Sauvegarde et restauration des données applicatives cloud

BlueXP backup and recovery

NetApp
April 18, 2024

Sommaire

Sauvegarde et restauration des données applicatives cloud

Protégez vos données d'applications cloud natives

La sauvegarde et la restauration BlueXP pour les applications offrent des fonctionnalités de protection des données cohérentes au niveau des applications pour les applications qui s'exécutent sur le stockage cloud NetApp. La sauvegarde et la restauration BlueXP assurent une protection efficace, cohérente au niveau des applications et basée sur des règles des applications suivantes :

- Bases de données Oracle hébergées sur Amazon FSX pour NetApp ONTAP, Cloud Volumes ONTAP et Azure NetApp Files
- Systèmes SAP HANA résidant sur Azure NetApp Files
- Bases de données Microsoft SQL Server résidant sur Amazon FSX pour NetApp ONTAP

Architecture

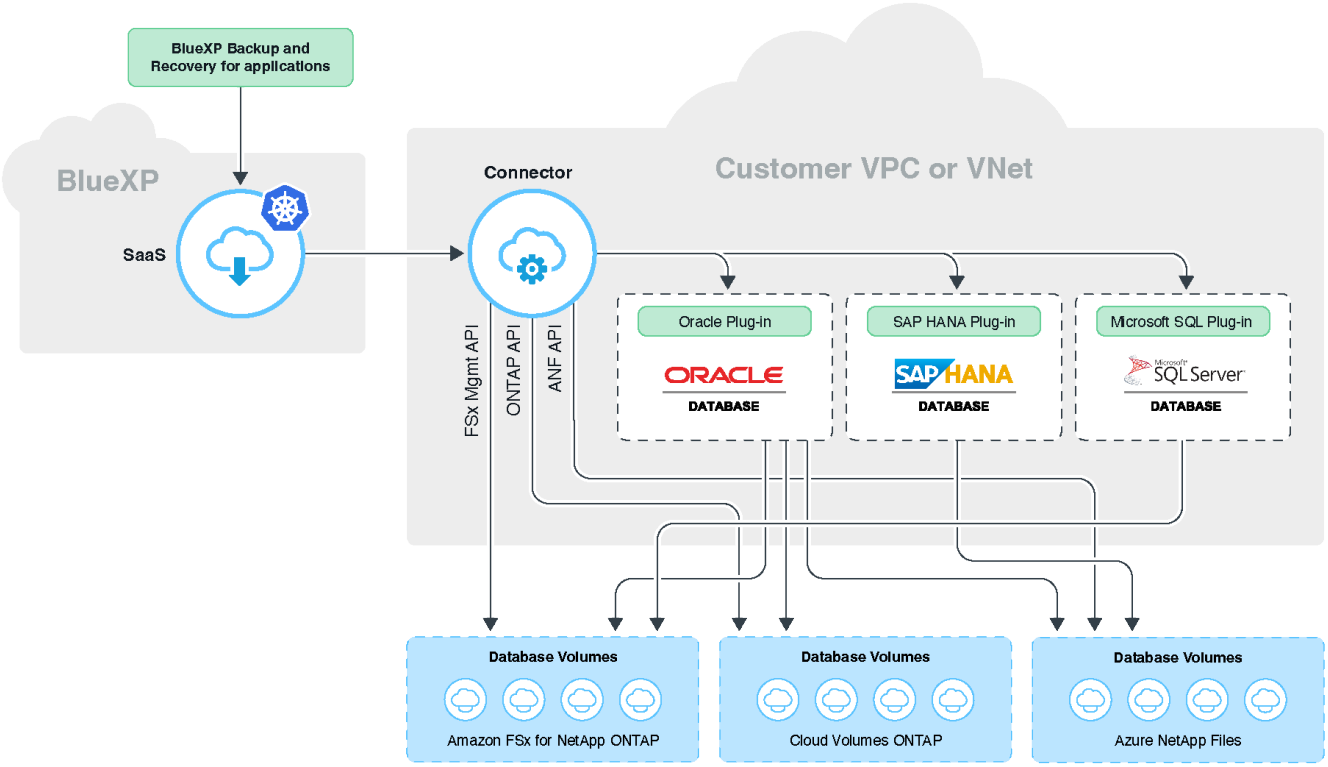
L'architecture de sauvegarde et de restauration BlueXP pour les applications inclut les composants suivants.

- La sauvegarde et la restauration BlueXP sont un ensemble de services de protection des données hébergés en tant que service SaaS 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 BlueXP offre des fonctionnalités de protection des données pour les applications. Elle est accessible depuis l'interface utilisateur BlueXP.
- BlueXP Connector est un composant qui s'exécute dans votre réseau cloud 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 BlueXP communique avec le service SaaS BlueXP qui, lors de la validation, traite la demande de la même manière. 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.

> L'infrastructure SaaS BlueXP est résiliente aux défaillances des zones 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.

Protection des bases de données Oracle

Caractéristiques

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

  Vous pouvez déployer le plug-in à l'aide de l'interface utilisateur, du script ou manuellement.

- Découverte automatique des bases de données Oracle

- Sauvegarde des bases de données Oracle hébergées sur Amazon FSX pour NetApp ONTAP, Cloud Volumes ONTAP et Azure NetApp Files
  - 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. Vous pouvez également spécifier les post-scripts qui seront exécutés après la sauvegarde réussie pour copier le snapshot sur le stockage secondaire.
- Les sauvegardes de bases de données Oracle sur Azure NetApp Files peuvent être cataloguées à l'aide d'Oracle RMAN
- Conservation des sauvegardes en fonction de la stratégie appliquée
- Restauration de bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP, Cloud Volumes ONTAP et Azure NetApp Files
  - Restauration de la base de données Oracle complète (fichiers de données + fichier de contrôle) 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
- Restauration des bases de données Oracle sur Azure NetApp Files vers un autre emplacement
- Clonage des bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP et Cloud Volumes ONTAP vers 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
- Mettez à niveau le plug-in hôte

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 est en panne ou si vous ne pouvez pas accéder à l'IP, les opérations de protection des données 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.

Protection des bases de données SAP HANA

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

Protégez la base de données Microsoft SQL Server

Caractéristiques

- Ajoutez manuellement l'hôte et déployez le plug-in
- Découvrir les bases de données manuellement
- Sauvegardez les instances SQL Server résidant sur Amazon FSX pour NetApp ONTAP
  - Sauvegarde à la demande
  - Sauvegarde planifiée basée sur la règle
  - Sauvegarde des journaux de l'instance de Microsoft SQL Server
- Restaurez la base de données à son emplacement d'origine

Limites

- La sauvegarde est prise en charge uniquement pour les instances SQL Server
- La configuration de l'instance de cluster de basculement (FCI) n'est pas prise en charge
- L'interface utilisateur BlueXP ne prend pas en charge les opérations spécifiques à une base de données SQL

  Toutes les opérations spécifiques à la base de données Microsoft SQL Server s'effectuent en exécutant des API REST.

- La restauration vers un autre emplacement n'est pas prise en charge

Sauvegarde des bases de données Oracle cloud natives

Démarrage rapide

Suivez ces étapes pour démarrer rapidement.

1 Vérifiez la prise en charge de votre configuration

- Système d'exploitation :
  - RHEL 7.5 ou version ultérieure et 8.x
  - OL 7.5 ou version ultérieure et 8.x
  - SLES 15 SP4
- Stockage cloud NetApp :
  - Amazon FSX pour NetApp ONTAP
  - Cloud Volumes ONTAP
  - Azure NetApp Files
- Disposition du stockage :
  - NFS v3 et v4.1 (y compris dNFS)
  - ISCSI avec ASM (ASMFD, ASMLib et ASMUdev)

> Azure NetApp Files ne prend pas en charge l'environnement SAN.

- 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 : 19c et 21c

2 Inscrivez-vous à BlueXP

BlueXP est accessible depuis une console web. Lorsque vous commencez à utiliser BlueXP, vous commencez par vous inscrire à l'aide de vos identifiants du site du support NetApp ou en créant un identifiant de connexion cloud NetApp. Pour plus d'informations, reportez-vous à la section "Inscrivez-vous à BlueXP".

3 Connectez-vous à BlueXP

Une fois que vous vous êtes inscrit à BlueXP, vous pouvez vous connecter à partir de la console web. Pour plus d'informations, reportez-vous à la section "Connectez-vous à BlueXP".

4 Gestion de votre compte BlueXP

Vous pouvez gérer votre compte en gérant les utilisateurs, les comptes de service, les espaces de travail et les connecteurs. Pour plus d'informations, reportez-vous à la section "Gestion de votre compte BlueXP".

Configurer FSX pour ONTAP

Avec BlueXP, vous devez créer un environnement de travail FSX pour ONTAP afin d'ajouter et de gérer des volumes et des services de données supplémentaires. Vous devez également créer un connecteur dans AWS permettant à BlueXP de gérer les ressources et les processus dans votre environnement de cloud public.

Créer un environnement de travail FSX pour ONTAP

Vous devez créer les environnements de travail 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 l'environnement de travail FSX pour ONTAP 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 compte doit créer un connecteur dans AWS permettant à BlueXP de gérer les ressources et les processus dans 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 et les bases de données FSX pour ONTAP.
- Si vous disposez de l'environnement de travail FSX pour ONTAP et des bases de données dans le même cloud privé virtuel (VPC), vous pouvez déployer le connecteur dans le même VPC.
- Si vous disposez de l'environnement de travail FSX pour ONTAP et de bases de données dans différents VPC :
  - Si des workloads NAS (NFS) sont configurés sur FSX for ONTAP, vous pouvez créer le connecteur sur l'un des VPC.
  - Si seules des charges de travail SAN sont configurées et que vous n'envisagez pas d'utiliser de charges de travail NAS (NFS), créez le connecteur dans le VPC où le système FSX pour ONTAP est créé.

> Pour l'utilisation de workloads NAS (NFS), vous devez disposer d'une passerelle de transit entre le VPC de la base de données et Amazon VPC. 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** > **My Working Environments** > **Add Working Environment** et suivez les invites pour ajouter l'environnement de travail. Assurez-vous qu'il existe une connectivité entre le connecteur et les hôtes de base de données Oracle et 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.

- Ajoutez l'environnement de travail en cliquant sur **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment**.

  Assurez-vous qu'il y a une connectivité entre le connecteur et les hôtes de base de données et l'environnement de travail FSX pour ONTAP. Le connecteur doit se connecter à l'adresse IP de gestion du

cluster de l'environnement de travail FSX pour ONTAP.

- Copiez l'ID du connecteur en cliquant sur **connecteur > gérer les connecteurs** et en sélectionnant le nom du connecteur.

Configurez Cloud Volumes ONTAP

Avec BlueXP, vous devez créer un environnement de travail Cloud Volumes ONTAP pour ajouter et gérer des volumes et des services de données supplémentaires. Vous devez également créer un connecteur pour votre environnement cloud permettant à BlueXP de gérer les ressources et les processus au sein de votre environnement de cloud public.

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 sections 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 Cloud Volumes ONTAP et les bases de données.

- Si votre environnement de travail Cloud Volumes ONTAP et vos bases de données se trouvent dans le même cloud privé virtuel (VPC) ou vnet, vous pouvez déployer le connecteur sur le même VPC ou vnet.
- Si vous disposez de l'environnement de travail Cloud Volumes ONTAP et des bases de données dans différents VPC ou réseaux virtuels, assurez-vous que les VPC ou les réseaux sont associés.

Configurez Azure NetApp Files

Avec BlueXP, vous devez créer un environnement de travail Azure NetApp Files pour ajouter et gérer des volumes et des services de données supplémentaires. Vous devez également créer un connecteur dans Azure permettant à BlueXP de gérer les ressources et les processus dans votre environnement de cloud public.

Créer un environnement de travail Azure NetApp Files

Vous devez créer des environnements de travail Azure NetApp Files dans lesquels vos bases de données sont hébergées. 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 compte BlueXP doit déployer un connecteur dans Azure qui permet à BlueXP de gérer les ressources et les processus dans votre environnement de cloud public.

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

- Assurez-vous qu'il y a une connectivité entre le connecteur et les hôtes de la base de données.
- Si vous disposez de l'environnement de travail Azure NetApp Files et des bases de données sur le même réseau virtuel (vnet), vous pouvez déployer le connecteur dans le même vnet.
- Si l'environnement de travail Azure NetApp Files et les bases de données se trouvent dans différents réseaux virtuels et que les charges de travail NAS (NFS) sont configurées sur Azure NetApp Files, vous pouvez créer le connecteur sur l'un des réseaux virtuels.

Après avoir créé le connecteur, ajoutez l'environnement de travail en cliquant sur **Storage** > **Canvas** > **Mes environnements de travail** > **Ajouter un environnement de travail**.

Installez le plug-in SnapCenter pour Oracle et ajoutez des hôtes de base de données

Vous devez installer le plug-in SnapCenter pour Oracle sur chacun des hôtes de base de données Oracle, ajouter les hôtes de base de données et découvrir les bases de données sur l'hôte pour attribuer des règles et créer des sauvegardes.

- Si SSH est activé pour l'hôte de base de données, vous pouvez installer le plug-in à l'aide de l'une des méthodes suivantes :
  - Installez le plug-in et ajoutez l'hôte à partir de l'interface utilisateur à l'aide de l'option SSH. En savoir plus >>.
  - Installez le plug-in à l'aide du script et ajoutez l'hôte à partir de l'interface utilisateur à l'aide de l'option manuelle. En savoir plus >>.
- Si SSH est désactivé, installez le plug-in manuellement et ajoutez l'hôte à partir de l'interface utilisateur à l'aide de l'option Manual. En savoir plus >>.

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.
- Vérifiez que le connecteur est connecté aux hôtes de base de données Oracle.

  Pour plus d'informations sur la résolution du problème de connectivité, reportez-vous à la section "Échec de validation de la connectivité entre l'hôte du connecteur BlueXP et l'hôte de la base de données d'applications".

  Lorsque le connecteur est perdu ou si vous avez créé un nouveau connecteur, vous devez associer le connecteur aux ressources d'application existantes. Pour obtenir des instructions sur la mise à jour du connecteur, reportez-vous à la section "Mettre à jour les détails du connecteur".

- Assurez-vous que l'utilisateur BlueXP a le rôle "Admin compte".
- Assurez-vous que le compte non racine (sudo) est présent sur l'hôte d'application pour les opérations de protection des données.
- 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.
- Assurez-vous que la communication du connecteur est activée sur le port SSH (par défaut : 22) si l'installation basée sur SSH est effectuée.

- Assurez-vous que la communication du connecteur est activée sur le port enfichable (par défaut : 8145) pour que les opérations de protection des données fonctionnent.
- Assurez-vous que la dernière version du plug-in est installée. Pour mettre à niveau le plug-in, reportez-vous à la section Mettez à niveau le plug-in SnapCenter pour bases de données Oracle.

Ajoutez l'hôte à partir de l'interface utilisateur à l'aide de l'option SSH

Étapes

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

   Si vous avez déjà ajouté un hôte et souhaitez en ajouter un autre, cliquez sur **applications** > **gérer les bases de données** > **Ajouter**, puis passez à l'étape 5.

2. Cliquez sur **découvrir les applications**.
3. Sélectionnez **Cloud Native** et cliquez sur **Next**.

   Un compte de service (*SnapCenter-account-<accountid>*) associé au rôle *SnapCenter System* est créé pour effectuer des opérations de protection des données planifiées pour tous les utilisateurs de ce compte. Le compte de service (*SnapCenter-account-<accountid>*) est utilisé pour exécuter les opérations de sauvegarde planifiées. Vous ne devez jamais supprimer le compte de service. Vous pouvez afficher le compte de service en cliquant sur **compte** > **gérer compte** > **membres**.

4. Sélectionnez Oracle comme type d'application.
5. Dans la page Détails de l'hôte, effectuez les opérations suivantes :

   a. Sélectionnez **utilisant SSH**.
   b. Spécifiez le FQDN ou l'adresse IP de l'hôte où vous souhaitez installer le plug-in.

      Assurez-vous que le connecteur peut communiquer avec l'hôte de la base de données à l'aide du nom de domaine complet ou de l'adresse IP.

   c. Spécifiez l'utilisateur non-root(sudo) utilisant lequel le module de plug-in sera copié sur l'hôte.

      L'utilisateur root n'est pas pris en charge.

   d. Spécifiez le port SSH et le port du plug-in.

      Le port SSH par défaut est 22 et le port du plug-in est 8145.

   Vous pouvez fermer le port SSH sur l'hôte de l'application après avoir installé le plug-in. Le port SSH n'est pas requis pour des opérations de protection des données.

   a. Sélectionnez le connecteur.
   b. (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.

      > La clé privée SSH n'est stockée nulle part dans l'application et n'est utilisée pour aucune autre opération.

   c. Cliquez sur **Suivant**.
6. Dans la page Configuration, effectuez les opérations suivantes :

a. Configurez l'accès sudo pour l'utilisateur SnapCenter dans l'hôte de base de données Oracle en vous connectant à la machine Linux exécutant la base de données Oracle.
b. Copiez le texte affiché dans l'interface utilisateur BlueXP.
c. Créez le fichier */etc/sudoers.d/snapcenter* sur la machine Linux et collez le texte copié.
d. Dans l'interface utilisateur BlueXP, cochez la case et cliquez sur **Suivant**.

7. Passez en revue les détails et cliquez sur **découvrir les applications**.
   - Une fois le plug-in installé, l'opération de découverte démarre.
   - Une fois l'opération de découverte terminée, toutes les bases de données de l'hôte s'affichent. Si l'authentification du système d'exploitation est désactivée pour la base de données, cliquez sur **configurer** pour activer l'authentification de la base de données. Pour plus d'informations, reportez-vous à la section Configurer les informations d'identification de la base de données Oracle.
   - Cliquez sur **Paramètres** et sélectionnez **hôtes** pour afficher tous les hôtes.
   - Cliquez sur **Paramètres** et sélectionnez **stratégies** pour afficher les stratégies prédéfinies. Examinez les règles prédéfinies et vous pouvez les modifier pour répondre à vos besoins ou créer une nouvelle police.

Ajoutez l'hôte à partir de l'interface utilisateur à l'aide de l'option manuelle et installez le plug-in à l'aide du script

Configurez l'authentification basée sur une clé SSH pour le compte utilisateur non-root de l'hôte Oracle et effectuez les étapes suivantes pour installer le plug-in.

Avant de commencer

Assurez-vous que la connexion SSH au connecteur est activée.

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 (*SnapCenter-account-<accountid>*) associé au rôle *SnapCenter System* est créé pour effectuer des opérations de protection des données planifiées pour tous les utilisateurs de ce compte. Le compte de service (*SnapCenter-account-<accountid>*) est utilisé pour exécuter les opérations de sauvegarde planifiées. Vous ne devez jamais supprimer le compte de service. Vous pouvez afficher le compte de service en cliquant sur **compte** > **gérer compte** > **membres**.

4. Sélectionnez Oracle comme type d'application.
5. Dans la page Détails de l'hôte, effectuez les opérations suivantes :
   a. Sélectionnez **Manuel**.
   b. Spécifiez le nom de domaine complet ou l'adresse IP de l'hôte sur lequel le plug-in est installé.

      Assurez-vous que le connecteur peut communiquer avec l'hôte de la base de données à l'aide du nom de domaine complet ou de l'adresse IP.

   c. Spécifiez le port du plug-in.

      Le port par défaut est 8145.

d. Spécifiez l'utilisateur non-root (sudo) qui utilisera le package de plug-in pour le copier sur l'hôte.
e. Sélectionnez le connecteur.
f. Cochez la case pour confirmer que le plug-in est installé sur l'hôte.
g. Cliquez sur **Suivant**.

6. Dans la page Configuration, effectuez les opérations suivantes :
   a. Configurez l'accès sudo pour l'utilisateur SnapCenter dans l'hôte de base de données Oracle en vous connectant à la machine Linux exécutant la base de données Oracle.
   b. Copiez le texte affiché dans l'interface utilisateur BlueXP.
   c. Créez le fichier */etc/sudoers.d/snapcenter* sur la machine Linux et collez le texte copié.
   d. Dans l'interface utilisateur BlueXP, cochez la case et cliquez sur **Suivant**.
7. Connectez-vous à la machine virtuelle du connecteur.
8. Installez le plug-in à l'aide du script fourni dans le connecteur.

```
sudo /var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

   Si vous utilisez un connecteur plus ancien, exécutez la commande suivante pour installer le plug-in.

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

Nom	Description	Obligatoire	Valeur par défaut
hôte_plugin	Spécifie l'hôte Oracle	Oui.	-
nom_utilisateur_hôte	Spécifie l'utilisateur SnapCenter avec des privilèges SSH sur l'hôte Oracle	Oui.	-
host_ssh_key	Spécifie la clé SSH de l'utilisateur SnapCenter et est utilisée pour se connecter à l'hôte Oracle	Oui.	-
plugin_port	Spécifie le port utilisé par le plug-in	Non	8145
port_ssh_hôte	Spécifie le port SSH sur l'hôte Oracle	Non	22

   Par exemple :

   - `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.`

```
sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk
```

- `sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

9. Dans l'interface utilisateur BlueXP, consultez les détails et cliquez sur **découvrir les applications**.
   - Une fois l'opération de découverte terminée, toutes les bases de données de l'hôte s'affichent. Si l'authentification du système d'exploitation est désactivée pour la base de données, cliquez sur **configurer** pour activer l'authentification de la base de données. Pour plus d'informations, reportez-vous à la section Configurer les informations d'identification de la base de données Oracle.
   - Cliquez sur **Paramètres** et sélectionnez **hôtes** pour afficher tous les hôtes.
   - Cliquez sur **Paramètres** et sélectionnez **stratégies** pour afficher les stratégies prédéfinies. Examinez les règles prédéfinies et vous pouvez les modifier pour répondre à vos besoins ou créer une nouvelle police.

Ajoutez l'hôte à partir de l'interface utilisateur à l'aide de l'option manuelle et installez le plug-in manuellement

Si l'authentification basée sur une clé SSH n'est pas activée sur l'hôte de base de données Oracle, vous devez effectuer les étapes manuelles suivantes pour installer le plug-in, puis ajouter l'hôte à partir de l'interface utilisateur à l'aide de l'option manuelle.

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 (*SnapCenter-account-<accountid>*) associé au rôle *SnapCenter System* est créé pour effectuer des opérations de protection des données planifiées pour tous les utilisateurs de ce compte. Le compte de service (*SnapCenter-account-<accountid>*) est utilisé pour exécuter les opérations de sauvegarde planifiées. Vous ne devez jamais supprimer le compte de service. Vous pouvez afficher le compte de service en cliquant sur **compte** > **gérer compte** > **membres**.

4. Sélectionnez Oracle comme type d'application.
5. Dans la page **Détails de l'hôte**, effectuez les opérations suivantes :
   a. Sélectionnez **Manuel**.
   b. Spécifiez le nom de domaine complet ou l'adresse IP de l'hôte sur lequel le plug-in est installé.

      Assurez-vous que le connecteur peut communiquer avec l'hôte de base de données à l'aide du FQDN ou de l'adresse IP.

   c. Spécifiez le port du plug-in.

      Le port par défaut est 8145.

   d. Spécifiez l'utilisateur sudo non-root (sudo) qui utilisera le package de plug-in pour le copier sur l'hôte.
   e. Sélectionnez le connecteur.
   f. Cochez la case pour confirmer que le plug-in est installé sur l'hôte.

g. Cliquez sur **Suivant**.

6. Dans la page Configuration, effectuez les opérations suivantes :
   a. Configurez l'accès sudo pour l'utilisateur SnapCenter dans l'hôte de base de données Oracle en vous connectant à la machine Linux exécutant la base de données Oracle.
   b. Copiez le texte affiché dans l'interface utilisateur BlueXP.
   c. Créez le fichier */etc/sudoers.d/snapcenter* sur la machine Linux et collez le texte copié.
   d. Dans l'interface utilisateur BlueXP, cochez la case et cliquez sur **Suivant**.
7. Connectez-vous à la machine virtuelle du connecteur.
8. 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'
   ```
   Le fichier binaire du plug-in est disponible à l'adresse suivante : *cd /var/lib/docker/volumes/service-Manager[1]-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po « cloudmanager_scs_cloud:.*? "|sed -e's/ *$/"|cut -f2 -d":")/sc-linux-host-plugin*
9. Copiez *snapcenter_linux_host_plugin_scs.bin* depuis le chemin ci-dessus vers */home/<non root user (sudo)>/.sc_netapp* path pour chacun des hôtes de base de données Oracle à l'aide de scp ou d'autres méthodes alternatives.
10. Connectez-vous à l'hôte de base de données Oracle à l'aide du compte non-root (sudo).
11. Remplacez le répertoire par */home/<non root user>/.sc_netapp/* et exécutez la commande suivante pour activer les autorisations d'exécution pour le binaire.
    ```
    chmod +x snapcenter_linux_host_plugin_scs.bin
    ```
12. Installez le plug-in Oracle en tant qu'utilisateur sudo SnapCenter.
    ```
    ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
    ```
13. Copiez *certificate.pem* de *<base_mount_path>/client/certificate/* chemin de la machine virtuelle du connecteur vers */var/opt/snapcenter/spl/etc/* sur l'hôte du plug-in.
14. Accédez à */var/opt/snapcenter/spl/etc* et exécutez la commande keytool pour importer le fichier certificate.pem.
    ```
    keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
    -deststorepass snapcenter -noprompt
    ```
15. Redémarrer SPL : `systemctl restart spl`
16. Vérifier que le plug-in est accessible depuis le connecteur en exécutant la commande ci-dessous à partir du connecteur.
    ```
    docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
    plug-in host>:<plug-in port>/PluginService/Version --cert
    /config/client/certificate/certificate.pem --key
    /config/client/certificate/key.pem
    ```
17. Dans l'interface utilisateur BlueXP, consultez les détails et cliquez sur **découvrir les applications**.
    - Une fois l'opération de découverte terminée, toutes les bases de données de l'hôte s'affichent. Si l'authentification du système d'exploitation est désactivée pour la base de données, cliquez sur **configurer** pour activer l'authentification de la base de données. Pour plus d'informations, reportez-vous à la section Configurer les informations d'identification de la base de données Oracle.
    - Cliquez sur **Paramètres** et sélectionnez **hôtes** pour afficher tous les hôtes.
    - Cliquez sur **Paramètres** et sélectionnez **stratégies** pour afficher les stratégies prédéfinies. Examinez

les règles prédéfinies et vous pouvez les modifier pour répondre à vos besoins ou créer une nouvelle police.

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

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

Étapes

1. Si l'authentification du système d'exploitation est désactivée pour la base de données, cliquez sur **configurer** pour modifier l'authentification de la base de données.
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**.

Mettez à niveau le plug-in SnapCenter pour bases de données Oracle

Il est conseillé de mettre à niveau le plug-in SnapCenter pour Oracle pour accéder aux nouvelles fonctionnalités et améliorations les plus récentes. Vous pouvez effectuer une mise à niveau à partir de l'interface utilisateur BlueXP ou à l'aide de la ligne de commande.

Avant de commencer

- Assurez-vous qu'aucune opération n'est en cours d'exécution sur l'hôte.

Étapes

1. Cliquez sur **sauvegarde et récupération** > **applications** > **hôtes**.
2. Vérifiez si la mise à niveau du plug-in est disponible pour l'un des hôtes en cochant la colonne État global.
3. Mettez à niveau le plug-in à partir de l'interface utilisateur ou à l'aide de la ligne de commande.

Mise à niveau avec l'interface utilisateur	Mise à niveau à l'aide de la ligne de commande

a. Cliquez sur ••• Correspondant à l'hôte et cliquez sur **Upgrade Plug-in**.
b. Dans la page Configuration, effectuez les opérations suivantes :
i. Configurez l'accès sudo pour l'utilisateur SnapCenter dans l'hôte de base de données Oracle en vous connectant à la machine Linux exécutant la base de données Oracle.
ii. Copiez le texte affiché dans l'interface utilisateur BlueXP.
iii. Modifiez le fichier */etc/sudoers.d/snapcenter* sur la machine Linux et collez le texte copié.
iv. Dans l'interface utilisateur BlueXP, cochez la case et cliquez sur **mettre à niveau**.
	a. Connectez-vous à Connector VM.
	b. Exécutez le script suivant.
	`sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`
	Si vous utilisez un connecteur plus ancien, exécutez la commande suivante pour mettre à niveau le plug-in.
	`sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`

Sauvegarde des bases de données Oracle cloud natives

Vous pouvez créer des sauvegardes planifiées ou à la demande en attribuant une règle prédéfinie ou la règle que vous avez créée.

Vous pouvez également cataloguer les sauvegardes de bases de données Oracle à l'aide d'Oracle Recovery Manager (RMAN) si vous avez activé le catalogage lors de la création d'une stratégie. Le catalogage (RMAN) est pris en charge uniquement pour les bases de données qui se trouvent sur Azure NetApp Files. Les sauvegardes cataloguées peuvent être utilisées ultérieurement pour les opérations de restauration au niveau des blocs ou de restauration à un point dans le temps de l'espace de stockage. La base de données doit être montée ou supérieure pour le catalogage.

Créez une règle pour protéger la base 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. Si vous avez sélectionné *Daily* et *Weekly* comme planning et que vous souhaitez activer le catalogage RMAN, sélectionnez **Catalog backup with Oracle Recovery Manager (RMAN)**.
7. (Facultatif) Entrez le chemin d'accès et le délai d'expiration du post-script qui seront exécutés après la sauvegarde réussie, comme la copie de l'instantané sur le stockage secondaire.

   Vous pouvez également spécifier les arguments.

   Vous devez conserver les post-scripts dans le chemin */var/opt/snapcenter/spl/scripts*.

   Le script post prend en charge un ensemble de variables d'environnement.

Variable d'environnement	Description
SC_ORACLE_SID	Spécifie le SID de la base de données Oracle.
SC_HÔTE	Spécifie le nom d'hôte de la base de données
SC_BACKUP_NAME	Spécifie le nom de la sauvegarde. Le nom de la sauvegarde des données et le nom de la sauvegarde du journal sont concaténés à l'aide de délimiteurs.
SC_BACKUP_POLICY_NAME	Spécifie le nom de la stratégie utilisée pour créer la sauvegarde.
SC_PRIMARY_DATA_VOLUME_FULL_PATH	Spécifie les chemins de volume de données concaténés avec "," comme délimiteur. Pour les volumes Azure NetApp Files, les informations sont concaténées à l'aide de « / ». _ /Abonnements/{subscription_ID}/resourceGroups/{Resource_group}/providers/{Provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumes/{volumName}_
SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH	Spécifie les chemins du volume du journal d'archives concaténés avec "," comme délimiteur. Pour les volumes Azure NetApp Files, les informations sont concaténées avec « / ». _ /Abonnements/{subscription_ID}/resourceGroups/{Resource_group}/providers/{Provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumes/{volumName}_

8. Cliquez sur **Créer**.

Configurer le référentiel de catalogue RMAN

Vous pouvez configurer la base de données du catalogue de restauration en tant que référentiel du catalogue RMAN. Si vous ne configurez pas le référentiel, par défaut, le fichier de contrôle de la base de données cible devient le référentiel de catalogue RMAN.

Avant de commencer

Vous devez enregistrer manuellement la base de données cible dans la base de données du catalogue RMAN.

Étapes

1. Dans la page applications, cliquez sur ••• > **Afficher les détails**.
2. Dans la section Détails de la base de données, cliquez sur Pour configurer le référentiel du catalogue RMAN.
3. Spécifiez les informations d'identification pour cataloguer les sauvegardes avec RMAN et le nom TNS (transparent Network Substrate) de la base de données de restauration de catalogue.
4. Cliquez sur **configurer**.

Créez une sauvegarde de la base de données Oracle

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

> Lors de la création de groupes de disques ASM sur Amazon FSX pour NetApp ONTAP ou Cloud Volumes ONTAP, assurez-vous qu'il n'y a pas de volumes communs à tous les groupes de disques. Chaque groupe de disques doit avoir des 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. Si vous avez activé le catalogue RMAN dans la règle, la sauvegarde à la fin du flux de travail lance l'opération de catalogage comme tâche séparée. La progression du catalogage est visible à partir du moniteur de tâches. Une fois le catalogage réussi, **Backup Details** affiche l'état du catalogue pour chaque sauvegarde.

   > Le compte de service (*SnapCenter-account-<account_id>*) est utilisé pour exécuter les 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 attribuées à l'application, sélectionnez la stratégie, le niveau de rétention, puis cliquez sur **Créer une sauvegarde**.

   Si vous avez activé le catalogue RMAN dans la règle, la sauvegarde à la fin du flux de travail lance l'opération de catalogage comme tâche séparée. La progression du catalogage est visible à partir du moniteur de tâches. Une fois le catalogage réussi, **Backup Details** affiche l'état du catalogue pour chaque sauvegarde.

Limites

- 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 sur Amazon FSX pour NetApp ONTAP ou Cloud Volumes ONTAP et configurées sur ASM, assurez-vous que vos noms de SVM sont uniques entre 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.
- 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".

Sauvegarde des bases de données SAP HANA cloud natives

Démarrage rapide

Suivez ces étapes pour démarrer rapidement.

1 Vérifiez la prise en charge de votre configuration

- Système d'exploitation :
  - RHEL 7.6 ou version ultérieure
  - RHEL 8.1 ou version ultérieure pour SAP-HANA SPS07
  - SLES 12 SP5 ou version ultérieure et plates-formes SPX 15 certifiées par SAP HANA
- Stockage cloud NetApp : Azure NetApp Files
- Dispositions de stockage : pour les fichiers de données et de journaux, Azure prend uniquement en charge NFSv4.1.
- Dispositions de la base de données :
  - SAP HANA Multitenant Database Container (MDC) 2.0SPS5, 2.0SPS6, 2.0SPS7 avec un ou plusieurs

locataires

  - Système hôte unique SAP HANA, système hôte multiple SAP HANA, réplication système HANA
- Plug-in SAP HANA sur l'hôte de base de données

2 Inscrivez-vous à BlueXP

BlueXP est accessible depuis une console web. Lorsque vous commencez à utiliser BlueXP, vous commencez par vous inscrire à l'aide de vos identifiants du site du support NetApp ou en créant un identifiant de connexion cloud NetApp. Pour plus d'informations, reportez-vous à la section "Inscrivez-vous à BlueXP".

3 Connectez-vous à BlueXP

Une fois que vous vous êtes inscrit à BlueXP, vous pouvez vous connecter à partir de la console web. Pour plus d'informations, reportez-vous à la section "Connectez-vous à BlueXP".

4 Gestion de votre compte BlueXP

Vous pouvez gérer votre compte en gérant les utilisateurs, les comptes de service, les espaces de travail et les connecteurs. Pour plus d'informations, reportez-vous à la section "Gestion de votre compte BlueXP".

Configurez Azure NetApp Files

Avec BlueXP, vous devez créer un environnement de travail Azure NetApp Files pour ajouter et gérer des volumes et des services de données supplémentaires. Vous devez également créer un connecteur dans Azure permettant à BlueXP de gérer les ressources et les processus dans votre environnement de cloud public.

Créer un environnement de travail Azure NetApp Files

Vous devez créer des environnements de travail Azure NetApp Files dans lesquels vos bases de données sont hébergées. 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 compte BlueXP doit déployer un connecteur dans Azure qui permet à BlueXP de gérer les ressources et les processus dans votre environnement de cloud public.

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

- Assurez-vous qu'il y a une connectivité entre le connecteur et les hôtes de la base de données.
- Si vous disposez de l'environnement de travail Azure NetApp Files et des bases de données sur le même réseau virtuel (vnet), vous pouvez déployer le connecteur dans le même vnet.
- Si l'environnement de travail Azure NetApp Files et les bases de données se trouvent dans différents réseaux virtuels et que les charges de travail NAS (NFS) sont configurées sur Azure NetApp Files, vous pouvez créer le connecteur sur l'un des réseaux virtuels.

Après avoir créé le connecteur, ajoutez l'environnement de travail en cliquant sur **Storage** > **Canvas** > **Mes environnements de travail** > **Ajouter un environnement de travail**.

Installez le plug-in SnapCenter pour SAP HANA et ajoutez des hôtes de base de données

Vous devez installer 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 suivantes pour installer le plug-in.

- Si SSH est activé pour l'hôte de base de données, vous pouvez installer le plug-in à l'aide de l'option SSH. En savoir plus >>.
- Si SSH est désactivé, installez le plug-in manuellement. En savoir plus >>.

Prérequis

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

- Assurez-vous que Java 11 (64 bits) Oracle Java ou OpenJDK est installé sur chacun des hôtes de base de données SAP HANA.
- Vous devez avoir ajouté l'environnement de travail et créé le connecteur.
- Vérifiez que le connecteur est connecté aux hôtes de base de données SAP HANA.

  Pour plus d'informations sur la résolution du problème de connectivité, reportez-vous à la section "Échec de validation de la connectivité entre l'hôte du connecteur BlueXP et l'hôte de la base de données d'applications".

  Lorsque le connecteur est perdu ou si vous avez créé un nouveau connecteur, vous devez associer le connecteur aux ressources d'application existantes. Pour obtenir des instructions sur la mise à jour du connecteur, reportez-vous à la section "Mettre à jour les détails du connecteur".

- Assurez-vous que l'utilisateur BlueXP a le rôle "Admin compte".
- Vous devez avoir créé l'utilisateur SnapCenter et configuré sudo pour l'utilisateur non-root (sudo). Pour plus d'informations, reportez-vous à la section "Configurez sudo pour l'utilisateur SnapCenter."
- Vous devez avoir installé le plug-in SnapCenter pour SAP HANA avant d'ajouter l'hôte de base de données.
- 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.

  Le nom d'hôte doit être identique à celui de l'hôte utilisé dans la réplication HSR.

- Assurez-vous que la communication du connecteur est activée sur le port SSH (par défaut : 22) si l'installation basée sur SSH est effectuée.
- Assurez-vous que la communication du connecteur est activée sur le port enfichable (par défaut : 8145) pour que les opérations de protection des données fonctionnent.
- Assurez-vous que la dernière version du plug-in est installée. Pour mettre à niveau le plug-in, reportez-vous à la section Mettez à niveau le plug-in SnapCenter pour les bases de données SAP HANA.

Configurez sudo pour l'utilisateur SnapCenter

Créez un utilisateur non-root (sudo) pour installer 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. Copiez le contenu de **sudoer.txt** situé à : */var/lib/docker/volumes/service-Manager-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po « cloudmanager_scs_cloud:.*? "|sed -e's/ *$/'|cut -f2 -d":")/sc-linux-host-plugin*
4. Connectez-vous à l'hôte du système SAP HANA à l'aide d'un compte utilisateur root.
5. Configurez l'accès sudo pour l'utilisateur non root en copiant le texte copié à l'étape 3 dans */etc/sudoers.d/snapcenter* file.

   Dans les lignes ajoutées au fichier */etc/sudoers.d/snapcenter*, remplacez *<LINUXUSER>* par l'utilisateur non-root et *<USER_HOME_DIRECTORY>* par *Home/<non-root-user>*.

Installez le plug-in à l'aide du script

Configurez l'authentification basée sur une clé SSH pour le compte utilisateur non root de l'hôte SAP HANA et effectuez les étapes suivantes pour installer le plug-in.

Avant de commencer

Assurez-vous que la connexion SSH au connecteur est activée.

Étapes

1. Connectez-vous à Connector VM.
2. Installez le plug-in à l'aide du script fourni dans le connecteur.
   ```
   sudo bash /var/lib/docker/volumes/service-manager-
   2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
   --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
   --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

   Si vous utilisez un connecteur plus ancien, exécutez la commande suivante pour installer le plug-in.
   ```
   sudo
   /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
   in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
   --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

Nom	Description	Obligatoire	Valeur par défaut
hôte_plugin	Spécifie l'hôte SAP HANA	Oui.	-

Nom	Description	Obligatoire	Valeur par défaut
nom_utilisateur_hôte	Spécifie l'utilisateur SnapCenter avec des privilèges SSH sur l'hôte SAP HANA	Oui.	-
host_ssh_key	Spécifie la clé SSH de l'utilisateur SnapCenter et est utilisée pour se connecter à l'hôte SAP HANA	Oui.	-
plugin_port	Spécifie le port utilisé par le plug-in	Non	8145
port_ssh_hôte	Spécifie le port SSH sur l'hôte SAP HANA	Non	22

Par exemple, `sudo bash /var/lib/docker/volumes/service-Manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username SnapCenter --sshkey /keys/netapp-ssh.ppk

Après avoir installé le plug-in, vous devez Ajouter des hôtes de base de données SAP HANA.

Installez le plug-in manuellement

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

Étapes

1. Connectez-vous à Connector VM.
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'
   ```

   Le fichier binaire du plug-in est disponible à l'adresse suivante : *cd /var/lib/docker/volumes/service-Manager-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po « cloudmanager_scs_cloud:.*? "|sed -e's/ *$/"|cut -f2 -d":")/sc-linux-host-plugin*
3. Copiez *snapcenter_linux_host_plugin_scs.bin* depuis le chemin ci-dessus vers */home/<non root user (sudo)>/.sc_netapp* path pour chacun des hôtes de base de données SAP HANA à l'aide de scp ou d'autres méthodes alternatives.
4. Connectez-vous à l'hôte de base de données SAP HANA à l'aide du compte non-root (sudo).
5. Remplacez le répertoire par */home/<non root user>/.sc_netapp/* et exécutez la commande suivante pour activer les autorisations d'exécution pour le binaire.
   ```
   chmod +x snapcenter_linux_host_plugin_scs.bin
   ```
6. Installez le plug-in SAP HANA en tant qu'utilisateur sudo SnapCenter.
   ```
   ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
   ```

7. Copiez *certificate.pem* de *<base_mount_path>/client/certificate/* chemin de la machine virtuelle du connecteur vers */var/opt/snapcenter/spl/etc/* sur l'hôte du plug-in.
8. Accédez à */var/opt/snapcenter/spl/etc* et exécutez la commande keytool pour importer le certificat.
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
   -deststorepass snapcenter -noprompt
   ```
9. Redémarrer SPL : `systemctl restart spl`
10. Vérifier que le plug-in est accessible depuis le connecteur en exécutant la commande ci-dessous à partir du connecteur.
    ```
    docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
    plug-in host>:<plug-in port>/PluginService/Version --cert
    config/client/certificate/certificate.pem --key
    /config/client/certificate/key.pem
    ```

Après avoir installé le plug-in, vous devez Ajouter des hôtes de base de données SAP HANA.

Mettez à niveau le plug-in SnapCenter pour les bases de données SAP HANA

Vous devez mettre à niveau le plug-in SnapCenter pour la base de données SAP HANA pour accéder aux nouvelles fonctionnalités et améliorations les plus récentes.

Avant de commencer

- Assurez-vous qu'aucune opération n'est en cours d'exécution sur l'hôte.

Étapes

1. Configurez sudo pour l'utilisateur SnapCenter. Pour plus d'informations, reportez-vous à la section Configurez sudo pour l'utilisateur SnapCenter.
2. Exécutez le script suivant.
   ```
   /var/lib/docker/volumes/service-manager-
   2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
   --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
   --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
   ```

   Si vous utilisez un connecteur plus ancien, exécutez la commande suivante pour mettre à niveau le plug-in.
   ```
   /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
   in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
   --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   --upgrade
   ```

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.

Étapes

1. Dans l'interface utilisateur **BlueXP**, sélectionnez **protection** > **sauvegarde et récupération** > **applications**.

2. Sélectionnez **découvrir les applications**.
3. Sélectionnez **Cloud Native** > **SAP HANA** et sélectionnez **Next**.
4. Dans la page **applications**, sélectionnez **Ajouter un système**.
5. Dans la page **Détails du système**, effectuez les opérations suivantes :

   a. Sélectionnez le type de système en tant que conteneur de base de données mutualisé ou volumes globaux non-données.

   b. Entrez le nom du système SAP HANA.

   c. Spécifier le SID du système SAP HANA.

   d. (Facultatif) Modifier l'utilisateur OSDB.

   e. Si le système HANA est configuré avec la réplication système HANA, activez **HANA System Replication (HSR) System**.

   f. Sélectionnez la zone de texte **HDB Secure User Store Keys** pour ajouter des détails sur les clés de stockage utilisateur.

      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. Sélectionnez **Suivant**.
7. Sur la page **Détails de l'hôte**, effectuez les opérations suivantes :

   a. Sélectionnez **Ajouter un nouvel hôte** ou **utiliser un hôte existant**.

   b. Sélectionnez **à l'aide de SSH** ou **Manuel**.

      Pour Manuel, saisissez le nom de domaine complet ou l'adresse IP de l'hôte, le connecteur, le nom d'utilisateur, le port SSH, le port du plug-in, et éventuellement ajouter et valider la clé privée SSH.

   Pour SSH, entrez le nom de domaine complet ou l'adresse IP de l'hôte, le connecteur, le nom d'utilisateur et le port du plug-in.

   a. Sélectionnez **Suivant**.

8. Sur la page **Configuration de l'hôte**, vérifiez si les exigences de configuration sont respectées.

   Cochez les cases pour confirmer.

9. Sélectionnez **Suivant**.
10. Sur la page **empreinte de stockage**, sélectionnez **Ajouter stockage** et effectuez les opérations suivantes :

    a. Sélectionnez l'environnement de travail et spécifiez le compte NetApp.

       Dans le volet de navigation de gauche, sélectionnez BlueXP **Canvas** pour ajouter un nouvel environnement de travail.

    b. Sélectionnez les volumes requis.

    c. Sélectionnez **Ajouter un stockage**.

11. Passez en revue tous les détails et sélectionnez **Ajouter un système**.

Vous pouvez modifier ou supprimer les systèmes SAP HANA de l'interface utilisateur.

Avant de supprimer le système SAP HANA, vous devez supprimer toutes les sauvegardes associées et supprimer la protection.

Ajouter des volumes non-données

Après avoir ajouté le système SAP HANA de type conteneur de base de données mutualisée, vous pouvez ajouter les volumes non-données du système HANA.

Vous pouvez ajouter ces ressources aux groupes de ressources pour effectuer des opérations de protection des données après avoir découvert les bases de données SAP HANA disponibles.

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 système SAP HANA de type conteneur de base de données mutualisé, vous pouvez ajouter les volumes mondiaux non-données 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.
6. . Sur la page **Détails de l'hôte**, effectuez les opérations suivantes :
   a. Spécifiez les SID associés du système SAP HANA.
   b. Sélectionnez l'hôte du plug-in
   c. Cliquez sur **Suivant**.
   d. Vérifiez tous les détails et cliquez sur **Ajouter système**.

Sauvegarde des bases de données SAP HANA cloud natives

Vous pouvez créer une sauvegarde en attribuant une règle prédéfinie ou la règle que vous avez créée.

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. "Scripts d'examen préliminaire et de post-script."
8. Cliquez sur **Créer**.

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 protection des données.

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` fichier.

```
[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 flux de travail de sauvegarde, les variables d'environnement suivantes sont disponibles dans le cadre du prescripteur et du postscript.

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

Variable d'environnement	Description
type_programme	Uniquement pour sauvegarde planifiée

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.

Avant de commencer

Vous devez avoir ajouté les hôtes de base de données SAP HANA."Ajouter des hôtes de base de données SAP HANA"

À propos de cette tâche

Pour la réplication système HANA (HSR), la tâche de sauvegarde planifiée ne se déclenche que pour le système HANA principal. 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 affectée au système HANA principal et secondaire, la planification échoue après le basculement.

Si des règles différentes sont attribuées aux systèmes HSR, la sauvegarde planifiée déclenche à la fois pour les systèmes HANA principaux et secondaires et la sauvegarde échoue 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**.

   Bien que la base de données soit protégée à l'aide d'une ou de plusieurs stratégies, vous pouvez, si nécessaire, continuer à affecter d'autres stratégies en cliquant sur ••• > **affecter stratégie**.

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

   Les sauvegardes sont créées conformément au calendrier défini dans la règle.

   > Le compte de service (*SnapCenter-account-<account_id>*) est utilisé pour exécuter les 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 cliquer 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.

   Pour plus d'informations, voir "Prescripts et Postscripts"

c. Cliquez sur **Créer une sauvegarde**.

Sauvegardez vos bases de données SQL Server natives du cloud à l'aide d'API REST

Démarrage rapide

Suivez ces étapes pour démarrer rapidement.

1 Vérifiez la prise en charge de votre configuration

- Système d'exploitation :
  - Windows 2016
  - Windows 2019
  - Windows 2022
- Stockage cloud NetApp : Amazon FSX pour NetApp ONTAP
- Disposition du stockage : SAN (ISCSI)

  La configuration NAS n'est pas prise en charge.

- Versions de la base de données :
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2019
  - Microsoft SQL Server 2022
- Configuration de la base de données :
  - Autonome

2 Inscrivez-vous à BlueXP

BlueXP est accessible depuis une console web. Lorsque vous commencez à utiliser BlueXP, vous commencez par vous inscrire à l'aide de vos identifiants du site du support NetApp ou en créant un identifiant de connexion cloud NetApp. Pour plus d'informations, reportez-vous à la section "Inscrivez-vous à BlueXP".

3 Connectez-vous à BlueXP

Une fois que vous vous êtes inscrit à BlueXP, vous pouvez vous connecter à partir de la console web. Pour plus d'informations, reportez-vous à la section "Connectez-vous à BlueXP".

4 Gestion de votre compte BlueXP

Vous pouvez gérer votre compte en gérant les utilisateurs, les comptes de service, les espaces de travail et les connecteurs. Pour plus d'informations, reportez-vous à la section "Gestion de votre compte BlueXP".

Configurer FSX pour ONTAP

Avec BlueXP, vous devez créer un environnement de travail FSX pour ONTAP afin d'ajouter et de gérer des volumes et des services de données supplémentaires. Vous devez également créer un connecteur dans AWS permettant à BlueXP de gérer les ressources et les processus dans votre environnement de cloud public.

Créer un environnement de travail FSX pour ONTAP

Vous devez créer les environnements de travail 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 l'environnement de travail FSX pour ONTAP 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 compte doit créer un connecteur dans AWS permettant à BlueXP de gérer les ressources et les processus dans 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 et les bases de données FSX pour ONTAP.
- Si vous disposez de l'environnement de travail FSX pour ONTAP et des bases de données dans le même cloud privé virtuel (VPC), vous pouvez déployer le connecteur dans le même VPC.
- Si vous disposez de l'environnement de travail FSX pour ONTAP et de bases de données dans différents VPC :
  - Si des workloads NAS (NFS) sont configurés sur FSX for ONTAP, vous pouvez créer le connecteur sur l'un des VPC.
  - Si seules des charges de travail SAN sont configurées et que vous n'envisagez pas d'utiliser de charges de travail NAS (NFS), créez le connecteur dans le VPC où le système FSX pour ONTAP est créé.

> Pour l'utilisation de workloads NAS (NFS), vous devez disposer d'une passerelle de transit entre le VPC de la base de données et Amazon VPC. 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** > **My Working Environments** > **Add Working Environment** et suivez les invites pour ajouter l'environnement de travail. Assurez-vous qu'il existe une connectivité entre le connecteur et les hôtes de base de données Oracle et 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.

- Ajoutez l'environnement de travail en cliquant sur **Storage** > **Canvas** > **My Working Environments** > **Add Working Environment**.

  Assurez-vous qu'il y a une connectivité entre le connecteur et les hôtes de base de données et l'environnement de travail FSX pour ONTAP. Le connecteur doit se connecter à l'adresse IP de gestion du cluster de l'environnement de travail FSX pour ONTAP.

- Copiez l'ID du connecteur en cliquant sur **connecteur > gérer les connecteurs** et en sélectionnant le nom du connecteur.

Installez le plug-in SnapCenter pour SQL Server et ajoutez des hôtes de base de données

Vous devez installer le plug-in SnapCenter pour SQL Server sur chacun des hôtes de base de données SQL, ajouter les hôtes de base de données, découvrir les instances de base de données et configurer les informations d'identification pour les instances de base de données.

Installez le plug-in SnapCenter pour SQL Server

Vous devez télécharger le plug-in **snapcenter_service_Windows_host_plugin.exe**, puis exécuter la commande Silent installer pour installer le plug-in sur l'hôte de base de données.

Avant de commencer

- Vous devez vous assurer que les conditions préalables suivantes sont remplies.
  - .Net 4.7.2 est installé
  - PowerShell 4.0 est installé
  - Un espace disque minimum de 5 Go est disponible
  - La taille minimale de la mémoire RAM est de 4 Go
- Vous devez exécuter l'API pour terminer l'intégration du client. Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Tenant%20Registration/createTenant

Étapes

1. Téléchargez le plug-in en exécutant l'API à partir de l'hôte du connecteur.
   ```
   docker exec -it cloudmanager_scs_cloud curl
   'http://127.0.0.1/api/v2/pluginpackage/windows'
   ```

   L'emplacement du fichier est */var/lib/docker/volumes/service-Manager-2_cloudmanager_scs_cloud_volume/_data/<agent_version>/sc-Windows-host-plugin/snapcenter_service_Windows_host_plugin.exe*.

2. Copiez *snapcenter_service_Windows_host_plugin.exe* depuis le connecteur vers chacun des hôtes de base de données du serveur MSSQL à l'aide de scp ou d'autres méthodes alternatives.

3. Installez le plug-in.
   '"C://<install_folder>/snapcenter_service_Windows_host_plugin.exe"/silent/debuglog "C://<install_folder>/HA_Suite_Silent_Install_SCSQL_FRESH.log" /log"C://install_folder/" BI_SNAPCENTER_PORT=8145 ISFeatureInstall=SCSQL'

4. Copiez le certificat auto-signé depuis */var/lib/docker/volumes/service-Manager-2_cloudmanager_scs_cloud_volume/_data/client/certificat/certificate.pem* vers les hôtes de base de

données du serveur MSSQL.

Vous pouvez également générer un certificat auto-signé ou un certificat signé par une autorité de certification si vous n'utilisez pas le certificat par défaut.

5. Convertissez le certificat du format .pem au format .crt dans l'hôte du connecteur.
   'openssl x509 -outform der -in certificate.pem -out certificate.crt'
6. Double-cliquez sur le certificat pour l'ajouter au magasin **personnel** et **autorités de certification racines de confiance**.

Ajoutez l'hôte de base de données SQL Server

Vous devez ajouter l'hôte de la base de données MSSQL à l'aide du nom de domaine complet de l'hôte.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/AddHosts

Cette API crée un travail qui peut être suivi à partir de l'onglet **Job Monitor** de l'interface utilisateur BlueXP.

Paramètres

Nom	Type	Obligatoire
adr	chaîne	Vrai
id_connecteur	chaîne	Vrai
type_plugin	chaîne	Vrai
méthode_installation	chaîne	Vrai
plugin_port	numéro	Vrai
nom d'utilisateur	chaîne	Vrai

Réponse

Si l'API est exécutée avec succès, le code de réponse 202 s'affiche.

Exemple :

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Afficher les hôtes de base de données SQL Server ajoutés

Vous pouvez exécuter cette API pour afficher tous les hôtes de base de données SQL Server ajoutés.

'OBTENEZ snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/GetHosts

Réponse

Si l'API est exécutée avec succès, le code de réponse 200 s'affiche.

Exemple :

```
{
  "num_records": 1,
    "total_records": 1,
    "records": [
        {
            "id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "addr": "scspa2722211001.rtp.openenglab.netapp.com",
            "status": "Running",
            "connector_id": "fBf8Iwbp4BscBfD02qBwWm6I03gGAesRclients",
            "plugin_port": 8145,
            "plugins": [
                {
                    "type": "mssql"
                }
            ],
            "os_type": "windows",
            "platform": "onprem",
            "username": "administrator",
            "operating_mode": "production"
        }
    ],
    "_links": {
        "next": {}
    }
}
```


Découvrir les instances de base de données

Vous pouvez exécuter cette API et entrer l'ID d'hôte pour découvrir toutes les instances MSSQL.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/discovery'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/MSSQLInstancesDiscoveryRequest

Cette API crée un travail qui peut être suivi à partir de l'onglet **Job Monitor** de l'interface utilisateur BlueXP.

Paramètre

Nom	Type	Obligatoire
id_hôte	chaîne	Vrai

Réponse

Si l'API est exécutée avec succès, le code de réponse 202 s'affiche.

Exemple :

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Afficher les instances de base de données découvertes

Vous pouvez exécuter cette API pour afficher toutes les instances de base de données découvertes.

'OBTENEZ snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/GetMSSQLInstancesRequest

Réponse

Si l'API est exécutée avec succès, le code de réponse 200 s'affiche.

Exemple :

```
{
    "num_records": 2,
    "total_records": 2,
    "records": [
        {
            "id": "953e66de-10d9-4fd9-bdf2-bf4b0eaabfd7",
            "name": "scspa2722211001\\NAMEDINSTANCE1",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Running",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        },
        {
            "id": "18e1b586-4c89-45bd-99c8-26268def787c",
            "name": "scspa2722211001",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Stopped",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        }
    ],
    "_links": {
        "next": {}
    }
}
```


Configurez les informations d'identification de l'instance de base de données

Vous pouvez exécuter cette API pour valider et définir les informations d'identification des instances de base de données.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql//api/mssql/credentials-configuration'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/ConfigureCredentialRequest

Cette API crée un travail qui peut être suivi à partir de l'onglet **Job Monitor** de l'interface utilisateur BlueXP.

Paramètre

Nom	Type	Obligatoire
id_hôte	chaîne	Vrai
id_instance	chaîne	Vrai
nom d'utilisateur	chaîne	Vrai
mot de passe	chaîne	Vrai
auth_mode	chaîne	Vrai

Réponse

Si l'API est exécutée avec succès, le code de réponse 202 s'affiche.

Exemple :

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Sauvegarde des bases de données Microsoft SQL Server cloud natives

Vous pouvez créer des sauvegardes planifiées ou à la demande en attribuant les stratégies que vous avez créées.

Création d'une règle de sauvegarde

Vous pouvez exécuter cette API pour créer la règle de sauvegarde.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backup/policies'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backup%20Policies/MSSQLBackupPolicyService_CreateMSSQLBackupPolicy

Cette API crée un travail qui peut être suivi à partir de l'onglet **Job Monitor** de l'interface utilisateur BlueXP.

Paramètres

Nom	Type	Obligatoire
nom	chaîne	Vrai
type_sauvegarde	chaîne	Vrai
copie_seule_sauvegarde	chaîne	Faux
est_système_défini	chaîne	Faux
backup_name_format	chaîne	Vrai
type_programme	chaîne	Vrai
heure_de_début	numéro	Vrai
heures_intervalle	numéro	Vrai
intervalle_minutes	numéro	Vrai
retention_type	chaîne	Vrai
retention_count	numéro	Vrai
heure_de_fin	numéro	Vrai

Réponse

Si l'API est exécutée avec succès, le code de réponse 201 s'affiche.

Exemple :

```
{
    "_links": {
    "self": {
        "href": "/api/resourcelink"
      }
    }
}
```

Attribuez une règle à une instance de base de données SQL

Vous pouvez exécuter cette API pour affecter une règle à une instance de base de données SQL.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/{id}/policy-assignment'

Où, *ID* est l'ID d'instance MSSQL obtenu en exécutant l'API d'instance de la base de données de découverte. Pour plus d'informations, reportez-vous à la section "Découvrir les instances de base de données".

Le tableau d'ID est la saisie ici. Par exemple :

```
[
  "c9f3e68d-1f9c-44dc-b9af-72a9dfc54320"
]
```

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Policy%20Assignment/PostMSSQLInstanceAssignPolicyRequest

Cette API crée un travail qui peut être suivi à partir de l'onglet **Job Monitor** de l'interface utilisateur BlueXP.

Réponse

Si l'API est exécutée avec succès, le code de réponse 202 s'affiche.

Exemple :

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Créez une sauvegarde à la demande

Vous pouvez exécuter cette API pour créer une sauvegarde à la demande.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/CreateMSSQLBackupRequest

Cette API crée un travail qui peut être suivi à partir de l'onglet **Job Monitor** de l'interface utilisateur BlueXP.

Paramètres

Nom	Type	Obligatoire
id Il s'agit de l'ID de l'instance de base de données MSSQL.	chaîne	Vrai
type_ressource	chaîne	Vrai
id_règle	chaîne	Vrai
type_programme	chaîne	Vrai

Réponse

Si l'API est exécutée avec succès, le code de réponse 202 s'affiche.

Exemple :

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Afficher les sauvegardes

Vous pouvez exécuter ces API pour afficher la liste de toutes les sauvegardes et les détails d'une sauvegarde spécifique.

'OBTENEZ snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups'

'OBTENEZ snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups/{id}'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/MSSQLGetBackupsRequest

Réponse

Si l'API est exécutée avec succès, le code de réponse 200 s'affiche.

Exemple :

```
{
    "total_records": 1,
    "num_records": 1,
    "records": [
        {
            "backup_id": "602d7796-8074-43fc-a178-eee8c78566ac",
            "resource_id": "a779578d-cf78-46f3-923d-b9223255938c",
            "backup_name":
"Hourly_policy2_scspa2722211001_NAMEDINSTANCE1_2023_08_08_07_02_01_81269_0
",
            "policy_name": "policy2",
            "schedule_type": "Hourly",
            "start_time": "2023-08-08T07:02:10.203Z",
            "end_time": "0001-01-01T00:00:00Z",
            "backup_status": "success",
            "backup_type": "FullBackup"
        }
    ],
    "_links": {
        "next": {}
    }
}
```


Restaurez des bases de données Oracle cloud natives

Restaurez des bases de données Oracle cloud à leur emplacement d'origine

En cas de perte de données, vous pouvez restaurer les fichiers de données, les fichiers de contrôle ou les deux à leur emplacement d'origine, puis récupérer la base de données.

Avant de commencer

Si la base de données Oracle 21c est à l'état DÉMARRÉ, l'opération de restauration échoue. Vous devez exécuter la commande suivante 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 **Restaurer**.
2. Sélectionnez le point de restauration vers lequel la base de données doit être restaurée et cliquez sur **Restaurer à l'emplacement d'origine**.
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**.

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

Dans l'infrastructure SAN d'Amazon FSX pour NetApp ONTAP ou de Cloud Volumes ONTAP, 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 connexion et de restauration des copies 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 **tous les journaux**.
Que vous souhaitez récupérer à un numéro de changement de système (SCN) spécifique	Sélectionnez **jusqu'à SCN** 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**.

Restaurez des bases de données Oracle cloud natives vers un autre emplacement

En cas de perte de données, vous pouvez restaurer la base de données Oracle à un autre emplacement uniquement sur Azure NetApp Files. L'autre emplacement peut se trouver sur un hôte différent ou sur le même hôte.

Avant de commencer

- Si la base de données Oracle 21c est à l'état DÉMARRÉ, l'opération de restauration échoue. Vous devez exécuter la commande suivante 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
  ```
- Vous devez vous assurer que la version d'Oracle sur l'hôte secondaire est identique à celle de l'hôte d'origine.

Description de la tâche

Lors du lancement de l'opération de restauration, vous n'êtes pas autorisé à modifier les configurations, à l'exception du répertoire racine Oracle, du débit de volume maximal, de la SID Oracle et des informations d'identification de la base de données.

La récupération complète est activée par défaut avec *jusqu'à ce que Cancel* soit défini sur true.

Le mode de journalisation des archives est désactivé par défaut pour la base de données restaurée. Vous pouvez activer le mode log d'archivage et conserver les journaux d'archivage sur le volume NetApp si nécessaire.

Étapes

1. Cliquez sur ••• Correspondant à la base de données à restaurer et cliquez sur **Restaurer**.
2. Sélectionnez le point de restauration auquel la base de données doit être restaurée et cliquez sur **Restaurer à un autre emplacement** > **Suivant**.
3. Dans la page Configuration, spécifiez les détails de l'emplacement secondaire, SID, Oracle_Home, les informations d'identification de la base de données et le débit de stockage.

   Pour les informations d'identification de la base de données, si l'authentification utilisateur du système d'exploitation est désactivée, vous devez fournir un mot de passe pour que l'utilisateur sys puisse se connecter à la base de données restaurée sur le même hôte ou sur l'hôte cible.

4. Cliquez sur **Suivant**, passez en revue les détails et cliquez sur **Restaurer**.

   La progression de l'opération de restauration peut être affichée dans la page surveillance des travaux. Une fois le travail terminé, cliquez sur **Actualiser la découverte** pour afficher la base de données restaurée. Toutefois, vous ne pouvez pas protéger la base de données restaurée à un autre emplacement.

Restaurez des bases de données SAP HANA cloud natives

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

Avant de commencer

- Le système SAP HANA doit être dans un état arrêté.
- Si le système SAP HANA est en cours d'exécution, vous pouvez fournir un médecin pour arrêter le système.

À propos de cette tâche

- Si vous activez les sauvegardes ANF sur un volume, une opération SnapRestore à fichier unique est effectuée.
- Pour les volumes non-données et les volumes non-données globaux, une opération de restauration de connexion et de copie est effectuée.
  - Les valeurs de qualité de service (QoS) pour l'opération de connexion et de restauration de copie sont récupérées sur les volumes source des volumes non-données ou des volumes non-données globaux.

> La QoS s'applique uniquement aux pools de capacité de type « Manuel ».

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 que vous souhaitez restaurer et cliquez sur **Restaurer**.
3. Dans la page **Restore System**, entrez les scripts. "Scripts d'examen préliminaire et de post-script."

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

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

4. Cliquez sur **Restaurer**.

Quoi de neuf

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

À propos de cette tâche

Pour une opération de connexion et de restauration de copie, accédez au portail Microsoft Azure, sélectionnez le volume, cliquez sur **Modifier** et activez **Masquer le chemin de l'instantané**.

Étapes

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

À propos de cette tâche

Pour une opération de connexion et de restauration de copie, accédez au portail Microsoft Azure, sélectionnez le volume, cliquez sur **Modifier** et activez **Masquer le chemin de l'instantané**.

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**.

Restaurez la base de données Microsoft SQL Server

Vous pouvez restaurer la base de données Microsoft SQL Server sur le même hôte. Vous devez d'abord obtenir la liste des bases de données, puis restaurer la base de données.

Afficher la liste des bases de données

Vous pouvez exécuter cette API pour afficher la liste des bases de données.

'OBTENEZ snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases'

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Databases/GetMSSQLDatabasesRequest

Réponse

Si l'API est exécutée avec succès, le code de réponse 200 s'affiche.

Exemple :

```
{
    "num_records": 3,
    "total_records": 3,
    "records": [
        {
            "id": "348901e5-aeaa-419f-88b1-80240de3b1fe",
            "name": "DB4",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "c79d33ab-7322-4ed6-92f5-51ad7a6944e0",
            "name": "DB5",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "40d6f35a-f4fb-48bc-8e0a-0ac93ddf0888",
            "name": "model",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.015625,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "System",
            "recovery_mode": "Full"
        }
    ],
    "_links": {
        "next": {}
    }
}
```

Restaurez et restaurez la base de données MSSQL

Vous pouvez exécuter cette API pour restaurer la base de données MSSQL.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases/{id}/restore'

Où, *ID* est l'ID de base de données MSSQL obtenu en exécutant l'API de base de données View. Pour plus d'informations, reportez-vous à la section Afficher la liste des bases de données.

Pour plus d'informations, se reporter à : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Database%20Restore/RestoreMSSQLDatabaseRequest

Cette API crée un travail qui peut être suivi à partir de l'onglet **Job Monitor** de l'interface utilisateur BlueXP.

Paramètres

Nom	Type	Obligatoire
id_sauvegarde	chaîne	Vrai
ecraser_database	bool	Vrai
paramètres_de_réplication_de_conservation	bool	Faux
recovery_mode	chaîne Les 3 chaînes prises en charge sont *Operational*, *nonoperationnel* et *ReadOnly*.	Vrai
dossier_fichier_d'annulation	chaîne	Vrai
restore_type	chaîne	Vrai

Réponse

Si l'API est exécutée avec succès, le code de réponse 202 s'affiche.

Exemple :

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Clonez des bases de données Oracle cloud natives

Concepts et conditions de clonage

Vous pouvez cloner une base de données Oracle résidant sur Amazon FSX pour NetApp ONTAP ou Cloud Volumes ONTAP en utilisant la sauvegarde de la base de données soit sur l'hôte de base de données source, soit 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
  - ORCL:* si vous utilisez ASMLIB
  - /Dev/<exact_device_location> si vous utilisez ASMUDEV
- 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.
  - Le logiciel Oracle 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

- Le clonage des bases de données résidant sur Azure NetApp Files n'est pas pris en charge.
- Le clonage des bases de données résidant sur qtree n'est pas pris en charge.
- La sauvegarde d'une base de données clonée n'est pas prise en charge.
- Si des sauvegardes automatiques quotidiennes sont activées sur Amazon FSX pour NetApp ONTAP, les volumes clonés sur Amazon FSX pour NetApp ONTAP ne peuvent pas être supprimés de l'interface utilisateur BlueXP, car FSX aurait créé des sauvegardes sur les volumes clonés.
  Vous devez supprimer les volumes clonés après la suppression de toutes les sauvegardes du volume dans l'interface utilisateur FSX, puis supprimer les clones de l'option force de l'interface utilisateur BlueXP.

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.

Paramètre	Description
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
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 *mm/jj/aaaa hh:mm:ss*.

Paramètre	Description
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.
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 **Clone SID**.
- Si vous avez sélectionné la méthode du fichier de spécifications, le suffixe sera le suffixe **Suffix** 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 spécifie 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_scro2417819002_07-20- 2021_1,RG2_scspr24819002_07-21-2021_12.16.48.9267_spri1_07_22_2021_12.16.48.9267_12.16.48.9267_1__1_spri1
- 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 cloud natives

Vous pouvez cloner une base de données Oracle résidant sur Amazon FSX pour NetApp ONTAP ou Cloud Volumes ONTAP en utilisant la sauvegarde de la base de données soit sur l'hôte de base de données source, soit 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.

Avant de commencer

Vous devez comprendre les concepts de clonage et vous assurer que toutes les conditions sont remplies. "En savoir plus >>".

Étapes

1. Cliquez sur ••• Correspondant à la base de données à cloner et cliquer 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…
De base	a. Sélectionnez l'hôte clone. 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. b. Spécifiez la SID du clone. c. Sélectionnez la structure de nommage des clones. 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. d. Spécifiez le chemin d'accès à Oracle Home. e. (Facultatif) spécifiez les informations d'identification de la base de données. ◦ Informations d'identification de la base de données : si l'authentification utilisateur du système d'exploitation est désactivée, vous devez fournir un mot de passe pour que l'utilisateur sys puisse se connecter à la base de données clonée sur le même hôte ou sur l'hôte cible. ◦ 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. ⓘ Assurez-vous que l'écouteur est actif et fonctionne sur l'hôte cible. f. Cliquez sur **Suivant**. g. Cliquez sur **Clone**.

Si vous avez sélectionné…	Procédez comme ça…
Fichier de spécifications	a. Cliquez sur **Télécharger le fichier** pour télécharger le fichier de spécifications. b. Sélectionnez la structure de nommage des clones. Si vous sélectionnez **généré automatiquement**, vous devez spécifier le suffixe. c. Modifiez le fichier de spécifications selon les besoins et téléchargez-le en cliquant sur le bouton **Parcourir**. d. Sélectionnez l'hôte clone. 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. e. Spécifiez la SID du clone. f. (Facultatif) spécifiez les informations d'identification de la base de données. ◦ Informations d'identification de la base de données : si l'authentification utilisateur du système d'exploitation est désactivée, vous devez fournir un mot de passe pour que l'utilisateur sys puisse se connecter à la base de données clonée sur le même hôte ou sur l'hôte cible. ◦ 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. ⓘ Assurez-vous que l'écouteur est actif et fonctionne sur l'hôte cible. g. Cliquez sur **Suivant**. h. Cliquez sur **Clone**.

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

Actualisez le système cible SAP HANA

Vous pouvez actualiser un système cible SAP HANA avec les données d'un système source SAP HANA. Il peut être utilisé pour fournir les données de production actuelles dans un système de test. La sauvegarde et la restauration BlueXP vous permettent de sélectionner une copie Snapshot à partir d'un système source et de créer un volume Azure NetApp Files basé sur la copie Snapshot. Des exemples de scripts sont disponibles, qui exécute les opérations requises sur l'hôte de base de données pour restaurer la base de données SAP HANA.

Avant de commencer

- Vous devez installer le système cible SAP HANA avant d'exécuter la première opération d'actualisation.
- Vous devez ajouter manuellement les systèmes HANA source et cible dans la sauvegarde et la restauration BlueXP.
- Vérifiez que la version de la base de données SAP HANA est identique sur le système source et le système cible.
- Vous devez avoir décidé des scripts d'actualisation à utiliser. Les scripts d'actualisation sont disponibles dans le rapport technique de la solution.

  "Scripts d'exemple d'automatisation"

  Vous pouvez personnaliser les scripts d'actualisation.

- Les variables d'environnement suivantes sont disponibles dans le cadre du prescripteur et du postscript :
  - CHEMIN_MONTAGE_VOLUMES_CLONÉS
  - DESTINATION_<SOURCEVOLUME>
  - TYPE_BASE_DE_DONNÉES_HANA
  - NOM_BASE_DE_DONNÉES_LOCATAIRE
- Vous devez mettre à niveau le plug-in vers la version 3.0.
- Les chemins de montage doivent être les mêmes pour le volume de données sur les systèmes SAP HANA source et cible.
- Avant la première opération d'actualisation, assurez-vous que le fichier '/etc/fstab' ne contient pas d'entrées pour les volumes de données du système SAP HANA cible.

À propos de cette tâche

- L'actualisation du système est prise en charge uniquement pour le système HANA de conteneur de base de données mutualisé.
- Les stratégies existantes seront valides après l'actualisation du système.
- Les nouveaux volumes créés auront la nomenclature établie suivante : <sourcevolumename>-<timestamp>
  - Format d'horodatage : <year> <month> <day>-<hour> <minute> <second>

    Par exemple, si le volume source est vol1, le nom du volume actualisé sera vol1-20230109-184501

Le nouveau volume sera placé dans le même pool de capacité que celui des volumes cibles.

- Le chemin de jonction sera le même que le nom du volume.
- Le « nombre maximal de débit » du nouveau volume est sélectionné dans le volume du système cible avec des pools de capacité de qualité de service (QoS) manuels.
  Pour les pools de capacité QoS automatique, le débit est défini par la capacité du volume source.
- Lors de l'actualisation du système, le montage et le démontage automatiques des volumes sont effectués à l'aide de workflows au lieu de scripts.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Dans la page **applications**, cliquez sur ••• Pour sélectionner l'action correspondant au système que vous souhaitez actualiser et sélectionnez **Rafraîchir système**.
3. Dans la page **actualisation du système**, effectuez les opérations suivantes :
   a. Sélectionnez le système source et la copie Snapshot.
   b. (Facultatif) Entrez les adresses d'exportation à partir desquelles les nouveaux volumes sont accessibles.
   c. (Facultatif) Entrez le débit de stockage maximal (MIB).
   d. Saisissez le prescripteur, le postscript et les chemins de script d'échec. Le script en cas d'échec est exécuté uniquement lorsque l'opération d'actualisation du système échoue.
   e. Cliquez sur **Actualiser**.

Gérez la protection des données applicatives cloud

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.

Les tâches planifiées sont répertoriées sur la page de contrôle des tâches BlueXP après un délai de 5 minutes (maximum) à compter de l'heure d'achèvement du travail.

Pour plus d'informations, reportez-vous à la section "Contrôler l'état des tâches".

Maintenance des hôtes de base de données Oracle

Un administrateur peut placer manuellement les hôtes de base de données en mode de maintenance pour effectuer des tâches de maintenance sur les hôtes. Lors de la mise à niveau, les hôtes sont automatiquement mis en mode maintenance et après la mise à niveau, ils sont automatiquement basculés en mode production.

Lorsque les hôtes sont mis en mode maintenance, les opérations à la demande échouent et les tâches planifiées sont ignorées.

Vous ne pouvez pas vérifier si des tâches sont en cours d'exécution pour les ressources sur les hôtes avant de mettre les hôtes en mode de maintenance.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et restauration** > **applications**
2. Sélectionnez **Oracle** comme type d'application.
3. Cliquez sur **Paramètres** > **hôtes**.
4. Effectuez l'une des opérations suivantes :

Si…	Procédez comme ça…
Vous souhaitez placer l'hôte en mode de maintenance	Cliquez sur ••• Correspondant à l'hôte et sélectionnez **Activer le mode de maintenance**.
Souhaite sortir l'hôte du mode de maintenance	Cliquez sur ••• Correspondant à l'hôte en cours de maintenance et sélectionnez **Désactiver le mode de maintenance**.

Données d'audit

Lorsque vous exécutez une API directement ou que vous utilisez l'interface utilisateur pour effectuer l'appel d'API vers l'une des API exposées en externe de la sauvegarde et de la restauration BlueXP pour les applications, les détails de la demande tels que les en-têtes, le rôle, le corps de la demande, Les informations d'API sont consignées dans la chronologie BlueXP et les entrées d'audit sont conservées indéfiniment dans le calendrier. 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.

Les fonctionnalités de sauvegarde et de restauration BlueXP pour les applications consignent les entrées telles que l'adresse IP de l'hôte, le corps de la requête, le nom de l'opération, l'auteur de l'opération, 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.

Étapes

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. Pour plus d'informations, reportez-vous à la section Mettre à jour les détails du connecteur.

Supprimer le clone

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

Étapes

1.

Cliquez sur + À côté de **Filter by** et sélectionnez **Clone options** > **Clone parents**.

2. Cliquez sur ••• Correspondant à l'application et cliquer 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 du connecteur

Vous devez déployer un nouveau connecteur, si le connecteur utilisé lors de l'enregistrement de l'hôte d'application n'existe plus ou est corrompu. 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.

Après avoir mis à jour les détails du connecteur pour les hôtes Oracle ou SAP HANA, procédez comme suit pour vérifier que les détails du connecteur ont été correctement mis à jour.

Étapes

1. Connectez-vous à BlueXP Connector VM et effectuez les opérations suivantes :
   a. Vérifier que le plug-in est accessible depuis le connecteur en exécutant la commande ci-dessous à partir du connecteur.
   ```
   docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the plug-in host>:<plug-in port>/getVersion
   --cert/config/client/certificate/certificate.pem
   --key/config/client/certificate/key.pem
   ```
   b. 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
   ```
   c. Copiez Certificate.pem de *<base_mount_path>/client/certificate/* path de la machine virtuelle du connecteur vers */var/opt/snapcenter/spl/etc/* sur l'hôte du plug-in.
2. Connectez-vous à l'hôte du plug-in et effectuez les opérations suivantes :
   a. Accédez à */var/opt/snapcenter/spl/etc* et exécutez la commande keytool pour importer le fichier certificate.pem.
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks -deststorepass snapcenter -noprompt
   ```
   b. Redémarrer SPL : `systemctl restart spl`
   c. Effectuez l'une des opérations suivantes :

Si vous êtes sur…	Procédez comme ça…
Hôte de base de données Oracle	i. S'assurer que tous les "prérequis" sont satisfaits. ii. Cliquez sur **sauvegarde et récupération** > **applications** iii. Cliquez sur ••• Correspondant à l'application et cliquer sur **Afficher les détails**. iv. Modifier **ID connecteur**.
Hôte de base de données SAP HANA	i. S'assurer que tous les "prérequis" sont satisfaits. ii. Exécutez la commande suivante : `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 des connecteurs seront mis à jour avec succès si le plug-in SnapCenter pour le service SAP HANA est installé et en cours d'exécution sur tous les hôtes, et également 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 BlueXP Connector

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.

Étapes

1. Effectuez les étapes suivantes sur le connecteur pour utiliser le certificat de l'autorité de certification comme certificat client lorsque le connecteur se connecte au plug-in.
   a. Connectez-vous au connecteur.
   b. Exécutez 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
   ```
   c. Supprimez tous les fichiers existants situés dans *<base_mount_path>/client/certificate* dans le connecteur.
   d. Copiez le certificat signé par l'autorité de certification et le fichier de clé dans *<base_mount_path>/client/certificate* dans le 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.

   e. Créez le format PKCS12 du certificat avec le nom certificate.p12 et conservez-le à *<base_mount_path>/client/certificat*.

      Exemple : openssl pkcs12 -inkey key key.pem -in certificate.pem -export -out certificate.p12

2. Procédez comme suit sur l'hôte du plug-in pour valider le certificat envoyé par le connecteur.
   a. Connectez-vous à l'hôte du plug-in.
   b. Copiez le certificat.pem et les certificats de l'autorité de certification intermédiaire et de l'autorité de certification racine du connecteur vers l'hôte du plug-in à l'adresse */var/opt/snapcenter/spl/etc/*.

      Le format du certificat CA intermédiaire et du certificat CA racine doit être au format .crt.

   c. Accédez à */var/opt/snapcenter/spl/etc* et exécutez la commande keytool pour importer le fichier certificate.pem.
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore
   keystore.jks -deststorepass snapcenter -noprompt
   ```
   d. Importer l'autorité de certification racine et les certificats intermédiaires.
   ```
   keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter
   -alias trustedca -file <certificate.crt>
   ```

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

   e. Redémarrer SPL : `systemctl restart spl`

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

Le nom du certificat de l'autorité de certification doit être identique à celui enregistré dans Cloud Backup pour l'hôte du plug-in.

Étapes

1. Procédez comme suit sur l'hôte du plug-in pour héberger le plug-in à l'aide du certificat CA.

   a. Accédez au dossier contenant le keystore 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*.

      Le certificat.pem doit avoir toute la chaîne des certificats comme CA intermédiaire et CA racine.

   Exemple : openssl pkcs12 -inkey key key.pem -in certificate.pem -export -out certificate.p12 -name splkeystore

   a. Ajoutez le certificat d'autorité de certification créé à l'étape ci-dessus.
      ```
      keytool -importkeystore -srckeystore certificate.p12 -srcstoretype pkcs12
      -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore
      -destalias splkeystore -noprompt
      ```

   b. Vérifiez les certificats.
      ```
      keytool -list -v -keystore keystore.jks
      ```

   c. Redémarrer SPL : `systemctl restart spl`

2. Effectuez les étapes suivantes sur le connecteur pour que le connecteur puisse vérifier le certificat du plug-in.

   a. Connectez-vous au connecteur en tant qu'utilisateur non-root.

   b. Exécutez 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
      ```

   c. Copiez les fichiers de l'autorité de certification racine et de l'autorité de certification intermédiaire dans le répertoire du serveur.
      ```
      cd <base_mount_path>
      mkdir server
      ```

      Les fichiers CA doivent être au format pem.

   d. 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
      ```

   e. Redémarrez le conteneur Cloud Manager_scs_Cloud.
      ```
      sudo docker restart cloudmanager_scs_cloud
      ```

Accès aux API REST

Les API REST permettant de protéger les applications dans le cloud sont disponibles dans : https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/.

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".