



# **Sauvegardez les données des applications cloud natives**

## **Cloud Backup**

NetApp  
January 09, 2023

# Table des matières

- Sauvegardez les données des applications cloud natives . . . . . 1
  - Sauvegardez les bases de données Oracle cloud natives . . . . . 1
  - Sauvegardez les bases de données SAP HANA cloud natives . . . . . 8

# Sauvegardez les données des applications cloud natives

## Sauvegardez les bases de données Oracle cloud natives

### Accéder à BlueXP

Vous devriez ["Inscrivez-vous au site Web NetApp BlueXP"](#), ["Connectez-vous à BlueXP"](#), puis configurez un ["Compte NetApp"](#).

### Configurer FSX pour ONTAP

Vous devez créer l'environnement de travail FSX pour ONTAP et le connecteur.

#### Créer un environnement de travail FSX pour ONTAP

Vous devez créer les environnements de travail Amazon FSX pour ONTAP dans lesquels vos bases de données sont hébergées. Pour plus d'informations, reportez-vous à la section ["Commencez avec Amazon FSX pour ONTAP"](#) et ["Créer et gérer un environnement de travail Amazon FSX pour ONTAP"](#).

Vous pouvez créer NetApp FSX à l'aide de BlueXP ou d'AWS. Si vous avez créé à l'aide d'AWS, vous devriez découvrir FSX pour les systèmes ONTAP dans BlueXP.

#### Créer un connecteur

Un administrateur de comptes doit déployer un connecteur dans AWS qui permet à BlueXP de gérer les ressources et les processus au sein de votre environnement de cloud public.

Pour plus d'informations, reportez-vous à la section ["Création d'un connecteur dans AWS à partir de BlueXP"](#).

- Vous devez utiliser le même connecteur pour gérer à la fois l'environnement de travail FSX et les bases de données Oracle.
- Si vous disposez de l'environnement de travail FSX et des bases de données Oracle dans le même VPC, vous pouvez déployer le connecteur dans le même VPC.
- Si vous disposez de l'environnement de travail FSX et des bases de données Oracle dans différents VPC :
  - Si des charges de travail NAS (NFS) sont configurées sur FSX, vous pouvez créer le connecteur sur l'un des VPC.
  - Si seules des charges de travail SAN sont configurées et que vous ne prévoyez pas d'utiliser des charges de travail NAS (NFS), vous devez créer le connecteur dans le VPC où le système FSX est créé.



Pour utiliser des charges de travail NAS (NFS), vous devez disposer d'une passerelle de transit entre le VPC de la base de données Oracle et le VPC FSX. L'adresse IP NFS qui est une adresse IP flottante est accessible depuis un autre VPC uniquement via la passerelle de transit. Nous ne pouvons pas accéder aux adresses IP flottantes en peering des VPC.

Après avoir créé le connecteur, cliquez sur **Storage > Canvas > Mes environnements de travail > Ajouter**

**un environnement de travail** et suivez les invites pour ajouter l'environnement de travail. Assurez-vous que le connecteur est connecté aux hôtes de base de données Oracle et à l'environnement de travail FSX. Le connecteur doit pouvoir se connecter à l'adresse IP de gestion du cluster de l'environnement de travail FSX.



Après avoir créé le connecteur, cliquez sur **Connector > Manage Connectors**, sélectionnez le nom du connecteur et copiez l'ID du connecteur.

## Configurez Cloud Volumes ONTAP

Vous devez créer l'environnement de travail Cloud Volumes ONTAP et le connecteur.

### Créer un environnement de travail Cloud Volumes ONTAP

Vous pouvez découvrir et ajouter des systèmes Cloud Volumes ONTAP existants à BlueXP. Pour plus d'informations, reportez-vous à la section "[Ajout de systèmes Cloud Volumes ONTAP existants à BlueXP](#)".

### Créer un connecteur

Vous pouvez commencer à utiliser Cloud Volumes ONTAP pour votre environnement cloud en quelques étapes. Pour plus d'informations, reportez-vous à l'une des méthodes suivantes :

- "[Démarrage rapide de Cloud Volumes ONTAP dans AWS](#)"
- "[Démarrage rapide de Cloud Volumes ONTAP dans Azure](#)"
- "[Démarrage rapide pour Cloud Volumes ONTAP dans Google Cloud](#)"

Vous devez utiliser le même connecteur pour gérer à la fois l'environnement de travail CVO et les bases de données Oracle.

- Si vous disposez de l'environnement de travail CVO et des bases de données Oracle dans le même VPC ou VNet, vous pouvez déployer le connecteur dans le même VPC ou vNet.
- Si vous disposez de l'environnement de travail CVO et des bases de données Oracle dans différents VPC ou VNets, assurez-vous que les VPC ou VNets sont associés.

## Ajouter l'hôte et découvrir les bases de données Oracle

Vous devez ajouter l'hôte et découvrir les bases de données sur l'hôte pour affecter des stratégies et créer des sauvegardes. Vous pouvez ajouter l'hôte manuellement lorsque vous avez déjà déployé le plug-in ou l'ajouter à l'aide de SSH.

### Prérequis

Avant d'ajouter l'hôte, vous devez vous assurer que les prérequis sont respectés.

- Vous devriez avoir créé l'environnement de travail et le connecteur.
- Assurez-vous que le connecteur est connecté à l'environnement de travail et aux hôtes de la base de données Oracle.
- Assurez-vous que l'utilisateur BlueXP a le rôle "Admin compte".
- Assurez-vous que Java 11 (64 bits) Oracle Java ou OpenJDK est installé sur chacun des hôtes de base de données Oracle et QUE LA variable JAVA\_HOME est correctement définie.

- Vous devez avoir créé l'utilisateur non-root. Pour plus d'informations, reportez-vous à la section [Configurer un utilisateur non-racine](#).
- Si vous souhaitez ajouter l'hôte manuellement, vous devez d'abord déployer le plug-in. Vous pouvez déployer le plug-in [manuellement](#) ou [à l'aide du script](#).

Vous devez déployer le plug-in sur chacun des hôtes de la base de données Oracle.

## Configurer un utilisateur non-racine

Vous devez configurer un utilisateur non-root pour déployer le plug-in.

### Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Téléchargez le binaire du plug-in hôte SnapCenter Linux.  

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Obtenez le chemin de montage de base.  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
```
4. Copiez les lignes 1 à 16 à partir du fichier **oracle\_checksum\_scs.txt** situé à **base\_mount\_path/version/sc-linux-host-plugin/**.
5. Connectez-vous à l'hôte de la base de données Oracle et effectuez les opérations suivantes :
  - a. Créez le compte utilisateur non-racine, la paire de clés privées et attribuez les autorisations. Pour plus d'informations, reportez-vous à la section "[Créez un compte utilisateur](#)".
  - b. Collez les lignes que vous avez copiées à l'étape 4 dans le fichier **/etc/sudoers** à l'aide de l'utilitaire visudo Linux.

Dans les lignes ci-dessus, remplacez le <LINUXUSER> par l'utilisateur non-root que vous avez créé et enregistrez le fichier dans l'utilitaire visudo.

## Déployez le plug-in à l'aide d'un script

Si l'authentification basée sur la clé SSH est activée sur l'hôte Oracle pour l'utilisateur non-root, vous pouvez effectuer les étapes suivantes pour déployer le plug-in. Avant d'effectuer les étapes, assurez-vous que la connexion SSH au connecteur est activée.

### Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Obtenez le chemin de montage de base.  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
```
3. Déployez le plug-in à l'aide du script d'assistance fourni dans le connecteur.  

```
sudo <base_mount_path>/scripts/oracle_plugin_copy_and_install.sh --host <host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port> --pluginport <plugin_port> --installdir <install_dir>
```

  - Host\_name est le nom de l'hôte Oracle et il s'agit d'un paramètre obligatoire.

- `ssh_key_file` est la clé SSH de l'utilisateur non-root et utilisée pour se connecter à l'hôte Oracle. Ce paramètre est obligatoire.
- `User_name` : utilisateur non-root disposant de privilèges SSH sur l'hôte Oracle et il s'agit d'un paramètre facultatif. La valeur par défaut est `EC2-user`.
- `ssh_port` : port SSH sur l'hôte Oracle et il s'agit d'un paramètre facultatif. La valeur par défaut est 22
- `Plugin_port` : port utilisé par le plug-in et il s'agit d'un paramètre facultatif. La valeur par défaut est 8145
- `Dossier_installation` : répertoire dans lequel le plug-in sera déployé et il s'agit d'un paramètre facultatif. La valeur par défaut est `/opt`.

Par exemple :

```
sudo /var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/oracle_plugin_copy_and_install.sh
--host xxx.xx.x.x --sshkey /keys/netapp-ssh.ppk
```

### Déployez le plug-in manuellement

Si l'authentification basée sur la clé SSH n'est pas activée sur l'hôte Oracle, effectuez les étapes manuelles suivantes pour déployer le plug-in.

### Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Téléchargez le binaire du plug-in hôte SnapCenter Linux.  

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Obtenez le chemin de montage de base.  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```
4. Obtenez le chemin binaire du plug-in téléchargé.  

```
sudo ls <base_mount_path> $(sudo docker ps|grep -Po
"cloudmanager_scs_cloud:.*? "|sed -e 's/ *$//'|cut -f2 -d":")/sc-linux-host
-plugin/snapcenter_linux_host_plugin_scs.bin
```
5. Copiez *snapcenter\_linux\_host\_plugin\_scs.bin* vers chacun des hôtes de base de données Oracle à l'aide de `scp` ou d'autres méthodes alternatives.

Le *snapcenter\_linux\_host\_plugin\_scs.bin* doit être copié dans un emplacement accessible par l'utilisateur non-root.

6. Connectez-vous à l'hôte de la base de données Oracle à l'aide du compte utilisateur non-root et exécutez la commande suivante pour activer les autorisations d'exécution pour le binaire.  

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```
7. Déployez le plug-in Oracle en tant qu'utilisateur non root `sudo`.  

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root-user>
```
8. Copiez *certificate.p12* de `<base_mount_path>/client/certificat/` chemin de la machine virtuelle du connecteur vers `/var/opt/snapcenter/spl/etc/` sur l'hôte du plug-in.
9. Accédez à `/var/opt/snapcenter/spl/etc` et exécutez la commande `keytool` pour importer le certificat.  

```
keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12
-destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter
```

```
-deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt
```

10. Redémarrer SPL : `systemctl restart spl`

## Ajouter hôte

Vous devez ajouter l'hôte et découvrir les bases de données Oracle.

### Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Cliquez sur découvrir les applications.
3. Sélectionnez **Cloud Native** et cliquez sur **Next**.

Un compte de service avec le rôle *SnapCenter System* est créé pour exécuter des opérations de protection des données planifiées pour tous les utilisateurs de ce compte.

- Cliquez sur **compte > gérer compte > membres** pour afficher le compte de service.



Le compte de service (*SnapCenter-account-**<accountid>***) est utilisé pour l'exécution des opérations de sauvegarde planifiées. Vous ne devez jamais supprimer le compte de service.

4. Dans la page Ajouter un hôte, effectuez l'une des opérations suivantes :

Si...	Procédez comme ça...
Ont déployé le plug-in non plus <a href="#">manuellement</a> ou à <a href="#">l'aide du script</a>	<ol style="list-style-type: none"><li>a. Sélectionnez <b>Manuel</b>.</li><li>b. Spécifiez le FQDN ou l'adresse IP de l'hôte où le plug-in est déployé.  Assurez-vous que le connecteur peut communiquer avec l'hôte de base de données à l'aide du FQDN ou de l'adresse IP.</li><li>c. Spécifiez le port du plug-in.  Le port par défaut est 8145.</li><li>d. Sélectionnez le connecteur.</li><li>e. Cochez la case pour confirmer que le plug-in est installé sur l'hôte</li><li>f. Cliquez sur <b>découvrir les applications</b>.</li></ol>

Si...	Procédez comme ça...
Déploiement automatique du plug-in	<p>a. Sélectionnez <b>utilisant SSH</b>.</p> <p>b. Spécifiez le FQDN ou l'adresse IP de l'hôte où vous souhaitez installer le plug-in.</p> <p>c. Spécifiez le nom d'utilisateur (<b>utilisateur non-root</b>) à l'aide de laquelle le module du plug-in sera copié sur l'hôte.</p> <p>d. Spécifiez le port SSH et le port du plug-in.</p> <p>Le port SSH par défaut est 22 et le port du plug-in est 8145.</p> <p>Vous pouvez fermer le port SSH sur l'hôte de l'application après avoir installé le plug-in. Le port SSH n'est requis pour aucune autre opération de plug-in.</p> <p>e. Sélectionnez le connecteur.</p> <p>f. (Facultatif) si l'authentification sans clé n'est pas activée entre le connecteur et l'hôte, vous devez spécifier la clé privée SSH qui sera utilisée pour communiquer avec l'hôte.</p> <div>  <p>La clé privée SSH n'est pas stockée n'importe où dans l'application et ne sera pas utilisée pour d'autres opérations.</p> </div> <p>g. Cliquez sur <b>Suivant</b>.</p>

- Affiche toutes les bases de données sur l'hôte. Si l'authentification OS est désactivée pour la base de données, vous devez configurer l'authentification de la base de données en cliquant sur **configurer**. Pour plus d'informations, reportez-vous à la section <https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/Configurer les informations d'identification de la base de données Oracle>.
- Cliquez sur **Paramètres** et sélectionnez **hôtes** pour afficher tous les hôtes. Cliquez sur **Supprimer** pour supprimer un hôte de base de données.



Le filtre permettant d'afficher un hôte spécifique ne fonctionne pas. Lorsque vous spécifiez un nom d'hôte dans le filtre, tous les hôtes sont affichés.

- Cliquez sur **Paramètres** et sélectionnez **stratégies** pour afficher les stratégies prédéfinies. Passez en revue les stratégies pré-prédéfinies et, si vous le souhaitez, vous pouvez les modifier pour répondre à vos exigences ou créer une nouvelle stratégie.



## Configurer les informations d'identification de la base de données Oracle

Vous devez configurer les informations d'identification utilisées pour effectuer des opérations de protection des données sur les bases de données Oracle.

### Étapes

1. Si l'authentification OS est désactivée pour la base de données, vous devez configurer l'authentification de la base de données en cliquant sur **configurer**.
2. Spécifiez le nom d'utilisateur, le mot de passe et les détails du port.

Si la base de données réside dans ASM, vous devez également configurer les paramètres ASM.

L'utilisateur Oracle doit disposer des privilèges sysdba et l'utilisateur ASM doit disposer des privilèges sysasm.

3. Cliquez sur **configurer**.

## Sauvegardez les bases de données Oracle cloud natives

Vous devez affecter une stratégie pré-prédéfinie ou la stratégie que vous avez créée, puis effectuer une sauvegarde.

### Créez une règle pour protéger les bases de données Oracle

Vous pouvez créer des stratégies si vous ne souhaitez pas modifier les stratégies prédéfinies.

### Étapes

1. Dans la page applications, dans la liste déroulante Paramètres, sélectionnez **stratégies**.
2. Cliquez sur **Créer une stratégie**.
3. Spécifiez un nom de stratégie.
4. (Facultatif) modifiez le format du nom de la sauvegarde.
5. Spécifiez la planification et les informations de conservation.
6. Cliquez sur **Créer**.

### Créez une sauvegarde de la base de données Oracle

Vous pouvez soit affecter une stratégie pré-prédéfinie, soit créer une stratégie, puis l'affecter à la base de données. Une fois la stratégie attribuée, les sauvegardes sont créées conformément au planning défini dans la stratégie.



Pour Oracle, lors de la création de groupes de disques ASM, assurez-vous qu'il n'y a pas de volumes communs entre les groupes de disques. Chaque groupe de disques doit disposer de volumes dédiés.

### Étapes

1. Dans la page applications, si la base de données n'est pas protégée à l'aide d'aucune stratégie, cliquez sur **affecter stratégie**.

Si la base de données est protégée à l'aide d'une ou de plusieurs stratégies, vous pouvez attribuer davantage de stratégies en cliquant sur **...** > **affecter stratégie**.

2. Sélectionnez la stratégie et cliquez sur **affecter**.

Les sauvegardes seront créées conformément à la planification définie dans la stratégie.



Le compte de service (*SnapCenter-account- $\langle$ Account\_ID $\rangle$* ) est utilisé pour l'exécution des opérations de sauvegarde planifiées.

## Création d'une sauvegarde à la demande de la base de données Oracle

Après avoir affecté la stratégie, vous pouvez créer une sauvegarde à la demande de l'application.

### Étapes

1. Dans la page applications, cliquez sur **...** Correspondant à l'application et cliquez sur **On-Demand Backup**.
2. Si plusieurs stratégies sont affectées à l'application, sélectionnez la stratégie, la valeur de conservation, puis cliquez sur **Créer une sauvegarde**.

### Plus d'informations

Après la restauration d'une base de données volumineuse (250 Go ou plus), si vous effectuez une sauvegarde en ligne complète sur la même base de données, l'opération risque d'échouer avec l'erreur suivante :

```
failed with status code 500, error
{"error":{"code":"app_internal_error","message":"Failed to create
snapshot. Reason: Snapshot operation not allowed due to clones backed by
snapshots. Try again after sometime.
```

Pour plus d'informations sur la façon de résoudre ce problème, reportez-vous à : ["Opération de snapshot non autorisée en raison de clones sauvegardés par des snapshots"](#).

### Limites

- Ne prend pas en charge les sauvegardes de données en ligne ou de journaux uniquement
- Ne prend pas en charge les sauvegardes hors ligne
- Ne prend pas en charge la sauvegarde de la base de données Oracle résidant sur des points de montage récursifs
- Ne prend pas en charge les snapshots de groupes de cohérence pour les bases de données Oracle résidant sur plusieurs groupes de disques ASM avec chevauchement des volumes FSX
- Si vos bases de données Oracle sont configurées sur ASM, assurez-vous que les noms de vos SVM sont uniques sur les systèmes FSX. Si vous disposez du même nom de SVM sur les systèmes FSX, la sauvegarde des bases de données Oracle résidant sur ces SVM ne est pas prise en charge.

## Sauvegardez les bases de données SAP HANA cloud natives

## Accéder à BlueXP

Vous devriez "[Inscrivez-vous au site Web NetApp BlueXP](#)", "[Connectez-vous à BlueXP](#)", puis configurez un "[Compte NetApp](#)".

## Configurez Azure NetApp Files

Vous devez créer l'environnement de travail Azure NetApp Files et le connecteur.

### Créer un environnement de travail Azure NetApp Files

Nous vous recommandons de créer des environnements de travail Azure NetApp Files (ANF) dans lesquels sont hébergées vos bases de données. Pour plus d'informations, reportez-vous à la section "[Découvrez Azure NetApp Files](#)" et "[Créer un environnement de travail Azure NetApp Files](#)".

### Créer un connecteur

Un administrateur de comptes doit déployer un connecteur dans ANF qui permet à BlueXP de gérer les ressources et les processus au sein de votre environnement de cloud public.



Vous ne pouvez pas mettre à jour le nouvel ID\_connecteur à partir de l'interface utilisateur.

Pour plus d'informations, reportez-vous à la section "[Créez un connecteur dans Azure à partir de BlueXP](#)".

## Déployez le plug-in SnapCenter pour SAP HANA

Vous devez déployer le plug-in SnapCenter pour SAP HANA sur chacun des hôtes de base de données SAP HANA. Selon que l'authentification basée sur une clé SSH est activée ou non sur l'hôte SAP HANA, vous pouvez suivre l'une des méthodes de déploiement du plug-in.



Assurez-vous que Java 11 (64 bits) Oracle Java ou OpenJDK est installé sur chacun des hôtes de base de données SAP HANA.

### Configurer un utilisateur non-racine

Vous devez créer un utilisateur non racine pour déployer le plug-in.

#### Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Téléchargez le binaire du plug-in hôte Linux.  

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Obtenez le chemin de montage de base.  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
```
4. Copier les lignes 1 à 16 à partir du `oracle_checksum_scs.txt` dossier situé à `base_mount_path/version/sc-linux-host-plugin/`

5. Connectez-vous à l'hôte de la base de données SAP HANA et effectuez les opérations suivantes :
  - a. Créez le compte utilisateur non-racine, la paire de clés privées et attribuez les autorisations.
  - b. Collez les lignes que vous avez copiées à l'étape 4 dans le `/etc/sudoers` Fichier à l'aide de l'utilitaire Linux de visualisation.

Dans les lignes ci-dessus, remplacez le `<LINUXUSER>` par l'utilisateur non racine que vous avez créé et enregistrez dans l'utilitaire de visualisation.

## Déployez le plug-in avec l'authentification basée sur des clés SSH

Si l'authentification basée sur la clé SSH est activée sur l'hôte HANA, vous pouvez effectuer les étapes suivantes pour déployer le plug-in. Avant d'effectuer les étapes, assurez-vous que la connexion SSH au connecteur est activée.

### Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Obtenez le chemin de montage de base.

```
# sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
```
3. Déployez le plug-in.

```
# sudo <base_mount_path>/scripts/hana_plugin_copy_and_install.sh --host <host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port> --pluginport <plugin_port> --installdir <install_dir>
```

  - `Host_name` est le nom de l'hôte HANA, et il s'agit d'un paramètre obligatoire.
  - `ssh_key_file` est la clé SSH utilisée pour la connexion à l'hôte HANA, et il s'agit d'un paramètre obligatoire.
  - `Nom_utilisateur` : utilisateur avec privilèges SSH sur l'hôte HANA, et il s'agit d'un paramètre facultatif. La valeur par défaut est `azureuser`.
  - `ssh_port` : port SSH sur l'hôte HANA, et ce paramètre est facultatif. La valeur par défaut est 22.
  - `Plugin_port` : port utilisé par le plug-in, et il s'agit d'un paramètre facultatif. La valeur par défaut est 8145.
  - `Dossier_installation` : répertoire dans lequel le plug-in sera déployé, et il s'agit d'un paramètre facultatif. La valeur par défaut est `/opt`.

## Déployez le plug-in manuellement

Si l'authentification basée sur la clé SSH n'est pas activée sur l'hôte HANA, vous devez effectuer les étapes manuelles suivantes pour déployer le plug-in.

### Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Téléchargez le binaire du plug-in hôte Linux.

```
# sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Obtenez le chemin de montage de base.

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
```

```
docker volume inspect | grep Mountpoint
```

4. Obtenez le chemin binaire du plug-in téléchargé.

```
sudo ls <base_mount_path> $(sudo docker ps|grep -Po  
"cloudmanager_scs_cloud:.*? " | sed -e 's/ *$//' | cut -f2 -d":")/sc-linux-host  
-plugin/snapcenter_linux_host_plugin_scs.bin
```

5. Copier snapcenter\_linux\_host\_plugin\_scs.bin Vers chacun des hôtes de la base de données SAP HANA à l'aide de scp ou d'autres méthodes alternatives.

6. Sur l'hôte de la base de données SAP HANA, exécutez la commande suivante pour activer les autorisations d'exécution pour le binaire.

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```

7. Déployez le plug-in SAP HANA en tant qu'utilisateur non root.

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root-user>
```

8. Copier certificate.p12 de <base\_mount\_path>/client/certificate/ Chemin d'accès de la machine virtuelle connecteur à /var/opt/snapcenter/spl/etc/ sur l'hôte du plug-in.

a. Accédez à /var/opt/snapcenter/spl/etc et exécutez la commande keytool pour importer le certificat.

```
keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12  
-destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter  
-deststorepass snapcenter -srccalias agentcert -destalias agentcert -noprompt
```

b. Redémarrer SPL:systemctl restart spl

## Sauvegardez les bases de données SAP HANA cloud natives

Avant de créer une sauvegarde de la base de données SAP HANA, vous devez ajouter les hôtes de la base de données SAP HANA et affecter une règle prédéfinie ou la règle que vous avez créée.

### Ajouter des hôtes de base de données SAP HANA

Vous devez ajouter manuellement des hôtes de base de données SAP HANA pour attribuer des règles et créer des sauvegardes. La découverte automatique de l'hôte de base de données SAP HANA n'est pas prise en charge.

#### Ce dont vous aurez besoin

- Vous devez avoir ajouté l'environnement de travail et créé le connecteur.
- Assurez-vous que le connecteur est connecté à l'environnement de travail
- Assurez-vous que l'utilisateur BlueXP a le rôle "Admin compte".
- Vous devez avoir déployé le plug-in SnapCenter pour SAP HANA. ["En savoir plus >>"](#)
- Lors de l'ajout des hôtes de base de données SAP HANA, vous devez ajouter les clés de stockage HDB. La clé de stockage sécurisée HDB est utilisée pour stocker les informations de connexion des hôtes de base de données SAP HANA en toute sécurité sur le client et le client HDBSQL utilise la clé de stockage utilisateur sécurisée pour se connecter à l'hôte de base de données SAP HANA.
- Pour la réplication système HANA (HSR), pour protéger les systèmes HANA, vous devez enregistrer manuellement les systèmes HANA primaires et secondaires.

## Étapes

1. Dans l'interface utilisateur **BlueXP**, cliquez sur **protection > sauvegarde et restauration > applications**.
2. Cliquez sur **découvrir les applications**.
3. Sélectionnez **Cloud Native > SAP HANA** et cliquez sur **Next**.
4. Dans la page **applications**, cliquez sur **Ajouter système**.
5. Dans la page **Détails du système**, effectuez les opérations suivantes :

- a. Sélectionnez le Type de système comme conteneur de base de données mutualisé ou conteneur unique.
- b. Entrez le nom du système SAP HANA.
- c. Spécifier le SID du système SAP HANA.
- d. (Facultatif) spécifiez l'utilisateur HDBSQL OS.
- e. Sélectionnez Plug-in host. (Facultatif) si l'hôte n'est pas ajouté ou si vous souhaitez ajouter plusieurs hôtes, cliquez sur **Ajouter hôte de plug-in**.
- f. Si le système HANA est configuré avec la réplication système HANA, activez **HANA System Replication (HSR) System**.
- g. Cliquez sur **HDB Secure User Store Keys** (clés de stockage d'utilisateur sécurisées) pour ajouter les détails des clés de la boutique d'utilisateurs.

Spécifiez le nom de la clé, les détails du système, le nom d'utilisateur et le mot de passe, puis cliquez sur **Ajouter une clé**.

Vous pouvez supprimer ou modifier les clés de la boutique utilisateur.

6. Cliquez sur **Suivant**.
7. Dans la page **empreinte de stockage**, cliquez sur **Ajouter un stockage** et effectuez les opérations suivantes :
  - a. Sélectionnez l'environnement de travail et spécifiez le compte NetApp.  
  
Accédez à la page **Canvas** pour ajouter un nouvel environnement de travail
  - b. Sélectionnez les volumes requis.
  - c. Cliquez sur **Ajouter un stockage**.
8. Vérifiez tous les détails et cliquez sur **Ajouter système**.



Le filtre permettant d'afficher un hôte spécifique ne fonctionne pas. Lorsque vous spécifiez un nom d'hôte dans le filtre, tous les hôtes sont affichés

Vous pouvez modifier et supprimer les systèmes SAP HANA à l'aide de l'API REST. Avant de supprimer le système HANA, vous devez supprimer toutes les sauvegardes associées et supprimer la protection.

### Ajouter des volumes non-données

Après avoir ajouté le conteneur de base de données mutualisé ou un système SAP HANA de type conteneur unique, vous pouvez ajouter les volumes non-Data du système HANA.

### Étapes

1. Dans l'interface utilisateur **BlueXP**, cliquez sur **protection > sauvegarde et restauration > applications**.

2. Cliquez sur **découvrir les applications**.
3. Sélectionnez **Cloud Native > SAP HANA** et cliquez sur **Next**.
4. Dans la page **applications**, cliquez sur **...** Correspondant au système pour lequel vous souhaitez ajouter les volumes non-données et sélectionner **gérer le système > non-Data Volume**.

## Ajouter des volumes globaux non-données

Après avoir ajouté le conteneur de base de données mutualisée ou un seul type de conteneur SAP HANA, vous pouvez ajouter le système non-Data volumes global du système HANA.

### Étapes

1. Dans l'interface utilisateur **BlueXP**, cliquez sur **protection > sauvegarde et restauration > applications**.
2. Cliquez sur **découvrir les applications**.
3. Sélectionnez **Cloud Native > SAP HANA** et cliquez sur **Next**.
4. Dans la page **applications**, cliquez sur **Ajouter système**.
5. Dans la page **Détails du système**, effectuez les opérations suivantes :
  - a. Dans la liste déroulante Type de système, sélectionnez **Volume global hors données**.
  - b. Entrez le nom du système SAP HANA.
  - c. Spécifiez les SID associés du système SAP HANA.
  - d. Sélectionnez l'hôte du plug-in

(Facultatif) pour ajouter plusieurs hôtes, cliquez sur **Ajouter hôte du plug-in** et spécifiez le nom d'hôte et le port, puis cliquez sur **Ajouter hôte**.

  - e. Cliquez sur **Suivant**.
  - f. Vérifiez tous les détails et cliquez sur **Ajouter système**.

### Préscripts et postscripts

Vous pouvez fournir des scripts prescripteurs, des scripts postaux et des scripts d'exit pendant la création d'une stratégie. Ces scripts sont exécutés sur l'hôte HANA lors de la création des sauvegardes.

Le format pris en charge pour les scripts est .sh, le script python, le script perl, etc.

Le prescripteur et le PostScript devraient être enregistrés par l'administrateur hôte dans `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` file

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

### Variables environnementales

Pour le workflow de restauration, les variables d'environnement suivantes sont disponibles dans le cadre du programme prescripteur et PostScript.

Variable d'environnement	Description
SID	Identifiant système de la base de données HANA sélectionnée pour la restauration
BackupName	Nom de sauvegarde choisi pour l'opération de restauration
UserStoreKeyNames	Clé userstore configurée pour la base de données HANA
OSDBUser	OSDBUser configuré pour la base de données HANA
NomPolicy	Uniquement pour sauvegarde planifiée
type_programme	Uniquement pour sauvegarde planifiée

## Créez une règle pour protéger la base de données SAP HANA

Vous pouvez créer des stratégies si vous ne voulez pas utiliser ou modifier les stratégies prédéfinies.

1. Dans la page **applications**, dans la liste déroulante Paramètres, sélectionnez **stratégies**.
2. Cliquez sur **Créer une stratégie**.
3. Spécifiez un nom de stratégie.
4. (Facultatif) modifiez le format du nom de la copie Snapshot.
5. Sélectionnez le type de stratégie.
6. Spécifiez la planification et les informations de conservation.
7. (Facultatif) spécifiez les scripts.
8. Cliquez sur **Créer**.

## Créez une sauvegarde de la base de données SAP HANA

Vous pouvez soit affecter une stratégie pré-prédéfinie, soit créer une stratégie, puis l'affecter à la base de données. Une fois la stratégie attribuée, les sauvegardes sont créées conformément au planning défini dans la stratégie.

### À propos de cette tâche

Pour la réplication système HANA (HSR), la tâche de sauvegarde planifiée se déclenchera uniquement pour le système HANA principal et si le système bascule vers le système HANA secondaire, les planifications existantes déclenchent une sauvegarde sur le système HANA principal actuel. Si la règle n'est pas attribuée au système HANA, après le basculement, les planifications échouent.

Si différentes politiques sont attribuées aux systèmes HSR, la sauvegarde planifiée sera déclenchée pour les systèmes et la sauvegarde échouera pour le système HANA secondaire.

### Étapes



1. Dans la page applications, si la base de données n'est pas protégée à l'aide d'aucune stratégie, cliquez sur **affecter stratégie**.

Si la base de données est protégée à l'aide d'une ou de plusieurs stratégies, vous pouvez attribuer davantage de stratégies en cliquant sur **...** > **affecter stratégie**.

2. Sélectionnez la stratégie et cliquez sur **affecter**.

Les sauvegardes seront créées conformément à la planification définie dans la stratégie.



Le compte de service (*SnapCenter-account-`<Account_ID>`*) est utilisé pour l'exécution des opérations de sauvegarde planifiées.

## Création d'une sauvegarde à la demande de la base de données SAP HANA

Après avoir affecté la stratégie, vous pouvez créer une sauvegarde à la demande de l'application.

### Étapes

1. Dans la page **applications**, cliquez sur **...** Correspondant à l'application et cliquez sur **On-Demand Backup**.
2. Sélectionnez un type de sauvegarde à la demande.
3. Pour la sauvegarde basée sur la stratégie, sélectionnez la stratégie, le niveau de rétention, puis cliquez sur **Créer une sauvegarde**.
4. Pour une seule fois, sélectionnez Snapshot basé sur une copie ou fichier, effectuez les opérations suivantes :
  - a. Sélectionnez la valeur de rétention et spécifiez le nom de la sauvegarde.
  - b. (Facultatif) spécifiez les scripts et le chemin des scripts.
  - c. Cliquez sur **Créer une sauvegarde**.

## Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

## Informations sur les marques commerciales

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