



# Protéger PostgreSQL

## SnapCenter software

NetApp  
January 09, 2026

# Sommaire

Protéger PostgreSQL .....	1
Plug-in SnapCenter pour PostgreSQL .....	1
Présentation du plug-in SnapCenter pour PostgreSQL .....	1
Ce que vous pouvez faire à l'aide du plug-in SnapCenter pour PostgreSQL .....	1
Plug-in SnapCenter pour les fonctionnalités PostgreSQL .....	1
Types de stockage pris en charge par le plug-in SnapCenter pour PostgreSQL .....	2
Privilèges ONTAP minimum requis pour le plug-in PostgreSQL .....	3
Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour PostgreSQL .....	6
Stratégie de sauvegarde pour PostgreSQL .....	6
Stratégie de restauration et de récupération pour PostgreSQL .....	9
Préparez l'installation du plug-in SnapCenter pour PostgreSQL .....	10
Workflow d'installation du plug-in SnapCenter pour PostgreSQL .....	10
Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour PostgreSQL .....	11
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows .....	14
Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux .....	15
Configurez les informations d'identification du plug-in SnapCenter pour PostgreSQL .....	16
Configurez GMSA sur Windows Server 2016 ou version ultérieure .....	18
Installez le plug-in SnapCenter pour PostgreSQL .....	19
Configurer le certificat CA .....	25
Préparation à la protection des données .....	33
Conditions préalables à l'utilisation du plug-in SnapCenter pour PostgreSQL .....	33
Utilisation des ressources, des groupes de ressources et des règles pour protéger PostgreSQL .....	34
Sauvegarder les ressources PostgreSQL .....	34
Sauvegarder les ressources PostgreSQL .....	34
Découverte automatique des clusters .....	37
Ajoutez des ressources manuellement au plug-in hôte .....	37
Créez des règles de sauvegarde pour PostgreSQL .....	39
Créer des groupes de ressources et attacher des stratégies .....	43
Créer des groupes de ressources et activez la protection secondaire des ressources PostgreSQL sur les systèmes ASA r2 .....	47
Créez une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour PostgreSQL .....	49
Sauvegardez PostgreSQL .....	51
Sauvegarder les groupes de ressources .....	57
Surveillez les opérations de sauvegarde PostgreSQL .....	58
Annulez les opérations de sauvegarde pour PostgreSQL .....	59
Affichez les sauvegardes et clones PostgreSQL dans la page topologie .....	60
Restaurer PostgreSQL .....	61
Restaurer le flux de travail .....	62
Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement .....	62
Restaurez et récupérez une sauvegarde de cluster découverte automatiquement .....	66
Restaurer des ressources à l'aide des applets de commande PowerShell .....	69
Surveillez les opérations de restauration PostgreSQL .....	71

Cloner les sauvegardes de ressources PostgreSQL . . . . .	72
Workflow de clonage . . . . .	72
Cloner une sauvegarde PostgreSQL . . . . .	73
Surveillez les opérations de clonage PostgreSQL . . . . .	76
Séparer un clone . . . . .	77
Supprimez ou répartissez 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 le cluster PostgreSQL est un composant côté hôte du logiciel NetApp SnapCenter qui permet la gestion de la protection des données compatible avec 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 un seul cluster et à plusieurs clusters. 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.

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

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

L'organisation du stockage virtuel VMDK, vVol et RDM est prise en charge.

### Ce que vous pouvez faire à l'aide du plug-in SnapCenter pour PostgreSQL

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

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

### Plug-in SnapCenter pour les fonctionnalités PostgreSQL

SnapCenter s'intègre avec l'application de plug-in et avec les technologies NetApp sur le système de stockage. Pour utiliser 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 dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- **Administration centrale automatisée**

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

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

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

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

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

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

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

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

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

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

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

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"> <li>• LUN connectés via FC</li> <li>• LUN connectées à l'iSCSI</li> <li>• Volumes connectés par NFS</li> </ul>
VMware ESXi	<ul style="list-style-type: none"> <li>• L'exécution des LUN RDM connectés par un HBA FC ou iSCSI ESXi peut prendre du temps car SnapCenter analyse tous les adaptateurs de bus hôte présents dans l'hôte.</li> </ul> <p style="margin-top: 10px;">Vous pouvez modifier le fichier <b>LinuxConfig.pm</b> situé à  <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> pour définir la valeur du paramètre <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> à 1 pour analyser uniquement les HBA répertoriés dans les NOMS de PILOTE HBA.</p> <ul style="list-style-type: none"> <li>• LUN iSCSI connectés directement au système invité par l'initiateur iSCSI</li> <li>• VMDK sur des datastores NFS</li> <li>• VMDK sur VMFS</li> <li>• Volumes NFS connectés directement au système invité</li> <li>• Datastores vVol sur NFS et SAN</li> </ul> <p style="margin-top: 10px;">Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.</p>

## Privilèges ONTAP minimum requis pour le plug-in PostgreSQL

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

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - la création de lun
  - la création de lun
  - la création de lun
  - suppression de la lun

- lun igrup add
- créez un groupe initiateur lun
- suppression du groupe initiateur lun
- renommer la lun igrup
- renommer la lun igrup
- affichage de la lun igrup
- lun mapping des nœuds supplémentaires
- création d'un mappage de lun
- suppression du mappage de lun
- mappage de lun supprimer-rapports-nœuds
- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- suppression de la réservation persistante de lun
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes

- volume fichier show-disk-usage
  - volume hors ligne
  - volume en ligne
  - modification de volume
  - création de qtree volume
  - suppression qtree du volume
  - modification de qtree volume
  - volume qtree show
  - restrictions de volume
  - volume affiché
  - création de copies snapshot de volume
  - suppression du snapshot de volume
  - modification de snapshot de volume
  - volume snapshot modify-snaplock-expiration-time
  - renommage snapshot de volume
  - restauration snapshot du volume
  - fichier de restauration de snapshot de volume
  - snapshot de volume apparaît
  - démontage de volume
  - cifs vserver
  - création d'un partage cifs vserver
  - suppression du partage cifs vserver
  - vserver cifs shadowcopy show
  - vserver cifs share show
  - cifs montrer un vserver
  - vserver export-policy
  - vserver export-policy créé
  - vserver export-policy delete
  - vserver export-policy create
  - vserver export-policy règle show
  - vserver export-policy show
  - iscsi vserver
  - vserver iscsi connection show
  - vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
    - interface réseau
    - interface réseau affiche

- un vserver

## Préparez les systèmes de stockage pour SnapMirror et la réPLICATION SnapVault pour PostgreSQL

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

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



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

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



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

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

## 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 vos ressources. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

#### Description de la tâche

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

#### Étapes

1. Déterminez à quel moment il est nécessaire de sauvegarder vos ressources.

2. Déterminer le nombre de tâches de sauvegarde dont vous avez besoin
3. Choisissez le nom de vos sauvegardes.
4. Décidez si vous souhaitez créer une règle basée sur les copies Snapshot pour sauvegarder des copies Snapshot cohérentes au niveau des applications du cluster.
5. Choisissez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réPLICATION ou la technologie NetApp SnapVault pour la conservation à long terme.
6. Déterminer 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 prescripteur 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 avoir installé le 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.

## Types de sauvegardes pris en charge

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge les types de sauvegarde basés sur la copie Snapshot pour les clusters PostgreSQL.

### Sauvegarde basée sur des copies Snapshot

Les sauvegardes basées sur des copies Snapshot utilisent la technologie NetApp Snapshot 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 snapshots de groupes de cohérence

Vous pouvez utiliser le plug-in pour créer des snapshots de groupes de ressources. Un groupe de cohérence est un conteneur qui peut héberger plusieurs volumes, de sorte que vous puissiez les gérer comme une entité unique. Un groupe de cohérence est une copie instantanée de plusieurs volumes, fournissant ainsi des copies cohérentes d'un groupe de volumes.

Vous pouvez également spécifier le temps d'attente nécessaire au contrôleur de stockage pour regrouper les snapshots de manière cohérente. Les options de temps d'attente disponibles sont **urgent**, **Moyen** et **détendu**. Vous pouvez également activer ou désactiver la synchronisation WAFL (Write Anywhere File Layout) lors d'une opération de snapshot de groupe cohérente. WAFL Sync améliore les performances d'un snapshot de groupe de cohérence.

### Comment SnapCenter gère la gestion de la gestion des sauvegardes de données

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

Les snapshots sur le stockage primaire ou secondaire et les entrées correspondantes dans le catalogue

PostgreSQL sont supprimés en fonction des paramètres de conservation.

### **Considérations relatives à la détermination des plannings de sauvegarde pour PostgreSQL**

Le facteur le plus important dans la détermination d'un planning de sauvegarde est le taux de modification de la ressource. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. D'autres facteurs entrent en ligne de compte l'importance des ressources pour votre entreprise, votre contrat de niveau de service et votre objectif de point de récupération (RPO).

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes (fréquence des sauvegardes)

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

- Plannings de sauvegarde (exactement au moment où les sauvegardes doivent être effectuées)

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

### **Nombre de tâches de sauvegarde requises 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 changement de la ressource et votre contrat de niveau de service.

### **Conventions de nommage des sauvegardes pour le plug-in pour les clusters PostgreSQL**

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

`resourcegroupname_hostname_timestamp`

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

`dts1_mach1x88_03-12-2015_23.17.26`

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

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

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

## Stratégie de restauration et de récupération pour PostgreSQL

### Définissez une stratégie de restauration et de récupération pour les ressources PostgreSQL

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



Seule la récupération manuelle du cluster est prise en charge.

### Étapes

1. Déterminez les stratégies de restauration prises en charge pour les ressources PostgreSQL ajoutées manuellement
2. Déterminez les stratégies de restauration prises en charge pour les clusters PostgreSQL découverts automatiquement
3. Choisissez le type d'opérations de restauration à effectuer.

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

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter.



Vous ne pouvez pas récupérer les ressources PostgreSQL ajoutées manuellement.

### Restauration des ressources terminée

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



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

**REMARQUE :** le plug-in pour PostgreSQL crée une étiquette\_sauvegarde et une table\_map dans le dossier `/<OS_temp_folder>/postgresql_sc_Recovery<Restore_JobId>/_` pour faciliter la restauration manuelle .

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

Vous devez définir une stratégie pour pouvoir effectuer les 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. Cette opération 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 SnapRestore de fichiers uniques et les types de restauration de connexion et de copie pour les clusters PostgreSQL découverts automatiquement.

**Single File SnapRestore s'effectue dans des 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 **Complete Resource** est sélectionnée

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

- Si seule l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde est sélectionnée depuis un emplacement secondaire SnapMirror ou SnapVault et l'option **Complete Resource** est sélectionnée

#### **Types d'opérations de restauration pris en charge pour les clusters PostgreSQL**

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

- Restaurez le cluster à l'état le plus récent
- Restaurer le cluster à un point dans le temps spécifique

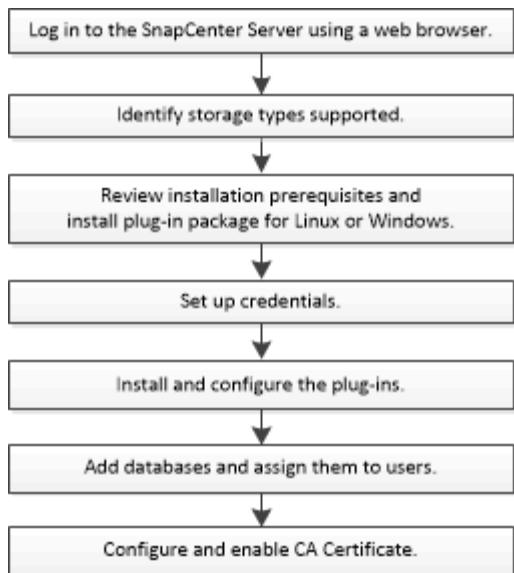
Vous devez indiquer la date et l'heure de la récupération.

SnapCenter propose également l'option aucune restauration pour les clusters PostgreSQL.

## **Préparez l'installation du plug-in SnapCenter pour PostgreSQL**

### **Workflow d'installation du plug-in SnapCenter pour PostgreSQL**

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



## Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour PostgreSQL

Avant d'ajouter un hôte et d'installer les modules d'extension, 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 un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte. Le plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in PostgreSQL sur les hôtes Windows.
- Le serveur SnapCenter doit avoir accès au port 8145 ou personnalisé du plug-in pour l'hôte PostgreSQL.

### Hôtes Windows

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

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

## Hôtes Linux

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

### "Télécharger JAVA pour tous les systèmes d'exploitation"

- Pour les clusters PostgreSQL qui s'exécutent sur un hôte Linux, lors de l'installation du plug-in pour PostgreSQL, le plug-in SnapCenter pour UNIX est installé automatiquement.
- Vous devez 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 des commandes supplémentaires sur l'hôte du plug-in, ouvrez le fichier *allowed\_commands.config* dans un éditeur. Entrez 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 le joindre entre guillemets ("") s'il contient des espaces.

Par exemple :

Commande : mount command : commande umount : « C:\Program Files\NetApp\SnapCreator commands\sdcli.exe » commande : myscript.bat

Si le fichier *allowed\_commands.config* n'est pas présent, les commandes ou l'exécution du script seront bloquées et le flux de travail échouera avec l'erreur suivante :

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

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 flux de travail échouera avec l'erreur suivante :

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



Vous ne devez pas utiliser de caractère générique (\*) pour autoriser toutes les commandes.

## Configurez 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 de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

## Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, 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 de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du 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 priviléges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- /Home/LINUX\_USER/.sc\_netapp/snapcenter\_linux\_host\_plugin.bin
- /Custom\_location/NetApp/snapcenter/spl/installation/plugins/désinstaller
- /Custom\_location/NetApp/snapcenter/spl/bin/spl

## Étapes

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour Linux.
2. Ajoutez les lignes suivantes au fichier */etc/sudoers* à l'aide de l'utilitaire visudo Linux.

```

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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, 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 *checksum\_value* à partir du fichier **sc\_unix\_plugins\_checksum.txt**, situé à l'adresse suivante :

- *\_C:\ProgramData\NetApp\SnapCenter\Package Repository\sc\_unix\_plugins\_checksum.txt* \_ si le serveur SnapCenter est installé sur l'hôte Windows.
- *\_/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc\_unix\_plugins\_checksum.txt* \_ si le serveur SnapCenter est installé sur un hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

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

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

Élément	De formation
Systèmes d'exploitation	<p>Microsoft Windows</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">"Matrice d'interopérabilité NetApp"</a>.</p>

Élément	De formation
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <p></p> <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p>
Packs logiciels requis	<ul style="list-style-type: none"> <li>ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>PowerShell Core 7.4.2</li> </ul> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section "<a href="#">La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet.</a>"</p>

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

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

Élément	De formation
Systèmes d'exploitation	<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux</li> <li>SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO

Élément	De formation
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>2 GO</p> <p></p> <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p>
Packs 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 /var/opt/snapcenter/spl/etc/spl.properties est définie sur la version JAVA correcte et le chemin correct.</p>

## Configurez les informations d'identification du plug-in SnapCenter pour PostgreSQL

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

### Description de la 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 priviléges sudo pour installer et démarrer le processus de plug-in.

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

- Hôtes Windows

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

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

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

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.
Nom d'utilisateur	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"><li>• Administrateur de domaine ou tout membre du groupe d'administrateurs</li></ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"><li>◦ <i>NetBIOS\username</i></li><li>◦ <i>Domain FQDN\username</i></li></ul> <ul style="list-style-type: none"><li>• Administrateur local (groupes de travail uniquement)</li></ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <i>username</i></p> <p>N'utilisez pas de guillemets ("") ou de contre-coches ("") dans les mots de passe. Vous ne devez pas utiliser moins de (&lt;) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins&lt;!10, moins dix&lt;!, contre-recul 12.</p>

Pour ce champ...	Procédez comme ça...
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.
Utilisez les privilèges sudo	<p>Cochez la case <b>utiliser privilèges sudo</b> si vous créez des informations d'identification pour un utilisateur non-root.</p> <p> Applicable uniquement aux utilisateurs Linux.</p>

## 5. Cliquez sur OK.

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

## Configurez GMSA sur Windows Server 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 de compte 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$  
.. Ajouter des objets d'ordinateur au groupe.  
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour  
créer le GMSA.
```

Par exemple :

```

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

```

#### 4. Configurez le GMSA sur vos hôtes :

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

Pour ce faire lancer la commande suivante depuis PowerShell :

```

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

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

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

Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----           -----
True    No            Success        {Active Directory Domain Services,
Active ...}

WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.

```

- Redémarrez votre hôte.
  - Installez 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 d'administration au GMSA configuré sur l'hôte.
  - Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

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

## Installez le plug-in SnapCenter pour PostgreSQL

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

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis

installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter l'hôte et installer des modules d'extension pour un hôte individuel.

## Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des priviléges d'administration.

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

## Description de la 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 **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	<p>Sélectionnez le type d'hôte :</p> <ul style="list-style-type: none"><li>• Répertoires de base</li><li>• Linux</li></ul> <p> Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL et cet hôte peut se trouver sur un système Windows ou Linux.</p>

Pour ce champ...	Procédez comme ça...
Nom d'hôte	<p>Entrez le nom d'hôte de communication. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p>
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez fourni.</p> <p> Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p>

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

Lorsque vous utilisez 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 champ...	Procédez comme ça...
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 est affiché comme port par défaut.</p> <p> Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p>

Pour ce champ...	Procédez comme ça...
Chemin d'installation	<p>Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL et cet hôte peut se trouver sur un système Windows ou Linux.</p> <ul style="list-style-type: none"> <li>Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez également personnaliser le chemin.</li> <li>Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/NetApp/snapcenter. Vous pouvez également personnaliser le chemin.</li> </ul>
Ignorer les vérifications de préinstallation	<p>Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.</p>
Ajoutez tous les hôtes du cluster	<p>Cochez cette case pour ajouter tous les nœuds du cluster.</p>
Utilisez le 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 le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.</p> <p> Indiquez le nom GMSA au format suivant : domainname\accountName\$.</p> <p> GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows.</p>

#### 7. Cliquez sur **soumettre**.

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

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



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

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

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



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

## 9. Surveillez la progression de l'installation.

- Pour le plug-in Windows, les journaux d'installation et de mise à niveau se trouvent à l'adresse suivante : C:\Windows\SnapCenter plugin\Install<JOBID>\\_
- Pour le plug-in Linux, les journaux d'installation se trouvent à l'adresse suivante : /var/opt/snapcenter/logs/SnapCenter\_Linux\_Host\_Plug-in\_Install<JOBID>.log\_ et les journaux de mise à niveau se trouvent à l'adresse : /var/opt/snapcenter/logs/SnapCenter\_Linux\_Host\_Plug-in\_Upgrade<JOBID>.log\_

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

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

### Avant de commencer

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

### Étapes

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

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

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

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

## Installez le plug-in SnapCenter pour 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 en utilisant l'interface utilisateur 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 cluster Plug-in pour PostgreSQL en mode console ou en mode silencieux à l'aide de l'interface de ligne de commande.

## Avant de commencer

- Vous devez installer le cluster Plug-in pour PostgreSQL sur chacun des hôtes Linux où réside le client PostgreSQL.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour le cluster PostgreSQL doit répondre à la configuration logicielle, cluster et système d'exploitation requise.

Le "[Outil de matrice d'interopérabilité \(IMT\)](#)" Contient les informations les plus récentes sur les configurations prises en charge.

- Le cluster SnapCenter Plug-in pour PostgreSQL fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer SnapCenter Plug-ins Package pour Linux, vous devez avoir déjà installé SnapCenter sur un hôte Windows.

## Étapes

1. Copiez le fichier d'installation du pack 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. Installez le plug-in :  
path\_to\_installation\_bin\_file/snapcenter\_linux\_host\_plugin.bin  
-i silent -DPORT=port\_number\_for\_host -DSERVER\_IP=server\_name\_or\_ip\_address  
-DSERVER\_HTTPS\_PORT=port\_number\_for\_server
  - -DPORT spécifie le port de communication SMCore HTTPS.
  - -DSERVER\_IP spécifie l'adresse IP du serveur SnapCenter.
  - -DSERVER\_HTTPS\_PORT spécifie le port HTTPS du serveur SnapCenter.
  - -DUSER\_INSTALL\_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
  - DINSTALL\_LOG\_NAME indique le nom du fichier journal.

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

4. Modifiez le fichier /<installation directory>/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 relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "Guide de référence de l'applet de commande du logiciel SnapCenter".

## Surveillez l'état d'installation du plug-in pour PostgreSQL

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

### Description de la tâche

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

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

### Étapes

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

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

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

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



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

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

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

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

### Importer des certificats CA

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

#### Étapes

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

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



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

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

## Obtenez le certificat CA imprimé

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

### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
  - a. Double-cliquez sur le certificat.
  - b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
  - c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
  - d. Copiez les caractères hexadécimaux de la zone.
  - e. Supprimez les espaces entre les nombres hexadécimaux.

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

2. Effectuer les opérations suivantes à partir de PowerShell :

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

```
Get-ChildItem -Path Cert:\LocalMachine\My
```

- b. Copiez l'empreinte.

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

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

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

### Étapes

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

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

Par exemple :

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

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

### Configurez le certificat CA pour le service SnapCenter PostgreSQL Plug-ins sur l'hôte Linux

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin 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 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.

C'est la valeur correspondant à la clé 'KEYSTORE\_PASS'.

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

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

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

Procédez de même pour la clé KEYSTORE\_PASS dans le fichier `agent.properties`.

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



Le mot de passe du magasin de clés 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 magasin de confiance.

#### 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 magasin de clés :

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

4. Ajouter un certificat racine ou intermédiaire :

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

• Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour le plug-in trust-store.



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

#### 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 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 magasin de clés :

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

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

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

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

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

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.

7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut 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 du certificat de l'autorité de certification est long et contient de l'espace ou des caractères spéciaux ("*", ",,"), remplacez le nom d'alias par un nom simple :
```

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

Mettez cette valeur à jour par rapport à la clé SCC\_CERTIFICATE\_ALIAS.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

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

##### Description de la 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 du fichier agent.properties par rapport à la clé CRL\_PATH.

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

#### Configurez le certificat CA pour le service SnapCenter PostgreSQL Plug-ins sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin 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 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.

C'est la valeur correspondant à la clé *KEYSTORE\_PASS*.

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

```
keytool -storepasswd -keystore keystore.jks
```



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

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

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

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

Procédez de même pour la clé *KEYSTORE\_PASS* dans le fichier *agent.properties*.

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



Le mot de passe du magasin de clés 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 magasin de confiance.

### 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 magasin de clés :

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

4. Ajouter un certificat racine ou intermédiaire :

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

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour le plug-in trust-store.



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

## **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 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 magasin de clés :

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

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

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

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

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

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

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé KEYSTORE\_PASS dans le fichier agent.properties.

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

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

Mettez cette valeur à jour par rapport à la clé SCC\_CERTIFICATE\_ALIAS.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

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

### **Description de la tâche**

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section "[Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter](#)".
- Les plug-ins 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 du fichier *agent.properties* par rapport à la clé CRL\_PATH.

2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

### Activez les certificats CA pour les plug-ins

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

#### Avant de commencer

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

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

#### Étapes

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

#### Une fois que vous avez terminé

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

- Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
- Indique que le certificat CA a été 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 l'état est jaune ou vert, les opérations de protection des données s'achèvent correctement.

## Préparation à la protection des données

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

Avant d'utiliser le plug-in SnapCenter pour PostgreSQL, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches requises.

- Installer et configurer SnapCenter Server.
- Connectez-vous au serveur SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage et en créant des identifiants, le cas échéant.
- Installez Java 11 sur votre hôte Linux ou Windows.

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

- Configurer SnapMirror et SnapVault pour la réPLICATION de sauvegarde.

## **Utilisation des ressources, des groupes de ressources et des règles pour protéger PostgreSQL**

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

- Les ressources sont généralement des 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 en fonction du planning que vous spécifiez pour le groupe de ressources.

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

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

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

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

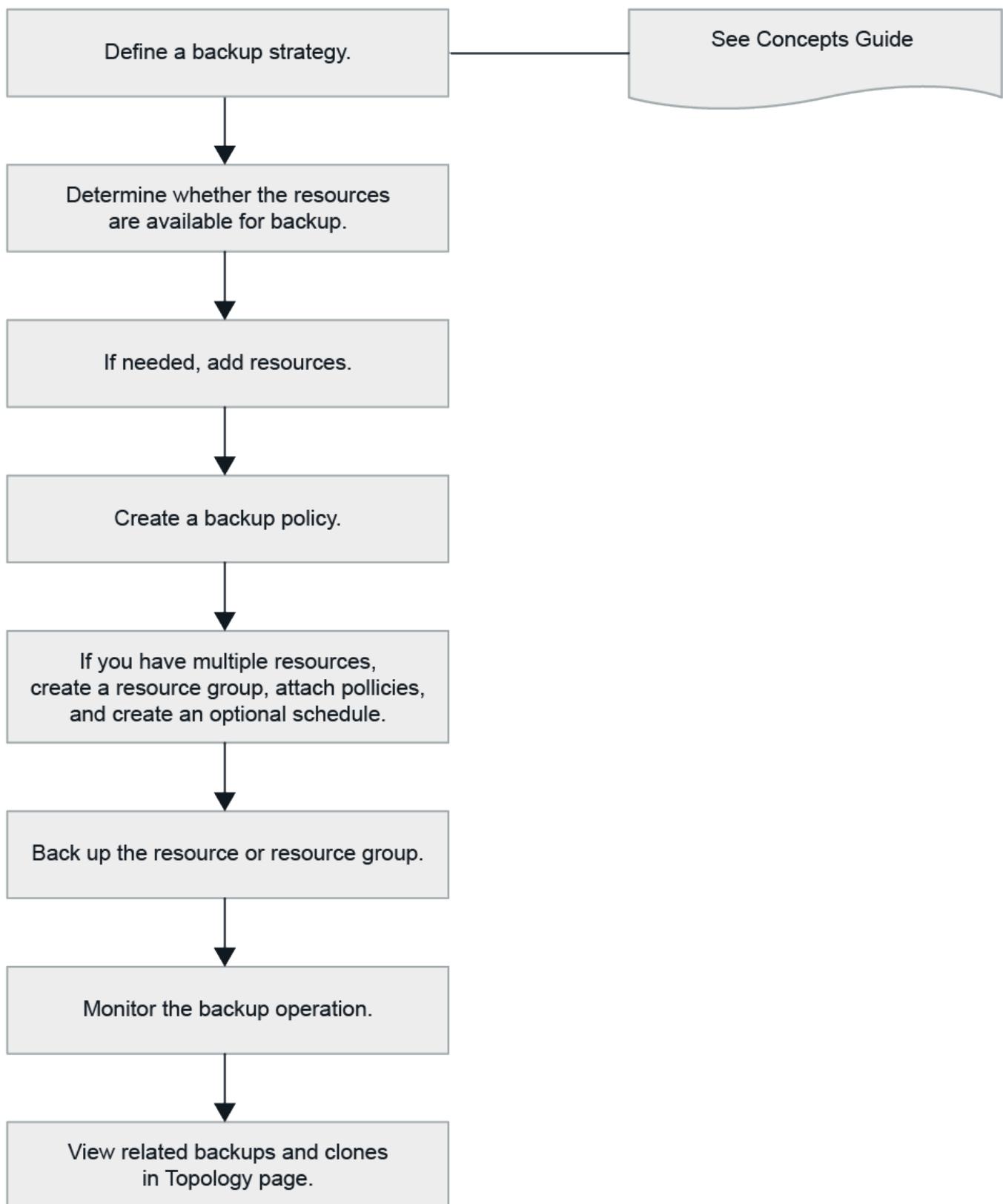
## **Sauvegarder les ressources PostgreSQL**

### **Sauvegarder les ressources PostgreSQL**

Vous pouvez créer une sauvegarde d'une ressource (cluster) ou d'un groupe de

ressources. Le workflow de sauvegarde comprend la planification, l'identification des clusters à sauvegarder, la gestion des stratégies de sauvegarde, la création de groupes de ressources et de stratégies de connexion, la création de sauvegardes et la surveillance des opérations.

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



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

## Découverte automatique des clusters

Les ressources sont des clusters PostgreSQL sur l'hôte Linux qui sont gérés par SnapCenter. Vous pouvez ajouter des ressources à des groupes de ressources pour exécuter les opérations de protection des données une fois que vous avez découvert les clusters PostgreSQL disponibles.

### Avant de commencer

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

### Description de la tâche

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

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

### Étapes

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

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

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

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

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



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

## Ajoutez des ressources manuellement au plug-in hôte

La découverte automatique n'est pas prise en charge sur l'hôte Windows. Vous devez ajouter manuellement les ressources de cluster PostgreSQL.

### Avant de commencer

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

## Description de la tâche

La détection 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 Détails de la ressource, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Spécifier le nom du cluster
Nom d'hôte	Entrez le nom d'hôte.
Type	Sélectionnez cluster.
Fréquence	Spécifiez le nom de l'instance, qui est le parent du cluster.
Informations d'identification	Sélectionnez les informations d'identification ou ajoutez-les.  Cette option est facultative.

4. Sur la page fournir l'empreinte du stockage, sélectionnez un type de stockage et choisissez un ou plusieurs volumes, LUN et qtrees, puis cliquez sur **Enregistrer**.

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

5. Facultatif : dans la page Paramètres de ressources, pour les ressources sur l'hôte Windows, entrez des paires clé-valeur personnalisées pour le plug-in PostgreSQL
6. Vérifiez le résumé, puis cliquez sur **Terminer**.

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

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

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

### Une fois que vous avez terminé

- Après avoir ajouté les clusters, vous pouvez modifier les détails du cluster PostgreSQL.

- Les ressources migrées (tablespace et clusters) à partir 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 depuis SnapCenter 5.0 ou une version antérieure, procédez comme suit dans la page **Paramètres de ressource** pour les paires de valeurs de clé personnalisées :
  - Spécifiez le terme "PORT" dans le champ **Nom**.
  - Spécifiez le numéro de port dans le champ **valeur**.

## Créez des règles de sauvegarde pour PostgreSQL

Avant d'utiliser SnapCenter pour sauvegarder des ressources PostgreSQL, vous devez créer une stratégie de sauvegarde pour le groupe de ressources ou de ressources que vous souhaitez sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes.

### Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde.

Pour plus d'informations, reportez-vous aux 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 du système de stockage et l'ajout de ressources.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir affecté des SVM aux volumes source et de destination.

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

### Description de la tâche

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
  - La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un plus grand nombre d'instantanés que le nombre spécifié dans la règle.
  - Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

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

4. Dans la page Nom, entrez le nom et les détails de la stratégie.
  5. Dans la page Type de stratégie, effectuez les opérations suivantes :
    - 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 valeurs de clé à transmettre au plug-in.
6. Dans la page sauvegarde et réPLICATION, effectuez les opérations suivantes :
    - a. Spécifiez la fréquence d'horaire en sélectionnant **sur demande**, **horaire**, **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 partageant la même stratégie et la même fréquence de sauvegarde, mais aussi d'affecter des programmes de sauvegarde différents à chaque stratégie.



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

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

Les fonctions que vous recherchez...	Alors...
Conserver un certain nombre d'instantanés	<p>Sélectionnez <b>copies à conserver</b>, puis indiquez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <p></p> <p>Si vous prévoyez d'activer la réPLICATION SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> <p></p> <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>
Conserver les instantanés pendant un certain nombre de jours	<p>Sélectionnez <b>conserver les copies pour</b>, puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.</p>
Période de verrouillage de la copie instantanée	<p>Sélectionnez <b>Période de verrouillage de la copie instantanée</b> et spécifiez les jours, les mois ou les années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>

## 7. Sélectionnez un libellé de stratégie.



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 des options de réPLICATION secondaires suivantes ou les deux :

Pour ce champ...	Procédez comme ça...
<p><b>Mettre à jour SnapMirror après avoir créé une copie Snapshot locale</b></p>	<p>Sélectionnez ce champ pour créer des copies en 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-fort sélectionnée.</p> <p>Lors de la réPLICATION secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal.</p> <p>Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Voir "<a href="#">Affichez les sauvegardes et clones liés aux ressources PostgreSQL dans la page topologie</a>".</p>
<p><b>Mettre à jour SnapVault après avoir créé une copie Snapshot locale</b></p>	<p>Sélectionnez cette option pour effectuer la réPLICATION de sauvegarde disque à disque (sauvegardes SnapVault).</p> <p>Lors de la réPLICATION secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquez sur le bouton <b>Actualiser</b> de la page topologie pour actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.</p> <p>Pour plus d'informations sur le coffre-fort SnapLock, reportez-vous à la section archivage des snapshots en mode WORM sur un coffre-fort destination</p> <p>Voir "<a href="#">Affichez les sauvegardes et clones liés aux ressources PostgreSQL dans la page topologie</a>".</p>

Pour ce champ...	Procédez comme ça...
<b>Nombre de tentatives d'erreur</b>	Saisissez le nombre maximal de tentatives de réPLICATION pouvant être autorisées avant l'arrêt de l'opération.



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

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

## Créer des groupes de ressources et attacher des stratégies

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

### Description de la tâche

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

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

<b>Pour ce champ...</b>	<b>Procédez comme ça...</b>
Utilisez un format de nom personnalisé pour la copie Snapshot	<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, clienttext_Resource group_policy_hostname ou Resource group_hostname. Par défaut, un horodatage est ajouté au nom du snapshot.</p>

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

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

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

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

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

<b>Pour ce champ...</b>	<b>Procédez comme ça...</b>
Attendez la fin de l'opération de snapshot de groupe de cohérence	<p>Sélectionnez <b>urgent</b>, <b>Moyen</b> ou <b>relâché</b> pour spécifier le temps d'attente pour l'exécution de l'opération de snapshot.</p> <p>Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.</p>
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

- Cliquez sur la flèche **scripts** et entrez les commandes pré et post pour les opérations quiesce, snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
- Cliquez sur la flèche **configurations personnalisées** et entrez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Réglage	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archive de supprimer les journaux d'archive.
ARCHIVAGE_LOG_RÉTENTION	nombre_de_jours	Indique le nombre de jours pendant lesquels les journaux d'archive sont conservés.  Ce paramètre doit être supérieur ou égal à NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_répertoire/logs	Indique le chemin d'accès au répertoire contenant les journaux d'archive.
ARCHIVE_LOG_EXT	extension_fichier	Spécifie l'extension du fichier journal d'archivage.  Par exemple, si le journal d'archivage est log_backup_0_1.log, spécifiez .log comme extension de fichier.

Paramètre	Réglage	Description
ARCHIVE_LOG_RÉCURSIVE_SE ARCH	(O/N)	<p>Permet la gestion des journaux d'archivage dans les sous-répertoires.</p> <p>Vous devez utiliser ce paramètre si les journaux d'archivage sont situés sous des sous-répertoires.</p>



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 de création de snapshots :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows et mettre le système de fichiers dans un état cohérent avant de créer un snapshot. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
SnapCenter pour créer un snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .
Pour saisir la commande à exécuter sur l'hôte afin de créer des copies Snapshot.	Sélectionnez <b>autre</b> , puis entrez la commande à exécuter sur l'hôte pour créer un instantané.

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

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



Vous pouvez également créer une police en cliquant sur \* \*

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

b.

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

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

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

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

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

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

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

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

## Créez des groupes de ressources et activez la protection secondaire des 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 les ressources ONTAP 9.x et 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 ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonction **Secondaryprotection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources passe 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 mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez 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 des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

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



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

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 a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent 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 dans la section Ressources sélectionnées.

6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.

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

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



Vous pouvez également créer une stratégie en cliquant sur .

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

b.

Cliquez sur Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur OK.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

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

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

a. Sélectionnez le type de la règle de réPLICATION.



Règle de réPLICATION synchrone non prise en charge.

b. Indiquez le suffixe du groupe de cohérence à utiliser.

c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.

-  Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.
-  Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

1. Sur la page Vérification, effectuez les opérations suivantes :
  - a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
  - b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
  - c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'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 programmes appliqués.

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

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

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

## Créez 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 SVM (Storage Virtual machine) et des informations d'identification avant d'utiliser les applets de commande PowerShell pour sauvegarder, restaurer ou cloner les clusters PostgreSQL..

## Avant de commencer

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

Les installations de plug-in d'hôte ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache d'hôte peut ne pas être mis à jour et l'état des clusters peut être affiché dans l'interface graphique de 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 des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

## Étapes

1. Lancez une session de connexion PowerShell 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 une nouvelle information d'identification à l'aide de l'applet de commande Add-SmCredential.

Cet exemple montre comment créer un nouvel identifiant nommé 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 au serveur SnapCenter.

```
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 d'accès à SQLLIB.

Pour Windows, le plug-in PostgreSQL utilisera le chemin par défaut du 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 relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Sauvegardez 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 stratégie de sauvegarde.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.
- Pour l'opération de sauvegarde basée sur des copies Snapshot, vérifiez que tous les clusters de locataires sont valides et actifs.
- Pour les commandes PRE et post pour les opérations quiesce, Snapshot et unquiesce, vous devez vérifier que les commandes existent dans la liste de commandes disponible sur l'hôte plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\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 de commandes, l'opération échoue.

## UI 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 **View** en fonction du type de ressource.

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

3. Sélectionnez la ressource à sauvegarder.

4. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, *customtext\_policy\_hostname* ou *Resource\_hostname*. Par défaut, un horodatage est ajouté au nom du Snapshot.

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

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

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

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

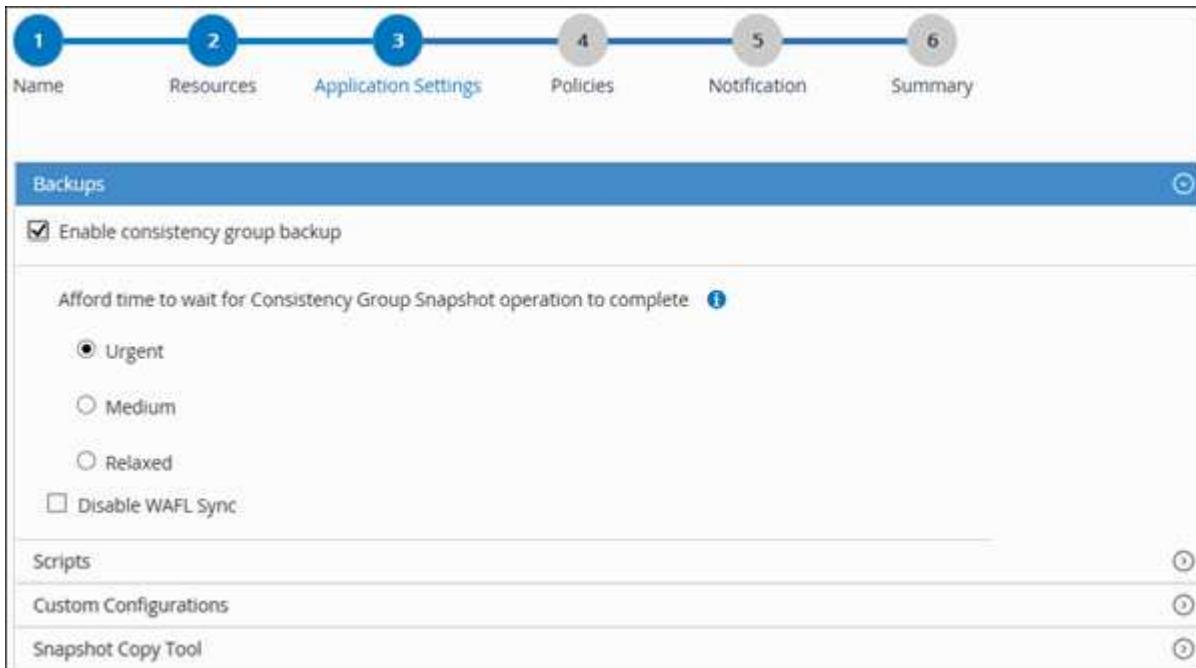
- Sélectionnez la flèche **scripts** pour exécuter des commandes pré et post pour les opérations quiesce, Snapshot et unquiesce.

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

- Sélectionnez la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
- Sélectionnez la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows afin de mettre le système de fichiers dans un état cohérent, puis de créer un Snapshot	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
Pour saisir la commande permettant de créer un Snapshot	Sélectionnez <b>autre</b> , puis entrez la commande pour créer un instantané.



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

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



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

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

- b. Sélectionnez \* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

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

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

8. Passez en revue le résumé, puis sélectionnez **Terminer**.

La page topologie des ressources s'affiche.

9. Sélectionnez **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

- Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

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

- Sélectionnez **Backup**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

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

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

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

## Applets de commande PowerShell

### Étapes

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

- 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 la cmdlet 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 en échec) à l'aide de l'applet de commande Get-smJobSummaryReport.

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

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

```

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

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la "[Guide de référence de l'apple 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 associé à une stratégie.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.

### Description de la tâche

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une

stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

## Étapes

1. Dans le volet de navigation de gauche, 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 effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en sélectionnant , puis en  sélectionnant la balise. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.  
Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.
  - b. Sélectionnez **Backup**.
5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Surveillez les opérations de sauvegarde PostgreSQL

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

### Description de la tâche

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

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

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.

- b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



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

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

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

## Surveillez les opérations de protection des données sur les clusters PostgreSQL dans le volet activité

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

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

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur le volet activité pour afficher les cinq opérations les plus récentes.

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

## Annulez les opérations de sauvegarde pour PostgreSQL

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

### Ce dont vous aurez besoin

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

### Étapes

1. Effectuez l'une des opérations suivantes :

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

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

## Affichez les sauvegardes et clones PostgreSQL dans la page topologie

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

### Description de la tâche

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

-  affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
  -  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
  -  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.
-  Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.
-  Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

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

## Étapes

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

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

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

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

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

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Après une sauvegarde à la demande, en cliquant sur le bouton **Refresh**, vous actualisez les détails de la sauvegarde ou du clone.

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

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

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



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

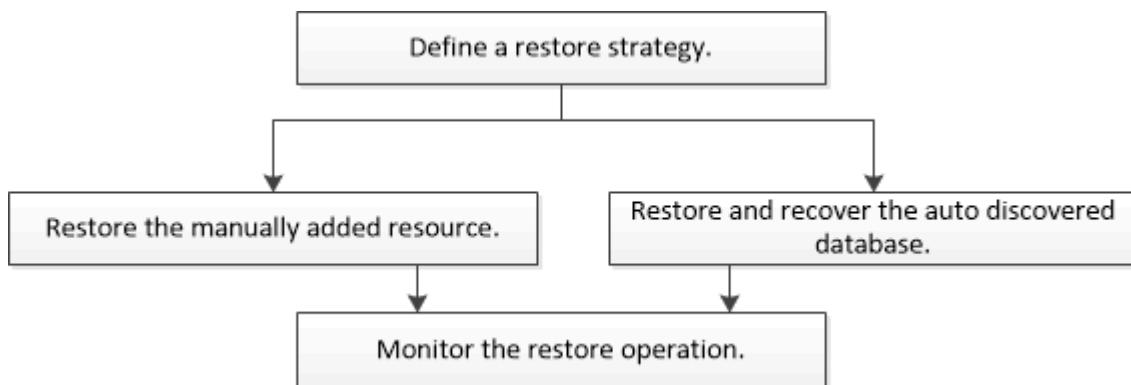
7. Pour supprimer un clone, sélectionnez-le dans le tableau, puis cliquez sur .
8. Si vous souhaitez diviser un clone, sélectionnez-le dans le tableau, puis cliquez sur .

## Restaurer PostgreSQL

## Restaurer le flux de travail

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

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



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

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

## Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement

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

### Avant de commencer

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

### Description de la tâche

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

## UI 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 **View** en fonction du type de ressource.

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



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

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

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

La page topologie de ressources s'affiche.

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



Primary Backup(s)	
Backup Name	End Date
rg1_scapr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restore Scope, sélectionnez **Complete Resource**.

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

Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, 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 des volumes, qtrees ou LUN sont restaurés.

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

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

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

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

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

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

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

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### 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 une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup

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

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

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

SmBackupId      : 113
SmJobId        : 2032
StartTime       : 2/2/2015 6:57:03 AM
EndTime         : 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
StartTime       : 2/2/2015 1:02:41 PM
EndTime         : 2/2/2015 1:02:38 PM
Duration        : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

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

```

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

```

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

## **Restaurez et récupérez 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 en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :

- 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 de commandes, l'opération échoue.

## Description de la tâche

- Les copies de sauvegarde basées sur des fichiers ne peuvent pas être restaurées depuis SnapCenter.
- Pour les ressources découvertes automatiquement, la restauration est prise en charge par 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 du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du 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, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

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



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

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

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

La page topologie de ressources s'affiche.

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

Primary Backup(s)	
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.0463	1/5/2017 1:35:27 AM

- Dans la page Restore Scope, sélectionnez **Complete Resource** pour restaurer les volumes de données configurés du cluster PostgreSQL.

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

Si...	Procédez comme ça...
Vous souhaitez effectuer une restauration aussi proche que possible de l'heure actuelle	Sélectionnez <b>récupérer à l'état le plus récent</b> . Pour les ressources de conteneur unique, spécifiez un ou plusieurs emplacements de sauvegarde de journaux et de catalogues.
Vous souhaitez effectuer une restauration au point dans le temps spécifié	Sélectionnez <b>récupérer à un point dans le temps</b> . <ol style="list-style-type: none"> <li>Entrez la date et l'heure. Entrez la date et l'heure. Par exemple, l'hôte PostgreSQL se trouve à Sunnyvale, en Californie, et l'utilisateur de Raleigh, en Caroline du Nord, récupère les journaux dans SnapCenter. Si l'utilisateur souhaite effectuer une récupération à 5 a.m . Sunnyvale, CA, alors l'utilisateur doit définir le fuseau horaire du navigateur sur le fuseau horaire de l'hôte PostgreSQL Linux, qui est GMT-07:00 et spécifier la date et l'heure à 5:00</li> </ol>
Ne pas récupérer	Sélectionnez <b>pas de récupération</b> .



Vous ne pouvez pas récupérer les ressources PostgreSQL ajoutées manuellement.



Le plug-in SnapCenter pour PostgreSQL crée une étiquette\_sauvegarde et une table\_map dans le dossier <OS\_temp\_folder>/postgresql\_sc\_Recovery<Restore\_JobId>/\_ pour faciliter la restauration manuelle.

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

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

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

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

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

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

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

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

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

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

### Étapes

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

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

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

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

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

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

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

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId        : 2032
StartTime       : 2/2/2015 6:57:03 AM
EndTime         : 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
StartTime       : 2/2/2015 1:02:41 PM
EndTime         : 2/2/2015 1:02:38 PM
Duration        : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

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

```

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

```

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

## Surveillez les opérations de restauration PostgreSQL

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

### Description de la tâche

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

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

-  En cours

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

## Étapes

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

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

# Cloner les sauvegardes de ressources PostgreSQL

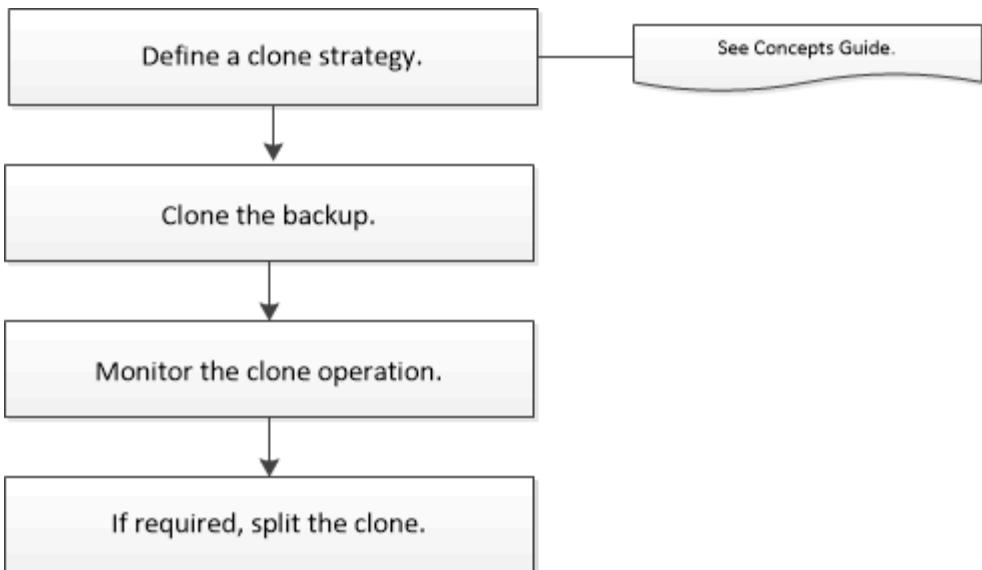
## Workflow de clonage

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

### Description de la tâche

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

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



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

## Cloner une sauvegarde PostgreSQL

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

### Avant de commencer

- Vous devriez avoir sauvegardé les ressources ou le groupe de ressources.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Pour les commandes pré-clone ou post-clone, vérifiez si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
  - 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 de commandes, l'opération échoue.

### Description de la tâche

- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à "Séparer un volume FlexClone de son volume parent" la section, .
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI 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 **View** en fonction du type de ressource.

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

3. Sélectionnez la ressource ou le groupe de ressources.

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

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

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

Pour ce champ...	Procédez comme ça...
Serveur clone	Choisissez l'hôte sur lequel le clone doit être créé.
Port cible	Entrez le port cible PostgreSQL à cloner à partir des sauvegardes existantes.
Adresse IP d'exportation NFS	Entrez les adresses IP ou les noms d'hôte sur lesquels les volumes clonés seront exportés.  Cela s'applique uniquement à la ressource de type de stockage NFS.
Capacité du pool max. Débit (Mio/s)	Entrez le débit maximal d'un pool de capacité.  Cela s'applique uniquement aux ressources de type de stockage ANF.

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



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

- a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.
  - Commande pré-clonage : supprimez les clusters existants portant le même nom
  - Commande post-clonage : vérification d'un cluster ou démarrage d'un cluster

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

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

Exemple pour NFS : `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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

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

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

10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

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

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

Cet exemple montre que la sauvegarde à cloner a une adresse NFSExportalIP 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 clone.

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

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

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

SmCloneId	:	1
SmJobId	:	186
StartDateTime	:	8/3/2015 2:43:02 PM
EndDateTime	:	8/3/2015 2:44:08 PM
Duration	:	00:01:06.6760000
Status	:	Completed
ProtectionGroupName	:	Draper
SmProtectionGroupId	:	4
PolicyName	:	OnDemand_Clone
SmPolicyId	:	4
BackupPolicyName	:	OnDemand_Full_Log
SmBackupPolicyId	:	1
CloneHostName	:	SCSPR0054212005.mycompany.com
CloneHostId	:	4
CloneName	:	Draper_clone_08-03-2015_14.43.53
SourceResources	:	{Don, Betty, Bobby, Sally}
ClonedResources	:	{Don_DRAPER, Betty_DRAPER, Bobby_DRAPER, Sally_DRAPER}
SmJobError	:	

## Surveillez les opérations de clonage PostgreSQL

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

### Description de la tâche

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

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

## Étapes

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

## Séparer un clone

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

### Description de la tâche

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

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

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

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

## Étapes

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

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

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

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

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

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

Par exemple :

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

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

#### Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

#### Supprimez ou répartissez 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 séparer les clones de la page topologie de la ressource à partir de laquelle les clones ont été créés.

#### Description de la tâche

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

## Étapes

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

La page topologie de ressources s'affiche.

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

## **Informations sur le copyright**

Copyright © 2026 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 JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

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

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

## **Informations sur les marques commerciales**

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