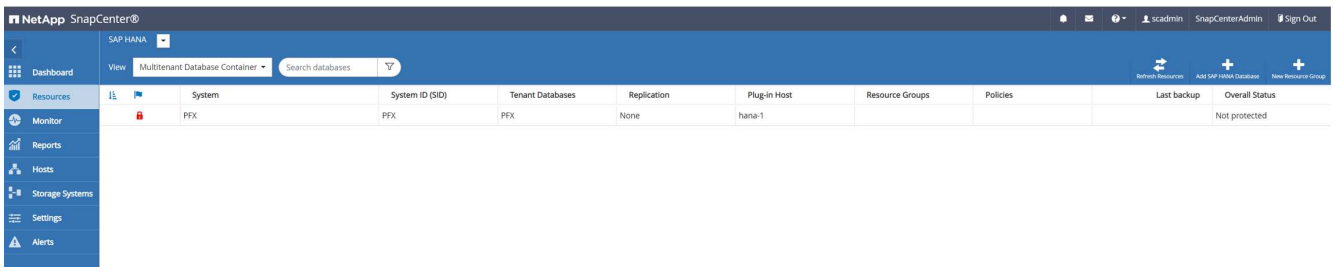


Configuration et protection d'une ressource HANA

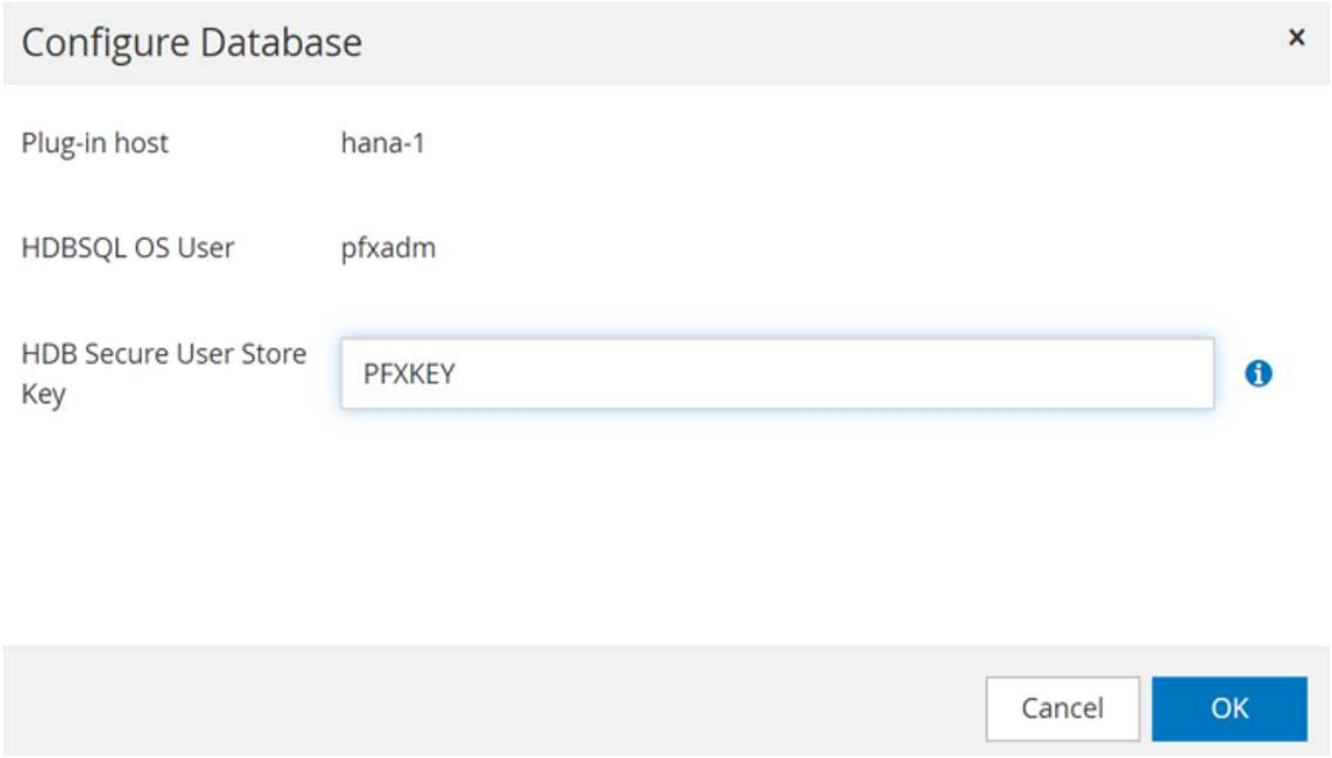
Une fois l'installation du plug-in terminée, le processus de détection automatique de la ressource HANA démarre automatiquement. Dans l'écran Ressources, une nouvelle ressource est créée, marquée comme étant verrouillée par l'icône de cadenas rouge. Pour configurer et protéger la nouvelle ressource HANA, effectuez la procédure suivante :

1. Sélectionnez et cliquez sur la ressource pour poursuivre la configuration.

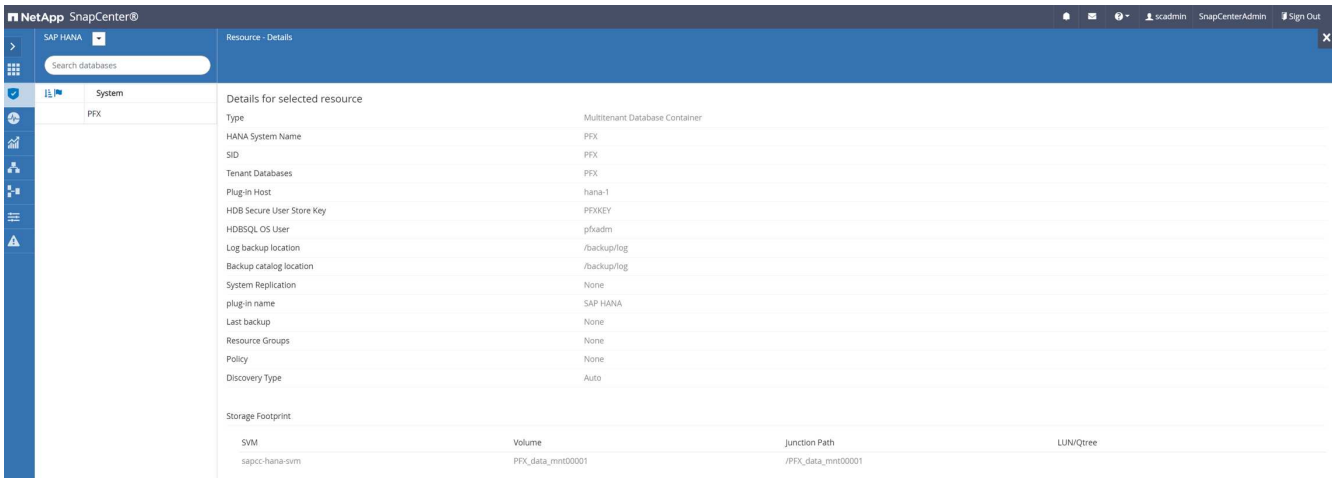
   Vous pouvez également déclencher manuellement le processus de détection automatique dans l'écran Ressources en cliquant sur Actualiser les ressources.



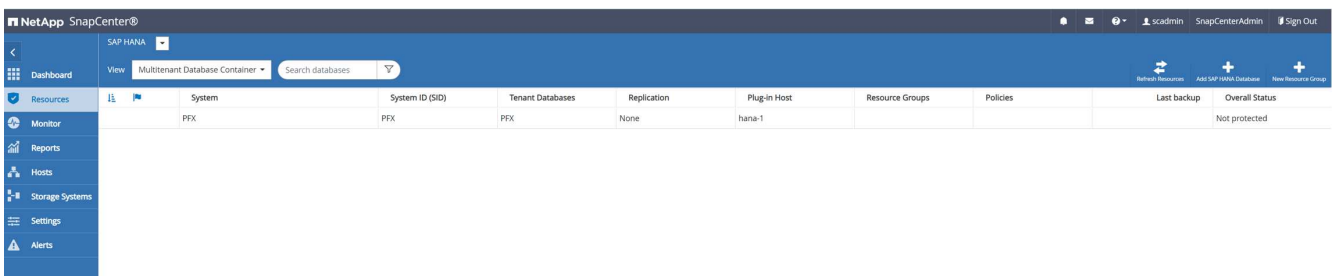
2. Fournissez la clé de magasin d'utilisateurs pour la base de données HANA.



La détection automatique du second niveau commence par la découverte des informations relatives aux données des locataires et à l'encombrement du stockage.



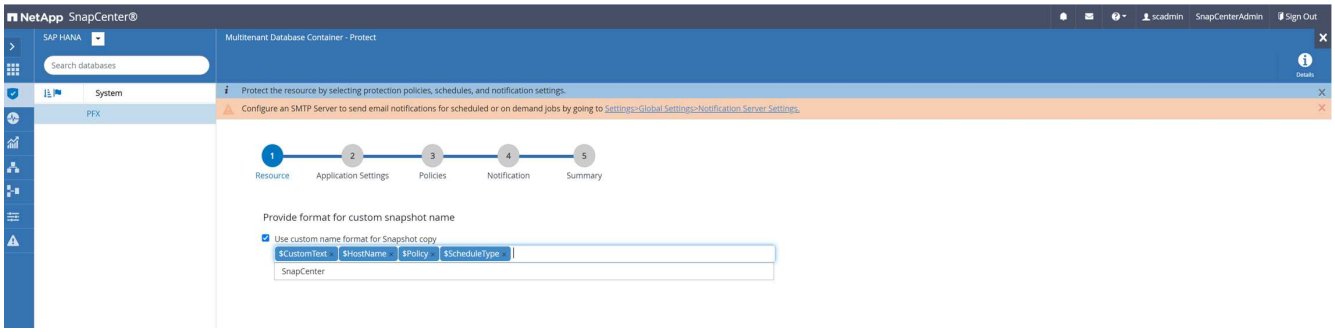
3. Dans l'onglet Ressources, double-cliquez sur la ressource pour configurer la protection des ressources.



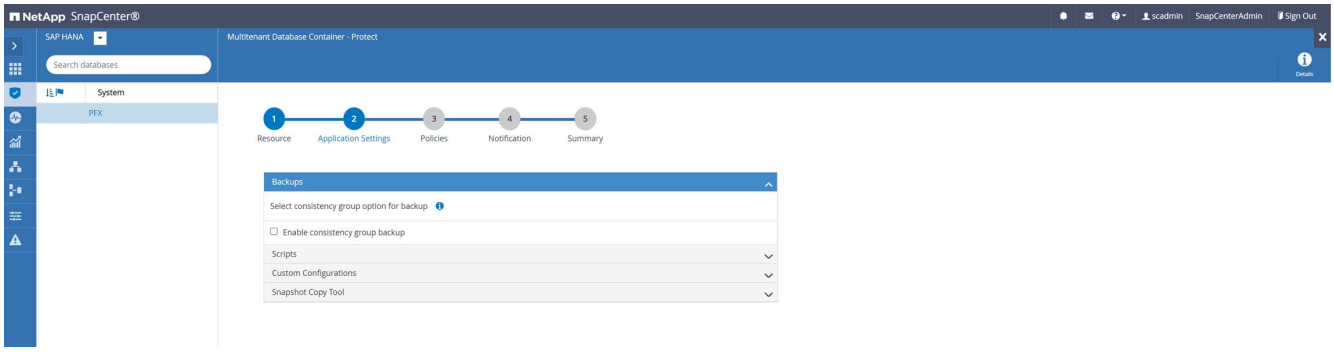
4. Configurez un format de nom personnalisé pour la copie Snapshot.

   NetApp recommande d'utiliser un nom de copie Snapshot personnalisé pour identifier facilement les

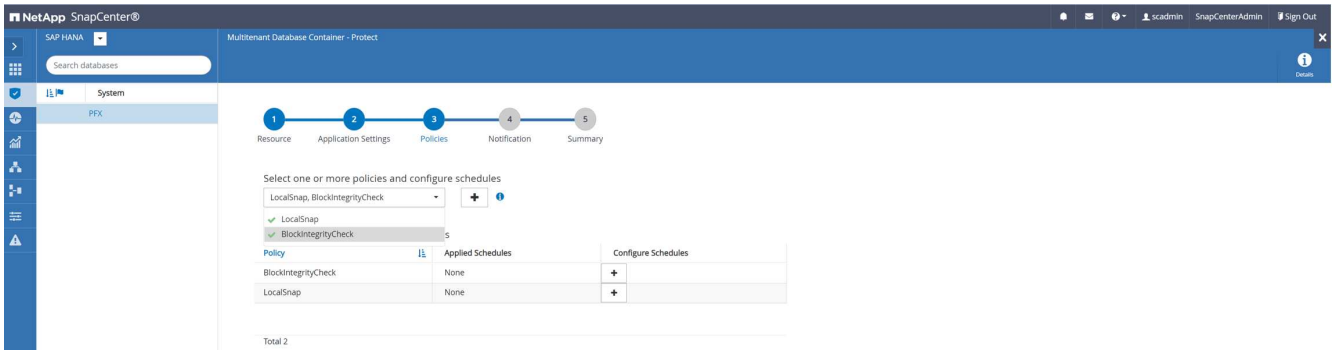
sauvegardes qui ont été créées avec quel type de règle et de planification. L'ajout du type de planification dans le nom de la copie Snapshot permet de distinguer les sauvegardes planifiées et à la demande. Le `schedule name` la chaîne pour les sauvegardes à la demande est vide, tandis que les sauvegardes planifiées incluent la chaîne `Hourly`, `Daily`, `or Weekly`.



5. Aucun paramètre spécifique ne doit être défini sur la page Paramètres de l'application. Cliquez sur Suivant.

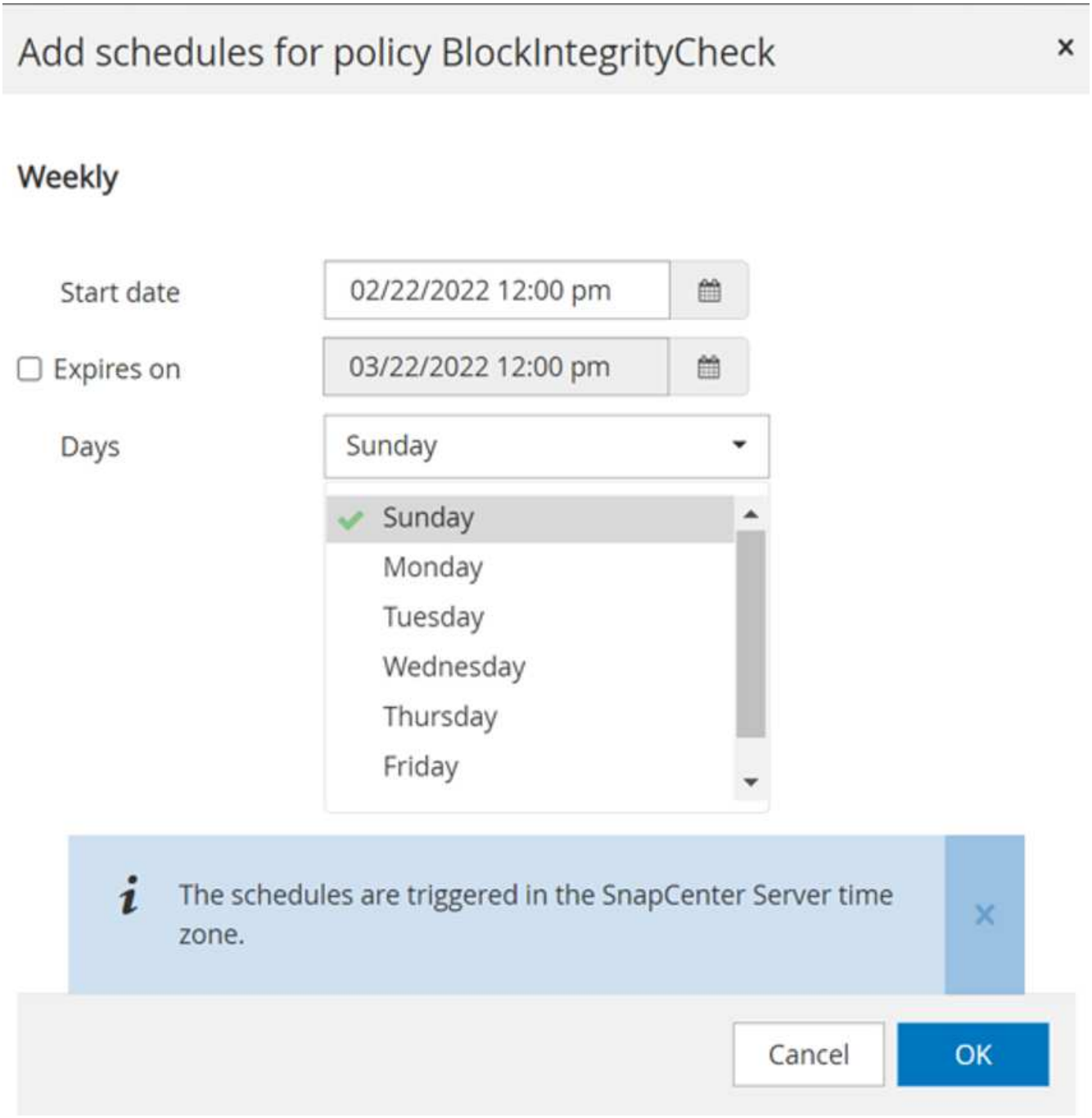


6. Sélectionnez les stratégies à ajouter à la ressource.



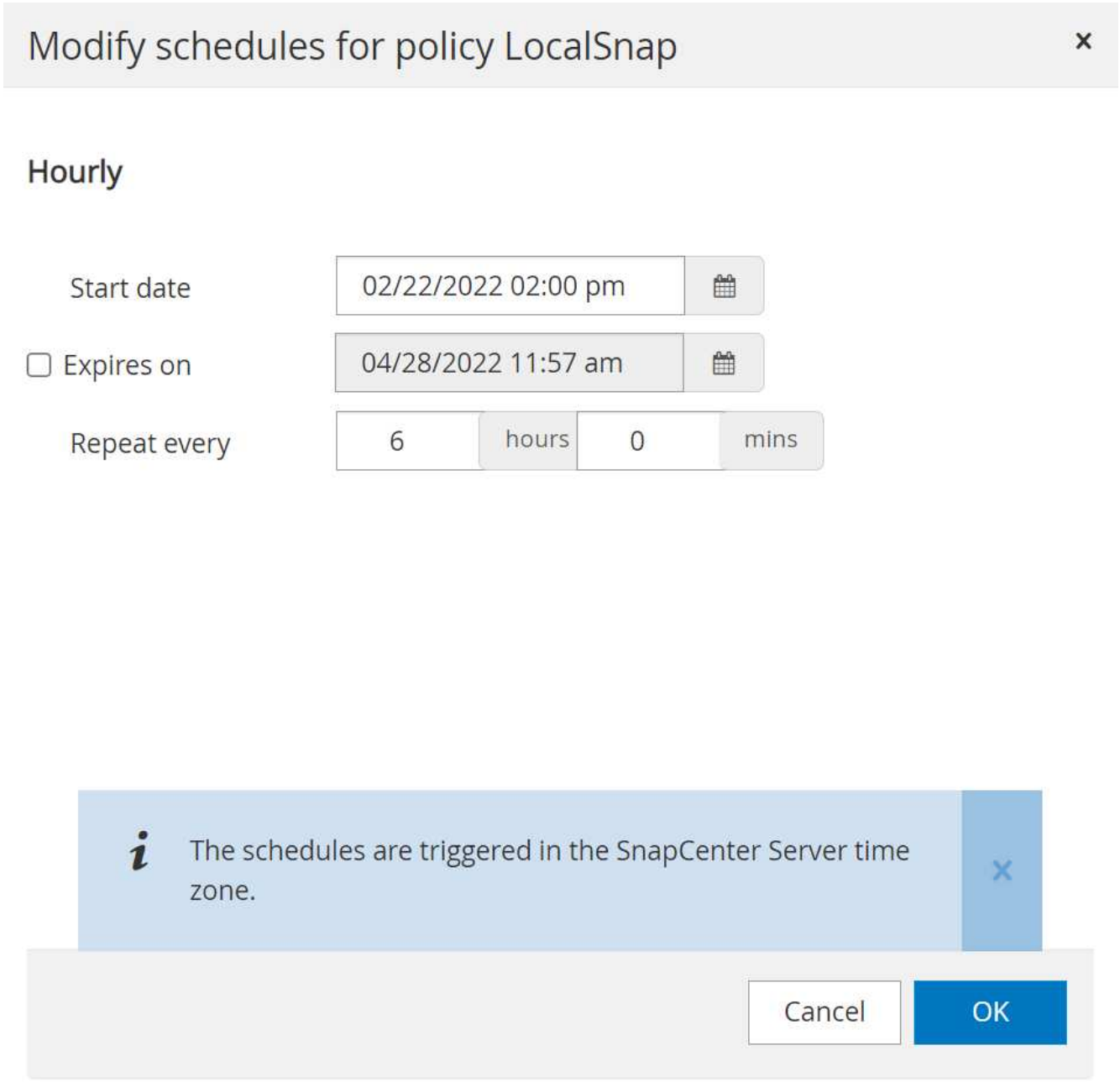
7. Définissez le planning de la règle de contrôle d'intégrité des blocs.

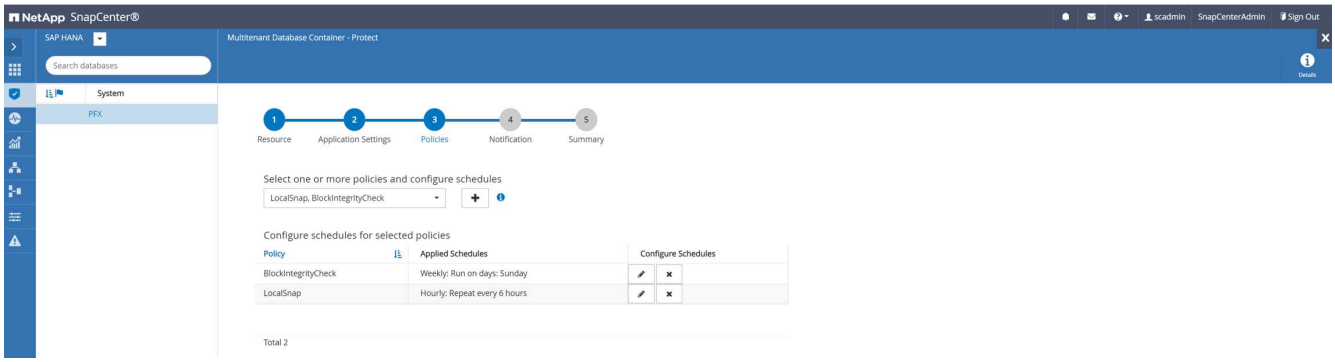
   Dans cet exemple, il est défini pour une fois par semaine.



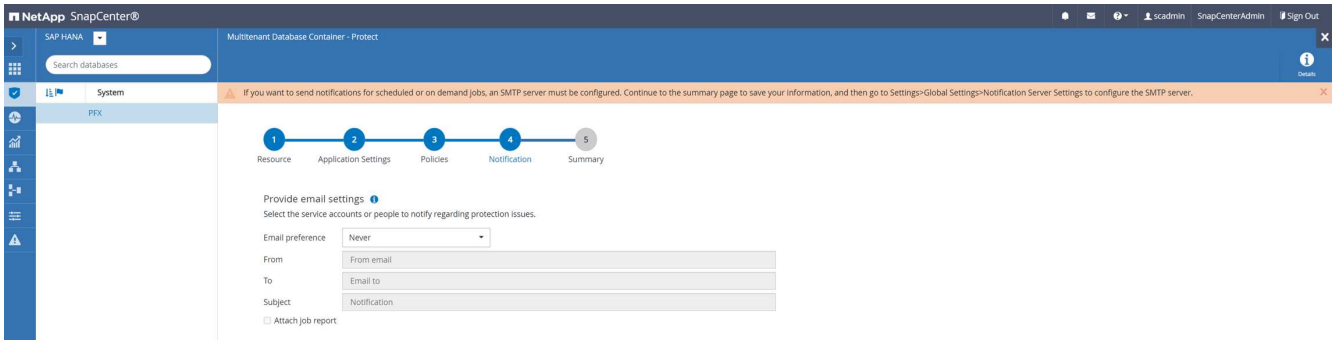
8. Définissez la planification de la règle Snapshot locale.

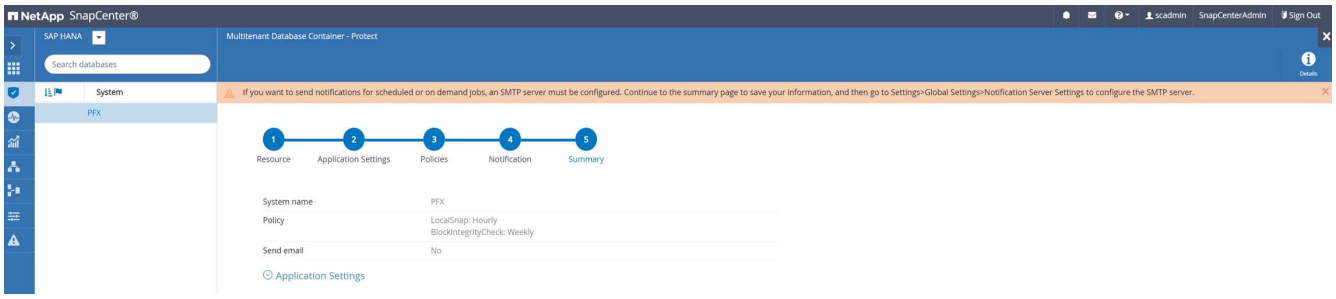
   Dans cet exemple, il est défini toutes les 6 heures.



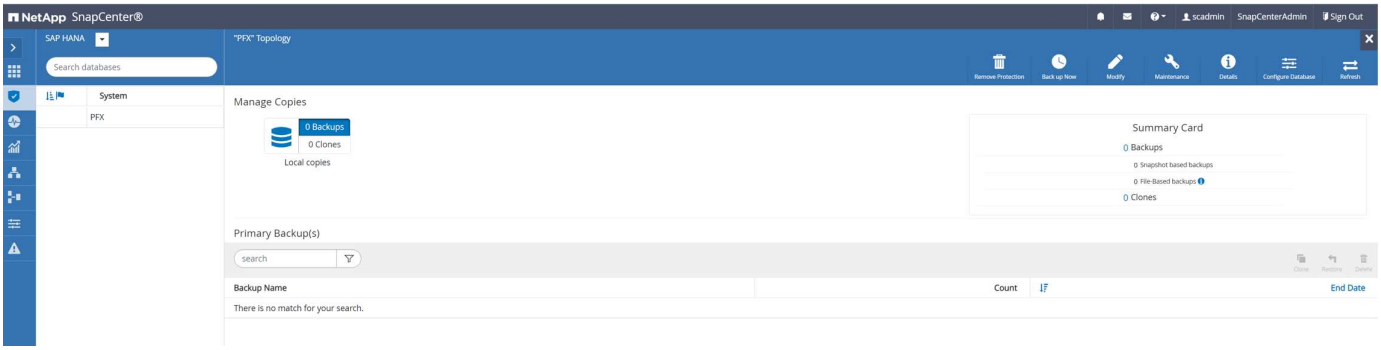


9. Fournir des informations sur la notification par e-mail.





La configuration des ressources HANA est maintenant terminée et vous pouvez exécuter les sauvegardes.



Opérations de sauvegarde SnapCenter

Vous pouvez créer une sauvegarde Snapshot à la demande et effectuer un contrôle d'intégrité des blocs à la demande.

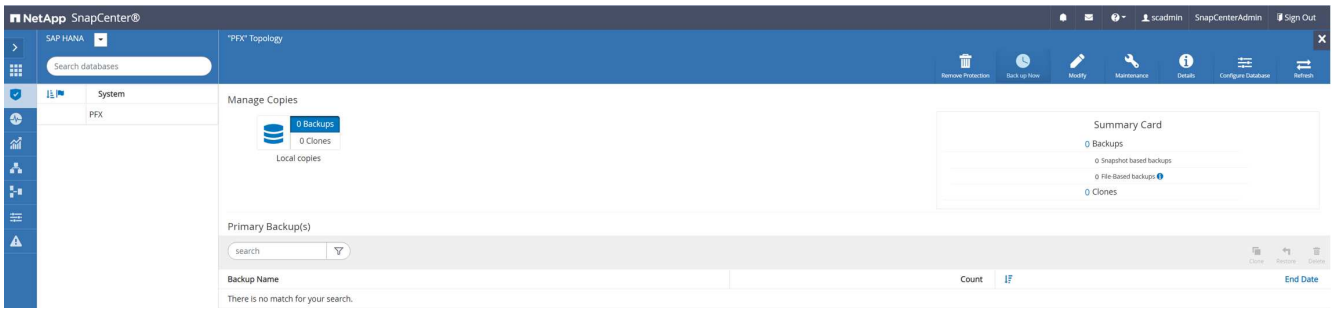
Créer une sauvegarde Snapshot à la demande

Procédez comme suit pour créer des sauvegardes Snapshot à la demande.

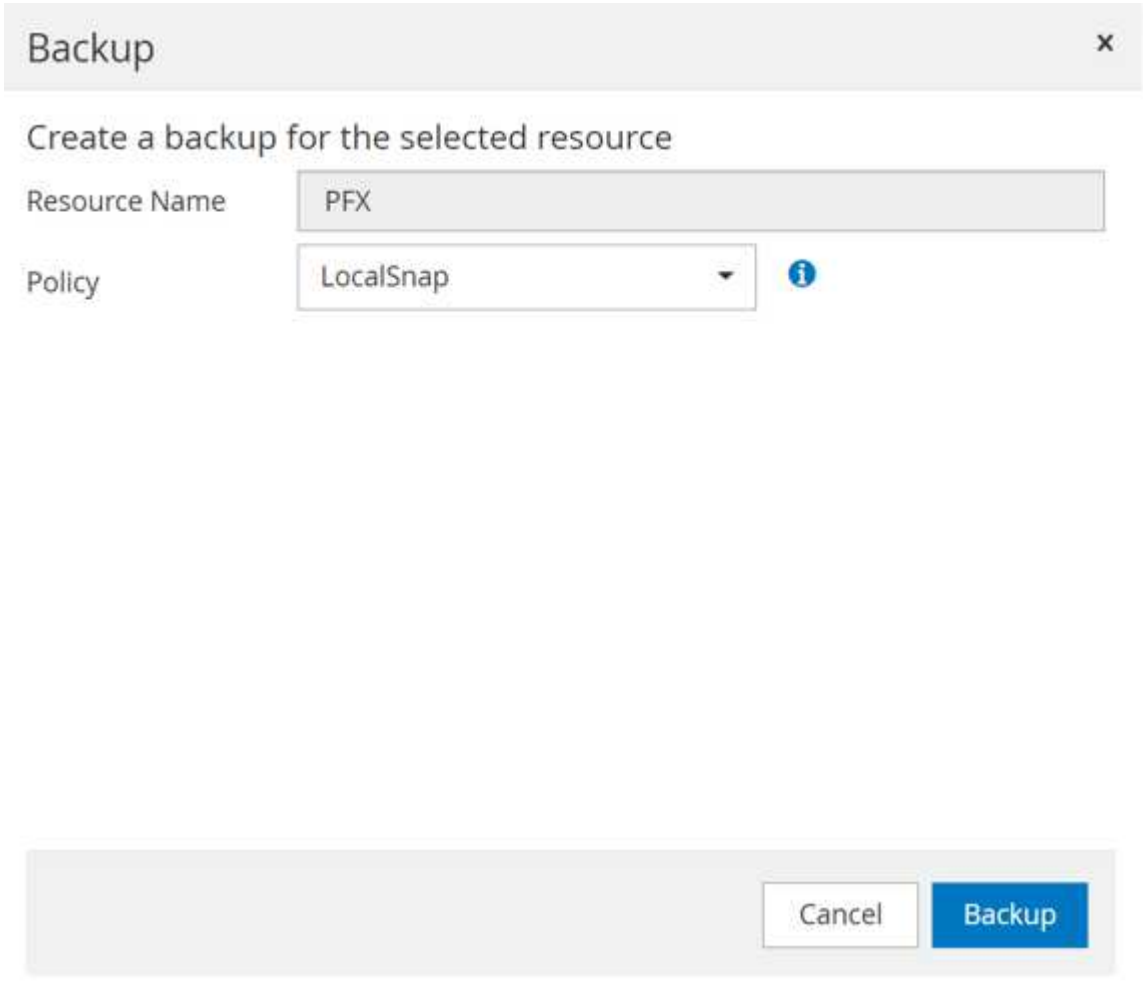
1. Dans la vue ressource, sélectionnez la ressource et double-cliquez sur la ligne pour passer à la vue topologie.

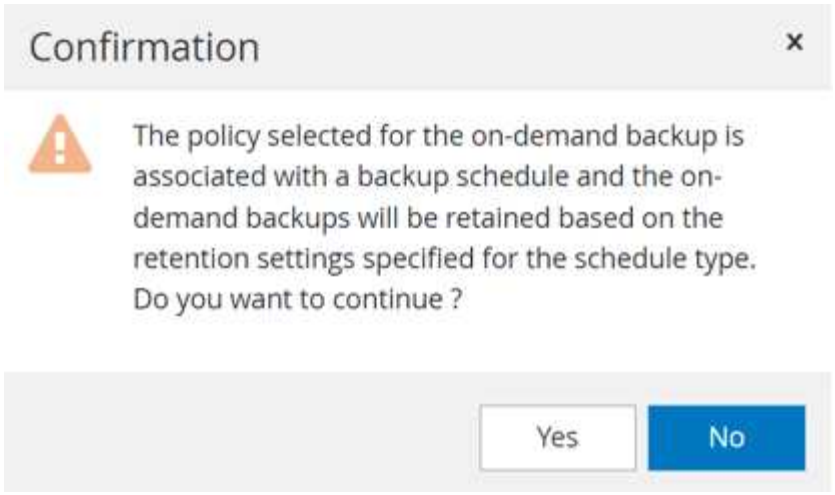
   La vue topologie des ressources fournit une vue d'ensemble de toutes les sauvegardes disponibles qui ont été créées à l'aide de SnapCenter. La partie supérieure de cette vue affiche la topologie de sauvegarde indiquant les sauvegardes sur le stockage primaire (copies locales) et, le cas échéant, sur le stockage de sauvegarde hors site (copies vault).

2. Dans la ligne supérieure, sélectionnez l'icône Sauvegarder maintenant pour lancer une sauvegarde à la demande.



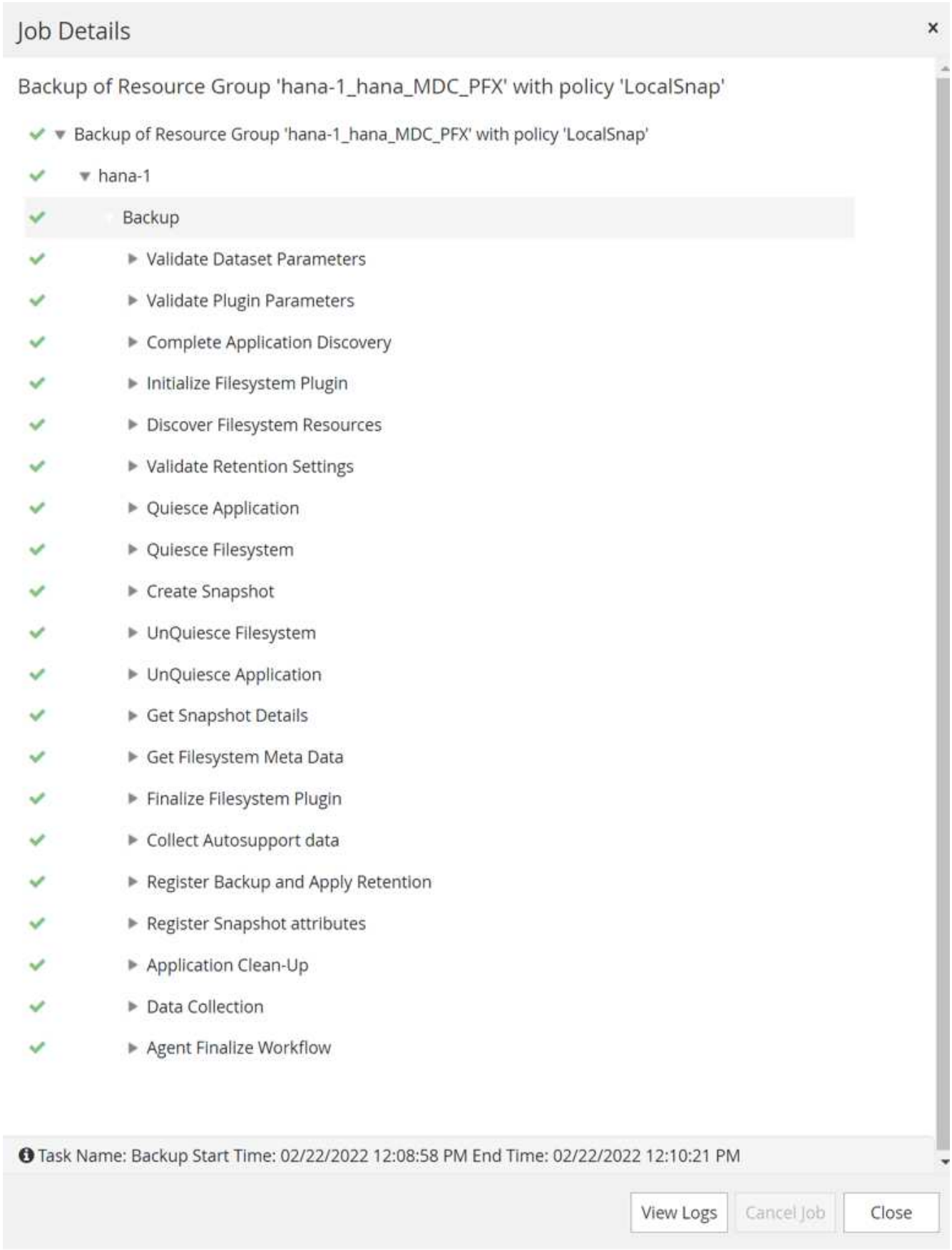
3. Dans la liste déroulante, sélectionnez la stratégie de sauvegarde `LocalSnap`, Puis cliquez sur Sauvegarder pour démarrer la sauvegarde à la demande.





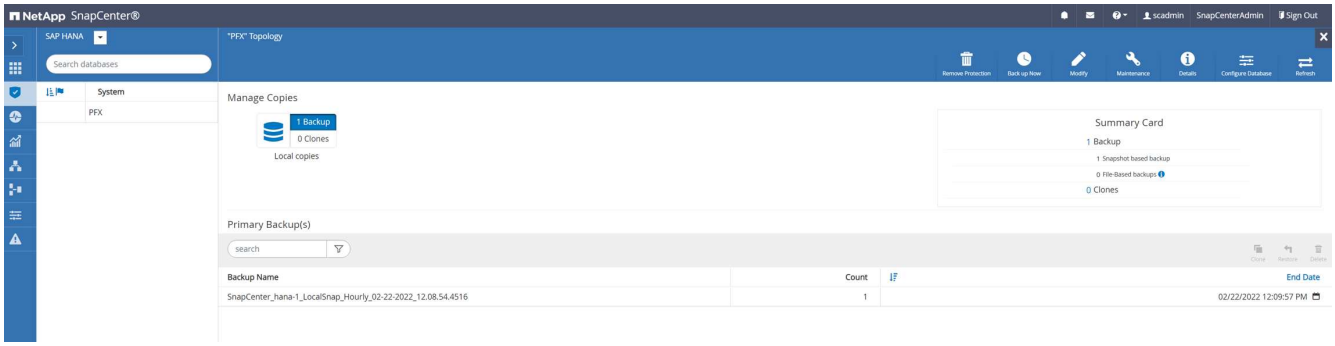
Un journal des cinq tâches précédentes est affiché dans la zone activité au bas de la vue topologie.

4. Les détails du travail s'affichent lorsque vous cliquez sur la ligne d'activité du travail dans la zone activité. Vous pouvez ouvrir un journal détaillé des travaux en cliquant sur Afficher les journaux

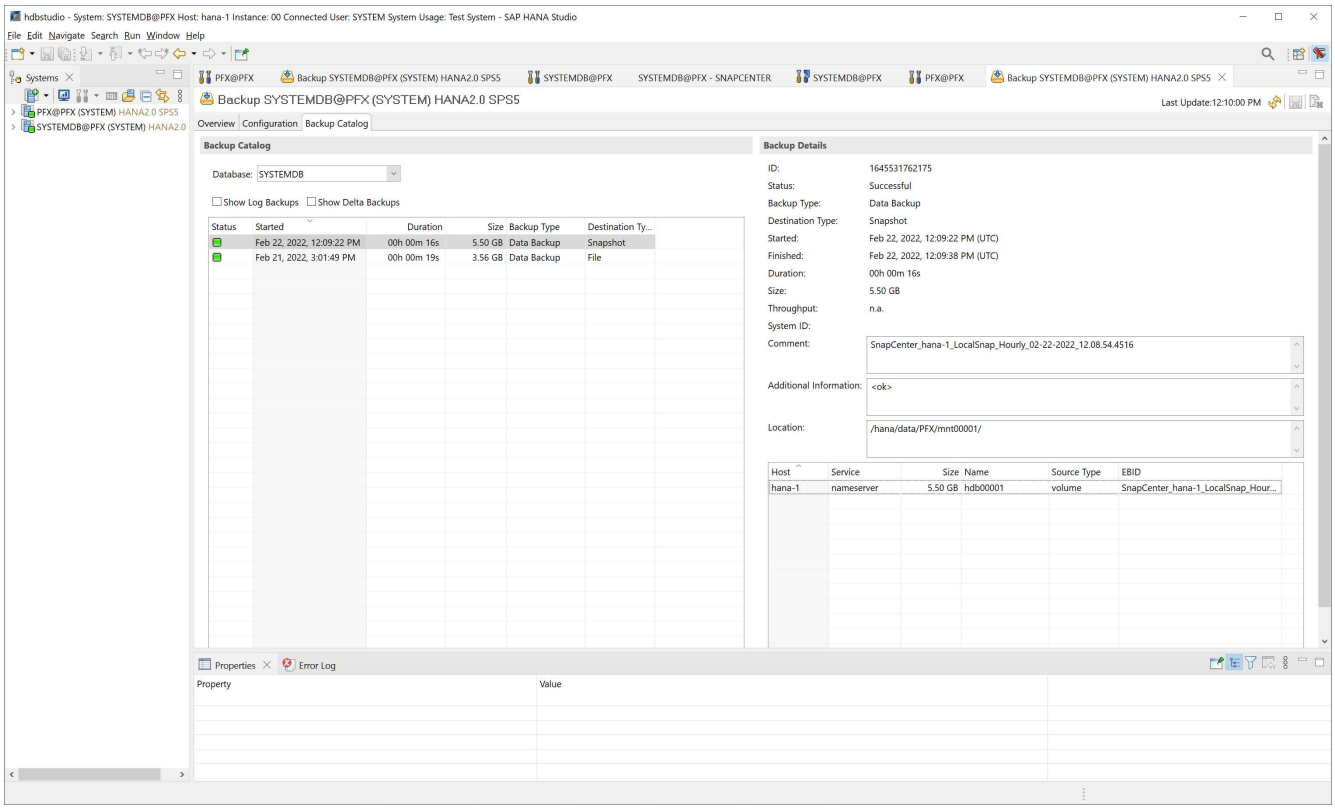


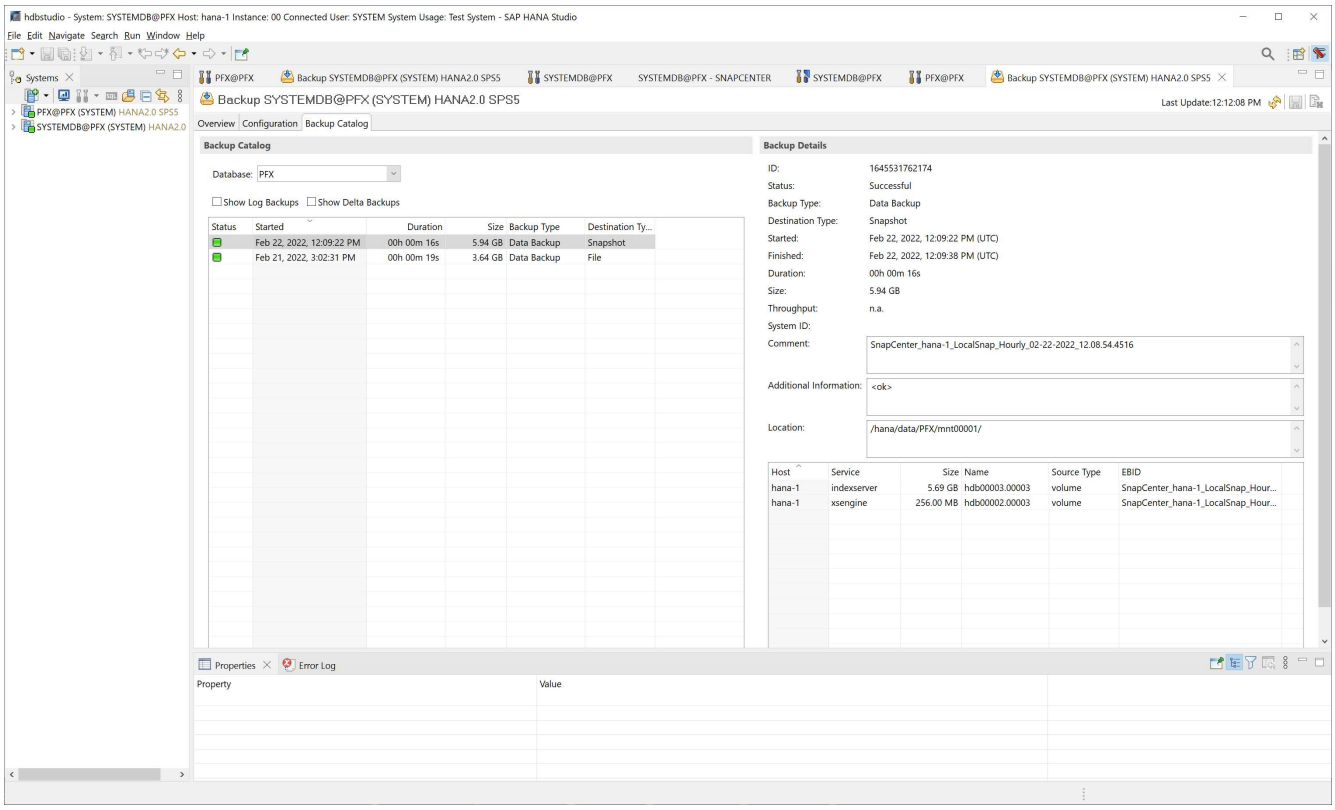
Une fois la sauvegarde terminée, une nouvelle entrée s'affiche dans la vue topologique. Les noms de sauvegarde suivent la même nomenclature que le nom de Snapshot défini dans la section "« Configurer et protéger une ressource HANA »."

Vous devez fermer et rouvrir la vue topologique pour afficher la liste des sauvegardes mise à jour.



Dans le catalogue des sauvegardes SAP HANA, le nom de la sauvegarde SnapCenter est stocké comme A. `Comment` champ également `External Backup ID (EBID)`. Cette figure est présentée dans la figure suivante pour la base de données système et dans la figure suivante pour la base de données de tenant PFX.



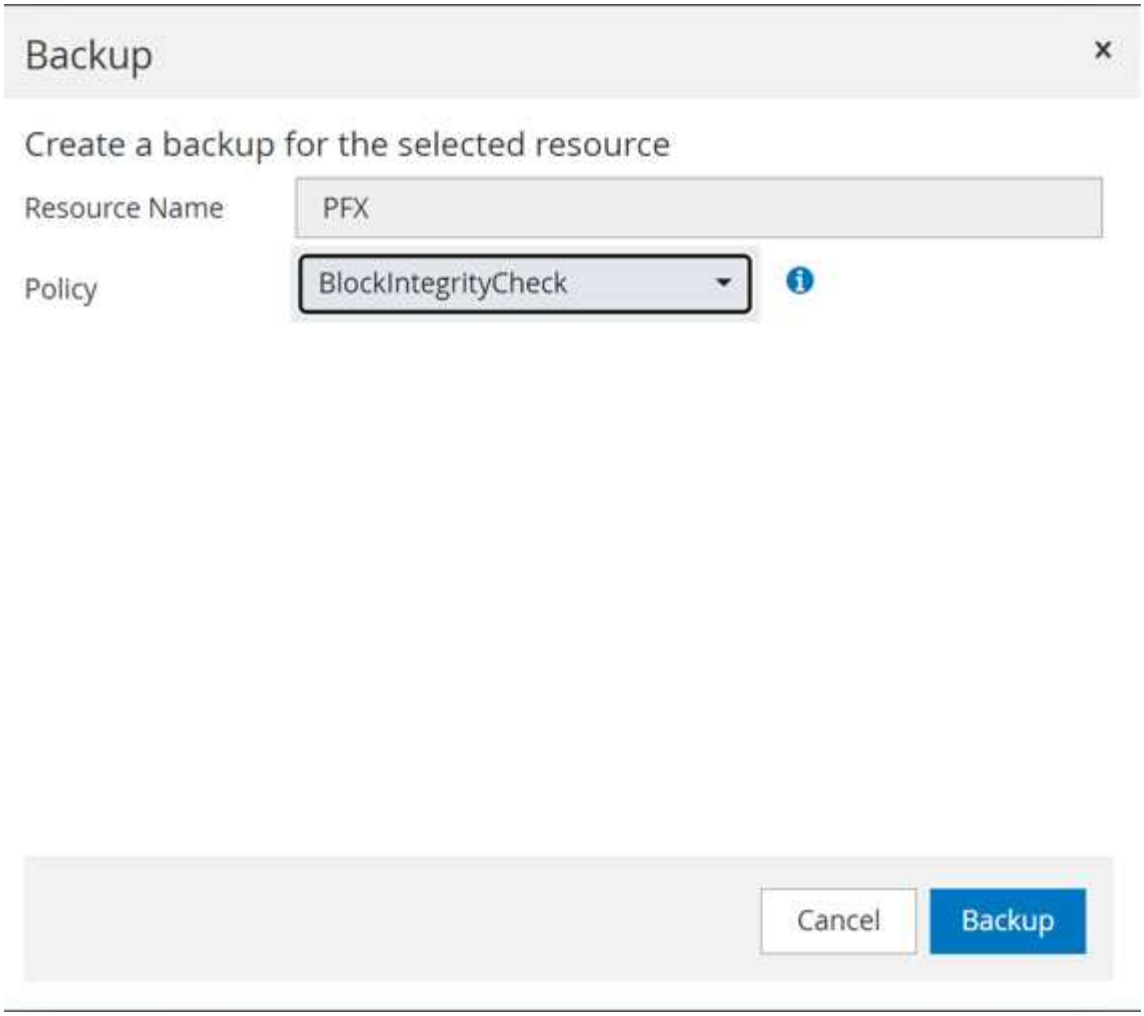


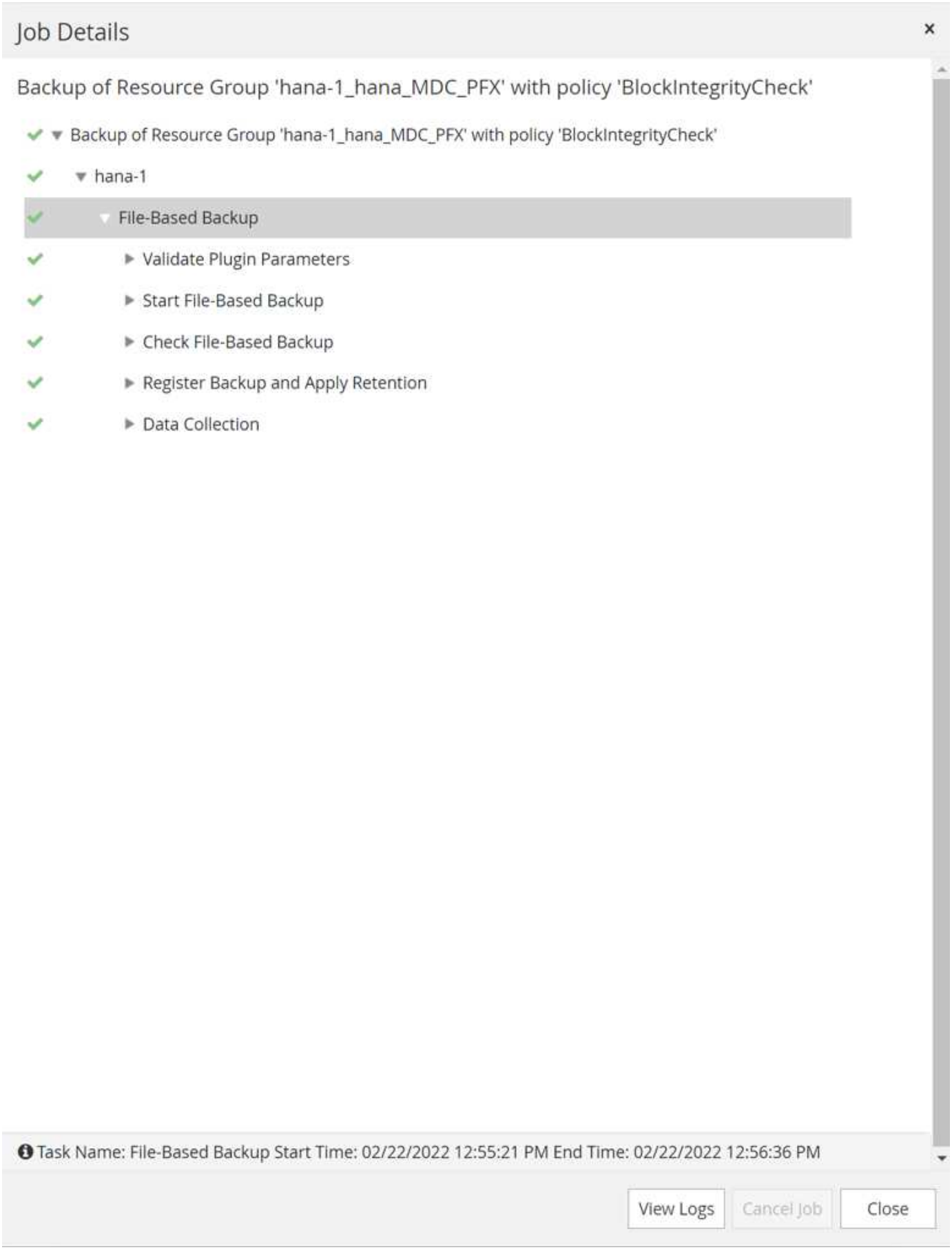
Sur le système de fichiers FSX pour ONTAP, vous pouvez lister les sauvegardes Snapshot en vous connectant à la console de la SVM.

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

Créer une opération de contrôle d'intégrité des blocs à la demande

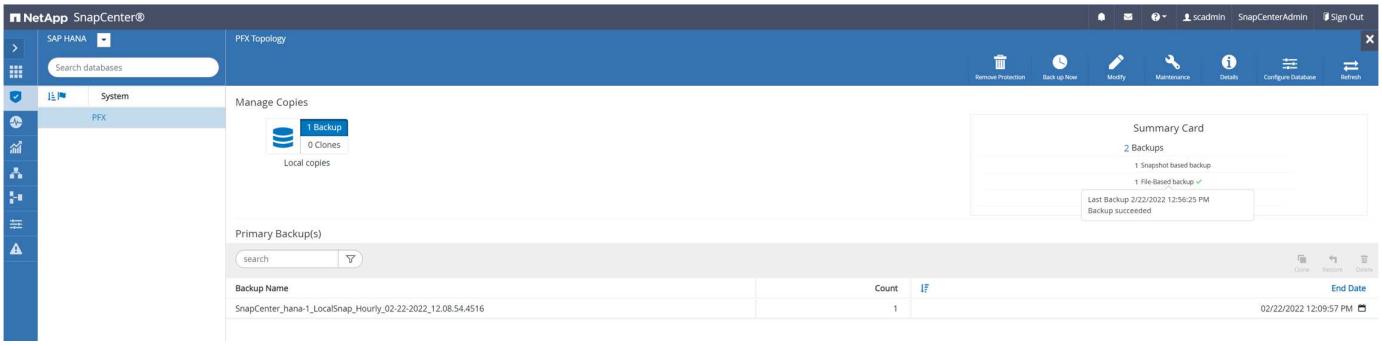
Une opération de vérification de l'intégrité des blocs à la demande est exécutée de la même manière qu'une tâche de sauvegarde Snapshot, en sélectionnant la règle BlockIntegrtyCheck. Lorsque vous planifiez des sauvegardes à l'aide de cette règle, SnapCenter crée une sauvegarde standard des fichiers SAP HANA pour les bases de données système et locataires.


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

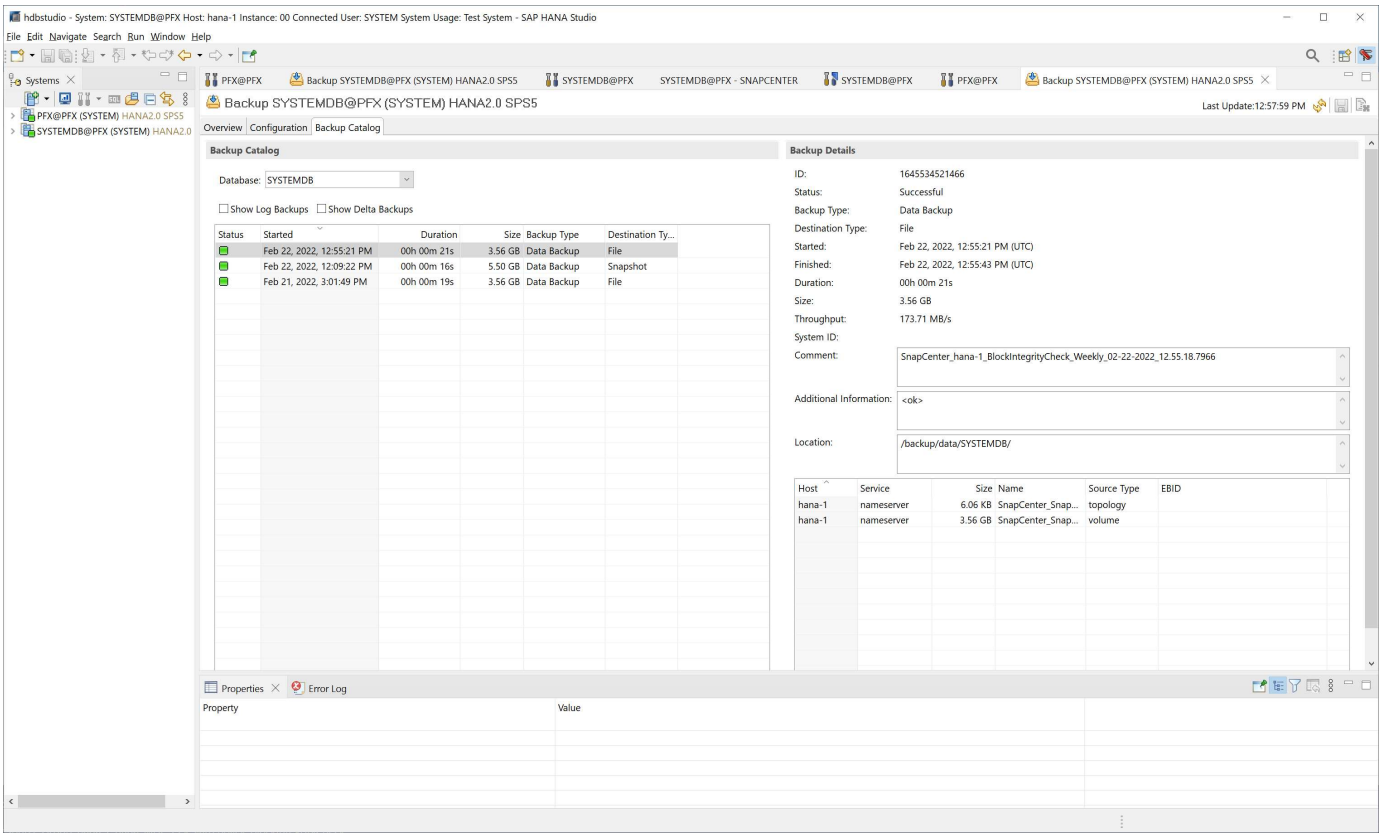


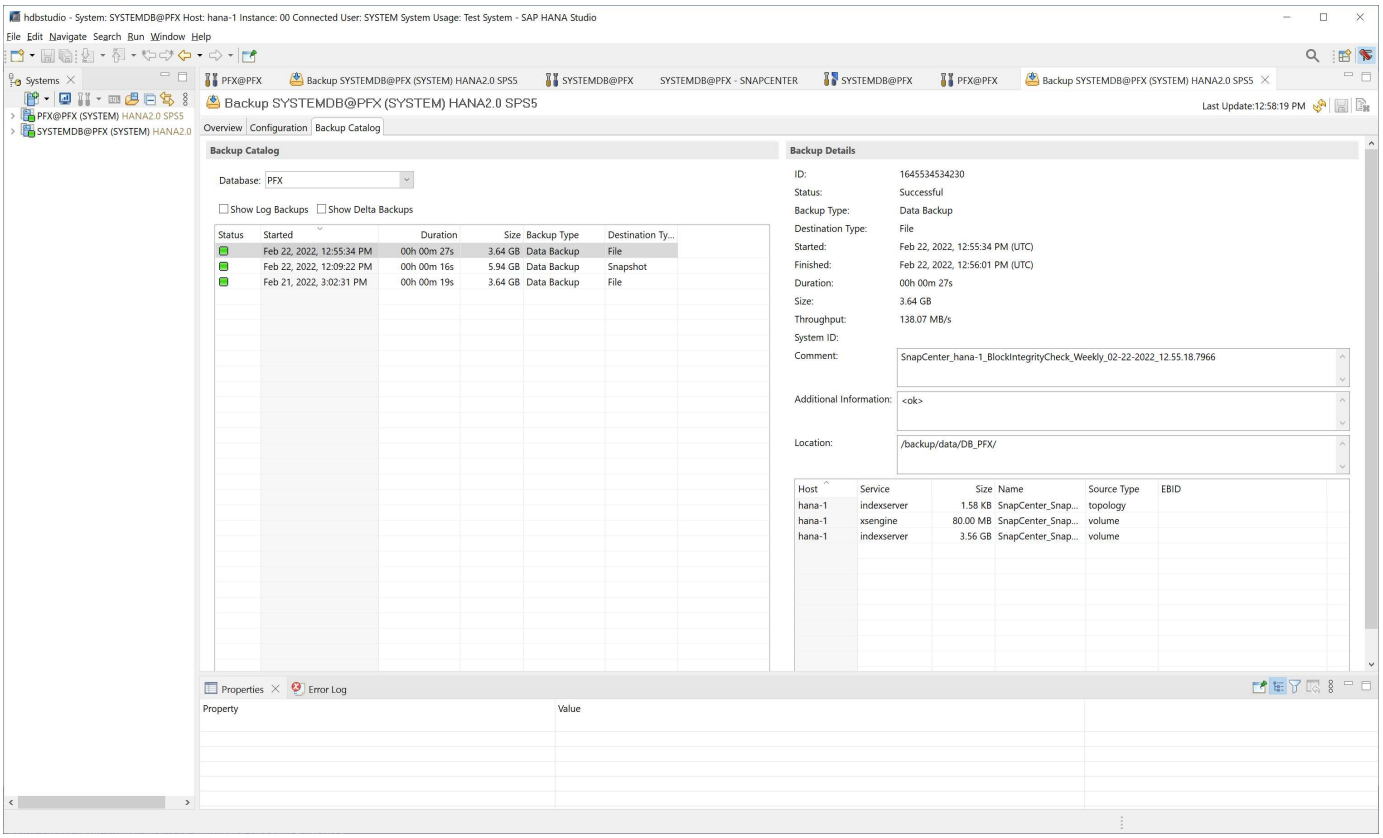
SnapCenter n’affiche pas la vérification de l’intégrité des blocs, de la même manière que les sauvegardes

basées sur des copies Snapshot. À la place, la carte récapitulative affiche le nombre de sauvegardes basées sur des fichiers et l'état de la sauvegarde précédente.



Le catalogue de sauvegardes SAP HANA affiche les entrées des bases de données système et locataire. Les figures suivantes montrent le contrôle d'intégrité des blocs SnapCenter dans le catalogue de sauvegarde du système et de la base de données des locataires.





Un contrôle réussi de l'intégrité des blocs crée des fichiers de sauvegarde standard des données SAP HANA. SnapCenter utilise le chemin de sauvegarde qui a été configuré avec la base de données HANA pour des opérations de sauvegarde de données basées sur des fichiers.

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

Sauvegarde de volumes non-données

La sauvegarde de volumes non-data fait partie intégrante de SnapCenter et du plug-in SAP HANA.

La protection du volume des données de la base de données est suffisante pour restaurer et restaurer la base de données SAP HANA à un point donné dans le temps, à condition que les ressources d'installation de la base de données et les journaux requis soient toujours disponibles.

Pour restaurer des données à partir de situations où d'autres fichiers non data doivent être restaurés, NetApp

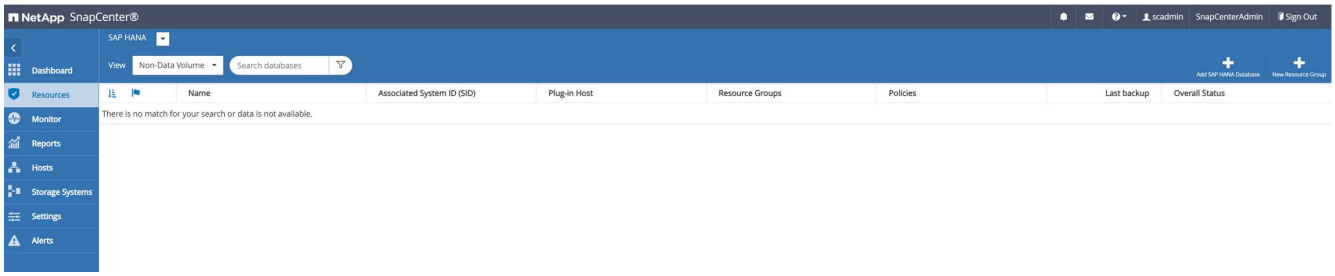
recommande de développer une stratégie de sauvegarde supplémentaire pour les volumes sans data afin de compléter la sauvegarde de la base de données SAP HANA. En fonction de vos besoins spécifiques, la sauvegarde de volumes non-données peut varier dans les paramètres de fréquence de planification et de conservation. Il est également important de tenir compte de la fréquence à laquelle les fichiers ne sont pas des données sont modifiés. Par exemple, le volume HANA `/hana/shared` Contient des exécutables mais aussi des fichiers de trace SAP HANA. Alors que les exécutables ne changent que lorsque la base de données SAP HANA est mise à niveau, les fichiers de trace SAP HANA peuvent avoir besoin d'une fréquence de sauvegarde plus élevée pour prendre en charge l'analyse des problèmes avec SAP HANA.

La sauvegarde de volumes sans données SnapCenter permet de créer en quelques secondes des copies Snapshot de tous les volumes concernés avec la même efficacité d'espace que les sauvegardes de bases de données SAP HANA. La différence est qu'aucune communication SQL avec une base de données SAP HANA n'est requise.

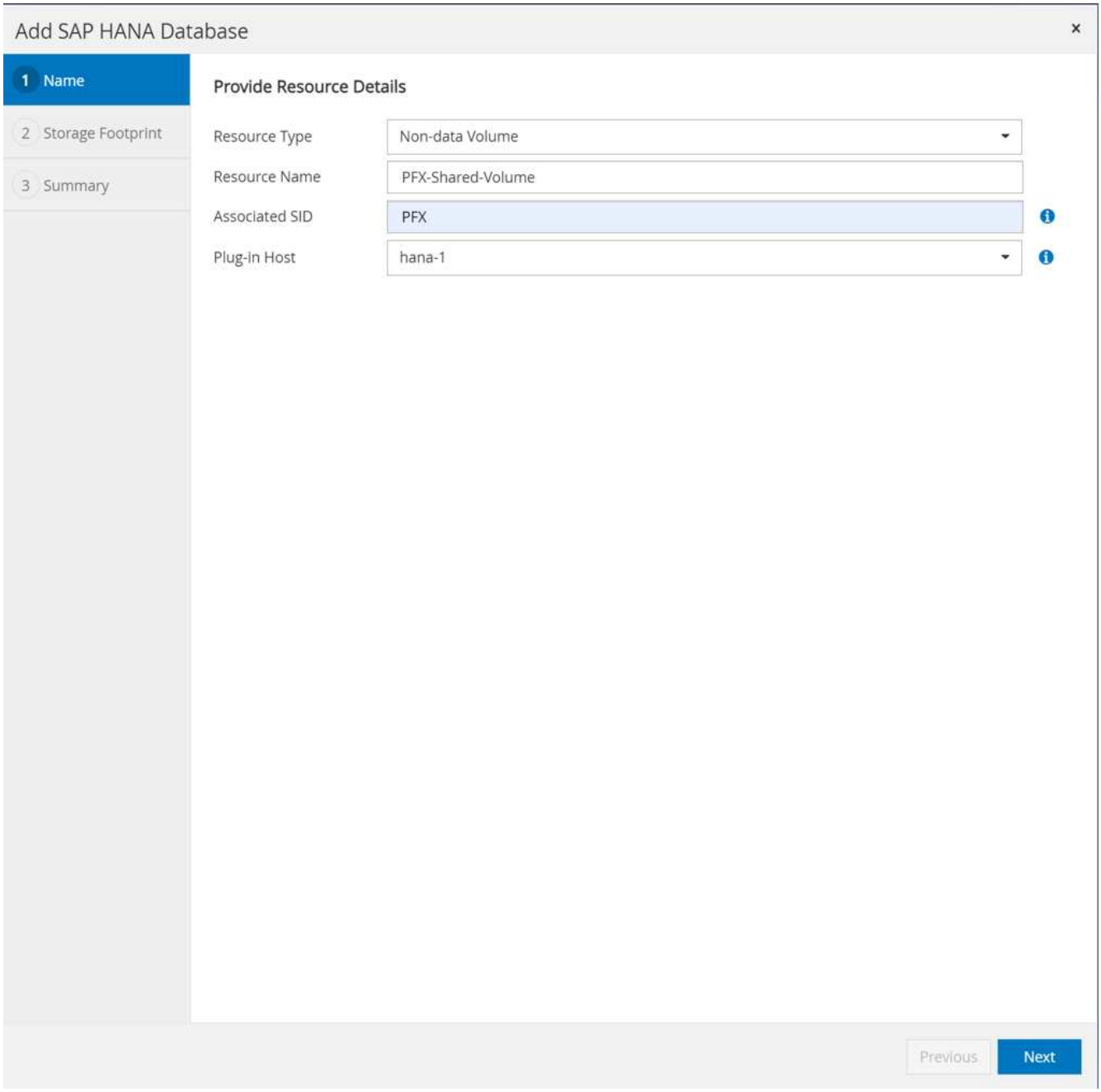
Configurez les ressources sans volume de données

La procédure suivante permet de configurer des ressources sans volume de données :

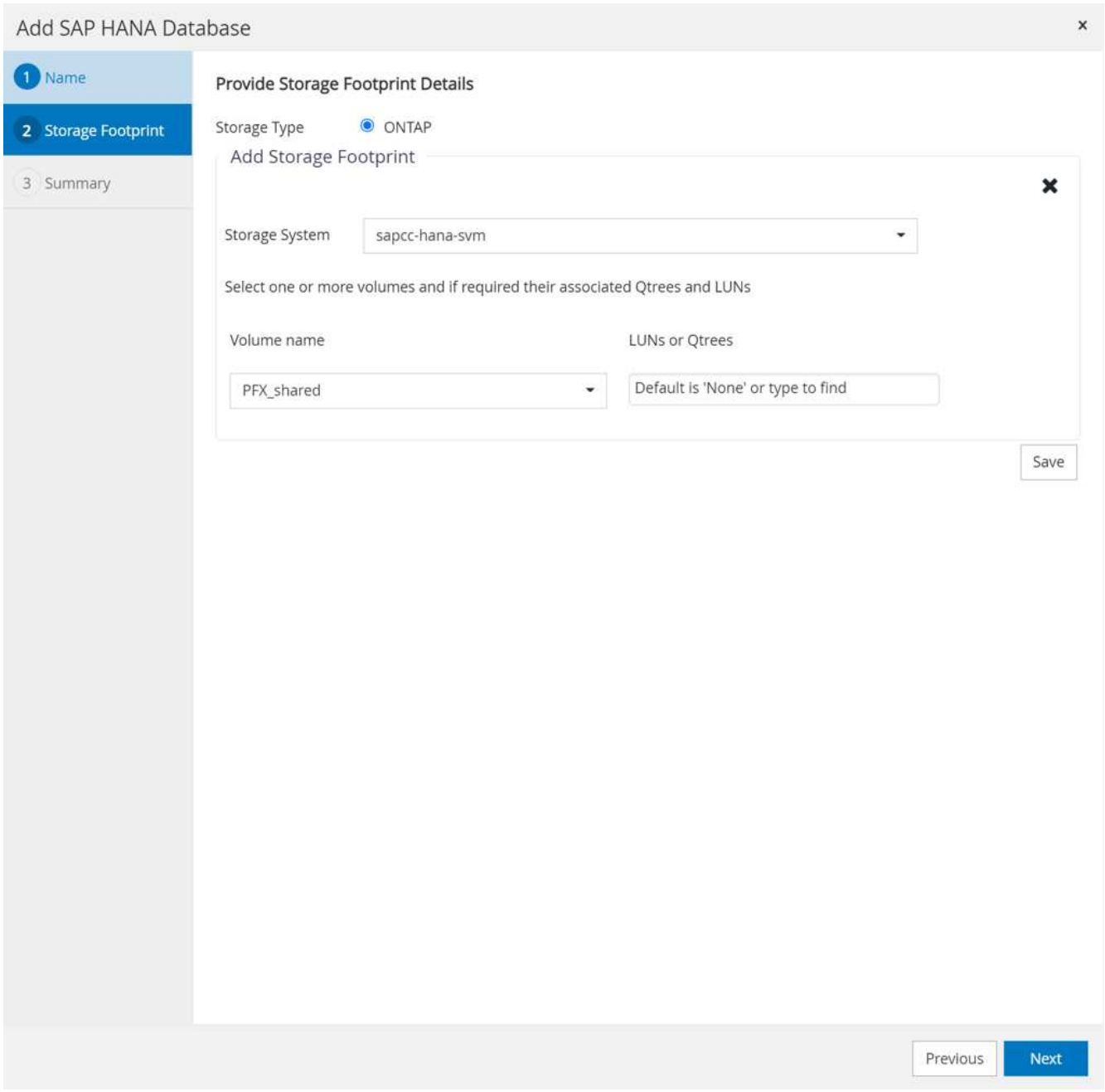
1. Dans l'onglet Ressources, sélectionnez non-Volume de données et cliquez sur Ajouter base de données SAP HANA.



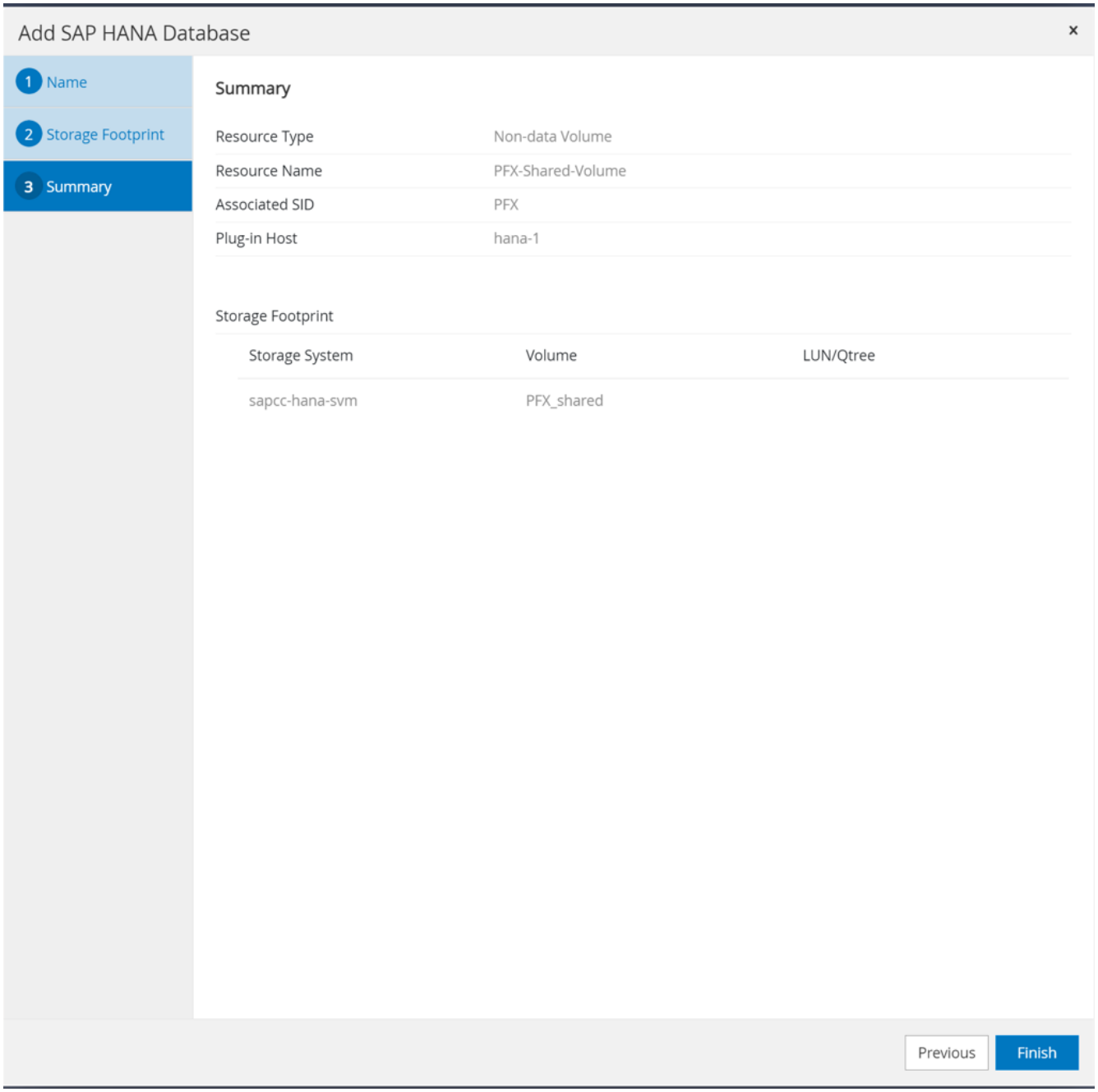
2. À l'étape une de la boîte de dialogue Ajouter une base de données SAP HANA, dans la liste Type de ressource, sélectionnez volumes non-data. Spécifiez un nom pour la ressource, le SID associé et l'hôte du plug-in SAP HANA que vous souhaitez utiliser pour la ressource, puis cliquez sur Next (Suivant).



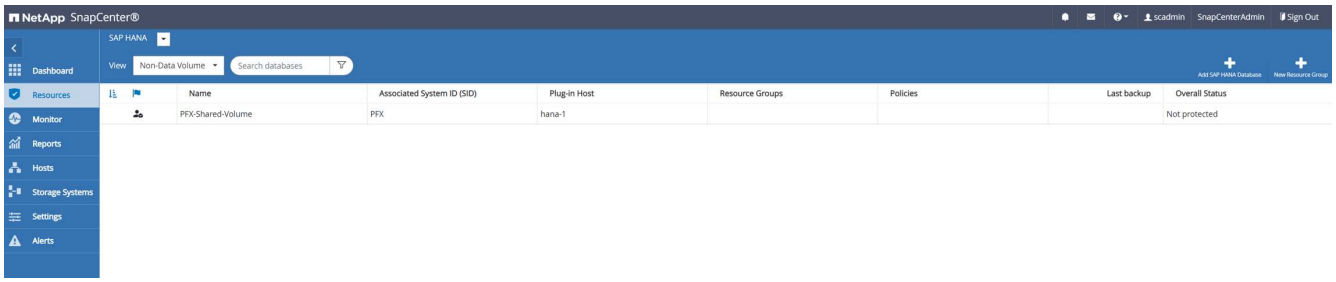
3. Ajoutez le SVM et le volume de stockage comme empreinte du stockage, puis cliquez sur « Next » (Suivant).



4. Pour enregistrer les paramètres, cliquez sur Terminer à l'étape de résumé.



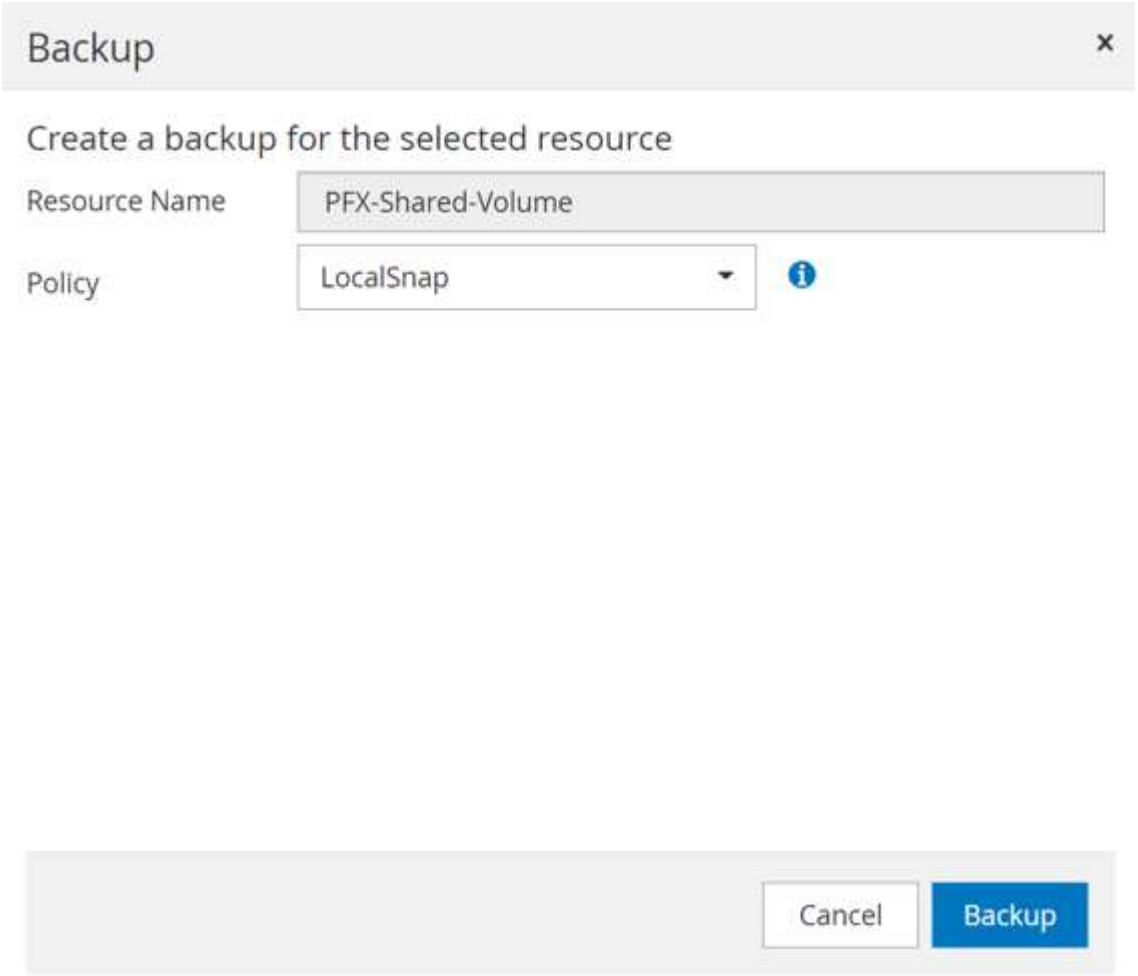
Le nouveau volume sans données est maintenant ajouté à SnapCenter. Double-cliquez sur la nouvelle ressource pour exécuter la protection des ressources.



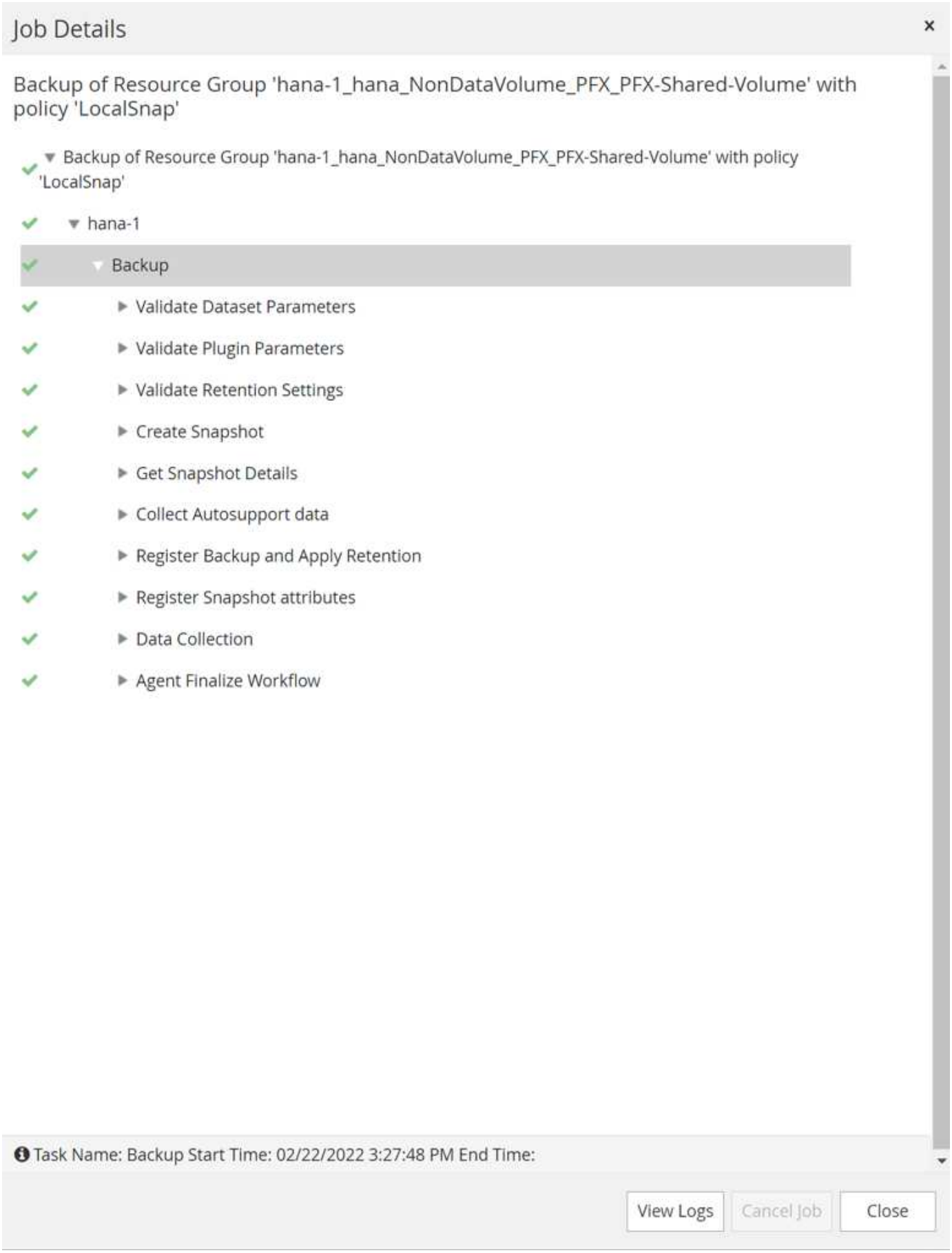
La protection des ressources est effectuée de la même manière que pour une ressource de base de données HANA.

5. Vous pouvez maintenant exécuter une sauvegarde en cliquant sur Backup Now.

6. Sélectionnez la stratégie et démarrez l'opération de sauvegarde.

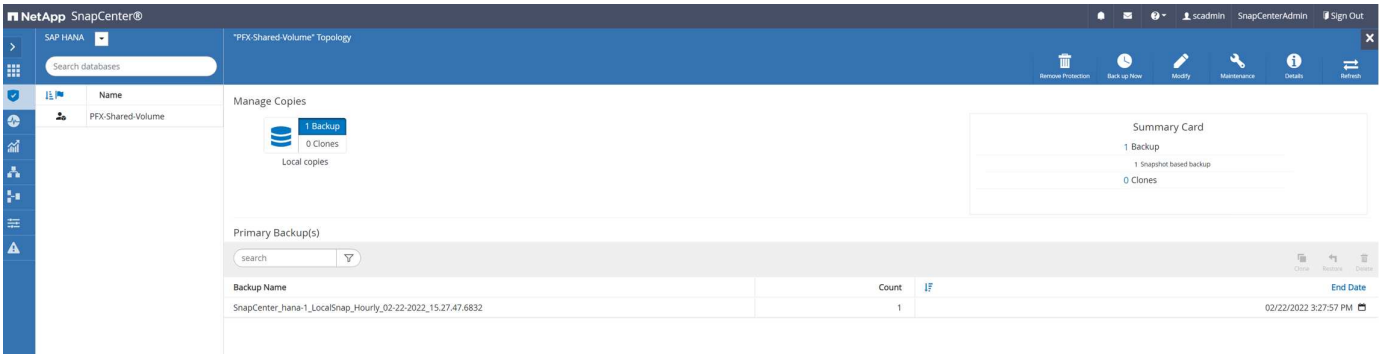


Le journal des travaux SnapCenter affiche les différentes étapes du flux de travail.



La nouvelle sauvegarde est désormais visible dans la vue des ressources de la ressource sans volume de

données.



Restaurer et restaurer

Avec SnapCenter, les opérations de restauration et de restauration automatisées sont prises en charge pour les systèmes MDC à un seul hôte HANA avec un seul locataire. Pour les systèmes à plusieurs hôtes ou MDC avec plusieurs locataires, SnapCenter n'exécute l'opération de restauration que et vous devez effectuer la restauration manuellement.

Vous pouvez exécuter une opération de restauration et de récupération automatisée en procédant comme suit :

1. Sélectionnez la sauvegarde à utiliser pour l'opération de restauration.
2. Sélectionnez le type de restauration. Sélectionnez Complete Restore with Volume Revert ou with Volume Revert.
3. Sélectionnez le type de récupération parmi les options suivantes :
   - À l'état le plus récent
   - Point dans le temps
   - À une sauvegarde de données spécifique
   - Pas de récupération

     Le type de restauration sélectionné est utilisé pour la récupération du système et de la base de données des locataires.

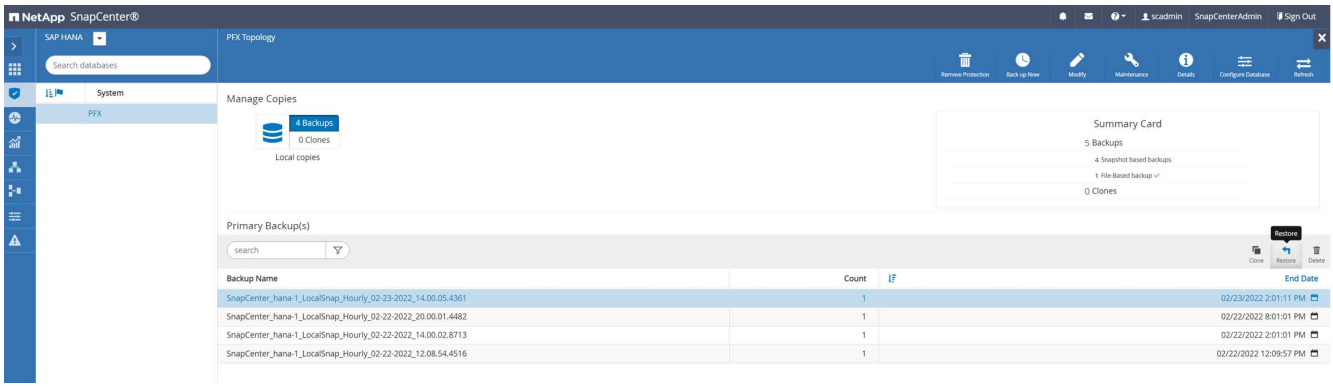
Ensuite, SnapCenter effectue les opérations suivantes :

1. Elle arrête la base de données HANA.
2. Elle restaure la base de données. Selon le type de restauration sélectionné, différentes opérations sont exécutées.
   - Si vous sélectionnez Restauration du volume, SnapCenter démonte le volume, restaure celui-ci à l'aide d'une mémoire SnapRestore basée sur les volumes sur la couche de stockage, puis monte le volume.
   - Si l'option Revert volume n'est pas sélectionnée, SnapCenter restaure tous les fichiers à l'aide d'opérations SnapRestore de fichiers uniques sur la couche de stockage.
3. Il restaure la base de données :
   a. En récupérant la base de données système
   b. récupération de la base de données des locataires
   c. Démarrage de la base de données HANA

Si aucune récupération est sélectionnée, SnapCenter se ferme et vous devez effectuer manuellement l'opération de restauration pour le système et la base de données de tenant.

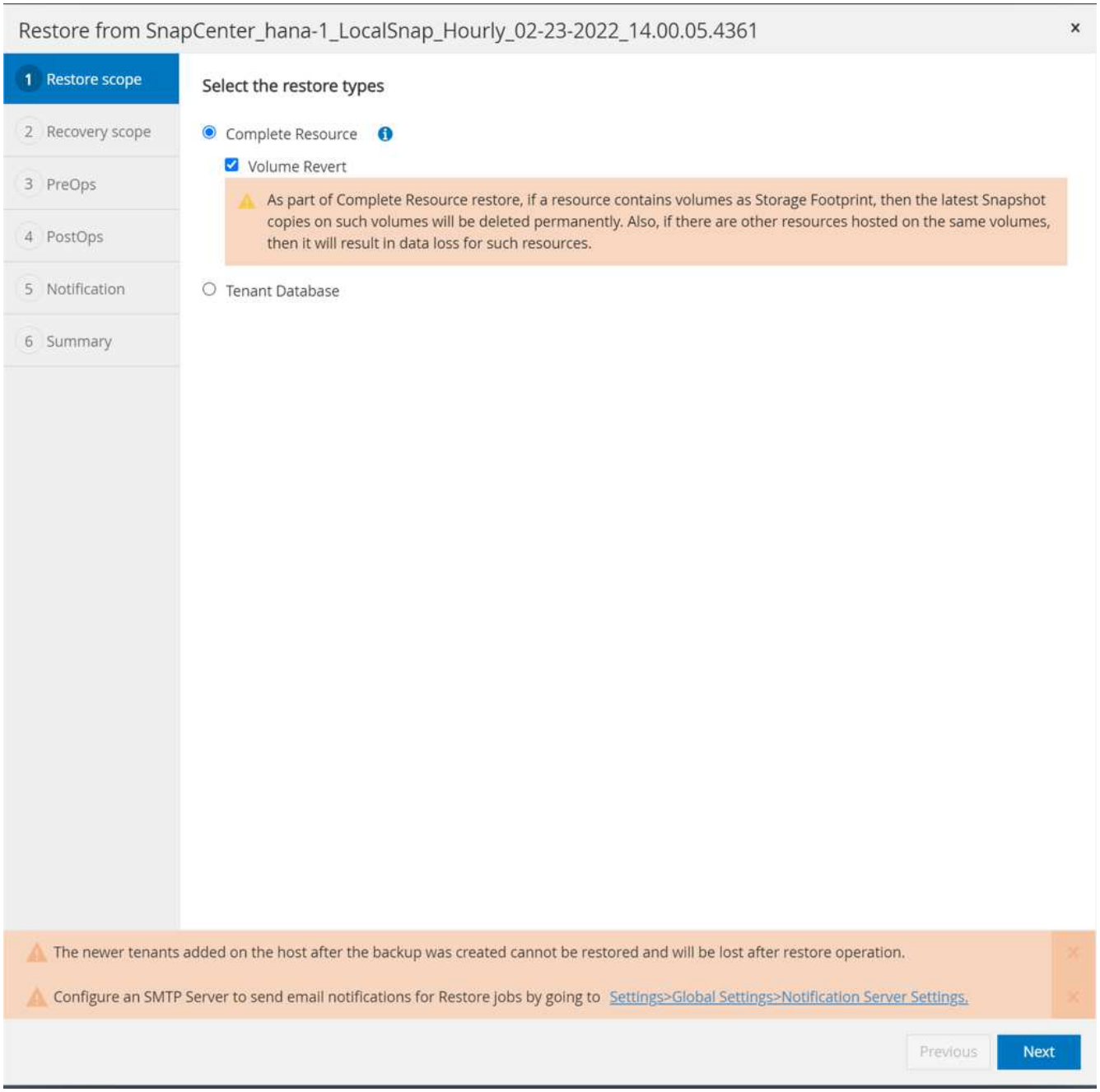
Pour effectuer une opération de restauration manuelle, procédez comme suit :

1. Sélectionnez une sauvegarde dans SnapCenter à utiliser pour l'opération de restauration.



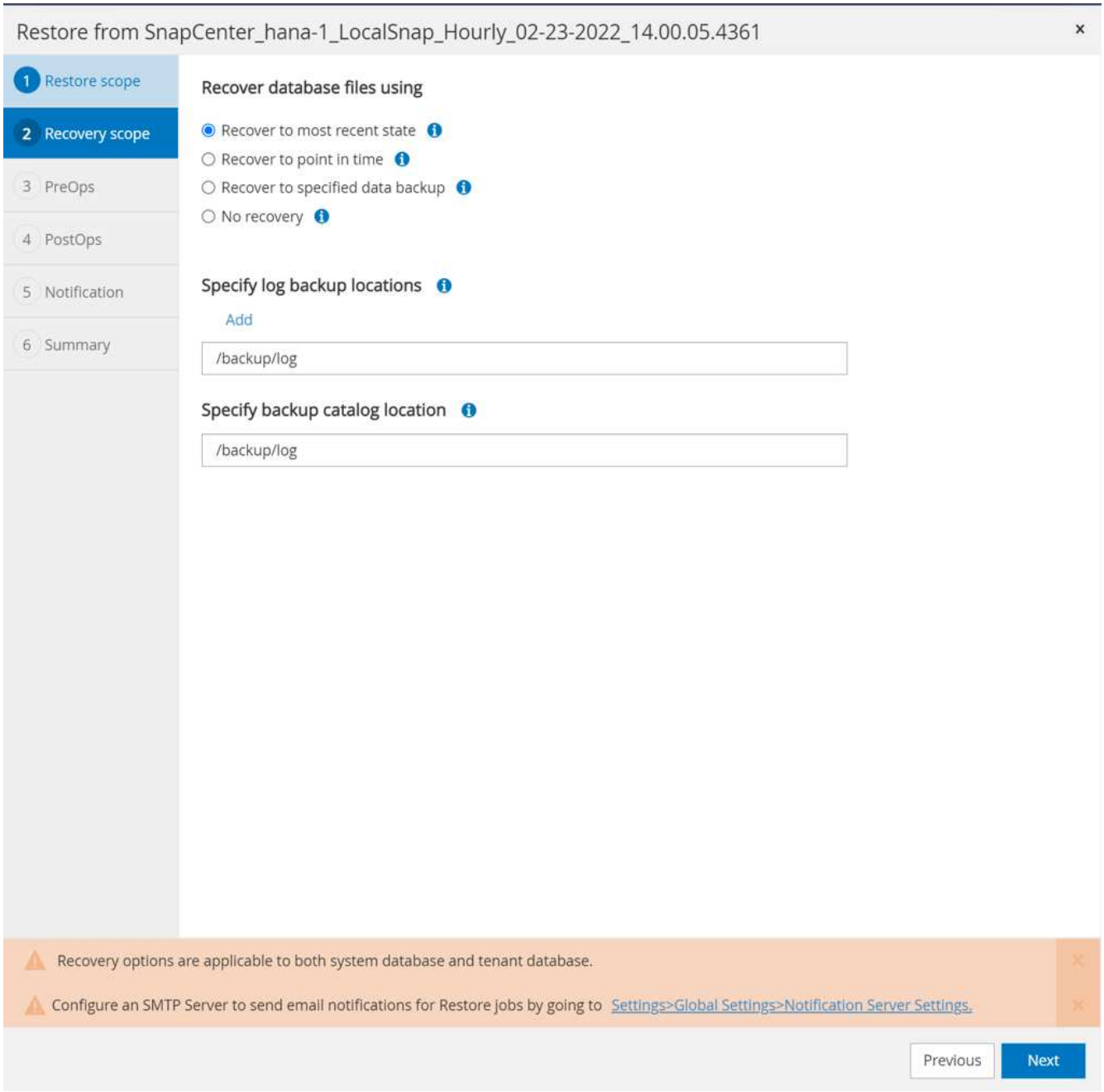
2. Sélectionnez la portée et le type de restauration.

   Pour les systèmes HANA MDC à un seul locataire, le scénario standard consiste à utiliser une ressource complète avec restauration du volume. Dans le cas d'un système MDC HANA avec plusieurs locataires, il se peut que vous ne souhaitiez restaurer qu'un seul locataire. Pour plus d'informations sur la restauration d'un seul locataire, reportez-vous à la section "Restauration et récupération (netapp.com)".

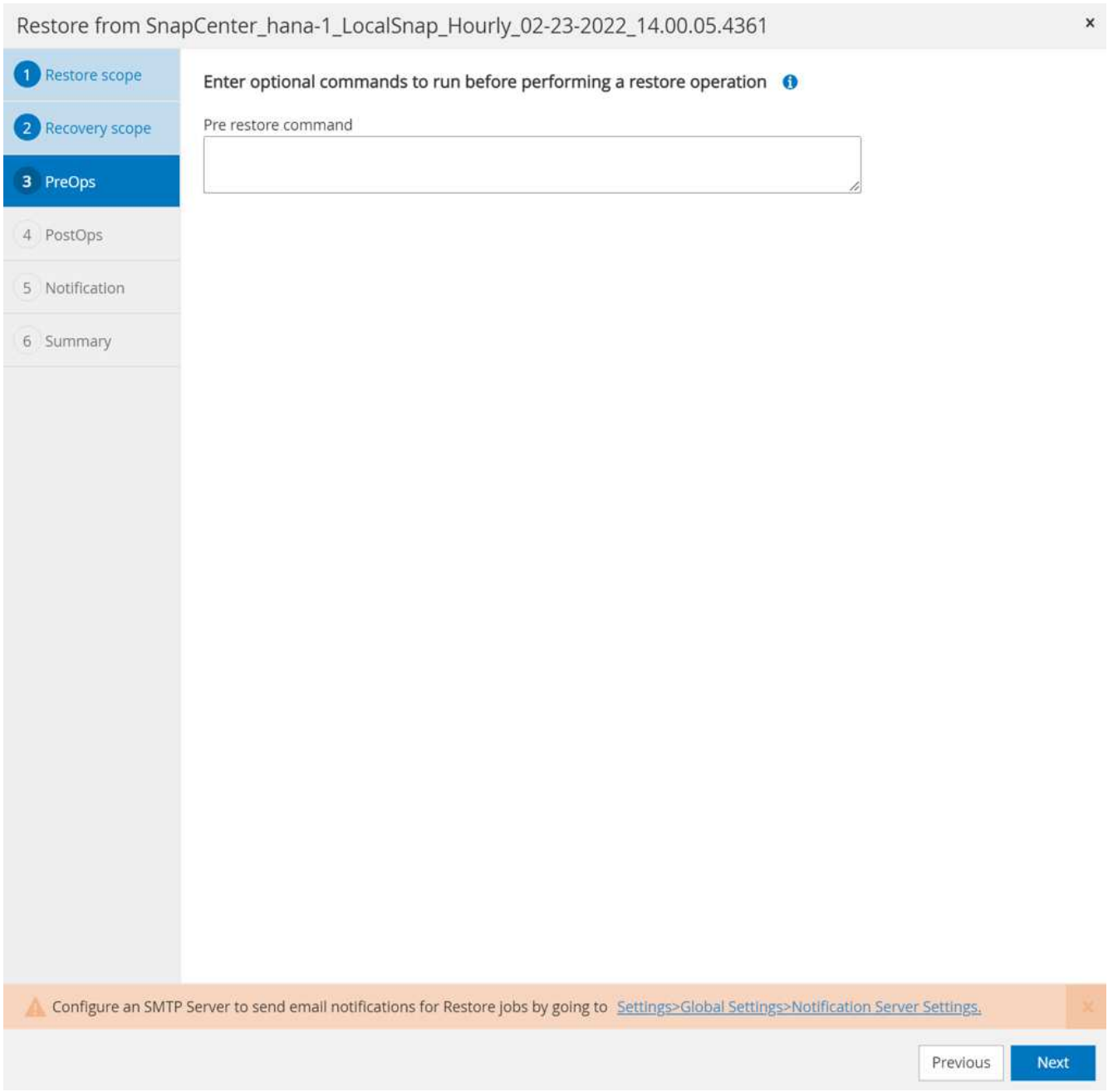


3. Sélectionnez étendue de la récupération et indiquez l'emplacement de sauvegarde du journal et du catalogue.

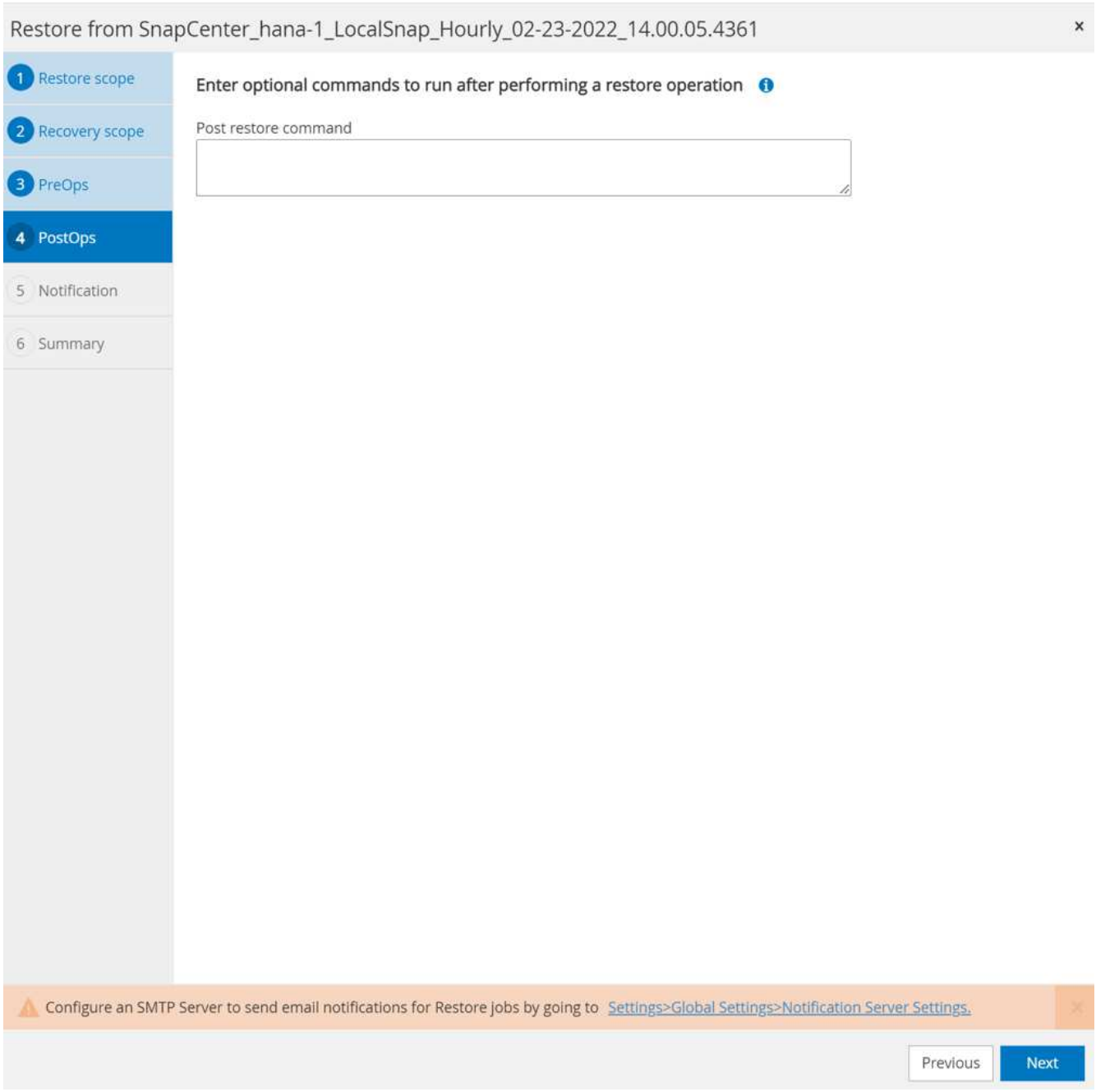
   SnapCenter utilise le chemin par défaut ou les chemins modifiés dans le fichier HANA global.ini pour remplir à l'avance les emplacements de sauvegarde du journal et du catalogue.



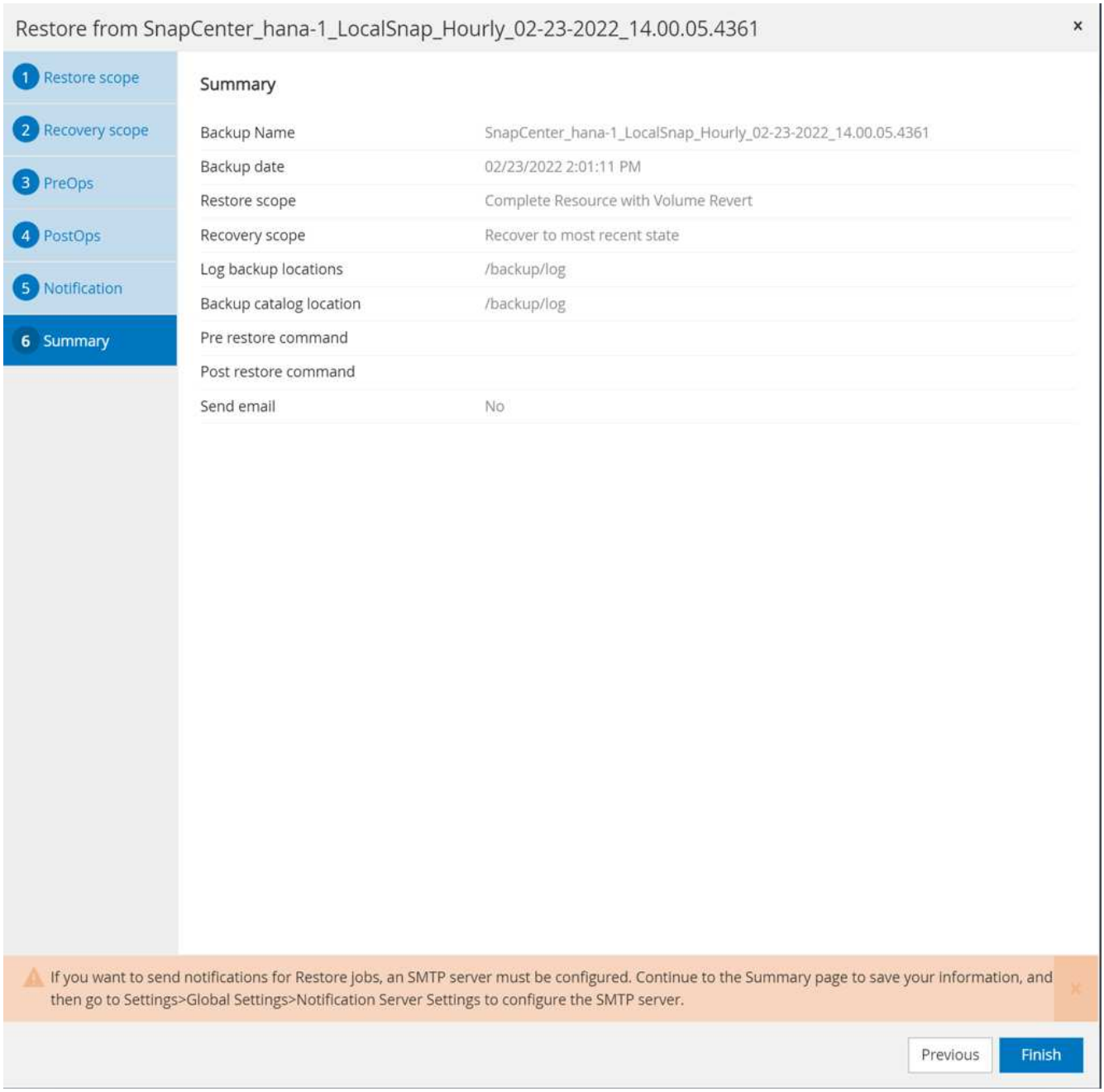
4. Entrez les commandes facultatives de pré-restauration.



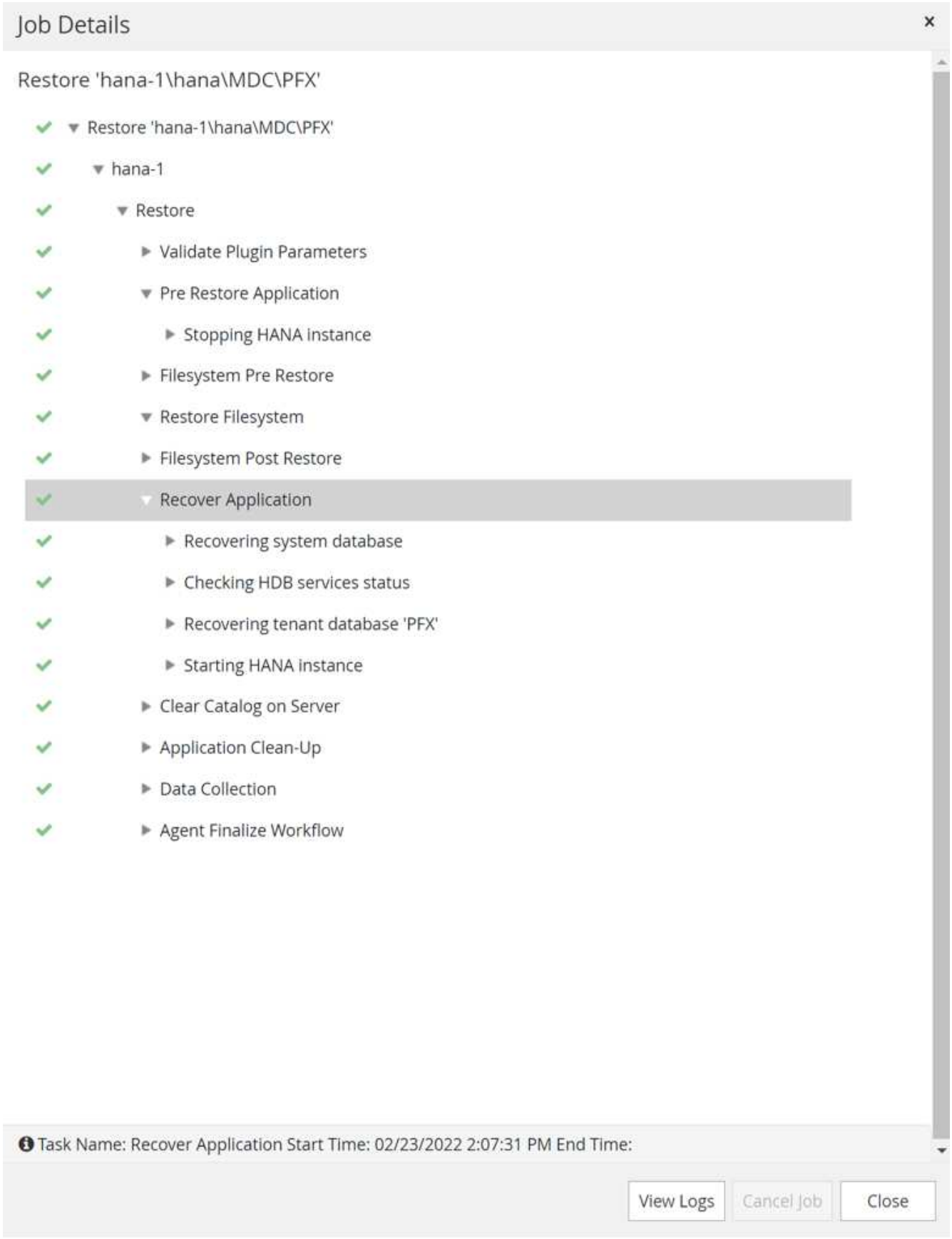
5. Entrez les commandes facultatives de post-restauration.



6. Pour lancer l'opération de restauration et de récupération, cliquez sur Terminer.



SnapCenter exécute l'opération de restauration et de restauration. Cet exemple montre les détails du travail de restauration et de récupération.

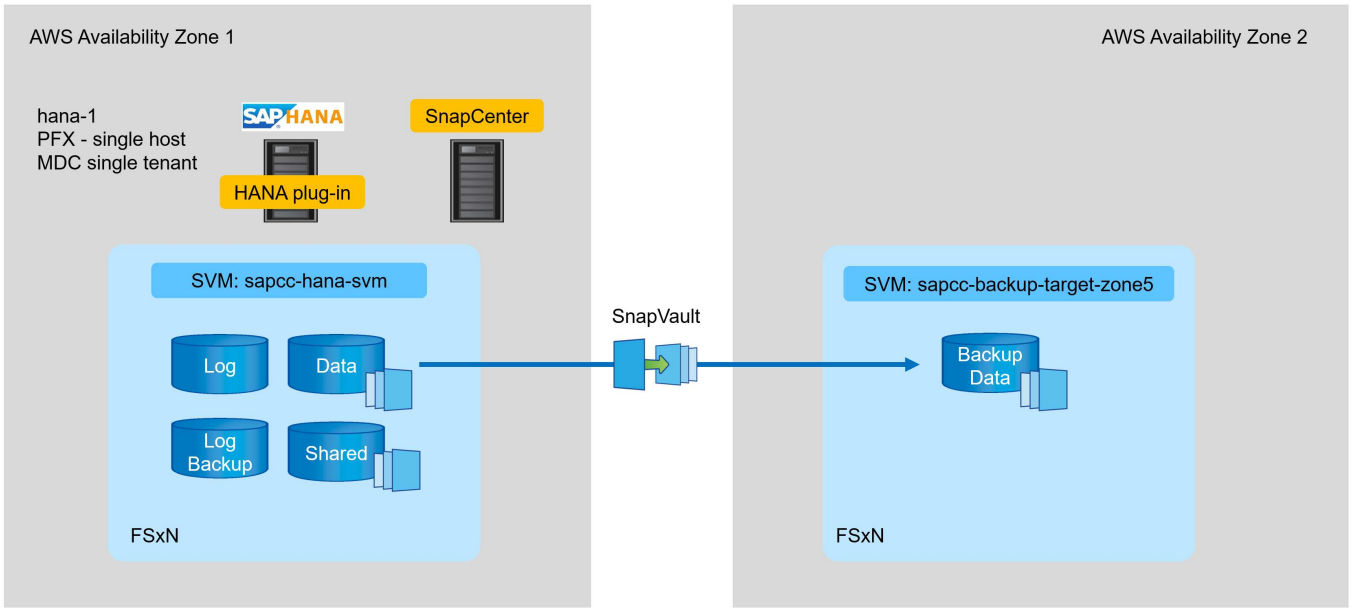

Job Details
Restore 'hana-1\hana\MDC\PFX'
Restore 'hana-1\hana\MDC\PFX'
hana-1
Restore
Validate Plugin Parameters
Pre Restore Application
Stopping HANA instance
Filesystem Pre Restore
Restore Filesystem
Filesystem Post Restore
Recover Application
Recovering system database
Checking HDB services status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

Réplication des sauvegardes avec SnapVault

Présentation - Sauvegarder la réplication avec SnapVault

Dans notre configuration de laboratoire, nous utilisons un deuxième système de fichiers FSX pour ONTAP dans une deuxième zone de disponibilité AWS pour présenter la réplication des sauvegardes pour le volume de données HANA.

Comme indiqué au chapitre "« Stratégie de protection des données »", La cible de réplication doit être une deuxième FSX pour le système de fichiers ONTAP dans une autre zone de disponibilité pour être protégée contre une défaillance de la FSX principale pour le système de fichiers ONTAP. Par ailleurs, le volume partagé HANA doit être répliqué sur la FSX secondaire pour le système de fichiers ONTAP.



Présentation des étapes de configuration

Il existe plusieurs étapes de configuration que vous devez exécuter sur la couche FSX pour ONTAP. Vous pouvez effectuer cette opération soit avec NetApp Cloud Manager, soit avec la ligne de commande FSX pour ONTAP.

1. Peer FSX pour les systèmes de fichiers ONTAP. FSX pour les systèmes de fichiers ONTAP doit être mis à niveau pour permettre la réplication entre eux.
2. SVM homologues. Les SVM doivent être associés de manière à permettre la réplication entre les deux.
3. Créer un volume cible. Création d'un volume au niveau du SVM cible avec un type de volume `DP`. Type `DP` est requis pour être utilisé comme volume cible de réplication.
4. Créer une règle SnapMirror Cette option permet de créer une règle pour la réplication avec type `vault`.
    a. Ajouter une règle à la stratégie. La règle contient l'étiquette SnapMirror et la conservation des sauvegardes sur le site secondaire. Vous devez configurer la même étiquette SnapMirror plus loin dans la règle SnapCenter de sorte que SnapCenter crée des sauvegardes Snapshot sur le volume source contenant cette étiquette.
5. Créer une relation SnapMirror Définit la relation de réplication entre les volumes source et cible et attache une stratégie.

6. Initialiser SnapMirror Cette opération démarre la réplication initiale dans laquelle toutes les données source sont transférées vers le volume cible.

Une fois la configuration de réplication de volume terminée, vous devez configurer la réplication de sauvegarde dans SnapCenter comme suit :

1. Ajouter le SVM cible à SnapCenter
2. Créez une nouvelle règle SnapCenter pour la sauvegarde Snapshot et la réplication SnapVault.
3. Ajoutez la règle à la protection des ressources HANA.
4. Vous pouvez désormais exécuter des sauvegardes avec la nouvelle stratégie.

Les chapitres suivants décrivent chaque étape plus en détail.

Configurer les relations de réplication sur FSX pour les systèmes de fichiers ONTAP

Pour plus d'informations sur les options de configuration de SnapMirror, consultez la documentation ONTAP à l'adresse "Workflow de réplication SnapMirror (netapp.com)".

- FSX source pour système de fichiers ONTAP : `FsxId00fa9e3c784b6abbb`
- SVM source : `sapcc-hana-svm`
- Cible FSX pour système de fichiers ONTAP : `FsxId05f7f00af49dc7a3e`
- SVM cible : `sapcc-backup-target-zone5`

Peer FSX pour les systèmes de fichiers ONTAP

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

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

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

`peer-addrs` Les adresses IP de cluster du cluster cible sont-elles des.

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

SVM homologues

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

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

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

Créer un volume cible

Vous devez créer le volume cible avec le type `DP` pour le marquer comme cible de réplication.

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

Créer une règle SnapMirror

La règle SnapMirror et la règle ajoutée définissent la rétention et l'étiquette SnapMirror pour identifier les snapshots à répliquer. Lorsque vous créez la stratégie SnapCenter ultérieurement, vous devez utiliser le même libellé.

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

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

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

Créer une relation SnapMirror

Maintenant la relation entre les volumes source et cible est définie, ainsi que le type XDP et la règle que nous avons créée précédemment.

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

Initialiser SnapMirror

Avec cette commande, la réplication initiale démarre. Il s'agit d'un transfert complet de toutes les données depuis le volume source vers le volume cible.

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

Vous pouvez vérifier l'état de la réplication avec `snapmirror show` commande.

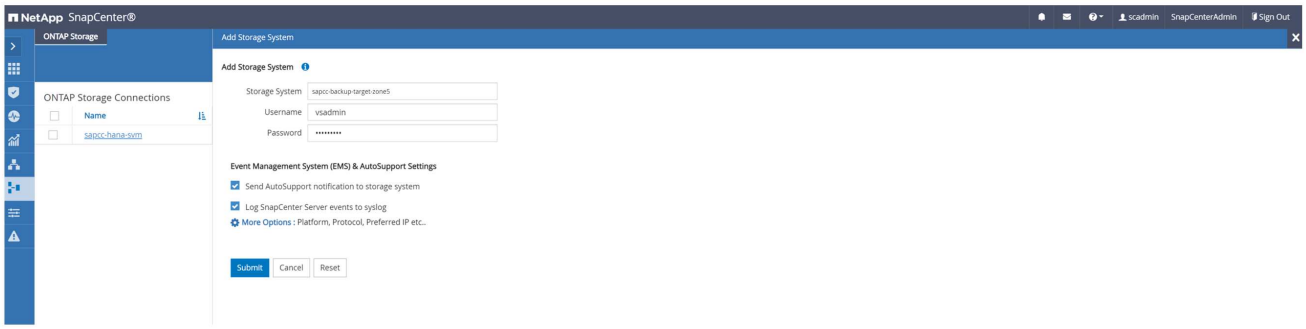
```
FsxId05f7f00af49dc7a3e::> snapmirror show

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

```
FsxId05f7f00af49dc7a3e::> snapmirror show

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

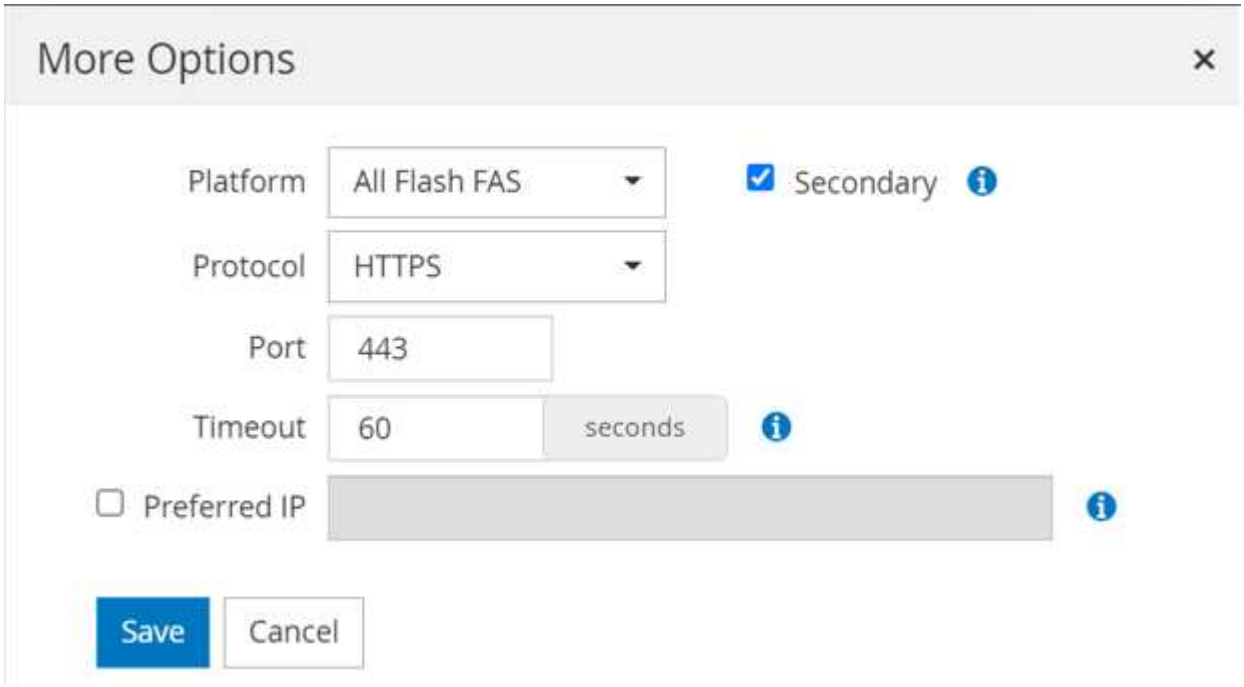
Ajout d'un SVM de sauvegarde à SnapCenter

Pour ajouter un SVM de sauvegarde à SnapCenter, effectuez la procédure suivante :

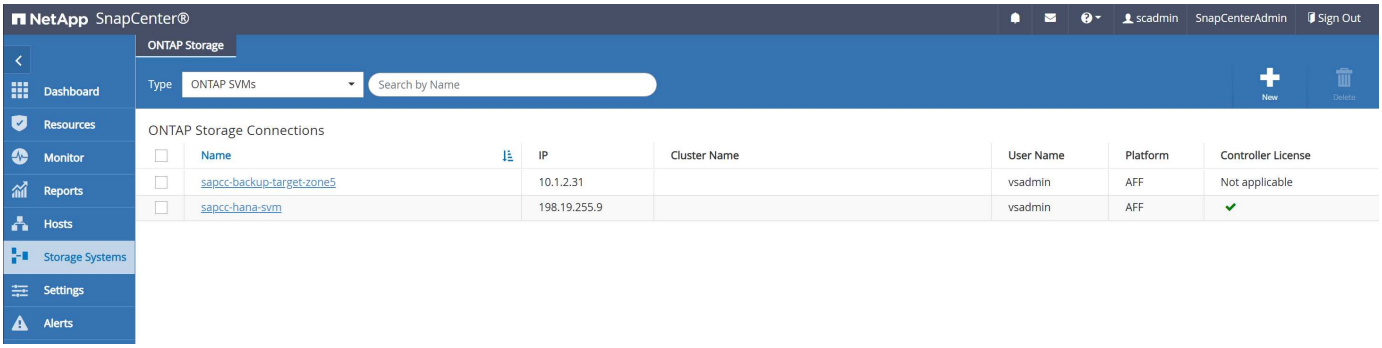
1. Configurer le SVM où le volume cible SnapVault est situé dans SnapCenter



2. Dans la fenêtre plus d'options, sélectionnez All Flash FAS comme plate-forme et sélectionnez secondaire.



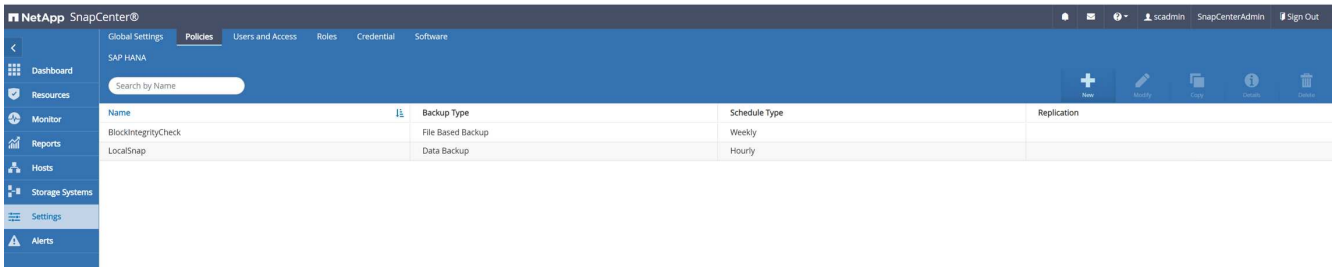
La SVM est désormais disponible dans SnapCenter.



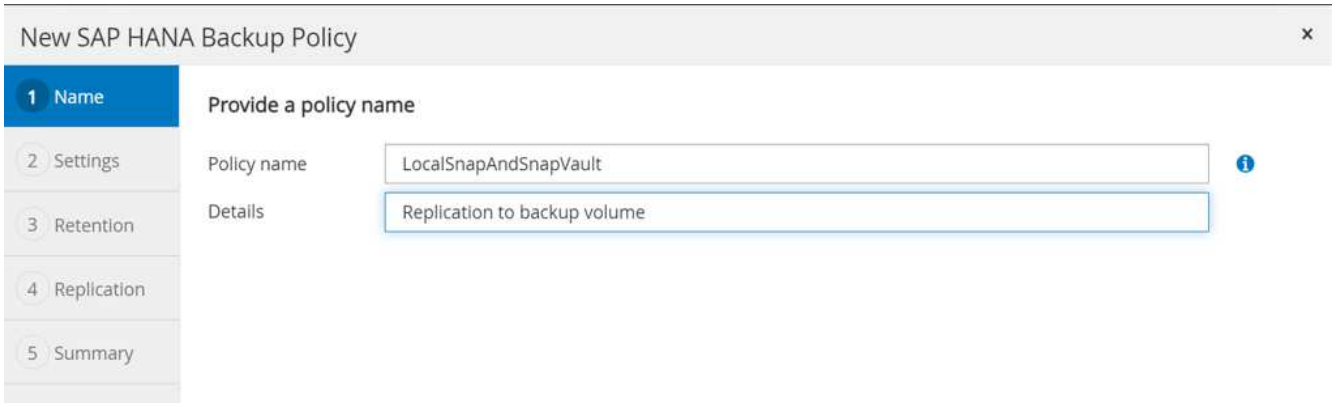
Créez une nouvelle règle SnapCenter pour la réplication des sauvegardes

Vous devez configurer une stratégie pour la réplication de sauvegarde comme suit :

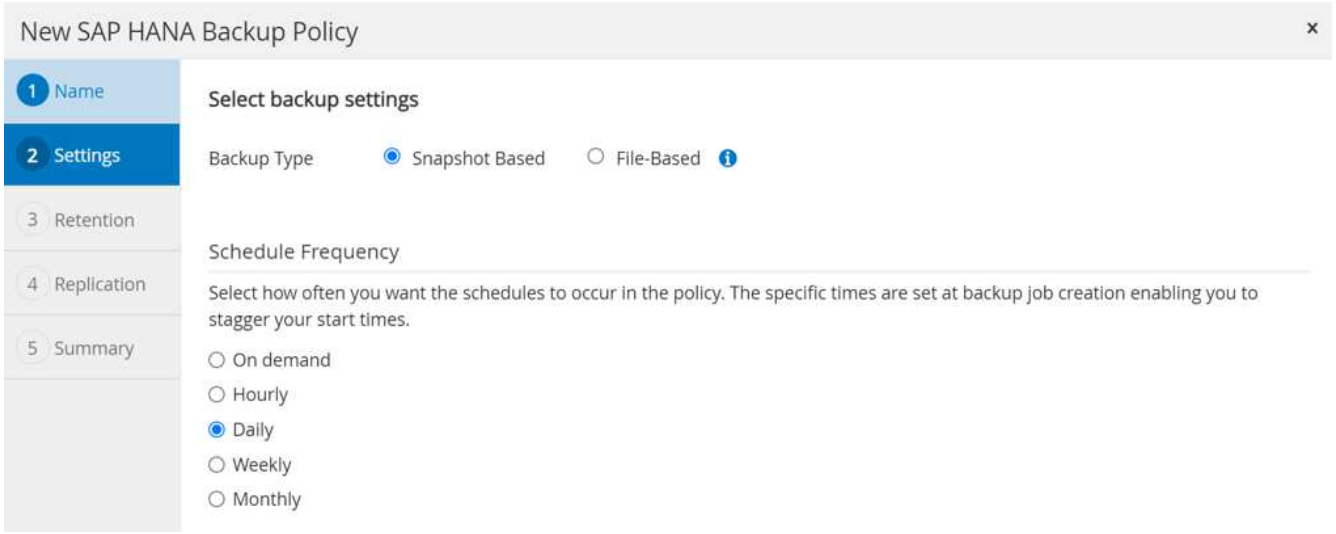
1. Indiquez un nom pour la règle.



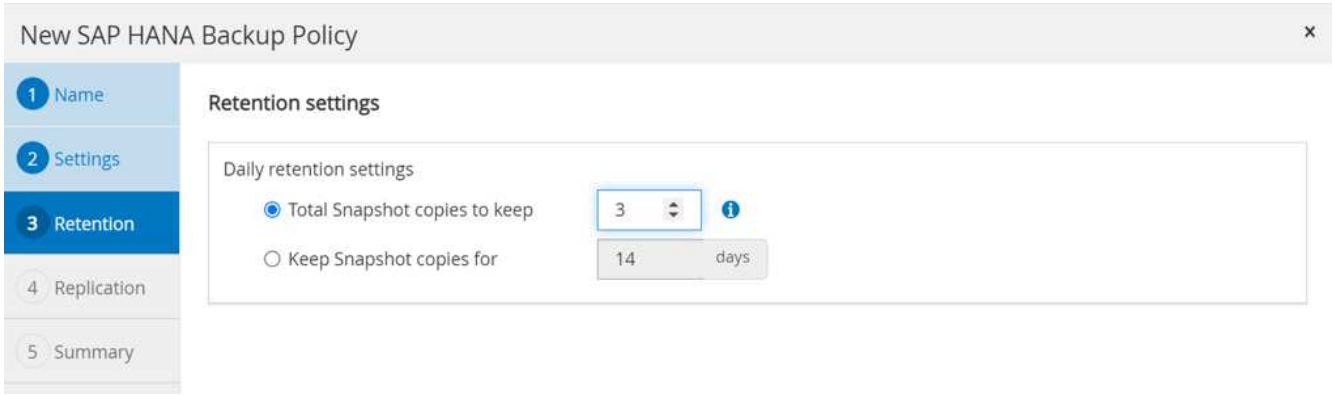
2. Sélectionnez sauvegarde Snapshot et fréquence de planification. Chaque jour est généralement utilisé pour la réplication de sauvegarde.



3. Sélectionnez la conservation des sauvegardes Snapshot.

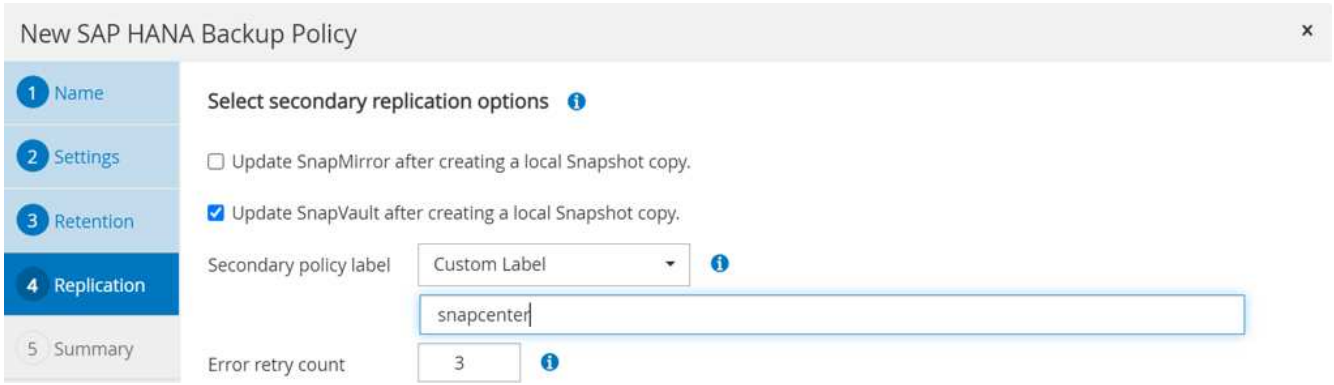


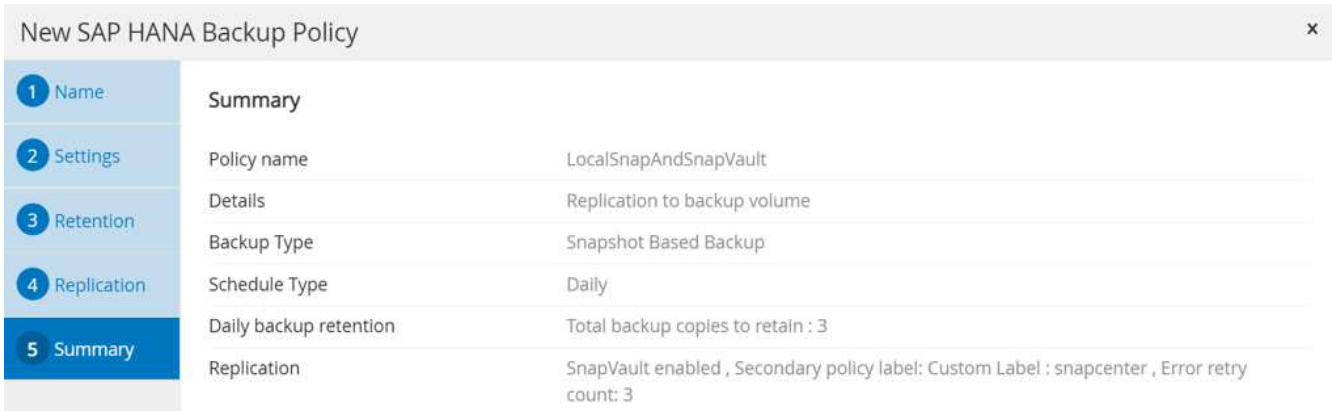
Il s'agit de la conservation des sauvegardes Snapshot quotidiennes effectuées sur le stockage primaire. La conservation pour les sauvegardes secondaires sur la cible SnapVault a déjà été configurée au préalable à l'aide de la commande add rule au niveau de ONTAP. Reportez-vous à la section "Configuration des relations de réplication sur FSX pour les systèmes de fichiers ONTAP" (xref).



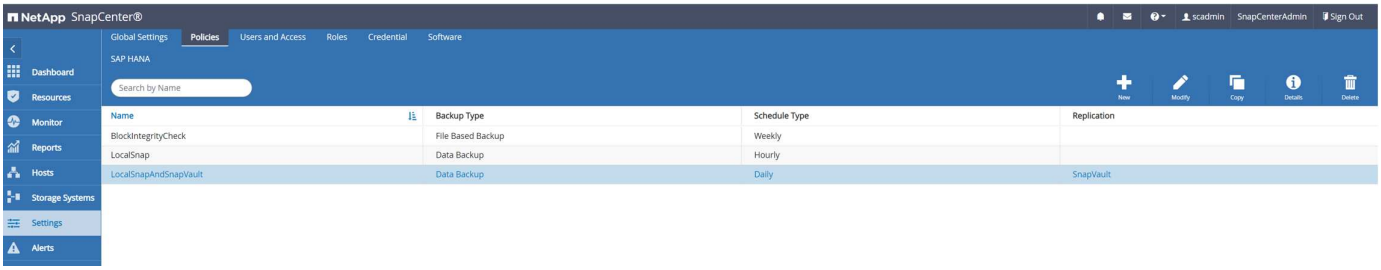
4. Sélectionnez le champ SnapVault de mise à jour et fournissez un libellé personnalisé.

   Cette étiquette doit correspondre à l'étiquette SnapMirror fournie dans le `add rule` Commande au niveau de ONTAP.



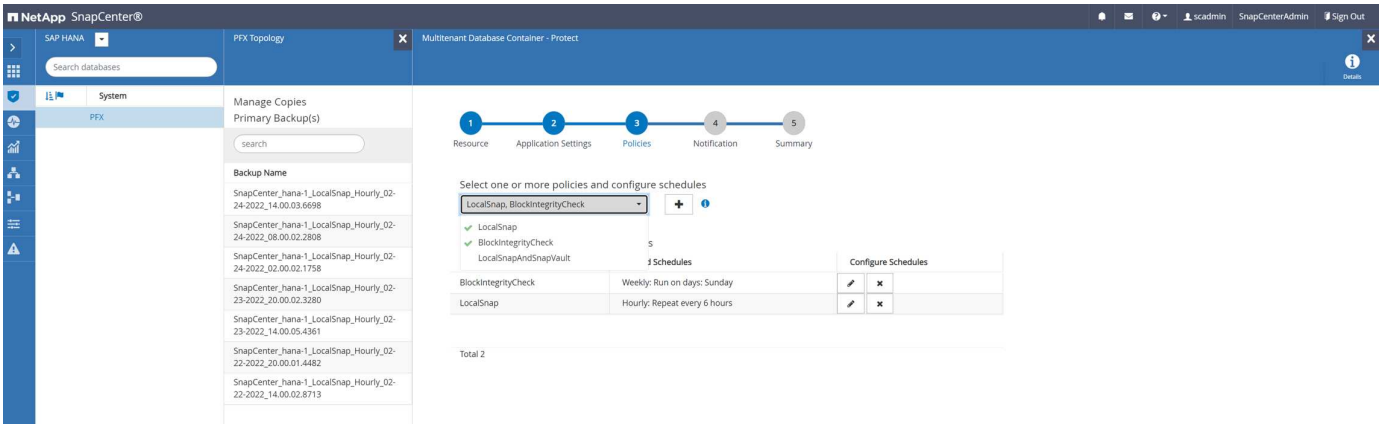


La nouvelle règle SnapCenter est maintenant configurée.

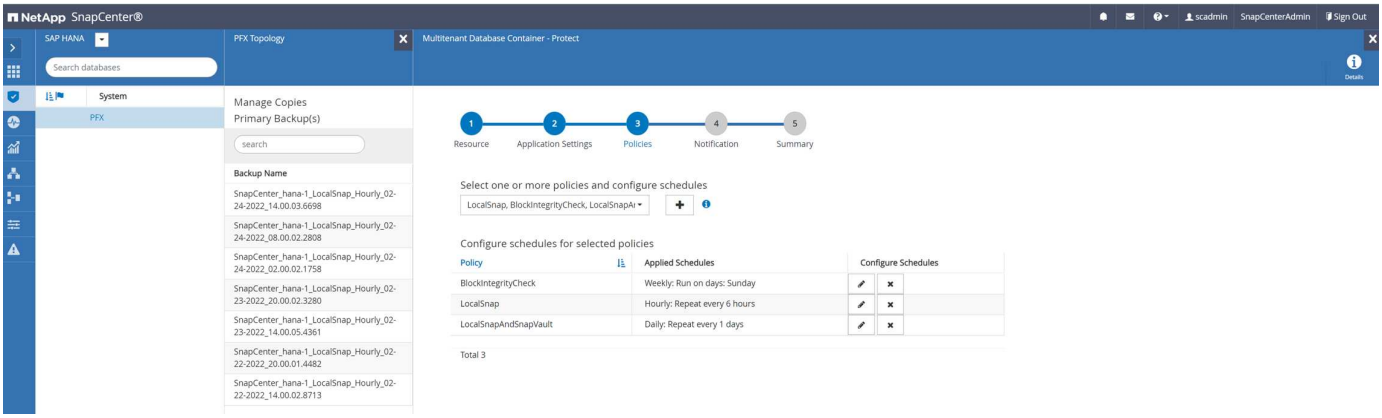


Ajouter une règle à la protection des ressources

Vous devez ajouter la nouvelle règle à la configuration de protection des ressources HANA, comme illustré dans la figure suivante.



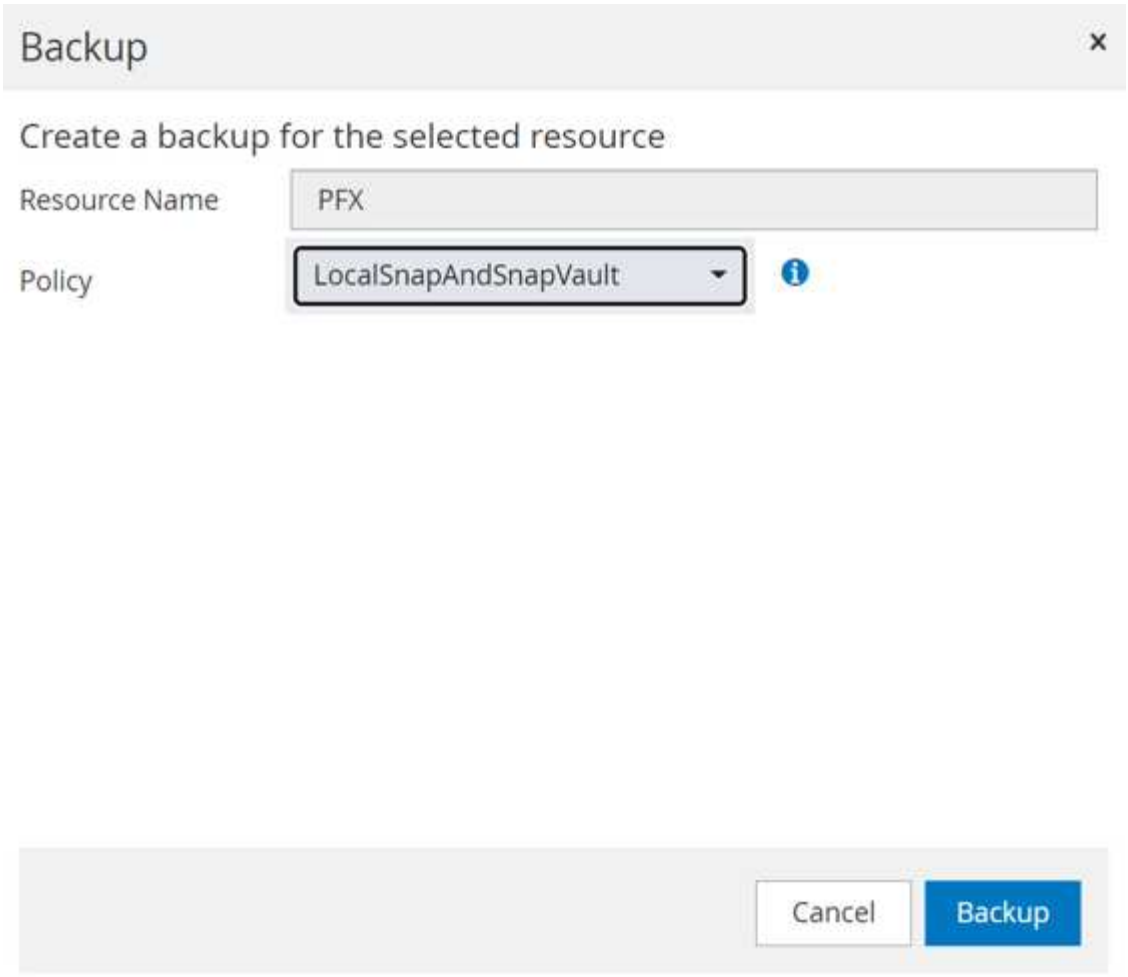
Un horaire quotidien est défini dans notre configuration.



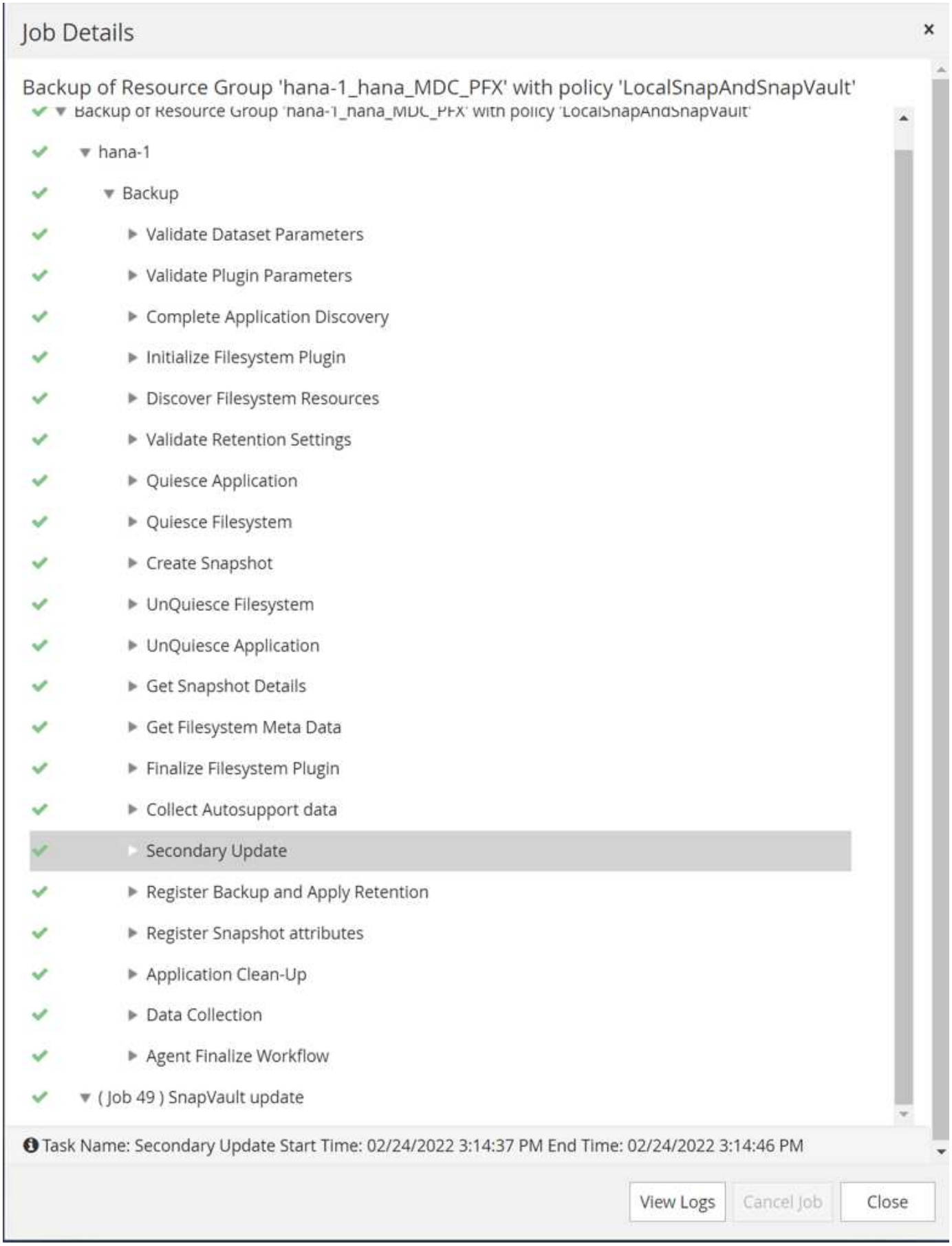
Créer une sauvegarde avec la réplication

La création d'une sauvegarde est effectuée de la même manière que pour une copie Snapshot locale.

Pour créer une sauvegarde avec réplication, sélectionnez la stratégie qui inclut la réplication de sauvegarde et cliquez sur Sauvegarder.



Dans le journal des tâches SnapCenter, vous pouvez voir l'étape mise à jour secondaire, qui lance une opération de mise à jour SnapVault. Réplication des blocs modifiés depuis le volume source vers le volume cible.



Sur le système de fichiers FSX pour ONTAP, un snapshot du volume source est créé à l'aide de l'étiquette

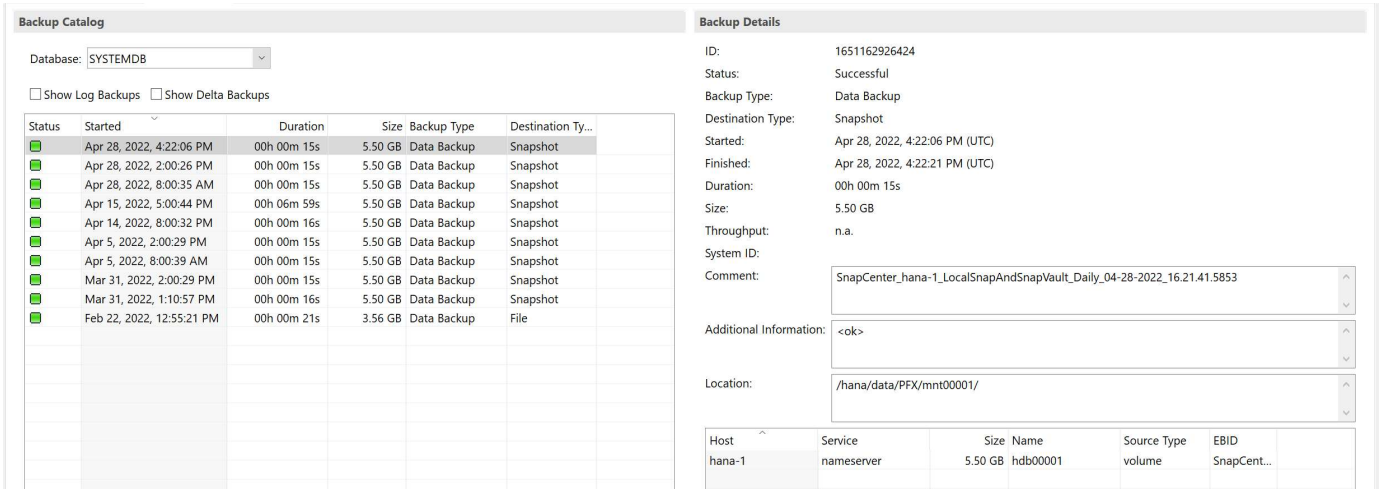
SnapMirror, `snapcenter`, Tel qu'il est configuré dans la politique SnapCenter.

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

snapcenter
8 entries were displayed.
```

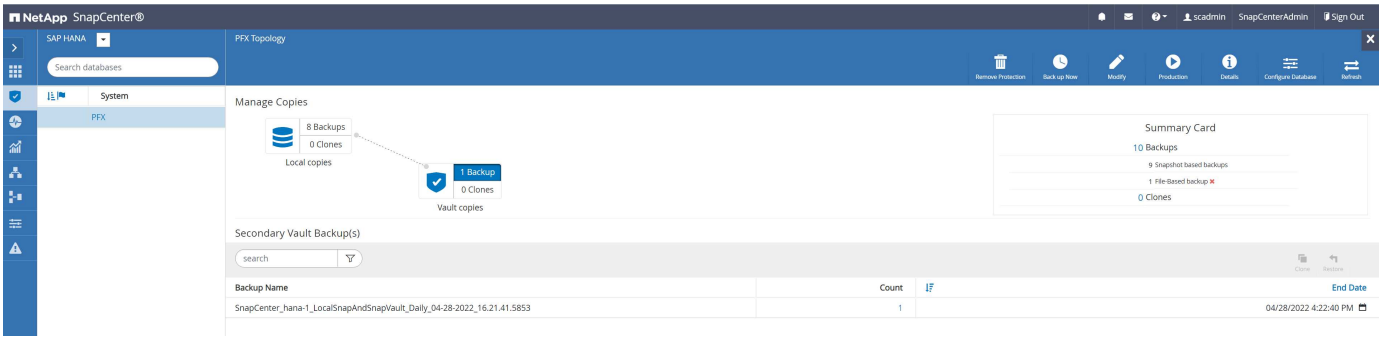
Au niveau du volume cible, une copie Snapshot portant le même nom est créée.

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

La nouvelle sauvegarde Snapshot est également incluse dans le catalogue de sauvegardes HANA.



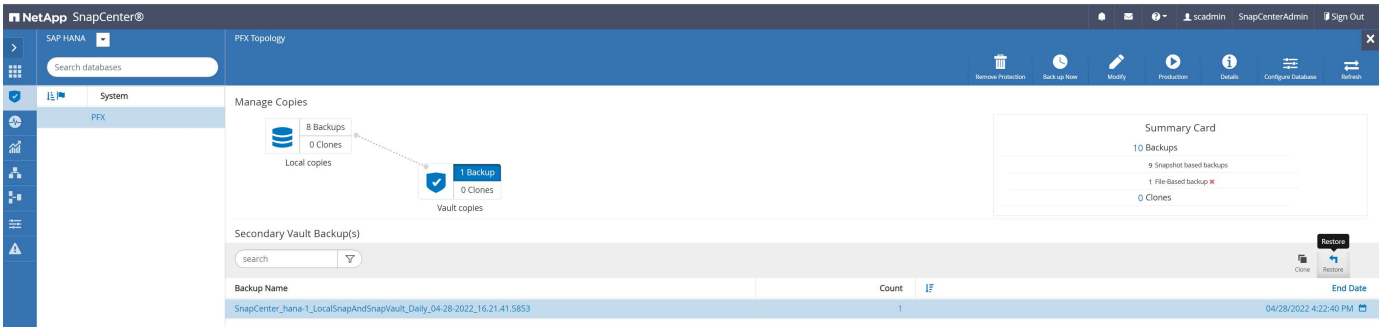
Dans SnapCenter, vous pouvez lister les sauvegardes répliquées en cliquant sur les copies du coffre-fort dans la vue topologique.



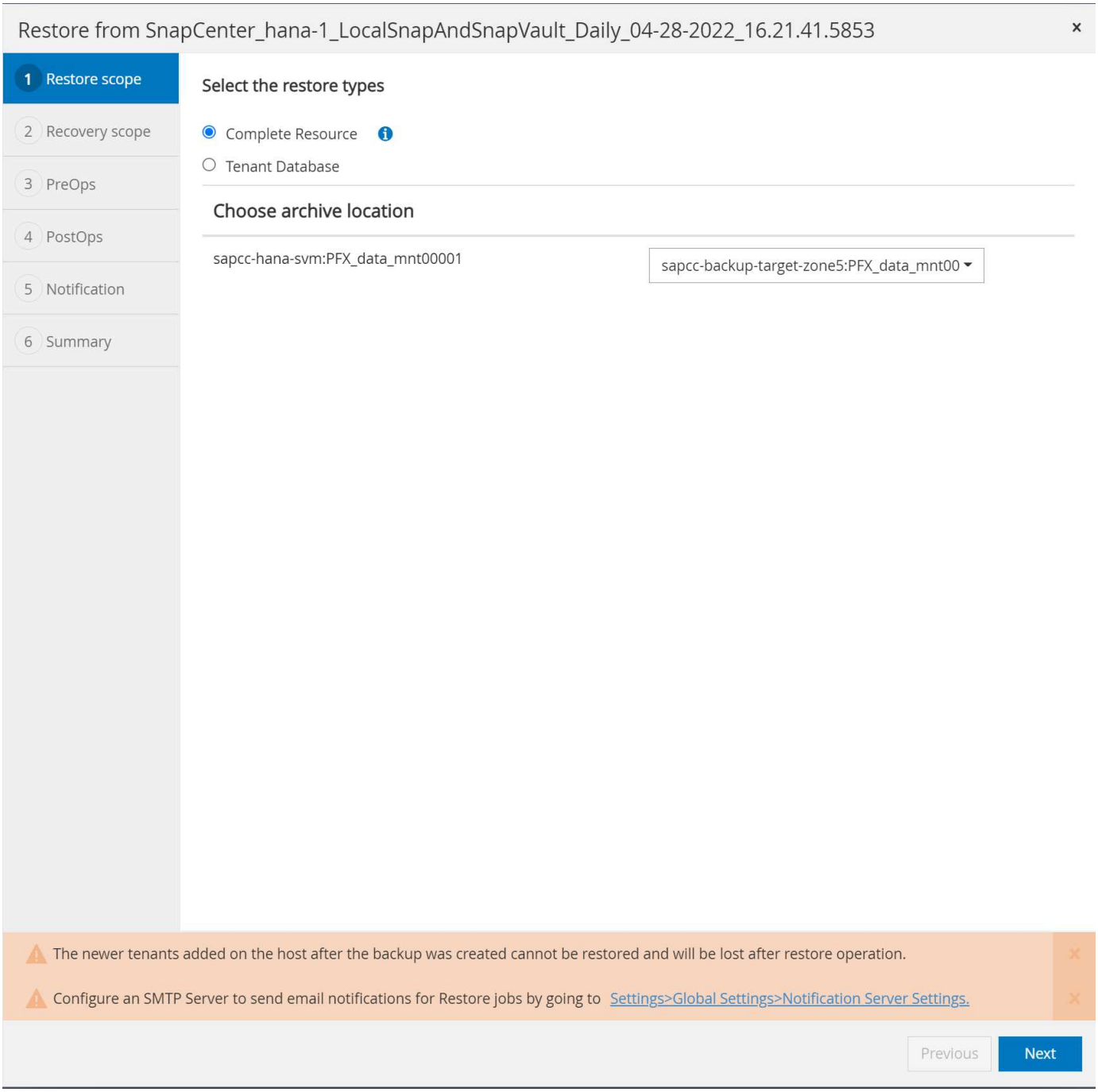
Restaurer et restaurer des données à partir du stockage secondaire

Pour restaurer et récupérer à partir d'un stockage secondaire, procédez comme suit :

Pour récupérer la liste de toutes les sauvegardes du stockage secondaire, dans la vue topologie SnapCenter, cliquez sur copies du coffre-fort, sélectionnez une sauvegarde et cliquez sur Restaurer.



La boîte de dialogue de restauration affiche les emplacements secondaires.



Les autres étapes de restauration et de restauration sont identiques à celles précédemment décrites pour une sauvegarde Snapshot sur le stockage primaire.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Guide de l'utilisateur FSX pour NetApp ONTAP — Qu'est-ce qu'Amazon FSX pour NetApp ONTAP ?

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

- Page des ressources SnapCenter

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

- Documentation du logiciel SnapCenter

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

- Tr-4667 : automatisation des opérations de copie système et de clonage SAP HANA avec SnapCenter

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

- Tr-4719 : réplication système SAP HANA : sauvegarde et restauration avec SnapCenter

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

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Mai 2022	Version initiale.

Sauvegarde et restauration SAP HANA avec SnapCenter

Tr-4614 : sauvegarde et restauration SAP HANA avec SnapCenter

Nils Bauer, NetApp

Les entreprises ont besoin aujourd'hui d'une disponibilité continue et sans interruption pour leurs applications SAP. Elles espèrent obtenir des niveaux de performance prévisibles dans un contexte où les volumes de données ne cessent d'augmenter et nécessitent des tâches de maintenance de routine comme les sauvegardes système. Le processus de sauvegarde des bases de données SAP est une tâche critique qui peut affecter les performances du système SAP de production.

Les fenêtres de sauvegarde diminuent, alors que le volume des données à sauvegarder augmente. Par conséquent, il est difficile de trouver une heure où les sauvegardes peuvent être effectuées avec un impact minimal sur les processus de l'entreprise. Le temps nécessaire à la restauration et à la restauration des systèmes SAP est un problème, car les temps d'indisponibilité des systèmes de production et hors production SAP doivent être réduits au minimum afin de limiter les pertes de données et les coûts pour l'entreprise.

Les points suivants résument les défis liés à la sauvegarde et la restauration SAP :

- **Effets sur les performances des systèmes SAP de production.** en général, les sauvegardes traditionnelles basées sur la copie créent une importante augmentation des performances des systèmes SAP de production en raison des lourdes charges placées sur le serveur de base de données, le système de stockage et le réseau de stockage.
- **Fenêtres de sauvegarde réduites.** les sauvegardes conventionnelles ne peuvent être effectuées que lorsque peu d'activités de dialogue ou de lots sont en cours sur le système SAP. La planification des sauvegardes devient plus difficile lorsque les systèmes SAP sont utilisés 24 h/24.
- **Croissance rapide des données.** la croissance rapide des données et la réduction des fenêtres de sauvegarde exigent des investissements continus en infrastructure de sauvegarde. En d'autres termes, vous devez vous procurer plus de lecteurs de bandes, plus d'espace disque de sauvegarde supplémentaire et des réseaux de sauvegarde plus rapides. Vous devez également couvrir les dépenses

courantes liées au stockage et à la gestion de ces actifs de bandes. Les sauvegardes incrémentielles ou différentielles peuvent résoudre ces problèmes, mais cette configuration entraîne une procédure de restauration très lente, fastidieuse et complexe qui est plus difficile à vérifier. Ces systèmes augmentent généralement le temps requis pour atteindre des objectifs de durée de restauration (RTO) et de point de récupération (RPO), de manière non acceptable pour l'activité.

- * Augmentation du coût des temps d'arrêt.* les temps d'arrêt imprévus d'un système SAP affectent généralement les finances de l'entreprise. Les temps d'indisponibilité non planifiés sont, en grande partie, consommés par la restauration du système SAP. Par conséquent, le RTO souhaité dicte la conception de l'architecture de sauvegarde et de restauration.
- **Temps de sauvegarde et de restauration pour les projets de mise à niveau SAP.** le plan de projet pour une mise à niveau SAP comprend au moins trois sauvegardes de la base de données SAP. Ces sauvegardes réduisent considérablement le temps disponible pour le processus de mise à niveau. La décision de procéder est généralement basée sur le temps nécessaire à la restauration et à la récupération de la base de données à partir de la sauvegarde précédemment créée. Plutôt que de restaurer un système à son état précédent, une restauration rapide offre plus de temps pour résoudre les problèmes susceptibles de se produire lors d'une mise à niveau.

La solution NetApp

La technologie Snapshot de NetApp peut être utilisée pour créer des sauvegardes de bases de données en quelques minutes. Le temps nécessaire à la création d'une copie Snapshot ne dépend pas de la taille de la base de données, car cette copie ne déplace aucun bloc de données sur la plateforme de stockage. De plus, l'utilisation de la technologie Snapshot de NetApp n'a pas d'impact sur la performance de votre système SAP en direct, car cette technologie n'effectue aucun déplacement ni aucune copie de blocs de données lors de la création de la copie Snapshot ou lors de la modification des données du système de fichier actif. Ainsi, la création de copies Snapshot peut être planifiée sans tenir compte des périodes de pointe de dialogue ou d'activité de lots. Les clients SAP et NetApp programraient généralement plusieurs sauvegardes Snapshot en ligne pendant la journée, par exemple, toutes les quatre heures sont courantes. Ces sauvegardes Snapshot sont généralement conservées pendant trois à cinq jours sur le système de stockage principal, avant d'être supprimées.

Les copies Snapshot offrent également des avantages clés pour les opérations de restauration et de reprise. Le logiciel de restauration des données NetApp SnapRestore permet de restaurer l'intégralité d'une base de données ou, alternativement, une partie d'une base de données à un point dans le temps, en fonction des copies Snapshot disponibles. Ce processus ne dure que quelques minutes, quelle que soit la taille de la base de données. Comme plusieurs sauvegardes Snapshot en ligne sont créées pendant la journée, le temps nécessaire au processus de restauration est considérablement réduit par rapport à une approche de sauvegarde traditionnelle. Étant donné qu'une restauration peut être effectuée avec une copie Snapshot datant de quelques heures seulement (au lieu de 24 heures), moins de journaux de transaction doivent être appliqués. Par conséquent, le RTO est réduit à quelques minutes, au lieu de plusieurs heures requises pour les sauvegardes sur bande conventionnelles à un cycle unique.

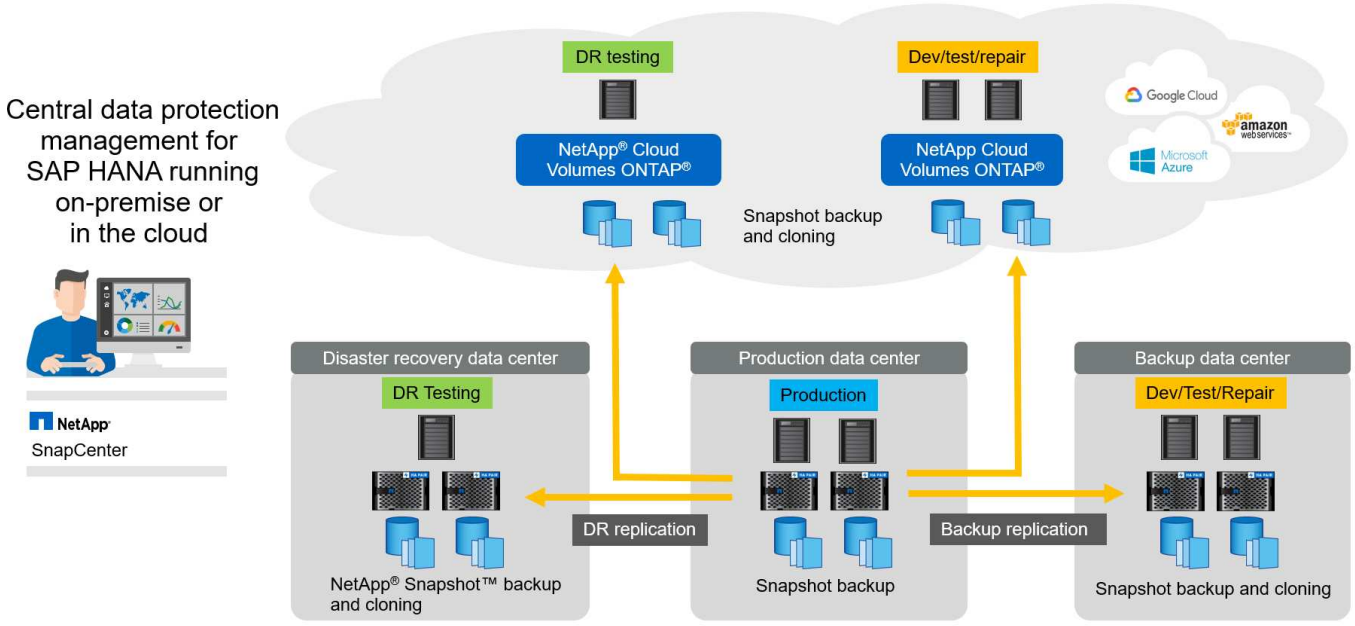
Les sauvegardes de copie Snapshot sont stockées sur le même système de disque que les données en ligne actives. Par conséquent, NetApp recommande d'utiliser les sauvegardes de copies Snapshot comme supplément plutôt que comme remplacement des sauvegardes sur un emplacement secondaire. La plupart des actions de restauration et de restauration sont gérées à l'aide d'SnapRestore sur le système de stockage primaire. Les restaurations depuis un emplacement secondaire sont uniquement nécessaires si le système de stockage primaire contenant les copies Snapshot est endommagé. L'emplacement secondaire peut également être utilisé si la restauration d'une sauvegarde qui n'est plus disponible à partir d'une copie Snapshot : sauvegarde de fin de mois, par exemple.

Une sauvegarde vers un emplacement secondaire repose sur des copies Snapshot créées sur le système de stockage primaire. Par conséquent, les données sont lues directement depuis le système de stockage primaire sans générer de charge sur le serveur de base de données SAP. Le stockage primaire communique

directement avec le stockage secondaire et envoie les données de sauvegarde vers le destination via une sauvegarde disque à disque SnapVault NetApp.

SnapVault offre des avantages significatifs par rapport aux sauvegardes traditionnelles. Après le transfert initial des données, dans lequel toutes les données ont été transférées de la source vers la destination, toutes les sauvegardes ultérieures copient uniquement les blocs modifiés vers le stockage secondaire. Par conséquent, la charge sur le système de stockage primaire et le temps nécessaire à une sauvegarde complète sont considérablement réduits. Étant donné que SnapVault stocke uniquement les blocs modifiés au niveau de la destination, une sauvegarde complète de base de données nécessite moins d'espace disque.

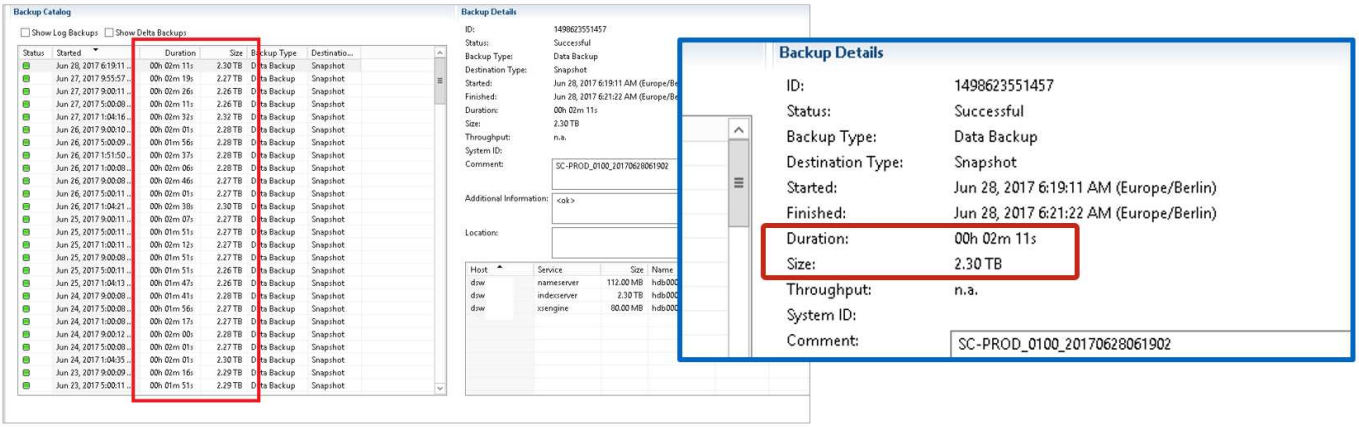
La solution peut également être étendue en toute transparence à un modèle d'exploitation de cloud hybride. La réplication des données à des fins de reprise après incident ou de sauvegarde hors site peut être effectuée depuis les systèmes NetApp ONTAP sur site vers les instances Cloud Volumes ONTAP exécutées dans le cloud. Vous pouvez utiliser SnapCenter comme outil central pour gérer la protection et la réplication des données, indépendamment si le système SAP HANA s'exécute sur site ou dans le cloud. La figure suivante présente une présentation de la solution de sauvegarde.



Exécution des sauvegardes Snapshot

La capture d'écran suivante montre l'atelier HANA d'un client exécutant SAP HANA sur un système de stockage NetApp. Le client utilise des copies Snapshot pour sauvegarder la base de données HANA. L'image montre que la base de données HANA (environ 2,3 To de taille) est sauvegardée en 2 minutes et 11 secondes à l'aide de la technologie de sauvegarde Snapshot.

La majeure partie du temps d'exécution du workflow de sauvegarde est le temps nécessaire pour exécuter l'opération de point de sauvegarde HANA, et cette étape dépend de la charge exercée sur la base de données HANA. La sauvegarde Snapshot de stockage elle-même s'effectue toujours en quelques secondes.



Comparaison des objectifs de délai de restauration (RTO)

Cette section présente une comparaison RTO des sauvegardes Snapshot basées sur les fichiers et le stockage. Le RTO est défini par la somme du temps nécessaire à la restauration de la base de données, ainsi que du temps nécessaire au démarrage et à la restauration de cette base de données.

Temps nécessaire pour restaurer la base de données

Avec une sauvegarde basée sur des fichiers, le temps de restauration dépend de la taille de l'infrastructure de base de données et de sauvegarde, qui définit la vitesse de restauration en mégaoctets par seconde. Par exemple, si l'infrastructure prend en charge une opération de restauration à une vitesse de 250 Mo, il faut environ 1 heure et 10 minutes pour restaurer une base de données de 1 To.

Avec les sauvegardes de copie Snapshot du stockage, la durée de restauration ne dépend pas de la taille de la base de données et reste dans la plage de quelques secondes lorsque la restauration peut être effectuée à partir du stockage primaire. Une restauration à partir du stockage secondaire n'est nécessaire que dans le cas d'un incident lorsque le stockage primaire n'est plus disponible.

Temps nécessaire au démarrage de la base de données

L'heure de début de la base de données dépend de la taille du magasin de lignes et de colonnes. Pour le magasin de colonnes, l'heure de début dépend également de la quantité de données préchargées lors du démarrage de la base de données. Dans les exemples suivants, nous supposons que l'heure de début est de 30 minutes. L'heure de début est identique pour une restauration et une restauration basées sur des fichiers, ainsi qu'une restauration et une restauration basées sur des snapshots.

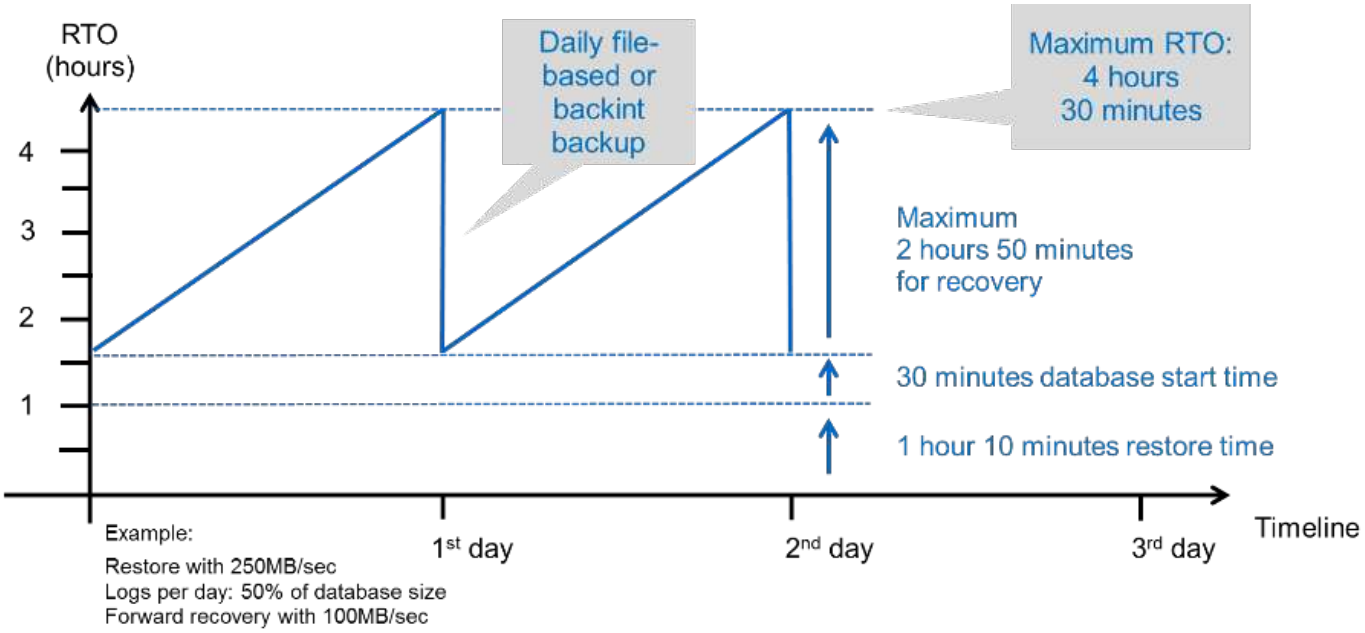
Temps nécessaire pour restaurer la base de données

La durée de restauration dépend du nombre de journaux qui doivent être appliqués après la restauration. Ce nombre est déterminé par la fréquence à laquelle les sauvegardes de données sont effectuées.

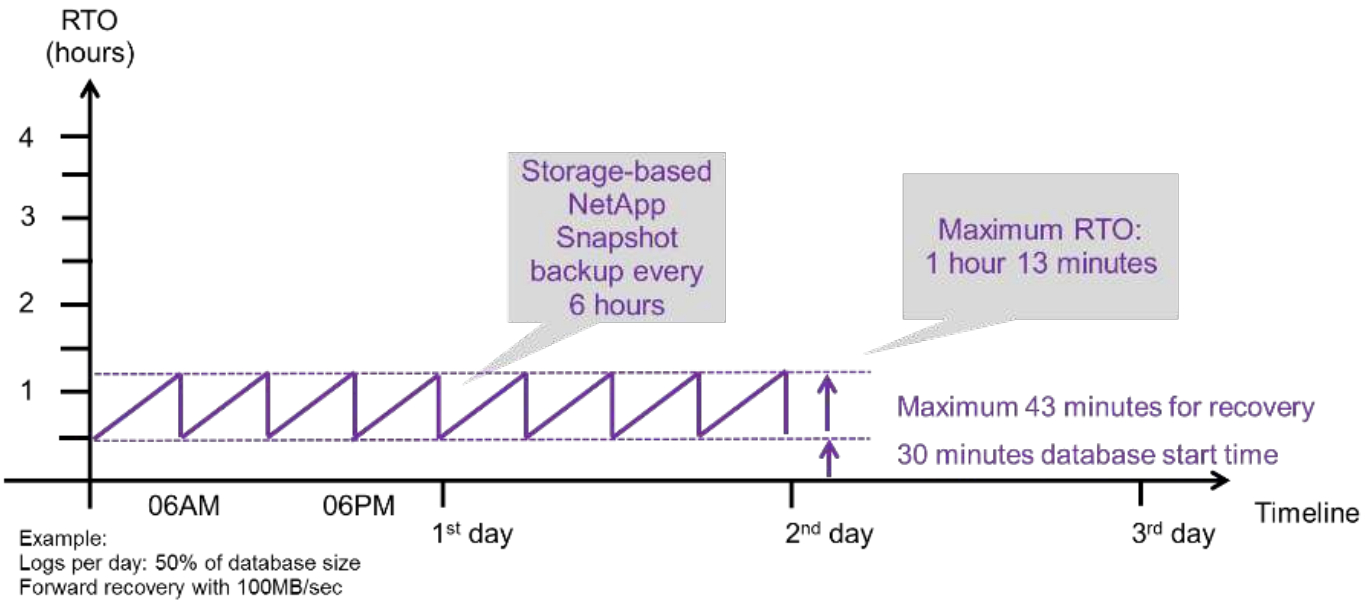
Avec les sauvegardes de données basées sur des fichiers, la planification des sauvegardes est généralement une fois par jour. Étant donné que la sauvegarde dégrade les performances en termes de production, une fréquence de sauvegarde plus élevée est généralement impossible. Par conséquent, dans le pire des cas, tous les journaux qui ont été écrits pendant la journée doivent être appliqués lors de la récupération avant.

Les sauvegardes de données de copie Snapshot du stockage sont généralement planifiées à une fréquence plus élevée, car elles n'influencent pas les performances de la base de données SAP HANA. Par exemple, si des sauvegardes Snapshot sont planifiées toutes les six heures, le temps de restauration est, dans le pire des cas, d'un quart de la durée de restauration d'une sauvegarde basée sur des fichiers (6 heures/24 heures = 1/4).

La figure suivante représente un exemple de RTO pour une base de données de 1 To lorsque des sauvegardes de données basées sur des fichiers sont utilisées. Dans cet exemple, une sauvegarde est effectuée une fois par jour. L'objectif RTO diffère selon le moment où la restauration et la restauration ont été effectuées. Si la restauration et la restauration ont été effectuées immédiatement après la sauvegarde, le RTO se base principalement sur la durée de restauration, qui est de 1 heure et 10 minutes dans l'exemple. La durée de restauration a été augmentée à 2 heures et 50 minutes lorsque la restauration et la restauration ont été effectuées immédiatement avant la prochaine sauvegarde, et le RTO maximal était de 4 heures et 30 minutes.

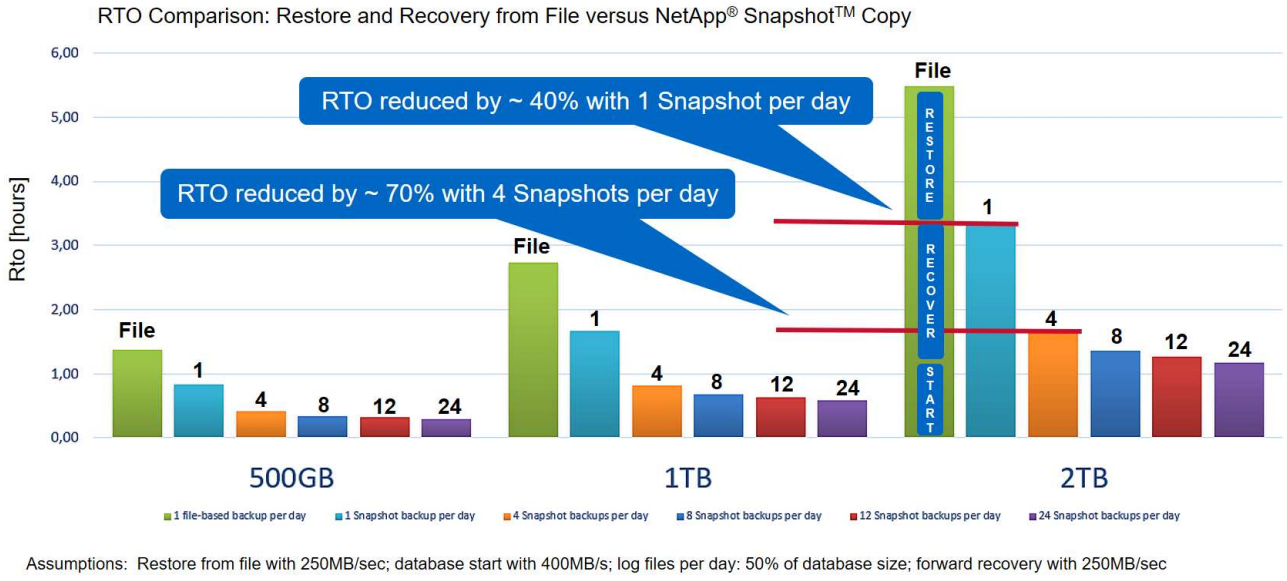


La figure suivante montre un exemple de RTO pour une base de données de 1 To lorsque des sauvegardes Snapshot sont utilisées. Avec les sauvegardes Snapshot basées sur le stockage, le RTO ne dépend que des temps de démarrage de la base de données et du délai de restauration suivant, car la restauration s'effectue en quelques secondes, quelle que soit la taille de la base de données. Le temps de restauration par progression augmente également en fonction de la durée de la restauration et de la restauration, mais étant donné la fréquence plus élevée des sauvegardes (toutes les six heures dans cet exemple), le temps de restauration par progression est de 43 minutes au maximum. Dans cet exemple, le RTO maximal est de 1 heure et 13 minutes.



La figure ci-dessous présente une comparaison RTO des sauvegardes Snapshot basées sur les fichiers et le stockage pour différentes tailles de bases de données et fréquences de sauvegardes Snapshot. La barre verte indique la sauvegarde basée sur des fichiers. Les autres barres affichent les sauvegardes de copies Snapshot avec différentes fréquences de sauvegarde.

Avec une seule sauvegarde de données à copie Snapshot par jour, le RTO est déjà réduit de 40 % par rapport à une sauvegarde de données basée sur des fichiers. La réduction augmente à 70 % lorsque quatre sauvegardes Snapshot sont effectuées par jour. La figure montre également qu'elle n'a pas de courbe, si la fréquence des sauvegardes Snapshot augmente, elle passe à plus de quatre à six sauvegardes Snapshot par jour. Par conséquent, nos clients configurent généralement entre quatre et six sauvegardes Snapshot par jour.



Assumptions: Restore from file with 250MB/sec; database start with 400MB/s; log files per day: 50% of database size; forward recovery with 250MB/sec

Le graphique indique la taille de la RAM du serveur HANA. La taille de la base de données en mémoire est calculée comme étant égale à la moitié de la taille de la mémoire vive du serveur.

La durée de restauration et de récupération est calculée en fonction des hypothèses suivantes. La base de données peut être restaurée à 250 Mbit/s. Le nombre de fichiers journaux par jour est de 50 % de la taille de la base de données. Par exemple, une base de données de 1 To crée 500 Mo de fichiers journaux par jour. Une restauration peut être effectuée à 100 Mbit/s.

Architecture SnapCenter

SnapCenter est une plateforme unifiée et évolutive qui assure la cohérence de la protection des données au niveau des applications. SnapCenter offre un contrôle et une surveillance centralisés, tout en déléguant aux utilisateurs la possibilité de gérer les tâches de sauvegarde, de restauration et de clonage spécifiques aux applications. Avec SnapCenter, les administrateurs de bases de données et de stockage apprennent à utiliser un seul outil pour gérer les opérations de sauvegarde, de restauration et de clonage des différentes applications et bases de données.

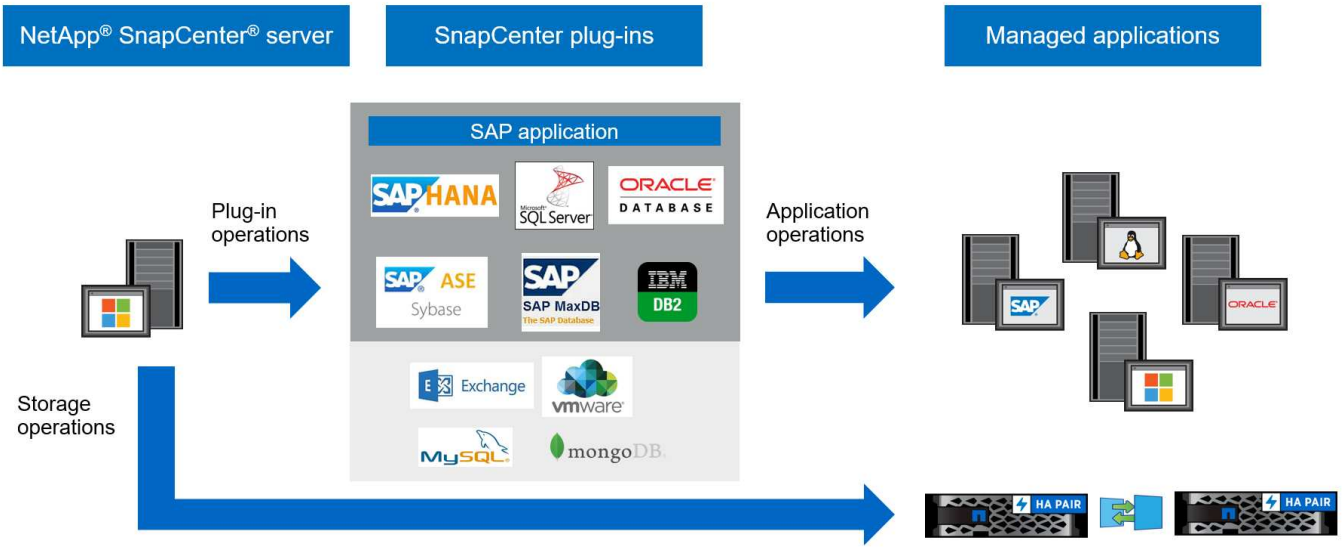
SnapCenter gère les données dans les différents terminaux de la Data Fabric optimisée par NetApp. Vous pouvez l'utiliser SnapCenter pour répliquer des données entre les environnements sur site, entre les environnements sur site et le cloud, ou entre les clouds privés, hybrides et publics.

Composants de SnapCenter

SnapCenter inclut le serveur SnapCenter, le module de plug-in SnapCenter pour Windows et le module de plug-ins SnapCenter pour Linux. Chaque offre comprend des plug-ins à SnapCenter pour divers composants d'infrastructure et d'applications.

Les plug-ins personnalisés SnapCenter vous permettent de créer vos propres plug-ins et de protéger votre application à l'aide de la même interface SnapCenter.

La figure suivante décrit les composants SnapCenter.



Solution de sauvegarde SnapCenter SAP HANA

Cette section répertorie les composants, les versions et configurations SAP HANA prises en charge et les améliorations de SnapCenter 4.6 utilisées dans cette solution.

Composants de la solution

La solution de sauvegarde SnapCenter pour SAP HANA couvre les domaines suivants :

- Sauvegarde des données SAP HANA avec copies Snapshot basées sur le stockage :
  - Planification des sauvegardes
  - La gestion de la conservation
  - Gestion du catalogue des sauvegardes SAP HANA
- Volume sans données (par exemple, `/hana/shared`) Sauvegarde avec copies Snapshot basées sur le stockage :
  - Planification des sauvegardes
  - La gestion de la conservation
- Réplication vers un emplacement de sauvegarde ou de reprise après incident hors site :
  - Sauvegardes Snapshot de données SAP HANA
  - Sans volumes de données
  - Configuration de la gestion de la conservation sur des systèmes de stockage de sauvegarde hors site
  - Gestion du catalogue des sauvegardes SAP HANA
- Contrôles de l'intégrité des blocs de base de données à l'aide d'une sauvegarde basée sur des fichiers :
  - Planification des sauvegardes
  - La gestion de la conservation
  - Gestion du catalogue des sauvegardes SAP HANA
- Gestion de la conservation de la sauvegarde des journaux de base de données HANA :
  - La conservation des données en fonction de la conservation des sauvegardes
  - Gestion du catalogue des sauvegardes SAP HANA
- Découverte automatique des bases de données HANA
- Restauration et reprise automatisées
- Opérations de restauration en locataire unique avec les systèmes MDC (conteneur de base de données mutualisée SAP HANA)

SnapCenter exécute également des sauvegardes de fichiers de données de bases de données en association avec le plug-in pour SAP HANA. Le plug-in définit le point de sauvegarde de la base de données SAP HANA pour que les copies Snapshot, qui sont créées sur le système de stockage principal, soient basées sur une image cohérente de la base de données SAP HANA.

SnapCenter permet la réplication d'images cohérentes de bases de données vers un emplacement de sauvegarde ou de reprise après incident hors site à l'aide de SnapVault ou de NetApp SnapMirror. fonction. Généralement, différentes règles de conservation sont définies selon l'emplacement des sauvegardes sur le stockage primaire et sur le stockage de sauvegarde hors site. SnapCenter gère la conservation au niveau du stockage primaire, et ONTAP gère la conservation au niveau du stockage de sauvegarde hors site.

Pour permettre une sauvegarde complète de toutes les ressources SAP HANA, SnapCenter vous permet également de sauvegarder tous les volumes non-data à l'aide du plug-in SAP HANA avec des copies Snapshot basées sur le stockage. Il est possible de planifier des volumes non-data indépendamment de la sauvegarde des données de la base de données afin de mettre en place des règles de conservation et de protection individuelles.

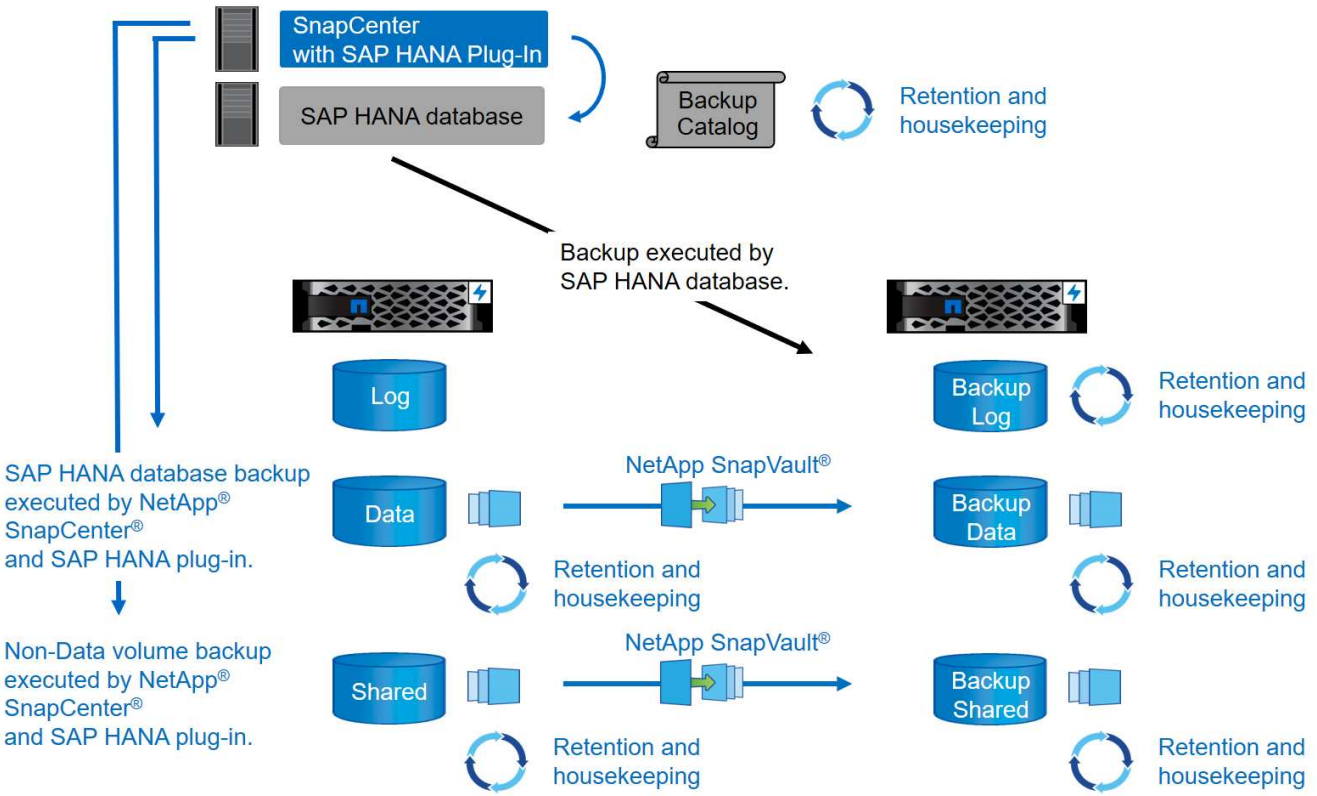
La base de données SAP HANA exécute automatiquement des sauvegardes des journaux. Selon les objectifs de point de restauration, plusieurs options existent pour l'emplacement de stockage des sauvegardes de journaux :

- La sauvegarde des journaux est écrite sur un système de stockage qui assure la mise en miroir synchrone des données sur un second emplacement avec le logiciel de stockage NetApp MetroCluster haute disponibilité et de reprise après incident.
- La destination de sauvegarde des journaux peut être configurée sur le même système de stockage primaire, puis répliquée de manière synchrone ou asynchrone vers un stockage secondaire avec SnapMirror.
- La destination de sauvegarde des journaux peut être configurée sur le même stockage de sauvegarde hors site dans lequel les sauvegardes des bases de données sont répliquées avec SnapVault. Avec cette configuration, le stockage de sauvegarde hors site a des besoins en disponibilité tels que ceux du stockage primaire, de sorte que les sauvegardes des journaux puissent être écrites sur le stockage de sauvegarde hors site.

SAP recommande de combiner des sauvegardes Snapshot basées sur le stockage et une sauvegarde hebdomadaire basée sur des fichiers pour exécuter une vérification de l'intégrité des blocs. La vérification de l'intégrité des blocs peut être exécutée depuis SnapCenter. En fonction de vos règles de conservation configurables, SnapCenter gère l'organisation des sauvegardes de fichiers de données dans le système de stockage primaire, les sauvegardes de fichiers journaux et le catalogue de sauvegardes SAP HANA.

SnapCenter gère la conservation au niveau du stockage primaire, tandis que ONTAP gère la conservation des sauvegardes secondaires.

La figure suivante présente un aperçu de la configuration de sauvegarde des bases de données et des journaux, dans laquelle les sauvegardes des journaux sont écrites sur un montage NFS du stockage de sauvegarde hors site.



Lors de l'exécution d'une sauvegarde Snapshot basée sur le stockage de volumes non-données, SnapCenter effectue les tâches suivantes :

1. Création d'une copie Snapshot de stockage du volume sans données.
2. L'exécution d'une mise à jour de SnapVault ou de SnapMirror pour le volume de données, si configurée.
3. Suppression des copies Snapshot de stockage au niveau du stockage primaire selon la règle de conservation définie.

Lors de l'exécution d'une sauvegarde Snapshot basée sur le stockage de la base de données SAP HANA, SnapCenter effectue les tâches suivantes :

1. Création d'un point de sauvegarde SAP HANA pour créer une image cohérente sur la couche de persistance.
2. Création d'une copie Snapshot de stockage du volume de données.
3. Enregistrement du Snapshot de stockage dans le catalogue des sauvegardes SAP HANA.
4. Version du point de sauvegarde de SAP HANA.
5. L'exécution d'une mise à jour de SnapVault ou de SnapMirror pour le volume de données, si configurée.
6. Suppression des copies Snapshot de stockage au niveau du stockage primaire selon la règle de conservation définie.
7. Suppression des entrées du catalogue de sauvegardes SAP HANA si les sauvegardes n'existent plus sur le stockage de sauvegarde primaire ou hors site.
8. Lorsqu'une sauvegarde a été supprimée en fonction de la stratégie de conservation ou manuellement, SnapCenter supprime toutes les sauvegardes de journaux antérieures à la sauvegarde de données la plus ancienne. Les sauvegardes des journaux sont supprimées dans le système de fichiers et dans le catalogue de sauvegardes SAP HANA.

Versions et configurations SAP HANA prises en charge

SnapCenter prend en charge les configurations SAP HANA à un ou plusieurs hôtes à l'aide de systèmes de stockage NetApp NFS ou FC (AFF et FAS), ainsi que les systèmes SAP HANA qui s'exécutent sur Cloud Volumes ONTAP dans AWS, Azure, Google Cloud Platform et AWS FSX ONTAP à l'aide de NFS.

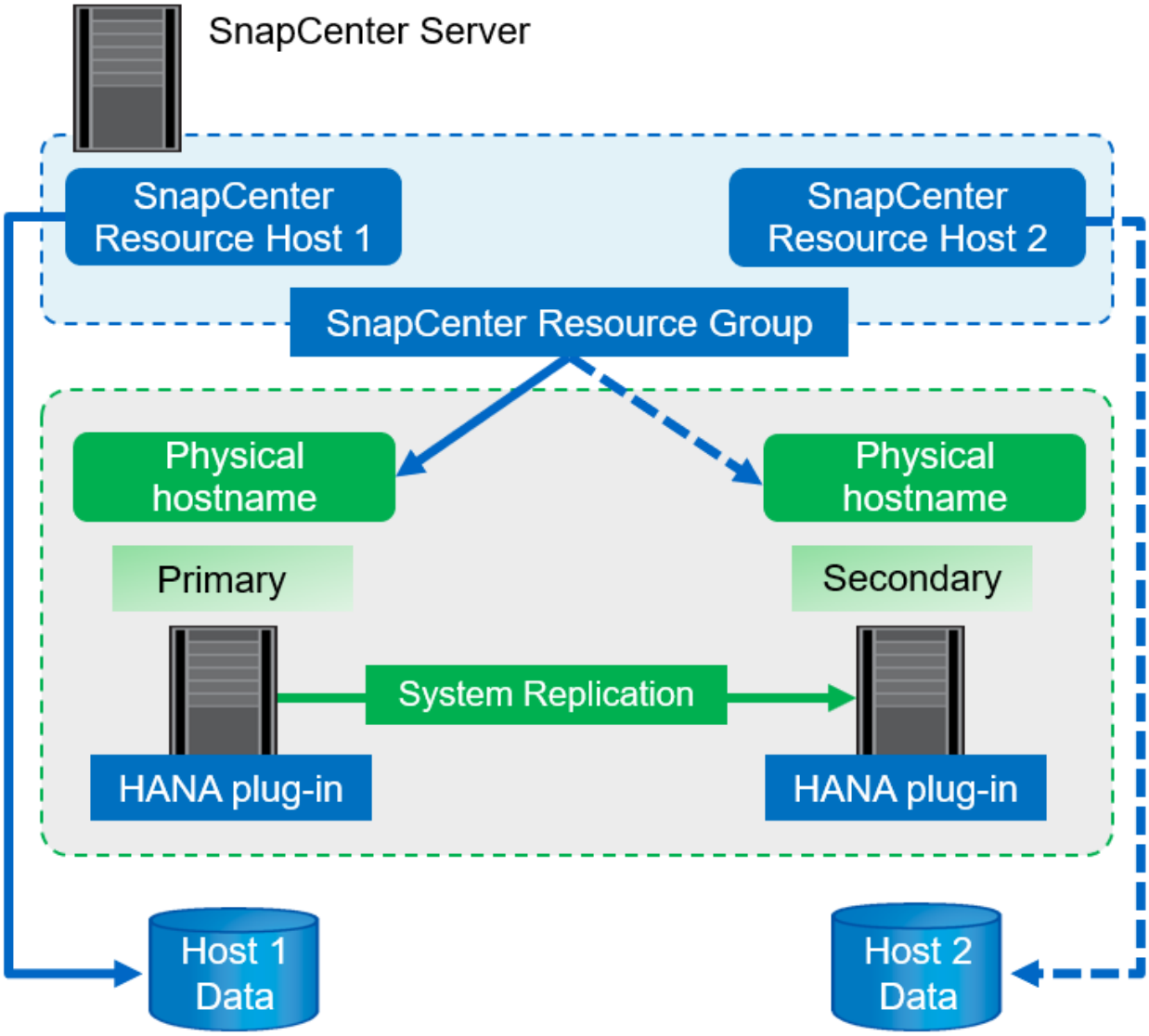
SnapCenter prend en charge plusieurs architectures et versions SAP HANA :

- Conteneur unique SAP HANA : SAP HANA 1.0 SPS12
- Conteneur de base de données mutualisée SAP HANA (MDC) pour un seul locataire : SAP HANA 2.0 SPS3 et version ultérieure
- Conteneur de base de données mutualisée SAP HANA (MDC) pour plusieurs locataires : SAP HANA 2.0 SPS4 et ultérieure

Améliorations apportées à SnapCenter 4.6

À partir de la version 4.6, SnapCenter prend en charge la découverte automatique des systèmes HANA configurés dans une relation de réplication système HANA. Chaque hôte est configuré à l'aide de son adresse IP physique (nom d'hôte) et de son volume de données individuel sur la couche de stockage. Les deux ressources SnapCenter sont combinées dans un groupe de ressources, SnapCenter identifie automatiquement l'hôte principal ou secondaire, puis exécute les opérations de sauvegarde requises en conséquence. La gestion des données de conservation pour les sauvegardes Snapshot et basées sur les fichiers créées avec SnapCenter s'effectue sur les deux hôtes pour s'assurer que les anciennes sauvegardes sont également supprimées sur l'hôte secondaire actuel. La figure suivante présente une vue d'ensemble

générale. Vous trouverez une description détaillée de la configuration et du fonctionnement des systèmes HANA HANA compatibles avec la réplication dans le SnapCenter "Tr-4719 réplication système SAP HANA, sauvegarde et restauration avec SnapCenter".



Concepts et bonnes pratiques SnapCenter

Cette section décrit les concepts et les bonnes pratiques SnapCenter concernant la configuration et le déploiement de ressources SAP HANA.

Concepts et options de configuration des ressources SAP HANA

Avec SnapCenter, la configuration des ressources de bases de données SAP HANA peut être effectuée de deux approches différentes.

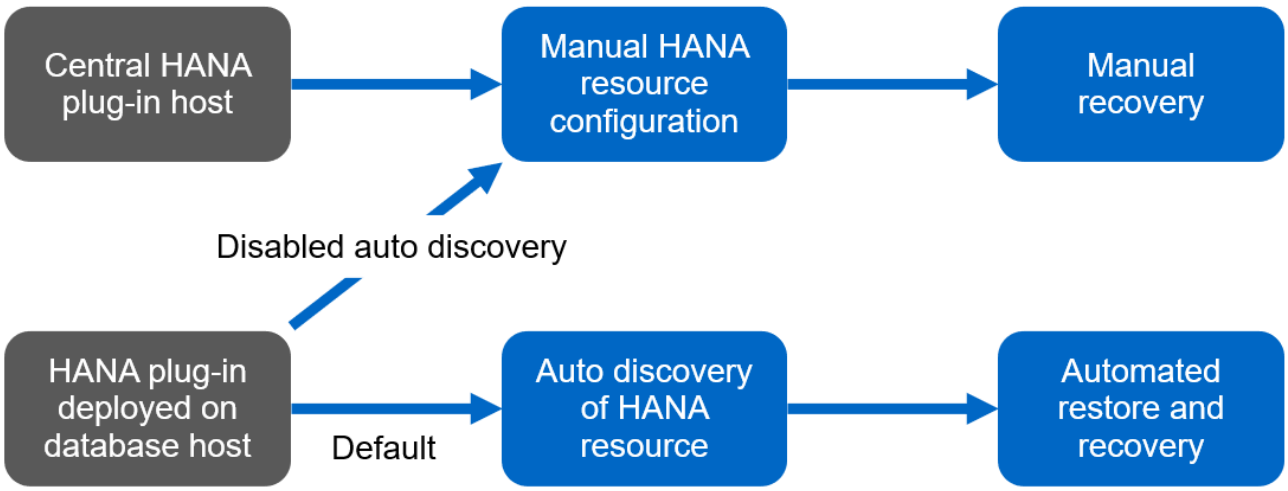
- **Configuration manuelle des ressources.** les informations de ressource et d'empreinte de stockage HANA doivent être fournies manuellement.
- **Découverte automatique des ressources HANA** la découverte automatique simplifie la configuration des bases de données HANA dans SnapCenter et permet la restauration et la restauration automatisées.

Il est important de comprendre que seules les ressources de bases de données HANA dans SnapCenter qui ont été automatiquement découvertes sont activées pour la restauration et la restauration automatisées. Les ressources de bases de données HANA configurées manuellement dans SnapCenter doivent être restaurées manuellement après une opération de restauration dans SnapCenter.

Par contre, la détection automatique avec SnapCenter n'est pas prise en charge pour toutes les architectures HANA et les configurations d'infrastructure. Par conséquent, les paysages HANA peuvent nécessiter une approche mixte dans laquelle certains systèmes HANA (systèmes hôtes multiples HANA) nécessitent une configuration manuelle des ressources et tous les autres peuvent être configurés via la détection automatique.

La détection automatique ainsi que la restauration et la restauration automatisées dépendent de la capacité à exécuter des commandes du système d'exploitation sur l'hôte de base de données. La découverte de systèmes de fichiers et d'empreinte de stockage, et les opérations de détection de démonter, monter ou LUN sont des exemples. Ces opérations sont exécutées avec le plug-in SnapCenter Linux, qui est automatiquement déployé avec le plug-in HANA. Par conséquent, il est nécessaire de déployer le plug-in HANA sur l'hôte de base de données pour activer la découverte automatique, ainsi que la restauration et la récupération automatisées. Il est également possible de désactiver la détection automatique après le déploiement du plug-in HANA sur l'hôte de base de données. Dans ce cas, la ressource sera configurée manuellement.

La figure suivante résume les dépendances. Pour plus d'informations sur les options de déploiement HANA, reportez-vous à la section « Options de déploiement du plug-in SAP HANA ».



Les plug-ins HANA et Linux ne sont actuellement disponibles que pour les systèmes basés sur Intel. Si les bases de données HANA s'exécutent sur IBM Power Systems, un plug-in HANA central doit être utilisé.

Architectures HANA prises en charge pour la détection automatique et la restauration automatisée

Grâce à SnapCenter, la détection automatique, ainsi que la restauration et la récupération automatisées sont prises en charge pour la plupart des configurations HANA, à l'exception de ce que plusieurs systèmes hôtes HANA requièrent une configuration manuelle.

Le tableau suivant présente les configurations HANA prises en charge pour la détection automatique.

Le plug-in HANA est installé sur :	Architecture HANA	Configuration du système HANA	Infrastructures
Hôte de base de données HANA	Un seul hôte	• Conteneur unique HANA • Conteneurs de base de données mutualisée SAP HANA (MDC) avec un ou plusieurs locataires • Réplication système HANA	• Bare-Metal avec NFS • Bare Metal avec XFS et FC avec ou sans Linux Logical Volume Manager (LVM) • VMware avec des montages NFS directs de système d'exploitation

Les systèmes MDC HANA avec plusieurs locataires sont pris en charge pour la détection automatique, mais pas pour la restauration et la restauration automatisées avec la version actuelle de SnapCenter.

Architectures HANA prises en charge pour la configuration manuelle des ressources HANA

La configuration manuelle des ressources HANA est prise en charge pour toutes les architectures HANA, mais elle nécessite un plug-in HANA central. Le plug-in central peut être le serveur SnapCenter lui-même ou un hôte Linux ou Windows distinct.

Lorsque le plug-in HANA est déployé sur l'hôte de base de données HANA, la ressource est automatiquement découverte par défaut. La détection automatique peut être désactivée pour les hôtes individuels, afin que le plug-in puisse être déployé. Par exemple, sur un hôte de base de données avec la réplication système HANA activée et dans une version SnapCenter < 4.6, où la détection automatique n'est pas prise en charge. Pour plus d'informations, reportez-vous à la section ""Désactiver la détection automatique sur l'hôte du plug-in HANA.""

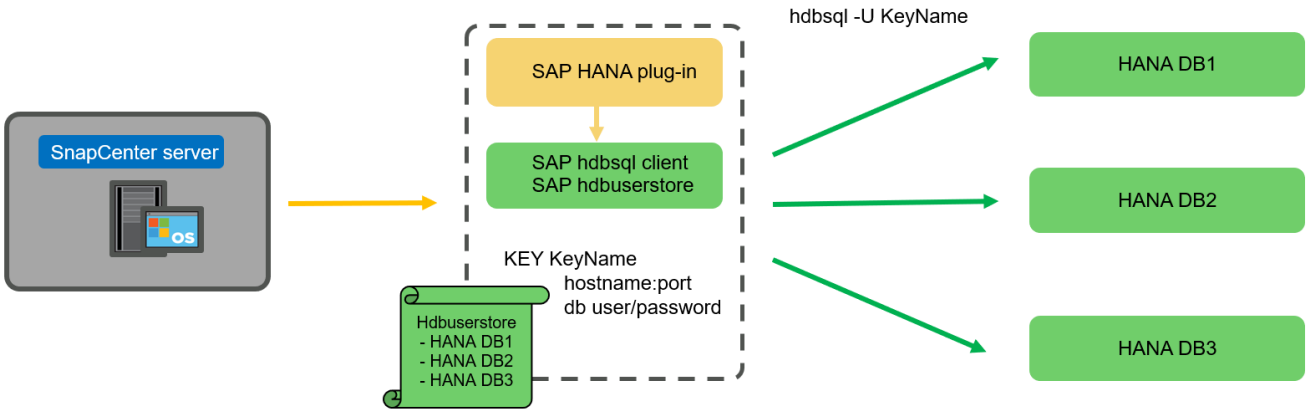
Le tableau suivant présente les configurations HANA prises en charge pour la configuration manuelle des ressources HANA.

Plug-in HANA installé sur :	Architecture HANA	Configuration du système HANA	Infrastructures
Hôte de plug-in central (serveur SnapCenter ou hôte Linux distinct)	Un ou plusieurs hôtes	• Conteneur unique HANA • MDC HANA avec un ou plusieurs locataires • Réplication système HANA	• Bare-Metal avec NFS • Bare Metal avec XFS et FC avec ou sans Linux LVM • VMware avec des montages NFS directs de système d'exploitation

Options de déploiement pour le plug-in SAP HANA

La figure suivante montre la vue logique et la communication entre le serveur SnapCenter et les bases de données SAP HANA.

Le serveur SnapCenter communique via le plug-in SAP HANA avec les bases de données SAP HANA. Le plug-in SAP HANA utilise le logiciel client SAP HANA hdbsql pour exécuter des commandes SQL sur les bases de données SAP HANA. Le hdbuserstore SAP HANA permet de fournir les identifiants de l'utilisateur, le nom de l'hôte et les informations de port pour accéder aux bases de données SAP HANA.



Le plug-in SAP HANA et le logiciel client SAP hdbsql, qui inclut l'outil de configuration hdbuserstore, doivent être installés ensemble sur le même hôte.

L'hôte peut être le serveur SnapCenter lui-même, un hôte de plug-in central distinct ou les hôtes de base de données SAP HANA individuels.

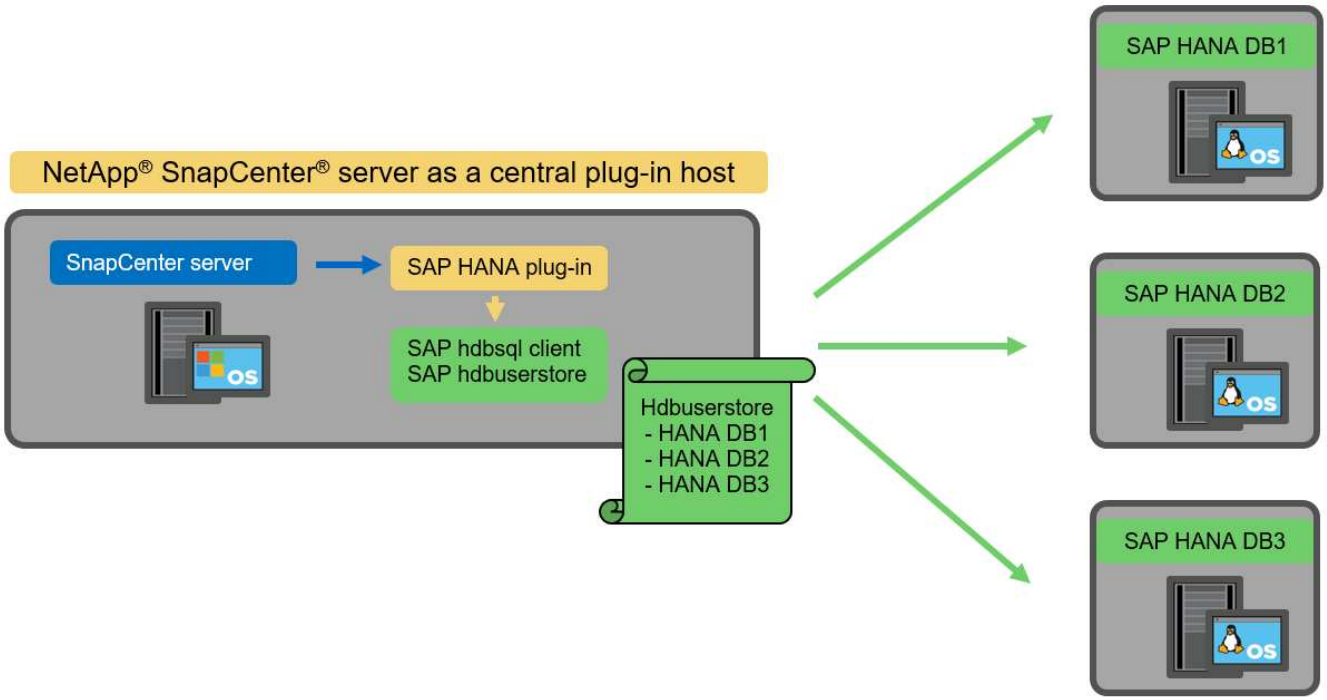
Haute disponibilité du serveur SnapCenter

SnapCenter peut être configuré en configuration haute disponibilité à deux nœuds. Dans une telle configuration, un équilibreur de charge (par exemple, F5) est utilisé en mode actif/passif à l'aide d'une adresse IP virtuelle pointant vers l'hôte SnapCenter actif. Le référentiel SnapCenter (base de données MySQL) est répliqué par SnapCenter entre les deux hôtes de sorte que les données SnapCenter soient toujours en mode synchrone.

SnapCenter Server HA n'est pas pris en charge si le plug-in HANA est installé sur le serveur SnapCenter. Si vous prévoyez d'installer SnapCenter dans une configuration HA, n'installez pas le plug-in HANA sur le serveur SnapCenter. Vous trouverez plus d'informations sur la haute disponibilité SnapCenter dans ce document "Page de la base de connaissances NetApp".

Serveur SnapCenter en tant qu'hôte plug-in HANA central

La figure suivante montre une configuration dans laquelle le serveur SnapCenter est utilisé comme hôte plug-in central. Le plug-in SAP HANA et le logiciel client SAP hdbsql sont installés sur le serveur SnapCenter.



Comme le plug-in HANA peut communiquer avec les bases de données HANA gérées par hdbclient via le réseau, il n'est pas nécessaire d'installer de composants SnapCenter sur les hôtes de base de données HANA individuels. SnapCenter peut protéger les bases de données HANA en utilisant un hôte plug-in HANA central sur lequel toutes les clés de magasin d'utilisateurs sont configurées pour les bases de données gérées.

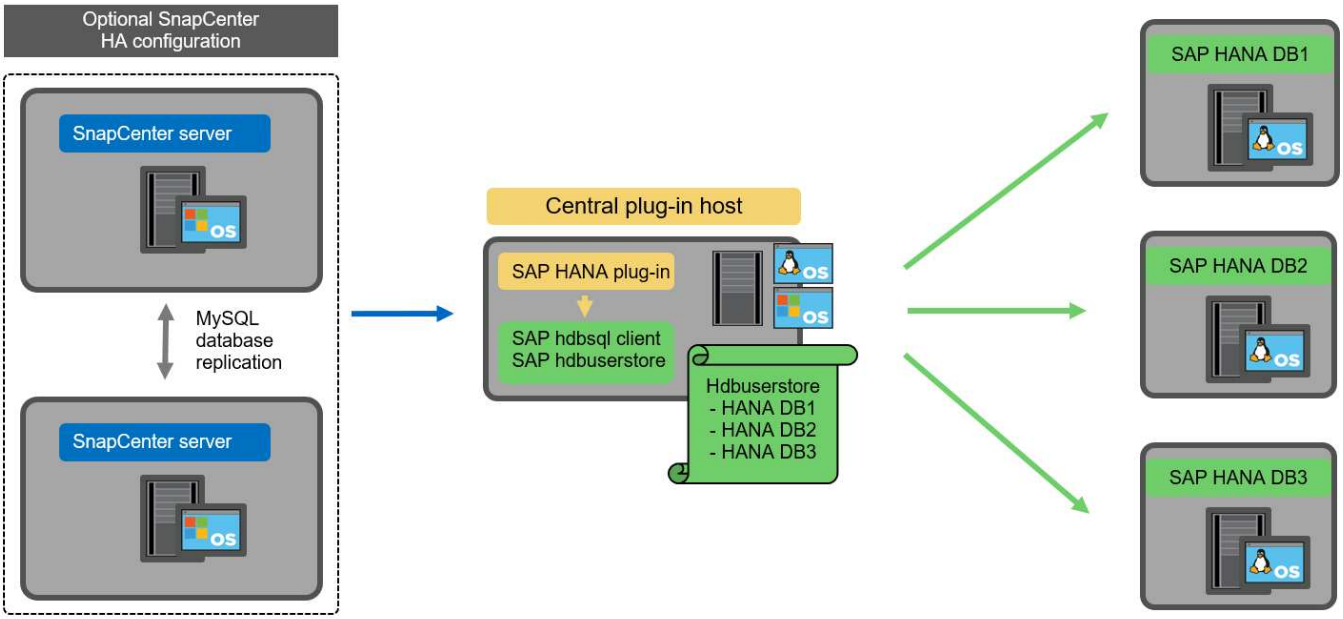
D'autre part, l'automatisation améliorée des flux de travail pour la découverte automatique, l'automatisation de la restauration et de la récupération, ainsi que les opérations de mise à jour du système SAP exigent l'installation de composants SnapCenter sur l'hôte de base de données. Lorsque vous utilisez un plug-in HANA central, ces fonctionnalités ne sont pas disponibles.

Par ailleurs, la haute disponibilité du serveur SnapCenter via la fonctionnalité HA intégrée ne peut pas être utilisée lorsque le plug-in HANA est installé sur le serveur SnapCenter. La haute disponibilité peut être obtenue en utilisant VMware HA si le serveur SnapCenter est exécuté sur une machine virtuelle au sein d'un cluster VMware.

Hôte séparé en tant qu'hôte plug-in HANA central

La figure suivante montre une configuration dans laquelle un hôte Linux distinct est utilisé comme hôte plug-in central. Dans ce cas, le plug-in SAP HANA et le logiciel client SAP hdbsql sont installés sur l'hôte Linux.

ⓘ L'hôte distinct de plug-in central peut également être un hôte Windows.

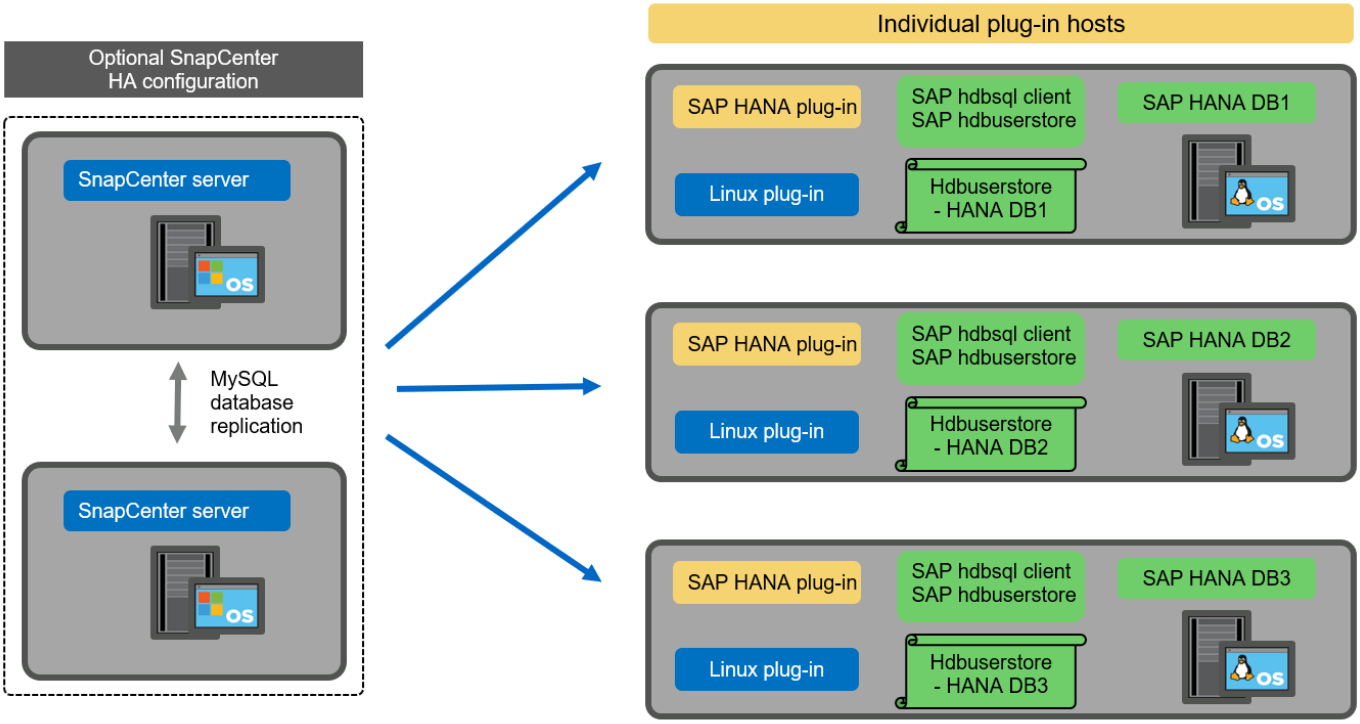


La même restriction concernant la disponibilité des fonctionnalités décrite dans la section précédente s'applique également à un hôte de plug-in central distinct.

Cependant, grâce à cette option de déploiement, le serveur SnapCenter peut être configuré avec la fonctionnalité In-Build HA. Le plug-in central doit également être HA, par exemple, en utilisant une solution de cluster Linux.

Le plug-in HANA est déployé sur des hôtes de base de données HANA individuels

La figure suivante montre une configuration dans laquelle le plug-in SAP HANA est installé sur chaque hôte de base de données SAP HANA.



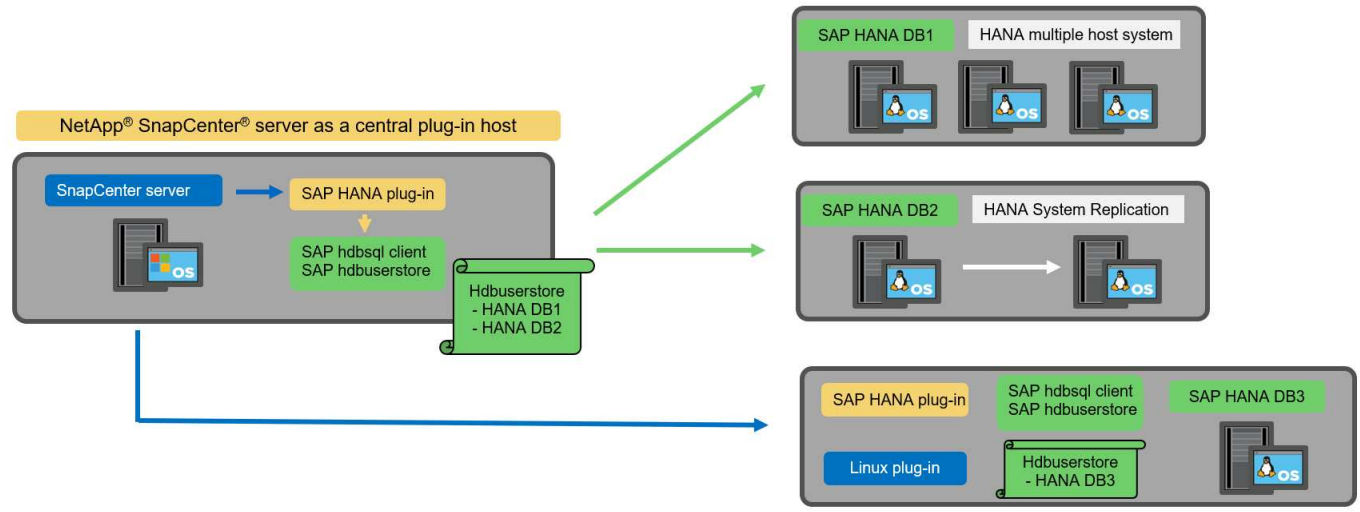
Lorsque le plug-in HANA est installé sur chaque hôte de base de données HANA individuel, toutes les fonctionnalités, telles que la découverte automatique et la restauration et la récupération automatisées, sont disponibles. Par ailleurs, le serveur SnapCenter peut être configuré dans une configuration haute disponibilité.

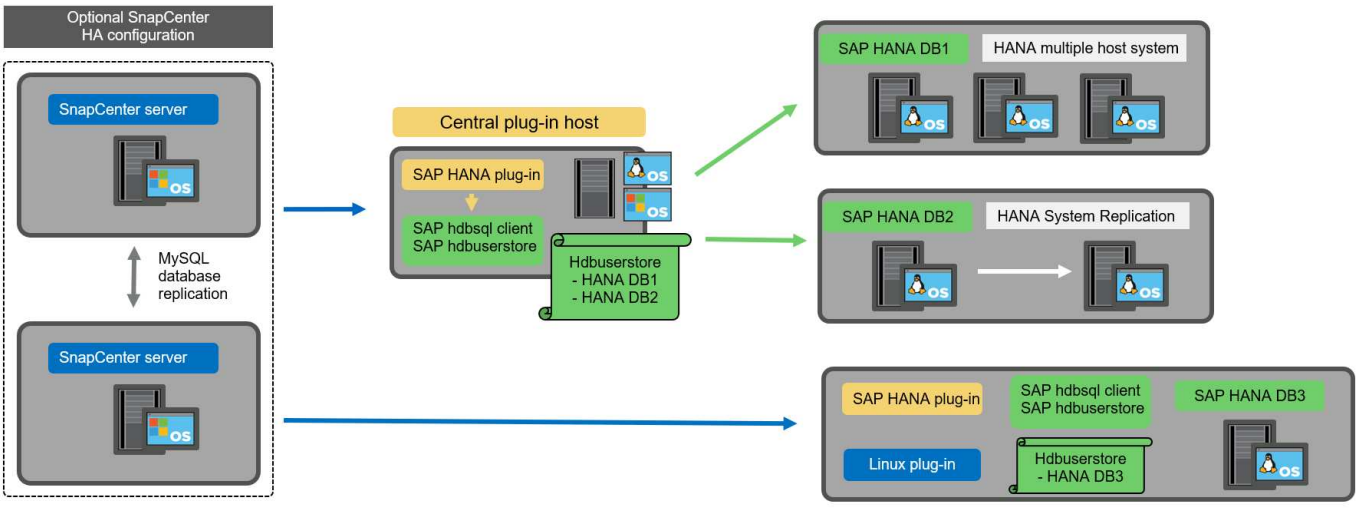
Déploiement de plug-in HANA mixtes

Comme indiqué au début de cette section, certaines configurations système HANA, telles que les systèmes à plusieurs hôtes, requièrent un hôte de plug-in central. Par conséquent, la plupart des configurations SnapCenter nécessitent un déploiement mixte du plug-in HANA.

NetApp recommande de déployer le plug-in HANA sur l'hôte de base de données HANA pour toutes les configurations de système HANA prises en charge pour la découverte automatique. D'autres systèmes HANA, tels que les configurations à plusieurs hôtes, doivent être gérés avec un hôte plug-in HANA central.

Les deux figures suivantes présentent des déploiements de plug-ins mixtes avec le serveur SnapCenter ou un hôte Linux distinct en tant qu'hôte de plug-in central. La seule différence entre ces deux déploiements est la configuration haute disponibilité en option.





Résumé et recommandations

De manière générale, NetApp vous recommande de déployer le plug-in HANA sur chaque hôte SAP HANA

pour activer toutes les fonctionnalités SnapCenter HANA disponibles et améliorer l'automatisation des workflows.

> Les plug-ins HANA et Linux ne sont actuellement disponibles que pour les systèmes basés sur Intel. Si les bases de données HANA s'exécutent sur IBM Power Systems, un plug-in HANA central doit être utilisé.

Pour les configurations HANA dans lesquelles la détection automatique n'est pas prise en charge, telles que les configurations plusieurs hôtes HANA, un plug-in HANA central supplémentaire doit être configuré. L'hôte du plug-in central peut être le serveur SnapCenter si VMware HA peut être utilisé pour SnapCenter HA. Si vous prévoyez d'utiliser la fonctionnalité de haute disponibilité intégrée d'SnapCenter, utilisez un hôte de plug-in Linux séparé.

Le tableau suivant récapitule les différentes options de déploiement.

Option de déploiement	Dépendances
Plug-in hôte HANA central installé sur le serveur SnapCenter	Avantages : * plug-in HANA unique, configuration centrale du magasin d'utilisateur HDB * pas de composants logiciels SnapCenter requis sur les hôtes de base de données HANA individuels * prise en charge de toutes les architectures HANA inconvénients : * Configuration manuelle des ressources * récupération manuelle * pas de prise en charge de la restauration d'un seul locataire * toutes les étapes pré et post-script sont exécutées sur l'hôte du plug-in central * haute disponibilité SnapCenter intégrée non prise en charge * la combinaison SID et nom de locataire doit être unique dans toutes les bases de données HANA gérées * Log Activation/désactivation de la gestion de la conservation des sauvegardes pour toutes les bases de données HANA gérées
Plug-in hôte HANA central installé sur un serveur Linux ou Windows distinct	Avantages : * plug-in HANA unique, configuration centrale du magasin d'utilisateur HDB * pas de composants logiciels SnapCenter requis sur les hôtes de base de données HANA individuels * prise en charge de toutes les architectures HANA * SnapCenter haute disponibilité prise en charge : * Configuration manuelle des ressources * récupération manuelle * pas de prise en charge de la restauration d'un seul locataire * toutes les étapes pré et post-script sont exécutées sur l'hôte du plug-in central * la combinaison SID et nom de locataire doit être unique pour toutes les bases de données HANA gérées * gestion de la conservation des sauvegardes de journaux activée/désactivée pour toutes les personnes gérées Les bases de données HANA

Option de déploiement	Dépendances
Plug-in hôte HANA individuel installé sur le serveur de base de données HANA	Avantages : * détection automatique des ressources HANA * restauration et restauration automatisées * restauration par locataire unique * automatisation pré et post-script pour les mises à jour du système SAP * haute disponibilité SnapCenter intégrée prise en charge * la gestion de la conservation des sauvegardes des journaux peut être activée/désactivée pour chaque serveur de bases de données HANA individuel : * Non pris en charge pour toutes les architectures HANA. Plug-in central supplémentaire requis pour plusieurs systèmes hôtes HANA. * Le plug-in HANA doit être déployé sur chaque hôte de base de données HANA

Stratégie de protection des données

Avant de configurer SnapCenter et le plug-in SAP HANA, la stratégie de protection des données doit être définie en fonction des exigences RTO et RPO des divers systèmes SAP.

Une approche commune consiste à définir des types de systèmes tels que la production, le développement, les tests ou les systèmes sandbox. Tous les systèmes SAP d'un même type de système ont généralement les mêmes paramètres de protection des données.

Les paramètres à définir sont les suivants :

- À quelle fréquence une sauvegarde Snapshot doit-elle être exécutée ?
- Combien de temps les sauvegardes de copies Snapshot doivent-elles être conservées sur le système de stockage primaire ?
- À quelle fréquence un contrôle d'intégrité des blocs doit-il être exécuté ?
- Les sauvegardes primaires doivent-elles être répliquées sur un site de sauvegarde hors site ?
- Combien de temps les sauvegardes doivent-elles être conservées sur le stockage de sauvegarde hors site ?

Le tableau suivant présente un exemple de paramètres de protection des données pour la production, le développement et le test du type de système. Pour le système de production, une fréquence de sauvegarde élevée a été définie et les sauvegardes sont répliquées sur un site de sauvegarde hors site une fois par jour. Les systèmes de test présentent des exigences moindres, et aucune réplication des sauvegardes n'est possible.

Paramètres	Systèmes de production	Systèmes de développement	Systèmes de test
Fréquence des sauvegardes	Toutes les 4 heures	Toutes les 4 heures	Toutes les 4 heures
Conservation primaire	2 jours	2 jours	2 jours
Vérification de l'intégrité des blocs	Une fois par semaine	Une fois par semaine	Non
La réplication vers un site de sauvegarde hors site	Une fois par jour	Une fois par jour	Non

Paramètres	Systèmes de production	Systèmes de développement	Systèmes de test
Conservation des sauvegardes hors site	2 semaines	2 semaines	Sans objet

Le tableau suivant présente les règles à configurer pour les paramètres de protection des données.

Paramètres	PolicySnap	PolicySnapperSnapVault	Contrôles de PolicyBlockIntegris
Type de sauvegarde	Basé sur Snapshot	Basé sur Snapshot	Basée sur un fichier
Fréquence de programmation	Horaire	Tous les jours	Hebdomadaire
Conservation primaire	Nombre = 12	Nombre = 3	Nombre = 1
Réplication SnapVault	Non	Oui.	Sans objet

La politique `LocalSnapshot` Utilisé dans les systèmes de production, de développement et de test pour couvrir les sauvegardes Snapshot locales avec une durée de conservation de deux jours.

Dans la configuration de la protection des ressources, le planning est défini différemment pour les types de système :

- **Production.** horaire toutes les 4 heures.
- **Développement.** horaire toutes les 4 heures.
- **Test.** horaire toutes les 4 heures.

La politique `LocalSnapAndSnapVault` utilisé pour les systèmes de production et de développement afin de couvrir la réplication quotidienne vers le stockage de sauvegarde hors site.

Dans la configuration de la protection des ressources, le planning est défini pour la production et le développement :

- **Production.** Calendrier tous les jours.
- **Développement.** Calendrier tous les jours.

La politique `BlockIntegrityCheck` utilisé par les systèmes de production et de développement pour couvrir le contrôle hebdomadaire de l'intégrité des blocs à l'aide d'une sauvegarde basée sur des fichiers.

Dans la configuration de la protection des ressources, le planning est défini pour la production et le développement :

- **Production.** horaire chaque semaine.
- **Développement.** horaire chaque semaine.

Pour chaque base de données SAP HANA individuelle qui utilise une règle de sauvegarde hors site, une relation de protection doit être configurée sur la couche de stockage. La relation de protection définit quels volumes sont répliqués et la conservation de sauvegardes sur le stockage de sauvegarde hors site.

Dans notre exemple, pour chaque système de production et de développement, une durée de conservation de deux semaines est définie sur le stockage de sauvegarde hors site.

Dans notre exemple, les règles de protection et la conservation des ressources de bases de données SAP HANA et de volumes autres que de données ne sont pas différentes.

Les opérations de sauvegarde

SAP a introduit la prise en charge des sauvegardes Snapshot pour les systèmes MDC à plusieurs locataires avec HANA 2.0 SPS4. SnapCenter prend en charge les opérations de sauvegarde Snapshot des systèmes MDC HANA avec plusieurs locataires. SnapCenter prend également en charge deux opérations de restauration différentes d'un système MDC HANA. Vous pouvez restaurer l'ensemble du système, la base de données système et tous les locataires, ou bien restaurer un seul locataire. Certains critères requis sont requis pour permettre à SnapCenter d'exécuter ces opérations.

Dans un système MDC, la configuration du locataire n'est pas nécessairement statique. Il est possible d'ajouter des locataires ou de les supprimer. SnapCenter ne peut pas compter sur la configuration découverte lorsque la base de données HANA est ajoutée à SnapCenter. SnapCenter doit savoir quels locataires sont disponibles au moment de l'exécution de l'opération de sauvegarde.

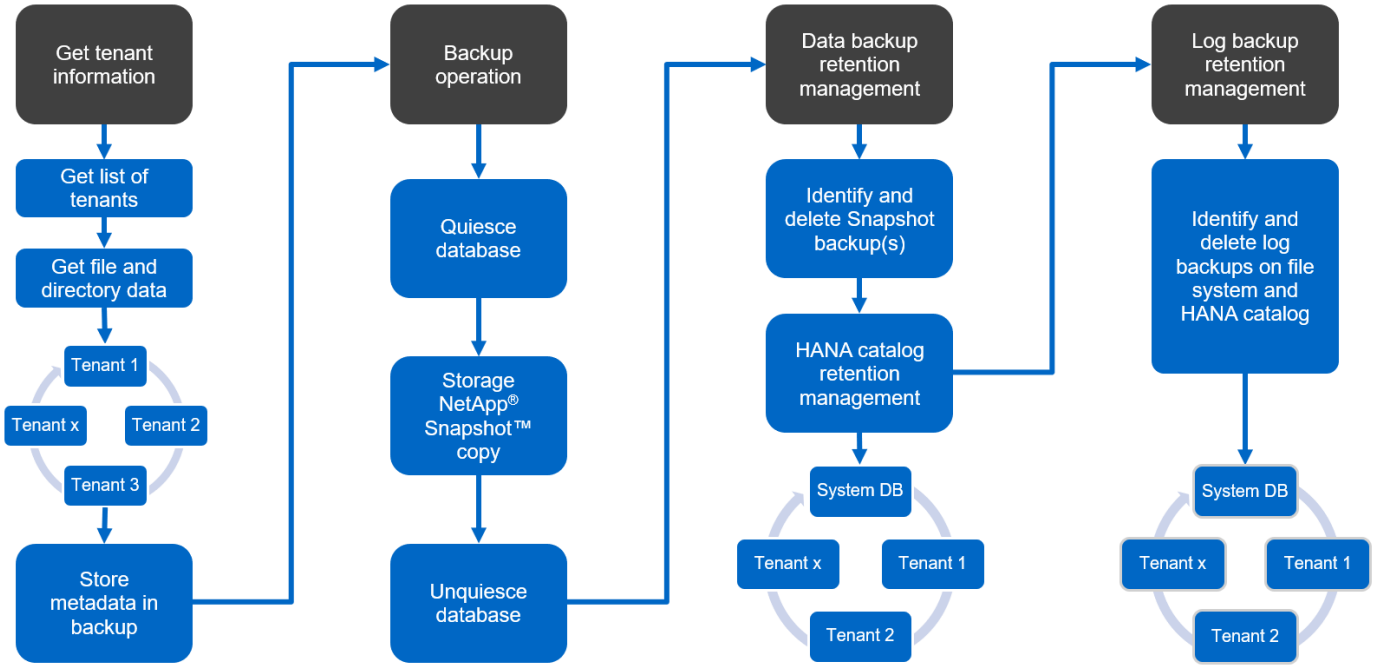
Pour permettre une opération de restauration par locataire unique, SnapCenter doit savoir quels locataires sont inclus dans chaque sauvegarde Snapshot. En outre, le département informatique doit savoir quels fichiers et répertoires appartiennent à chaque locataire inclus dans la sauvegarde Snapshot.

Par conséquent, à chaque opération de sauvegarde, la première étape du workflow consiste à obtenir les informations de locataire. Cela inclut les noms de tenant ainsi que les informations de fichier et de répertoire correspondantes. Ces données doivent être stockées dans les métadonnées de sauvegarde Snapshot afin de pouvoir prendre en charge une seule opération de restauration locataire. L'étape suivante est l'opération de sauvegarde Snapshot elle-même. Cette étape inclut la commande SQL pour déclencher le point de sauvegarde HANA, la sauvegarde Snapshot de stockage et la commande SQL pour fermer l'opération Snapshot. En utilisant la commande close, la base de données HANA met à jour le catalogue de sauvegardes du BDD système et de chaque locataire.

SAP ne prend pas en charge les opérations de sauvegarde Snapshot pour les systèmes MDC lorsque un ou plusieurs locataires sont arrêtés.

Pour la gestion de la conservation des sauvegardes de données et de la gestion des catalogues de sauvegardes HANA, SnapCenter doit exécuter les opérations de suppression du catalogue pour la base de données système et toutes les bases de données de locataires identifiées lors de la première étape. De la même façon pour les sauvegardes de journaux, le flux de travail SnapCenter doit fonctionner sur chaque locataire qui faisait partie de l'opération de sauvegarde.

La figure suivante présente une vue d'ensemble du workflow de sauvegarde.



Workflow de sauvegarde pour les sauvegardes Snapshot de la base de données HANA

SnapCenter sauvegarde la base de données SAP HANA dans l'ordre suivant :

1. SnapCenter lit la liste des locataires de la base de données HANA.
2. SnapCenter lit les fichiers et les répertoires de chaque locataire à partir de la base de données HANA.
3. Les informations des locataires sont stockées dans les métadonnées SnapCenter pour cette opération de sauvegarde.
4. SnapCenter déclenche un point de sauvegarde global synchronisé SAP HANA pour créer une image de base de données cohérente sur la couche de persistance.

> Pour un système SAP HANA MDC à un ou plusieurs locataires, un point de sauvegarde global synchronisé est créé pour la base de données du système et pour chaque base de données des locataires.

5. SnapCenter crée des copies Snapshot de stockage pour tous les volumes de données configurés pour la ressource. Dans notre exemple de base de données HANA à un seul hôte, un seul volume de données est disponible. Une base de données SAP HANA à plusieurs hôtes existe plusieurs volumes de données.
6. SnapCenter enregistre la sauvegarde Snapshot de stockage dans le catalogue des sauvegardes SAP HANA.
7. SnapCenter supprime le point de sauvegarde SAP HANA.
8. SnapCenter démarre une mise à jour de SnapVault ou de SnapMirror pour tous les volumes de données configurés dans la ressource.

> Cette étape s'exécute uniquement si la policy sélectionnée inclut une réplication SnapVault ou SnapMirror.

9. SnapCenter supprime les copies Snapshot de stockage et les entrées de sauvegarde dans sa base de données, ainsi que dans le catalogue de sauvegardes SAP HANA, en fonction de la règle de conservation définie pour les sauvegardes sur le stockage primaire. Les opérations du catalogue de sauvegardes HANA

sont effectuées pour la base de données système et tous les locataires.

> Si la sauvegarde est toujours disponible dans le stockage secondaire, l'entrée du catalogue SAP HANA n'est pas supprimée.

10. SnapCenter supprime toutes les sauvegardes des journaux du système de fichiers et du catalogue de sauvegardes SAP HANA antérieures à la sauvegarde de données la plus ancienne identifiée dans le catalogue de sauvegardes SAP HANA. Ces opérations sont effectuées pour la base de données du système et tous les locataires.

> Cette étape est exécutée uniquement si le nettoyage de la sauvegarde des journaux n'est pas désactivé.

Flux de production de sauvegarde pour les opérations de vérification de l'intégrité des blocs

SnapCenter exécute le contrôle d'intégrité des blocs dans l'ordre suivant :

1. SnapCenter lit la liste des locataires de la base de données HANA.
2. SnapCenter déclenche une opération de sauvegarde basée sur des fichiers pour la base de données système et chaque locataire.
3. SnapCenter supprime les sauvegardes basées sur des fichiers de sa base de données, dans le système de fichiers et dans le catalogue de sauvegardes SAP HANA, en fonction de la règle de conservation définie pour les opérations de vérification de l'intégrité des blocs. La suppression des sauvegardes sur le système de fichiers et les opérations du catalogue de sauvegardes HANA sont effectuées pour la base de données système et tous les locataires.
4. SnapCenter supprime toutes les sauvegardes des journaux du système de fichiers et du catalogue de sauvegardes SAP HANA antérieures à la sauvegarde de données la plus ancienne identifiée dans le catalogue de sauvegardes SAP HANA. Ces opérations sont effectuées pour la base de données du système et tous les locataires.

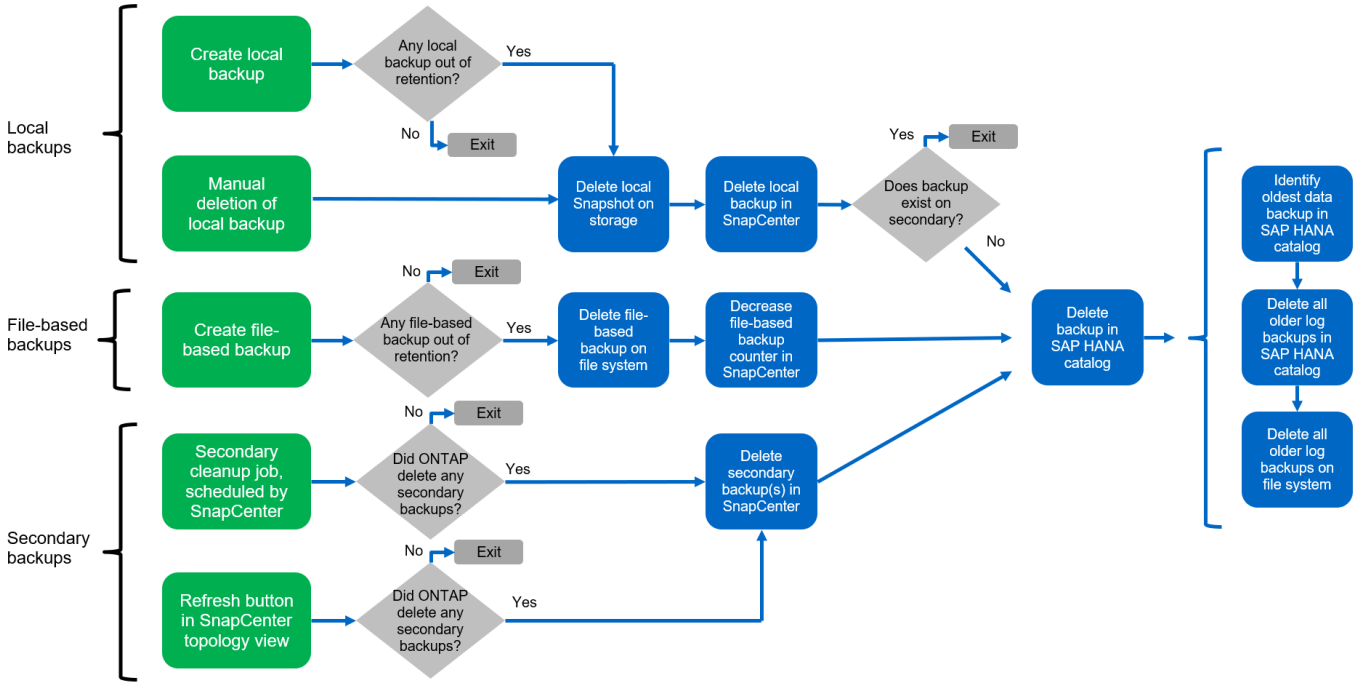
> Cette étape est exécutée uniquement si le nettoyage de la sauvegarde des journaux n'est pas désactivé.

Gestion de la conservation des sauvegardes et organisation des sauvegardes des données et des journaux

La gestion de la conservation des sauvegardes de données et le nettoyage des sauvegardes de journaux peuvent être divisés en cinq domaines, notamment la gestion de la conservation de :

- Sauvegardes locales sur le système de stockage primaire
- Sauvegardes basées sur des fichiers
- Sauvegardes sur le système de stockage secondaire
- Sauvegardes de données dans le catalogue de sauvegardes SAP HANA
- Sauvegardes des journaux dans le catalogue de sauvegardes SAP HANA et dans le système de fichiers

La figure suivante présente les différents flux de travail et les dépendances de chaque opération. Les sections suivantes décrivent en détail les différentes opérations.



Gestion de la conservation des sauvegardes locales sur le stockage primaire

SnapCenter gère l'organisation des sauvegardes de bases de données SAP HANA et des sauvegardes sans volume de données en supprimant les copies Snapshot sur le stockage primaire et dans le référentiel SnapCenter conformément à la règle de sauvegarde SnapCenter.

La logique de gestion de la conservation est exécutée avec chaque workflow de sauvegarde dans SnapCenter.

Notez que SnapCenter gère la gestion de la conservation de façon individuelle pour les sauvegardes planifiées et à la demande.

Les sauvegardes locales sur le stockage primaire peuvent également être supprimées manuellement dans SnapCenter.

Gestion de la conservation des sauvegardes basées sur des fichiers

SnapCenter gère l'organisation des sauvegardes basées sur des fichiers en supprimant les sauvegardes du système de fichiers conformément à la conservation définie dans la règle de sauvegarde de SnapCenter.

La logique de gestion de la conservation est exécutée avec chaque workflow de sauvegarde dans SnapCenter.

Notez que SnapCenter gère la gestion de la conservation de façon individuelle pour les sauvegardes planifiées ou à la demande.

Gestion de la conservation des sauvegardes sur le système de stockage secondaire

La gestion de la conservation des sauvegardes sur le stockage secondaire est gérée par ONTAP en fonction de la conservation définie dans la relation de protection ONTAP.

Pour synchroniser ces modifications sur le stockage secondaire du référentiel SnapCenter, SnapCenter utilise

une tâche de nettoyage planifiée. Cette tâche de nettoyage synchronise l'ensemble des sauvegardes de stockage secondaire avec le référentiel SnapCenter pour tous les plug-ins SnapCenter et toutes les ressources.

La tâche de nettoyage est planifiée une fois par semaine par défaut. Ce planning hebdomadaire génère un délai de suppression des sauvegardes dans SnapCenter et SAP HANA Studio par rapport aux sauvegardes qui ont déjà été supprimées sur le système de stockage secondaire. Pour éviter ces incohérences, les clients peuvent modifier le calendrier à une fréquence plus élevée, par exemple, une fois par jour.

> La tâche de nettoyage peut également être déclenchée manuellement pour une ressource individuelle en cliquant sur le bouton d'actualisation dans la vue topologique de la ressource.

Pour plus d'informations sur l'adaptation du planning du travail de nettoyage ou sur le déclenchement d'une actualisation manuelle, reportez-vous à la section ""Modification de la fréquence de synchronisation des sauvegardes avec le stockage de sauvegarde hors site.""

Gestion de la conservation des sauvegardes de données dans le catalogue des sauvegardes SAP HANA

Lorsque SnapCenter a supprimé des sauvegardes, des copies Snapshot locales ou des fichiers, ou identifié la suppression de la sauvegarde sur le stockage secondaire, cette sauvegarde de données est également supprimée dans le catalogue de sauvegardes SAP HANA.

Avant de supprimer l'entrée du catalogue SAP HANA pour une sauvegarde Snapshot locale sur le stockage primaire, SnapCenter vérifie si la sauvegarde existe toujours au niveau du stockage secondaire.

Gestion de la conservation des sauvegardes des journaux

La base de données SAP HANA crée automatiquement des sauvegardes de journaux. Cette sauvegarde de journaux exécute la création de fichiers de sauvegarde pour chaque service SAP HANA individuel dans un répertoire de sauvegarde configuré dans SAP HANA.

Les sauvegardes de journaux antérieures à la dernière sauvegarde de données ne sont plus nécessaires pour la restauration avant et peuvent donc être supprimées.

SnapCenter gère l'organisation des sauvegardes des fichiers journaux au niveau du système de fichiers ainsi que dans le catalogue de sauvegardes SAP HANA en exécutant la procédure suivante :

1. SnapCenter lit le catalogue de sauvegardes SAP HANA pour obtenir l'ID de sauvegarde des sauvegardes Snapshot ou basées sur des fichiers les plus anciennes.
2. SnapCenter supprime toutes les sauvegardes des journaux du catalogue SAP HANA et du système de fichiers antérieures à cet ID de sauvegarde.

> SnapCenter gère uniquement les sauvegardes qui ont été créées par SnapCenter, Si des sauvegardes supplémentaires basées sur des fichiers sont créées en dehors de SnapCenter, vous devez vous assurer que les sauvegardes basées sur des fichiers sont supprimées du catalogue de sauvegardes. Si une telle sauvegarde de données n'est pas supprimée manuellement du catalogue de sauvegardes, elle peut devenir la sauvegarde de données la plus ancienne et les anciennes sauvegardes de journaux ne sont pas supprimées tant que cette sauvegarde basée sur des fichiers n'est pas supprimée.

Même si une conservation est définie pour des sauvegardes à la demande dans la configuration de règles, l'organisation des données n'est effectuée que lorsqu'une autre sauvegarde à la demande est exécutée. Par conséquent, les sauvegardes à la demande doivent généralement être supprimées manuellement dans SnapCenter afin d'être certain que ces sauvegardes sont également supprimées dans le catalogue de sauvegardes SAP HANA, et que les services de gestion des sauvegardes de journaux ne reposent pas sur une sauvegarde à la demande trop ancienne.

La gestion de la conservation des sauvegardes de journaux est activée par défaut. Si nécessaire, il peut être désactivé comme décrit dans la section ""Désactiver la détection automatique sur l'hôte du plug-in HANA.""

Besoins de stockage pour les sauvegardes Snapshot

La vitesse de modification des blocs sur la couche de stockage est supérieure par rapport aux bases de données classiques. Du fait du processus de fusion de table HANA du magasin de colonnes, le tableau complet est écrit sur le disque, et pas uniquement les blocs modifiés.

Les données de notre base client montrent un taux de modification quotidien compris entre 20 et 50 % si plusieurs sauvegardes Snapshot sont effectuées pendant la journée. Sur la cible SnapVault, si la réplication n'est effectuée qu'une seule fois par jour, le taux de modification quotidien est généralement inférieur.

Les opérations de restauration et de reprise

Restaurez les opérations avec SnapCenter

Pour la base de données HANA, SnapCenter prend en charge deux opérations de restauration différentes.

- **Restauration de la ressource complète.** toutes les données du système HANA sont restaurées. Si le système HANA contient un ou plusieurs locataires, les données de la base de données système et les données de tous les locataires sont restaurées.
- **Restauration d'un seul locataire.** seules les données du locataire sélectionné sont restaurées.

Du point de vue du stockage, les opérations de restauration ci-dessus doivent être exécutées de façon différente selon le protocole de stockage utilisé (NFS ou SAN Fibre Channel), la protection des données configurée (stockage primaire avec ou sans stockage de sauvegarde hors site), et la sauvegarde sélectionnée à utiliser pour l'opération de restauration (restauration à partir du stockage de sauvegarde primaire ou hors site).

Restauration de l'ensemble des ressources à partir du stockage primaire

Lors de la restauration de la ressource complète à partir du stockage primaire, SnapCenter prend en charge deux fonctionnalités ONTAP différentes pour exécuter l'opération de restauration. Vous pouvez choisir entre les deux fonctions suivantes :

- **SnapRestore basé sur les volumes.** Une SnapRestore basée sur les volumes restaure le contenu du volume de stockage à l'état de la sauvegarde Snapshot sélectionnée.
  - Case à cocher Revert de volume disponible pour les ressources détectées automatiquement via NFS.
  - Cliquez sur le bouton radio ressource pour accéder aux ressources configurées manuellement.
- **SnapRestore basé sur les fichiers.** SnapRestore basé sur les fichiers, également appelé SnapRestore de fichier unique, restaure tous les fichiers individuels (NFS) ou tous les LUN (SAN).
  - Méthode de restauration par défaut pour les ressources découvertes automatiquement. Il est possible de modifier des volumes à l'aide de la case à cocher Volume revert pour NFS.

◦ Bouton radio de niveau fichier pour les ressources configurées manuellement.

Le tableau suivant compare les différentes méthodes de restauration.

	SnapRestore basée sur les volumes	SnapRestore basé sur fichiers
Vitesse de la restauration	Très rapide, indépendant de la taille du volume	Opération de restauration très rapide, mais utilise des tâches de copie en arrière-plan sur le système de stockage qui bloquent la création de nouvelles sauvegardes Snapshot
Historique des sauvegardes Snapshot	Restaurez vos données vers une ancienne sauvegarde Snapshot et supprimez toutes les sauvegardes Snapshot les plus récentes.	Aucune influence
Restauration de la structure du répertoire	La structure du répertoire est également restaurée	NFS : restaure uniquement les fichiers individuels, pas la structure de répertoires. Si la structure du répertoire est également perdue, elle doit être créée manuellement avant d'exécuter l'opération de restauration SAN : la structure du répertoire est également restaurée
Ressource configurée avec réplication sur un stockage de sauvegarde hors site	Aucune restauration basée sur les volumes ne peut être effectuée vers une sauvegarde de copie Snapshot antérieure à la copie Snapshot utilisée pour la synchronisation SnapVault	Toutes les sauvegardes Snapshot peuvent être sélectionnées

Restauration de l'ensemble des ressources à partir d'un stockage de sauvegarde hors site

Une restauration à partir du stockage de sauvegarde hors site est toujours exécutée à partir d'une opération de restauration SnapVault, où tous les fichiers ou toutes les LUN du volume de stockage sont remplacés par le contenu de la sauvegarde Snapshot.

Restauration d'un seul locataire

La restauration d'un seul locataire requiert une opération de restauration basée sur les fichiers. En fonction du protocole de stockage utilisé, différents flux de restauration sont exécutés par SnapCenter.

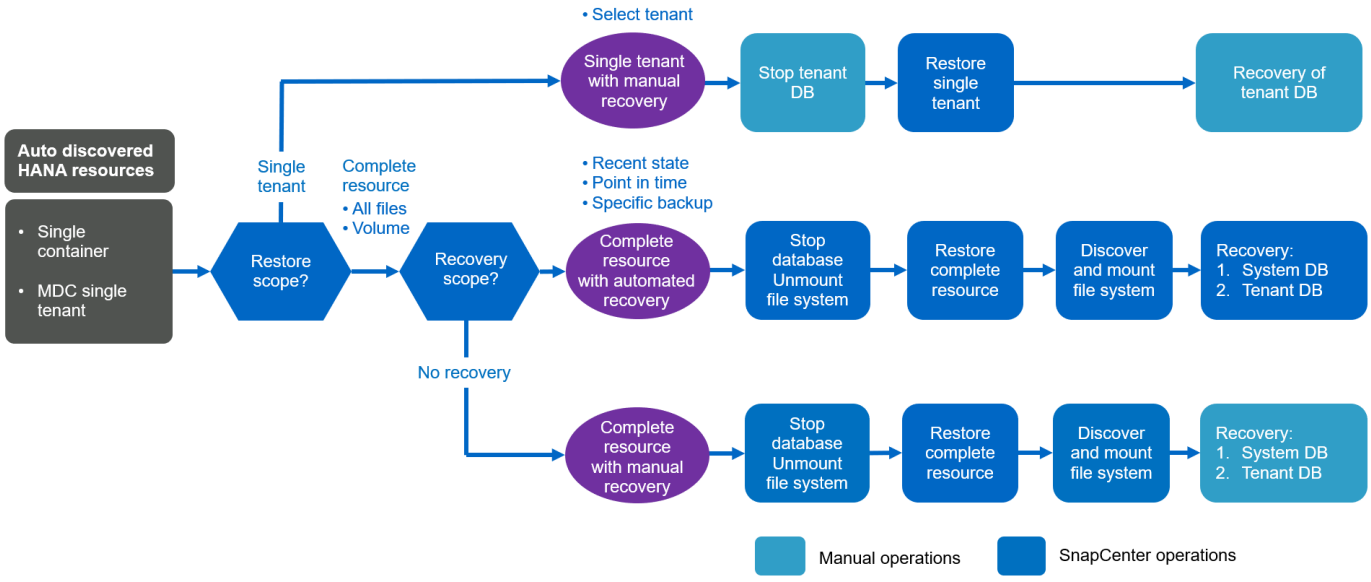
- NFS :
  - Le stockage primaire Les opérations SnapRestore basées sur des fichiers sont exécutées pour tous les fichiers de la base de données des locataires.
  - Stockage de sauvegarde hors site : les opérations de restauration SnapVault sont exécutées pour tous les fichiers de la base de données des locataires.
- SAN :
  - Le stockage primaire Clonez et connectez le LUN à l'hôte de base de données, puis copiez tous les fichiers de la base de données du locataire.

- Stockage de sauvegarde hors site. Clonez et connectez le LUN à l'hôte de base de données, puis copiez tous les fichiers de la base de données du locataire.

Restauration et restauration des systèmes de conteneur unique HANA et MDC automatiquement découverts

Les systèmes à un seul conteneur HANA et MDC HANA qui ont été découverts automatiquement sont activés pour la restauration et la restauration automatisées avec SnapCenter. Pour ces systèmes HANA, SnapCenter prend en charge trois workflows de restauration et de restauration différents, comme illustré dans la figure suivante :

- **Locataire unique avec récupération manuelle.** si vous sélectionnez une opération de restauration locataire unique, SnapCenter répertorie tous les locataires inclus dans la sauvegarde Snapshot sélectionnée. Vous devez arrêter et restaurer manuellement la base de données des locataires. L'opération de restauration avec SnapCenter est effectuée avec des opérations de copie SnapRestore de fichiers uniques pour les environnements NFS ou de clonage, de montage et de copie.
- **Ressource complète avec récupération automatisée.** si vous sélectionnez une opération complète de restauration des ressources et de récupération automatisée, le flux de travail complet est automatisé avec SnapCenter. SnapCenter prend en charge des opérations de restauration ponctuelles, ponctuelles ou bien spécifiques aux sauvegardes. L'opération de restauration sélectionnée est utilisée pour le système et la base de données des locataires.
- **Ressource complète avec récupération manuelle.** si vous sélectionnez pas de récupération, SnapCenter arrête la base de données HANA et exécute les opérations de restauration et de démontage du système de fichiers requis. Vous devez restaurer manuellement la base de données du système et des locataires.

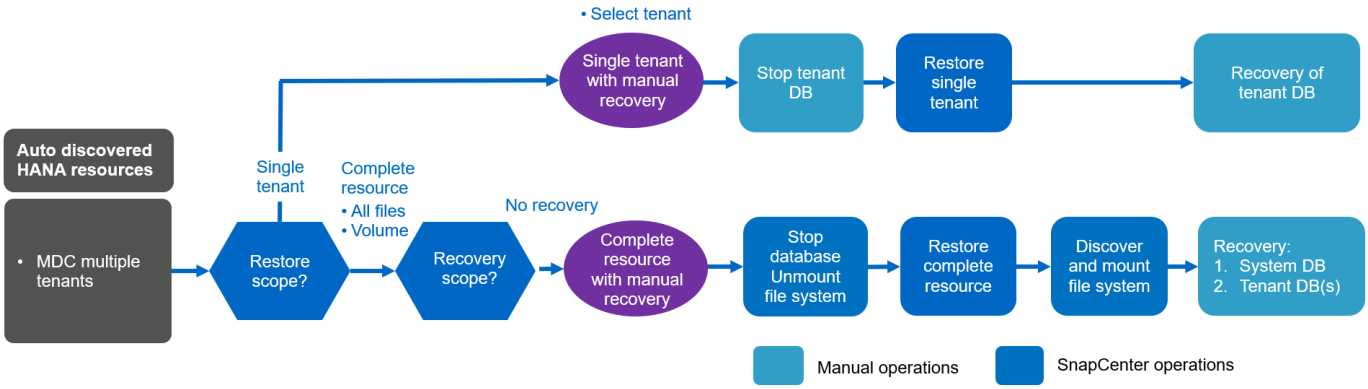


Restauration et restauration des systèmes multilocataires HANA MDC automatiquement découverts

Même si les systèmes MDC HANA avec plusieurs locataires sont automatiquement découverts, la restauration et la restauration automatisées ne sont pas prises en charge pour la version actuelle de SnapCenter. Pour les systèmes MDC comptant plusieurs locataires, SnapCenter prend en charge deux flux de travail de restauration et de restauration différents, comme l'illustre la figure suivante :

- Locataire unique avec restauration manuelle
- Ressource complète avec récupération manuelle

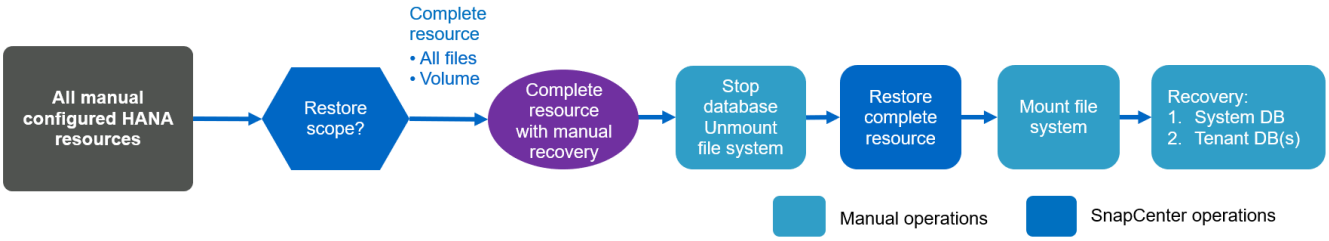
Les flux de travail sont les mêmes que ceux décrits dans la section précédente.



Restauration et restauration des ressources HANA configurées manuellement

Les ressources HANA configurées manuellement ne sont pas activées pour la restauration et la restauration automatisées. En outre, pour les systèmes MDC avec un ou plusieurs locataires, une opération de restauration de locataire unique n'est pas prise en charge.

Pour les ressources HANA configurées manuellement, SnapCenter prend uniquement en charge la restauration manuelle, comme illustré dans la figure suivante. Le flux de travail pour la récupération manuelle est le même que celui décrit dans les sections précédentes.



Récapitulatif des opérations de restauration et de reprise

Le tableau suivant résume les opérations de restauration et de reprise selon la configuration des ressources HANA dans SnapCenter.

Configuration des ressources SnapCenter	Options de restauration et de récupération	Arrêtez la base de données HANA	Démontez-le avant, montez-le après l'opération de restauration	Opération de reprise
Découverte automatique d'un seul tenant MDC pour conteneur	• Compléter la ressource avec l'un ou l'autre • Par défaut (tous les fichiers) • Restauration des volumes (NFS depuis le stockage primaire uniquement) • Restauration automatique sélectionnée	Automatisation avec SnapCenter	Automatisation avec SnapCenter	Automatisation avec SnapCenter
	• Compléter la ressource avec l'un ou l'autre • Par défaut (tous les fichiers) • Restauration des volumes (NFS depuis le stockage primaire uniquement) • Aucune restauration sélectionnée	Automatisation avec SnapCenter	Automatisation avec SnapCenter	Manuel
	• Restauration des locataires	Manuel	Non requis	Manuel

Configuration des ressources SnapCenter	Options de restauration et de récupération	Arrêtez la base de données HANA	Démontez-le avant, montez-le après l'opération de restauration	Opération de reprise
Découverte automatique de plusieurs locataires MDC	• Compléter la ressource avec l'un ou l'autre • Par défaut (tous les fichiers) • Restauration des volumes (NFS depuis le stockage primaire uniquement) • Restauration automatisée non prise en charge	Automatisation avec SnapCenter	Automatisation avec SnapCenter	Manuel
	• Restauration des locataires	Manuel	Non requis	Manuel
Toutes les ressources configurées manuellement	• Ressource complète (= restauration de volume, disponible uniquement pour les protocoles NFS et SAN à partir du stockage primaire) • Niveau fichier (tous les fichiers) • Restauration automatisée non prise en charge	Manuel	Manuel	Manuel

Configuration de laboratoire utilisée pour ce rapport

Le rapport technique utilisé pour la configuration de laboratoire inclut cinq configurations SAP HANA différentes :

- **MS1.**
  - Système mutualisé multi-hôte MDC SAP HANA

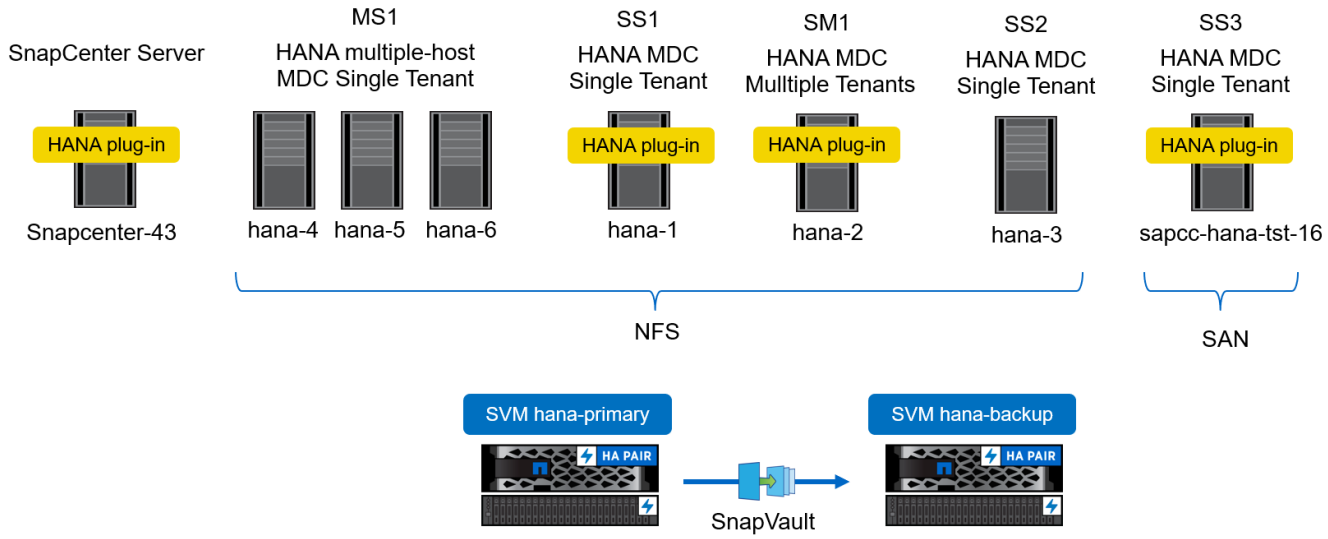
- Gestion avec un hôte plug-in central (serveur SnapCenter)
- Utilise NFS comme protocole de stockage

- **SS1.**
  - Système locataire unique MDC à hôte unique SAP HANA
  - Découverte automatique avec le plug-in HANA installé sur l'hôte de base de données HANA
  - Utilise NFS comme protocole de stockage
- **SM1.**
  - Système multitenant MDC à hôte unique SAP HANA
  - Découverte automatique avec le plug-in HANA installé sur l'hôte de base de données HANA
  - Utilise NFS comme protocole de stockage
- **SS2.**
  - Système locataire unique MDC à hôte unique SAP HANA
  - Gestion avec un hôte plug-in central (SnapCenter Server)
  - Utilise NFS comme protocole de stockage
- **SS3.**
  - Système locataire unique MDC à hôte unique SAP HANA
  - Découverte automatique avec le plug-in HANA installé sur l'hôte de base de données HANA
  - Utilise SAN Fibre Channel comme protocole de stockage

Les sections suivantes décrivent la configuration complète et les flux de travail de sauvegarde, de restauration et de récupération. Cette description couvre les sauvegardes Snapshot locales, ainsi que la réplication sur le stockage de sauvegarde via SnapVault. Les serveurs virtuels de stockage sont les serveurs virtuels `hana-primary` pour le stockage primaire et `hana-backup` pour le stockage de sauvegarde hors site.

Le serveur SnapCenter est utilisé en tant qu'hôte de plug-in HANA central pour les systèmes HANA MS1 et SS2.

La figure suivante illustre la configuration du laboratoire.

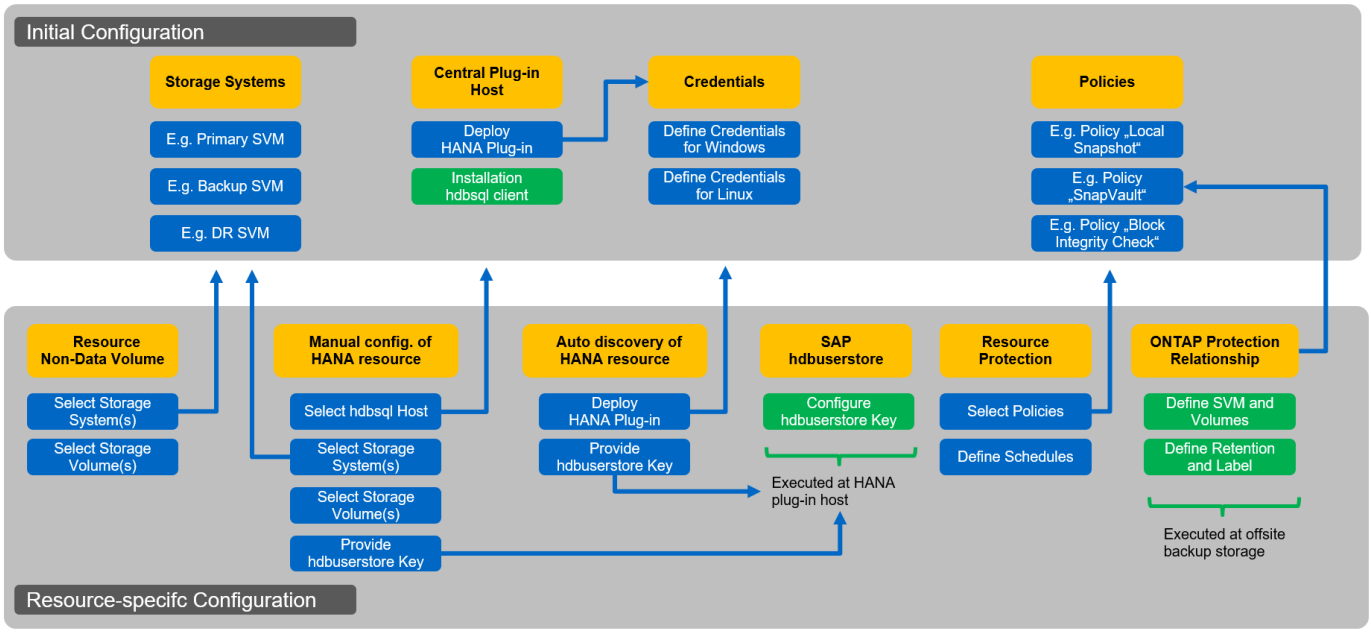


Configuration SnapCenter

La configuration SnapCenter peut être séparée en deux zones principales :

- **Configuration initiale.** couvre les configurations génériques, indépendamment d'une base de données SAP HANA individuelle. Configurations telles que les systèmes de stockage, les hôtes du plug-in HANA central et les règles, sélectionnées lors de l'exécution des configurations spécifiques aux ressources.
- **Configuration spécifique à une ressource.** couvre les configurations propres au système SAP HANA et doit être effectuée pour chaque base de données SAP HANA.

La figure suivante présente les composants de configuration et leurs dépendances. Les cases vertes indiquent les étapes de configuration à effectuer en dehors de SnapCenter ; les cases bleues indiquent les étapes à suivre à l'aide de l'interface graphique de SnapCenter.



Avec la configuration initiale, les composants suivants sont installés et configurés :

- **Système de stockage.** Configuration des informations d'identification pour tous les SVM utilisés par les systèmes SAP HANA : en général, sauvegarde primaire, hors site et stockage de reprise après incident.

> Les identifiants du cluster de stockage peuvent également être configurés à la place des identifiants SVM individuels.

- **Informations d'identification.** Configuration des informations d'identification utilisées pour déployer le plug-in SAP HANA sur les hôtes.
- **Hôtes (pour hôtes du plug-in HANA central).** déploiement du plug-in SAP HANA. Installation du logiciel SAP HANA hdbclient sur l'hôte. Le logiciel hdbclient SAP doit être installé manuellement.
- **Stratégies.** Configuration du type de sauvegarde, de la conservation et de la réplication. Généralement, au moins une règle pour les copies Snapshot locales, une pour la réplication SnapVault et une autre pour la sauvegarde basée sur les fichiers sont requises.

La configuration spécifique aux ressources doit être effectuée pour chaque base de données SAP HANA et inclut les configurations suivantes :

- Configuration des ressources sans volume de données SAP HANA :
  - Systèmes de stockage et volumes
- Configuration des clés du magasin de hdbuserStore pour SAP :
  - La configuration de la clé hdbuserstore SAP pour la base de données SAP HANA spécifique doit être effectuée sur l'hôte du plug-in central ou sur l'hôte de la base de données HANA, selon l'endroit où le plug-in HANA est déployé.
- Ressources de base de données SAP HANA découvertes automatiquement :
  - Déploiement du plug-in SAP HANA sur l'hôte de base de données
  - Fournir une clé hdbuserstore
- Configuration manuelle des ressources de base de données SAP HANA :
  - SID de base de données SAP HANA, hôte de plug-in, clé hdbuserstore, systèmes de stockage et volumes
- Configuration de la protection des ressources :
  - Sélection des politiques requises
  - Définition du planning pour chaque règle
- Configuration de protection des données ONTAP :
  - Nécessaire uniquement si les sauvegardes doivent être répliquées sur un stockage de sauvegarde hors site.
  - Définition de la relation et de la conservation.

Configuration initiale de SnapCenter

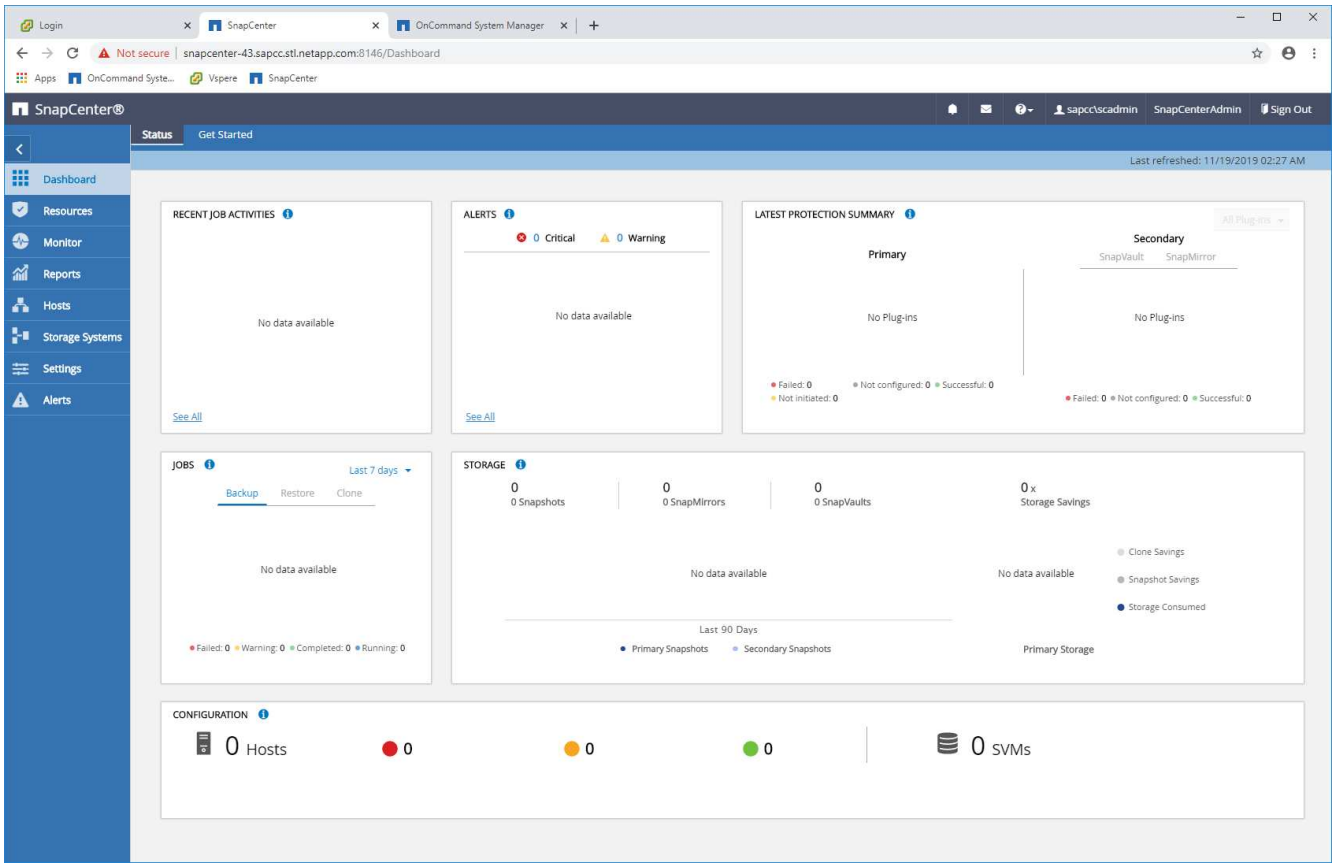
La configuration initiale comprend les étapes suivantes :

1. Configuration du système de stockage
2. Configuration des informations d'identification pour l'installation du plug-in
3. Pour un plug-in HANA central :
   a. Configuration de l'hôte et déploiement du plug-in SAP HANA
   b. Installation et configuration du logiciel client SAP HANA hdbsql
4. Configuration des règles

Les sections suivantes décrivent la procédure de configuration initiale.

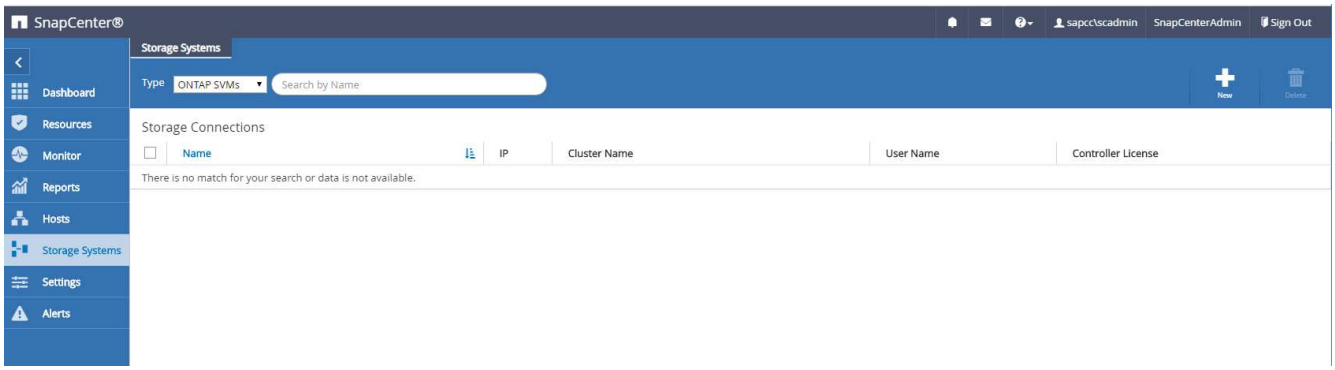
Configuration du système de stockage

1. Connectez-vous à l'interface graphique du serveur SnapCenter.



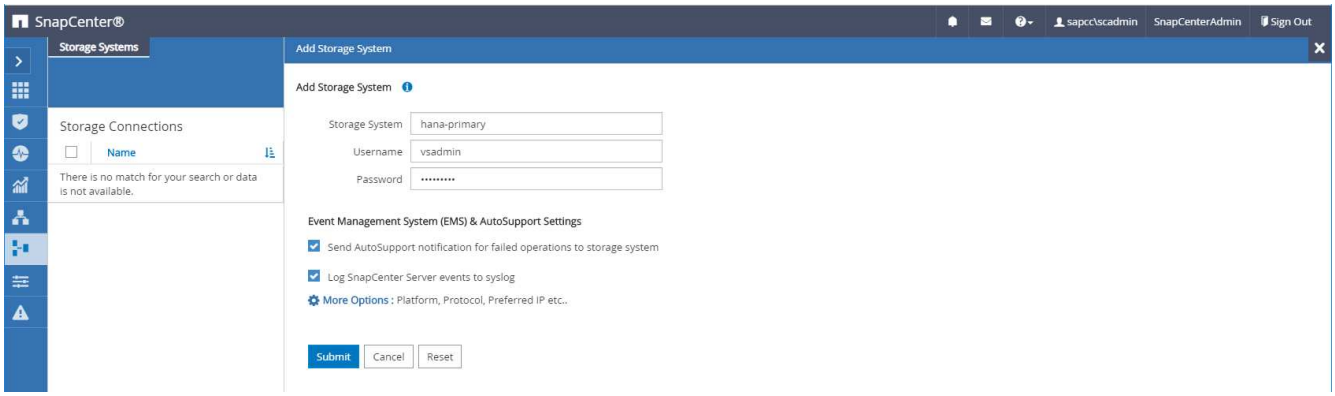
2. Sélectionnez Storage Systems.

À l'écran, vous pouvez sélectionner le type de système de stockage, qui peut être ONTAP SVM ou ONTAP clusters. Si vous configurez les systèmes de stockage au niveau des SVM, vous devez avoir une LIF de gestion configurée pour chaque SVM. Vous pouvez également utiliser l'accès de gestion SnapCenter au niveau du cluster. La gestion de SVM est utilisée dans l'exemple suivant.



3. Cliquez sur Nouveau pour ajouter un système de stockage et fournir le nom d'hôte et les informations d'identification requis.

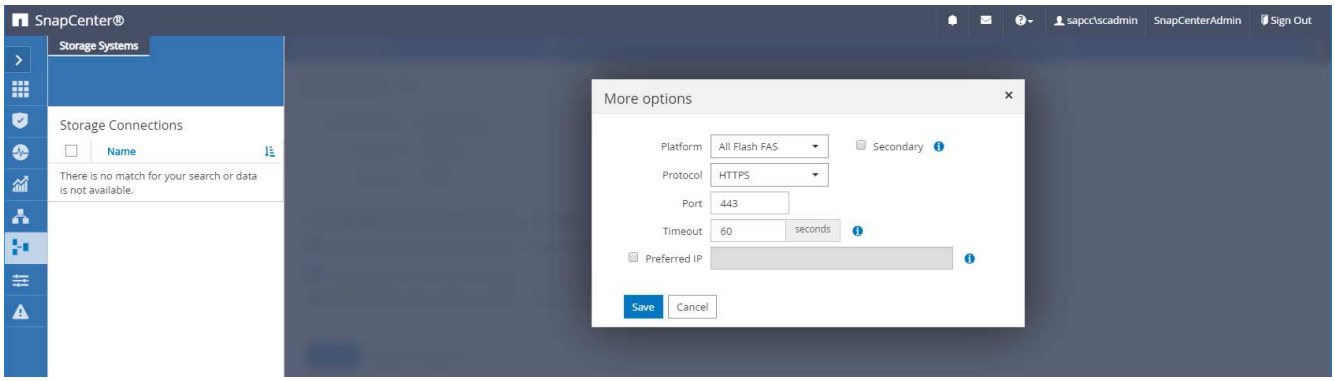
L'utilisateur SVM n'est pas requis pour être l'utilisateur vsadmin, comme indiqué dans la capture d'écran. En général, un utilisateur est configuré sur le SVM et se voit attribuer les autorisations requises pour exécuter les opérations de sauvegarde et de restauration. Pour plus d'informations sur les privilèges requis, consultez le "Guide d'installation de SnapCenter" Dans la section intitulée « privilèges minimum de ONTAP requis ».



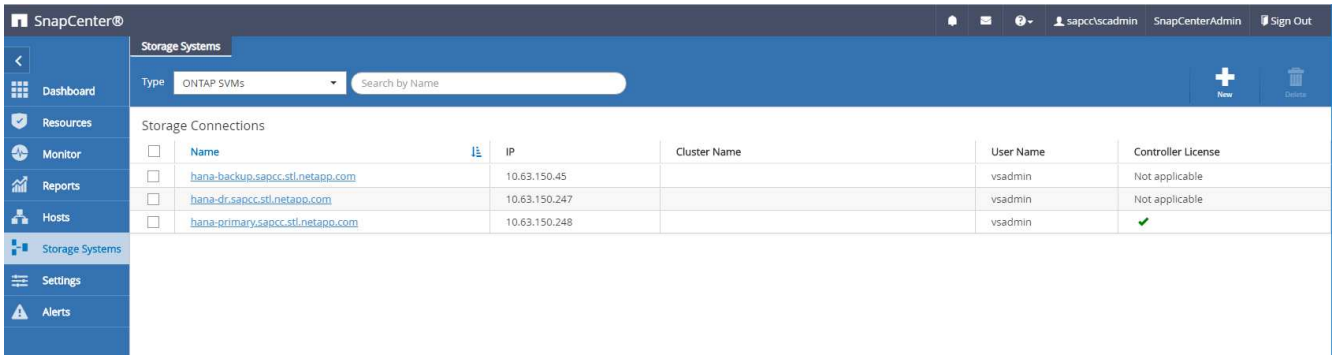
4. Cliquez sur plus d'options pour configurer la plate-forme de stockage.

   La plateforme de stockage peut être FAS, AFF, ONTAP Select ou Cloud Volumes ONTAP.

   Dans le cas d'un système utilisé comme cible SnapVault ou SnapMirror, sélectionner l'icône secondaire.

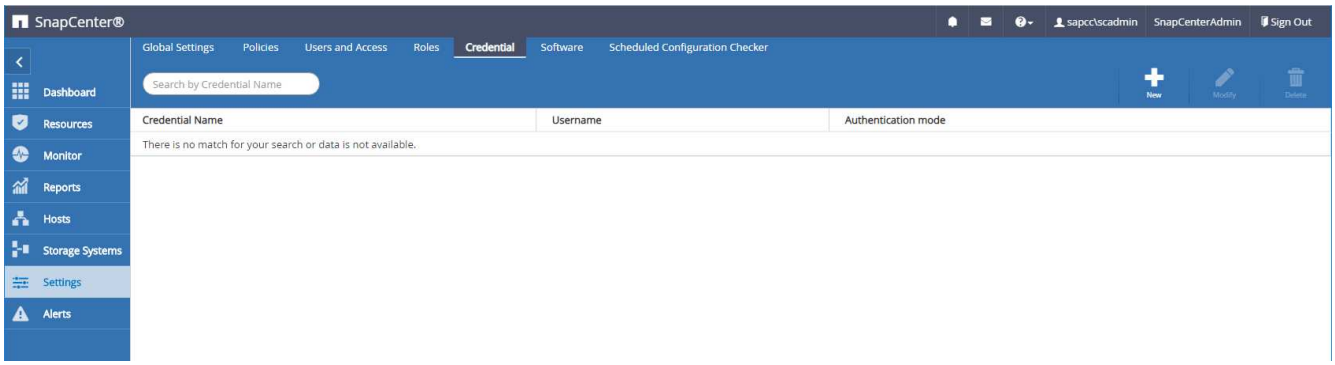


5. Ajoutez des systèmes de stockage supplémentaires selon les besoins. Dans notre exemple, un autre stockage de sauvegarde hors site et un stockage de reprise sur incident ont été ajoutés.

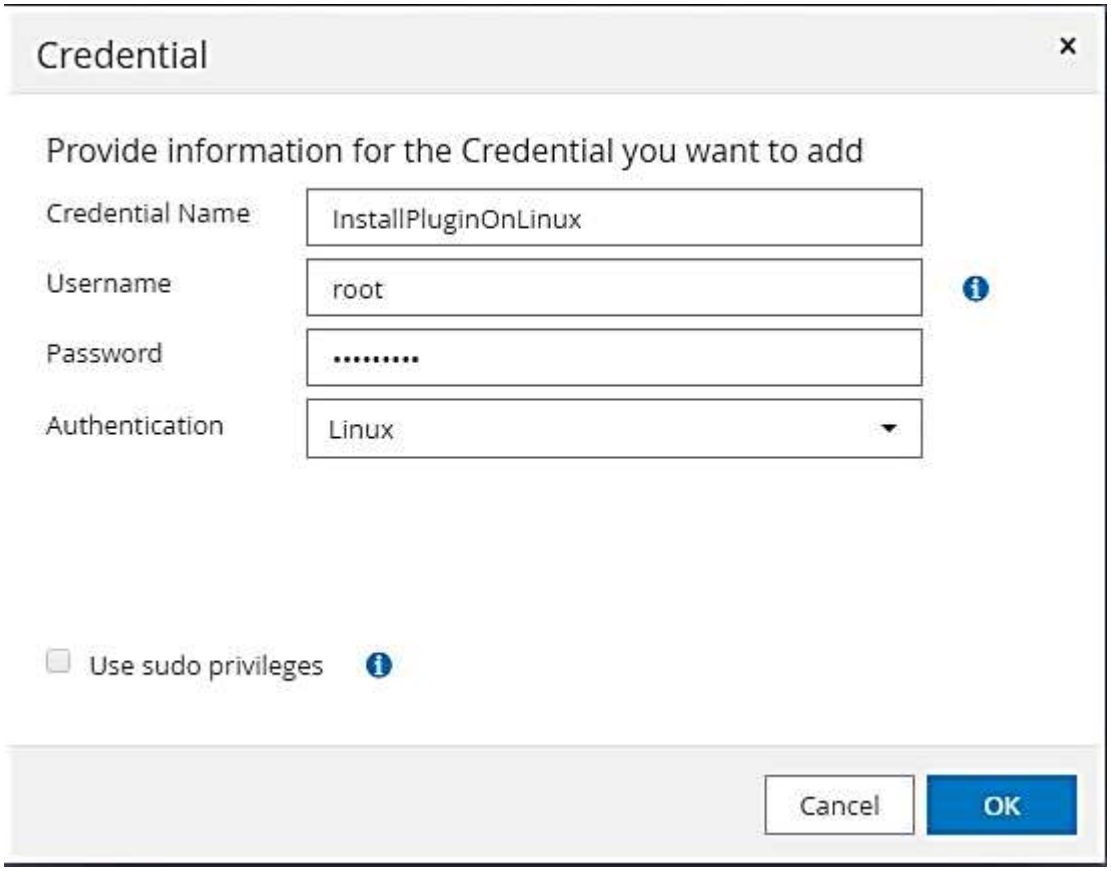


Configuration des identifiants

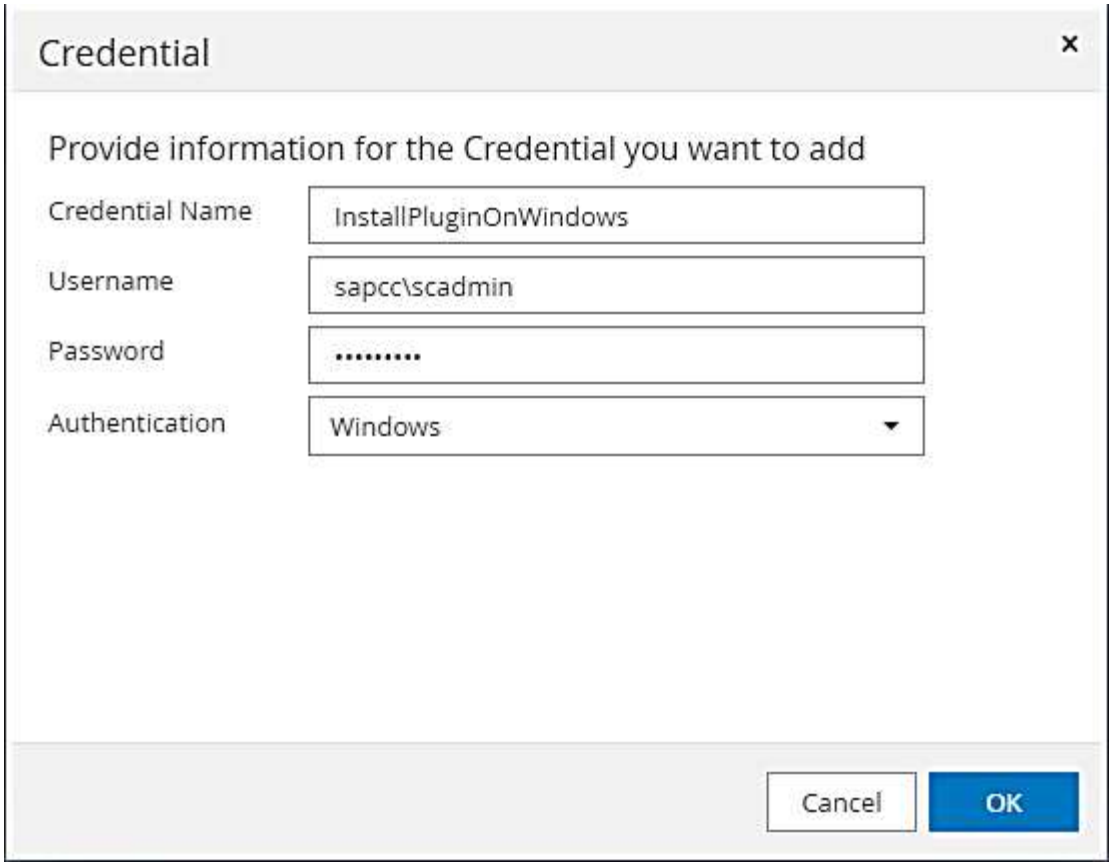
1. Accédez à Paramètres, sélectionnez informations d'identification, puis cliquez sur Nouveau.



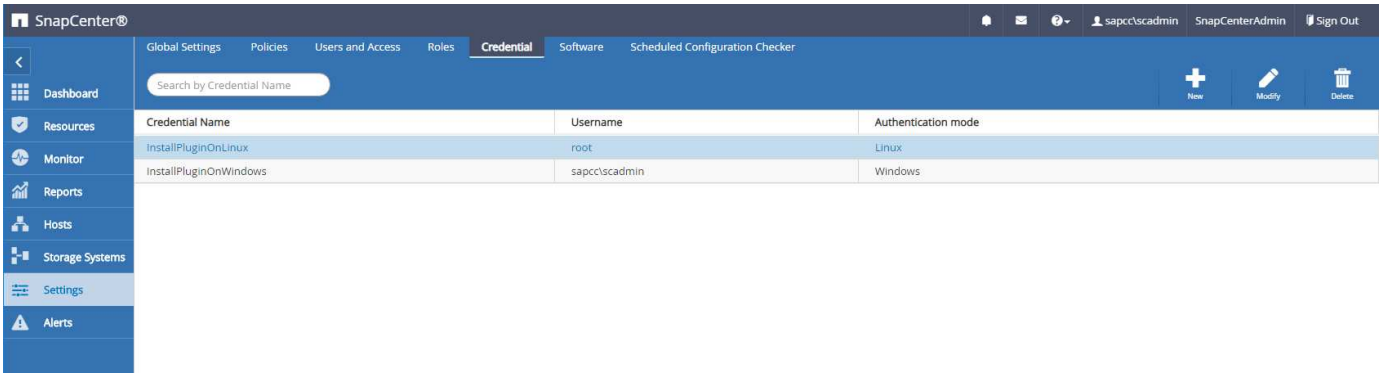
2. Indiquez les informations d'identification de l'utilisateur utilisées pour les installations de plug-in sur les systèmes Linux.



3. Indiquez les informations d'identification de l'utilisateur utilisées pour les installations de plug-in sur les systèmes Windows.



La figure suivante montre les informations d'identification configurées.

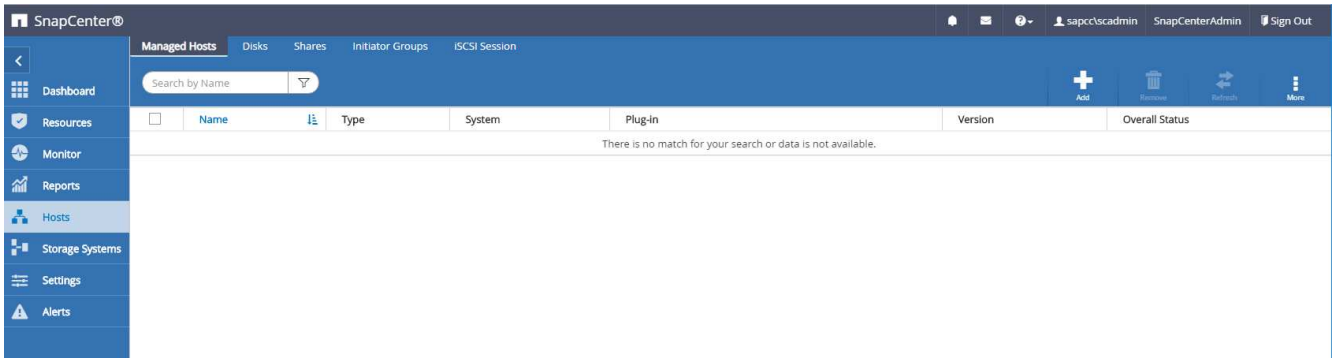


Installation du plug-in SAP HANA sur un hôte plug-in central

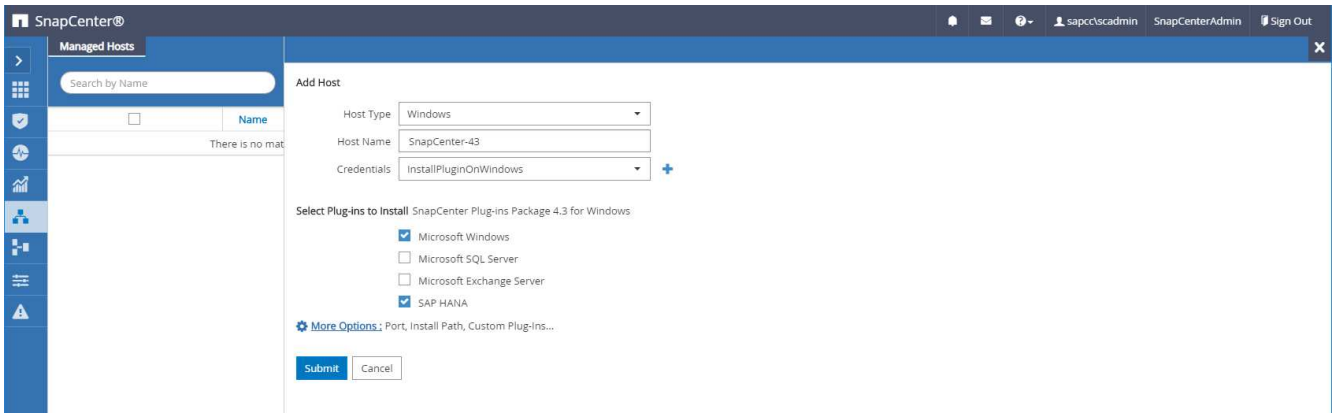
Lors de la configuration en laboratoire, le serveur SnapCenter est également utilisé comme plug-in HANA central. L'hôte Windows sur lequel s'exécute SnapCenter Server est ajouté en tant qu'hôte, et le plug-in SAP HANA est installé sur l'hôte Windows.

Le plug-in SAP HANA requiert Java 64 bits version 1.8. Java doit être installé sur l'hôte avant le déploiement du plug-in SAP HANA.

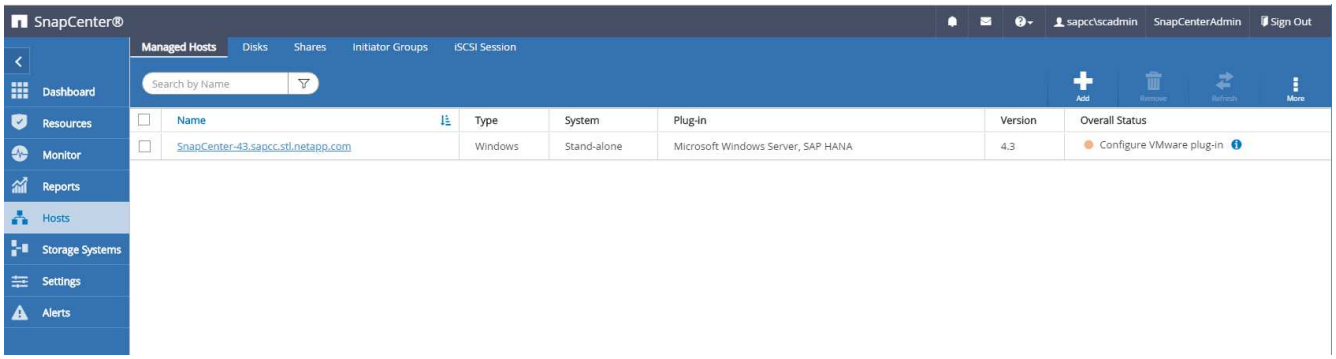
1. Accédez à hosts et cliquez sur Add.



2. Fournissez les informations d'hôte requises. Cliquez sur soumettre.



La figure suivante montre tous les hôtes configurés une fois le plug-in HANA déployé.



Installation et configuration du logiciel client SAP HANA hdbsql

Le logiciel client SAP HANA hdbsql doit être installé sur le même hôte sur lequel le plug-in SAP HANA est installé. Le logiciel peut être téléchargé à partir du "Portail de support SAP".

L'utilisateur HDBSQL OS configuré pendant la configuration de la ressource doit pouvoir exécuter l'exécutable hdbsql. Le chemin d'accès à l'exécutable hdbsql doit être configuré dans l' `hana.properties` fichier.

- Windows :

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

- Linux :

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

Configuration des règles

Comme indiqué dans la section "« Stratégie de protection des données »," Les règles sont généralement configurées indépendamment des ressources et peuvent être utilisées par plusieurs bases de données SAP HANA.

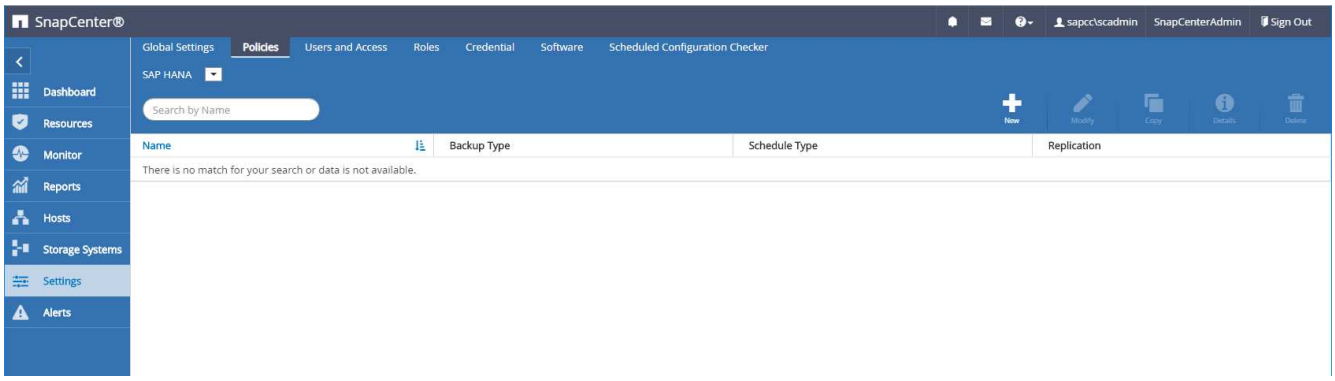
Une configuration minimale typique comprend les règles suivantes :

- Règle pour les sauvegardes horaires sans réplication : `LocalSnap`
- Règle pour les sauvegardes quotidiennes avec réplication SnapVault : `LocalSnapAndSnapVault`
- Règles pour une vérification hebdomadaire de l'intégrité des blocs à l'aide d'une sauvegarde basée sur des fichiers : `BlockIntegrityCheck`

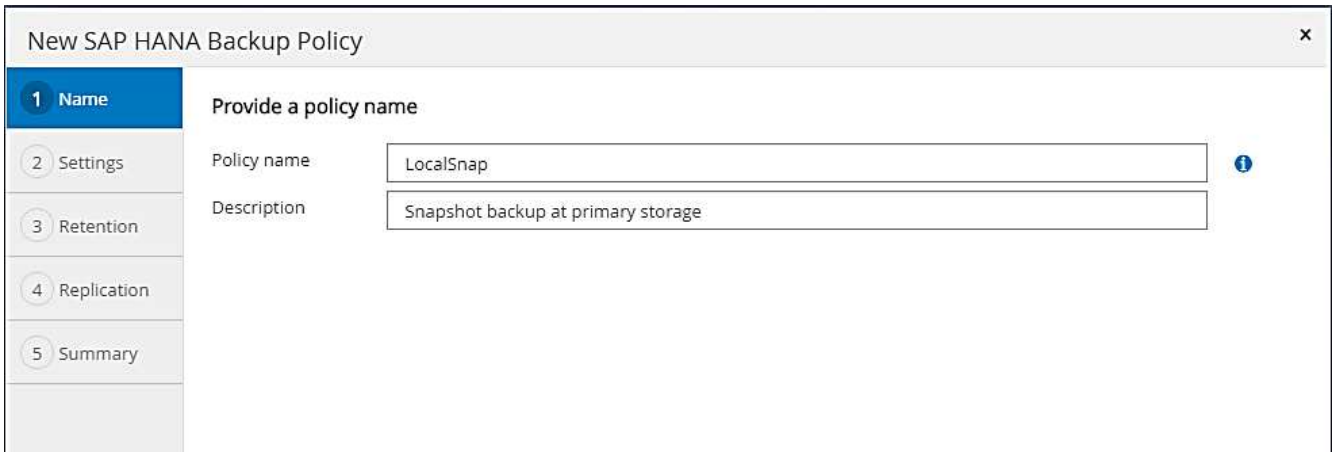
Les sections suivantes décrivent la configuration de ces trois règles.

Règle pour les sauvegardes Snapshot par heure

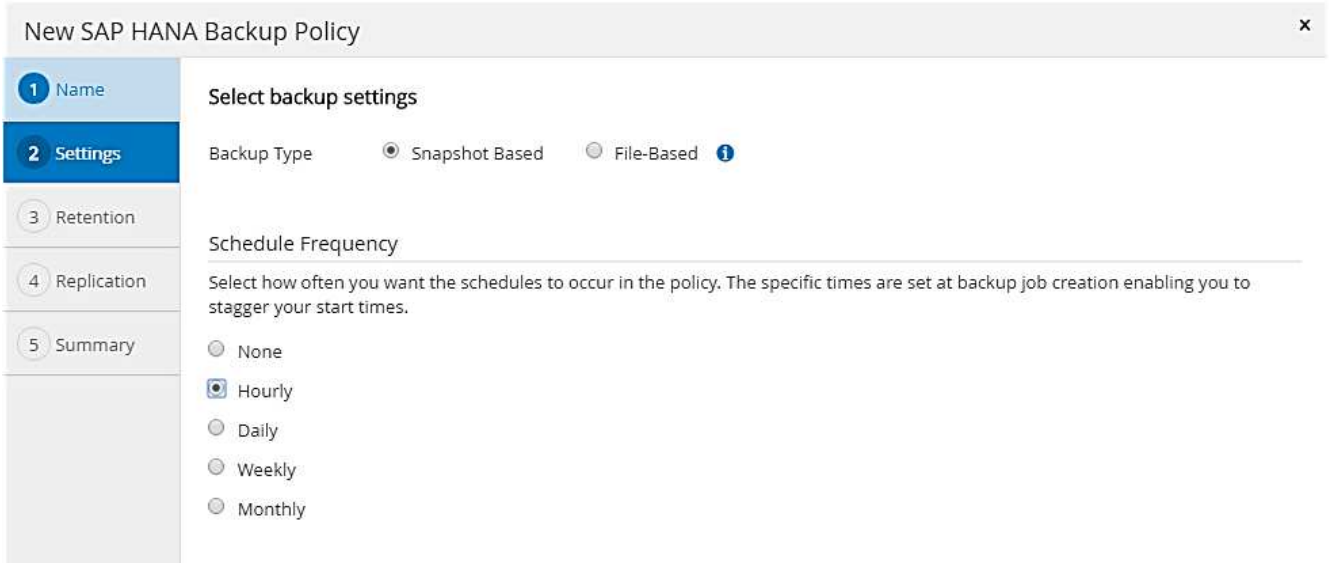
1. Accédez à Paramètres > stratégies et cliquez sur Nouveau.



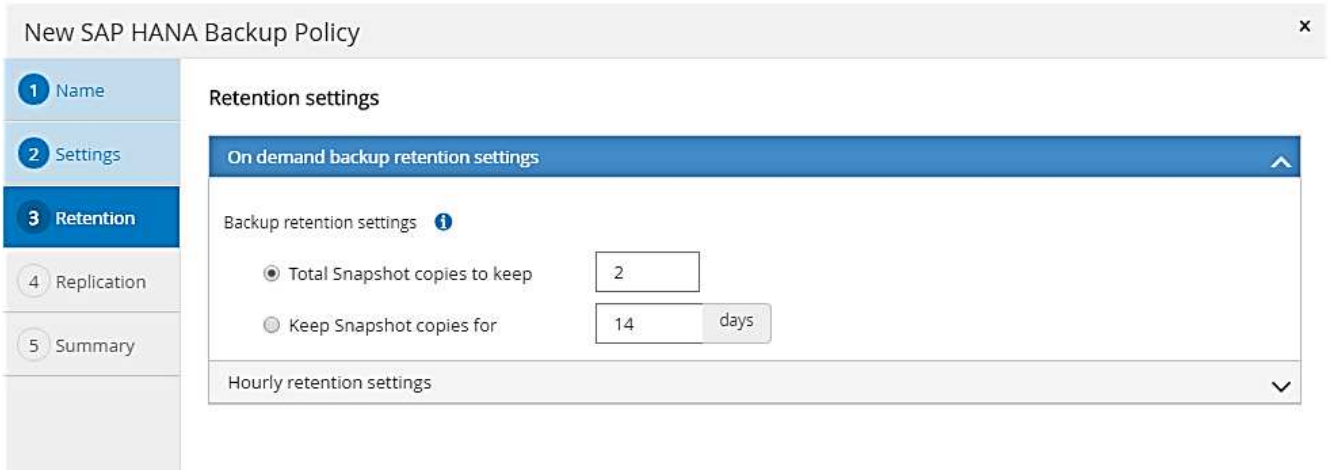
2. Entrez le nom et la description de la stratégie. Cliquez sur Suivant.



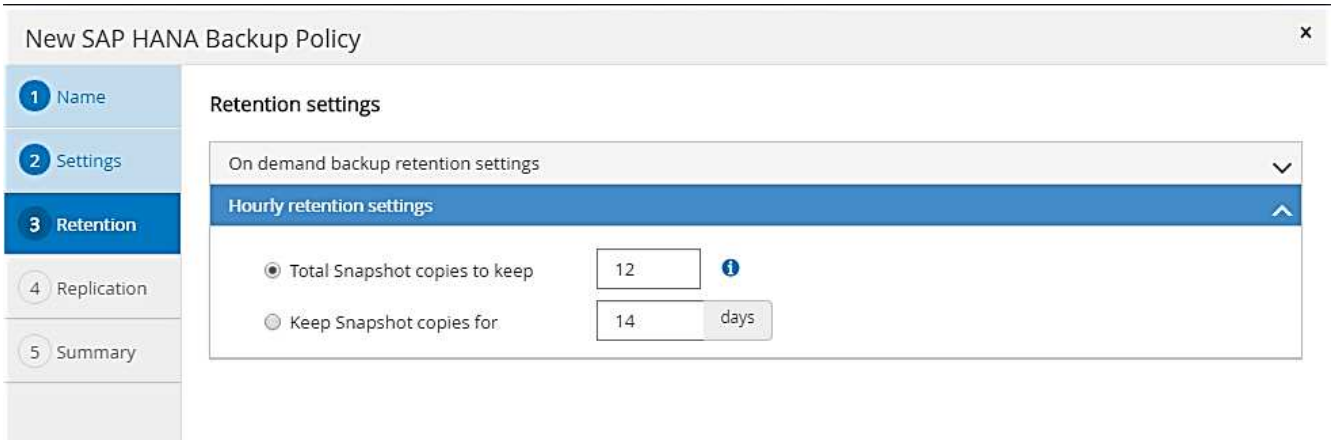
3. Sélectionnez le type de sauvegarde comme basé sur Snapshot et sélectionnez horaire pour la fréquence d'horaire.



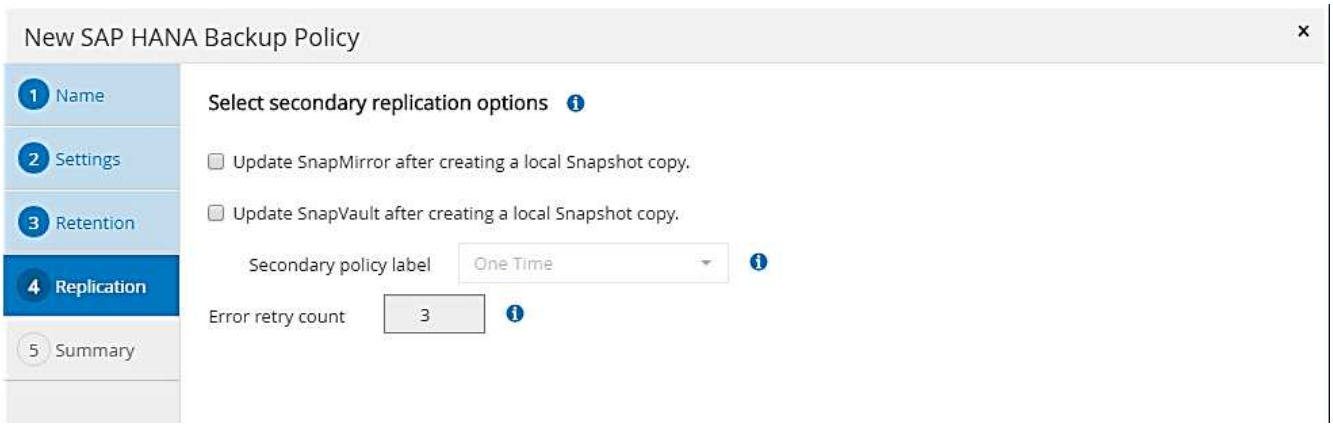
4. Configurez les paramètres de conservation pour les sauvegardes à la demande.



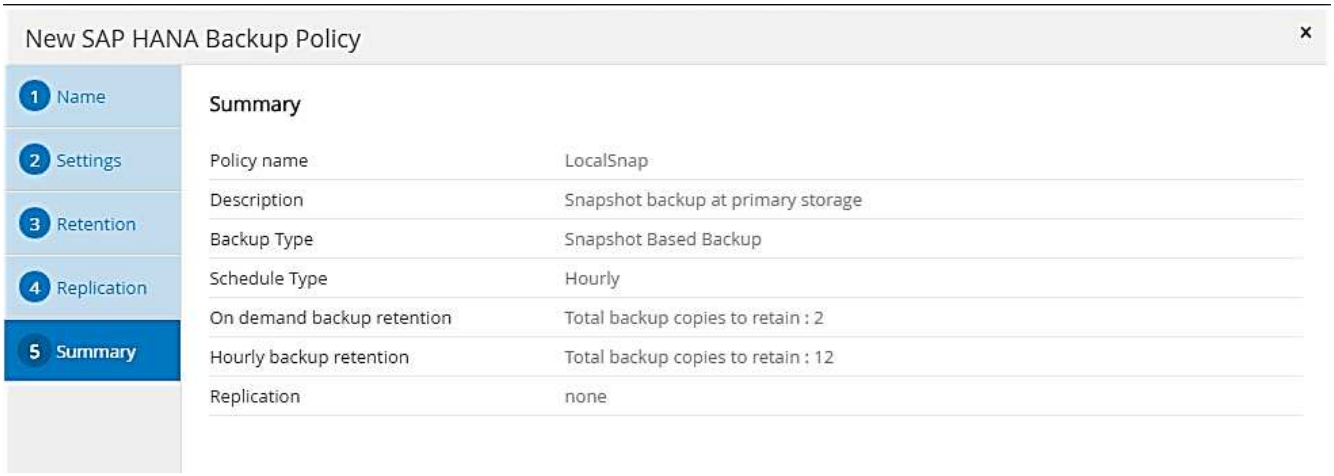
5. Configurez les paramètres de conservation pour les sauvegardes planifiées.



6. Configurez les options de réplication. Dans ce cas, aucune mise à jour de SnapVault ou de SnapMirror n'est sélectionnée.

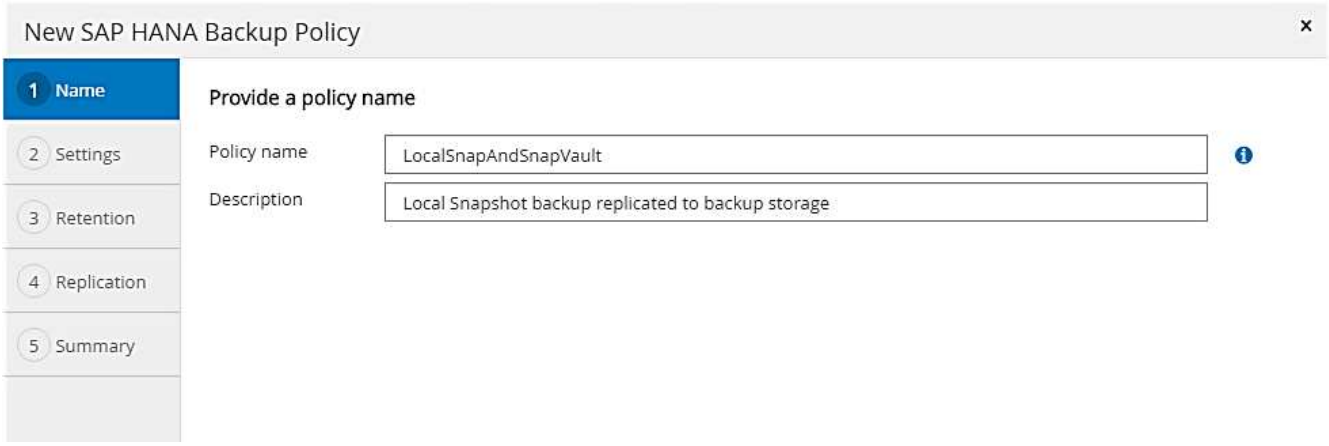


7. Sur la page Récapitulatif, cliquez sur Terminer.

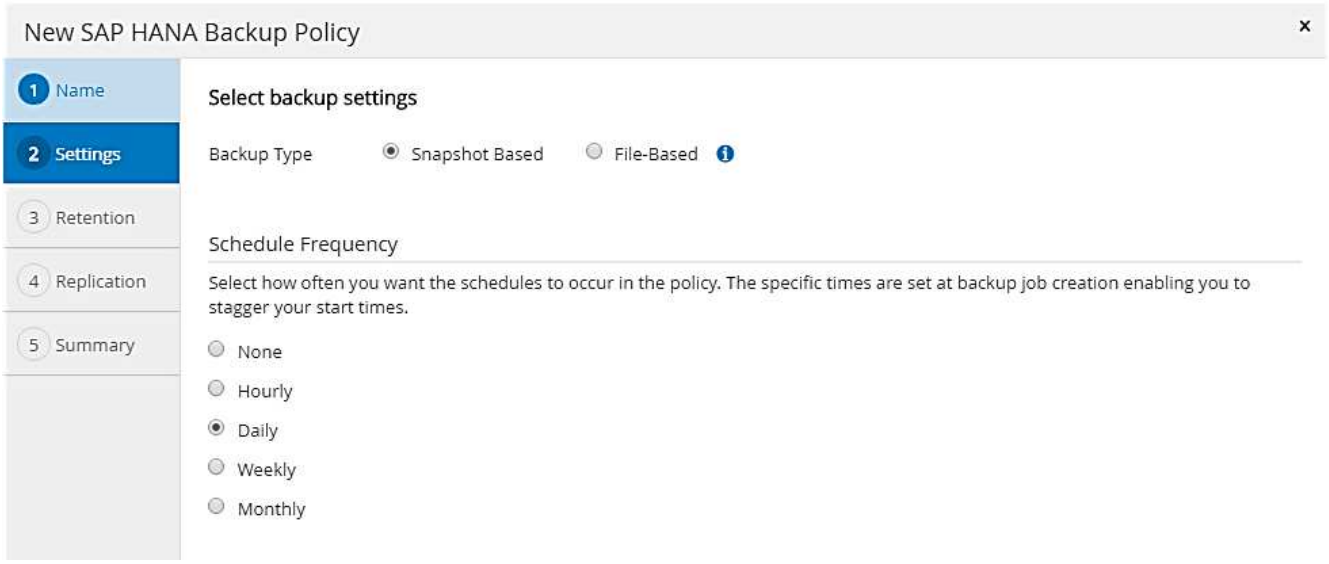


Règle applicable aux sauvegardes Snapshot quotidiennes avec réplication SnapVault

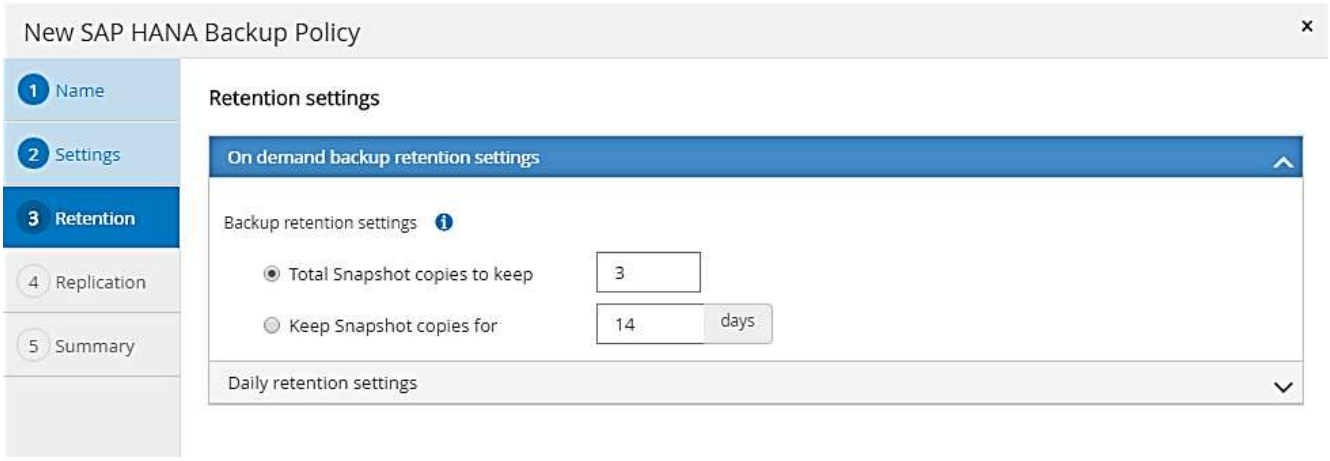
1. Accédez à Paramètres > stratégies et cliquez sur Nouveau.
2. Entrez le nom et la description de la stratégie. Cliquez sur Suivant.



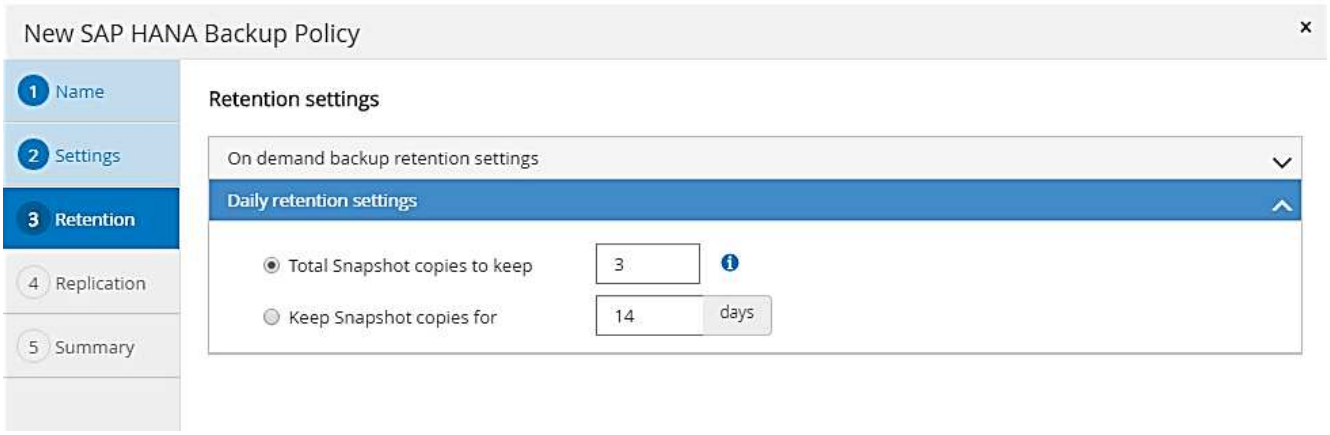
3. Définissez le type de sauvegarde sur basé sur Snapshot et la fréquence de planification sur quotidien.



4. Configurez les paramètres de conservation pour les sauvegardes à la demande.

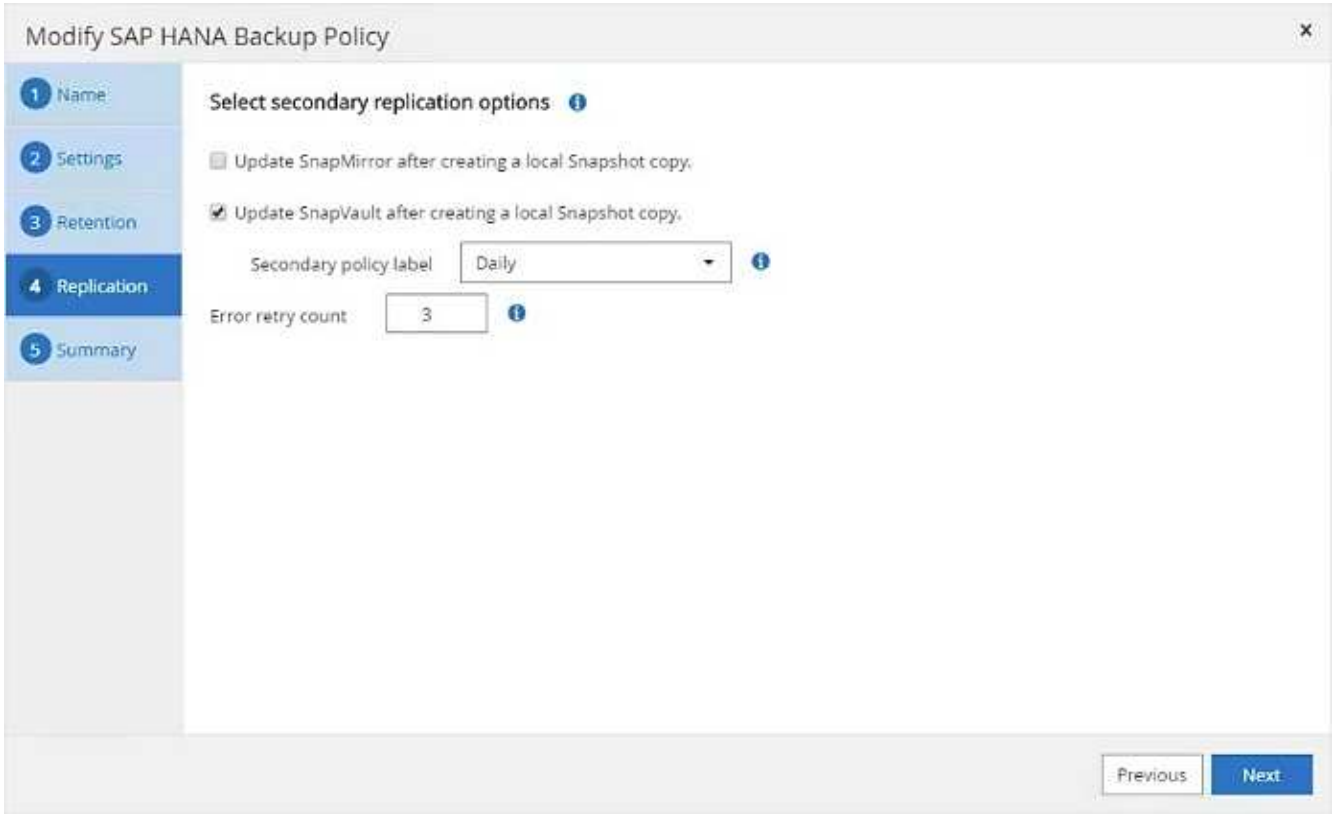


5. Configurez les paramètres de conservation pour les sauvegardes planifiées.

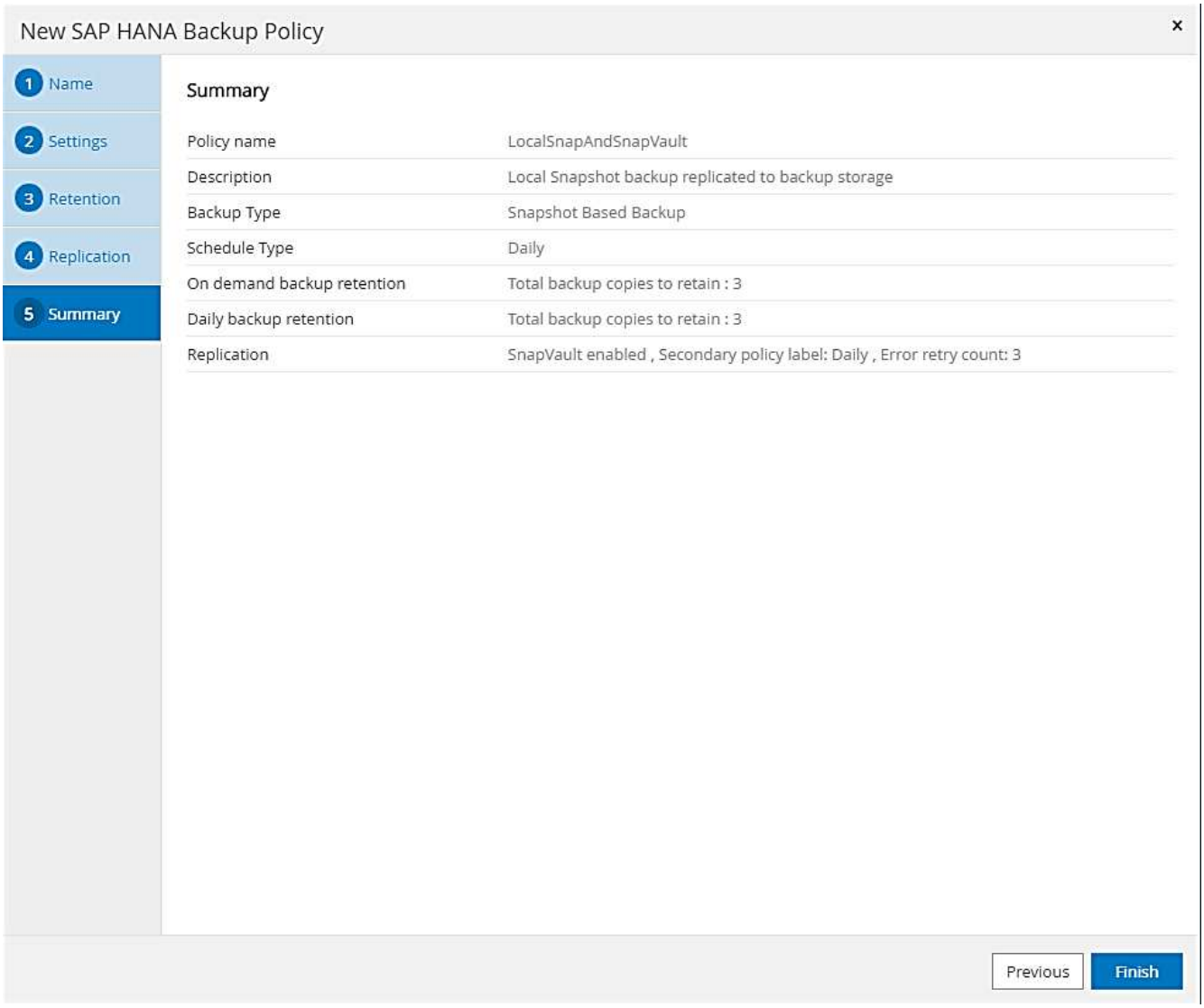


6. Sélectionnez mettre à jour SnapVault après avoir créé une copie Snapshot locale.

L'étiquette de règle secondaire doit être identique à l'étiquette SnapMirror dans la configuration de protection des données sur la couche de stockage. Voir la section ""Configuration de la protection des données sur le stockage de sauvegarde hors site.""

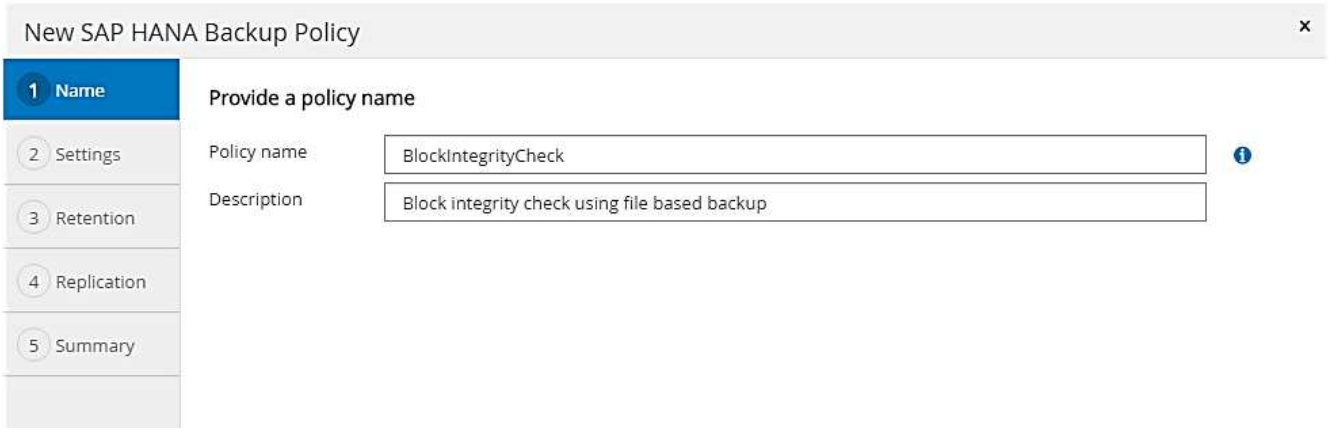


7. Sur la page Récapitulatif, cliquez sur Terminer.

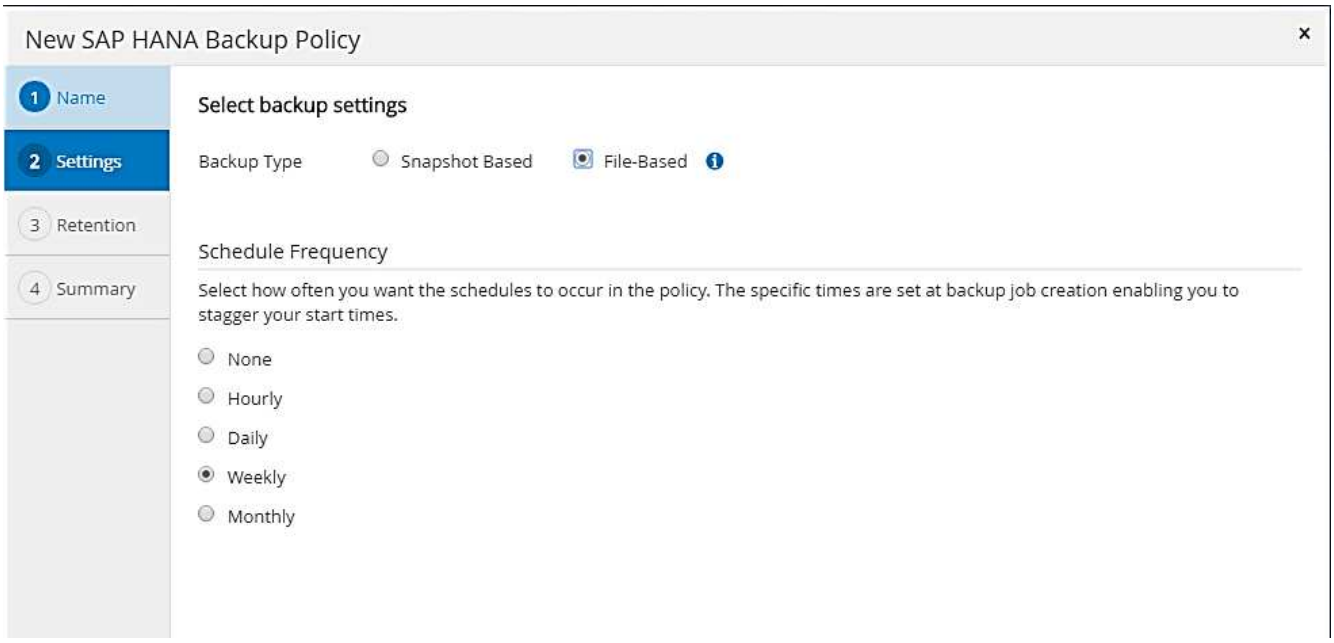


Politique relative à la vérification hebdomadaire de l'intégrité des blocs

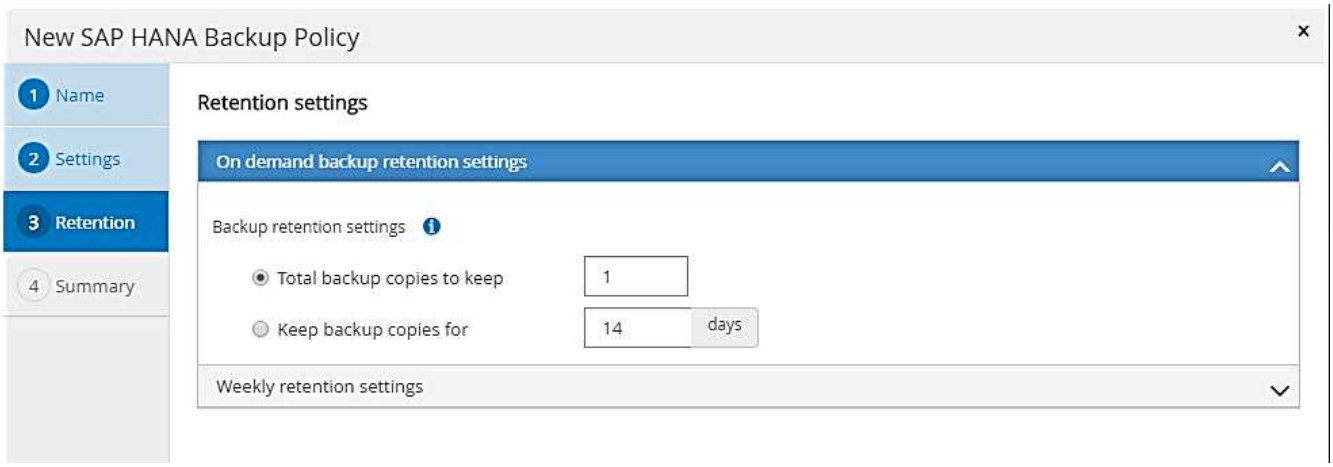
1. Accédez à Paramètres > stratégies et cliquez sur Nouveau.
2. Entrez le nom et la description de la stratégie. Cliquez sur Suivant.



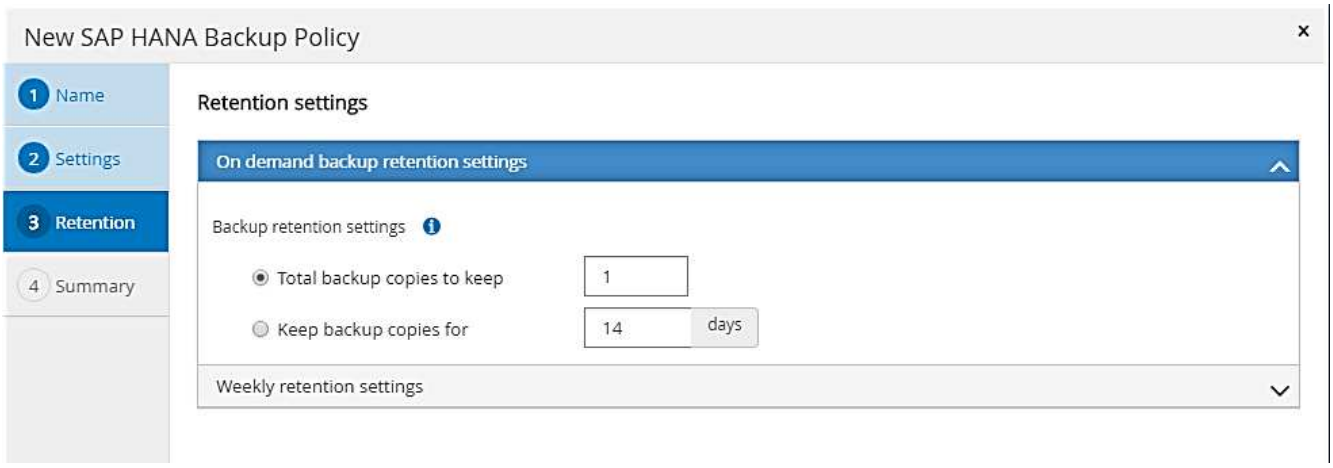
3. Définissez le type de sauvegarde sur fichier et fréquence de planification sur hebdomadaire.



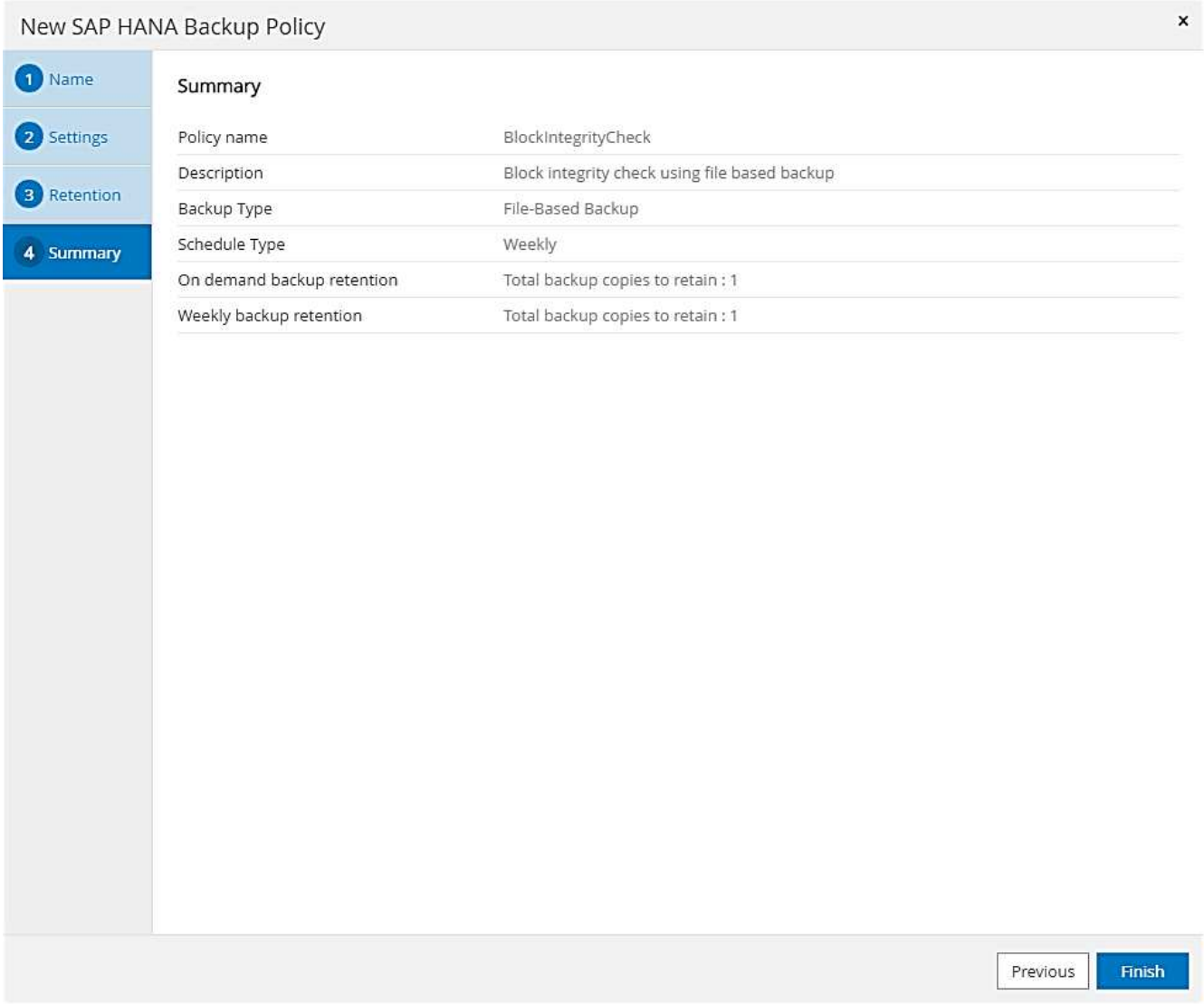
4. Configurez les paramètres de conservation pour les sauvegardes à la demande.



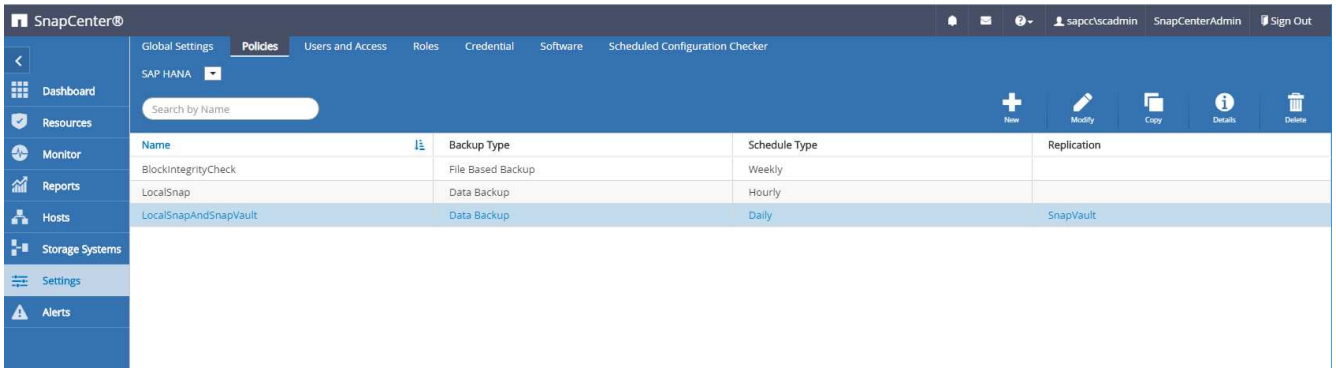
5. Configurez les paramètres de conservation pour les sauvegardes planifiées.



6. Sur la page Récapitulatif, cliquez sur Terminer.



La figure suivante présente un récapitulatif des règles configurées.



Configuration SnapCenter propre aux ressources pour les sauvegardes de bases de données SAP HANA

Cette section décrit les étapes de configuration pour deux exemples de configuration.

- **SS2.**

- Système à locataire unique SAP HANA MDC unique utilisant NFS pour l'accès au stockage
- La ressource est configurée manuellement dans SnapCenter.
- La ressource est configurée pour créer des sauvegardes Snapshot locales et vérifier l'intégrité des blocs de la base de données SAP HANA à l'aide d'une sauvegarde hebdomadaire basée sur des fichiers.

- **SS1.**
  - Système à locataire unique SAP HANA MDC unique utilisant NFS pour l'accès au stockage
  - La ressource est découverte automatiquement avec SnapCenter.
  - La ressource est configurée pour créer des sauvegardes Snapshot locales, effectuer la réplication sur un stockage de sauvegarde hors site avec SnapVault et vérifier l'intégrité des blocs pour la base de données SAP HANA à l'aide d'une sauvegarde hebdomadaire basée sur des fichiers.

Les différences entre un système connecté à un SAN, un seul conteneur ou plusieurs hôtes sont reflétées dans les étapes de configuration ou de workflow correspondantes.

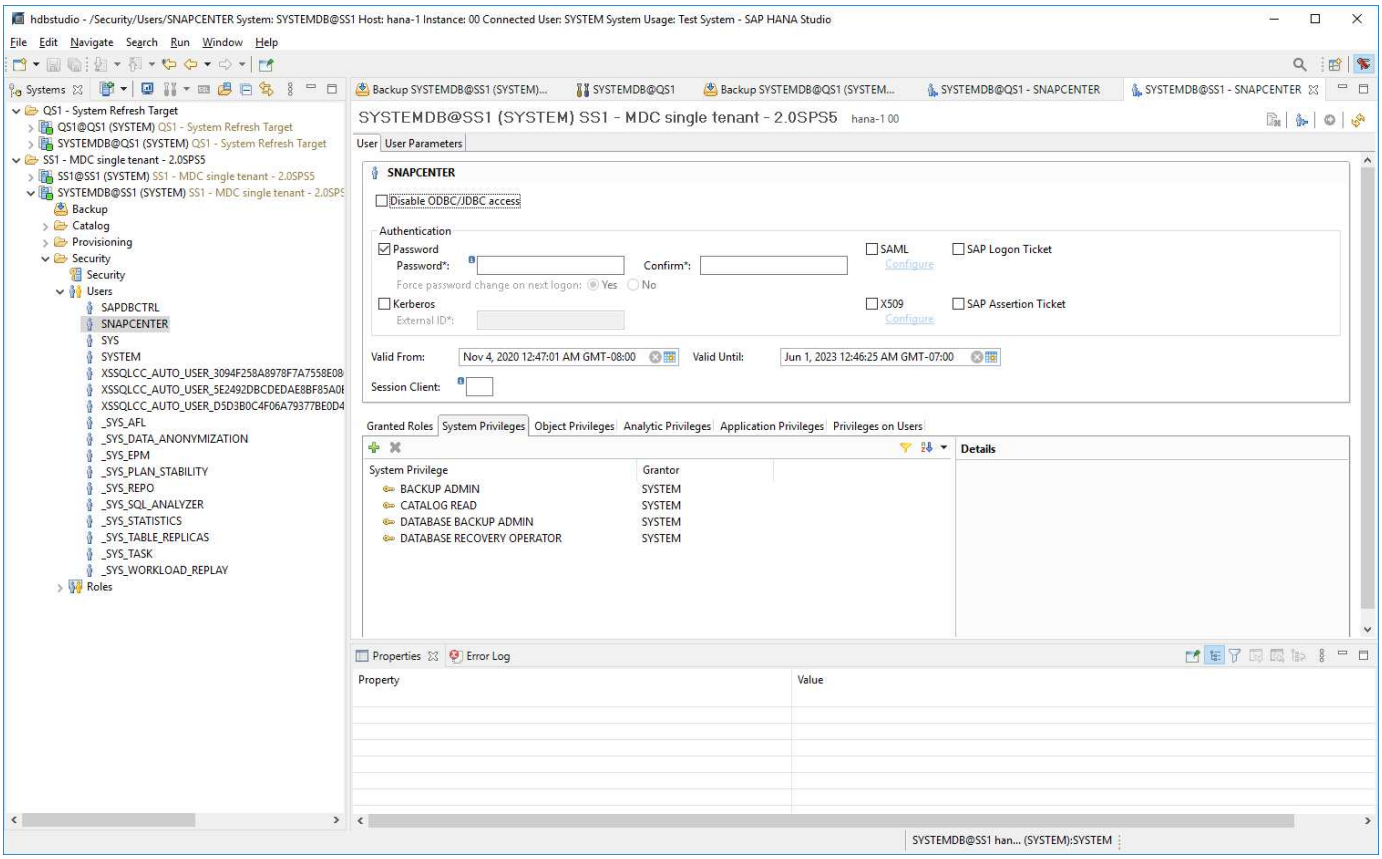
L'utilisateur de sauvegarde SAP HANA et la configuration du hdbuserstore

NetApp recommande de configurer un utilisateur de base de données dédiée sur la base de données HANA pour exécuter les opérations de sauvegarde avec SnapCenter. Dans la deuxième étape, une clé de magasin utilisateur SAP HANA est configurée pour cet utilisateur de sauvegarde, et cette clé de magasin utilisateur est utilisée dans la configuration du plug-in SnapCenter SAP HANA.

La figure suivante montre SAP HANA Studio par l'intermédiaire de lequel l'utilisateur de sauvegarde peut être créé.

Les privilèges requis ont été modifiés avec la version HANA 2.0 SPS5 : administrateur des sauvegardes, lecture du catalogue, administrateur des sauvegardes de bases de données et opérateur de récupération de bases de données. Pour les versions antérieures, l'administrateur des sauvegardes et la lecture du catalogue suffisent.

Pour un système MDC SAP HANA, l'utilisateur doit être créé dans la base de données du système car toutes les commandes de sauvegarde pour le système et les bases de données des locataires sont exécutées à l'aide de la base de données du système.



Sur l'hôte du plug-in HANA, sur lequel est installé le plug-in SAP HANA et le client SAP hdbsql, une clé de magasin utilisateur doit être configurée.

Configuration Userstore sur le serveur SnapCenter utilisé comme hôte de plug-in HANA central

Si le plug-in SAP HANA et le client SAP hdbsql sont installés sur Windows, l'utilisateur système local exécute les commandes hdbsql et est configuré par défaut dans la configuration de la ressource. Comme l'utilisateur système n'est pas un utilisateur de connexion, la configuration du magasin utilisateur doit être effectuée avec un autre utilisateur et avec le `-u <User>` option.

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

Le logiciel SAP HANA hdbclient doit d'abord être installé sur l'hôte Windows.

Configuration Userstore sur un hôte Linux distinct utilisé en tant qu'hôte de plug-in HANA central

Si le plug-in SAP HANA et le client SAP hdbsql sont installés sur un hôte Linux distinct, la commande suivante est utilisée pour la configuration du magasin utilisateur avec l'utilisateur défini dans la configuration de la ressource :

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

Le logiciel SAP HANA hdbclient doit d'abord être installé sur l'hôte Linux.

Configuration Userstore sur l'hôte de la base de données HANA

Si le plug-in SAP HANA est déployé sur l'hôte de la base de données HANA, la commande suivante est utilisée pour la configuration du magasin des utilisateurs avec le `<sid>adm` utilisateur :

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

SnapCenter utilise le `<sid>adm` L'utilisateur doit communiquer avec la base de données HANA. Par conséquent, la clé de stockage utilisateur doit être configurée à l'aide de l'utilisateur <sID> adm sur l'hôte de base de données.

En général, le logiciel client SAP HANA hdbsql est installé avec l'installation du serveur de base de données. Si ce n'est pas le cas, l'hdbclient doit être installé en premier.

Configuration de Userstore en fonction de l'architecture du système HANA

Dans une configuration SAP HANA MDC à un seul locataire, port `3<instanceNo>13` Est le port standard pour l'accès SQL à la base de données système et doit être utilisé dans la configuration hdbuserstore.

Pour une configuration à conteneur unique SAP HANA, port `3<instanceNo>15` Est le port standard pour l'accès SQL au serveur d'index et doit être utilisé dans la configuration hdbuserstore.

Dans le cas d'une configuration SAP HANA à plusieurs hôtes, les clés de magasin d'utilisateurs de tous les hôtes doivent être configurées. SnapCenter tente de se connecter à la base de données à l'aide de chacune des clés fournies et peut donc opérer indépendamment d'un basculement d'un service SAP HANA vers un autre hôte.

Exemples de configuration de l'UserStore

En laboratoire, un déploiement mixte de plug-in SAP HANA est utilisé. Le plug-in HANA est installé sur le serveur SnapCenter pour certains systèmes HANA et déployé sur les serveurs de base de données HANA individuels pour d'autres systèmes.

Système SAP HANA SS1, locataire unique MDC, instance 00

Le plug-in HANA a été déployé sur l'hôte de la base de données. Par conséquent, la clé doit être configurée sur l'hôte de la base de données avec l'utilisateur ss1adm.

```
hana-1:/ # su - ss1adm
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE       : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

Système SAP HANA MS1, instance unique MDC multihôte, instance 00

Pour plusieurs systèmes hôtes HANA, un plug-in central est requis dans notre configuration, que nous avons utilisé le serveur SnapCenter. Par conséquent, la configuration du magasin utilisateur doit être effectuée sur le serveur SnapCenter.

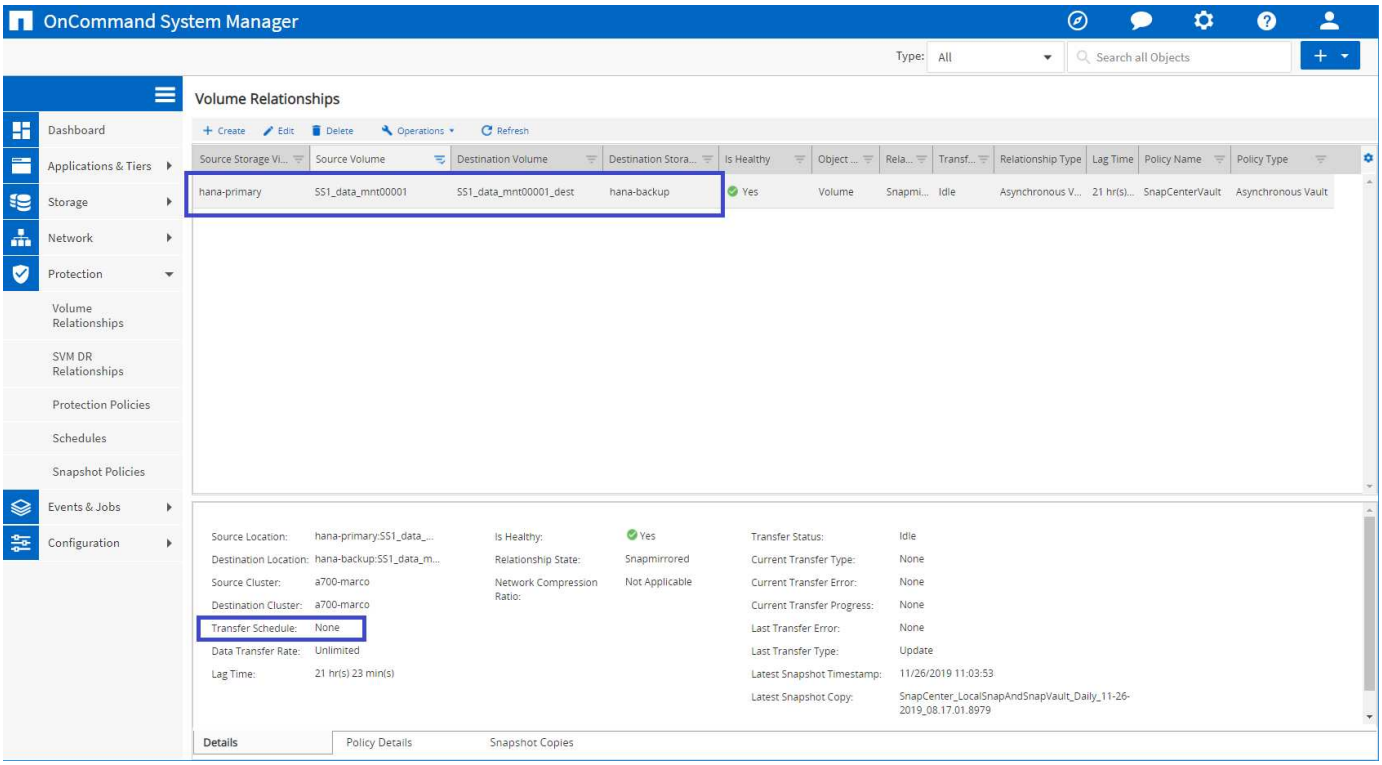
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE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

Configuration de la protection des données sur le stockage de sauvegarde hors site

La configuration de la relation de protection des données, ainsi que le transfert de données initial doivent être exécutés avant que les mises à jour de réplication puissent être gérées par SnapCenter.

La figure suivante montre la relation de protection configurée pour le système SAP HANA SS1. Dans notre exemple, le volume source `SS1_data_mnt00001` Au niveau du SVM `hana-primary` Est répliqué sur la SVM `hana-backup` et le volume cible `SS1_data_mnt00001_dest`.

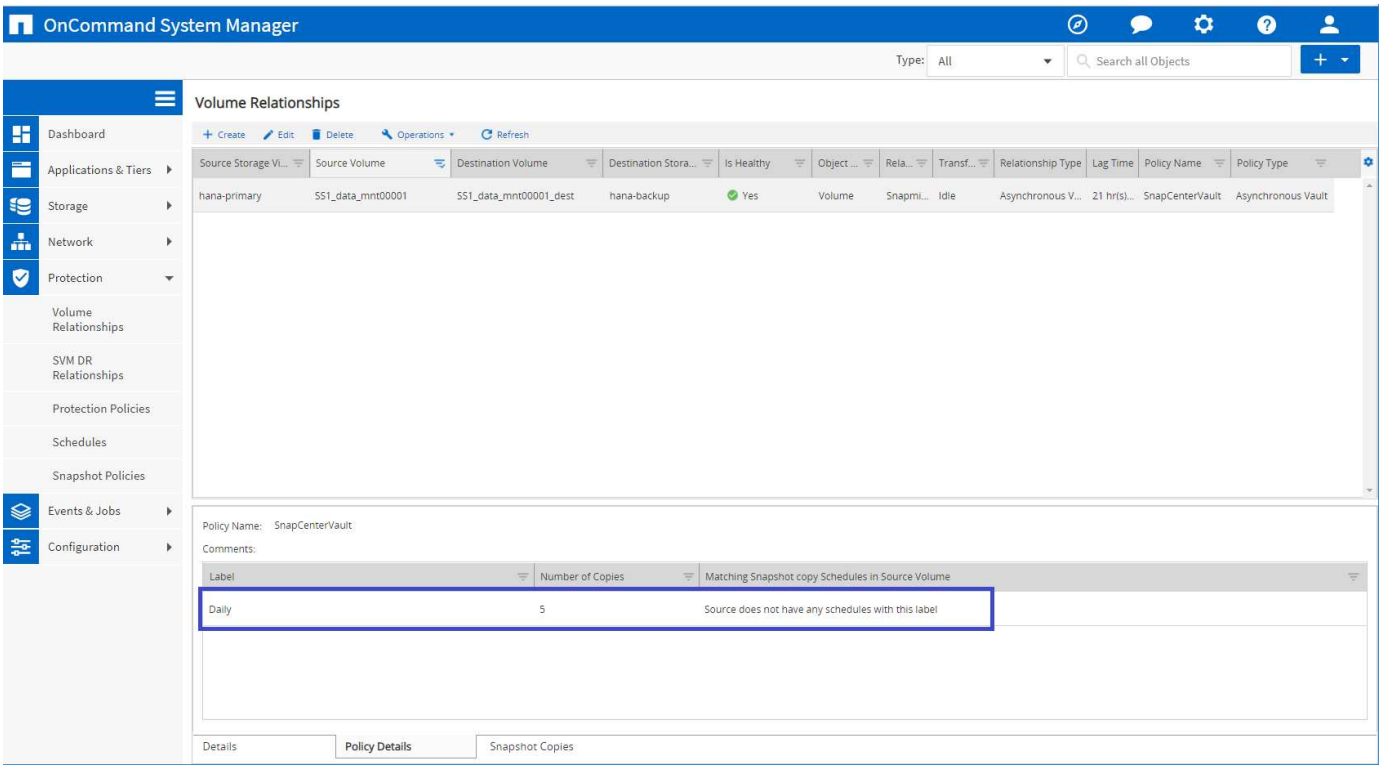
La planification de la relation doit être définie sur aucun, car SnapCenter déclenche la mise à jour SnapVault.



La figure suivante illustre la règle de protection. La règle de protection utilisée pour la relation de protection définit l'étiquette SnapMirror, ainsi que la conservation des sauvegardes sur le stockage secondaire. Dans notre exemple, l'étiquette utilisée est `Daily`, et la rétention est définie sur 5.

L'étiquette SnapMirror de la règle en cours de création doit correspondre à l'étiquette définie dans la configuration de la règle SnapCenter. Pour plus de détails, reportez-vous à la section «Règle applicable aux sauvegardes Snapshot quotidiennes avec réplication SnapVault. »

La conservation des sauvegardes sur le stockage de sauvegarde hors site est définie dans la règle et contrôlée par ONTAP.



Configuration manuelle des ressources HANA

Cette section décrit la configuration manuelle des ressources SAP HANA SS2 et MS1.

- SS2 est un système à locataire unique MDC à un seul hôte
- MS1 est un système à un seul tenant MDC à plusieurs hôtes.

a. Dans l'onglet Ressources, sélectionnez SAP HANA et cliquez sur Ajouter une base de données SAP HANA.

b. Entrez les informations relatives à la configuration de la base de données SAP HANA et cliquez sur Next (Suivant).

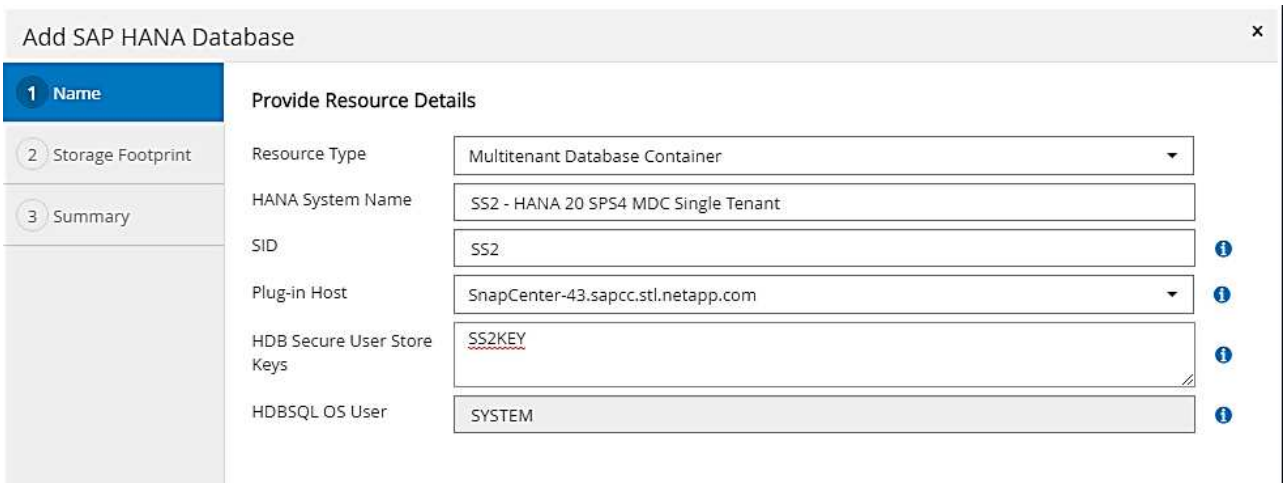
Sélectionnez le type de ressource dans notre exemple, Multitenant Database Container.

Pour un système à conteneur unique HANA, le type de ressource conteneur unique doit être sélectionné. Toutes les autres étapes de configuration sont identiques.

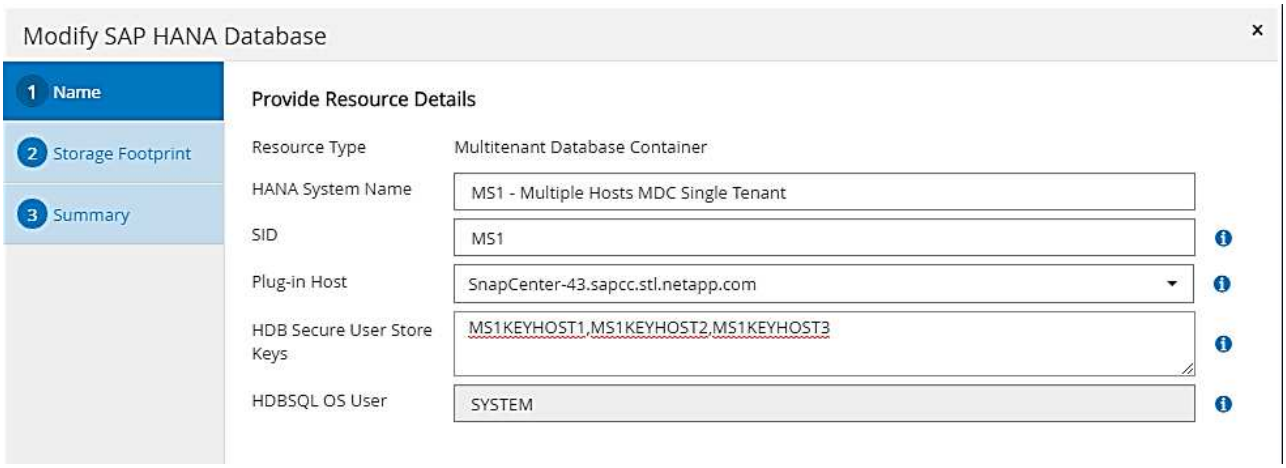
Pour notre système SAP HANA, SID est SS2.

Dans notre exemple, le plug-in HANA est le serveur SnapCenter.

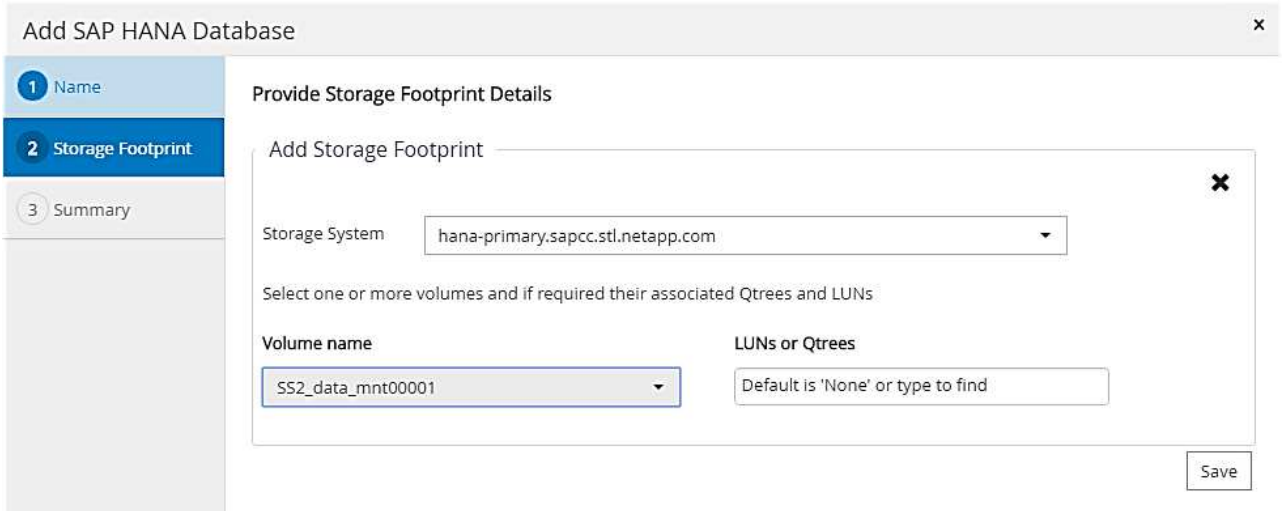
La clé hdbuserstore doit correspondre à la clé configurée pour la base de données HANA SS2. Dans notre exemple, il s'agit de SS2KEY.



Pour un système SAP HANA à plusieurs hôtes, les clés de hdbuserstore pour tous les hôtes doivent être incluses, comme illustré dans la figure suivante. SnapCenter essaie de se connecter à la première clé de la liste et continuera dans l'autre cas, si la première clé ne fonctionne pas. Cette configuration est nécessaire pour prendre en charge le basculement HANA sur un système à plusieurs hôtes avec des hôtes workers et de secours.

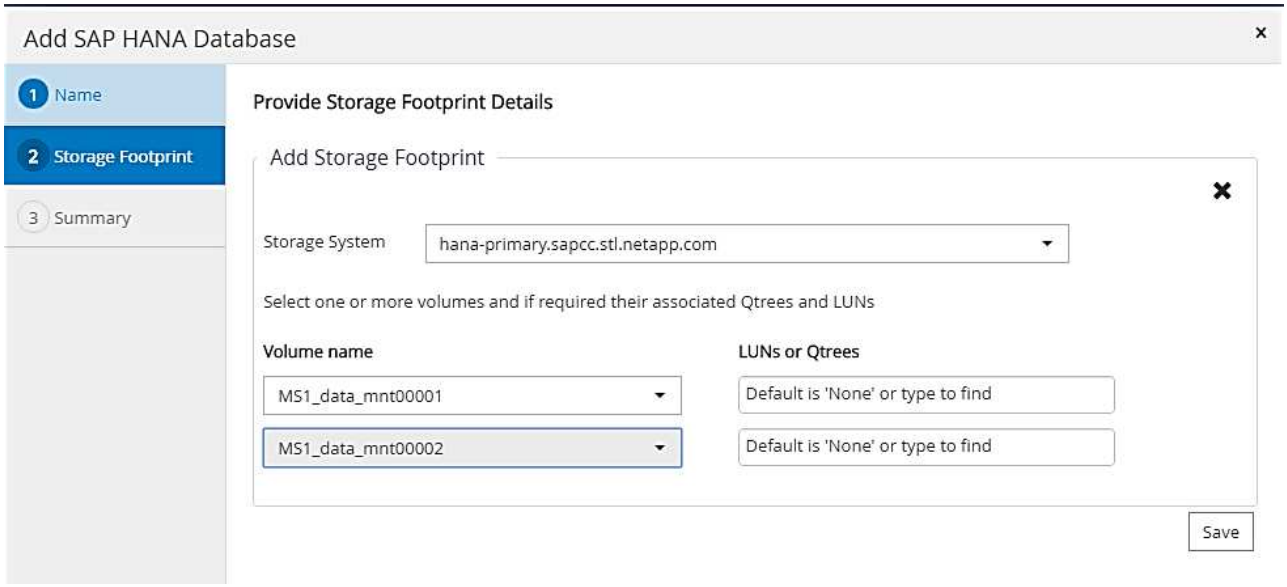


c. Sélectionner les données requises pour le système de stockage (SVM) et le nom du volume.



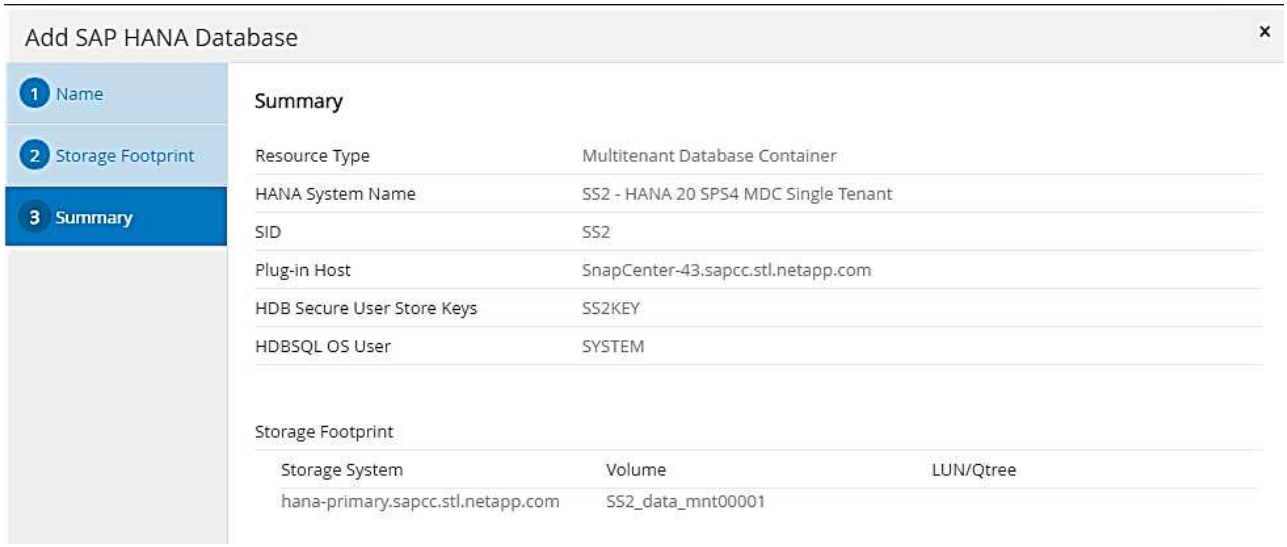
Dans le cas d'une configuration SAN Fibre Channel, la LUN doit également être sélectionnée.

Pour un système SAP HANA à plusieurs hôtes, tous les volumes de données du système SAP HANA doivent être sélectionnés, comme illustré dans la figure suivante.



L'écran récapitulatif de la configuration de la ressource s'affiche.

a. Cliquez sur Terminer pour ajouter la base de données SAP HANA.



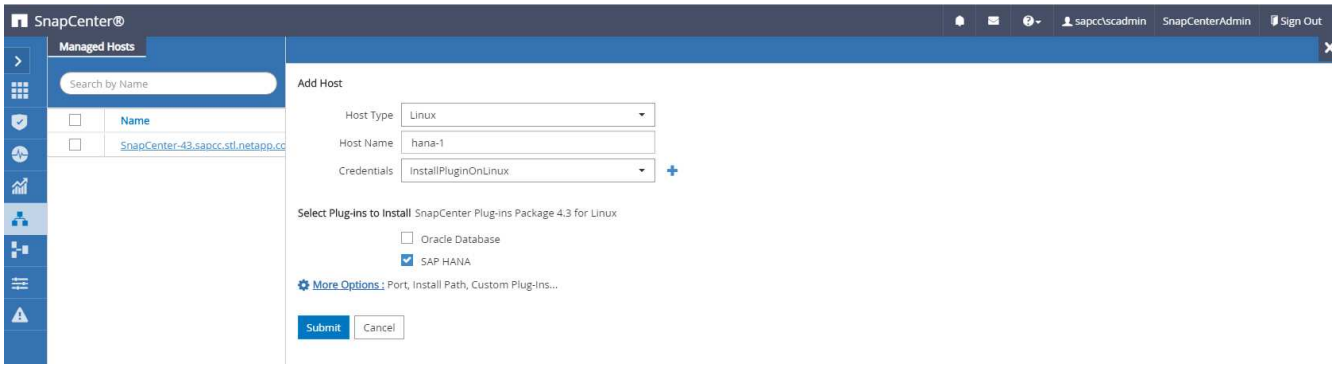
b. Une fois la configuration des ressources terminée, effectuez la configuration de la protection des ressources comme décrit dans la section «Configuration de la protection des ressources. »

Découverte automatique des bases de données HANA

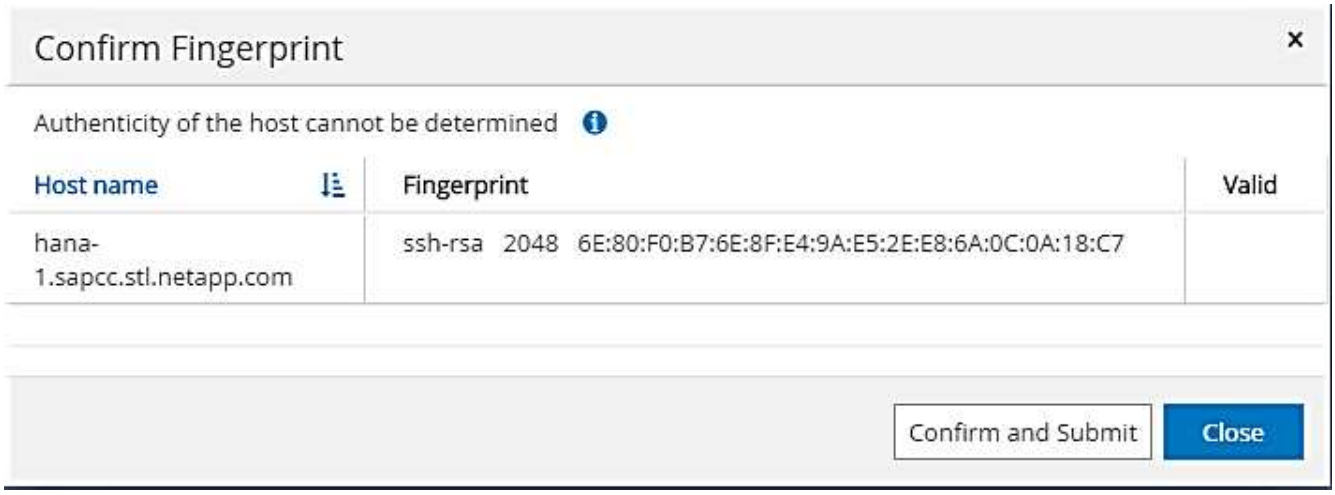
Cette section décrit la découverte automatique de la ressource SAP HANA SS1 (système unique MDC pour un seul hôte avec NFS). Toutes les étapes décrites sont identiques pour un seul conteneur HANA, pour les systèmes de plusieurs locataires HANA MDC et pour un système HANA qui utilise SAN Fibre Channel.

Le plug-in SAP HANA requiert Java 64 bits version 1.8. Java doit être installé sur l'hôte avant le déploiement du plug-in SAP HANA.

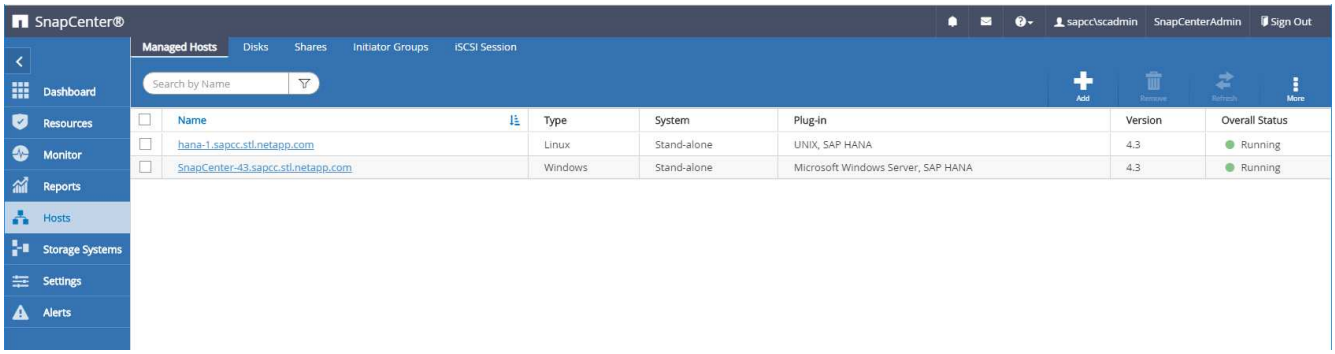
1. Dans l'onglet hôte, cliquez sur Ajouter.
2. Fournissez des informations sur l'hôte et sélectionnez le plug-in SAP HANA à installer. Cliquez sur soumettre.



3. Confirmez l'empreinte digitale.



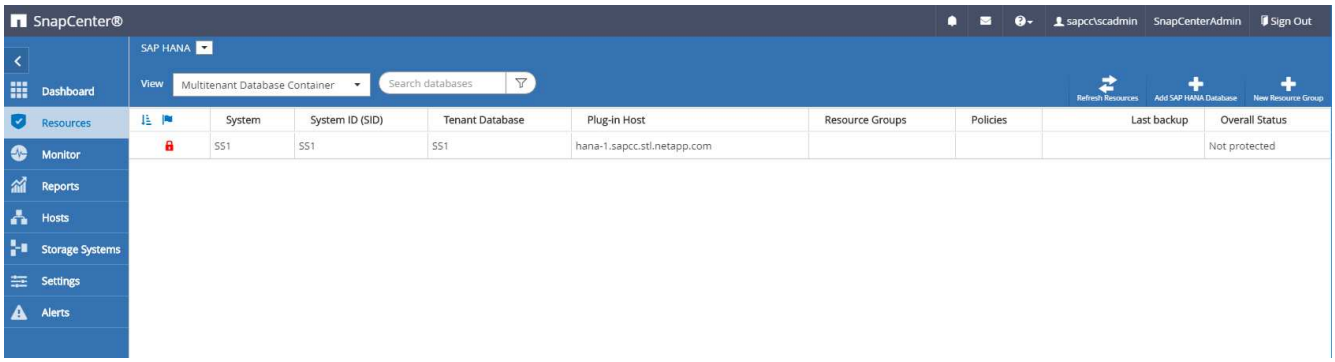
L'installation du plug-in HANA et du plug-in Linux démarre automatiquement. Lorsque l'installation est terminée, la colonne d'état de l'hôte indique exécution. Il s'affiche également que le plug-in Linux est installé avec le plug-in HANA.



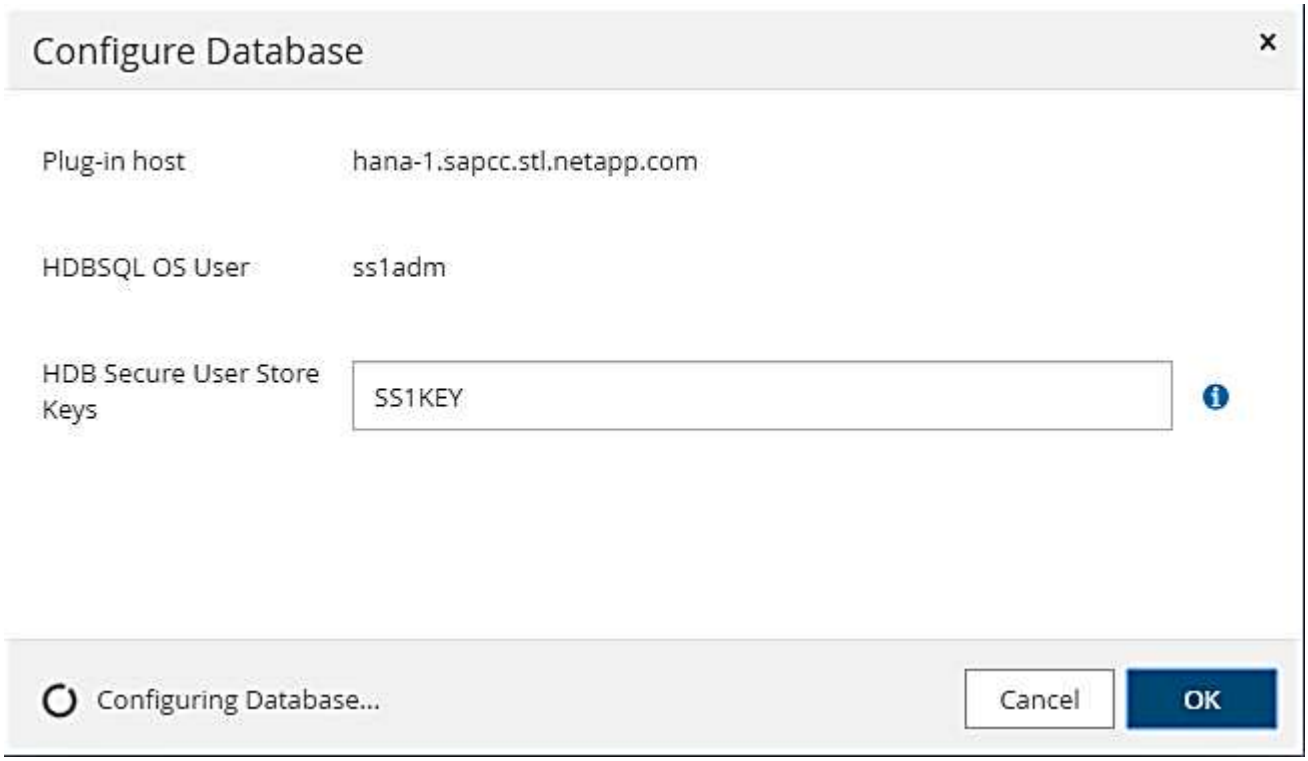
Une fois l'installation du plug-in terminée, le processus de détection automatique de la ressource HANA démarre automatiquement. Dans l'écran Ressources, une nouvelle ressource est créée, marquée comme étant verrouillée par l'icône de cadenas rouge.

4. Sélectionnez et cliquez sur la ressource pour poursuivre la configuration.

Vous pouvez également déclencher le processus de détection automatique manuellement dans l'écran Ressources en cliquant sur Actualiser les ressources.

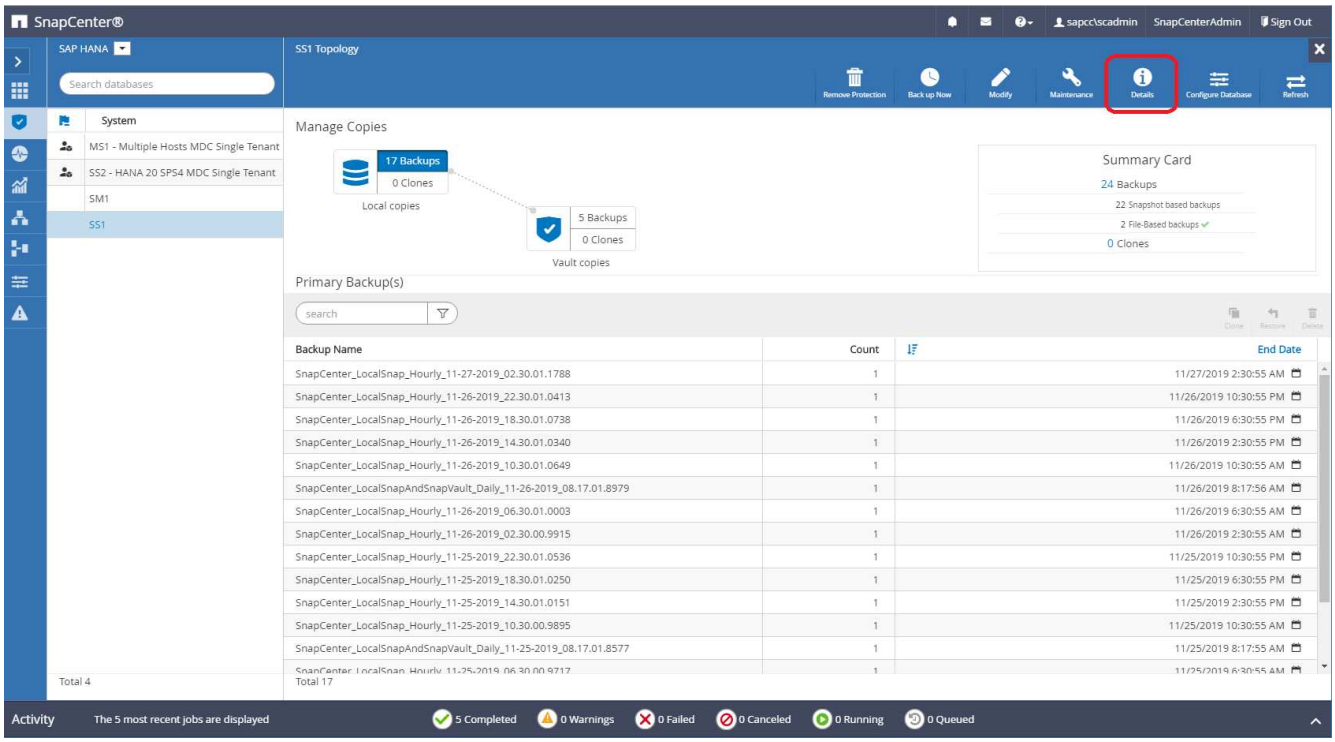


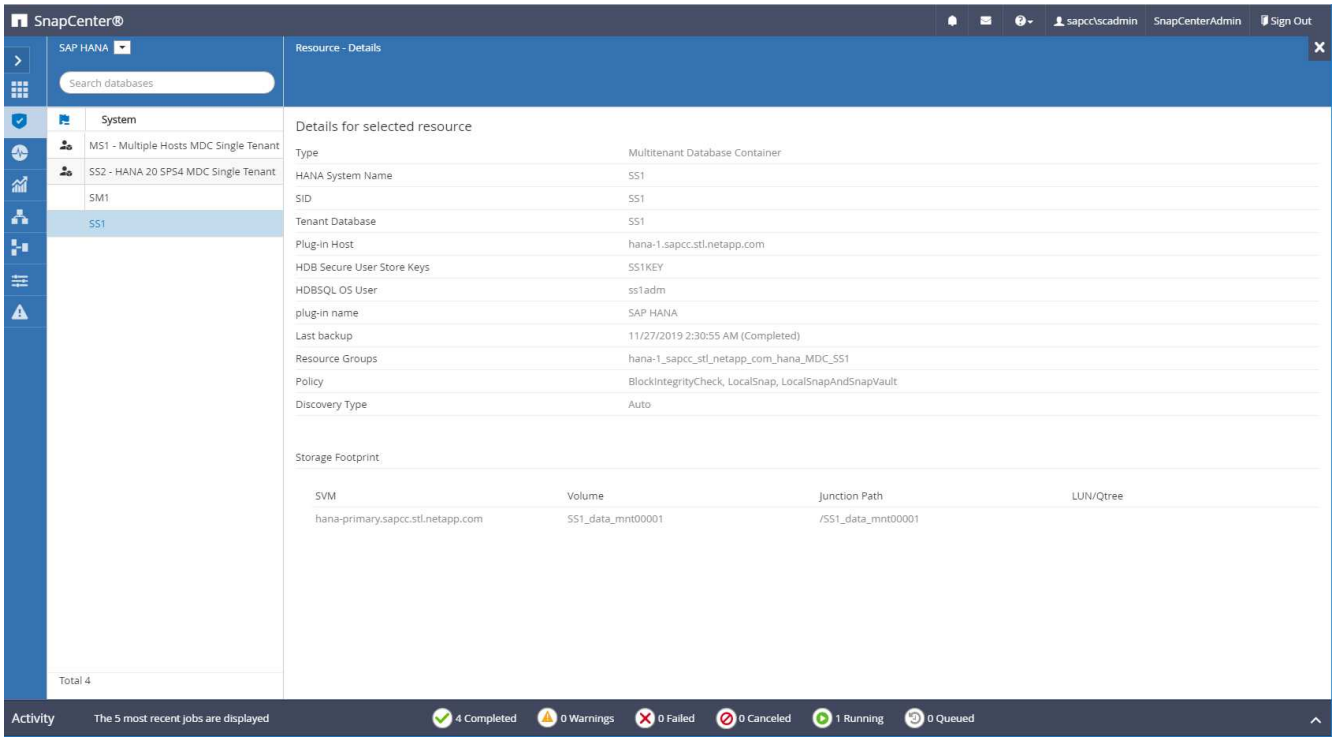
5. Fournissez la clé de magasin d'utilisateurs pour la base de données HANA.



La détection automatique du second niveau commence par la découverte des informations relatives aux données des locataires et à l'encombrement du stockage.

6. Cliquez sur Details pour consulter les informations de configuration des ressources HANA dans la vue topologique des ressources.





Lorsque la configuration des ressources est terminée, la configuration de la protection des ressources doit être exécutée comme décrit dans la section suivante.

Configuration de la protection des ressources

Cette section décrit la configuration de la protection des ressources. La configuration de protection des ressources est identique, que la ressource ait été découverte automatique ou configurée manuellement. Elle est également identique pour toutes les architectures HANA, des hôtes uniques ou multiples, un seul conteneur ou un système MDC.

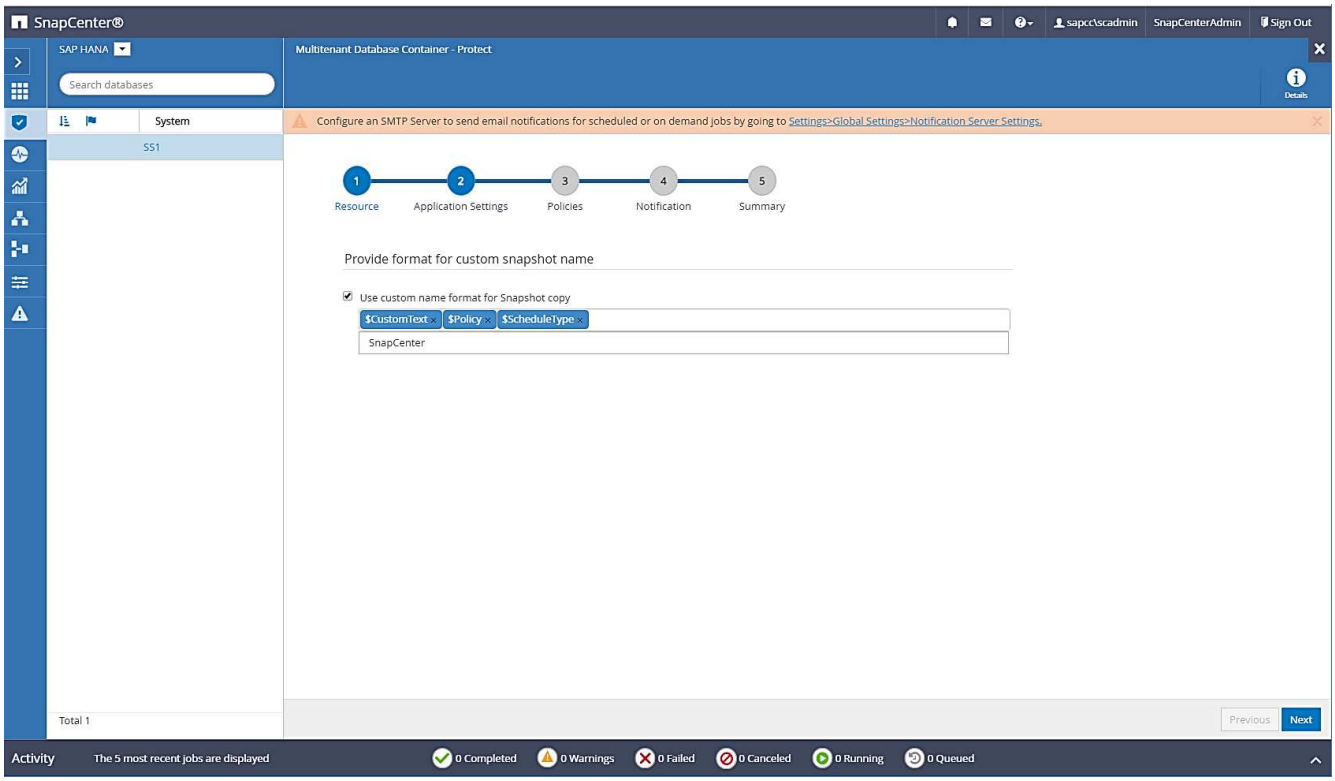
1. Dans l'onglet Ressources, double-cliquez sur la ressource.
2. Configurez un format de nom personnalisé pour la copie Snapshot.

> NetApp recommande d'utiliser un nom de copie Snapshot personnalisé pour identifier facilement les sauvegardes qui ont été créées avec quel type de règle et de planification. L'ajout du type de planification dans le nom de la copie Snapshot permet de distinguer les sauvegardes planifiées et à la demande. Le `schedule name` la chaîne pour les sauvegardes à la demande est vide, tandis que les sauvegardes planifiées incluent la chaîne `Hourly`, `Daily`, `or Weekly`.

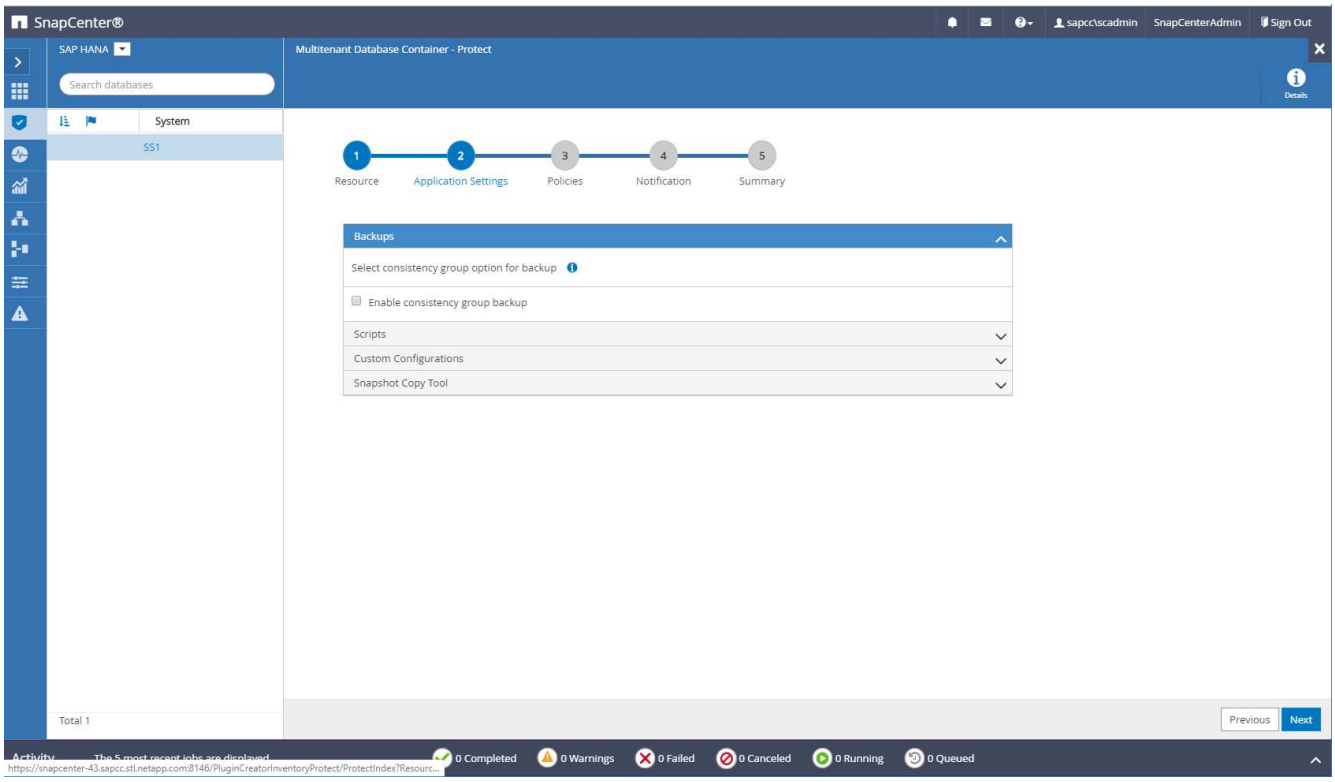
Dans la configuration indiquée dans la figure suivante, les noms de sauvegarde et de copie Snapshot ont le format suivant :

- Sauvegardes horaires programmées : `SnapCenter_LocalSnap_Hourly_<time_stamp>`
- Sauvegarde quotidienne planifiée : `SnapCenter_LocalSnapAndSnapVault_Daily_<time_stamp>`
- Sauvegarde horaire à la demande : `SnapCenter_LocalSnap_<time_stamp>`
- Sauvegarde quotidienne à la demande : `SnapCenter_LocalSnapAndSnapVault_<time_stamp>`

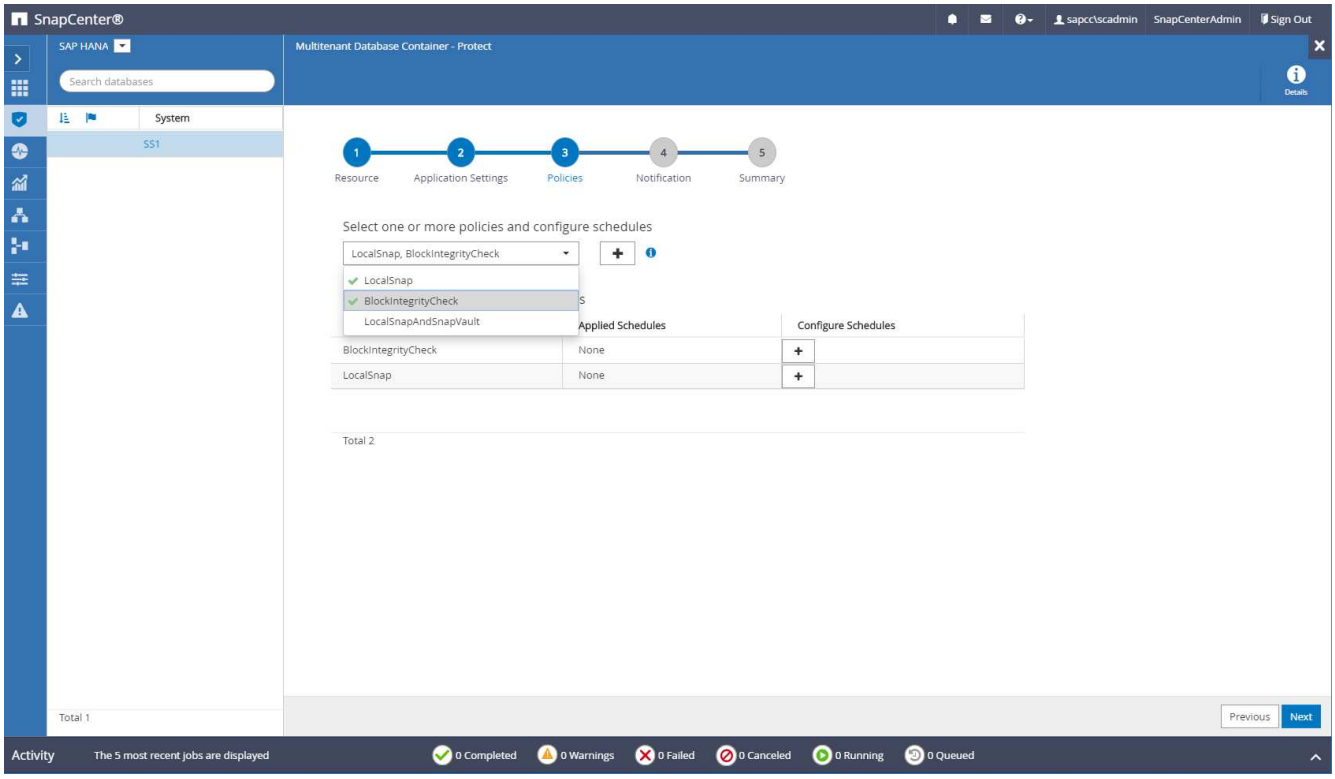
> Même si une conservation est définie pour des sauvegardes à la demande dans la configuration de règles, l'organisation des données n'est effectuée que lorsqu'une autre sauvegarde à la demande est exécutée. Par conséquent, les sauvegardes à la demande doivent généralement être supprimées manuellement dans SnapCenter afin d'assurer que ces sauvegardes sont également supprimées dans le catalogue de sauvegardes SAP HANA et que les services de gestion des sauvegardes de journaux ne reposent pas sur une sauvegarde à la demande trop ancienne.



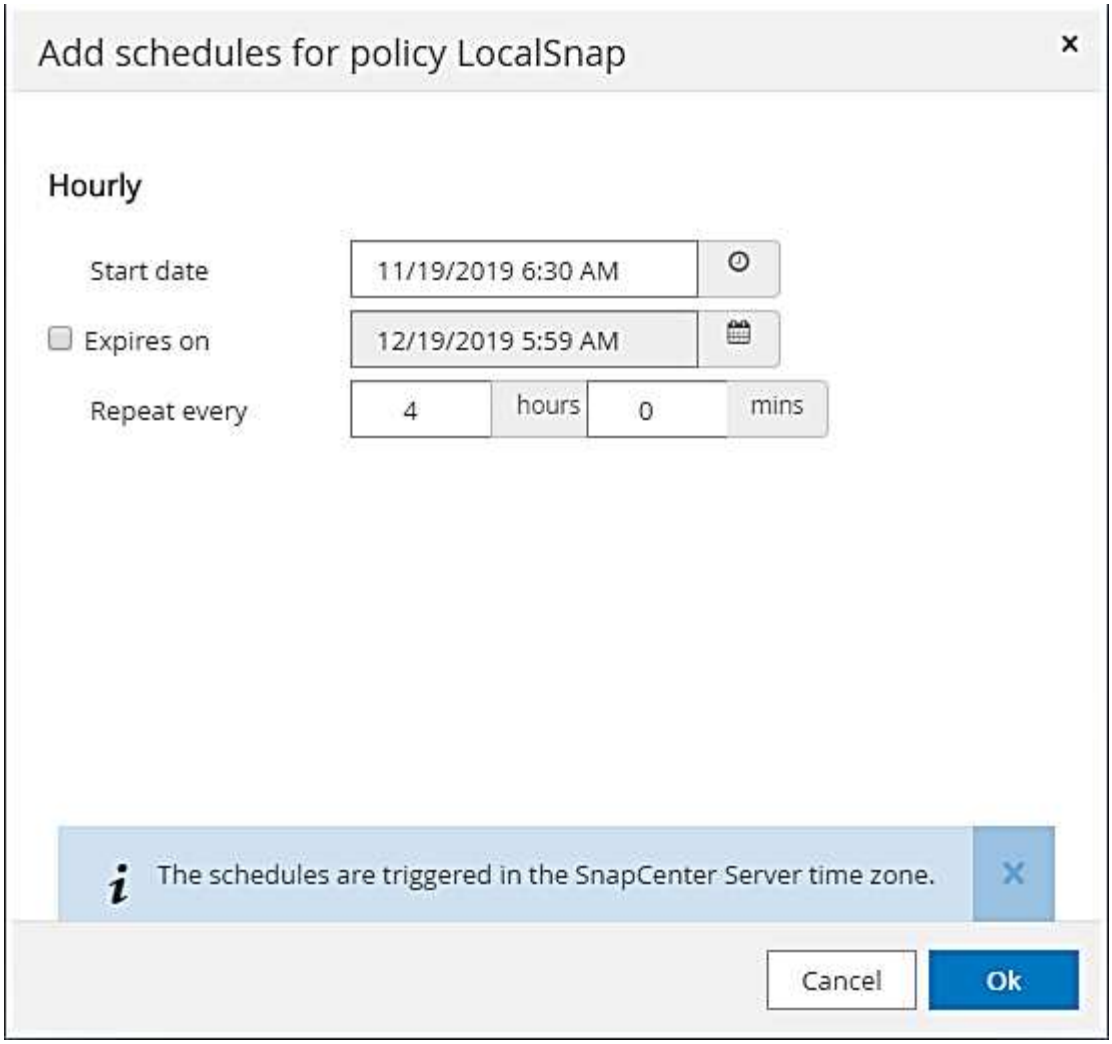
3. Aucun paramètre spécifique ne doit être défini sur la page Paramètres de l'application. Cliquez sur Suivant.



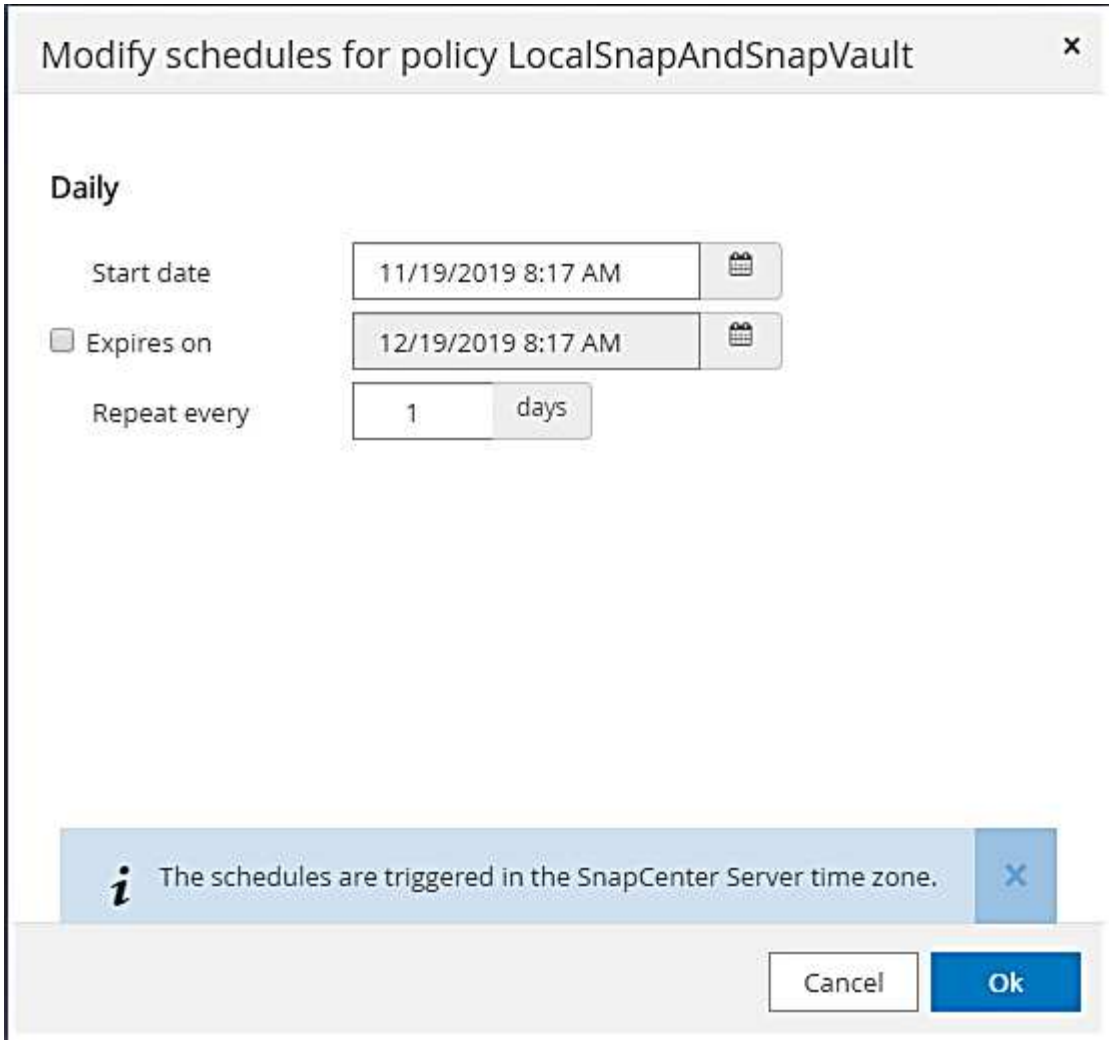
4. Sélectionnez les stratégies à ajouter à la ressource.



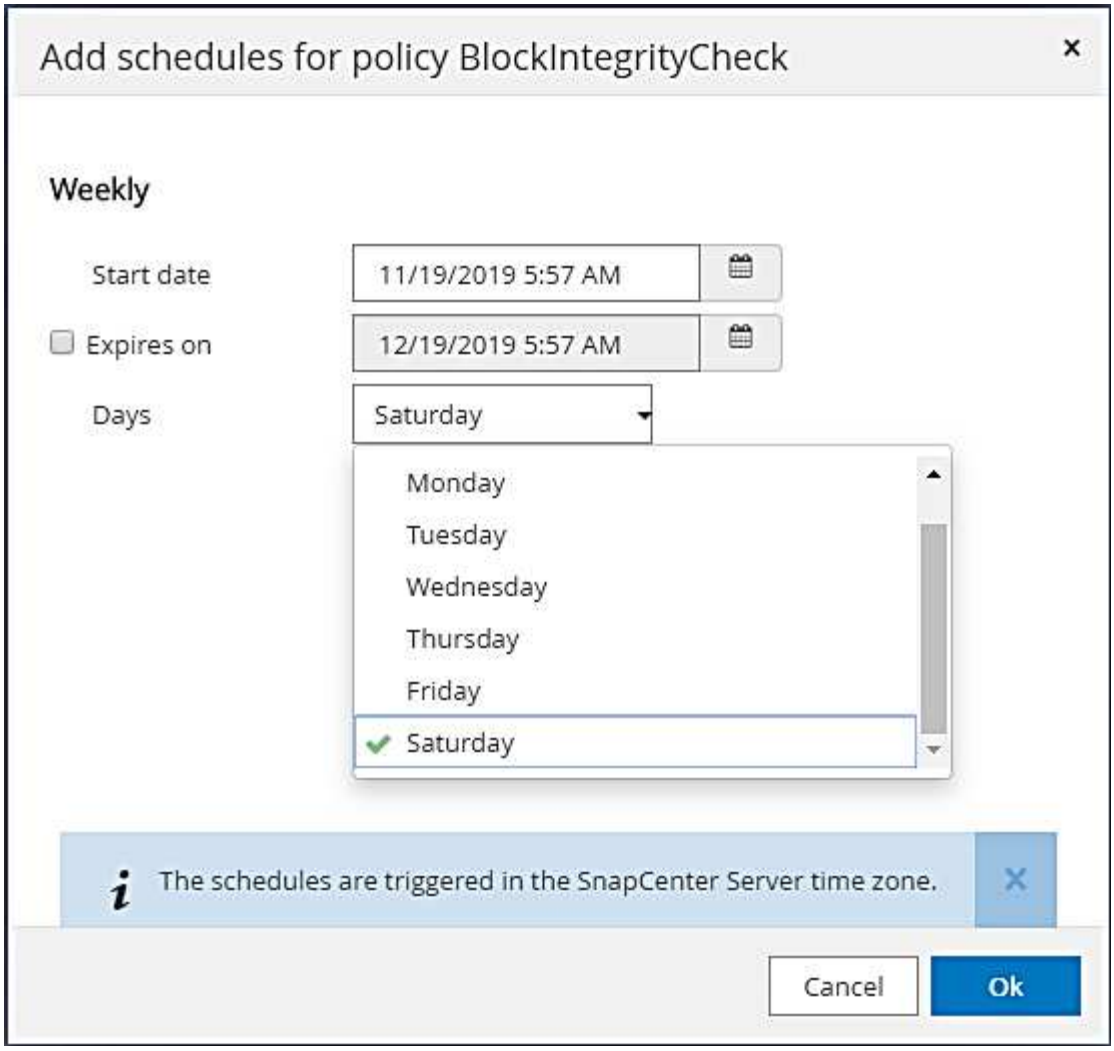
5. Définissez le planning de la stratégie LocalSnap (dans cet exemple, toutes les quatre heures).



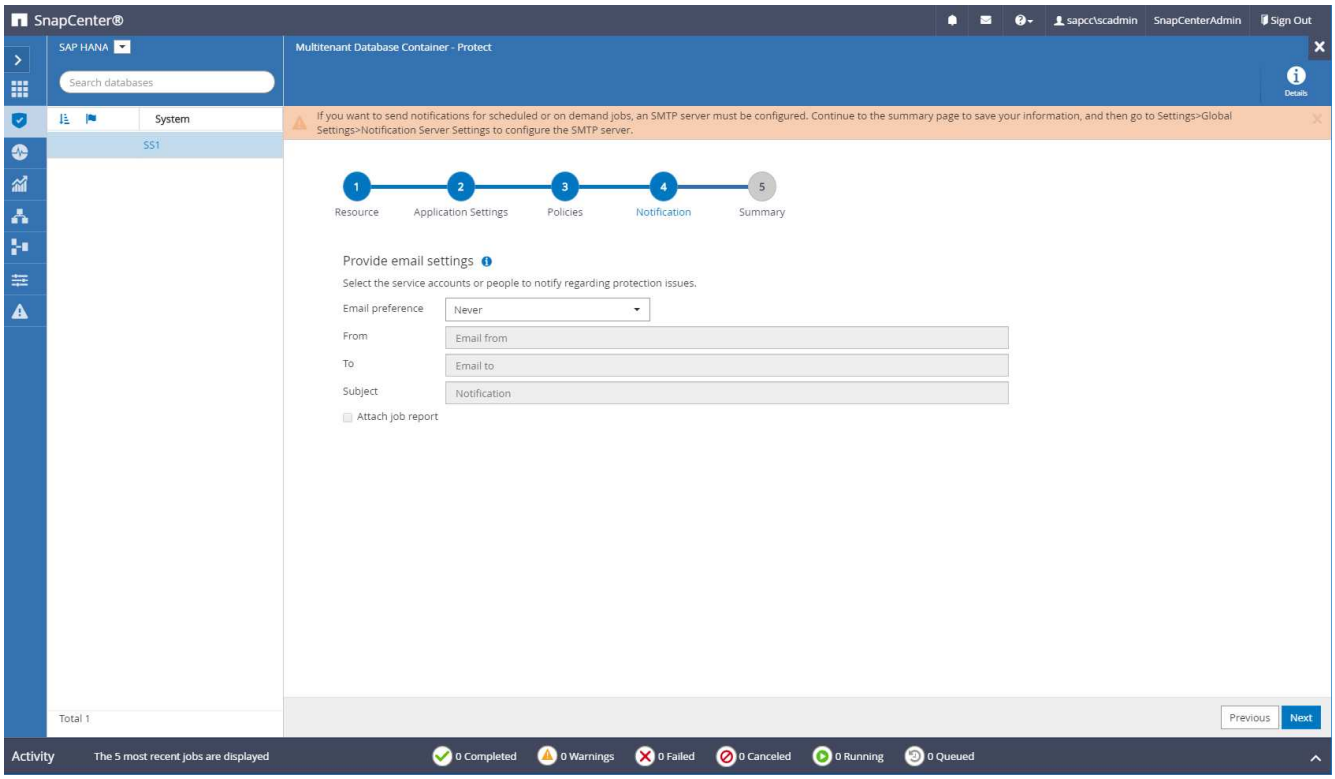
6. Définissez la planification de la stratégie LocalSnapAndSnapVault (dans cet exemple, une fois par jour).



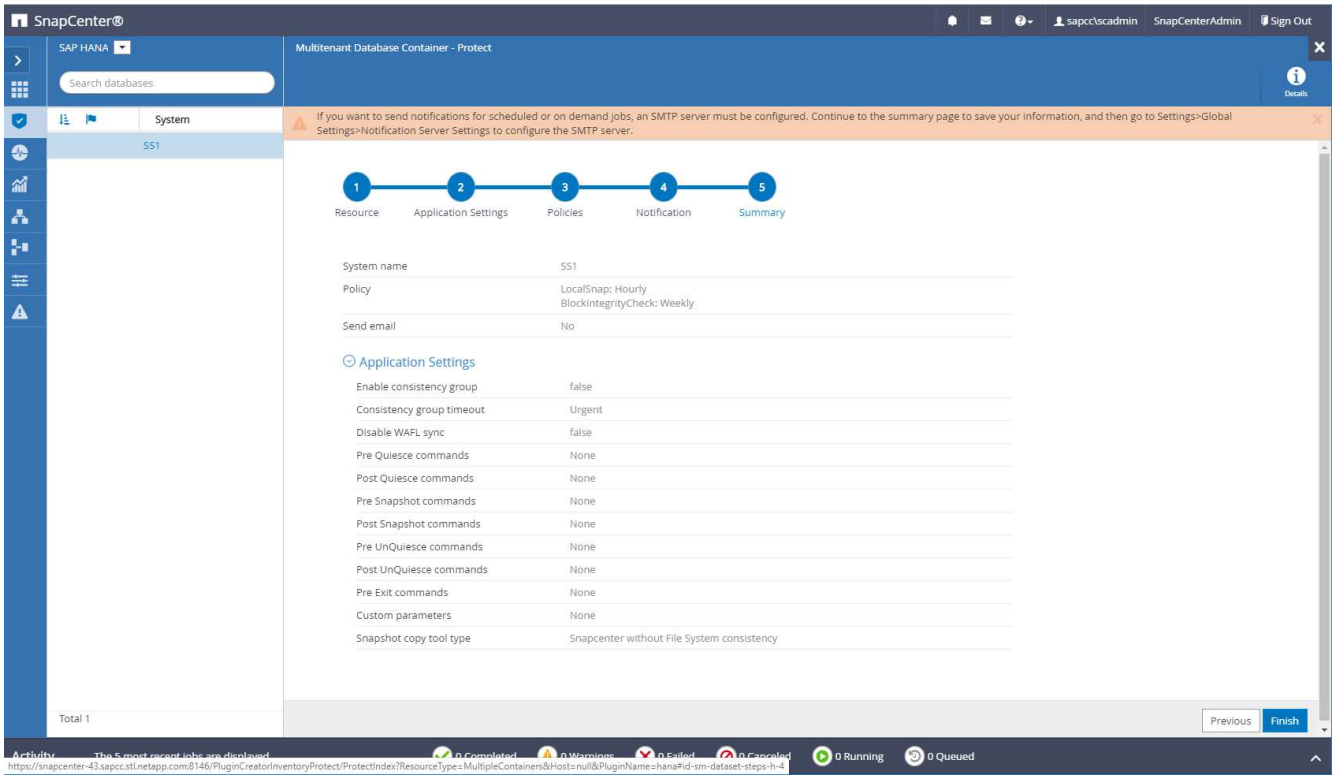
7. Définissez le planning de la stratégie de contrôle d'intégrité des blocs (dans cet exemple, une fois par semaine).



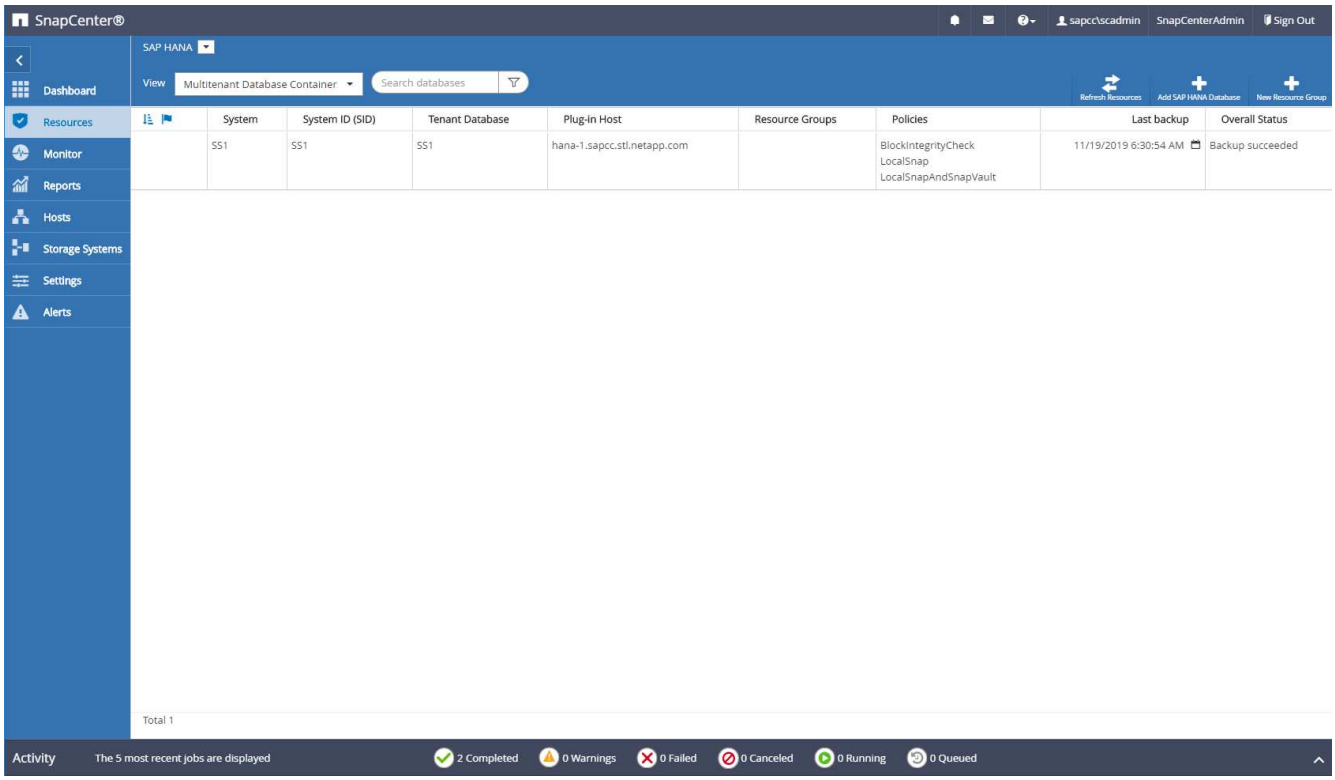
8. Fournir des informations sur la notification par e-mail.



9. Sur la page Récapitulatif, cliquez sur Terminer.



10. Des sauvegardes à la demande peuvent désormais être créées sur la page topologie. Les sauvegardes planifiées s'exécutent en fonction des paramètres de configuration.



Étapes de configuration supplémentaires pour les environnements SAN Fibre Channel

En fonction de la version HANA et du déploiement du plug-in HANA, des étapes de configuration supplémentaires sont requises pour les environnements dans lesquels les systèmes SAP HANA utilisent Fibre Channel et le système de fichiers XFS.

> Ces étapes de configuration supplémentaires sont uniquement nécessaires pour les ressources HANA, qui sont configurées manuellement dans SnapCenter. Elle est également requise uniquement pour les versions HANA 1.0 et HANA 2.0 jusqu'à SPS2.

Lorsqu'un point de sauvegarde HANA est déclenché par SnapCenter dans SAP HANA, SAP HANA écrit les fichiers Snapshot ID pour chaque locataire et service de base de données en dernière étape (par exemple, `/hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1`). Ces fichiers font partie du volume de données présent sur le stockage et font donc partie de la copie Snapshot de stockage. Ce fichier est obligatoire lors de l'exécution d'une récupération dans une situation où la sauvegarde est restaurée. En raison de la mise en cache des métadonnées avec le système de fichiers XFS sur l'hôte Linux, le fichier n'est pas immédiatement visible au niveau de la couche de stockage. La configuration XFS standard pour la mise en cache des métadonnées est de 30 secondes.

> Avec HANA 2.0 SPS3, SAP a modifié l'opération d'écriture de ces fichiers d'ID Snapshot de manière synchrone pour que la mise en cache des métadonnées ne pose pas de problème.

> Avec SnapCenter 4.3, si le plug-in HANA est déployé sur l'hôte de la base de données, le plug-in Linux exécute une opération de vidage du système de fichiers sur l'hôte avant le déclenchement du Snapshot de stockage. Dans ce cas, la mise en cache des métadonnées n'est pas un problème.

Dans SnapCenter, vous devez configurer un `postquiesce` Commande qui attend que le cache de métadonnées XFS soit vidé vers la couche disque.

La configuration réelle de la mise en cache des métadonnées peut être vérifiée à l'aide de la commande suivante :

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

NetApp recommande d'utiliser un temps d'attente deux fois supérieur à celui du `fs.xfs.xfssyncd_centisecs` paramètre. Comme la valeur par défaut est de 30 secondes, réglez la commande SLEEP sur 60 secondes.

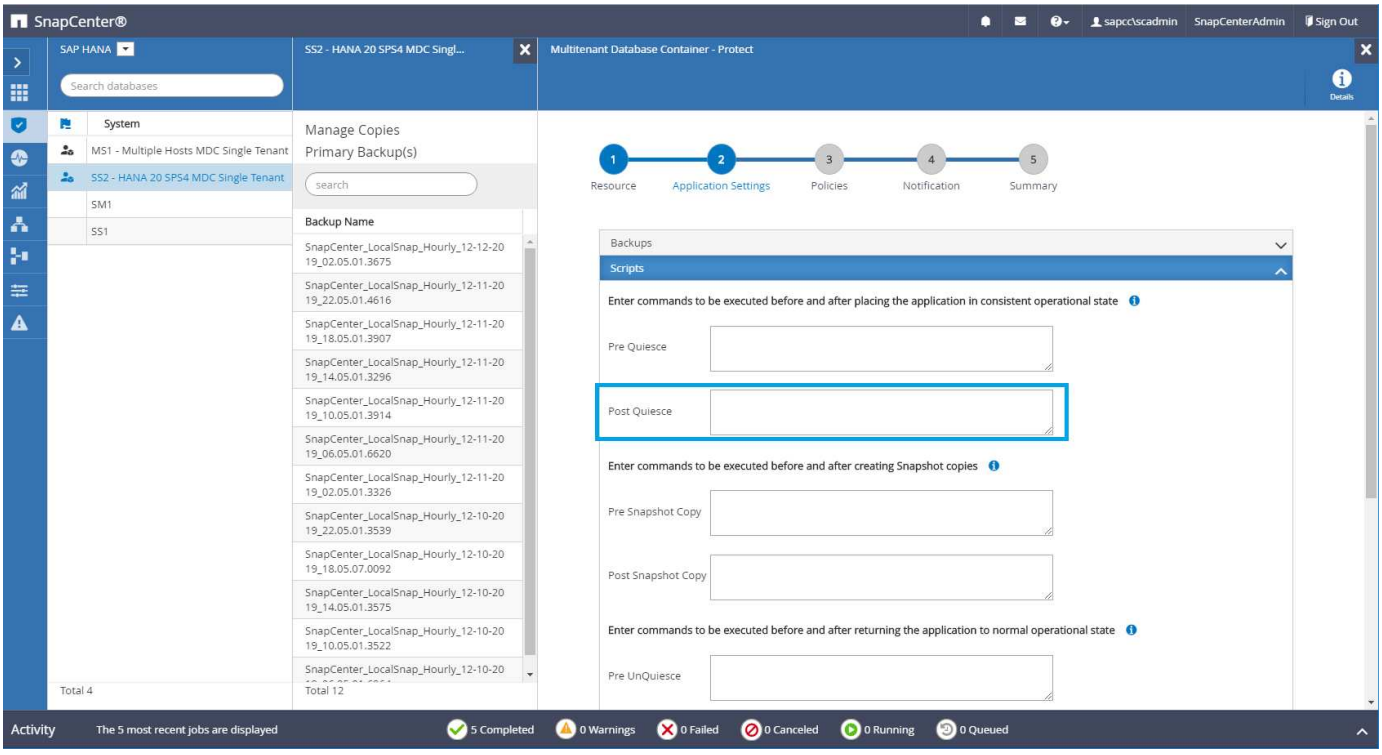
Si le serveur SnapCenter est utilisé en tant qu'hôte de plug-in HANA central, un fichier de commandes peut être utilisé. Le fichier de lot doit avoir le contenu suivant :

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

Le fichier batch peut être enregistré, par exemple, sous `C:\Program Files\NetApp\Wait60Sec.bat`. Dans la configuration de protection des ressources, le fichier batch doit être ajouté en tant que commande Post Quiesce.

Si un hôte Linux distinct est utilisé en tant qu'hôte de plug-in HANA central, vous devez configurer la commande `/bin/sleep 60` Comme commande Post Quiesce dans l'interface utilisateur SnapCenter.

La figure suivante montre la commande Post Quiesce dans l'écran de configuration de la protection des ressources.



Configuration SnapCenter propre à une ressource pour les sauvegardes de volumes autres que de données

La sauvegarde de volumes non-données fait partie intégrante du plug-in SAP HANA. La protection du volume des données de la base de données est suffisante pour restaurer et restaurer la base de données SAP HANA à un point donné dans le temps, à condition que les ressources d'installation de la base de données et les journaux requis soient toujours disponibles.

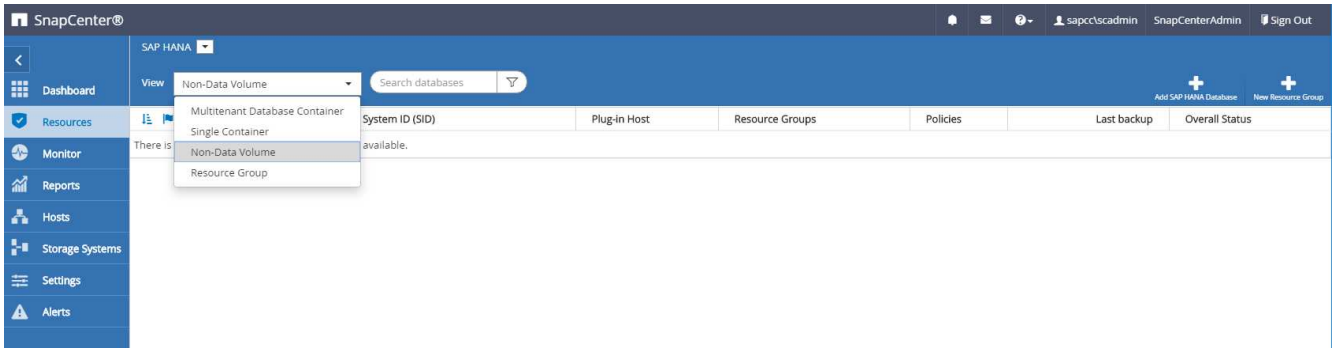
Pour restaurer des données à partir de situations où d'autres fichiers non data doivent être restaurés, NetApp recommande de développer une stratégie de sauvegarde supplémentaire pour les volumes sans data afin de compléter la sauvegarde de la base de données SAP HANA. En fonction de vos besoins spécifiques, la sauvegarde de volumes non-données peut varier dans les paramètres de fréquence de planification et de conservation. Il est également important de tenir compte de la fréquence à laquelle les fichiers ne sont pas des données sont modifiés. Par exemple, le volume HANA `/hana/shared` Contient des exécutables mais aussi des fichiers de trace SAP HANA. Alors que les exécutables ne changent que lorsque la base de données SAP HANA est mise à niveau, les fichiers de trace SAP HANA peuvent avoir besoin d'une fréquence de sauvegarde plus élevée pour prendre en charge l'analyse des problèmes avec SAP HANA.

La sauvegarde de volumes sans données SnapCenter permet de créer en quelques secondes des copies Snapshot de tous les volumes concernés avec la même efficacité d'espace que les sauvegardes de bases de données SAP HANA. La différence est qu'aucune communication SQL avec une base de données SAP HANA n'est requise.

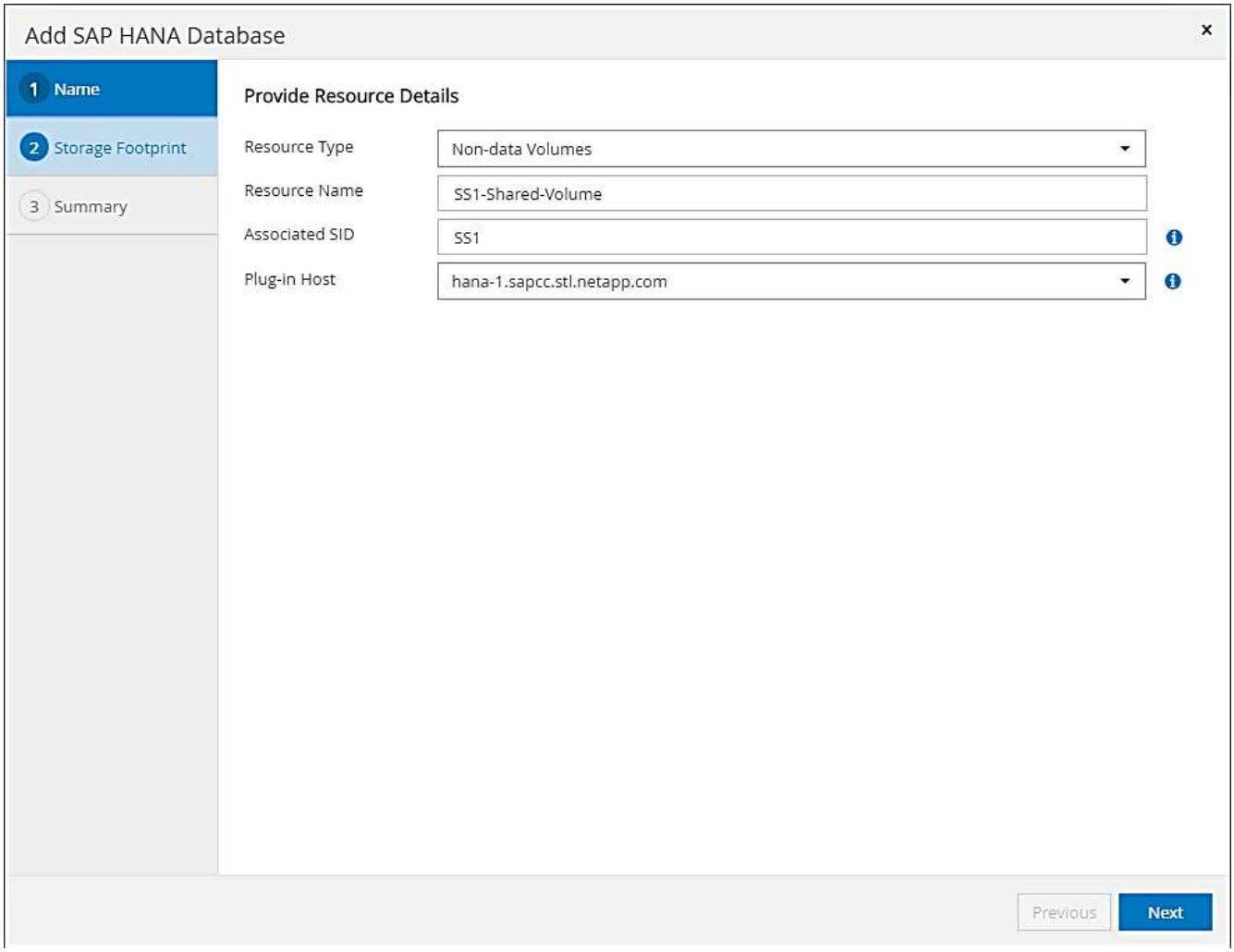
Configuration de ressources sans volume de données

Dans cet exemple, nous voulons protéger les volumes non-données de la base de données SAP HANA SS1.

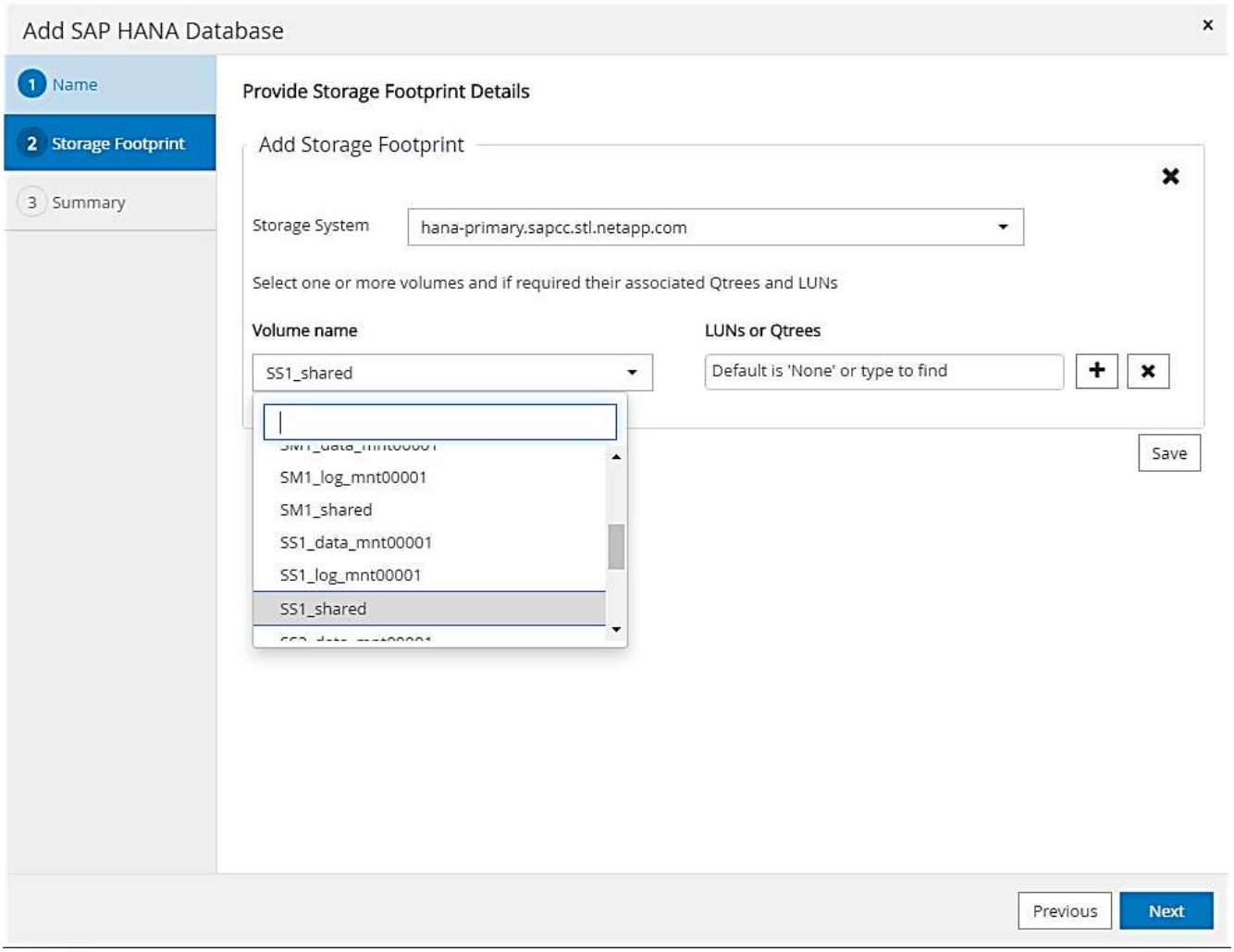
1. Dans l'onglet ressource, sélectionnez non-Volume de données et cliquez sur Ajouter base de données SAP HANA.



2. À l'étape une de la boîte de dialogue Ajouter une base de données SAP HANA, dans la liste Type de ressource, sélectionnez volumes non data. Spécifiez un nom pour la ressource, le SID associé et l'hôte du plug-in SAP HANA que vous souhaitez utiliser pour la ressource, puis cliquez sur Next (Suivant).



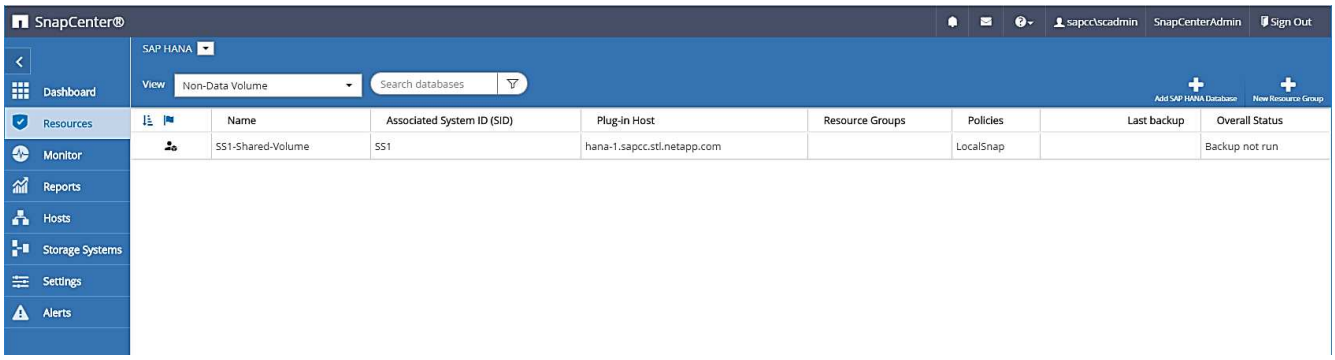
3. Ajoutez le SVM et le volume de stockage comme empreinte du stockage, puis cliquez sur « Next » (Suivant).



4. Dans l'étape de résumé, cliquez sur Terminer pour enregistrer les paramètres.
5. Répétez ces étapes pour tous les volumes autres que de données requis.
6. Poursuivre la configuration de protection de la nouvelle ressource.

> La protection des données pour des ressources sans volume de données est identique au workflow pour les ressources de base de données SAP HANA et peut être définie au niveau des ressources individuelles.

La figure suivante présente la liste des ressources de volumes non-données configurées.



Groupes de ressources

Les groupes de ressources sont un moyen pratique de définir la protection de plusieurs ressources qui nécessitent les mêmes règles de protection et la même planification. Les ressources individuelles faisant partie d'un groupe de ressources peuvent toujours être protégées au niveau individuel.

Les groupes de ressources offrent les fonctions suivantes :

- Vous pouvez ajouter une ou plusieurs ressources à un groupe de ressources. Toutes les ressources doivent appartenir au même plug-in SnapCenter.
- La protection peut être définie au niveau d'un groupe de ressources. Toutes les ressources du groupe de ressources utilisent la même stratégie et la même planification lorsqu'elles sont protégées.
- Toutes les sauvegardes du référentiel SnapCenter et des copies Snapshot de stockage portent le même nom défini dans la protection des ressources.
- Les opérations de restauration sont appliquées à un seul niveau de ressources et non à un groupe de ressources.
- Lors de l'utilisation de SnapCenter pour supprimer la sauvegarde d'une ressource créée au niveau d'un groupe de ressources, cette sauvegarde est supprimée pour toutes les ressources du groupe de ressources. La suppression de la sauvegarde inclut la suppression de la sauvegarde du référentiel SnapCenter ainsi que la suppression des copies Snapshot de stockage.
- Les groupes de ressources se servent principalement lorsqu'un client souhaite utiliser les sauvegardes créées avec SnapCenter pour le clonage de système avec SAP Landscape Management. Ceci est décrit dans la section suivante.

Avec SnapCenter et la gestion de l'environnement SAP

Avec SAP Landscape Management (SAP Lama), les clients peuvent gérer des paysages de système SAP complexes dans des data centers sur site ainsi que des systèmes exécutés dans le cloud. SAP Lama, associé à NetApp Storage Services Connector (SSC), peut exécuter des opérations de stockage telles que le clonage et la réplication pour les cas d'utilisation de clonage, de copie et d'actualisation des systèmes SAP à l'aide des technologies Snapshot et FlexClone. Vous pouvez ainsi automatiser entièrement la copie du système SAP selon la technologie de clonage du stockage et le post-traitement SAP requis. Pour plus d'informations sur les solutions NetApp pour SAP Lama, consultez "Tr-4018 : intégration des systèmes NetApp ONTAP à la gestion du paysage SAP".

NetApp SSC et SAP Lama peuvent créer des copies Snapshot à la demande directement avec NetApp SSC, mais ils peuvent également utiliser des copies Snapshot créées à l'aide de SnapCenter. Pour utiliser les sauvegardes SnapCenter comme base des opérations de clonage et de copie du système avec SAP Lama, les conditions préalables suivantes doivent être remplies :

- SAP Lama requiert que tous les volumes soient inclus dans la sauvegarde, notamment les données SAP HANA, les journaux et les volumes partagés.
- Tous les noms de snapshot de stockage doivent être identiques.
- Les noms des snapshots de stockage doivent commencer par VCM.

> Dans les opérations de sauvegarde normales, NetApp ne recommande pas d'inclure le volume du journal. Si vous restaurez le volume du journal à partir d'une sauvegarde, il écrase les derniers journaux de reprise actifs et empêche la restauration de la base de données vers le dernier état récent.

Les groupes de ressources SnapCenter répondent à toutes ces exigences. Trois ressources sont configurées

dans SnapCenter : une ressource pour le volume de données, le volume du journal et le volume partagé. Les ressources sont placées dans un groupe de ressources et la protection est ensuite définie au niveau du groupe de ressources. Dans la protection du groupe de ressources, le nom d'instantané personnalisé doit être défini avec VCM au début.

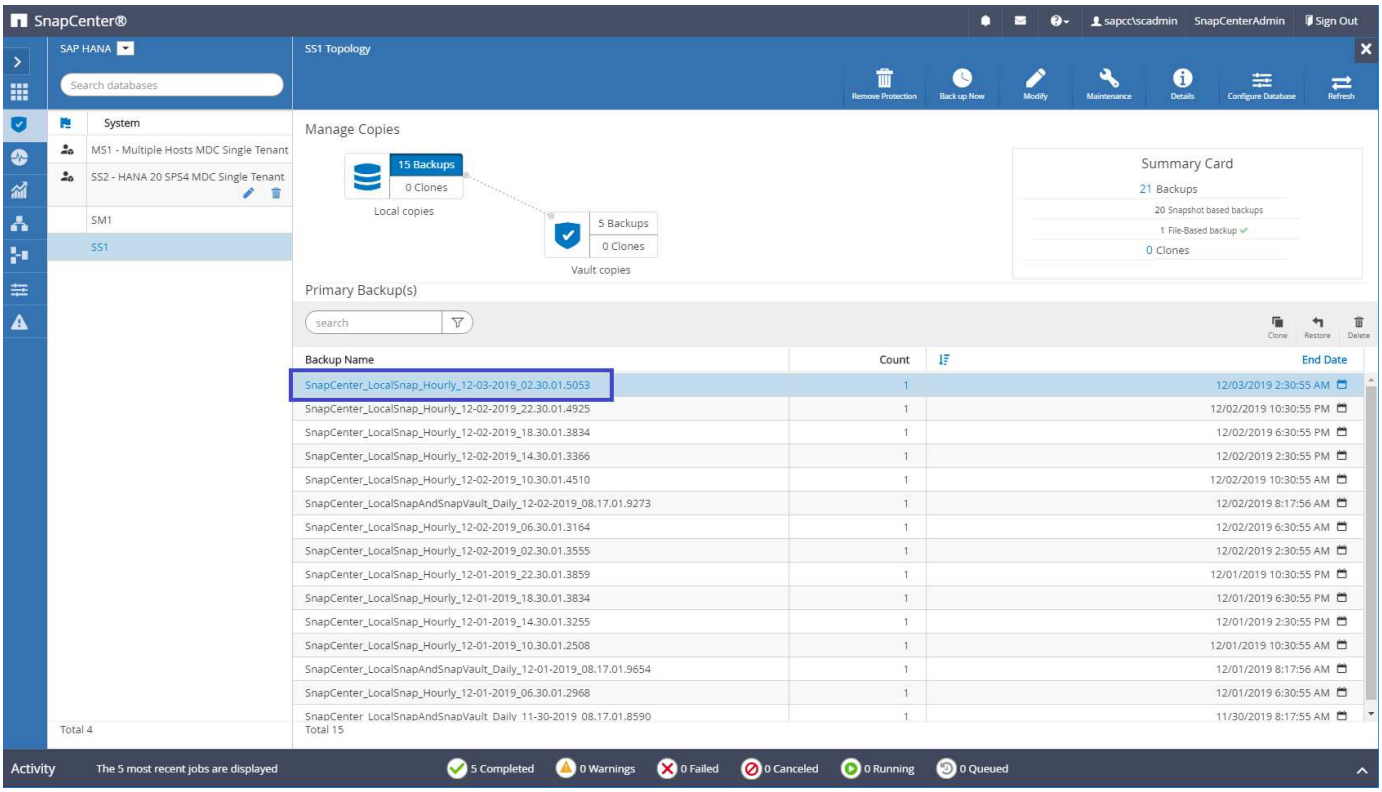
Sauvegardes de bases de données

Dans SnapCenter, les sauvegardes de bases de données sont généralement exécutées à l'aide des planifications définies dans la configuration de protection des ressources de chaque base de données HANA.

Il est possible d'effectuer une sauvegarde de base de données à la demande via l'interface graphique SnapCenter, une ligne de commande PowerShell ou des API REST.

Identification des sauvegardes SnapCenter dans SAP HANA Studio

La topologie de ressource SnapCenter affiche la liste des sauvegardes créées à l'aide de SnapCenter. La figure suivante montre les sauvegardes disponibles dans le stockage primaire et souligne la sauvegarde la plus récente.

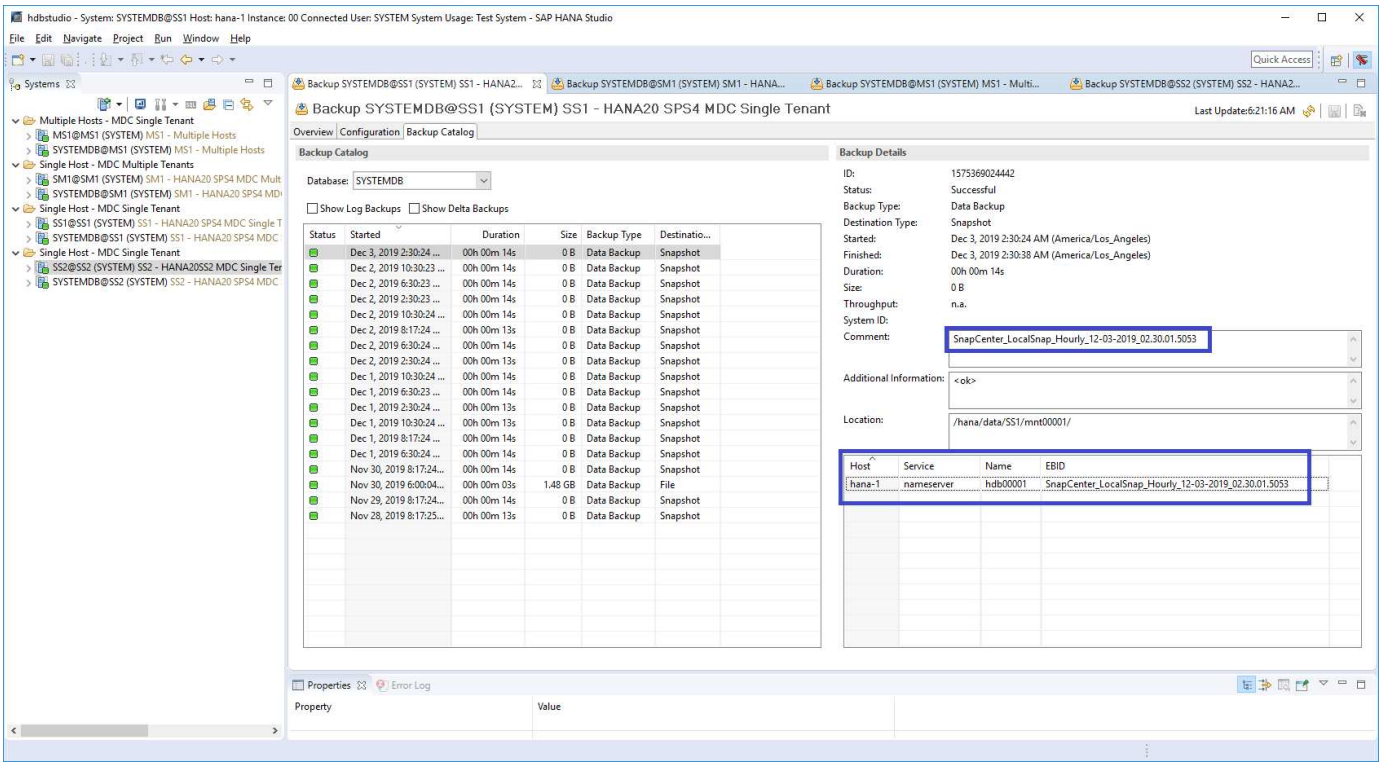


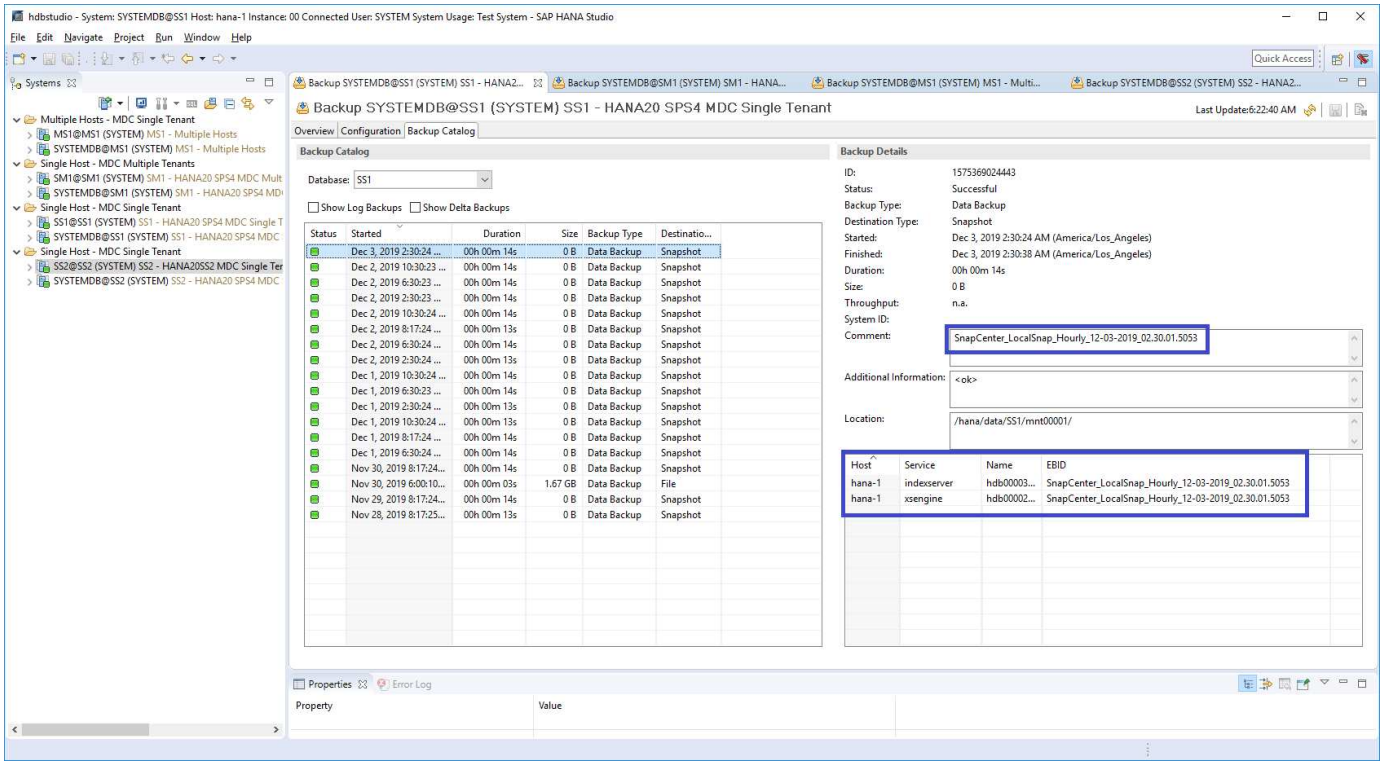
Lors de l'exécution d'une sauvegarde avec des copies Snapshot de stockage pour un système SAP HANA MDC, une copie Snapshot du volume de données est créée. Ce volume de données contient les données de la base de données système ainsi que les données de toutes les bases de données des locataires. Pour refléter cette architecture physique, SAP HANA effectue en interne une sauvegarde combinée de la base de données système et de toutes les bases de données en locataire lorsqu'SnapCenter déclenche une sauvegarde Snapshot. Ce qui entraîne la création de plusieurs entrées de sauvegarde distinctes dans le catalogue des sauvegardes SAP HANA : une pour la base de données système et une pour chaque locataire.

Pour les systèmes à conteneur unique SAP HANA, le volume de base de données ne contient que la seule base de données et il n'existe qu'une seule entrée dans le catalogue de sauvegarde de SAP HANA.

Dans le catalogue des sauvegardes SAP HANA, le nom de la sauvegarde SnapCenter est stocké comme A. `Comment` champ également `External Backup ID (EBID)`. Cette illustration est présentée dans la capture d'écran suivante pour la base de données du système et dans la capture d'écran qui suit pour la base de données du locataire SS1. Les deux chiffres mettent en évidence le nom de sauvegarde SnapCenter stocké dans le champ de commentaire et EBID.

La version HANA 2.0 SPS4 (révision 40 et 41) affiche toujours une taille de sauvegarde de zéro pour les sauvegardes basées sur des snapshots. Ceci a été corrigé avec la révision 42. Pour plus d'informations, consultez la note SAP "https://launchpad.support.sap.com/#/notes/2795010".

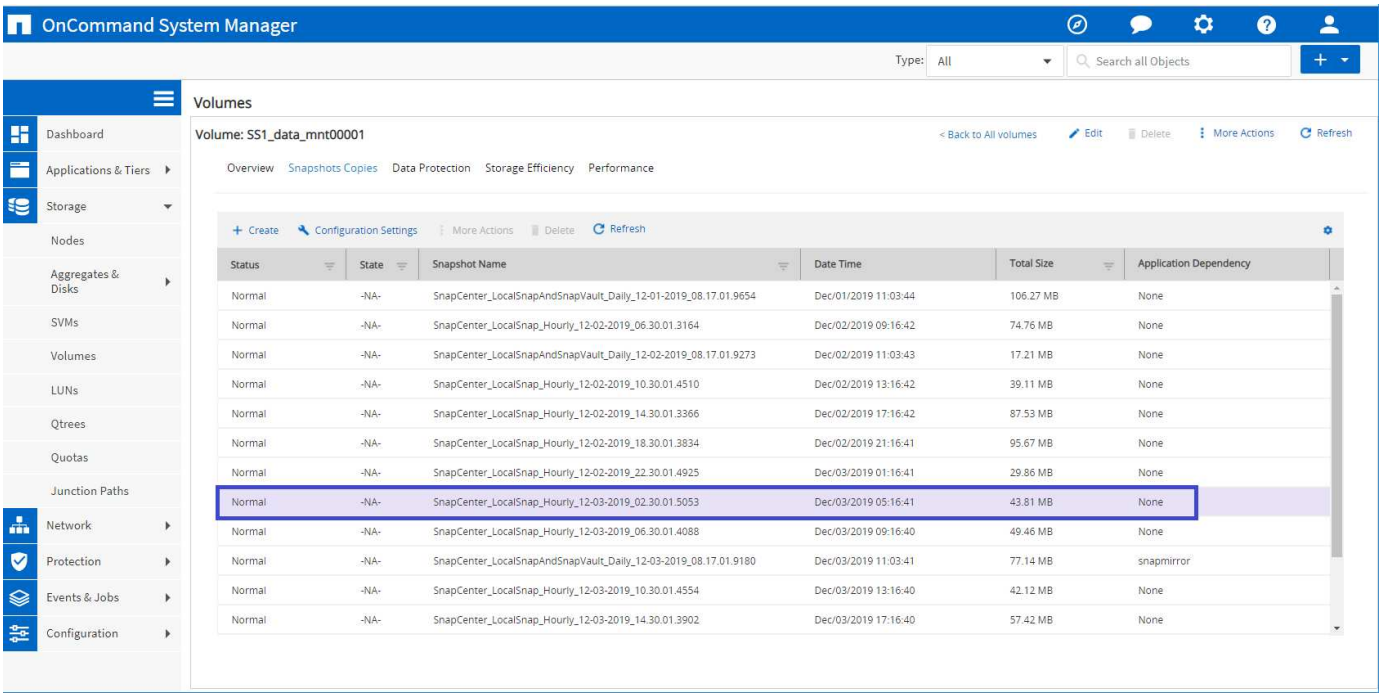




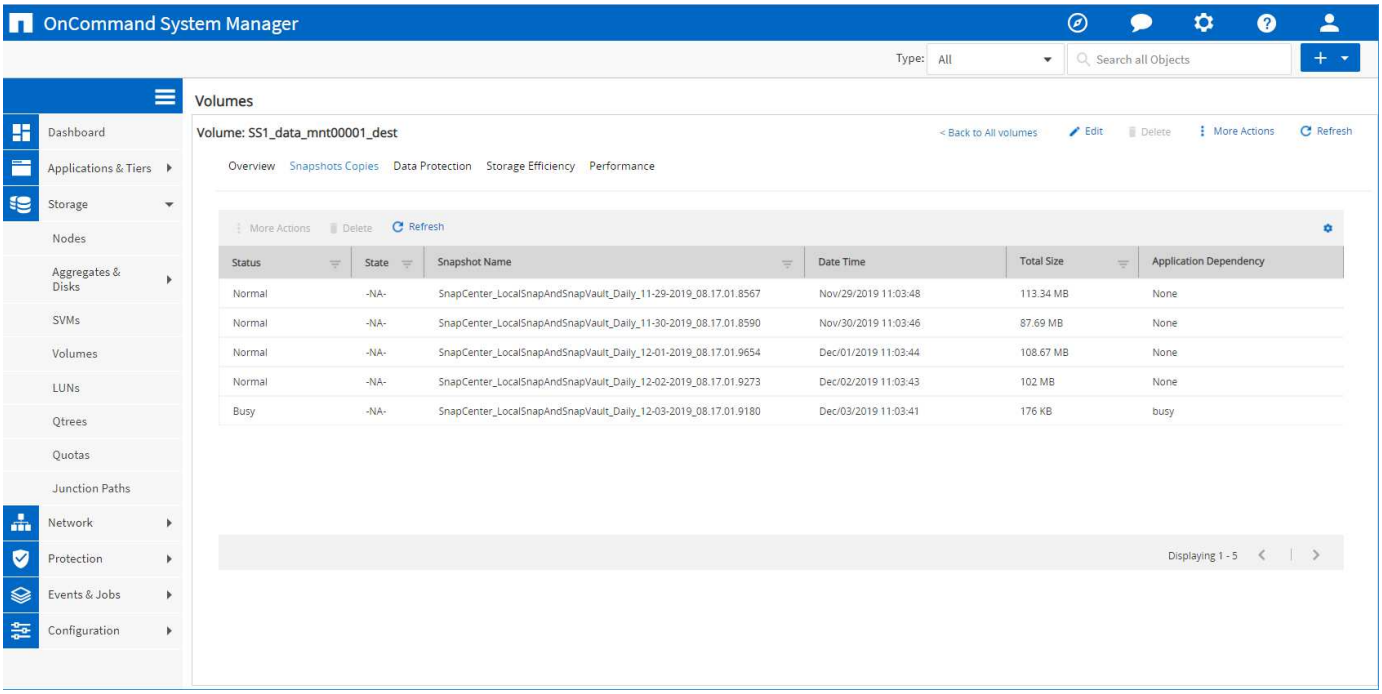
SnapCenter ne connaît que ses propres sauvegardes. Les sauvegardes supplémentaires créées, par exemple avec SAP HANA Studio, sont visibles dans le catalogue SAP HANA, mais pas dans SnapCenter.

Identification des sauvegardes SnapCenter sur les systèmes de stockage

Pour afficher les sauvegardes sur la couche de stockage, utilisez NetApp OnCommand System Manager et sélectionnez le volume de base de données dans la vue SVM—Volume. L'onglet inférieur des copies Snapshot affiche les copies Snapshot du volume. La capture d'écran suivante montre les sauvegardes disponibles pour le volume de base de données `SS1_data_mnt00001` au niveau du stockage primaire. La sauvegarde mise en surbrillance est la sauvegarde présentée dans SnapCenter et SAP HANA Studio dans les images précédentes et respectant la même convention de nom.



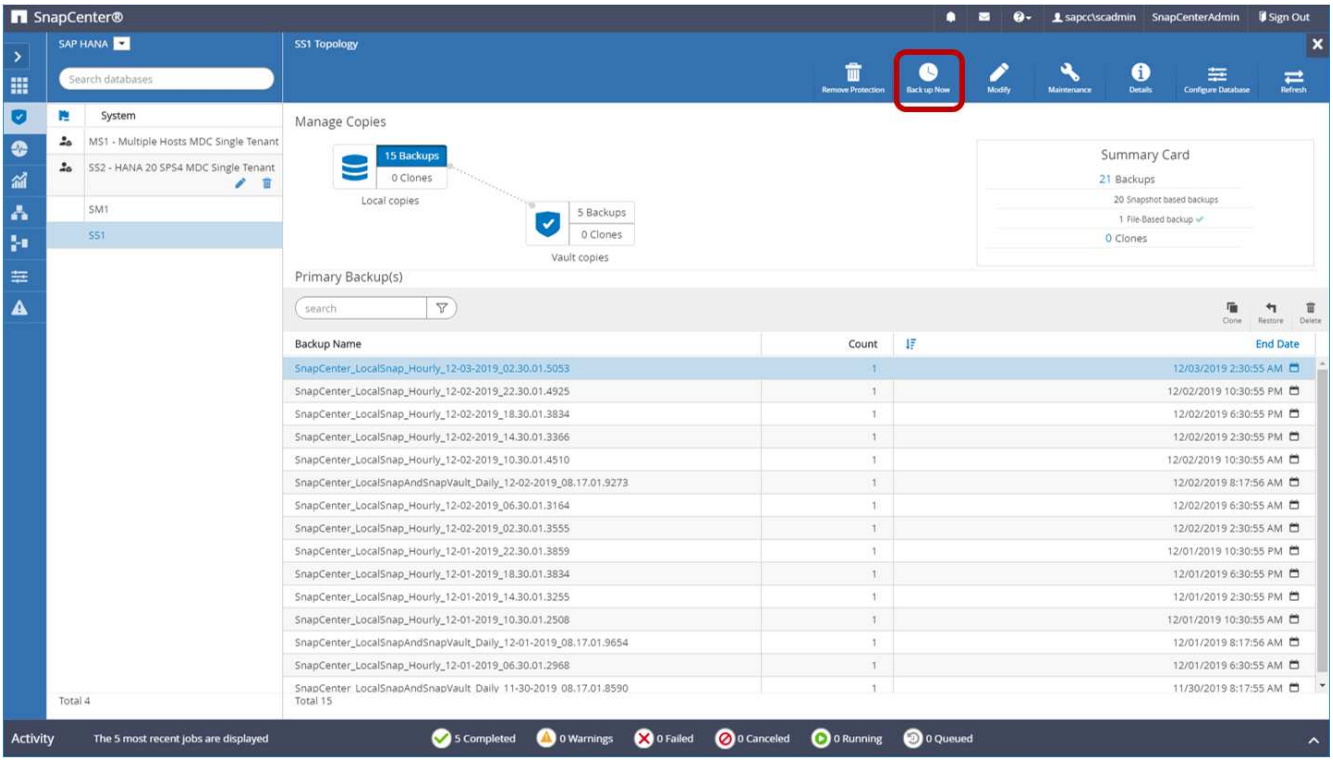
La capture d'écran suivante présente les sauvegardes disponibles pour le volume cible de réplication `hana_SA1_data_mnt00001_dest` au niveau du système de stockage secondaire.



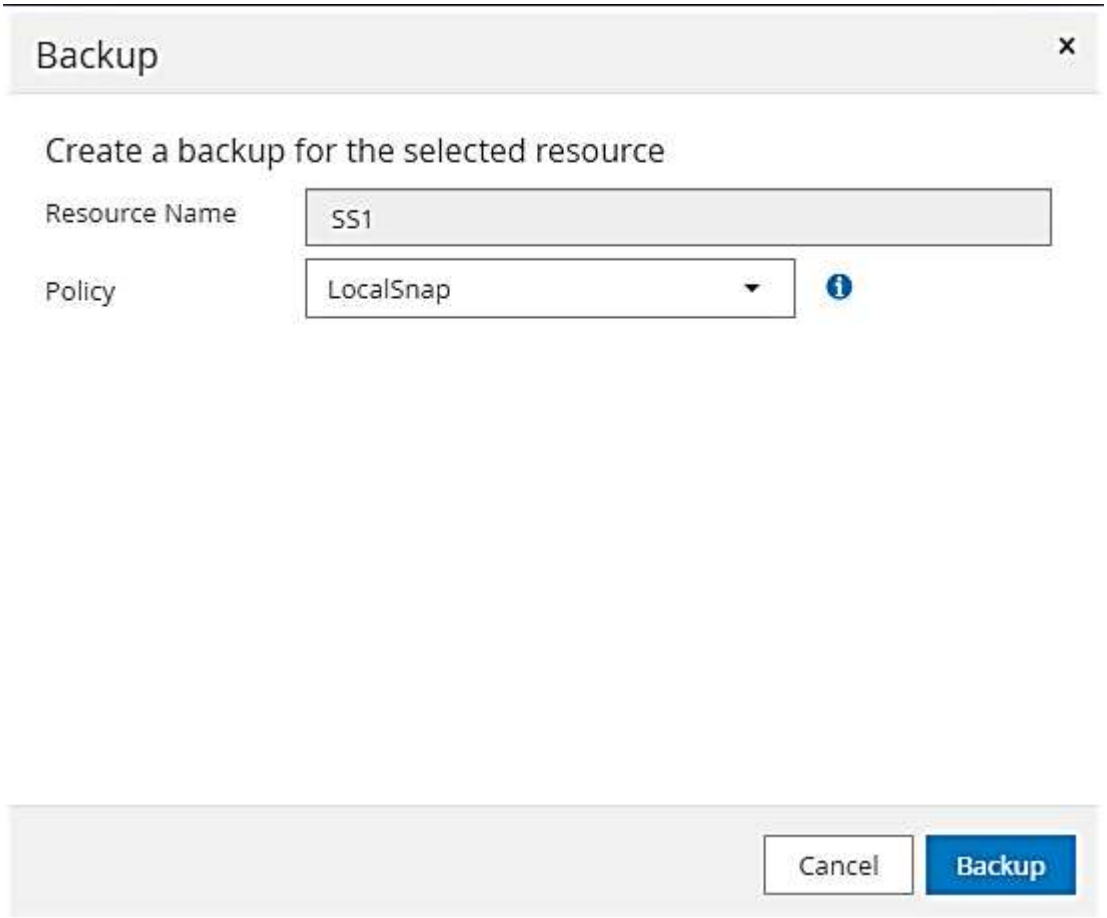
Sauvegarde de base de données sur demande dans le stockage primaire

1. Dans la vue ressource, sélectionnez la ressource et double-cliquez sur la ligne pour passer à la vue topologique.

   La vue topologie des ressources fournit une vue d'ensemble de toutes les sauvegardes disponibles qui ont été créées à l'aide de SnapCenter. La partie supérieure de cette vue affiche la topologie de sauvegarde, en affichant les sauvegardes sur le stockage primaire (copies locales) et, le cas échéant, sur le stockage de sauvegarde hors site (copies vault).

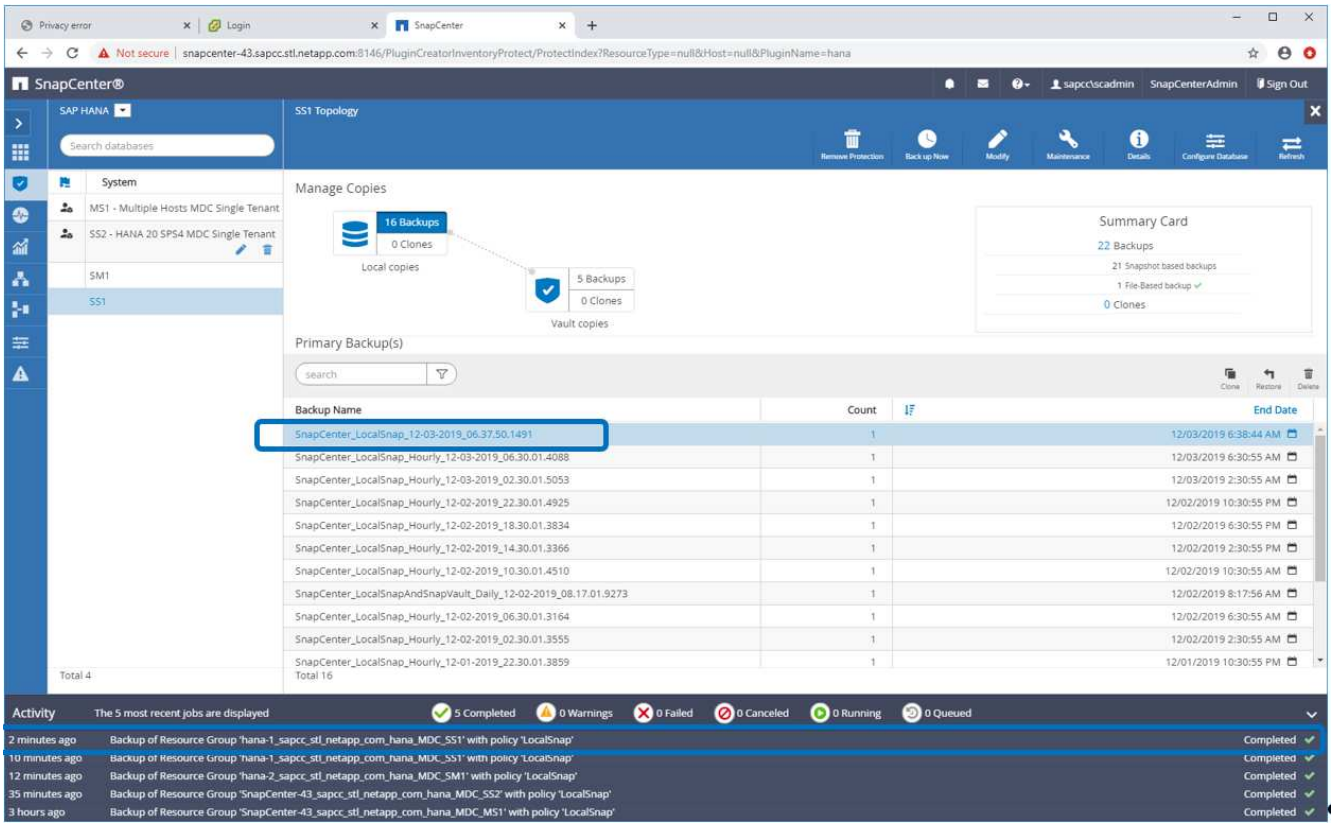


2. Dans la ligne supérieure, sélectionnez l'icône Sauvegarder maintenant pour lancer une sauvegarde à la demande. Dans la liste déroulante, sélectionnez la stratégie de sauvegarde `LocalSnap` Cliquez ensuite sur Sauvegarder pour lancer la sauvegarde à la demande.

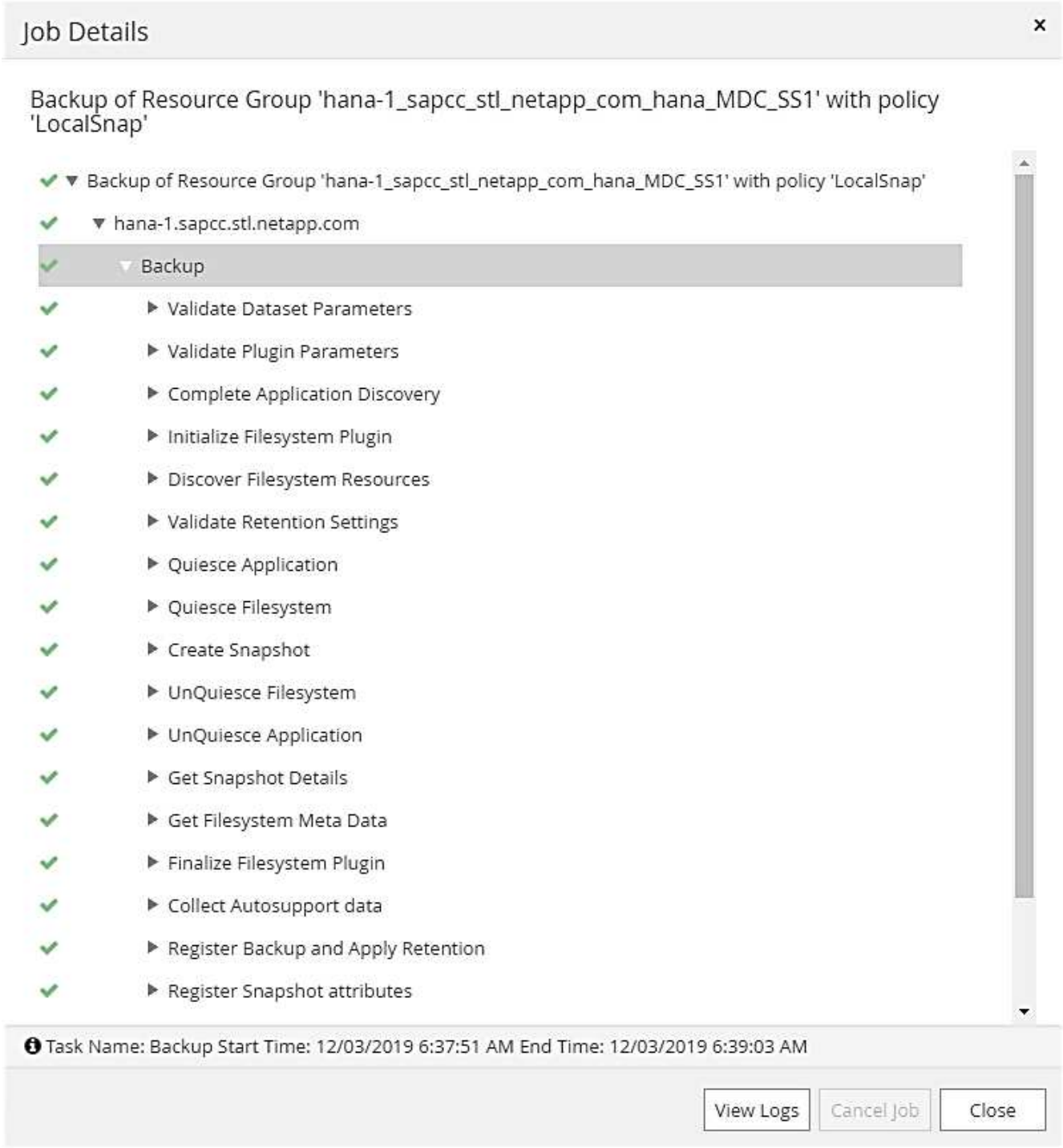


Cette opération démarre la procédure de sauvegarde. Un journal des cinq tâches précédentes est affiché dans la zone activité sous la vue topologique. Une fois la sauvegarde terminée, une nouvelle entrée s'affiche dans la vue topologique. Les noms de sauvegarde suivent la même nomenclature que le nom de Snapshot défini dans la section ""“Configuration de la protection des ressources.”"

Vous devez fermer et rouvrir la vue topologique pour afficher la liste des sauvegardes mise à jour.



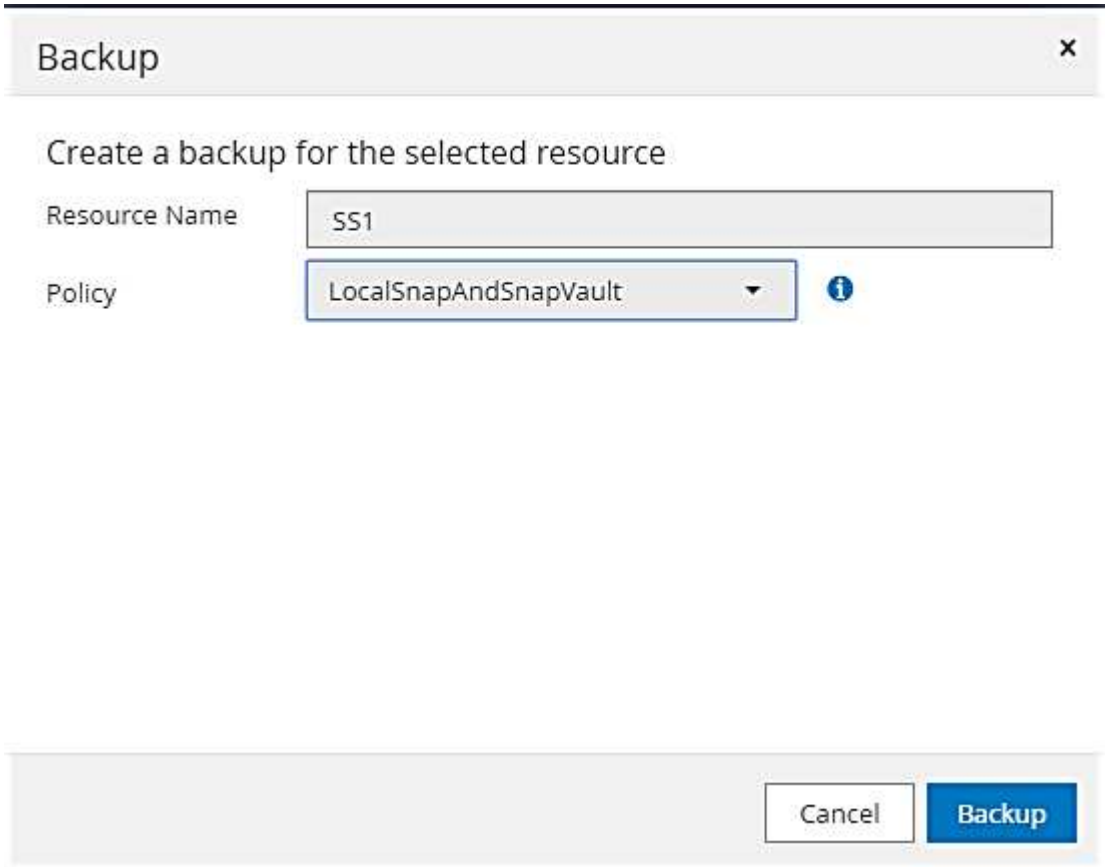
3. Les détails du travail s'affichent lorsque vous cliquez sur la ligne d'activité du travail dans la zone activité. Vous pouvez ouvrir un journal détaillé des travaux en cliquant sur Afficher les journaux.



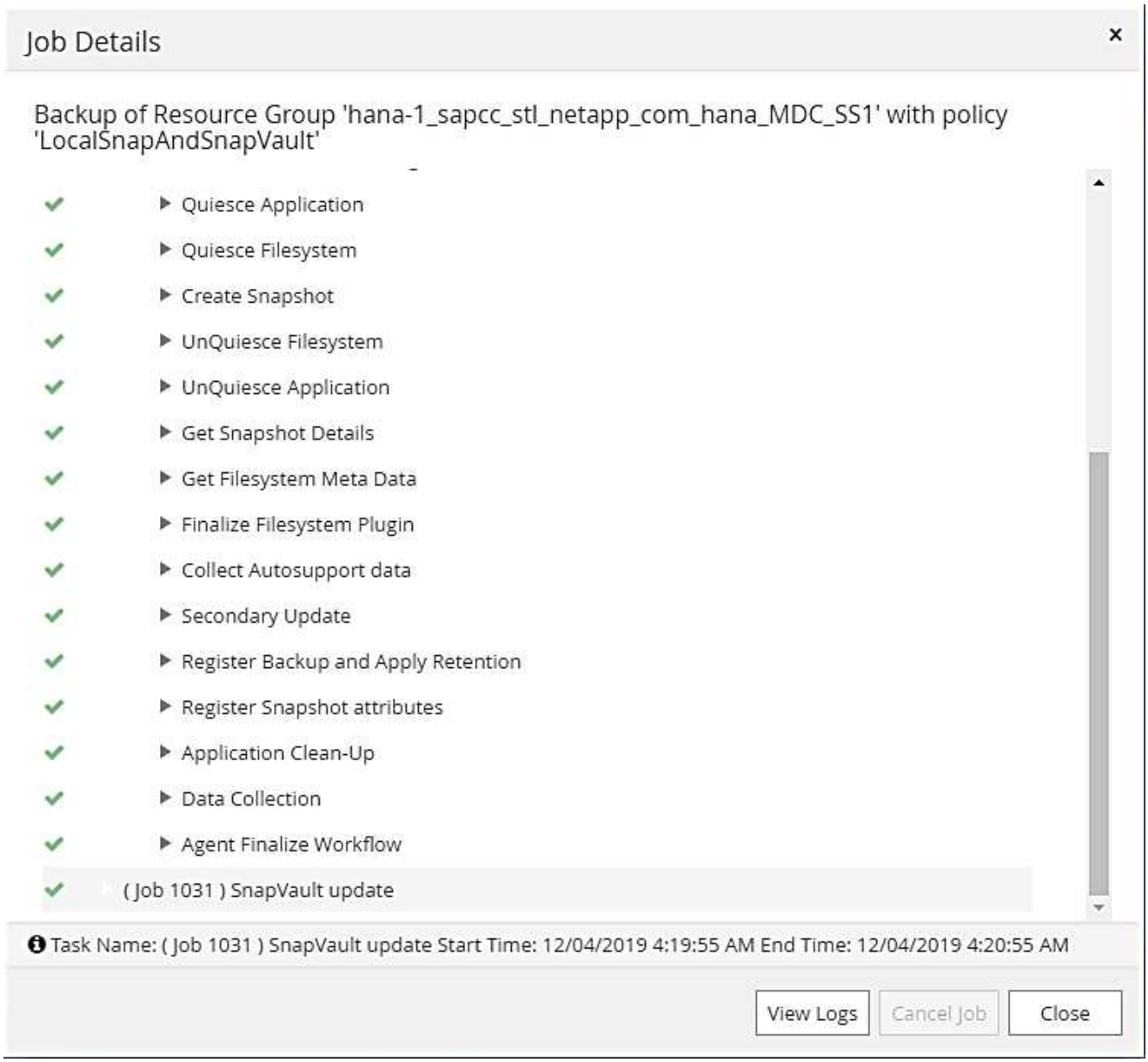
4. Dans SAP HANA Studio, la nouvelle sauvegarde est visible dans le catalogue des sauvegardes. Le même nom de sauvegarde dans SnapCenter est également utilisé dans le commentaire et dans le champ EBID du catalogue de sauvegarde.

Sauvegardes de bases de données sur demande avec la réplication SnapVault

1. Dans la vue ressource, sélectionnez la ressource et double-cliquez sur la ligne pour passer à la vue topologique.
2. Dans la ligne supérieure, sélectionnez l'icône Sauvegarder maintenant pour lancer une sauvegarde à la demande. Dans la liste déroulante, sélectionnez la stratégie de sauvegarde `LocalSnapAndSnapVault`, Puis cliquez sur Sauvegarder pour démarrer la sauvegarde à la demande.

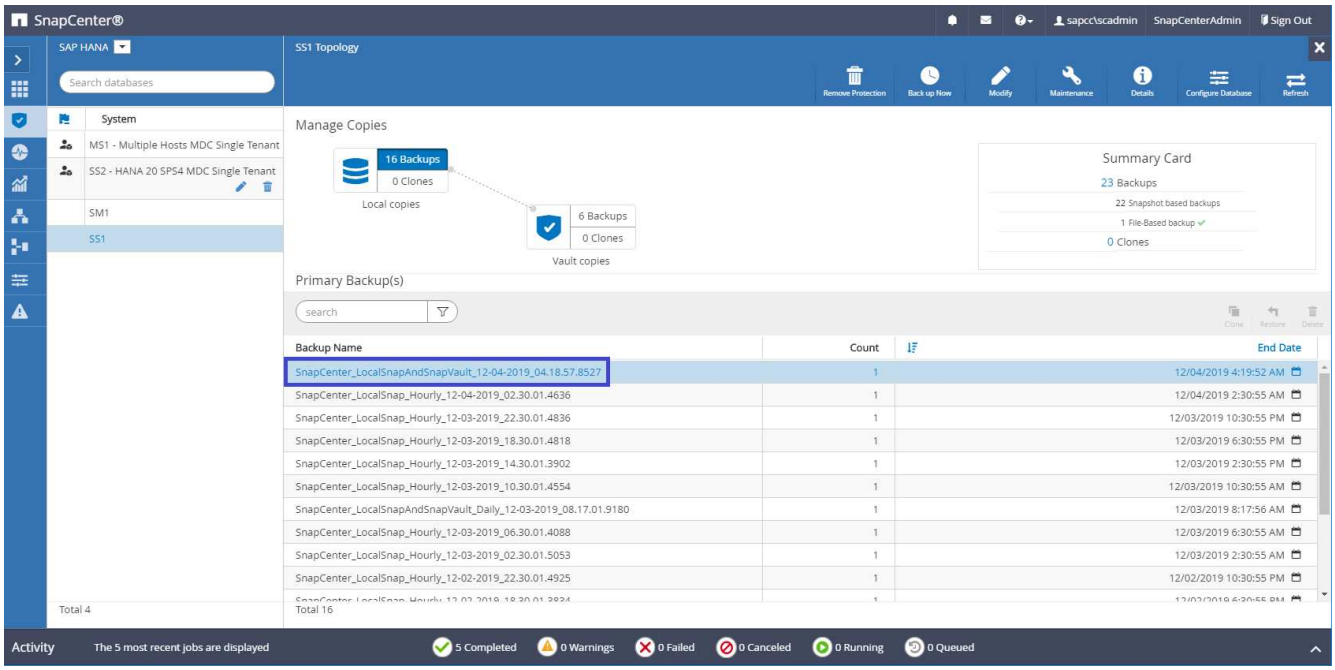


3. Les détails du travail s’affichent lorsque vous cliquez sur la ligne d’activité du travail dans la zone activité.

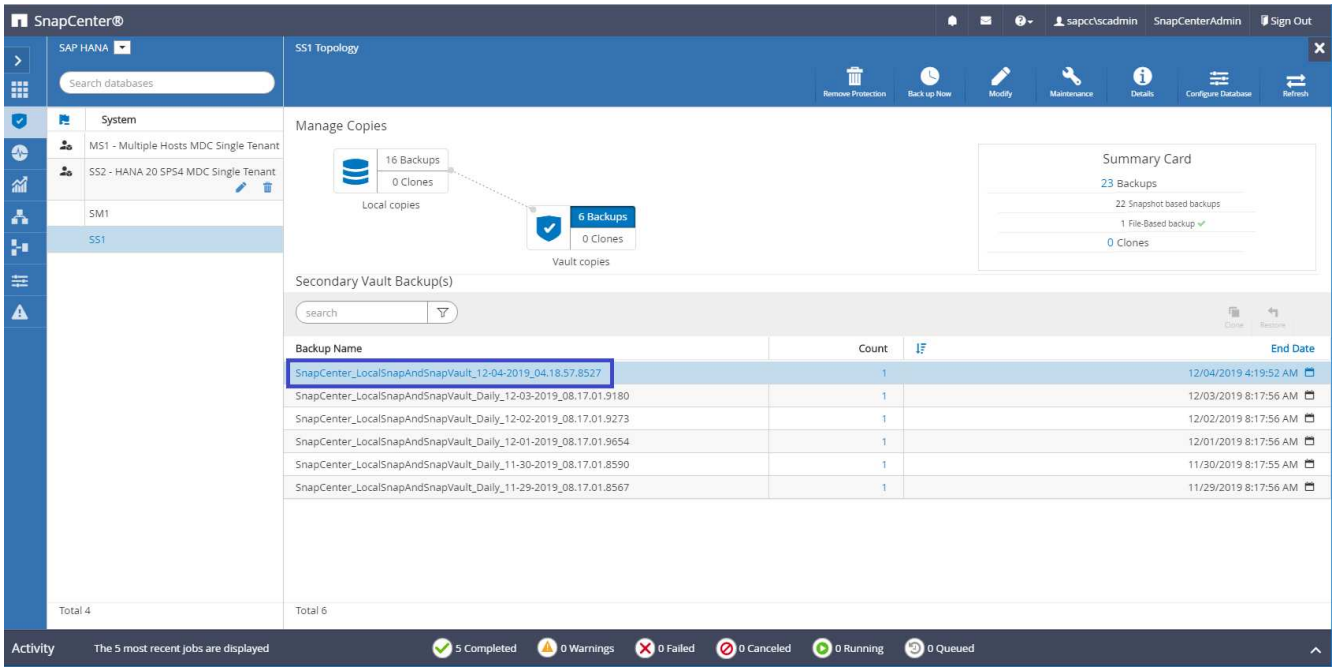


4. Une fois la sauvegarde terminée, une nouvelle entrée s'affiche dans la vue topologique. Les noms de sauvegarde suivent la même nomenclature que le nom de Snapshot défini dans la section ""Configuration de la protection des ressources."".

Vous devez fermer et rouvrir la vue topologique pour afficher la liste des sauvegardes mise à jour.



5. En sélectionnant les copies du coffre-fort, les sauvegardes sur le stockage secondaire sont affichées. Le nom de la sauvegarde répliquée est identique au nom de la sauvegarde sur le stockage primaire.



6. Dans SAP HANA Studio, la nouvelle sauvegarde est visible dans le catalogue des sauvegardes. Le même nom de sauvegarde dans SnapCenter est également utilisé dans le commentaire et dans le champ EBID du catalogue de sauvegarde.

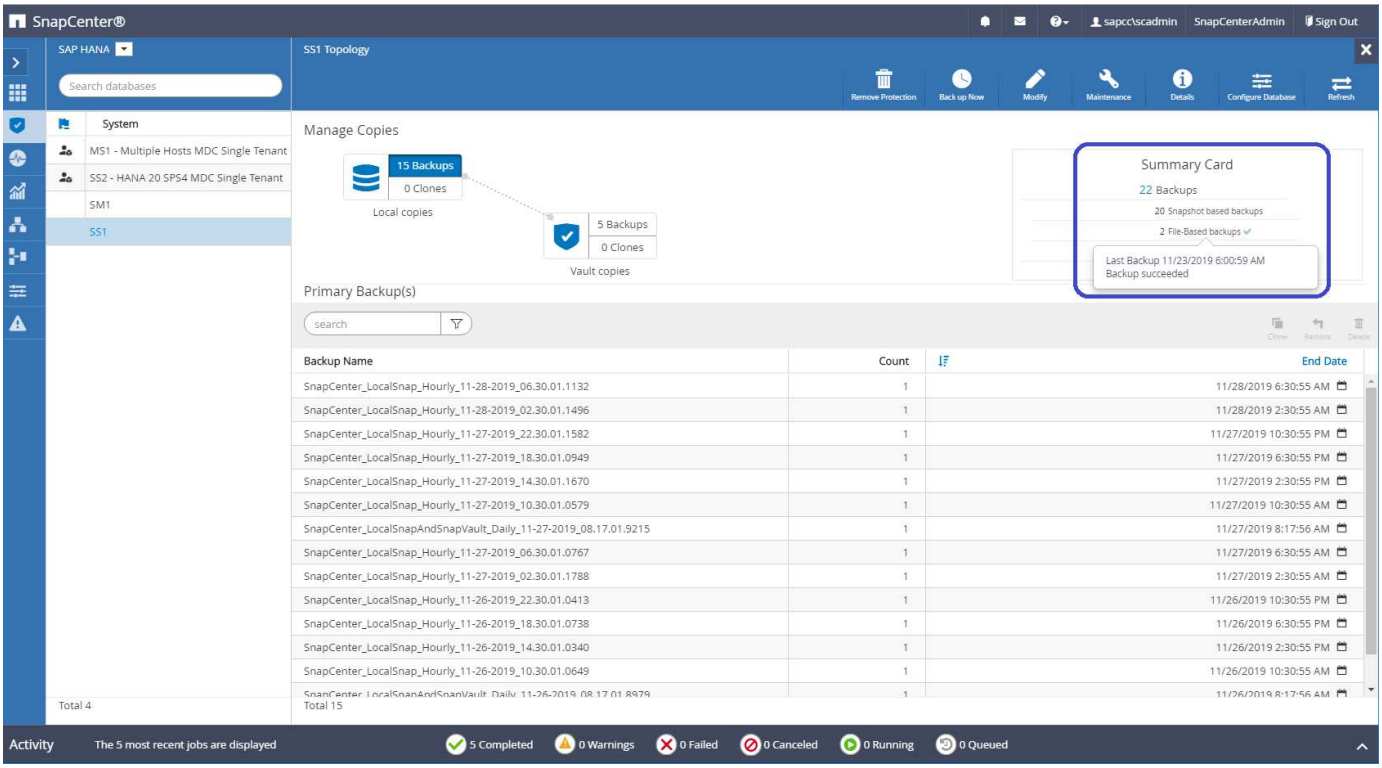
Vérification de l’intégrité des blocs

SAP recommande de combiner des sauvegardes Snapshot basées sur le stockage et une sauvegarde hebdomadaire basée sur des fichiers pour exécuter une vérification de l’intégrité des blocs. SnapCenter prend en charge la vérification de l’intégrité des blocs grâce à une règle permettant de sélectionner la sauvegarde basée sur des fichiers

comme type de sauvegarde.

Lorsque vous planifiez des sauvegardes à l'aide de cette règle, SnapCenter crée une sauvegarde standard des fichiers SAP HANA pour les bases de données système et locataires.

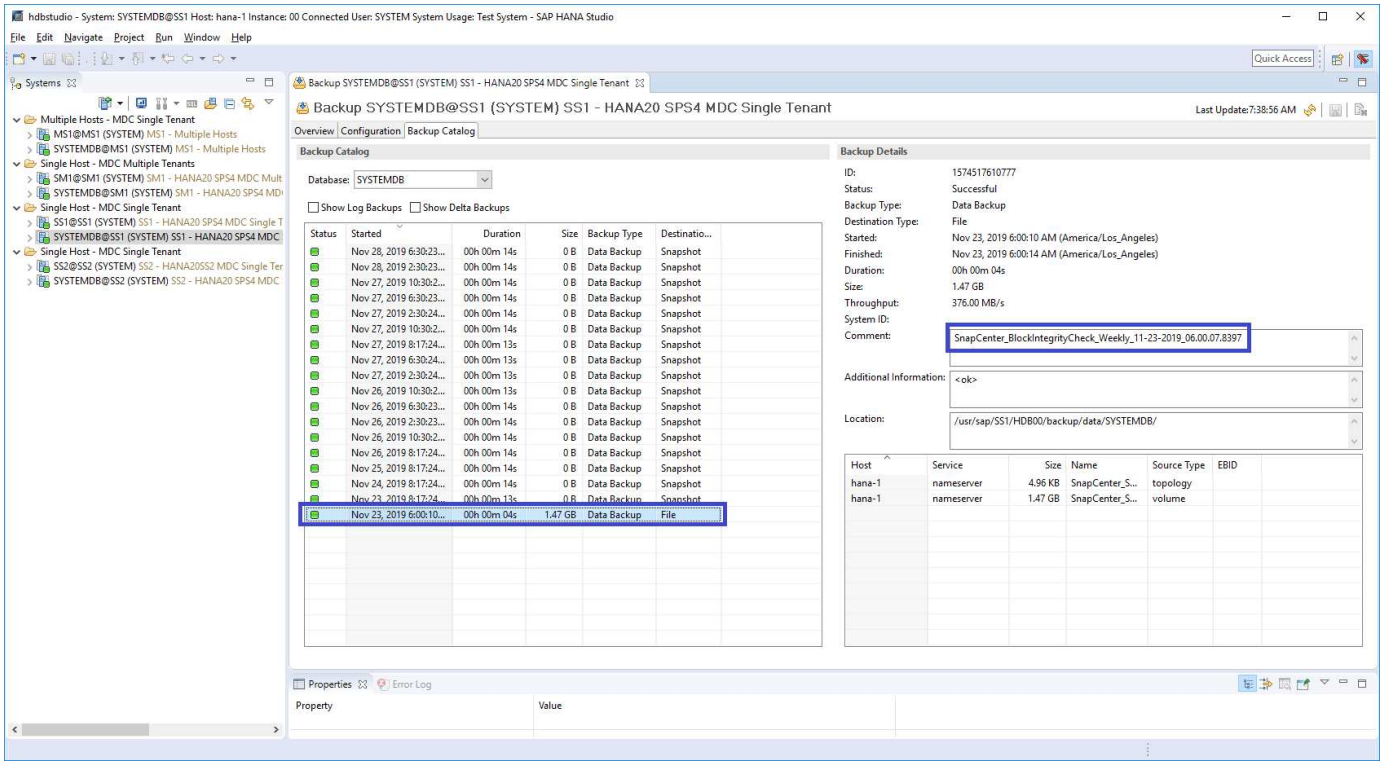
SnapCenter n'affiche pas la vérification de l'intégrité des blocs, de la même manière que les sauvegardes basées sur des copies Snapshot. À la place, la carte récapitulative affiche le nombre de sauvegardes basées sur des fichiers et l'état de la sauvegarde précédente.



Une sauvegarde de contrôle d'intégrité des blocs ne peut pas être supprimée à l'aide de l'interface utilisateur SnapCenter, mais pourra être supprimée à l'aide des commandes PowerShell.

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

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

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


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



PS C:\Users\scadmin>
```

Le catalogue de sauvegardes SAP HANA affiche les entrées des bases de données système et locataire. La figure suivante montre une vérification de l'intégrité des blocs SnapCenter dans le catalogue de sauvegardes de la base de données système.



Un contrôle réussi de l'intégrité des blocs crée des fichiers de sauvegarde standard des données SAP HANA. SnapCenter utilise le chemin de sauvegarde configuré dans la base de données HANA pour des opérations de sauvegarde de données basées sur des fichiers.

```
hana-1:/usr/sap/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 1710840
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:25 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys   83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ss1adm sapsys 1660952576 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_3_1
SYSTEMDB:
total 1546340
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:24 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys 1577066496 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_1_1
```

Restauration et reprise

Les sections qui suivent décrivent les flux de travail de restauration et de restauration de trois scénarios et exemples de configuration.

- Restauration et récupération automatisées :
  - Système HANA SS1 découvert automatiquement
  - SAP HANA à un seul hôte, système MDC à un seul locataire utilisant NFS
- Restauration et restauration d'un seul locataire :
  - Système HANA SM1 découvert automatiquement
  - SAP HANA à un seul hôte, système MDC pour plusieurs locataires utilisant NFS
- Restauration avec récupération manuelle :
  - Système HANA SS2 configuré manuellement
  - SAP HANA à un seul hôte, système MDC pour plusieurs locataires utilisant NFS

Les différences entre les hôtes SAP HANA uniques et plusieurs hôtes et les systèmes HANA connectés SAN Fibre Channel sont mises en évidence dans les sections suivantes.

Les exemples montrent SAP HANA Studio comme outil d'exécution manuelle de la restauration. Vous pouvez

également utiliser des instructions SAP HANA Cockpit ou HANA SQL.

Restauration et reprise automatisées

Avec SnapCenter 4.3, les opérations automatisées de restauration sont prises en charge pour les systèmes HANA à un seul conteneur ou MDC, qui ont été découverts automatiquement par SnapCenter.

Vous pouvez exécuter une opération de restauration et de récupération automatisée en procédant comme suit :

1. Sélectionnez la sauvegarde à utiliser pour l'opération de restauration. La sauvegarde peut être sélectionnée parmi les options de stockage suivantes :
   - Le stockage primaire
   - Stockage de sauvegarde hors site (cible SnapVault)
2. Sélectionnez le type de restauration. Sélectionnez Complete Restore with Volume Revert ou with Volume Revert.

   L'option Volume Revert n'est disponible que pour les opérations de restauration à partir du stockage primaire et si la base de données HANA utilise NFS comme protocole de stockage.

3. Sélectionnez le type de récupération parmi les options suivantes :
   - À l'état le plus récent
   - Point dans le temps
   - À une sauvegarde de données spécifique
   - Pas de récupération

   Le type de restauration sélectionné est utilisé pour la récupération du système et de la base de données des locataires.

Ensuite, SnapCenter effectue les opérations suivantes :

1. Elle arrête la base de données HANA.
2. Elle restaure la base de données.

   Selon le type de restauration sélectionné et le protocole de stockage utilisé, différentes opérations sont exécutées.

   - Si NFS et Volume Revert sont sélectionnés, puis SnapCenter démonte le volume, restaure le volume à l'aide d'une mémoire SnapRestore basée sur les volumes sur la couche de stockage, puis monte le volume.
   - Si NFS est sélectionné et que la fonction Restauration du volume n'est pas sélectionnée, SnapCenter restaure tous les fichiers à l'aide des opérations SnapRestore à un seul fichier sur la couche de stockage.
   - Si SAN Fibre Channel est sélectionné, SnapCenter démonte la ou les LUN, restaure les LUN à l'aide d'opérations SnapRestore de fichier unique sur la couche de stockage, puis détecte et monte les LUN.
3. Il restaure la base de données :
   a. Il restaure la base de données du système.

b. Il restaure la base de données des locataires.

   Ou, pour les systèmes à conteneurs uniques HANA, la restauration est exécutée en une seule étape :

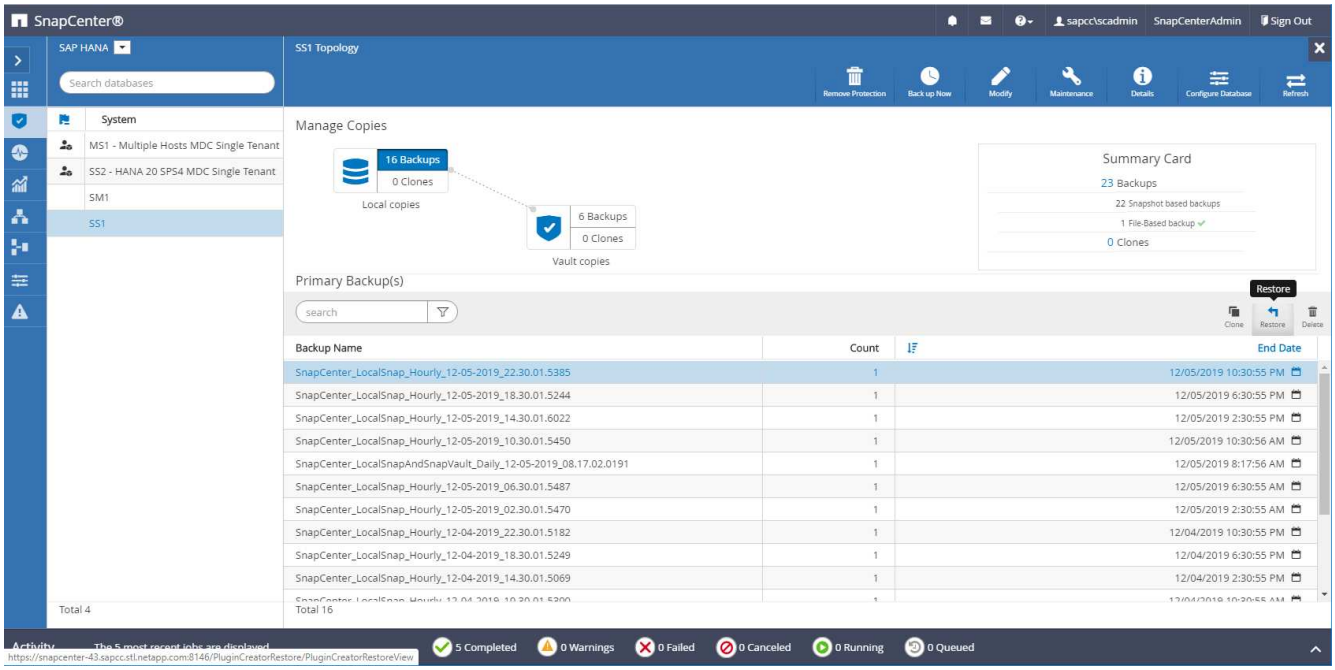
c. Elle démarre la base de données HANA.

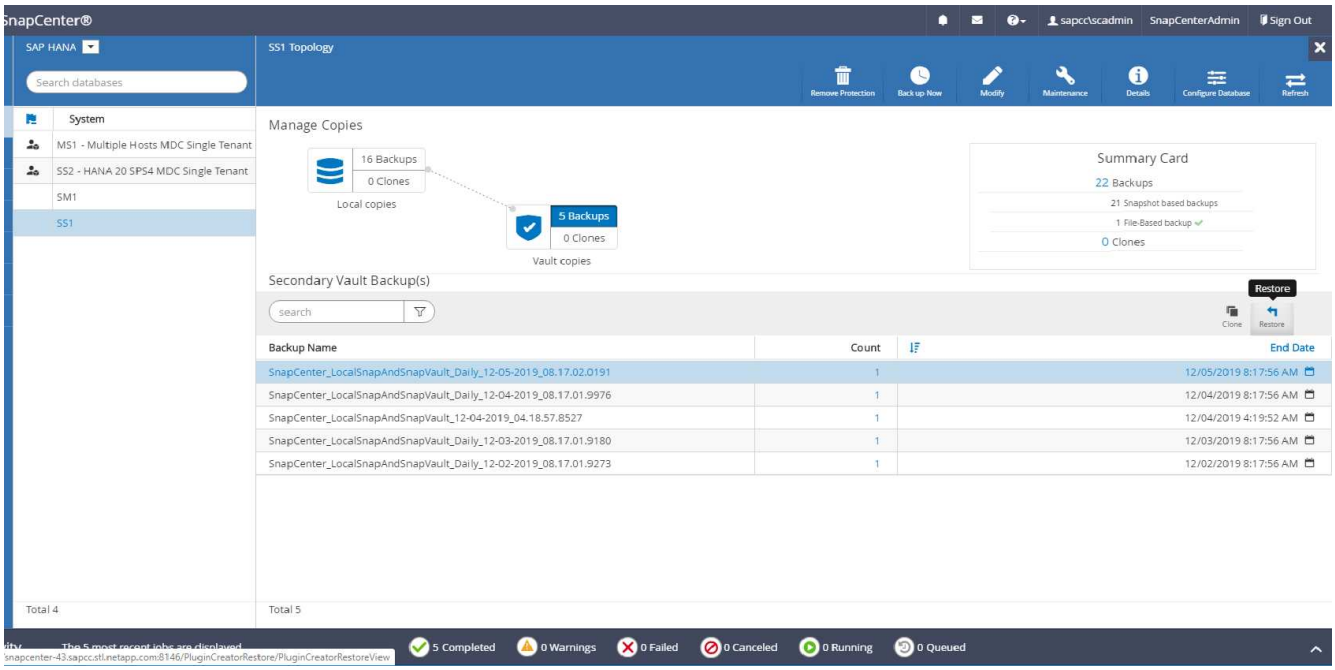
> Si aucune récupération est sélectionnée, SnapCenter se ferme et l'opération de récupération du système et de la base de données des locataires doit être effectuée manuellement.

Cette section décrit les étapes du processus de restauration et de restauration automatisées du système SS1 HANA à détection automatique (hôte unique SAP HANA, système MDC à locataire unique via NFS).

1. Sélectionnez une sauvegarde dans SnapCenter à utiliser pour l'opération de restauration.

> Vous pouvez sélectionner la restauration depuis le stockage de sauvegarde primaire ou hors site.



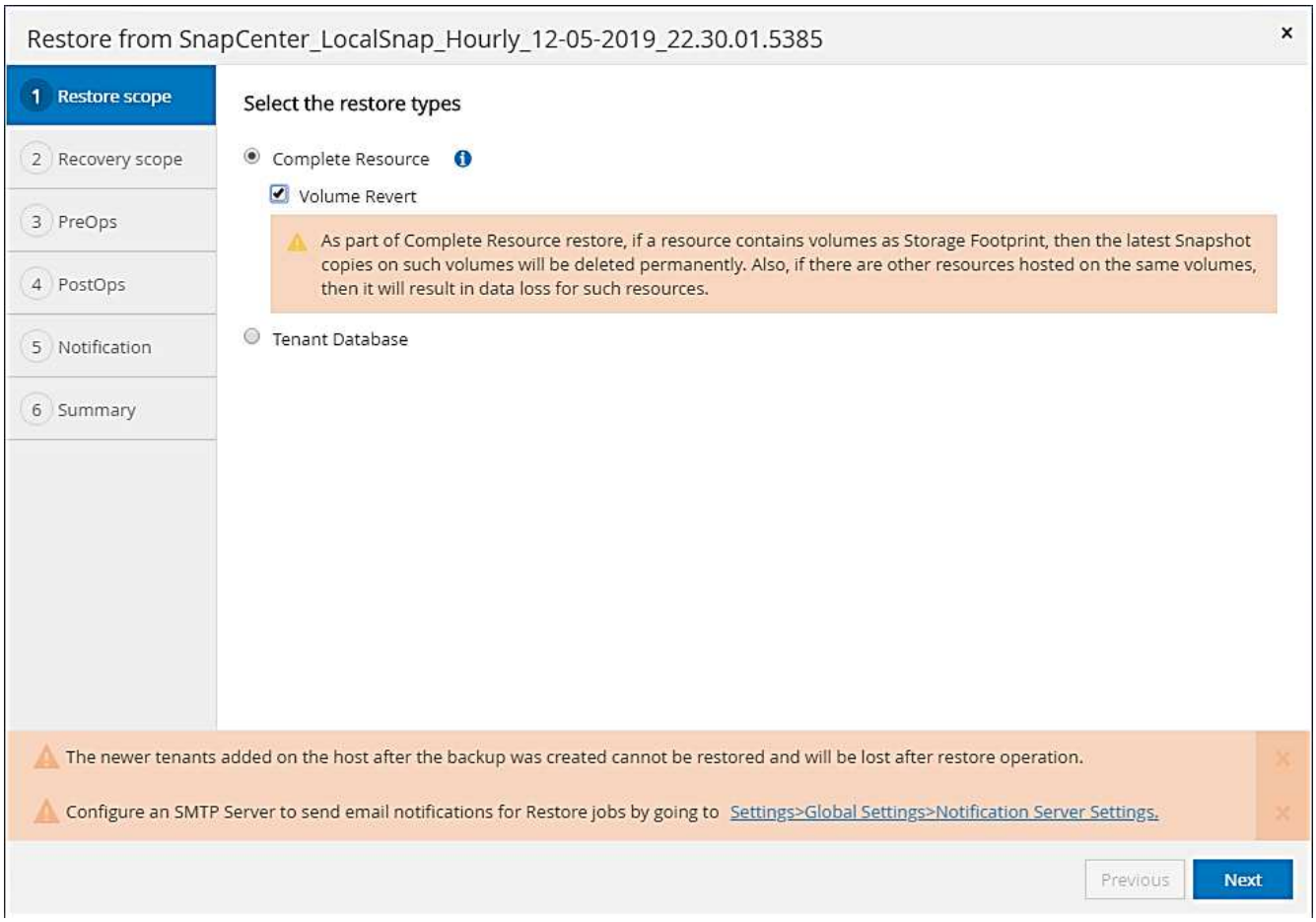


2. Sélectionnez la portée et le type de restauration.

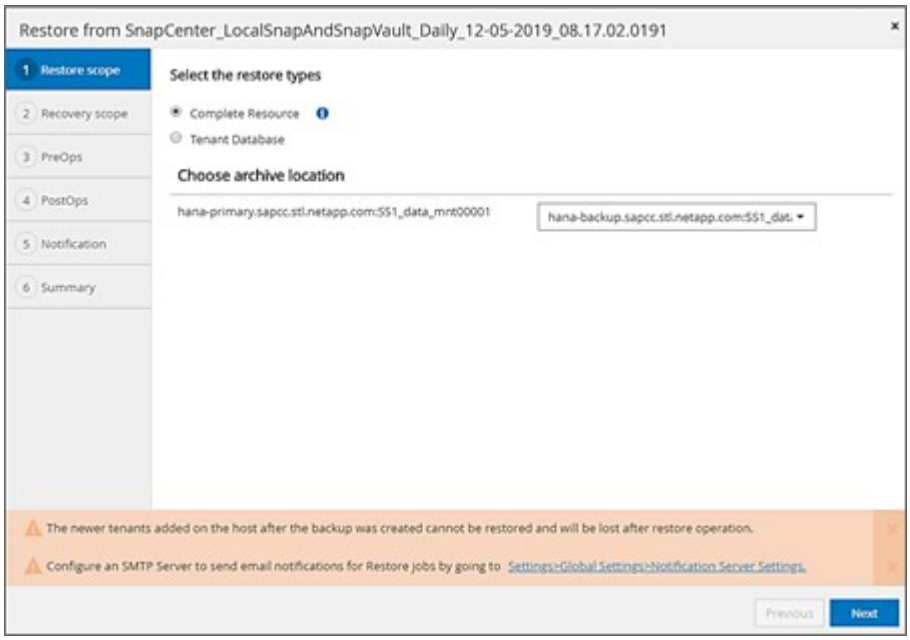
   Les trois captures d'écran suivantes présentent les options de restauration à partir du système primaire avec NFS, de restauration à partir du système secondaire avec NFS et de restauration à partir du système primaire avec SAN Fibre Channel.

   Les options de type de restauration pour la restauration à partir du stockage primaire.

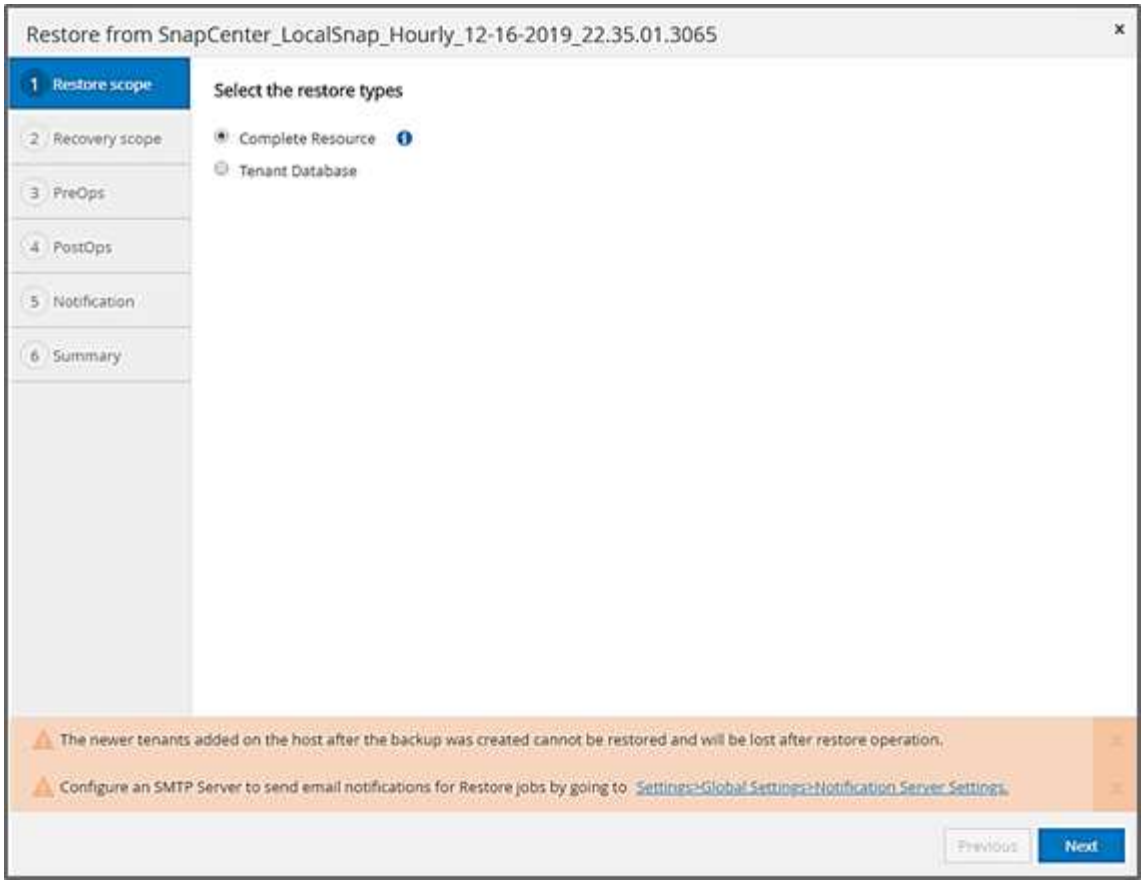
   > L'option Volume Revert n'est disponible que pour les opérations de restauration depuis le système principal avec NFS.



Options de type de restauration à partir d'un stockage de sauvegarde hors site.

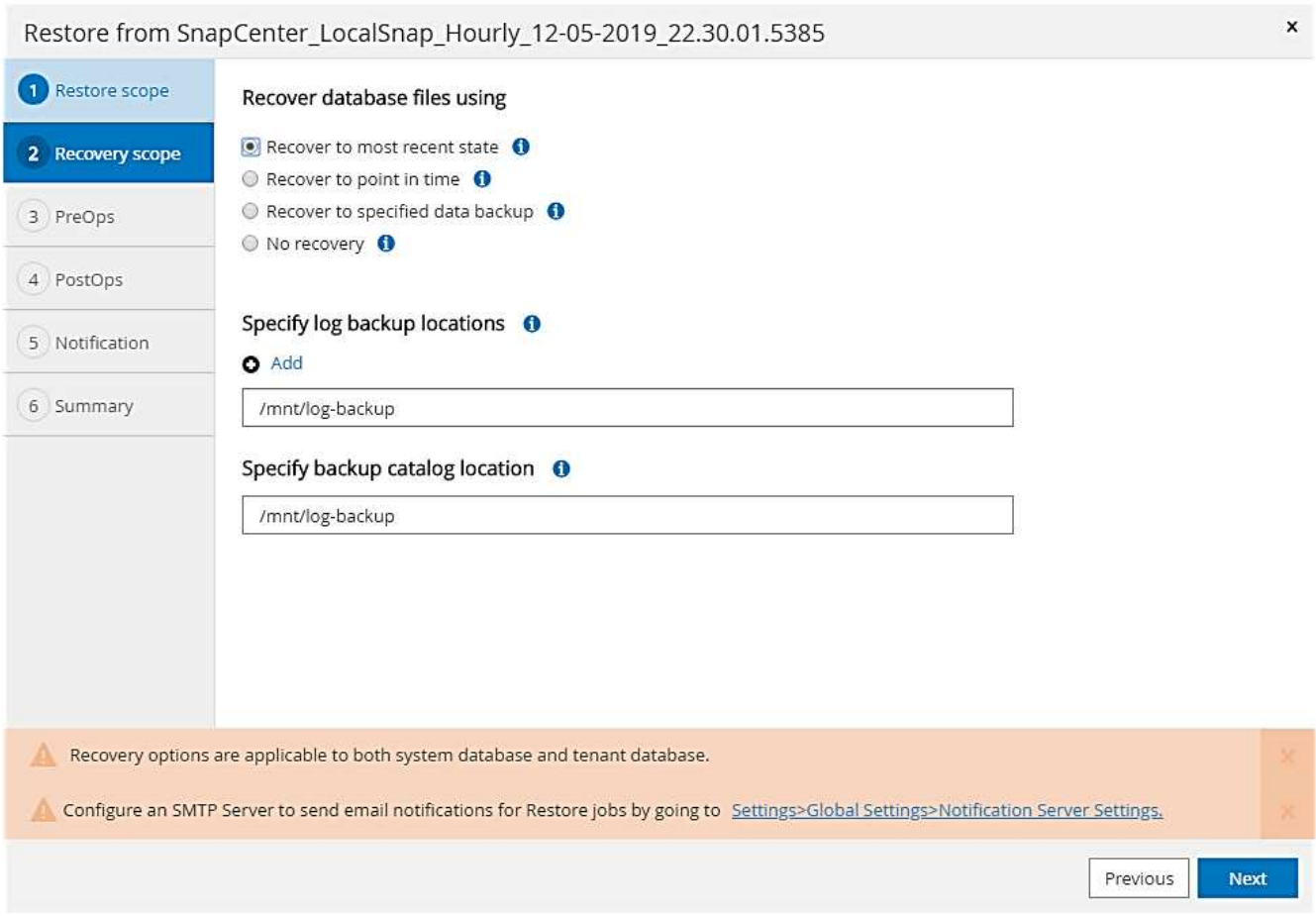


Les options de type de restauration pour le stockage primaire avec SAN Fibre Channel.

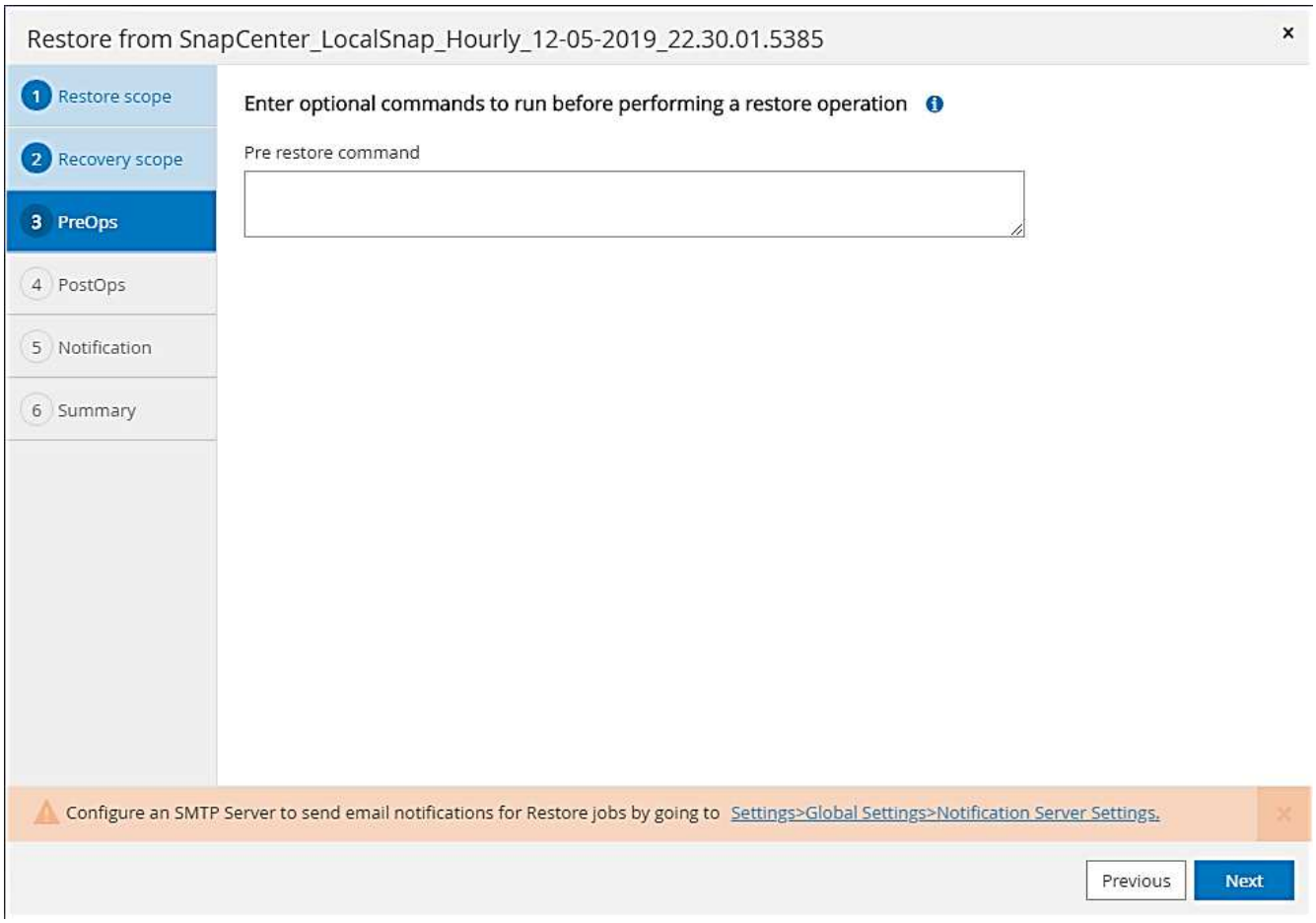


3. Sélectionnez étendue de la récupération et indiquez l'emplacement de sauvegarde du journal et du catalogue.

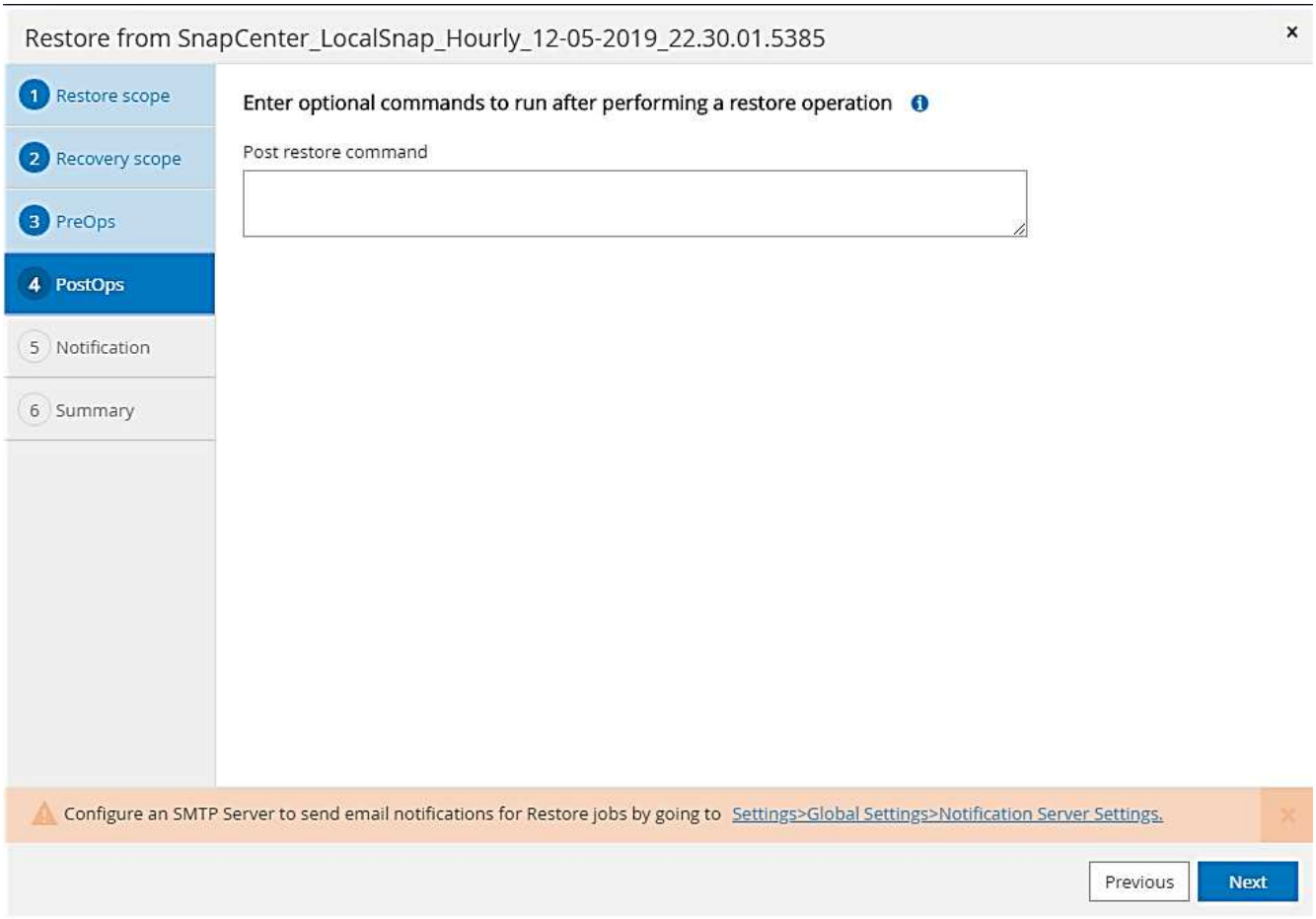
SnapCenter utilise le chemin par défaut ou les chemins modifiés dans le fichier HANA global.ini pour pré-remplir les emplacements de sauvegarde du journal et du catalogue.



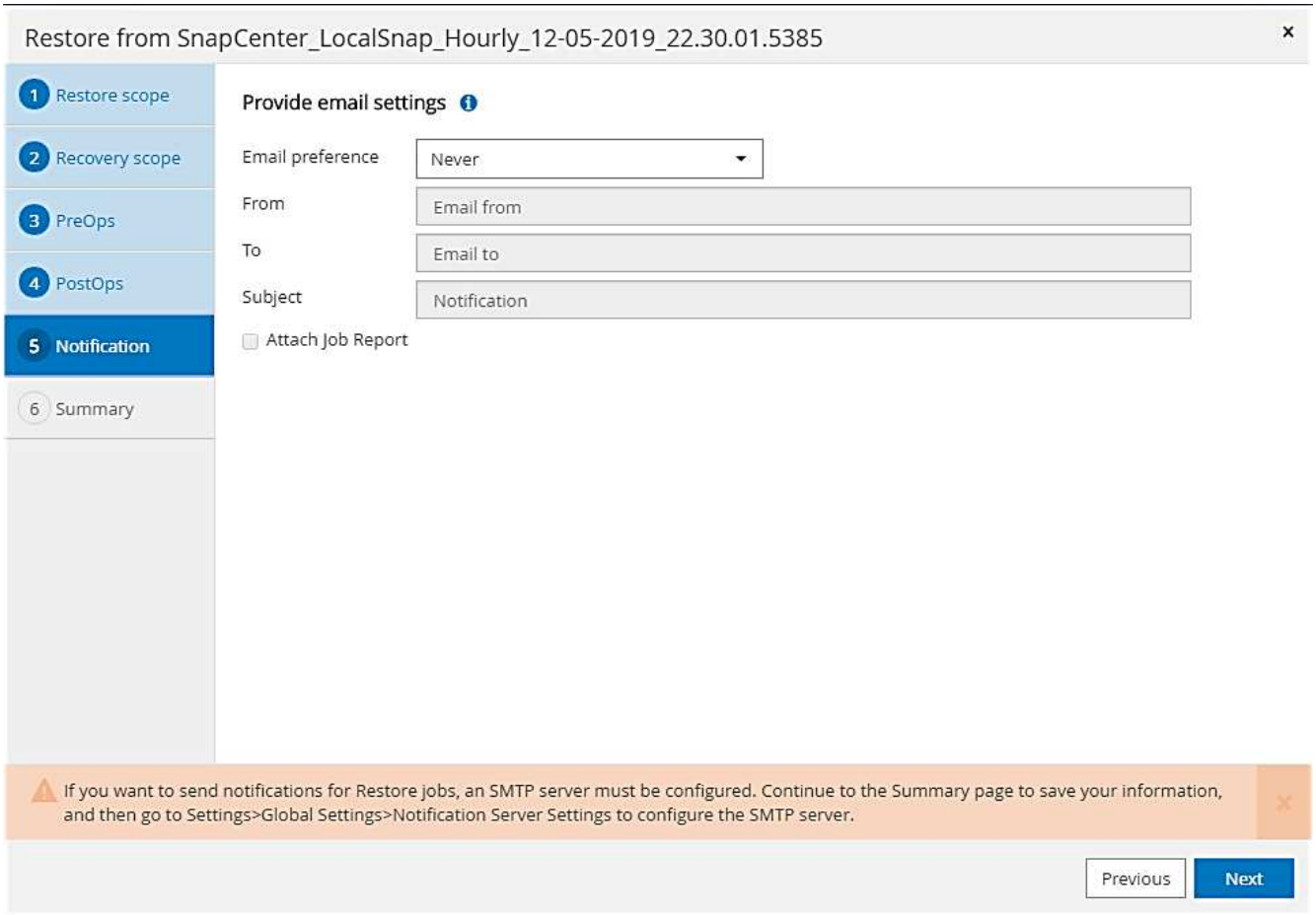
4. Entrez les commandes pré-enregistrement facultatives.



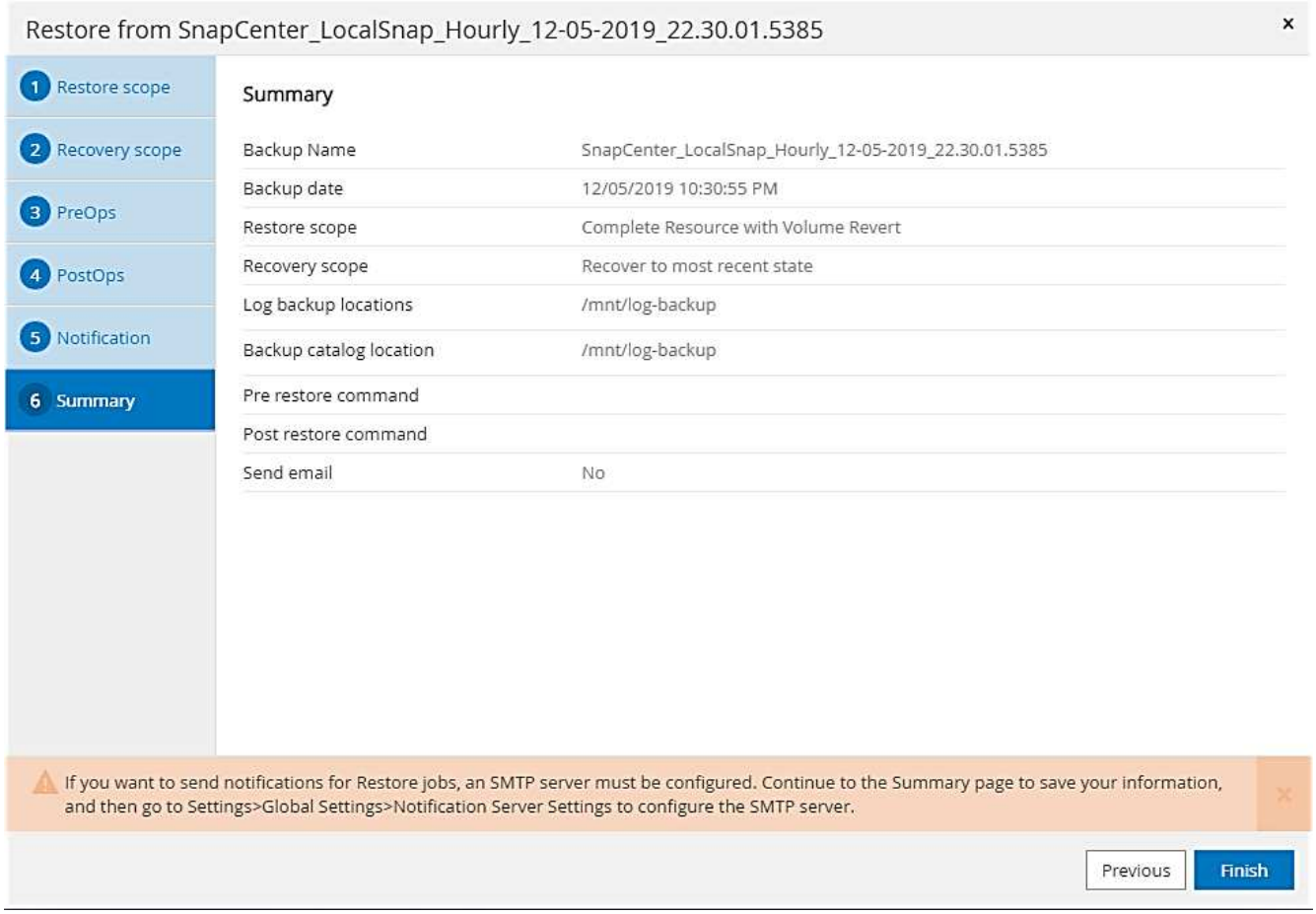
5. Entrez les commandes facultatives de post-restauration.



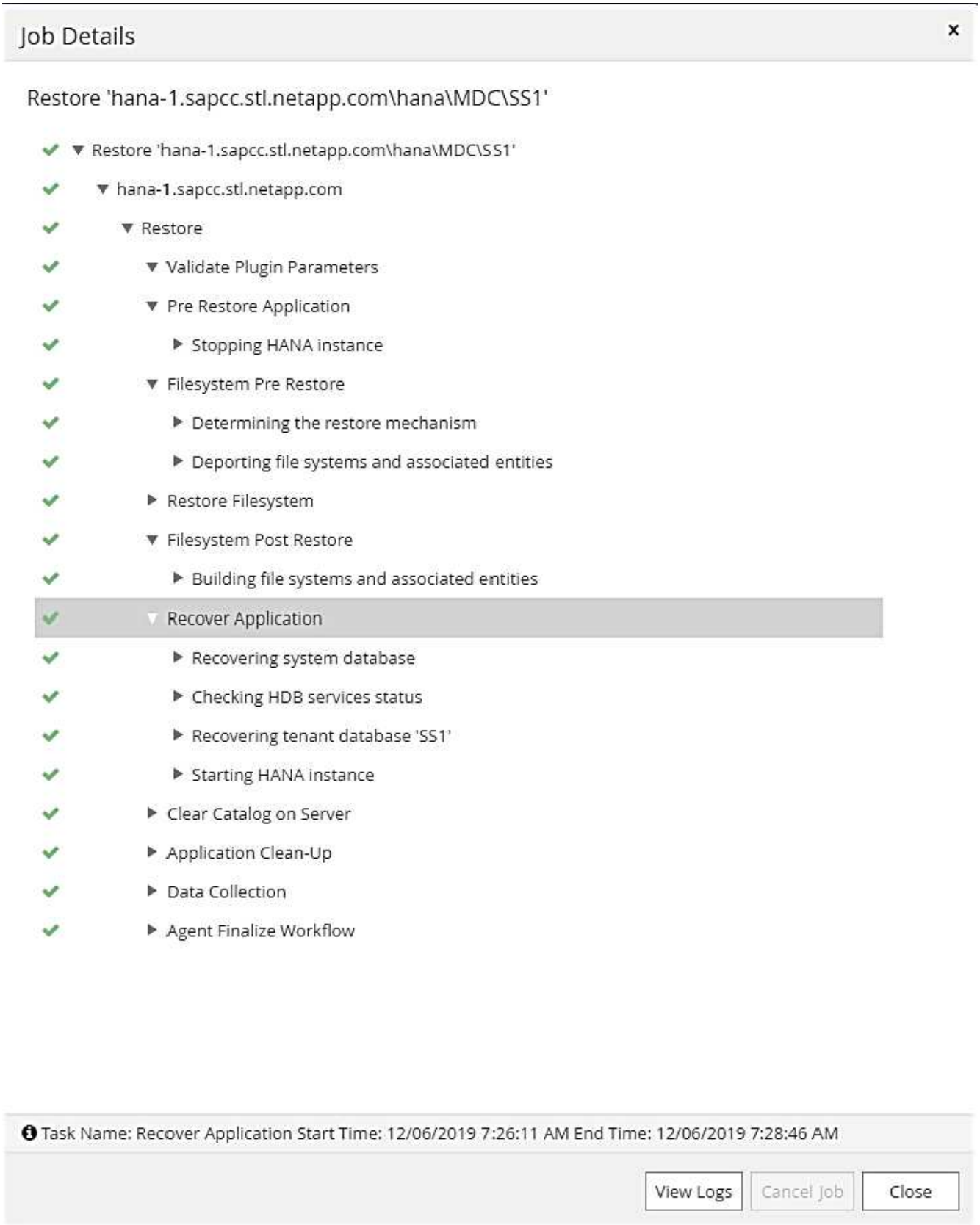
6. Entrez les paramètres de messagerie facultatifs.



7. Pour lancer l'opération de restauration, cliquez sur Terminer.



8. SnapCenter exécute l'opération de restauration et de restauration. Cet exemple montre les détails du travail de restauration et de récupération.



Opérations de restauration et de restauration par locataire unique

Avec SnapCenter 4.3, les opérations de restauration par locataire unique sont prises en charge sur les systèmes MDC HANA avec un seul locataire ou plusieurs locataires qui ont été découverts automatiquement par SnapCenter.

Vous pouvez effectuer une opération de restauration et de restauration par locataire unique en procédant comme suit :

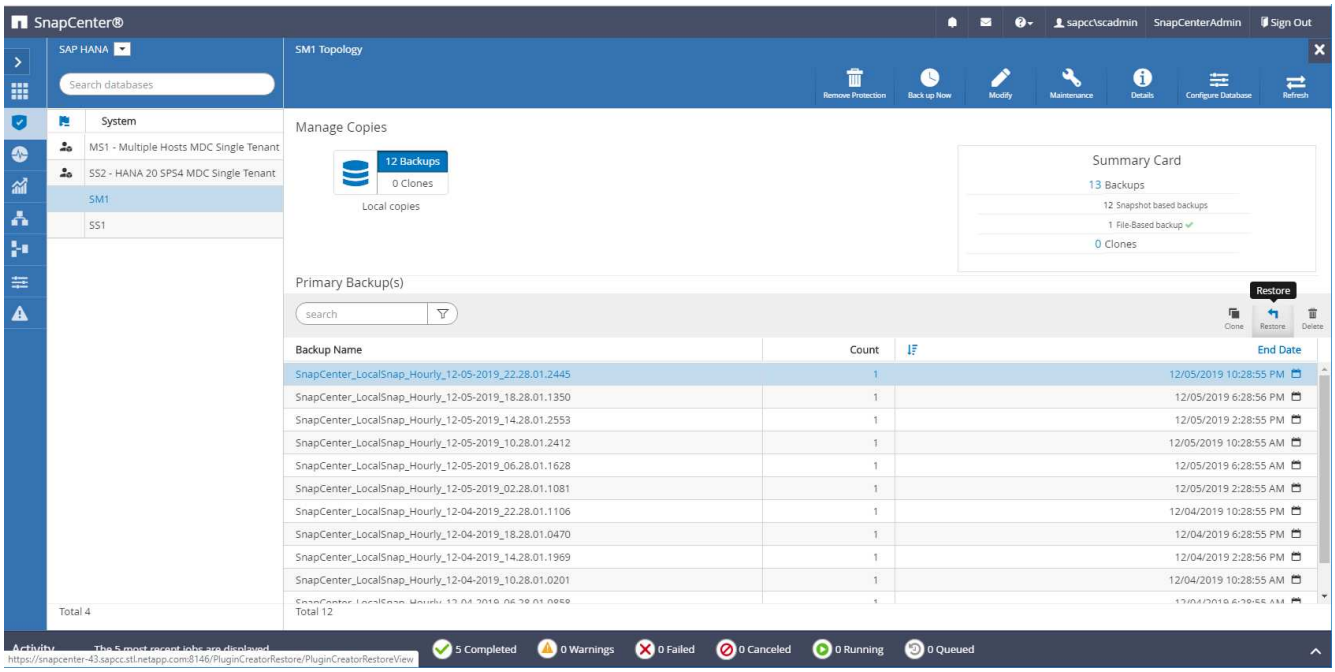
1. Arrêter le locataire à restaurer et à récupérer.
2. Restaurez le locataire avec SnapCenter.
   - Pour une restauration à partir du stockage primaire, SnapCenter exécute les opérations suivantes :
     - **NFS.** opérations Storage Single File SnapRestore pour tous les fichiers de la base de données tenant.
     - **SAN.** Clone et connectez le LUN à l'hôte de base de données et copiez tous les fichiers de la base de données du locataire.
   - Pour une restauration à partir du stockage secondaire, SnapCenter exécute les opérations suivantes :
     - **NFS.** opérations de restauration de Storage SnapVault pour tous les fichiers de la base de données du locataire
     - **SAN.** Clone et connectez le LUN à l'hôte de base de données et copiez tous les fichiers de la base de données du locataire
3. Restaurez le locataire avec HANA Studio, Cockpit ou une déclaration SQL.

Cette section décrit les étapes de l'opération de restauration et de récupération à partir du stockage principal du système HANA SM1 découvert automatiquement (système à un seul hôte SAP HANA, MDC à plusieurs locataires via NFS). Du point de vue des entrées utilisateur, les flux de travail sont identiques pour une restauration à partir d'une configuration secondaire ou d'une restauration dans une configuration SAN Fibre Channel.

1. Arrêtez la base de données des locataires.

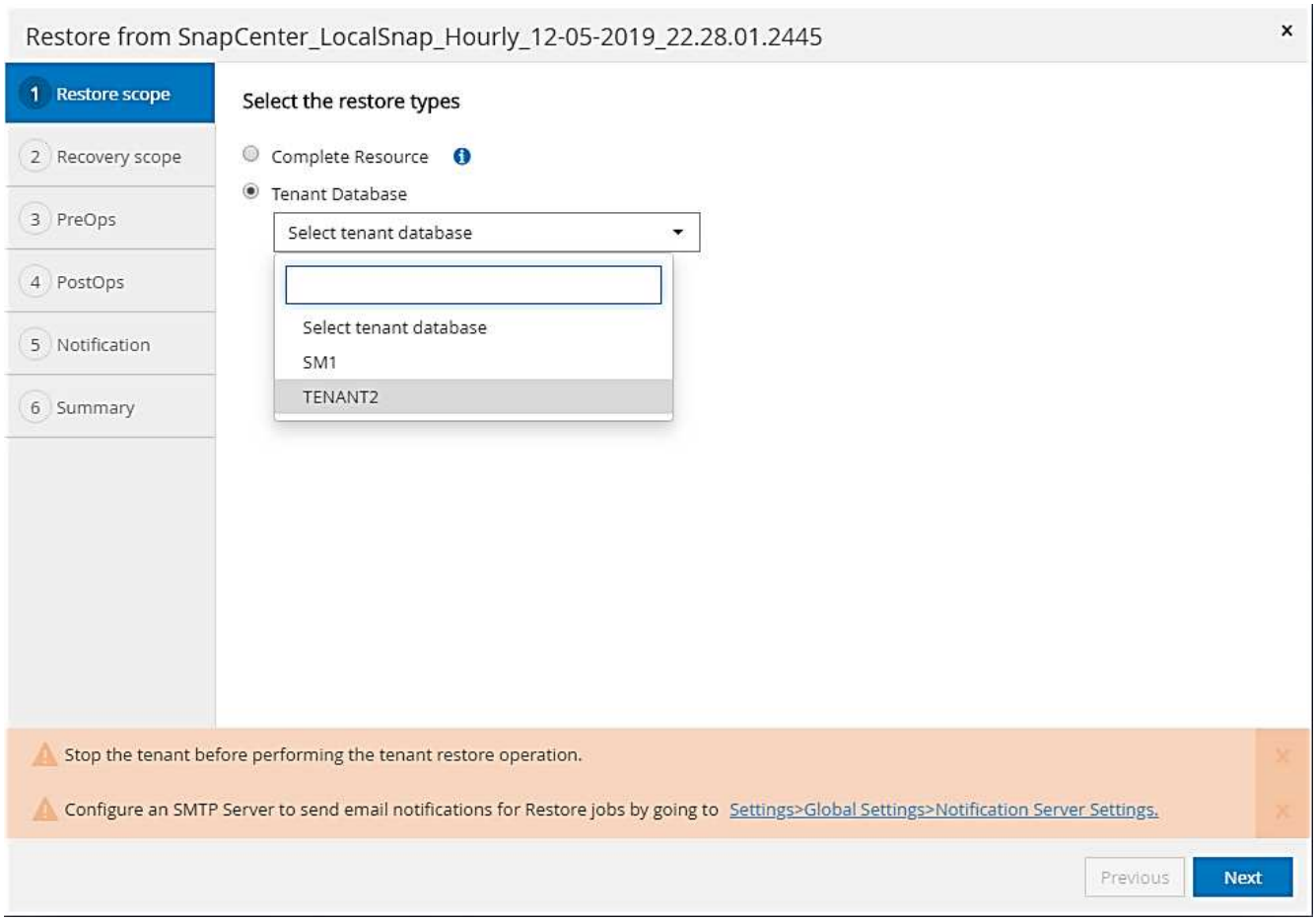
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql SYSTEMDB=>
```

2. Sélectionnez une sauvegarde dans SnapCenter à utiliser pour l'opération de restauration.

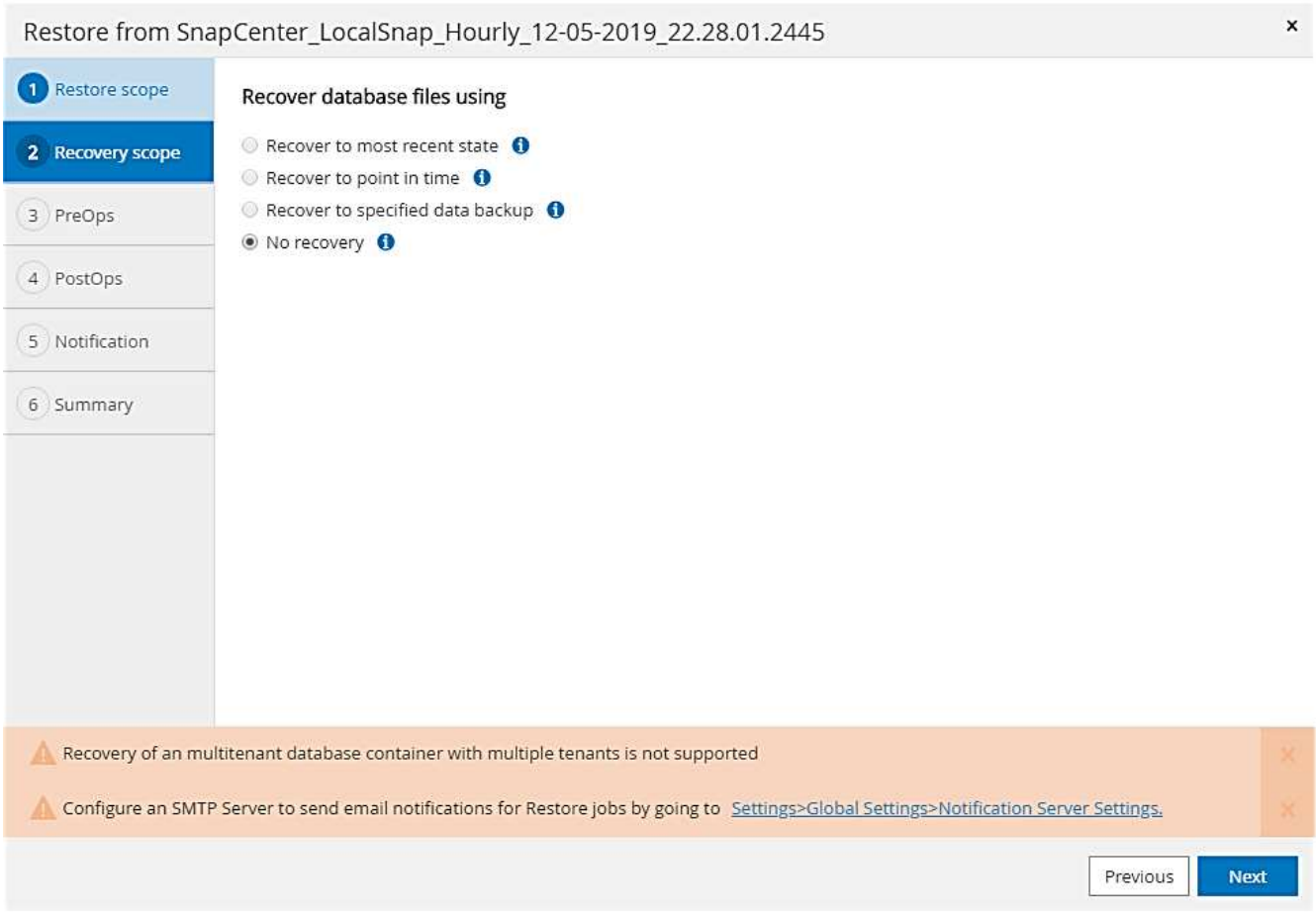


3. Sélectionnez le locataire à restaurer.

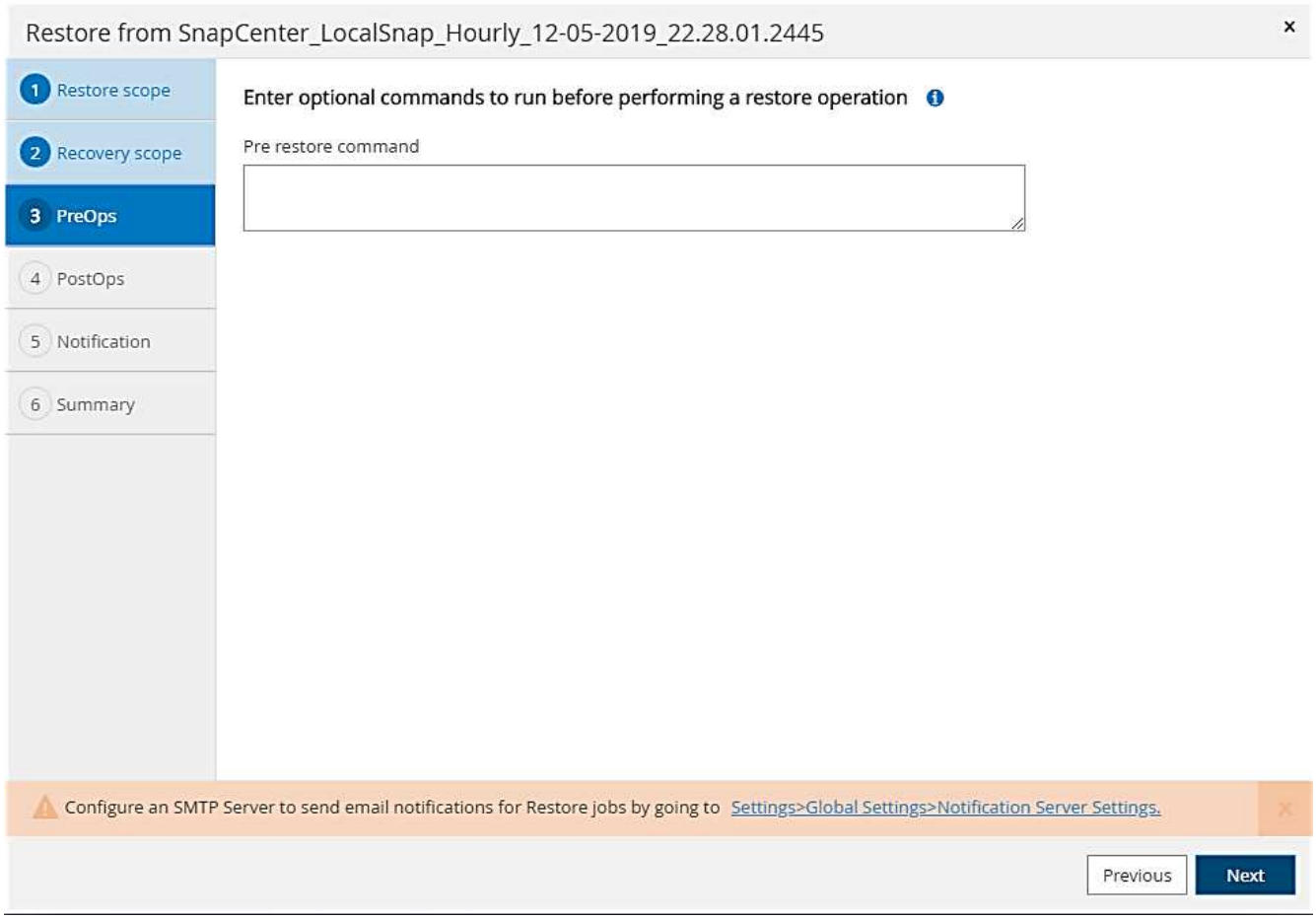
SnapCenter affiche la liste de tous les locataires inclus dans la sauvegarde sélectionnée.



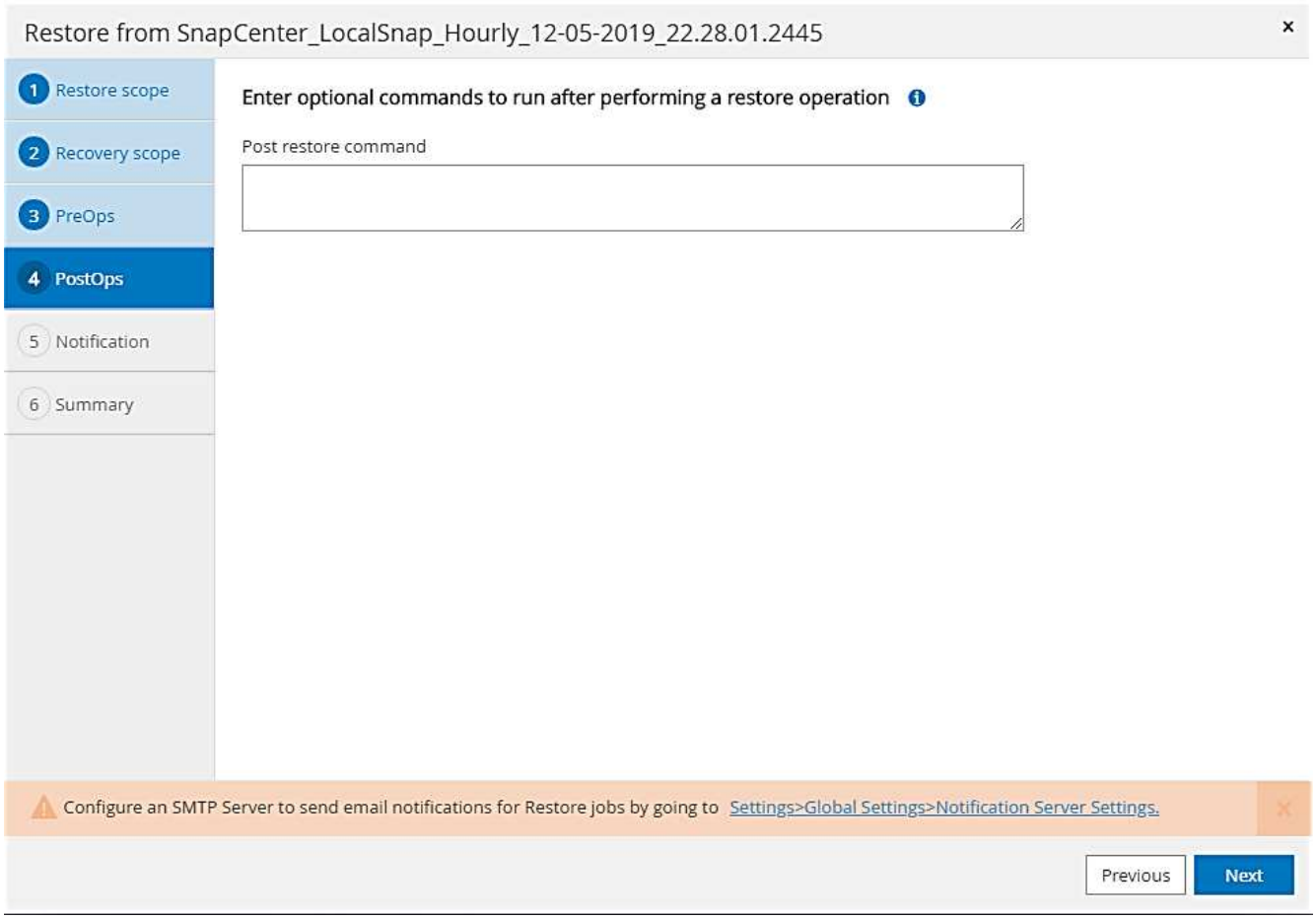
La restauration d'un seul locataire n'est pas prise en charge par SnapCenter 4.3. Aucune récupération n'est présélectionnée et ne peut pas être modifiée.



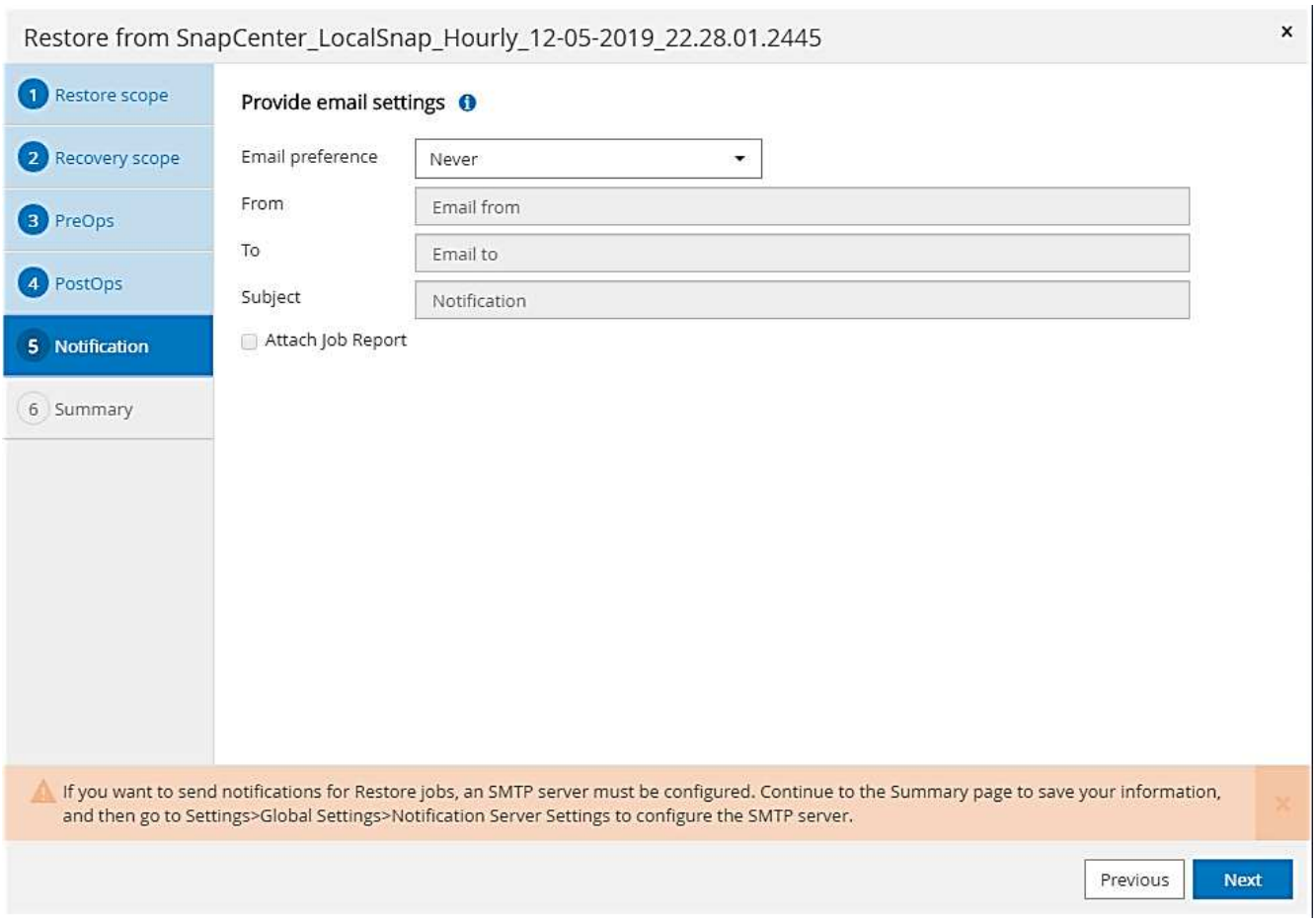
4. Entrez les commandes pré-enregistrement facultatives.



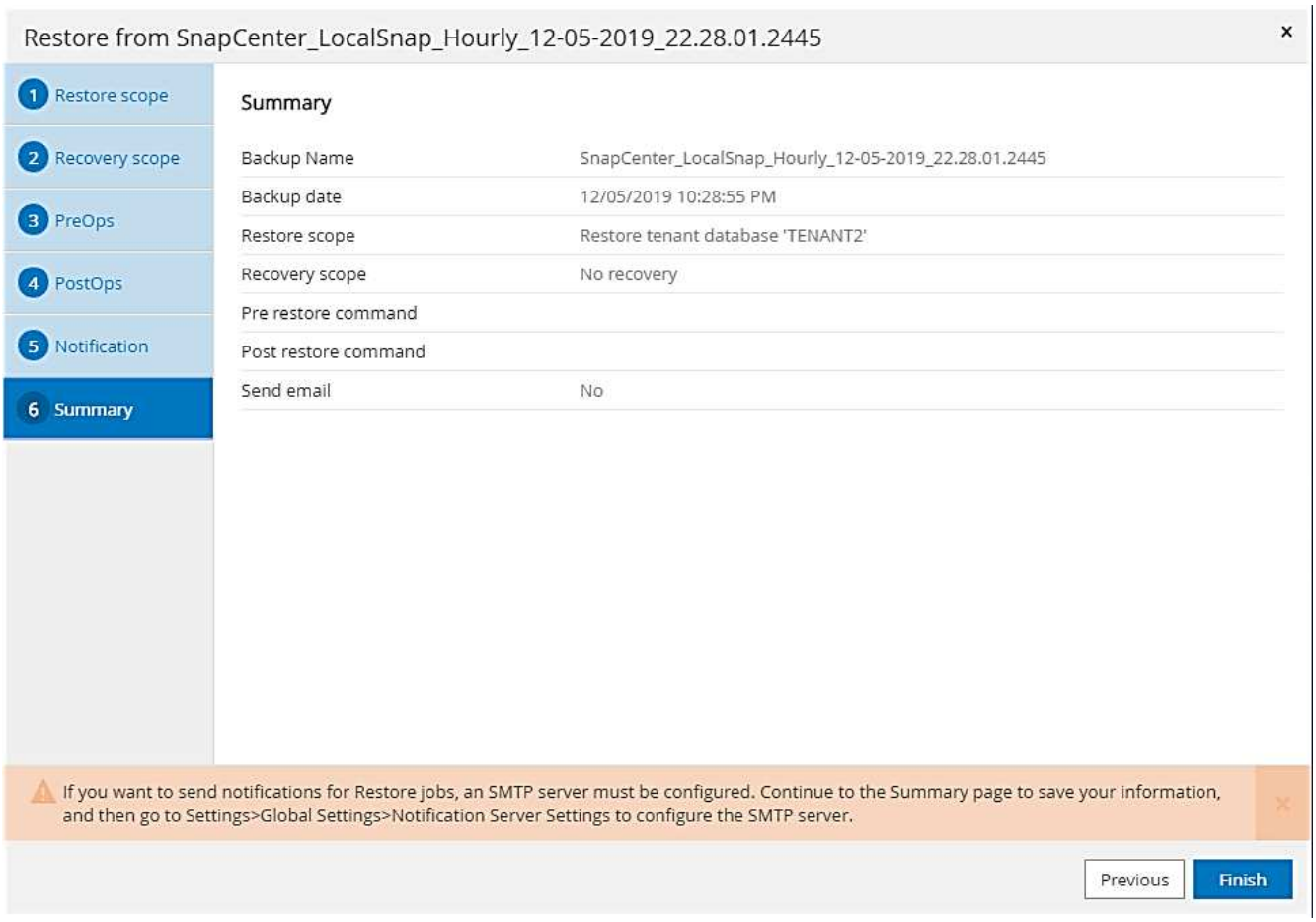
5. Entrez des commandes post-restauration facultatives.



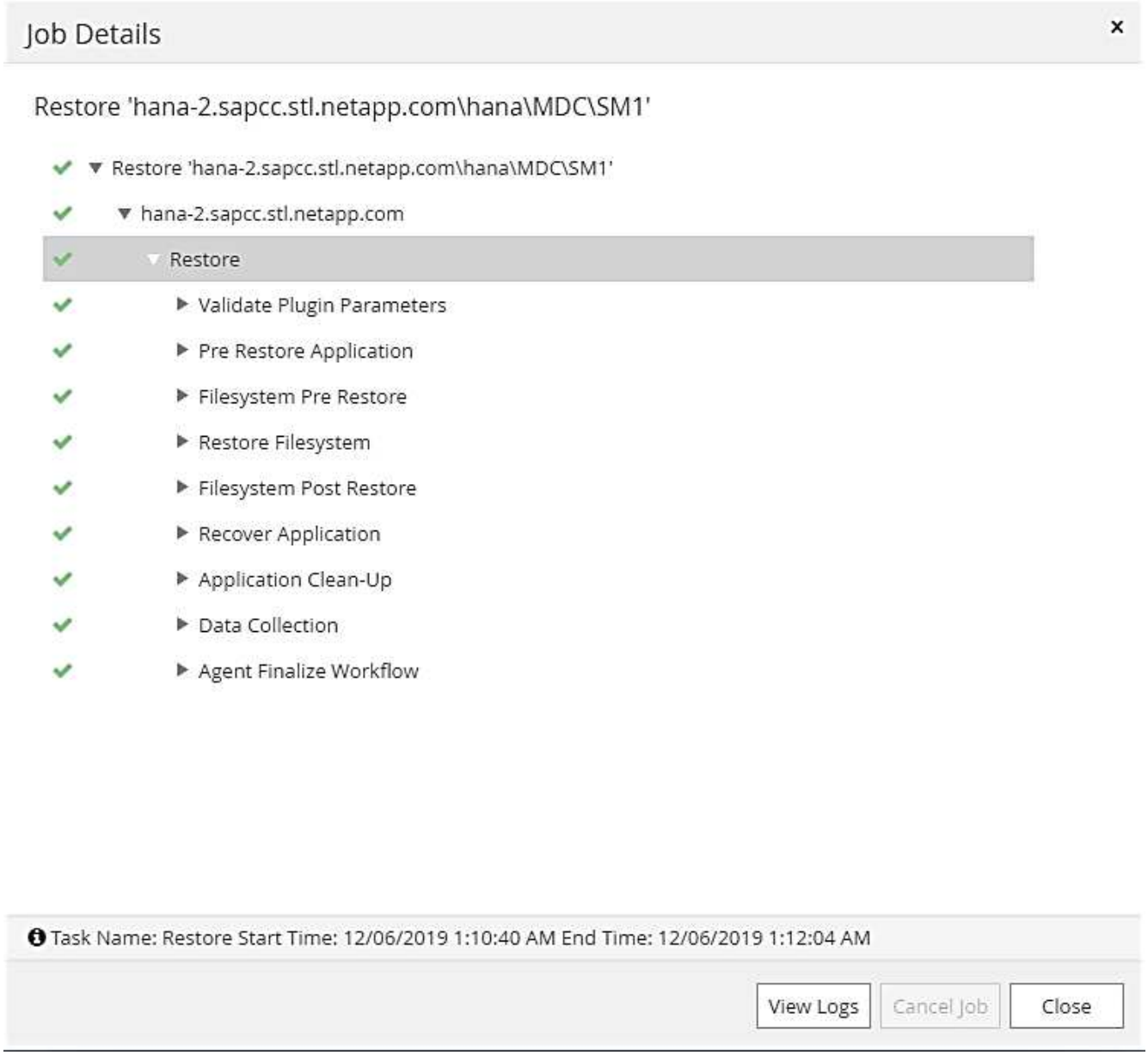
6. Entrez les paramètres de messagerie facultatifs.



7. Pour lancer l'opération de restauration, cliquez sur Terminer.



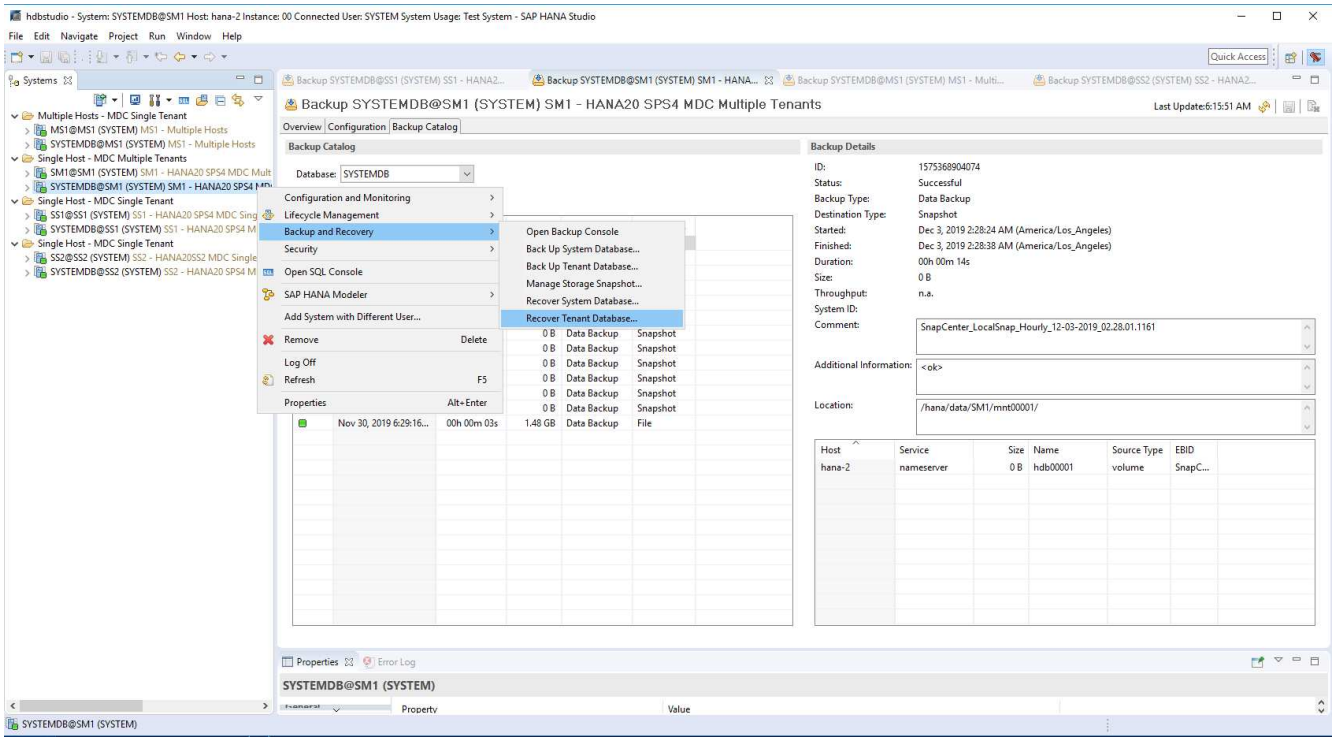
L’opération de restauration est exécutée par SnapCenter. Cet exemple montre les détails du travail de restauration.



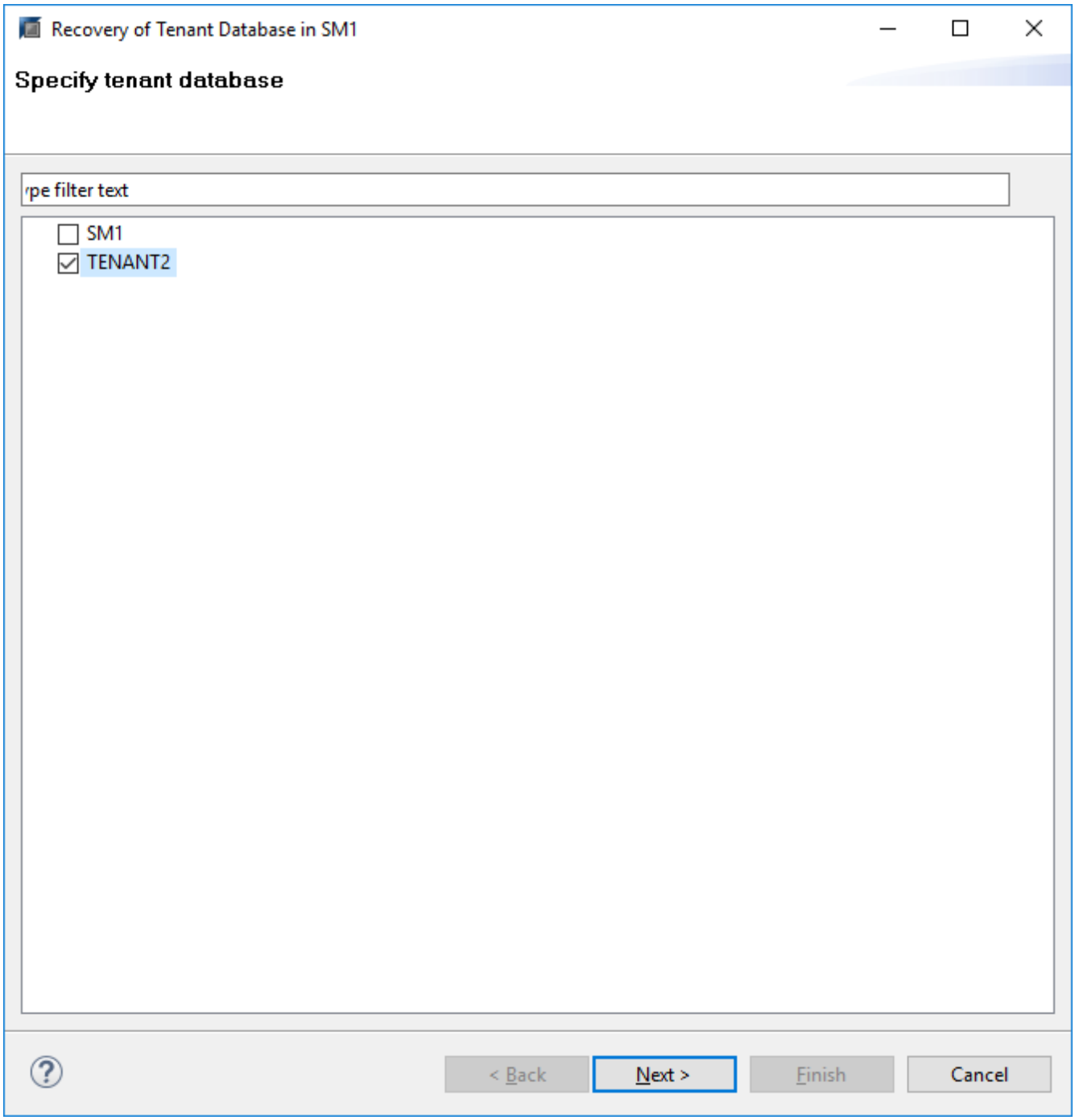
Lorsque l'opération de restauration du locataire est terminée, seules les données pertinentes du locataire sont restaurées. Sur le système de fichiers de l'hôte de la base de données HANA, le fichier de données restauré et le fichier d'ID de sauvegarde Snapshot du locataire sont disponibles.

```
sm1adm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 sm1adm sapsys   17 Dec  6 04:01
/hana/data/SM1/mnt00001/nameserver.lck
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r----- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r----- 1 sm1adm sapsys          0 Nov 20 08:36
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys         36 Nov 20 08:37 landscape.id
/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 sm1adm sapsys      4096 Nov 20 08:37 .
drwxr-x--- 6 sm1adm sapsys      4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 201441280 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys         0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 03:57 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 01:14 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 09:35
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys     155648 Dec  6 01:14
snapshot_databackup_0_1
/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
sm1adm@hana-2:/usr/sap/SM1/HDB00>
```

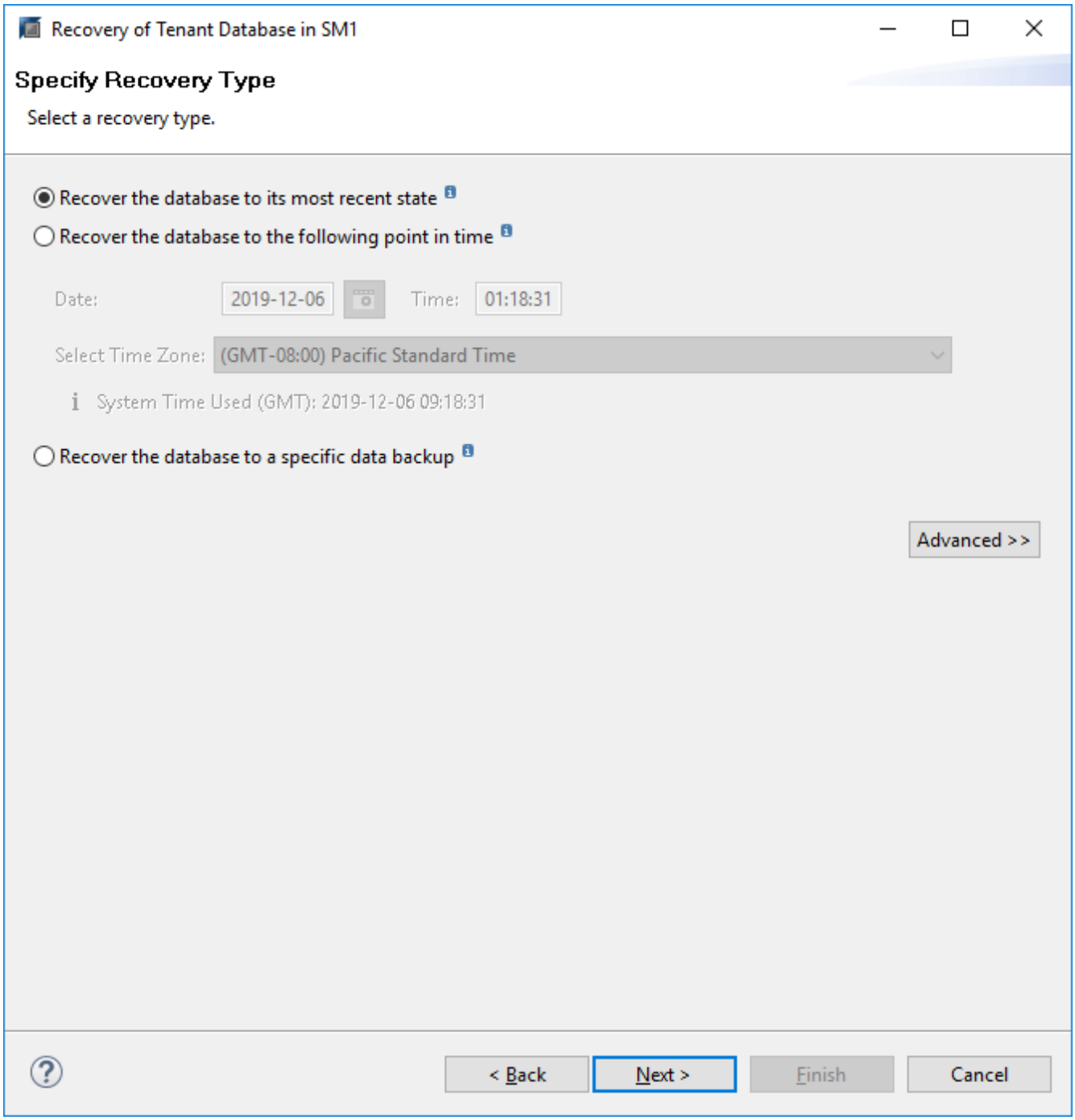
8. Commencez la restauration avec HANA Studio.



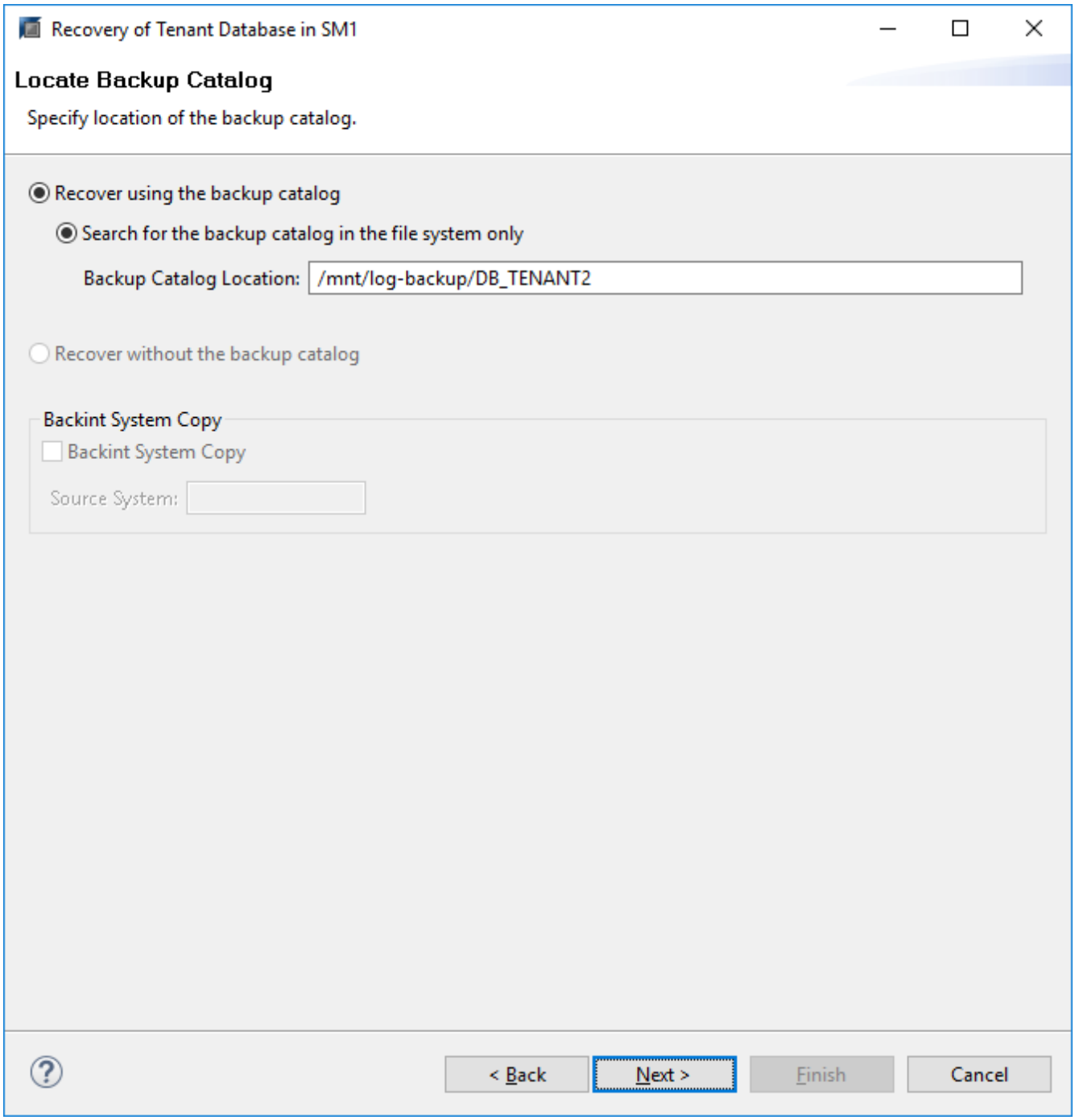
9. Sélectionnez le locataire.

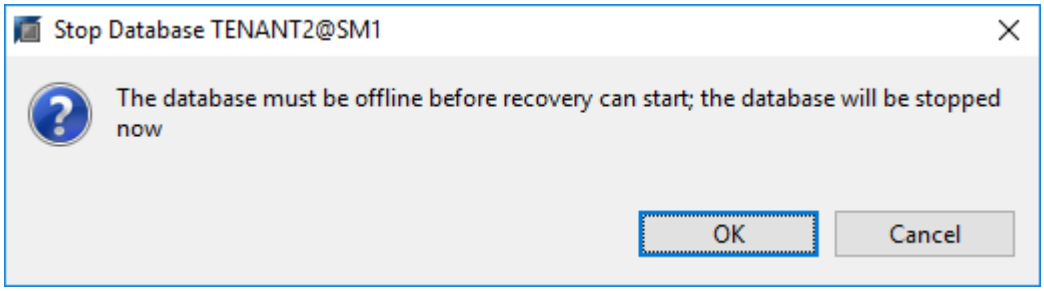


10. Sélectionnez le type de restauration.



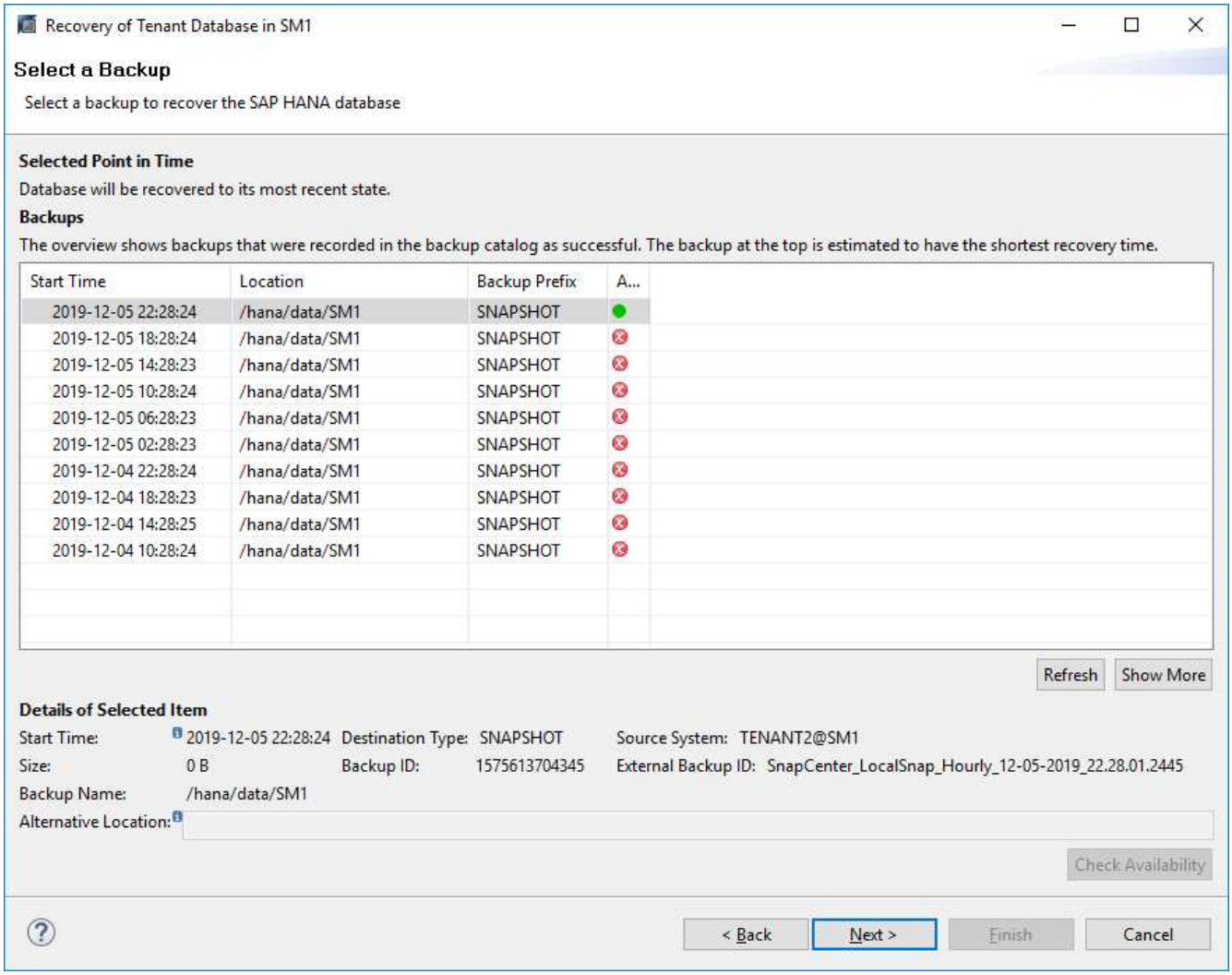
11. Fournir l’emplacement du catalogue de sauvegardes.



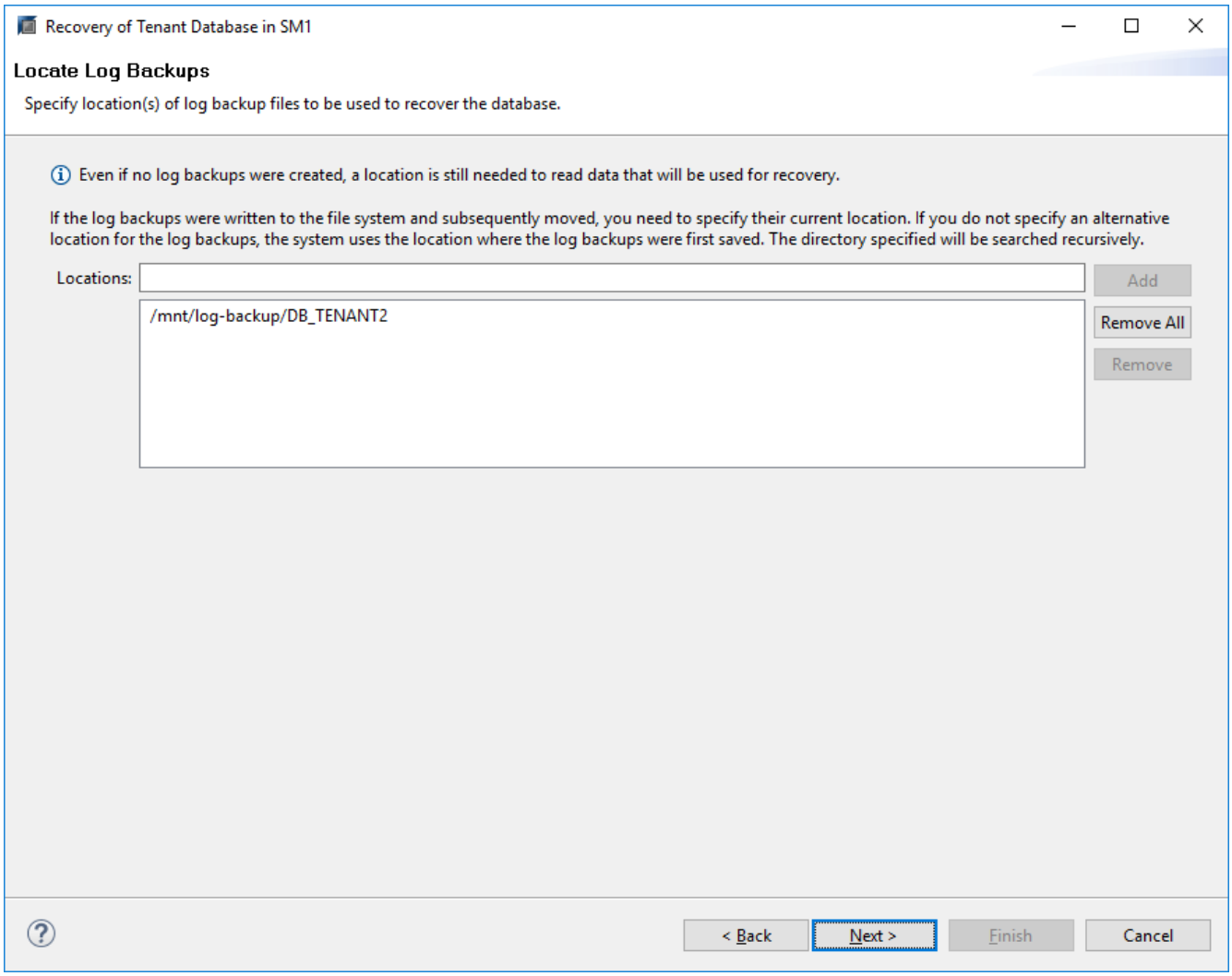


Dans le catalogue de sauvegarde, la sauvegarde restaurée est mise en évidence par une icône verte. L'ID de sauvegarde externe indique le nom de sauvegarde précédemment sélectionné dans SnapCenter.

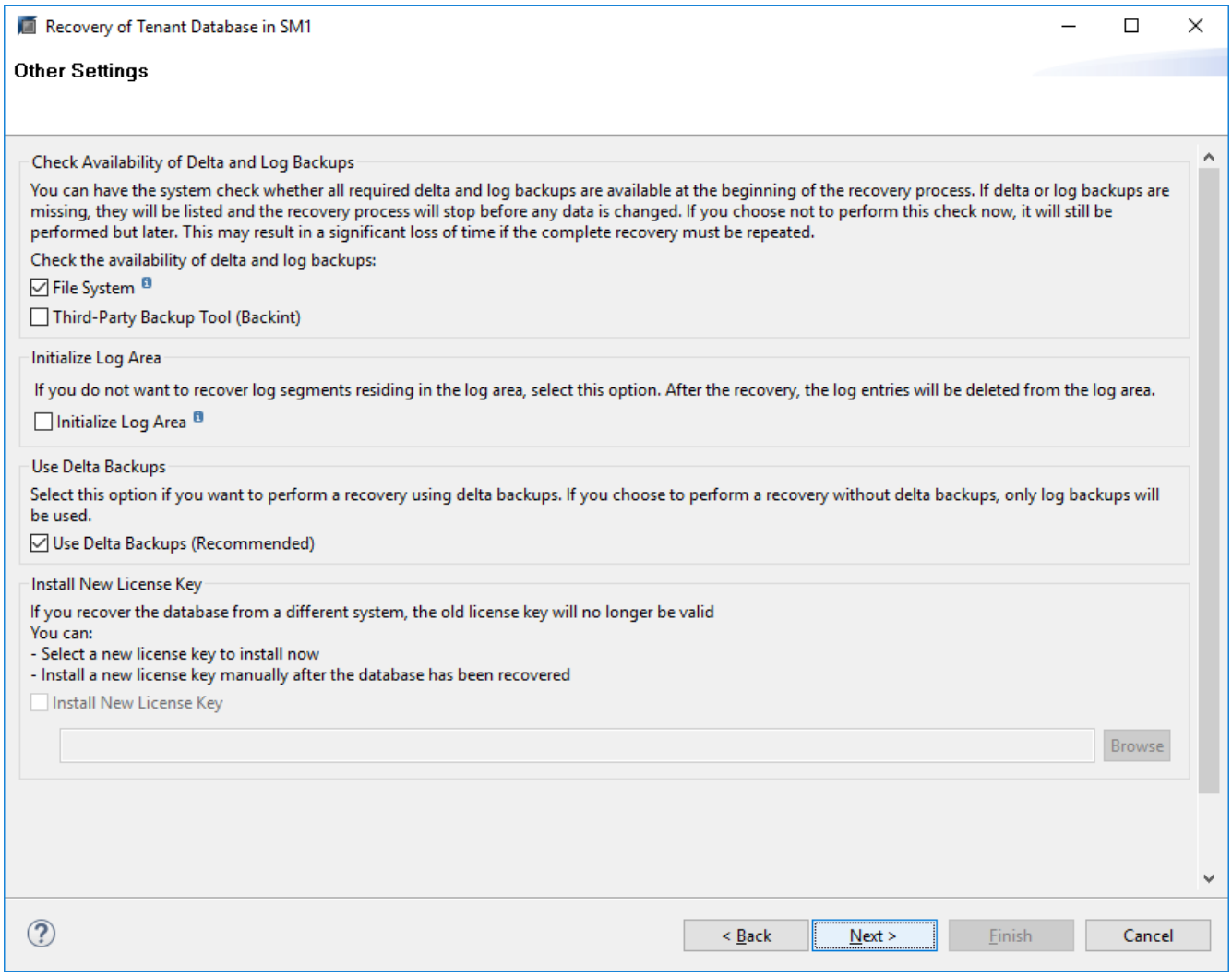
12. Sélectionnez l'entrée avec l'icône verte et cliquez sur Suivant.



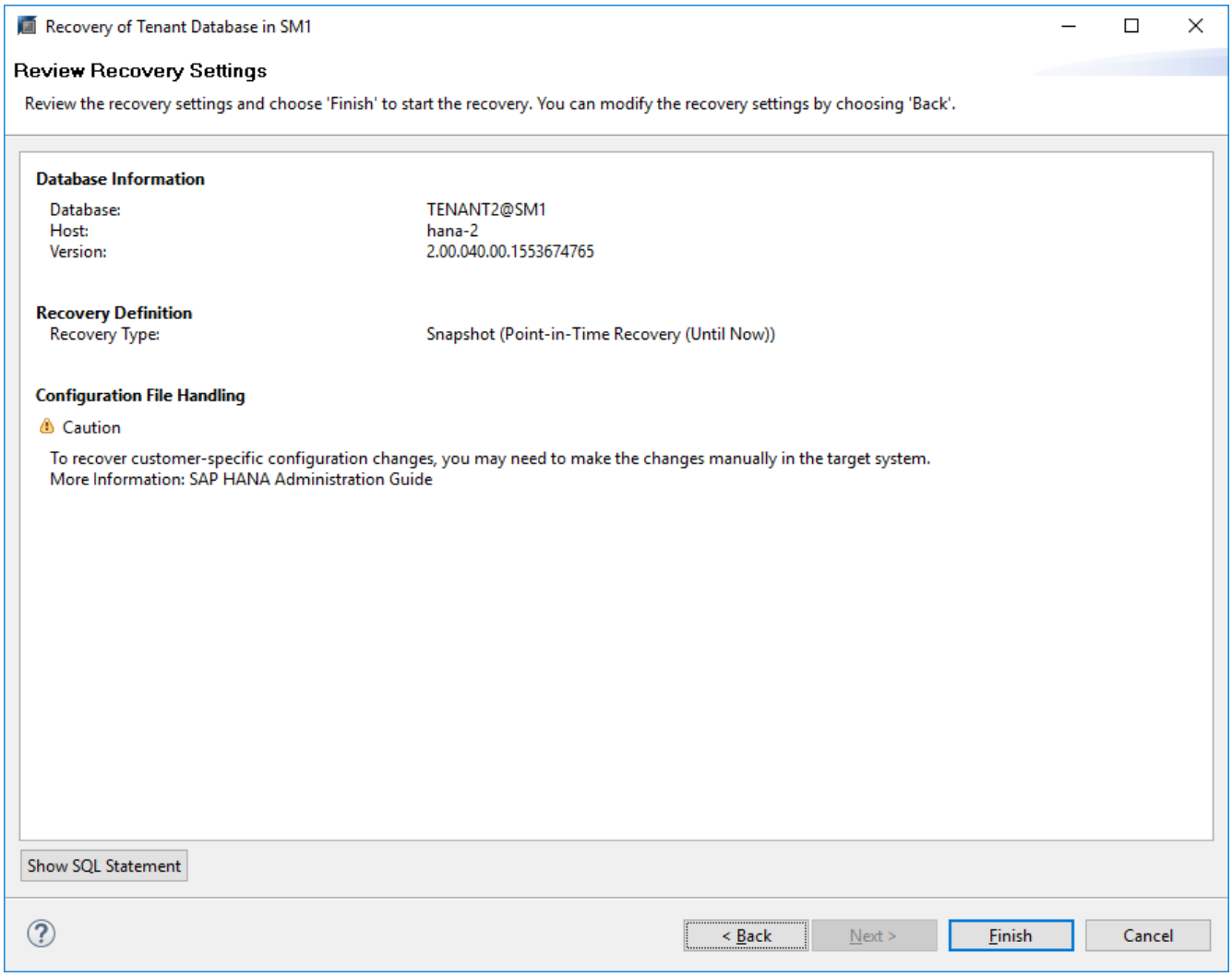
13. Indiquez l'emplacement de sauvegarde du journal.

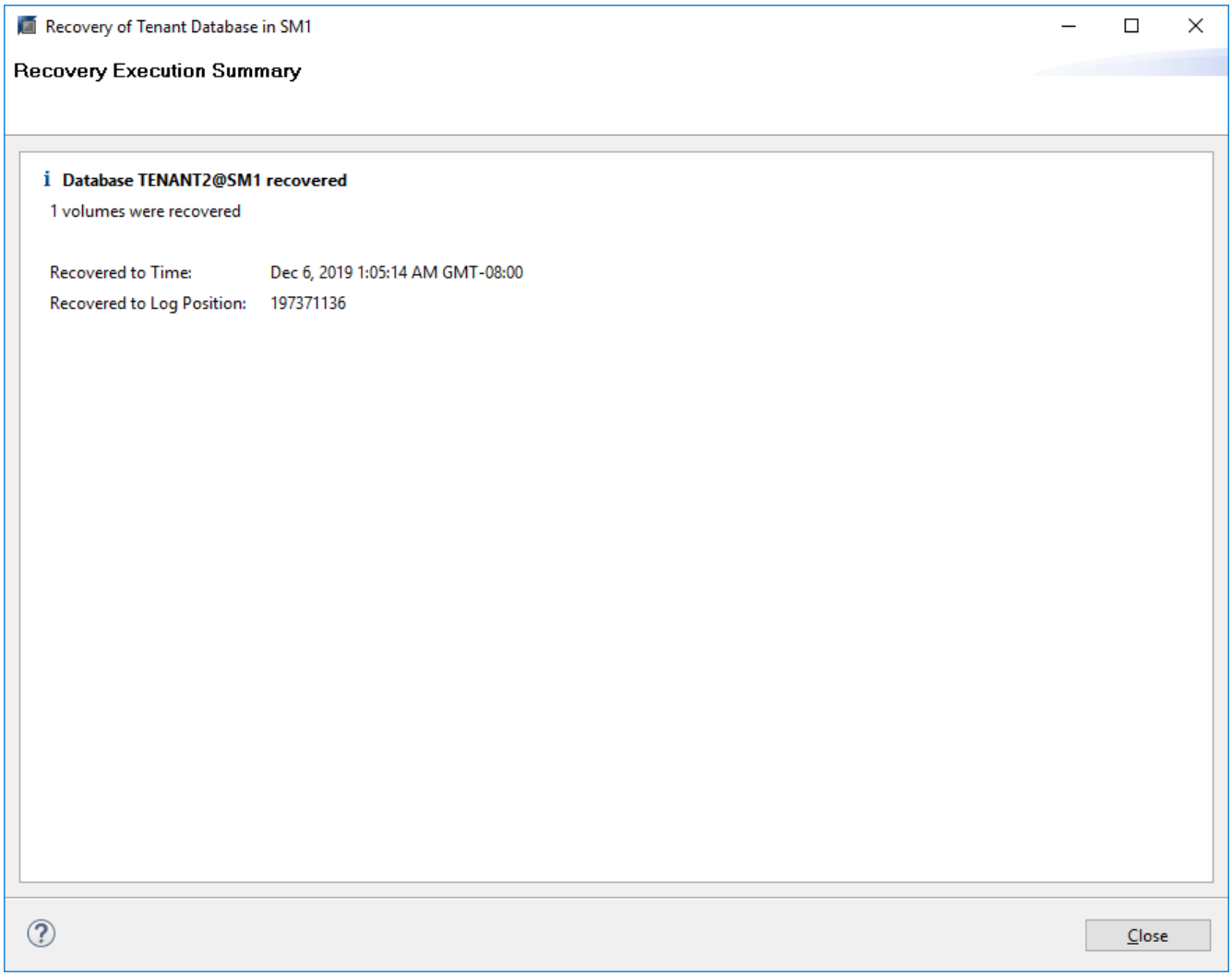


14. Sélectionnez les autres paramètres requis.



15. Démarrer l’opération de restauration des locataires.


Recovery of Tenant Database in SM1
Review Recovery Settings
Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.
Database Information
Database: TENANT2@SM1
Host: hana-2
Version: 2.00.040.00.1553674765
Recovery Definition
Recovery Type: Snapshot (Point-in-Time Recovery (Until Now))
Configuration File Handling
Caution
To recover customer-specific configuration changes, you may need to make the changes manually in the target system.
More Information: SAP HANA Administration Guide
Show SQL Statement
< Back
Next >
Finish
Cancel



Restauration avec récupération manuelle

Pour restaurer et restaurer un système à locataire unique SAP HANA MDC à l'aide de SAP HANA Studio et SnapCenter, effectuez les opérations suivantes :

1. Préparez le processus de restauration et de restauration avec SAP HANA Studio :
   a. Sélectionnez Recover System Database et confirmez l'arrêt du système SAP HANA.
   b. Sélectionnez le type de récupération et l'emplacement de sauvegarde du journal.
   c. La liste des sauvegardes de données s'affiche. Sélectionnez Sauvegarder pour afficher l'ID de sauvegarde externe.
2. Exécutez le processus de restauration avec SnapCenter :
   a. Dans la vue topologique de la ressource, sélectionnez les copies locales à restaurer à partir du stockage principal ou des copies du coffre-fort si vous souhaitez effectuer une restauration à partir d'un stockage de sauvegarde hors site.
   b. Sélectionnez la sauvegarde SnapCenter qui correspond au champ ID de sauvegarde externe ou commentaire de SAP HANA Studio.
   c. Démarrez le processus de restauration.

Si une restauration basée sur les volumes à partir du stockage primaire est choisie, les volumes de données doivent être démontés de tous les hôtes de base de données SAP HANA avant la restauration et montés de nouveau une fois le processus de restauration terminé.

Dans une configuration SAP HANA à plusieurs hôtes avec FC, les opérations de démontage et de montage sont exécutées par le serveur de noms SAP HANA dans le cadre du processus d'arrêt et de démarrage de la base de données.

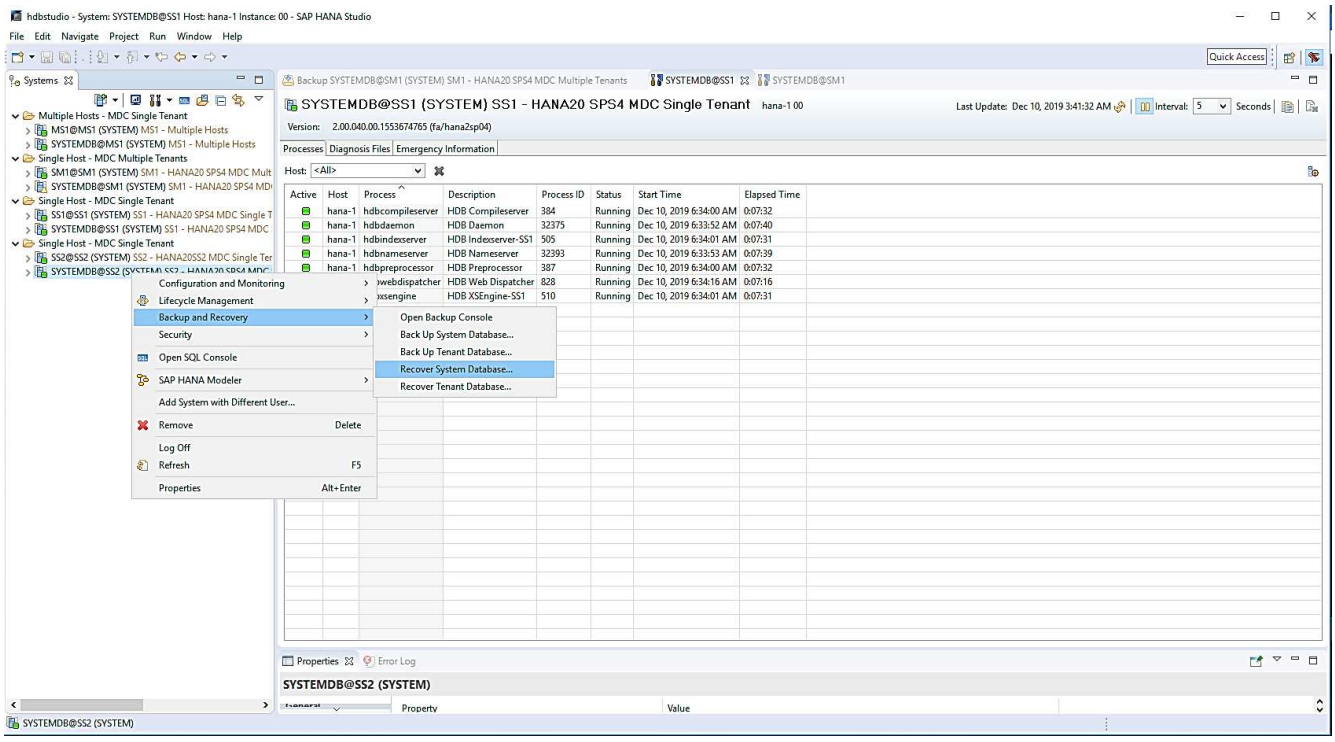
3. Exécutez le processus de restauration de la base de données système avec SAP HANA Studio :
   a. Cliquez sur Actualiser dans la liste de sauvegarde et sélectionnez la sauvegarde disponible pour la restauration (indiquée par une icône verte).
   b. Démarrez le processus de restauration. Une fois le processus de récupération terminé, la base de données système démarre.
4. Exécutez le processus de restauration de la base de données des locataires avec SAP HANA Studio :
   a. Sélectionnez récupérer la base de données des locataires et sélectionnez le locataire à récupérer.
   b. Sélectionnez le type de récupération et l'emplacement de sauvegarde du journal.

      Une liste de sauvegardes de données s'affiche. Le volume de données ayant déjà été restauré, la sauvegarde du locataire est indiquée comme disponible (en vert).

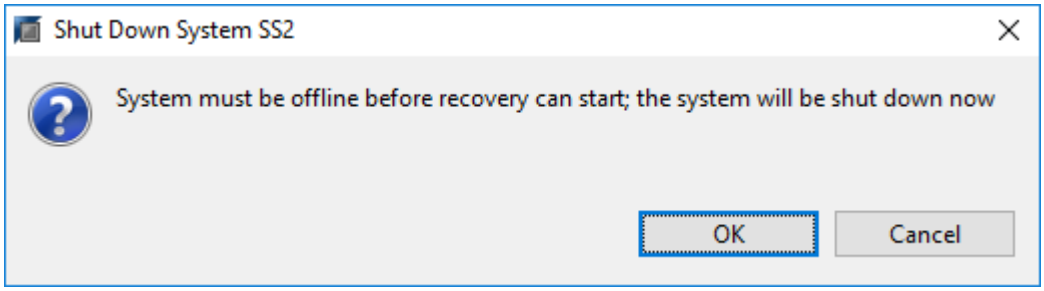
   c. Sélectionnez cette sauvegarde et démarrez le processus de restauration. Une fois le processus de restauration terminé, la base de données des locataires démarre automatiquement.

La section suivante décrit les étapes des opérations de restauration et de restauration du système HANA SS2 configuré manuellement (hôte unique SAP HANA, système mutualisé MDC multiple via NFS).

1. Dans SAP HANA Studio, sélectionnez l'option récupérer la base de données système pour démarrer la récupération de la base de données système.

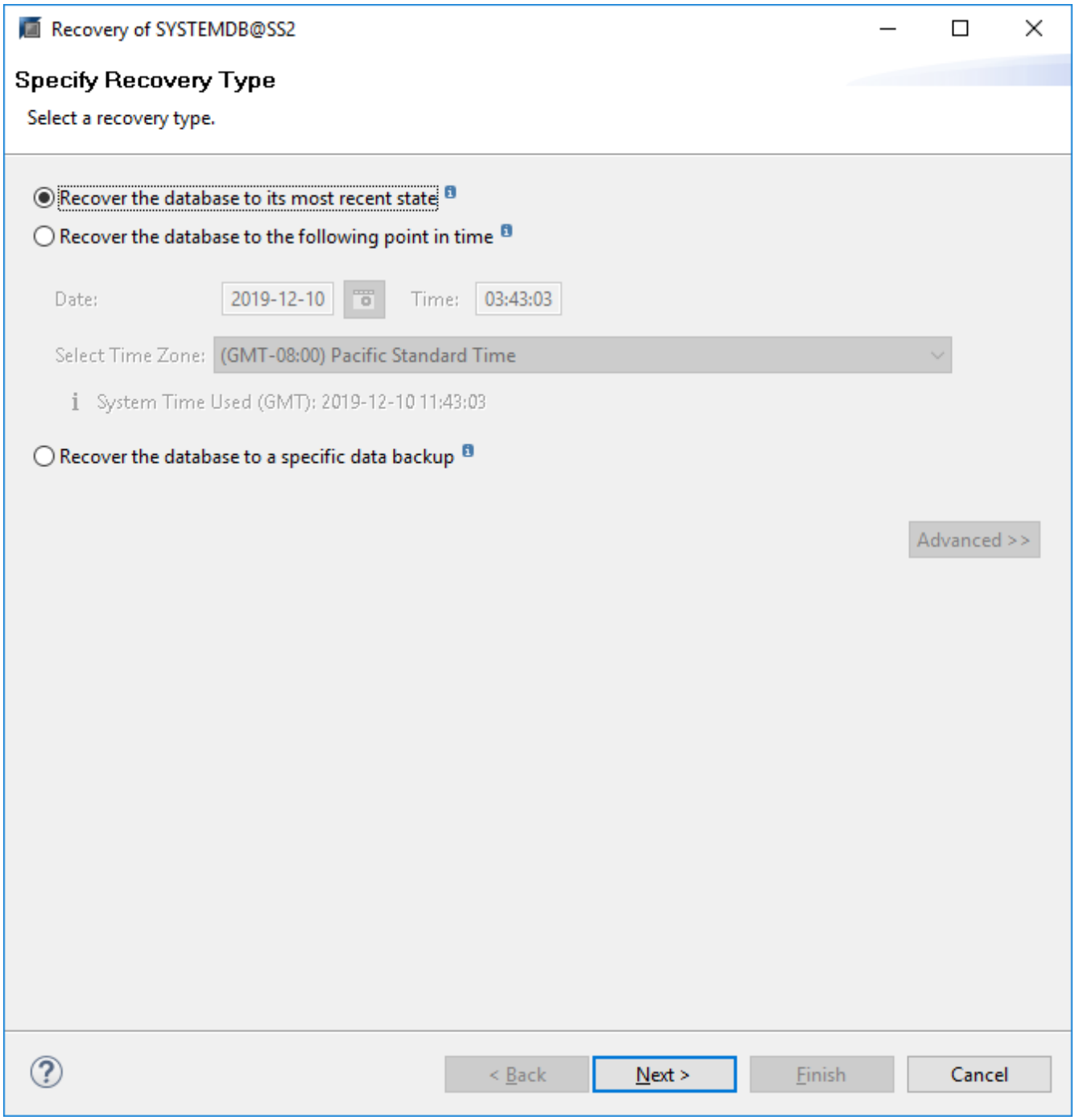


2. Cliquez sur OK pour arrêter la base de données SAP HANA.

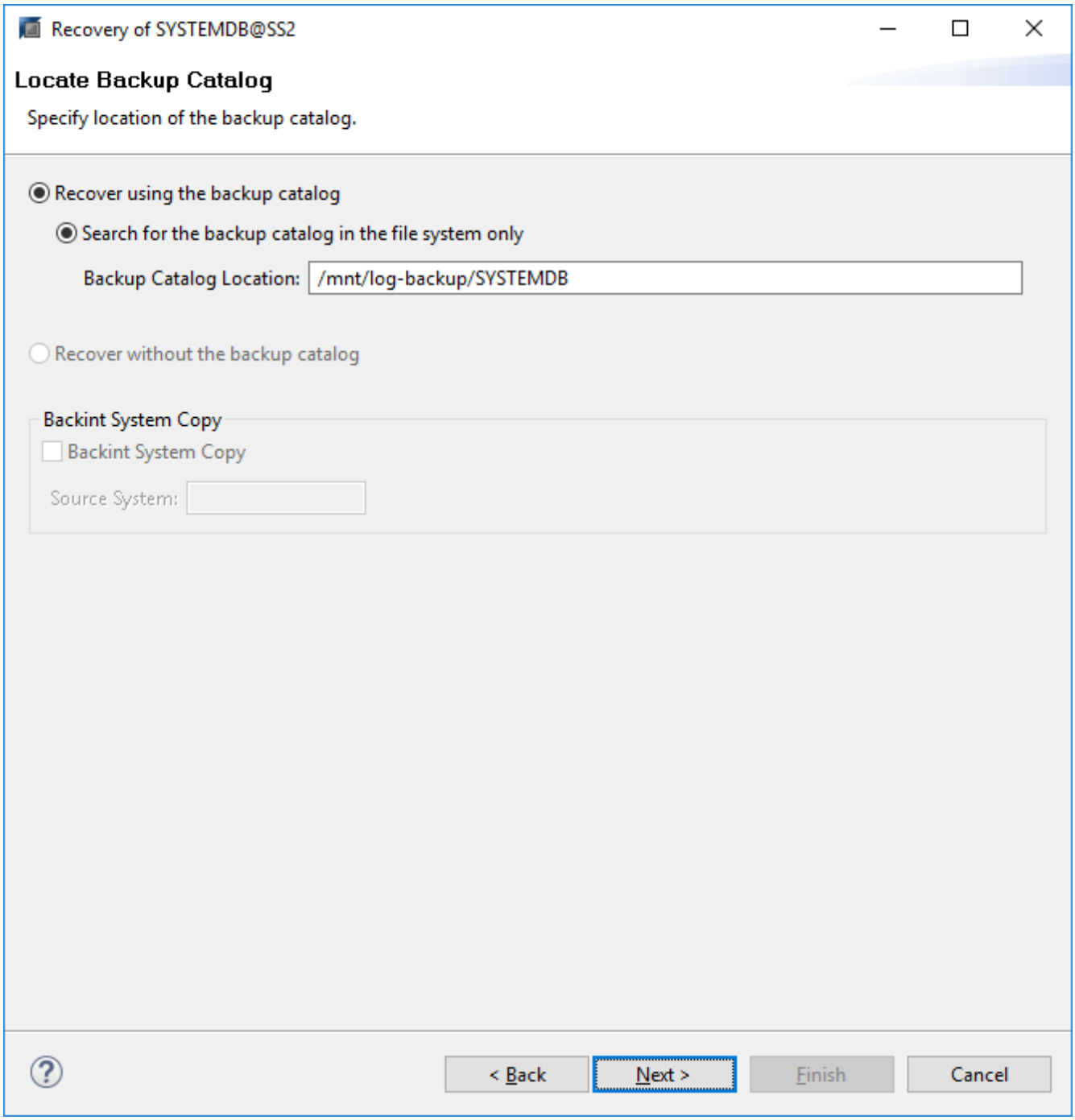


Le système SAP HANA s'arrête et l'assistant de restauration est démarré.

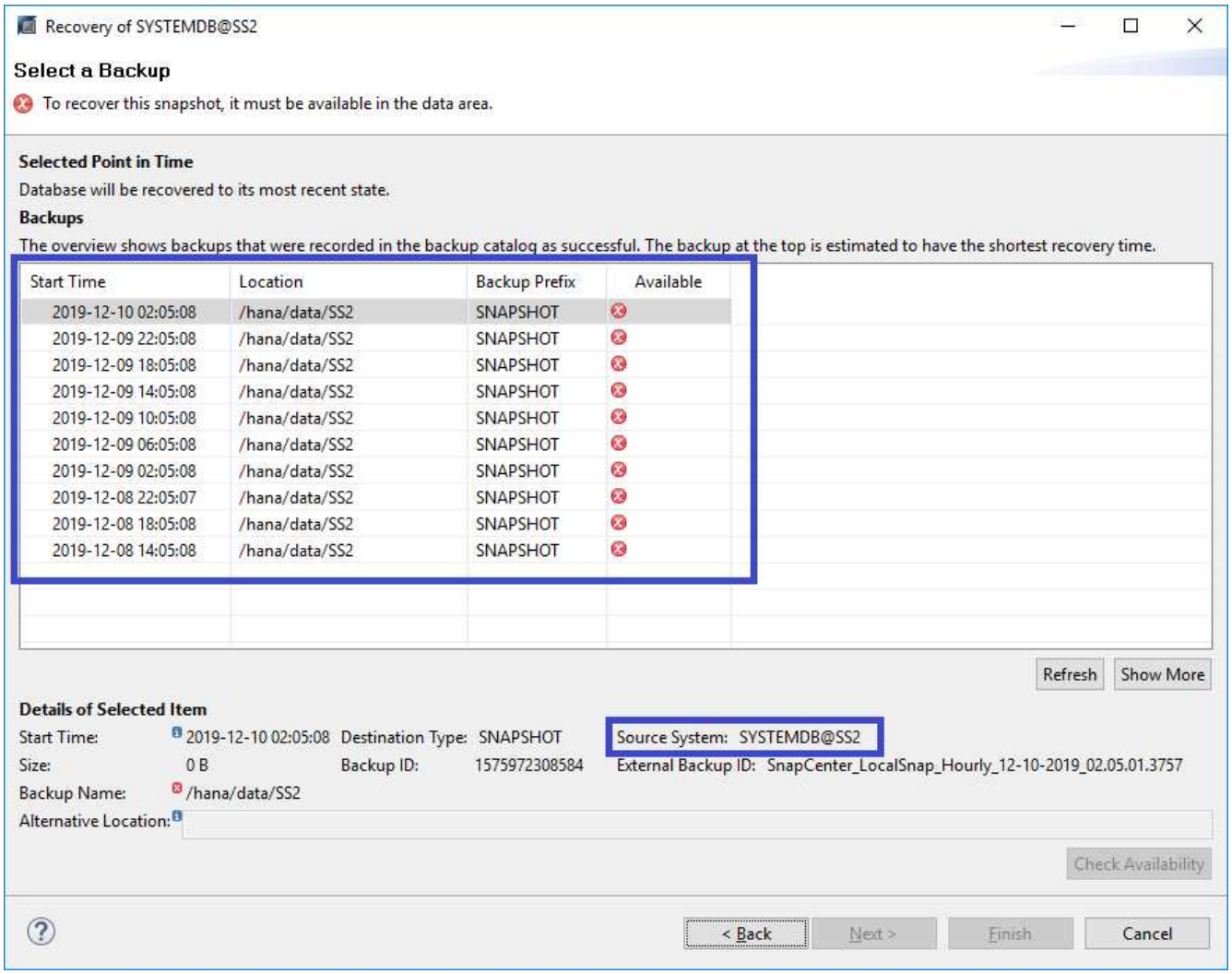
3. Sélectionnez le type de récupération et cliquez sur Suivant.



4. Indiquez l’emplacement du catalogue de sauvegardes et cliquez sur Next (Suivant).



5. Une liste des sauvegardes disponibles s'affiche en fonction du contenu du catalogue de sauvegardes. Choisissez la sauvegarde souhaitée et notez l'ID de sauvegarde externe : dans notre exemple, la sauvegarde la plus récente.



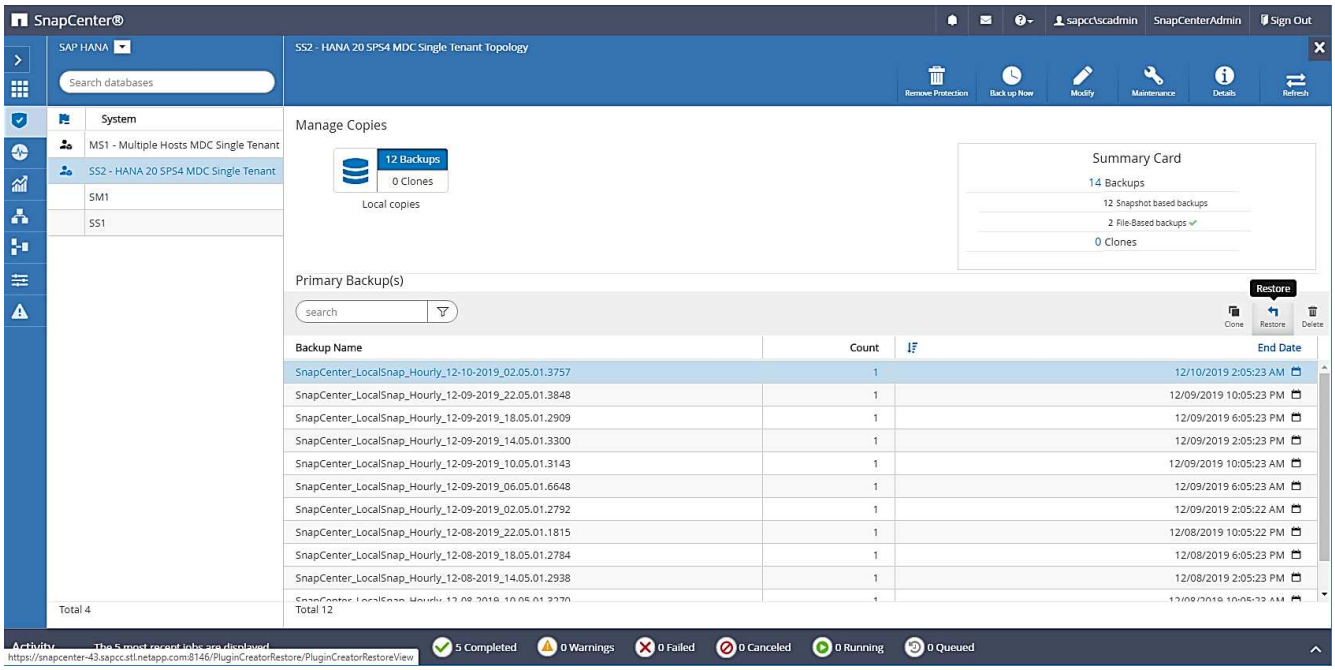
6. Démontez tous les volumes de données.

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

Pour un système hôte SAP HANA équipé de la technologie NFS, tous les volumes de données sur chaque hôte doivent être démontés.

Dans une configuration SAP HANA à plusieurs hôtes avec FC, l'opération de démontage est exécutée par le serveur de noms SAP HANA dans le cadre du processus d'arrêt.

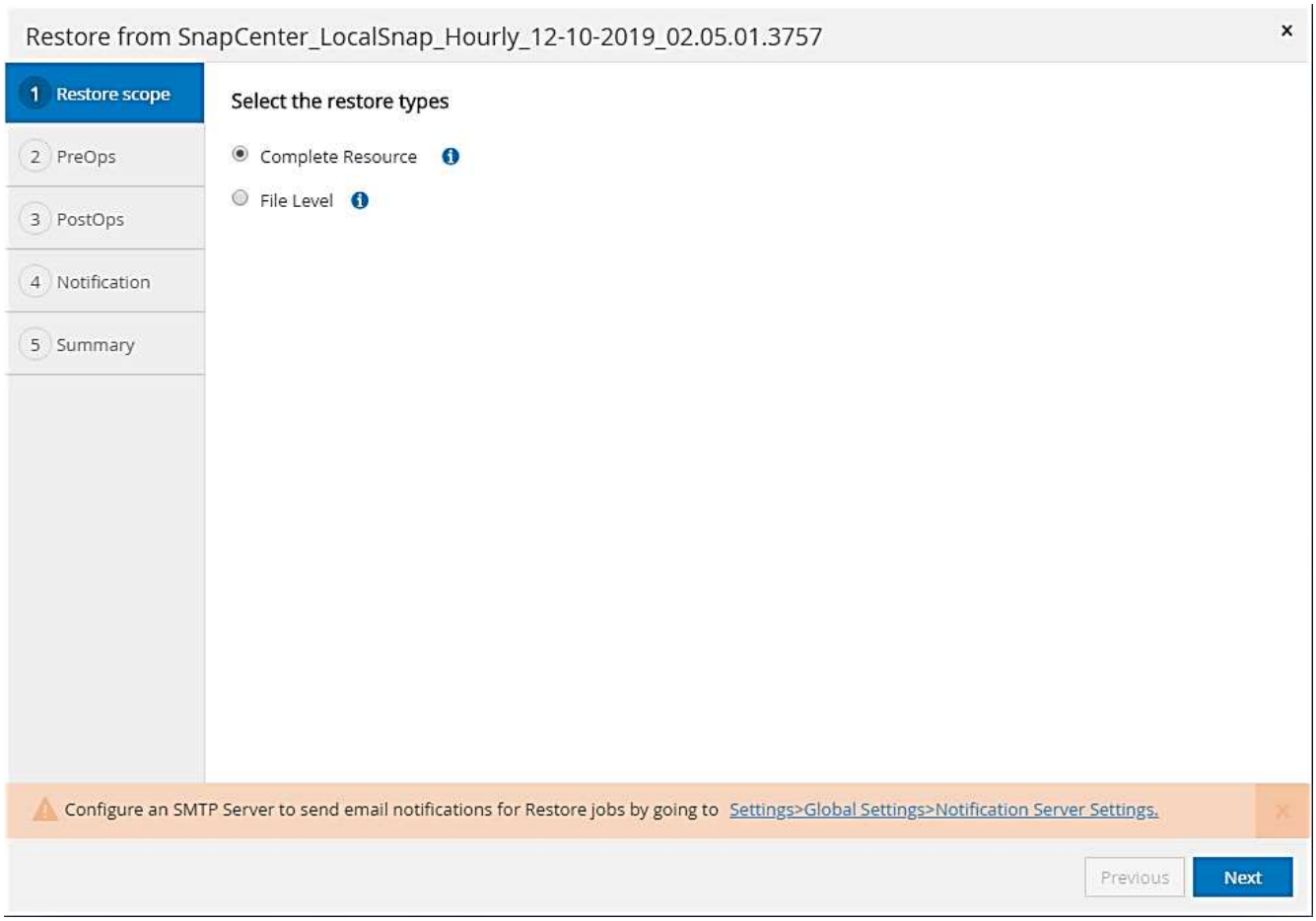
7. Dans l'interface graphique de SnapCenter, sélectionnez la vue topologique des ressources et sélectionnez la sauvegarde à restaurer, dans notre exemple, la sauvegarde principale la plus récente. Cliquez sur l'icône Restaurer pour lancer la restauration.



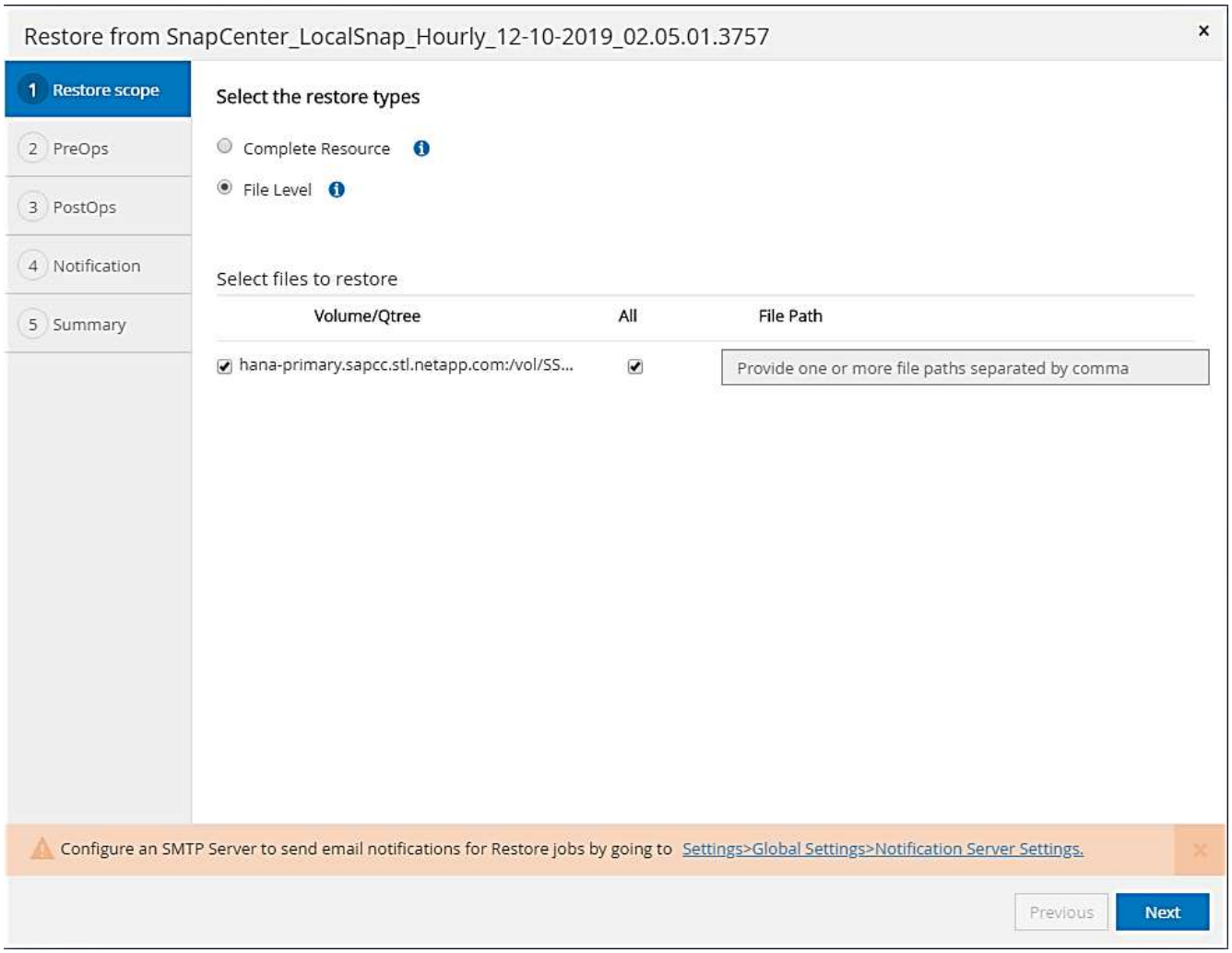
L'assistant de restauration SnapCenter démarre.

8. Sélectionnez le type de restauration ressource complète ou niveau de fichier.

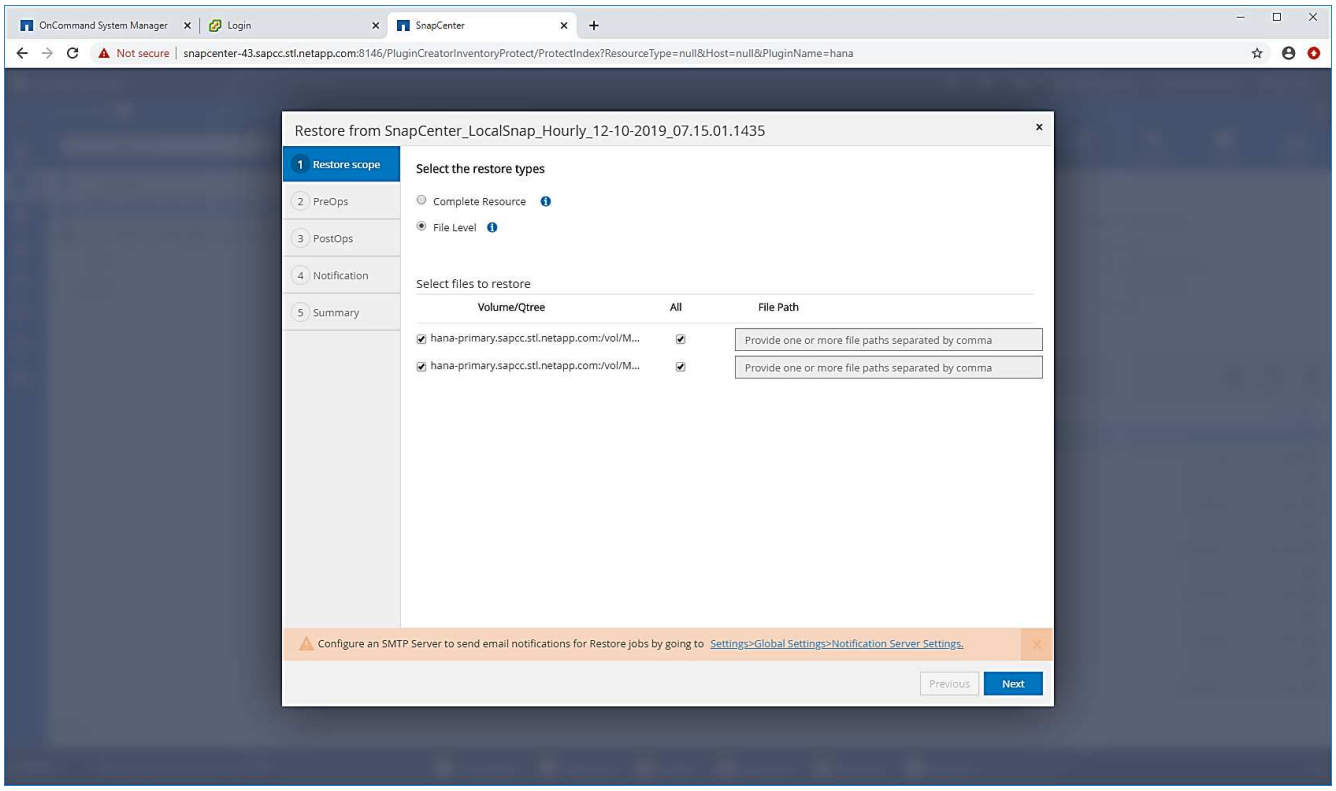
   Sélectionnez ressource complète pour utiliser une restauration basée sur le volume.



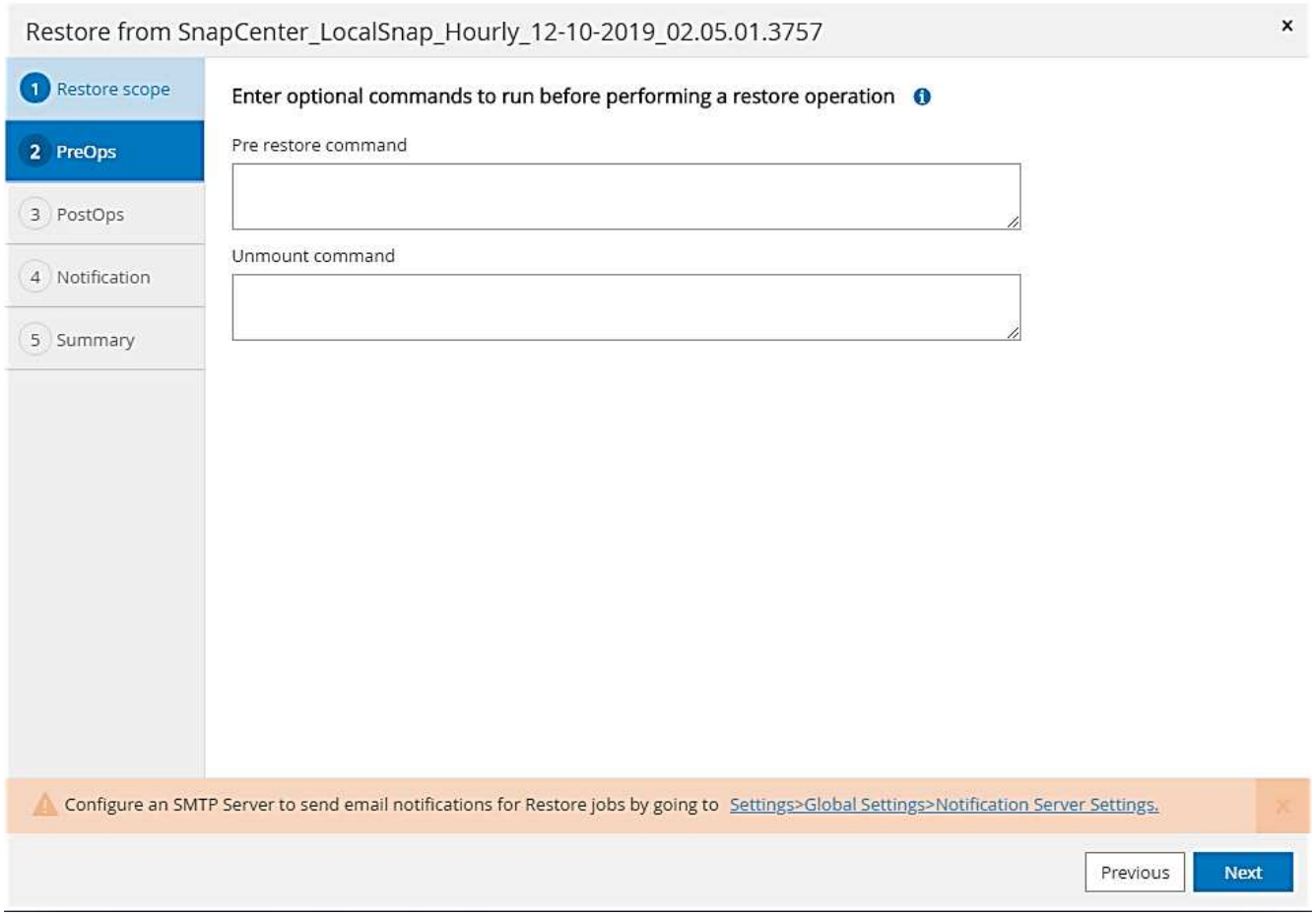
9. Sélectionnez niveau de fichier et tous pour utiliser une opération SnapRestore à un seul fichier pour tous les fichiers.



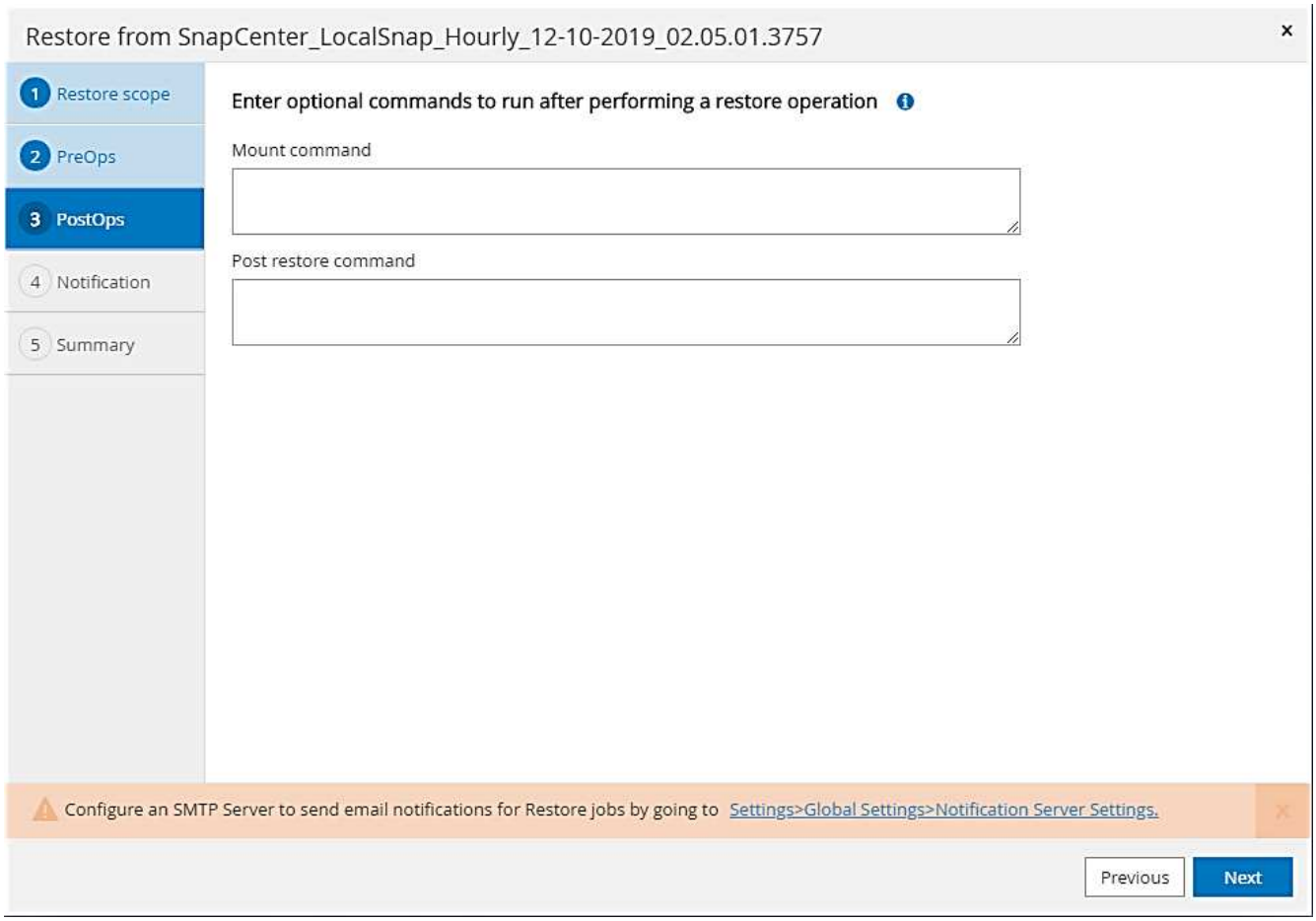
Pour effectuer une restauration au niveau fichier d'un système hôte SAP HANA multiple, sélectionnez tous les volumes.



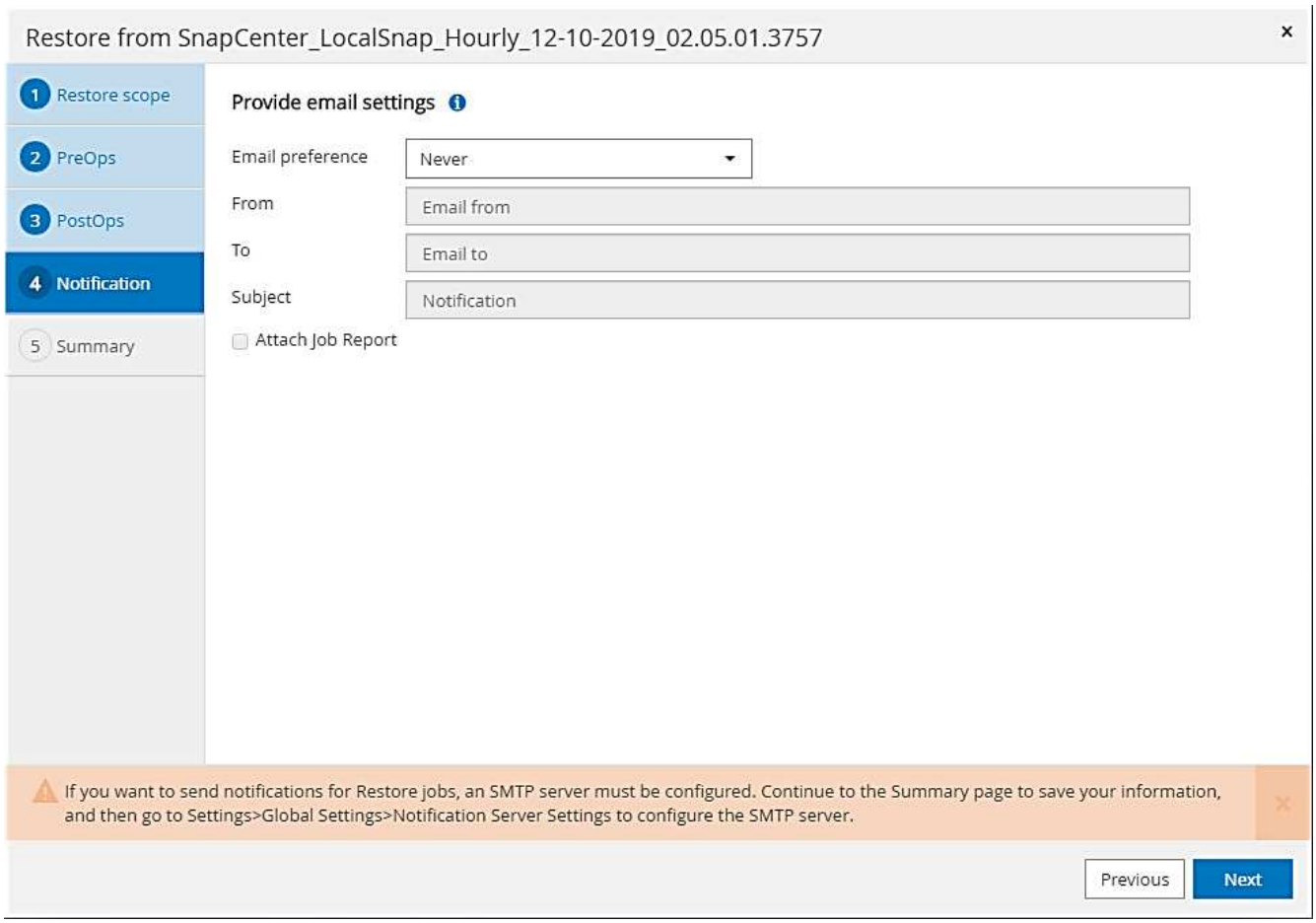
10. (Facultatif) spécifiez les commandes à exécuter depuis le plug-in SAP HANA exécuté sur l'hôte du plug-in HANA central. Cliquez sur Suivant.



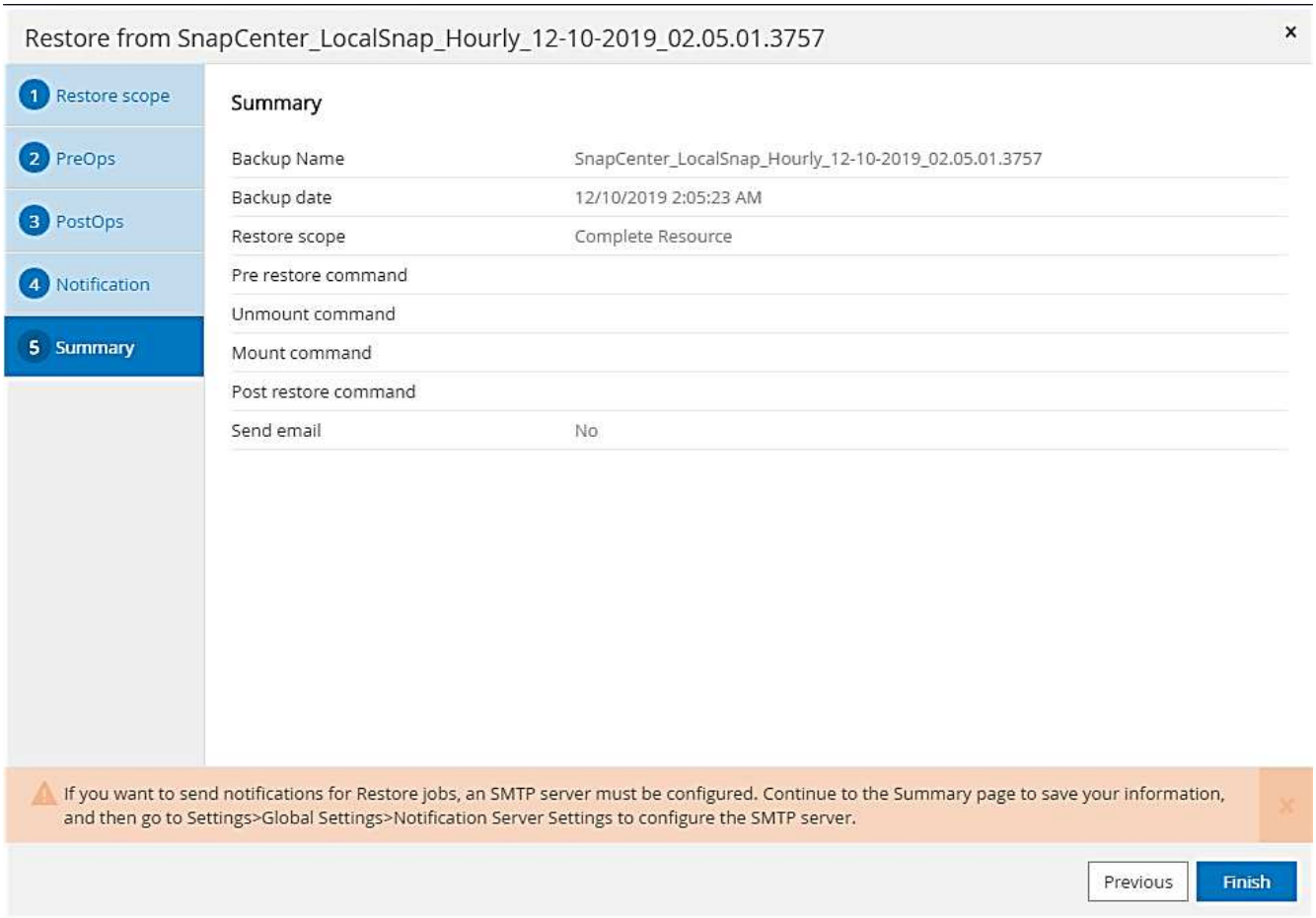
11. Spécifiez les commandes facultatives et cliquez sur Next (Suivant).



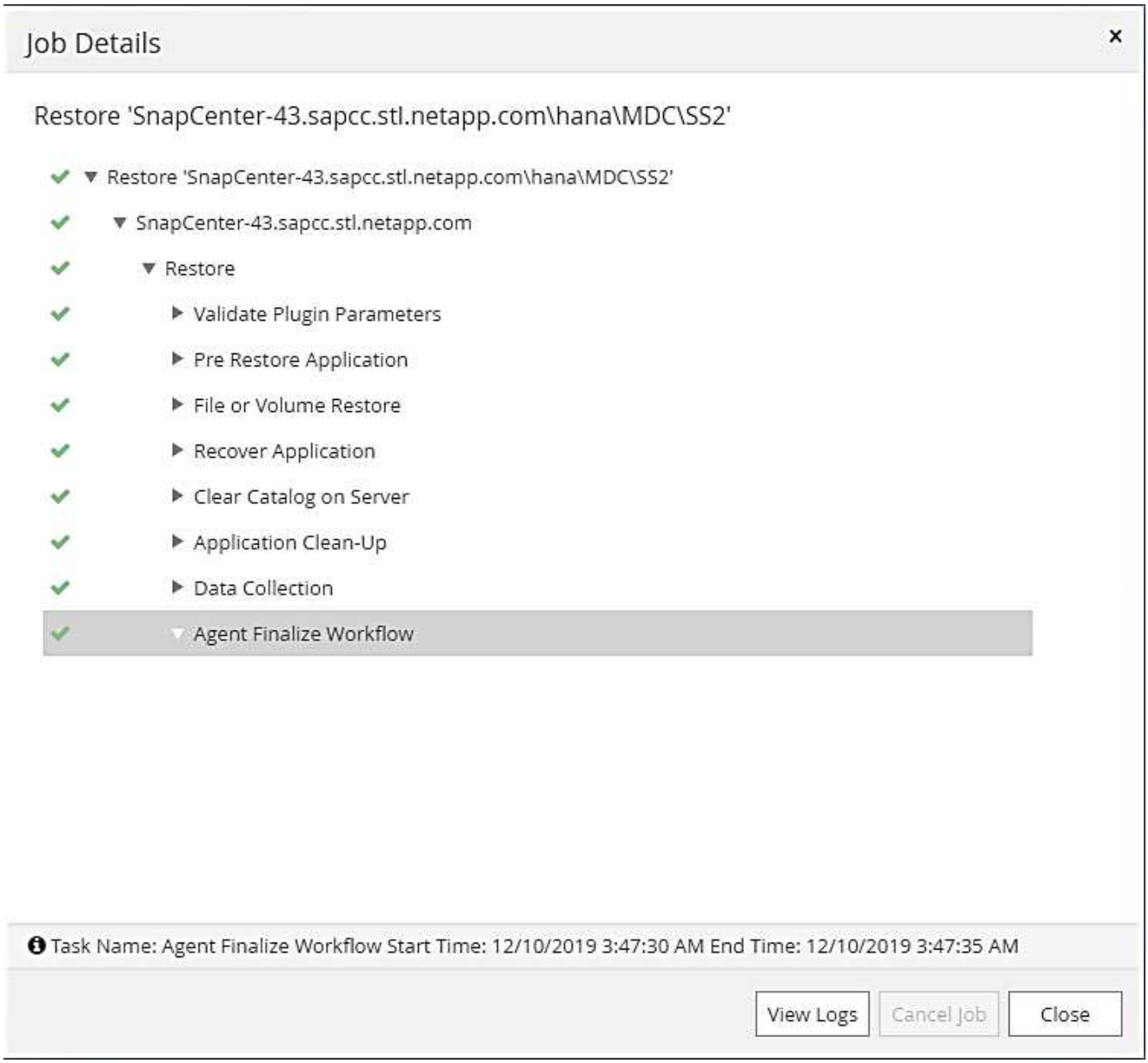
12. Spécifiez les paramètres de notification afin que SnapCenter puisse envoyer un e-mail d'état et un journal des tâches. Cliquez sur Suivant.



13. Vérifiez le résumé et cliquez sur Terminer pour lancer la restauration.



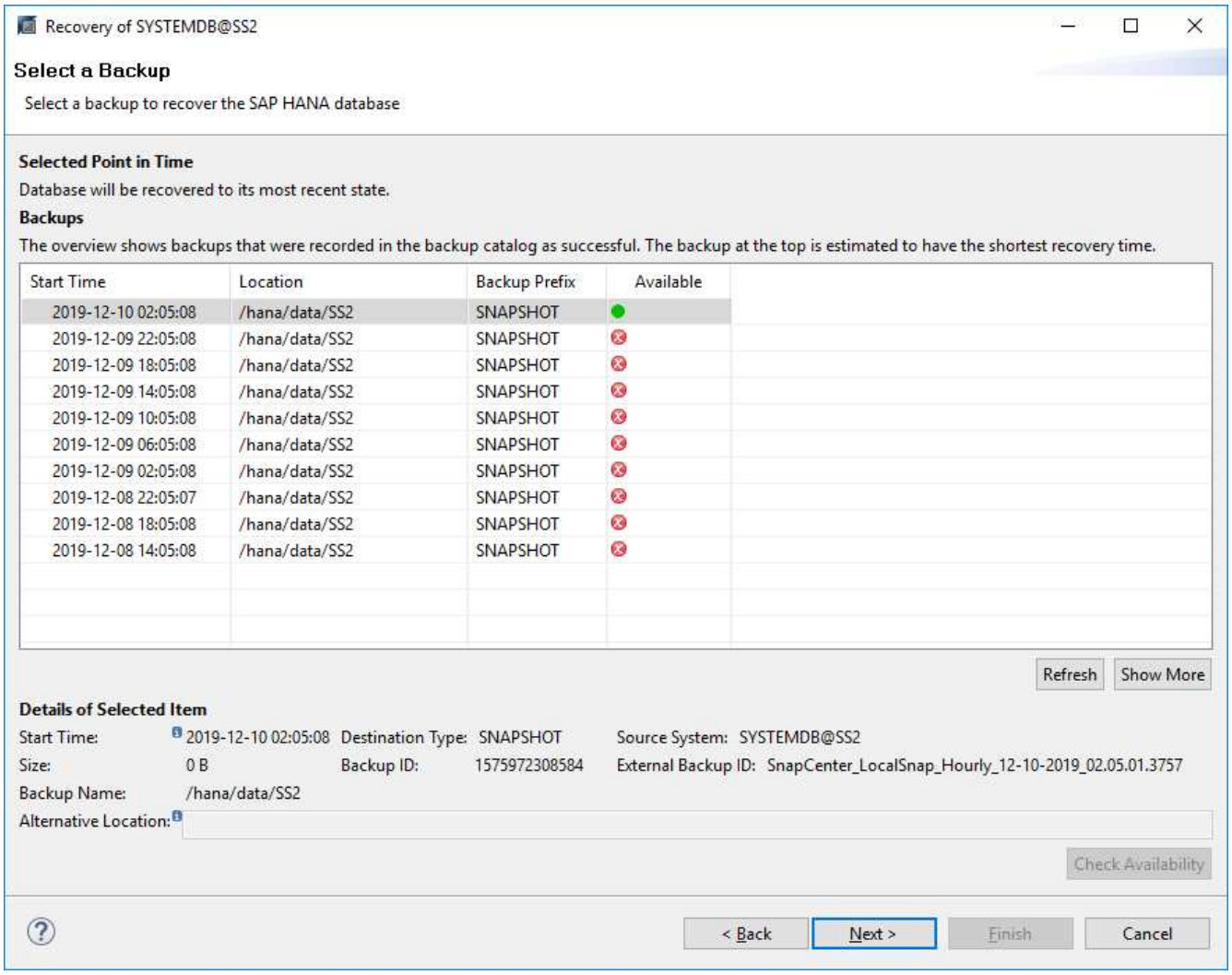
14. La tâche de restauration démarre et le journal des travaux peut être affiché en double-cliquant sur la ligne de journal dans le volet activité.



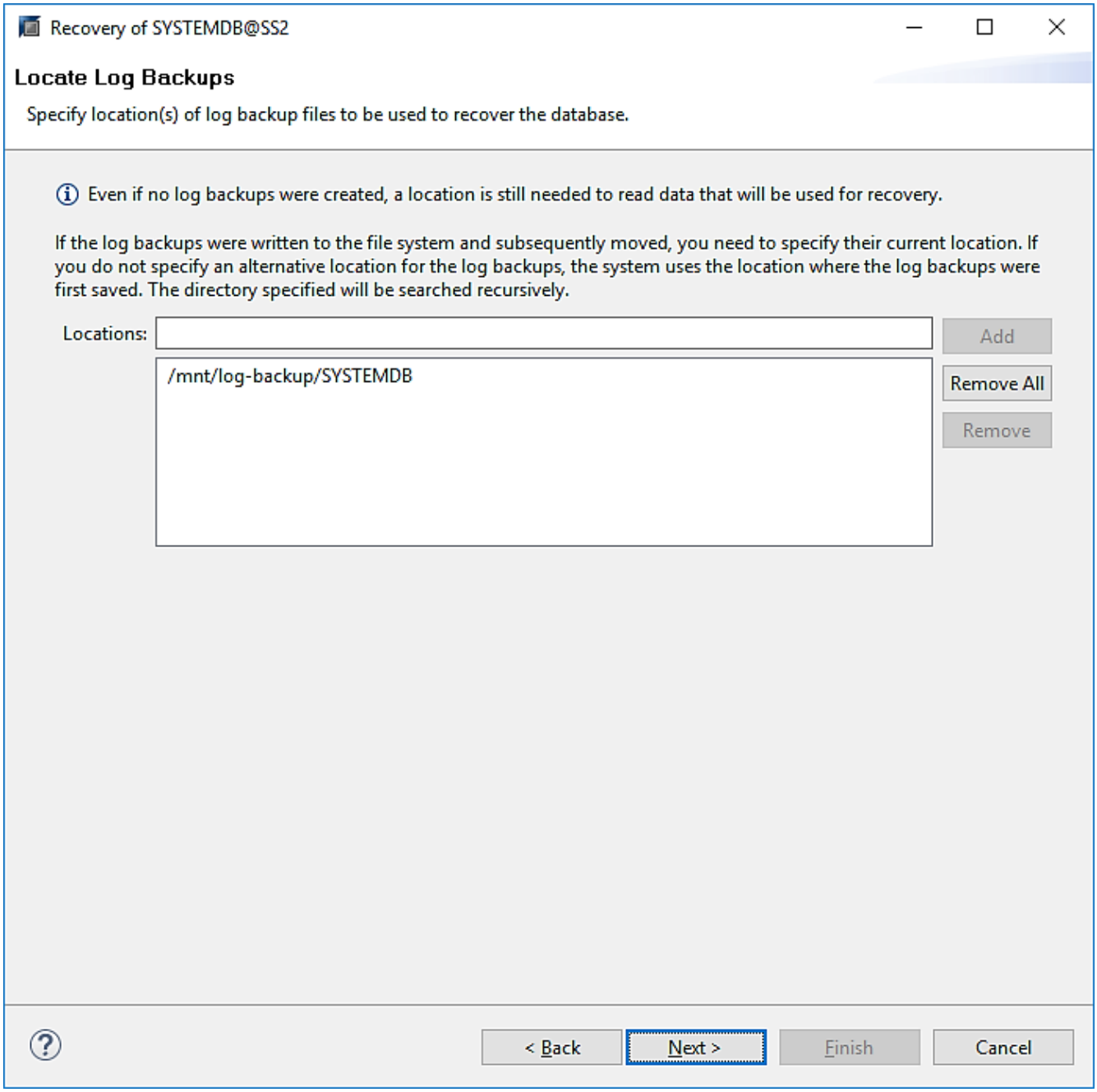
15. Attendez la fin du processus de restauration. Montez tous les volumes de données sur chaque hôte de base de données. Dans notre exemple, un seul volume doit être remonté sur l'hôte de base de données.

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

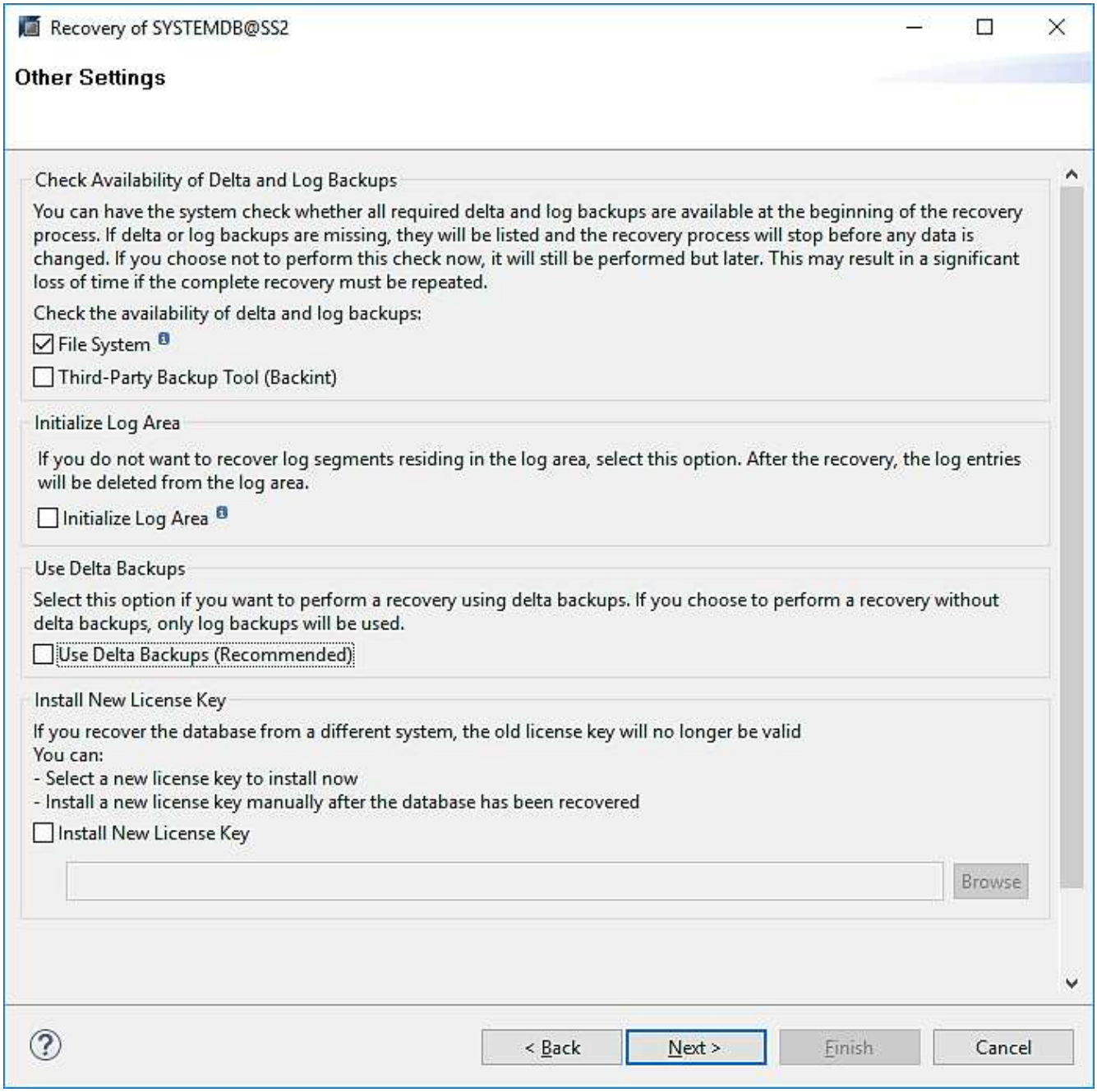
16. Accédez à SAP HANA Studio et cliquez sur Actualiser pour mettre à jour la liste des sauvegardes disponibles. La sauvegarde restaurée avec SnapCenter s'affiche avec une icône verte dans la liste des sauvegardes. Sélectionnez la sauvegarde et cliquez sur Suivant.



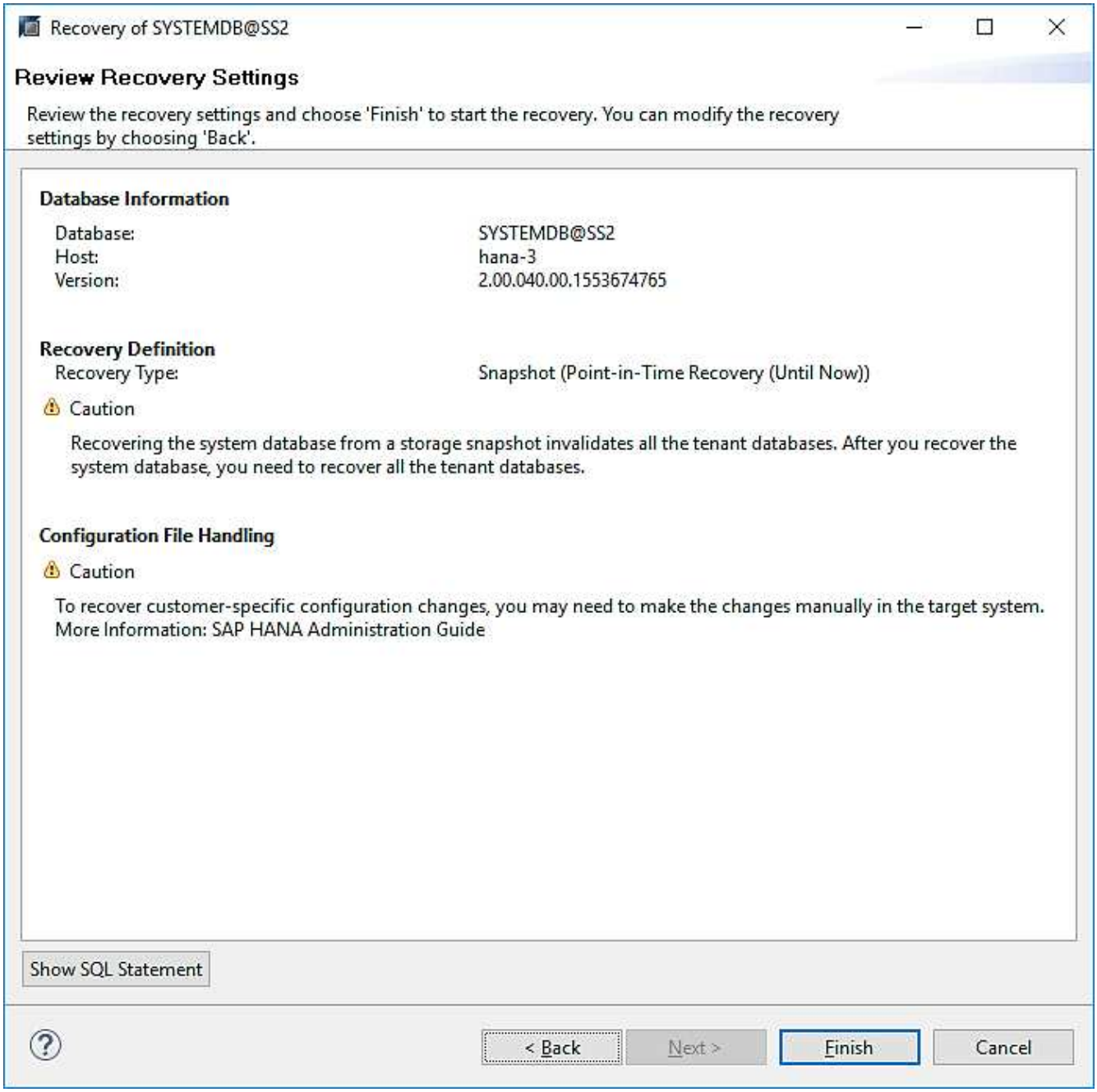
17. Indiquez l’emplacement des sauvegardes des journaux. Cliquez sur Suivant.



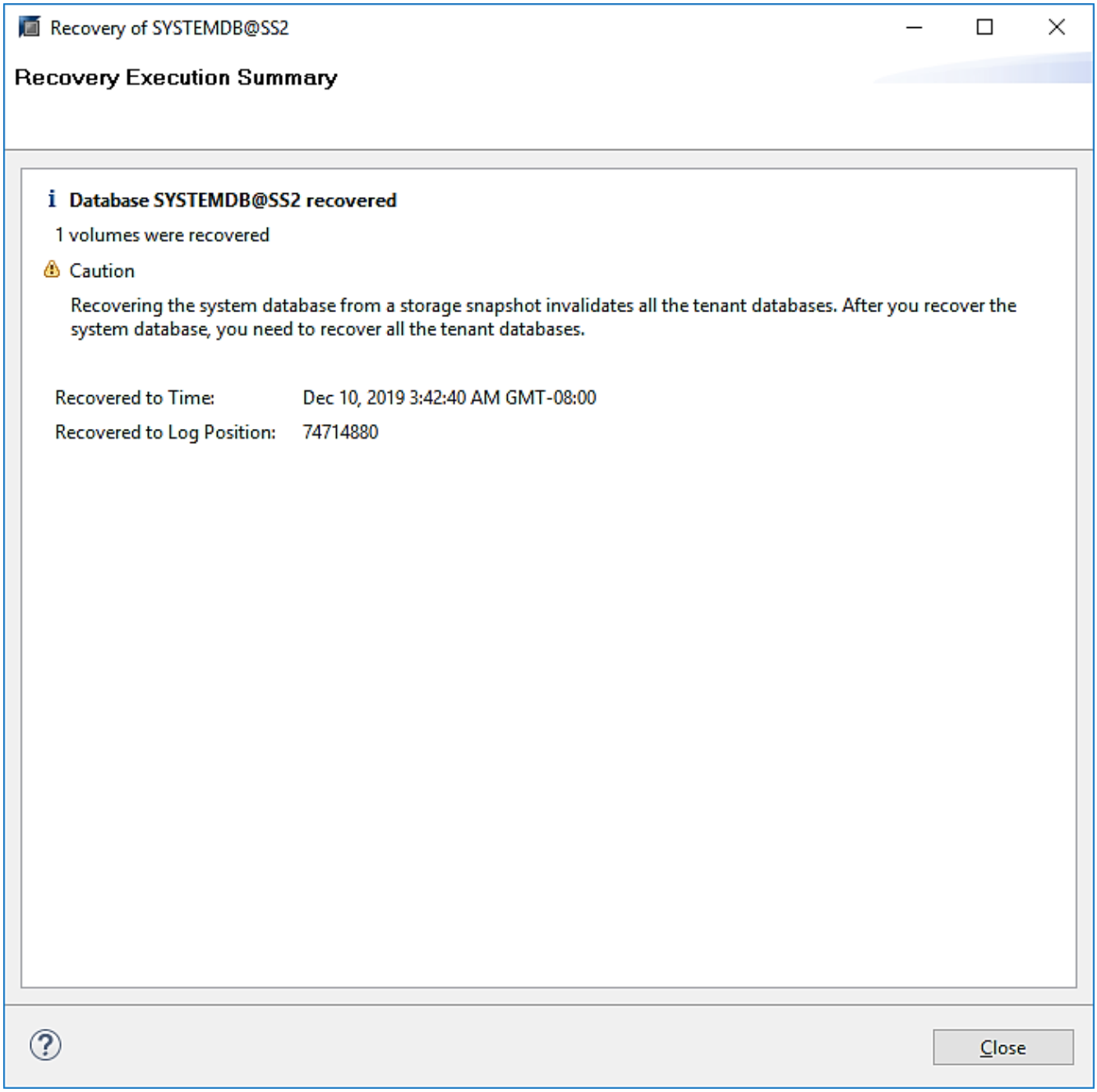
18. Sélectionnez les autres paramètres requis. Assurez-vous que l'option utiliser les sauvegardes Delta n'est pas sélectionnée. Cliquez sur Suivant.



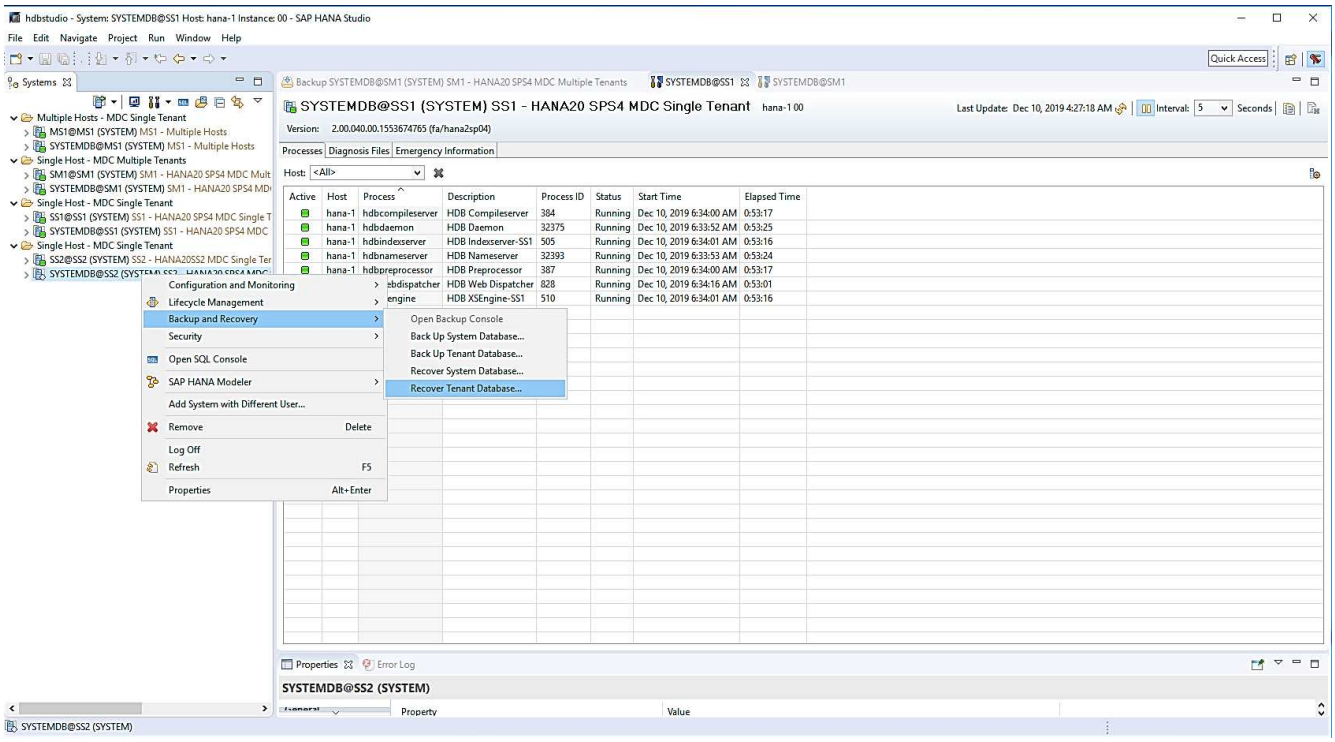
19. Vérifiez les paramètres de restauration et cliquez sur Terminer.



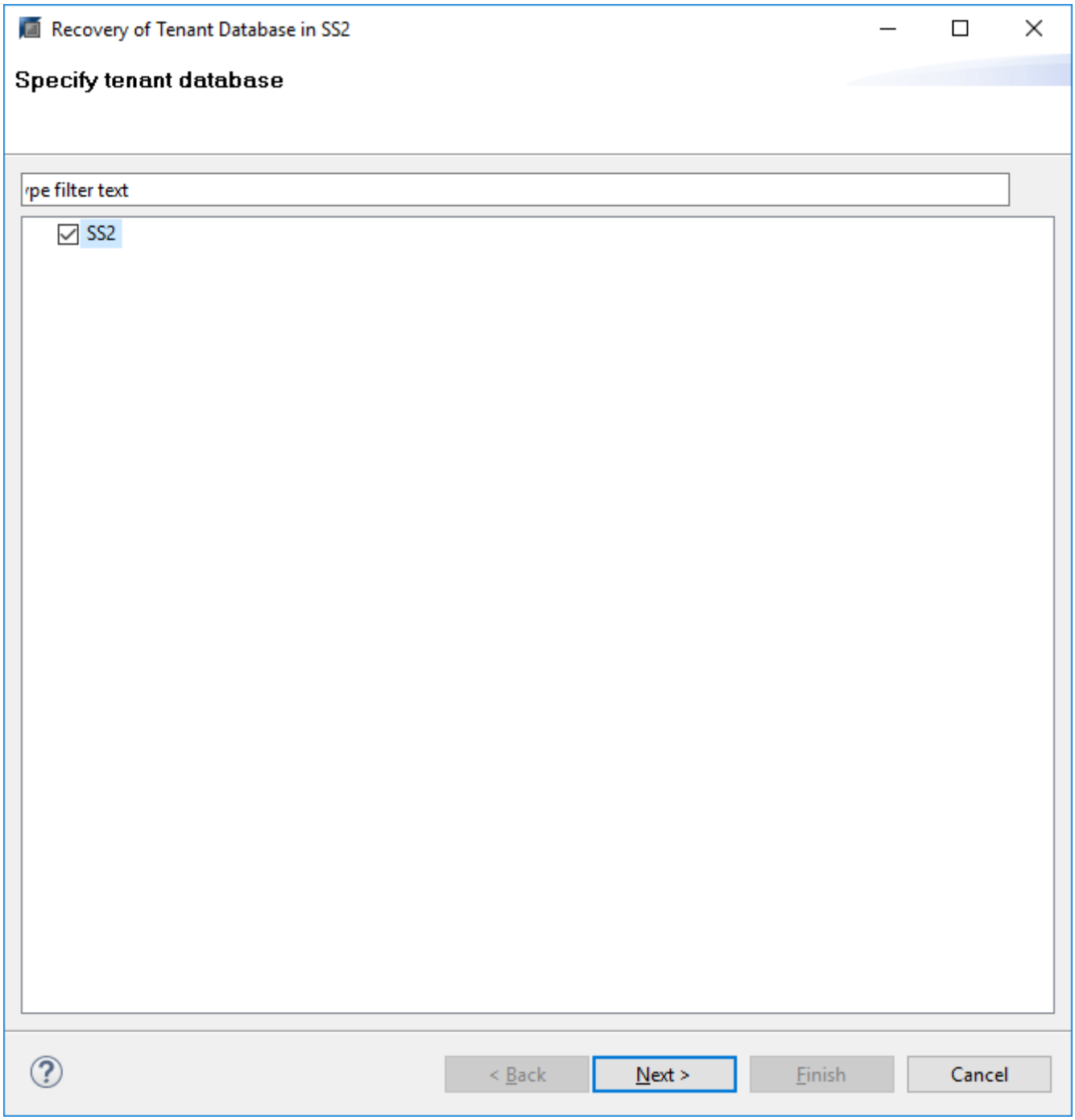
20. Le processus de restauration démarre. Attendez la fin de la restauration de la base de données système.



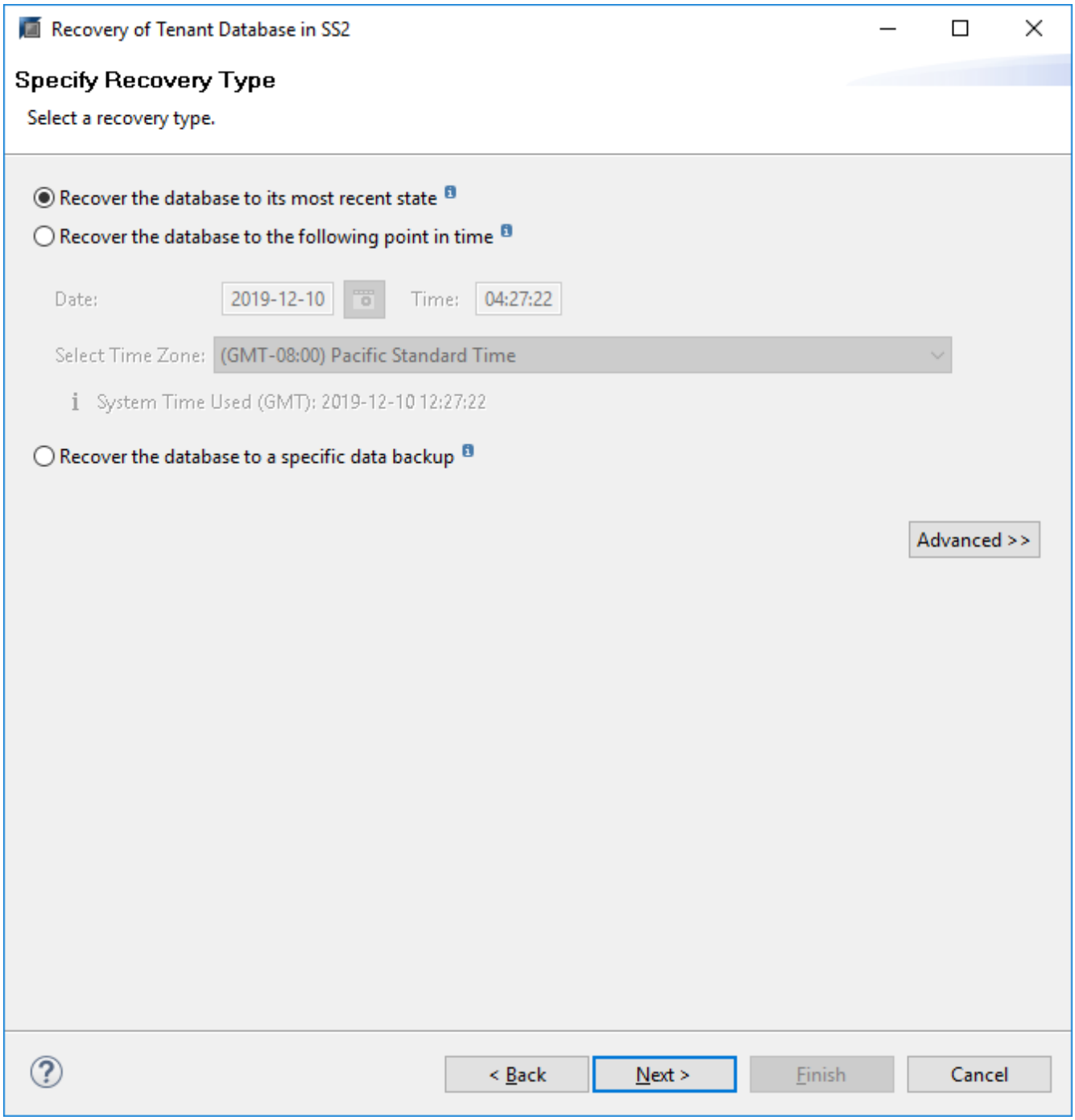
21. Dans SAP HANA Studio, sélectionnez l'entrée de la base de données système et lancez Backup Recovery - recover tenant Database.



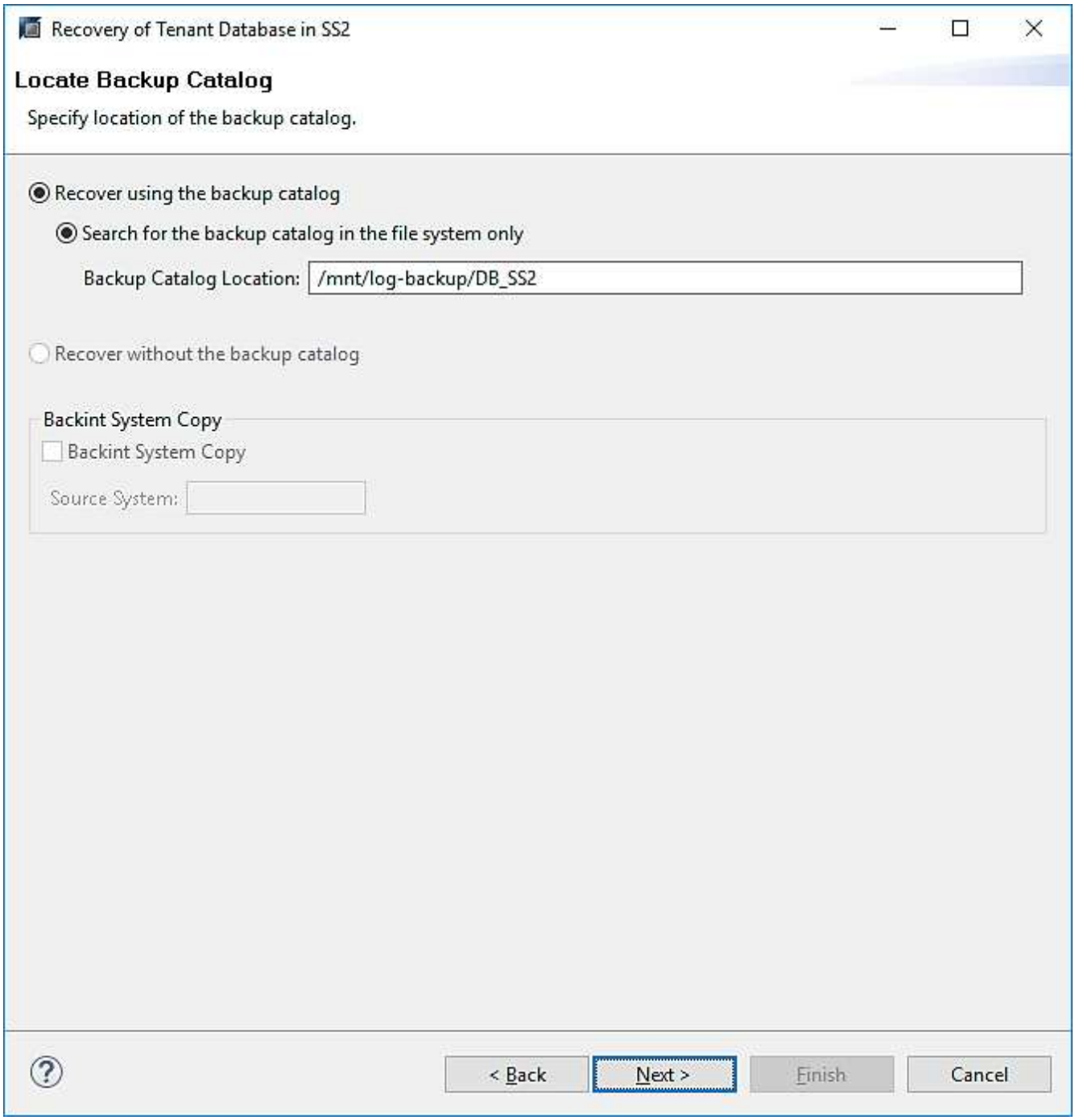
22. Sélectionnez le locataire à restaurer et cliquez sur Next (Suivant).



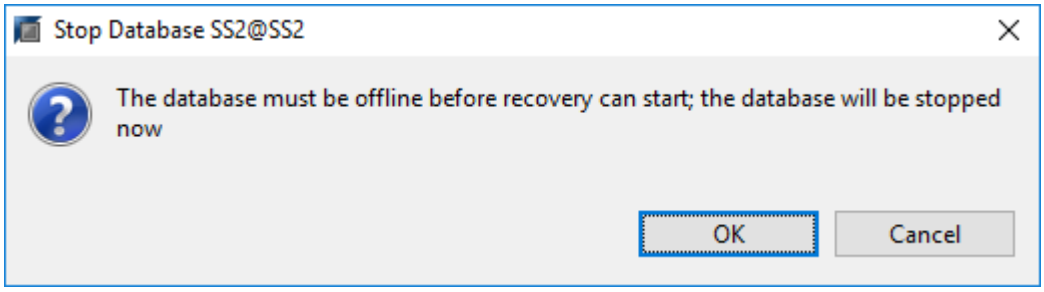
23. Spécifiez le type de récupération et cliquez sur Suivant.



24. Confirmez l’emplacement du catalogue de sauvegarde et cliquez sur Next (Suivant).

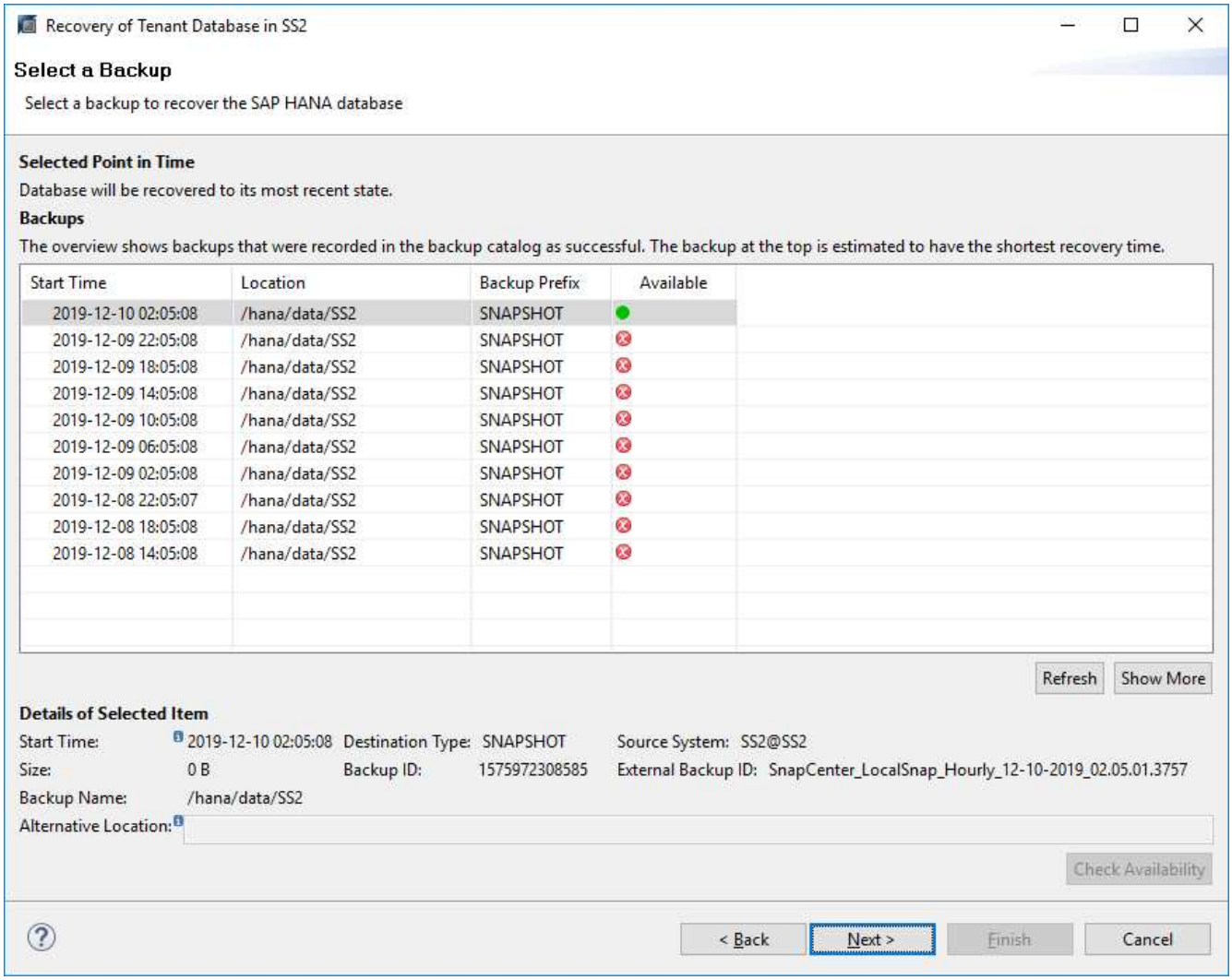


25. Vérifiez que la base de données des locataires est hors ligne. Cliquez sur OK pour continuer.

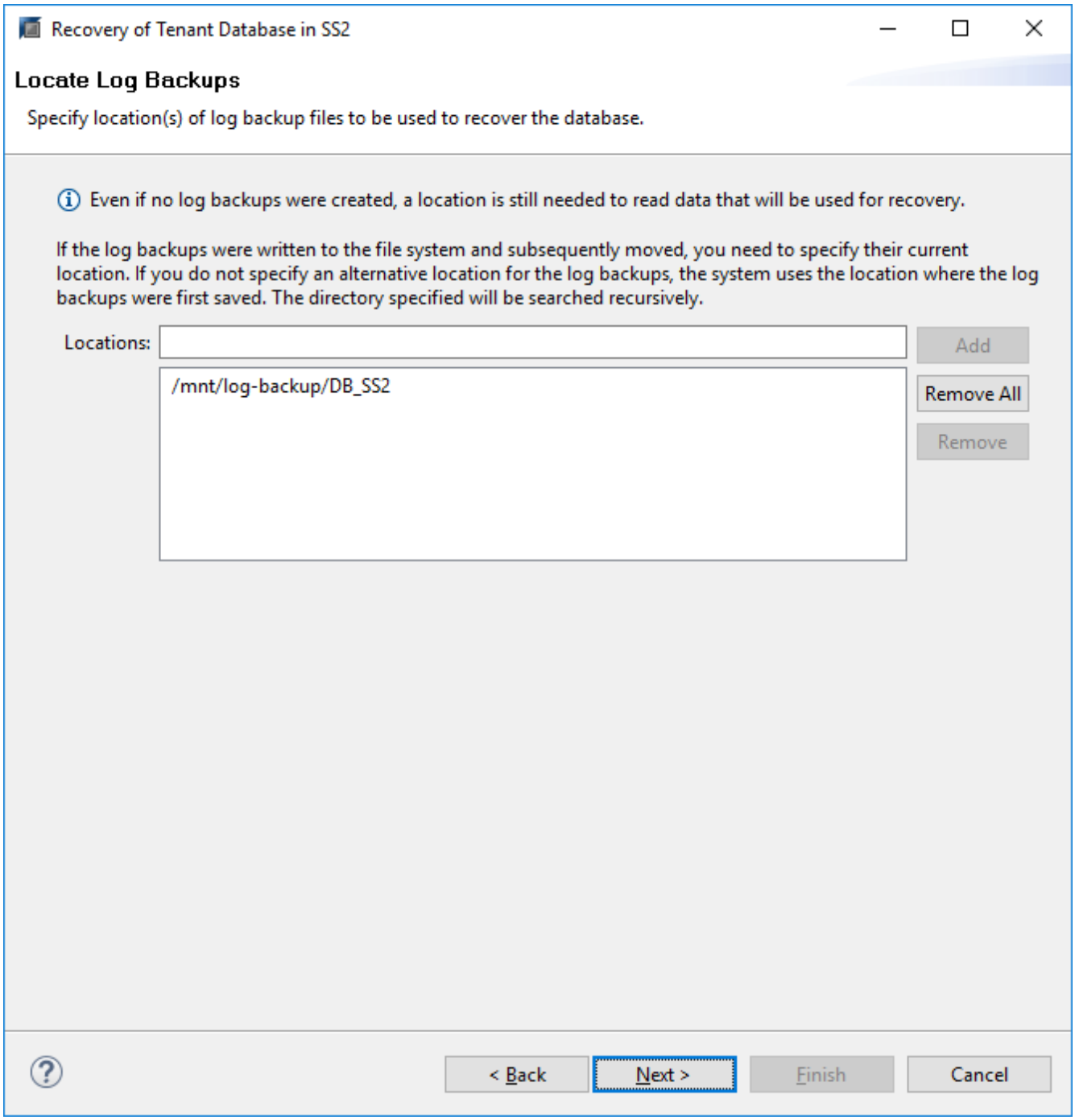


26. Étant donné que la restauration du volume de données s'est produite avant la restauration de la base de données du système, la sauvegarde du locataire est immédiatement disponible. Sélectionnez la

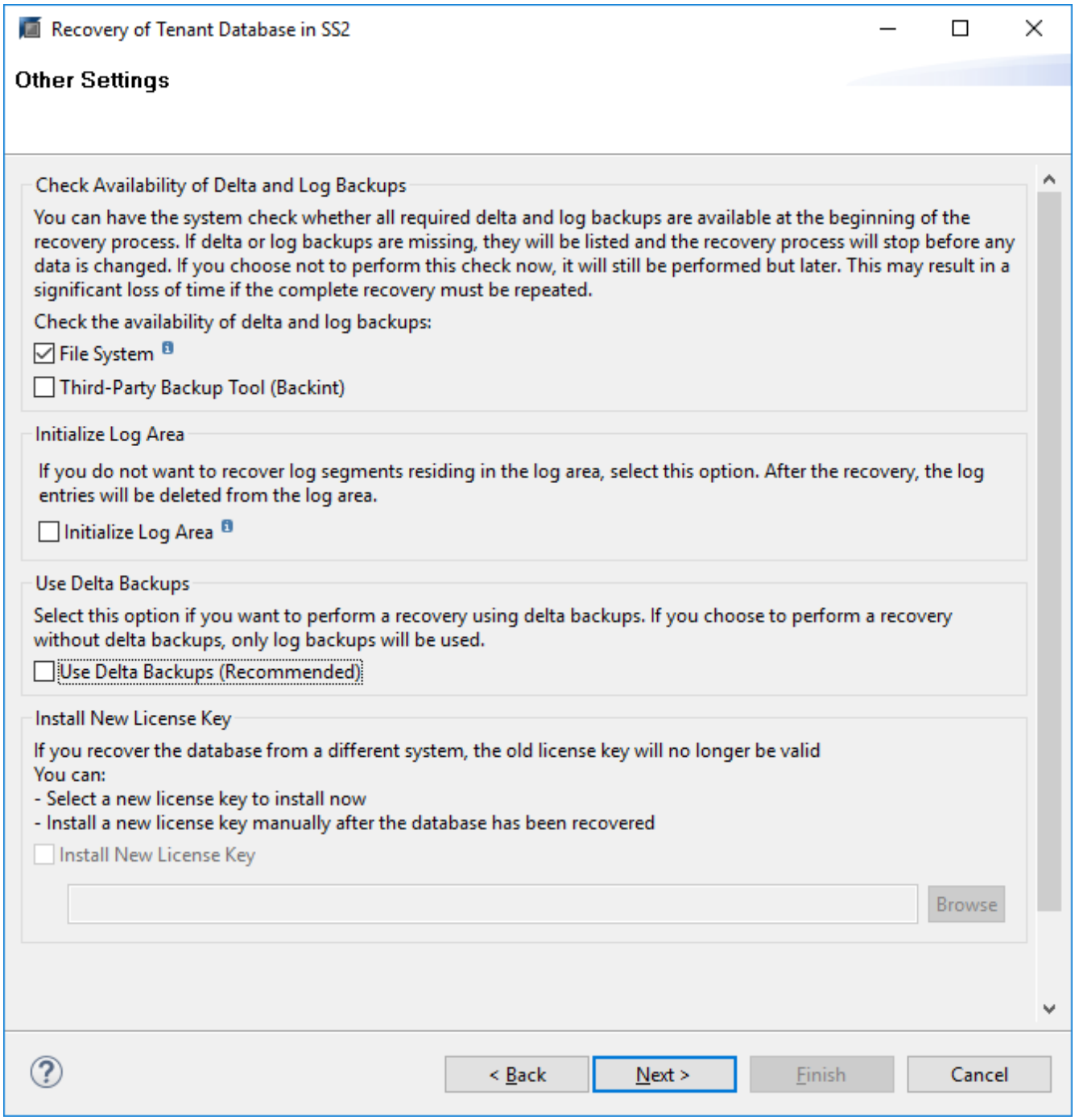
sauvegarde en vert et cliquez sur Suivant.



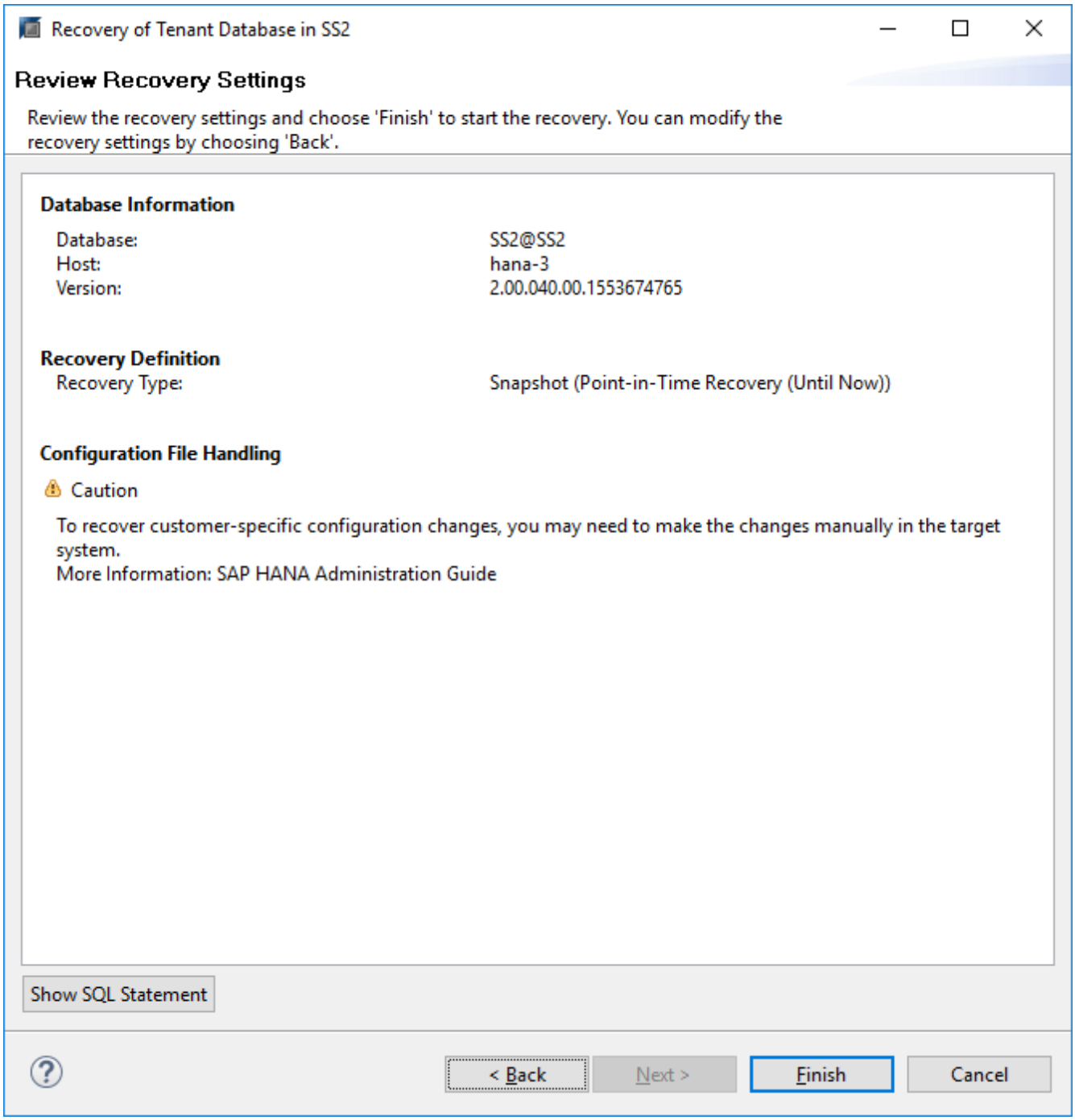
27. Confirmez l’emplacement de sauvegarde du journal et cliquez sur Suivant.



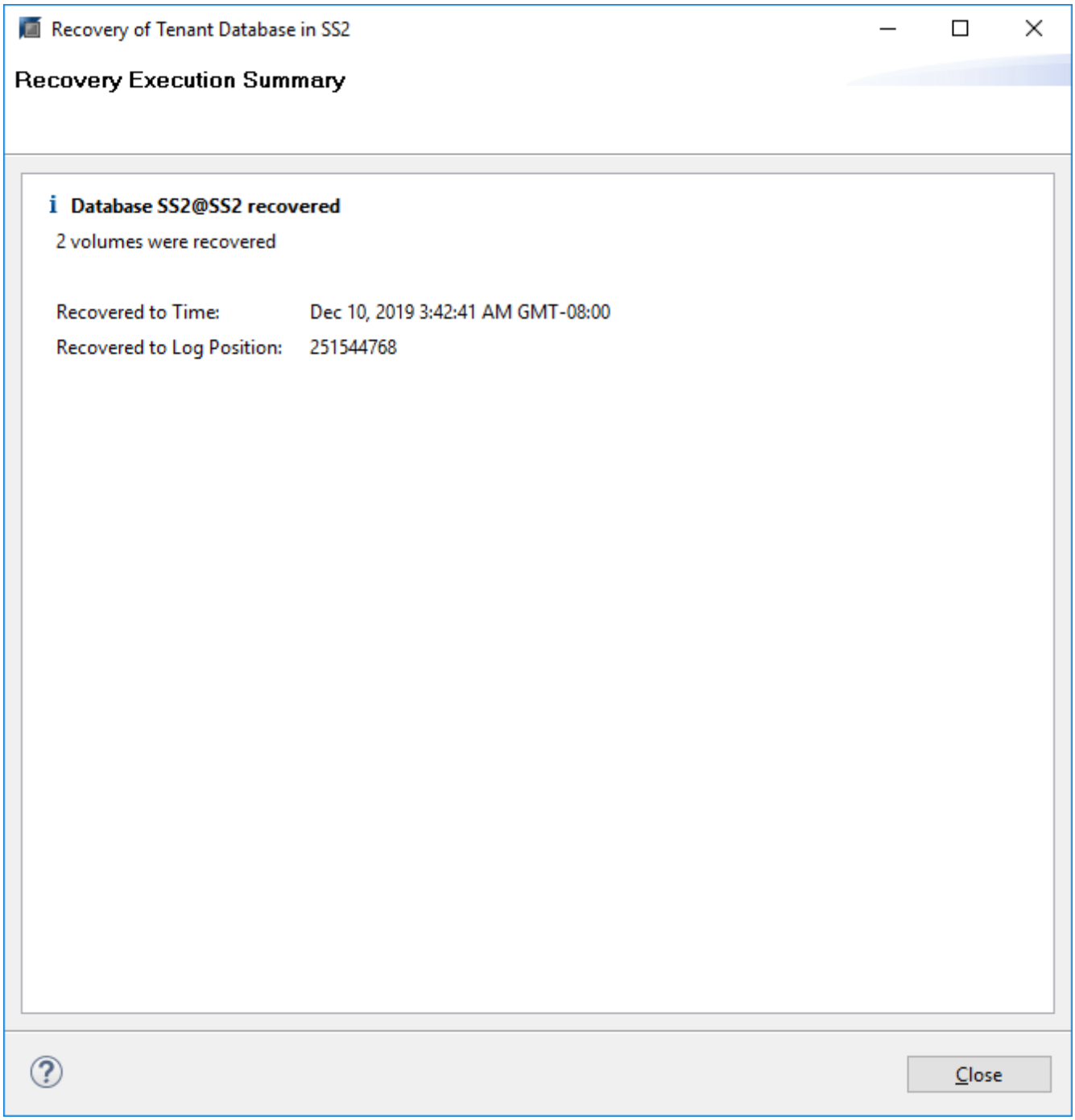
28. Sélectionnez les autres paramètres requis. Assurez-vous que l'option utiliser les sauvegardes Delta n'est pas sélectionnée. Cliquez sur Suivant.



29. Vérifiez les paramètres de restauration et démarrez le processus de restauration de la base de données des locataires en cliquant sur Terminer.



30. Attendez que la récupération soit terminée et que la base de données des locataires démarre.



Le système SAP HANA est opérationnel.

Pour un système MDC SAP HANA avec plusieurs locataires, vous devez répéter les étapes 20 à 29 pour chaque locataire.

Configuration avancée et réglage

Cette section décrit les options de configuration et d'optimisation que les clients peuvent utiliser pour adapter la configuration de SnapCenter à leurs besoins spécifiques. Certains paramètres ne s'appliquent pas à tous les scénarios client.

Activez la communication sécurisée sur la base de données HANA

Si les bases de données HANA sont configurées avec une communication sécurisée, le `hdbsql` La commande exécutée par SnapCenter doit utiliser des options de ligne de commande supplémentaires. Cela peut être réalisé à l'aide d'un script wrapper qui appelle `hdbsql` avec les options requises.

> Il existe plusieurs options pour configurer la communication SSL. Dans les exemples suivants, la configuration client la plus simple est décrite à l'aide de l'option de ligne de commande, où aucune validation de certificat de serveur n'est effectuée. Si la validation de certificat côté serveur et/ou client est nécessaire, différentes options de ligne de commande hdbsql sont nécessaires et vous devez configurer l'environnement PSE en conséquence, comme décrit dans le Guide de sécurité SAP HANA.

Au lieu de configurer le `hdbsql` exécutable dans le `hana.properties` fichiers, le script wrapper est ajouté.

Pour un hôte plug-in HANA central sur le serveur SnapCenter Windows, vous devez ajouter le contenu suivant dans `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\hana.properties`.

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

Le script wrapper `hdbsql-ssl.cmd` appels `hdbsql.exe` avec les options de ligne de commande requises.

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

> Le `-e - ssltrustcert` L'option de ligne de commande hdbsql fonctionne également pour les systèmes HANA où SSL n'est pas activé. Cette option peut donc également être utilisée avec un hôte plug-in HANA central, où tous les systèmes HANA ne sont pas activés ou désactivés.

Si le plug-in HANA est déployé sur des hôtes de base de données HANA individuels, la configuration doit être effectuée sur chaque hôte Linux en conséquence.

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

Le script wrapper `hdbsqls` appels `hdbsql` avec les options de ligne de commande requises.

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

Désactiver la détection automatique sur l'hôte du plug-in HANA

Pour désactiver la détection automatique sur l'hôte du plug-in HANA, effectuez les opérations suivantes :

1. Sur le serveur SnapCenter, ouvrez PowerShell. Connectez-vous au serveur SnapCenter en exécutant

`Open- SmConnection` entrez le nom d'utilisateur et le mot de passe dans la fenêtre d'ouverture de session.

2. Pour désactiver la détection automatique, exécutez le `Set- SmConfigSettings` commande.

   Pour un hôte HANA `hana-2`, la commande est comme suit :

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

3. Vérifiez la configuration en exécutant le `Get- SmConfigSettings` commande.

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

   La configuration est écrite dans le fichier de configuration de l'agent sur l'hôte et reste disponible après une mise à niveau du plug-in avec SnapCenter.

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

Désactiver l'organisation automatique des sauvegardes de journaux

L'organisation des sauvegardes de journaux est activée par défaut et peut être désactivée au niveau de l'hôte du plug-in HANA. Il existe deux options pour modifier ces paramètres.

Modifiez le fichier hana.property

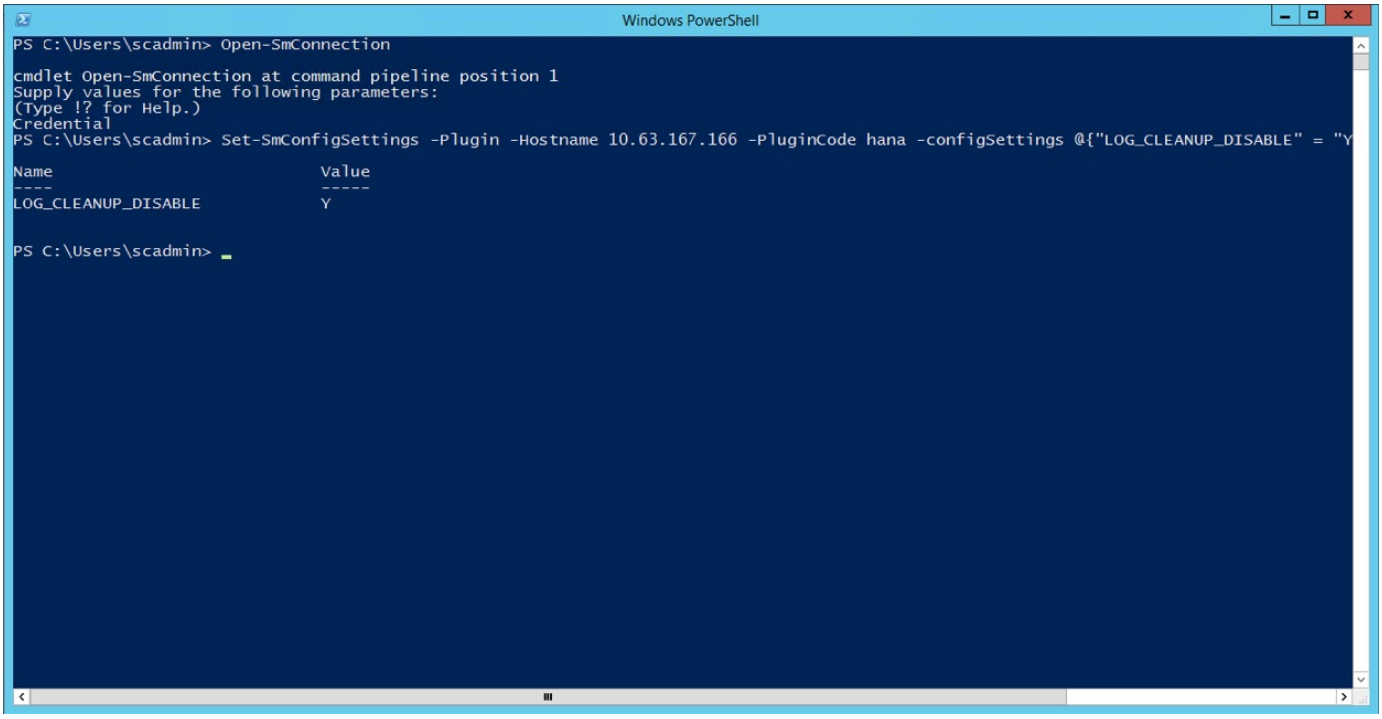
Y compris le paramètre `LOG_CLEANUP_DISABLE = Y` dans le `hana.property` Le fichier de configuration désactive le service de sauvegarde des journaux pour toutes les ressources utilisant ce plug-in SAP HANA en tant qu'hôte de communication :

- Pour l'hôte de communication Hdbsql sous Windows, le `hana.property` le fichier est situé à `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`.
- Pour l'hôte de communication Hdbsql sous Linux, le `hana.property` le fichier est situé à `/opt/NetApp/snapcenter/scc/etc`.

Utiliser la commande PowerShell

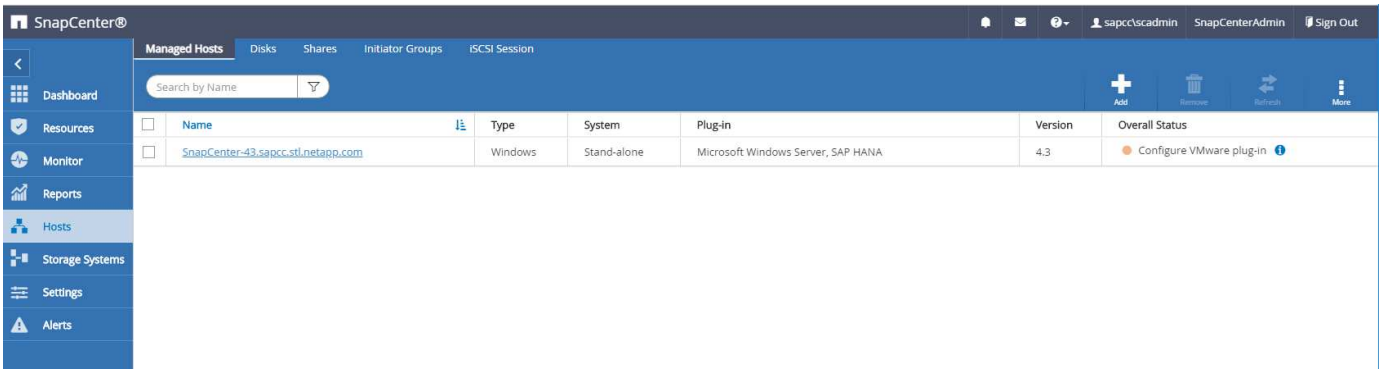
Une seconde option pour configurer ces paramètres consiste à utiliser une commande SnapCenter PowerShell.

1. Sur le serveur SnapCenter, ouvrez un PowerShell. Connectez-vous au serveur SnapCenter à l'aide de la commande `Open- SmConnection` et spécifiez le nom d'utilisateur et le mot de passe dans la fenêtre d'ouverture de session.
2. Avec la commande `Set- SmConfigSettings -Plugin - HostName <pluginhostname> - PluginCode hana - configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}`, Les modifications sont configurées pour l'hôte du plug-in SAP HANA `<pluginhostname>` Spécifié par l'adresse IP ou le nom d'hôte (voir la figure suivante).



Désactivez cet avertissement lors de l'exécution du plug-in SAP HANA dans un environnement virtuel

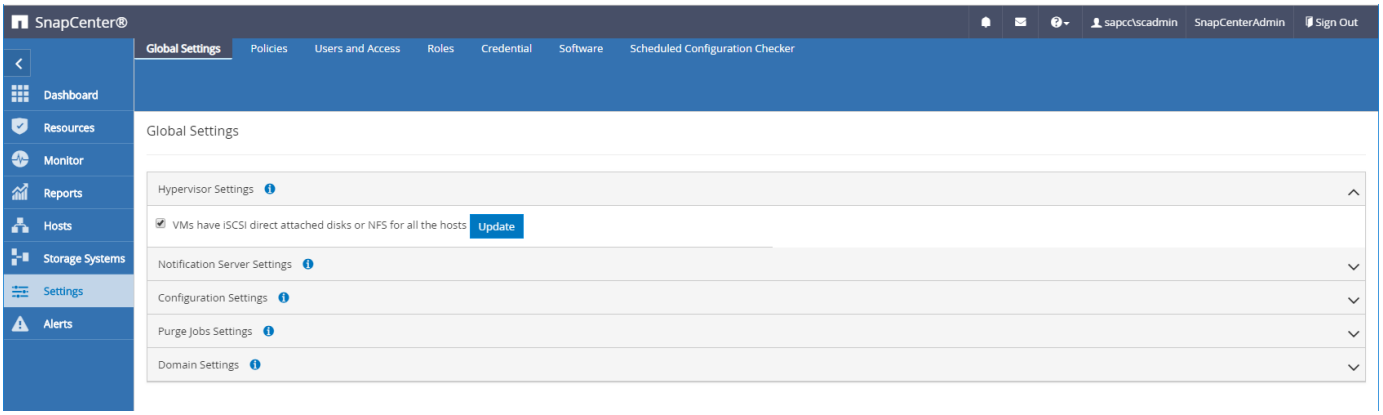
SnapCenter détecte si le plug-in SAP HANA est installé dans un environnement virtualisé. Il peut s'agir d'un environnement VMware ou d'une installation de SnapCenter chez un fournisseur de cloud public. Dans ce cas, SnapCenter affiche un avertissement pour configurer l'hyperviseur, comme illustré dans la figure suivante.



Il est possible de supprimer cet avertissement globalement. Dans ce cas, SnapCenter ne connaît pas les environnements virtualisés et ne montre donc pas ces avertissements.

Pour configurer SnapCenter pour supprimer cet avertissement, la configuration suivante doit être appliquée :

1. Dans l'onglet Paramètres, sélectionnez Paramètres globaux.
2. Pour les paramètres de l'hyperviseur, sélectionnez les machines virtuelles disposent de disques iSCSI à connexion directe ou de NFS pour tous les hôtes et mettez à jour les paramètres.



Modifier la fréquence de la synchronisation des sauvegardes avec le stockage de sauvegarde hors site

Comme décrit dans la section "« Gestion de la conservation des sauvegardes au niveau du stockage secondaire »," La gestion de la conservation des sauvegardes de données sur un stockage de sauvegardes hors site est assurée par ONTAP. SnapCenter vérifie régulièrement si ONTAP a supprimé des sauvegardes du stockage de sauvegarde hors site en exécutant une tâche de nettoyage avec une planification hebdomadaire par défaut.

La tâche de nettoyage SnapCenter supprime les sauvegardes du référentiel SnapCenter ainsi que dans le catalogue des sauvegardes SAP HANA si des sauvegardes supprimées du stockage de sauvegarde hors site ont été identifiées.

La tâche de nettoyage exécute également le nettoyage des sauvegardes des journaux SAP HANA.

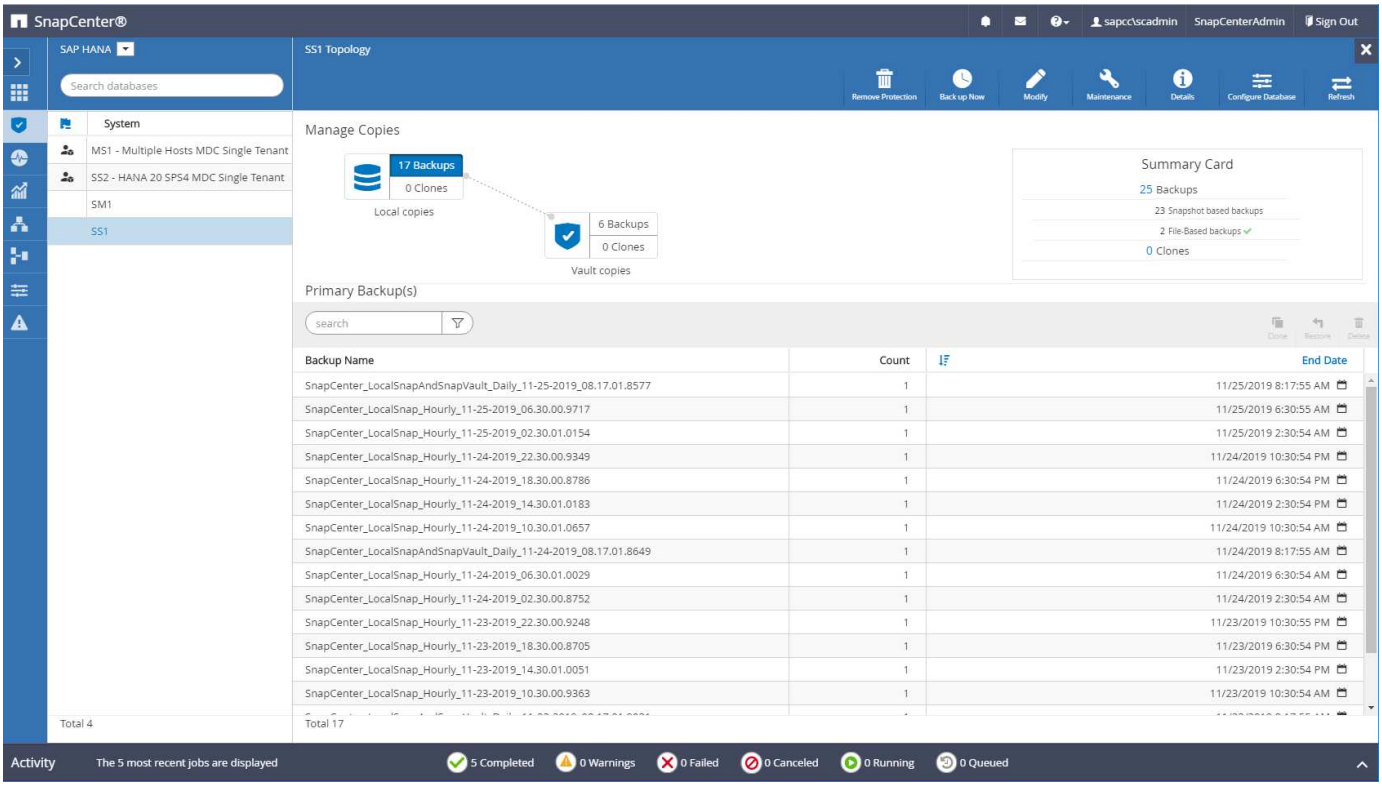
Jusqu'à ce que ce nettoyage planifié soit terminé, SAP HANA et SnapCenter peuvent toujours afficher les sauvegardes qui ont déjà été supprimées du stockage de sauvegarde hors site.

Il est ainsi possible que des sauvegardes de journaux supplémentaires soient conservées, même si les sauvegardes Snapshot correspondantes basées sur le stockage de sauvegarde hors site ont déjà été supprimées.

Les sections suivantes décrivent deux façons d'éviter cette divergence temporaire.

Actualisation manuelle au niveau des ressources

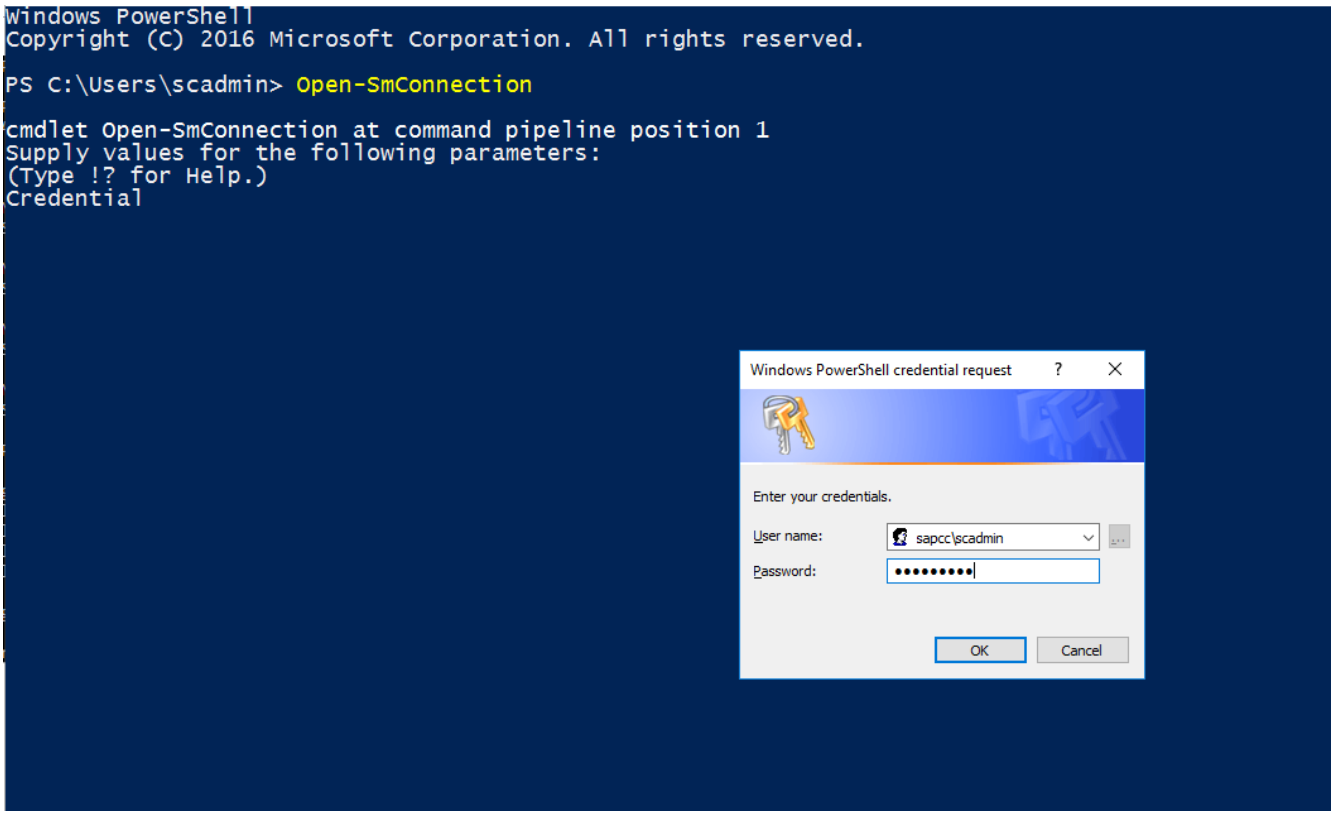
Dans la vue topologique d'une ressource, SnapCenter affiche les sauvegardes du stockage de sauvegarde hors site lors de la sélection des sauvegardes secondaires, comme l'illustre la capture d'écran suivante. SnapCenter exécute une opération de nettoyage avec l'icône Actualiser pour synchroniser les sauvegardes de cette ressource.



Modifiez la fréquence de la tâche de nettoyage SnapCenter

SnapCenter exécute la tâche de nettoyage `SnapCenter_RemoveSecondaryBackup` Par défaut pour toutes les ressources sur une base hebdomadaire à l'aide du mécanisme de planification des tâches Windows. Vous pouvez modifier cette configuration à l'aide d'une cmdlet SnapCenter PowerShell.

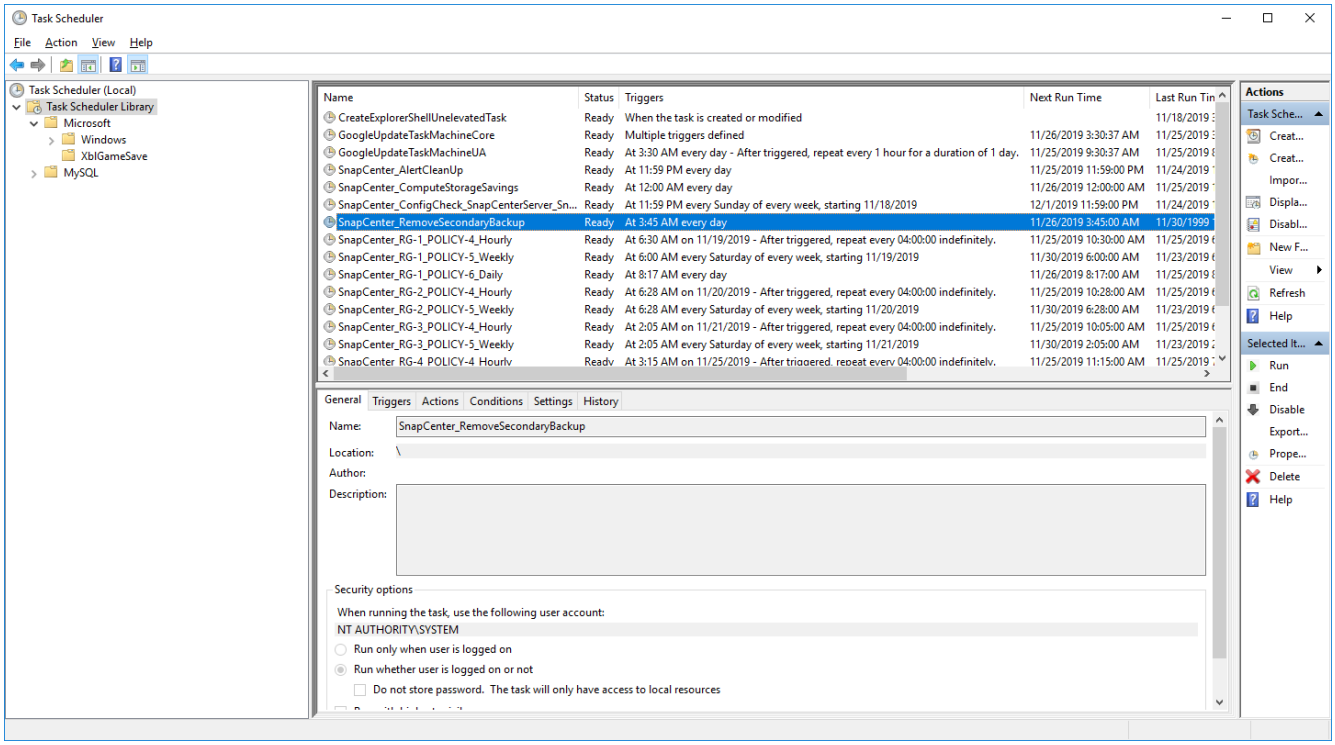
1. Démarrez une fenêtre de commande PowerShell sur le serveur SnapCenter.
2. Ouvrez la connexion au serveur SnapCenter et entrez les informations d'identification de l'administrateur SnapCenter dans la fenêtre de connexion.



3. Pour passer d'une planification hebdomadaire à une base quotidienne, utilisez l'applet de commande `Set-SmSchedule`.

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

4. Vous pouvez vérifier les propriétés du travail dans le Planificateur de tâches Windows.



Où trouver des informations supplémentaires et l'historique des versions

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Page Ressources SnapCenter

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

- Documentation du logiciel SnapCenter

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

- Tr-4667 : automatisation des copies du système SAP à l'aide de SnapCenter

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

- Tr-4719 : réplication, sauvegarde et restauration système SAP HANA avec SnapCenter

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

- Tr-4018 : intégration des systèmes NetApp ONTAP à la gestion du paysage SAP

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

- Tr-4646 : reprise après incident de SAP HANA avec réplication du stockage

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

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Juillet 2017	• Version initiale.
Version 1.1	Septembre 2017	• Ajout de la section "Configuration avancée et réglage". • Corrections mineures.
Version 2.0	Mars 2018	• Mises à jour relatives à SnapCenter 4.0 : Nouvelle ressource de volume de données Amélioration du fonctionnement de Single File SnapRestore
Version 3.0	Janvier 2020	• Ajout de la section « concepts et meilleures pratiques SnapCenter ». • Mises à jour relatives à SnapCenter 4.3 : Détection automatique Restauration et reprise automatisées Prise en charge de plusieurs locataires MDC HANA Opération de restauration mutualisée unique
Version 3.1	Juillet 2020	• Mises à jour et corrections mineures : Prise en charge de NFSv4 avec SnapCenter 4.3.1 Configuration de la communication SSL Déploiement centralisé de plug-in pour Linux sur IBM Power
Version 3.2	Novembre 2020	• Ajout des privilèges d’utilisateur de base de données requis pour HANA 2.0 SPS5.
Version 3.3	Mai 2021	• Mise à jour de la section de configuration hdbsql SSL. • Ajout de la prise en charge LVM de Linux.

Version	Date	Historique des versions du document
Version 3.4	Août 2021	• Ajout de la description de la configuration de désactivation de la détection automatique.
Version 3.5	Février 2022	• Mises à jour mineures pour couvrir SnapCenter 4.6 et la prise en charge de la détection automatique pour les systèmes HANA compatibles avec la réplication du système.

Sauvegarde et restauration BlueXP pour SAP HANA : stockage objet dans le cloud comme destination de sauvegarde

Sauvegarde et restauration BlueXP pour SAP HANA : stockage objet dans le cloud comme destination de sauvegarde

Présentation

Ce document décrit l'installation et la configuration de SAP HANA pour la protection des données depuis les magasins d'objets sur site vers les magasins d'objets dans le cloud avec NetApp BlueXP. Il couvre la partie sauvegarde et restauration BlueXP de la solution. Cette solution est une amélioration de la solution de sauvegarde SAP HANA sur site utilisant NetApp Snap Center. Elle offre une méthode économique pour l'archivage à long terme des sauvegardes SAP HANA dans un stockage objet basé sur le cloud. Elle offre également un Tiering facultatif du stockage objet vers un stockage d'archivage tel qu'AWS Glacier/Deep Glacier, Microsoft Azure Blob Archive et le stockage d'archives GCP.

La configuration de la solution de sauvegarde et de restauration SAP HANA sur site est décrite dans le "Tr-4614 : sauvegarde et restauration SAP HANA avec SnapCenter (netapp.com)".

Ce rapport technique décrit uniquement comment améliorer la solution de sauvegarde et de restauration SnapCenter sur site avec la sauvegarde et la restauration BlueXP pour SAP HANA à l'aide du stockage objet AWS S3. L'installation et la configuration utilisant le stockage objet Microsoft Azure et GCP à la place d'AWS S3 sont similaires, mais ne sont pas décrites dans ce document.

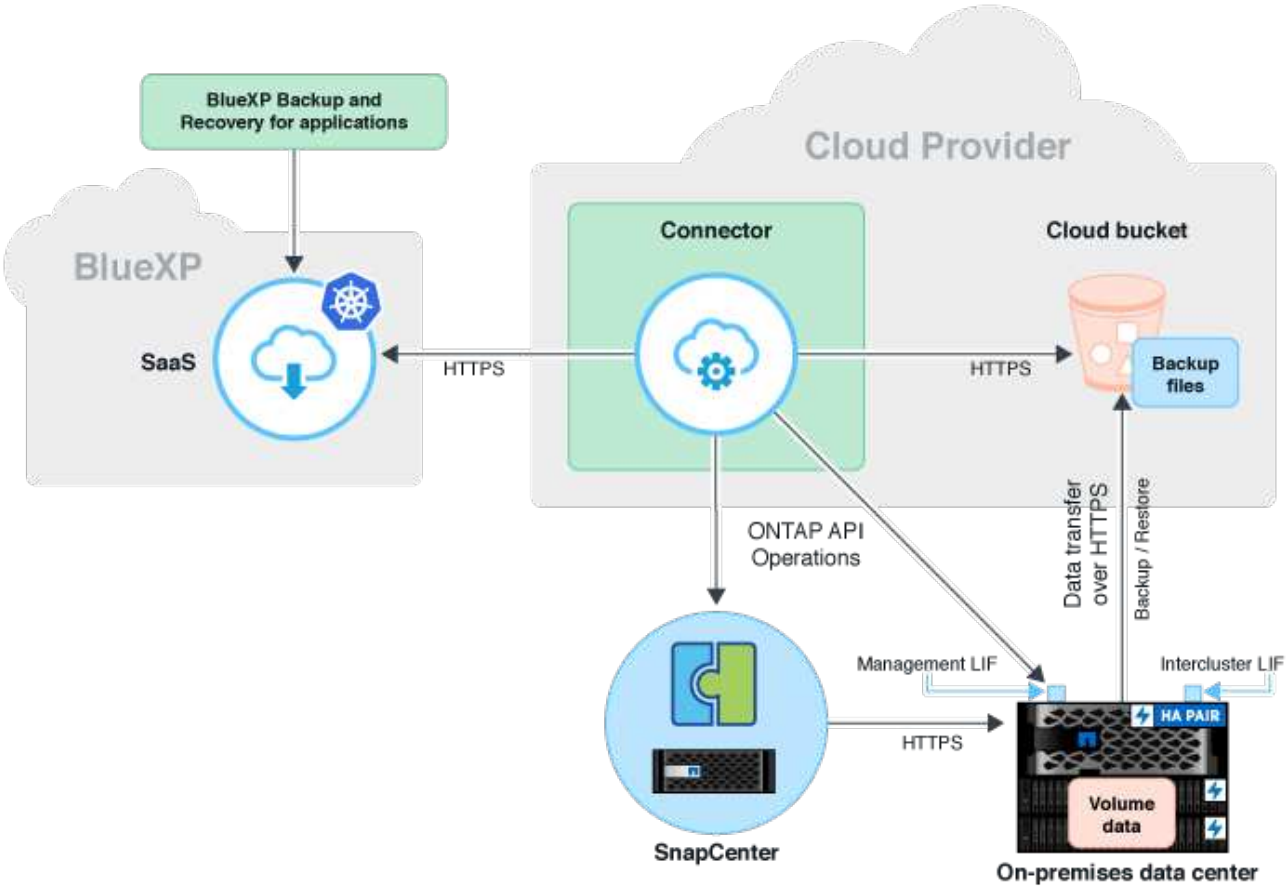
Architecture de sauvegarde et de restauration BlueXP

BlueXP Backup and Recovery est une solution SaaS qui offre des fonctionnalités de protection des données pour les applications qui s'exécutent sur le stockage NetApp sur site vers le cloud. Il offre une protection SAP HANA basée sur des règles, efficace et cohérente avec les applications grâce au stockage NetApp. En outre, la sauvegarde et la restauration BlueXP assurent un contrôle et une surveillance centralisés, tout en déléguant aux utilisateurs la gestion des opérations de sauvegarde et de restauration spécifiques aux applications.

La sauvegarde et la restauration BlueXP s'exécutent SaaS dans NetApp BlueXP et tirent parti du framework et de l'interface utilisateur. La structure de l'environnement de travail BlueXP est utilisée pour configurer et gérer les identifiants du stockage NetApp ONTAP basé sur site et du serveur NetApp SnapCenter.

Un connecteur BlueXP doit être déployé au sein du réseau virtuel du client. Une connexion entre l'environnement sur site et l'environnement cloud est requise, par exemple une connexion VPN de site à site. La communication entre les composants SaaS NetApp et l'environnement client s'effectue exclusivement via le connecteur. Le connecteur exécute les opérations de stockage à l'aide des API de gestion ONTAP et SnapCenter.

Le transfert des données entre le stockage sur site et le compartiment cloud est protégé de bout en bout avec le chiffrement AES 256 bits au repos, le chiffrement TLS/HTTPS à la volée et la prise en charge des clés gérées par le client (CMK).
Les données sauvegardées peuvent être stockées dans un état WORM immuable et indélébile. La seule façon d'accéder aux données à partir du stockage objet est de les restaurer dans un stockage basé sur NetApp ONTAP, y compris NetApp CVO.



Présentation des étapes d'installation et de configuration

Les étapes d'installation et de configuration requises peuvent être divisées en trois zones.
Le prérequis est que la configuration de sauvegarde SAP HANA ait été configurée dans NetApp Snap Center. Pour configurer Snap Center pour SAP HANA en premier lieu, reportez-vous à la section "Configuration SnapCenter (netapp.com)".

1. Installation et configuration des composants NetApp BlueXP.

   Doit être effectué une fois lors de la configuration initiale de la solution de protection des données.

2. Étapes de préparation à NetApp SnapCenter.

   Doit être fait pour chaque base de données SAP HANA, qui doit être protégée.

3. Étapes de configuration de la sauvegarde et de la restauration BlueXP.

   Doit être fait pour chaque base de données SAP HANA, qui doit être protégée.

Installation et configuration de la sauvegarde d'application hybride NetApp BlueXP

L'installation et la configuration des composants NetApp BlueXP sont décrites dans le "Protection des données applicatives sur site | Documentation NetApp".

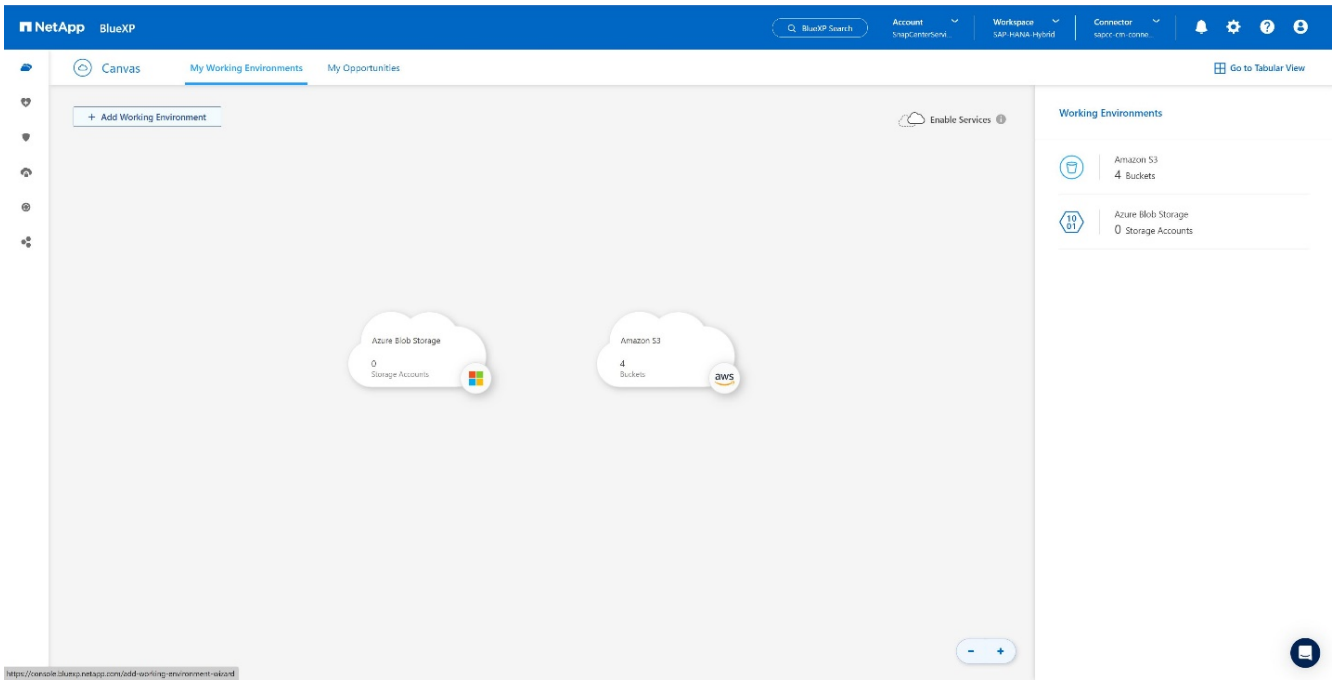
1. Inscrivez-vous à BlueXP et configurez un compte NetApp à l'adresse https://bluexp.netapp.com/.
2. Déployez le connecteur BlueXP dans votre environnement. La description est disponible à l'adresse "En savoir plus sur les connecteurs | Documentation NetApp".
3. Ajoutez/achetez une licence Cloud Backup sur BlueXP : https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-licensing-cloud-backup.html.
4. Créez un environnement de travail pour l'environnement sur site NetApp et votre destination cloud dans BlueXP en ajoutant votre stockage sur site.
5. Créez une nouvelle relation de magasin d'objets pour le stockage sur site dans un compartiment AWS S3.
6. Configurez la ressource système SAP HANA sur SnapCenter.
7. Ajoutez Snap Center à votre environnement de travail.
8. Création d'une stratégie pour votre environnement
9. Protégez votre système SAP HANA.

Configuration de la sauvegarde et de la restauration BlueXP pour SAP HANA

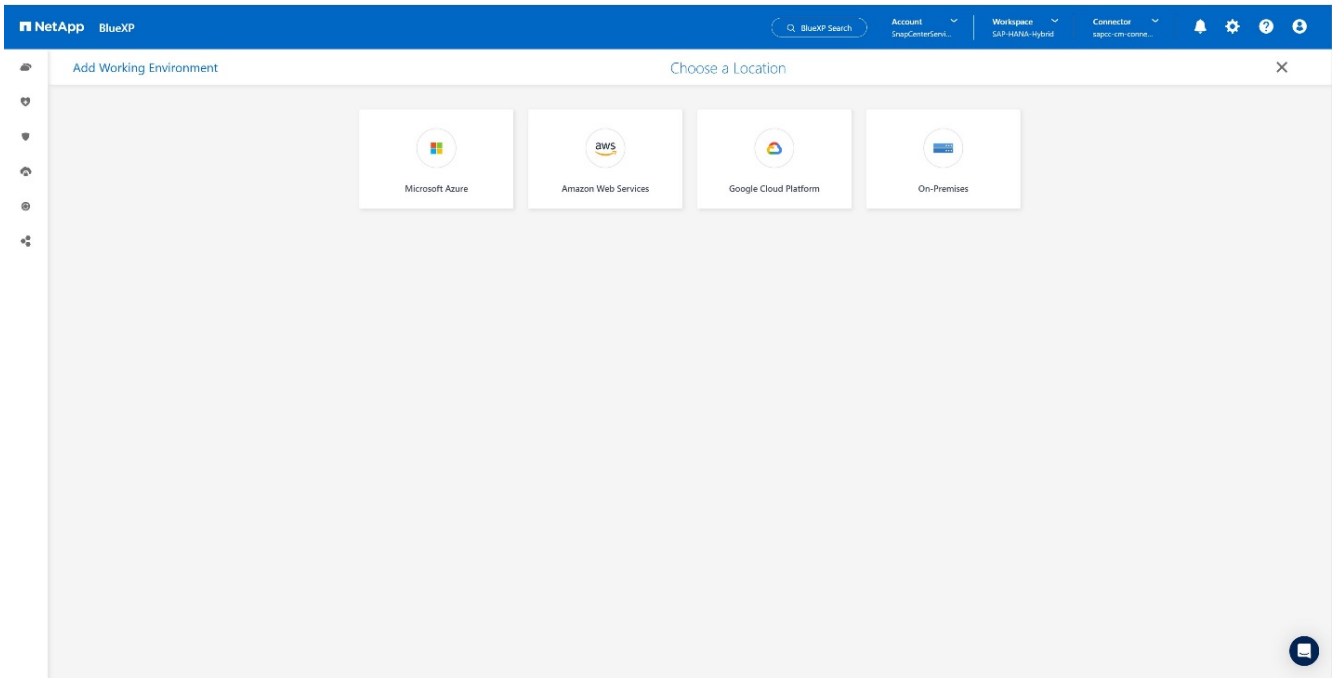
Création d'un environnement de travail pour BlueXP

Ajoutez le système de stockage sur site à votre environnement de travail.

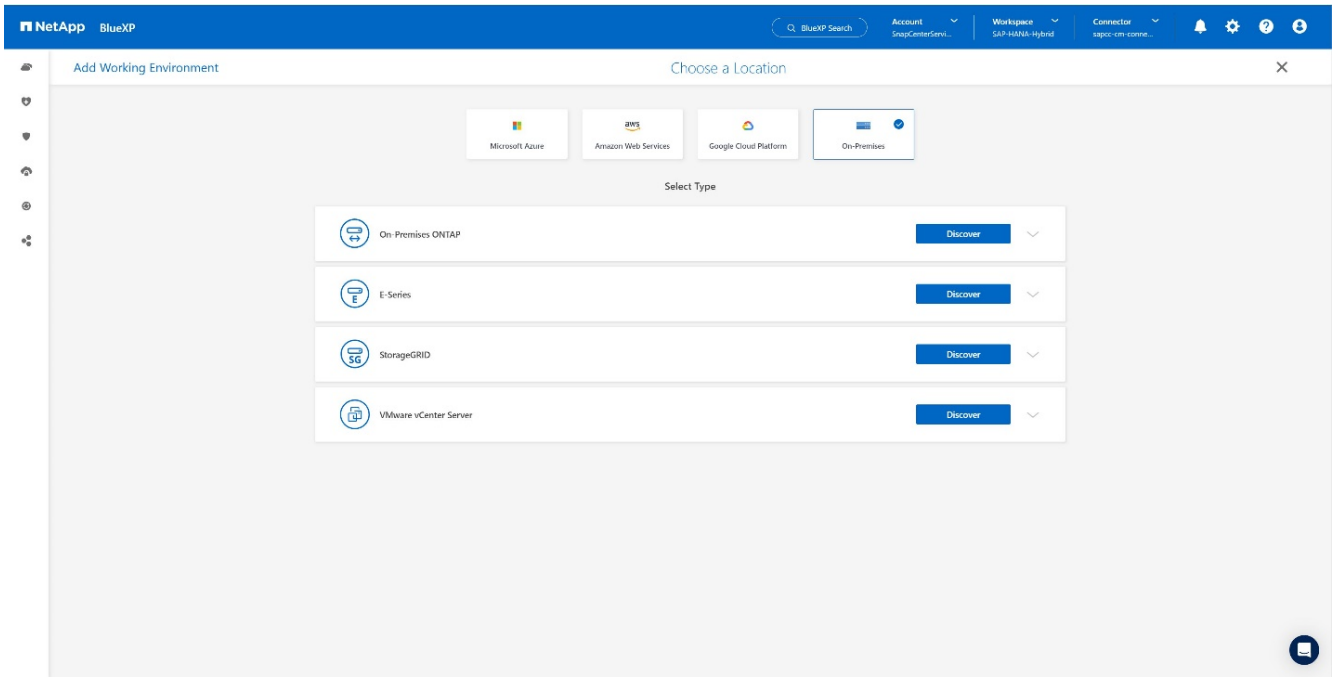
1. Dans le menu de gauche, choisissez **Storage** → **Canvas** → **My Working** Environment.
2. Appuyez sur **+ Ajouter un environnement de travail**.



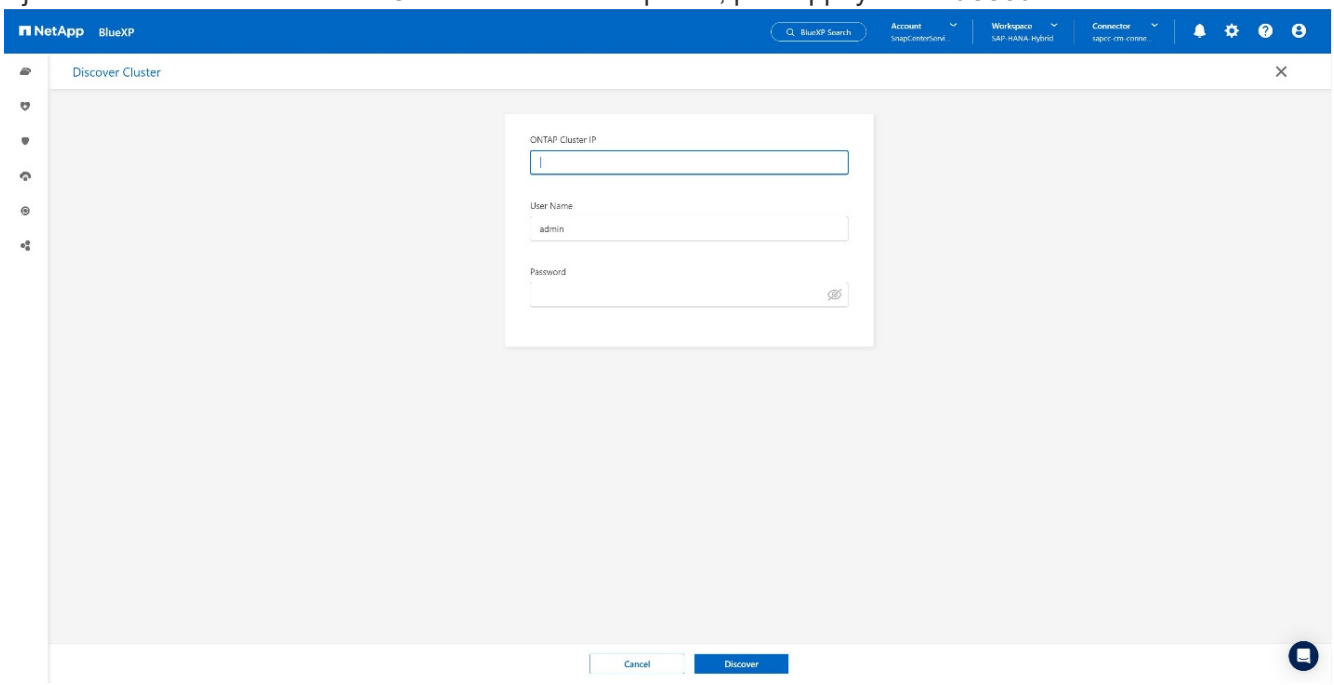
3. Choisissez **sur place**.



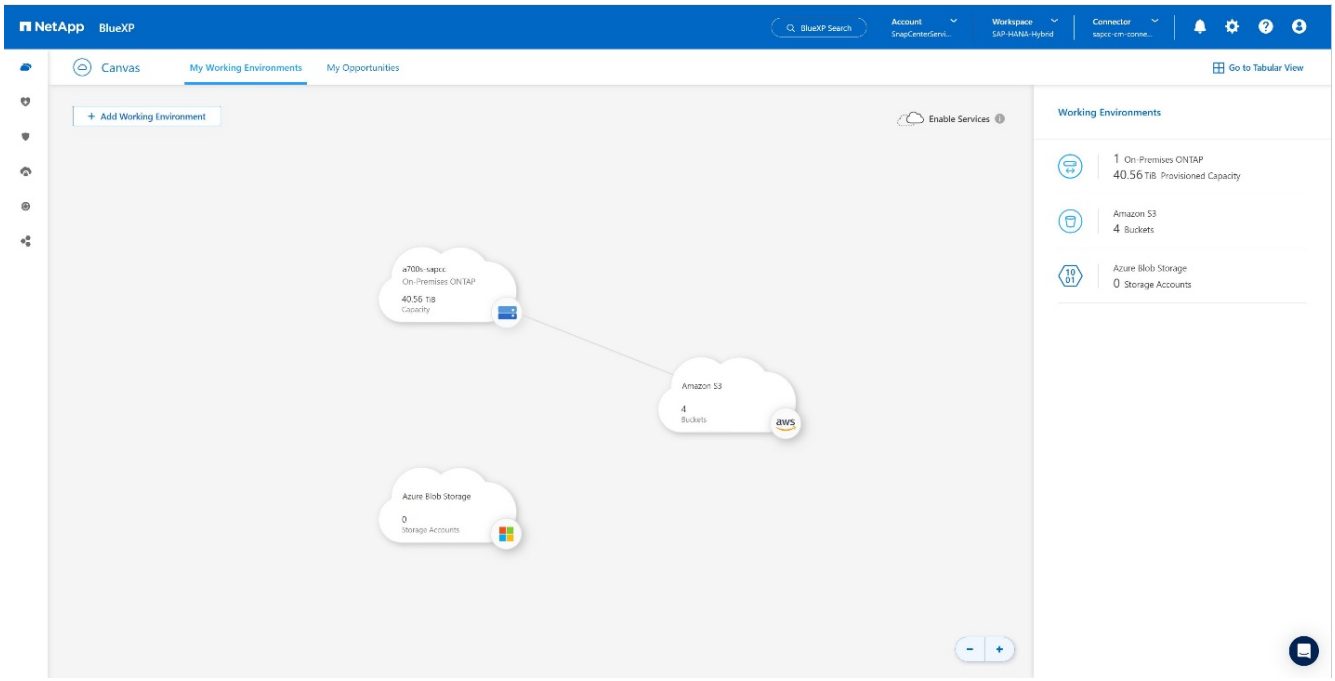
4. Choisissez **découvrir ONTAP** sur place.



5. Ajoutez l'adresse IP du cluster ONTAP et le mot de passe, puis appuyez sur **découvrir**.



6. Le cluster ONTAP est désormais disponible.

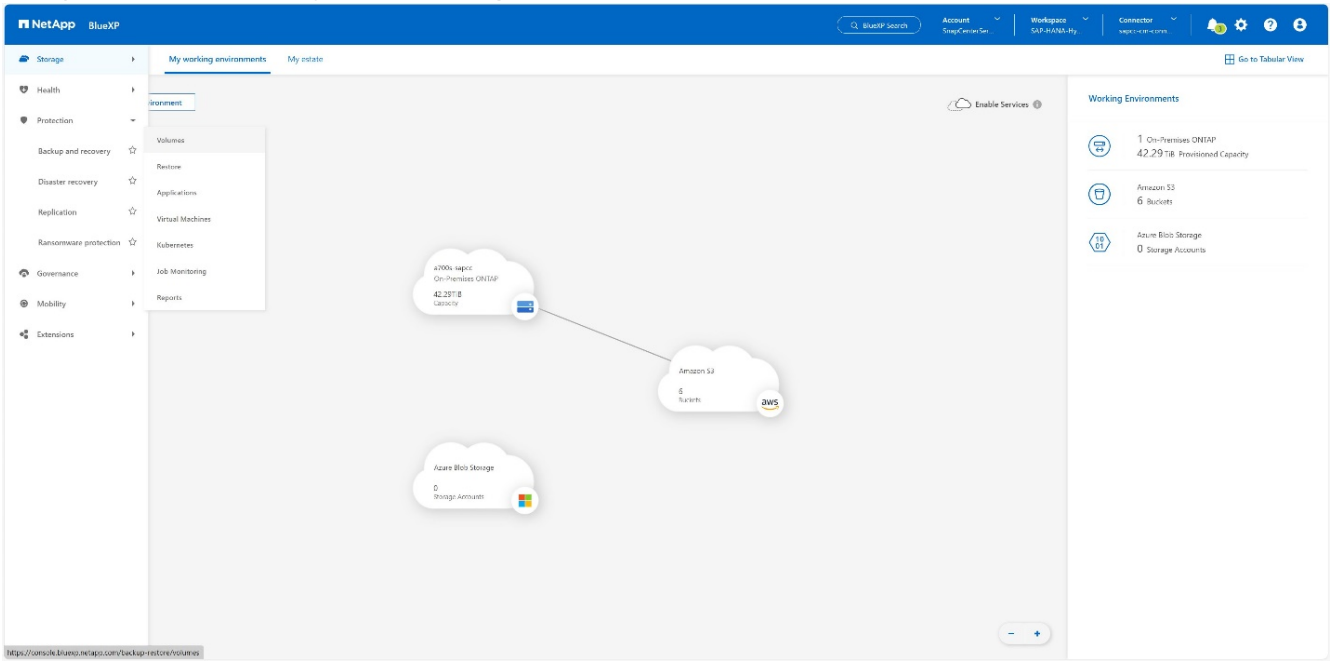


Création d'une relation entre le système de stockage sur site et un compartiment de stockage objet

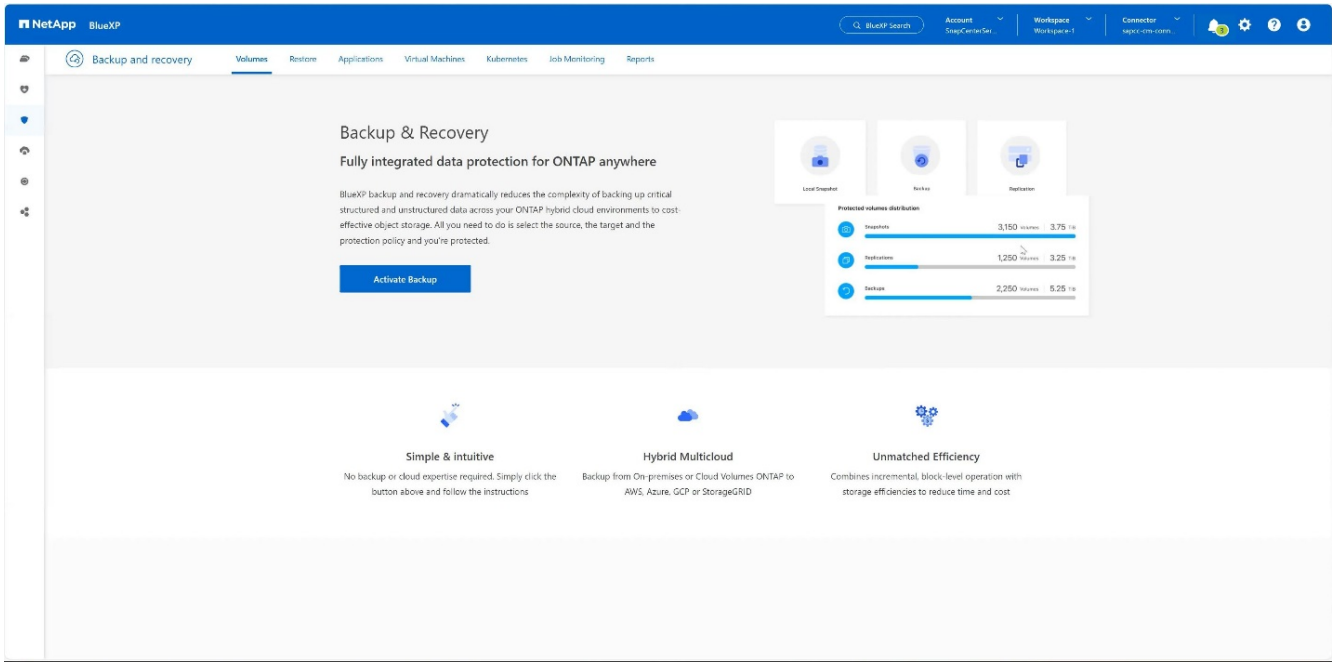
La relation entre le stockage sur site et le compartiment S3 s'effectue par la création d'une sauvegarde de volume ou par l'activation de la sauvegarde d'une application. Si un VPN de site à site doit être utilisé pour transférer les données d'un environnement sur site vers S3, une sauvegarde de volume doit être utilisée pour créer la relation entre le stockage sur site et le compartiment S3 lorsque les terminaux VPC doivent être utilisés.
Au moment de la création de ce document, le workflow de sauvegarde de l'application ne propose pas de terminaux VPC pour l'accès aux compartiments S3.
Reportez-vous à la section "Terminaux de passerelle pour Amazon S3 : cloud privé virtuel Amazon" Comment configurer les terminaux VPC pour S3 dans votre VPC.

Pour créer une première sauvegarde de volume, effectuez les opérations suivantes :

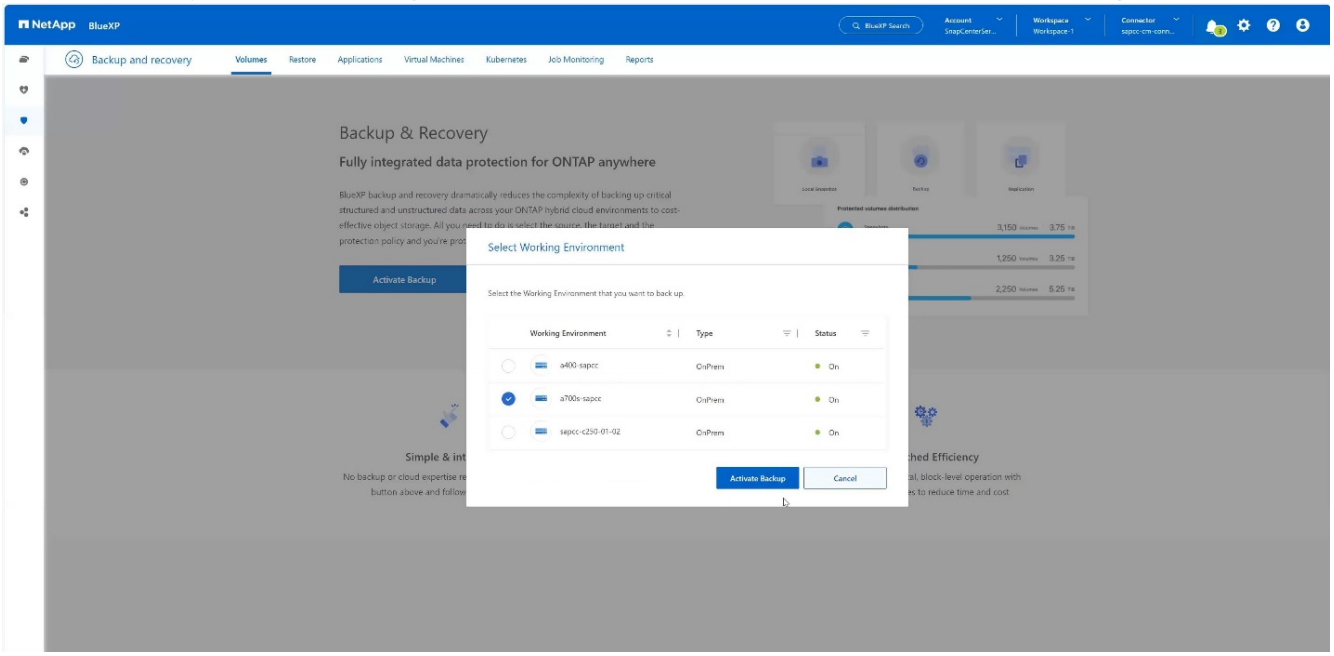
1. Naviguez via **protection** jusqu'à **sauvegarde et récupération** et choisissez **volumes**.



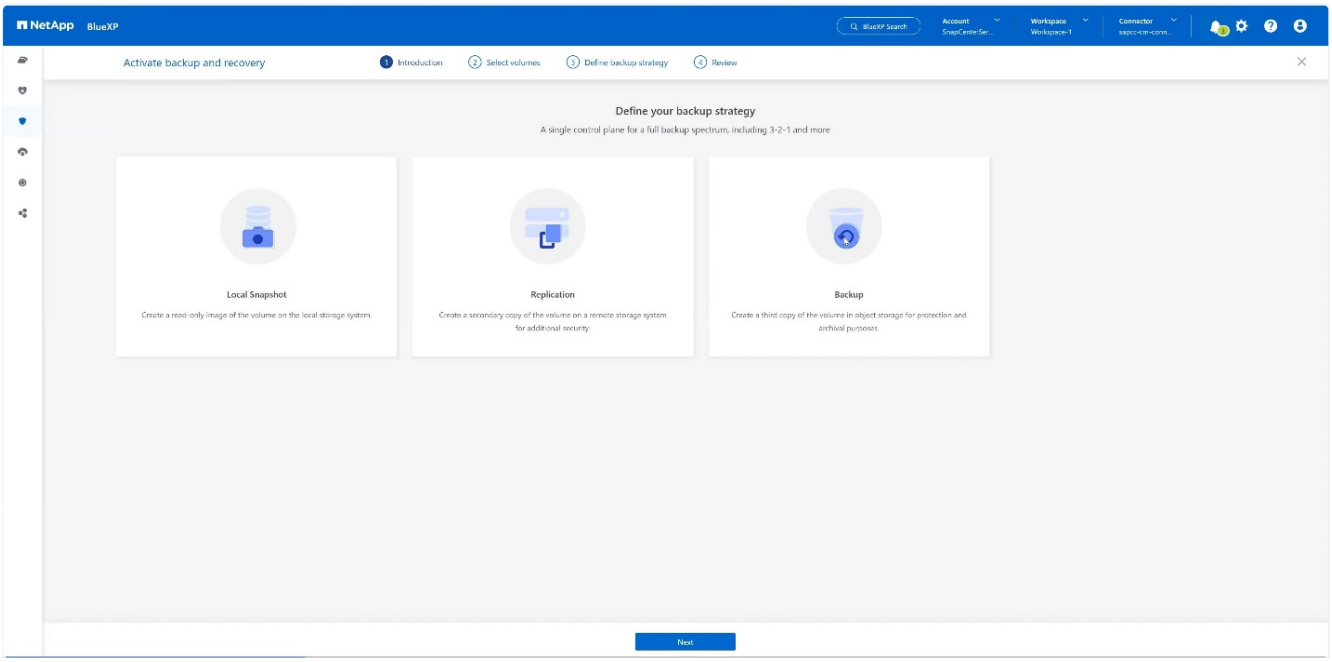
2. Appuyez sur le bouton **Activer la sauvegarde**.



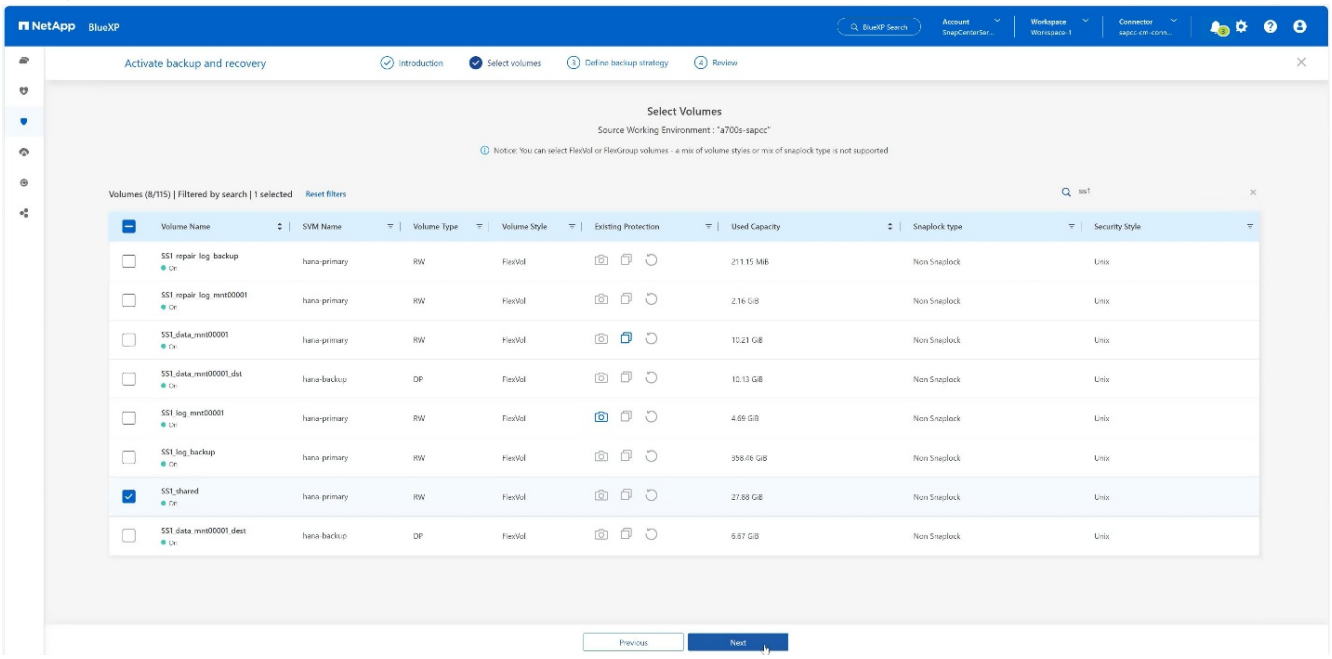
3. Choisissez le système de stockage sur site de votre choix et cliquez sur **Activer la sauvegarde**.



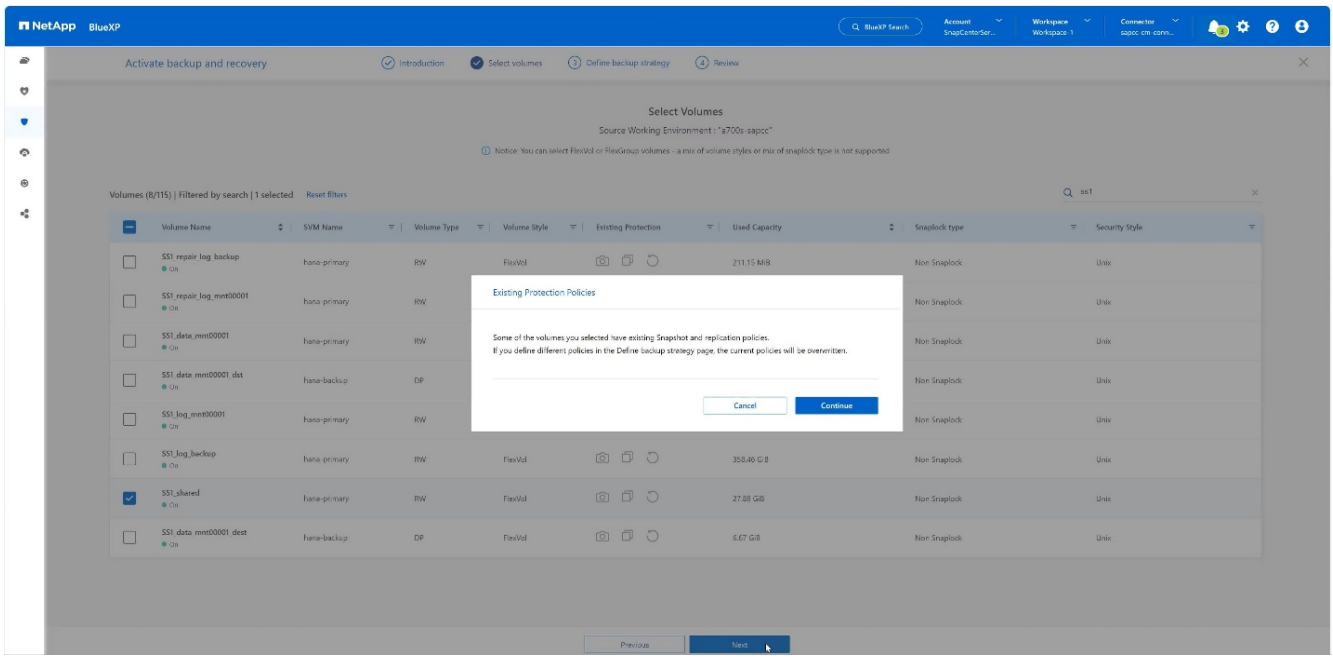
4. Choisissez **Backup**.



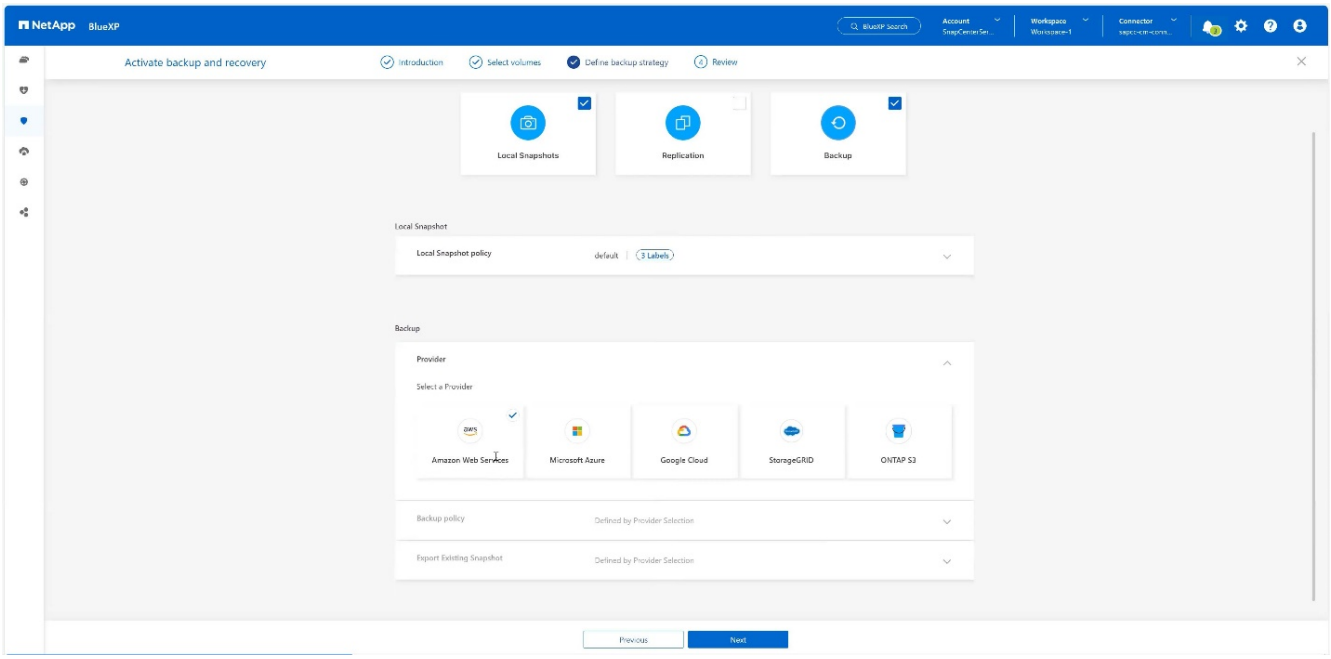
5. Choisissez un volume qui est stocké sur le même SVM que vos fichiers de données SAP HANA et appuyez sur **Suivant**. Dans cet exemple, le volume pour /hana/shared a été choisi.



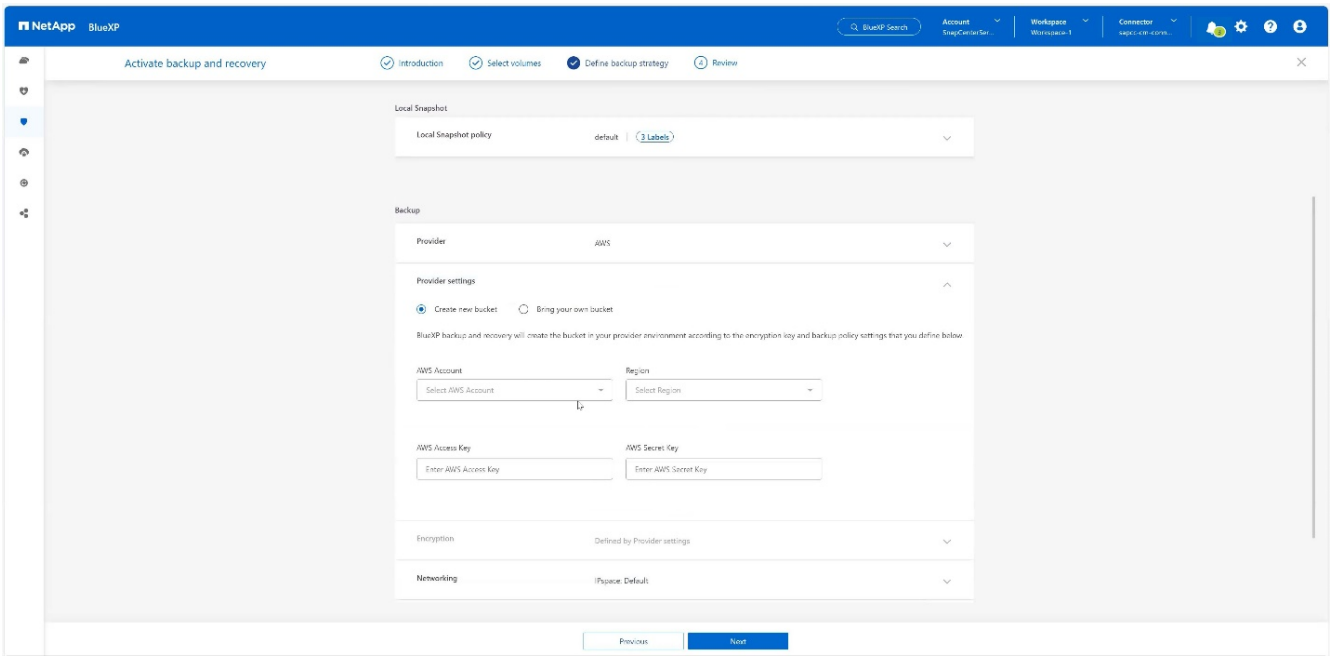
6. **Continuer**, s'il existe une politique existante.



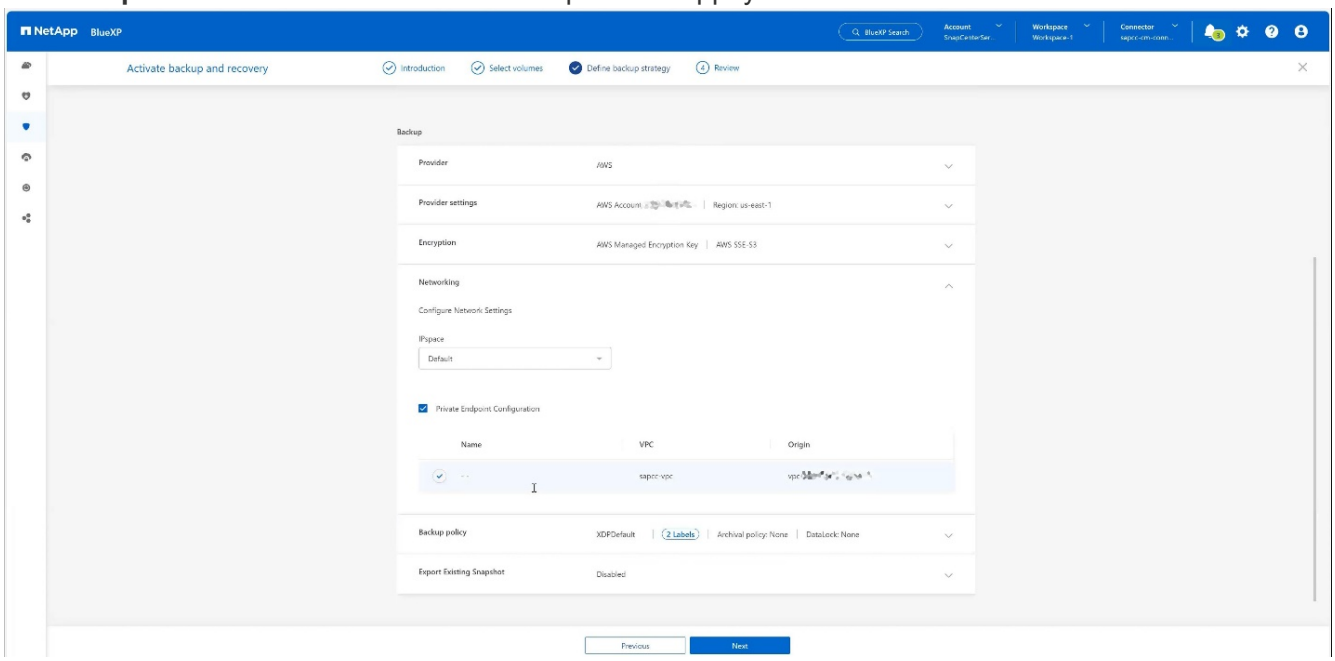
7. Cochez **option de sauvegarde** et choisissez le fournisseur de sauvegarde de votre choix. Dans cet exemple, AWS.
   Conservez l'option cochée pour les stratégies existantes.
   Décochez les options que vous ne souhaitez pas utiliser.



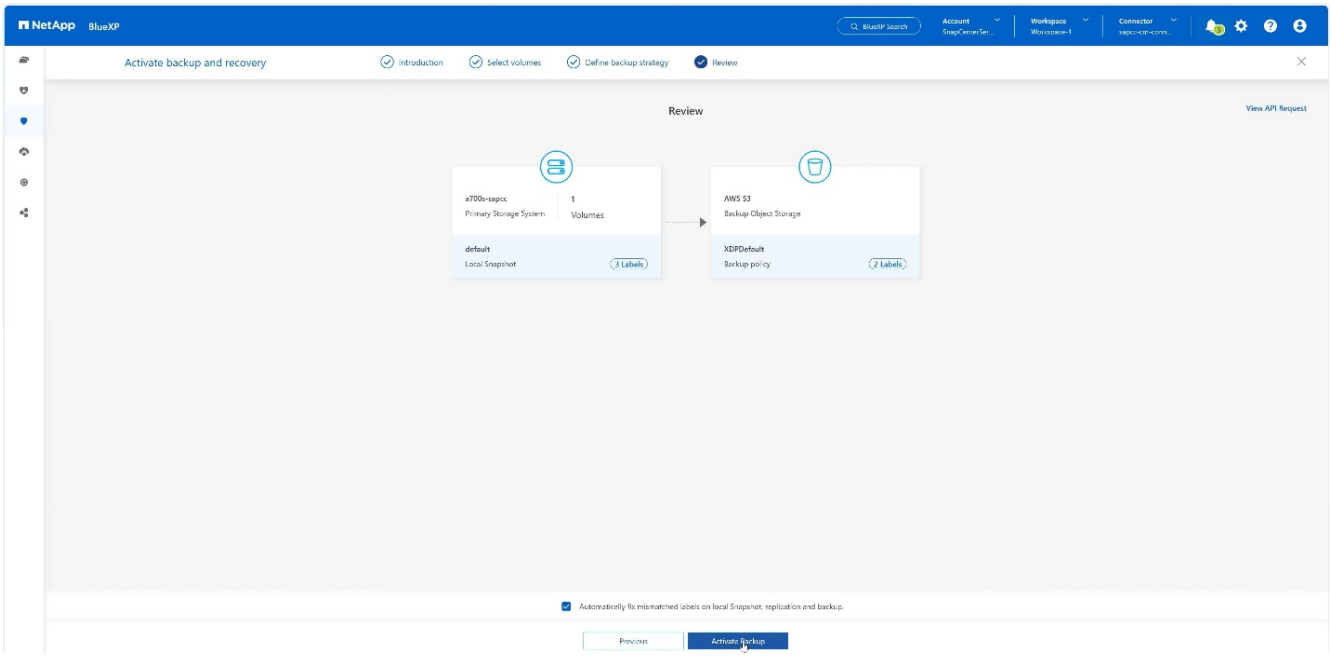
8. Créez un nouveau compartiment ou choisissez un compartiment existant. Indiquez les paramètres de votre compte AWS, la régio, votre clé d'accès et la clé secrète. Appuyez sur **Suivant**.



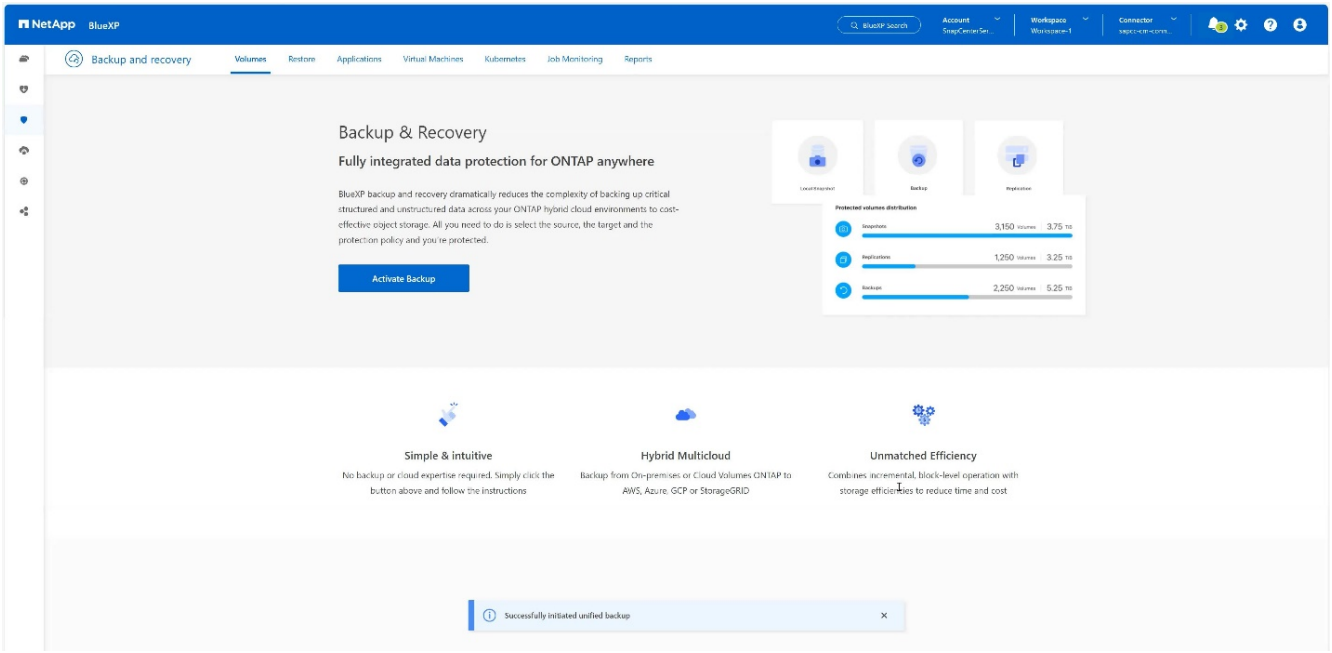
9. Choisissez l'IPspace approprié de votre système de stockage sur site, sélectionnez **Configuration du terminal privé** et choisissez le terminal VPC pour S3. Appuyez sur **Suivant**.



10. Vérifiez votre configuration et appuyez sur **Activer la sauvegarde**.

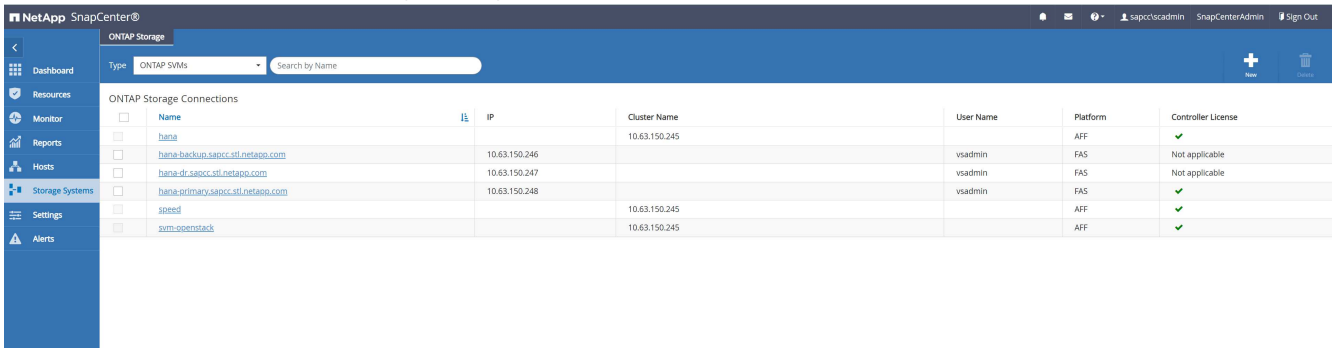


11. La sauvegarde a été lancée avec succès.

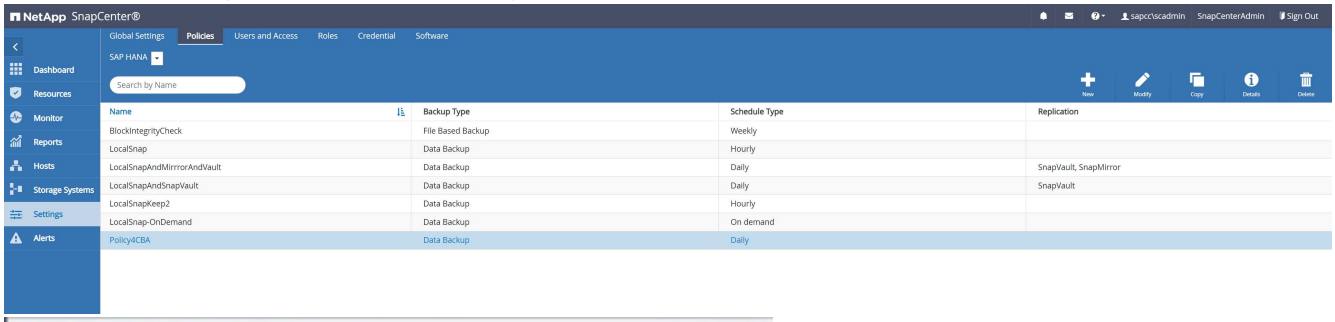


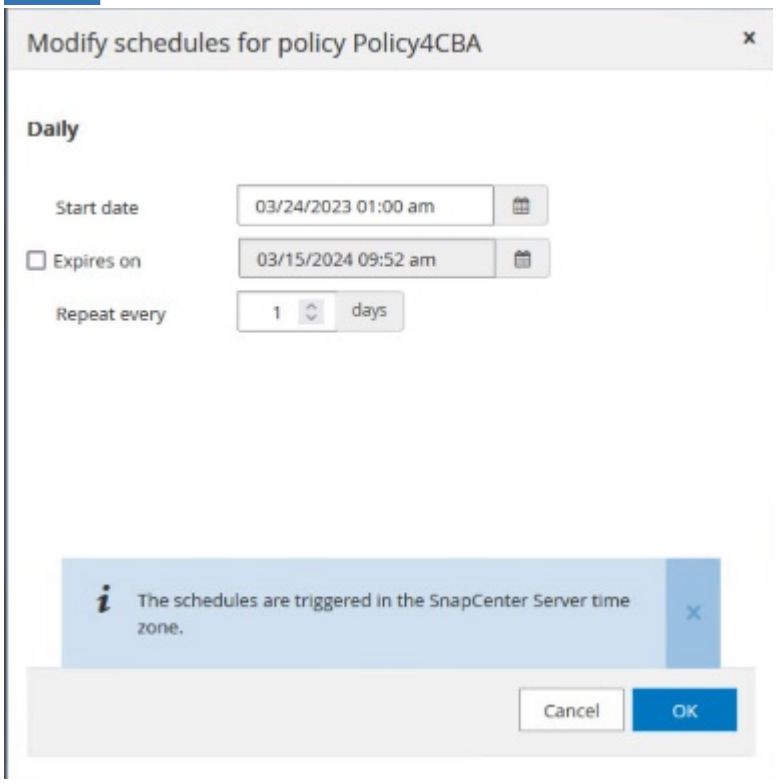
Configurez la ressource système SAP HANA sur SnapCenter

1. Vérifiez si le SVM (hana dans cet exemple) sur lequel votre système SAP HANA est stocké a été ajouté via le cluster. Si seul le SVM a été ajouté, ajouter le cluster.

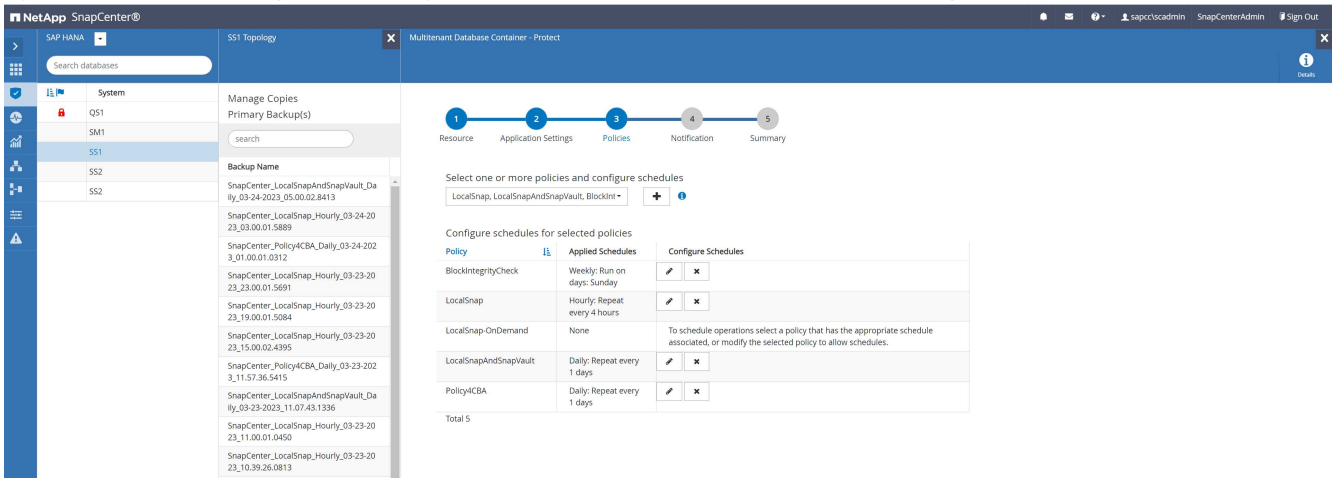


2. Définissez une règle d'horaires avec un type d'horaire quotidien, hebdomadaire ou mensuel.

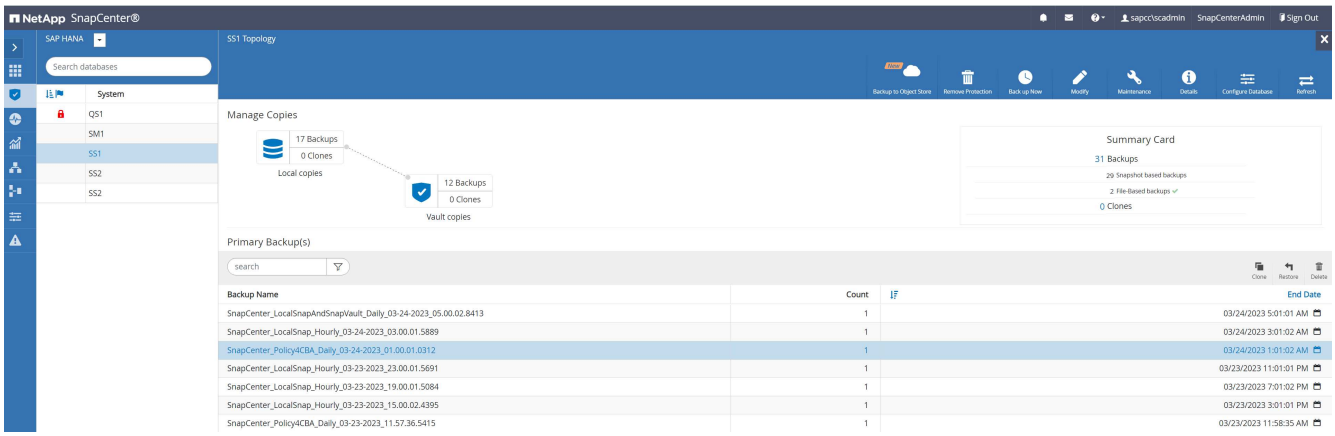




3. Ajoutez la nouvelle règle à votre système SAP HANA et attribuez un planning quotidien.

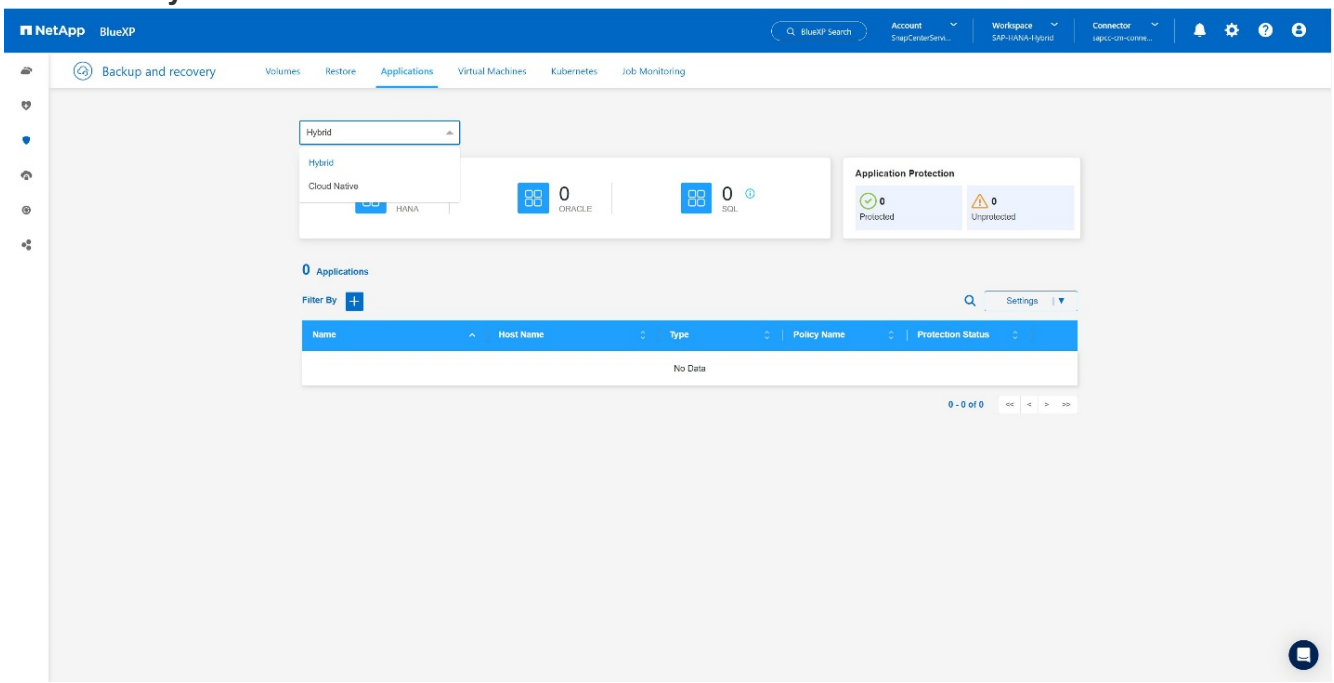


4. Une fois les nouvelles sauvegardes configurées avec cette stratégie seront disponibles une fois la règle exécutée conformément au calendrier défini.

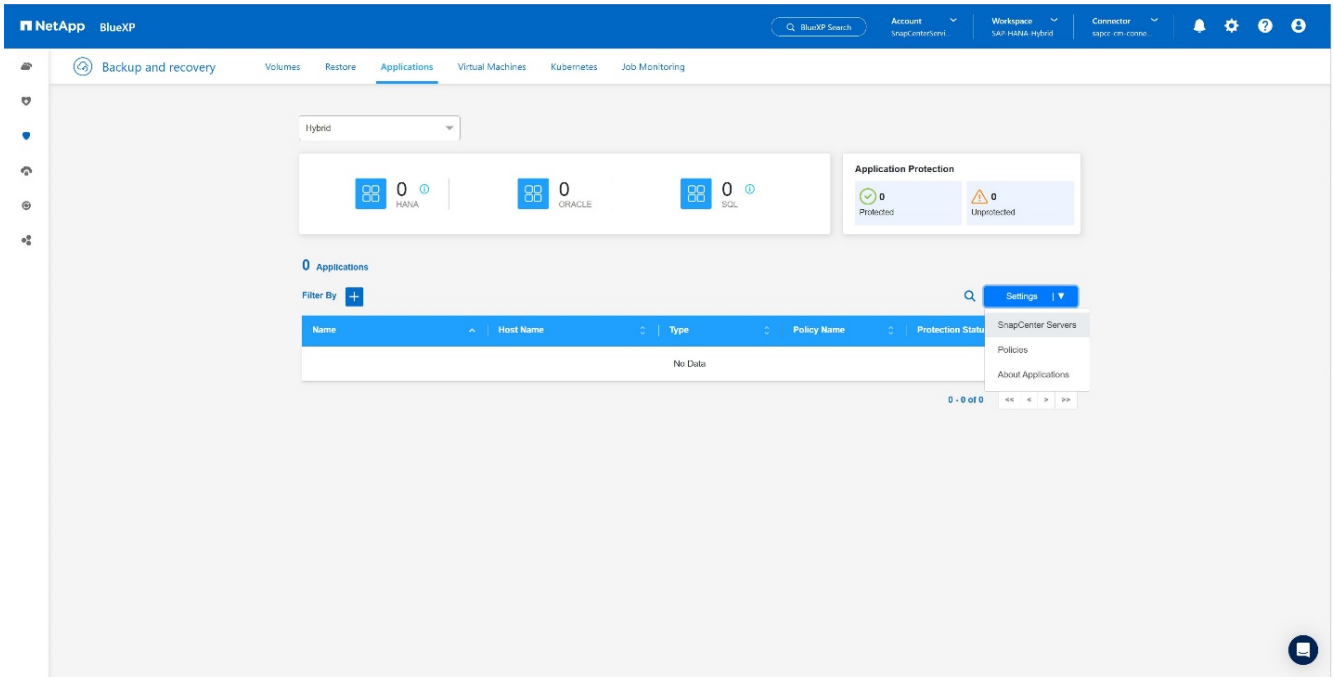


Ajout de SnapCenter à l'environnement de travail BlueXP

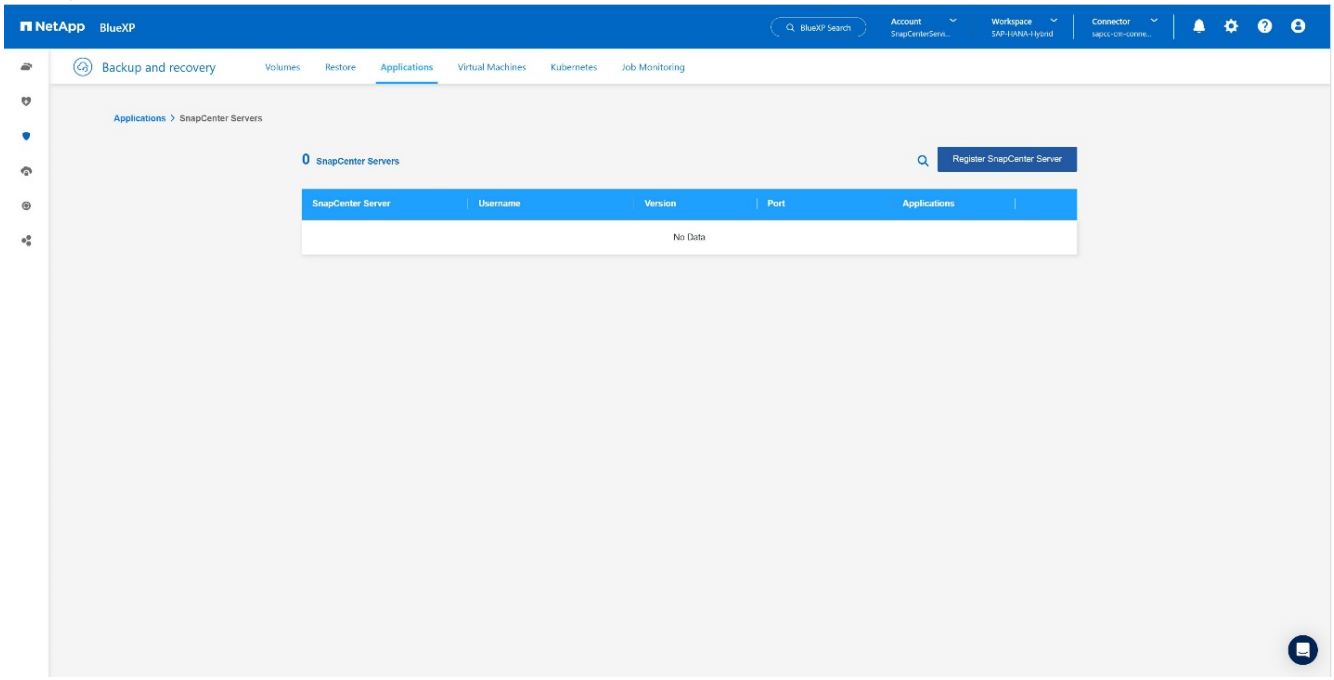
1. Dans le menu de gauche, choisissez **protection → sauvegarde et récupération → applications**.
2. Choisissez **Hybrid** dans le menu déroulant.



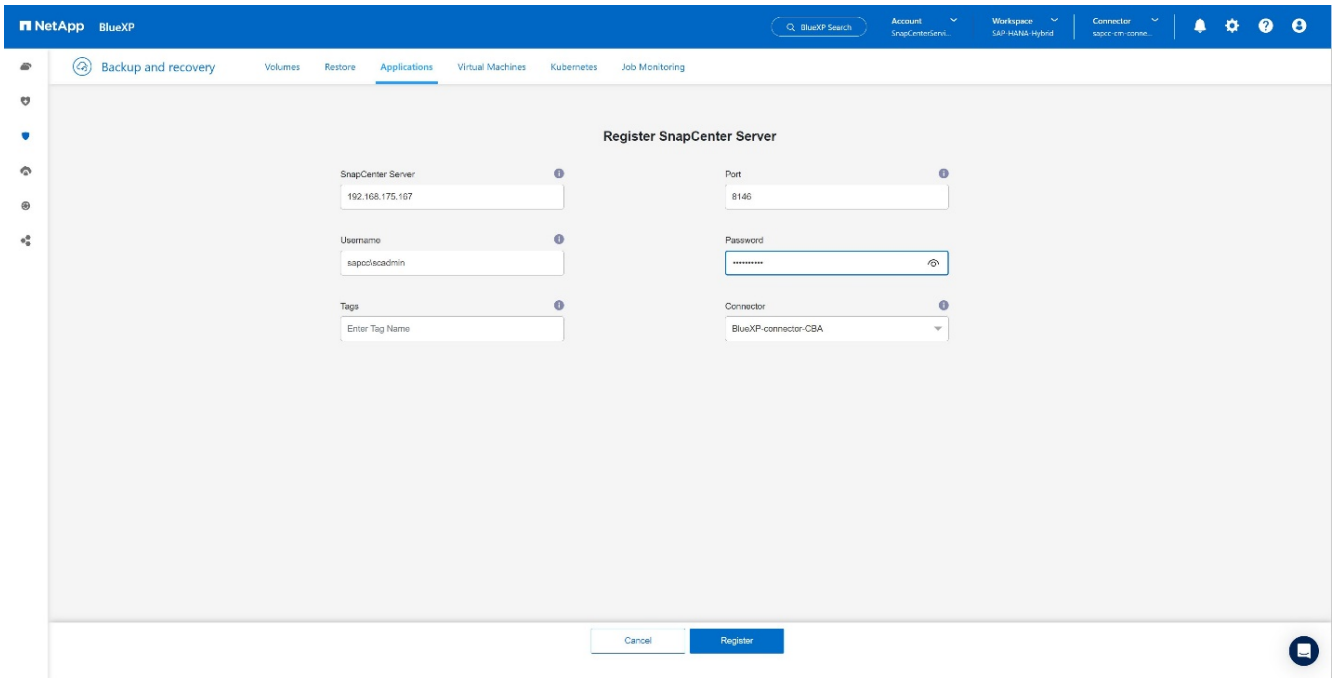
3. Choisissez **serveurs SnapCenter** dans le menu Paramètres.



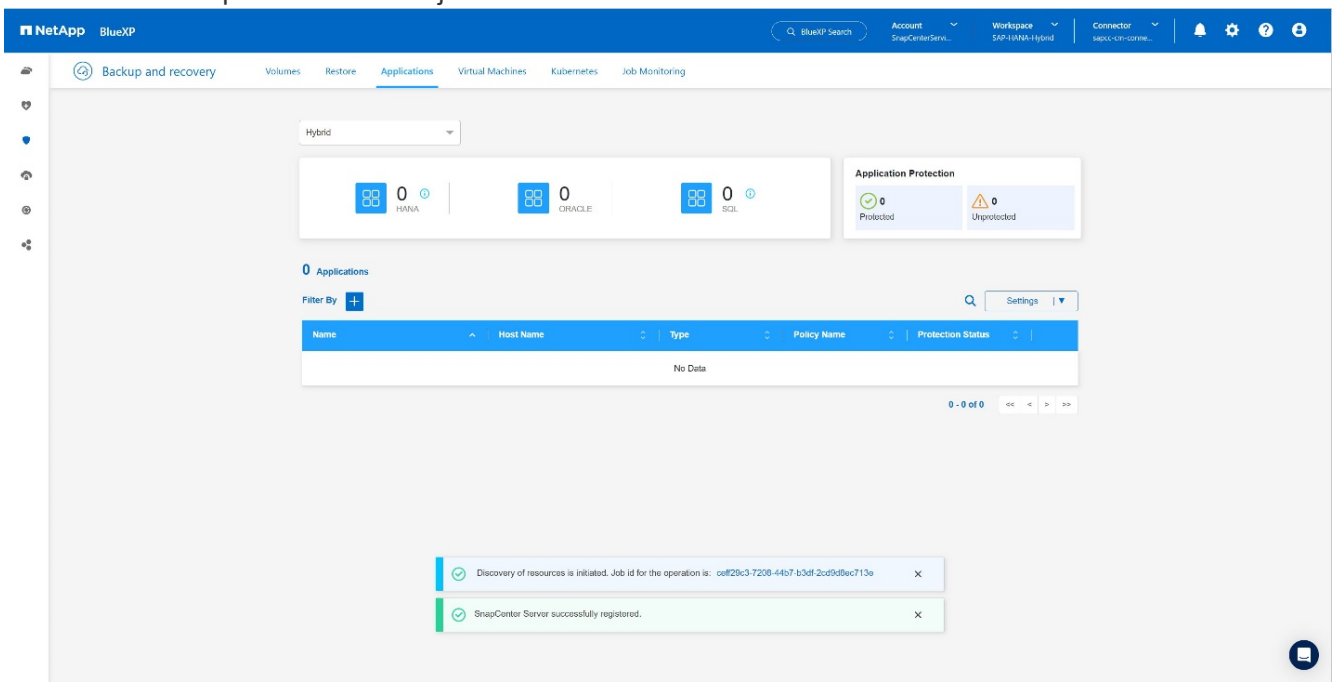
4. Enregistrez le serveur SnapCenter.



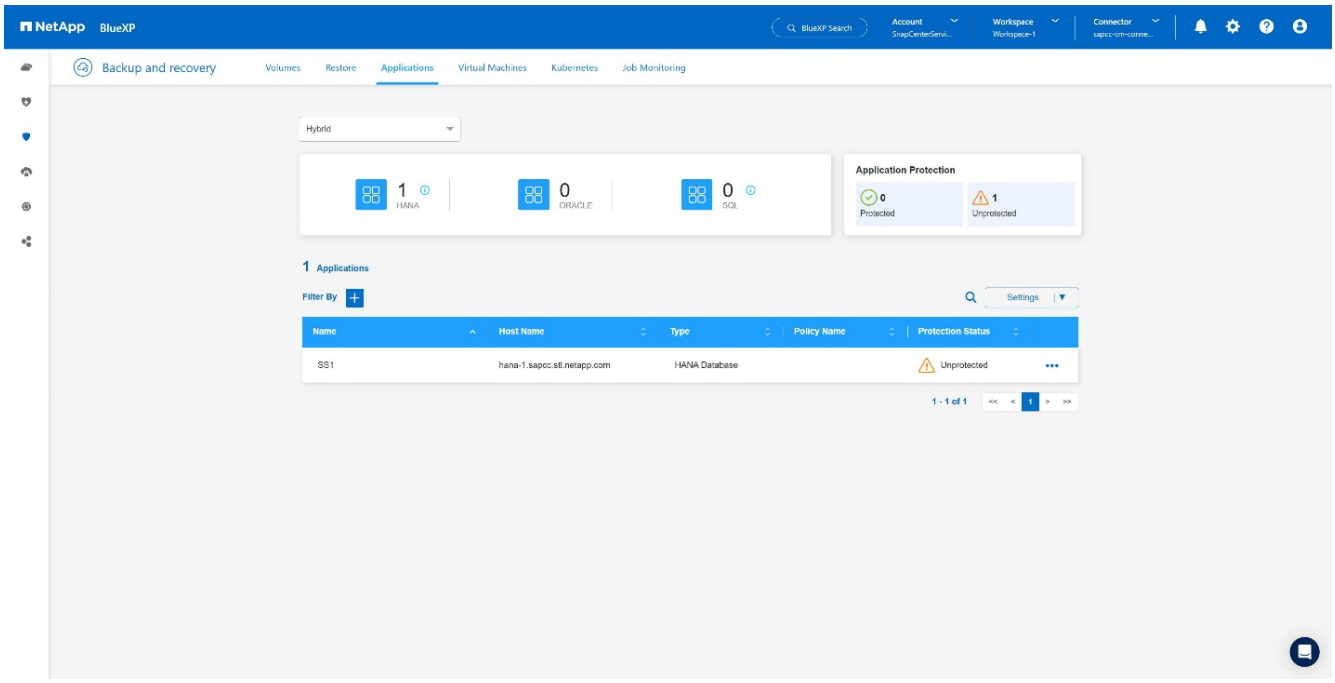
5. Ajoutez les informations d’identification du serveur SnapCenter.



6. Les serveurs SnapCenter ont été ajoutés et les données seront découvertes.

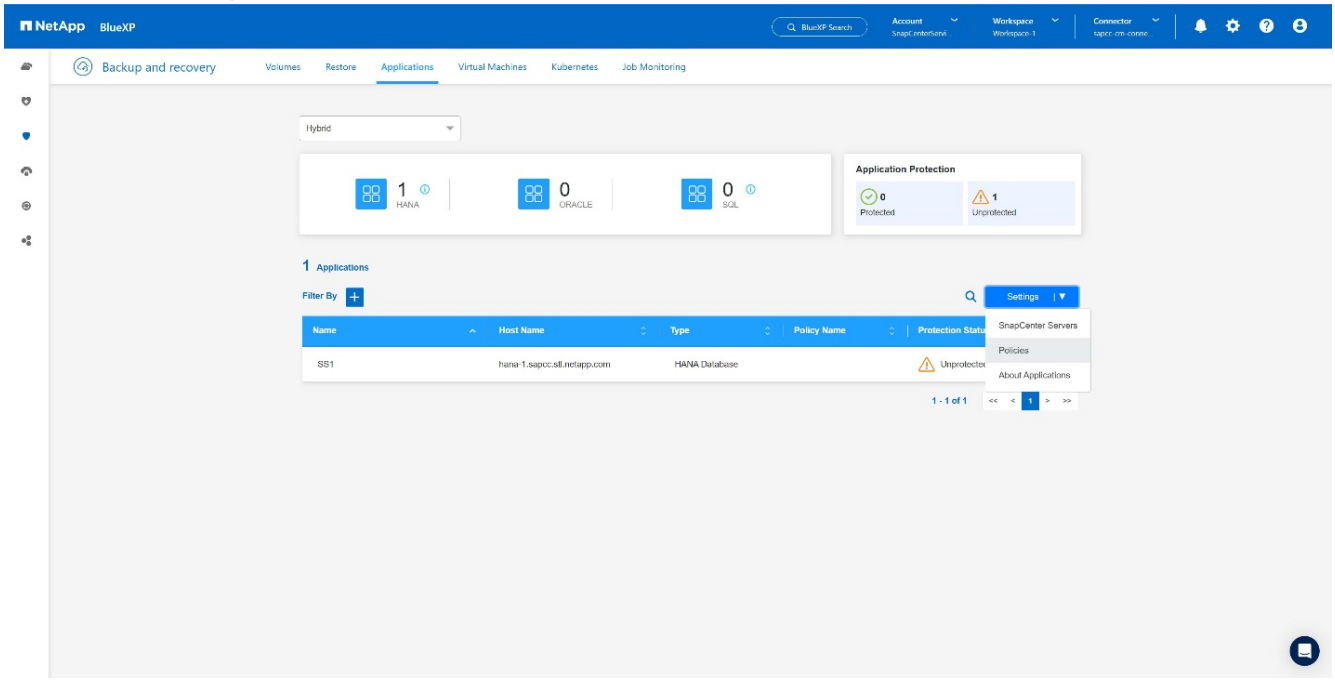


7. Une fois la tâche de découverte terminée, le système SAP HANA est disponible.

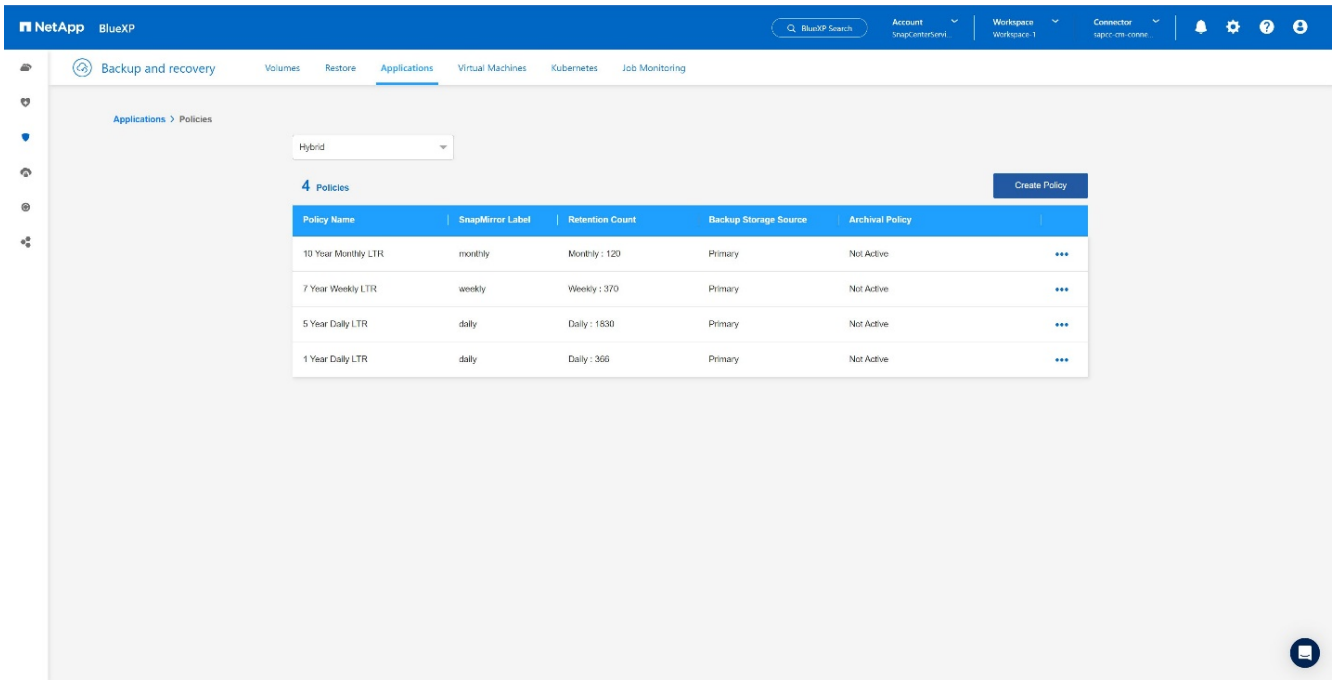


Création d'une règle de sauvegarde pour la sauvegarde des applications

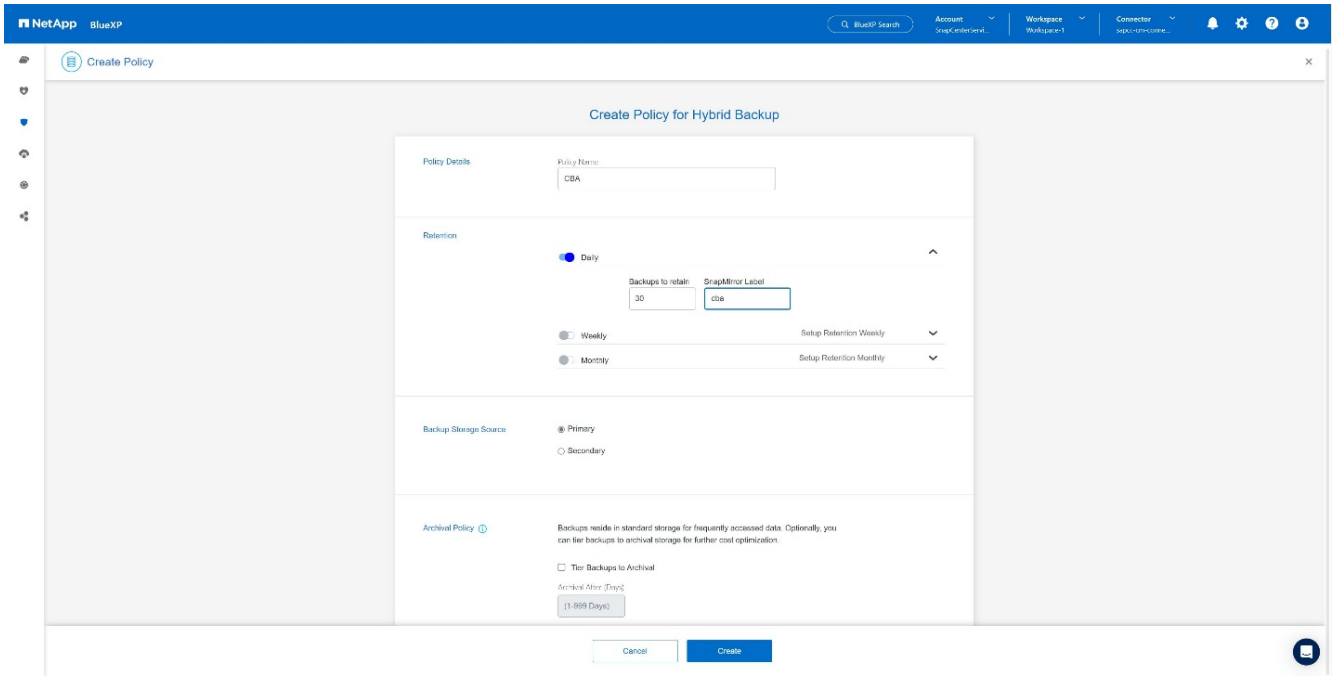
1. Choisissez **stratégies** dans le menu des paramètres.



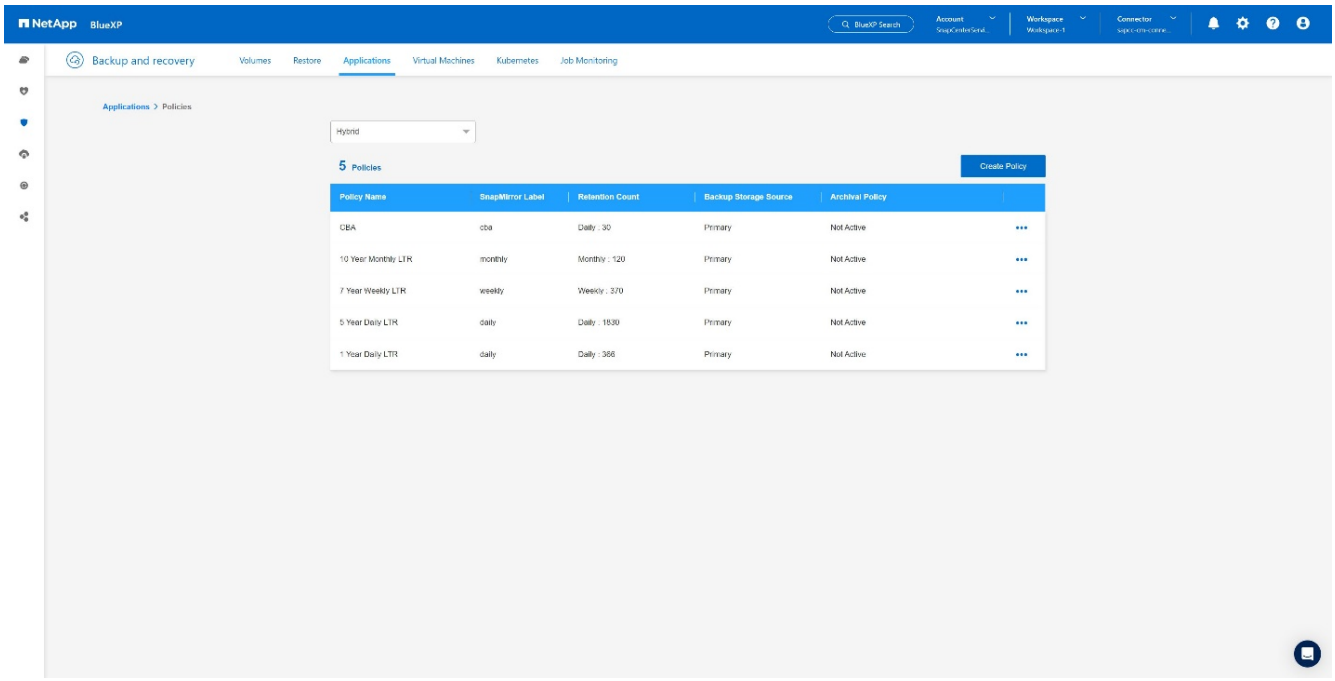
2. Créez une nouvelle stratégie, si vous le souhaitez, en cliquant sur **Créer une stratégie**.



3. Indiquez le nom de la règle, le libellé SnapMirror souhaité, choisissez les options souhaitées, puis appuyez sur **Create**.

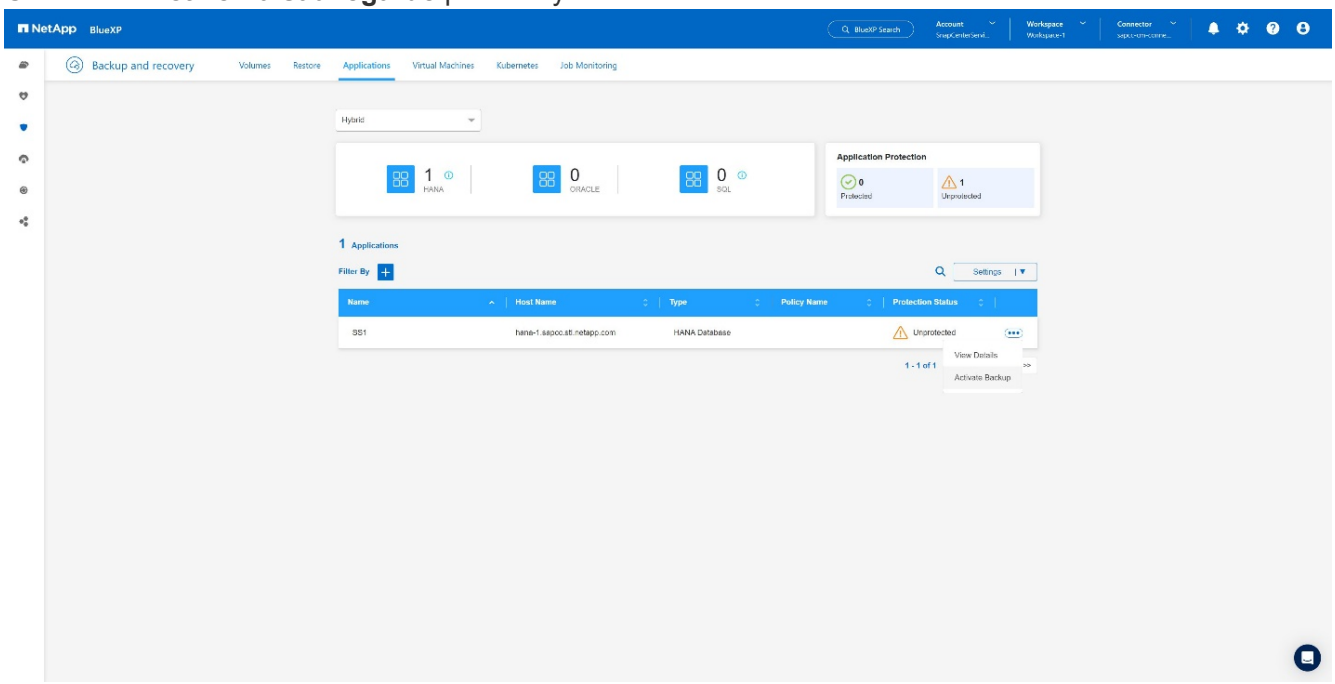


4. La nouvelle politique est disponible.

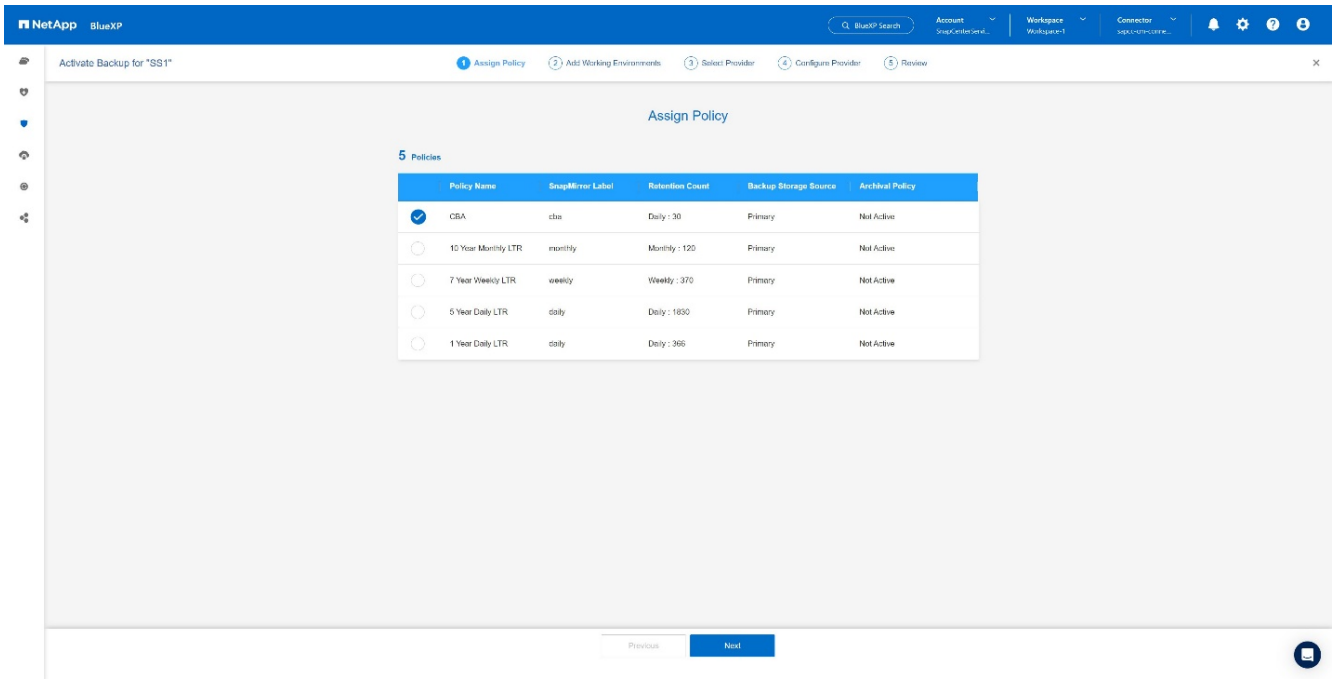


Protection de la base de données SAP HANA avec Cloud Backup pour les applications

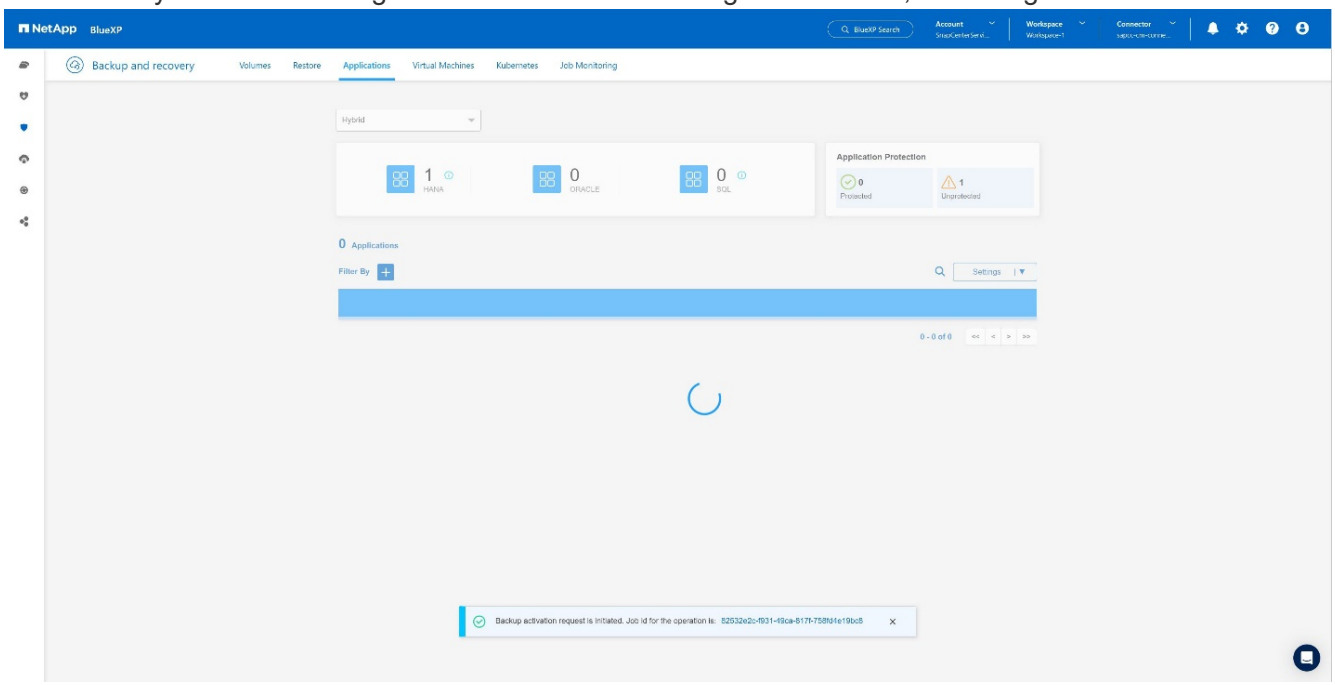
1. Choisissez **Activer la sauvegarde** pour le système SAP HANA.



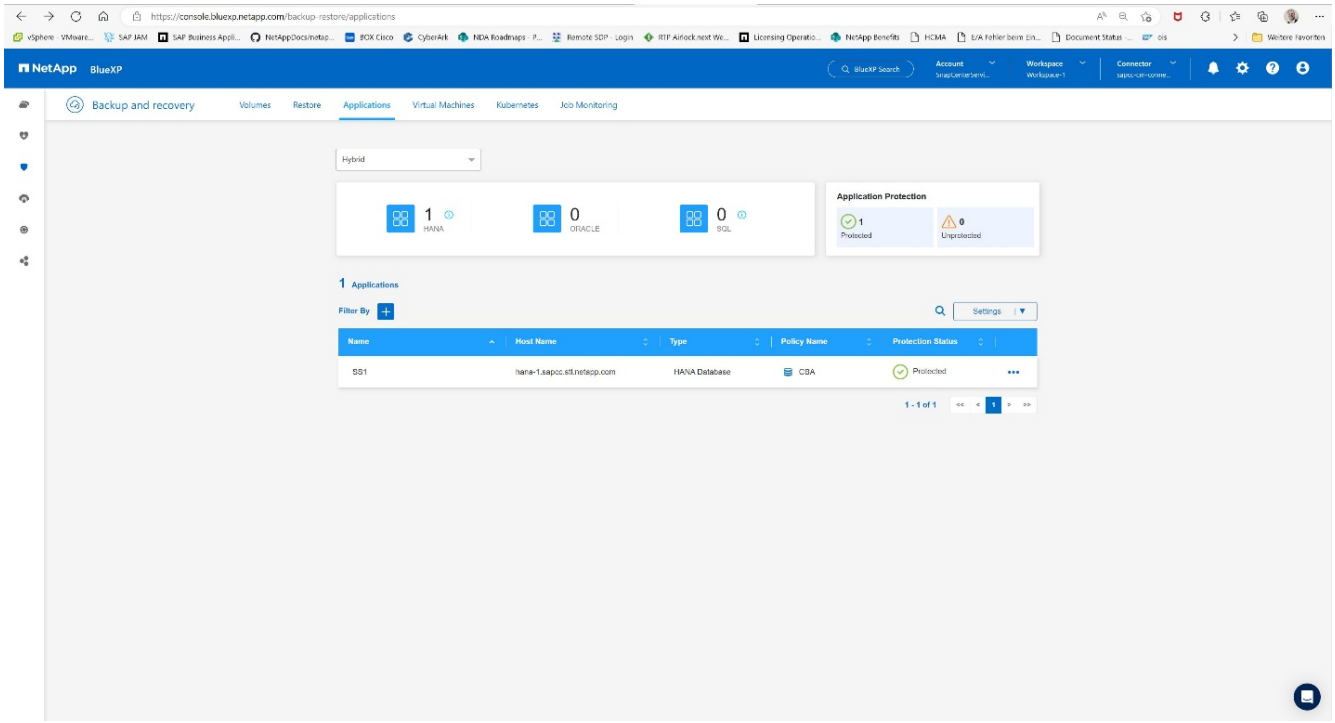
2. Choisissez la stratégie précédemment créée et cliquez sur **Suivant**.



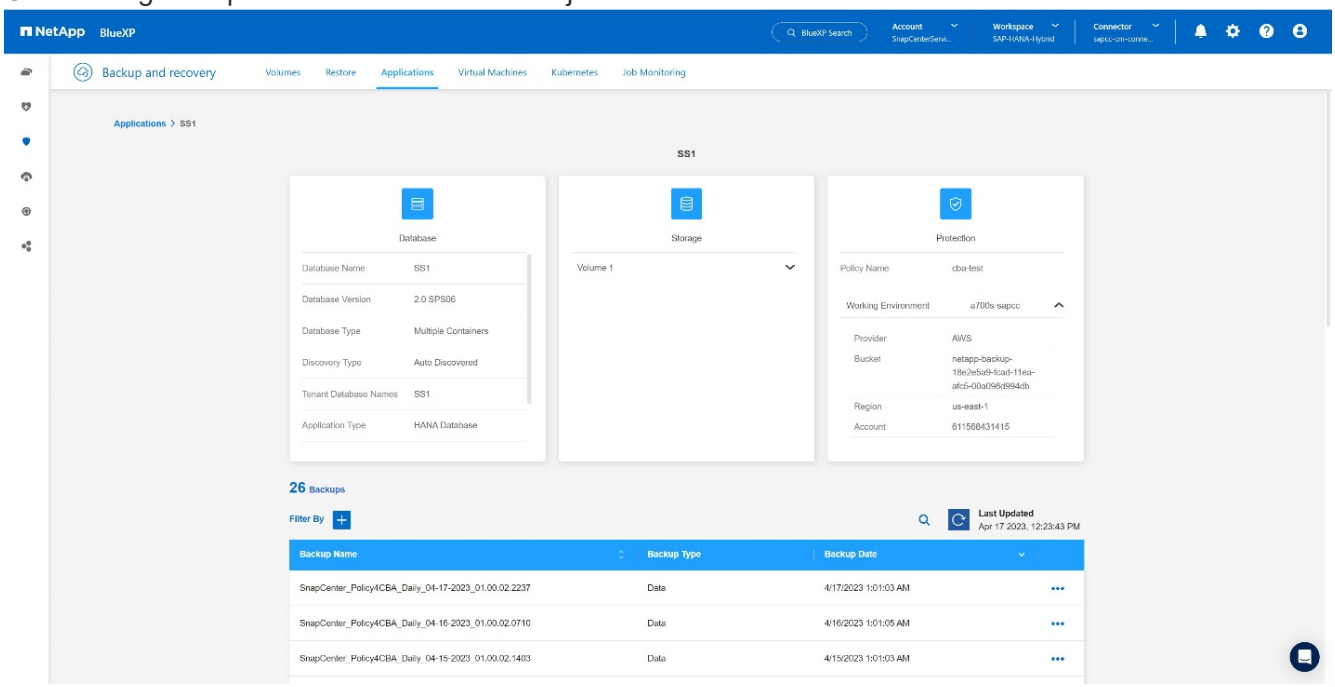
3. Comme le système de stockage et le connecteur ont configuré en amont, la sauvegarde est activée.



4. Une fois la tâche terminée, le système s'affiche.



5. Après un certain temps, les sauvegardes seront répertoriées dans la vue détaillée du système SAP HANA. Une sauvegarde quotidienne sera affichée le jour suivant.

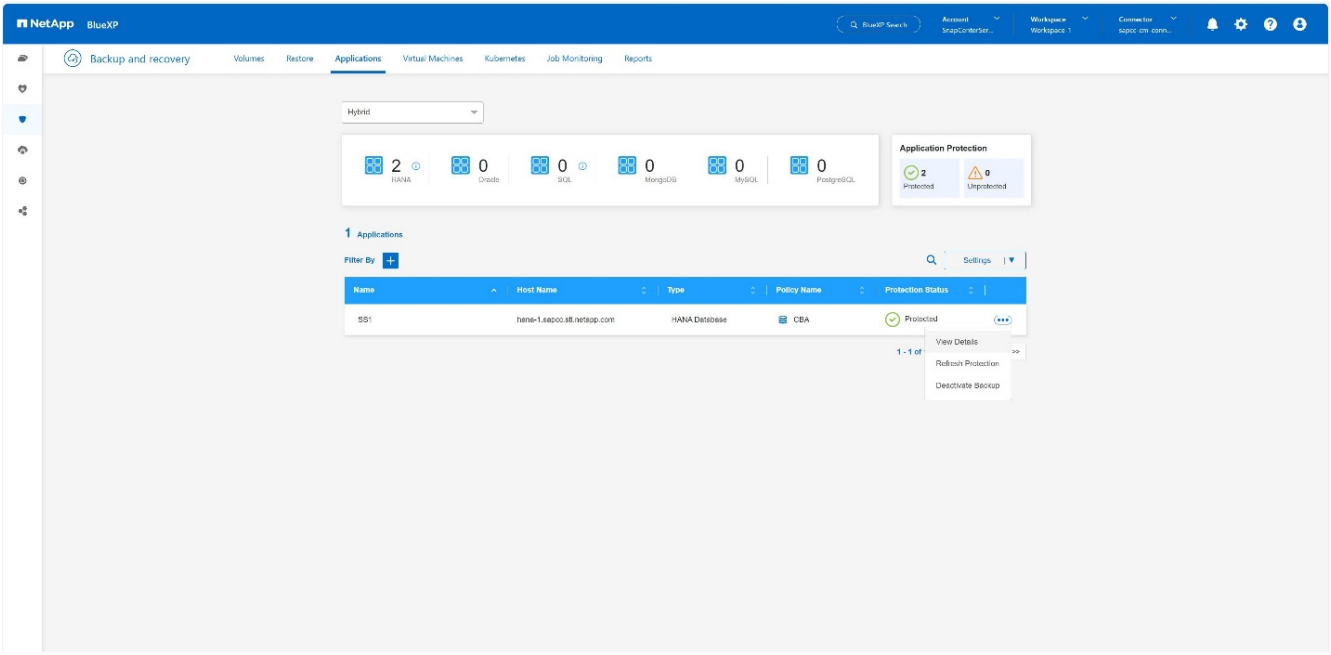


Dans certains environnements, il peut être nécessaire de supprimer les paramètres de planification existants de la source snapmirror. Pour ce faire, exécutez la commande suivante sur le système ONTAP source : *snapmirror modify -destination-path <hana-cloud-svm>:<SID_data_mnt00001>_copy -schedule ""* .

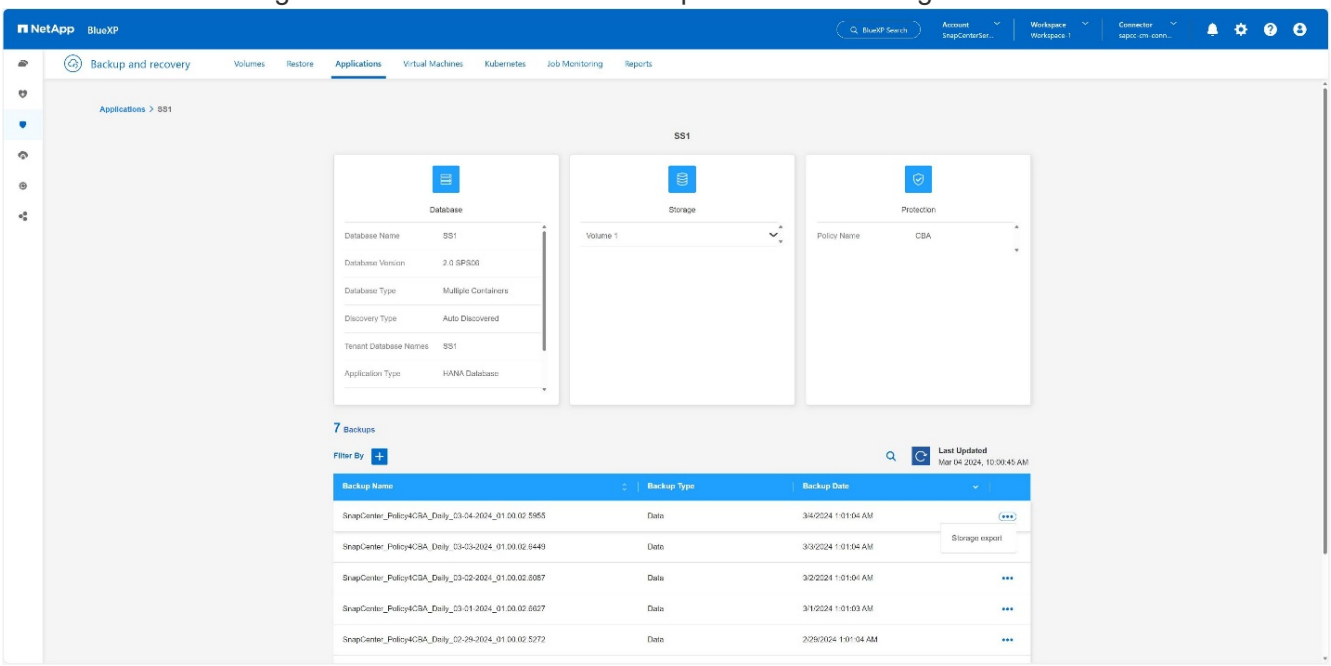
Restauration de la sauvegarde SAP HANA BlueXP

Une restauration à partir de la sauvegarde peut uniquement être effectuée sur un système de stockage NetApp ONTAP sur site ou NetApp CVO dans le cloud. Vous pouvez effectuer une restauration en procédant comme suit :

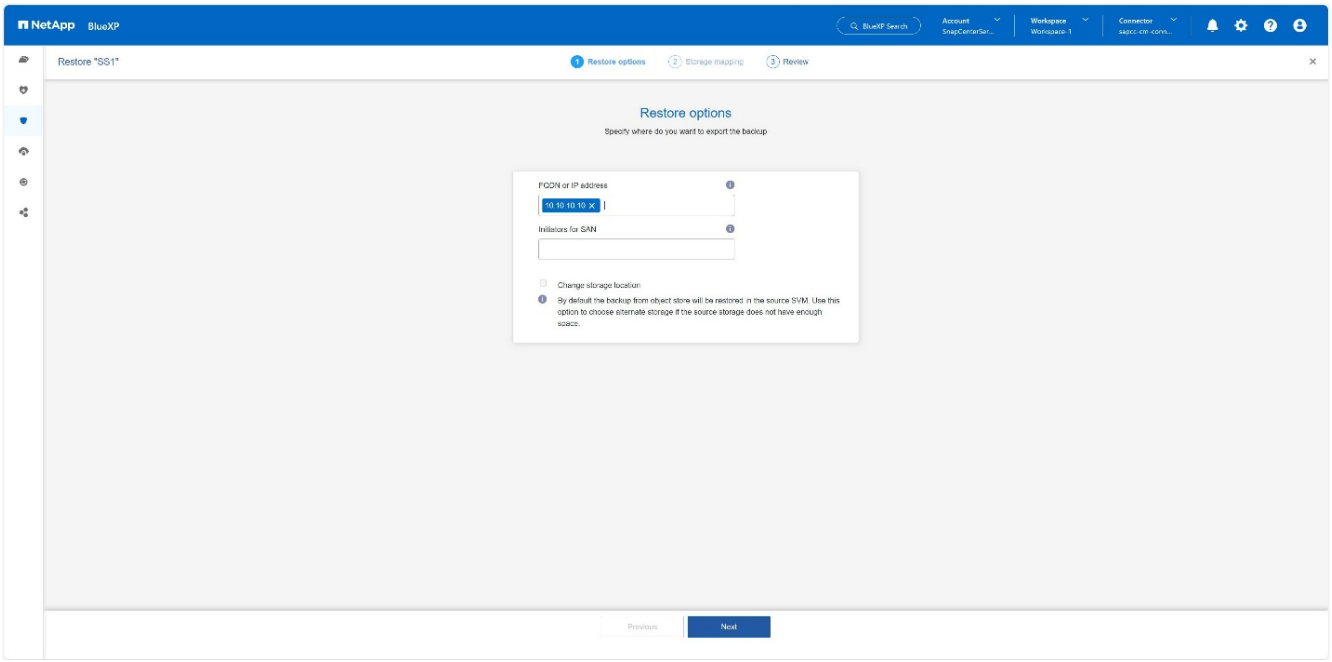
1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et restauration** > **applications** et choisissez hybride.
2. Dans le champ **Filtrer par**, sélectionnez le filtre **Type** et dans la liste déroulante, sélectionnez **HANA**.
3. Cliquez sur **Afficher les détails** correspondant à la base de données que vous souhaitez restaurer.



4. Sélectionnez la sauvegarde souhaitée et choisissez exportation du stockage.



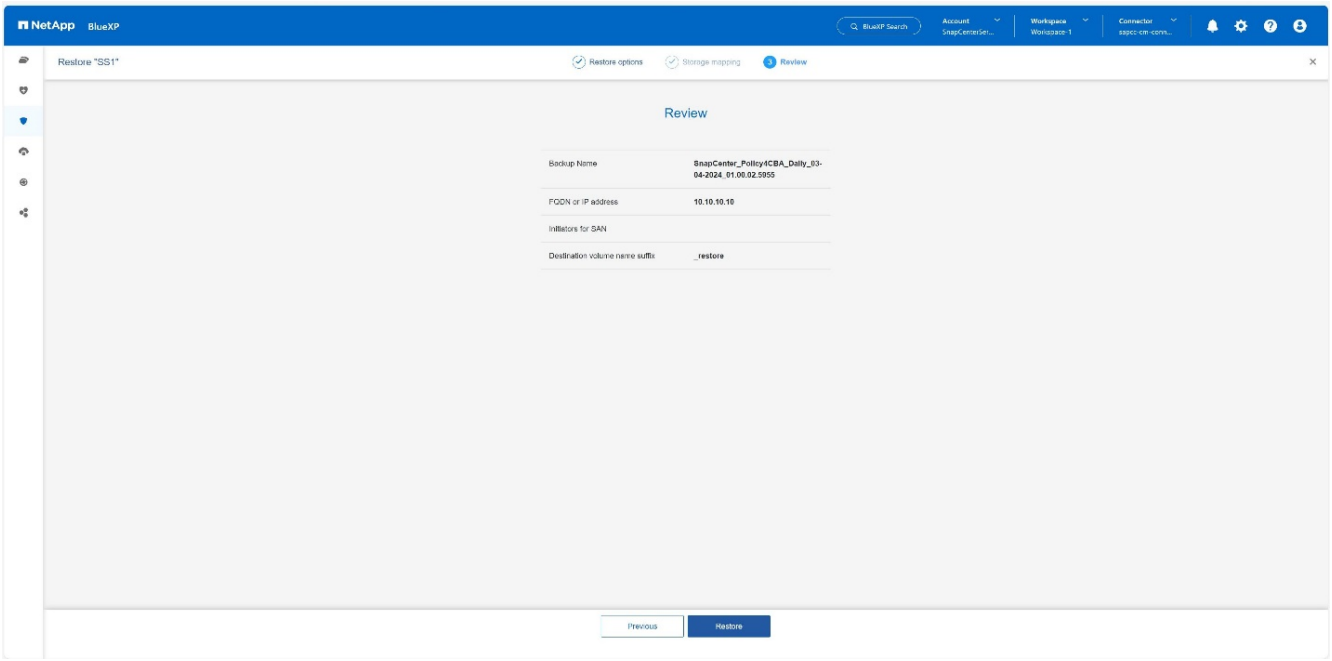
5. Fournissez les options souhaitées :



a. Pour l'environnement NAS, spécifiez le nom de domaine complet ou l'adresse IP de l'hôte vers lequel les volumes restaurés à partir du magasin d'objets doivent être exportés.

b. Pour l'environnement SAN, spécifiez les initiateurs de l'hôte sur lesquels les LUN des volumes restaurés à partir du magasin d'objets doivent être mappées.

6. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.
7. S'il n'y a pas assez d'espace sur le stockage source ou si le stockage source est en panne, sélectionnez **Modifier l'emplacement de stockage**.
8. Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination. Cliquez sur **Suivant**.
9. Si vous avez sélectionné Modifier l'emplacement de stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données restaurées à partir du magasin d'objets seront stockées dans la page mappage de stockage et cliquez sur **Suivant**.
10. Vérifiez les détails et cliquez sur **Restaurer**.



Cette opération n'effectue que l'exportation du stockage de la sauvegarde restaurée pour l'hôte donné. Vous devez monter manuellement le système de fichiers sur l'hôte et ouvrir la base de données. Après avoir utilisé le volume, l'administrateur du stockage peut le supprimer du cluster ONTAP.

Informations supplémentaires et historique des versions

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Documentation du produit de sauvegarde et de restauration NetApp BlueXP
  "Protection des données applicatives sur site | Documentation NetApp"
- Sauvegarde et restauration SAP HANA avec SnapCenter
  https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-br-scs-overview.html#the-netapp-solution

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Mars 2024	Version initiale

Reportez-vous à la "Matrice d'interopérabilité (IMT)" Le site de support NetApp vous assure que les versions de produits et de fonctionnalités mentionnées dans le présent document sont prises en charge par votre environnement. NetApp IMT définit les composants et versions de produits qu'il est possible d'utiliser pour créer des configurations prises en charge par NetApp. Les résultats spécifiques dépendent de l'installation de chaque client conformément aux spécifications publiées.

Réplication système SAP HANA : sauvegarde et restauration avec SnapCenter

Tr-4719 : réplication système SAP HANA - sauvegarde et restauration avec SnapCenter

Nils Bauer, NetApp

La réplication système SAP HANA est souvent utilisée comme solution haute disponibilité ou de reprise après incident pour les bases de données SAP HANA. La réplication système SAP HANA propose différents modes de fonctionnement selon le cas d'utilisation ou les besoins de disponibilité.

Deux cas d'utilisation principaux peuvent être combinés :

- Haute disponibilité avec un objectif de point de récupération nul et un objectif de délai de restauration minimal grâce à un hôte SAP HANA secondaire dédié.
- Reprise après incident sur de grandes distances. L'hôte SAP HANA secondaire peut également être utilisé pour le développement ou les tests en fonctionnement normal.

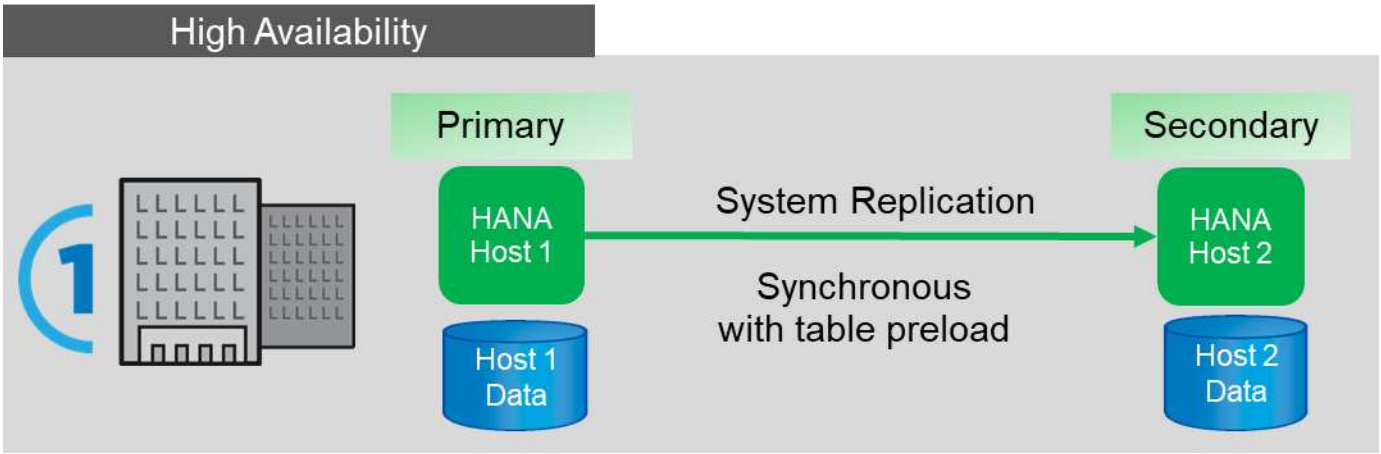
Haute disponibilité avec un RPO nul et un RTO minimal

La réplication système est configurée avec une réplication synchrone à l'aide de tableaux préchargés dans la mémoire sur l'hôte SAP HANA secondaire. Cette solution haute disponibilité peut être utilisée pour résoudre les défaillances matérielles ou logicielles et réduire les temps d'arrêt planifiés lors des mises à niveau du logiciel SAP HANA (temps d'indisponibilité quasi nul).

Les opérations de basculement sont souvent automatisées par un logiciel de cluster tiers ou avec un workflow en un clic grâce au logiciel SAP Landscape Management.

Du point de vue des exigences de sauvegarde, vous devez pouvoir créer des sauvegardes indépendamment de l'hôte SAP HANA principal ou secondaire. Une infrastructure de sauvegarde partagée est utilisée pour restaurer toute sauvegarde, quel que soit l'hôte sur lequel la sauvegarde a été créée.

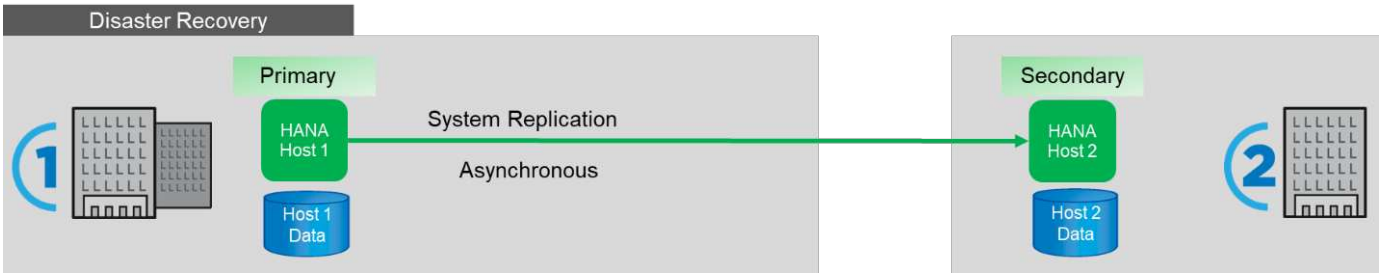
Le reste de ce document se concentre sur les opérations de sauvegarde avec la réplication système SAP configurée comme une solution haute disponibilité.



Reprise après incident sur de grandes distances

La réplication système peut être configurée avec une réplication asynchrone sans table préchargée dans la mémoire de l'hôte secondaire. Cette solution répond aux défaillances du data Center et les opérations de basculement sont généralement réalisées manuellement.

Concernant les exigences de sauvegarde, vous devez être en mesure de créer des sauvegardes pendant le fonctionnement normal du data Center 1 et pendant la reprise sur incident dans le data Center 2. Une infrastructure de sauvegarde distincte est disponible dans les data centers 1 et 2, et les opérations de sauvegarde sont activées dans le cadre du basculement d'incident. L'infrastructure de sauvegarde n'est généralement pas partagée, et l'opération de restauration d'une sauvegarde créée sur l'autre data Center n'est pas possible.



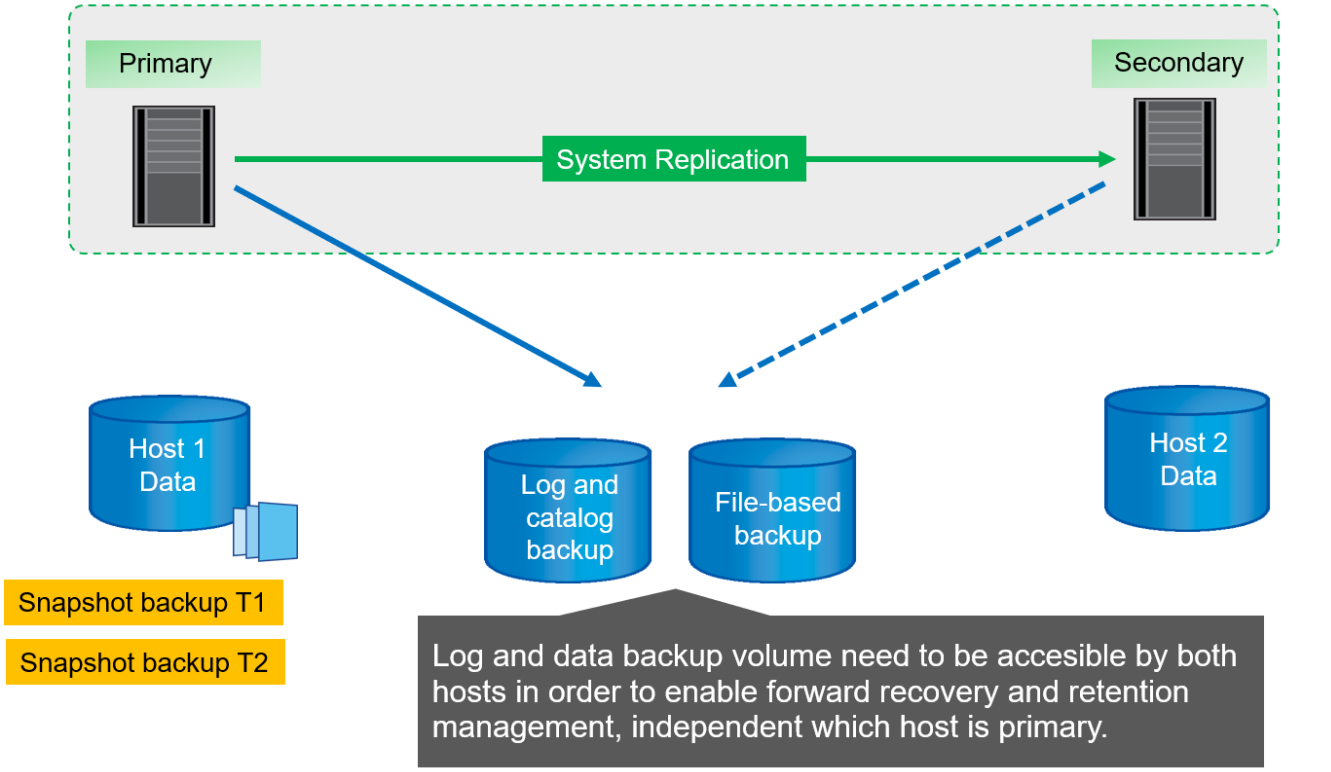
Sauvegardes Snapshot de stockage et réplication système SAP

Les opérations de sauvegarde sont toujours effectuées sur l'hôte SAP HANA principal. Les commandes SQL requises pour l'opération de sauvegarde ne peuvent pas être exécutées sur l'hôte SAP HANA secondaire.

Pour les opérations de sauvegarde SAP HANA, les hôtes SAP HANA principaux et secondaires sont une entité unique. Ils partagent le même catalogue de sauvegardes SAP HANA et utilisent les sauvegardes pour la restauration et la restauration, que la sauvegarde ait été créée sur l'hôte SAP HANA principal ou secondaire.

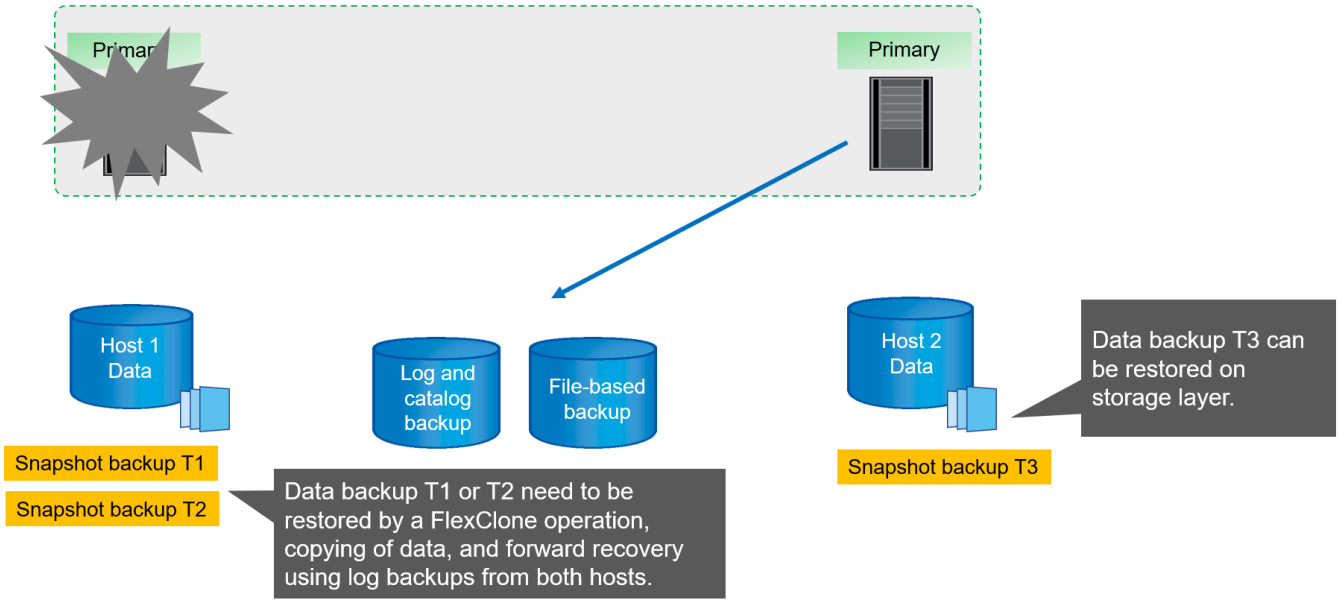
Pour utiliser n'importe quelle sauvegarde pour la restauration et effectuer une restauration avant via des sauvegardes de journaux depuis les deux hôtes, vous devez disposer d'un emplacement de sauvegarde de journal partagé accessible depuis les deux hôtes. NetApp recommande d'utiliser un volume de stockage partagé. Cependant, vous devez également séparer la destination de sauvegarde du journal en sous-répertoires dans le volume partagé.

Chaque hôte SAP HANA dispose de son propre volume de stockage. Lorsque vous utilisez un Snapshot basé sur le stockage pour effectuer une sauvegarde, un Snapshot cohérent avec la base de données est créé sur le volume de stockage de l'hôte SAP HANA principal.



Lorsqu'un basculement vers l'hôte 2 est effectué, l'hôte 2 devient l'hôte principal, les sauvegardes sont exécutées sur l'hôte 2 et les sauvegardes Snapshot sont créées au niveau du volume de stockage de l'hôte 2.

La sauvegarde créée au niveau de l'hôte 2 peut être restaurée directement au niveau de la couche de stockage. Si vous devez utiliser une sauvegarde créée sur l'hôte 1, la sauvegarde doit être copiée depuis le volume de stockage de l'hôte 1 vers le volume de stockage de l'hôte 2. La restauration par transfert utilise les sauvegardes des journaux des deux hôtes.

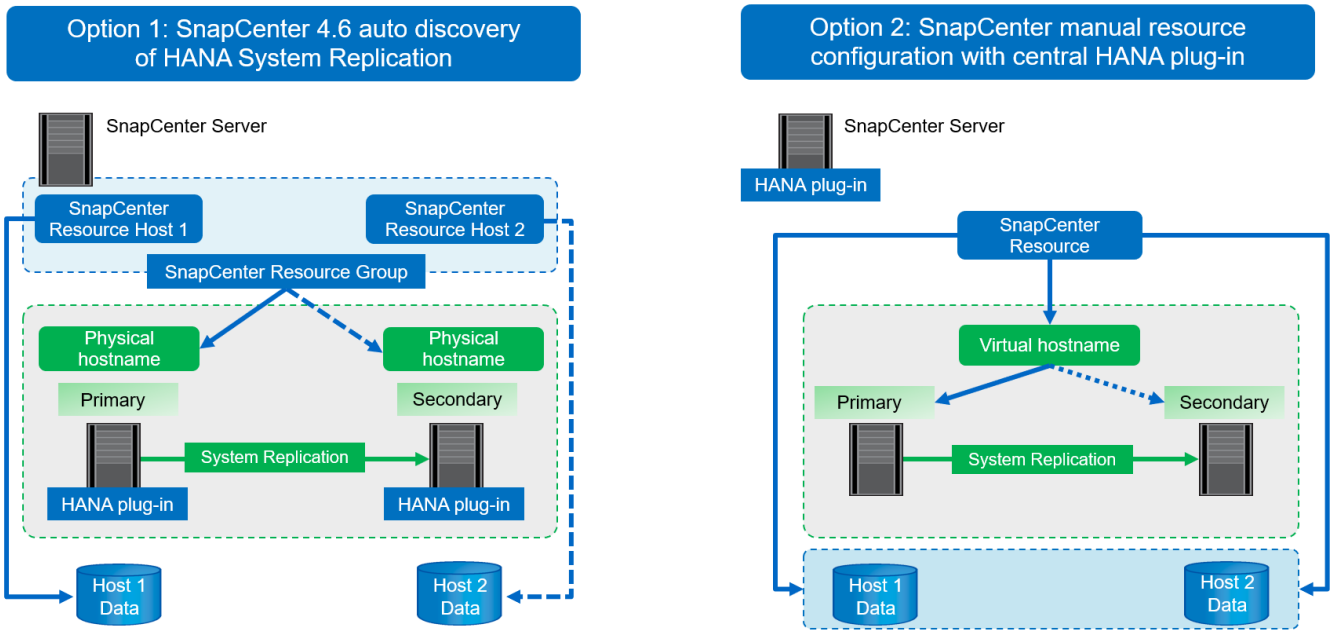


Options de configuration de SnapCenter pour la réplication des systèmes SAP

Deux options permettent de configurer la protection des données avec le logiciel NetApp

SnapCenter dans un environnement de réplication système SAP HANA :

- Groupe de ressources SnapCenter incluant à la fois des hôtes SAP HANA et une détection automatique avec SnapCenter version 4.6 ou ultérieure.
- Une seule ressource SnapCenter pour les deux hôtes SAP HANA utilisant une adresse IP virtuelle.



Depuis SnapCenter 4.6, SnapCenter prend en charge la découverte automatique des systèmes HANA configurés dans une relation de réplication système HANA. Chaque hôte est configuré à l'aide de son adresse IP physique (nom d'hôte) et de son volume de données individuel sur la couche de stockage. Les deux ressources SnapCenter sont combinées dans un groupe de ressources, et SnapCenter identifie automatiquement l'hôte principal ou secondaire et exécute les opérations de sauvegarde requises en conséquence. La gestion des données de conservation pour les sauvegardes Snapshot et basées sur les fichiers créées par SnapCenter s'effectue sur les deux hôtes pour s'assurer que les anciennes sauvegardes sont également supprimées sur l'hôte secondaire actuel.

Avec une configuration à ressource unique pour les deux hôtes SAP HANA, la ressource SnapCenter unique est configurée à l'aide de l'adresse IP virtuelle des hôtes de réplication système SAP HANA. Les deux volumes de données des hôtes SAP HANA sont inclus dans la ressource SnapCenter. Étant donné qu'il s'agit d'une seule ressource SnapCenter, la gestion de la conservation pour les sauvegardes Snapshot et basées sur des fichiers créées par SnapCenter fonctionne indépendamment de l'hôte principal ou secondaire actuellement. Toutes les versions de SnapCenter peuvent donc choisir cette option.

Le tableau suivant récapitule les principales différences entre les deux options de configuration.

	Groupe de ressources avec SnapCenter 4.6	**Ressource SnapCenter unique et adresse IP virtuelle**
Opération de sauvegarde (copies Snapshot et fichiers)	Identification automatique de l'hôte principal dans le groupe de ressources	Utiliser automatiquement l'adresse IP virtuelle
Gestion de la conservation (basée sur des copies Snapshot et des fichiers)	Exécution automatique sur les deux hôtes	Utiliser automatiquement une seule ressource

	Groupe de ressources avec SnapCenter 4.6	Ressource SnapCenter unique et adresse IP virtuelle
Besoins en capacité de sauvegarde	Les sauvegardes sont uniquement créées sur le volume d'hôte principal	Les sauvegardes sont toujours créées au niveau des deux volumes hôtes. La sauvegarde du second hôte est uniquement cohérente après panne et ne peut pas être utilisée pour effectuer une restauration vers l'avant.
Opération de restauration	Des sauvegardes à partir de l'hôte actif actuel sont disponibles pour l'opération de restauration	Script de pré-sauvegarde requis pour identifier les sauvegardes valides et pouvant être utilisées pour la restauration
Opération de reprise	Toutes les options de récupération disponibles, comme pour toute ressource découverte automatique	Restauration manuelle requise

De manière générale, NetApp recommande d'utiliser l'option de configuration de groupe de ressources avec SnapCenter 4.6 pour protéger les systèmes HANA avec la réplication système HANA activée. L'utilisation d'une seule configuration de ressource SnapCenter n'est nécessaire que si l'approche SnapCenter repose sur un hôte plug-in central et que le plug-in HANA n'est pas déployé sur les hôtes de base de données HANA.

Ces deux options sont présentées en détail dans les sections suivantes.

Configuration de SnapCenter 4.6 à l'aide d'un groupe de ressources

SnapCenter 4.6 prend en charge la détection automatique des systèmes HANA configurés avec la réplication système HANA. SnapCenter 4.6 inclut la logique permettant d'identifier les hôtes HANA principaux et secondaires pendant les opérations de sauvegarde, et gère également la gestion de la conservation sur les hôtes HANA. De plus, la restauration et la restauration automatisées sont désormais disponibles pour les environnements de réplication système HANA.

Configuration SnapCenter 4.6 des environnements de réplication système HANA

La figure suivante illustre la configuration de laboratoire utilisée pour ce chapitre. Deux hôtes HANA, hana-3 et hana-4, ont été configurés avec la réplication système HANA.

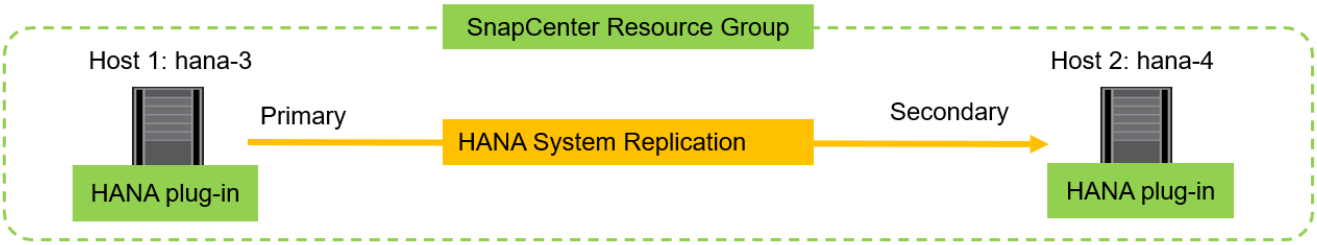
Un utilisateur de base de données "SnapCenter" a été créé pour la base de données système HANA avec les privilèges requis pour exécuter les opérations de sauvegarde et de restauration (voir "SAP HANA : sauvegarde et restauration avec SnapCenter"). Une clé de magasin d'utilisateurs HANA doit être configurée sur les deux hôtes à l'aide de l'utilisateur de base de données ci-dessus.

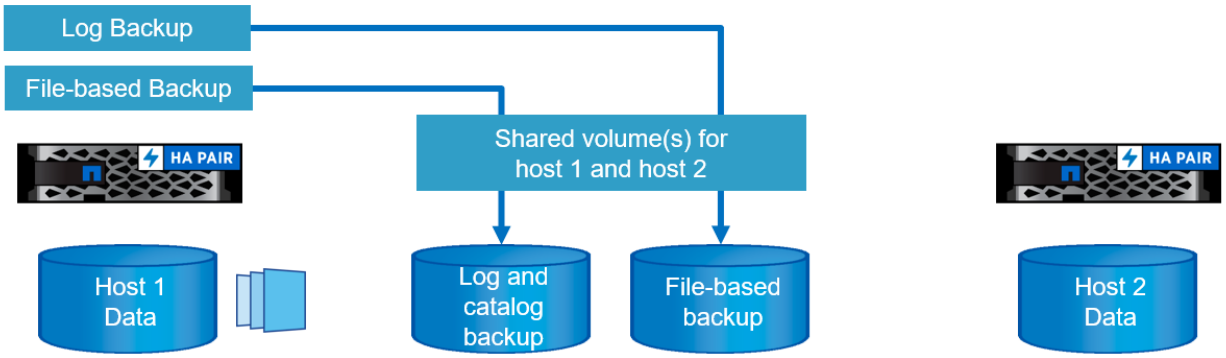
```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

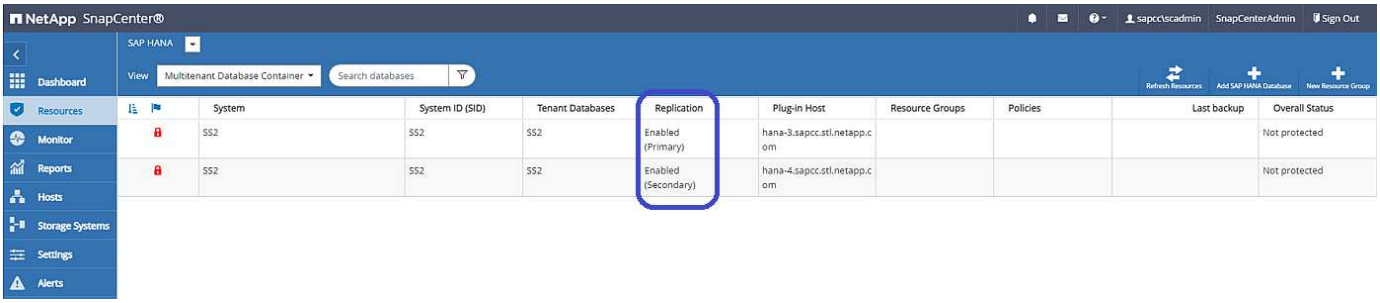
De manière générale, vous devez effectuer les étapes suivantes pour configurer la réplication système HANA dans SnapCenter.

1. Installez le plug-in HANA sur les hôtes principal et secondaire. La détection automatique est exécutée et l'état de réplication du système HANA est détecté pour chaque hôte principal ou secondaire.
2. Exécuter SnapCenter `configure database` et fournir le `hdbuserstore` clé. D'autres opérations de découverte automatique sont exécutées.
3. Créez un groupe de ressources, y compris les hôtes et configurez la protection.

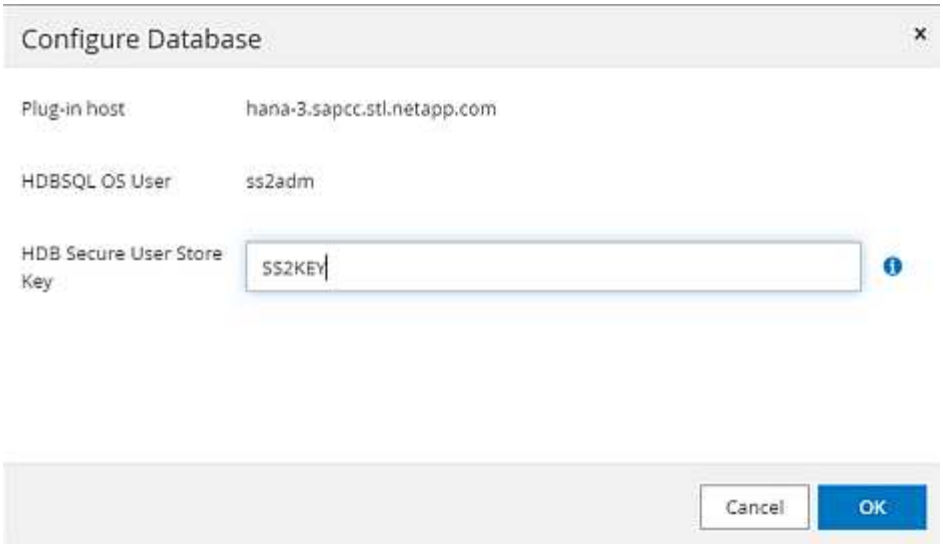




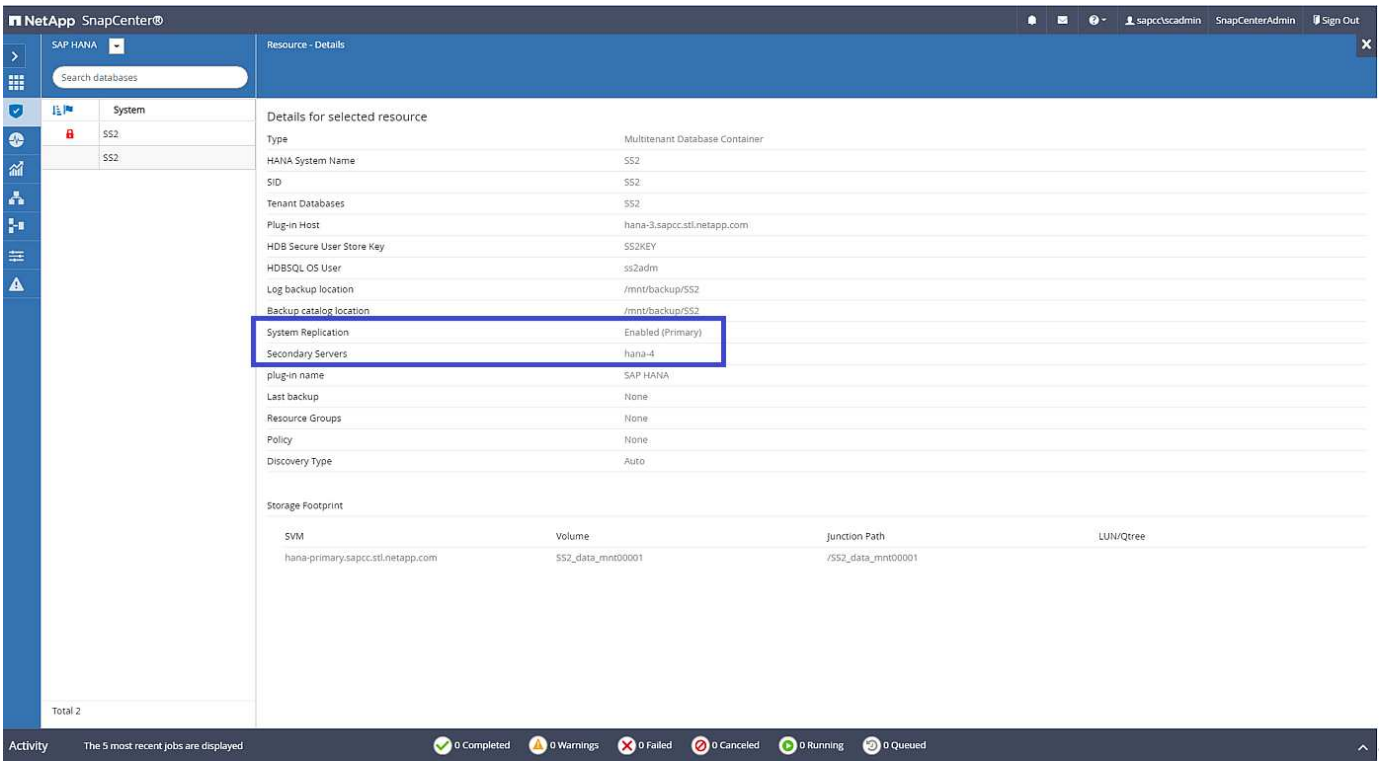
Une fois le plug-in SnapCenter HANA installé sur les deux hôtes HANA, les systèmes HANA s'affichent dans la vue des ressources SnapCenter de la même manière que les autres ressources autodécouvertes. Depuis la version SnapCenter 4.6, une colonne supplémentaire affiche l'état de la réplication système HANA (activée/désactivée, principale/secondaire).



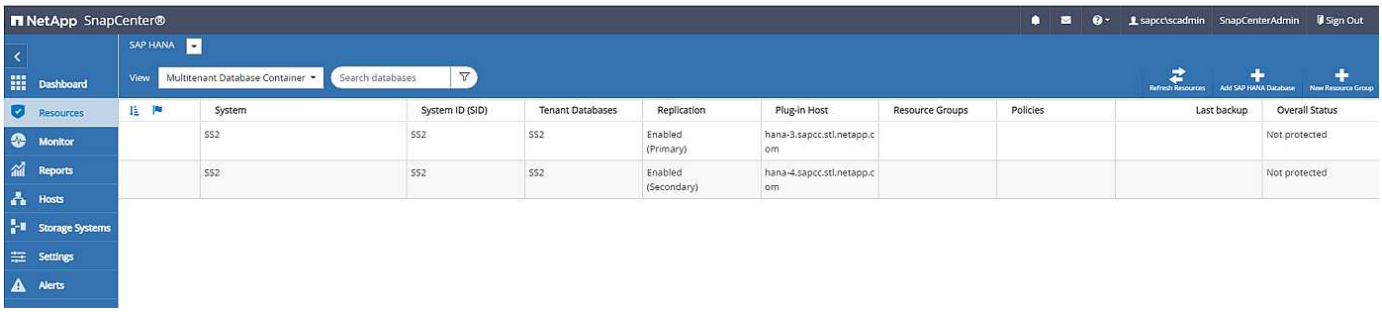
En cliquant sur la ressource, SnapCenter demande la clé de magasin utilisateur HANA pour le système HANA.



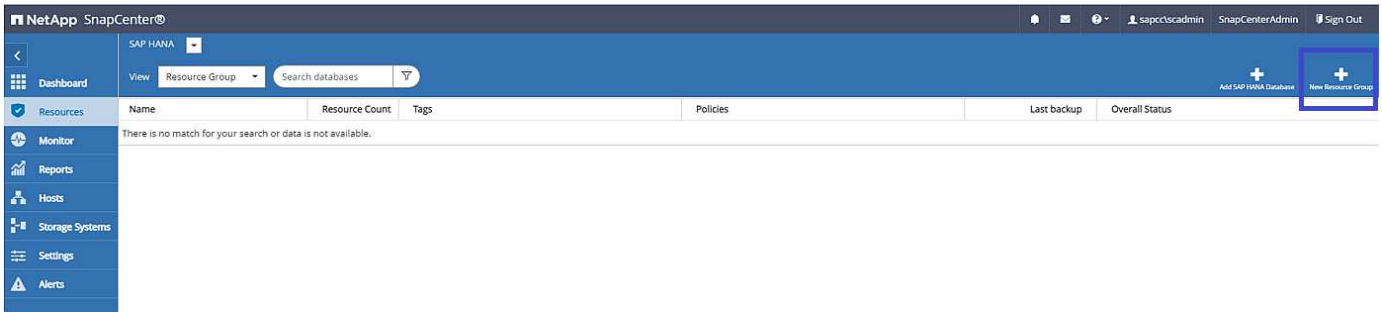
D'autres étapes de découverte automatique sont exécutées. SnapCenter affiche les détails des ressources. Avec SnapCenter 4.6, l'état de réplication du système et le serveur secondaire sont répertoriés dans cette vue.



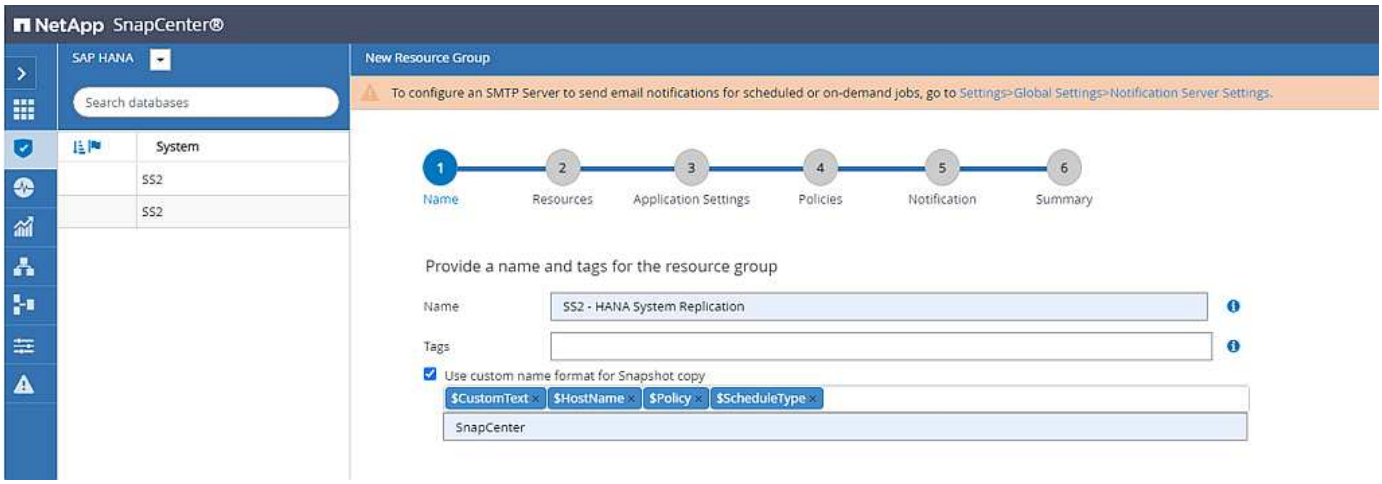
Après avoir effectué les mêmes étapes pour la seconde ressource HANA, le processus de détection automatique est terminé et les deux ressources HANA sont configurées dans SnapCenter.



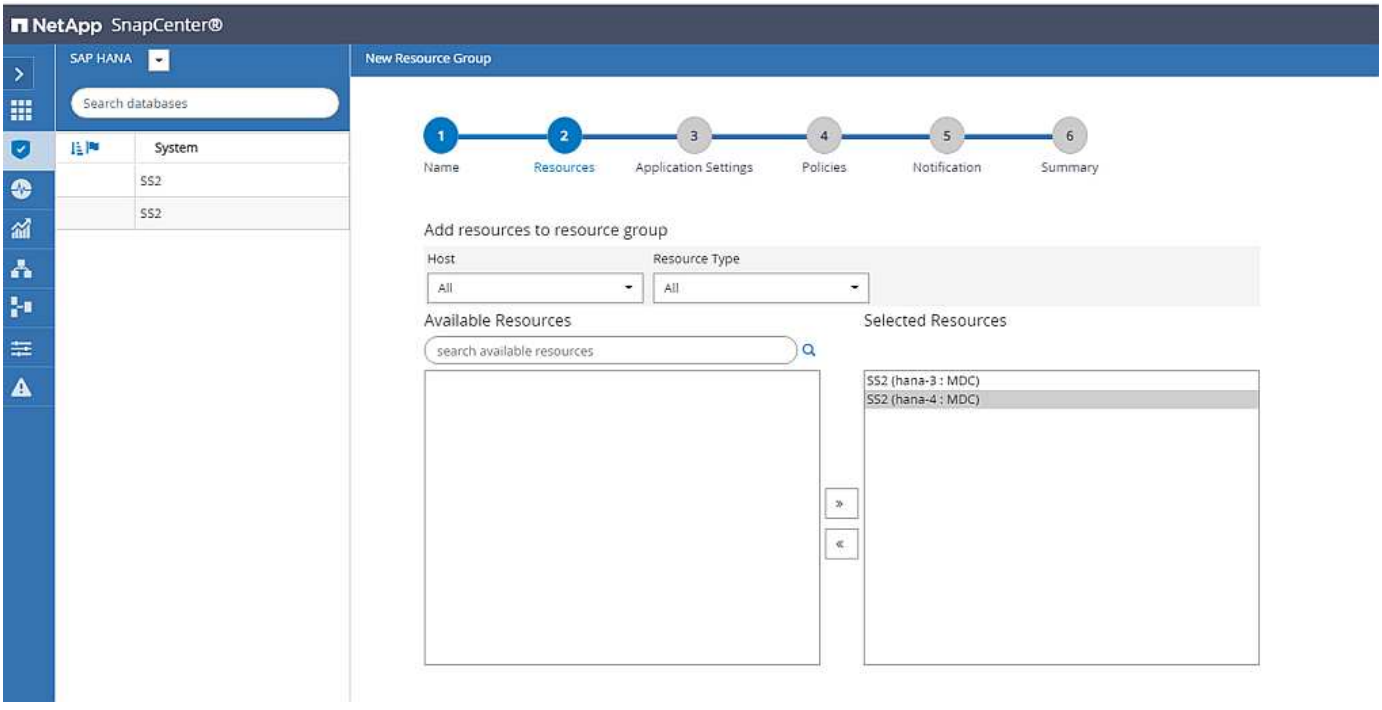
Pour les systèmes compatibles avec la réplication système HANA, vous devez configurer un groupe de ressources SnapCenter, y compris les deux ressources HANA.



NetApp recommande d'utiliser un format de nom personnalisé pour le nom du snapshot, qui doit inclure le nom d'hôte, la règle et la planification.

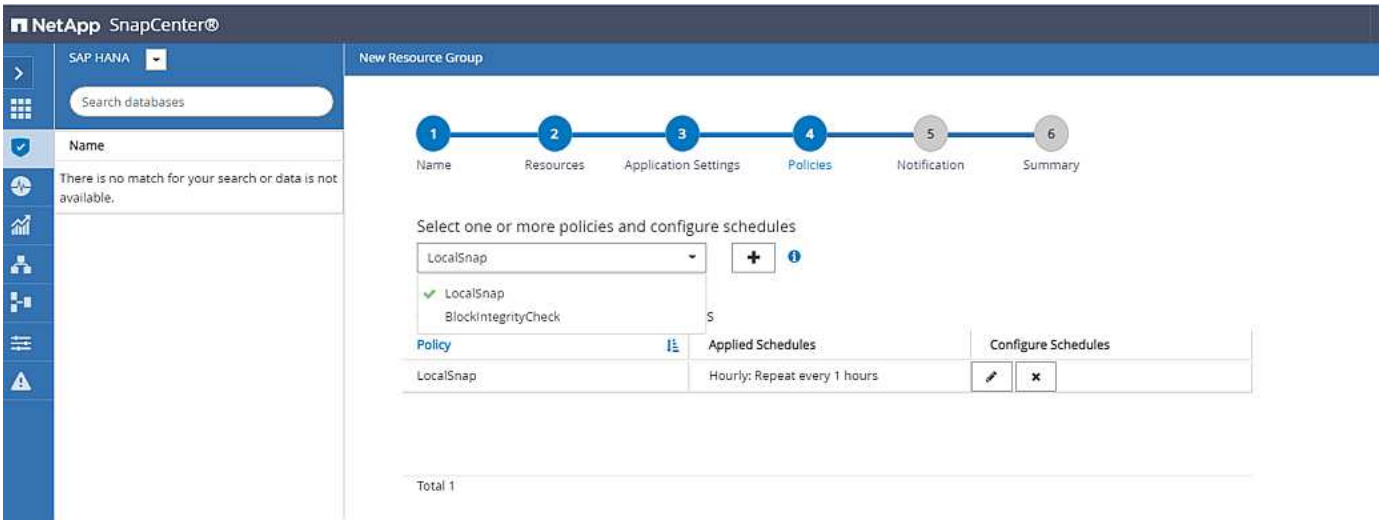


Vous devez ajouter les deux hôtes HANA au groupe de ressources.

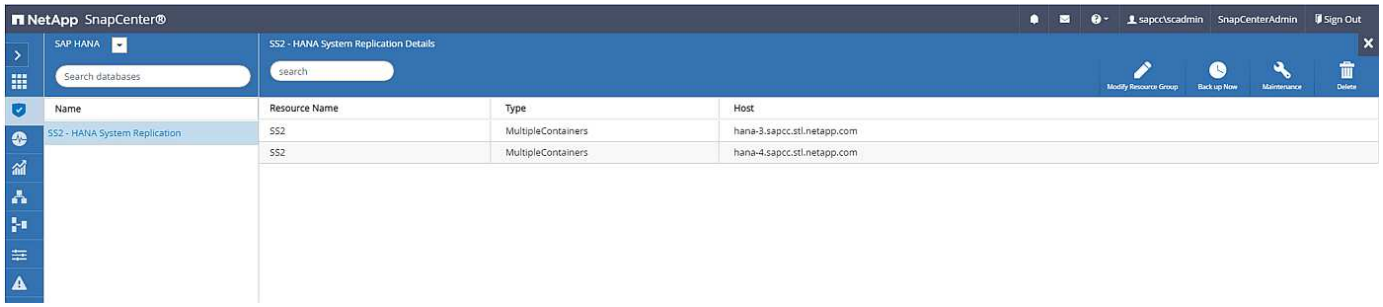


Les stratégies et les planifications sont configurées pour le groupe de ressources.

> La conservation définie dans la règle est utilisée sur les deux hôtes HANA. Si, par exemple, une rétention de 10 est définie dans la règle, la somme des sauvegardes des deux hôtes est utilisée comme critère pour la suppression de la sauvegarde. SnapCenter supprime la sauvegarde la plus ancienne de manière indépendante si elle a été créée sur l'hôte principal ou secondaire actuel.

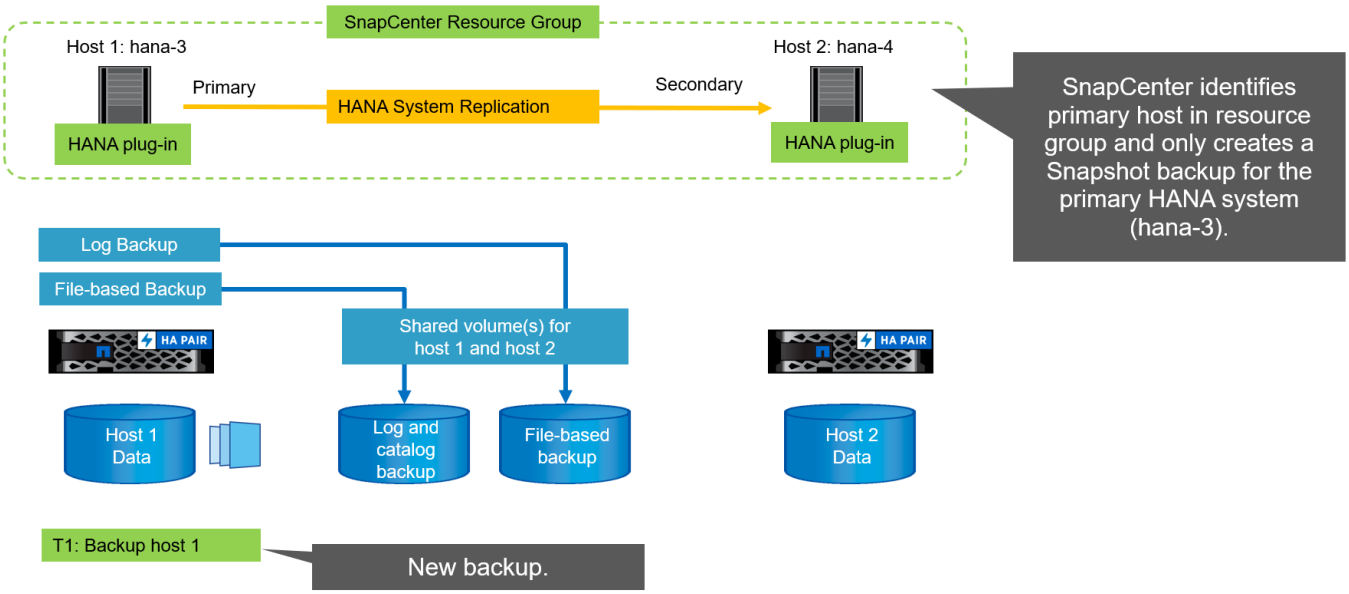


La configuration des groupes de ressources est maintenant terminée et les sauvegardes peuvent être exécutées.

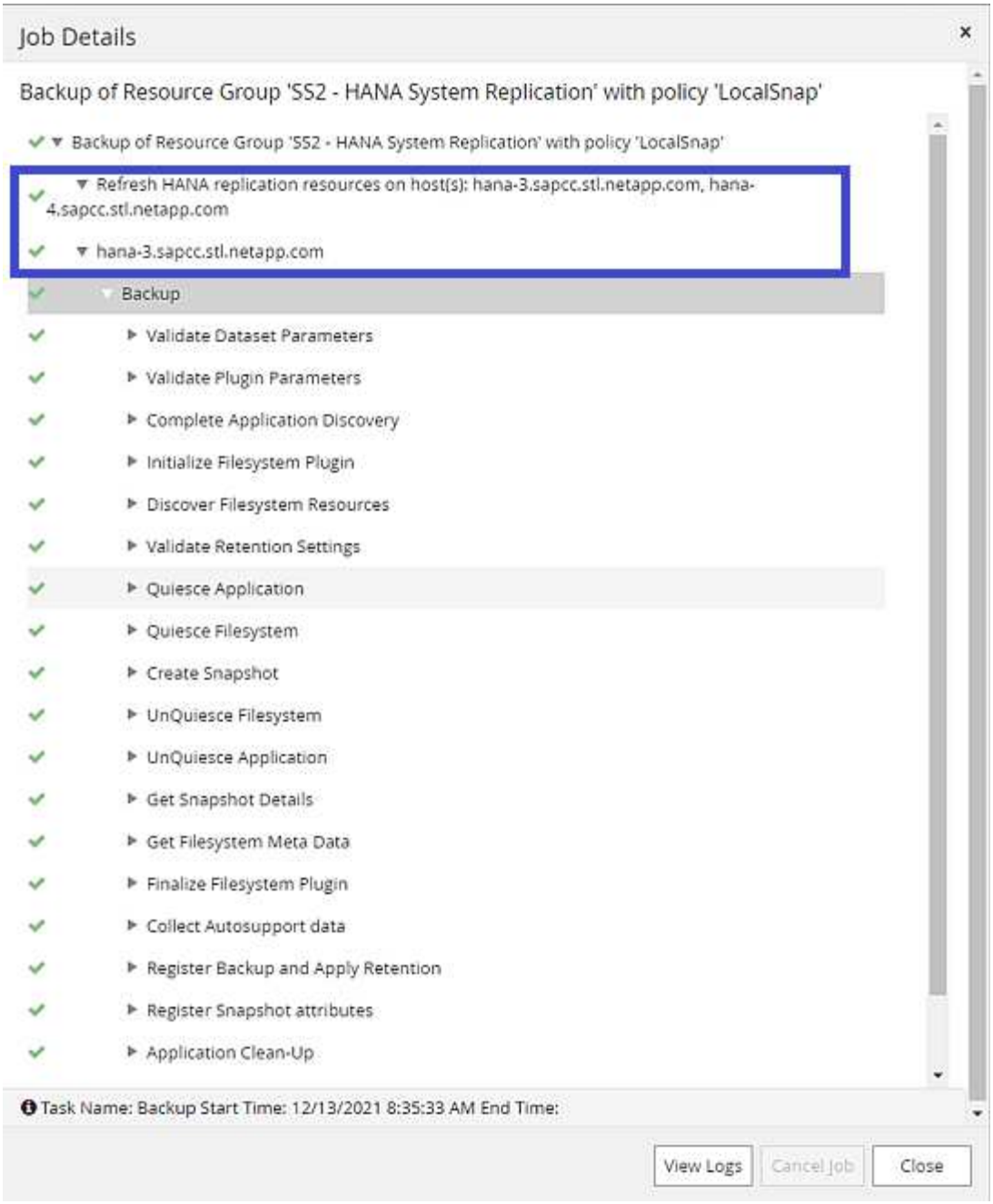


Opérations de sauvegarde Snapshot

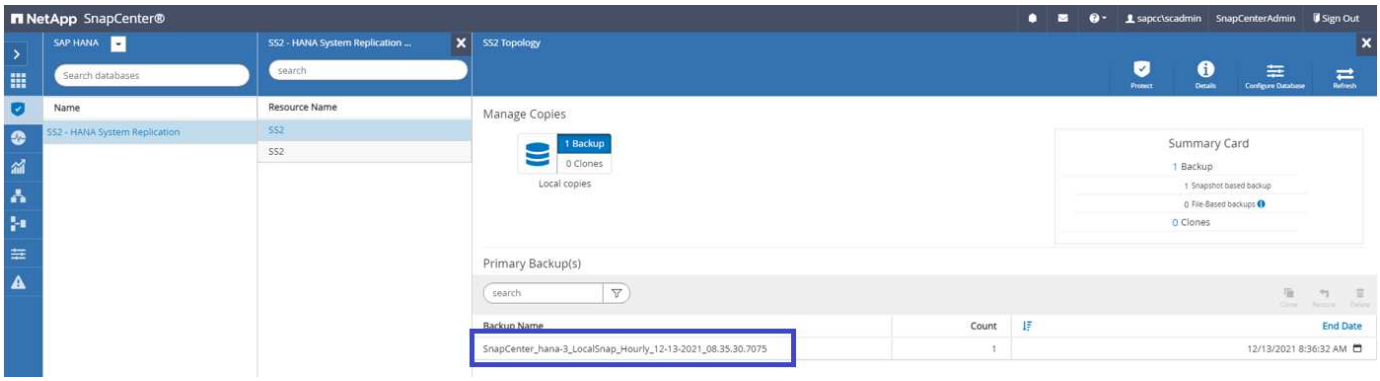
Lors de l'exécution d'une opération de sauvegarde du groupe de ressources, SnapCenter identifie l'hôte principal et déclenche uniquement une sauvegarde sur l'hôte principal. Cela signifie que seul le volume de données de l'hôte principal sera snapshotted. Dans notre exemple, hana-3 est l'hôte principal actuel, et une sauvegarde est exécutée sur cet hôte.



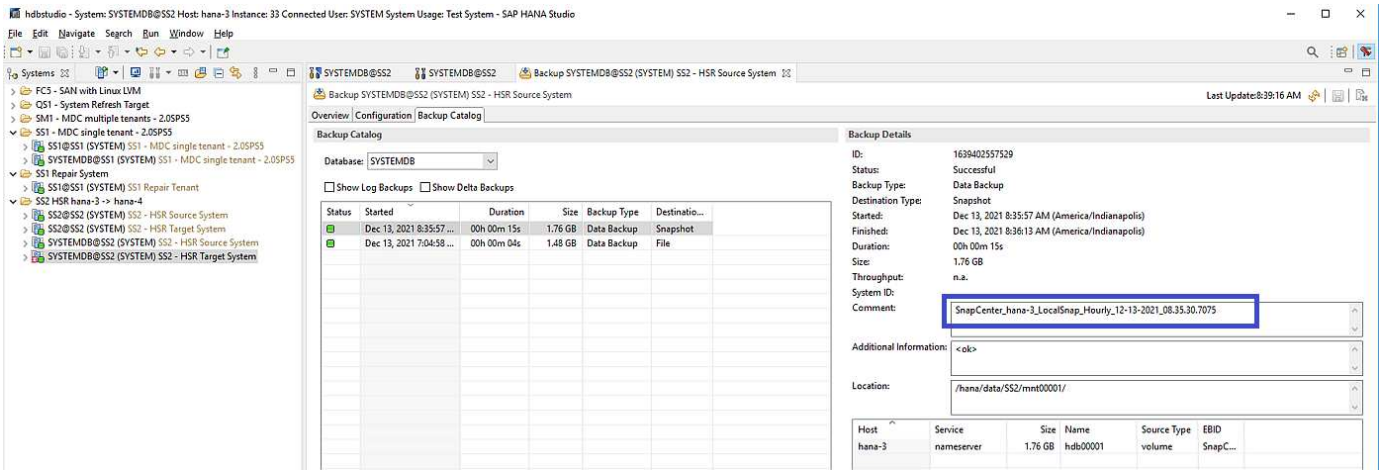
Le journal des tâches SnapCenter affiche l'opération d'identification et l'exécution de la sauvegarde sur l'hôte principal actuel hana-3.



Une sauvegarde Snapshot a été créée au niveau de la ressource HANA principale. Le nom d'hôte inclus dans le nom de la sauvegarde indique hana-3.

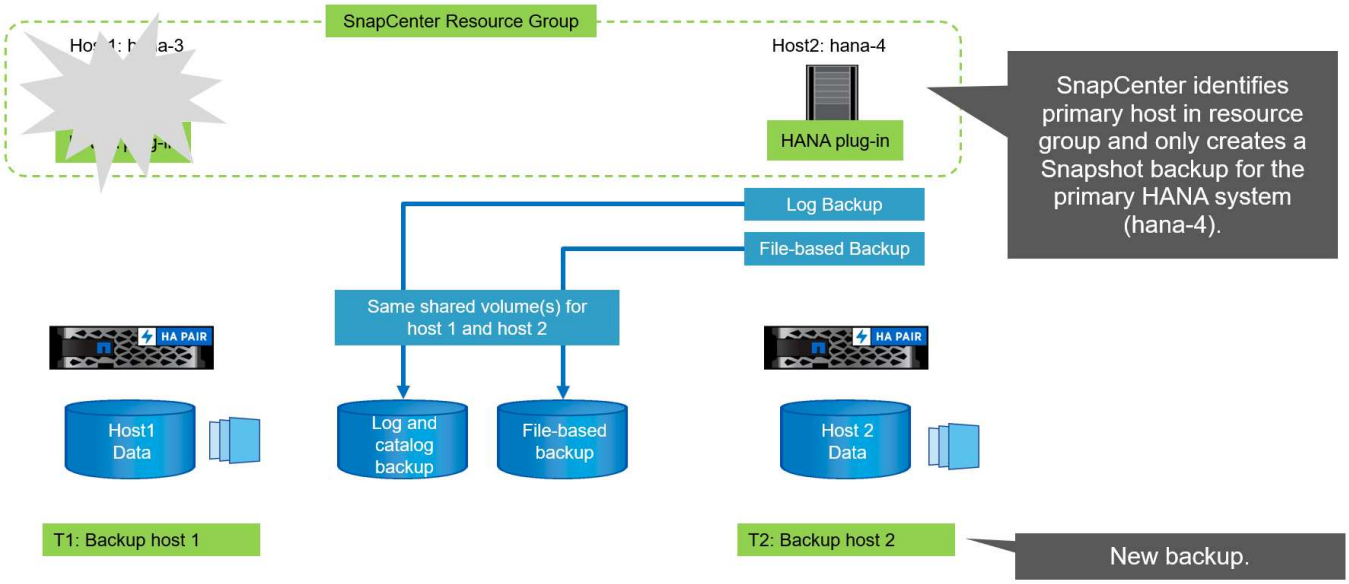


La même sauvegarde Snapshot est également visible dans le catalogue des sauvegardes HANA.

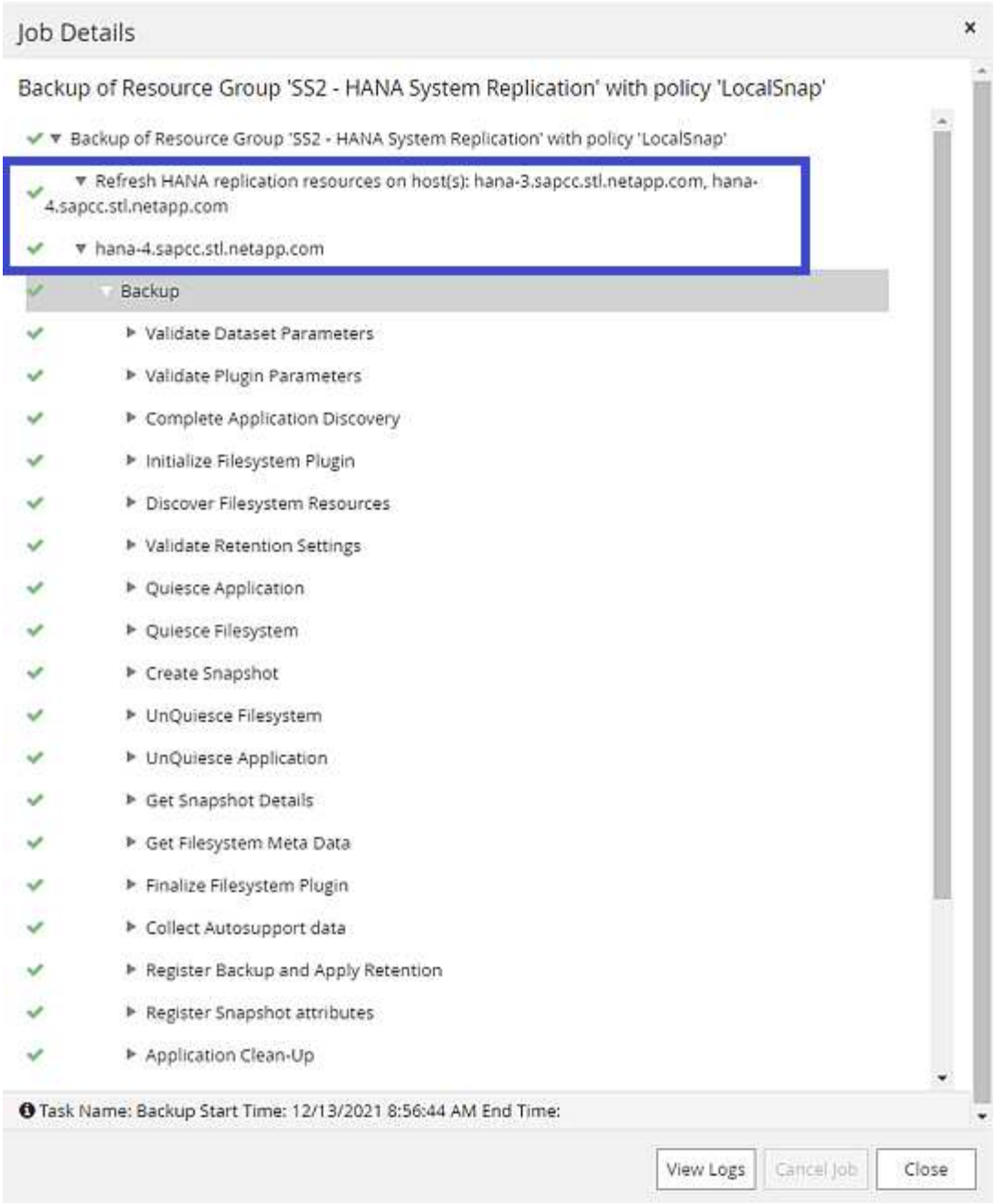


Lors de l'exécution d'une opération de basculement, d'autres sauvegardes SnapCenter identifient désormais l'ancien hôte secondaire (hana-4) comme hôte principal et l'opération de sauvegarde est exécutée sur hana-4. Là encore, seul le volume de données du nouvel hôte principal (hana-4) est snapshotted.

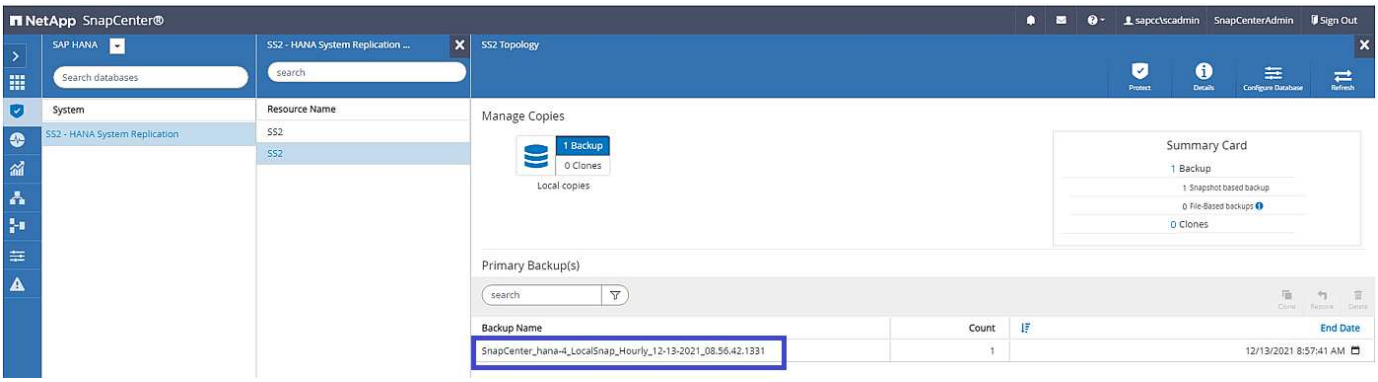
> La logique d'identification SnapCenter couvre uniquement les scénarios dans lesquels les hôtes HANA font partie d'une relation primaire-secondaire ou lorsque l'un des hôtes HANA est hors ligne.



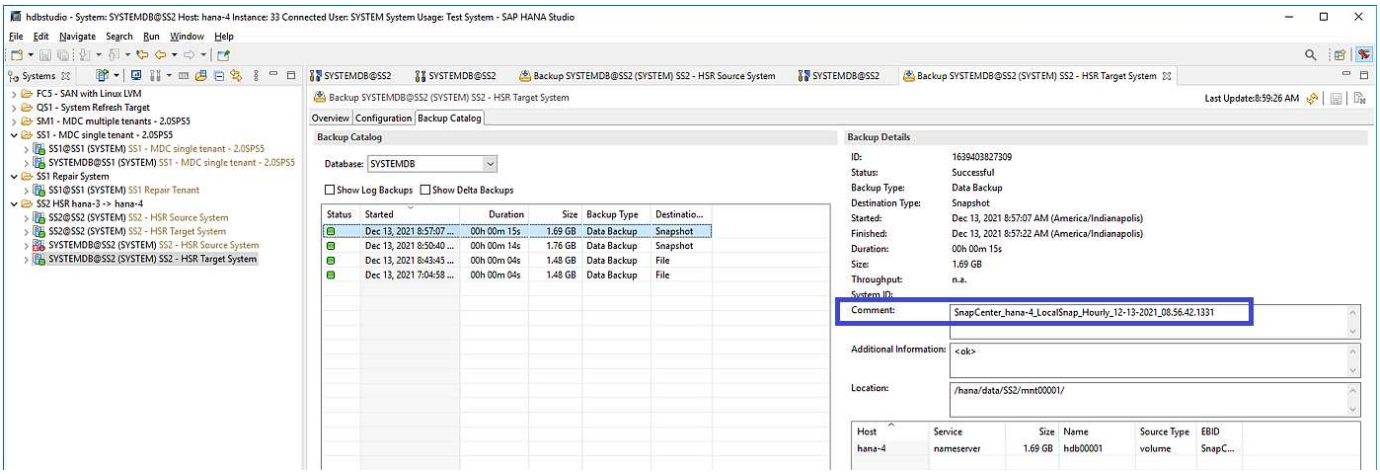
Le journal des tâches SnapCenter affiche l'opération d'identification et l'exécution de la sauvegarde sur l'hôte principal actuel hana-4.



Une sauvegarde Snapshot a été créée au niveau de la ressource HANA principale. Le nom d'hôte inclus dans le nom de la sauvegarde indique hana-4.



La même sauvegarde Snapshot est également visible dans le catalogue des sauvegardes HANA.



Opérations de contrôle de l'intégrité des blocs avec les sauvegardes basées sur des fichiers

SnapCenter 4.6 utilise la même logique que celle décrite pour les opérations de sauvegarde de Snapshot dans le cadre des opérations de vérification de l'intégrité des blocs avec des sauvegardes basées sur des fichiers. SnapCenter identifie l'hôte HANA principal actuel et exécute la sauvegarde basée sur les fichiers pour cet hôte. La gestion de la conservation s'effectue également sur les deux hôtes, de sorte que la sauvegarde la plus ancienne soit supprimée, quel que soit l'hôte utilisé actuellement comme système primaire.

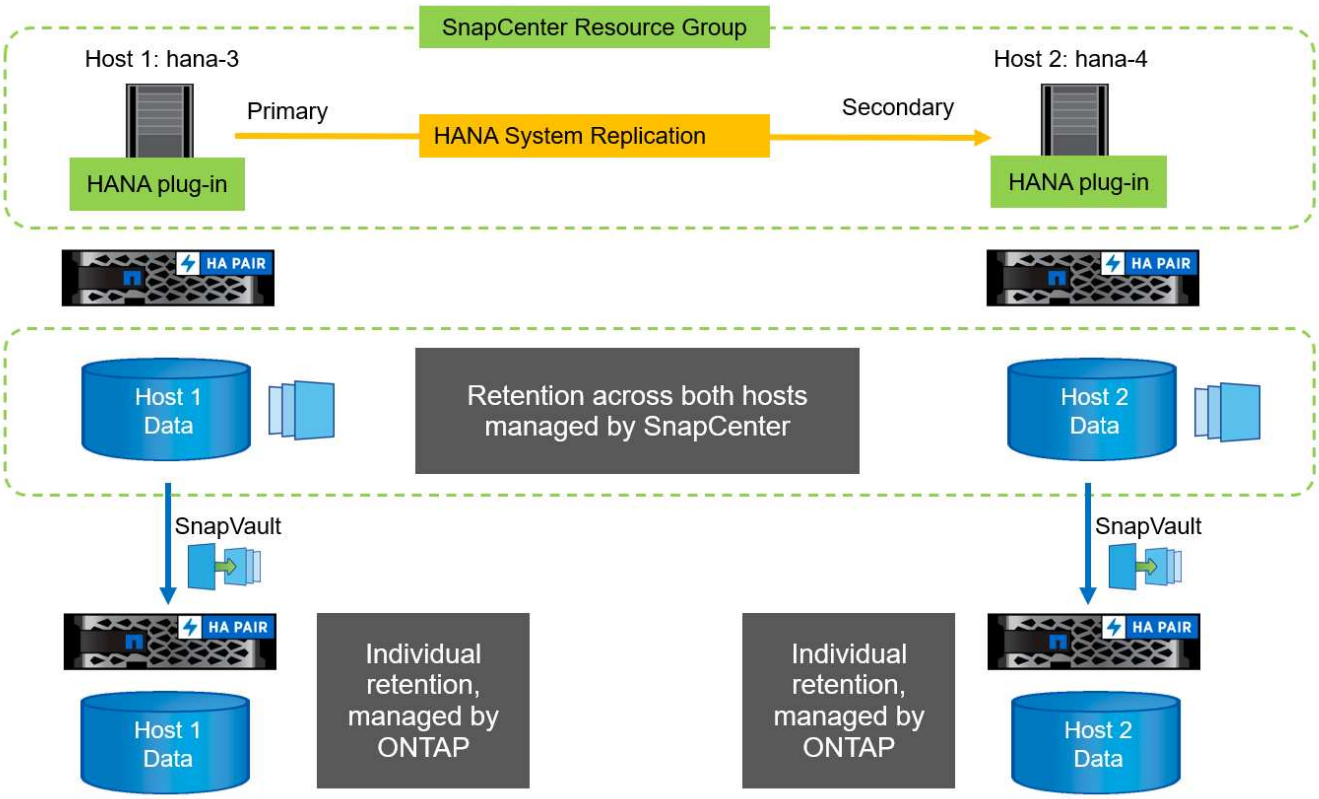
Réplication SnapVault

Pour permettre des opérations de sauvegarde transparentes sans interaction manuelle en cas de basculement et quel hôte HANA est actuellement l'hôte primaire, vous devez configurer une relation SnapVault pour les volumes de données des deux hôtes. SnapCenter exécute une opération de mise à jour SnapVault pour l'hôte principal actuel à chaque sauvegarde.

> Si un basculement vers l'hôte secondaire n'est pas effectué pendant une longue période, le nombre de blocs modifiés pour la première mise à jour SnapVault sur l'hôte secondaire sera élevé.

La gestion des durées de conservation de la cible SnapVault est gérée en dehors de SnapCenter par ONTAP, la conservation ne peut pas être gérée entre les deux hôtes HANA. Les sauvegardes créées avant le basculement ne sont donc pas supprimées avec les opérations de sauvegarde de l'ancien système secondaire. Ces sauvegardes restent tant que l'ancien système primaire n'est pas de nouveau primaire. Pour ne pas bloquer la gestion des durées de conservation des sauvegardes des journaux, ces sauvegardes doivent être supprimées manuellement au niveau de la cible SnapVault ou dans le catalogue de sauvegardes HANA.

> Un nettoyage de toutes les copies SnapVault Snapshot n'est pas possible, car une copie Snapshot est bloquée en tant que point de synchronisation. Si vous devez également supprimer la dernière copie Snapshot, la relation de réplication SnapVault doit être supprimée. Dans ce cas, NetApp recommande de supprimer les sauvegardes du catalogue de sauvegardes HANA pour débloquer la gestion de la conservation des sauvegardes de journaux.



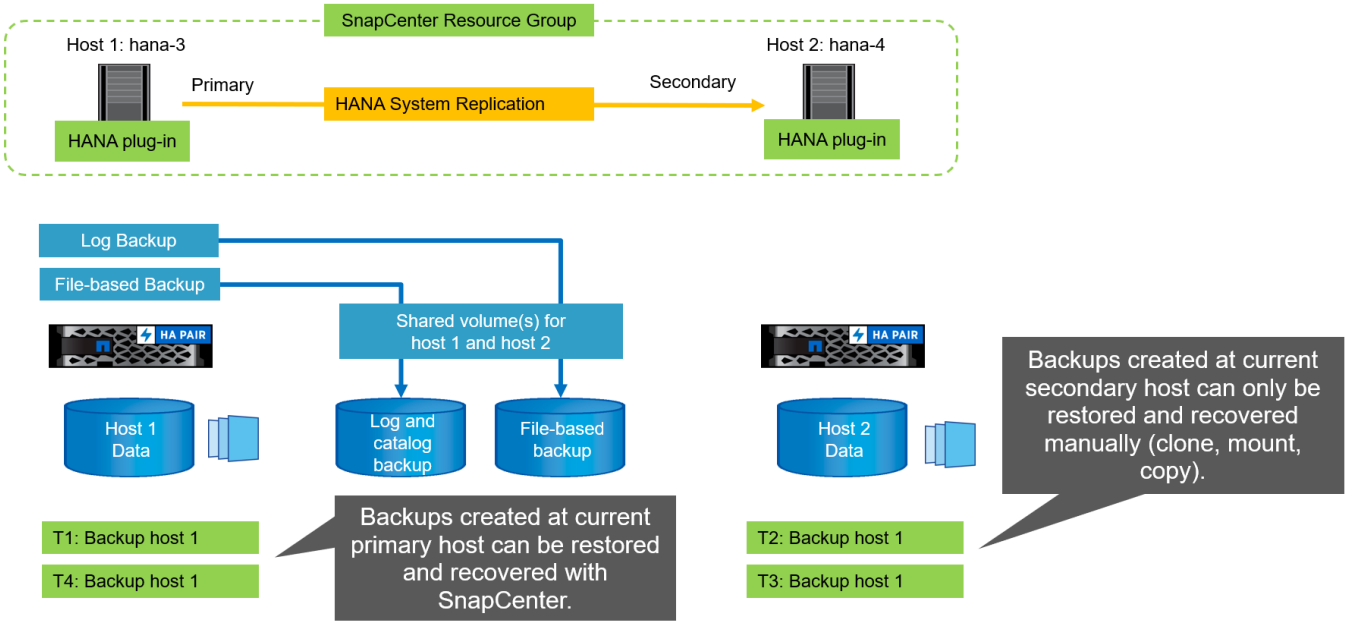
La gestion de la conservation

SnapCenter 4.6 gère la conservation pour les sauvegardes Snapshot, les opérations de contrôle de l'intégrité des blocs, les entrées du catalogue de sauvegardes HANA et les sauvegardes de journaux (s'ils ne sont pas désactivés) entre les deux hôtes HANA, ce qui n'importe quel hôte est actuellement principal ou secondaire. Les sauvegardes (données et journaux) et les entrées du catalogue HANA sont supprimées en fonction de la conservation définie, que la suppression soit nécessaire sur l'hôte principal ou secondaire actuel. En d'autres termes, aucune interaction manuelle n'est requise si une opération de basculement est effectuée et/ou si la réplication est configurée dans l'autre direction.

Si la réplication SnapVault fait partie de la stratégie de protection des données, une interaction manuelle est nécessaire pour des scénarios spécifiques, comme décrit dans la section [SnapVault Replication].

Restauration et reprise

La figure suivante représente un scénario dans lequel plusieurs sauvegardes Snapshot ont été exécutées sur les deux sites. Avec le statut actuel, l'hôte hana-3 est l'hôte principal et la dernière sauvegarde est T4, qui a été créée à l'hôte hana-3. Si vous devez effectuer une opération de restauration et de récupération, les sauvegardes T1 et T4 sont disponibles pour la restauration et la récupération dans SnapCenter. Les sauvegardes, qui ont été créées sur l'hôte hana-4 (T2, T3), ne peuvent pas être restaurées à l'aide de SnapCenter. Ces sauvegardes doivent être copiées manuellement vers le volume de données hana-3 à des fins de restauration.



Les opérations de restauration et de récupération d'une configuration de groupes de ressources SnapCenter 4.6 sont identiques à celles d'une configuration de réplication non système autodécouverte. Toutes les options de restauration et de récupération automatisée sont disponibles. Pour plus d'informations, consultez le rapport technique "Tr-4614 : sauvegarde et restauration SAP HANA avec SnapCenter".

Une opération de restauration à partir d'une sauvegarde créée sur l'autre hôte est décrite dans la section "Restauration à partir d'une sauvegarde créée sur l'autre hôte".

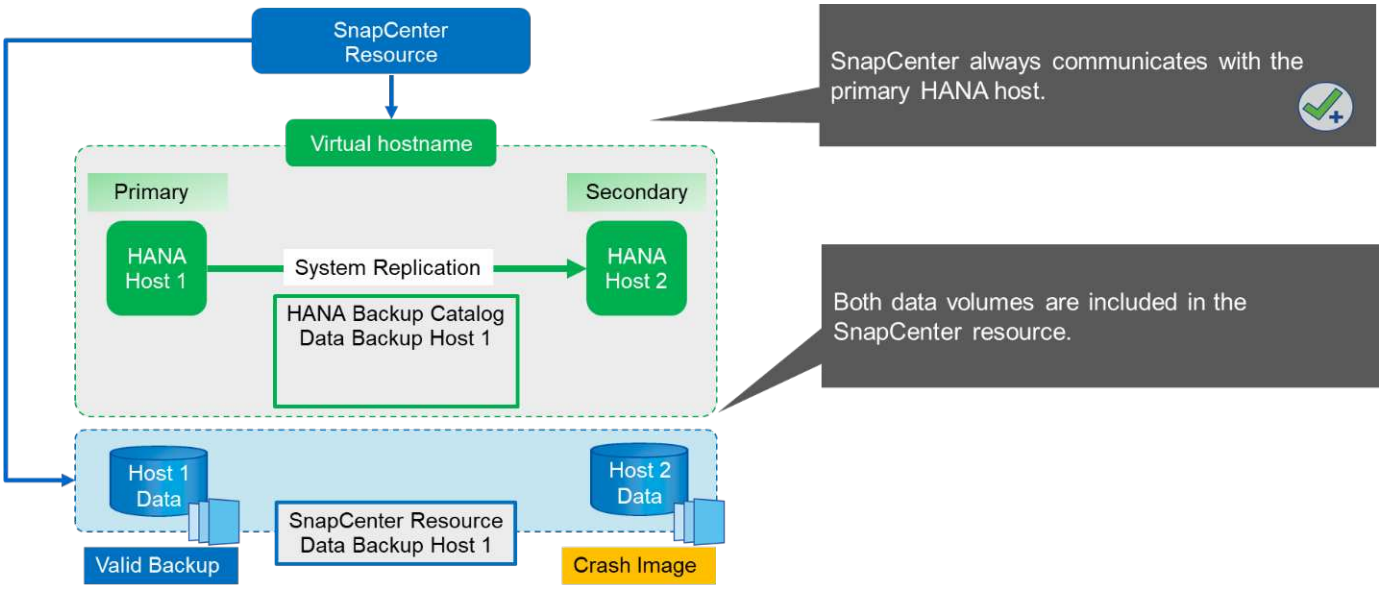
Configuration SnapCenter avec une seule ressource

Une ressource SnapCenter est configurée avec l'adresse IP virtuelle (nom d'hôte) de l'environnement de réplication système HANA. Avec cette approche, SnapCenter communique toujours avec l'hôte principal, que l'hôte 1 ou l'hôte 2 soit principal. Les volumes de données des deux hôtes SAP HANA sont inclus dans la ressource SnapCenter.

Nous supposons que l'adresse IP virtuelle est toujours liée à l'hôte SAP HANA principal. Le basculement de l'adresse IP virtuelle est effectué en dehors de SnapCenter dans le cadre du workflow de basculement de réplication du système HANA.

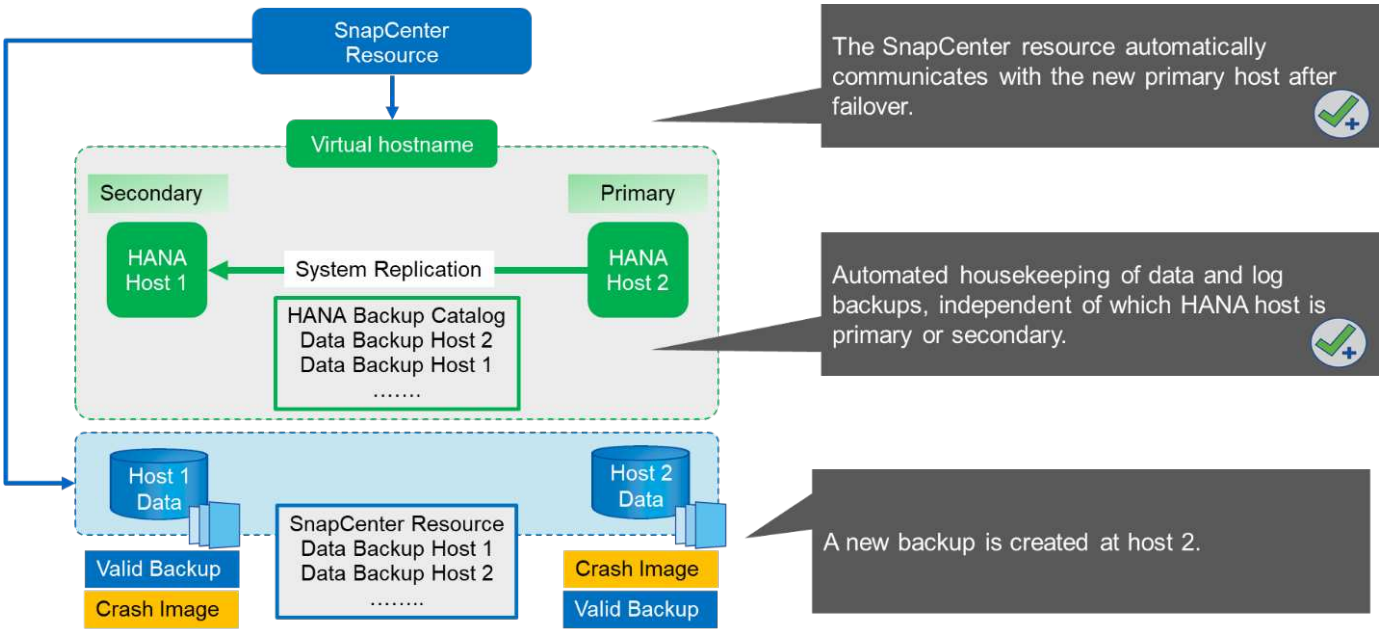
Lors de l'exécution d'une sauvegarde avec l'hôte 1 comme hôte principal, une sauvegarde Snapshot cohérente avec la base de données est créée au niveau du volume de données de l'hôte 1. Le volume de données de l'hôte 2 faisant partie de la ressource SnapCenter, une autre copie Snapshot est créée pour ce volume. Cette copie Snapshot n'est pas cohérente avec la base de données. Il s'agit plutôt d'une image de panne de l'hôte secondaire.

Le catalogue de sauvegardes SAP HANA et la ressource SnapCenter comprennent la sauvegarde créée à l'hôte 1.



La figure suivante montre l'opération de sauvegarde après le basculement vers l'hôte 2 et la réplication de l'hôte 2 vers l'hôte 1. SnapCenter communique automatiquement avec l'hôte 2 en utilisant l'adresse IP virtuelle configurée dans la ressource SnapCenter. Les sauvegardes sont maintenant créées sur l'hôte 2. Deux copies Snapshot sont créées par SnapCenter : une sauvegarde cohérente avec la base de données au niveau du volume de données de l'hôte 2 et une copie Snapshot d'image de panne au niveau du volume de données de l'hôte 1. Le catalogue de sauvegardes SAP HANA et la ressource SnapCenter incluent désormais la sauvegarde créée sur l'hôte 1 et la sauvegarde créée sur l'hôte 2.

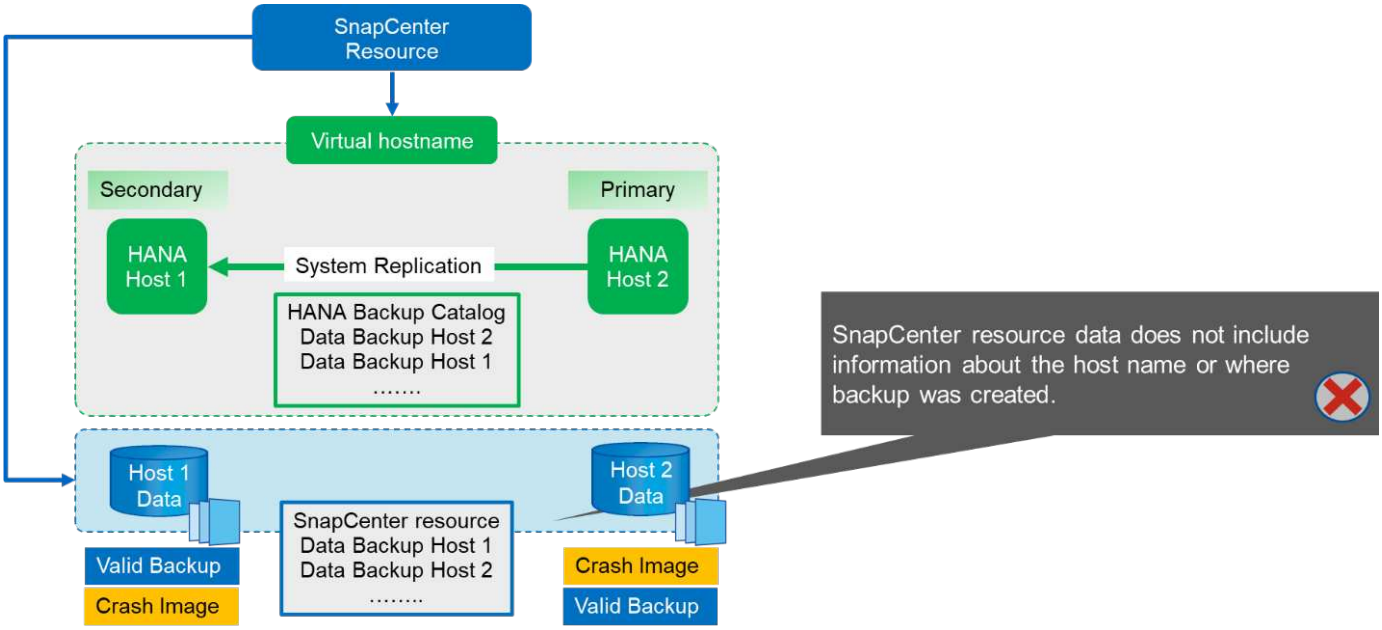
La gestion des sauvegardes de données et de journaux dépend de la règle de conservation SnapCenter définie ; les sauvegardes sont supprimées, quel que soit l'hôte principal ou secondaire.



Comme indiqué dans la section "Sauvegardes Snapshot de stockage et réplication système SAP", Une opération de restauration avec des sauvegardes Snapshot basées sur le stockage est différente, selon la sauvegarde à restaurer. Il est important d'identifier l'hôte sur lequel la sauvegarde a été créée pour déterminer si la restauration peut être effectuée sur le volume de stockage local, ou si la restauration doit être effectuée sur le volume de stockage de l'autre hôte.

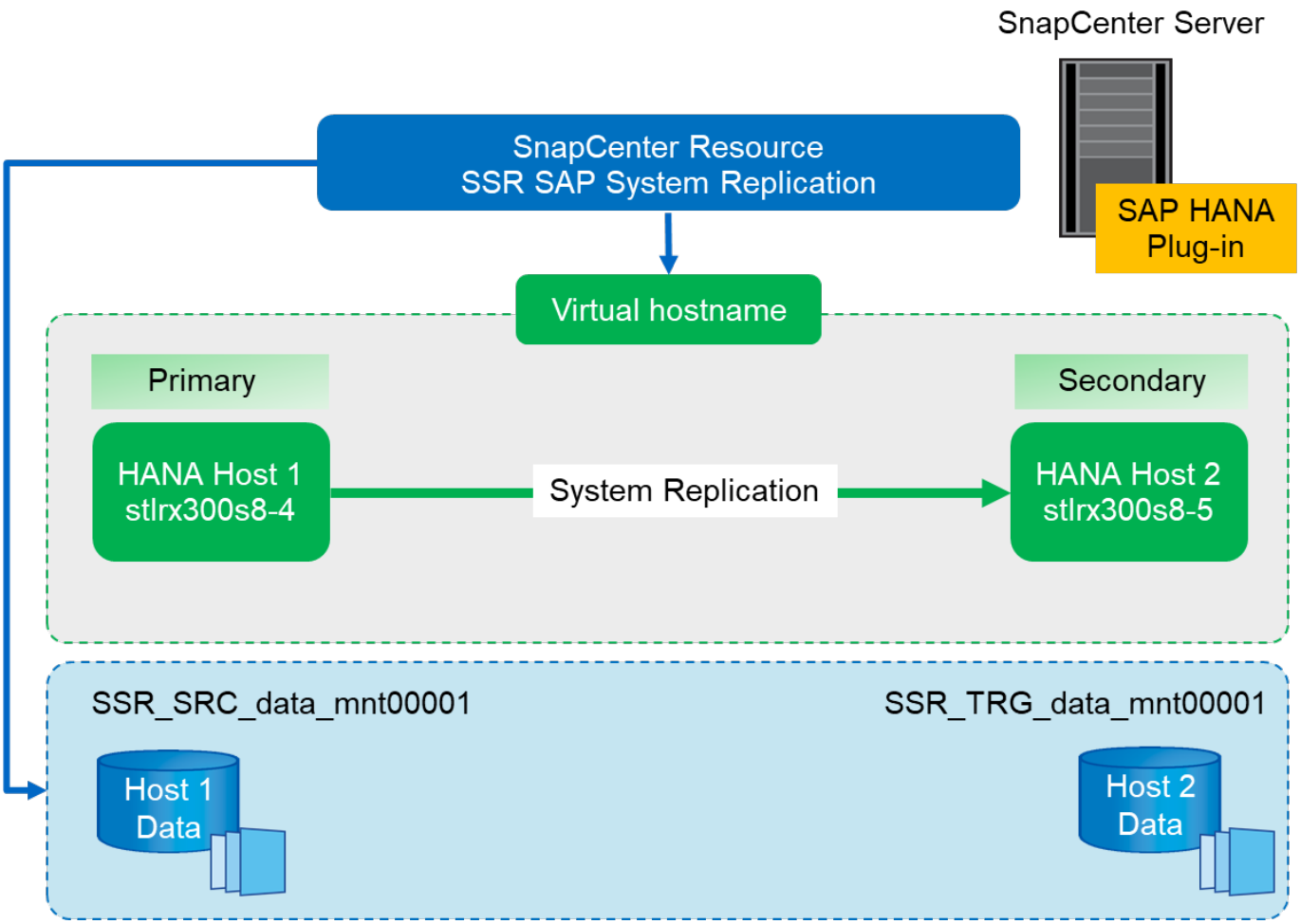
Avec la configuration SnapCenter à ressource unique, SnapCenter ne sait pas où la sauvegarde a été créée. NetApp vous recommande donc d'ajouter un script de présauvegarde au workflow de sauvegarde SnapCenter pour identifier l'hôte qui est actuellement le principal hôte SAP HANA.

La figure suivante décrit l'identification de l'hôte de sauvegarde.



Configuration SnapCenter

La figure suivante présente la configuration du laboratoire et un aperçu de la configuration SnapCenter requise.



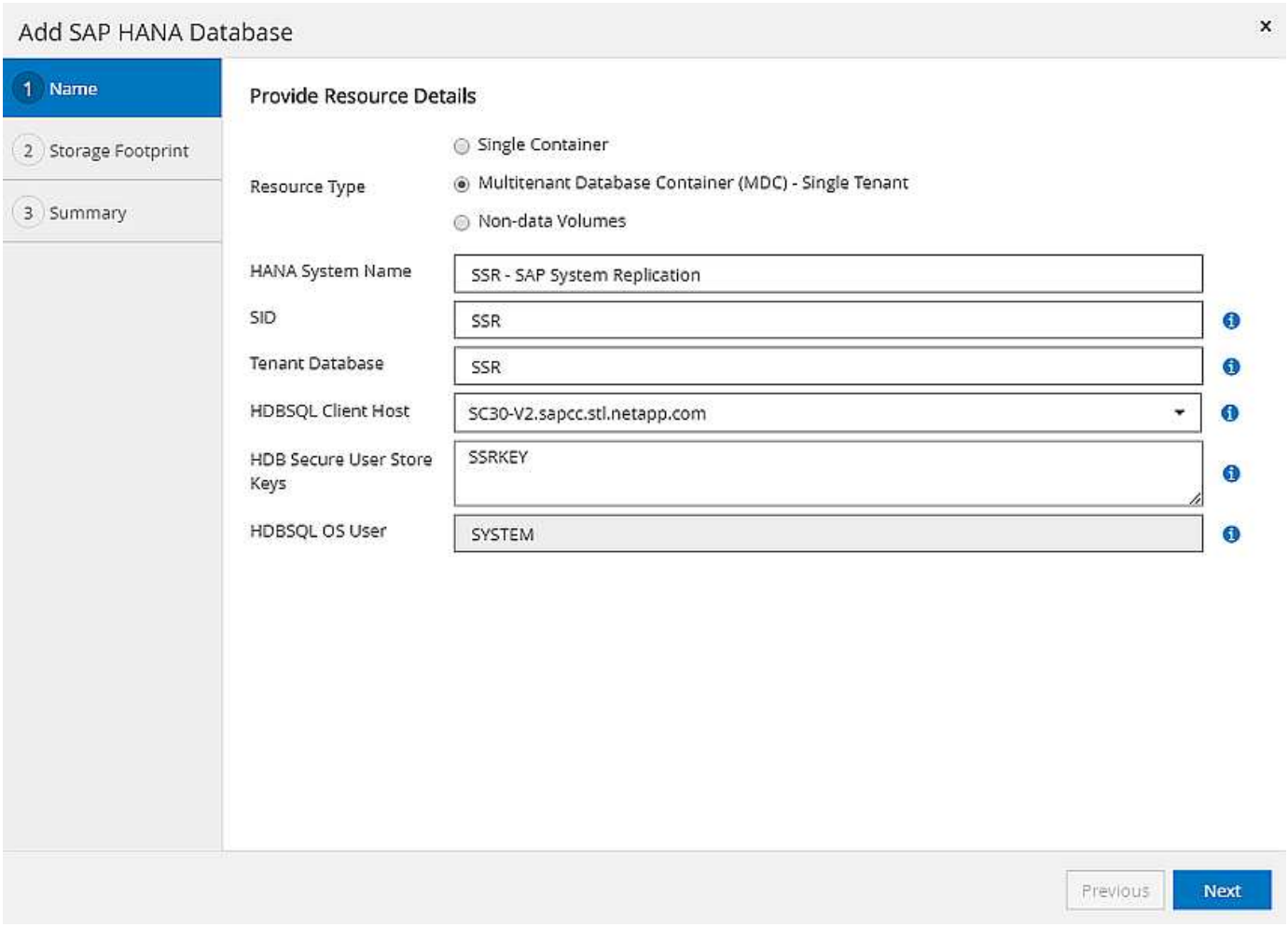
Pour effectuer des opérations de sauvegarde, quel que soit l'hôte SAP HANA principal et même lorsqu'un hôte est en panne, le plug-in SnapCenter SAP HANA doit être déployé sur un hôte plug-in central. Dans notre configuration de laboratoire, nous avons utilisé le serveur SnapCenter comme plug-in central, et nous avons déployé le plug-in SAP HANA sur le serveur SnapCenter.

Un utilisateur a été créé dans la base de données HANA pour effectuer des opérations de sauvegarde. Une clé de magasin utilisateur a été configurée au niveau du serveur SnapCenter sur lequel le plug-in SAP HANA a été installé. La clé de magasin utilisateur inclut l'adresse IP virtuelle des hôtes de réplication système SAP HANA (`ssr-vip`).

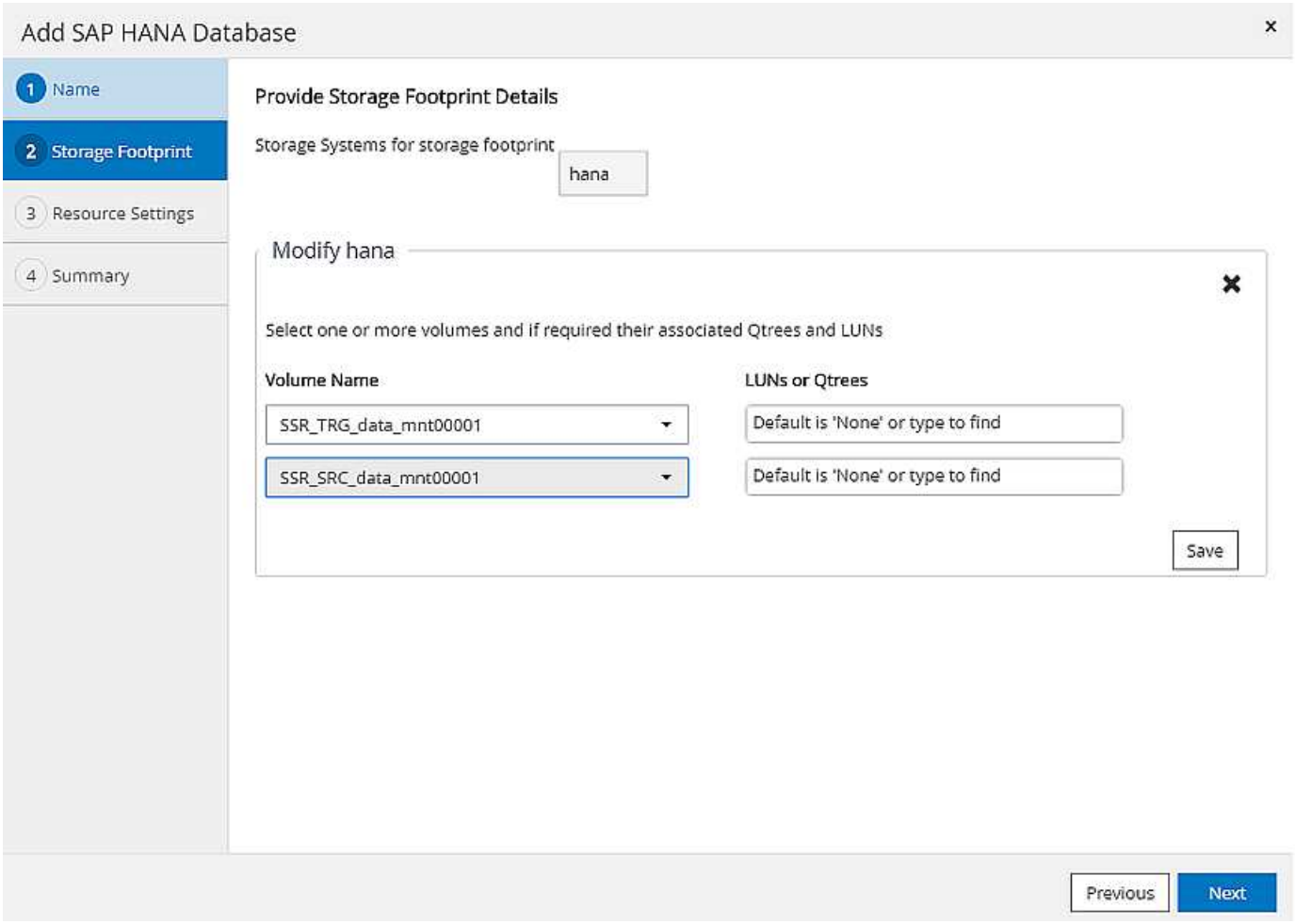
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Pour plus d'informations sur les options de déploiement du plug-in SAP HANA et la configuration des magasins d'utilisateurs, consultez le rapport technique TR-4614 : "SAP HANA : sauvegarde et restauration avec SnapCenter".

Dans SnapCenter, la ressource est configurée comme indiqué dans la figure suivante en utilisant la clé de stockage utilisateur, configurée avant, et le serveur SnapCenter comme `hdbsql` hôte de communication.

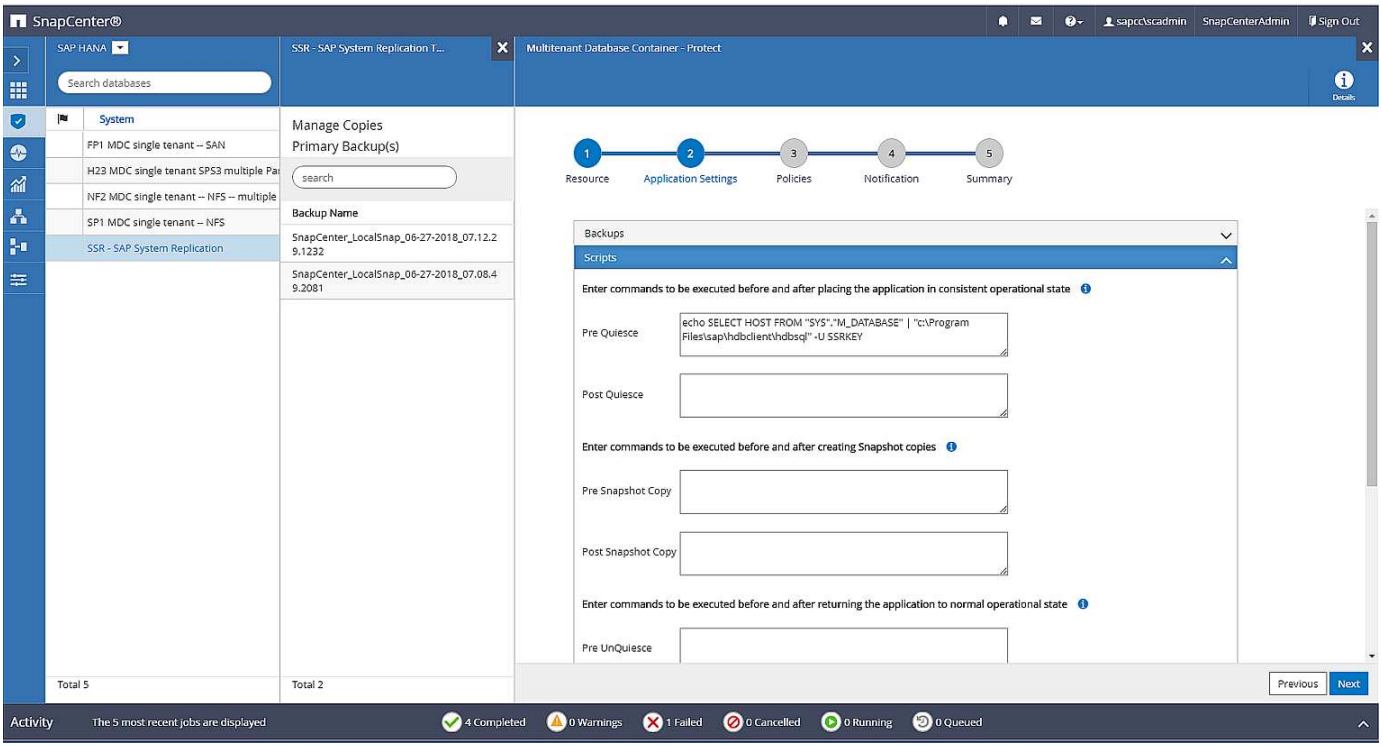


Les volumes de données des deux hôtes SAP HANA sont inclus dans la configuration de l'empreinte du stockage, comme le montre la figure suivante.



Comme indiqué précédemment, SnapCenter ne sait pas où la sauvegarde a été créée. NetApp vous recommande donc d'ajouter un script de pré-sauvegarde dans le workflow de sauvegarde SnapCenter pour identifier l'hôte qui est actuellement l'hôte SAP HANA principal. Vous pouvez effectuer cette identification à l'aide d'une instruction SQL ajoutée au flux de travail de sauvegarde, comme le montre la figure suivante.

```
Select host from "SYS".M_DATABASE
```

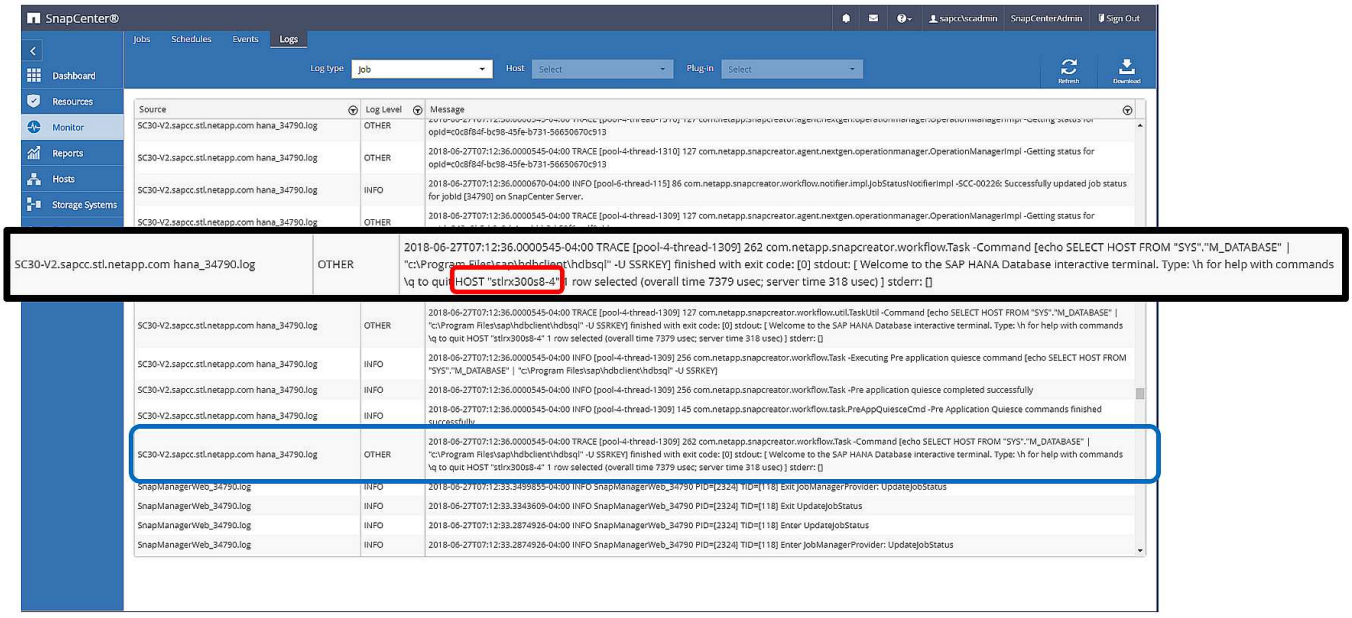


Opération de sauvegarde SnapCenter

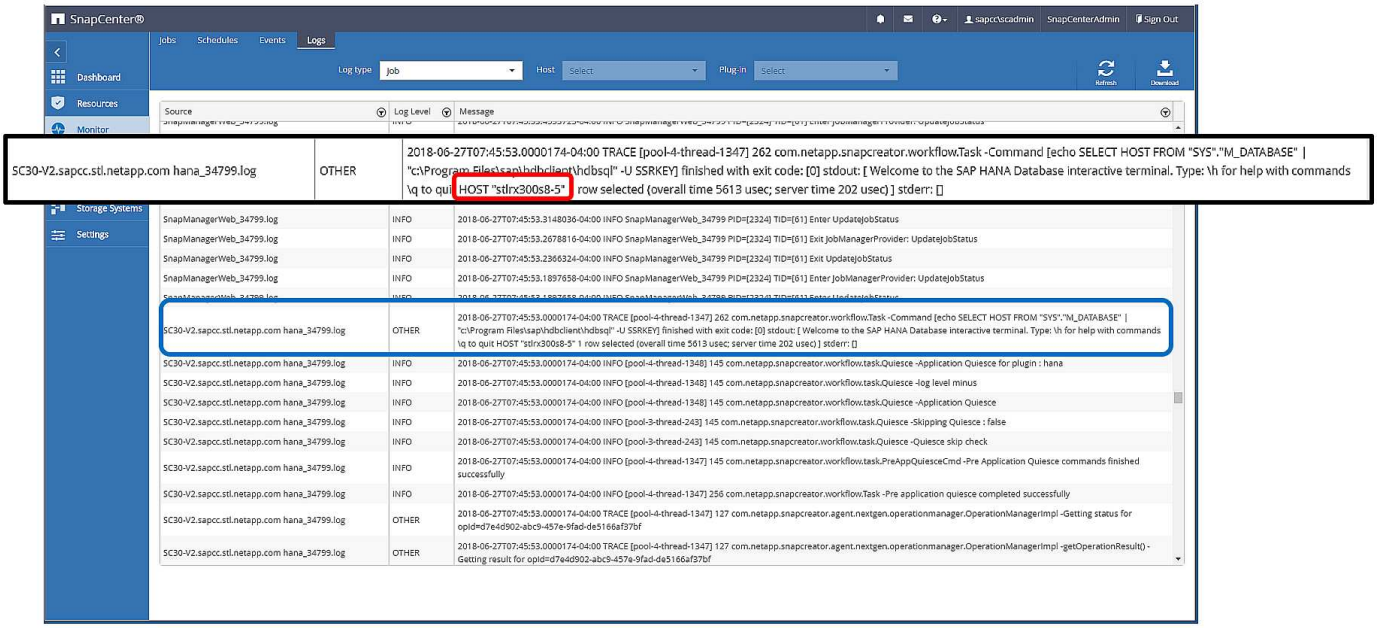
Les opérations de sauvegarde sont désormais exécutées normalement. L'organisation des sauvegardes des données et des journaux est indépendante desquelles l'hôte SAP HANA est primaire ou secondaire.

Les journaux des tâches de sauvegarde incluent la sortie de l'instruction SQL, qui vous permet d'identifier l'hôte SAP HANA où la sauvegarde a été créée.

La figure suivante montre le journal des tâches de sauvegarde avec l'hôte 1 comme hôte principal.

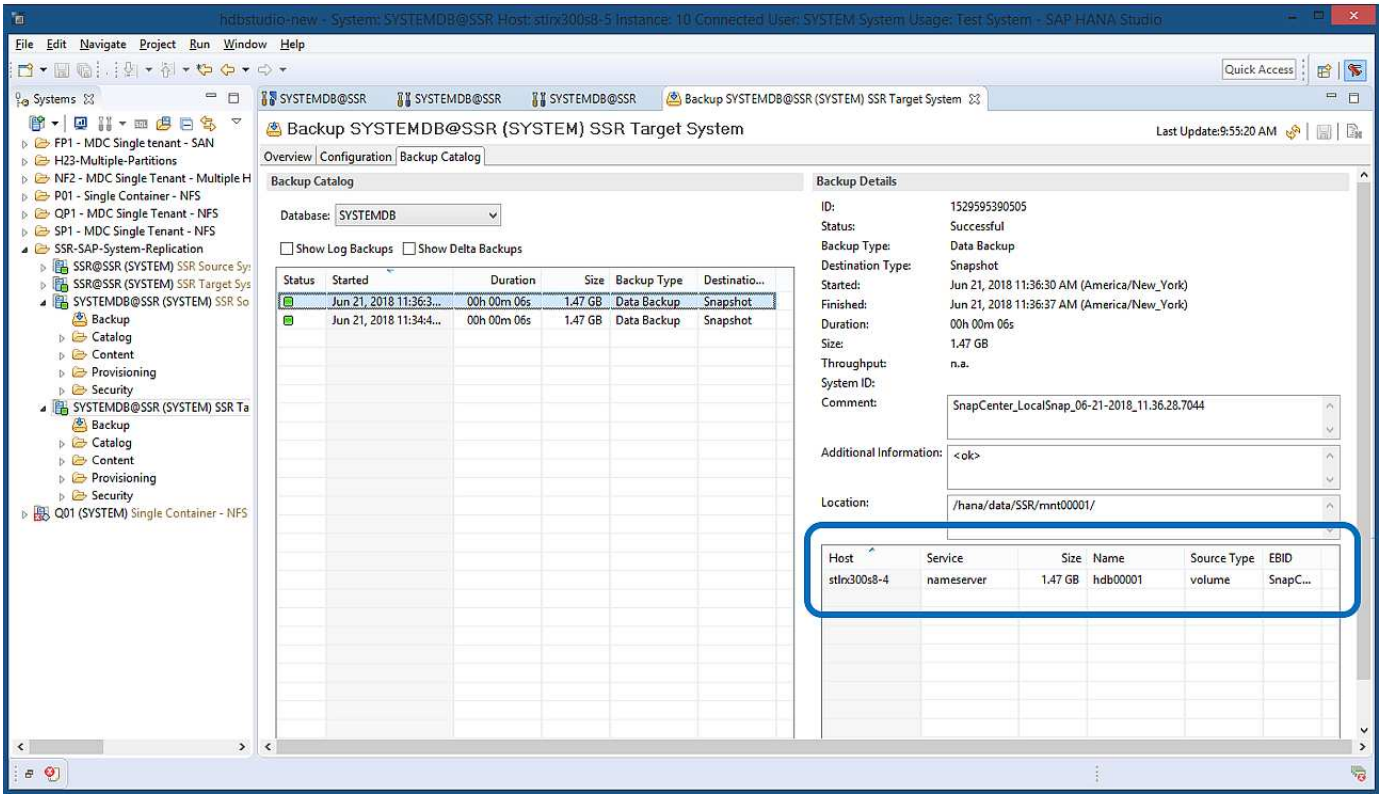


Cette figure illustre le journal des tâches de sauvegarde avec l'hôte 2 comme hôte principal.



La figure suivante présente le catalogue des sauvegardes SAP HANA dans SAP HANA Studio. Lorsque la base de données SAP HANA est en ligne, l'hôte SAP HANA sur lequel la sauvegarde a été créée est visible dans SAP HANA Studio.

Le catalogue de sauvegardes SAP HANA sur le système de fichiers, utilisé lors d'une opération de restauration et de restauration, n'inclut pas le nom d'hôte sur lequel la sauvegarde a été créée. La seule façon d'identifier l'hôte lorsque la base de données est en panne est de combiner les entrées du catalogue de sauvegarde avec le `backup.log` Fichier des deux hôtes SAP HANA.



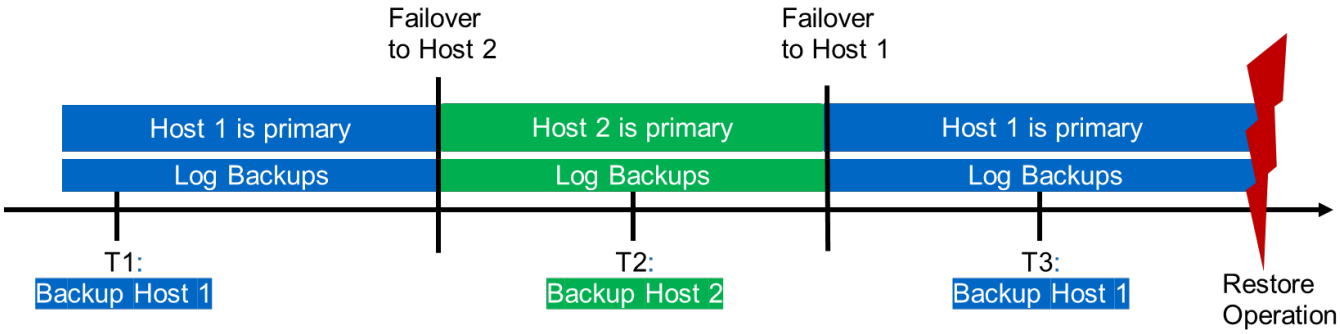
Restauration et reprise

Comme indiqué précédemment, vous devez être en mesure d'identifier l'emplacement de création de la sauvegarde sélectionnée pour définir l'opération de restauration requise. Si la base de données SAP HANA est toujours en ligne, vous pouvez utiliser SAP HANA Studio pour identifier l'hôte sur lequel la sauvegarde a été créée. Si la base de données est hors ligne, les informations sont uniquement disponibles dans le journal des tâches de sauvegarde SnapCenter.

La figure suivante illustre les différentes opérations de restauration en fonction de la sauvegarde sélectionnée.

Si une opération de restauration doit être effectuée après l'horodatage T3 et que l'hôte 1 est le primaire, vous pouvez restaurer la sauvegarde créée à T1 ou T3 à l'aide de SnapCenter. Ces sauvegardes Snapshot sont disponibles au niveau du volume de stockage rattaché à l'hôte 1.

Si vous devez restaurer à l'aide de la sauvegarde créée au niveau de l'hôte 2 (T2), qui est une copie Snapshot au niveau du volume de stockage de l'hôte 2, la sauvegarde doit être mise à disposition de l'hôte 1. Vous pouvez mettre cette sauvegarde à disposition en créant une copie NetApp FlexClone à partir de la sauvegarde, en montant la copie FlexClone sur l'hôte 1 et en copiant les données à l'emplacement d'origine.



Restore Operation With	
Backup T1	SnapCenter
Backup T2	Create FlexClone from „Backup host 2“, mount and copy
Backup T3	SnapCenter

Avec une configuration de ressource SnapCenter unique, des copies Snapshot sont créées au niveau des deux volumes de stockage des hôtes de réplication système SAP HANA. Seule la sauvegarde Snapshot créée au niveau du volume de stockage de l'hôte SAP HANA principal peut être utilisée pour la restauration suivante. La copie Snapshot créée au niveau du volume de stockage de l'hôte SAP HANA secondaire est une image de panne qui ne peut pas être utilisée pour la restauration avant.

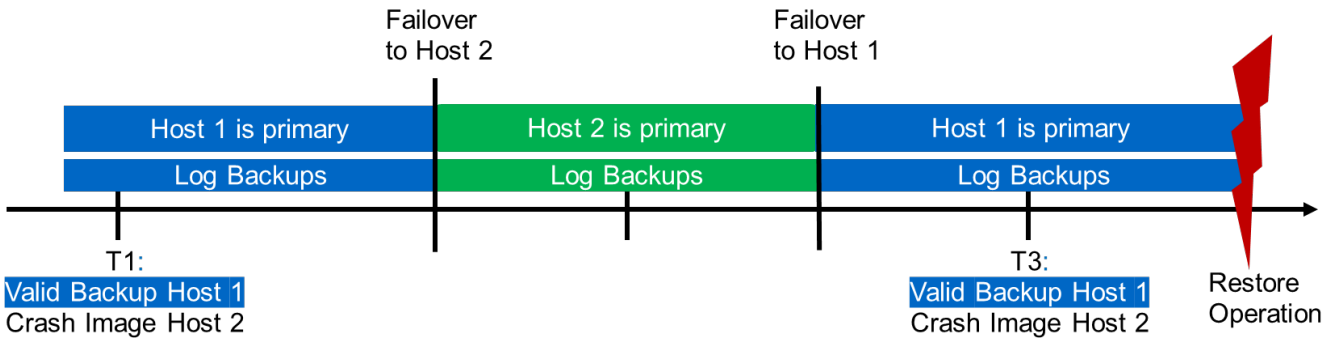
Vous pouvez effectuer une opération de restauration avec SnapCenter de deux manières différentes :

- Restaurez uniquement la sauvegarde valide
- Restaurer la ressource complète, y compris la sauvegarde valide et l'image de planeLes sections suivantes décrivent plus en détail les deux opérations de restauration différentes.

Une opération de restauration à partir d'une sauvegarde créée sur l'autre hôte est décrite dans la section "Restauration à partir d'une sauvegarde créée sur l'autre hôte".

La figure suivante illustre les opérations de restauration avec une configuration de ressource SnapCenter

unique.

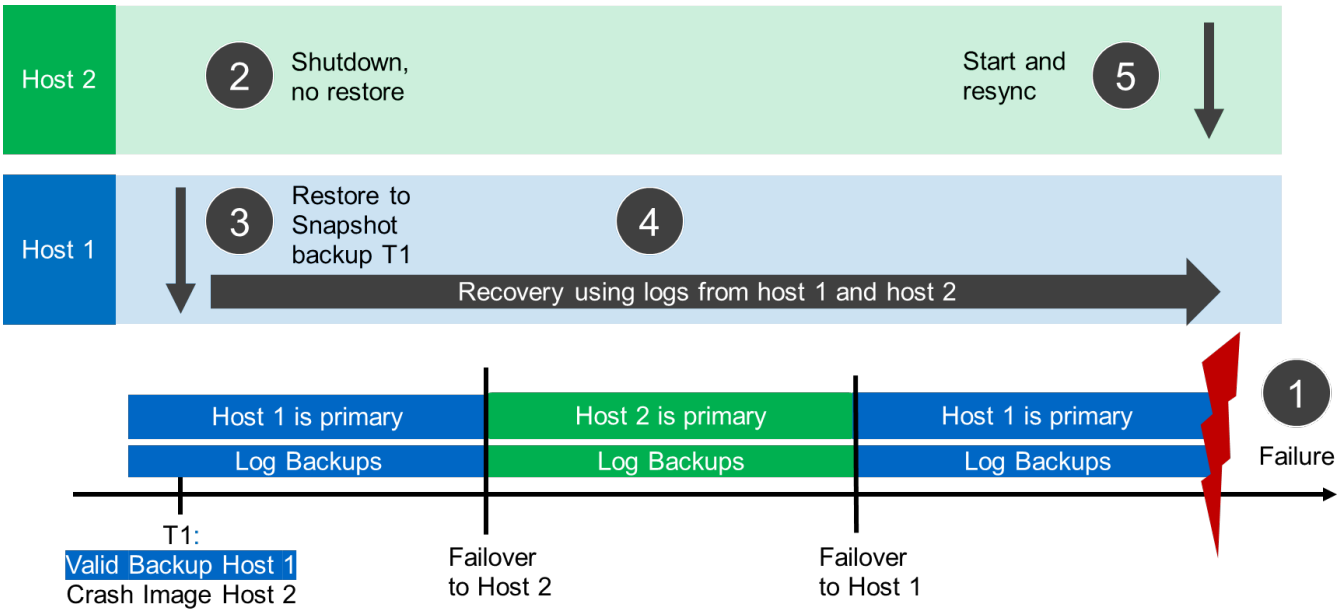


Restauration SnapCenter de la sauvegarde valide uniquement

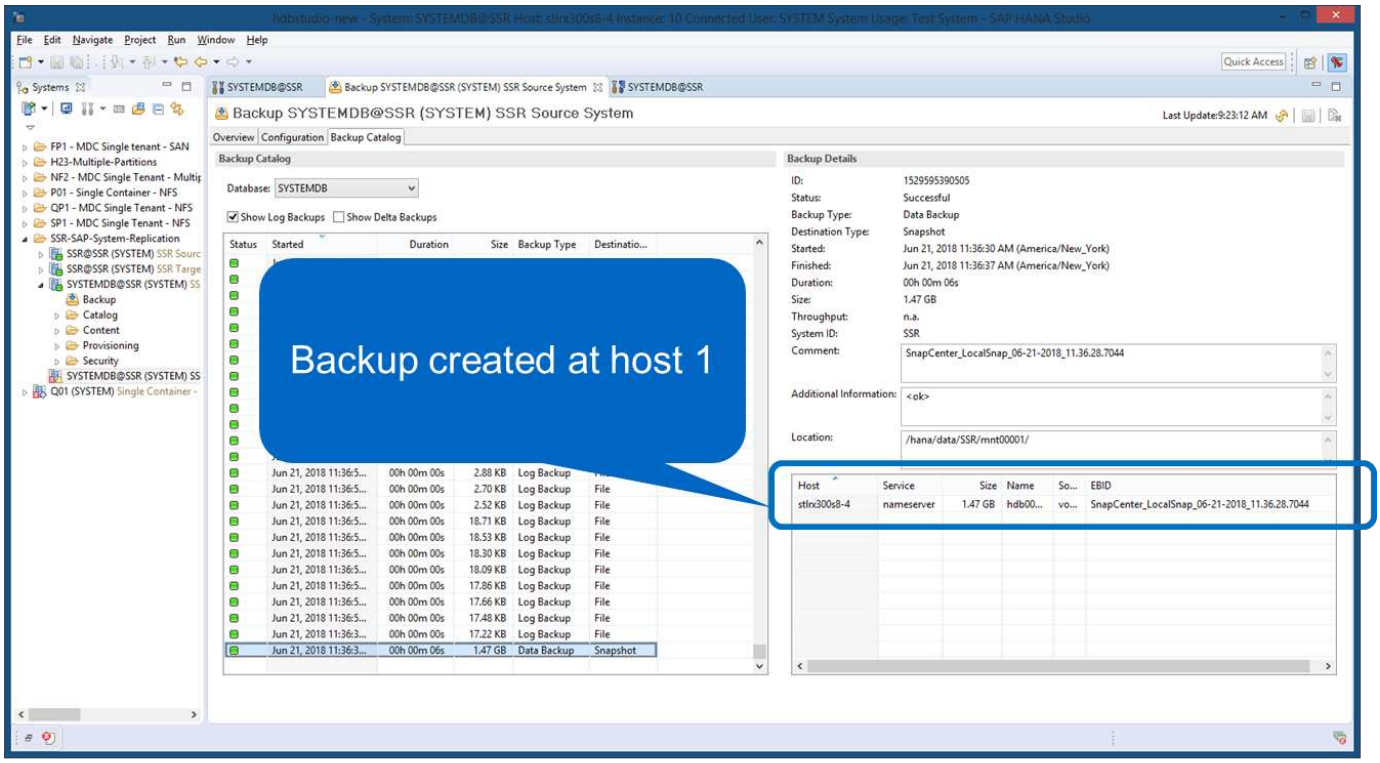
La figure suivante présente un aperçu du scénario de restauration et de récupération décrit dans cette section.

Une sauvegarde a été créée au niveau de T1 sur l'hôte 1. Un basculement a été effectué sur l'hôte 2. Après un certain point dans le temps, un autre basculement vers l'hôte 1 a été effectué. Au point actuel dans le temps, l'hôte 1 est l'hôte principal.

1. Un échec s'est produit et vous devez restaurer la sauvegarde créée sur T1 à l'hôte 1.
2. L'hôte secondaire (hôte 2) est arrêté, mais aucune opération de restauration n'est exécutée.
3. Le volume de stockage de l'hôte 1 est restauré dans la sauvegarde créée à T1.
4. Une restauration de transfert est effectuée avec des journaux de l'hôte 1 et de l'hôte 2.
5. L'hôte 2 est démarré et une resynchronisation de réplication système de l'hôte 2 est automatiquement démarrée.



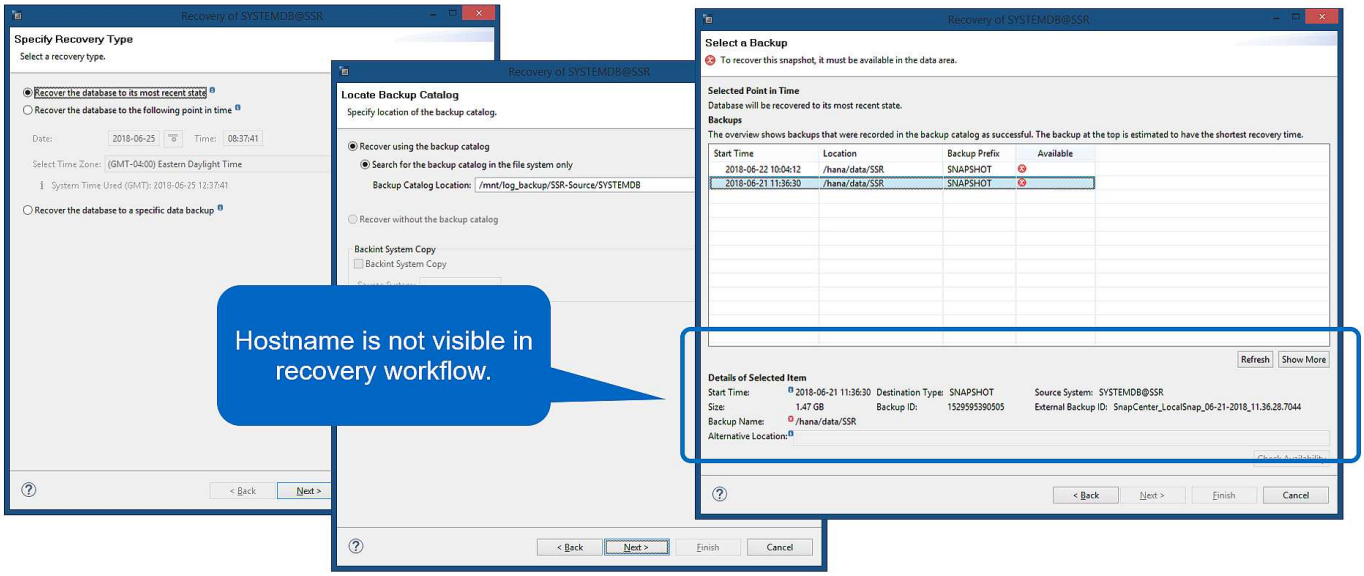
La figure suivante présente le catalogue des sauvegardes SAP HANA dans SAP HANA Studio. La sauvegarde mise en surbrillance montre la sauvegarde créée au niveau de T1 sur l'hôte 1.



25

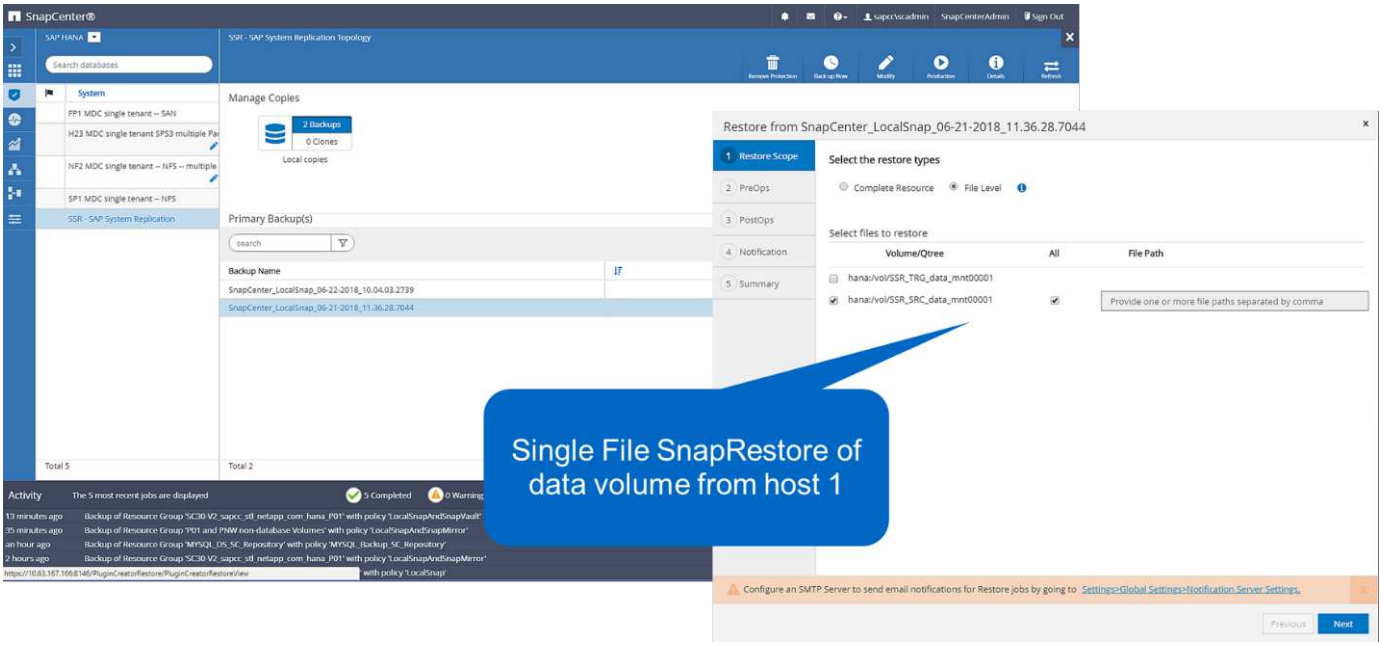
Une opération de restauration et de reprise est lancée dans SAP HANA Studio. Comme le montre la figure suivante, le nom de l'hôte sur lequel la sauvegarde a été créée n'est pas visible dans le workflow de restauration et de reprise.

Dans notre scénario de test, nous avons pu identifier la sauvegarde appropriée (la sauvegarde créée sur l'hôte 1) dans SAP HANA Studio lorsque la base de données était toujours en ligne. Si la base de données n'est pas disponible, vous devez consulter le journal des tâches de sauvegarde SnapCenter pour identifier la sauvegarde adéquate.

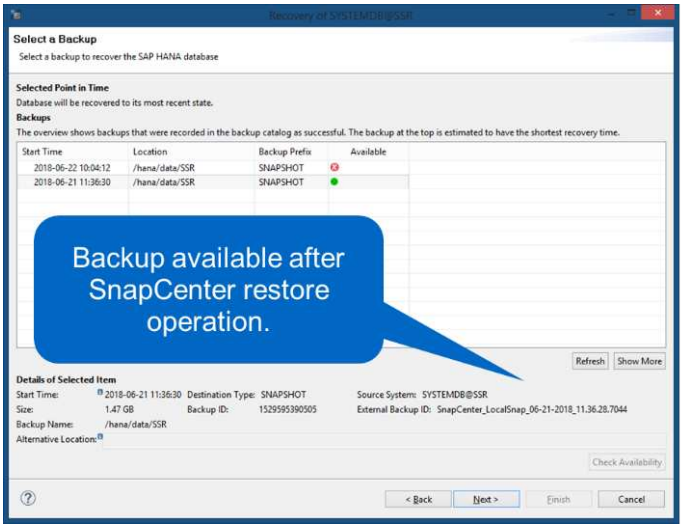


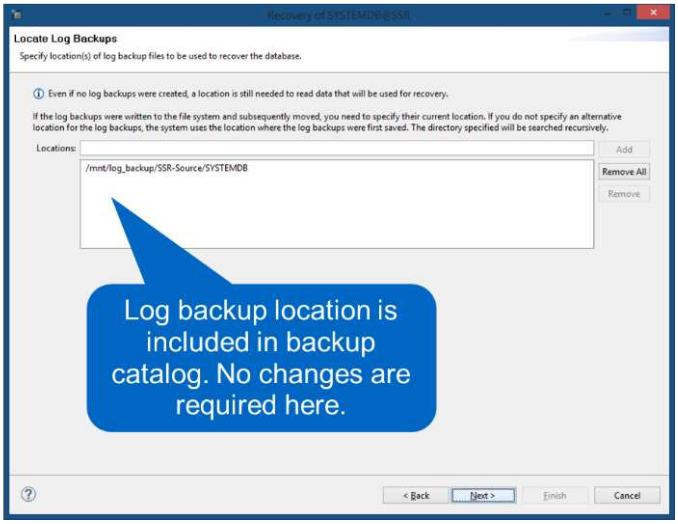
Dans SnapCenter, la sauvegarde est sélectionnée et une opération de restauration au niveau des fichiers est

effectuée. Sur l'écran de restauration au niveau des fichiers, seul le volume hôte 1 est sélectionné pour que seule la sauvegarde valide soit restaurée.



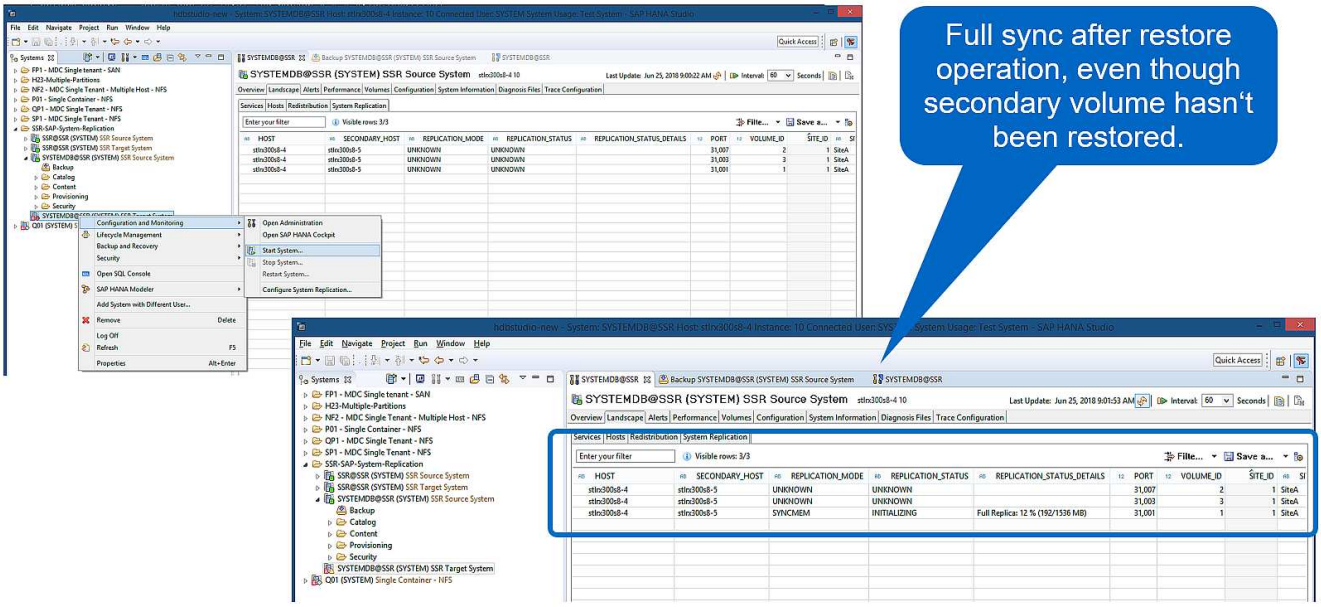
Une fois l'opération de restauration effectuée, la sauvegarde est mise en surbrillance en vert dans SAP HANA Studio. Vous n'avez pas besoin d'entrer un emplacement de sauvegarde de journal supplémentaire, car le chemin d'accès aux fichiers des sauvegardes de journaux de l'hôte 1 et de l'hôte 2 est inclus dans le catalogue de sauvegarde.





Une fois la restauration par transfert terminée, l'hôte secondaire (hôte 2) est démarré et la resynchronisation de réplication du système SAP HANA est démarrée.

Bien que l'hôte secondaire soit à jour (aucune opération de restauration n'a été effectuée pour l'hôte 2), SAP HANA exécute une réplication complète de toutes les données. Ce comportement est standard après une opération de restauration et de reprise avec la réplication système SAP HANA.

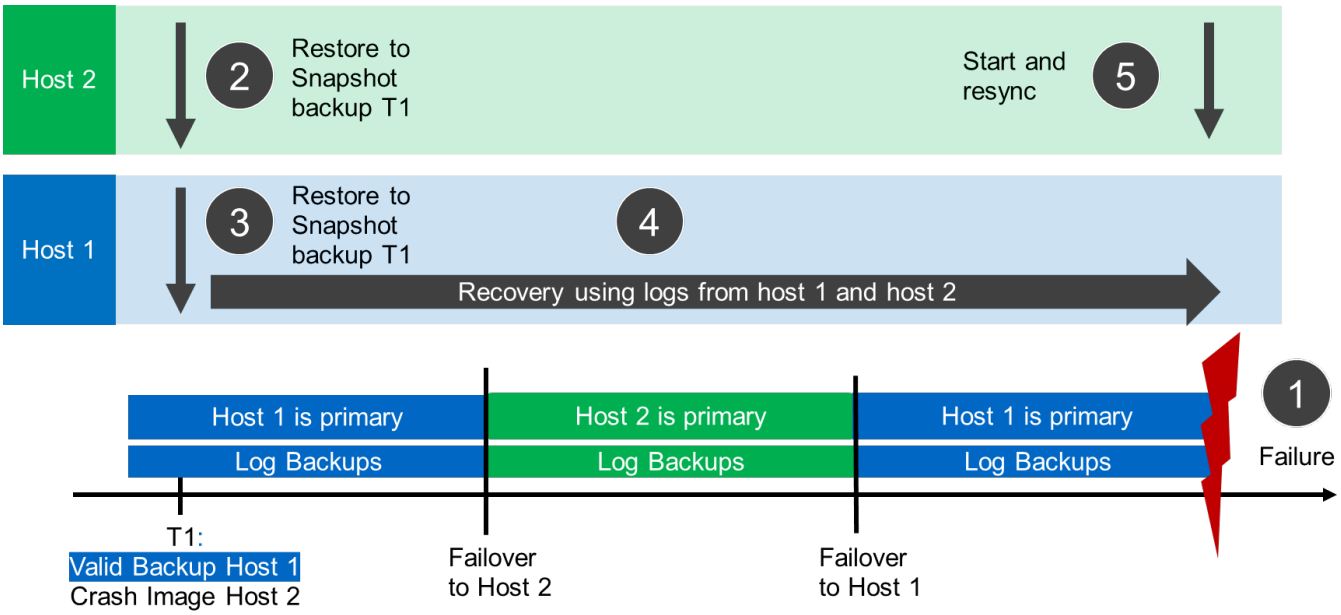


Restauration SnapCenter d’une image de sauvegarde et de panne valide

La figure suivante présente un aperçu du scénario de restauration et de récupération décrit dans cette section.

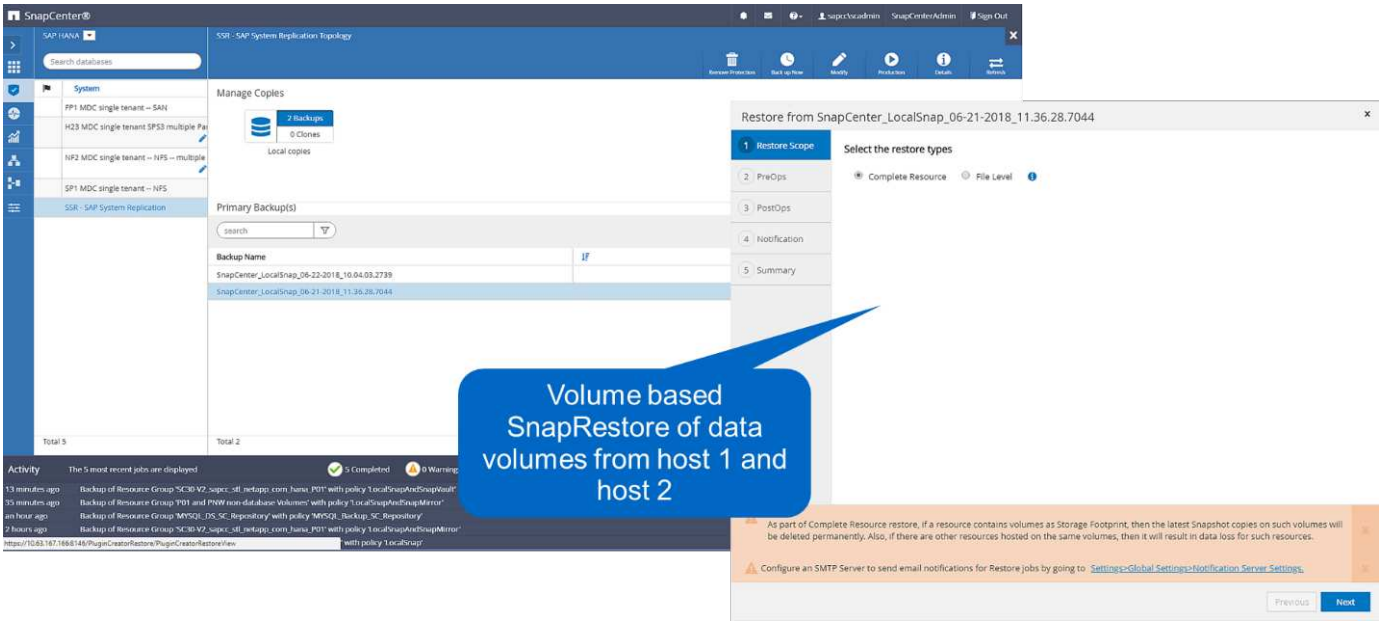
Une sauvegarde a été créée au niveau de T1 sur l’hôte 1. Un basculement a été effectué sur l’hôte 2. Après un certain point dans le temps, un autre basculement vers l’hôte 1 a été effectué. Au point actuel dans le temps, l’hôte 1 est l’hôte principal.

1. Un échec s’est produit et vous devez restaurer la sauvegarde créée sur T1 à l’hôte 1.
2. L’hôte secondaire (hôte 2) est arrêté et l’image de panne T1 est restaurée.
3. Le volume de stockage de l’hôte 1 est restauré dans la sauvegarde créée à T1.
4. Une restauration de transfert est effectuée avec des journaux de l’hôte 1 et de l’hôte 2.
5. L’hôte 2 est démarré et une resynchronisation de réplication système de l’hôte 2 est automatiquement démarrée.

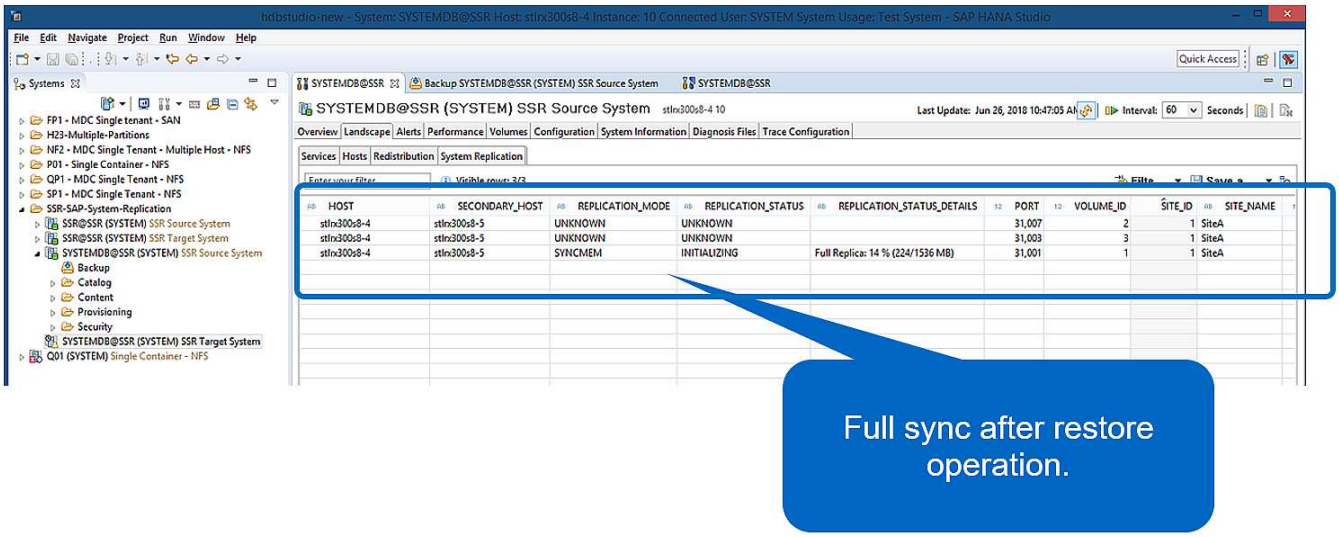


L’opération de restauration et de restauration avec SAP HANA Studio est identique aux étapes décrites dans la section "Restauration SnapCenter de la sauvegarde valide uniquement".

Pour effectuer l’opération de restauration, sélectionnez ressource complète dans SnapCenter. Les volumes des deux hôtes sont restaurés.



Une fois la restauration par transfert terminée, l’hôte secondaire (hôte 2) est démarré et la resynchronisation de réplication du système SAP HANA est démarrée. Une réplication complète de toutes les données est exécutée.



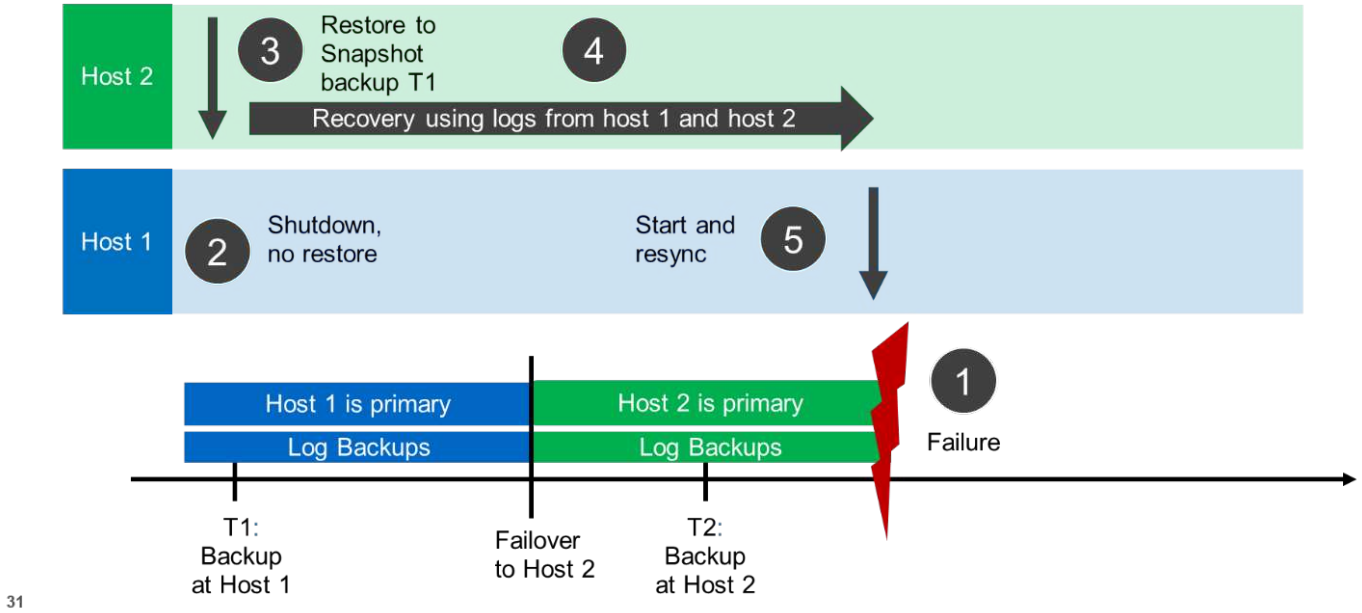
Restauration et récupération à partir d’une sauvegarde créée sur l’autre hôte

Une opération de restauration à partir d’une sauvegarde créée sur l’autre hôte SAP HANA est un scénario valide pour les deux options de configuration SnapCenter.

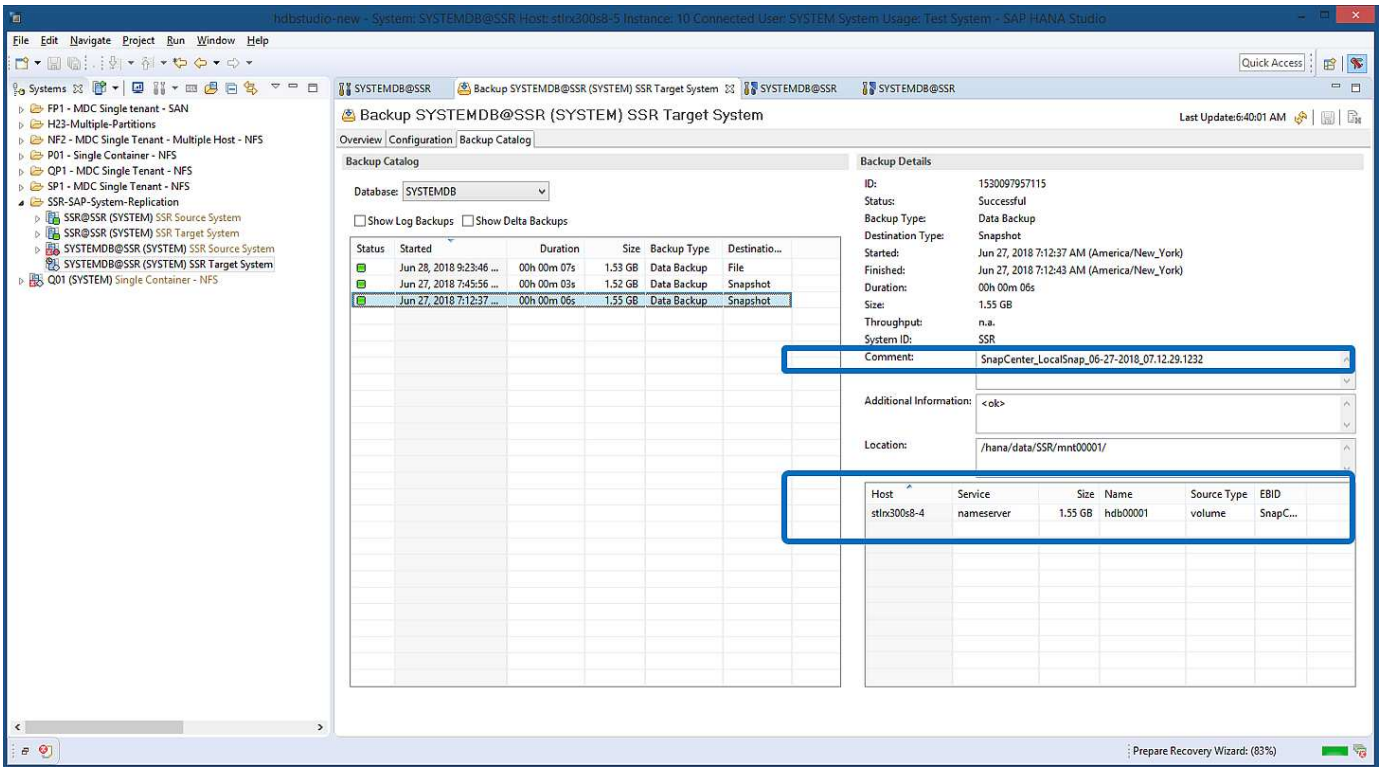
La figure suivante présente un aperçu du scénario de restauration et de récupération décrit dans cette section.

Une sauvegarde a été créée au niveau de T1 sur l'hôte 1. Un basculement a été effectué sur l'hôte 2. Au point actuel dans le temps, l'hôte 2 est l'hôte principal.

1. Un échec s'est produit et vous devez restaurer la sauvegarde créée sur T1 à l'hôte 1.
2. L'hôte principal (hôte 1) est arrêté.
3. Les données de sauvegarde T1 de l'hôte 1 sont restaurées sur l'hôte 2.
4. Une restauration de transfert est effectuée à l'aide des journaux de l'hôte 1 et de l'hôte 2.
5. L'hôte 1 est démarré et une resynchronisation de réplication système de l'hôte 1 est automatiquement démarrée.



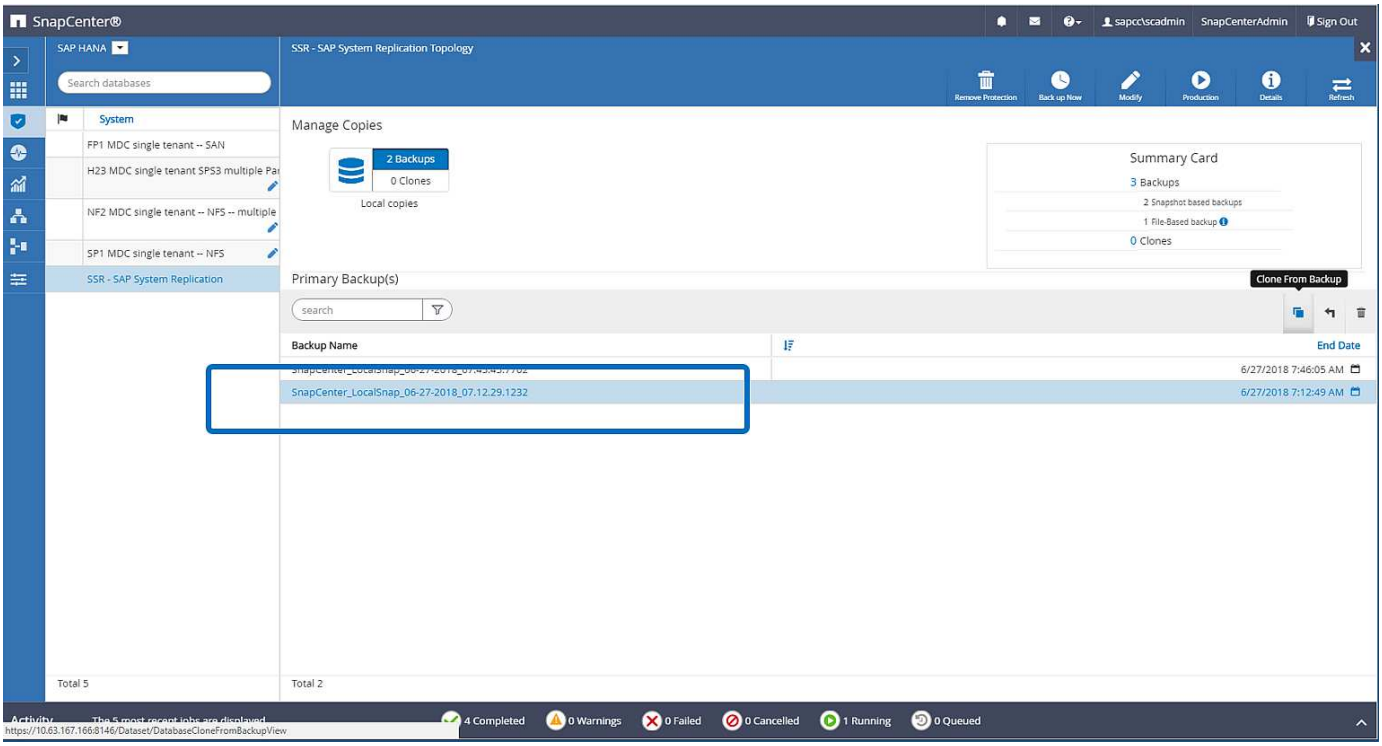
La figure suivante montre le catalogue de sauvegardes SAP HANA et met en évidence la sauvegarde créée sur l'hôte 1, qui a été utilisée pour l'opération de restauration et de reprise.



L'opération de restauration implique les étapes suivantes :

1. Créez un clone à partir de la sauvegarde créée sur l'hôte 1.
2. Monter le volume cloné sur l'hôte 2.
3. Copiez les données à partir du volume cloné vers l'emplacement d'origine.

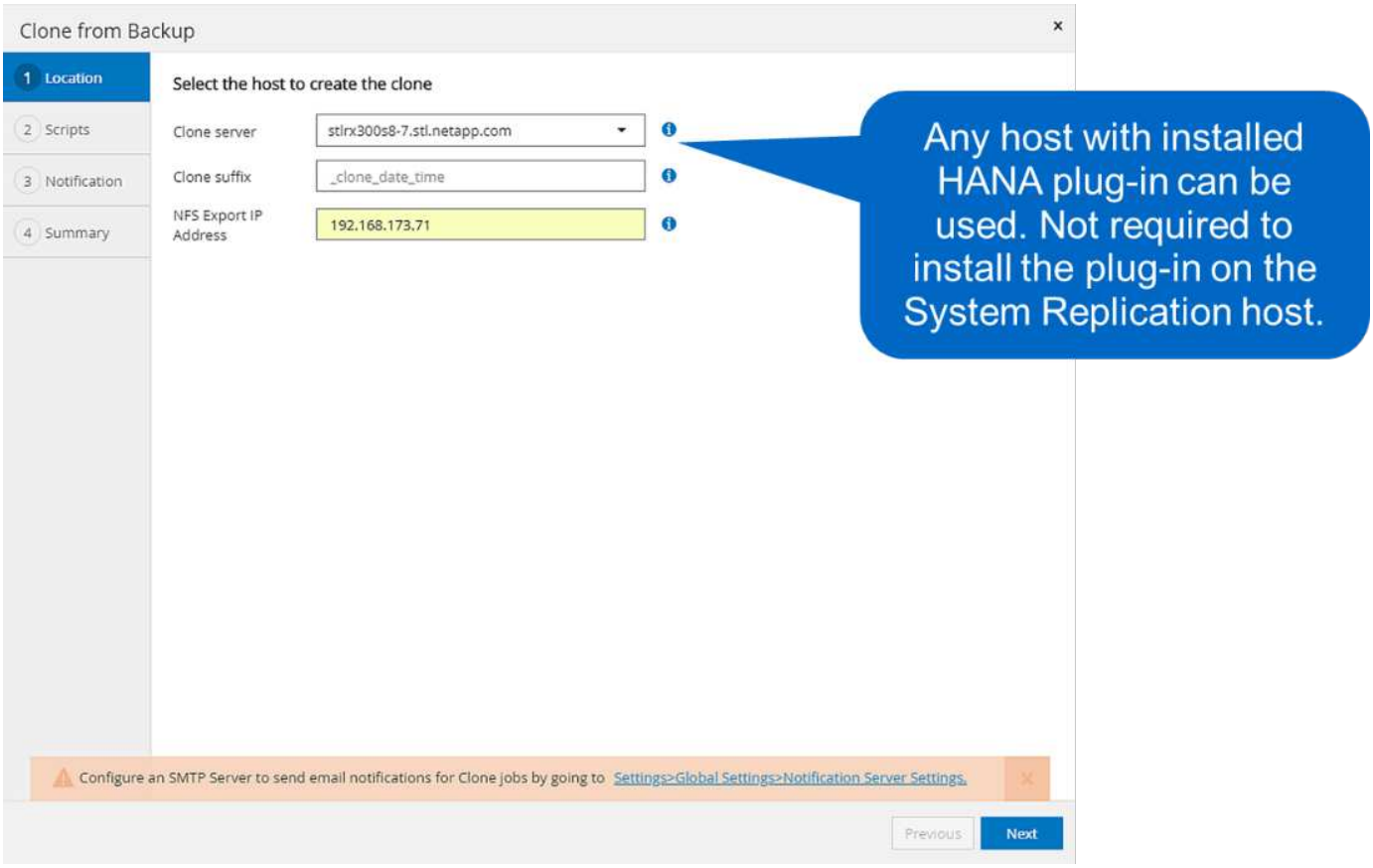
Dans SnapCenter, la sauvegarde est sélectionnée et l'opération de clonage est démarrée.



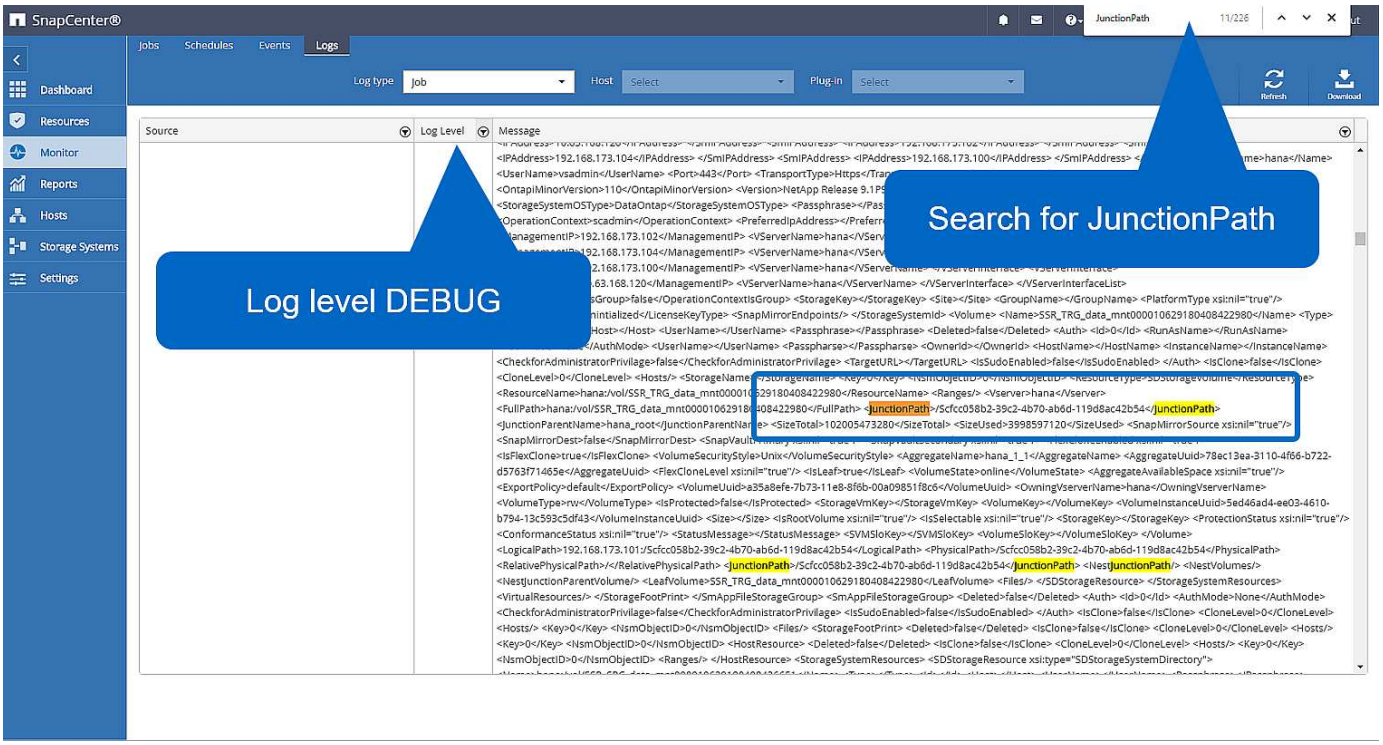
Vous devez fournir le serveur clone et l'adresse IP d'exportation NFS.

Dans une configuration SnapCenter à ressource unique, le plug-in SAP HANA n'est pas installé sur l'hôte de la base de données. Pour exécuter le workflow de clone SnapCenter, tout hôte disposant d'un plug-in HANA installé peut être utilisé comme serveur clone.

+ dans une configuration SnapCenter avec des ressources distinctes, l'hôte de base de données HANA est sélectionné comme serveur clone, et un script de montage est utilisé pour monter le clone sur l'hôte cible.



Pour déterminer le chemin de jonction nécessaire au montage du volume cloné, vérifiez le journal des tâches de la tâche de clonage, comme le montre la figure suivante.



Le volume cloné peut désormais être monté.

```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Scc373da37-00ff-4694-b1e1-
8153dbd46caf /mnt/tmp
```

Le volume cloné contient les données de la base de données HANA.

```
stlrx300s8-5:/mnt/tmp/# ls -al
drwxr-x--x 2 ssradm sapsys 4096 Jun 27 11:12 hdb00001
drwx------ 2 ssradm sapsys 4096 Jun 21 09:38 hdb00002.00003
drwx------ 2 ssradm sapsys 4096 Jun 27 11:12 hdb00003.00003
-rw-r--r-- 1 ssradm sapsys   22 Jun 27 11:12 nameserver.lck
```

Les données sont copiées à l'emplacement d'origine.

```
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00001 /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00002.00003/ /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00003.00003/ /hana/data/SSR/mnt00001/
```

La restauration avec SAP HANA Studio est effectuée comme décrit dans la section "Restauration SnapCenter de la sauvegarde valide uniquement".

Où trouver des informations complémentaires

Pour en savoir plus sur les informations fournies dans ce document, consultez ces

documents :

- SAP HANA : sauvegarde et restauration avec SnapCenter

  "https://www.netapp.com/us/media/tr-4614.pdf"

- Automatisation des opérations de copie et de clonage du système SAP HANA avec SnapCenter

  "https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html"

- Reprise après incident de SAP HANA avec la réplication du stockage

  "https://www.netapp.com/us/media/tr-4646.pdf"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Octobre 2018	Version initiale
Version 2.0	Janvier 2022	Mise à jour pour couvrir la prise en charge de la réplication système SnapCenter 4.6 HANA

Reprise après incident de SAP HANA avec Azure NetApp Files

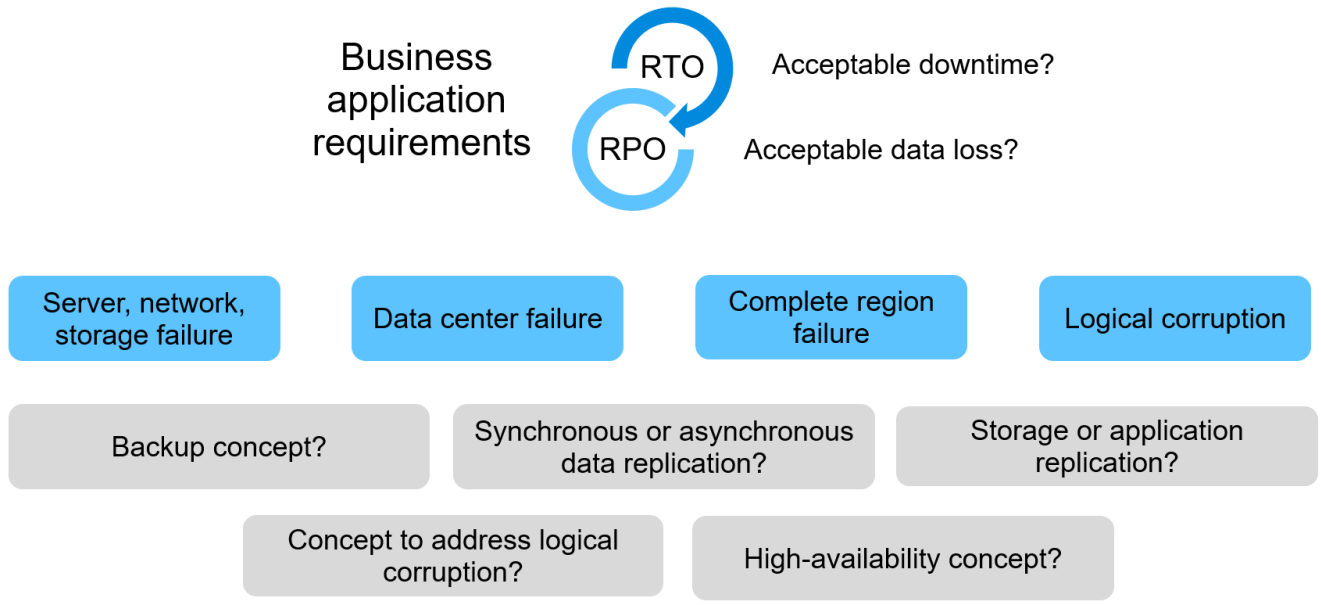
Tr-4891 : reprise après incident de SAP HANA avec Azure NetApp Files

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.



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.

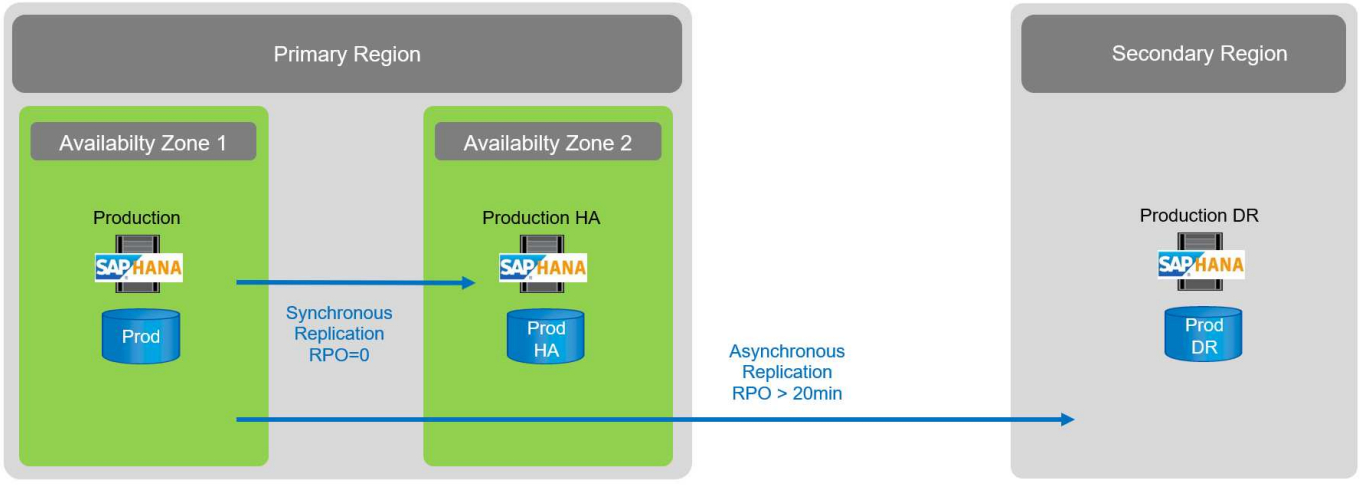
Comparaison des solutions de reprise d'activité

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.

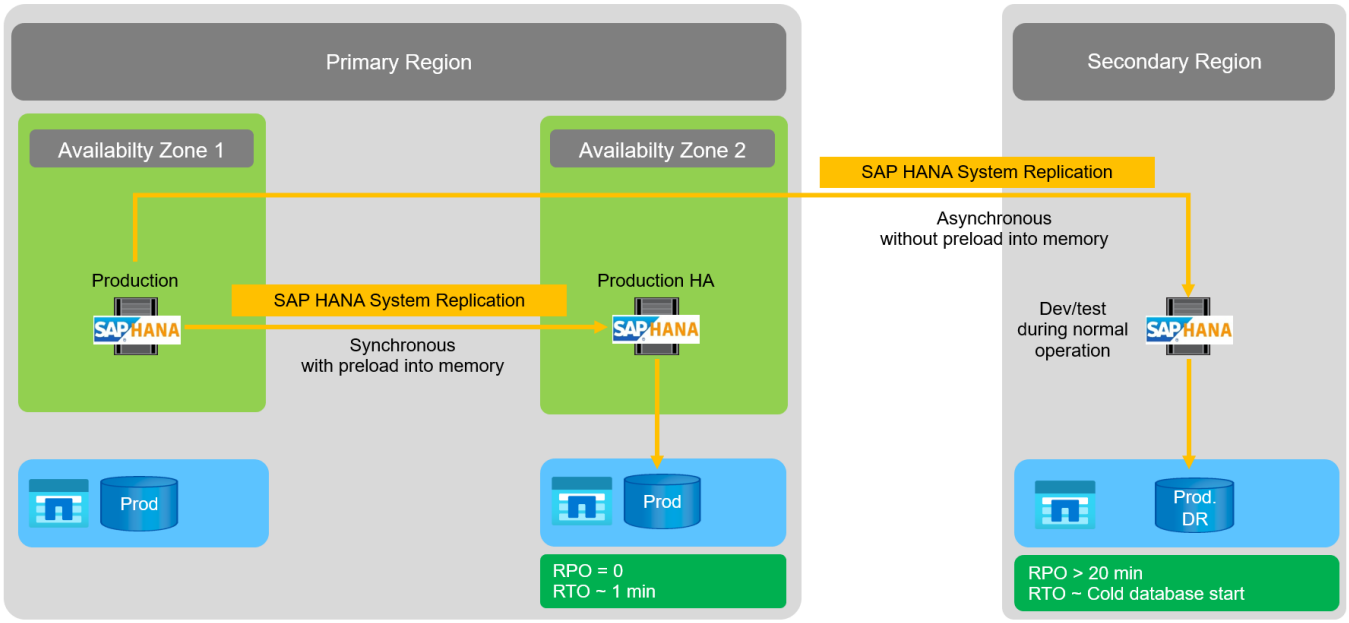
La réplication système SAP HANA peut être exploitée selon l'un des deux modes suivants :

- 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.

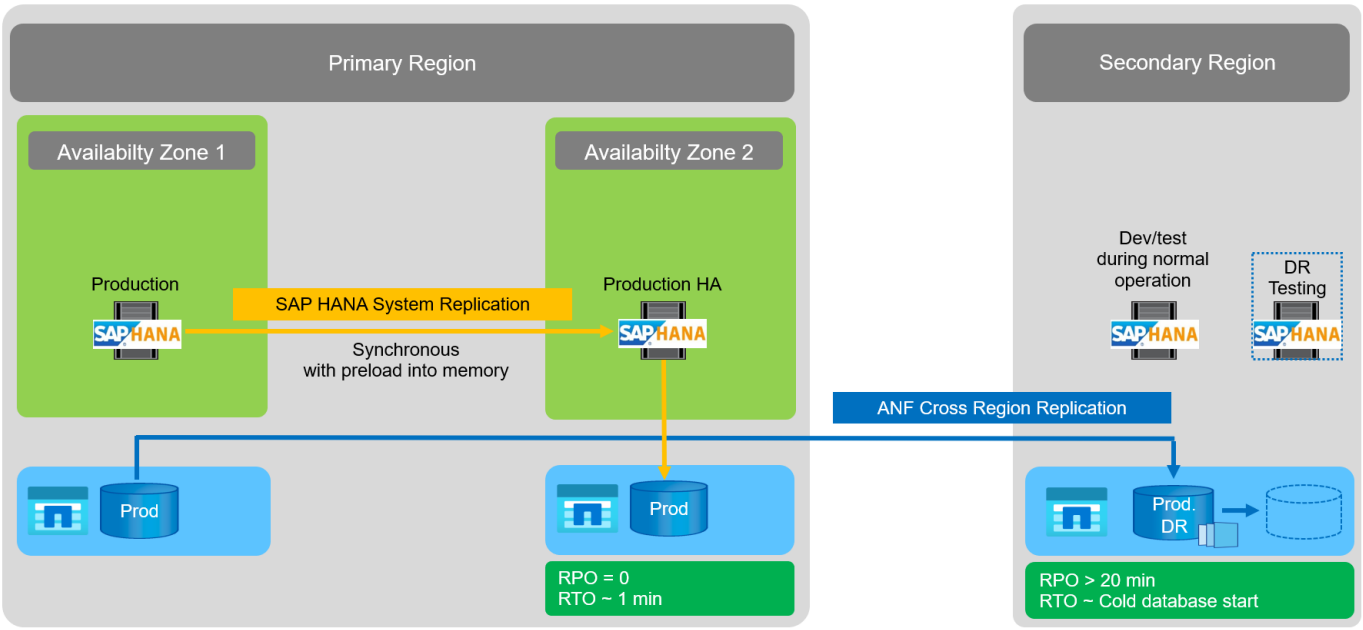
La figure suivante présente un exemple de solution de reprise après incident dans deux régions avec la réplication ANF Cross- Region. Dans cet exemple, le système HANA est protégé avec la réplication système HANA dans la région primaire, comme indiqué au chapitre précédent. La réplication vers une région 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

	Réplication du stockage	Réplication du système SAP HANA	
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.

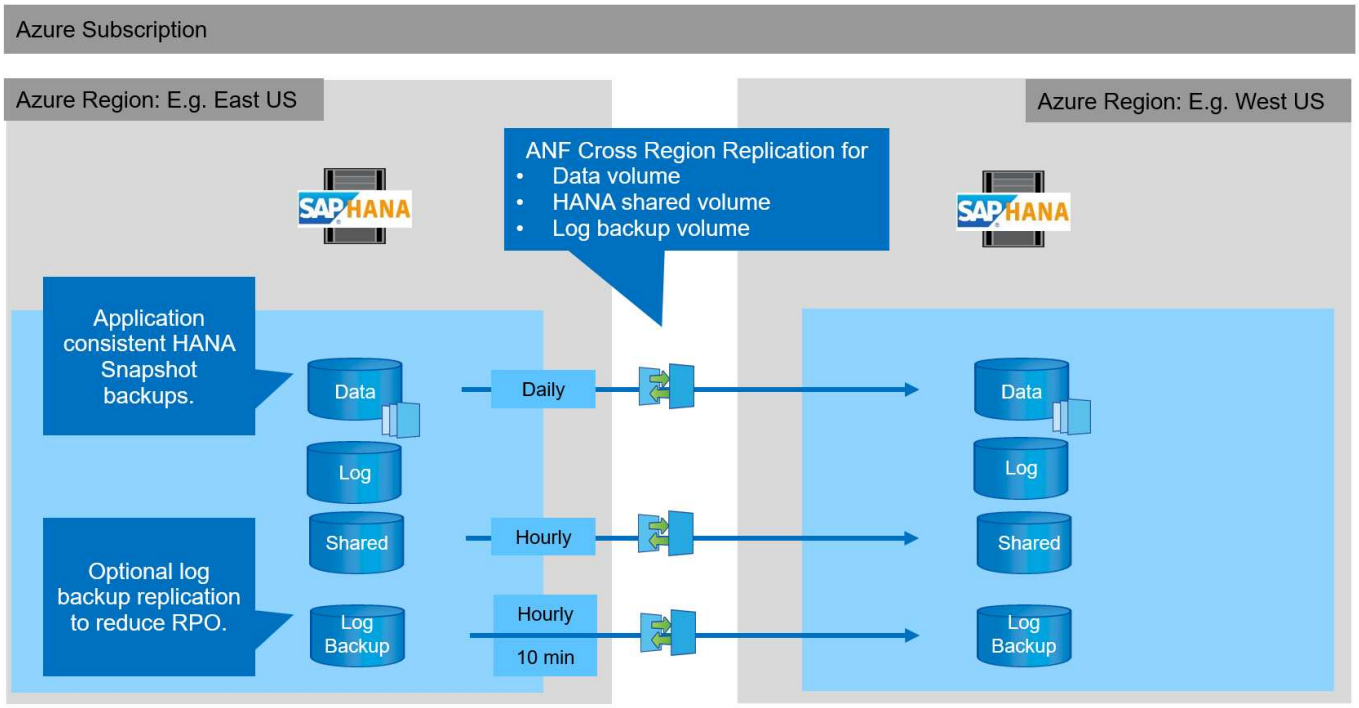
Le terme « sauvegarde du journal » utilisé dans ce document inclut la sauvegarde du journal et la sauvegarde du catalogue de sauvegardes HANA. Le catalogue de sauvegardes HANA est nécessaire pour exécuter les opérations de récupération par transfert.

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

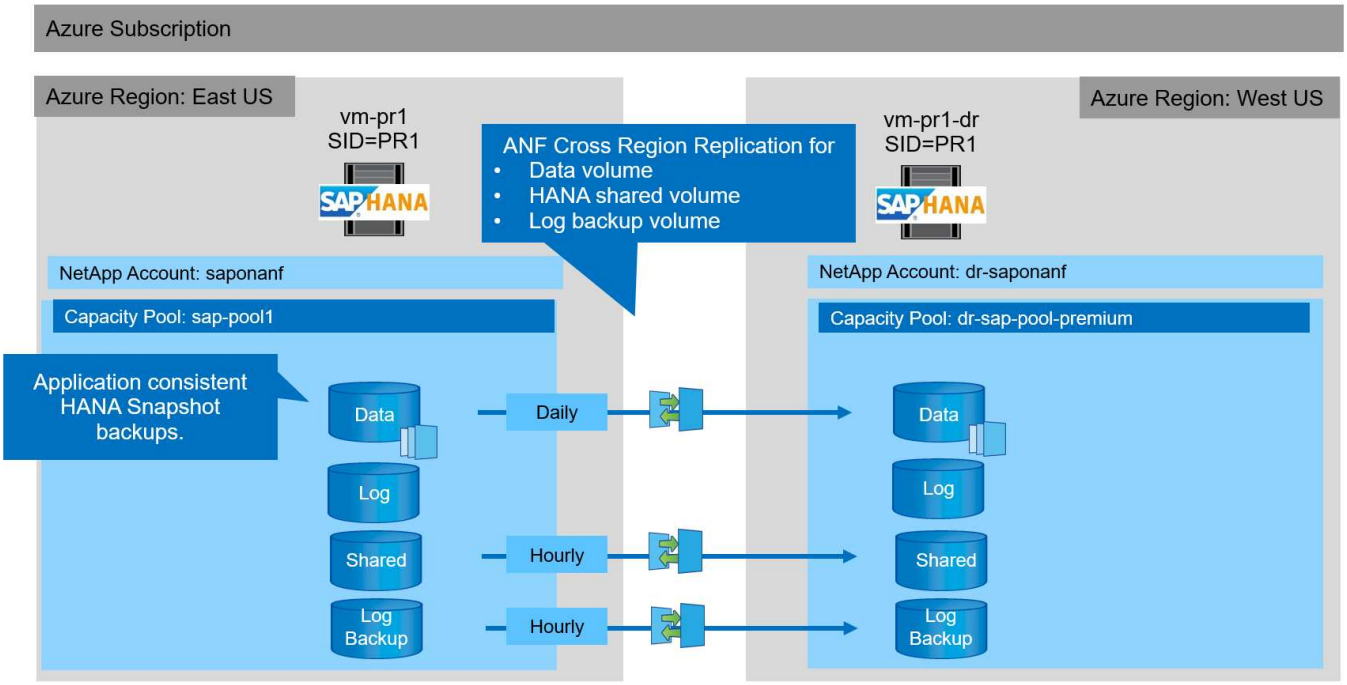
de volume partagé sont tous configurés. Le basculement et les tests de reprise après incident ont été validés avec un point de sauvegarde ainsi que pour les opérations de reprise après incident.

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.

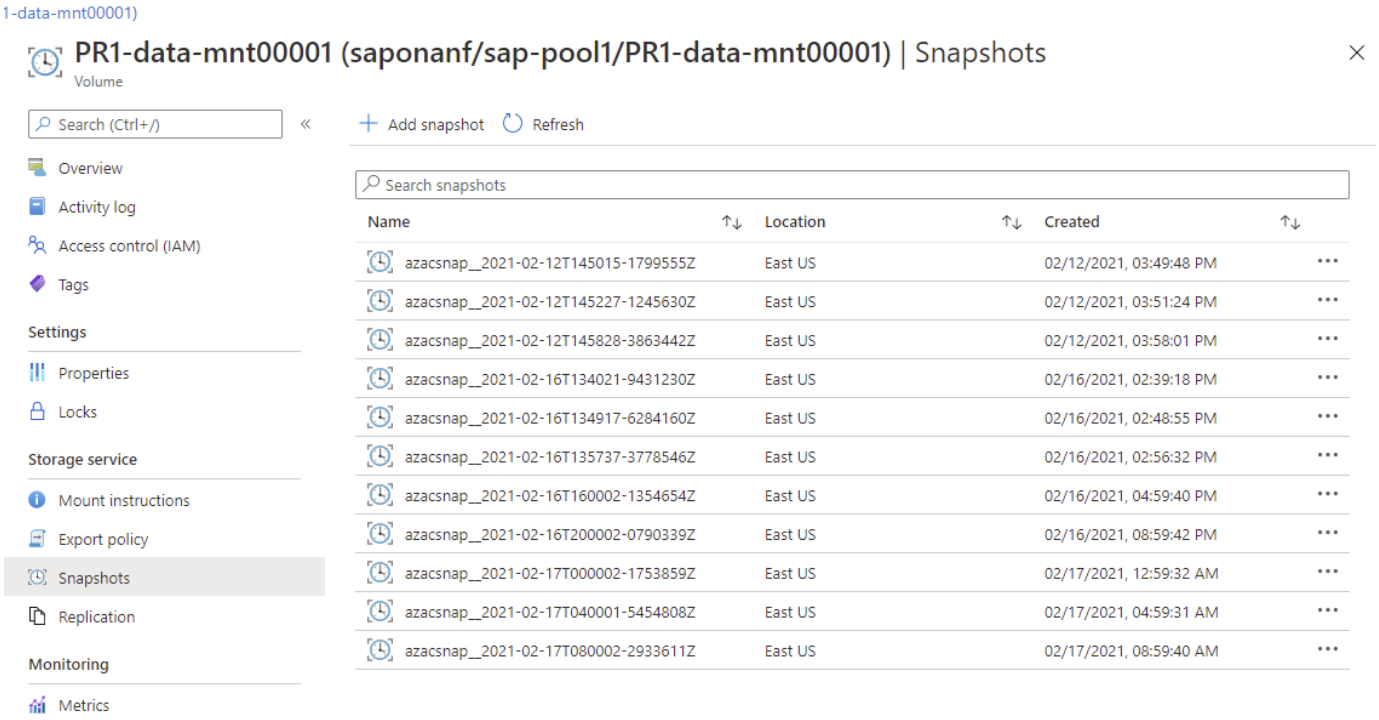


Configuration de sauvegarde Snapshot avec AzAcSnap

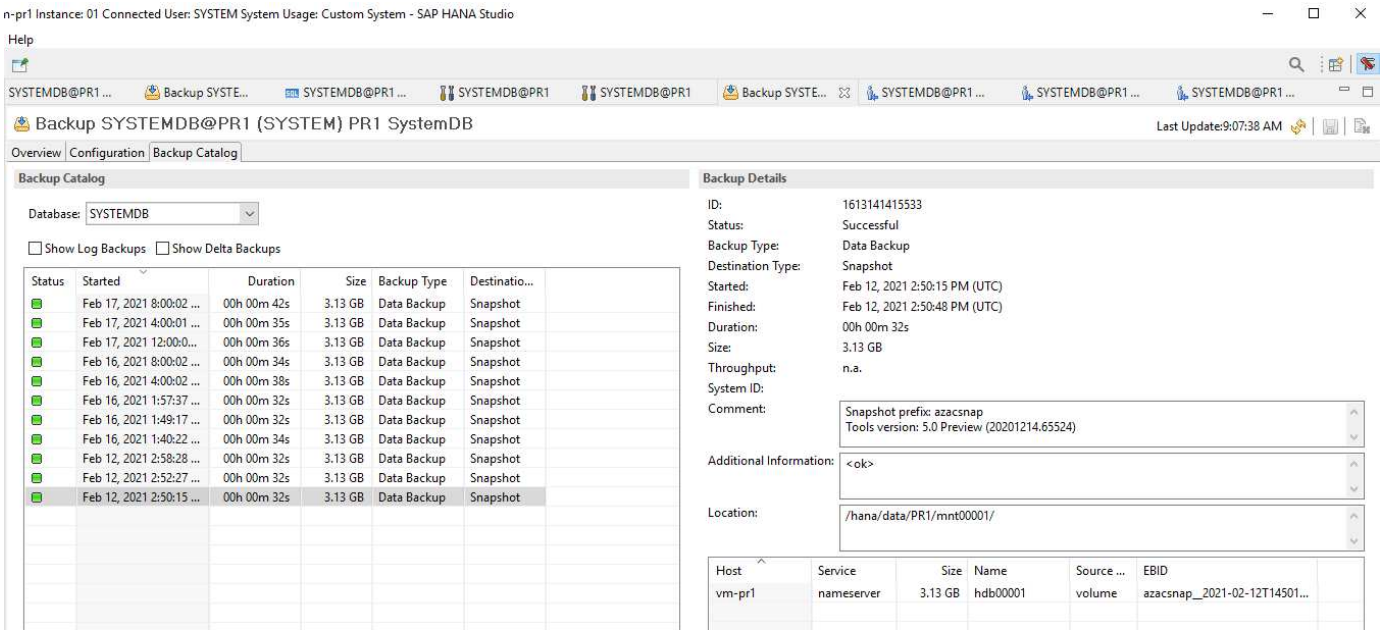
Sur le site principal, AzAcSnap a été configuré pour créer des sauvegardes Snapshot cohérentes au niveau des applications du système HANA PR1. Ces sauvegardes Snapshot sont disponibles au niveau du volume de données ANF du système PR1 HANA et sont également enregistrées dans le catalogue des sauvegardes 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 :

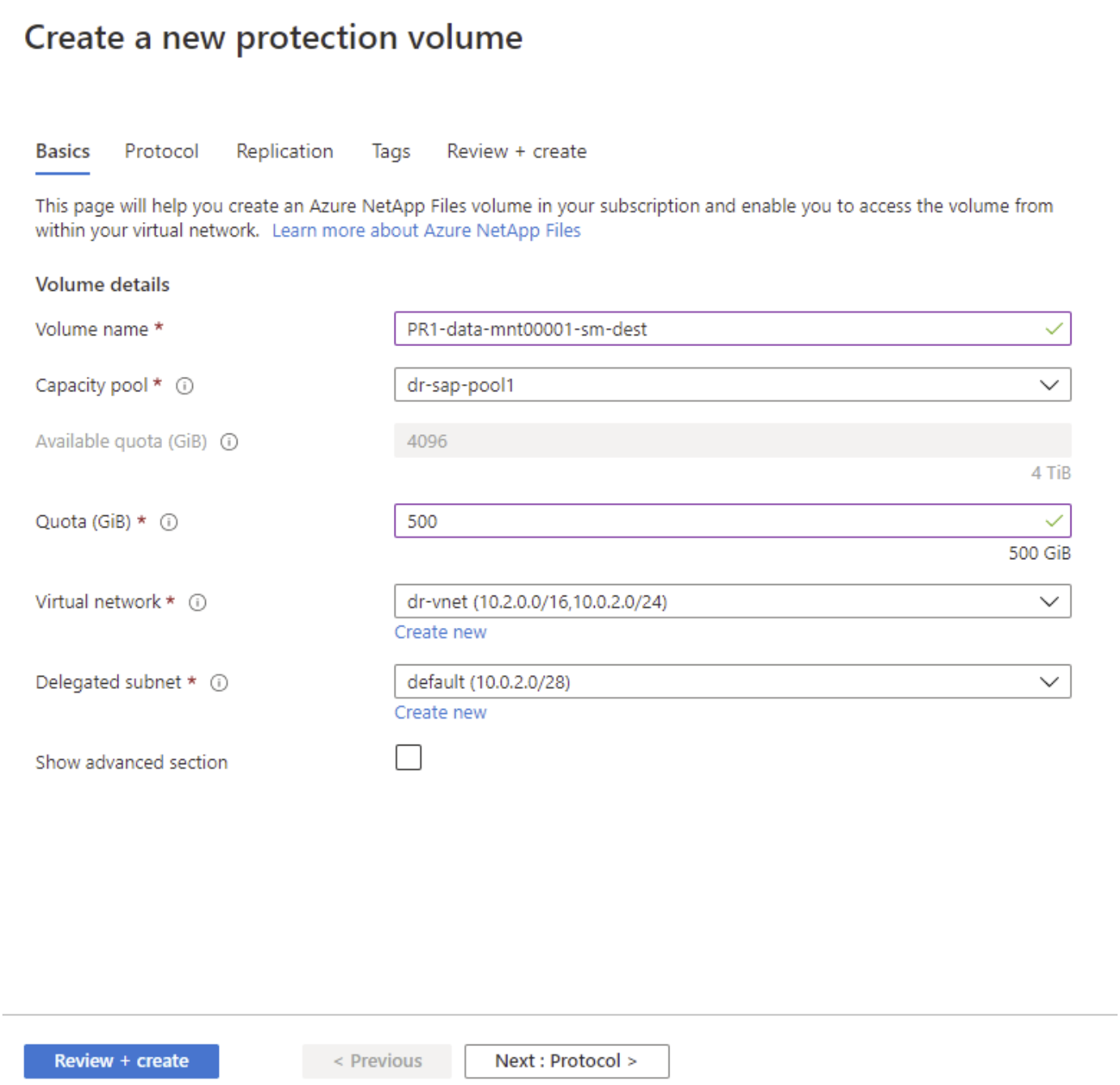
1. Créez un nouveau volume de protection sur le site de reprise après incident :
   a. Indiquez le nom du volume, le pool de capacité, le quota et les informations réseau.
   b. Fournissez le protocole et les informations d'accès aux volumes.
   c. Indiquez l'ID du volume source et la planification de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

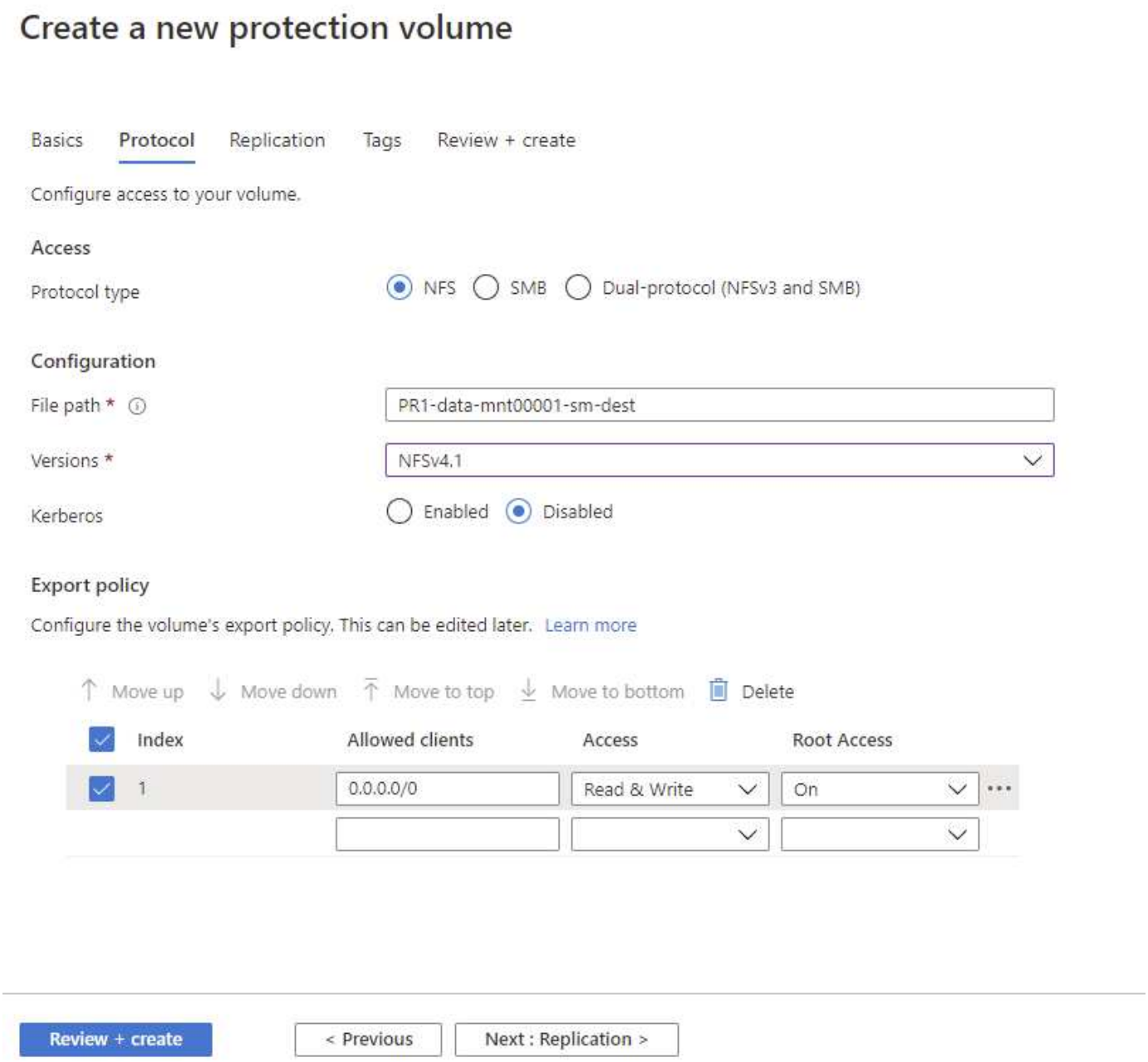
> Le quota du volume peut être défini en fonction des exigences de capacité, car les performances du volume n'ont aucun impact sur le processus de réplication. Dans le cas d'un basculement de reprise après incident, le quota doit être ajusté pour répondre aux exigences de performances réelles.

> 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.



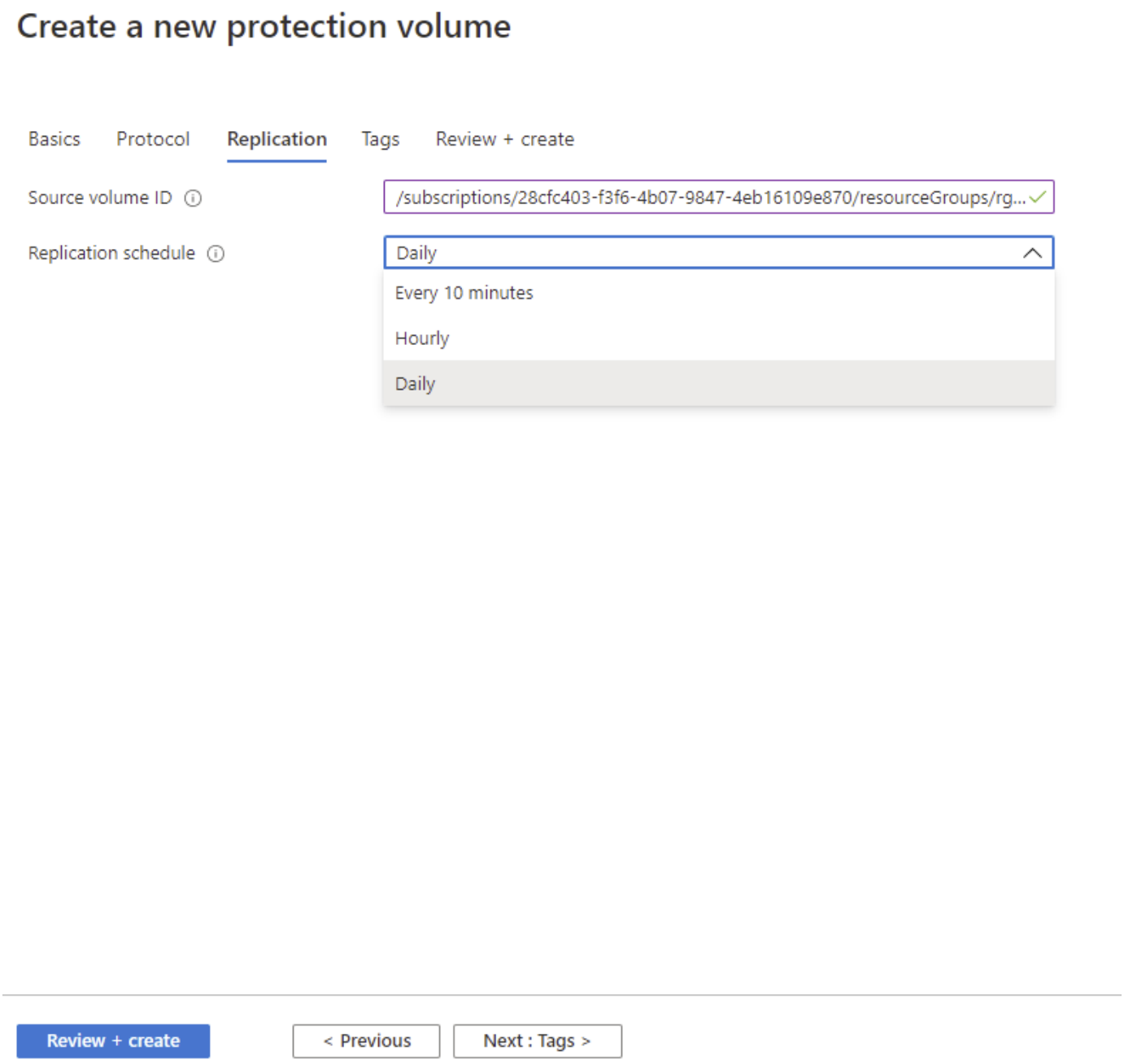
Dans l'onglet Protocol, vous devez fournir le protocole réseau, le chemin du réseau et la export policy.

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



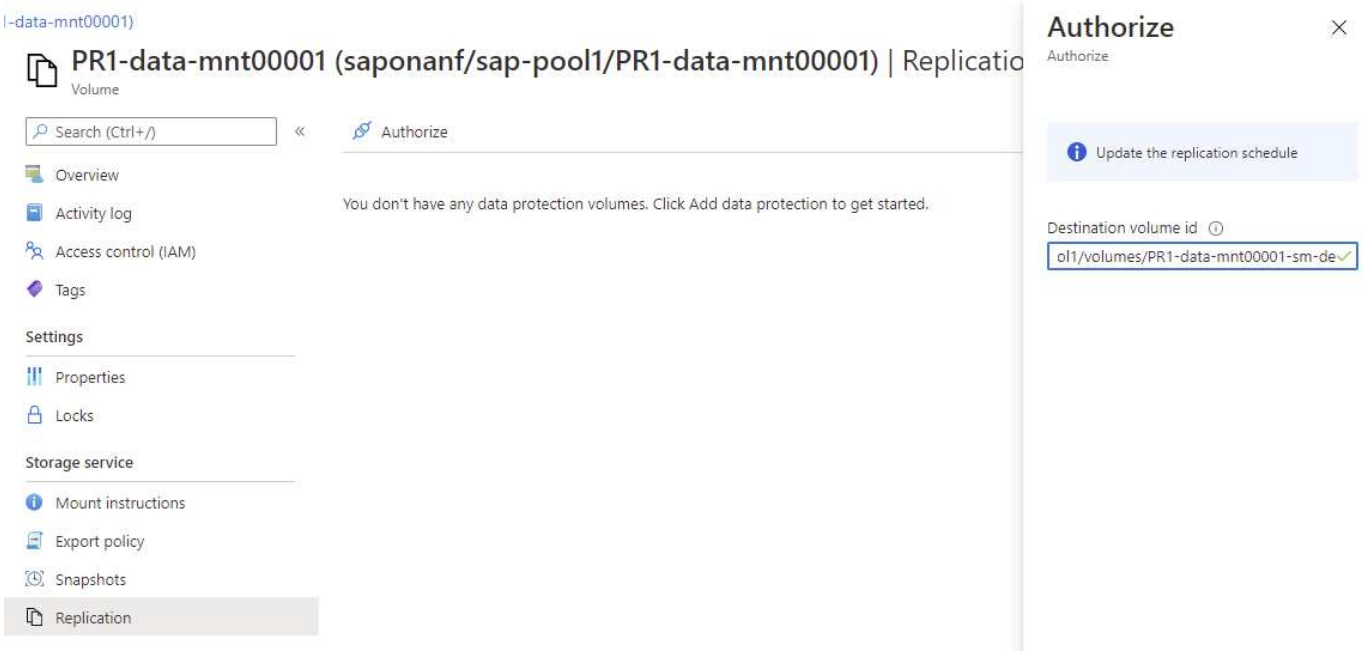
Dans l'onglet réplication, vous devez configurer l'ID du volume source et la planification de réplication. Pour la réplication du volume de données, nous avons configuré une planification de réplication quotidienne pour notre configuration de laboratoire.

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

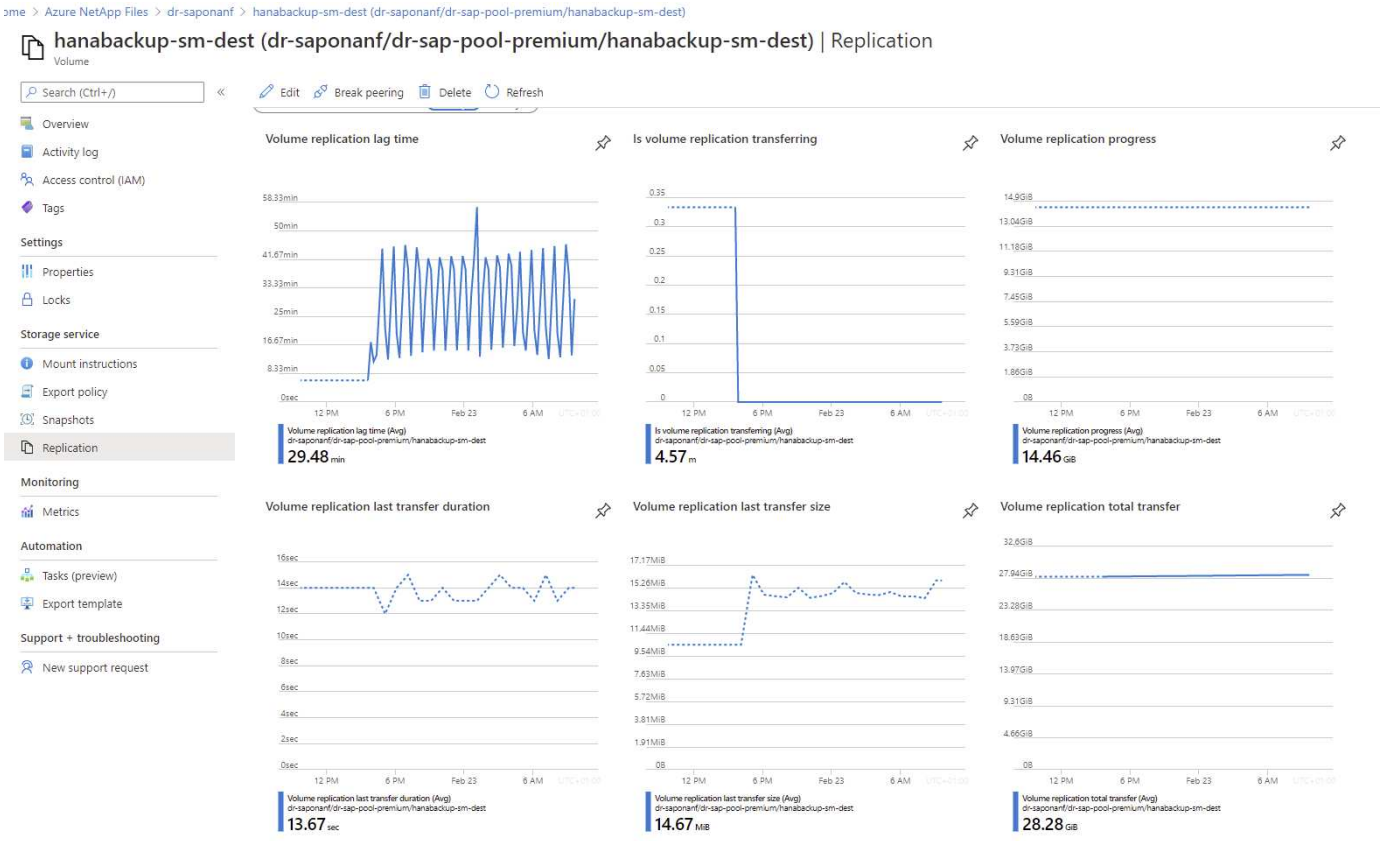
Les trois captures d'écran suivantes indiquent l'état de la réplication pour les données, la sauvegarde du journal et les volumes partagés.

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.

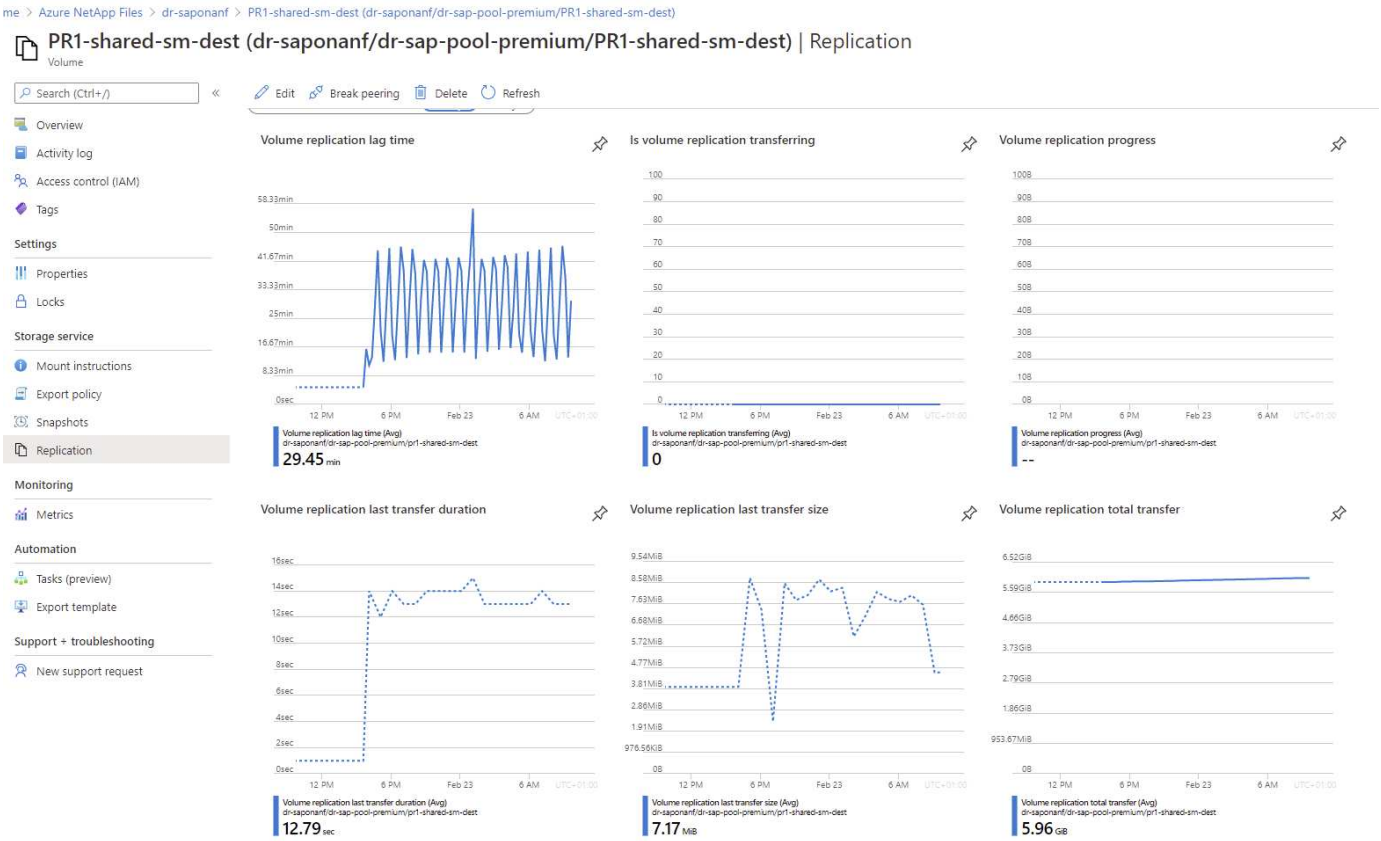
La durée du transfert et la taille du transfert fournissent des informations précieuses sur les besoins en bande passante et modifient le taux du volume répliqué.

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.



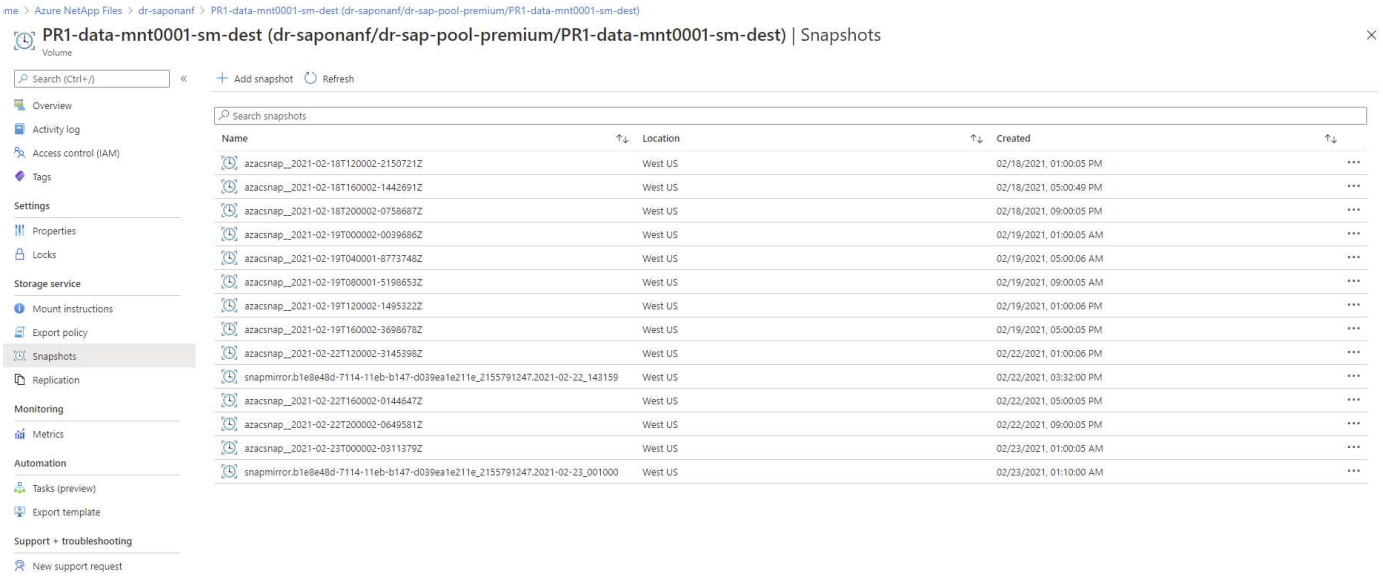
La capture d'écran suivante montre l'état de réplication du volume partagé HANA.



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.

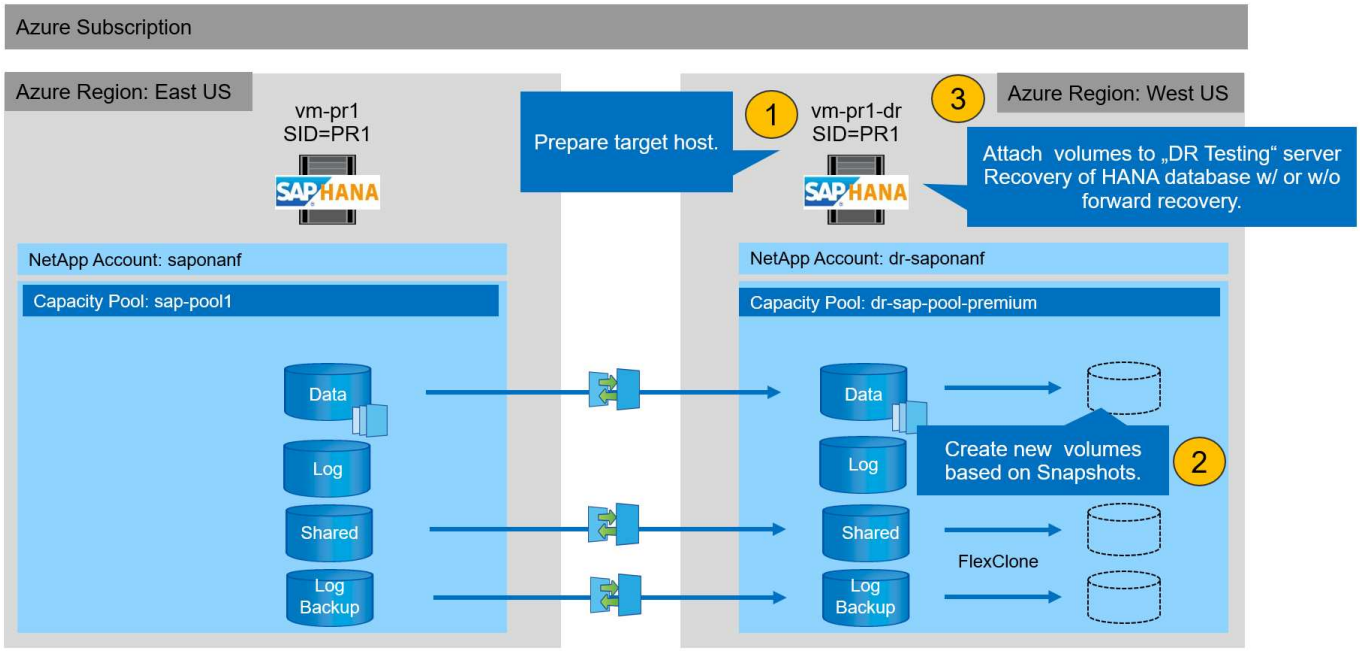
Le workflow de test de reprise d'activité utilise l'ensemble de fonctionnalités ANF pour créer des volumes basés sur des sauvegardes Snapshot existantes à la cible de reprise d'activité. Voir "Fonctionnement des snapshots Azure NetApp Files | Microsoft Docs".

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.

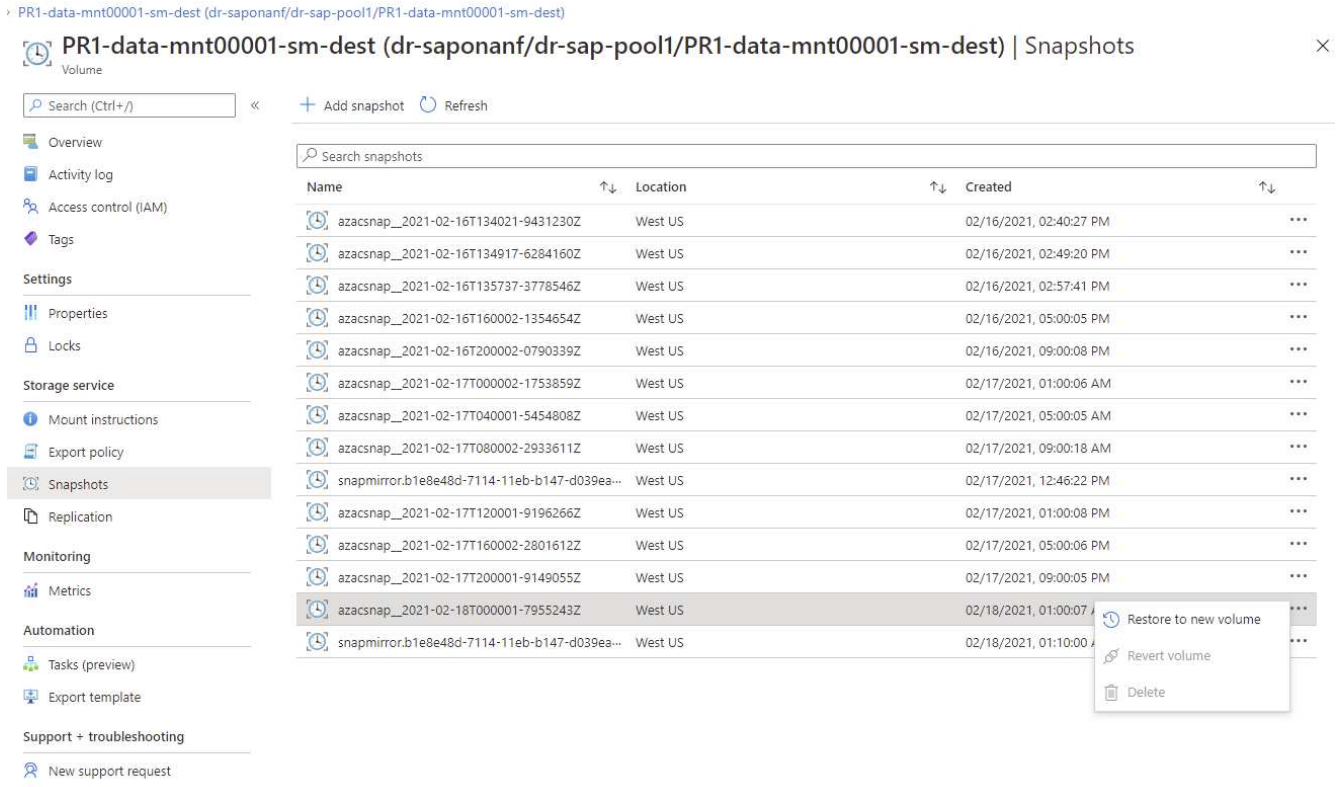
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa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

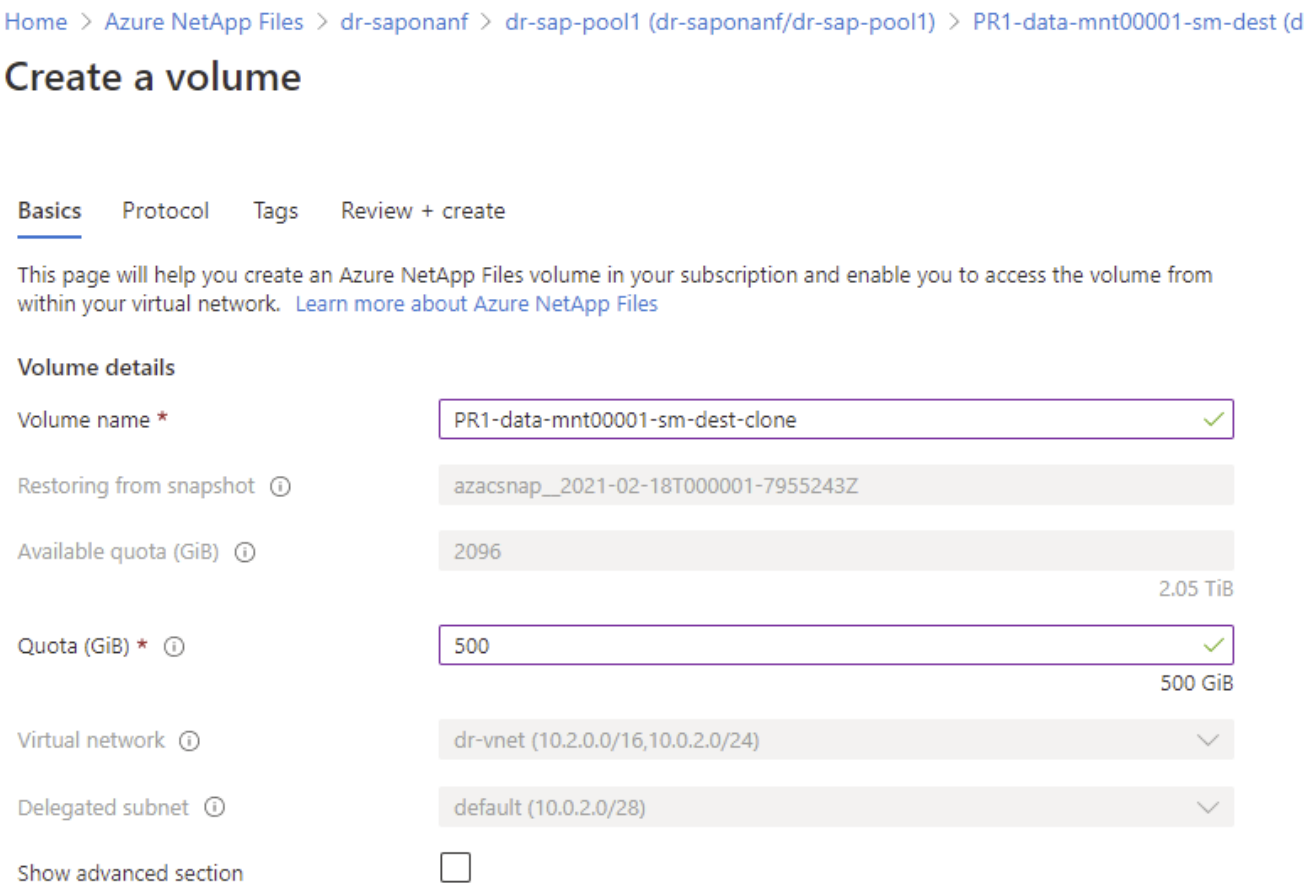
Selon la configuration de reprise après incident (avec ou sans réplication de sauvegarde des journaux), il faut créer deux ou trois nouveaux volumes basés sur des sauvegardes Snapshot. Dans les deux cas, un nouveau volume de données et le volume partagé HANA doivent être créés.

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.

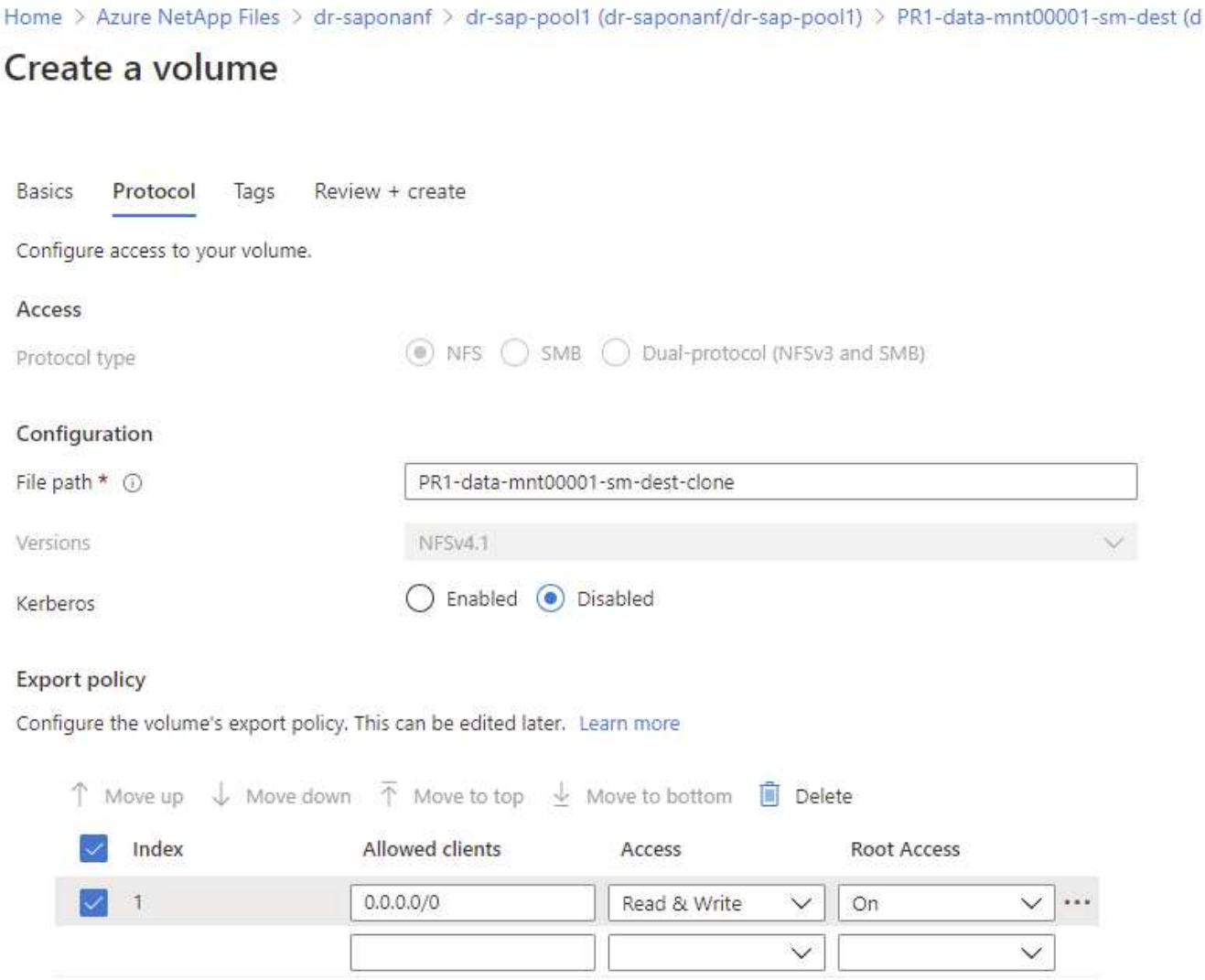
1. L’une des sauvegardes Snapshot cohérentes au niveau des applications est sélectionnée comme source pour le nouveau volume du volume de données HANA. L’option Restaurer vers un nouveau volume est sélectionnée pour créer un nouveau volume basé sur la sauvegarde snapshot.



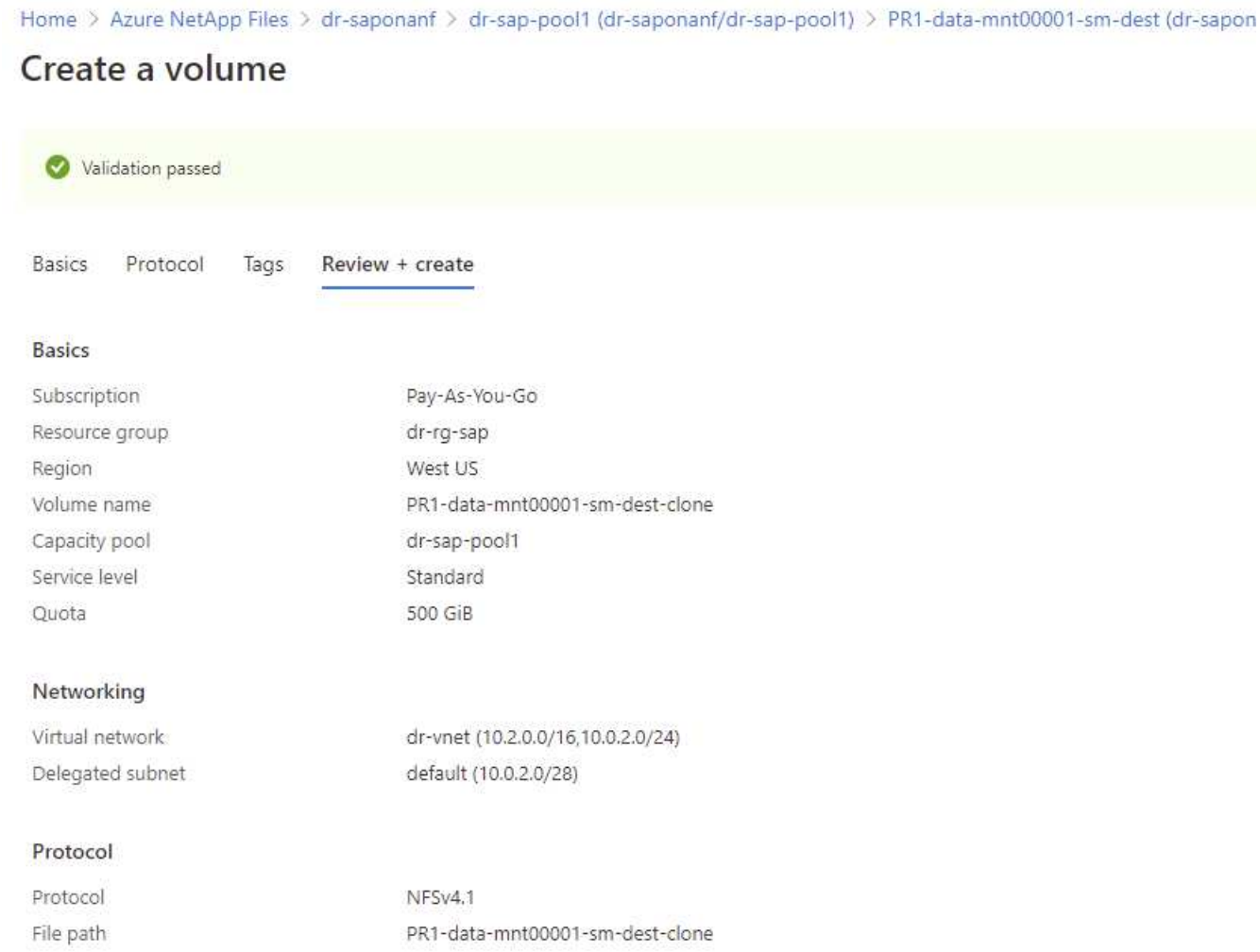
2. Le nouveau nom de volume et quota doivent être fournis dans l’interface utilisateur.



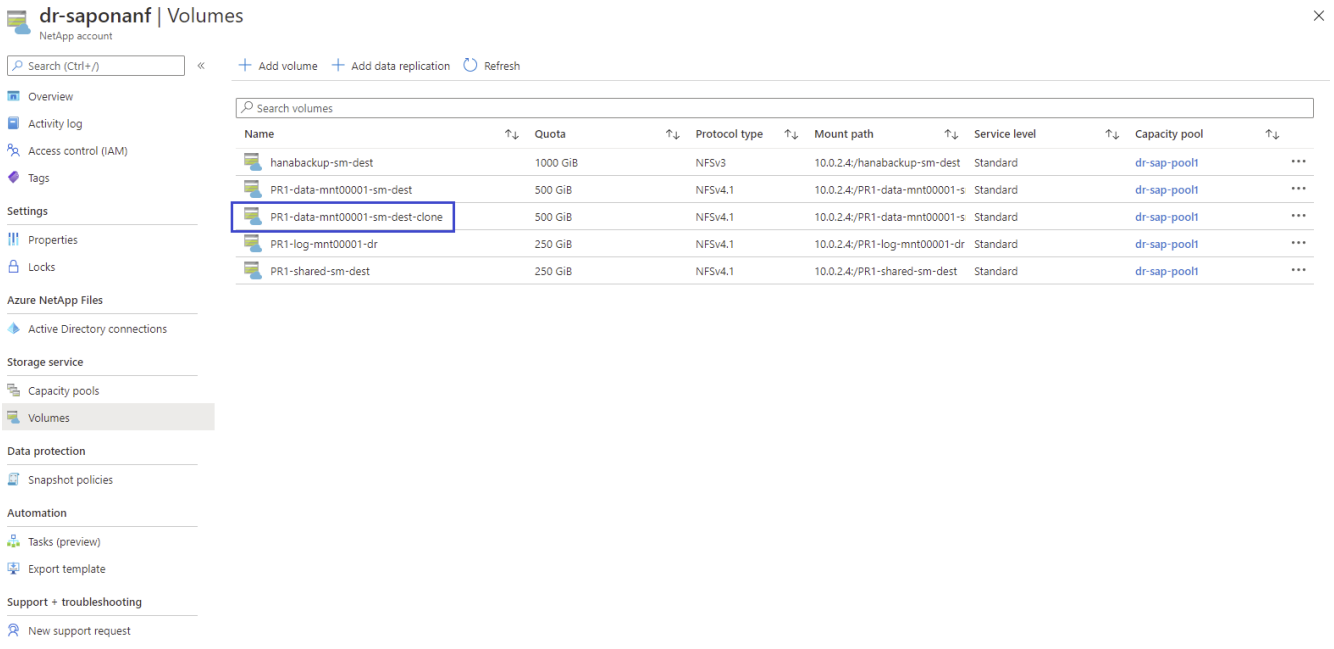
3. Le chemin des fichiers et l'export policy sont configurés dans l'onglet Protocol.



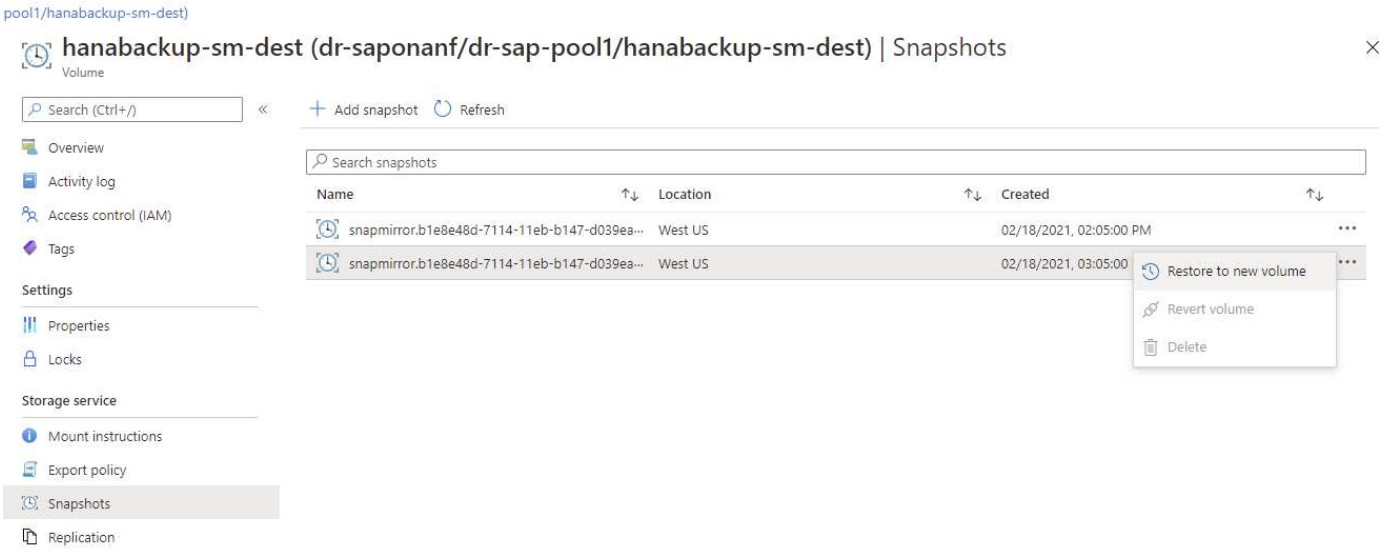
4. L'écran Créer et revoir résume la configuration.



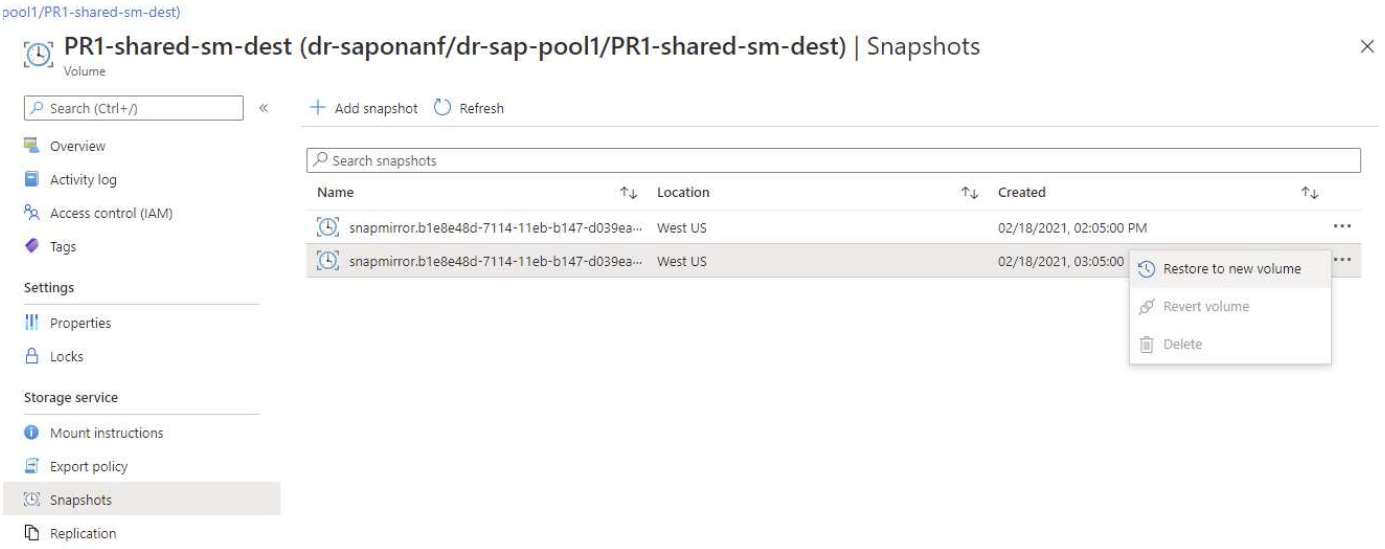
5. Un nouveau volume a été créé à partir de la sauvegarde snapshot HANA.



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

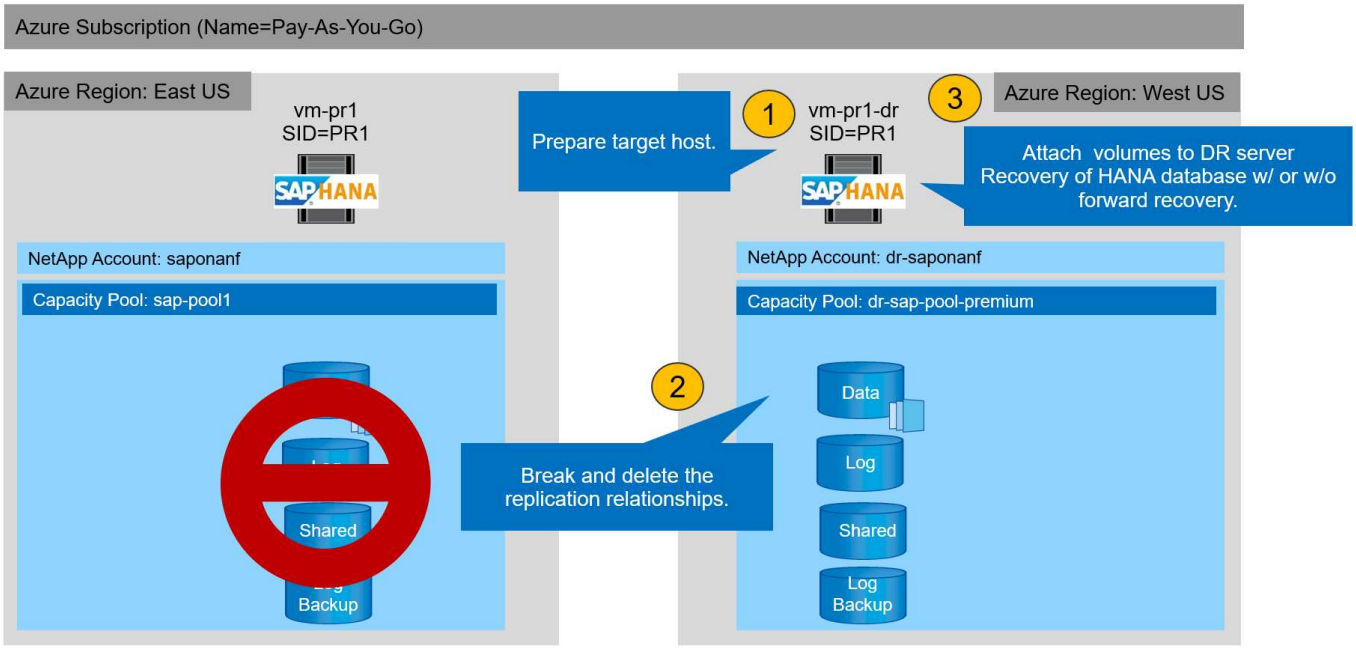
Selon que la réplication de sauvegarde des journaux fait partie de la configuration de reprise sur incident, les étapes de la reprise sur incident sont légèrement différentes. Cette section décrit le basculement de reprise après incident pour la réplication de données uniquement à des fins de sauvegarde,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

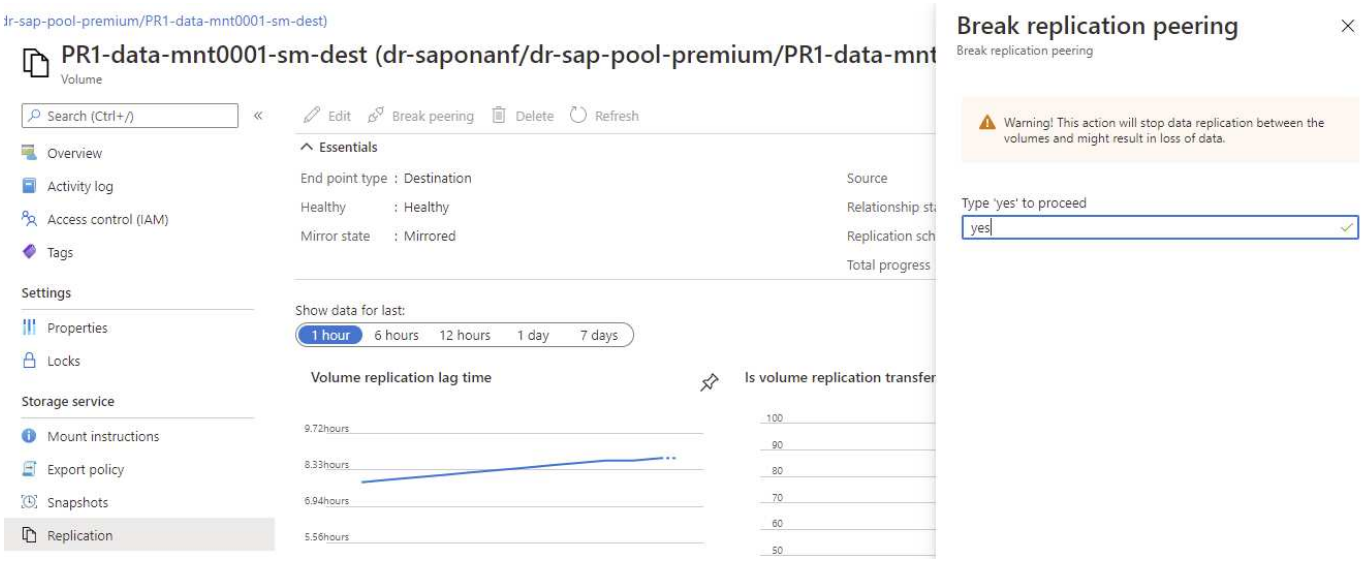
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa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

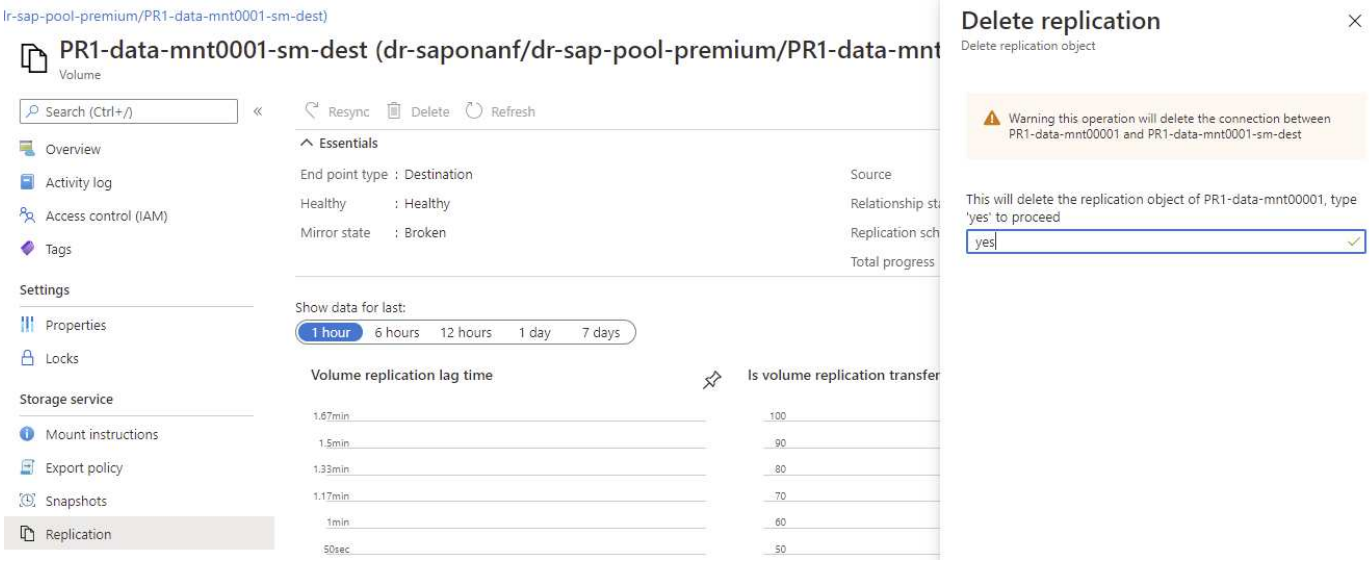
Interrompre et supprimer le peering de réplication

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.

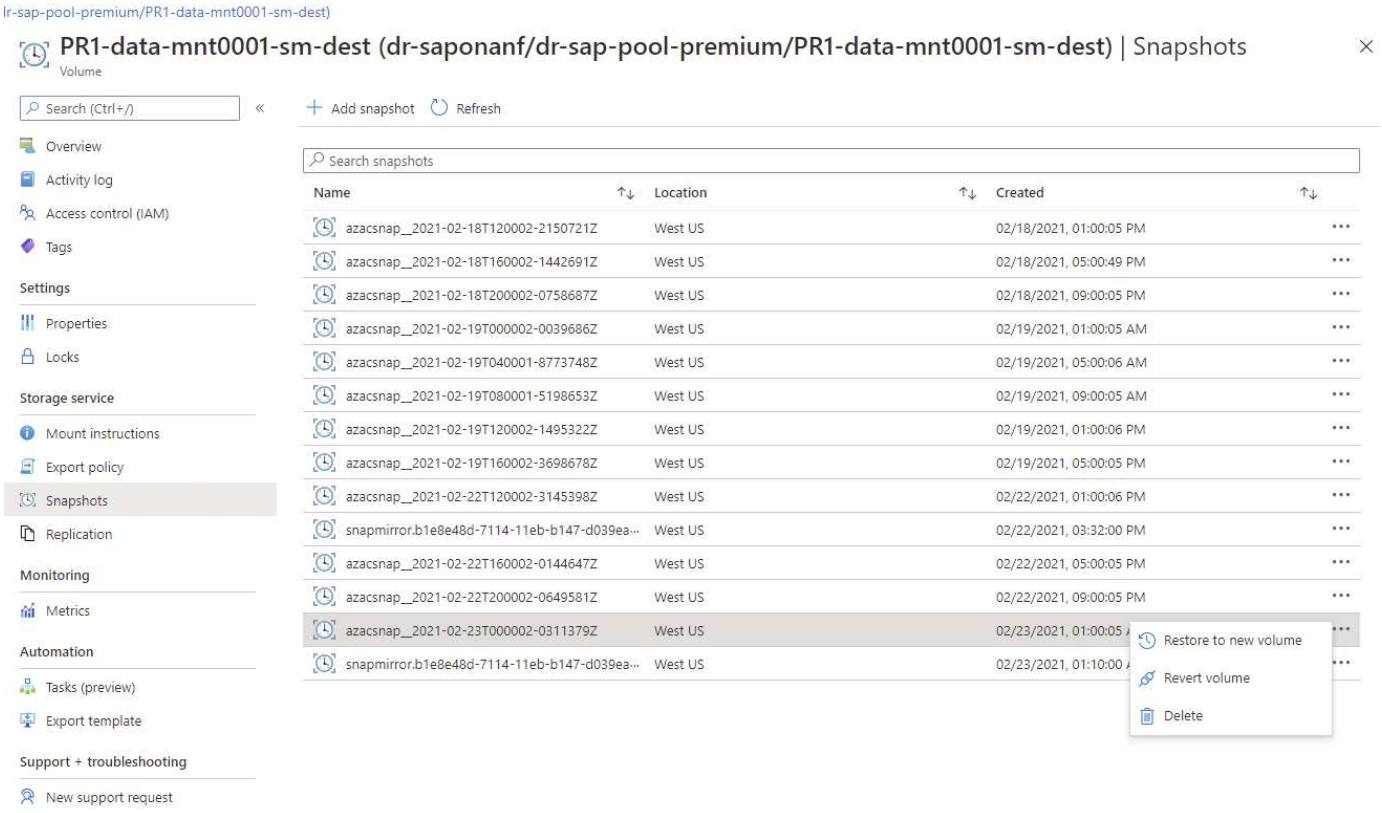
Pour le volume de données HANA, vous devez restaurer le volume vers la dernière sauvegarde Snapshot HANA créée avec AzAcSnap. Cette opération de restauration de volume n'est pas possible si le snapshot de réplication le plus récent est marqué comme étant occupé en raison du peering de réplication. Par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

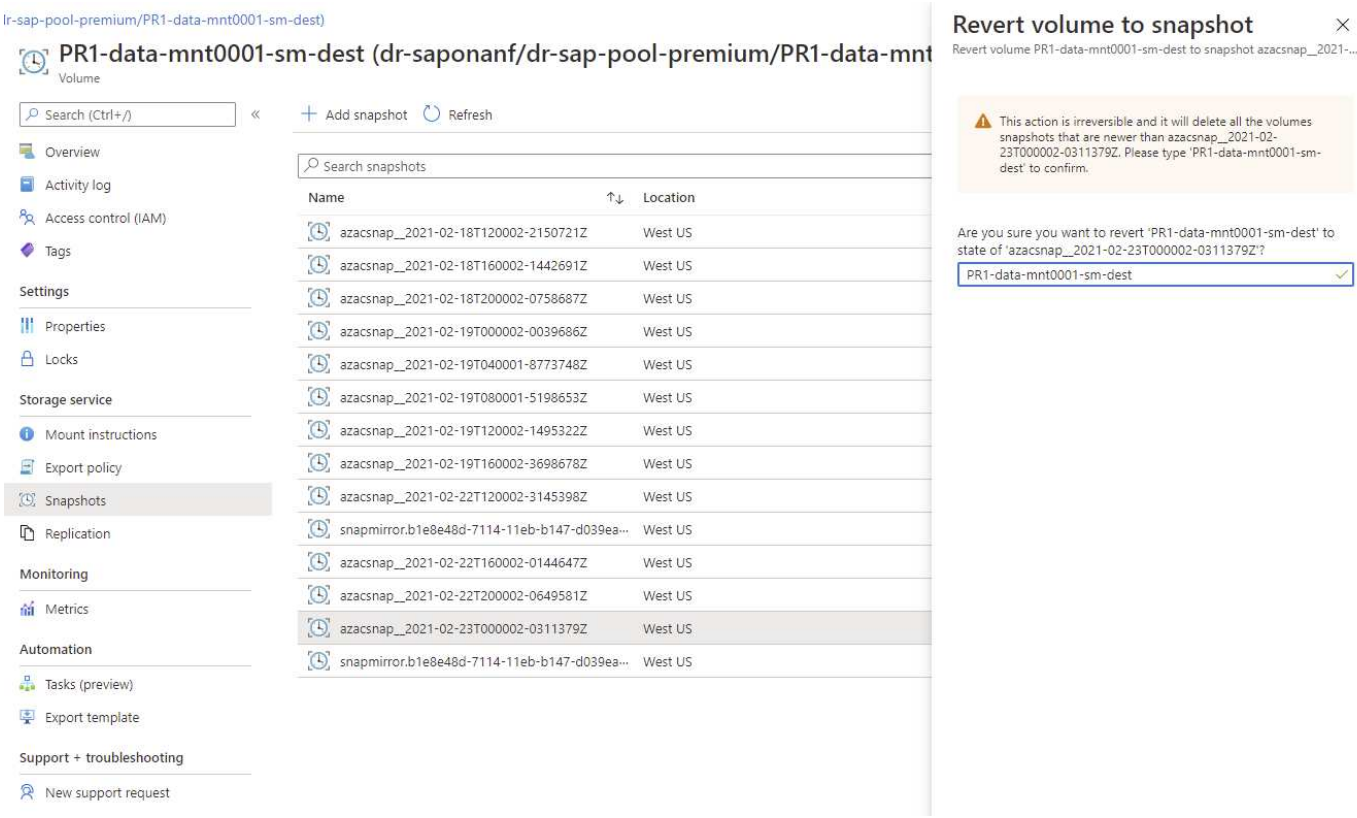
Les deux captures d'écran suivantes montrent l'opération de peering et de suppression pour le volume de données HANA. Les mêmes opérations doivent être effectuées pour la sauvegarde du journal et le volume partagé HANA.





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

Tr-4646 : reprise après incident de SAP HANA avec réplication du stockage

Nils Bauer, NetApp

Le rapport TR-4646 présente les options de protection de la reprise après incident pour SAP HANA. Vous y trouverez des informations détaillées sur la configuration et une description des cas d'utilisation d'une solution de reprise après incident sur trois sites basée sur la réplication du stockage NetApp SnapMirror synchrone et

asynchrone. La solution décrite utilise NetApp SnapCenter avec le plug-in SAP HANA pour gérer la cohérence des bases de données.

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

Tr-4313 : sauvegarde et restauration de SAP HANA à l'aide de Snap Creator

Nils Bauer, NetApp

Le rapport TR-4313 décrit l'installation et la configuration de la solution NetApp de sauvegarde et de restauration pour SAP HANA. La solution repose sur la structure NetApp Snap Creator et sur le plug-in Snap Creator pour SAP HANA. Cette solution est prise en charge par l'appliance multinœud Cisco SAP HANA certifiée combiné au stockage NetApp. Cette solution est également prise en charge avec des systèmes SAP HANA à un ou plusieurs nœuds dans le cadre de projets TDI (Tailored Data Center Integration).

https://www.netapp.com/pdf.html?item=/media/19779-tr-4313.pdf

Tr-4711 : sauvegarde et restauration de SAP HANA avec les systèmes de stockage NetApp et le logiciel CommVault

Marco Schoen, NetApp

Dr Tristan Daude, CommVault Systems

Le rapport TR-4711 décrit la conception d'une solution NetApp et CommVault pour SAP HANA, qui inclut la technologie de gestion des snapshots de CommVault IntelliSnap et la technologie NetApp Snapshot. La solution repose sur le stockage NetApp et la suite de protection des données CommVault.

https://www.netapp.com/pdf.html?item=/media/17050-tr4711pdf.pdf

NVA-1147-DESIGN : SAP HANA sur une baie SAN 100 % NetApp - SAN moderne, protection des données et reprise après incident

Nils Bauer, Roland Wartenberg, Darryl Clekshs, Daniel Hohman, Marco Schöen, Steve Botkin, Michael Peppers, Vidula Aiyer, Steve Collins, Pavan Jhamnani, Lee Dorrier, NetApp

Jim Zucchero, Naem Saafein, Ph.D., Broadcom Brocade

Cette architecture vérifiée NetApp couvre la modernisation des systèmes SAP et des opérations pour SAP HANA sur les systèmes de stockage ASA 100 % SAN NetApp avec structure SAN FC Brocade. Elle inclut la sauvegarde et la restauration, la reprise après incident et la protection des données. Cette solution exploite NetApp SnapCenter pour automatiser la sauvegarde, la restauration et la restauration SAP HANA, ainsi que les workflows de clonage. Les scénarios de configuration, de test et de basculement de la reprise d'activité sont décrits à l'aide du logiciel de réplication des données NetApp SnapMirror synchrone. Enfin, la protection des données SAP avec CommVault est décrite.

https://www.netapp.com/pdf.html?item=/media/10235-nva-1147-design.pdf

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.