Sauvegardez les données des applications cloud natives

Cloud Backup

NetApp
December 19, 2022

Table des matières

Sauvegardez les données des applications cloud natives

Sauvegardez les bases de données Oracle cloud natives

Accéder à BlueXP

Vous devriez "Inscrivez-vous au site Web NetApp BlueXP", "Connectez-vous à BlueXP", puis configurez un "Compte NetApp".

Configurer FSX pour ONTAP

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

Créer un environnement de travail FSX pour ONTAP

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

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

Créer un connecteur

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

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

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

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

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

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

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

Configurez Cloud Volumes ONTAP

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

Créer un environnement de travail Cloud Volumes ONTAP

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

Créer un connecteur

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

- "Démarrage rapide de Cloud Volumes ONTAP dans AWS"
- "Démarrage rapide de Cloud Volumes ONTAP dans Azure"
- "Démarrage rapide pour Cloud Volumes ONTAP dans Google Cloud"

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

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

Ajouter l'hôte et découvrir les bases de données Oracle

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

Prérequis

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

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

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

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

Configurer un utilisateur non-racine

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

Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Téléchargez le binaire du plug-in hôte SnapCenter Linux.
   ```
   sudo docker exec -it cloudmanager_scs_cloud curl -X GET
   'http://127.0.0.1/deploy/downloadLinuxPlugin'
   ```
3. Obtenez le chemin de montage de base.
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
   docker volume inspect | grep Mountpoint
   ```
4. Copiez les lignes 1 à 16 à partir du fichier **oracle_checksum_scs.txt** situé à ***base_mount_path*/*version*/sc-linux-host-plugin/**.
5. Connectez-vous à l'hôte de la base de données Oracle et effectuez les opérations suivantes :
   a. Créez le compte utilisateur non-racine, la paire de clés privées et attribuez les autorisations. Pour plus d'informations, reportez-vous à la section "Créez un compte utilisateur".
   b. Collez les lignes que vous avez copiées à l'étape 4 dans le fichier */etc/sudoers* à l'aide de l'utilitaire visudo Linux.

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

Déployez le plug-in manuellement

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

Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Téléchargez le binaire du plug-in hôte SnapCenter Linux.
   ```
   sudo docker exec -it cloudmanager_scs_cloud curl -X GET
   'http://127.0.0.1/deploy/downloadLinuxPlugin'
   ```
3. Obtenez le chemin de montage de base.
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
   docker volume inspect | grep Mountpoint
   ```
4. Obtenez le chemin binaire du plug-in téléchargé.
   ```
   sudo ls <base_mount_path> $(sudo docker ps|grep -Po
   "cloudmanager_scs_cloud:.*? "|sed -e 's/ *$//'|cut -f2 -d":")/sc-linux-host
   ```

`-plugin/snapcenter_linux_host_plugin_scs.bin`

5. Copiez *snapcenter_linux_host_plugin_scs.bin* vers chacun des hôtes de base de données Oracle à l'aide de scp ou d'autres méthodes alternatives.

   Le *snapcenter_linux_host_plugin_scs.bin* doit être copié dans un emplacement accessible par l'utilisateur non-root.

6. Connectez-vous à l'hôte de la base de données Oracle à l'aide du compte utilisateur non-root et exécutez la commande suivante pour activer les autorisations d'exécution pour le binaire.
   `chmod +x snapcenter_linux_host_plugin_scs.bin`
7. Déployez le plug-in Oracle en tant qu'utilisateur non root sudo.
   `./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root-user>`
8. Copiez *certificate.p12* de *<base_mount_path>/client/certificat/* chemin de la machine virtuelle du connecteur vers */var/opt/snapcenter/spl/etc/* sur l'hôte du plug-in.
9. Accédez à */var/opt/snapcenter/spl/etc* et exécutez la commande keytool pour importer le certificat.
   `keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter -deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt`
10. Redémarrer SPL : `systemctl restart spl`

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

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

Étapes

1. Connectez-vous à la machine virtuelle du connecteur.
2. Obtenez le chemin de montage de base.
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`
3. Déployez le plug-in à l'aide du script d'assistance fourni dans le connecteur.
   `sudo <base_mount_path>/scripts/oracle_plugin_copy_and_install.sh --host <host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port> --pluginport <plugin_port> --installdir <install_dir>`
   - Host_name est le nom de l'hôte Oracle et il s'agit d'un paramètre obligatoire.
   - ssh_key_file est la clé SSH de l'utilisateur non-root et utilisée pour se connecter à l'hôte Oracle. Ce paramètre est obligatoire.
   - User_name : utilisateur non-root disposant de privilèges SSH sur l'hôte Oracle et il s'agit d'un paramètre facultatif. La valeur par défaut est EC2-user.
   - ssh_port : port SSH sur l'hôte Oracle et il s'agit d'un paramètre facultatif. La valeur par défaut est 22
   - Plugin_port : port utilisé par le plug-in et il s'agit d'un paramètre facultatif. La valeur par défaut est 8145
   - Dossier_installation : répertoire dans lequel le plug-in sera déployé et il s'agit d'un paramètre facultatif. La valeur par défaut est /opt.

Par exemple :

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

Ajouter hôte

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

Étapes

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

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

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

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

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

Si…	Procédez comme ça…
Ont déployé le plug-in non plus manuellement ou à l'aide du script	a. Sélectionnez **Manuel**. b. Spécifiez le FQDN ou l'adresse IP de l'hôte où le plug-in est déployé. Assurez-vous que le connecteur peut communiquer avec l'hôte de base de données à l'aide du FQDN ou de l'adresse IP. c. Spécifiez le port du plug-in. Le port par défaut est 8145. d. Sélectionnez le connecteur. e. Cochez la case pour confirmer que le plug-in est installé sur l'hôte f. Cliquez sur **découvrir les applications**.

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

- Affiche toutes les bases de données sur l’hôte. Si l’authentification OS est désactivée pour la base de données, vous devez configurer l’authentification de la base de données en cliquant sur configurer. Pour plus d’informations, reportez-vous à la section https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/gcp/Configurer les informations d&.html#8217;identification de la base de données Oracle.
- Cliquez sur **Paramètres** et sélectionnez **hôtes** pour afficher tous les hôtes. Cliquez sur **Supprimer** pour supprimer un hôte de base de données.

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

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

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

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

Étapes

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

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

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

Sauvegardez les bases de données Oracle cloud natives

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

Créez une règle pour protéger les bases de données Oracle

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

Étapes

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

Créez une sauvegarde de la base de données Oracle

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

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

Étapes

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

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

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

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

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

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

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

Étapes

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

Plus d'informations

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

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

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

Limites

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