



## Référence

### BlueXP backup and recovery

NetApp  
April 18, 2024

# Sommaire

- Référence..... 1
  - Classes de stockage d'archivage AWS S3 et délais de récupération des données ..... 1
  - Niveaux d'archivage Azure et délais de récupération ..... 2
  - Classes de stockage d'archivage Google et temps de récupération ..... 3
  - Configurer la sauvegarde pour l'accès à plusieurs comptes dans Azure ..... 4
  - Restaurez les données de sauvegarde et de restauration BlueXP dans un site invisible ..... 11
  - Redémarrez le service de sauvegarde et de restauration BlueXP ..... 16

# Référence

## Classes de stockage d'archivage AWS S3 et délais de récupération des données

La sauvegarde et la restauration BlueXP prennent en charge deux classes de stockage d'archives S3 et la plupart des régions.

### Classes de stockage d'archivage S3 prises en charge pour la sauvegarde et la restauration BlueXP

Lorsque des fichiers de sauvegarde sont créés initialement, ils sont stockés dans le stockage S3 *Standard*. Il est optimisé pour stocker les données peu utilisées, mais vous pouvez également y accéder immédiatement. Après 30 jours, les sauvegardes passent à la classe de stockage S3 *Standard-Infrequent Access* pour réduire les coûts.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les sauvegardes vers un stockage S3 *Glacier* ou S3 *Glacier Deep Archive* après un certain nombre de jours (généralement plus de 30 jours) pour optimiser les coûts. Vous pouvez régler ce paramètre sur « 0 » ou sur 1-999 jours. Si vous le définissez sur « 0 » jours, vous ne pouvez pas le modifier plus tard à 1-999 jours.

Les données de ces niveaux ne sont pas accessibles immédiatement lorsque cela s'avère nécessaire. Par conséquent, les coûts de récupération sont plus élevés, vous devez déterminer la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section à propos de [restauration des données à partir du stockage d'archivage](#).

- Si vous ne sélectionnez aucun Tier d'archivage dans votre première stratégie de sauvegarde lors de l'activation de la sauvegarde et de la restauration BlueXP, S3 *Glacier* sera votre seule option d'archivage pour les futures stratégies.
- Si vous sélectionnez S3 *Glacier* dans votre première règle de sauvegarde, vous pouvez passer au niveau S3 *Glacier Deep Archive* pour les futures règles de sauvegarde de ce cluster.
- Si vous sélectionnez S3 *Glacier Deep Archive* dans votre première règle de sauvegarde, ce niveau sera le seul Tier d'archivage disponible pour les futures règles de sauvegarde de ce cluster.

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du compartiment dans votre compte AWS.

["Découvrez les classes de stockage S3"](#).

## Restauration des données à partir du stockage d'archivage

Le stockage de fichiers de sauvegarde plus anciens dans un stockage d'archivage est bien moins coûteux que le stockage Standard ou Standard-IA. L'accès aux données à partir d'un fichier de sauvegarde dans un stockage d'archivage à des fins de restauration prendra plus de temps et coûtera plus d'argent.

### Combien coûte la restauration des données à partir d'Amazon S3 Glacier et d'Amazon S3 Glacier ?

Il existe 3 priorités en matière de restauration pour la récupération des données depuis Amazon S3 Glacier et 2 priorités en matière de restauration lors de la récupération des données depuis Amazon S3 Glacier Deep Archive. Les frais d'archivage en profondeur S3 Glacier sont inférieurs à ceux de S3 Glacier :

Tier d'archivage	Restaurer les priorités et les coûts		
	Haut	Standard	Faible
<b>Glacier S3</b>	Récupération plus rapide, coût le plus élevé	Récupération plus lente, coûts réduits	Récupération la plus lente, coût le plus bas
<b>Archive en profondeur du glacier S3</b>		Récupération plus rapide, coûts supérieurs	Récupération plus lente, coûts réduits

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification S3 Glacier par région AWS, rendez-vous sur le ["Page tarifaire d'Amazon S3"](#).

## Combien de temps faut-il pour restaurer mes objets archivés dans Amazon S3 Glacier ?

Deux parties composent la durée totale de restauration :

- **Heure de récupération** : le moment de récupérer le fichier de sauvegarde à partir de l'archive et de le placer dans le stockage standard. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie.

Tier d'archivage	Restauration de la priorité et de l'heure de récupération		
	Haut	Standard	Faible
<b>Glacier S3</b>	3-5 minutes	3-5 heures	5-12 heures
<b>Archive en profondeur du glacier S3</b>		12 heures	48 heures

- **Temps de restauration** : temps de restauration des données à partir du fichier de sauvegarde dans le stockage standard. Ce temps n'est pas différent de l'opération de restauration standard directement depuis le stockage standard - lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Amazon S3 Glacier et S3 Glacier Deep Archive, consultez ["Forum aux questions d'Amazon sur ces classes de stockage"](#).

## Niveaux d'archivage Azure et délais de récupération

La sauvegarde et la restauration BlueXP prennent en charge un Tier d'accès à l'archivage Azure et la plupart des régions.

### Tiers d'accès Azure Blob pris en charge pour la sauvegarde et la restauration BlueXP

Lorsque les fichiers de sauvegarde sont créés initialement, ils sont stockés dans le niveau d'accès *Cool*. Il est optimisé pour le stockage des données rarement utilisées, mais à la demande, il est possible d'y accéder immédiatement.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les sauvegardes entre *Cool* et *Azure Archive Storage* après un certain nombre de jours (généralement plus de 30 jours) afin d'optimiser les coûts. Vous n'avez pas accès immédiatement aux données de ce niveau quand vous en avez besoin. Par conséquent, vos coûts de récupération sont plus élevés. Vous devez donc déterminer la fréquence à laquelle vous devrez restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section suivante sur [restauration des données à partir du stockage d'archivage](#).

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du conteneur dans votre compte Azure.

["Découvrez les niveaux d'accès d'Azure Blob".](#)

## Restauration des données à partir du stockage d'archivage

Le stockage d'anciens fichiers de sauvegarde dans des archives est bien moins coûteux que le stockage Cool, mais l'accès aux données à partir d'un fichier de sauvegarde dans Azure Archive à des fins de restauration prendra plus de temps et coûtera plus cher.

### Combien coûte la restauration des données à partir d'Azure Archive ?

Vous pouvez choisir deux priorités en matière de restauration lors de la récupération des données à partir d'Azure Archive :

- **Élevé** : Récupération la plus rapide, coût plus élevé
- **Standard** : récupération plus lente, coût moindre

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification d'Azure Archive par région Azure, rendez-vous sur la ["Page tarifaire d'Azure"](#).



La priorité élevée n'est pas prise en charge lors de la restauration des données depuis Azure vers les systèmes StorageGRID.

### Quel est le délai de restauration des données archivées dans Azure Archive ?

La durée de restauration est fonction de deux parties :

- **Temps de récupération** : le temps de récupérer le fichier de sauvegarde archivé à partir d'Azure Archive et de le placer dans Cool Storage. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie :
  - **Haut** : < 1 heure
  - **Standard** : < 15 heures
- **Restore Time** : le temps de restauration des données à partir du fichier de sauvegarde dans Cool Storage. Ce temps n'est pas différent de l'opération de restauration typique directement depuis Cool Storage - lorsque vous n'utilisez pas un niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Azure Archive, reportez-vous à ["Forum aux questions sur Azure"](#).

## Classes de stockage d'archivage Google et temps de récupération

La sauvegarde et la restauration BlueXP prennent en charge une classe de stockage d'archivage Google et la plupart des régions.

### Classes de stockage d'archivage Google prises en charge pour la sauvegarde et la restauration BlueXP

Lors de la création initiale des fichiers de sauvegarde, ils sont stockés dans le stockage *Standard*. Il est

optimisé pour stocker les données peu utilisées, mais vous pouvez également y accéder immédiatement.

Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de transférer les sauvegardes plus anciennes vers un stockage *Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours (en général plus de 30 jours) pour optimiser les coûts. Les données de ce niveau nécessitent un coût de récupération plus élevé, vous devez donc déterminer la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section à propos de [restauration des données à partir du stockage d'archivage](#).

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du compartiment dans votre compte Google.

["En savoir plus sur les classes de stockage Google"](#).

## Restauration des données à partir du stockage d'archivage

Le stockage d'anciens fichiers de sauvegarde dans un stockage d'archivage est bien moins coûteux que le stockage standard. En revanche, l'accès aux données à partir d'un fichier de sauvegarde dans le stockage d'archivage à des fins de restauration prendra un peu plus de temps et coûtera plus d'argent.

### Combien coûte la restauration des données à partir de Google Archive ?

Pour obtenir des informations détaillées sur la tarification de Google Cloud Storage par région, rendez-vous sur le ["Page de tarification de Google Cloud Storage"](#).

### Combien de temps faut-il pour restaurer mes objets archivés dans Google Archive ?

Deux parties composent la durée totale de restauration :

- **Temps de récupération** : le temps de récupérer le fichier de sauvegarde à partir de l'archive et de le placer dans le stockage standard. Ce temps est parfois appelé le temps de « réhydratation ». Contrairement aux solutions de stockage les plus inactives des autres fournisseurs de cloud, vos données sont accessibles en quelques millisecondes.
- **Temps de restauration** : temps de restauration des données à partir du fichier de sauvegarde dans le stockage standard. Ce temps n'est pas différent de l'opération de restauration standard directement depuis le stockage standard - lorsque vous n'utilisez pas de niveau d'archivage.

## Configurer la sauvegarde pour l'accès à plusieurs comptes dans Azure

Avec la sauvegarde et la restauration BlueXP, vous pouvez créer des fichiers de sauvegarde sur un compte Azure différent de l'emplacement de vos volumes Cloud Volumes ONTAP source. Ces deux comptes peuvent être différents du compte sur lequel réside le connecteur BlueXP.

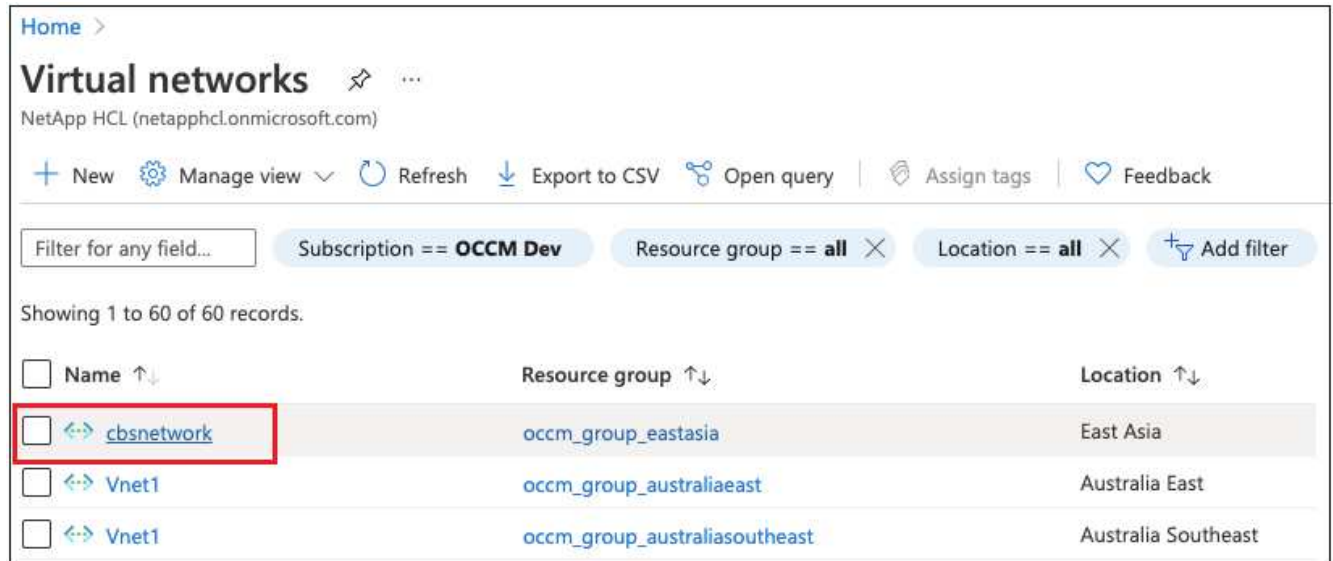
Ces étapes sont requises uniquement lorsque vous l'êtes ["Sauvegarde des données Cloud Volumes ONTAP dans le stockage Azure Blob"](#).

Suivez simplement les étapes ci-dessous pour configurer votre configuration de cette façon.

## Configurez le peering de vnet entre comptes

Notez que si vous souhaitez que BlueXP gère votre système Cloud Volumes ONTAP dans un autre compte/région, vous devez configurer VNet peering. Le peering de vnet n'est pas requis pour la connectivité du compte de stockage.

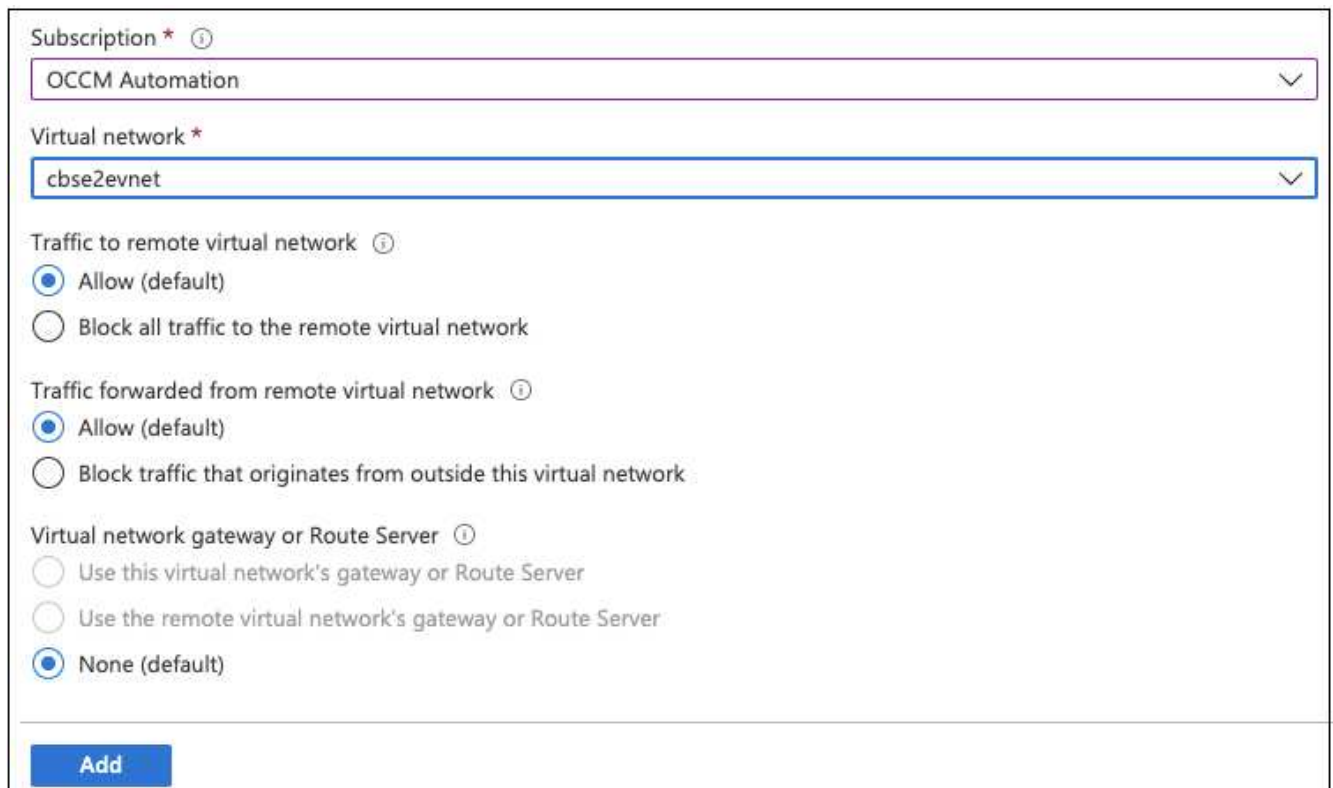
1. Connectez-vous au portail Azure et depuis domicile, sélectionnez Virtual Networks.
2. Sélectionnez l'abonnement que vous utilisez en tant qu'abonnement 1 et cliquez sur le vnet où vous souhaitez configurer le peering.



The screenshot shows the Azure Virtual Networks portal. At the top, there's a 'Home' link and the title 'Virtual networks' with a star icon. Below the title, it says 'NetApp HCL (netapphcl.onmicrosoft.com)'. There are several action buttons: '+ New', 'Manage view' (with a dropdown arrow), 'Refresh' (circular arrow icon), 'Export to CSV' (download icon), 'Open query' (link icon), 'Assign tags' (tag icon), and 'Feedback' (heart icon). Below these buttons is a filter bar with a text input 'Filter for any field...' and three filter buttons: 'Subscription == OCCM Dev', 'Resource group == all', and 'Location == all'. There's also an 'Add filter' button. Below the filter bar, it says 'Showing 1 to 60 of 60 records.' There is a table with three columns: 'Name', 'Resource group', and 'Location'. The first row is highlighted with a red box and contains the following data: Name: 'cbsnetwork', Resource group: 'occm\_group\_eastasia', Location: 'East Asia'. The second row contains: Name: 'Vnet1', Resource group: 'occm\_group\_australiaeast', Location: 'Australia East'. The third row contains: Name: 'Vnet1', Resource group: 'occm\_group\_australiasoutheast', Location: 'Australia Southeast'.

Name	Resource group	Location
cbsnetwork	occm_group_eastasia	East Asia
Vnet1	occm_group_australiaeast	Australia East
Vnet1	occm_group_australiasoutheast	Australia Southeast

3. Sélectionnez **cbsnetwork** et, dans le panneau de gauche, cliquez sur **Peerings**, puis cliquez sur **Add**.



The screenshot shows the 'Add' dialog for VNet peering. It has a 'Subscription' dropdown menu with 'OCCM Automation' selected. Below it is a 'Virtual network' dropdown menu with 'cbse2evnet' selected. There are two sections of radio buttons. The first section is 'Traffic to remote virtual network' with 'Allow (default)' selected and 'Block all traffic to the remote virtual network' unselected. The second section is 'Traffic forwarded from remote virtual network' with 'Allow (default)' selected and 'Block traffic that originates from outside this virtual network' unselected. At the bottom, there is a 'Virtual network gateway or Route Server' section with three options: 'Use this virtual network's gateway or Route Server' (unselected), 'Use the remote virtual network's gateway or Route Server' (unselected), and 'None (default)' (selected). At the bottom left, there is a blue 'Add' button.

4. Entrez les informations suivantes sur la page peering, puis cliquez sur **Ajouter**.

- Nom de la liaison de peering pour ce réseau : vous pouvez donner un nom quelconque afin d'identifier la connexion de peering.
- Nom de la liaison de peering de réseau virtuel distant : entrez un nom pour identifier le vnet distant.
- Conserver toutes les sélections comme valeurs par défaut.
- Sous abonnement, sélectionnez l'abonnement 2.
- Réseau virtuel, sélectionnez le réseau virtuel dans l'abonnement 2 auquel vous souhaitez configurer le peering.

The screenshot shows the 'cbsnetwork | Peerings' page in the Azure portal. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and a Settings section with Address space, Connected devices, Subnets, DDoS protection, Firewall, Security, DNS servers, and Peerings (which is highlighted). The main content area has a search bar, 'Add' and 'Refresh' buttons, and a table of peerings.

Name	Peering status	Peer
cbsnetwork	Connected	cbse2evnet

5. Effectuez les mêmes étapes dans Subscription 2 VNet et spécifiez les détails de l'abonnement et de vnet distant de l'abonnement 1.



Subscription \* ⓘ

OCCM Dev

Virtual network \*

cbsnetwork

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☒ None (default)

Add

Les paramètres de peering sont ajoutés.

cbse2evnet | Peerings ...

Virtual network

Search (Cmd+/) << + Add ↻ Refresh

Filter by name...

Name	Peering status	Peer
cbsnetworkpeer	Connected	cbsnetwork

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

## Créez un terminal privé pour le compte de stockage

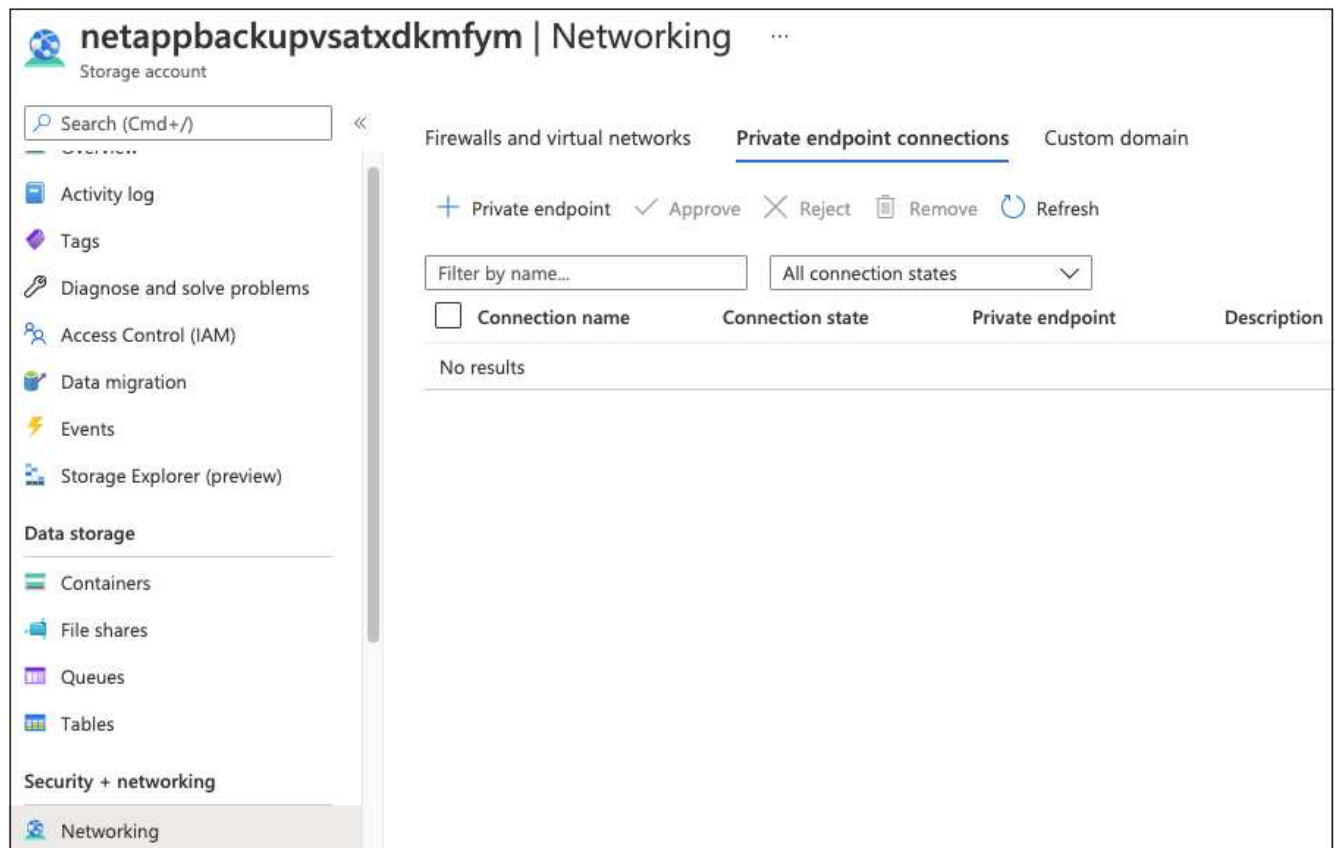
Il est maintenant nécessaire de créer un terminal privé pour le compte de stockage. Dans cet exemple, le compte de stockage est créé dans l'abonnement 1 et le système Cloud Volumes ONTAP fonctionne dans l'abonnement 2.



Vous avez besoin de l'autorisation de contributeur réseau pour effectuer l'action suivante.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

1. Accédez à compte de stockage > mise en réseau > connexions de points de terminaison privés et cliquez sur **+ point de terminaison privé**.



## 2. Dans la page Private Endpoint *Basics* :

- Sélectionnez l'abonnement 2 (où le connecteur BlueXP et le système Cloud Volumes ONTAP sont déployés) et le groupe de ressources.
- Entrez un nom de point final.
- Sélectionnez la région.

### Create a private endpoint

1 Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

**Project details**

Subscription \* ⓘ OCCM Dev

Resource group \* ⓘ cbsoccmdevcvo-rg [Create new](#)

**Instance details**

Name \* cbse2e ✓

Region \* (Asia Pacific) East Asia

## 3. Dans la page *Resource*, sélectionnez sous-ressource cible comme **blob**.

## Create a private endpoint ...

✓ Basics **2 Resource** 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription OCCM Dev (d333af45-0d07-4154-943d-c25fbbce1b18)

Resource type Microsoft.Storage/storageAccounts

Resource test150521

Target sub-resource \* ⓘ

4. Dans la page Configuration :

- Sélectionnez le réseau virtuel et le sous-réseau.
- Cliquez sur le bouton radio **Oui** pour "intégrer à la zone DNS privée".

## Create a private endpoint ...

✓ Basics ✓ Resource **3 Configuration** 4 Tags 5 Review + create

### Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network \* ⓘ

Subnet \* ⓘ

ⓘ If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

### Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net

**Review + create** < Previous Next : Tags >

5. Dans la liste zone DNS privée, assurez-vous que la zone privée est sélectionnée dans la région correcte, puis cliquez sur **Revue + Créer**.

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net
		<input type="text" value="Filter private DNS zones"/> <ul style="list-style-type: none"> <li>occm_group_centralus privatelink.blob.core.windows.net</li> <li>occm_group_eastus privatelink.blob.core.windows.net</li> <li>occm_group_eastus2 privatelink.blob.core.windows.net</li> </ul>

Désormais, le compte de stockage (dans l'abonnement 1) a accès au système Cloud Volumes ONTAP exécuté dans l'abonnement 2.

6. Réessayez d'activer la sauvegarde et la restauration BlueXP sur le système Cloud Volumes ONTAP. Cette fois, vous devriez réussir.

## Restaurez les données de sauvegarde et de restauration BlueXP dans un site invisible

Lors de l'utilisation de la sauvegarde et de la restauration BlueXP sur un site sans accès à Internet, connu sous le nom de *mode privé*, les données de configuration de sauvegarde et de restauration BlueXP sont sauvegardées dans le compartiment StorageGRID ou ONTAP S3 où sont stockées vos sauvegardes. En cas de problème avec le système hôte du connecteur BlueXP, vous pouvez déployer un nouveau connecteur et restaurer les données de sauvegarde et de restauration BlueXP stratégiques.

Notez que lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un environnement SaaS où le connecteur BlueXP est déployé dans votre fournisseur cloud ou sur votre propre système hôte disposant d'un accès Internet, toutes les données importantes de configuration de la sauvegarde et de la restauration BlueXP sont sauvegardées et protégées dans le cloud. Si vous rencontrez un problème avec le connecteur, il vous suffit de créer un nouveau connecteur et d'ajouter vos environnements de travail. Les détails de la sauvegarde sont automatiquement restaurés.

Il existe 2 types de données sauvegardées :

- Base de données de sauvegarde et de restauration BlueXP : contient la liste de tous les volumes, fichiers de sauvegarde, règles de sauvegarde et informations de configuration.
- Fichiers de catalogue indexés : contient des index détaillés qui sont utilisés pour la fonctionnalité de recherche et de restauration qui rendent vos recherches très rapides et efficaces lors de la recherche de données de volume que vous souhaitez restaurer.

Ces données sont sauvegardées une fois par jour à minuit, et un maximum de 7 copies de chaque fichier sont conservées. Si le connecteur gère plusieurs environnements de travail ONTAP sur site, les fichiers de

sauvegarde et de restauration BlueXP seront situés dans le compartiment de l'environnement de travail qui a été activé en premier.



Aucune donnée de volume n'est jamais incluse dans la base de données de sauvegarde et de restauration BlueXP ou dans les fichiers de catalogue indexés.

## Restaurez les données de sauvegarde et de restauration BlueXP sur un nouveau connecteur

Si votre connecteur sur site présente une défaillance majeure, vous devrez installer un nouveau connecteur, puis restaurer les données de sauvegarde et de restauration BlueXP sur le nouveau connecteur.

Pour rétablir votre système de sauvegarde et de restauration BlueXP opérationnel, vous devez effectuer 4 tâches :

- Installez un nouveau connecteur BlueXP
- Restaurez la base de données de sauvegarde et de restauration BlueXP
- Restaurez les fichiers de catalogue indexés
- Redécouvrez tous vos systèmes ONTAP et StorageGRID sur site dans l'interface utilisateur BlueXP

Une fois que vous avez vérifié que votre système est de nouveau en bon état de fonctionnement, nous vous recommandons de créer de nouveaux fichiers de sauvegarde.

### Ce dont vous avez besoin

Vous devez accéder aux sauvegardes de base de données et d'index les plus récentes à partir du compartiment StorageGRID ou ONTAP S3 où vos fichiers de sauvegarde sont stockés :

- Sauvegarde et restauration BlueXP fichier de base de données MySQL

Ce fichier se trouve à l'emplacement suivant dans le compartiment `netapp-backup-<GUID>/mysql_backup/`, et il est nommé `CBS_DB_Backup_<day>_<month>_<year>.sql`.

- Fichier zip de sauvegarde du catalogue indexé

Ce fichier se trouve à l'emplacement suivant dans le compartiment `netapp-backup-<GUID>/catalog_backup/`, et il est nommé `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`.

### Installez un nouveau connecteur sur un nouvel hôte Linux sur site

Lors de l'installation d'un nouveau connecteur BlueXP, assurez-vous de télécharger la même version de logiciel que celle installée sur le connecteur d'origine. Les modifications périodiques de la structure de la base de données de sauvegarde et de restauration BlueXP peuvent rendre incompatibles les nouvelles versions logicielles avec les sauvegardes de base de données d'origine. C'est possible ["Mettez à niveau le logiciel du connecteur vers la version la plus récente après avoir restauré la base de données de sauvegarde"](#).

1. ["Installez le connecteur BlueXP sur un nouvel hôte Linux sur site"](#)
2. Connectez-vous à BlueXP à l'aide des informations d'identification utilisateur administrateur que vous venez de créer.

## Restaurez la base de données de sauvegarde et de restauration BlueXP

1. Copiez la sauvegarde MySQL de l'emplacement de sauvegarde vers le nouvel hôte de connecteur. Nous utiliserons le nom de fichier exemple « CBS\_DB\_Backup\_23\_05\_2023.sql » ci-dessous.
2. Copiez la sauvegarde dans le conteneur MySQL docker à l'aide de la commande suivante :

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Entrez le shell du conteneur MySQL à l'aide de la commande suivante :

```
docker exec -it ds_mysql_1 sh
```

4. Dans le conteneur, déployez l'« env ».
5. Vous aurez besoin du mot de passe MySQL DB, donc copiez la valeur de la clé "MYSQL\_ROOT\_PASSWORD".
6. Restaurez la base de données MySQL de sauvegarde et de restauration BlueXP à l'aide de la commande suivante :

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Vérifiez que la base de données MySQL de sauvegarde et de restauration BlueXP a été correctement restaurée à l'aide des commandes SQL suivantes :

```
mysql -u root -p cloud_backup
```

Saisissez le mot de passe.

```
mysql> show tables;  
mysql> select * from volume;
```

Vérifiez si les volumes affichés sont identiques à ceux qui existaient dans votre environnement d'origine.

## Restaurez les fichiers de catalogue indexés

1. Copiez le fichier zip de sauvegarde du catalogue indexé (nous utiliserons l'exemple de nom de fichier « Indexed\_Catalog\_DB\_Backup\_catalogdb1\_23\_05\_2023.zip ») de l'emplacement de sauvegarde vers le nouvel hôte du connecteur dans le dossier « /opt/application/netapp/cbs ».
2. Décompressez le fichier « Indexed\_Catalog\_DB\_Backup\_catalogdb1\_23\_05\_2023.zip » à l'aide de la commande suivante :

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Exécutez la commande **ls** pour vous assurer que le dossier "catalog 1" a été créé avec les sous-dossiers "modifications" et "instantanés" ci-dessous.

## Découvrir les clusters ONTAP et les systèmes StorageGRID

1. "Découvrez tous les environnements de travail ONTAP sur site" qui étaient disponibles dans votre environnement précédent. Cela inclut le système ONTAP que vous avez utilisé comme serveur S3.
2. "Découvrir vos systèmes StorageGRID".

## Configurer les détails de l'environnement StorageGRID

Ajoutez les détails du système StorageGRID associé à vos environnements de travail ONTAP tels qu'ils ont été configurés dans la configuration du connecteur d'origine à l'aide du "API BlueXP".

Ces étapes sont nécessaires pour chaque système ONTAP qui sauvegarde des données sur StorageGRID.

1. Extrayez le jeton d'autorisation à l'aide de l'API oauth/token suivante.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100101 Firefox/108.0' -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '{"username":admin@netapp.com,"password":"Netapp@123","grant_type":"password"}'> '
```

Cette API renvoie une réponse comme suit. Vous pouvez récupérer le jeton d'autorisation comme indiqué ci-dessous.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiaXVkiJpbImh0dHBzOi8vYXBpLmNsb3Vklm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3Vklm5ldGFwcC5jb20vZnVsbF9uYW11IjoIYWRTaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWx1IiwiaWF0IjoxNjc5NzM2MDIzLCJleHAiOjE2NzI3NTc2MjMsIm1zcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CjtrRDY23PokyLglif67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-114v_pNDsPyNDyWqHaKizThdjJHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5ykoDNDmrv5At_f9HHp0-xVMYHqywZ4nNFalMvAh4xESc5jfoKOZc-IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSolIwIeHXZJJV-Uswun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoelFg3ch--7JFkFl-rrXDOjklSUmumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Extrayez l'ID de l'environnement de travail et l'ID-agent-X à l'aide de l'API location/externe/ressource.



```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxiwiYXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW11IjoieYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWx1IiwiaWF0IjoxNjc5NzIyNzEzLCJleHAiOiE2NzI3NDQzMtMTsImlzcyl6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdsWjWcNvw2rRkFzjHpWrETgfgAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVYjbBL4krOewgKHGfo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRdstcFgJLdJHtowweNH2829KsjEGBTtcBd08SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Cette API renvoie une réponse comme suit. La valeur sous "resourcelidentfier" désigne l'ID *WorkingEnvironment* et la valeur sous "agentID" indique *x-agent-ID*.

3. Mettez à jour la base de données de sauvegarde et de restauration BlueXP avec les détails du système StorageGRID associé aux environnements de travail. Veillez à saisir le nom de domaine complet du StorageGRID, ainsi que la clé d'accès et la clé de stockage, comme indiqué ci-dessous :

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxiwiYXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW11IjoieYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWx1IiwiaWF0IjoxNjc5NzIyNzEzLCJleHAiOiE2NzI3NDQzMtMTsImlzcyl6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdsWjWcNvw2rRkFzjHpWrETgfgAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVYjbBL4krOewgKHGfo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRdstcFgJLdJHtowweNH2829KsjEGBTtcBd08SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfB1LIhqDgIPA0wclients' \
> -d '{
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }' }
```

## Vérifiez les paramètres de sauvegarde et de restauration BlueXP

1. Sélectionnez chaque environnement de travail ONTAP et cliquez sur **Afficher les sauvegardes** en regard du service de sauvegarde et de restauration dans le panneau de droite.

Vous devriez pouvoir voir toutes les sauvegardes qui ont été créées pour vos volumes.

2. Dans le Tableau de bord de restauration, sous la section Rechercher et restaurer, cliquez sur **Paramètres d'indexation**.

Assurez-vous que les environnements de travail où le catalogage indexé est activé précédemment restent activés.

3. À partir de la page Rechercher et restaurer, exécutez quelques recherches de catalogue pour confirmer que la restauration du catalogue indexé a bien été effectuée.

## Redémarrez le service de sauvegarde et de restauration BlueXP

Dans certains cas, vous devrez peut-être redémarrer le service de sauvegarde et de restauration BlueXP.

La fonctionnalité de sauvegarde et de restauration BlueXP est intégrée au connecteur BlueXP. Vous devrez suivre différentes étapes initiales pour redémarrer le service selon que vous avez déployé le connecteur dans le cloud ou si vous avez installé le connecteur manuellement sur un système Linux.

### Étapes

1. Connectez-vous au système Linux sur lequel le connecteur s'exécute.

Emplacement du connecteur	Procédure
Déploiement cloud	Suivez les instructions de la section " <a href="#">Connexion à la machine virtuelle Connector Linux</a> " en fonction du fournisseur cloud que vous utilisez.
Installation manuelle	Connectez-vous au système Linux.

2. Entrez la commande pour redémarrer le service.

Emplacement du connecteur	Commande
Déploiement cloud	<code>docker restart cloudmanager_cbs</code>
Installation manuelle avec accès à Internet	<code>docker restart cloudmanager_cbs</code>
Installation manuelle sans accès à Internet	<code>docker restart ds_cloudmanager_cbs_1</code>

## 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.