



Protéger PostgreSQL

SnapCenter software

NetApp

November 06, 2025

This PDF was generated from <https://docs.netapp.com/fr-fr/snapcenter-61/protect-postgresql/snapcenter-plug-in-for-postgresql-overview.html> on November 06, 2025. Always check docs.netapp.com for the latest.

Sommaire

Protéger PostgreSQL	1
Plug-in SnapCenter pour PostgreSQL	1
Présentation du plug-in SnapCenter pour PostgreSQL	1
Ce que vous pouvez faire en utilisant le plug-in SnapCenter pour PostgreSQL	1
Fonctionnalités du plug-in SnapCenter pour PostgreSQL	1
Types de stockage pris en charge par le plug-in SnapCenter pour PostgreSQL	2
Privilèges ONTAP minimaux requis pour le plug-in PostgreSQL	3
Préparer les systèmes de stockage pour la réplication SnapMirror et SnapVault pour PostgreSQL	6
Stratégie de sauvegarde pour PostgreSQL	6
Stratégie de restauration et de récupération pour PostgreSQL	9
Préparez-vous à installer le plug-in SnapCenter pour PostgreSQL	10
Flux de travail d'installation du plug-in SnapCenter pour PostgreSQL	10
Conditions préalables pour ajouter des hôtes et installer le plug-in SnapCenter pour PostgreSQL	11
Configuration requise pour l'installation du package de plug-ins SnapCenter pour Windows	14
Configuration requise pour l'installation du package de plug-ins SnapCenter pour Linux	15
Configurer les informations d'identification pour le plug-in SnapCenter pour PostgreSQL	16
Configurer gMSA sur Windows Server 2016 ou version ultérieure	19
Installer le plug-in SnapCenter pour PostgreSQL	20
Configurer le certificat CA	26
Préparez-vous à la protection des données	34
Conditions préalables à l'utilisation du plug-in SnapCenter pour PostgreSQL	34
Comment les ressources, les groupes de ressources et les politiques sont utilisés pour protéger PostgreSQL	35
Sauvegarder les ressources PostgreSQL	35
Sauvegarder les ressources PostgreSQL	35
Découvrir les clusters automatiquement	37
Ajouter des ressources manuellement à l'hôte du plug-in	37
Créer des politiques de sauvegarde pour PostgreSQL	39
Créer des groupes de ressources et attacher des politiques	43
Créer des groupes de ressources et activer la protection secondaire pour les ressources PostgreSQL sur les systèmes ASA r2	47
Créer une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour PostgreSQL	50
Sauvegarder PostgreSQL	51
Sauvegarder les groupes de ressources	57
Surveiller les opérations de sauvegarde PostgreSQL	58
Annuler les opérations de sauvegarde pour PostgreSQL	59
Afficher les sauvegardes et les clones PostgreSQL dans la page Topologie	60
Restaurer PostgreSQL	62
Restaurer le flux de travail	62
Restaurer et récupérer une sauvegarde de ressources ajoutée manuellement	62
Restaurer et récupérer une sauvegarde de cluster découverte automatiquement	66
Restaurer les ressources à l'aide des applets de commande PowerShell	69

Surveiller les opérations de restauration PostgreSQL	71
Cloner les sauvegardes de ressources PostgreSQL	72
Cloner le flux de travail	72
Cloner une sauvegarde PostgreSQL	73
Surveiller les opérations de clonage PostgreSQL	76
Diviser un clone	77
Supprimer ou diviser les clones de cluster PostgreSQL après la mise à niveau de SnapCenter	78

Protéger PostgreSQL

Plug-in SnapCenter pour PostgreSQL

Présentation du plug-in SnapCenter pour PostgreSQL

Le plug-in SnapCenter pour cluster PostgreSQL est un composant côté hôte du logiciel NetApp SnapCenter software qui permet la gestion de la protection des données basée sur les applications des clusters PostgreSQL. Le plug-in pour cluster PostgreSQL automatise la sauvegarde, la restauration et le clonage des clusters PostgreSQL dans votre environnement SnapCenter .

SnapCenter prend en charge les configurations PostgreSQL à cluster unique et à clusters multiples. Vous pouvez utiliser le plug-in pour les clusters PostgreSQL dans les environnements Linux et Windows. Dans les environnements Windows, PostgreSQL sera pris en charge en tant que ressource manuelle.

Lorsque le plug-in pour le cluster PostgreSQL est installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies miroir de jeux de sauvegarde sur un autre volume. Vous pouvez également utiliser le plug-in avec la technologie NetApp SnapVault pour effectuer une réplication de sauvegarde de disque à disque pour la conformité aux normes.

Le plug-in SnapCenter pour PostgreSQL prend en charge les dispositions de stockage NFS et SAN sur ONTAP et Azure NetApp File.

La disposition de stockage virtuel VMDK, vVol et RDM est prise en charge.

Ce que vous pouvez faire en utilisant le plug-in SnapCenter pour PostgreSQL

Lorsque vous installez le plug-in pour le cluster PostgreSQL dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner des clusters PostgreSQL et leurs ressources. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Ajouter des clusters.
- Créer des sauvegardes.
- Restaurer à partir de sauvegardes.
- Cloner des sauvegardes.
- Planifier des opérations de sauvegarde.
- Surveillez les opérations de sauvegarde, de restauration et de clonage.
- Afficher les rapports sur les opérations de sauvegarde, de restauration et de clonage.

Fonctionnalités du plug-in SnapCenter pour PostgreSQL

SnapCenter s'intègre à l'application plug-in et aux technologies NetApp sur le système de stockage. Pour travailler avec le plug-in pour le cluster PostgreSQL, vous utilisez l'interface utilisateur graphique SnapCenter .

- **Interface utilisateur graphique unifiée**

L'interface SnapCenter assure la standardisation et la cohérence entre les plug-ins et les environnements. L'interface SnapCenter vous permet d'effectuer des opérations de sauvegarde, de restauration et de clonage cohérentes sur tous les plug-ins, d'utiliser des rapports centralisés, d'utiliser des vues de tableau de bord en un coup d'œil, de configurer le contrôle d'accès basé sur les rôles (RBAC) et de surveiller les tâches sur tous les plug-ins.

- **Administration centrale automatisée**

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

- **Technologie de copie instantanée NetApp non perturbatrice**

SnapCenter utilise la technologie de snapshot NetApp avec le plug-in pour cluster PostgreSQL pour sauvegarder les ressources.

L'utilisation du plug-in pour PostgreSQL offre également les avantages suivants :

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

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

- Création de copies de ressources à faible encombrement et ponctuelles pour les tests ou l'extraction de données à l'aide de la technologie NetApp FlexClone

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

- Prise en charge de la fonctionnalité de snapshot du groupe de cohérence (CG) d' ONTAP dans le cadre de la création de sauvegardes.
- Capacité à exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de ressources

En une seule opération, les snapshots sont consolidés lorsque les ressources d'un seul hôte partagent le même volume.

- Capacité à créer des instantanés à l'aide de commandes externes.
- Prise en charge de Linux LVM sur le système de fichiers XFS.

Types de stockage pris en charge par le plug-in SnapCenter pour PostgreSQL

SnapCenter prend en charge une large gamme de types de stockage sur les machines physiques et les machines virtuelles (VM). Vous devez vérifier la prise en charge de votre type de stockage avant d'installer SnapCenter Plug-in pour PostgreSQL.

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"> • LUN connectés au FC • LUN connectés à iSCSI • Volumes connectés NFS
VMware ESXi	<ul style="list-style-type: none"> • L'analyse des adaptateurs de bus hôte (HBA) peut prendre beaucoup de temps, car SnapCenter analyse tous les adaptateurs de bus hôte présents dans l'hôte. <p>Vous pouvez modifier le fichier LinuxConfig.pm situé dans <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> pour définir la valeur du paramètre SCSI_HOSTS_OPTIMIZED_RESCAN sur 1 afin de réanalyser uniquement les HBA répertoriés dans HBA_DRIVER_NAMES.</p> <ul style="list-style-type: none"> • LUN iSCSI connectés directement au système invité par l'initiateur iSCSI • VMDK sur les banques de données NFS • VMDK sur VMFS • Volumes NFS connectés directement au système invité • Banques de données vVol sur NFS et SAN <p>La banque de données vVol ne peut être provisionnée qu'avec ONTAP Tools pour VMware vSphere.</p>

Privilèges ONTAP minimaux requis pour le plug-in PostgreSQL

Les privilèges ONTAP minimaux requis varient en fonction des plug-ins SnapCenter que vous utilisez pour la protection des données.

- Commandes d'accès complet : privilèges minimaux requis pour ONTAP 9.12.1 et versions ultérieures
 - événement générer-autosupport-log
 - historique de travail afficher
 - arrêt de travail
 - lune
 - création de lun
 - création de lun
 - création de lun
 - suppression de lun

- lun igroup ajouter
- création de groupe i lun
- suppression du groupe i lun
- renommer le groupe i de lun
- renommer le groupe i de lun
- émission igroup lun
- mappage lun add-reporting-nodes
- création de mappage LUN
- suppression du mappage LUN
- suppression des nœuds de rapport de mappage LUN
- émission de cartographie LUN
- lun modifier
- volume de déplacement lun
- lun hors ligne
- lun en ligne
- lun réservation persistante claire
- redimensionner lun
- série lun
- spectacle lunaire
- règle d'ajout de politique SnapMirror
- règle de modification de la politique SnapMirror
- règle de suppression de la politique SnapMirror
- afficher la politique de SnapMirror
- restauration snapmirror
- spectacle snapmirror
- historique des émissions de SnapMirror
- mise à jour de SnapMirror
- mise à jour snapmirror-ls-set
- liste-destinations snapmirror
- version
- création de clone de volume
- spectacle de clone de volume
- démarrage fractionné du clonage de volume
- volume clone fractionnement arrêt
- création de volume
- destruction de volume
- création de clone de fichier de volume

- fichier de volume show-disk-usage
- volume hors ligne
- volume en ligne
- modification du volume
- création de volume qtree
- suppression du volume qtree
- volume qtree modifier
- volume qtree afficher
- restriction de volume
- spectacle de volume
- création d'un instantané de volume
- suppression d'instantané de volume
- modification de l'instantané du volume
- modification de l'instantané du volume-snaplock-expiration-time
- renommer l'instantané du volume
- restauration d'instantanés de volume
- fichier de restauration d'instantané de volume
- affichage de l'instantané du volume
- démontage du volume
- cifs de serveur virtuel
- création de partage cifs vserver
- suppression du partage cifs du serveur virtuel
- affichage de la copie fantôme cifs du serveur virtuel
- affichage du partage cifs du serveur virtuel
- affichage cifs du serveur virtuel
- politique d'exportation du serveur virtuel
- création de politique d'exportation de serveur virtuel
- suppression de la politique d'exportation du serveur virtuel
- création d'une règle de politique d'exportation de serveur virtuel
- afficher la règle de politique d'exportation du serveur virtuel
- afficher la politique d'exportation du serveur virtuel
- serveur virtuel iscsi
- affichage de la connexion vserver iscsi
- spectacle de serveur virtuel
- Commandes en lecture seule : privilèges minimaux requis pour ONTAP 8.3.0 et versions ultérieures
 - interface réseau
 - affichage de l'interface réseau

- serveur virtuel

Préparer les systèmes de stockage pour la réplication SnapMirror et SnapVault pour PostgreSQL

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

SnapCenter exécute les mises à jour de SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour de SnapMirror et SnapVault sont effectuées dans le cadre du travail SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous accédez à SnapCenter à partir 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 stockage principal (le volume source) vers le stockage secondaire (le volume de destination). Lorsque vous initialisez la relation, ONTAP transfère 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 les volumes SnapMirror et SnapVault (**Primaire** > **Miroir** > **Vault**). Vous devez utiliser des relations en éventail.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles en termes de version. Pour plus de détails sur les relations SnapMirror flexibles en fonction des versions et sur la façon de les configurer, consultez le "[Documentation ONTAP](#)".

Stratégie de sauvegarde pour PostgreSQL

Définir une stratégie de sauvegarde pour PostgreSQL

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 avec succès vos ressources. Votre contrat de niveau de service (SLA), votre objectif de temps de récupération (RTO) et votre objectif de point de récupération (RPO) déterminent en grande partie votre stratégie de sauvegarde.

À propos de cette tâche

Un SLA définit le niveau de service attendu et aborde de nombreux problèmes liés au service, notamment la disponibilité et les performances du service. Le RTO est le temps pendant lequel un processus métier doit être restauré après une interruption de service. Le RPO définit la stratégie relative à l'âge des fichiers qui doivent être récupérés à partir du stockage de sauvegarde pour que les opérations régulières reprennent après une panne. SLA, RTO et RPO contribuent à la stratégie de protection des données.

Étapes

1. Déterminez quand vous devez sauvegarder vos ressources.

2. Décidez du nombre de tâches de sauvegarde dont vous avez besoin.
3. Décidez comment nommer vos sauvegardes.
4. Décidez si vous souhaitez créer une stratégie basée sur une copie d'instantanés pour sauvegarder les instantanés cohérents avec les applications du cluster.
5. Décidez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réplication ou la technologie NetApp SnapVault pour la conservation à long terme.
6. Déterminez la période de conservation des snapshots sur le système de stockage source et la destination SnapMirror .
7. Déterminez si vous souhaitez exécuter des commandes avant ou après l'opération de sauvegarde et fournissez un prescript ou un postscript.

Découverte automatique des ressources sur l'hôte Linux

Les ressources sont des clusters et des instances PostgreSQL sur l'hôte Linux qui sont gérés par SnapCenter. Après l'installation du plug-in SnapCenter pour PostgreSQL, les clusters PostgreSQL de toutes les instances de cet hôte Linux sont automatiquement découverts et affichés dans la page Ressources.

Type de sauvegardes prises en charge

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge le type de sauvegarde basé sur une copie instantanée pour les clusters PostgreSQL.

Sauvegarde basée sur une copie instantanée

Les sauvegardes basées sur des copies instantanées exploitent la technologie de capture instantanée NetApp pour créer des copies en ligne en lecture seule des volumes sur lesquels résident les clusters PostgreSQL.

Comment le plug-in SnapCenter pour PostgreSQL utilise les instantanés de groupe de cohérence

Vous pouvez utiliser le plug-in pour créer des instantanés de groupe de cohérence pour les groupes de ressources. Un groupe de cohérence est un conteneur qui peut héberger plusieurs volumes afin que vous puissiez les gérer comme une seule entité. Un groupe de cohérence est constitué d'instantanés simultanés de plusieurs volumes, fournissant des copies cohérentes d'un groupe de volumes.

Vous pouvez également spécifier le temps d'attente pour que le contrôleur de stockage regroupe systématiquement les snapshots. 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) pendant l'opération de capture instantanée de groupe cohérente. La synchronisation WAFL améliore les performances d'un instantané de groupe de cohérence.

Comment SnapCenter gère la maintenance des sauvegardes de données

SnapCenter gère la maintenance des sauvegardes de données au niveau du système de stockage et du système de fichiers.

Les instantanés sur le stockage principal ou secondaire et leurs entrées correspondantes dans le catalogue

PostgreSQL sont supprimés en fonction des paramètres de conservation.

Considérations pour déterminer les planifications de sauvegarde pour PostgreSQL

Le facteur le plus critique dans la détermination d'un calendrier de sauvegarde est le taux de changement de la ressource. Vous pouvez sauvegarder une ressource très utilisée toutes les heures, tandis que vous pouvez sauvegarder une ressource rarement utilisée une fois par jour. D'autres facteurs incluent l'importance de la ressource pour votre organisation, votre contrat de niveau de service (SLA) et votre objectif de point de récupération (RPO).

Les planifications de sauvegarde comportent deux parties, comme suit :

- Fréquence de sauvegarde (à quelle fréquence les sauvegardes doivent être effectuées)

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

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

Les planifications de sauvegarde font partie d'une configuration de ressource ou de groupe de ressources. Par exemple, si vous disposez d'un groupe de ressources dont la politique est configurée pour des sauvegardes hebdomadaires, vous pouvez configurer la planification pour effectuer une sauvegarde tous les jeudis à 22h00.

Nombre de tâches de sauvegarde nécessaires pour PostgreSQL

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 variation de la ressource et votre contrat de niveau de service (SLA).

Conventions de nommage des sauvegardes pour les clusters Plug-in for PostgreSQL

Vous pouvez utiliser la convention de nommage par défaut des instantanés ou une convention de nommage personnalisée. La convention de dénomination de sauvegarde par défaut ajoute un horodatage aux noms d'instantanés qui vous aide à identifier le moment où les copies ont été créées.

L'instantané utilise la convention de dénomination 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 les significations suivantes :

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

Vous pouvez également spécifier le format du nom de l'instantané lors de la protection des ressources ou des groupes de ressources en sélectionnant **Utiliser un format de nom personnalisé pour la copie de l'instantané**. Par exemple, `customtext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Par défaut, le suffixe d'horodatage est ajouté au nom de l'instantané.

Stratégie de restauration et de récupération pour PostgreSQL

Définir une stratégie de restauration et de récupération pour les ressources PostgreSQL

Vous devez définir une stratégie avant de restaurer et de récupérer votre cluster afin de pouvoir effectuer les opérations de restauration et de récupération avec succès.



Seule la récupération manuelle du cluster est prise en charge.

Étapes

1. Déterminer les stratégies de restauration prises en charge pour les ressources PostgreSQL ajoutées manuellement
2. Déterminer les stratégies de restauration prises en charge pour les clusters PostgreSQL découverts automatiquement
3. Décidez du type d'opérations de récupération que vous souhaitez effectuer.

Types de stratégies de restauration prises en charge pour les ressources PostgreSQL ajoutées manuellement

Vous devez définir une stratégie avant de pouvoir effectuer avec succès des opérations de restauration à l'aide de SnapCenter.



Vous ne pouvez pas récupérer les ressources PostgreSQL ajoutées manuellement.

Restauration complète des ressources

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



Si la ressource contient des volumes ou des qtrees, les snapshots pris après le snapshot sélectionné pour la restauration sur ces volumes ou qtrees sont supprimés et ne peuvent pas être récupérés. De plus, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

REMARQUE : le plug-in pour PostgreSQL crée un `backup_label` et un `tablespace_map` dans le dossier `/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/_` pour faciliter la récupération manuelle.

Type de stratégie de restauration pris en charge pour PostgreSQL découvert automatiquement

Vous devez définir une stratégie avant de pouvoir effectuer avec succès des opérations de restauration à l'aide de SnapCenter.

La restauration complète des ressources est la stratégie de restauration prise en charge pour les clusters PostgreSQL découverts automatiquement. Cela restaure tous les volumes, qtrees et LUN d'une ressource.

Types d'opérations de restauration pour PostgreSQL découvert automatiquement

Le plug-in SnapCenter pour PostgreSQL prend en charge les types de restauration SnapRestore à fichier unique et de connexion et de copie pour les clusters PostgreSQL découverts automatiquement.

Single File SnapRestore est effectué dans les environnements NFS pour les scénarios suivants :

- Si seule l'option **Ressource complète** est sélectionnée
- Lorsque la sauvegarde sélectionnée provient d'un emplacement secondaire SnapMirror ou SnapVault et que l'option **Ressource complète** est sélectionnée

Single File SnapRestore est exécuté dans les environnements SAN pour les scénarios suivants :

- Si seule l'option **Ressource complète** est sélectionnée
- Lorsque la sauvegarde est sélectionnée à partir d'un emplacement secondaire SnapMirror ou SnapVault et que l'option **Ressource complète** est sélectionnée

Types d'opérations de récupération pris en charge pour les clusters PostgreSQL

SnapCenter vous permet d'effectuer différents types d'opérations de récupération pour les clusters PostgreSQL.

- Récupérer le cluster jusqu'à l'état le plus récent
- Récupérer le cluster jusqu'à un moment précis

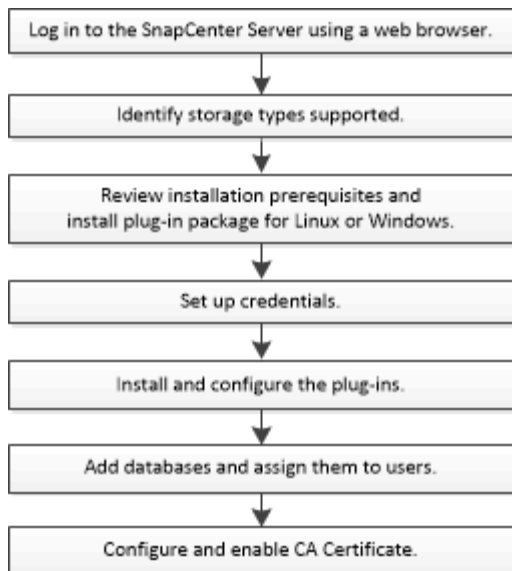
Vous devez spécifier la date et l'heure de récupération.

SnapCenter fournit également l'option Aucune récupération pour les clusters PostgreSQL.

Préparez-vous à installer le plug-in SnapCenter pour PostgreSQL

Flux de travail d'installation du plug-in SnapCenter pour PostgreSQL

Vous devez installer et configurer le plug-in SnapCenter pour PostgreSQL si vous souhaitez protéger les clusters PostgreSQL.



Conditions préalables pour ajouter des hôtes et installer le plug-in SnapCenter pour PostgreSQL

Avant d'ajouter un hôte et d'installer les packages de plug-ins, vous devez remplir toutes les conditions requises. Le plug-in SnapCenter pour PostgreSQL est disponible dans les environnements Windows et Linux.

- Vous devez avoir installé Java 11 sur votre hôte.



IBM Java n'est pas pris en charge sur les hôtes Windows et Linux.

- Pour Windows, le service de création de plug-in doit être exécuté à l'aide de l'utilisateur Windows « LocalSystem », qui est le comportement par défaut lorsque le plug-in pour PostgreSQL est installé en tant qu'administrateur de domaine.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez des informations d'identification qui ne sont pas intégrées 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 PostgreSQL sur les hôtes Windows.
- SnapCenter Server doit avoir accès au port 8145 ou au port personnalisé de l'hôte Plug-in pour PostgreSQL.

hôtes Windows

- Vous devez disposer d'un utilisateur de domaine avec des privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour PostgreSQL sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH basée sur un mot de passe pour l'utilisateur root ou non root.
- Vous devez avoir installé Java 11 sur votre hôte Windows.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Outil de matrice d'interopérabilité NetApp"](#)

Hôtes Linux

- Vous devez avoir activé la connexion SSH basée sur un mot de passe pour l'utilisateur root ou non root.
- Vous devez avoir installé Java 11 sur votre hôte Linux.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Outil de matrice d'interopérabilité NetApp"](#)

- Pour les clusters PostgreSQL exécutés sur un hôte Linux, lors de l'installation du plug-in pour PostgreSQL, le plug-in SnapCenter pour UNIX est installé automatiquement.
- Vous devriez avoir **bash** comme shell par défaut pour l'installation du plug-in.

Commandes supplémentaires

Pour exécuter une commande supplémentaire sur le plug-in SnapCenter pour PostgreSQL, vous devez l'inclure dans le fichier *allowed_commands.config*.

- Emplacement par défaut sur l'hôte Windows : *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Emplacement par défaut sur l'hôte Linux : */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Pour autoriser les commandes supplémentaires sur l'hôte du plug-in, ouvrez le fichier *allowed_commands.config* dans un éditeur. Saisissez chaque commande sur une ligne distincte et les commandes ne sont pas sensibles à la casse. Assurez-vous de spécifier le chemin d'accès complet et de placer le chemin d'accès entre guillemets (") s'il contient des espaces.

Par exemple:

commande : mount commande : umount commande : "C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe" commande : myscript.bat

Si le fichier *allowed_commands.config* n'est pas présent, l'exécution des commandes ou du script sera bloquée et le workflow échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plugin."

Si la commande ou le script n'est pas présent dans *allowed_commands.config*, l'exécution de la commande ou du script sera bloquée et le workflow échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plugin."



Vous ne devez pas utiliser d'entrée générique (*) pour autoriser toutes les commandes.

Configurer les privilèges sudo pour les utilisateurs non root pour l'hôte Linux

SnapCenter permet à un utilisateur non root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus du plug-in s'exécuteront en tant qu'utilisateur non root effectif. Vous devez configurer les privilèges sudo pour l'utilisateur non root afin de fournir l'accès à plusieurs chemins.

Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si le masque est 0027, assurez-vous que le dossier Java et tous les fichiers qu'il contient doivent avoir l'autorisation 555. Dans le cas contraire, l'installation du plug-in risque d'échouer.
- Pour l'utilisateur non root, assurez-vous que le nom de l'utilisateur non root et le groupe de l'utilisateur doivent être identiques.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification des messages : MAC hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après avoir mis à jour le fichier de configuration.

Exemple:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

À propos de cette tâche

Vous devez configurer les privilèges sudo pour l'utilisateur non root afin de fournir l'accès aux chemins suivants :

- `/home/LINUX_USER/sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/emplacement_personnalisé/ NetApp/snapcenter/spl/bin/spl`

Mesures

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer le package de plug-ins SnapCenter pour Linux.
2. Ajoutez les lignes suivantes au fichier `/etc/sudoers` en utilisant l'utilitaire Linux visudo.


```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

LINUX_USER est le nom de l'utilisateur non root que vous avez créé.

Vous pouvez obtenir la *valeur de somme de contrôle* à partir du fichier **sc_unix_plugins_checksum.txt**, qui se trouve à :


- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` _ si SnapCenter Server est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` _ si SnapCenter Server est installé sur un hôte Linux.



L'exemple doit être utilisé uniquement comme référence pour la création de vos propres données.


Configuration requise pour l'installation du package de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez vous familiariser avec certaines exigences de base en matière d'espace et de taille du système hôte.

Article	Exigences
Systèmes d'exploitation	<p>Microsoft Windows</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 Go
Espace minimum d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 Go</p> <div>  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace journal 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 récemment exécutées.</p> </div>
Logiciels requis	<ul style="list-style-type: none"> • Pack d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs) • PowerShell Core 7.4.2 <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, consultez "La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes hérités qui ne disposent pas de connectivité Internet."</p>

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

Avant d'installer le package de plug-ins SnapCenter pour Linux, vous devez vous familiariser avec certaines exigences de base en matière d'espace et de taille du système hôte.

Article	Exigences
Systèmes d'exploitation	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Serveur d'entreprise SUSE Linux (SLES) <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 Go
Espace minimum d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>2 Go</p> <div>  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace journal 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 récemment exécutées.</p> </div>
Logiciels requis	<p>Java 11 Oracle Java et OpenJDK</p> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .</p>

Configurer les informations d'identification pour le plug-in SnapCenter pour PostgreSQL

SnapCenter utilise des informations d'identification 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 effectuer des opérations de protection des données sur des clusters 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 du plug-in.

Meilleure pratique : bien que vous soyez autorisé à créer des informations d'identification pour Linux après avoir déployé des hôtes et installé des plug-ins, la meilleure pratique consiste à créer des informations d'identification après avoir ajouté des 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 des privilèges d'administrateur, y compris des 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 attribuer au moins les privilèges de groupe de ressources et 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 **Informations d'identification**.
3. Cliquez sur **Nouveau**.
4. Dans la page Informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce domaine...	Fais ceci...
Nom d'identification	Entrez un nom pour les informations d'identification.

Pour ce domaine...	Fais ceci...
Nom d'utilisateur	<p>Saisissez le nom d'utilisateur et le mot de passe qui doivent être utilisés pour l'authentification.</p> <ul style="list-style-type: none"> Administrateur de domaine ou tout membre du groupe d'administrateurs <p>Indiquez l'administrateur du domaine ou tout membre du groupe d'administrateurs du système sur lequel vous installez le plug-in SnapCenter . Les formats valides pour le champ Nom d'utilisateur sont :</p> <ul style="list-style-type: none"> <i>NetBIOS\Nom d'utilisateur</i> <i>Domaine FQDN\Nom d'utilisateur</i> Administrateur local (pour les groupes de travail uniquement) <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré du système sur lequel vous installez le plug-in SnapCenter . Vous pouvez spécifier un compte utilisateur local appartenant au groupe des administrateurs locaux si ce compte dispose de privilèges élevés ou si la fonctionnalité de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide pour le champ Nom d'utilisateur est : <i>UserName</i></p> <p>N'utilisez pas de guillemets doubles (") ou de backtick (`) dans les mots de passe. Vous ne devez pas utiliser les symboles inférieur à (<) et d'exclamation (!) ensemble dans les mots de passe. Par exemple, lessthan<!10, lessthan10<!, backtick`12.</p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.
Utiliser les privilèges sudo	<p>Cochez la case Utiliser les privilèges sudo si vous créez des informations d'identification pour un utilisateur non root.</p> <div>  <p>Applicable uniquement aux utilisateurs Linux.</p> </div>

5. Cliquez sur **OK**.

Une fois que vous avez terminé de configurer les informations d'identification, vous souhaitez peut-être attribuer la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs dans la page Utilisateur et accès.

Configurer gMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (gMSA) qui fournit une gestion automatisée des mots de passe des comptes de service à partir d'un compte de domaine géré.

Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 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 -EffectiveImmediately
3. Créez et configurez votre gMSA :
 - a. Créez un compte de groupe d'utilisateurs au format suivant :

```
domainName\accountName$  
.. Ajoutez des objets informatiques 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,...>  
.. Courir `Get-ADServiceAccount` commande 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, exécutez 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.

- Redémarrez votre hôte.
 - Installez le gMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`
 - Vérifiez votre compte gMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`
- Attribuez les privilèges administratifs au gMSA configuré sur l'hôte.
 - Ajoutez l'hôte Windows en spécifiant le compte gMSA configuré dans le serveur SnapCenter .

SnapCenter Server installera les plug-ins sélectionnés sur l'hôte et le gMSA spécifié sera utilisé comme compte de connexion au service pendant l'installation du plug-in.

Installer le plug-in SnapCenter pour PostgreSQL

Ajouter des hôtes et installer des packages de plug-ins sur des hôtes distants

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

Avant de commencer

- Si le système d'exploitation de l'hôte SnapCenter Server est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, vous devez effectuer les opérations suivantes :
 - Mise à niveau vers Windows Server 2019 (build du système d'exploitation 17763.5936) ou version ultérieure
 - Mise à niveau vers Windows Server 2022 (build du système d'exploitation 20348.2402) ou version ultérieure

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation de plug-in, tel que le rôle Administrateur SnapCenter .
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez des informations d'identification qui ne sont pas intégrées ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Vous devez vous assurer 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 un compte de service géré de groupe (gMSA), vous devez configurer gMSA avec des privilèges administratifs.


["Configurer un compte de service géré de groupe sur Windows Server 2016 ou version ultérieure pour PostgreSQL"](#)


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 .

Étapes

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


Pour ce domaine...	Fais ceci...
Type d'hôte	<p>Sélectionnez le type d'hôte :</p> <ul style="list-style-type: none"> • Windows • Linux <div>  <p>Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL, et cet hôte peut être sur un système Windows ou un système Linux.</p> </div>
Nom d'hôte	<p>Entrez le nom de l'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.</p>



Pour ce domaine...	Fais ceci...
Informations d'identification	<p>Sélectionnez le nom des informations d'identification que vous avez créées ou créez de nouvelles informations d'identification. L'identifiant doit disposer de droits administratifs sur l'hôte distant. Pour plus de détails, consultez les informations sur la création d'informations d'identification.</p> <p>Vous pouvez afficher les détails des informations d'identification en positionnant votre curseur sur le nom des informations d'identification que vous avez fournies.</p> <div>  <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajouter un hôte.</p> </div>

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

Lors de l'utilisation de l'API REST pour installer le plug-in pour PostgreSQL, vous devez transmettre la version 3.0. Par exemple, PostgreSQL:3.0

6. (Facultatif) Cliquez sur **Plus d'options**.

Pour ce domaine...	Fais ceci...
Port	<p>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 sera affiché comme port par défaut.</p> <div>  <p>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Sinon, l'opération échoue.</p> </div>

Pour ce domaine...	Fais ceci...
Chemin d'installation	<p>Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL, et cet hôte peut être sur un système Windows ou un système Linux.</p> <ul style="list-style-type: none"> • Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\ NetApp\ SnapCenter. En option, vous pouvez personnaliser le chemin. • Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/ NetApp/snapcenter. En option, vous pouvez personnaliser le chemin.
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas valider si l'hôte répond aux exigences d'installation du plug-in.
Ajouter tous les hôtes du cluster	Cochez cette case pour ajouter tous les nœuds du cluster.
Utiliser un compte de service géré de groupe (gMSA) pour exécuter les services du plug-in	<p>Pour l'hôte Windows, cochez cette case si vous souhaitez utiliser un compte de service géré de groupe (gMSA) pour exécuter les services de plug-in.</p> <div>  <p>Fournissez le nom gMSA au format suivant : domainName\accountName\$.</p> </div> <div>  <p>gMSA sera utilisé comme compte de service de connexion uniquement pour le service SnapCenter Plug-in pour Windows.</p> </div>

7. Cliquez sur **Soumettre**.

Si vous n'avez pas coché la case « Ignorer les pré-vérifications », l'hôte est validé afin de vérifier s'il répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version de PowerShell, la version de .NET, l'emplacement (pour les plug-ins Windows) et la version de Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. Si les exigences minimales ne sont pas respectées, 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 dans C:\Program Files\ NetApp\ SnapCenter WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez résoudre le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez mettre à jour le fichier 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 digitale de chacun des nœuds du cluster.



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

9. Surveiller la progression de l'installation.

- Pour le plug-in Windows, les journaux d'installation et de mise à niveau se trouvent à : `C:\Windows\SnapCenter plugin\Install<JOBID>_`
- Pour le plug-in Linux, les journaux d'installation se trouvent à : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_` et les journaux de mise à niveau se trouvent à : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_`

Installer les packages de plug-ins SnapCenter pour Linux ou Windows sur plusieurs hôtes distants à l'aide d'applets de commande

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

Avant de commencer

Vous devez vous être connecté à SnapCenter en tant qu'utilisateur de domaine avec des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le package de plug-in.

Étapes

1. Lancez PowerShell.
2. Sur l'hôte SnapCenter Server, établissez une session à l'aide de l'applet de commande `Open-SmConnection`, puis entrez 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 concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Alternativement, vous pouvez également vous référer 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 que vous ne souhaitez pas valider 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 PostgreSQL sur les hôtes Linux à l'aide de l'interface de ligne de commande

Vous devez installer le plug-in SnapCenter pour le cluster PostgreSQL à l'aide de l'interface utilisateur (UI) de SnapCenter. Si votre environnement ne permet pas

l'installation à distance du plug-in à partir de l'interface utilisateur SnapCenter , vous pouvez installer le plug-in pour le cluster PostgreSQL en mode console ou en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

Avant de commencer

- Vous devez installer le plug-in pour le cluster PostgreSQL sur chacun des hôtes Linux sur lesquels réside le client PostgreSQL.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour le cluster PostgreSQL doit répondre aux exigences logicielles, de cluster et de système d'exploitation dépendantes.

L'outil de matrice d'interopérabilité (IMT) contient les informations les plus récentes sur les configurations prises en charge.

"Outil de matrice d'interopérabilité NetApp"

- Le plug-in SnapCenter pour le cluster PostgreSQL fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer le package de plug-ins SnapCenter pour Linux, vous devez déjà avoir 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 sur lequel vous souhaitez installer le plug-in pour PostgreSQL.

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. Installer 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 HTTPS SMCore.
 - -DSERVER_IP spécifie l'adresse IP du serveur SnapCenter .
 - -DSERVER_HTTPS_PORT spécifie le port HTTPS du serveur SnapCenter .
 - -DUSER_INSTALL_DIR spécifie le répertoire dans lequel vous souhaitez installer le package de plug-ins SnapCenter pour Linux.
 - DINSTALL_LOG_NAME spécifie 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 = PostgreSQL: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 concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

Surveiller l'état d'installation du plug-in pour PostgreSQL

Vous pouvez surveiller la progression de l'installation du package de plug-in SnapCenter à l'aide de la page Tâches. Vous souhaitez peut-être 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 Tâches et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu 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 **Tâches**.
3. Dans la page **Tâches**, pour filtrer la liste afin que seules les opérations d'installation de plug-ins soient répertoriées, procédez comme suit :
 - a. Cliquez sur **Filtre**.
 - b. Facultatif : précisez la date 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 la tâche d'installation et cliquez sur **Détails** pour afficher les détails de la tâche.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Configurer le certificat CA

Générer le fichier CSR du certificat CA

Vous pouvez générer une demande 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 CSR générée. Le certificat aura une clé privée associée.

Le CSR est un bloc de texte codé qui est remis à un fournisseur de certificats autorisé pour obtenir le certificat CA signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3 072 bits.

Pour plus d'informations sur la génération d'un CSR, voir ["Comment générer un fichier CSR de certificat CA"](#).



Si vous possédez le certificat CA pour votre domaine (*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat CA. Vous pouvez déployer le certificat CA existant avec SnapCenter.

Pour les configurations de cluster, le nom du cluster (FQDN du cluster virtuel) et les noms d'hôtes respectifs doivent être mentionnés dans le certificat CA. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat générique (*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôtes du domaine.

Importer des certificats CA

Vous devez importer les certificats CA 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 un composant logiciel enfichable**.
2. Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable Certificats, sélectionnez l'option **Compte d'ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Racine de la console > Certificats – Ordinateur local > Autorités de certification racines de confiance > Certificats**.
5. Cliquez avec le bouton droit sur le dossier « Autorités de certification racines de confiance », puis sélectionnez **Toutes les tâches > Importer** pour démarrer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer la clé privée	Sélectionnez l'option Oui , importez la clé privée, puis cliquez sur Suivant .
Format de fichier d'importation	N'effectuez aucune modification ; cliquez sur Suivant .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur Suivant .
Terminer l'assistant d'importation de certificat	Consultez le résumé, puis cliquez sur Terminer pour démarrer 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 ».

Obtenir l'empreinte numérique du certificat CA

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

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 **Empreinte digitale**.
 - d. Copiez les caractères hexadécimaux de la boîte.
 - e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte digitale est : « a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b », après avoir supprimé les espaces, elle sera : « a909502dd82ae41433e6f83886b00d4277a32a7b ».

2. Effectuez les opérations suivantes à partir de PowerShell :
 - a. Exécutez la commande suivante pour répertorier l'empreinte numérique du certificat installé et identifier le certificat récemment installé par le nom du sujet.

```
Get-ChildItem -Chemin Cert:\LocalMachine\Mon
```

- b. Copiez l'empreinte digitale.

Configurer le certificat CA avec les services de plug-in hôte Windows

Vous devez configurer le certificat CA avec les services de plug-in hôte Windows pour activer le certificat numérique installé.

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

Étapes

1. Supprimez la liaison de certificat existante 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
. Liez le certificat nouvellement 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"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configurer le certificat CA pour le service de plug-ins SnapCenter PostgreSQL sur l'hôte Linux

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

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

Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

Étapes

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

Il s'agit de la valeur correspondant à la clé 'KEYSTORE_PASS'.

2. Modifier le mot de passe du keystore :

```
keytool -storepasswd -keystore keystore.jks
. Modifiez le mot de passe de tous les alias des entrées de clés privées
dans le magasin de clés avec le même mot de passe que celui utilisé pour
le magasin de clés :
```

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

Mettez à jour la même chose 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 du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le trust-store.

Étapes

1. Accédez au dossier contenant le keystore du plug-in : `/opt/ NetApp/snapcenter/scc/etc`.
2. Localisez le fichier « `keystore.jks` ».
3. Répertoriez les certificats ajoutés dans le keystore :

```
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  
intermédiaires pour connecter le magasin de confiance.
```



Vous devez ajouter le certificat CA racine, puis les certificats CA intermédiaires.

Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de clés de confiance du plug-in.

Étapes

1. Accédez au dossier contenant le keystore du plug-in `/opt/ NetApp/snapcenter/scc/etc`.
2. Localisez le fichier « `keystore.jks` ».
3. Répertoriez les certificats ajoutés dans le keystore :

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

4. Ajoutez le certificat CA contenant à la fois 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. Répertoriez les certificats ajoutés dans le keystore.

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

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat CA, 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 par défaut du magasin de clés du plug-in est la valeur de la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

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

. Si le nom d'alias dans le certificat CA est long et contient des espaces 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 à jour cette valeur 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 pour le plug-in trust-store.

Configurer la liste de révocation des certificats (CRL) pour les plug-ins

À propos de cette tâche

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

Étapes

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

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

Configurer le certificat CA pour le service de plug-ins SnapCenter PostgreSQL sur l'hôte Windows

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

Les plug-ins utilisent le fichier `keystore.jks`, qui se trouve dans `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc` à la fois comme magasin de confiance et comme magasin de clés.

Étapes

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

Il s'agit de la valeur correspondant à la clé `KEYSTORE_PASS`.

2. Modifier le mot de passe du keystore :

```
keytool -storepasswd -keystore magasin de clés.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\<version_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Modifiez le mot de passe de tous les alias des entrées de clés privées dans le magasin de clés avec le même mot de passe que celui utilisé pour le magasin de clés :

```
keytool -keypasswd -alias "nom_d'alias_dans_cert" -keystore keystore.jks
```

Mettez à jour la même chose 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 du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le trust-store.

Étapes

1. Accédez au dossier contenant le keystore 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 keystore :

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

4. Ajouter un certificat racine ou intermédiaire :

```
keytool -import -trustcacerts -alias myRootCA -fichier /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour connecter le magasin de confiance.



Vous devez ajouter le certificat CA racine, puis les certificats CA intermédiaires.

Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de clés de confiance du plug-in.

Étapes

1. Accédez au dossier contenant le keystore 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 keystore :

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

4. Ajoutez le certificat CA contenant à la fois 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. Répertoriez les certificats ajoutés dans le keystore.

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

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat CA, 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 par défaut du magasin de clés du plug-in est la valeur de la clé KEYSTORE_PASS dans le fichier *agent.properties*.

```
keytool -keypasswd -alias "nom_d'alias_dans_CA_cert" -keystore keystore.jks
```

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

Mettez à jour cette valeur 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 pour le plug-in trust-store.

Configurer la liste de révocation des certificats (CRL) pour les plug-ins SnapCenter

À propos de cette tâche

- Pour télécharger le dernier fichier CRL pour le certificat CA associé, voir ["Comment mettre à jour le fichier de liste de révocation de certificats dans SnapCenter CA Certificate"](#) .
- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins 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 dans le 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 par rapport à chaque CRL.

Activer les certificats CA pour les plug-ins

Vous devez configurer les certificats CA et déployer les certificats CA sur le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat CA pour les plug-ins.

Avant de commencer

- Vous pouvez activer ou désactiver les certificats d'autorité de certification à l'aide de l'applet de commande `run Set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat des plug-ins à l'aide de `Get-SmCertificateSettings`.





Les informations concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Alternativement, vous pouvez également vous référer à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Hôtes gérés**.
3. Sélectionnez un ou plusieurs hôtes de plug-in.
4. Cliquez sur **Plus d'options**.
5. Sélectionnez **Activer la validation du certificat**.

Après avoir terminé

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

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



Lorsque le statut est jaune ou vert, les opérations de protection des données se terminent avec succès.

Préparez-vous à la protection des données

Conditions préalables à l'utilisation du plug-in SnapCenter pour PostgreSQL

Avant d'utiliser SnapCenter Plug-in pour PostgreSQL, 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 informations d'identification, le cas échéant.
- Installez Java 11 sur votre hôte Linux ou Windows.

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

- Configurez SnapMirror et SnapVault si vous souhaitez une réplication de sauvegarde.

Comment les ressources, les groupes de ressources et les politiques sont utilisés pour protéger PostgreSQL

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

- Les ressources sont généralement des clusters PostgreSQL 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 selon la planification 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 uniques et des groupes de ressources.

- Les politiques spécifient la fréquence de sauvegarde, 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 politique lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

Considérez un groupe de ressources comme définissant ce que vous souhaitez protéger et quand vous souhaitez le protéger en termes de jour et d'heure. Considérez une politique comme définissant la manière dont vous souhaitez la protéger. Si vous sauvegardez tous les clusters, par exemple, vous pouvez créer un groupe de ressources qui inclut tous les clusters de l'hôte. Vous pouvez ensuite attacher deux politiques au groupe de ressources : une politique quotidienne et une politique horaire. Lorsque vous créez le groupe de ressources et attachez les stratégies, vous pouvez configurer le groupe de ressources pour effectuer une sauvegarde complète quotidienne.

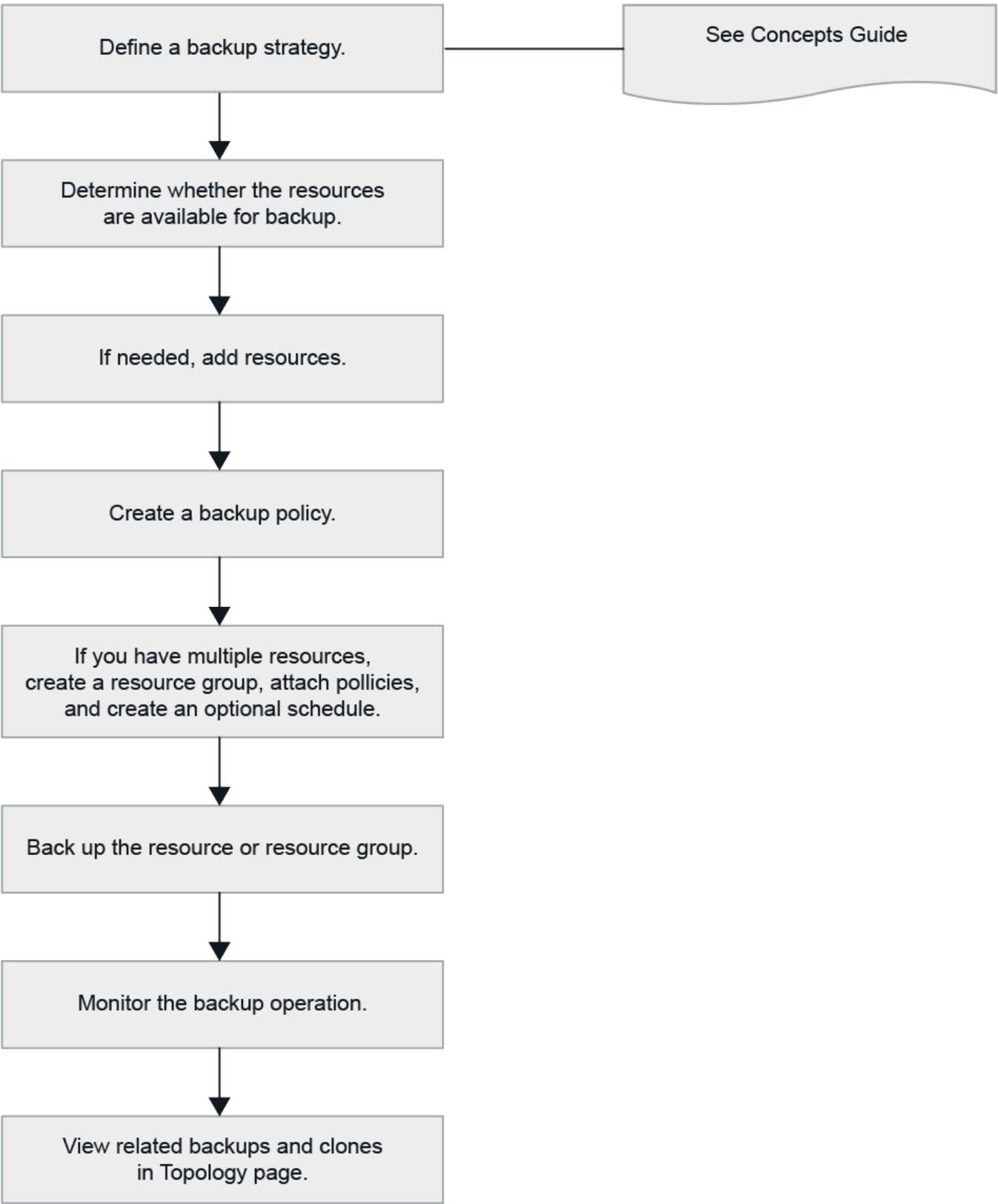
Sauvegarder les ressources PostgreSQL

Sauvegarder les ressources PostgreSQL

Vous pouvez créer une sauvegarde d'une ressource (cluster) ou d'un groupe de ressources. Le flux de travail de sauvegarde comprend la planification, l'identification des clusters à sauvegarder, la gestion des politiques de sauvegarde, la création de groupes

de ressources et l’attachement de politiques, la création de sauvegardes et la surveillance des opérations.

Le flux de travail 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 effectuer des opérations de sauvegarde, de restauration et de clonage. L'aide de l'applet de SnapCenter et les informations de référence de l'applet de commande contiennent plus d'informations sur les applets de commande PowerShell. "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

Découvrir les clusters automatiquement

Les ressources sont des clusters PostgreSQL sur l'hôte Linux qui sont gérés par SnapCenter. Vous pouvez ajouter les ressources aux groupes de ressources pour effectuer des opérations de protection des données après avoir découvert les clusters PostgreSQL disponibles.

Avant de commencer


- Vous devez déjà avoir effectué des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la configuration des connexions au système de stockage.
- Le plug-in SnapCenter pour PostgreSQL ne prend pas en charge la découverte automatique des ressources résidant dans les environnements virtuels RDM/VMDK.

À propos de cette tâche

- Après l'installation du plug-in, tous les clusters de cet hôte Linux sont automatiquement découverts et affichés sur la page Ressources.
- Seuls les clusters sont découverts automatiquement.

Les ressources découvertes 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 PostgreSQL dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste Affichage.
3. (Facultatif) Cliquez sur  *, puis sélectionnez le nom de l'hôte.

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

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

Les ressources sont affichées avec des informations telles que le type de ressource, le nom de l'hôte, les groupes de ressources associés, le type de sauvegarde, les politiques et l'état général.

- Si le cluster se trouve sur un stockage NetApp et n'est pas protégé, la mention « Non protégé » s'affiche dans la colonne État général.
- Si le cluster se trouve sur un système de stockage NetApp et est protégé, et si aucune opération de sauvegarde n'est effectuée, la sauvegarde non exécutée s'affiche dans la colonne État général. Dans le cas contraire, le statut passera à Sauvegarde échouée ou Sauvegarde réussie en fonction du dernier statut de sauvegarde.



Vous devez actualiser les ressources si les clusters sont renommés en dehors de SnapCenter.

Ajouter des ressources manuellement à l'hôte du plug-in

La découverte automatique n'est pas prise en charge sur l'hôte Windows. Vous devez

ajouter les ressources du cluster Postgresql manuellement.

Avant de commencer

- Vous devez avoir effectué des tâches telles que l’installation du serveur SnapCenter , l’ajout d’hôtes et la configuration des connexions au système de stockage.

À propos de cette tâche


La découverte automatique n’est pas prise en charge pour les configurations suivantes :

- Dispositions RDM et VMDK

Étapes

1. Dans le volet de navigation de gauche, sélectionnez le plug-in SnapCenter pour Postgresql dans la liste déroulante, puis cliquez sur **Ressources**.
2. Dans la page Ressources, cliquez sur **Ajouter des ressources Postgresql**.
3. Dans la page Fournir les détails des ressources, effectuez les actions suivantes :

Pour ce domaine...	Fais ceci...
Nom	Spécifiez le nom du cluster.
Nom d'hôte	Entrez le nom de l'hôte.
Type	Sélectionnez le cluster.
Exemple	Spécifiez le nom de l'instance, qui est le parent du cluster.
Informations d'identification	Sélectionnez les informations d'identification ou ajoutez des informations pour les informations d'identification. Ceci est facultatif.

4. Sur la page Fournir l’empreinte de stockage, sélectionnez un type de stockage et choisissez un ou plusieurs volumes, LUN et qtrees, puis cliquez sur **Enregistrer**.
- Facultatif : Vous pouvez cliquer sur le *  * icône pour ajouter plus de volumes, de LUN et de qtrees à partir d’autres systèmes de stockage.
5. Facultatif : dans la page Paramètres des ressources, pour les ressources sur l’hôte Windows, saisissez des paires clé-valeur personnalisées pour le plug-in PostgreSQL
 6. Consultez le résumé, puis cliquez sur **Terminer**.

Les clusters sont affichés avec des informations telles que le nom de l’hôte, les groupes de ressources et les politiques associés, ainsi que l’état général

Si vous souhaitez fournir aux utilisateurs l’accès aux ressources, vous devez attribuer les ressources aux utilisateurs. Cela permet aux utilisateurs d’effectuer les actions pour lesquelles ils disposent d’autorisations sur

les actifs qui leur sont attribués.

["Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources"](#)

Après avoir terminé

- Après avoir ajouté les clusters, vous pouvez modifier les détails du cluster PostgreSQL.
- Les ressources migrées (espace table et clusters) de SnapCenter 5.0 seront marquées comme type de cluster PostgreSQL dans SnapCenter 6.0.
- Lorsque vous modifiez les ressources ajoutées manuellement qui sont migrées à partir de SnapCenter 5.0 ou d'une version antérieure, procédez comme suit dans la page **Paramètres des ressources** pour les paires clé-valeur personnalisées :
 - Spécifiez le terme « PORT » dans le champ **Nom**.
 - Spécifiez le numéro de port dans le champ **Valeur**.

Créer des politiques de sauvegarde pour PostgreSQL

Avant d'utiliser SnapCenter pour sauvegarder des ressources PostgreSQL, vous devez créer une politique de sauvegarde pour la ressource ou le groupe de ressources que vous souhaitez sauvegarder. Une politique de sauvegarde est un ensemble de règles qui régissent la manière dont vous gérez, planifiez et conservez les sauvegardes.

Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde.

Pour plus de détails, consultez les informations sur la définition d'une stratégie de protection des données pour les clusters PostgreSQL.

- 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 au système de stockage et l'ajout de ressources.
- L'administrateur SnapCenter doit vous avoir attribué les SVM pour les volumes source et de destination si vous répliquez des snapshots vers un miroir ou un coffre.

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

À propos de cette tâche

- SnapLock
 - Si l'option « Conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation de SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
 - La spécification d'une période de verrouillage des instantanés empêche la suppression des instantanés jusqu'à l'expiration de la période de conservation. Cela pourrait conduire à conserver un nombre d'instantanés supérieur au nombre spécifié dans la politique.
 - Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots SnapLock Vault dans le cadre de la restauration hériteront du délai d'expiration de SnapLock Vault. L'administrateur de stockage doit nettoyer manuellement les clones après l'expiration de SnapLock .

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Politiques**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, saisissez le nom et les détails de la politique.
5. Dans la page Type de politique, procédez comme suit :
 - a. Sélectionnez le type de stockage.
 - b. 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 clés-valeurs à transmettre au plug-in.

6. Dans la page Sauvegarde et réplication, effectuez les actions suivantes :
 - a. Spécifiez la fréquence de planification en sélectionnant **À la demande**, **Toutes les heures**, **Quotidien**, **Hebdomadaire** ou **Mensuel**.




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 qui partagent la même politique et la même fréquence de sauvegarde, mais vous permet également d'attribuer des planifications de sauvegarde différentes à chaque politique.



Si vous avez programmé à 2 h 00 du matin, la planification ne sera pas déclenchée pendant l'heure d'été (DST).

- a. Dans la section Paramètres d'instantané, spécifiez les paramètres de conservation pour le type de sauvegarde et le type de planification sélectionné dans la page **Type de sauvegarde** :

Si vous voulez...	Alors...
Conserver un certain nombre de clichés	<p>Sélectionnez Copies à conserver, puis spécifiez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés, les copies les plus anciennes étant supprimées en premier.</p> <div>  <p>Vous devez définir le nombre de rétention sur 2 ou plus si vous prévoyez d'activer la réplication SnapVault . Si vous définissez le nombre de rétention sur 1, l'opération de rétention peut échouer car le premier instantané est l'instantané de référence pour la relation SnapVault jusqu'à ce qu'un instantané plus récent soit répliqué sur la cible.</p> </div> <div>  <p>La valeur de rétention maximale est de 1018. Les sauvegardes échoueront si la rétention est définie sur une valeur supérieure à celle prise en charge par la version ONTAP .</p> </div>
Conservez les instantanés pendant un certain nombre de jours	Sélectionnez Conserver les copies pendant , puis spécifiez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage de la copie instantanée	<p>Sélectionnez Période de verrouillage de la copie instantanée et spécifiez les jours, les mois ou les années.</p> <p>La période de conservation de SnapLock doit être inférieure à 100 ans.</p>

7. Sélectionnez une étiquette de politique.



Vous pouvez attribuer des étiquettes SnapMirror aux snapshots principaux pour la réplication à distance, permettant ainsi aux snapshots principaux de décharger l'opération de réplication de snapshot de SnapCenter vers les systèmes secondaires ONTAP . Cela peut être fait sans activer l'option SnapMirror ou SnapVault dans la page de politique.

8. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une ou les deux options de réplication secondaire suivantes :

Pour ce domaine...	Fais ceci...
<p>Mettre à jour SnapMirror après avoir créé une copie Snapshot locale</p>	<p>Sélectionnez ce champ pour créer des copies miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).</p> <p>Si la relation de protection dans ONTAP est de type Miroir et Coffre-fort et si vous sélectionnez uniquement cette option, le snapshot créé sur le primaire ne sera pas transféré vers la destination, mais sera répertorié dans la destination. Si cet instantané est sélectionné à partir de la destination pour effectuer une opération de restauration, le message d'erreur suivant s'affiche : L'emplacement secondaire n'est pas disponible pour la sauvegarde en miroir/en coffre sélectionnée.</p> <p>Lors de la réplication secondaire, l'heure d'expiration de SnapLock charge l'heure d'expiration de SnapLock principale.</p> <p>Cliquer sur le bouton Actualiser dans la page Topologie actualise l'heure d'expiration du SnapLock secondaire et principal récupérée à partir d' ONTAP.</p> <p>Voir "Afficher les sauvegardes et les clones liés aux ressources PostgreSQL dans la page Topologie" .</p>
<p>Mettre à jour SnapVault après avoir créé une copie Snapshot locale</p>	<p>Sélectionnez cette option pour effectuer une réplication de sauvegarde de disque à disque (sauvegardes SnapVault).</p> <p>Lors de la réplication secondaire, l'heure d'expiration de SnapLock charge l'heure d'expiration de SnapLock principale. Cliquer sur le bouton Actualiser dans la page Topologie actualise l'heure d'expiration du SnapLock secondaire et principal récupérée à partir d' ONTAP.</p> <p>Lorsque SnapLock est configuré uniquement sur le secondaire d' ONTAP appelé SnapLock Vault, cliquer sur le bouton Actualiser dans la page Topologie actualise la période de verrouillage sur le secondaire récupéré à partir d' ONTAP.</p> <p>Pour plus d'informations sur SnapLock Vault, consultez Valider les instantanés sur WORM sur une destination de coffre-fort</p> <p>Voir "Afficher les sauvegardes et les clones liés aux ressources PostgreSQL dans la page Topologie" .</p>

Pour ce domaine...	Fais ceci...
Erreur lors du nombre de tentatives	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.



Vous devez configurer la stratégie de rétention SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale de snapshots sur le stockage secondaire.

- Consultez le résumé, puis cliquez sur **Terminer**.

Créer des groupes de ressources et attacher des politiques


Un groupe de ressources est le conteneur auquel vous devez ajouter les 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 attacher une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez effectuer.

À propos de cette tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots SnapLock Vault dans le cadre de la restauration hériteront du délai d'expiration de SnapLock Vault. L'administrateur de stockage doit nettoyer manuellement les clones après l'expiration de SnapLock .

Étapes

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

Pour ce domaine...	Fais ceci...
Nom	<p>Saisissez un nom pour le groupe de ressources.</p> <div>  <p>Le nom du groupe de ressources ne doit pas dépasser 250 caractères.</p> </div>
Mots-clés	<p>Saisissez une ou plusieurs étiquettes qui vous aideront à rechercher ultérieurement le groupe de ressources.</p> <p>Par exemple, si vous ajoutez RH comme balise à plusieurs groupes de ressources, vous pouvez ultérieurement trouver tous les groupes de ressources associés à la balise RH.</p>

Pour ce domaine...	Fais ceci...
Utiliser un format de nom personnalisé pour la copie instantanée	<p>Cochez cette case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.</p> <p>Par exemple, customtext_resource group_policy_hostname ou resource group_hostname. Par défaut, un horodatage est ajouté au nom de l'instantané.</p>

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

Cela permet de filtrer les informations sur l'écran.

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

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

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

Pour ce domaine...	Fais ceci...
Prévoir le temps d'attendre que l'opération de capture instantanée du groupe de cohérence soit terminée	<p>Sélectionnez Urgent, Moyen ou Relaxé pour spécifier le temps d'attente avant la fin de l'opération de capture instantanée.</p> <p>Urgent = 5 secondes, Moyen = 7 secondes et Détendu = 20 secondes.</p>
Désactiver la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL .

1

2

3

4

5

6

Name

Resources

Application Settings

Policies

Notification

Summary

Backups

☒ Enable consistency group backup

Afford time to wait for Consistency Group Snapshot operation to complete

Urgent

Medium

Relaxed

☐ Disable WAFL Sync

Scripts

Custom Configurations

Snapshot Copy Tool

- Cliquez sur la flèche **Scripts** et entrez les commandes pré et post pour les opérations de mise en veille, de capture instantanée et de reprise. Vous pouvez également saisir les commandes préalables à exécuter avant de quitter en cas de panne.
- Cliquez sur la flèche **Configurations personnalisées** et saisissez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Paramètre	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archives de supprimer les journaux d'archives.
CONSERVATION_DU_JOURNAL_D'ARCHIVES	nombre_de_jours	<p>Spécifie le nombre de jours pendant lesquels les journaux d'archive sont conservés.</p> <p>Ce paramètre doit être égal ou supérieur à NTAP_SNAPSHOT_RETENTIONS.</p>
ARCHIVE_LOG_DIR	change_info_directory/logs	Spécifie le chemin d'accès au répertoire qui contient les journaux d'archive.

Paramètre	Paramètre	Description
ARCHIVE_LOG_EXT	extension_de_fichier	Spécifie la longueur de l'extension du fichier journal d'archive. Par exemple, si le journal d'archive est log_backup_0_0_0_0.161518551942 9 et si la valeur file_extension est 5, alors l'extension du journal conservera 5 chiffres, soit 16151.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(O/N)	Permet la gestion des journaux d'archives dans les sous-répertoires. Vous devez utiliser ce paramètre si les journaux d'archive sont situés dans des sous-répertoires.



Les paires clé-valeur personnalisées sont prises en charge pour les systèmes de plug-in PostgreSQL Linux et ne sont pas prises en charge pour les clusters PostgreSQL enregistrés en tant que plug-in Windows centralisé.

- c. Cliquez sur la flèche **Snapshot Copy Tool** pour sélectionner l'outil permettant de créer des instantanés :

Si tu veux...	Alors...
SnapCenter pour utiliser le plug-in pour Windows et mettre le système de fichiers dans un état cohérent avant de créer un instantané. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez * SnapCenter avec cohérence du système de fichiers*.
SnapCenter pour créer un instantané du niveau de stockage	Sélectionnez * SnapCenter sans cohérence du système de fichiers*.
Pour saisir la commande à exécuter sur l'hôte pour créer des copies instantanées.	Sélectionnez Autre , puis entrez la commande à exécuter sur l'hôte pour créer un instantané.


7. Dans la page Politiques, effectuez les étapes suivantes :

- a. Sélectionnez une ou plusieurs politiques dans la liste déroulante.



Vous pouvez également créer une politique en cliquant sur *  *.

Les politiques sont répertoriées dans la section Configurer les planifications pour les politiques sélectionnées.

- b. Dans la colonne Configurer les planifications, cliquez sur *  * pour la politique que vous souhaitez configurer.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy_name*, configurez la planification, puis cliquez sur **OK**.

Où, *policy_name* est le nom de la politique que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne **Planifications appliquées**.

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

8. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

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. Consultez le résumé, puis cliquez sur **Terminer**.

Créer des groupes de ressources et activer la protection secondaire pour les ressources PostgreSQL sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas à la fois des ressources ONTAP 9.x et des ressources ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et des ressources ASA r2.

À propos de cette tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonctionnalité **SecondaryProtection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources est mis en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors du mode maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clonée.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources** et 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 actions suivantes :
 - a. Saisissez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ Balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez RH comme balise à plusieurs groupes de ressources, vous pouvez ultérieurement trouver tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, `customtext_resource group_policy_hostname` ou `resource group_hostname`. Par défaut, un horodatage est ajouté au nom de l'instantané.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Vous devez utiliser exactement la même destination que celle définie dans l'application, y compris le préfixe, si nécessaire.

- 4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **Hôte**.




Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource est découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaîtront dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

- 5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les vers la section Ressources sélectionnées.
- 6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
- 7. Dans la page Politiques, effectuez les étapes suivantes :
 - a. Sélectionnez une ou plusieurs politiques dans la liste déroulante.



Vous pouvez également créer une politique en cliquant sur .

Dans la section Configurer les planifications pour les stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez  dans la colonne Configurer les planifications pour la politique pour laquelle vous souhaitez configurer une planification.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy_name*, configurez la planification, puis cliquez sur **OK**.

Où, *policy_name* est le nom de la politique que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne Planifications appliquées.

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

8. Si la protection secondaire est activée pour la politique que vous avez sélectionnée, la page Protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

a. Sélectionnez le type de politique de réplication.



La politique de réplication synchrone n'est pas prise en charge.

b. Spécifiez le suffixe du groupe de cohérence que vous souhaitez utiliser.

c. Dans les listes déroulantes Cluster de destination et SVM de destination, sélectionnez le cluster apparié et le SVM que vous souhaitez utiliser.




Le peering de cluster et de SVM n'est pas pris en charge par SnapCenter. Vous devez utiliser System Manager ou les CLI ONTAP pour effectuer l'appairage de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, ces ressources seront affichées dans la section Ressources protégées secondaires.

1. Sur la page de vérification, effectuez les étapes suivantes :

a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer la vérification sur le stockage secondaire.

b. Cliquez  dans la colonne Configurer les planifications pour configurer la planification de vérification pour tous les types de planification de la politique.

c. Dans la boîte de dialogue Ajouter des planifications de vérification policy_name, effectuez les actions suivantes :

Si vous voulez...	Fais ceci...
Exécuter la vérification après la sauvegarde	Sélectionnez Exécuter la vérification après la sauvegarde .
Planifier une vérification	Sélectionnez Exécuter la vérification planifiée , puis sélectionnez le type de planification dans la liste déroulante.

d. Sélectionnez **Vérifier sur un emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.

e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne Planifications appliquées.

2. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **Joindre le rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell Set-SmSmtServer.

3. Consultez le résumé, puis cliquez sur **Terminer**.

Créer une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour PostgreSQL

Vous devez créer une connexion à une machine virtuelle de stockage (SVM) et des informations d'identification avant d'utiliser les applets de commande PowerShell pour sauvegarder, restaurer ou cloner des clusters PostgreSQL.

Avant de commencer

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

Les installations de plug-ins hôtes ne doivent pas être en cours lors de l'ajout d'une connexion au système de stockage, car le cache hôte peut ne pas être mis à jour et l'état des clusters peut s'afficher dans l'interface graphique SnapCenter comme « Non disponible pour la sauvegarde » ou « Pas 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 différents clusters. Chaque système de stockage pris en charge par SnapCenter doit avoir un nom unique et une adresse IP LIF de données unique.

Étapes

1. Lancez une session de connexion PowerShell Core à l'aide de l'applet de commande Open-SmConnection.

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

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 de nouvelles informations d'identification à l'aide de l'applet de commande Add-SmCredential.

Cet exemple montre comment créer une nouvelle information d'identification nommée FinanceAdmin avec les informations d'identification Windows :

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

4. Ajoutez l'hôte de communication PostgreSQL à SnapCenter Server.

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

5. Installez le package et le plug-in SnapCenter pour PostgreSQL sur l'hôte.

Pour Linux :

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

Pour Windows :

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

6. Définissez le chemin vers SQLLIB.

Pour Windows, le plug-in PostgreSQL utilisera le chemin par défaut pour le dossier SQLLIB : « C:\Program Files\IBM\SQLLIB\BIN »

Si vous souhaitez remplacer le chemin par défaut, utilisez la commande suivante.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode  
PostgreSQL -configSettings @{ "PostgreSQL_SQLLIB_CMD" =  
"<custom_path>\IBM\SQLLIB\BIN" }
```

Les informations concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Sauvegarder PostgreSQL

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

Avant de commencer

- Vous devez avoir créé une politique de sauvegarde.
- Si vous souhaitez sauvegarder une ressource qui a une relation SnapMirror avec un stockage secondaire,

le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « snapmirror all ». Cependant, si vous utilisez le rôle « vsadmin », le privilège « snapmirror all » n'est pas requis.

- Pour l'opération de sauvegarde basée sur une copie instantanée, assurez-vous que tous les clusters de locataires sont valides et actifs.
- Pour les commandes pré et post pour les opérations de mise en veille, de capture instantanée et de réactivation, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
 - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Emplacement par défaut sur l'hôte Linux : */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*





Si les commandes n'existent pas dans la liste des commandes, l'opération échouera.

Interface utilisateur de SnapCenter

Étapes

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

Sélectionner  *, puis sélectionnez le nom d'hôte et le type de ressource pour filtrer les ressources. Vous pouvez ensuite sélectionner  pour fermer le volet de filtre.

3. Sélectionnez la ressource que vous souhaitez sauvegarder.
4. Dans la page Ressource, sélectionnez **Utiliser un format de nom personnalisé pour la copie d'instantané**, puis saisissez un format de nom personnalisé que vous souhaitez utiliser pour le nom d'instantané.

Par exemple, *customtext_policy_hostname* ou *resource_hostname*. Par défaut, un horodatage est ajouté au nom de l'instantané.

5. Dans la page Paramètres de l'application, procédez comme suit :

- Sélectionnez la flèche **Sauvegardes** pour définir des options de sauvegarde supplémentaires :

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

Pour ce domaine...	Fais ceci...
Prévoir du temps pour attendre que l'opération « Instantané du groupe de cohérence » soit terminée	Sélectionnez Urgent , Moyen ou Relaxé pour spécifier le temps d'attente avant la fin de l'opération Snapshot. Urgent = 5 secondes, Moyen = 7 secondes et Détendu = 20 secondes.
Désactiver la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL .

- Sélectionnez la flèche **Scripts** pour exécuter les commandes pré et post pour les opérations de mise en veille, de capture instantanée et de reprise.

Vous pouvez également exécuter des commandes préalables avant de quitter l'opération de sauvegarde. Les prescripts et les post-scripts sont exécutés dans le serveur SnapCenter .

- Sélectionnez la flèche **Configurations personnalisées**, puis saisissez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
- Sélectionnez la flèche **Snapshot Copy Tool** pour sélectionner l'outil permettant de créer des instantanés :

Si tu veux...	Alors...
SnapCenter pour créer un instantané au niveau du stockage	Sélectionnez * SnapCenter sans cohérence du système de fichiers*.

Si tu veux...	Alors...
SnapCenter pour utiliser le plug-in pour Windows pour mettre le système de fichiers dans un état cohérent, puis créer un instantané	Sélectionnez * SnapCenter avec cohérence du système de fichiers*.
Pour entrer la commande pour créer un instantané	Sélectionnez Autre , puis entrez la commande pour créer un instantané.


6. Dans la page Politiques, effectuez les étapes suivantes :

- a. Sélectionnez une ou plusieurs politiques dans la liste déroulante.



Vous pouvez également créer une politique en cliquant sur *  *.

Dans la section Configurer les planifications pour les stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Sélectionner *  * dans la colonne Configurer les planifications pour la politique pour laquelle vous souhaitez configurer une planification.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy_name*, configurez la planification, puis sélectionnez **OK**.

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

Les planifications configurées sont répertoriées dans la colonne Planifications appliquées.

7. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

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. Consultez le résumé, puis sélectionnez **Terminer**.

La page de topologie des ressources s'affiche.

9. Sélectionnez **Sauvegarder maintenant**.

10. Dans la page Sauvegarde, effectuez les étapes suivantes :

- a. Si vous avez appliqué plusieurs politiques à la ressource, dans la liste déroulante **Politique**, sélectionnez la politique que vous souhaitez utiliser pour la sauvegarde.

Si la politique sélectionnée pour la sauvegarde à la demande est associée à une planification de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de planification.

- b. Sélectionnez **Sauvegarde**.

11. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

- Dans les configurations MetroCluster , SnapCenter peut ne pas être en mesure de détecter 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 VMDK et que la taille du tas Java pour le SnapCenter Plug-in for VMware vSphere n'est pas suffisamment grande, la sauvegarde peut échouer.

Pour augmenter la taille du tas Java, recherchez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, la commande `do_start method` démarre le service de plug-in SnapCenter VMware. Mettez à jour cette commande comme suit : `Java -jar -Xmx8192M -Xms4096M`

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`.

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

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

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

Cet exemple montre comment ajouter une instance PostgreSQL :

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.
4. Protégez la ressource ou ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.
5. Lancez une nouvelle tâche de sauvegarde à l'aide de l'applet de commande New-SmBackup.

Cet exemple montre comment sauvegarder un groupe de ressources :

```
C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
-Policy postgresql_policy1
```

Cet exemple sauvegarde une ressource protégée :

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
-Policy postgresql_policy2
```

6. Surveillez l'état du travail (en cours d'exécution, terminé ou échoué) 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 tels que l'ID de sauvegarde, le nom de la 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 concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

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.

Avant de commencer



- Vous devez avoir créé un groupe de ressources avec une politique associée.
- Si vous souhaitez sauvegarder une ressource qui a une relation SnapMirror avec un stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « snapmirror all ». Cependant, si vous utilisez le rôle « vsadmin », le privilège « snapmirror 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 un groupe de ressources dispose d'une politique associée et d'une planification configurée, les sauvegardes se produisent automatiquement selon la planification.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **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 rechercher le groupe de ressources soit en saisissant le nom du groupe de ressources dans la zone de recherche, soit en sélectionnant , puis en sélectionnant la balise. Vous pouvez ensuite sélectionner  pour fermer le volet de filtre.

3. Dans la page Groupes de ressources, sélectionnez le groupe de ressources que vous souhaitez sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page Sauvegarde, effectuez les étapes 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 politique sélectionnée pour la sauvegarde à la demande est associée à une planification de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de planification.







- b. Sélectionnez **Sauvegarde**.
5. Surveillez la progression de l'opération en sélectionnant **Surveillance > Tâches**.

Surveiller les opérations de sauvegarde PostgreSQL

Vous pouvez surveiller la progression des différentes opérations de sauvegarde en utilisant la page SnapCenterJobs. Vous souhaitez peut-être 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 Tâches et indiquent l'état correspondant des opérations :


-  En cours
-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
-  En file d'attente
-  Annulé

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.
2. Dans la page Moniteur, cliquez sur **Tâches**.
3. Dans la page Emplois, effectuez les étapes suivantes :

- a. Cliquez  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
 - b. Précisez les dates de début et de fin.
 - c. Dans la liste déroulante **Type**, sélectionnez **Sauvegarde**.
 - d. Dans la liste déroulante **Statut**, sélectionnez l'état de la sauvegarde.
 - e. Cliquez sur **Appliquer** pour afficher les opérations terminées 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 de la tâche, vous pouvez voir que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées par des signes 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.

Surveiller les opérations de protection des données sur les clusters PostgreSQL dans le volet Activité

Le volet Activité affiche les cinq opérations les plus récentes effectuées. Le volet Activité affiche également le moment où l'opération a été lancée et l'état de l'opération.

Le volet Activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

Étapes

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


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

Ce dont vous aurez besoin

- Vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail pour annuler les opérations.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Surveillance** ou du volet **Activité**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours.
- 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 le travail** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **Tous les membres de ce rôle peuvent voir et utiliser les objets des autres membres** dans la page Utilisateurs\Groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente des autres membres lors de l'utilisation de ce rôle.

Mesures

1. Effectuez l'une des actions suivantes :

Du...	Action
Page de surveillance	<ol style="list-style-type: none">Dans le volet de navigation de gauche, cliquez sur Surveillance > Tâches.Sélectionnez l'opération, puis cliquez sur Annuler le travail.
Volet d'activité	<ol style="list-style-type: none">Après avoir lancé l'opération de sauvegarde, cliquez sur ** dans le volet Activité pour afficher les cinq opérations les plus récentes.Sélectionnez l'opération.Dans la page Détails du travail, cliquez sur Annuler le travail.




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

Afficher les sauvegardes et les clones PostgreSQL dans la page Topologie

Lorsque vous vous préparez à sauvegarder ou à cloner une ressource, il peut être utile d'afficher une représentation graphique de toutes les sauvegardes et de tous les clones sur le stockage principal 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 miroir ou copies Vault).

-  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 stockage secondaire à l'aide de la technologie SnapMirror .
-  affiche le nombre de sauvegardes et de clones répliqués sur le 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 politique visant à conserver uniquement 4 sauvegardes, le nombre de sauvegardes affichées est 6.



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

Dans la page Topologie, vous pouvez voir toutes les sauvegardes et tous les 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 **Afficher**.
3. Sélectionnez la ressource soit à partir de la vue des détails de la ressource, soit à partir de la vue des détails du groupe de ressources.

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

4. Consultez la **carte récapitulative** pour voir un résumé du nombre de sauvegardes et de clones disponibles sur le stockage principal et secondaire.

La section **Carte récapitulative** affiche le nombre total de sauvegardes basées sur des copies Snapshot et des clones.

Cliquer sur le bouton **Actualiser** lance une requête sur le stockage pour afficher un décompte précis.

Si une sauvegarde activée par SnapLock est effectuée, cliquer sur le bouton **Actualiser** actualise l'heure d'expiration principale et secondaire de SnapLock récupérée à partir d' ONTAP. Un calendrier hebdomadaire actualise également l'heure d'expiration du SnapLock principal et secondaire récupérée à partir d' ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration de SnapLock pour la sauvegarde correspond au délai d'expiration de SnapLock le plus long défini pour un snapshot dans un volume. Le délai d'expiration SnapLock le plus long est récupéré à partir d' ONTAP.

Après une sauvegarde à la demande, cliquez sur le bouton **Actualiser** pour actualiser les détails de la sauvegarde ou du clonage.



5. Dans la vue Gérer les copies, cliquez sur **Sauvegardes** ou **Clones** à partir du stockage principal ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Les détails des sauvegardes et des clones sont affichés 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 pas renommer ou supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

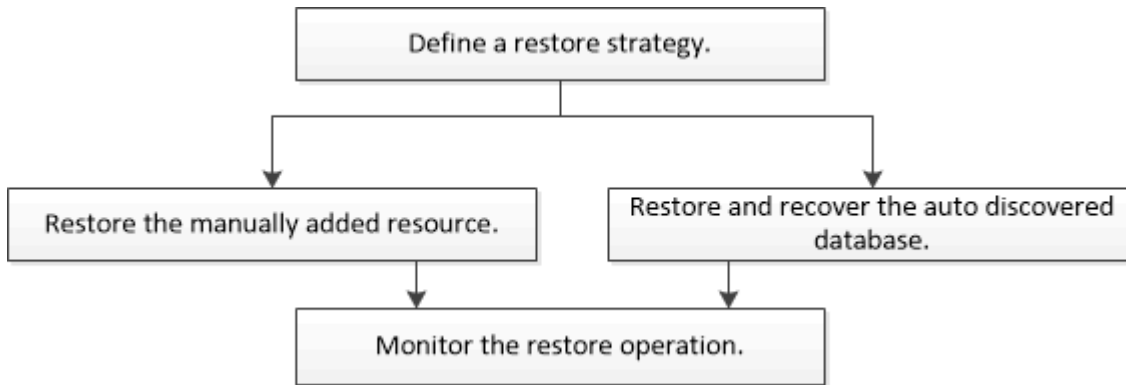
7. Si vous souhaitez supprimer un clone, sélectionnez le clone dans le tableau, puis cliquez sur .
8. Si vous souhaitez diviser un clone, sélectionnez le clone dans le tableau, puis cliquez sur .

Restaurer PostgreSQL

Restaurer le flux de travail

Le flux de travail de restauration et de récupération comprend la planification, l'exécution des opérations de restauration et la surveillance des opérations.

Le flux de travail suivant montre la séquence dans laquelle vous devez effectuer l'opération de restauration :



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

["Guide de référence de l'applet de commande du logiciel SnapCenter"](#) .

Restaurer et récupérer une sauvegarde de ressources ajoutée manuellement

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

Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde actuellement en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, de post-restauration, de montage et de démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
 - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Emplacement par défaut sur l'hôte Linux : `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste des commandes, l'opération échouera.

À propos de cette tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des instantanés SnapLock Vault dans le cadre de la restauration hériteront du délai d'expiration de SnapLock Vault. L'administrateur de stockage doit nettoyer manuellement les clones après l'expiration de SnapLock .

Interface utilisateur de SnapCenter

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 **Afficher** en fonction du type de ressource.

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




Bien qu'une sauvegarde puisse concerner 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 protégé » s'affiche dans la colonne État général. Cela peut signifier soit que la ressource n'est pas protégée, soit 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 de topologie des ressources s'affiche.

4. Dans la vue Gérer les copies, sélectionnez **Sauvegardes** à partir des systèmes de stockage principal ou secondaire (en miroir ou en coffre).
5. Dans le tableau Sauvegarde(s) principale(s), sélectionnez la sauvegarde à partir de laquelle vous souhaitez effectuer la restauration, puis cliquez sur *  *.



Primary Backup(s)	
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restaurer l'étendue, sélectionnez **Ressource complète**.

- a. Si vous sélectionnez **Ressource complète**, tous les volumes de données configurés du cluster PostgreSQL sont restaurés.

Si la ressource contient des volumes ou des qtrees, les instantanés pris après l'instantané sélectionné pour la restauration sur ces volumes ou qtrees sont supprimés et ne peuvent pas être récupérés. De plus, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

Vous pouvez sélectionner plusieurs LUN.



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

7. Dans la page Pré-opérations, saisissez 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 découvertes automatiquement.

8. Dans la page Post-opérations, saisissez les commandes mount et post-restauration à exécuter après avoir effectué une tâche de restauration.

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

9. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

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 sur la page **Paramètres > Paramètres globaux**.

10. Consultez le résumé, puis cliquez sur **Terminer**.

11. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

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.

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

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

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
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 affiche des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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 à partir de la sauvegarde à l'aide de l'applet de commande `Restore-SmBackup`.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Restaurer et récupérer une sauvegarde de cluster découverte automatiquement

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

Avant de commencer

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

chemins suivants :

- Emplacement par défaut sur l'hôte Windows : `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Emplacement par défaut sur l'hôte Linux : `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste des commandes, l'opération échouera.

À propos de cette tâche

- Les copies de sauvegarde basées sur des fichiers ne peuvent pas être restaurées à partir de SnapCenter.
- Pour les ressources découvertes automatiquement, la restauration est prise en charge avec SFSR.
- La récupération automatique n'est pas prise en charge.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots SnapLock Vault dans le cadre de la restauration hériteront du délai d'expiration de SnapLock Vault. L'administrateur de stockage doit nettoyer manuellement les clones après l'expiration de SnapLock .

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 **Afficher** en fonction du type de ressource.

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






Bien qu'une sauvegarde puisse concerner 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 protégé » s'affiche dans la colonne État général. Cela peut signifier soit que la ressource n'est pas protégée, soit 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 de topologie des ressources s'affiche.

4. Dans la vue Gérer les copies, sélectionnez **Sauvegardes** à partir des systèmes de stockage principal ou secondaire (en miroir ou en coffre).
5. Dans le tableau Sauvegarde(s) principale(s), sélectionnez la sauvegarde à partir de laquelle vous souhaitez effectuer la restauration, puis cliquez sur *  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

- Dans la page Restaurer l'étendue, sélectionnez **Ressource complète** pour restaurer les volumes de données configurés du cluster PostgreSQL.
- Dans la page Étendue de la récupération, sélectionnez l'une des options suivantes :

Si tu...	Fais ceci...
Vous souhaitez récupérer au plus près 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.
Vous souhaitez récupérer jusqu'au moment spécifié	Sélectionnez Récupérer jusqu'à un moment précis . a. Entrez la date et l'heure. Entrez la date et l'heure. Par exemple, l'hôte Linux PostgreSQL est situé à Sunnyvale, en Californie, et l'utilisateur à Raleigh, en Caroline du Nord, récupère les journaux dans SnapCenter. Si l'utilisateur souhaite effectuer une récupération à 5 heures du matin à Sunnyvale, en Californie, il doit définir le fuseau horaire du navigateur sur le fuseau horaire de l'hôte Linux PostgreSQL, qui est GMT-07:00 et spécifier la date et l'heure à 5h00 du matin.
Je ne veux pas récupérer	Sélectionnez Aucune récupération .



Vous ne pouvez pas récupérer les ressources PostgreSQL ajoutées manuellement.



Le plug-in SnapCenter pour PostgreSQL crée un backup_label et un tablespace_map dans le dossier `/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/` pour faciliter la récupération manuelle.

- Dans la page Pré-opérations, saisissez 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 découvertes automatiquement.

- Dans la page Post-opérations, saisissez les commandes mount et post-restauration à exécuter après avoir effectué une tâche de restauration.

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

- Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

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 sur la page **Paramètres > Paramètres globaux**.

4. Consultez le résumé, puis cliquez sur **Terminer**.
5. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

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

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

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

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

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
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 affiche des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :


```

PS C:\> Get-SmBackupReport -FromDate "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 à partir de la sauvegarde à l'aide de l'applet de commande Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant *Get-Help command_name*. Alternativement, vous pouvez également vous référer à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).


Surveiller les opérations de restauration PostgreSQL






Vous pouvez surveiller la progression des différentes opérations de restauration de SnapCenter à l'aide de la page Tâches. Vous souhaitez peut-être 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 entreprendre.

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

-  En cours

-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
-  En file d'attente
-  Annulé

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.
2. Dans la page **Moniteur**, cliquez sur **Tâches**.
3. Dans la page **Emplois**, effectuez les étapes suivantes :
 - a. Cliquez  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
 - b. Précisez les dates de début et de fin.
 - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
 - d. Dans la liste déroulante **État**, sélectionnez l'état de restauration.
 - e. Cliquez sur **Appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez la tâche de restauration, puis cliquez sur **Détails** pour afficher les détails de la tâche.
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.

Cloner les sauvegardes de ressources PostgreSQL

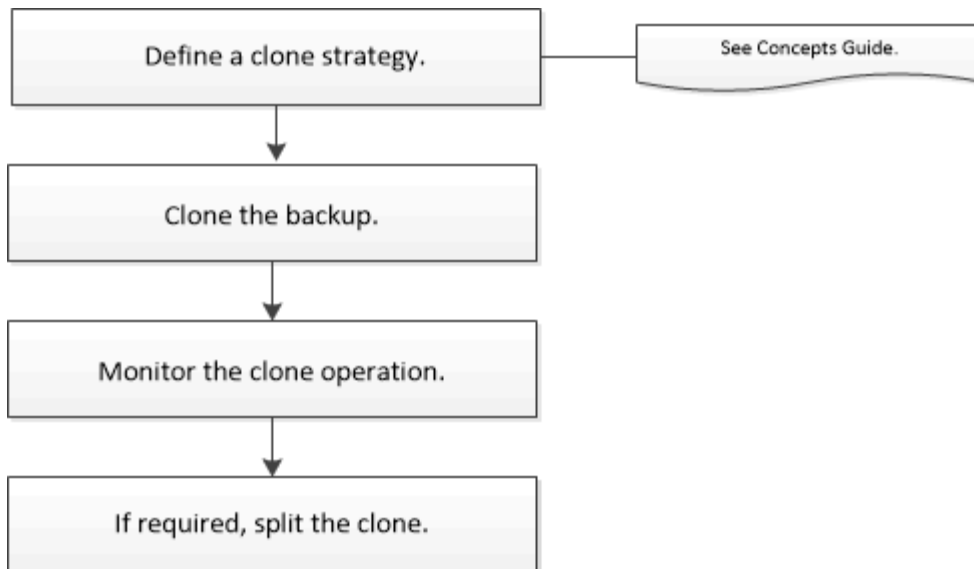
Cloner le flux de travail

Le flux de travail de clonage comprend l'exécution de l'opération de clonage et la surveillance de l'opération.

À propos de cette tâche

- Vous pouvez cloner sur le serveur PostgreSQL source.
- Vous pouvez cloner des sauvegardes de ressources pour les raisons suivantes :
 - Pour tester les fonctionnalités qui doivent être implémentées à l'aide de la structure et du contenu des ressources actuelles pendant les cycles de développement des applications
 - Pour les outils d'extraction et de manipulation de données lors du remplissage des entrepôts de données
 - Pour récupérer des données supprimées ou modifiées par erreur

Le flux de travail suivant montre 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 effectuer des opérations de sauvegarde, de restauration et de clonage. L'aide de l'applet de commande SnapCenter et les informations de référence de l'applet de commande contiennent des informations détaillées sur les applets de commande PowerShell.

Cloner une sauvegarde PostgreSQL

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

Avant de commencer

- Vous auriez dû sauvegarder les ressources ou le groupe de ressources.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent figurer dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Pour les commandes de pré-clonage ou de post-clonage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
 - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Emplacement par défaut sur l'hôte Linux : `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste des commandes, l'opération échouera.

À propos de cette tâche

- Pour plus d'informations sur les opérations de division de volume FlexClone , voir, <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["Diviser un volume FlexClone de son volume parent"] .
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des instantanés SnapLock Vault dans le cadre de la restauration hériteront du délai d'expiration de SnapLock Vault. L'administrateur de stockage doit nettoyer manuellement les clones après l'expiration de SnapLock .

Interface utilisateur de SnapCenter

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 **Afficher** en fonction du type de ressource.

Les ressources sont affichées avec des informations telles que le type, l'hôte, les groupes de ressources et les politiques associés, ainsi que 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 de topologie des ressources ou du groupe de ressources s'affiche.

4. Dans la vue Gérer les copies, sélectionnez **Sauvegardes** à partir des systèmes de stockage principal ou secondaire (en miroir ou en coffre).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page Emplacement, effectuez les actions suivantes :

Pour ce domaine...	Fais ceci...
Cloner le serveur	Choisissez un hôte sur lequel le clone doit être créé.
Port cible	Saisissez le port cible PostgreSQL à cloner à partir des sauvegardes existantes.
Adresse IP d'exportation NFS	Saisissez les adresses IP ou les noms d'hôtes sur lesquels les volumes clonés seront exportés. Ceci s'applique uniquement aux ressources de type de stockage NFS.
Pool de capacité Débit max. (Mio/s)	Saisissez le débit maximal d'un pool de capacité. Ceci s'applique uniquement aux ressources de type de stockage ANF.

7. Dans la page Scripts, effectuez les étapes suivantes :



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

- a. Saisissez les commandes de pré-clonage ou de post-clonage qui doivent être exécutées respectivement avant ou après l'opération de clonage.
 - Commande de pré-clonage : supprimer les clusters existants portant le même nom
 - Commande de post-clonage : vérifier un cluster ou démarrer un cluster.

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

Commande de montage 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 **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

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

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

10. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

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.

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

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

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 a une adresse NFSEXPORtIPs de 10.32.212.14 :

Pour le cluster PostgreSQL :

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```



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

4. Vérifiez que les sauvegardes ont été clonées avec succès en utilisant l'applet de commande Get-SmCloneReport pour afficher les détails du travail de clonage.

Vous pouvez afficher des détails tels 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           :
```

Surveiller les opérations de clonage PostgreSQL


Vous pouvez surveiller la progression des opérations de clonage de SnapCenter à l'aide de la page Tâches. Vous souhaitez peut-être 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 Tâches et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
-  En file d'attente
-  Annulé

Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.
2. Dans la page **Moniteur**, cliquez sur **Tâches**.
3. Dans la page **Emplois**, effectuez les étapes suivantes :
 - a. Cliquez  pour filtrer la liste afin que seules les opérations de clonage soient répertoriées.
 - b. Précisez les dates de début et de fin.
 - c. Dans la liste déroulante **Type**, sélectionnez **Cloner**.
 - d. Dans la liste déroulante **Statut**, sélectionnez le statut du clonage.
 - e. Cliquez sur **Appliquer** pour afficher les opérations terminées avec succès.
4. Sélectionnez la tâche de clonage, puis cliquez sur **Détails** pour afficher les détails de la tâche.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Diviser un clone

Vous pouvez utiliser SnapCenter pour diviser 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 division 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 division de clone sur clone1. Cependant, vous pouvez effectuer l'opération de division de clone sur clone2.

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

- Lorsque vous divisez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de division de volume FlexClone, voir, "[Diviser un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat sur le 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. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Afficher :

Option	Description
Pour les applications de base de données	Sélectionnez Base de données dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez Chemin dans la liste Affichage.

3. Sélectionnez la ressource appropriée dans la liste.

La page de topologie des ressources s'affiche.

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

L'opération de division du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter l'applet de commande Stop-SmJob pour arrêter l'opération de division du clonage, puis réessayer l'opération de division du clonage.

Si vous souhaitez 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 pendant lequel SMCore doit interroger l'état de l'opération de division du clone. La valeur est en millisecondes et la valeur par défaut est de 5 minutes.

Par exemple:

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

L'opération de démarrage du fractionnement du clone échoue si une sauvegarde, une restauration ou un autre fractionnement du clone est en cours. Vous ne devez redémarrer l'opération de division du clone qu'une fois les opérations en cours terminées.

Informations connexes

["Le clonage ou la vérification de SnapCenter échoue avec l'agrégat qui n'existe pas"](#)

Supprimer ou diviser les clones de cluster PostgreSQL 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 diviser les clones à partir 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 cachés, exécutez la commande suivante :

```
Get-SmClone -ListStorageFootprint
```

Étapes

1. Supprimez les sauvegardes des ressources clonées à l'aide de l'applet de commande `remove-smbbackup`.
2. Supprimez le groupe de ressources des ressources clonées à l'aide de l'applet de commande `remove-smresourcegroup`.
3. Supprimez la protection de la ressource clonée à l'aide de l'applet de commande `remove-smprotectresource`.
4. Sélectionnez la ressource parent sur la page Ressources.

La page de topologie des ressources s'affiche.

5. Dans la vue Gérer les copies, sélectionnez les clones à partir des systèmes de stockage principaux ou secondaires (en miroir ou répliqués).
6. Sélectionnez les clones, puis cliquez sur  pour supprimer les clones ou cliquez sur  pour diviser les clones.
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 DÉLICTELLE (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.