



Sauvegarde et restauration des données des applications sur site

BlueXP backup and recovery

NetApp
September 09, 2024

Sommaire

- Sauvegarde et restauration des données des applications sur site 1
 - Protection des données applicatives sur site 1
 - Enregistrez SnapCenter Server 2
 - Créez une règle pour sauvegarder les applications 4
 - Sauvegardez les données des applications sur site dans Amazon Web Services 4
 - Sauvegardez les données applicatives sur site dans Microsoft Azure 5
 - Sauvegardez les données des applications sur site dans Google Cloud Platform 6
 - Sauvegardez les données applicatives sur site dans StorageGRID 7
 - Gérer la protection des applications 9
 - Restaurez les données des applications sur site 13

Sauvegarde et restauration des données des applications sur site

Protection des données applicatives sur site

La sauvegarde et la restauration BlueXP pour les applications fournissent des fonctionnalités de protection des données pour les copies Snapshot cohérentes au niveau des applications, du stockage primaire ONTAP sur site au fournisseur cloud.

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

Pour plus d'informations sur la sauvegarde et la restauration BlueXP pour les applications, consultez :

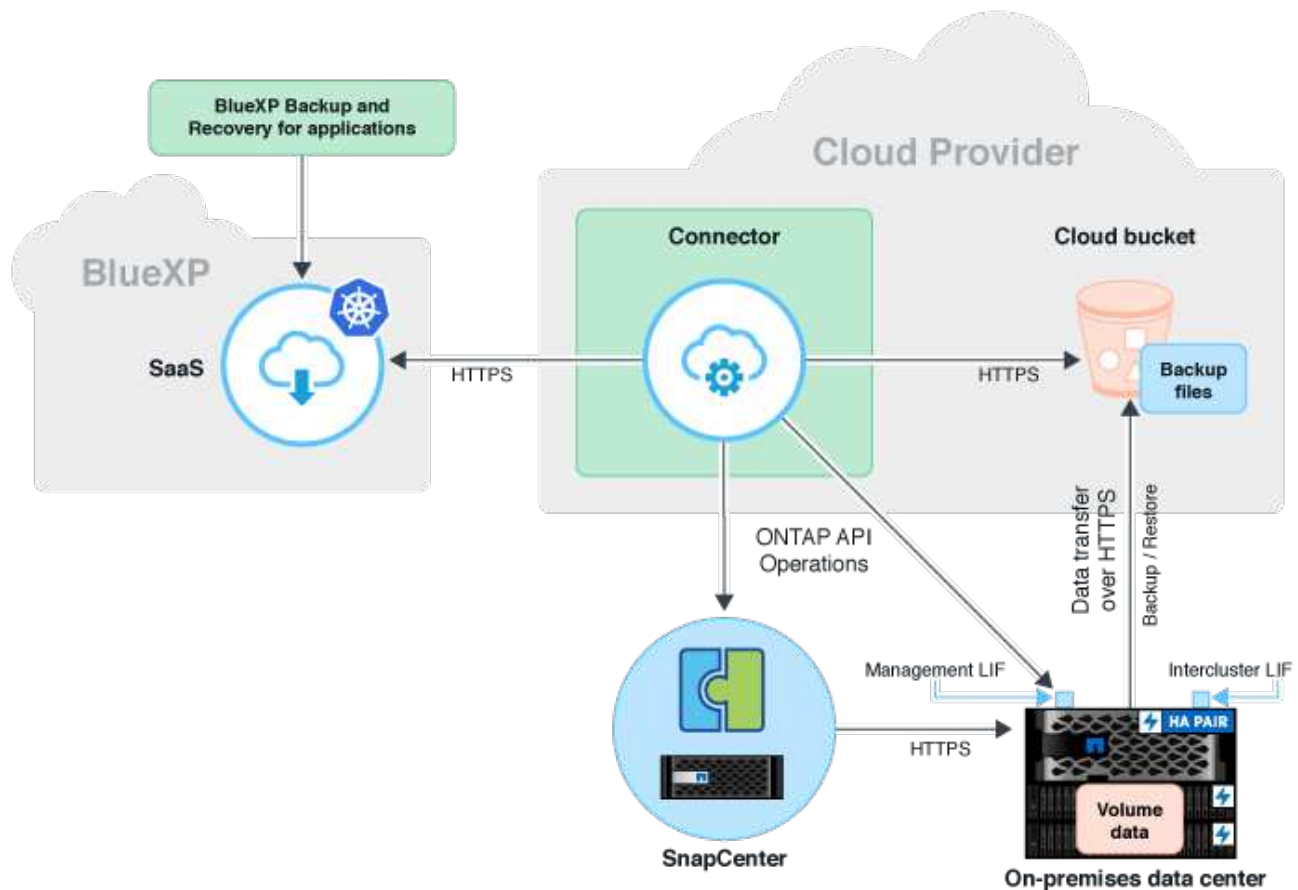
- ["Sauvegarde intégrant la cohérence applicative avec la sauvegarde et la restauration BlueXP et SnapCenter"](#)
- ["Podcast sur la sauvegarde et la restauration BlueXP pour les applications"](#)

De formation

Lisez les conditions suivantes pour vous assurer que votre configuration est prise en charge avant de commencer à sauvegarder les données d'application sur votre fournisseur cloud.

- ONTAP 9.8 ou version ultérieure
- BlueXP
- SnapCenter Server 4.6 ou version ultérieure
 - Vous devez utiliser SnapCenter Server 4.7 ou une version ultérieure si vous souhaitez utiliser les fonctions suivantes :
 - Protégez les sauvegardes du stockage secondaire sur site
 - Protégez les applications SAP HANA
 - Protégez les applications Oracle et SQL présentes dans l'environnement VMware
 - Exportation du stockage d'une sauvegarde
 - Désactiver les sauvegardes
 - Annuler l'enregistrement du serveur SnapCenter
 - Vous devez utiliser SnapCenter Server 4.9 ou une version ultérieure si vous souhaitez utiliser les fonctions suivantes :
 - Monter les sauvegardes de bases de données Oracle
 - Restaurer sur le stockage secondaire
 - Vous devez utiliser le serveur SnapCenter 4.9P1 pour protéger les applications MongoDB, MySQL et PostgreSQL
- Au moins une sauvegarde par application doit être disponible dans SnapCenter Server
- Au moins une règle quotidienne, hebdomadaire ou mensuelle dans SnapCenter, sans étiquette ni même étiquette que celle de la règle dans BlueXP

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 :



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 de serveur SnapCenter dans BlueXP.

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 l'hôte du serveur SnapCenter est en cours d'exécution.

Assurez-vous que le port est ouvert pour que la communication ait lieu entre le serveur SnapCenter et BlueXP.

- 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. Sélectionnez le connecteur dans la liste déroulante **Connector**.

6. Cliquez sur **Enregistrer**.

Une fois que vous avez terminé

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.

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
- MongoDB
- MySQL
- PostgreSQL

Les bases de données suivantes ne sont pas affichées :

- 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 devez créer une stratégie pour sauvegarder les données d'application dans le cloud.

Avant de commencer

- Si vous souhaitez transférer les sauvegardes du magasin d'objets vers le stockage d'archivage, vérifiez que vous utilisez la version ONTAP requise.
 - Si vous utilisez Amazon Web Services, vous devez utiliser ONTAP 9.10.1 ou une version ultérieure
 - Si vous utilisez Microsoft Azure, vous devez utiliser ONTAP 9.10.1 ou une version ultérieure
 - Si vous utilisez Google Cloud, vous devez utiliser ONTAP 9.12.1 ou une version ultérieure
 - Si vous utilisez StorageGRID, vous devez utiliser ONTAP 9.12.1 ou une version ultérieure
- Vous devez configurer le niveau d'accès d'archivage pour chaque fournisseur de cloud.

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**.
7. Cliquez sur **Créer**.



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

Sauvegardez les données des applications sur site dans Amazon Web Services

Procédez en quelques étapes pour sauvegarder les données d'applications de ONTAP vers Amazon Web Services.

BlueXP prend en charge le verrouillage des données et la protection contre les ransomware. Si le cluster ONTAP s'exécute sous ONTAP 9.11.1 ou version ultérieure et si vous n'avez pas configuré de stockage d'archivage, vous pouvez protéger les sauvegardes contre le remplacement, la suppression et les menaces de ransomware.

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.

Configurez la LIF de gestion de cluster à détecter par BlueXP. 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. Préciser l'adresse IP de la LIF de cluster management.
 - ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du 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 si vous avez configuré le stockage d'archives dans la stratégie.

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. Configurez le verrouillage des données et la protection contre les ransomware.


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

Sauvegardez les données applicatives sur site dans Microsoft Azure

Procédez en quelques étapes pour sauvegarder les données d'applications de ONTAP vers Microsoft Azure.

BlueXP prend en charge le verrouillage des données et la protection contre les ransomware. Si le cluster ONTAP s'exécute sous ONTAP 9.12.1 ou version ultérieure et si vous n'avez pas configuré de stockage d'archivage, vous pouvez protéger les sauvegardes contre le remplacement, la suppression et les menaces de ransomware.

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.

Configurez la LIF de gestion de cluster à détecter par BlueXP. 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. Préciser l'adresse IP de la LIF de cluster management.
 - ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du 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 si vous avez configuré le stockage d'archives dans la stratégie.

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. Configurez le verrouillage des données et la protection contre les ransomware.

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

Sauvegardez les données des applications sur site dans Google Cloud Platform

Effectuez quelques étapes pour sauvegarder les données d'applications de ONTAP vers Google Cloud Platform.

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.

Configurez la LIF de gestion de cluster à détecter par BlueXP. 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. Préciser l'adresse IP de la LIF de cluster management.
 - ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du 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.

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 StorageGRID

Effectuez quelques étapes pour sauvegarder les données d'applications de ONTAP vers StorageGRID.

BlueXP prend en charge le verrouillage des données et la protection contre les ransomware. Si le cluster ONTAP s'exécute sur ONTAP 9.11.1 ou version ultérieure, si les systèmes StorageGRID sont version 11.6.0.3 ou ultérieure et si vous n'avez pas configuré le stockage d'archivage, vous pouvez protéger les sauvegardes contre le remplacement, la suppression et les menaces de ransomware.

Avant de commencer

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, voir "[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.

Configurez la LIF de gestion de cluster à détecter par BlueXP. 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. Préciser l'adresse IP du LIF de cluster Management.

- ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du 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.
- e. Spécifiez le niveau d'archivage si vous avez configuré le stockage d'archives dans la stratégie.

Si vous sélectionnez...	Effectuez les opérations suivantes...
AWS	<ul style="list-style-type: none">i. Sélectionnez le StorageGRID dans le menu déroulant ou ajoutez le cluster StorageGRID.ii. Spécifier le compte AWSiii. Dans le champ clé d'accès AWS, spécifiez la clé.iv. Dans le champ clé secrète AWS, spécifiez le mot de passe.v. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.vi. Cliquez sur Enregistrer.
Azure	<ul style="list-style-type: none">i. Sélectionnez le cluster StorageGRID dans la liste déroulante ou ajoutez-le.ii. Spécifiez l'ID d'abonnement Azure.iii. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.iv. Créez un nouveau groupe de ressources ou utilisez un groupe de ressources existant.v. Cliquez sur Enregistrer.

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. Configurez le verrouillage des données et la protection contre les ransomware.
- 7. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Gérer la protection des applications

Vous pouvez gérer la protection des applications en visualisant les règles, en visualisant les sauvegardes, en visualisant les modifications de la disposition, des règles et du groupe de ressources de la base de données, et en surveillant toutes les 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.

Étapes

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 dans SnapCenter.

Les informations concernant les paramètres qui peuvent être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant la commande `Get-Help nom`.

Affichez les sauvegardes sur le cloud

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

Étapes

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



Le temps nécessaire à l'affichage des sauvegardes dépend de la planification de réplication par défaut d'ONTAP.

- Pour les bases de données Oracle, les sauvegardes de données et de journaux, le numéro de modification système (SCN) pour chaque sauvegarde et la date de fin pour chaque sauvegarde sont indiqués. Vous pouvez sélectionner uniquement la sauvegarde des données et restaurer la base de données à son emplacement d'origine. Vous pouvez monter la sauvegarde des données et des journaux à un autre emplacement.
- 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 à son emplacement d'origine ou à un autre emplacement.
- Pour l'instance Microsoft SQL Server, les sauvegardes des 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 exporter le stockage sur un hôte donné.

- Pour MongoDB, MySQL et PostgreSQL, seules les sauvegardes de données et la date de fin de chaque sauvegarde sont répertoriées. Vous pouvez sélectionner la sauvegarde et exporter le stockage sur un hôte donné.



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` dans SnapCenter. Les informations concernant les paramètres qui peuvent être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant la commande `Get-Help nom`.

Désactiver la sauvegarde

Vous pouvez supprimer toutes les sauvegardes déplacées vers le magasin d'objets depuis SnapCenter et le magasin d'objets.

Étapes

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

Par défaut, cette case est cochée et supprime toutes les sauvegardes qui sont déplacées vers le magasin d'objets depuis SnapCenter et le magasin d'objets.

Si vous décochez cette case, les sauvegardes sont conservées uniquement dans le magasin d'objets, mais elles ne peuvent pas être utilisées pour la restauration au niveau de l'application. Plus tard, lorsque vous activez la sauvegarde pour cette application, les sauvegardes conservées dans le magasin d'objets ne sont pas répertoriées pour la restauration.

3. Cliquez sur **Désactiver la sauvegarde**.

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 disposent pas du terminal de magasin d'objets et vous devez actualiser les volumes en effectuant les étapes suivantes :

Étapes

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 ajouté à l'application après la configuration du fournisseur cloud, le serveur SnapCenter marque les snapshots pour les nouvelles sauvegardes sur lesquelles l'application réside.

- Vous devez supprimer manuellement la relation de magasin d'objets si le volume supprimé n'est utilisé par aucune autre application.
- 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 SnapCenter ou du groupe de ressources, vous devez actualiser la relation de protection.

Étapes

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

Étapes

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**.

Par défaut, cette case est cochée et supprime toutes les sauvegardes qui sont déplacées vers le magasin d'objets depuis SnapCenter et le magasin d'objets.

Si vous décochez cette case, les sauvegardes sont conservées uniquement dans le magasin d'objets, mais elles ne peuvent pas être utilisées pour la restauration au niveau de l'application. Plus tard, lorsque vous activez la sauvegarde pour cette application, les sauvegardes conservées dans le magasin d'objets ne sont pas répertoriées pour la restauration.

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.

Étapes

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.

Configurer les certificats CA

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

Configurez le certificat signé par l'autorité de certification SnapCenter dans BlueXP Connector

Vous devez configurer le certificat signé par l'autorité de certification SnapCenter dans BlueXP Connector de manière à ce que le connecteur puisse vérifier le certificat de SnapCenter.

Avant de commencer

Exécutez la commande suivante dans le connecteur BlueXP pour obtenir `<base_mount_path>`:

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

Étapes

1. Connectez-vous au connecteur.

```
cd <base_mount_path> mkdir -p server/certificate
```

2. Copiez les fichiers de l'autorité de certification racine et de l'autorité de certification intermédiaire dans le répertoire `<base_mount_path>/Server/certificate`.

Les fichiers CA doivent être au format .pem.

3. Si vous disposez de fichiers CRL, effectuez les opérations suivantes :

- a. `cd <base_mount_path> mkdir -p server/crl`

- b. Copiez les fichiers CRL dans le répertoire `<base_mount_path>/Server/crl`.

4. Connectez-vous au `cloudManager_snapcenter` et modifiez `enableCACert` dans `config.yml` à `true`.

```
sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert:
false/enableCACert: true/g' /opt/netapp/cloudmanager-
snapcenter/config/config.yml
```

5. Redémarrez le conteneur `cloudManager_snapcenter`.

```
sudo docker restart cloudmanager_snapcenter
```

Configurer le certificat signé par l'autorité de certification pour BlueXP Connector

Si le protocole SSL à 2 voies est activé dans SnapCenter, vous devez effectuer les étapes suivantes sur le connecteur pour utiliser le certificat CA comme certificat client lorsque le connecteur se connecte à SnapCenter.

Avant de commencer

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

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

Étapes

1. Connectez-vous au connecteur.

```
cd <base_mount_path> mkdir -p client/certificate
```

2. Copiez le certificat signé par l'autorité de certification et le fichier de clé dans `<base_mount_path>/client/certificate` dans le connecteur.

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

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

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

4. Connectez-vous au `cloudManager_snapcenter` et modifiez le `sendCACert` dans `config.yml` à `true`.

```
sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert:
false/sendCACert: true/g' /opt/netapp/cloudmanager-
snapcenter/config/config.yml
```

5. Redémarrez le conteneur cloudManager_snapcenter.
`sudo docker restart cloudmanager_snapcenter`
6. Effectuez les étapes suivantes sur le SnapCenter pour valider le certificat envoyé par le connecteur.
 - a. Connectez-vous à l'hôte de serveur SnapCenter.
 - b. Cliquez sur **Démarrer > lancer la recherche**.
 - c. Tapez mmc et appuyez sur **entrée**.
 - d. Cliquez sur **Oui**.
 - e. Dans le menu fichier, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
 - f. Cliquez sur **certificats > Ajouter > compte ordinateur > Suivant**.
 - g. Cliquez sur **ordinateur local > Terminer**.
 - h. Si vous n'avez plus de snap-ins à ajouter à la console, cliquez sur **OK**.
 - i. Dans l'arborescence de la console, double-cliquez sur **certificats**.
 - j. Cliquez avec le bouton droit de la souris sur le magasin **autorités de certification racines de confiance**.
 - k. Cliquez sur **Importer** pour importer les certificats et suivez les étapes de l'assistant **importation de certificat**.

Restaurez les données des applications sur site

Restaurez la base de données Oracle

Vous pouvez restaurer la base de données Oracle à l'emplacement d'origine ou dans un autre emplacement. Dans le cas d'une base de données RAC, les données sont restaurées vers le nœud sur site sur lequel la sauvegarde a été créée.

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.

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. Dans la page Options de restauration, spécifiez l'emplacement où vous souhaitez restaurer les fichiers de base de données.

Si...	Procédez comme ça...
<p data-bbox="183 159 794 191">Vous souhaitez restaurer l'emplacement d'origine</p>	<div data-bbox="857 159 1468 548"> <p data-bbox="857 159 1414 222">a. Sélectionnez Restaurer à l'emplacement d'origine.</p> <p data-bbox="857 243 1451 338">b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.</p> <p data-bbox="857 359 1143 390">c. Cliquez sur Suivant.</p> <p data-bbox="857 411 1451 548">d. 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.</p> </div> <p data-bbox="889 579 1468 674">Les différents États d'une base de données de niveau supérieur à inférieur sont ouverts, montés, démarrés et shutdown.</p> <ul data-bbox="915 716 1484 1283" style="list-style-type: none"> ◦ Si la base de données est dans un état supérieur mais que l'état doit être modifié en état inférieur pour effectuer une opération de restauration, vous devez cocher cette case. ◦ 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. <p data-bbox="857 1314 1354 1346">e. Spécifier le périmètre de restauration.</p> <ul data-bbox="915 1356 1468 1692" style="list-style-type: none"> ◦ Sélectionnez tous les journaux si vous souhaitez récupérer la dernière transaction. ◦ Sélectionnez jusqu'à ce que SCN (Numéro de changement de système) si vous souhaitez restaurer un SCN spécifique. ◦ Sélectionnez Date et heure si vous souhaitez restaurer des données et une heure spécifiques. <p data-bbox="938 1734 1451 1829">Vous devez spécifier la date et l'heure du fuseau horaire de l'hôte de la base de données.</p> <ul data-bbox="915 1860 1468 1923" style="list-style-type: none"> ◦ Sélectionnez pas de récupération si vous ne voulez pas récupérer. <p data-bbox="889 1955 1484 2081">Si les journaux d'archivage ne sont pas présents dans le système de fichiers actif, vous devez spécifier l'emplacement qui contient les journaux d'archivage requis pour la restauration.</p>

Si...	Procédez comme ça...
<p data-bbox="183 159 818 289">Vous souhaitez effectuer une restauration temporaire dans un autre espace de stockage, puis copier les fichiers restaurés à leur emplacement d'origine</p>	<ol data-bbox="859 159 1463 426" style="list-style-type: none"> Sélectionnez Restaurer à l'emplacement d'origine. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. Sélectionnez Modifier l'emplacement de stockage. <p data-bbox="891 464 1482 625">Si vous sélectionnez Modifier l'emplacement de stockage, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, _restore est ajouté par défaut au volume de destination.</p> <ol data-bbox="859 663 1463 884" style="list-style-type: none"> Cliquez sur Suivant. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données restaurées à partir du magasin d'objets seront stockées temporairement. <p data-bbox="891 921 1482 1083">Si vous sélectionnez un système ONTAP sur site et si vous n'avez pas configuré la connexion au cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires concernant le magasin d'objets.</p> <ol data-bbox="859 1121 1463 1304" style="list-style-type: none"> Cliquez sur Suivant. 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. <p data-bbox="891 1341 1463 1440">Les différents États d'une base de données de niveau supérieur à inférieur sont ouverts, montés, démarrés et shutdown.</p> <ul style="list-style-type: none"> <li data-bbox="915 1478 1482 1640">◦ Si la base de données est dans un état supérieur mais que l'état doit être modifié en état inférieur pour effectuer une opération de restauration, vous devez cocher cette case. <li data-bbox="915 1667 1482 1860">◦ 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. <li data-bbox="915 1887 1482 2049">◦ 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.

Si...	Procédez comme ça...
Restauration dans un autre emplacement	<p>a. Sélectionnez Restaurer à un autre emplacement.</p> <p>b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.</p> <p>c. Si vous souhaitez restaurer sur un autre stockage, effectuez les opérations suivantes :</p> <ol style="list-style-type: none"> Sélectionnez Modifier l'emplacement de stockage. Si vous sélectionnez Modifier l'emplacement de stockage, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, _restore est ajouté par défaut au volume de destination. Cliquez sur Suivant. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données du magasin d'objets doivent être restaurées. <p>d. Cliquez sur Suivant.</p> <p>e. Dans la page hôte de destination, sélectionnez l'hôte sur lequel la base de données sera montée.</p> <ol style="list-style-type: none"> (Facultatif) pour l'environnement NAS, spécifiez le nom de domaine complet ou l'adresse IP de l'hôte vers lequel les volumes restaurés à partir du magasin d'objets doivent être exportés. (Facultatif) dans le cas d'un environnement SAN, spécifiez les initiateurs de l'hôte sur lesquels les LUN des volumes restaurés à partir du magasin d'objets doivent être mappées. <p>f. Cliquez sur Suivant.</p>

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

L'option **Restaurer à un autre emplacement** monte la sauvegarde sélectionnée sur l'hôte donné. Vous devez ouvrir manuellement la base de données.

Après avoir monté la sauvegarde, vous ne pouvez pas la monter à nouveau tant qu'elle n'est pas démontée. Vous pouvez utiliser l'option **Unmount** de l'interface utilisateur pour démonter la sauvegarde.

Pour plus d'informations sur l'affichage de la base de données Oracle, reportez-vous à la section ["Article de la base de connaissances"](#).

Restaurez la base de données SQL Server

Vous pouvez restaurer la base de données SQL Server à l'emplacement d'origine ou à l'autre emplacement.





La restauration de fichiers uniques (SFR), la récupération des sauvegardes de journaux et la réamorçage des groupes de disponibilité ne sont pas pris en charge.

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. Dans la page Options de restauration, spécifiez l'emplacement où vous souhaitez restaurer les fichiers de base de données.

Si...	Procédez comme ça...
Vous souhaitez restaurer l'emplacement d'origine	<ol style="list-style-type: none">a. Sélectionnez Restaurer à l'emplacement d'origine.b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.c. Cliquez sur Suivant.
Vous souhaitez effectuer une restauration temporaire dans un autre espace de stockage, puis copier les fichiers restaurés à leur emplacement d'origine	<ol style="list-style-type: none">a. Sélectionnez Restaurer à l'emplacement d'origine.b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.c. Sélectionnez Modifier l'emplacement de stockage. Si vous sélectionnez Modifier l'emplacement de stockage, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, _restore est ajouté par défaut au volume de destination.d. Cliquez sur Suivant.e. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données restaurées à partir du magasin d'objets seront stockées temporairement.f. Cliquez sur Suivant.

Si...	Procédez comme ça...
Restauration dans un autre emplacement	<p>a. Sélectionnez Restaurer à un autre emplacement.</p> <p>b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.</p> <p>c. Cliquez sur Suivant.</p> <p>d. Sur la page hôte de destination, sélectionnez un nom d'hôte, indiquez un nom de base de données (facultatif), sélectionnez une instance et spécifiez les chemins de restauration.</p> <div data-bbox="922 625 976 688">  </div> <div data-bbox="1036 590 1450 726"> <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>e. Cliquez sur Suivant.</p>

Si...	Procédez comme ça...
Vous souhaitez effectuer une restauration temporaire sur un autre stockage, puis copier les fichiers restaurés à l'autre emplacement	<p>a. Sélectionnez Restaurer à un autre emplacement.</p> <p>b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.</p> <p>c. Sélectionnez Modifier l'emplacement de stockage.</p> <p>Si vous sélectionnez Modifier l'emplacement de stockage, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, _restore est ajouté par défaut au volume de destination.</p> <p>d. Cliquez sur Suivant.</p> <p>e. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données restaurées à partir du magasin d'objets seront stockées temporairement.</p> <p>f. Cliquez sur Suivant.</p> <p>g. Sur la page hôte de destination, sélectionnez un nom d'hôte, indiquez un nom de base de données (facultatif), sélectionnez une instance et spécifiez les chemins de restauration.</p> <div style="display: flex; align-items: center; margin-top: 20px;"> <div style="text-align: center; margin-right: 10px;">  </div> <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> </div> <p>h. Cliquez sur Suivant.</p>

6. Dans la case **pré-opérations**, 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.

7. Dans la section **Post-Operations**, pour spécifier l'état de la base de données pour la restauration de 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.

8. Cliquez sur **Suivant**.

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

Restorez la base de données SAP HANA

Vous pouvez restaurer la base de données SAP HANA sur n'importe quel hôte.

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 dans la liste déroulante, sélectionnez **HANA**.
3. Cliquez sur **View Details** correspondant à la base de données à restaurer et cliquez sur **Restore**.
4. Dans la page Options de restauration, spécifiez l'une des options suivantes :
 - a. Pour l'environnement NAS, spécifiez le nom de domaine complet ou l'adresse IP de l'hôte vers lequel les volumes restaurés à partir du magasin d'objets doivent être exportés.
 - b. Pour l'environnement SAN, spécifiez les initiateurs de l'hôte sur lesquels les LUN des volumes restaurés à partir du magasin d'objets doivent être mappées.
5. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.
6. S'il n'y a pas assez d'espace sur le stockage source ou si le stockage source est en panne, sélectionnez **Modifier l'emplacement de stockage**.

Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination.

7. Cliquez sur **Suivant**.
8. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire dans lequel les données restaurées à partir du magasin d'objets seront stockées.
9. Cliquez sur **Suivant**.
10. Vérifiez les détails et cliquez sur **Restaurer**.

Cette opération n'effectue que l'exportation du stockage de la sauvegarde sélectionnée sur l'hôte donné. Vous devez monter manuellement le système de fichiers et faire apparaître la base de données. Après avoir utilisé

le volume, l'administrateur du stockage peut le supprimer du cluster ONTAP.

Pour plus d'informations sur l'affichage de 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](#)".

Restaurez les bases de données MongoDB, MySQL et PostgreSQL

Vous pouvez restaurer des bases de données MongoDB, MySQL et PostgreSQL sur n'importe quel hôte.

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 dans la liste déroulante, sélectionnez **MongoDB**, **MySQL** ou **PostgreSQL**.
3. Cliquez sur **View Details** correspondant à la base de données à restaurer et cliquez sur **Restore**.
4. Dans la page Options de restauration, spécifiez l'une des options suivantes :
 - a. Pour l'environnement NAS, spécifiez le nom de domaine complet ou l'adresse IP de l'hôte vers lequel les volumes restaurés à partir du magasin d'objets doivent être exportés.
 - b. Pour l'environnement SAN, spécifiez les initiateurs de l'hôte sur lesquels les LUN des volumes restaurés à partir du magasin d'objets doivent être mappées.
5. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.
6. S'il n'y a pas assez d'espace sur le stockage source ou si le stockage source est en panne, sélectionnez **Modifier l'emplacement de stockage**.

Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination.
7. Cliquez sur **Suivant**.
8. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire dans lequel les données restaurées à partir du magasin d'objets seront stockées.
9. Cliquez sur **Suivant**.
10. Vérifiez les détails et cliquez sur **Restaurer**.

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

Informations sur le copyright

Copyright © 2024 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.