



# **Protégez les données applicatives cloud natives**

## **Cloud Backup**

NetApp  
December 19, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/concept-protect-cloud-app-data-to-cloud.html> on December 19, 2022. Always check docs.netapp.com for the latest.

# Table des matières

- Protégez les données applicatives cloud natives . . . . . 1
  - Protégez vos données applicatives cloud natives . . . . . 1
  - Sauvegardez les données des applications cloud natives . . . . . 5
  - Restaurez les données des applications cloud natives . . . . . 19
  - Clonez les données des applications cloud natives . . . . . 22
  - Gérez la protection des données applicatives cloud natives . . . . . 31

# Protégez les données applicatives cloud natives

## Protégez vos données applicatives cloud natives

Cloud Backup pour applications est un service SaaS qui fournit des fonctionnalités de protection des données pour les applications exécutées sur NetApp Cloud Storage. Cloud Backup pour les applications activées dans BlueXP (anciennement Cloud Manager) offre une protection efficace et cohérente avec les applications et basée sur des règles pour les applications suivantes :

- Bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP et Cloud Volumes ONTAP
- Systèmes SAP HANA résidant sur Azure NetApp Files (ANF).

### Architecture

L'architecture Cloud Backup pour applications comprend plusieurs composants :

- Cloud Backup pour les applications est un ensemble de services de protection des données hébergés à la demande par NetApp et basés sur la plateforme SaaS BlueXP.

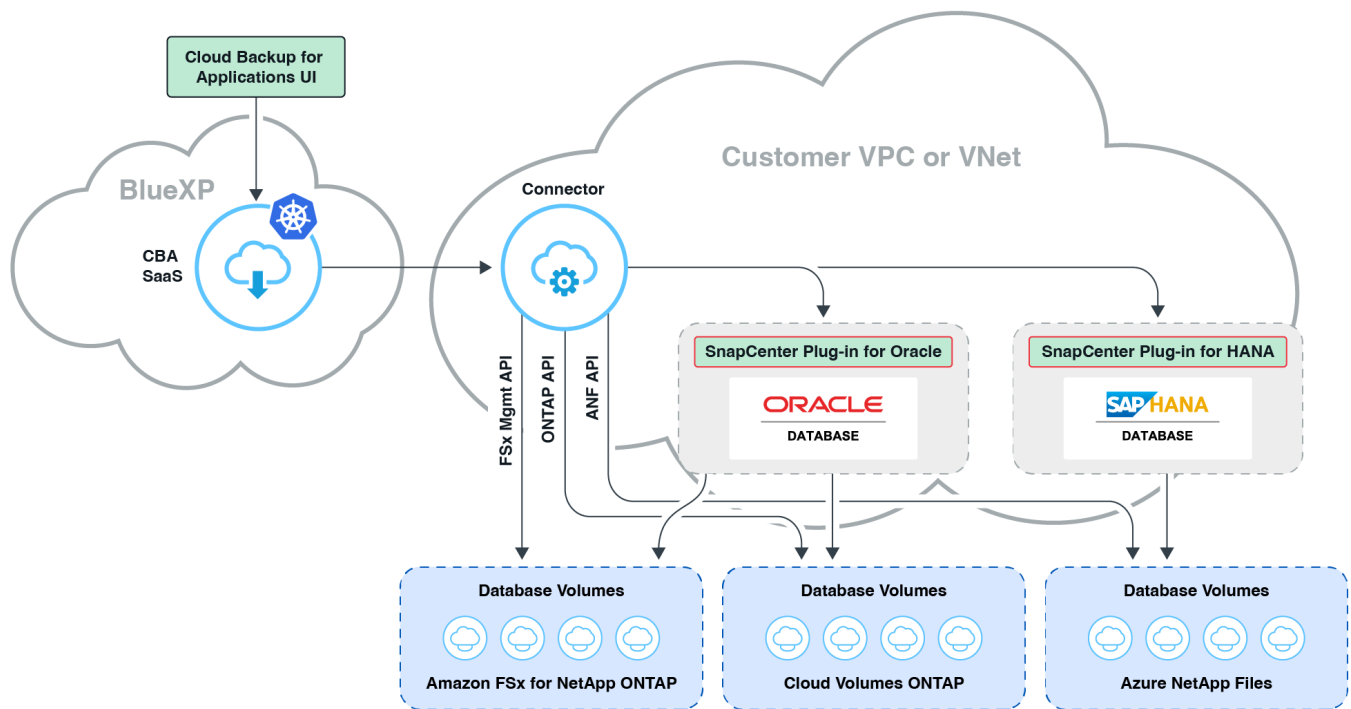
Il orchestre les workflows de protection des données pour les applications qui résident sur NetApp Cloud Storage.

- L'interface utilisateur Cloud Backup pour applications est accessible depuis l'interface utilisateur BlueXP.

L'interface utilisateur de Cloud Backup pour les applications offre des fonctionnalités de protection des données pour les applications.

- BlueXP Connector est un composant qui s'exécute dans le réseau cloud de l'utilisateur et interagit avec les systèmes de stockage et les plug-ins spécifiques aux applications.
- Le plug-in spécifique aux applications est un composant qui s'exécute sur chaque hôte d'application. Il interagit avec les bases de données exécutées sur l'hôte tout en exécutant les opérations de protection des données.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux :



Pour toute demande initiée par l'utilisateur, l'interface utilisateur Cloud Backup pour applications communique avec le service BlueXP SaaS qui, lors de la validation de la demande, traite la même chose. Si la demande consiste à exécuter un workflow tel qu'une sauvegarde, une restauration ou un clone, le service SaaS lance le workflow et, le cas échéant, transmet l'appel au connecteur BlueXP. Le connecteur communique ensuite avec le système de stockage et le plug-in spécifique à l'application dans le cadre de l'exécution des tâches du flux de travail.

Le connecteur peut être déployé dans le même VPC ou dans le même vnet que celui des applications, ou dans un autre. Si le connecteur et les applications se trouvent sur un autre réseau, vous devez établir une connectivité réseau entre eux.



Un connecteur BlueXP unique peut communiquer avec plusieurs systèmes de stockage et plusieurs plug-ins d'applications. Vous aurez besoin d'un connecteur unique pour gérer vos applications tant que la connectivité entre le connecteur et les hôtes d'application est disponible.



Cloud Backup pour applications l'infrastructure SaaS est résiliente aux défaillances de zone de disponibilité dans une région. Il prend en charge les défaillances régionales en effectuant le basculement vers une nouvelle région et ce basculement implique une interruption de l'activité d'environ 2 heures.

## Protéger la base de données Oracle

### Configurations compatibles

- Système d'exploitation :
  - RHEL 7.5 ou version ultérieure et 8.x
  - OL 7.5 ou version ultérieure et 8.x
- Système de stockage :
  - Amazon FSX pour ONTAP

- Cloud Volumes ONTAP
- Disposition du stockage :
  - NFS v3 et v4.1 (y compris dNFS)
  - iSCSI avec ASM (ASMFD, ASMLib et ASMUdev)
- Dispositions de la base de données : Oracle Standard et Oracle Enterprise Standalone (CDB et boîtier de distribution électrique existant et mutualisé)
- Versions de base de données : 12cR2, 18c, 19c et 21c

## Caractéristiques

- Ajoutez de l'hôte et déployez le plug-in

Vous pouvez déployer le plug-in manuellement, à l'aide d'un script ou automatiquement.

- Découverte automatique des bases de données Oracle
- Sauvegarde des bases de données Oracle
  - Sauvegarde complète (données + contrôle + fichiers journaux d'archive)
  - Sauvegarde à la demande
  - Sauvegarde planifiée en fonction des règles personnalisées ou définies par le système

Vous pouvez spécifier différentes fréquences d'horaires, telles que les heures, les jours, les semaines et les mois dans la police.

- Conservation des sauvegardes en fonction de la stratégie appliquée
- Restauration de la base de données Oracle complète (fichiers de données + fichier de contrôle) à partir de la sauvegarde spécifiée
- Restauration des fichiers de données uniquement et des fichiers de contrôle uniquement à partir de la sauvegarde spécifiée
- Récupération de la base de données Oracle avec jusqu'à SCN, jusqu'au moment, tous les journaux disponibles et aucune option de récupération
- Clonage de bases de données Oracle sur des hôtes source ou cible de remplacement
  - Clone de base en un clic
  - Clonage avancé à l'aide d'un fichier de spécifications de clonage personnalisé
  - Le nom des entités de clonage peut être généré automatiquement ou identique à la source
  - Affichage de la hiérarchie des clones
  - Suppression des bases de données clonées
- Surveillance des sauvegardes, de la restauration, du clonage et d'autres tâches
- Affichage du récapitulatif de protection sur le tableau de bord
- Envoi d'alertes par e-mail

## Limites

- Ne prend pas en charge Oracle 11g
- Ne prend pas en charge les opérations de montage, de catalogue et de vérification sur les sauvegardes

- Ne prend pas en charge Oracle sur RAC et Data Guard
- Pour la haute disponibilité Cloud Volumes ONTAP, seule une des adresses IP de l'interface réseau est utilisée. Si la connectivité de l'IP tombe en panne ou si vous ne pouvez pas accéder à l'IP, les opérations échouent.
- Les adresses IP de l'interface réseau d'Amazon FSX pour NetApp ONTAP ou Cloud Volumes ONTAP doivent être uniques dans le compte et la région BlueXP.

## Protégez la base de données SAP HANA

### Configurations compatibles

- Système d'exploitation :
  - RHEL 7.5 ou version ultérieure, 8.x plates-formes certifiées par SAP HANA
  - SLES 12 SP5 ou version ultérieure et plates-formes SPX 15 certifiées par SAP HANA
- Système de stockage : Azure NetApp Files (ANF)
- Dispositions de stockage : pour les données et les journaux, Azure prend uniquement en charge NFSv4.1.
- Dispositions de la base de données :
  - Conteneur unique version 1.0SPS12
  - Conteneur de base de données mutualisé SAP HANA (MDC) 2.0SPS4, 2.0SPS5, 2.0SPS6 avec un ou plusieurs locataires
  - Système hôte unique SAP HANA, système hôte multiples SAP HANA (sans hôte de secours), réplication système HANA
- Plug-in SAP HANA sur l'hôte de base de données

### Caractéristiques

- Ajoutez manuellement des systèmes SAP HANA
- Sauvegarde des bases de données SAP HANA
  - Sauvegarde à la demande (basée sur les fichiers et les copies Snapshot)
  - Sauvegarde planifiée en fonction des règles personnalisées ou définies par le système

Vous pouvez spécifier différentes fréquences d'horaires, telles que les heures, les jours, les semaines et les mois dans la police.

- Compatibilité avec la réplication système HANA (HSR)
- Conservation des sauvegardes en fonction de la stratégie appliquée
- Restauration de la base de données SAP HANA complète à partir de la sauvegarde spécifiée
- Sauvegarde et restauration de volumes HANA non-Data et de volumes globaux sans données
- Prise en charge des scripts prescripteurs et postscripts utilisant des variables d'environnement pour les opérations de sauvegarde et de restauration
- Création d'un plan d'action pour les scénarios d'échec à l'aide de l'option de pré-sortie

### Limites

- Pour la configuration HSR, seul le HSR 2 nœuds est pris en charge (1 principal et 1 secondaire)

- La rétention ne sera pas déclenchée si le script PostScript échoue pendant l'opération de restauration

## 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 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`

## 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
```

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>	<div>a. Sélectionnez <b>Manuel</b>.</div> <div>b. Spécifiez le FQDN ou l'adresse IP de l'hôte où le plug-in est déployé.</div> <div>Assurez-vous que le connecteur peut communiquer avec l'hôte de base de données à l'aide du FQDN ou de l'adresse IP.</div> <div>c. Spécifiez le port du plug-in.</div> <div>Le port par défaut est 8145.</div> <div>d. Sélectionnez le connecteur.</div> <div>e. Cochez la case pour confirmer que le plug-in est installé sur l'hôte</div> <div>f. Cliquez sur <b>découvrir les applications</b>.</div>

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-**<Account\_ID>***) 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 cliquer 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 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 sur l'hôte du plug-in.
  - a. Accédez à `/var/opt/snapcenter/spl/etc` and execute the `keytool` command to import the certificate.  

```
`keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype  
PKCS12 -destkeystore keystore.jks -deststoretype JKS -srcstorepass  
snapcenter -deststorepass snapcenter -srcalias agentcert -destalias  
agentcert -noprompt
```
  - b. Redémarrer SPL:  

```
systemctl restart spl`
```

### 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.

## 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

Variable d'environnement	Description
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**.

## Restaurez les données des applications cloud natives

### Restaurez les bases de données Oracle cloud natives

En cas de perte de données, vous pouvez restaurer les fichiers de données, les fichiers de contrôle ou les deux, puis restaurer la base de données.

#### Ce dont vous aurez besoin

Si la base de données Oracle 21c est à l'état DÉMARRÉ, l'opération de restauration échoue. Vous devez exécuter les étapes suivantes pour restaurer la base de données avec succès.

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar  
/opt/NetApp/snapcenter/spl/plugins/sco/lib ojdbc8-8.jar
```

#### Étapes

1. Cliquez sur ... Correspondant à la base de données à restaurer et cliquez sur **Afficher les détails**.
2. Cliquez sur ... Correspondant à la sauvegarde de données à utiliser pour la restauration et cliquez sur **Restaurer**.
3. Dans la section objectif de restauration, effectuez les opérations suivantes :

Si...	Procédez comme ça...
Vous souhaitez restaurer uniquement les fichiers de données	Sélectionnez <b>tous les fichiers de données</b> .
Vous souhaitez restaurer uniquement les fichiers de contrôle	Sélectionnez <b>fichiers de contrôle</b>
Veulent restaurer à la fois les fichiers de données et les fichiers de contrôle	Sélectionnez <b>tous les fichiers de données et fichiers de contrôle</b> .



La restauration des fichiers de données avec des fichiers de contrôle ou uniquement des fichiers de contrôle ne sont pas prises en charge pour iSCSI sur la disposition ASM.

Vous pouvez également sélectionner la case à cocher **forcer la restauration sur place**.

Dans la disposition SAN, si le plug-in SnapCenter pour Oracle trouve des fichiers étrangers autres que les fichiers de données Oracle sur le groupe de disques ASM, la méthode de restauration de connexion et de copie est exécutée. Les fichiers étrangers peuvent être de type un ou plusieurs des types suivants :

- Paramètre
- Mot de passe
- journal d'archivage
- journal en ligne
- Fichier de paramètres ASM.

L'option **forcer la restauration sur place** remplace le paramètre de type, le mot de passe et le journal d'archivage des fichiers étrangers. Vous devez utiliser la dernière sauvegarde lorsque l'option \* forcer la restauration sur place\* est sélectionnée.

4. Dans la section étendue de la récupération, effectuez les opérations suivantes :

Si...	Procédez comme ça...
Que vous souhaitez restaurer à la dernière transaction	Sélectionnez <b>tous les journaux</b> .
Que vous souhaitez récupérer à un numéro de changement de système (SCN) spécifique	Sélectionnez <b>jusqu'à ce que Numéro de changement de système</b> et spécifiez le SCN.
Vous souhaitez effectuer une restauration à une date et une heure précises	Sélectionnez <b>Date et heure</b> .
Ne pas récupérer	Sélectionnez <b>pas de récupération</b> .

Pour la portée de récupération sélectionnée, dans le champ **emplacements des fichiers journaux d'archives**, vous pouvez éventuellement spécifier l'emplacement qui contient les journaux d'archivage requis pour la restauration.

Cochez la case si vous souhaitez ouvrir la base de données en mode LECTURE-ÉCRITURE après la restauration.

5. Cliquez sur **Suivant** et vérifiez les détails.

6. Cliquez sur **Restaurer**.

## Limites

- Ne prend pas en charge les restaurations granulaires, par exemple la restauration des espaces de stockage et des bases de données de niveau fichier
- Les méthodes de restauration sur place et connexion/copie sont utilisées si certains groupes de disques contiennent des fichiers étrangers. Cependant, l'utilisation des deux méthodes en même temps pour effectuer la restauration n'est pas prise en charge et l'opération de restauration échoue. La base de données reste à l'état monté et vous devez la mettre manuellement à l'état ouvert.

Le message d'échec en raison de la présence de fichiers étrangers ne s'affiche pas sur la page de travail dans l'interface utilisateur en raison d'un problème connu. Vérifiez les journaux de connecteurs en cas de défaillance lors de l'étape de pré-restauration SAN pour connaître la cause du problème.

## Restaurez la base de données SAP HANA cloud native

En cas de perte de données, vous pouvez restaurer les fichiers de données et non de données, puis récupérer la base de données.

### 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 pendant l'opération de restauration.

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

Variable d'environnement	Description
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

## Restaurez la base de données SAP HANA cloud native

### Ce dont vous avez besoin

1. Le système SAP HANA doit être dans un état arrêté.
2. Vous pouvez fournir un prescripteur pour arrêter le système SAP HANA.

### Étapes

1. Cliquez sur [...](#) Correspondant à la base de données à restaurer et cliquer sur **Afficher les détails**.
2. Cliquez sur [...](#) Correspondant à la sauvegarde de données à utiliser pour la restauration et cliquer sur **Restaurer**.
3. Dans la page **Restore System**, entrez les scripts.
4. Cliquez sur **Restaurer**.

### Après la fin

- Après une restauration, restaurez manuellement le système SAP HANA ou fournissez un script final qui exécute la restauration du système SAP HANA.

## Restaurez un volume sans données

1. Dans la page **applications**, sélectionnez Volume sans données dans la liste déroulante.
2. Cliquez sur [...](#) Correspondant à la sauvegarde que vous souhaitez restaurer, puis cliquez sur **Restaurer**.

## Restaurez le volume global sans données

### Étapes

1. Dans la page **applications**, cliquez sur le volume global sans données que vous souhaitez restaurer.
2. Cliquez sur [...](#) Correspondant au volume global hors données que vous souhaitez restaurer, puis cliquez sur **Restaurer**.

# Clonez les données des applications cloud natives

## Clonez des bases de données Oracle natives du cloud



## Concepts et conditions de clonage

Vous pouvez cloner une base de données Oracle à l'aide de la sauvegarde de la base de données sur l'hôte de la base de données source ou sur un autre hôte. Vous pouvez cloner la sauvegarde à partir de systèmes de stockage primaires.

Avant de cloner la base de données, vous devez comprendre les concepts de clonage et vous assurer que toutes les exigences sont respectées.

### Conditions requises pour le clonage d'une base de données Oracle

Avant de cloner une base de données Oracle, vous devez vous assurer que les prérequis sont terminés.

- Vous devriez avoir créé une sauvegarde de la base de données. Vous devez avoir créé une sauvegarde des journaux et des données en ligne pour que l'opération de clonage réussisse.
- Dans le paramètre `asm_diskstring`, vous devez configurer `AFD:*` si vous utilisez ASMFD ou `ORCL:*` si vous utilisez ASMLIB.
- Si vous créez le clone sur un autre hôte, celui-ci doit répondre aux exigences suivantes :
  - Le plug-in doit être installé sur l'autre hôte.
  - L'hôte clone doit être en mesure de détecter les LUN à partir du stockage si vous clonez une base de données résidant sur le stockage SAN iSCSI. Si vous effectuez un clonage vers un autre hôte, assurez-vous qu'une session iSCSI est établie entre le stockage et l'hôte secondaire.
  - Si la base de données source est une base de données ASM :
    - L'instance ASM doit être active sur l'hôte sur lequel le clone sera exécuté.
    - Le groupe de disques ASM doit être provisionné avant l'opération de clonage si vous souhaitez placer les fichiers journaux d'archive de la base de données clonée dans un groupe de disques ASM dédié.
    - Le nom du groupe de disques de données peut être configuré mais assurez-vous que le nom n'est pas utilisé par tout autre groupe de disques ASM sur l'hôte où le clone sera effectué.
    - Les fichiers de données résidant sur le groupe de disques ASM sont provisionnés dans le cadre du flux de travail clone.

### Limites des clones

- Les clones programmés (gestion du cycle de vie des clones) ne sont pas pris en charge.
- Le clonage d'une base de données clonée n'est pas pris en charge.
- Le clonage des bases de données résidant sur `qtree` n'est pas pris en charge.
- Le clonage des sauvegardes du journal d'archivage n'est pas pris en charge.
- La sauvegarde d'une base de données clonée n'est pas prise en charge.

### Méthodes de clonage

Vous pouvez créer un clone à l'aide de la méthode de base ou du fichier de spécifications du clone.

#### Cloner à l'aide de la méthode de base

Vous pouvez créer le clone avec les configurations par défaut basées sur la base de données source et la sauvegarde sélectionnée.

- Les paramètres de base de données, home et OS user sont définis par défaut dans la base de données source.
- Les chemins des fichiers de données sont nommés en fonction du schéma de nommage sélectionné.
- Les instructions pré-script, post-script et SQL ne peuvent pas être spécifiées.
- L'option de récupération est par défaut **jusqu'à annuler** et utilise la sauvegarde de journal associée à la sauvegarde de données pour la récupération

### Cloner à l'aide d'un fichier de spécifications

Vous pouvez définir les configurations dans le fichier de spécification clone et l'utiliser pour cloner la base de données. Vous pouvez télécharger le fichier de spécifications, le modifier selon vos besoins, puis télécharger le fichier. "[En savoir plus >>](#)".

Les différents paramètres définis dans le fichier de spécifications et pouvant être modifiés sont les suivants :

Paramètre	Description
fichiers_de_contrôle	Emplacement des fichiers de contrôle de la base de données clone.  Le nombre de fichiers de contrôle sera identique à celui de la base de données source. Si vous souhaitez remplacer le chemin du fichier de contrôle, vous pouvez fournir un chemin différent pour le fichier de contrôle. Le système de fichiers ou le groupe de disques ASM doit exister sur l'hôte.
redo_logs	Emplacement, taille, groupe de reprise nombre des journaux de reprise.  Un minimum de deux groupes de fichiers journaux de reprise sont nécessaires pour cloner la base de données. Si vous souhaitez remplacer le chemin du fichier journal de reprise, vous pouvez personnaliser le chemin du fichier journal de reprise sur un système de fichiers différent de celui de la base de données source. le système de fichiers ou le groupe de disques ASM devrait exister sur l'hôte.
version_oracle	Version d'Oracle sur l'hôte cible.
oracle_home	Accueil Oracle sur l'hôte cible.
activer_archive_log_mode	Contrôle le mode du journal d'archivage de la base de données clone
paramètres_base_de_données	Paramètres de base de données pour la base de données clonée

Paramètre	Description
instructions sql	Les instructions SQL à exécuter sur la base de données après le clonage
os_user_detail	Utilisateur Oracle OS sur la base de données clone cible
port_base_de_données	Port utilisé pour communiquer avec la base de données si l'authentification OS est désactivée sur l'hôte.
port_asm	Port utilisé pour communiquer avec la base de données ASM si les informations d'identification sont fournies dans l'entrée de création de clone.
ignorer_récupération	N'effectue pas l'opération de récupération.
jusqu'à_scn	Récupère la base de données jusqu'au numéro de modification du système spécifié (scn).
jusqu'à l'heure	Récupère la base de données jusqu'à la date et l'heure spécifiées.  Le format accepté est <i>mm/jj/aaaa hh:mm:ss</i> .
jusqu'à_annuler	Récupère en montant la sauvegarde de journal associée à la sauvegarde de données sélectionnée pour le clonage.  La base de données clonée est restaurée jusqu'au fichier journal manquant ou corrompu.
chemins_journaux	D'autres emplacements des chemins du journal d'archivage à utiliser pour la récupération de la base de données clonée.
emplacement_source	Emplacement du groupe de disques ou du point de montage sur l'hôte de la base de données source.
emplacement_clone	Emplacement du groupe de disques ou du point de montage qui doit être créé sur l'hôte cible correspondant à l'emplacement source.

Paramètre	Description
type_emplacement	Il peut s'agir d'ASM_diskGroup ou d'un point de montage.  Les valeurs sont remplies automatiquement au moment du téléchargement du fichier. Vous ne devez pas modifier ce paramètre.
pré_script	Script à exécuter sur l'hôte cible avant de créer le clone.
post_script	Script à exécuter sur l'hôte cible après la création du clone.
chemin	Chemin absolu du script sur l'hôte clone.  Vous devez stocker le script soit dans /var/opt/snapcenter/spl/scripts, soit dans un dossier de ce chemin.
délai dépassé	Délai d'expiration spécifié pour le script exécuté sur l'hôte cible.
arguments	Arguments spécifiés pour les scripts.

### Schéma de nommage des clones

Le schéma de nommage des clones définit l'emplacement des points de montage et le nom des groupes de disques de la base de données clonée. Vous pouvez sélectionner **identique** ou **généré automatiquement**.

### Schéma de nommage identique

Si vous sélectionnez le schéma de nommage des clones comme **identique**, l'emplacement des points de montage et le nom des groupes de disques de la base de données clonée seront identiques à la base de données source.

Par exemple, si le point de montage de la base de données source est `/netapp_source/data_1 , +DATA1_DG`, pour la base de données clonée, le point de montage reste le même pour NFS et ASM sur SAN.

- Les configurations telles que le nombre et le chemin des fichiers de contrôle et de reprise seront identiques à celles de la source.



Si les journaux de reprise ou les chemins des fichiers de contrôle se trouvent sur les volumes autres que les données, l'utilisateur doit avoir provisionné le groupe de disques ASM ou le point de montage dans l'hôte cible.

- L'utilisateur Oracle OS et la version d'Oracle seront identiques à la base de données source.
- Le nom du volume de stockage clone aura le format suivant : `sourceVolNameSCS_Clone_CurrentTimeStampNumber`.

Par exemple, si le nom du volume de la base de données source est *sourceVolName*, le nom du volume cloné sera *sourceVolNameSCS\_Clone\_1661420020304608825*.



Le *CurrentTimeStampNumber* fournit l'unicité du nom du volume.

## Schéma de nommage généré automatiquement

Si vous sélectionnez le schéma de clonage comme **généré automatiquement**, l'emplacement des points de montage et le nom des groupes de disques de la base de données clonée sont ajoutés avec un suffixe. \* Si vous avez sélectionné la méthode de clonage de base, le suffixe sera le **Clone SID**. \* Si vous avez sélectionné la méthode du fichier de spécifications, le suffixe sera le **suffixe** spécifié lors du téléchargement du fichier de spécifications clone.

Par exemple, si le point de montage de la base de données source est */netapp\_source/data\_1* et le **Clone SID** ou le **suffixe** est *HR*, alors le point de montage de la base de données clonée sera */netapp\_source/data\_1\_HR*.

- Le nombre de fichiers de contrôle et de fichiers journaux de reprise sera identique à la source.
- Tous les fichiers journaux de reprise et les fichiers de contrôle se trouvent sur l'un des points de montage de données clonés ou sur les groupes de disques Data ASM.
- Le nom du volume de stockage clone aura le format suivant : *sourceVolNameSCS\_Clone\_CurrentTimeStampNumber*.

Par exemple, si le nom du volume de la base de données source est *sourceVolName*, le nom du volume cloné sera *sourceVolNameSCS\_Clone\_1661420020304608825*.



Le *CurrentTimeStampNumber* fournit l'unicité du nom du volume.

- Le format du point de montage NAS sera *SourceNASMountPoint\_suffix*.
- Le format du groupe de disques ASM sera *SourceDiskgroup\_suffix*.



Si le nombre de caractères du groupe de disques clone est supérieur à 25, il aura *SC\_hashCode\_suffix*.

## Paramètres de la base de données

La valeur des paramètres de base de données suivants sera identique à celle de la base de données source, quel que soit le schéma de nommage des clones.

- *format\_d'archive\_journal*
- *audit\_trail*
- *processus*
- *pga\_aggregate\_target*
- *remote\_login\_passwordfile*
- *annuler\_espace\_table*
- *open\_curseurs*
- *sga\_target*

- db\_block\_size

La valeur des paramètres de base de données suivants sera ajoutée avec un suffixe basé sur le SID du clone.

- audit\_file\_dest = {sourcedatabase\_parametervalue}\_suffixe
- log\_archive\_dest\_1 = {sourcedatabase\_oraclehome}\_suffixe

#### **Variables d'environnement prédéfinies prises en charge pour le prescripteur et le PostScript spécifiques au clone**

Vous pouvez utiliser les variables d'environnement prédéfinies prises en charge lorsque vous exécutez le prescripteur et le PostScript lors du clonage d'une base de données.

- SC\_ORIGINAL\_SID spécifie le SID de la base de données source. Ce paramètre sera renseigné pour les volumes d'application. Exemple : NFSB32
- SC\_ORIGINAL\_HOST spécifie le nom de l'hôte source. Ce paramètre sera renseigné pour les volumes d'application. Exemple : asmrac1.gdl.englab.netapp.com
- SC\_ORACLE\_HOME indique le chemin du répertoire racine Oracle de la base de données cible. Exemple : /ora01/app/oracle/product/18.1.0/db\_1
- SC\_BACKUP\_NAME » indique le nom de la sauvegarde. Ce paramètre sera renseigné pour les volumes d'application. Exemples :
  - Si la base de données n'est pas exécutée en mode ARCHIVELOG :  
DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
  - Si la base de données est exécutée en mode ARCHIVELOG : DATA@RG2\_SCspr24819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_1, RG2\_scspr24819002\_07-21-2021\_12.16.48.9267\_spr1\_07\_22\_2021\_12.16.48.9267\_12.16.48.9267\_1\_\_1\_spr1
- SC\_ORIGINAL\_OS\_USER indique le propriétaire du système d'exploitation de la base de données source. Exemple : oracle
- SC\_ORIGINAL\_OS\_GROUP spécifie le groupe du système d'exploitation de la base de données source. Exemple : oinstall
- SC\_TARGET\_SID » spécifie le SID de la base de données clonée. Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie. Ce paramètre sera renseigné pour les volumes d'application. Exemple : clonedb
- SC\_TARGET\_HOST spécifie le nom de l'hôte sur lequel la base de données sera clonée. Ce paramètre sera renseigné pour les volumes d'application. Exemple : asmrac1.gdl.englab.netapp.com
- SC\_TARGET\_OS\_USER indique le propriétaire du système d'exploitation de la base de données clonée. Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie. Exemple : oracle
- SC\_TARGET\_OS\_GROUP spécifie le groupe de systèmes d'exploitation de la base de données clonée. Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie. Exemple : oinstall
- SC\_TARGET\_DB\_PORT spécifie le port de base de données de la base de données clonée. Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie. Exemple : 1521

#### **Délimiteurs pris en charge**

- @ est utilisé pour séparer les données de son nom de base de données et pour séparer la valeur de sa clé. Exemple : DATA@RG2\_SCspr24819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- | est utilisé pour séparer les données entre deux entités différentes pour le paramètre

SC\_BACKUP\_NAME. Exemple : DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1

- , est utilisé pour séparer un ensemble de variables pour la même clé. Exemple :  
DATA@RG2\_SCspr24819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_SCvspr24819002\_07-20-2021\_12.16.48.9267\_1, RG2\_SCspr24819002\_07-21-2021\_12.16.48.9267\_1, RG2\_SCspr24819002\_07\_22\_2021\_12.16.48.9267\_\_\_\_1

## Clonez des bases de données Oracle natives du cloud

Vous pouvez cloner une base de données Oracle à l'aide de la sauvegarde de la base de données sur l'hôte de la base de données source ou sur un autre hôte.



Il est possible de cloner des bases de données pour les raisons suivantes :

- Afin de tester les fonctionnalités qui doivent être implémentées à l'aide de la structure et du contenu de la base de données en cours au cours des cycles de développement d'applications.
- Pour renseigner les data warehouses à l'aide d'outils d'extraction et de manipulation de données.
- Pour récupérer les données qui ont été supprimées ou modifiées par erreur.

## Ce dont vous aurez besoin

Avant de cloner la base de données, vous devez comprendre les concepts de clonage et vous assurer que toutes les exigences sont respectées. ["En savoir plus >>"](#).


## Étapes

1. Cliquez sur  Correspondant à la base de données à cloner et cliquez sur **Afficher les détails**.
2. Cliquez sur  Correspondant à la sauvegarde de données et cliquez sur **Clone**.
3. Sur la page Cloner les détails, sélectionnez l'une des options de clonage.
4. Selon l'option sélectionnée, effectuez les opérations suivantes :

Si vous avez sélectionné...	Procédez comme ça...
<p><b>De base</b></p>	<p>a. Sélectionnez l'hôte clone.</p> <p>Si vous souhaitez créer le clone sur un autre hôte, sélectionnez l'hôte ayant la même version d'Oracle et de système d'exploitation que celle de l'hôte de base de données source.</p> <p>b. Spécifiez la SID du clone.</p> <p>c. Sélectionnez la structure de nommage des clones.</p> <p>Si la base de données est clonée sur l'hôte source, le schéma de nommage des clones est généré automatiquement. Si la base de données est clonée sur un autre hôte, la structure de nommage des clones est identique.</p> <p>d. Spécifiez le chemin d'accès à Oracle Home.</p> <p>e. (Facultatif) spécifiez les informations d'identification de la base de données.</p> <ul style="list-style-type: none"> <li>◦ Informations d'identification de la base de données : si l'authentification de l'utilisateur OS est désactivée, vous devez fournir un mot de passe à l'utilisateur sys pour le définir sur l'hôte cible.</li> <li>◦ Informations d'identification ASM : si l'authentification de l'utilisateur OS est désactivée sur l'hôte cible, vous devez fournir les informations d'identification de l'utilisateur privilégié sysasm pour vous connecter à l'instance ASM sur l'hôte cible.</li> </ul> <p>f. Cliquez sur <b>Suivant</b>.</p> <p>g. Cliquez sur <b>Clone</b>.</p>



Si vous avez sélectionné...	Procédez comme ça...
Fichier de spécifications	<p>a. Cliquez sur <b>Télécharger le fichier</b> pour télécharger le fichier de spécifications.</p> <p>b. Sélectionnez la structure de nommage des clones.</p> <p>Si vous sélectionnez <b>généré automatiquement</b>, vous devez spécifier le suffixe.</p> <p>c. Modifiez le fichier de spécifications selon les besoins et téléchargez-le en cliquant sur le bouton <b>Parcourir</b>.</p> <p>d. Sélectionnez l'hôte clone.</p> <p>Si vous souhaitez créer le clone sur un autre hôte, sélectionnez l'hôte ayant la même version d'Oracle et de système d'exploitation que celle de l'hôte de base de données source.</p> <p>e. Spécifiez la SID du clone.</p> <p>f. (Facultatif) spécifiez les informations d'identification de la base de données.</p> <ul style="list-style-type: none"> <li>◦ Informations d'identification de la base de données : si l'authentification de l'utilisateur OS est désactivée, vous devez fournir un mot de passe à l'utilisateur sys pour le définir sur l'hôte cible.</li> <li>◦ Informations d'identification ASM : si l'authentification de l'utilisateur OS est désactivée sur l'hôte cible, vous devez fournir les informations d'identification de l'utilisateur privilégié sysasm pour vous connecter à l'instance ASM sur l'hôte cible.</li> </ul> <p>g. Cliquez sur <b>Suivant</b>.</p> <p>h. Cliquez sur <b>Clone</b>.</p>

5. Cliquez sur  À côté de **Filter by** et sélectionnez **Clone options > clones** pour afficher les clones.

## Gérez la protection des données applicatives cloud natives

### Surveiller les tâches

Vous pouvez surveiller l'état des travaux lancés dans vos environnements de travail. Cela vous permet de voir les travaux qui ont réussi, ceux qui sont en cours et ceux qui ont échoué afin de diagnostiquer et de résoudre tout problème.

Vous pouvez afficher la liste de toutes les opérations et leur état. Chaque opération, ou tâche, a un ID et un

état uniques. Le statut peut être :

- Réussi
- En cours
- En file d'attente
- Avertissement
- Échec

## Étapes

1. Cliquez sur **sauvegarde et restauration**.
2. Cliquez sur **surveillance des travaux**

Vous pouvez cliquer sur le nom d'un travail pour afficher les détails correspondant à cette opération. Si vous recherchez un emploi spécifique, vous pouvez :

- utilisez le sélecteur de temps en haut de la page pour afficher les tâches pour une certaine plage horaire
- Entrez une partie du nom du travail dans le champ Rechercher
- pour trier les résultats, utilisez le filtre de chaque en-tête de colonne

## Données d'audit

Lorsque vous exécutez une API directement ou que vous utilisez l'interface utilisateur pour passer l'appel d'API à l'une des API exposées en externe de Cloud Backup pour applications, les détails de la demande tels que les en-têtes, le rôle, le corps de la demande, Et les informations API seront consignées dans le calendrier BlueXP et les entrées d'audit seront conservées dans le calendrier pour toujours. L'état et la réponse à l'erreur de l'appel API sont également audités après l'exécution de l'opération. Dans le cas de réponses d'API asynchrones telles que des travaux, l'ID de travail est également consigné dans le cadre de la réponse.

Cloud Backup pour applications journaliser les entrées telles que l'adresse IP de l'hôte, le corps de la demande, le nom de l'opération, les personnes ayant déclenché, certains en-têtes, Et l'état de fonctionnement de l'API.

## Afficher les détails de la sauvegarde

Vous pouvez afficher le nombre total de sauvegardes créées, les stratégies utilisées pour créer des sauvegardes, la version de la base de données et l'ID de l'agent.





1. Cliquez sur **sauvegarde et restauration > applications**.
2. Cliquez sur **...** Correspondant à l'application et cliquer sur **Afficher les détails**.



L'ID de l'agent est associé au connecteur. Si un connecteur utilisé lors de l'enregistrement de l'hôte SAP HANA n'existe plus, les sauvegardes suivantes de cette application échouent car l'ID agent du nouveau connecteur est différent. Vous devez modifier l'ID du connecteur dans l'hôte.

## Supprimer le clone

Vous pouvez supprimer un clone si vous n'en avez plus besoin.

1. Cliquez sur  À côté de **Filter by** et sélectionnez **Clone options > Clone parents**.
2. Cliquez sur  Correspondant à l'application et cliquez sur **Afficher les détails**.
3. Dans la page Détails de la base de données, cliquez sur  À côté de **Filter by** et sélectionnez **Clone**.
4. Cliquez sur  Correspondant au clone que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. (Facultatif) cochez la case **forcer la suppression**.

## Mettre à jour les détails de connecteur pour l'hôte de base de données SAP HANA

Si le connecteur utilisé lors de l'enregistrement de l'hôte d'application n'existe plus ou est corrompu, vous devez déployer un nouveau connecteur. Après le déploiement du nouveau connecteur, exécutez l'API **Connector-update** pour mettre à jour les détails du connecteur pour tous les hôtes enregistrés à l'aide de l'ancien connecteur.

```
curl --location --request PATCH
'https://snapcenter.cloudmanager.cloud.netapp.com/api/saphana/hosts/connector/update' \
--header 'x-account-id: <CM account-id>' \
--header 'Authorization: Bearer token' \
--header 'Content-Type: application/json' \
--data-raw '{
  "old_connector_id": "Old connector id that no longer exists",
  "new_connector_id": "New connector Id"
}'
```

Les détails du connecteur seront mis à jour avec succès si le plug-in SnapCenter pour le service SAP HANA est installé et exécuté, mais aussi si tous sont accessibles depuis le nouveau connecteur.

## Configurer le certificat signé par l'autorité de certification

Vous pouvez configurer un certificat signé par l'autorité de certification si vous souhaitez inclure une sécurité supplémentaire à votre environnement.

### Configurer le certificat signé par l'autorité de certification pour l'authentification par certificat client

Le connecteur utilise un certificat auto-signé pour communiquer avec le plug-in. Le certificat auto-signé est importé dans le magasin de clés par le script d'installation. Vous pouvez effectuer les étapes suivantes pour remplacer le certificat auto-signé par un certificat signé par l'autorité de certification.

### Ce dont vous aurez besoin

Vous pouvez exécuter la commande suivante pour obtenir le *<base\_mount\_path>* :

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

### Étapes

1. Connectez-vous au connecteur.
2. Supprimez tous les fichiers existants situés à `<base_mount_path>/client/certificat` de la machine virtuelle de connecteur.
3. Copiez le certificat signé de l'autorité de certification et le fichier de clé dans le `<base_mount_path>/client/certificat` de la machine virtuelle du connecteur.

Le nom du fichier doit être `Certificate.pem` et `key.pem`. Le `certificat.pem` doit avoir toute la chaîne des certificats comme CA intermédiaire et CA racine.

4. Créez le format PKCS12 du certificat avec le nom `certificate.p12` et conservez-le à `<base_mount_path>/client/certificat`.
5. Copiez le `certificate.p12` et les certificats pour tous les CA et CA racine intermédiaires vers l'hôte du plug-in à l'adresse `/var/opt/snapcenter/spl/etc/`.
6. Connectez-vous à l'hôte du plug-in.
7. Accédez à `/var/opt/snapcenter/spl/etc` et exécutez la commande `keytool` pour importer le fichier `Certificate.p12`.

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

8. Importer l'autorité de certification racine et les certificats intermédiaires.

```
keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter
-alias trustedca -file <certificate.crt>
```



Le `certfile.crt` fait référence aux certificats de l'autorité de certification racine ainsi qu'à l'autorité de certification intermédiaire.

9. Redémarrer SPL : `systemctl restart spl`

## Configurez le certificat signé par l'autorité de certification pour le certificat de serveur du plug-in

Le certificat CA doit avoir le nom exact de l'hôte du plug-in avec lequel la machine virtuelle du connecteur communique.

### Ce dont vous aurez besoin

Vous pouvez exécuter la commande suivante pour obtenir le `<base_mount_path>` :

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

### Étapes

1. Effectuez les opérations suivantes sur l'hôte du plug-in :
  - a. Accédez au dossier contenant le magasin de clés de la SPL `/var/opt/snapcenter/spl/etc`.
  - b. Créez le format PKCS12 du certificat ayant à la fois le certificat et la clé avec alias `splkeystore`.
  - c. Ajoutez le certificat CA.
 

```
keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype
pkcs12 -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore
-destalias splkeystore -noprompt
```

- d. Vérifiez les certificats.

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

- e. Redémarrer SPL : `systemctl restart spl`

## 2. Effectuez les opérations suivantes sur le connecteur :

- a. Connectez-vous au connecteur en tant qu'utilisateur non-root.
- b. Copiez l'ensemble de la chaîne de certificats CA sur le volume persistant situé à `<base_mount_path>/Server`.

Créez le dossier du serveur s'il n'existe pas.

- c. Connectez-vous au `cloudManager_scs_Cloud` et modifiez le **enableCACert** dans `config.yml` sur **true**.

```
sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert:
false/enableCACert: true/g' /opt/netapp/cloudmanager-scs-
cloud/config/config.yml
```

- d. Redémarrez le conteneur `Cloud Manager_scs_Cloud`.

```
sudo docker restart cloudmanager_scs_cloud
```

## Accès aux API REST

Les API REST pour protéger les applications dans le cloud sont disponibles "[ici](#)".

Vous devez obtenir le jeton utilisateur avec l'authentification fédérée pour accéder aux API REST. Pour plus d'informations sur l'obtention du jeton utilisateur, reportez-vous à la section "[Créez un jeton utilisateur avec authentification fédérée](#)".

## Informations sur le copyright

Copyright © 2022 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.