Sauvegarde des bases de données Oracle cloud natives

BlueXP backup and recovery

NetApp
April 18, 2024

Sommaire

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

Nom	Description	Obligatoire	Valeur par défaut
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".