Protection des bases de données SAP HANA

SnapCenter Software 4.7

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/snapcenter-47/protect-hana/concept_snapcenter_plug_in_for_sap_hana_database_overview.html on September 26, 2025. Always check docs.netapp.com for the latest.

Sommaire

Protection des bases de données SAP HANA . . . 1
Plug-in SnapCenter pour bases de données SAP HANA . . . 1
Présentation du plug-in SnapCenter pour les bases de données SAP HANA . . . 1
Comment utiliser le plug-in SnapCenter pour base de données SAP HANA . . . 1
Fonctionnalités du plug-in SnapCenter pour les bases de données SAP HANA . . . 1
Types de stockage pris en charge par le plug-in SnapCenter pour la base de données SAP HANA . . . 2
Privilèges ONTAP minimum requis pour le plug-in SAP HANA . . . 3
Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault pour les bases de données SAP HANA . . . 7
Stratégie de sauvegarde pour les bases de données SAP HANA . . . 8
Stratégie de restauration et de récupération pour les bases de données SAP HANA . . . 12
Préparez l'installation du plug-in SnapCenter pour la base de données SAP HANA . . . 14
Workflow d'installation du plug-in SnapCenter pour la base de données SAP HANA . . . 14
Conditions préalables pour l'ajout d'hôtes et l'installation du plug-in SnapCenter pour la base de données SAP HANA . . . 14
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows . . . 15
Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux . . . 16
Configurer les identifiants du plug-in SnapCenter pour la base de données SAP HANA . . . 17
Configurez GMSA sur Windows Server 2012 ou version ultérieure . . . 20
Installez le plug-in SnapCenter pour les bases de données SAP HANA . . . 21
Configurer le certificat CA . . . 27
Installation du plug-in SnapCenter pour VMware vSphere . . . 36
Déployer le certificat d'autorité de certification . . . 36
Configurez le fichier CRL . . . 36
Préparation à la protection des données . . . 36
Conditions préalables à l'utilisation du plug-in SnapCenter pour la base de données SAP HANA . . . 36
Mode d'utilisation des ressources, des groupes de ressources et des règles pour la protection des bases de données SAP HANA . . . 37
Sauvegarde des ressources SAP HANA . . . 37
Sauvegarde des ressources SAP HANA . . . 37
Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA . . . 38
Découverte des ressources et préparation de conteneurs de bases de données mutualisés pour la protection des données . . . 39
Ajoutez des ressources manuellement au plug-in hôte . . . 42
Créez des règles de sauvegarde pour les bases de données SAP HANA . . . 44
Créer des groupes de ressources et attacher des stratégies . . . 49
Sauvegarde des bases de données SAP HANA . . . 53
Sauvegarder les groupes de ressources . . . 56
Créer une connexion au système de stockage et une certification à l'aide des applets de commande PowerShell pour la base de données SAP HANA . . . 57
Sauvegarder des bases de données à l'aide des applets de commande PowerShell . . . 59
Surveiller les opérations de sauvegarde . . . 62
Annuler les opérations de sauvegarde pour SAP HANA . . . 64

Affichez les sauvegardes et les clones des bases de données SAP HANA sur la page topologie 64
Restauration des bases de données SAP HANA 66
Restaurer le flux de travail 66
Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement 66
Restaurez et récupérez une sauvegarde de base de données découverte automatiquement 68
Restaurer la base de données SAP HANA à l'aide des applets de commande PowerShell 73
Restaurer des ressources à l'aide des applets de commande PowerShell 75
Surveillez les opérations de restauration des bases de données SAP HANA 77
Clonage des sauvegardes de ressources SAP HANA 78
Workflow de clonage 78
Cloner une sauvegarde de base de données SAP HANA 79
Cloner les sauvegardes de bases de données SAP HANA à l'aide des applets de commande PowerShell 81
Surveillez les opérations de clonage de bases de données SAP HANA 83
Séparer un clone 84
Supprimez ou séparez les clones de base de données SAP HANA après la mise à niveau de SnapCenter 85

Protection des bases de données SAP HANA

Plug-in SnapCenter pour bases de données SAP HANA

Présentation du plug-in SnapCenter pour les bases de données SAP HANA

Le plug-in SnapCenter pour base de données SAP HANA est un composant côté hôte du logiciel NetApp SnapCenter qui permet de gérer la protection des données des bases de données SAP HANA avec cohérence applicative. Le plug-in pour base de données SAP HANA automatise la sauvegarde, la restauration et le clonage des bases de données SAP HANA dans votre environnement SnapCenter.

SnapCenter prend en charge le MDC (conteneur unique et base de données mutualisée). Vous pouvez utiliser le plug-in pour base de données SAP HANA dans les environnements Windows et Linux. Le plug-in qui n'est pas installé sur l'hôte de base de données HANA est appelé le plug-in hôte centralisé. Le plug-in hôte centralisé peut gérer plusieurs bases de données HANA sur plusieurs hôtes.

Lorsque le plug-in pour la base de données SAP HANA est installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Vous pouvez également utiliser le plug-in doté de la technologie SnapVault de NetApp pour effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes.

Comment utiliser le plug-in SnapCenter pour base de données SAP HANA

Lorsque vous installez le plug-in pour base de données SAP HANA dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner les bases de données SAP HANA et leurs ressources. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Ajouter des bases de données.
- Création de sauvegardes.
- Effectuez des restaurations à partir des sauvegardes.
- Sauvegardes clones.
- Planifiez les opérations de sauvegarde.
- Contrôle des opérations de sauvegarde, de restauration et de clonage
- Afficher les rapports relatifs aux opérations de sauvegarde, de restauration et de clonage.

Fonctionnalités du plug-in SnapCenter pour les bases de données SAP HANA

SnapCenter s'intègre avec l'application de plug-in et avec les technologies NetApp sur le système de stockage. Pour travailler avec le plug-in pour base de données SAP HANA, vous utilisez l'interface graphique de SnapCenter.

- **Interface utilisateur graphique unifiée**

  L'interface SnapCenter assure la standardisation et la cohérence dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de

restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- **Administration centrale automatisée**

  Vous pouvez planifier des opérations de sauvegarde, configurer la conservation des sauvegardes basée sur des règles et effectuer des opérations de restauration. Vous pouvez également surveiller votre environnement de manière proactive en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie de copie Snapshot NetApp non disruptive**

  SnapCenter utilise la technologie de copie NetApp Snapshot avec le plug-in pour les bases de données SAP HANA pour sauvegarder les ressources.

L'utilisation du plug-in pour base de données SAP HANA offre également les avantages suivants :

- Prise en charge des workflows de sauvegarde, de restauration et de clonage
- Sécurité prise en charge par le RBAC et délégation centralisée des rôles

  Vous pouvez également définir les informations d'identification de sorte que les utilisateurs SnapCenter autorisés disposent de droits d'accès au niveau de l'application.

- Création de copies compactes et ponctuelles de ressources à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

  Une licence FlexClone est requise sur le système de stockage dans lequel vous souhaitez créer le clone.

- Prise en charge de la fonctionnalité de copie Snapshot de groupe de cohérence d'ONTAP dans le cadre de la création des sauvegardes.
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de ressources

  Lors d'une opération unique, les copies Snapshot sont consolidées lorsque les ressources d'un hôte unique partagent le même volume.

- Possibilité de créer des copies Snapshot à l'aide de commandes externes.
- Prise en charge des sauvegardes basées sur des fichiers.
- Prise en charge de Linux LVM sur le système de fichiers XFS.

Types de stockage pris en charge par le plug-in SnapCenter pour la base de données SAP HANA

SnapCenter prend en charge de nombreux types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier la prise en charge de votre type de stockage avant d'installer le plug-in SnapCenter pour la base de données SAP HANA.

Machine	Type de stockage
Serveurs physiques et virtuels	LUN connectés via FC
Serveur physique	LUN connectées à l'iSCSI

Machine	Type de stockage
Serveurs physiques et virtuels	Volumes connectés par NFS

Privilèges ONTAP minimum requis pour le plug-in SAP HANA

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

Commandes All-Access : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
event generate-autosupport-log
l'historique des tâches s'affiche fin de la tâche

Commandes All-Access : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
lun
la création de lun
suppression de la lun
lun igroup add
créez un groupe initiateur lun
suppression du groupe initiateur lun
renommer la lun igroup
affichage de la lun igroup
lun mapping des nœuds supplémentaires
création d’un mappage de lun
suppression du mappage de lun
mappage de lun supprimer-rapports-nœuds
les mappages de lun s’affichent
modification de lun
déplacement des lun dans le volume
lun hors ligne
lun en ligne
suppression de la réservation persistante de lun
redimensionner la lun
série de lun
affichage de la lun

Commandes All-Access : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
ajout de règle snapmirror règle de modification de snapmirror règle de suppression de snapmirror affichage des règles snapmirror restauration snapmirror montrer snapmirror historique des données du mode snapmirror mise à jour snapmirror snapmirror update-ls-set destinations des listes snapmirror
version

Commandes All-Access : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
création de clones de volumes
clone de volume affiche
démarrage du fractionnement du clone de volume
arrêt du fractionnement du clone de volume
création de volumes
destruction des volumes
création d’un clone de fichiers de volumes
volume fichier show-disk-usage
volume hors ligne
volume en ligne
modification de volume
création de qtree volume
suppression qtree du volume
modification de qtree volume
volume qtree show
restrictions de volume
volume affiché
création de copies snapshot de volume
suppression du snapshot de volume
modification de snapshot de volume
renommage snapshot de volume
restauration snapshot du volume
fichier de restauration de snapshot de volume
snapshot de volume apparaît
démontage de volume

Commandes All-Access : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
cifs vserver
création d'un partage cifs vserver
suppression du partage cifs vserver
vserver cifs shadowcopy show
vserver cifs share show
cifs montrer un vserver
vserver export-policy
vserver export-policy créé
vserver export-policy delete
vserver export-policy create
vserver export-policy règle show
vserver export-policy show
iscsi vserver
vserver iscsi connection show
vserver show

Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
interface réseau
interface réseau affiche
un vserver

Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault pour les bases de données SAP HANA

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération de copie Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne

créez pas de planification ONTAP distincte.

> Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.

> SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "Documentation ONTAP".

> SnapCenter ne prend pas en charge la réplication **sync_mirror**.

Stratégie de sauvegarde pour les bases de données SAP HANA

Définissez une stratégie de sauvegarde pour les bases de données SAP HANA

Définir une stratégie de sauvegarde avant de créer vos tâches de sauvegarde vous aide à disposer des sauvegardes dont vous avez besoin pour restaurer ou cloner vos ressources. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

À propos de cette tâche

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés à la prestation, notamment la disponibilité et les performances du service. Le RTO est le moment par lequel un processus métier doit être restauré suite à une interruption de service. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de protection des données.

Étapes

1. Déterminez à quel moment il est nécessaire de sauvegarder vos ressources.
2. Déterminer le nombre de tâches de sauvegarde dont vous avez besoin
3. Choisissez le nom de vos sauvegardes.
4. Décider de créer ou non une règle Snapshot pour sauvegarder des copies Snapshot cohérentes au niveau des applications de la base de données
5. Décidez si vous voulez vérifier l'intégrité de la base de données.
6. Choisissez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réplication ou la technologie NetApp SnapVault pour la conservation à long terme.
7. Déterminez la période de conservation des copies Snapshot sur le système de stockage source et la destination SnapMirror.

8. Déterminez si vous souhaitez exécuter des commandes avant ou après l'opération de sauvegarde et fournissez un prescripteur ou un PostScript.

Découverte automatique des ressources sur l'hôte Linux

Les ressources sont les bases de données SAP HANA et les volumes non data sur l'hôte Linux gérés par SnapCenter. Après avoir installé le plug-in SnapCenter pour la base de données SAP HANA, les bases de données SAP HANA sur cet hôte Linux sont automatiquement découvertes et affichées sur la page Ressources.

La découverte automatique est prise en charge pour les ressources SAP HANA suivantes :

- Des conteneurs uniques

  Après l'installation ou la mise à niveau du plug-in, les ressources du conteneur unique situées sur un plug-in hôte centralisé continueront d'être ajoutées manuellement.

  Après l'installation ou la mise à niveau du plug-in, les bases de données SAP HANA sont automatiquement découvertes uniquement sur les hôtes SAP HANA Linux, qui sont directement enregistrés dans SnapCenter.

- Conteneur de base de données mutualisée (MDC)

  Après l'installation ou la mise à niveau du plug-in, les ressources MDC situées sur un plug-in d'hôte centralisé continueront d'être ajoutées manuellement.

  Après la mise à niveau vers SnapCenter 4.3, vous devez continuer à ajouter manuellement les ressources MDC sur le plug-in d'hôte centralisé.

  Pour les hôtes SAP HANA Linux directement enregistrés dans SnapCenter, l'installation ou la mise à niveau du plug-in déclenchera une détection automatique des ressources sur l'hôte. Après la mise à niveau du plug-in, pour chaque ressource MDC située sur l'hôte du plug-in, une autre ressource MDC sera automatiquement découverte avec un format GUID différent et enregistrée dans SnapCenter. La nouvelle ressource sera à l'état verrouillé.

  Par exemple, dans SnapCenter 4.2, si la ressource MDC E90 était située sur l'hôte du plug-in et enregistrée manuellement, après la mise à niveau vers SnapCenter 4.3, une autre ressource MDC E90 avec un GUID différent sera découverte et enregistrée dans SnapCenter.

La détection automatique n'est pas prise en charge pour les configurations suivantes :

- Dispositions RDM et VMDK

  Lorsque les ressources ci-dessus sont découvertes, les opérations de protection des données ne sont pas prises en charge sur ces ressources.

- Configuration HANA avec plusieurs hôtes
- Plusieurs instances sur le même hôte
- Réplication système HANA scale-out multi-niveaux
- Environnement de réplication en cascade en mode réplication du système

Types de sauvegardes pris en charge

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge la sauvegarde basée sur fichier et les types de sauvegarde basés sur des copies Snapshot pour les bases de données SAP HANA.

Sauvegarde basée sur des fichiers

Les sauvegardes basées sur des fichiers vérifient l'intégrité de la base de données. Vous pouvez planifier l'opération de sauvegarde basée sur des fichiers afin d'effectuer à des intervalles spécifiques. Seuls les locataires actifs sont sauvegardés. Vous ne pouvez ni restaurer ni cloner des sauvegardes basées sur des fichiers à partir de SnapCenter.

Sauvegarde basée sur des copies Snapshot

Les sauvegardes basées sur des copies Snapshot exploitent la technologie de copie NetApp Snapshot pour créer des copies en ligne en lecture seule des volumes sur lesquels résident les bases de données SAP HANA.

Comment le plug-in SnapCenter pour la base de données SAP HANA utilise les copies Snapshot de groupe de cohérence

Ce plug-in permet de créer des copies Snapshot de groupe de cohérence pour les groupes de ressources. Un groupe de cohérence est un conteneur qui peut héberger plusieurs volumes, de sorte que vous puissiez les gérer comme une entité unique. Un groupe de cohérence est constitué de copies Snapshot simultanées de plusieurs volumes, ce qui permet d'obtenir des copies cohérentes d'un groupe de volumes.

Vous pouvez également spécifier le temps d'attente avant que le contrôleur de stockage ne grouper les copies Snapshot de manière cohérente. Les options de temps d'attente disponibles sont **urgent**, **Moyen** et **détendu**. Vous pouvez également activer ou désactiver la synchronisation WAFL (Write Anywhere File Layout) au cours des copies Snapshot de groupe cohérentes. La synchronisation WAFL améliore les performances de la copie Snapshot de groupe de cohérence.

SnapCenter gère l'organisation des sauvegardes de journaux et de données

SnapCenter gère l'organisation des sauvegardes des journaux et des données au niveau du système de stockage et des systèmes de fichiers, ainsi que dans le catalogue des sauvegardes SAP HANA.

Les copies Snapshot du stockage primaire ou secondaire et les entrées correspondantes dans le catalogue SAP HANA sont supprimées en fonction des paramètres de conservation. Les entrées du catalogue SAP HANA sont également supprimées lors de la sauvegarde et de la suppression des groupes de ressources.

Considérations relatives à la détermination des planifications de sauvegarde pour les bases de données SAP HANA

Le facteur le plus important dans la détermination d'un planning de sauvegarde est le taux de modification de la ressource. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. D'autres facteurs entrent en ligne de compte l'importance des

ressources pour votre entreprise, votre contrat de niveau de service et votre objectif de point de récupération (RPO).

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes (fréquence des sauvegardes)

  La fréquence de sauvegarde, également appelée type de planification pour certains plug-ins, fait partie d'une configuration de règles. Par exemple, vous pouvez configurer la fréquence des sauvegardes sous forme horaire, quotidienne, hebdomadaire ou mensuelle.

- Planifications de sauvegardes (exactement quand les sauvegardes doivent être effectuées

  Les planifications de sauvegarde font partie d'une configuration de ressource ou de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour la sauvegarder tous les jeudis à 10 h 00

Nombre de tâches de sauvegarde nécessaires pour les bases de données SAP HANA

Les facteurs qui déterminent le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la ressource, le nombre de volumes utilisés, le taux de changement de la ressource et votre contrat de niveau de service.

Conventions de nom de sauvegarde pour le plug-in pour bases de données SAP HANA

Vous pouvez utiliser la convention d'appellation de copie Snapshot par défaut ou la convention de nom personnalisée. la convention de nommage des sauvegardes par défaut ajoute un horodatage aux noms de copie Snapshot qui vous aide à identifier le moment de la création des copies.

La copie Snapshot utilise la convention de nom par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.
- *mach1x88* est le nom d'hôte.
- *03-12-2015_23.17.26* est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de la copie Snapshot tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, clienttext_resourcegroup_policy_hostname ou resourcegroup_hostname. Par défaut, le suffixe numérique est ajouté au nom de la copie Snapshot.

Stratégie de restauration et de récupération pour les bases de données SAP HANA

Définissez une stratégie de restauration et de reprise pour les ressources SAP HANA

Vous devez définir une stratégie avant de restaurer et de récupérer votre base de données pour que vous puissiez effectuer correctement les opérations de restauration et de récupération.

Étapes

1. Déterminez les stratégies de restauration prises en charge pour les ressources SAP HANA ajoutées manuellement
2. Déterminez les stratégies de restauration prises en charge pour les bases de données SAP HANA découvertes automatiquement
3. Choisissez le type d'opérations de restauration à effectuer.

Types de stratégies de restauration pris en charge pour les ressources SAP HANA ajoutées manuellement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter. Il existe deux types de stratégies de restauration pour les ressources SAP HANA ajoutées manuellement. Vous ne pouvez pas restaurer des ressources SAP HANA ajoutées manuellement.

Vous ne pouvez pas restaurer des ressources SAP HANA ajoutées manuellement.

Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource

Si la ressource contient des volumes ou des qtrees, les copies Snapshot sont supprimées après la copie Snapshot sélectionnée pour être restaurées sur de tels volumes ou qtrees et ne peuvent pas être restaurées. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

Restauration au niveau des fichiers

- Restaure les fichiers à partir de volumes, de qtrees ou de répertoires
- Restaure uniquement les LUN sélectionnées

Types de stratégies de restauration pris en charge pour les bases de données SAP HANA automatiquement découvertes

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter. Il existe deux types de stratégies de restauration pour les bases de données SAP HANA automatiquement découvertes.

Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource

◦ L'option **Volume Revert** doit être sélectionnée pour restaurer l'intégralité du volume.

> Si la ressource contient des volumes ou des qtrees, les copies Snapshot sont supprimées après la copie Snapshot sélectionnée pour être restaurées sur de tels volumes ou qtrees et ne peuvent pas être restaurées. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

Base de données des locataires

- Restaure la base de données des locataires

Si l'option **tenant Database** est sélectionnée, vous devez utiliser des scripts de reprise HANA Studio ou HANA externes à SnapCenter pour effectuer l'opération de reprise.

Types d'opérations de restauration des bases de données SAP HANA découvertes automatiquement

SnapCenter prend en charge la technologie SnapRestore (VBSR) basée sur des volumes, le SnapRestore de fichiers uniques et les types de restauration de connexion et de copie pour les bases de données SAP HANA automatiquement découvertes.

La technologie SnapRestore basée sur les volumes (VBSR) est effectuée dans des environnements NFS pour les scénarios suivants :

- Lorsque la sauvegarde sélectionnée pour la restauration est prise sur des versions antérieures à SnapCenter 4.3 et uniquement si l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde sélectionnée pour la restauration est prise dans SnapCenter 4.3 et si l'option **Retour volume** est sélectionnée

Single File SnapRestore s'effectue dans des environnements NFS pour les scénarios suivants :

- Lorsque la sauvegarde sélectionnée pour la restauration est prise dans SnapCenter 4.3 et que seule l'option **ressource complète** est sélectionnée
- Pour les conteneurs de base de données multilocataires (MDC), lorsque la sauvegarde sélectionnée pour la restauration est prise sur SnapCenter 4.3 et que l'option **base de données locataire** est sélectionnée
- Lorsque la sauvegarde sélectionnée provient d'un emplacement secondaire SnapMirror ou SnapVault et que l'option **Complete Resource** est sélectionnée

Single File SnapRestore s'effectue dans des environnements SAN pour les scénarios suivants :

- Lorsque des sauvegardes sont effectuées sur des versions antérieures à SnapCenter 4.3 et uniquement si l'option **ressource complète** est sélectionnée
- Lorsque des sauvegardes sont effectuées dans SnapCenter 4.3, et seulement si l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde est sélectionnée depuis un emplacement secondaire SnapMirror ou SnapVault et l'option **Complete Resource** est sélectionnée

La restauration par connexion ou copie s'effectue dans des environnements SAN pour le scénario suivant :

- Pour MDC, lorsque la sauvegarde sélectionnée pour la restauration est prise dans SnapCenter 4.3 et que l'option **base de données locataire** est sélectionnée

Les options ressource complète, **Retour de volume** et **base de données locataire** sont disponibles sur la page étendue de la restauration.

Types d'opérations de récupération pris en charge pour les bases de données SAP HANA

SnapCenter permet d'effectuer différents types d'opérations de restauration pour les bases de données SAP HANA.

- Restaurez la base de données à l'état le plus récent
- Restaurez la base de données à un point dans le temps spécifique

  Vous devez indiquer la date et l'heure de la récupération.

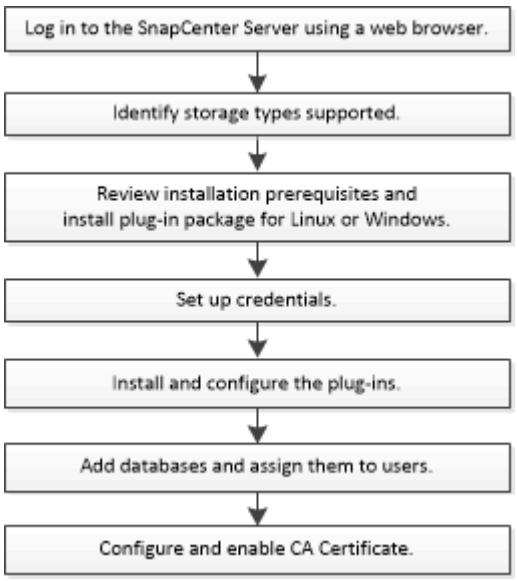
- Restaurer la base de données jusqu'à une sauvegarde de données spécifique

SnapCenter fournit également l'option pas de restauration pour les bases de données SAP HANA.

Préparez l'installation du plug-in SnapCenter pour la base de données SAP HANA

Workflow d'installation du plug-in SnapCenter pour la base de données SAP HANA

Vous devez installer et configurer le plug-in SnapCenter pour base de données SAP HANA si vous souhaitez protéger vos bases de données SAP HANA.



Conditions préalables pour l'ajout d'hôtes et l'installation du plug-in SnapCenter pour la base de données SAP HANA

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises. Le plug-in SnapCenter pour base de données SAP HANA est disponible dans les environnements Windows et Linux.

- Vous devez avoir installé Java 1.8 64 bits sur votre hôte.

  IBM Java n'est pas pris en charge.

- Vous devez avoir installé le terminal interactif de la base de données SAP HANA (client HDBSQL) sur l'hôte.
- Pour Windows, Plug-in Creator Service doit être en cours d'exécution à l'aide de l'utilisateur Windows « LocalSystem », ce qui est le comportement par défaut lorsque Plug-in pour SAP HANA Database est installé en tant qu'administrateur de domaine.
- Pour Windows, les clés de la boutique utilisateur doivent être créées en tant qu'utilisateur SYSTÈME.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte. Le plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in SAP HANA sur les hôtes Windows.
- Pour l'hôte Linux, les clés HDB Secure User Store sont accessibles en tant qu'utilisateur HDBSQL OS.
- Le serveur SnapCenter doit avoir accès au port 8145 ou personnalisé du plug-in pour l'hôte de base de données SAP HANA.

Hôtes Windows

- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour base de données SAP HANA sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 1.8 64 bits sur votre hôte Windows.

  "Téléchargements Java pour tous les systèmes d'exploitation"

  "Matrice d'interopérabilité NetApp"

Hôtes Linux

- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 1.8 64 bits sur votre hôte Linux.

  "Téléchargements Java pour tous les systèmes d'exploitation"

  "Matrice d'interopérabilité NetApp"

- Pour les bases de données SAP HANA qui s'exécutent sur un hôte Linux, lors de l'installation du plug-in pour base de données SAP HANA, le plug-in SnapCenter pour UNIX est installé automatiquement.

Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	Microsoft Windows Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	5 GO Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.
Packs logiciels requis	• Microsoft .NET Framework 4.7.2 ou version ultérieure • Windows Management Framework (WMF) 4.0 ou version ultérieure • PowerShell 4.0 ou version ultérieure Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp". Pour plus d'informations sur le dépannage de .NET, reportez-vous à la section "Échec de la mise à niveau ou de l'installation de SnapCenter pour les systèmes hérités qui ne disposent pas d'une connexion Internet".

Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux

Avant d'installer le module de plug-ins SnapCenter pour Linux, vous devez connaître certains besoins en espace système hôte de base et en dimensionnement.

Élément	De formation
Systèmes d'exploitation	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	2 GO Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.
Packs logiciels requis	Java 1.8.x (64 bits)Java Oracle et OpenJDK Flavors Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans /var/opt/snapcenter/spl/etc/spl.properties est définie sur la version JAVA correcte et le chemin correct. Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".

Configurer les identifiants du plug-in SnapCenter pour la base de données SAP HANA

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour exécuter des opérations de protection des données sur des bases de données ou des systèmes de fichiers Windows.

À propos de cette tâche

- Hôtes Linux

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Linux.

Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

Meilleure pratique: bien que vous soyez autorisé à créer des informations d'identification pour Linux après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

- Hôtes Windows

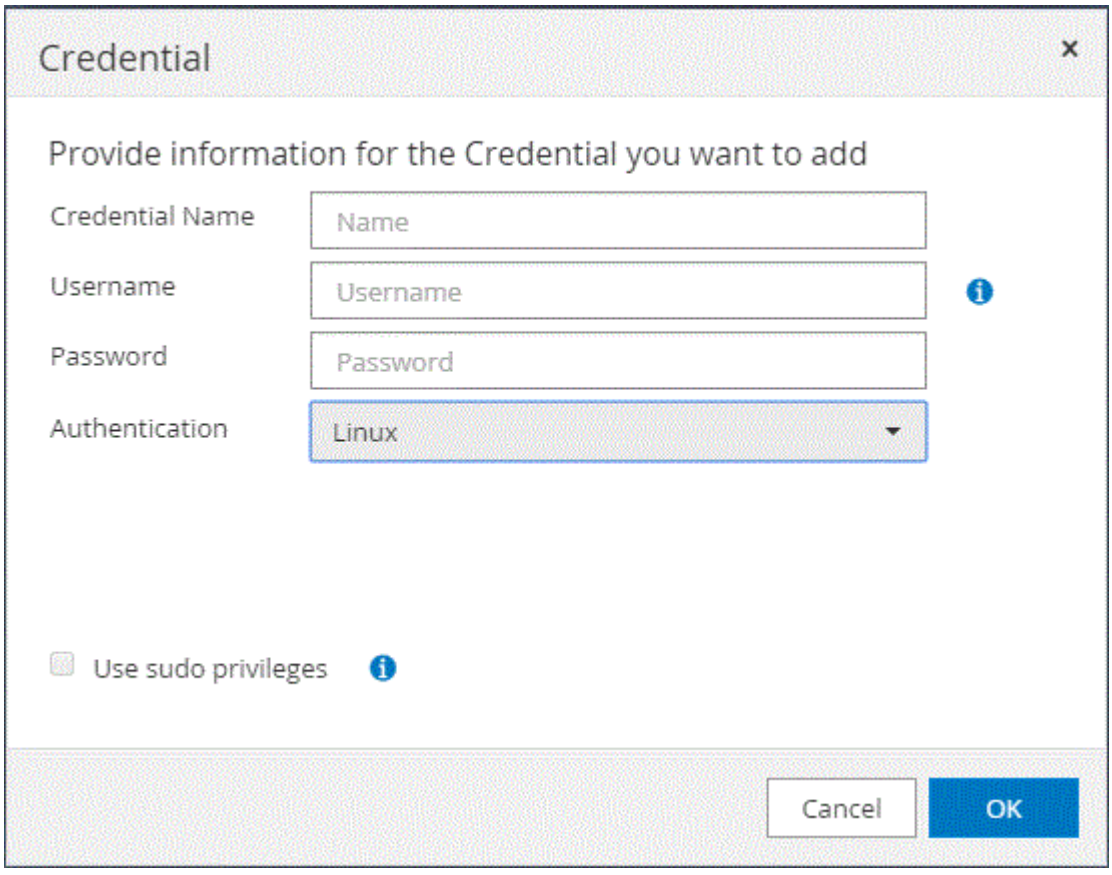
  Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

  Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.



4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des

informations d'identification :

Pour ce champ…	Procédez comme ça…
Nom d'identification	Saisissez un nom pour les informations d'identification.
Nom d'utilisateur	Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification. • Administrateur de domaine ou tout membre du groupe d'administrateurs Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants : ◦ *NetBIOS\username* ◦ *Domain FQDN\username* • Administrateur local (groupes de travail uniquement) Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : *username* N'utilisez pas de guillemets (") ou de contre-coches (") dans les mots de passe. Vous ne devez pas utiliser moins de (<) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins<!10, moins dix<!, contre-recul 12.
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.

Pour ce champ…	Procédez comme ça…
Utilisez les privilèges sudo	Cochez la case **utiliser privilèges sudo** si vous créez des informations d'identification pour un utilisateur non-root. Applicable uniquement aux utilisateurs Linux.

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs de la page utilisateur et accès.

Configurez GMSA sur Windows Server 2012 ou version ultérieure

Windows Server 2012 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

Ce dont vous aurez besoin

- Vous devez disposer d'un contrôleur de domaine Windows Server 2012 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2012 ou version ultérieure, qui est membre du domaine.

Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediely
3. Créez et configurez votre GMSA :
   a. Créez un compte de groupe d'utilisateurs au format suivant :

```
 domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.
```

   Par exemple :

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
```

4. Configurez le GMSA sur vos hôtes :

a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

   Pour ce faire lancer la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

   a. Redémarrez votre hôte.

   b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`

   c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`

5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

   Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

Installez le plug-in SnapCenter pour les bases de données SAP HANA

Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte individuel ou pour un cluster.

Ce dont vous aurez besoin

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.

- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

  "Configurez le compte de service géré par groupe sous Windows Server 2012 ou version ultérieure pour SAP HANA"

À propos de cette tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.
- Pour la réplication système SAP HANA afin de détecter les ressources sur les systèmes principal et secondaire, il est recommandé d'ajouter à la fois les systèmes principal et secondaire à l'aide de l'utilisateur root ou sudo.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ…	Procédez comme ça…
Type d'hôte	Sélectionnez le type d'hôte : • Répertoires de base • Linux Le plug-in pour SAP HANA est installé sur l'hôte client HDBSQL et cet hôte peut se trouver sur un système Windows ou Linux.
Nom d'hôte	Entrez le nom d'hôte de communication. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN. Vous devez configurer le client HDBSQL et HDBUserStore sur cet hôte.

Pour ce champ…	Procédez comme ça…
Informations d'identification	Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification. Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez fourni. Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.
6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ…	Procédez comme ça…
Port	Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut. Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.
Chemin d'installation	Le plug-in pour SAP HANA est installé sur l'hôte client HDBSQL et cet hôte peut se trouver sur un système Windows ou Linux. • Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez également personnaliser le chemin. • Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/NetApp/snapcenter. Vous pouvez également personnaliser le chemin.

Pour ce champ…	Procédez comme ça…
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	Pour l'hôte Windows, cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in. Indiquez le nom GMSA au format suivant : domainname\accountName$. GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows.

7. Cliquez sur **soumettre**.

   Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET, l'emplacement (pour les plug-ins Windows) et la version Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. Si la configuration minimale requise n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

   Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse C:\Program Files\NetApp\SnapCenter WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.

   Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

8. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

   Dans une configuration de cluster, vous devez vérifier l'empreinte de chacun des nœuds du cluster.

   La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte a été confirmée.

9. Surveillez la progression de l'installation.

   Les fichiers journaux spécifiques à l'installation se trouvent dans /custom_location/snapcenter/logs.

Installez les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer simultanément les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes à l'aide de l'applet de commande Install-SmHostPackage PowerShell.

Ce dont vous aurez besoin

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande Open-SmConnection, puis saisissez vos informations d'identification.
3. Installez le plug-in sur plusieurs hôtes à l'aide de l'applet de commande Install-SmHostPackage et des paramètres requis.

   Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

   Vous pouvez utiliser l'option -skipprecheck lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

4. Saisissez vos informations d'identification pour l'installation à distance.

Installez le plug-in SnapCenter pour SAP HANA Database sur des hôtes Linux à l'aide de l'interface de ligne de commandes

Vous devez installer le plug-in SnapCenter pour la base de données SAP HANA à l'aide de l'interface utilisateur de SnapCenter. Si votre environnement n'autorise pas l'installation à distance du plug-in à partir de l'interface utilisateur SnapCenter, vous pouvez installer le plug-in pour base de données SAP HANA en mode console ou en mode silencieux à l'aide de l'interface de ligne de commandes.

Ce dont vous aurez besoin

- Vous devez installer le plug-in pour la base de données SAP HANA sur chacun des hôtes Linux sur lesquels réside le client HDBSQL.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour la base de données SAP HANA doit répondre aux exigences des logiciels, bases de données et systèmes d'exploitation qui en dépendent.

  La matrice d'interopérabilité (IMT) contient les dernières informations sur les configurations prises en charge.

  "Matrice d'interopérabilité NetApp"

- Le plug-in SnapCenter pour base de données SAP HANA fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer SnapCenter Plug-ins Package pour Linux, vous devez avoir déjà installé

SnapCenter sur un hôte Windows.

Étapes

1. Copiez le fichier d'installation du package de plug-ins SnapCenter pour Linux (snapcenter_linux_host_plugin.bin) depuis C:\ProgramData\NetApp\SnapCenter\Package Repository vers l'hôte où vous souhaitez installer le plug-in pour la base de données SAP HANA.

   Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installez le plug-in : `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT spécifie le port de communication SMCore HTTPS.
   - -DSERVER_IP spécifie l'adresse IP du serveur SnapCenter.
   - -DSERVER_HTTPS_PORT spécifie le port HTTPS du serveur SnapCenter.
   - -DUSER_INSTALL_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
   - DINSTALL_LOG_NAME indique le nom du fichier journal.

   ```
   /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
   -DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
   -DUSER_INSTALL_DIR=/opt
   -DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
   -DCHOSEN_FEATURE_LIST=CUSTOM
   ```

4. Modifiez le fichier /<répertoire d'installation>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, puis ajoutez le paramètre PLUGINS_ENABLED = hana:3.0.
5. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande Add-Smhost et des paramètres requis.

   Les informations relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Contrôler l'état de l'installation du plug-in pour SAP HANA

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-

- En cours
- Terminé avec succès
- Échec
- Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
- En file d'attente

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, pour filtrer la liste de manière à ce que seules les opérations d'installation du plug-in soient répertoriées, procédez comme suit :
   a. Cliquez sur **Filtrer**.
   b. Facultatif : spécifiez les dates de début et de fin.
   c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
   d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
   e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Configurer le certificat CA

Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "Comment générer un fichier CSR de certificat CA".

> Si vous possédez le certificat de l'autorité de certification pour votre domaine (*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier** > **Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root** > **certificats – ordinateur local** > **autorités de certification racines de confiance** > **certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches** > **Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant…	Procédez comme suit…
Importer une clé privée	Sélectionnez l'option **Oui**, importez la clé privée, puis cliquez sur **Suivant**.
Importer le format de fichier	N'apportez aucune modification ; cliquez sur **Suivant**.
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur **Suivant**.
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur **Terminer** pour lancer l'importation.

> Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : *.pfx, *.p12 et *.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
   a. Double-cliquez sur le certificat.
   b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.

c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.

d. Copiez les caractères hexadécimaux de la zone.

e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :

a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

Get-ChildItem -Path Cert:\Localmachine\My

b. Copiez l'empreinte.

Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

Par exemple :

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte
Windows, en exécutant les commandes suivantes :
```

```
> $cert = "<certificate thumbprint>"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

Configurez le certificat d’autorité de certification pour le service de plug-ins SnapCenter SAP HANA sur l’hôte Linux

Vous devez gérer le mot de passe du magasin de clés de plug-ins personnalisé et de son certificat, configurer le certificat de l’autorité de certification, configurer les certificats racine ou intermédiaires sur le magasin de confiance des plug-ins personnalisés et configurer la paire de clés signée par l’autorité de certification sur le magasin de confiance des plug-ins personnalisés avec le service des plug-ins personnalisés SnapCenter pour activer le certificat numérique installé.

Les plug-ins personnalisés utilisent le fichier « keystore.jks », qui se trouve à l’adresse */opt/NetApp/snapcenter/scc/etc* comme magasin de confiance et comme magasin de clés.

Gérer le mot de passe pour le magasin de clés de plug-in personnalisé et l’alias de la paire de clés signée par l’autorité de certification utilisée

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés enfichable personnalisé à partir du fichier de propriétés de l’agent du plug-in personnalisé.

   C’est la valeur correspondant à la clé 'KEYSTORE_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
 keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   Procédez de même pour la clé KEYSTORE_PASS dans le fichier *agent.properties*.

3. Redémarrez le service après avoir modifié le mot de passe.

> Le mot de passe du magasin de clés de plug-in personnalisé et de tous les mots de passe d’alias associés à la clé privée doivent être identiques.

Configurez les certificats racine ou intermédiaire sur le magasin de confiance du plug-in personnalisé

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée sur le magasin de confiance du plug-in personnalisé.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in : /opt/NetApp/snapcenter/scc/etc
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Ajouter un certificat racine ou intermédiaire :

   ```
    keytool -import -trustcacerts -alias myRootCA -file
   /root/USERTrustRSA_Root.cer -keystore keystore.jks
   . Redémarrez le service après avoir configuré les certificats racine ou
   intermédiaire sur le magasin de confiance personnalisé du plug-in.
   ```

Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

Configurez la paire de clés signée CA sur un plug-in de stockage en fiducie personnalisé

Vous devez configurer la paire de clés signées CA dans le magasin de confiance personnalisé du plug-in.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in /opt/NetApp/snapcenter/scc/etc
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Répertorier les certificats ajoutés dans le magasin de clés.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe de magasin de clés personnalisé par défaut est la valeur du FICHIER KEYSTORE_PASS dans le fichier agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Si le nom d'alias du certificat de l'autorité de certification est
long et contient de l'espace ou des caractères spéciaux ("*",","),
remplacez le nom d'alias par un nom simple :
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurez le nom d'alias à partir du certificat CA dans le fichier
agent.properties.
```

Mettez cette valeur à jour par rapport à la clé SCC_CERTIFICATE_ALIAS.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification dans le magasin de confiance personnalisé du plug-in.

Configurez la liste de révocation de certificats (CRL) pour les plug-ins personnalisés SnapCenter

À propos de cette tâche

- Les plug-ins personnalisés SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins personnalisés SnapCenter est opt/NetApp/snapcenter/etc/crl.

Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier agent.properties par rapport à la clé CRL_PATH.

   Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

Configurez le certificat d'autorité de certification pour le service de plug-ins SnapCenter SAP HANA sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés de plug-ins personnalisé et de son certificat, configurer le certificat de l'autorité de certification, configurer les certificats racine ou intermédiaires sur le magasin de confiance des plug-ins personnalisés et configurer la paire de clés signée par l'autorité de certification sur le magasin de confiance des plug-ins personnalisés avec le service des plug-ins personnalisés SnapCenter pour activer le certificat numérique installé.

Les plug-ins personnalisés utilisent le fichier *keystore.jks*, qui se trouve à l'adresse *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc* comme magasin de confiance et magasin de clés.

Gérer le mot de passe pour le magasin de clés de plug-in personnalisé et l'alias de la paire de clés signée par l'autorité de certification utilisée

Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés enfichable personnalisé à partir du fichier de propriétés de l'agent du plug-in personnalisé.

   C'est la valeur correspondant à la clé *KEYSTORE_PASS*.

2. Modifiez le mot de passe du magasin de clés :

   keytool -storepasswd -keystore keystore.jks

   Si la commande "keytool" n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

   C:\Program Files\Java\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :

   keytool -keypasswd -alias "alias_name_in_cert" -keystore.jks

   Procédez de même pour la clé KEYSTORE_PASS dans le fichier *agent.properties*.

4. Redémarrez le service après avoir modifié le mot de passe.

   Le mot de passe du magasin de clés de plug-in personnalisé et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurez les certificats racine ou intermédiaire sur le magasin de confiance du plug-in personnalisé

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée sur le magasin de confiance du plug-in personnalisé.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

   keytool -list -v -keystore keystore.jks

4. Ajouter un certificat racine ou intermédiaire :

   Keytool -import -trucacts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaire sur le magasin de confiance personnalisé du plug-in.

Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

Configurez la paire de clés signée CA sur un plug-in de stockage en fiducie personnalisé

Vous devez configurer la paire de clés signées CA dans le magasin de confiance personnalisé du plug-in.

Étapes

1. Accédez au dossier contenant le magasin de clés personnalisé du plug-in *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Localisez le fichier *keystore.jks*.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

   keytool -list -v -keystore keystore.jks

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

   Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -desstoretype JKS

5. Répertorier les certificats ajoutés dans le magasin de clés.

   keytool -list -v -keystore keystore.jks

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

   Le mot de passe de magasin de clés personnalisé par défaut est la valeur du FICHIER KEYSTORE_PASS dans le fichier agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configurez le nom d'alias à partir du certificat CA dans le fichier *agent.properties*.

   Mettez cette valeur à jour par rapport à la clé SCC_CERTIFICATE_ALIAS.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification dans le magasin de confiance personnalisé du plug-in.

Configurez la liste de révocation de certificats (CRL) pour les plug-ins personnalisés SnapCenter

À propos de cette tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section "Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter".
- Les plug-ins personnalisés SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins personnalisés SnapCenter est *'C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\ etc\crl'*.

Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier *agent.properties* par rapport à la clé CRL_PATH.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

   Les certificats entrants seront vérifiés pour chaque CRL.

Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

Ce dont vous aurez besoin

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande run *set-SmCertificateSettings*.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de *get-SmCertificateSettings*.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

Après la fin

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

- * Indique que le certificat de l'autorité de certification n'est ni activé ni attribué à l'hôte du plug-in.
- * * Indique que le certificat de l'autorité de certification a été validé avec succès.
- * * Indique que le certificat de l'autorité de certification n'a pas pu être validé.
- * indique que les informations de connexion n'ont pas pu être récupérées.

> Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

Installation du plug-in SnapCenter pour VMware vSphere

Si votre base de données est stockée sur des machines virtuelles (VM) ou si vous souhaitez protéger des machines virtuelles et des datastores, vous devez déployer le plug-in SnapCenter pour l'appliance virtuelle VMware vSphere.

Pour plus d'informations sur le déploiement, reportez-vous à la section "Présentation du déploiement".

Déployer le certificat d'autorité de certification

Pour configurer le certificat d'autorité de certification avec le plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "Créez ou importez un certificat SSL".

Configurez le fichier CRL

Le plug-in SnapCenter pour VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour le plug-in SnapCenter pour VMware vSphere est */opt/netapp/config/crl*.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

Préparation à la protection des données

Conditions préalables à l'utilisation du plug-in SnapCenter pour la base de données SAP HANA

Avant d'utiliser le plug-in SnapCenter pour base de données SAP HANA, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches préalables.

- Installer et configurer SnapCenter Server.
- Connectez-vous au serveur SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage et en créant des identifiants, le cas échéant.
- Installez Java 1.7 ou Java 1.8 sur votre hôte Linux ou Windows.

  Vous devez définir le chemin Java dans la variable de chemin d'environnement de la machine hôte.

- Configurer SnapMirror et SnapVault pour la réplication de sauvegarde.
- Installez le client HDBSQL sur l'hôte sur lequel vous installerez le plug-in pour la base de données SAP HANA.

  Configurez les clés de magasin utilisateur pour les nœuds SAP HANA que vous allez gérer via cet hôte.

- Pour la base de données SAP HANA 2.0SPS05, si vous utilisez un compte utilisateur de base de données SAP HANA, assurez-vous que vous disposez des autorisations suivantes pour effectuer des opérations de sauvegarde, de restauration et de clonage dans SnapCenter Server :
  - Administrateur des sauvegardes

- Lecture du catalogue
- Administrateur de sauvegarde de base de données
- Opérateur de récupération de base de données

Mode d'utilisation des ressources, des groupes de ressources et des règles pour la protection des bases de données SAP HANA

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des bases de données SAP HANA que vous sauvegardez ou clonez avec SnapCenter.
- Un groupe de ressources SnapCenter est un ensemble de ressources sur un hôte.

  Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

  Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

- Les règles spécifient la fréquence des sauvegardes, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

  Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

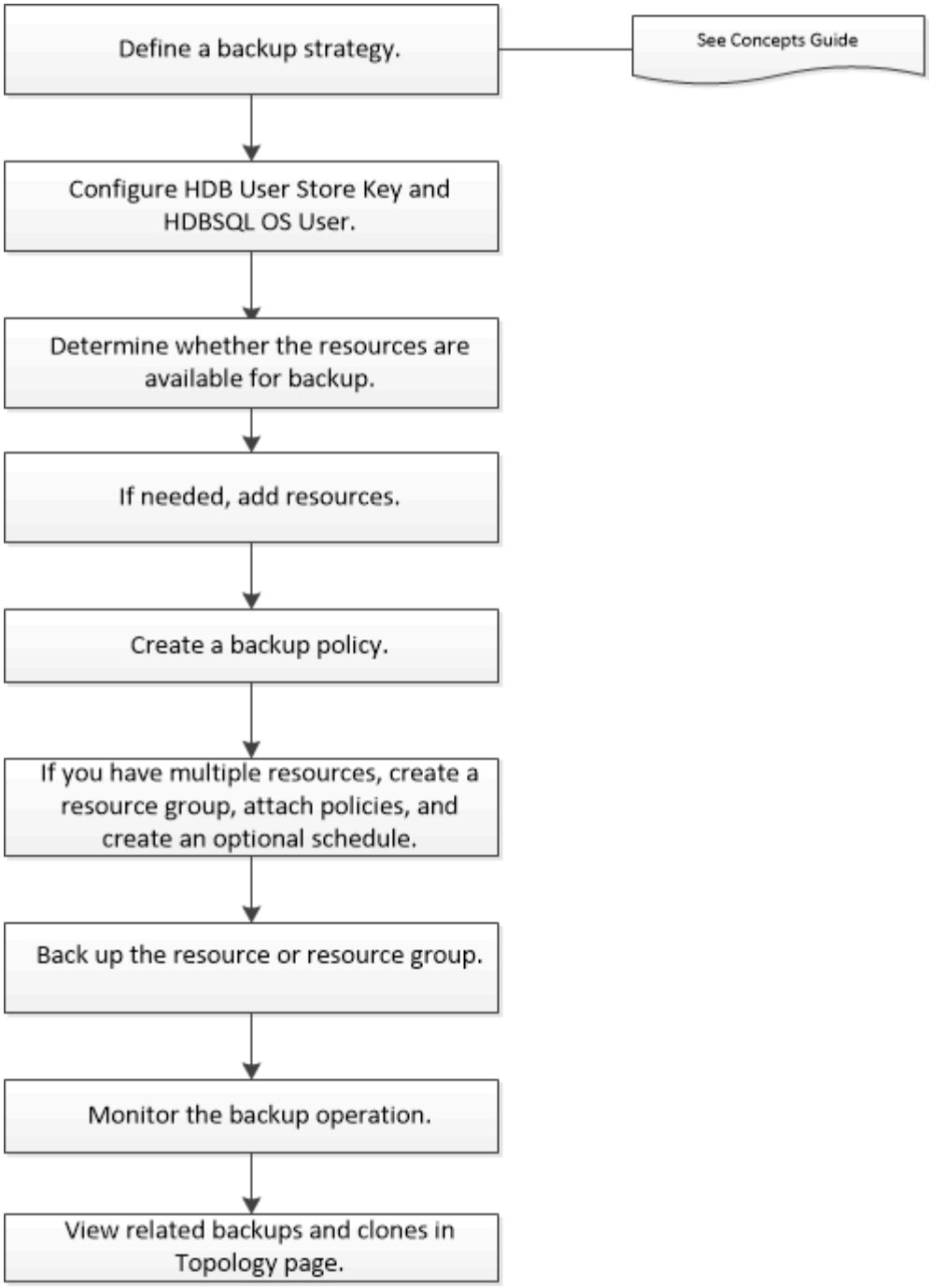
Considérez un groupe de ressources comme définissant ce que vous voulez protéger et quand vous voulez le protéger en termes de jour et d'heure. Considérez une stratégie comme une définition de la façon dont vous voulez la protéger. Si vous sauvegardez toutes les bases de données, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources de manière à effectuer une sauvegarde complète tous les jours.

Sauvegarde des ressources SAP HANA

Sauvegarde des ressources SAP HANA

Vous pouvez créer une sauvegarde d'une ressource (base de données) ou d'un groupe de ressources. Le workflow de sauvegarde inclut la planification, l'identification des bases de données pour la sauvegarde, la gestion des stratégies de sauvegarde, la création de groupes de ressources et la connexion de stratégies, la création de sauvegardes et le contrôle des opérations.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent plus d'informations sur les applets de commande PowerShell. "Guide de référence de l'applet de commande du logiciel SnapCenter".

Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA

Vous devez configurer la clé de stockage utilisateur HDB et l'utilisateur HDBSQL pour effectuer des opérations de protection des données sur des bases de données SAP HANA.

Ce dont vous aurez besoin

- Si la clé HDB Secure User Store et l'utilisateur HDB SQL OS ne sont pas configurés dans la base de données SAP HANA, une icône de cadenas rouge s'affiche uniquement pour les ressources découvertes automatiquement. Si, au cours d'une opération de découverte ultérieure, la clé de stockage sécurisée HDB configurée a été détectée comme incorrecte ou n'a pas fourni d'accès à la base de données elle-même, l'icône rouge du cadenas réapparaîtra.
- Vous devez configurer la clé du magasin d'utilisateurs sécurisé HDB et l'utilisateur HDB SQL OS pour pouvoir protéger la base de données ou l'ajouter à un groupe de ressources pour effectuer des opérations de protection des données.
- Vous devez configurer HDB SQL OS User pour accéder à la base de données système. Si HDB SQL OS User est configuré pour accéder uniquement à la base de données de tenant, l'opération de découverte échoue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez Plug-in SnapCenter pour base de données SAP HANA dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste **Affichage**.
3. (Facultatif) cliquez sur et sélectionnez le nom d'hôte.

   Vous pouvez ensuite cliquer sur pour fermer le volet de filtre.
4. Sélectionnez la base de données, puis cliquez sur **configurer la base de données**.
5. Dans la section configurer les paramètres de la base de données, entrez la clé de stockage sécurisée de l'utilisateur HDB.

   Le nom d'hôte du plug-in s'affiche et l'utilisateur HDB SQL OS est automatiquement renseigné sur <sid<adm.
6. Cliquez sur **OK**.

Vous pouvez modifier la configuration de la base de données à partir de la page topologie.

Découverte des ressources et préparation de conteneurs de bases de données mutualisés pour la protection des données

Découvrir les bases de données automatiquement

Les ressources sont les bases de données SAP HANA et les volumes non data sur l'hôte Linux gérés par SnapCenter. Vous pouvez ajouter ces ressources aux groupes de ressources pour effectuer des opérations de protection des données après avoir découvert les bases de données SAP HANA disponibles.

Ce dont vous aurez besoin

- Vous devez avoir déjà terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'une clé de stockage utilisateur HDB, l'ajout d'hôtes et la configuration des connexions du système de stockage.
- Vous devez avoir configuré la clé de stockage utilisateur sécurisée HDB et l'utilisateur HDB SQL OS sur l'hôte Linux.
  - Vous devez configurer la clé de stockage utilisateur HDB avec l'utilisateur adm SID. Par exemple, pour un système HANA avec A22 comme SID, la clé de stockage utilisateur HDB doit être configurée avec

a22adm.

- Le plug-in SnapCenter pour base de données SAP HANA ne prend pas en charge la découverte automatique des ressources résidant dans des environnements virtuels RDM/VMDK. Vous devez fournir les informations de stockage pour les environnements virtuels tout en ajoutant les bases de données manuellement.

À propos de cette tâche

Après l'installation du plug-in, toutes les ressources de cet hôte Linux sont automatiquement découvertes et affichées sur la page Ressources.

Les ressources détectées automatiquement ne peuvent pas être modifiées ou supprimées.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in pour la base de données SAP HANA dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste vue.
3. (Facultatif) cliquez sur * *, puis sélectionnez le nom d'hôte.

   Vous pouvez alors cliquer sur * *pour fermer le volet de filtre.

4. Cliquez sur **Actualiser les ressources** pour découvrir les ressources disponibles sur l'hôte.

   Les ressources s'affichent avec des informations telles que le type de ressource, le nom d'hôte, les groupes de ressources associés, le type de sauvegarde, les stratégies et l'état global.

   - Si la base de données se trouve sur un système de stockage NetApp et qu'elle n'est pas protégée, elle s'affiche dans la colonne État global.
   - Si la base de données se trouve sur un système de stockage NetApp et est protégée, et si aucune opération de sauvegarde n'est effectuée, alors l'option sauvegarde non exécutée s'affiche dans la colonne État global. Dans le cas contraire, l'état passe en échec de la sauvegarde ou la sauvegarde a réussi en fonction de l'état de la dernière sauvegarde.

Si une clé de stockage HDB Secure User Store n'est pas configurée dans la base de données SAP HANA, une icône de cadenas rouge apparaît à côté de la ressource. Si, au cours d'une opération de découverte ultérieure, la clé de stockage sécurisée HDB configurée a été détectée comme incorrecte ou n'a pas fourni d'accès à la base de données elle-même, l'icône rouge du cadenas réapparaîtra.

Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

Après la fin

Vous devez configurer la clé du magasin d'utilisateurs sécurisé HDB et l'utilisateur HDBSQL pour pouvoir protéger la base de données ou l'ajouter au groupe de ressources pour effectuer des opérations de protection des données.

"Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA"

Préparez des conteneurs de bases de données mutualisés pour protéger les données

Pour les hôtes SAP HANA directement enregistrés dans SnapCenter, l'installation ou la mise à niveau du plug-in SnapCenter pour base de données SAP HANA déclenchera une détection automatique des ressources sur l'hôte. Après l'installation ou la mise à niveau du plug-in, pour chaque ressource MDC (conteneur de base de données multitenant) située sur l'hôte du plug-in, une autre ressource MDC sera automatiquement découverte avec un format GUID différent et enregistrée dans SnapCenter. La nouvelle ressource sera à l'état « verrouillée ».

À propos de cette tâche

Par exemple, dans SnapCenter 4.2, si la ressource MDC E90 était située sur l'hôte du plug-in et enregistrée manuellement, après la mise à niveau vers SnapCenter 4.3, une autre ressource MDC E90 avec un GUID différent sera découverte et enregistrée dans SnapCenter.

> Les sauvegardes associées à la ressource de SnapCenter 4.2 et versions antérieures doivent être conservées jusqu'à l'expiration de la période de conservation. Après l'expiration de la période de conservation, vous pouvez supprimer l'ancienne ressource MDC et continuer à gérer la nouvelle ressource MDC découverte automatiquement.

`Old MDC resource` Est la ressource MDC pour un hôte de plug-in qui a été ajouté manuellement dans SnapCenter 4.2 ou une version antérieure.

Pour commencer à utiliser la nouvelle ressource découverte dans SnapCenter 4.3 pour les opérations de protection des données, procédez comme suit :

Étapes

1. Dans la page Ressources, sélectionnez l'ancienne ressource MDC avec les sauvegardes ajoutées à la version précédente de SnapCenter, puis placez-la dans "mode de maintenance" à partir de la page topologie.

   Si la ressource fait partie d'un groupe de ressources, placez le groupe de ressources dans "mode de provenance".

2. Configurez la nouvelle ressource MDC découverte après la mise à niveau vers SnapCenter 4.3 en sélectionnant la nouvelle ressource dans la page Ressources.

   « Nouvelle ressource MDC » est la nouvelle ressource MDC découverte une fois le serveur SnapCenter et l'hôte du plug-in mis à niveau vers 4.3. La nouvelle ressource MDC peut être identifiée comme une ressource avec le même SID que l'ancienne ressource MDC, pour un hôte donné, et avec une icône de cadenas rouge à côté de celle-ci dans la page Ressources.

3. Protégez la nouvelle ressource MDC détectée après la mise à niveau vers SnapCenter 4.3 en sélectionnant des stratégies de protection, des plannings et des paramètres de notification.
4. Supprimez les sauvegardes effectuées dans SnapCenter 4.2 ou les versions antérieures en fonction des paramètres de conservation.
5. Supprimez le groupe de ressources de la page topologie.
6. Supprimez l'ancienne ressource MDC de la page Ressources.

   Par exemple, si la période de conservation des copies Snapshot primaires est de 7 jours et que la

conservation des copies Snapshot secondaires est de 45 jours, après 45 jours et après la suppression de toutes les sauvegardes, vous devez supprimer le groupe de ressources et l'ancienne ressource MDC.

Plus d'informations

"Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA"

"Affichez les sauvegardes et les clones des bases de données SAP HANA sur la page topologie"

Ajoutez des ressources manuellement au plug-in hôte

La détection automatique n'est pas prise en charge pour certaines instances HANA. Vous devez ajouter ces ressources manuellement.

Ce dont vous aurez besoin

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes, la configuration des connexions du système de stockage et l'ajout d'une clé de stockage utilisateur HDB.
- Pour la réplication des systèmes SAP HANA, il est recommandé d'ajouter toutes les ressources de ce système HANA dans un groupe de ressources et de sauvegarder un groupe de ressources. Cela garantit une sauvegarde transparente en mode basculement/retour arrière.

"Créer des groupes de ressources et attacher des stratégies".

À propos de cette tâche

La détection automatique n'est pas prise en charge pour les configurations suivantes :

- Dispositions RDM et VMDK

> Lorsque les ressources ci-dessus sont découvertes, les opérations de protection des données ne sont pas prises en charge sur ces ressources.

- Configuration HANA avec plusieurs hôtes
- Plusieurs instances sur le même hôte
- Réplication système HANA scale-out multi-niveaux
- Environnement de réplication en cascade en mode réplication du système

Étapes

1. Dans le volet de navigation de gauche, sélectionnez le plug-in SnapCenter pour base de données SAP HANA dans la liste déroulante, puis cliquez sur **Ressources**.
2. Dans la page Ressources, cliquez sur **Ajouter une base de données SAP HANA**.
3. Dans la page Détails de la ressource, effectuez les opérations suivantes :

Pour ce champ…	Procédez comme ça…
Type de ressource	Entrez le type de ressource. Les types de ressources sont conteneur unique, conteneur de base de données mutualisé (MDC) et volume non data.
Nom du système HANA	Entrez le nom descriptif du système SAP HANA. Cette option n'est disponible que si vous avez sélectionné des types de ressources conteneur unique ou MDC.
SID	Saisissez l'ID système (SID). Le système SAP HANA installé est identifié par un SID unique.
Hôte de plug-in	Sélectionnez l'hôte du plug-in.
Clés de stockage sécurisé HDB	Entrez la clé pour vous connecter au système SAP HANA. La clé contient les informations de connexion à la base de données. Pour la réplication système SAP HANA, la clé utilisateur secondaire n'est pas validée. Ceci sera utilisé pendant le basculement.
Utilisateur HDBSQL	Entrez le nom d'utilisateur pour lequel la clé de stockage sécurisée de l'utilisateur HDB est configurée. Pour Windows, il est obligatoire que l'utilisateur HDBSQL OS soit l'utilisateur SYSTÈME. Par conséquent, vous devez configurer la clé de stockage sécurisée de l'utilisateur HDB pour l'utilisateur SYSTÈME.

4. Dans la page Entitetour Storage Footprint, sélectionnez un système de stockage et choisissez un ou plusieurs volumes, LUN et qtrees, puis cliquez sur **Save**.

   Facultatif : vous pouvez cliquer sur l'icône * + pour ajouter d'autres volumes, LUN et qtrees à partir d'autres systèmes de stockage.

5. Vérifiez le résumé, puis cliquez sur **Terminer**.

   Les bases de données s'affichent avec des informations telles que le SID, l'hôte du plug-in, les groupes de ressources et les stratégies associés et l'état global

Si vous souhaitez donner aux utilisateurs l'accès aux ressources, vous devez affecter ces ressources aux utilisateurs. Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

"Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources"

Après avoir ajouté les bases de données, vous pouvez modifier les détails de la base de données SAP HANA.

Vous ne pouvez pas modifier ce qui suit si des sauvegardes sont associées à la ressource SAP HANA :

- Conteneurs de base de données mutualisés (MDC) : SID ou hôte HDBSQL client (plug-in)
- Conteneur unique : SID ou hôte client HDBSQL (plug-in)
- Volume non-données : nom de la ressource, SID associé ou hôte du plug-in

Créez des règles de sauvegarde pour les bases de données SAP HANA

Avant d'utiliser SnapCenter pour sauvegarder les ressources de base de données SAP HANA, vous devez créer une règle de sauvegarde pour la ressource ou le groupe de ressources à sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes.

Ce dont vous aurez besoin

- Vous devez avoir défini votre stratégie de sauvegarde.

  Pour en savoir plus, découvrez comment définir une stratégie de protection des données pour les bases de données SAP HANA.

- Vous devez vous préparer à la protection des données en effectuant des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la configuration des connexions du système de stockage et l'ajout de ressources.
- L'administrateur SnapCenter doit avoir attribué les SVM aux volumes source et de destination, si vous répliquez les copies Snapshot sur un miroir ou un coffre-fort.

  En outre, vous pouvez spécifier des paramètres de réplication, de script et d'application dans la stratégie. Ces options vous permettent de gagner du temps lorsque vous souhaitez réutiliser la stratégie d'un autre groupe de ressources.

À propos de cette tâche

- Réplication système SAP HANA
  - Vous pouvez protéger le système SAP HANA principal et toutes les opérations de protection des données peuvent être effectuées.
  - Vous pouvez protéger le système SAP HANA secondaire, mais les sauvegardes ne peuvent pas être créées.

    Après le basculement, toutes les opérations de protection des données peuvent être effectuées lorsque le système SAP HANA secondaire devient le système SAP HANA principal.

  Vous ne pouvez pas créer de sauvegarde pour le volume de données SAP HANA, mais SnapCenter continue à protéger les volumes non-data.

Étapes

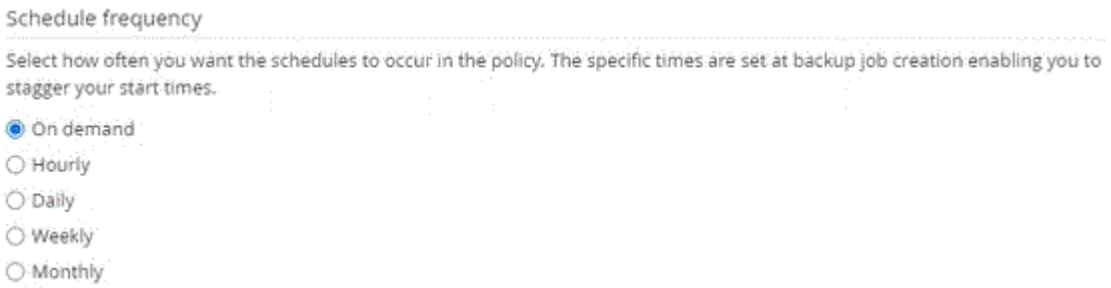
1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.

3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et la description de la stratégie.
5. Dans la page Paramètres, effectuez les opérations suivantes :
   - Choisissez un type de sauvegarde :

Les fonctions que vous recherchez…	Procédez comme ça…
Effectuer un contrôle d'intégrité de la base de données	Sélectionnez **sauvegarde basée sur fichier**. Seuls les locataires actifs sont sauvegardés.
Créer une sauvegarde à l'aide de la technologie de copie Snapshot	Sélectionnez **basé sur les instantanés**.

   - Spécifiez le type d'horaire en sélectionnant **On Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

> Vous pouvez spécifier la planification (date de début, date de fin et fréquence) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais aussi d'affecter des programmes de sauvegarde différents à chaque stratégie.



> Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

   - Dans la section **Paramètres de sauvegarde personnalisés**, indiquez tous les paramètres de sauvegarde spécifiques qui doivent être transmis au plug-in au format clé-valeur.

     Vous pouvez fournir plusieurs valeurs de clé à transmettre au plug-in.

6. Dans la page Retention, spécifiez les paramètres de conservation pour le type de sauvegarde et le type de programme sélectionné dans la page Type de sauvegarde :

Les fonctions que vous recherchez…	Alors…
Conserver un certain nombre de copies Snapshot	Sélectionnez **nombre total de copies Snapshot à conserver**, puis spécifiez le nombre de copies Snapshot que vous souhaitez conserver. Si le nombre de copies Snapshot dépasse le nombre spécifié, les copies Snapshot sont supprimées par les plus anciennes copies supprimées en premier. La valeur maximale de rétention est de 1018 pour les ressources sur ONTAP 9.4 ou version ultérieure et de 254 pour les ressources sur ONTAP 9.3 ou version antérieure. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente. Dans le cas des sauvegardes basées sur des copies Snapshot, vous devez définir le nombre de rétention à 2 ou plus si vous prévoyez d'activer la réplication SnapVault. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car la première copie Snapshot est la copie de référence pour la relation SnapVault jusqu'à ce qu'une nouvelle copie Snapshot soit répliquée vers la cible. Pour la réplication des systèmes SAP HANA, il est recommandé d'ajouter toutes les ressources du système SAP HANA dans un groupe de ressources unique. Cela permet de conserver le nombre adéquat de sauvegardes.

Les fonctions que vous recherchez…	Alors…
Conservez les copies Snapshot pendant un certain nombre de jours	Sélectionnez **conserver les copies Snapshot pour**, puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les copies Snapshot avant de les supprimer.

la plus ancienne est basée sur le nœud sur lequel se trouve la copie Snapshot la plus ancienne. Par exemple, la conservation est définie

7. Pour les sauvegardes basées sur des copies Snapshot, spécifiez les paramètres de réplication sur la page réplication :

Pour ce champ…	Procédez comme ça…
Mettre à jour SnapMirror après avoir créé une copie Snapshot locale	Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror). Si la relation de protection dans ONTAP est de type miroir et coffre-fort et si vous sélectionnez uniquement cette option, la copie Snapshot créée sur le système primaire ne sera pas transférée vers la destination, mais elle sera répertoriée dans le système de destination. Si cette copie Snapshot est sélectionnée à partir de la destination pour effectuer une opération de restauration, le message d'erreur emplacement secondaire n'est pas disponible pour la sauvegarde en copie/miroir sélectionnée s'affiche.
Mettre à jour SnapVault après avoir créé une copie Snapshot locale	Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).
Étiquette de politique secondaire	Sélectionnez une étiquette Snapshot. En fonction de l'étiquette de copie Snapshot que vous sélectionnez, ONTAP applique la règle de conservation des copies Snapshot secondaires correspondant à l'étiquette. Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

Pour ce champ…	Procédez comme ça…
Nombre de tentatives d'erreur	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.

Il est recommandé de configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter la limite maximale des copies Snapshot sur le stockage secondaire.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

Créer des groupes de ressources et attacher des stratégies

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

À propos de cette tâche

Pour créer des sauvegardes de réplication du système SAP HANA, il est recommandé d'ajouter toutes les ressources du système SAP HANA dans un groupe de ressources. Cela garantit une sauvegarde transparente en mode basculement/retour arrière.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ…	Procédez comme ça…
Nom	Entrez un nom pour le groupe de ressources. Le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources. Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

Pour ce champ…	Procédez comme ça…
Utilisez le format de nom personnalisé pour la copie Snapshot	Cochez cette case, puis entrez un format de nom personnalisé à utiliser pour le nom de la copie Snapshot. Par exemple, clienttext_Resource group_policy_hostname ou Resource group_hostname. Par défaut, un horodatage est ajouté au nom de la copie Snapshot.

4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.

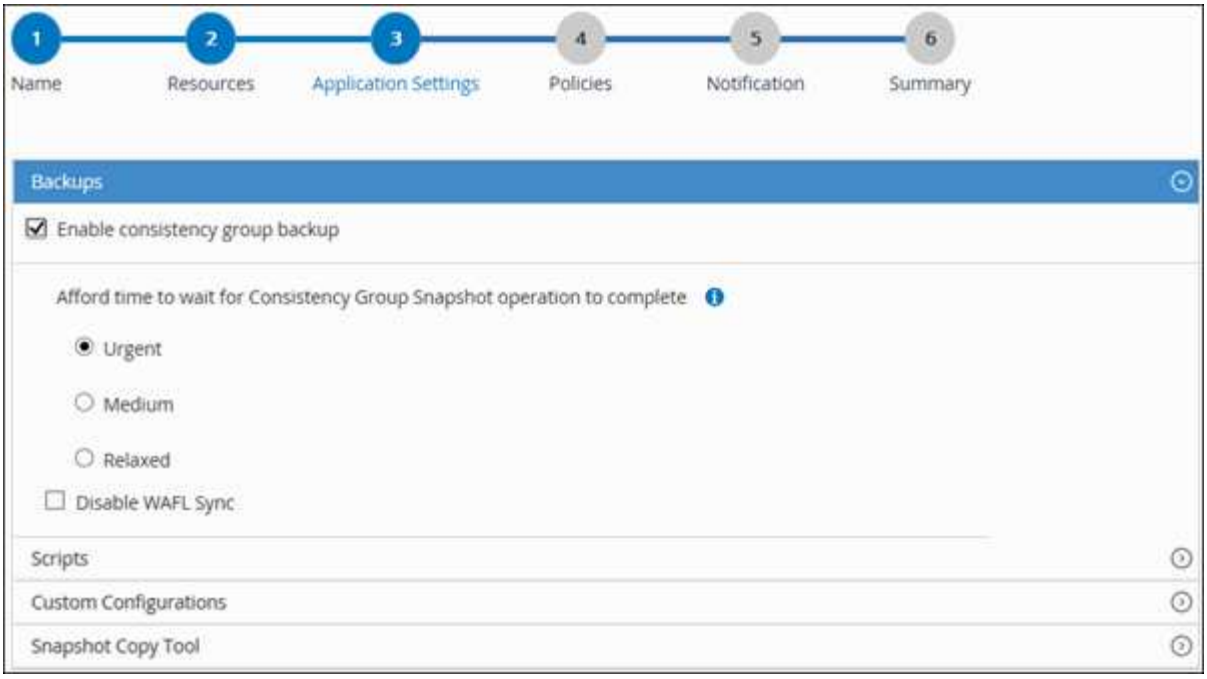
   Cela aide à filtrer les informations affichées à l'écran.

5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page Paramètres de l'application, procédez comme suit :

   a. Cliquez sur la flèche **backups** pour définir des options de sauvegarde supplémentaires :

      Activez la sauvegarde de groupe de cohérence et effectuez les tâches suivantes :

Pour ce champ…	Procédez comme ça…
Permet d'attendre la fin de l'opération Snapshot du groupe de cohérence	Sélectionnez **urgent**, **Moyen** ou **relâché** pour spécifier le temps d'attente de l'opération de copie Snapshot. Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

+ 

a. Cliquez sur la flèche **scripts** et entrez les commandes avant et après pour les opérations de mise en veille, de copie Snapshot et de mise en veille. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.

b. Cliquez sur la flèche **configurations personnalisées** et entrez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Réglage	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archive de supprimer les journaux d'archive.
ARCHIVAGE_LOG_RÉTENTION	nombre_de_jours	Indique le nombre de jours pendant lesquels les journaux d'archive sont conservés. Ce paramètre doit être supérieur ou égal à NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_répertoire/logs	Indique le chemin d'accès au répertoire contenant les journaux d'archive.

Paramètre	Réglage	Description
ARCHIVE_LOG_EXT	extension_fichier	Spécifie la longueur d'extension du fichier journal d'archives. Par exemple, si le journal d'archives est log_backup_0_0_0_0.16151855 1942 9 et si la valeur file_extension est 5, l'extension du journal conserve 5 chiffres, soit 16151.
ARCHIVE_LOG_RÉCURSIVE_ SE ARCH	(O/N)	Permet la gestion des journaux d'archivage dans les sous-répertoires. Vous devez utiliser ce paramètre si les journaux d'archivage sont situés sous des sous-répertoires.

Les paires de clé à valeur personnalisée sont prises en charge pour les systèmes du plug-in SAP HANA Linux et ne sont pas prises en charge pour la base de données SAP HANA enregistrée en tant que plug-in centralisé Windows.

c. Cliquez sur la flèche **Snapshot Copy Tool** pour sélectionner l'outil de création de copies Snapshot :

Les fonctions que vous recherchez…	Alors…
SnapCenter pour utiliser le plug-in pour Windows et placer le système de fichiers dans un état cohérent avant de créer une copie Snapshot. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez **SnapCenter avec cohérence du système de fichiers**. Cette option ne s'applique pas au plug-in SnapCenter pour base de données SAP HANA.
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez **SnapCenter sans cohérence du système de fichiers**.
Pour saisir la commande à exécuter sur l'hôte pour créer des copies Snapshot.	Sélectionnez **autre**, puis entrez la commande à exécuter sur l'hôte pour créer une copie Snapshot.

7. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.

Vous pouvez également créer une police en cliquant sur * * + .

Les stratégies sont répertoriées dans la section Configuration des planifications pour les stratégies

sélectionnées.

b. Dans la colonne configurer les plannings, cliquez sur * * pour la stratégie que vous souhaitez configurer.

c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy_name*, configurez le programme, puis cliquez sur **OK**.

Où, nom_stratégie est le nom de la règle que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne **programmes appliqués**.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Le serveur SMTP doit être configuré dans **Paramètres** > **Paramètres globaux**.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

Sauvegarde des bases de données SAP HANA

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

Ce dont vous aurez besoin

- Vous devez avoir créé une stratégie de sauvegarde.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.
- Pour une opération de sauvegarde basée sur des copies Snapshot, assurez-vous que toutes les bases de données de tenant sont valides et actives.
- Pour créer des sauvegardes de réplication du système SAP HANA, il est recommandé d'ajouter toutes les ressources du système SAP HANA dans un groupe de ressources. Cela garantit une sauvegarde transparente en mode basculement/retour arrière.

"Créer des groupes de ressources et attacher des stratégies".

"Sauvegarder les groupes de ressources"

- Si vous souhaitez créer une sauvegarde basée sur des fichiers alors qu'une ou plusieurs bases de données de tenant sont en panne, définissez le paramètre ALLOW_FILE_BASED_BACKUP_IFINA_TENANTS_PRESIDENT sur **YES** dans le fichier de propriétés HANA à l'aide de `Set-SmConfigSettings` applet de commande.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant Get-Help *command_name*. Vous pouvez également vous référer au "Guide de référence de l'applet de commande du logiciel SnapCenter"

- Pour les commandes pré et post pour les opérations de mise au repos, de copie Snapshot et d'annulation de la mise au repos, vous devez vérifier que les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :

  Pour Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands_list.txt*

  Pour Linux : */var/opt/snapcenter/scc/allowed_commands_list.txt*

Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

   Cliquez sur * *, puis sélectionnez le nom d'hôte et le type de ressource pour filtrer les ressources. Vous pouvez ensuite cliquer sur pour fermer le volet de filtre.
3. Cliquez sur la ressource à sauvegarder.
4. Sur la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de la copie Snapshot.

   Par exemple, *customtext_policy_hostname* ou *Resource_hostname*. Par défaut, un horodatage est ajouté au nom de la copie Snapshot.
5. Dans la page Paramètres de l'application, procédez comme suit :
   - Cliquez sur la flèche **backups** pour définir des options de sauvegarde supplémentaires :

     Activez la sauvegarde du groupe de cohérence, si nécessaire, et effectuez les tâches suivantes :

Pour ce champ…	Procédez comme ça…
Temps d'attente avant la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez **urgent**, ou **Moyen** ou **relâché** pour spécifier le temps d'attente pour la fin de l'opération de copie Snapshot. Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

   - Cliquez sur la flèche **scripts** pour exécuter des commandes de pré et post pour les opérations de mise en veille, de copie Snapshot et de mise en veille.

     Vous pouvez également exécuter des pré-commandes avant de quitter l'opération de sauvegarde. Des préscripts et des postscripts sont exécutés sur le serveur SnapCenter.

   - Cliquez sur la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.

◦ Cliquez sur la flèche **Snapshot Copy Tool** pour sélectionner l'outil de création de copies Snapshot :

Les fonctions que vous recherchez…	Alors…
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez **SnapCenter sans cohérence du système de fichiers**.
SnapCenter permettant d'utiliser le plug-in pour Windows afin de rétablir la cohérence du système de fichiers, puis de créer une copie Snapshot	Sélectionnez **SnapCenter avec cohérence du système de fichiers**.
Pour saisir la commande afin de créer une copie Snapshot	Sélectionnez **autre**, puis entrez la commande pour créer une copie Snapshot.

6. Dans la page stratégies, effectuez les opérations suivantes :

   a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.

      Vous pouvez également créer une police en cliquant sur * * + .

      Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

   b. Cliquez sur * * + dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.

   c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy_name*, configurez le programme, puis cliquez sur **OK**.

      policy_name est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

   Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans **Paramètres** > **Paramètres globaux**.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

   La page topologie des ressources s'affiche.

9. Cliquez sur **Sauvegarder maintenant**.
10. Dans la page sauvegarde, effectuez les opérations suivantes :
    a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

       Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

    b. Cliquez sur **Backup**.
11. Surveillez la progression de l'opération en cliquant sur **moniteur** > **travaux**.
    - Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

      Pour plus d'informations, voir : "Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"

    - Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer.

      Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script */opt/netapp/init_scripts/scvservice*. Dans ce script, la commande *do_start method* démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante : *Java -jar -Xmx8192M -Xms4096M*

Sauvegarder les groupes de ressources

Un groupe de ressources est un ensemble de ressources sur un hôte. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

Ce dont vous aurez besoin

- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.

À propos de cette tâche

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

   Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en cliquant sur , puis en sélectionnant la balise. Vous pouvez ensuite cliquer sur pour fermer le volet de filtre.
3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis cliquez sur **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
   a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

      Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

   b. Cliquez sur **Backup**.
5. Surveillez la progression de l'opération en cliquant sur **moniteur** > **travaux**.

Créer une connexion au système de stockage et une certification à l'aide des applets de commande PowerShell pour la base de données SAP HANA

Vous devez créer une connexion SVM (Storage Virtual machine) et une identifiant d'identification avant d'utiliser les applets de commande PowerShell pour sauvegarder, restaurer ou cloner les bases de données SAP HANA.

Ce dont vous aurez besoin

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

  Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».
- Les noms des systèmes de stockage doivent être uniques.

  SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom

unique et d'une adresse IP de LIF de données unique.

Étapes

1. Lancez une session de connexion PowerShell à l'aide de la cmdlet Open-SmConnection.

```
PS C:\> Open-SmStorageConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande Add-SmCredential.

   Cet exemple montre comment créer un nouvel identifiant nommé FinancieAdmin avec les informations d'identification Windows :

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Ajoutez l'hôte de communication SAP HANA au serveur SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Installez le package et le plug-in SnapCenter pour base de données SAP HANA sur l'hôte.

   Pour Linux :

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
hana
```

   Pour Windows :

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Définissez le chemin d'accès au client HDBSQL.

   Pour Windows :

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

Pour Linux :

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Sauvegarder des bases de données à l'aide des applets de commande PowerShell

La sauvegarde d'une base de données inclut l'établissement d'une connexion avec le serveur SnapCenter, l'ajout de ressources, l'ajout d'une stratégie, la création d'un groupe de ressources de sauvegarde et la sauvegarde.

Ce dont vous aurez besoin

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Vous devez avoir ajouté la connexion au système de stockage et créé une autorisation d'accès.

Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
   ```

   L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Ajoutez des ressources à l'aide de l'applet de commande Add-SmResources.

   Cet exemple montre comment ajouter une base de données SAP HANA de type SingleContainer :

   ```
   C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
   -DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
   (@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"})
   -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys 'HS10'
   -osdbuser 'h10adm' -filebackupprefix 'H10_'
   ```

Cet exemple montre comment ajouter une base de données SAP HANA de type MultipleContainers :

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType MultipleContainers
-StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.netapp.
com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType 'MultiTenant'
```

Cet exemple montre comment créer une ressource de volume autre que de données :

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.

   Dans cet exemple, une règle de sauvegarde est créée pour une sauvegarde basée sur des copies Snapshot :

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
   -PluginPolicyType hana -BackupType SnapShotBasedBackup
   ```

   Cet exemple crée une stratégie de sauvegarde pour une sauvegarde en mode fichier :

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
   -PluginPolicyType hana -BackupType FileBasedBackup
   ```

4. Protégez la ressource ou ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.

   Cet exemple protège une ressource de conteneur unique :

   ```
   C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
   hana_snapshotbased,hana_Filebased
    -Resources @{"Host"="host.example.com";"UID"="SID"} -Description test
   -usesnapcenterwithoutfilesystemconsistency
   ```

   Cet exemple protège plusieurs conteneurs :

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

Cet exemple crée un nouveau groupe de ressources avec la stratégie et les ressources spécifiées :

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Dans cet exemple, nous allons créer un groupe de ressources sans volume de données :

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="han
a"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"PluginName
"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDataVolume\
S10\NonDataVolume";"PluginName"="hana"}) -Policies hanaprimary
```

5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet New-SmBackup.

   Cet exemple montre comment sauvegarder un groupe de ressources :

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

   Cet exemple sauvegarde une ressource protégée :

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"} -Policy
hana_Filebased
```

6. Surveillez l'état du travail (en cours d'exécution, terminé ou en échec) à l'aide de l'applet de commande Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Surveillez les détails de la tâche de sauvegarde comme ID de sauvegarde, nom de sauvegarde pour effectuer une opération de restauration ou de clonage à l'aide de l'applet de commande Get-SmBackupReport.

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Surveiller les opérations de sauvegarde

Surveillez les opérations de sauvegarde des bases de données SAP HANA

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

- En cours
- Terminé avec succès
- Échec
- Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
- En file d'attente
- Annulée

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
   a. Cliquez sur pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
   b. Spécifiez les dates de début et de fin.
   c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
   d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
   e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.

   Bien que l'état de la tâche de sauvegarde s'affiche , lorsque vous cliquez sur les détails du travail, vous pouvez constater que certaines tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un signe d'avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

   Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

Surveillez les opérations de protection des données des bases de données SAP HANA dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée. Si vous utilisez le plug-in pour SQL Server ou le plug-in pour Exchange Server, le volet activité affiche également des informations sur l'opération de réamorçage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.

2. Cliquez sur le volet activité pour afficher les cinq opérations les plus récentes.

   Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page Détails du travail.

Annuler les opérations de sauvegarde pour SAP HANA

Vous pouvez annuler les opérations de sauvegarde mises en file d'attente.

Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d'exécution.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

Étapes

1. Effectuez l'une des opérations suivantes :

Du…	Action
Page moniteur	a. Dans le volet de navigation de gauche, cliquez sur **moniteur** > **travaux**. b. Sélectionnez l'opération, puis cliquez sur **Annuler le travail**.
Volet activité	a. Après avoir lancé l'opération de sauvegarde, cliquez sur * *dans le volet activité pour afficher les cinq opérations les plus récentes. b. Sélectionner l'opération. c. Dans la page Détails du travail, cliquez sur **Annuler le travail**.

L'opération est annulée et la ressource est rétablie à l'état précédent.

Affichez les sauvegardes et les clones des bases de données SAP HANA sur la page topologie

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et

clones sur le stockage primaire et secondaire.

À propos de cette tâche

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).

- affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
- Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
- Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.

  Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.

Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Pour les ressources primaires de réplication du système SAP HANA, les opérations de restauration et de suppression sont prises en charge, et pour les ressources secondaires, l'opération de clonage est prise en charge.

Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

   Si la ressource est protégée, la page topologique de la ressource sélectionnée s'affiche.

4. Consultez la **carte Résumé** pour afficher un résumé du nombre de sauvegardes et de clones disponibles sur le stockage primaire et secondaire.

   La section **Résumé Card** affiche le nombre total de sauvegardes basées sur les fichiers, de sauvegardes de copies Snapshot et de clones.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

   Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage et de suppression.

   Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

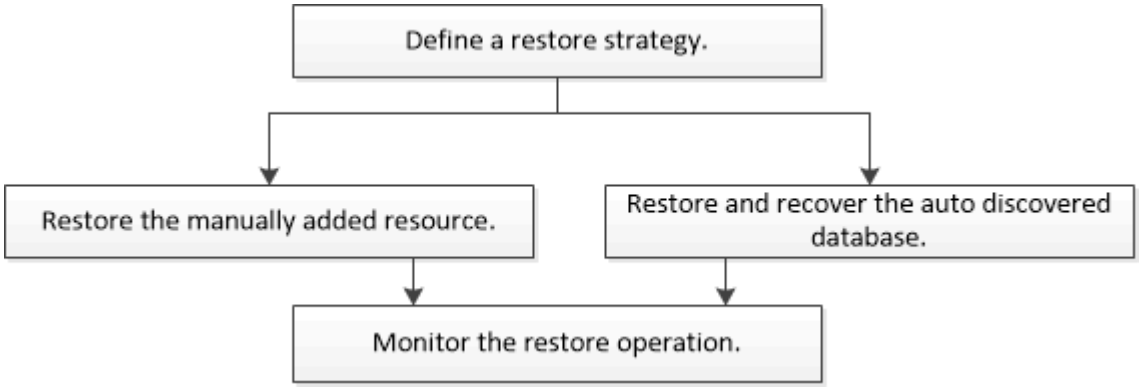
7. Si vous souhaitez supprimer un clone, sélectionnez-le dans la table, puis cliquez sur .
8. Si vous souhaitez diviser un clone, sélectionnez-le dans le tableau, puis cliquez sur .

Restauration des bases de données SAP HANA

Restaurer le flux de travail

Le workflow de restauration et de reprise comprend la planification, la réalisation des opérations de restauration et la surveillance des opérations.

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer l'opération de restauration :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

"Guide de référence de l'applet de commande du logiciel SnapCenter".

Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

Ce dont vous aurez besoin

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :

  Pour Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands_list.txt*

  Pour Linux : */var/opt/snapcenter/scc/allowed_commands_list.txt*

  Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

À propos de cette tâche

- Les copies de sauvegarde basées sur des fichiers ne peuvent pas être restaurées depuis SnapCenter.
- Après la mise à niveau vers SnapCenter 4.3, les sauvegardes effectuées dans SnapCenter 4.2 peuvent être restaurées, mais ne peuvent pas être restaurées. Vous devez utiliser des scripts de restauration HANA Studio ou HANA externes à SnapCenter pour restaurer les sauvegardes prises dans SnapCenter 4.2.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

   Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.

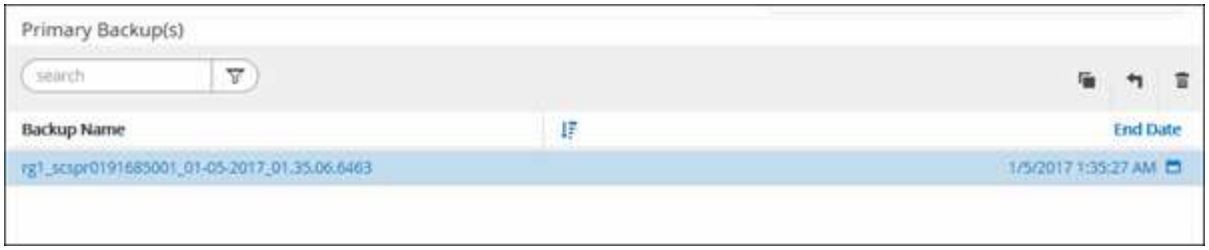
   Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

   Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

   La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur .



6. Dans la page objectif de restauration, sélectionnez **ressource complète** ou **niveau de fichier**.

   a. Si vous sélectionnez **Complete Resource**, tous les volumes de données configurés de la base de données SAP HANA sont restaurés.

      Si la ressource contient des volumes ou des qtrees, les copies Snapshot sont supprimées après la copie Snapshot sélectionnée pour être restaurées sur de tels volumes ou qtrees et ne peuvent pas être restaurées. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

   b. Si vous sélectionnez **File Level**, vous pouvez sélectionner **All** ou sélectionner des volumes ou des qtrees spécifiques, puis entrer le chemin d'accès associé à ces volumes ou qtrees, séparés par des virgules

      - Vous pouvez sélectionner plusieurs volumes et qtrees.
      - Si le type de ressource est LUN, l'ensemble de la LUN est restauré.

        Vous pouvez sélectionner plusieurs LUN.

   Si vous sélectionnez **tous**, tous les fichiers des volumes, qtrees ou LUN sont restaurés.

7. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

   Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

8. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

   Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

   Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres** > **Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez la progression de l'opération en cliquant sur **moniteur** > **travaux**.

Restaurez et récupérez une sauvegarde de base de données découverte automatiquement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

Ce dont vous aurez besoin

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :

  Pour Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands_list.txt*

  Pour Linux : */var/opt/snapcenter/scc/allowed_commands_list.txt*

  Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

À propos de cette tâche

- Les copies de sauvegarde basées sur des fichiers ne peuvent pas être restaurées depuis SnapCenter.
- Après la mise à niveau vers SnapCenter 4.3, les sauvegardes effectuées dans SnapCenter 4.2 peuvent être restaurées, mais ne peuvent pas être restaurées. Vous devez utiliser des scripts de restauration HANA Studio ou HANA externes à SnapCenter pour restaurer les sauvegardes prises dans SnapCenter 4.2.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

   Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.

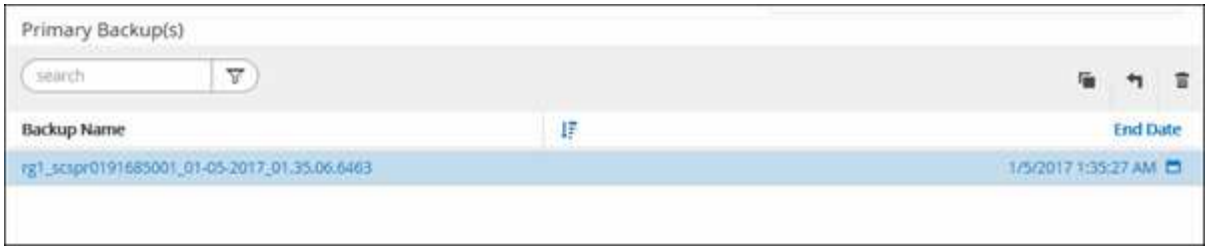
   Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

   Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

   La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur .



6. Sur la page étendue de la restauration, sélectionnez **ressource complète** pour restaurer les volumes de données configurés de la base de données SAP HANA.

   Vous pouvez sélectionner **Complete Resource** (avec ou sans **Volume Revert**) ou **tenant Database**.

   L'opération de récupération n'est pas prise en charge par le serveur SnapCenter pour plusieurs locataires lorsque l'utilisateur sélectionne l'option **base de données locataire** ou **Restauration complète**. Vous devez utiliser HANA Studio ou le script python HANA pour effectuer l'opération de restauration.

   a. Sélectionnez **Volume Revert** si vous souhaitez restaurer l'intégralité du volume.

      Cette option est disponible pour les sauvegardes prises en charge dans SnapCenter 4.3 dans les environnements NFS.

      Si la ressource contient des volumes ou des qtrees, les copies Snapshot sont supprimées après la copie Snapshot sélectionnée pour être restaurées sur de tels volumes ou qtrees et ne peuvent pas être restaurées. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée. Ceci est applicable lorsque l'option **Complete Resource** avec **Volume Revert** est sélectionnée pour la restauration.

   b. Sélectionnez **base de données de tenant**.

      Cette option n'est disponible que pour les ressources MDC.

      Assurez-vous d'arrêter la base de données des locataires avant d'effectuer l'opération de restauration.

   Si vous sélectionnez l'option **tenant Database**, vous devez utiliser HANA Studio ou utiliser des scripts de reprise HANA externes à SnapCenter pour effectuer l'opération de restauration.

7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :

Si…	Procédez comme ça…
Vous souhaitez effectuer une restauration aussi proche que possible de l'heure actuelle	Sélectionnez **récupérer à l'état le plus récent**. Pour les ressources de conteneur unique, spécifiez un ou plusieurs emplacements de sauvegarde de journaux et de catalogues. Pour les ressources MDC (conteneur de base de données mutualisée), spécifiez un ou plusieurs emplacements de sauvegarde du journal et l'emplacement du catalogue de sauvegarde. Pour les ressources MDC, le chemin doit contenir à la fois des journaux de base de données système et des bases de données de tenant.

Si…	Procédez comme ça…
Vous souhaitez effectuer une restauration au point dans le temps spécifié	Sélectionnez **récupérer à un point dans le temps**. a. Sélectionnez le fuseau horaire. Le fuseau horaire du navigateur est utilisé par défaut. Le fuseau horaire sélectionné et l'heure d'entrée sont convertis en GMT absolu. b. Entrez la date et l'heure. Par exemple, l'hôte Linux HANA est situé à Sunnyvale, CA et l'utilisateur à Raleigh, NC rétablit les journaux au SnapCenter. La différence de temps entre ces deux emplacements est de 3 heures et, puisque l'utilisateur s'est connecté à Raleigh, NC, le fuseau horaire par défaut du navigateur qui sera sélectionné dans l'interface utilisateur est GMT-04:00. Si l'utilisateur souhaite effectuer une restauration à 5 h, Sunnyvale, CA, l'utilisateur doit définir le fuseau horaire du navigateur sur le fuseau horaire de l'hôte HANA Linux, GMT-07:00 et préciser la date et l'heure à 5 h 00 Pour les ressources de conteneur unique, spécifiez un ou plusieurs emplacements de sauvegarde de journaux et de catalogues. Pour les ressources MDC, spécifiez un ou plusieurs emplacements de sauvegarde du journal et l'emplacement du catalogue de sauvegarde. Pour les ressources MDC, le chemin doit contenir à la fois des journaux de base de données système et des bases de données de tenant.
Veulent effectuer une restauration vers une sauvegarde de données spécifique	Sélectionnez **récupérer à la sauvegarde de données spécifiée**.
Ne pas récupérer	Sélectionnez **pas de récupération**. Vous devez effectuer l'opération de restauration manuellement à partir du studio HANA.

Vous ne pouvez restaurer que les sauvegardes effectuées après la mise à niveau vers SnapCenter 4.3, à condition que l'hôte et le plug-in soient mis à niveau vers SnapCenter 4.3, et que les sauvegardes

sélectionnées pour la restauration soient effectuées après la conversion ou la découverte automatique de la ressource.

8. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

   Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

9. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

   Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

10. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

    Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres** > **Paramètres globaux**.

11. Vérifiez le résumé, puis cliquez sur **Terminer**.
12. Surveillez la progression de l'opération en cliquant sur **moniteur** > **travaux**.

Restaurer la base de données SAP HANA à l'aide des applets de commande PowerShell

La restauration d'une sauvegarde de base de données SAP HANA inclut le lancement d'une session de connexion avec le serveur SnapCenter, la liste des sauvegardes, la récupération des informations de sauvegarde et la restauration d'une sauvegarde.

Ce dont vous aurez besoin

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Identifiez la sauvegarde que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

   Cet exemple montre que deux sauvegardes sont disponibles pour la restauration :

```
 PS C:\> Get-SmBackup

        BackupId    BackupName                    BackupTime
BackupType
        --------    ----------                    ----------
----------
         1          Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32 AM
Full Backup
         2          Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17 AM
```

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Démarrez le processus de restauration dans le studio HANA.

La base de données est arrêtée.

4. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

   AppObjectId est « Host\Plugin\UID », où UID = SID est pour une ressource de type conteneur unique et UID = MDC\SID est pour une ressource de conteneurs multiples. Vous pouvez obtenir ResourceID à partir de l'applet de commande Get-smResources.

   ```
   Get-smResources  -HostName cn24.sccore.test.com  -PluginCode HANA
   ```

   Cet exemple montre comment restaurer la base de données à partir du stockage primaire :

   ```
   Restore-SmBackup -PluginCode HANA -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 3
   ```

   Cet exemple montre comment restaurer la base de données à partir du stockage secondaire :

   ```
   Restore-SmBackup -PluginCode 'HANA' -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
   @{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
   Vserver>:<SecondaryVolume>"})
   ```

   Les sauvegardes seront disponibles dans HANA Studio à des fins de restauration.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Restaurer des ressources à l'aide des applets de commande PowerShell

La restauration d'une sauvegarde de ressources inclut le lancement d'une session de connexion avec le serveur SnapCenter, la liste des sauvegardes, la récupération des informations de sauvegarde et la restauration d'une sauvegarde.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName                    BackupTime
BackupType
--------                      ----------                    ----------
----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32 AM
Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17 AM
```

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Surveillez les opérations de restauration des bases de données SAP HANA

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

- En cours
- Terminé avec succès
- Échec
- Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
- En file d'attente
- Annulée

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
   a. Cliquez sur pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
   b. Spécifiez les dates de début et de fin.
   c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
   d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
   e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

   Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

Une fois l'opération de restauration basée sur le volume effectuée, les métadonnées de sauvegarde sont supprimées du référentiel SnapCenter, mais les entrées du catalogue de sauvegardes restent dans le catalogue SAP HANA. Bien que l'état de la tâche de restauration s'affiche , cliquez sur les détails du travail pour afficher le signe d'avertissement de certaines tâches enfants. Cliquez sur le signe d'avertissement et supprimez les entrées du catalogue de sauvegarde indiquées.

Clonage des sauvegardes de ressources SAP HANA

Workflow de clonage

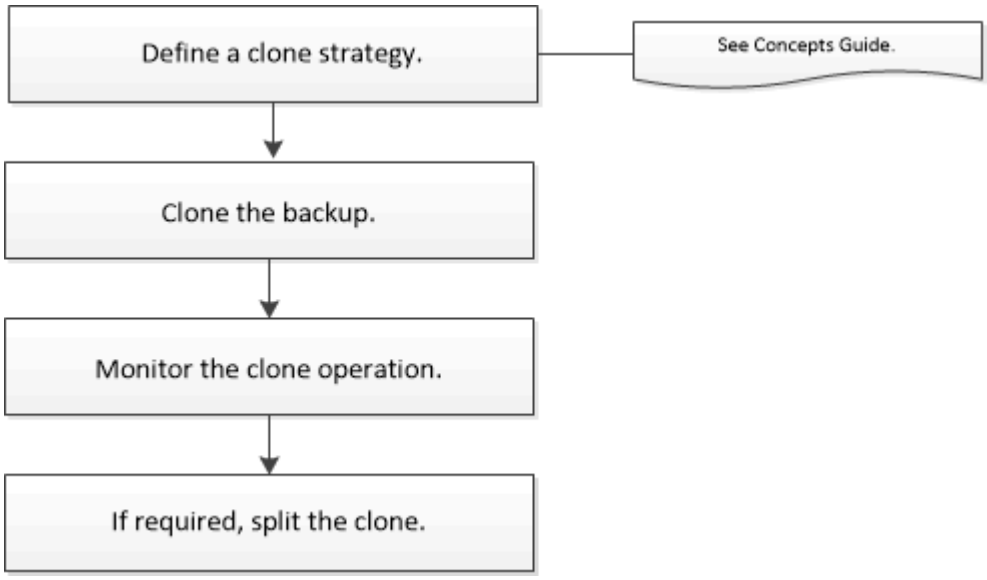
Le workflow de clonage inclut la réalisation de l'opération de clonage et le contrôle de l'opération.

À propos de cette tâche

- Vous pouvez cloner sur le serveur SAP HANA source.
- Vous pouvez cloner des sauvegardes de ressources pour les raisons suivantes :
  - Tester les fonctionnalités à implémenter à l'aide de la structure de ressources actuelle et du contenu pendant les cycles de développement d'applications
  - Pour les outils d'extraction et de manipulation de données lors du remplissage d'entrepôts de données

◦ Pour récupérer les données qui ont été supprimées ou modifiées par erreur

Le workflow suivant affiche la séquence dans laquelle vous devez effectuer l'opération de clonage :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

Cloner une sauvegarde de base de données SAP HANA

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde. Vous pouvez cloner à partir d'une sauvegarde principale ou secondaire.

Ce dont vous aurez besoin

- Vous devriez avoir sauvegardé les ressources ou le groupe de ressources.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Vous ne pouvez pas cloner des sauvegardes basées sur des fichiers.
- Le serveur clone cible doit avoir le même SID d'instance SAP HANA que celui fourni dans le champ SID de clone cible.
- Pour les commandes pré-clone ou post-clone, vérifiez si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :

  Pour Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands_list.txt*

  Pour Linux : */var/opt/snapcenter/scc/allowed_commands_list.txt*

Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

À propos de cette tâche

Pour plus d'informations sur les limites des opérations de fractionnement de clonage, reportez-vous à la section "Guide de gestion du stockage logique ONTAP 9".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

   Les ressources s'affichent avec des informations telles que le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.

3. Sélectionnez la ressource ou le groupe de ressources.

   Vous devez sélectionner une ressource si vous sélectionnez un groupe de ressources.

   La page topologie des ressources ou des groupes de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page emplacement, effectuez les opérations suivantes :

Pour ce champ…	Procédez comme ça…
Hôte de plug-in	Sélectionnez l'hôte sur lequel le clone doit être monté et le plug-in est installé.
SID de clone cible	Entrez l'ID d'instance SAP HANA à cloner à partir des sauvegardes existantes.
Adresse IP d'exportation NFS	Entrez les adresses IP ou les noms d'hôte sur lesquels les volumes clonés seront exportés.
Initiateur iSCSI	Entrez le nom de l'initiateur iSCSI de l'hôte sur lequel les LUN sont exportées. Cette option n'est disponible que si vous avez sélectionné le type de ressource LUN.
Protocole	Indiquez le protocole de LUN. Cette option n'est disponible que si vous avez sélectionné le type de ressource LUN.

   Si la ressource sélectionnée est une LUN et que vous effectuez un clonage à partir d'une sauvegarde secondaire, les volumes de destination sont répertoriés. Une source unique peut avoir plusieurs volumes de destination.

   Avant le clonage, vous devez vous assurer que l'initiateur iSCSI ou le FCP est présent et configuré et connecté aux hôtes secondaires.

7. Dans la page scripts, effectuez les opérations suivantes :

   Les scripts sont exécutés sur l'hôte du plug-in.

   a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.
      - Commande de pré-clonage : permet de supprimer les bases de données existantes portant le même nom
      - Commande post-clone : vérifiez une base de données ou démarrez une base de données.

   b. Entrez la commande mount pour monter un système de fichiers sur un hôte.

      Commande mount pour un volume ou un qtree sur une machine Linux :

      Exemple pour NFS :

      ```
      mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt
      ```

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

   Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.
10. Surveillez la progression de l'opération en cliquant sur **moniteur** > **travaux**.

Cloner les sauvegardes de bases de données SAP HANA à l'aide des applets de commande PowerShell

Le workflow de clonage inclut la planification, la réalisation de l'opération de clonage et le contrôle de l'opération.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

   ```
   Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Récupérez les sauvegardes pour effectuer l'opération de clonage à l'aide de l'applet de commande Get-SmBackup.

Cet exemple montre que deux sauvegardes sont disponibles pour le clonage :

```
 C:\PS> Get-SmBackup

        BackupId                        BackupName
BackupTime                    BackupType
        --------                        ----------
----------                    ----------
         1                       Payroll Dataset_vise-f6_08... 8/4/2015
11:02:32 AM          Full Backup
         2                       Payroll Dataset_vise-f6_08... 8/4/2015
11:23:17 AM
```

3. Lancez une opération de clonage à partir d'une sauvegarde existante et spécifiez les adresses IP d'exportation NFS sur lesquelles les volumes clonés sont exportés.

   Cet exemple montre que la sauvegarde à cloner possède une adresse NFSExportIPS de 10.232.206.169 :

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

   Si NFSExportIPS n'est pas spécifié, la valeur par défaut est exportée vers l'hôte cible du clone.

4. Vérifiez que les sauvegardes ont été correctement clonées à l'aide de l'applet de commande Get-SmCloneReport pour afficher les détails du travail clone.

   Vous pouvez afficher des informations telles que l'ID de clone, la date et l'heure de début, la date et l'heure de fin.

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

Surveillez les opérations de clonage de bases de données SAP HANA

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

- En cours
- Terminé avec succès
- Échec
- Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
- En file d'attente
- Annulée

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.

3. Dans la page travaux, effectuez les opérations suivantes :
   a. Cliquez sur pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
   b. Spécifiez les dates de début et de fin.
   c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
   d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
   e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

À propos de cette tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

  Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

  Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les limites des opérations de fractionnement de clonage, reportez-vous à la section "Guide de gestion du stockage logique ONTAP 9".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Sur la page Ressources, sélectionnez l'option appropriée dans la liste Afficher :

Option	Description
Des applications de base de données	Sélectionnez **Database** dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez **Path** dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

   La page topologie de ressources s'affiche.

4. Dans la vue gérer les copies, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur * * .
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur** > **travaux**.

   L'opération de fractionnement du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

   Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

   Par exemple :

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

Plus d'informations

"Le clone SnapCenter ou une vérification échoue avec un agrégat"

Supprimez ou séparez les clones de base de données SAP HANA après la mise à niveau de SnapCenter

Après la mise à niveau vers SnapCenter 4.3, vous ne verrez plus les clones. Vous pouvez supprimer le clone ou séparer les clones de la page topologie de la ressource à partir de laquelle les clones ont été créés.

À propos de cette tâche

Si vous souhaitez localiser l'empreinte de stockage des clones masqués, exécutez la commande suivante : `Get-SmClone -ListStorageFootprint`

Étapes

1. Supprimez les sauvegardes des ressources clonées à l'aide de la cmdlet remove-smbackup.
2. Supprimez le groupe de ressources des ressources clonées à l'aide de la cmdlet remove-smresregroupement.
3. Supprimez la protection de la ressource clonée à l'aide de l'applet de commande remove-smprotectResource.
4. Sélectionnez la ressource parente dans la page Ressources.

La page topologie de ressources s’affiche.

5. Dans la vue Manage copies (gérer les copies), sélectionnez les clones dans les systèmes de stockage principal ou secondaire (en miroir ou répliqué).
6. Sélectionnez les clones, puis cliquez sur pour supprimer les clones ou sur pour les séparer.
7. Cliquez sur **OK**.

Informations sur le copyright

Copyright © 2025 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.