



Sauvegarde et restauration des données des applications

Cloud Backup

NetApp
November 28, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/concept-protect-app-data-to-cloud.html> on November 28, 2022. Always check docs.netapp.com for the latest.

Table des matières

- Sauvegarde et restauration des données des applications 1
 - Sauvegarde et restauration des données des applications sur site 1
 - Sauvegarde et restauration des données d'applications cloud natives 16

Sauvegarde et restauration des données des applications

Sauvegarde et restauration des données des applications sur site

Protection des données applicatives sur site

Vous pouvez intégrer Cloud Backup pour applications, avec BlueXP (anciennement Cloud Manager) et SnapCenter sur site, pour sauvegarder les snapshots cohérents avec les applications depuis ONTAP sur site vers le cloud. Si nécessaire, vous pouvez restaurer les données depuis le cloud vers un serveur SnapCenter sur site.

Vous pouvez sauvegarder les données des applications Oracle, Microsoft SQL et SAP HANA depuis les systèmes ONTAP sur site vers Amazon Web Services, Microsoft Azure, Google Cloud Platform et StorageGRID.



Vous devez utiliser le logiciel SnapCenter version 4.6 ou ultérieure.

Pour en savoir plus sur Cloud Backup pour applications, consultez :

- ["Sauvegarde intégrant la cohérence applicative avec Cloud Backup et SnapCenter"](#)
- ["Podcast Cloud Backup pour les applications"](#)

De formation

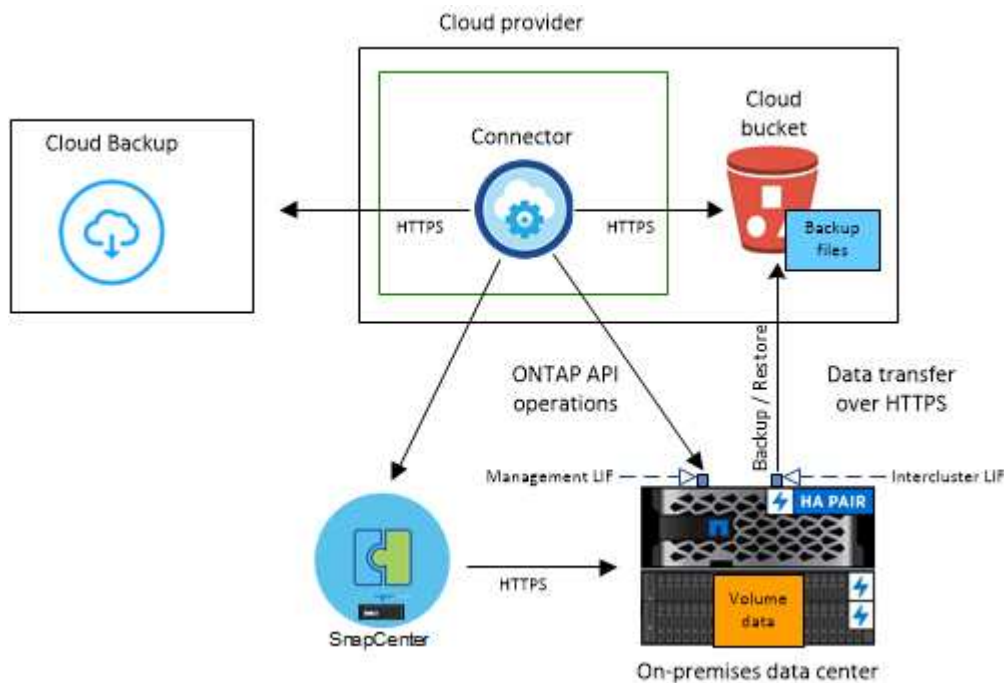
Avant de commencer à sauvegarder les données applicatives sur les services cloud, lisez les informations qui suivent pour vous assurer que la configuration est prise en charge.

- ONTAP 9.8 ou version ultérieure
- BlueXP 3.9
- SnapCenter Server 4.6 ou version ultérieure vous devez utiliser SnapCenter Server 4.7 si vous souhaitez utiliser les fonctions suivantes :
 - protection des sauvegardes depuis les systèmes de stockage secondaire sur site
 - Protégez les applications SAP HANA
 - Protégez les applications Oracle et SQL qui se trouvent sur un environnement VMware
 - montez les sauvegardes
 - désactiver les sauvegardes
 - Annuler l'enregistrement du serveur SnapCenter
- Au moins une sauvegarde par application doit être disponible dans SnapCenter Server
- Au moins une politique quotidienne, hebdomadaire ou mensuelle appliquée dans SnapCenter sans étiquette ni même étiquette que la politique de sauvegarde dans le Cloud dans BlueXP.

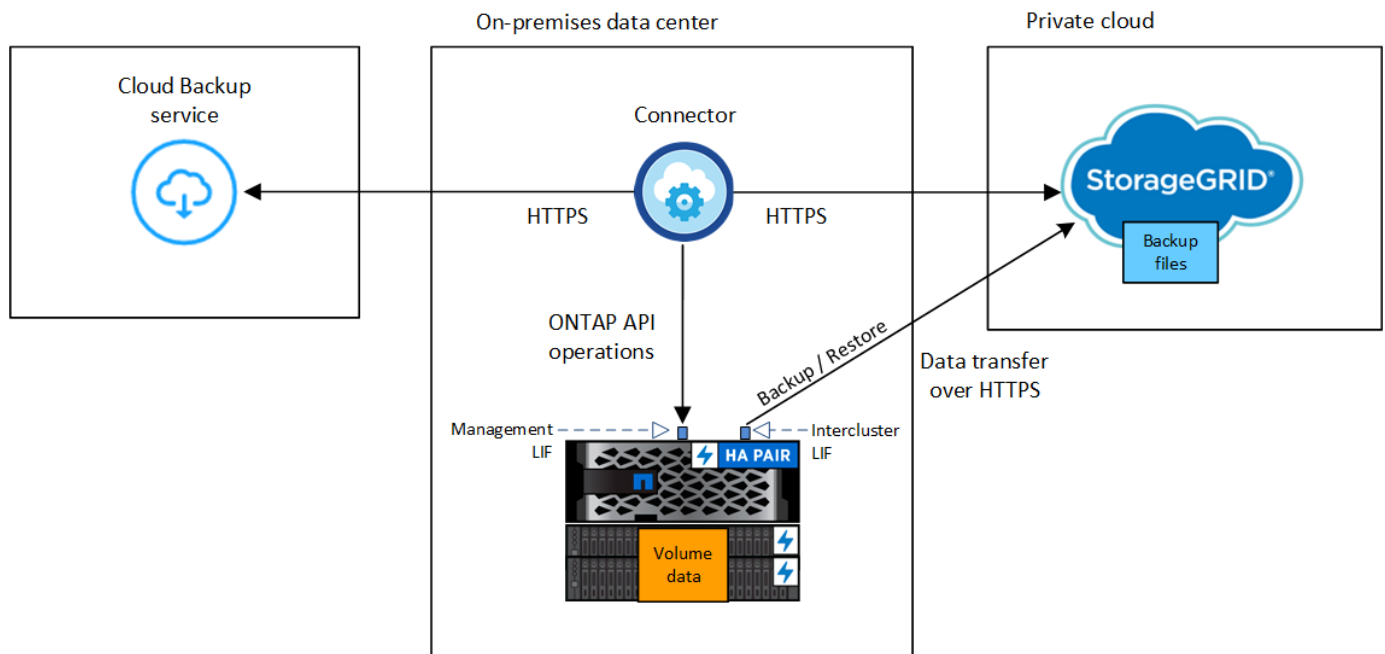


Cloud Backup pour les applications ne prend pas en charge la protection des applications qui se trouvent sur des SVM ajoutés avec un FQDN ou une adresse IP.

L'image suivante montre chaque composant lors de la sauvegarde dans le cloud et les connexions que vous devez préparer de l'un à l'autre :



L'image suivante montre chaque composant lors de la sauvegarde sur StorageGRID et les connexions dont vous avez besoin pour les préparer :



Enregistrez SnapCenter Server

Seul un utilisateur doté du rôle SnapCenterAdmin peut enregistrer l'hôte sur lequel

SnapCenter Server 4.6 ou version ultérieure est exécuté. Vous pouvez enregistrer plusieurs hôtes SnapCenter Server.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **serveurs SnapCenter**.
3. Cliquez sur **Enregistrer le serveur SnapCenter**.
4. Spécifiez les informations suivantes :
 - a. Dans le champ serveur SnapCenter, spécifiez le FQDN ou l'adresse IP de l'hôte du serveur SnapCenter.
 - b. Dans le champ Port, spécifiez le numéro de port sur lequel le serveur SnapCenter s'exécute.

Assurez-vous que le port est ouvert pour la communication entre le serveur SnapCenter et la sauvegarde dans le cloud pour les applications.
 - c. Dans le champ balises, spécifiez un nom de site, un nom de ville ou tout nom personnalisé avec lequel vous souhaitez marquer le serveur SnapCenter.

Les balises sont séparées par une virgule.
 - d. Dans le champ Nom d'utilisateur et Mot de passe, spécifiez les informations d'identification de l'utilisateur avec le rôle SnapCenterAdmin.
5. Cliquez sur **Enregistrer**.

Après la fin

Cliquez sur **Backup & Restore > applications** pour afficher toutes les applications protégées à l'aide de l'hôte serveur SnapCenter enregistré.

Par défaut, les applications sont automatiquement découvertes tous les jours à minuit. Vous pouvez configurer le planning pour détecter les applications.



Pour les bases de données SQL Server, la colonne Nom de l'application affiche le nom au format *nom_de_l'application (nom de l'instance)*.

Les applications prises en charge et leurs configurations sont les suivantes :

- Base de données Oracle :
 - Sauvegardes complètes (données + journal) créées avec au moins une planification quotidienne, hebdomadaire ou mensuelle
 - SAN, NFS, VMDK-SAN, VMDK-NFS ET RDM
- Base de données Microsoft SQL Server :
 - Autonome, basculement d'instances de cluster et groupes de disponibilité
 - Sauvegardes complètes créées avec au moins un planning quotidien, hebdomadaire ou mensuel
 - SAN, VMDK-SAN, VMDK-NFS ET RDM
- Base de données SAP HANA :
 - Conteneur unique 1.x

- Conteneur de bases de données multiples 2.x
- Réplication système HANA (HSR)

Vous devez sauvegarder au moins une sauvegarde sur le site principal et sur les sites secondaires. Vous pouvez décider d'effectuer une défaillance pro-active ou un basculement différé vers le secondaire.

- Les ressources non-data volumes (NDV), telles que les binaires HANA, le volume des journaux d'archives HANA, le volume partagé HANA, etc

Les bases de données suivantes ne s'affichent pas :

- Bases de données qui n'ont pas de sauvegarde
- Les bases de données avec des règles à la demande ou à l'heure
- Bases de données Oracle résidant sur NVMe

Créez une règle pour sauvegarder les applications

Vous pouvez soit utiliser l'une des règles prédéfinies, soit créer une règle personnalisée pour sauvegarder les données applicatives dans le cloud. Vous pouvez créer des stratégies si vous ne souhaitez pas modifier les stratégies prédéfinies.

Les règles prédéfinies sont les suivantes :

Nom de la règle	Étiquette	Valeur de conservation
1 an de LTR quotidien	Tous les jours	366
5 ans de LTR quotidien	Tous les jours	1830
LTR hebdomadaire de 7 ans	Hebdomadaire	370
10 ans de LTR mensuel	Tous les mois	120

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Dans la liste déroulante Paramètres, cliquez sur **stratégies > Créer une stratégie**.
3. Dans la section Détails de la stratégie, spécifiez le nom de la stratégie.
4. Dans la section Retention, sélectionnez l'un des types de rétention et indiquez le nombre de sauvegardes à conserver.
5. Sélectionnez primaire ou secondaire comme source de stockage de sauvegarde.
6. (Facultatif) si vous souhaitez transférer des sauvegardes du magasin d'objets vers le stockage d'archives après un certain nombre de jours pour l'optimisation des coûts, cochez la case **Tier backups to Archival**.

Vous pouvez déplacer les sauvegardes d'un magasin d'objets vers le stockage d'archivage uniquement si vous utilisez ONTAP 9.10.1 ou version ultérieure et Amazon Web Services ou Azure comme fournisseur cloud. Vous devez configurer le niveau d'accès d'archivage pour chaque fournisseur de cloud.

7. Cliquez sur **Créer**.

Vous pouvez modifier, copier et supprimer les stratégies personnalisées.



Vous ne pouvez pas modifier ou supprimer une stratégie associée à une application.

Sauvegardez les données des applications sur site dans Amazon Web Services

Vous pouvez sauvegarder les données applicatives de ONTAP vers Amazon Web Services en intégrant Cloud Backup pour les applications avec BlueXP et SnapCenter sur site.

Vous pouvez protéger une ou plusieurs applications simultanément dans le cloud à l'aide d'une seule règle.



Vous ne pouvez protéger qu'une seule application à la fois si vous utilisez l'interface graphique BlueXP. Toutefois, si vous utilisez des API REST, vous pouvez protéger plusieurs applications simultanément.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Cliquez sur **...** Correspondant à l'application et cliquez sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

Configurer le cluster ONTAP qui héberge le SVM sur lequel l'application est en cours d'exécution. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

- a. Sélectionner le SVM et cliquez sur **Ajouter un environnement de travail**.
- b. Dans l'assistant Ajouter un environnement de travail :
 - i. Spécifier l'adresse IP du cluster ONTAP
 - ii. Spécifiez les informations d'identification admin.

Cloud Backup pour applications ne prend en charge que les administrateurs de cluster.

- c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **Amazon Web Services** comme fournisseur de services clouds.
 - a. Spécifier le compte AWS
 - b. Dans le champ clé d'accès AWS, spécifiez la clé.
 - c. Dans le champ clé secrète AWS, spécifiez le mot de passe.
 - d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
 - e. Spécifiez l'espace IP.
 - f. Sélectionnez le niveau d'archivage.

Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne serez

pas autorisé à le configurer ultérieurement.

6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegardez les données applicatives sur site dans Microsoft Azure

Vous pouvez sauvegarder les données applicatives de ONTAP vers Microsoft Azure en intégrant Cloud Backup pour les applications avec BlueXP et SnapCenter sur site.

Vous pouvez protéger une ou plusieurs applications simultanément dans le cloud à l'aide d'une seule règle.



Vous ne pouvez protéger qu'une seule application à la fois si vous utilisez l'interface graphique BlueXP. Toutefois, si vous utilisez des API REST, vous pouvez protéger plusieurs applications simultanément.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Cliquez sur ... Correspondant à l'application et cliquez sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

Configurer le cluster ONTAP qui héberge le SVM sur lequel l'application est en cours d'exécution. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

- a. Sélectionner le SVM et cliquez sur **Ajouter un environnement de travail**.
- b. Dans l'assistant Ajouter un environnement de travail :
 - i. Spécifier l'adresse IP du cluster ONTAP
 - ii. Spécifiez les informations d'identification admin.

Cloud Backup pour applications ne prend en charge que les administrateurs de cluster.

- c. Cliquez sur **Ajouter un environnement de travail**.

5. Sélectionnez **Microsoft Azure** comme fournisseur cloud.

- a. Spécifiez l'ID d'abonnement Azure.
- b. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
- c. Créez un nouveau groupe de ressources ou utilisez un groupe de ressources existant.
- d. Spécifiez l'espace IP.
- e. Sélectionnez le niveau d'archivage.

Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne serez pas autorisé à le configurer ultérieurement.

6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegardez les données des applications sur site dans Google Cloud Platform

Vous pouvez sauvegarder les données applicatives de ONTAP vers Google Cloud Platform en intégrant Cloud Backup pour les applications avec BlueXP et SnapCenter sur site.

Vous pouvez protéger une ou plusieurs applications simultanément dans le cloud à l'aide d'une seule règle.



Vous ne pouvez protéger qu'une seule application à la fois si vous utilisez l'interface graphique BlueXP. Toutefois, si vous utilisez des API REST, vous pouvez protéger plusieurs applications simultanément.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Cliquez sur **...** Correspondant à l'application et cliquez sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

Configurer le cluster ONTAP qui héberge le SVM sur lequel l'application est en cours d'exécution. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

- a. Sélectionner le SVM et cliquez sur **Ajouter un environnement de travail**.
- b. Dans l'assistant Ajouter un environnement de travail :
 - i. Spécifier l'adresse IP du cluster ONTAP
 - ii. Spécifiez les informations d'identification admin.

Cloud Backup pour applications ne prend en charge que les administrateurs de cluster.

- c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **Google Cloud Platform** comme fournisseur cloud.
 - a. Sélectionnez le compartiment Google Cloud Project où vous souhaitez créer le compartiment Google Cloud Storage pour les sauvegardes.
 - b. Dans le champ clé d'accès Google Cloud, spécifiez la clé.
 - c. Dans le champ clé secrète Google Cloud, spécifiez le mot de passe.
 - d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
 - e. Spécifiez l'espace IP.
 6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegardez les données applicatives sur site dans StorageGRID

Vous pouvez sauvegarder les données applicatives de ONTAP vers StorageGRID en intégrant Cloud Backup pour les applications avec BlueXP et SnapCenter sur site.

Vous pouvez protéger une ou plusieurs applications simultanément vers StorageGRID à l'aide d'une seule règle.



Vous ne pouvez protéger qu'une seule application à la fois si vous utilisez l'interface graphique BlueXP. Toutefois, si vous utilisez des API REST, vous pouvez protéger plusieurs applications simultanément.

Ce dont vous aurez besoin

Lorsque vous sauvegardez des données dans StorageGRID, un connecteur doit être disponible sur site. Vous devrez soit installer un nouveau connecteur, soit vérifier que le connecteur actuellement sélectionné réside sur site. Le connecteur peut être installé sur un site avec ou sans accès à Internet.

Pour plus d'informations, reportez-vous à la section "[Créer des connecteurs pour StorageGRID](#)".

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Cliquez sur **...** Correspondant à l'application et cliquez sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

Configurer le cluster ONTAP qui héberge le SVM sur lequel l'application est en cours d'exécution. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

- a. Sélectionner le SVM et cliquer sur **Ajouter un environnement de travail**.
- b. Dans l'assistant Ajouter un environnement de travail :
 - i. Spécifier l'adresse IP du cluster ONTAP
 - ii. Spécifiez les informations d'identification admin.

Cloud Backup pour applications ne prend en charge que les administrateurs de cluster.

- c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **StorageGRID**.
 - a. Spécifiez le FQDN du serveur StorageGRID et le port sur lequel le serveur StorageGRID s'exécute.

Entrez les détails au format FQDN:PORT.
 - b. Dans le champ clé d'accès, spécifiez la clé.
 - c. Dans le champ clé secrète, spécifiez le mot de passe.
 - d. Spécifiez l'espace IP.
 6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Gérer la protection des applications

Vous pouvez gérer la protection des applications en effectuant différentes opérations à partir de l'interface utilisateur BlueXP.

Afficher les règles

Vous pouvez afficher toutes les règles. Pour chacune de ces stratégies, lorsque vous affichez les détails, toutes les applications associées sont répertoriées.

1. Cliquez sur **sauvegarde et restauration > applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **stratégies**.
3. Cliquez sur **Afficher les détails** correspondant à la stratégie dont vous souhaitez afficher les détails.

Les applications associées sont répertoriées.



Vous ne pouvez pas modifier ou supprimer une stratégie associée à une application.

Vous pouvez également afficher les règles de SnapCenter étendues au cloud en exécutant la `Get-SmResources` Cmdlet SnapCenter. Les informations concernant les paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `Get-Help nom_commande`. Vous pouvez également consulter le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Affichez les sauvegardes sur le cloud

Vous pouvez afficher les sauvegardes dans le cloud dans l'interface utilisateur BlueXP.

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



Le temps nécessaire pour figurer les sauvegardes dépend de la planification de réplication par défaut d'ONTAP (1 heure maximum) et de BlueXP (6 heures maximum).

- Pour les bases de données Oracle, les sauvegardes de données et de journaux, le numéro SCN pour chaque sauvegarde, la date de fin de chaque sauvegarde sont répertoriées. Vous pouvez uniquement sélectionner la sauvegarde des données et restaurer la base de données sur le serveur SnapCenter sur site.
- Pour les bases de données Microsoft SQL Server, seules les sauvegardes complètes et la date de fin de chaque sauvegarde sont répertoriées. Vous pouvez sélectionner la sauvegarde et restaurer la base de données sur le serveur SnapCenter sur site.
- Pour l'instance de Microsoft SQL Server, les sauvegardes ne sont pas répertoriées à la place uniquement les bases de données sous cette instance sont répertoriées.
- Pour les bases de données SAP HANA, seules les sauvegardes de données et la date de fin de chaque sauvegarde sont répertoriées. Vous pouvez sélectionner la sauvegarde et effectuer une opération de montage.



Les sauvegardes créées avant d'activer la protection dans le cloud ne sont pas répertoriées pour la restauration.

Vous pouvez également afficher ces sauvegardes en exécutant le `Get-SmBackup` Cmdlet SnapCenter. Les informations concernant les paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `Get-Help nom_commande`. Vous pouvez également consulter le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Changement de disposition de la base de données

Lorsque des volumes sont ajoutés à la base de données, le serveur SnapCenter étiquette automatiquement les snapshots sur les nouveaux volumes conformément à la règle et à la planification. Ces nouveaux volumes ne possèdent pas le point de terminaison du magasin d'objets et vous devez procéder à une actualisation en exécutant les étapes suivantes :

1. Cliquez sur **sauvegarde et restauration > applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **serveurs SnapCenter**.
3. Cliquez sur **...** Correspondant au serveur SnapCenter hébergeant l'application et cliquez sur **Actualiser**.

Les nouveaux volumes sont détectés.

4. Cliquez sur **...** Correspondant à l'application et cliquez sur **Actualiser la protection** pour activer la protection du Cloud pour le nouveau volume.

Si un volume de stockage est retiré de l'application après la configuration du service cloud, le serveur SnapCenter étiquette uniquement les snapshots sur lesquels l'application réside. Si le volume supprimé n'est pas utilisé par d'autres applications, vous devez supprimer manuellement la relation de magasin d'objets. Si vous mettez à jour l'inventaire des applications, il contiendra la disposition du stockage actuelle de l'application.

Modification de règle ou de groupe de ressources

En cas de modification de la règle ou du groupe de ressources SnapCenter, vous devez actualiser la protection.

1. Cliquez sur **sauvegarde et restauration > applications**.
2. Cliquez sur **...** Correspondant à l'application et cliquez sur **Actualiser la protection**.

Annuler l'enregistrement du serveur SnapCenter

1. Cliquez sur **sauvegarde et restauration > applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **serveurs SnapCenter**.
3. Cliquez sur **...** Correspondant au serveur SnapCenter et cliquez sur **Unregister**.

Surveiller les tâches

Des travaux sont créés pour toutes les opérations Cloud Backup. Vous pouvez surveiller tous les travaux et toutes les sous-tâches effectuées dans le cadre de chaque tâche.

1. Cliquez sur **sauvegarde et récupération > surveillance des tâches**.

Lorsque vous lancez une opération, une fenêtre s'affiche indiquant que le travail est lancé. Vous pouvez cliquer sur le lien pour surveiller le travail.

2. Cliquez sur la tâche principale pour afficher les sous-tâches et le statut de chacune de ces sous-tâches.

Définissez l'espace IP de l'environnement de travail principal

Si vous souhaitez restaurer ou monter une sauvegarde qui a été déplacée vers un magasin d'objets à partir d'un stockage secondaire, vous devez ajouter les détails de l'environnement de travail principal et définir l'espace IP.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **Storage > Canvas > Mes environnements de travail > Ajouter un environnement de travail**.
2. Spécifiez les détails de l'environnement de travail principal et cliquez sur **Ajouter**.
3. Cliquez sur **sauvegarde et restauration > volumes**.
4. Cliquez sur **...** Correspondant à l'un des volumes et cliquez sur **Détails**.
5. Cliquez sur **...** Correspondant à la sauvegarde et cliquez sur **Restaurer**.
6. Dans l'assistant, sélectionnez l'environnement de travail principal nouvellement ajouté comme destination.
7. Spécifiez l'espace IP.

Configurer les certificats CA

Si vous disposez de certificats CA, vous devez copier manuellement les certificats CA racine sur la machine de connecteur.

Toutefois, si vous ne disposez pas de certificats CA, vous pouvez continuer sans configurer les certificats CA.

Étapes

1. Copiez le certificat sur le volume accessible depuis l'agent docker.

```
° cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir  
  sc_certs  
° chmod 777 sc_certs
```

2. Copiez les fichiers de certificat RootCA dans le dossier ci-dessus de la machine de connecteur.

```
cp <path on connector>/<filename>  
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs
```

3. Copiez le fichier CRL sur le volume accessible depuis l'agent docker.

```
° cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_crl  
° chmod 777 sc_crl
```

4. Copiez les fichiers CRL dans le dossier ci-dessus sur l'ordinateur du connecteur.

```
cp <path on connector>/<filename>  
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_crl
```

5. Une fois les certificats et les fichiers CRL copiés, redémarrez le service Cloud Backup pour applications.

```
° sudo docker exec cloudmanager_snapcenter sed -i 's/skipSCCertValidation:  
true/skipSCCertValidation: false/g' /opt/netapp/cloudmanager-snapcenter-  
agent/config/config.yml  
° sudo docker restart cloudmanager_snapcenter
```

Restauration des données applicatives

Restaurez la base de données Oracle

Vous pouvez uniquement restaurer la base de données Oracle sur le même hôte SnapCenter Server, le même SVM ou sur le même hôte de base de données. Pour une base de données RAC, les données sont restaurées vers le nœud sur site sur lequel la sauvegarde a été créée.



La restauration des sauvegardes secondaires via le stockage primaire est prise en charge.

Seule la base de données complète avec restauration du fichier de contrôle est prise en charge. Si les journaux d'archive ne sont pas présents dans l'AFS, vous devez spécifier l'emplacement qui contient les journaux d'archive requis pour la récupération.



La restauration de fichiers uniques (SFR) n'est pas prise en charge.

Ce dont vous aurez besoin

Si vous souhaitez restaurer une sauvegarde déplacée vers un magasin d'objets à partir d'un stockage secondaire, vous devez ajouter les informations relatives à l'environnement de travail principal et définir l'espace IP. Pour plus d'informations, voir ["Définissez l'espace IP de l'environnement de travail principal"](#).

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Dans le champ **Filter by**, sélectionnez le filtre **Type** et sélectionnez **Oracle** dans la liste déroulante.
3. Cliquez sur **View Details** correspondant à la base de données à restaurer et cliquez sur **Restore**.
4. Sur la page Type de restauration, effectuez les opérations suivantes :

- a. Sélectionnez **Etat de la base de données** si vous souhaitez modifier l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de récupération.

Les différents États d'une base de données de niveau supérieur à inférieur sont ouverts, montés, démarrés et shutdown. Vous devez cocher cette case si la base de données est dans un état plus élevé mais que l'état doit être inférieur pour effectuer une opération de restauration. Si la base de données est dans un état inférieur mais que l'état doit être supérieur pour effectuer l'opération de restauration, l'état de la base de données est automatiquement modifié, même si vous ne cochez pas la case.

Si une base de données est à l'état ouvert et que pour restaurer la base de données doit être à l'état monté, l'état de la base de données n'est modifié que si vous cochez cette case.

- a. Sélectionnez **fichiers de contrôle** si vous souhaitez restaurer le fichier de contrôle avec la base de données complète.
 - b. Si le snapshot est en stockage d'archivage, spécifiez la priorité de restauration des données à partir du stockage d'archivage.
5. Sur la page étendue de la récupération, effectuez les opérations suivantes :
 - a. Spécifier le périmètre de restauration.

Si...	Procédez comme ça...
Que vous souhaitez restaurer à la dernière transaction	Sélectionnez tous les journaux .
Que vous souhaitez récupérer à un numéro de changement de système (SCN) spécifique	Sélectionnez jusqu'à ce que SCN (numéro de changement du système) .
Veulent restaurer des données et un temps spécifique	Sélectionnez Date et heure . Vous devez spécifier la date et l'heure du fuseau horaire de l'hôte de la base de données.
Ne pas récupérer	Sélectionnez pas de récupération .
Vous souhaitez spécifier les emplacements de journaux d'archives externes	Si les journaux d'archive ne sont pas présents dans l'AFS, vous devez spécifier l'emplacement qui contient les journaux d'archive requis pour la récupération.

- b. Cochez la case si vous souhaitez ouvrir la base de données après la récupération.

Dans une configuration RAC, seule l'instance RAC utilisée pour la restauration s'ouvre après une restauration.

6. Vérifiez les détails et cliquez sur **Restaurer**.

Restorez la base de données SQL Server

Vous pouvez restaurer la base de données SQL Server sur le même hôte ou sur l'autre hôte. La restauration des sauvegardes de journaux et du réamorçage des groupes de disponibilité ne sont pas prises en charge.



IMPORTANT : la restauration de sauvegardes secondaires via le stockage primaire est prise en charge.



La restauration de fichiers uniques (SFR) n'est pas prise en charge.


Ce dont vous aurez besoin

Si vous souhaitez restaurer une sauvegarde déplacée vers un magasin d'objets à partir d'un stockage secondaire, vous devez ajouter les informations relatives à l'environnement de travail principal et définir l'espace IP. Pour plus d'informations, voir ["Définissez l'espace IP de l'environnement de travail principal"](#).

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Dans le champ **Filtrer par**, sélectionnez le filtre **Type** et sélectionnez **SQL** dans la liste déroulante.
3. Cliquez sur **Afficher les détails** pour afficher toutes les sauvegardes disponibles.

4. Sélectionnez la sauvegarde et cliquez sur **Restaurer**.
5. Sélectionnez l'emplacement où vous souhaitez restaurer les fichiers de base de données.

Option	Description
Restaurer la base de données sur le même hôte où la sauvegarde a été créée	Sélectionnez cette option si vous souhaitez restaurer la base de données sur le même serveur SQL où les sauvegardes sont effectuées.
Restaurer la base de données sur un autre hôte	<p>Sélectionnez cette option si vous souhaitez que la base de données soit restaurée sur un autre serveur SQL dans le même hôte ou sur un hôte différent où des sauvegardes sont effectuées.</p> <p>Sélectionnez un nom d'hôte, indiquez un nom de base de données (facultatif), sélectionnez une instance et spécifiez les chemins de restauration.</p> <div>  <p>L'extension de fichier fournie dans le chemin alternatif doit être identique à celle du fichier de base de données d'origine.</p> </div> <p>Si l'option Restaurer la base de données sur un autre hôte n'est pas affichée dans la page Restaurer l'étendue, effacez le cache du navigateur.</p>

6. Si le snapshot est en stockage d'archivage, spécifiez la priorité de restauration des données à partir du stockage d'archivage.
7. Sur la page **Options de pré-restauration**, sélectionnez l'une des options suivantes :
 - Sélectionnez **Ecraser la base de données du même nom pendant la restauration** pour restaurer la base de données du même nom.
 - Sélectionnez **conserver les paramètres de réplication de base de données SQL** pour restaurer la base de données et conserver les paramètres de réplication existants.
8. Sur la page **Options de post-restauration**, pour spécifier l'état de la base de données pour restaurer des journaux transactionnels supplémentaires, sélectionnez l'une des options suivantes :
 - Sélectionnez **opérationnel, mais indisponible** si vous restaurez maintenant toutes les sauvegardes nécessaires.

Il s'agit du comportement par défaut, qui laisse la base de données prête à l'emploi en revenant les transactions non validées. Vous ne pouvez pas restaurer d'autres journaux de transactions tant que vous n'avez pas créé de sauvegarde.

 - Sélectionnez **non opérationnel, mais disponible** pour laisser la base de données non opérationnelle sans reprise des transactions non validées.

Des journaux de transactions supplémentaires peuvent être restaurés. Vous ne pouvez pas utiliser la base de données tant qu'elle n'a pas été restaurée.

- Sélectionnez **mode lecture seule et disponible** pour quitter la base de données en mode lecture seule.

Cette option annule les transactions non validées, mais enregistre les actions annulées dans un fichier de secours afin que les effets de récupération puissent être restaurés.

Si l'option Annuler le répertoire est activée, davantage de journaux de transactions sont restaurés. Si l'opération de restauration du journal de transactions échoue, les modifications peuvent être annulées. La documentation de SQL Server contient des informations supplémentaires.

9. Vérifiez les détails et cliquez sur **Restaurer**.

Montage des sauvegardes d'applications

SnapCenter ne prend pas en charge la restauration des sauvegardes Oracle et HANA sur l'hôte secondaire. Ainsi, Cloud Backup pour les applications vous permet de monter les sauvegardes Oracle et HANA sur l'hôte donné.

Ce dont vous aurez besoin

Si vous souhaitez monter une sauvegarde qui a été déplacée vers le magasin d'objets à partir d'un stockage secondaire, ajoutez les détails de l'environnement de travail principal et définissez l'espace IP. Pour plus d'informations, voir ["Définissez l'espace IP de l'environnement de travail principal"](#).

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > applications**.
2. Dans le champ Filtrer par, sélectionnez **Type** et sélectionnez **SAP HANA** ou **Oracle** dans la liste déroulante.
3. Cliquez sur **...** Correspondant à l'application protégée et sélectionnez **Afficher les détails**.
4. Cliquez sur **...** Correspondant à la sauvegarde et sélectionnez **Mount**.
 - a. Spécifiez l'une des options suivantes :
 - i. Pour l'environnement NAS, spécifiez le FQDN ou l'adresse IP de l'hôte vers lequel les autres volumes restaurés à partir du magasin d'objets doivent être exportés.
 - ii. Pour l'environnement SAN, spécifiez les initiateurs de l'hôte vers lequel les LUN du volume secondaire restauré à partir du magasin d'objets doivent être mappées.
 - b. Spécifiez le suffixe à ajouter au nom du volume secondaire.
 - c. Si le snapshot est en stockage d'archivage, spécifiez la priorité de récupération de vos données à partir du stockage d'archivage.
 - d. Cliquez sur **Mount**.

Cette opération ne monte que le stockage sur l'hôte donné. Vous devez monter manuellement le système de fichiers et faire apparaître la base de données. Après avoir utilisé le autre volume, l'administrateur du stockage peut supprimer le volume du cluster ONTAP.

Pour plus d'informations sur l'accès à la base de données SAP HANA, reportez-vous à la section, ["Tr-4667 : automatisation des opérations de copie système et de clonage SAP HANA avec SnapCenter"](#).

Sauvegarde et restauration des données d'applications cloud natives

Protégez vos données applicatives cloud natives

Cloud Backup pour applications est un service SaaS qui fournit des fonctionnalités de protection des données pour les applications exécutées sur NetApp Cloud Storage. Cloud Backup pour les applications activées dans NetApp BlueXP (anciennement Cloud Manager) offre des fonctionnalités de sauvegarde et de restauration efficaces et cohérentes avec les applications, basées sur des règles, et des bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP.

Architecture

L'architecture Cloud Backup pour applications comprend plusieurs composants :

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

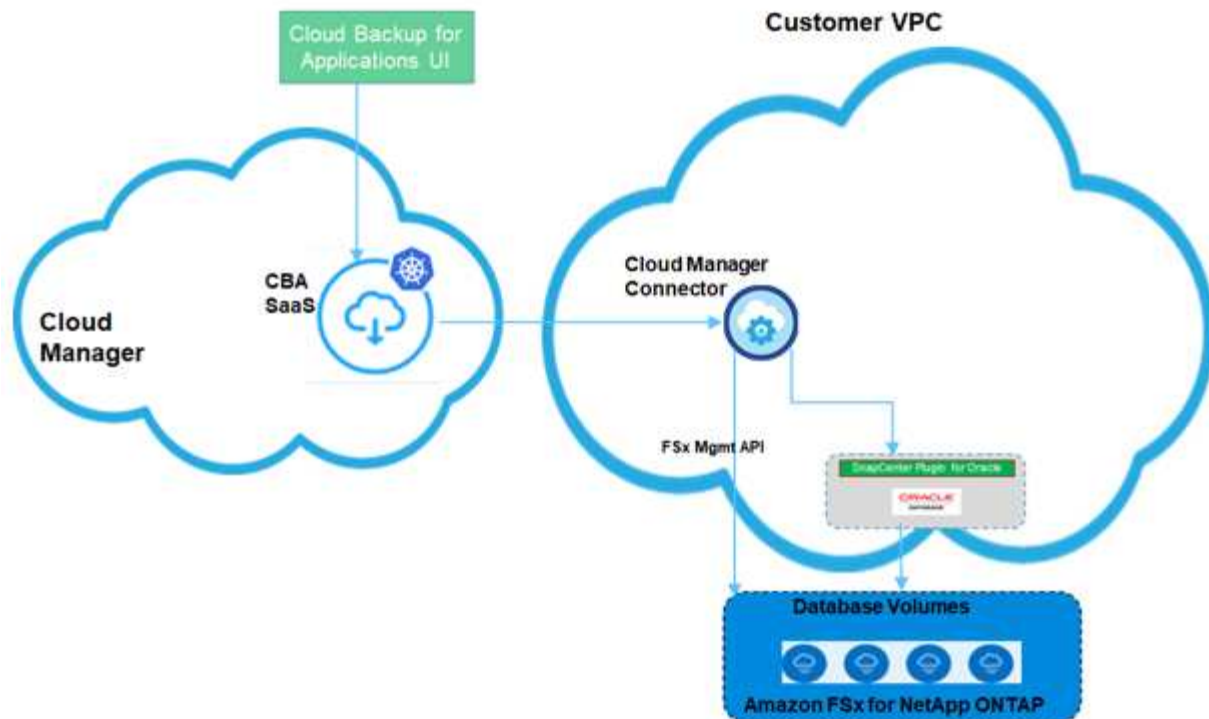
Il orchestre les workflows de protection des données pour les applications qui résident sur NetApp Cloud Storage.

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

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

- BlueXP Connector est un composant de BlueXP qui s'exécute dans votre réseau cloud et interagit avec les systèmes de fichiers de stockage Amazon FSX et le plug-in SnapCenter pour Oracle fonctionnant sur des hôtes de base de données Oracle.
- Le plug-in SnapCenter pour Oracle est un composant qui s'exécute sur chaque hôte de la base de données Oracle. Il interagit avec les bases de données Oracle exécutées sur l'hôte tout en exécutant des opérations de protection des données.

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



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

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



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

Configurations compatibles

- Système d'exploitation :
 - RHEL 7.5 ou version ultérieure et 8.x
 - OL 7.5 ou version ultérieure et 8.x
- Système de stockage : Amazon FSX pour ONTAP
- Dispositions de stockage : NFS v3 et v4.1 (dNFS est pris en charge) et iSCSI avec ASM (ASMFD, ASMLib et ASMUdev)
- Applications : Oracle Standard et Oracle Enterprise – autonome (ancienne génération et architecture mutualisée, CDB et PDB)
- Versions Oracle : 12cR2, 18c et 19c

Caractéristiques

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

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

- Conservation des sauvegardes en fonction de la stratégie appliquée
- Restauration de la base de données Oracle complète (fichiers de données + fichier de contrôle) à partir de la sauvegarde spécifiée
- Restauration des fichiers de données uniquement et des fichiers de contrôle uniquement à partir de la sauvegarde spécifiée
- Récupération de la base de données Oracle avec jusqu'à SCN, jusqu'au moment, tous les journaux disponibles et aucune option de récupération
- La surveillance des sauvegardes et autres tâches
- Affichage du récapitulatif de protection sur le tableau de bord
- Envoi d'alertes par e-mail

Limites

- Ne prend pas en charge les versions 11g et 21c d'Oracle
- Ne prend pas en charge les opérations de montage, de clonage, de catalogue et de vérification des sauvegardes
- Ne prend pas en charge Oracle sur RAC et Data Guard
- Limites des sauvegardes :
 - Ne prend pas en charge les sauvegardes de données en ligne ou de journaux uniquement
 - Ne prend pas en charge les sauvegardes hors ligne
 - Ne prend pas en charge la sauvegarde de la base de données Oracle résidant sur des points de montage récursifs
 - Ne prend pas en charge les snapshots de groupes de cohérence pour les bases de données Oracle résidant sur plusieurs groupes de disques ASM avec chevauchement des volumes FSX
 - Si vos bases de données Oracle sont configurées sur ASM, assurez-vous que les noms de vos SVM sont uniques sur les systèmes FSX. Si vous disposez du même nom de SVM sur les systèmes FSX, la sauvegarde des bases de données Oracle résidant sur ces SVM ne est pas prise en charge.
- Limites en matière de restauration :
 - Ne prend pas en charge les restaurations granulaires, par exemple la restauration des espaces de stockage et des bases de données de niveau fichier
 - Prend uniquement en charge la restauration sur place des bases de données Oracle sur des mises en page NAS et SAN
 - Ne prend pas en charge la restauration du fichier de contrôle uniquement ou des fichiers de données +

fichier de contrôle des bases de données Oracle sur des dispositions SAN

- Dans la disposition SAN, l'opération de restauration échoue si le plug-in SnapCenter pour Oracle trouve des fichiers étrangers autres que les fichiers de données Oracle sur le groupe de disques ASM. Les fichiers étrangers peuvent être de type un ou plusieurs des types suivants :

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

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



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

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

Prérequis

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

Accéder à BlueXP

Vous devriez ["Connectez-vous à BlueXP"](#), puis configurez un ["Compte NetApp"](#).

Créer un environnement de travail FSX pour ONTAP

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

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

Créer un connecteur

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

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

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

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



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

Après avoir créé le connecteur, cliquez sur **Storage > Canvas > Mes environnements de travail > Ajouter un environnement de travail** et suivez les invites pour ajouter l'environnement de travail. Assurez-vous que le connecteur est connecté aux hôtes de base de données Oracle et à l'environnement de travail FSX. Le connecteur doit pouvoir se connecter à l'adresse IP de gestion du cluster de l'environnement de travail FSX.



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

Déploiement du plug-in SnapCenter pour Oracle

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



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

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

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

1. Connectez-vous à la machine virtuelle de Connector en tant qu'utilisateur non root.
2. Obtenez le chemin de montage de base.


```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
```
3. Déployez le plug-in.


```
sudo <base_mount_path>/scripts/oracle_plugin_copy_and_install.sh --host <host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port> --pluginport <plugin_port> --installdir <install_dir>
```

- Host_name est le nom de l'hôte Oracle et il s'agit d'un paramètre obligatoire.

- `ssh_key_file` est une clé SSH utilisée pour la connexion à l'hôte Oracle. Il s'agit d'un paramètre obligatoire.
- `User_NAME` : utilisateur avec privilèges SSH sur l'hôte Oracle et il s'agit d'un paramètre facultatif. La valeur par défaut est `EC2-user`.
- `ssh_port` : port SSH sur l'hôte Oracle et il s'agit d'un paramètre facultatif. La valeur par défaut est 22
- `Plugin_port` : port utilisé par le plug-in et il s'agit d'un paramètre facultatif. La valeur par défaut est 8145
- `Dossier_installation` : répertoire dans lequel le plug-in sera déployé et il s'agit d'un paramètre facultatif. La valeur par défaut est `/opt`.

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

Déploiement manuel du plug-in

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

1. Connectez-vous à la machine virtuelle du connecteur.
2. Téléchargez le binaire du plug-in hôte SnapCenter Linux.

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Obtenez le chemin de montage de base.

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint
```
4. Obtenez le chemin binaire du plug-in téléchargé.

```
sudo ls <base_mount_path> $(sudo docker ps|grep -Po "cloudmanager_scs_cloud:.*? " | sed -e 's/ *$//'|cut -f2 -d":")/sc-linux-host-plugin/snapcenter_linux_host_plugin_scs.bin
```
5. Copiez *snapcenter_linux_host_plugin_scs.bin* vers chacun des hôtes de base de données Oracle à l'aide de `scp` ou d'autres méthodes alternatives.
6. Sur l'hôte de la base de données Oracle, exécutez la commande suivante pour activer les autorisations d'exécution pour le binaire.

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```
7. Déployez le plug-in Oracle en tant qu'utilisateur root.

```
./snapcenter_linux_host_plugin_scs.bin -i silent
```
8. Copiez *certificate.p12* de `<base_mount_path>/client/certificat/` chemin de la machine virtuelle du connecteur vers `/var/opt/snapcenter/spl/etc/` sur l'hôte du plug-in.
 - a. Accédez à `/var/opt/snapcenter/spl/etc` et exécutez la commande `keytool` pour importer le certificat.

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

Sauvegardez les données applicatives cloud natives

Découvrir les applications

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

Ce dont vous aurez besoin

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

Étapes

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

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

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



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

4. Dans la page Specify Host Details, entrez les détails de l'hôte de la base de données Oracle, cochez la case pour confirmer que le plug-in est installé sur l'hôte, puis cliquez sur **Discover**.
 - Affiche toutes les bases de données sur l'hôte. Si l'authentification OS est désactivée pour la base de données, vous devez configurer l'authentification de la base de données en cliquant sur **configurer**. Pour plus d'informations, reportez-vous à la section Oracle database credentials.
 - Cliquez sur **gérer l'application**, sélectionnez **Ajouter** pour ajouter un nouvel hôte, **Actualiser** pour découvrir de nouvelles bases de données ou **Supprimer** pour supprimer un hôte de base de données.
 - Cliquez sur **Paramètres** et sélectionnez **stratégies** pour afficher les stratégies prédéfinies. Passez en revue les stratégies pré-prédéfinies et, si vous le souhaitez, vous pouvez les modifier pour répondre à vos exigences ou créer une nouvelle stratégie.

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

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

Étapes

1. Si l'authentification OS est désactivée pour la base de données, vous devez configurer l'authentification de la base de données en cliquant sur **configurer**.

2. Spécifiez le nom d'utilisateur, le mot de passe et les détails du port dans la section Paramètres de la base de données ou Paramètres ASM.

L'utilisateur Oracle doit disposer des privilèges sysdba et l'utilisateur ASM doit disposer des privilèges sysasm.

3. Cliquez sur **configurer**.

Création de la règle

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

Étapes

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

Sauvegarder les données applicatives cloud natives

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



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

Étapes

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

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

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

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



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

Création de sauvegardes à la demande

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

Étapes

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

Plus d'informations

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

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

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

Gérez la protection des données applicatives cloud natives

Surveiller les tâches

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

Vous pouvez afficher la liste de toutes les opérations et leur état. Chaque opération, ou tâche, a un ID et un état uniques. Le statut peut être :

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

Étapes

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

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

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

Afficher les détails de la sauvegarde

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

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



L'ID de l'agent est associé au connecteur. Si un connecteur utilisé lors de l'enregistrement de l'hôte de base de données Oracle n'existe plus, les sauvegardes suivantes de cette application échoueront car l'ID agent du nouveau connecteur est différent. Vous devez exécuter l'API **Connector-update** pour modifier l'ID de l'agent.

Mettre à jour les détails du connecteur

Si un connecteur utilisé lors de l'enregistrement de l'hôte de base de données Oracle n'existe plus ou est corrompu dans AWS, vous devez déployer un nouveau connecteur. Après le déploiement du nouveau connecteur, exécutez l'API **Connector-update** pour mettre à jour les détails du connecteur.

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

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

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

Après avoir désinstallé le plug-in, vous pouvez le déployer. ["En savoir plus >>"](#).

Configurer le certificat signé par l'autorité de certification

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

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

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

Ce dont vous aurez besoin

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

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

Étapes

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

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

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

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

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

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



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

9. Redémarrer SPL : `systemctl restart spl`

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

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

Ce dont vous aurez besoin

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

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

```
docker volume inspect | grep Mountpoint
```

Étapes

1. Effectuez les opérations suivantes sur l'hôte du plug-in :

- a. Accédez au dossier contenant le magasin de clés de la SPL `/var/opt/snapcenter/spl/etc`.
- b. Créez le format PKCS12 du certificat ayant à la fois le certificat et la clé avec alias `splkeystore`.
- c. Ajoutez le certificat CA.

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

```
keytool -list -v -keystore keystore.jks
```
- e. Redémarrer SPL : `systemctl restart spl`

2. Effectuez les opérations suivantes sur le connecteur :

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

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

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

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

```
sudo docker restart cloudmanager_scs_cloud
```

Accès aux API REST



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

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

Restaurez les données applicatives cloud natives

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

Étapes

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

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



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

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

L'option **forcer la restauration sur place** remplace les fichiers spfile, les fichiers de mot de passe et les fichiers journaux d'archive du groupe de disques des fichiers de données. Vous devez utiliser la dernière sauvegarde lorsque l'option * forcer la restauration sur place* est sélectionnée.

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

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

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

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

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

6. Cliquez sur **Restaurer**.

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.