Sauvegarde et restauration des données d'applications cloud natives

Cloud Backup

NetApp
December 15, 2022

Table des matières

Sauvegarde et restauration des données d’applications 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 NetApp BlueXP (anciennement Cloud Manager) offre des fonctionnalités de sauvegarde et de restauration efficaces et cohérentes avec les applications, basées sur des règles, et des bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP.

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.

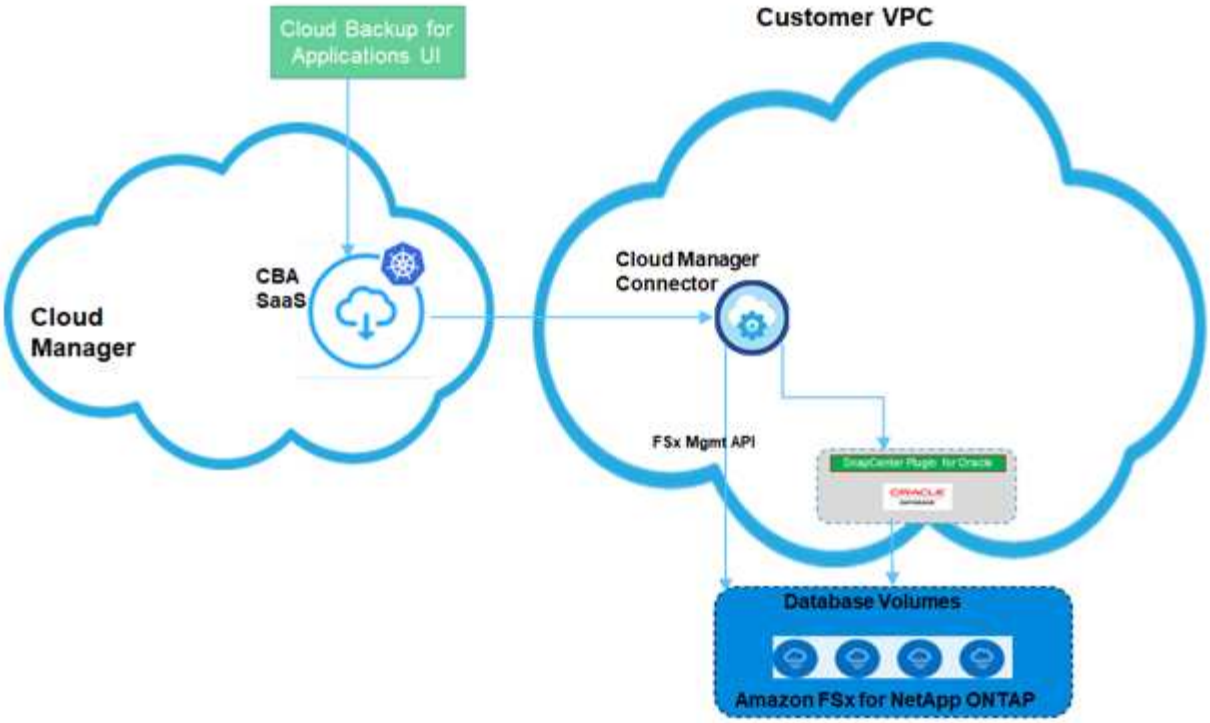
  Il orchestre les workflows de protection des données pour les applications qui résident sur NetApp Cloud Storage.

- L’interface utilisateur Cloud Backup pour applications est intégrée à l’interface utilisateur BlueXP.

  L’interface utilisateur de Cloud Backup pour les applications offre de nombreuses fonctionnalités de gestion du stockage et des données.

- BlueXP Connector est un composant de BlueXP qui s’exécute dans votre réseau cloud et interagit avec les systèmes de fichiers de stockage Amazon FSX et le plug-in SnapCenter pour Oracle fonctionnant sur des hôtes de base de données Oracle.
- Le plug-in SnapCenter pour Oracle est un composant qui s’exécute sur chaque hôte de la base de données Oracle. Il interagit avec les bases de données Oracle exécutées sur l’hôte tout en exécutant des 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 ou une restauration, le service SaaS lance le flux de travail et, le cas échéant, transmet l'appel au connecteur BlueXP. Le connecteur communique ensuite avec Amazon FSX pour NetApp ONTAP et le plug-in SnapCenter pour Oracle dans le cadre de l'exécution des tâches du flux de travail.

Le connecteur peut être déployé sur le même VPC que les bases de données Oracle, ou dans un autre. Si le connecteur et les bases de données Oracle se trouvent sur un autre réseau, vous devez établir une connectivité réseau entre eux.

Cloud Backup pour les applications l'infrastructure est résiliente aux défaillances de zone de disponibilité dans une région. Il prend désormais en charge les défaillances régionales en basculant vers une nouvelle région, ce qui entraîne une interruption de l'activité d'environ 2 heures.

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
- Dispositions de stockage : NFS v3 et v4.1 (dNFS est pris en charge) et iSCSI avec ASM (ASMFD, ASMLib et ASMUdev)
- Applications : Oracle Standard et Oracle Enterprise – autonome (ancienne génération et architecture mutualisée, CDB et PDB)
- Versions Oracle : 12cR2, 18c et 19c

Caractéristiques

- Découverte automatique des bases de données Oracle
- Sauvegarde des bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP
  - 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
- La surveillance des sauvegardes et autres tâches
- Affichage du récapitulatif de protection sur le tableau de bord
- Envoi d'alertes par e-mail

Limites

- Ne prend pas en charge les versions 11g et 21c d'Oracle
- Ne prend pas en charge les opérations de montage, de clonage, de catalogue et de vérification des sauvegardes
- Ne prend pas en charge Oracle sur RAC et Data Guard
- Limites des sauvegardes :
  - 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.
- Limites en matière de restauration :
  - Ne prend pas en charge les restaurations granulaires, par exemple la restauration des espaces de stockage et des bases de données de niveau fichier
  - Prend uniquement en charge la restauration sur place des bases de données Oracle sur des mises en page NAS et SAN

- Ne prend pas en charge la restauration du fichier de contrôle uniquement ou des fichiers de données + fichier de contrôle des bases de données Oracle sur des dispositions SAN
- Dans la disposition SAN, l'opération de restauration échoue si le plug-in SnapCenter pour Oracle trouve des fichiers étrangers autres que les fichiers de données Oracle sur le groupe de disques ASM. 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.

    Vous devez cocher la case forcer la restauration sur place pour remplacer le paramètre de type, le mot de passe et le journal d'archivage des fichiers étrangers.

> S'il existe d'autres types de fichiers étrangers, l'opération de restauration échoue et la base de données ne peut pas être récupérée. Si vous disposez d'un autre type de fichier étranger, vous devez les supprimer ou les déplacer vers un autre emplacement avant d'effectuer l'opération de restauration.

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.

Prérequis

Vous devez avoir accès à BlueXP, créer un compte BlueXP, créer l'environnement de travail et un connecteur, et déployer le plug-in SnapCenter pour Oracle.

Accéder à BlueXP

Vous devriez "Connectez-vous à BlueXP", puis configurez un "Compte NetApp".

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.

Déploiement du plug-in SnapCenter pour Oracle

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

> Assurez-vous que JAVA 8 est installé sur chacun des hôtes de base de données Oracle et que LA variable JAVA_HOME est correctement définie.

Déploiement dans des plug-ins à l'aide de l'authentification basée sur des clés SSH

Si l'authentification basée sur la clé SSH est activée sur l'hôte Oracle, 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.

1. Connectez-vous à la machine virtuelle de Connector en tant qu'utilisateur non root.
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/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 une clé SSH utilisée pour la connexion à l'hôte Oracle. Il s'agit d'un paramètre obligatoire.
- User_NAME : utilisateur avec 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`

Déploiement manuel du plug-in

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.

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.
6. Sur l'hôte de la base de données Oracle, 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 root.
   `./snapcenter_linux_host_plugin_scs.bin -i silent`
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.
   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 -srcalias agentcert -destalias agentcert -noprompt`
   b. Redémarrer SPL : `systemctl restart spl`

Sauvegardez les données applicatives cloud natives

Découvrir les applications

Vous devez découvrir les bases de données sur l'hôte pour attribuer des stratégies et créer des sauvegardes.

Ce dont vous aurez besoin

- Vous devez avoir créé l'environnement de travail FSX pour ONTAP et le connecteur.
- Assurez-vous que le connecteur est connecté à l'environnement de travail FSX pour ONTAP et aux hôtes de base de données Oracle.
- Assurez-vous que l'utilisateur BlueXP a le rôle "Admin compte".
- Vous devez avoir déployé le plug-in SnapCenter pour Oracle. "En savoir plus >>".

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 Specify Host Details, entrez les détails de l'hôte de la base de données Oracle, cochez la case pour confirmer que le plug-in est installé sur l'hôte, puis cliquez sur **Discover**.
   - 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/azure/Configurer les informations d&.html#8217;identification de la base de données Oracle.
   - Cliquez sur **gérer l'application**, sélectionnez **Ajouter** pour ajouter un nouvel hôte, **Actualiser** pour découvrir de nouvelles bases de données ou **Supprimer** pour supprimer un hôte de base de données.
   - 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 dans la section Paramètres de la base de données ou Paramètres ASM.

   L'utilisateur Oracle doit disposer des privilèges sysdba et l'utilisateur ASM doit disposer des privilèges sysasm.
3. Cliquez sur **configurer**.

Création de la règle

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**.

Sauvegarder les données applicatives cloud natives

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. Vous pouvez également créer une sauvegarde à la demande.

Lors de la création de groupes de disques ASM pour Oracle, 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 de sauvegardes à la demande

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".

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

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 de base de données Oracle n'existe plus, les sauvegardes suivantes de cette application échoueront car l'ID agent du nouveau connecteur est différent. Vous devez exécuter l'API **Connector-update** pour modifier l'ID de l'agent.

Mettre à jour les détails du connecteur

Si un connecteur utilisé lors de l'enregistrement de l'hôte de base de données Oracle n'existe plus ou est corrompu dans AWS, 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.

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

Après la mise à jour des détails du connecteur, vous devez vous connecter à l'hôte de la base de données Oracle et effectuer les opérations suivantes :

1. Obtenez les informations du plug-in en cours d'exécution sur l'hôte de la base de données Oracle.
   `rpm -qi netapp-snapcenter-plugin-oracle`
2. Désinstallez le plug-in.
   `sudo /opt/NetApp/snapcenter/spl/installation/plugins/uninstall`
3. Vérifiez que le plug-in est correctement désinstallé.
   `rpm -qi netapp-snapcenter-plugin-oracle`

Après avoir désinstallé le plug-in, vous pouvez le déployer. "En savoir plus >>".

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 certificat.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 d'autorité de certification doit avoir le nom exact de l'hôte du plug-in Oracle 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".

Restaurez les données applicatives 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.

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 section objectif de restauration, effectuez les opérations suivantes :

Si…	Procédez comme ça…
Vous souhaitez restaurer uniquement les fichiers de données	Sélectionnez **tous les fichiers de données**.
Vous souhaitez restaurer uniquement les fichiers de contrôle	Sélectionnez **fichiers de contrôle**
Veulent restaurer à la fois les fichiers de données et les fichiers de contrôle	Sélectionnez **tous les fichiers de données** et **fichiers de contrôle**.

> 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**.

L'option **forcer la restauration sur place** remplace les fichiers spfile, les fichiers de mot de passe et les fichiers journaux d'archive du groupe de disques des fichiers de données. 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 **tous les journaux**.
Que vous souhaitez récupérer à un numéro de changement de système (SCN) spécifique	Sélectionnez **jusqu'à ce que Numéro de changement de système** et spécifiez le SCN.
Vous souhaitez effectuer une restauration à une date et une heure précises	Sélectionnez **Date et heure**.
Ne pas récupérer	Sélectionnez **pas de récupération**.

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**.