



# **Documentation Cloud Backup**

## **Cloud Backup**

NetApp  
December 15, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/gcp/index.html> on December 15, 2022. Always check docs.netapp.com for the latest.

# Table des matières

Documentation Cloud Backup .....	1
Quelles sont les nouveautés de la sauvegarde dans le cloud .....	2
6 décembre 2022 .....	2
2 novembre 2022 .....	3
28 septembre 2022 .....	4
19 septembre 2022 .....	5
18 août 2022 .....	6
13 juillet 2022 .....	7
14 juin 2022 .....	7
2 mai 2022 .....	9
4 avril 2022 .....	10
3 mars 2022 .....	10
14 février 2022 .....	10
2 janvier 2022 .....	11
Commencez .....	12
Découvrir Cloud Backup .....	12
Configuration des licences pour Cloud Backup .....	14
Surveillance de l'état des tâches de sauvegarde et de restauration .....	19
Sauvegarde et restauration des données ONTAP .....	22
Protection des données du cluster ONTAP à l'aide de Cloud Backup .....	22
Sauvegarde des données Cloud Volumes ONTAP dans Google Cloud Storage .....	30
Sauvegarde des données ONTAP sur site dans Google Cloud Storage .....	37
La sauvegarde des données ONTAP sur site dans StorageGRID .....	47
Gestion des sauvegardes de vos systèmes ONTAP .....	56
Gestion des paramètres de sauvegarde au niveau du cluster .....	76
Restauration de données ONTAP à partir des fichiers de sauvegarde .....	81
Sauvegarde et restauration des données Kubernetes .....	101
Protection des données du cluster Kubernetes à l'aide de Cloud Backup .....	101
Sauvegarde des données de volume persistant Kubernetes dans un stockage Google Cloud .....	105
Gestion des sauvegardes pour vos systèmes Kubernetes .....	110
Restauration de données Kubernetes à partir de fichiers de sauvegarde .....	121
Sauvegarde et restauration des données des applications .....	124
Sauvegarde et restauration des données des applications sur site .....	124
Sauvegarde et restauration des données d'applications cloud natives .....	137
Sauvegarde et restauration des données des ordinateurs virtuels .....	150
Protection des données des machines virtuelles .....	150
Enregistrez le plug-in SnapCenter pour VMware vSphere .....	151
Créez une règle pour sauvegarder des machines virtuelles .....	152
Sauvegarde des datastores sur StorageGRID .....	152
Gérer la protection des machines virtuelles .....	153
Restaurer des machines virtuelles à partir du cloud .....	155
API Cloud Backup .....	156
Pour commencer .....	156

Exemple d'utilisation des API . . . . .	158
Référence API . . . . .	160
Référence . . . . .	162
Paramètres de configuration de la politique de Cloud Backup . . . . .	162
Classes de stockage d'archivage AWS S3 et délais de récupération des données . . . . .	167
Niveaux d'archivage Azure et délais de récupération . . . . .	169
Classes de stockage d'archivage Google et temps de récupération . . . . .	170
Configurer la sauvegarde pour l'accès à plusieurs comptes dans Azure . . . . .	171
Connaissances et support . . . . .	179
S'inscrire pour obtenir de l'aide . . . . .	179
Obtenez de l'aide . . . . .	183
Mentions légales . . . . .	187
Droits d'auteur . . . . .	187
Marques déposées . . . . .	187
Brevets . . . . .	187
Politique de confidentialité . . . . .	187
Source ouverte . . . . .	187

# Documentation Cloud Backup

# Quelles sont les nouveautés de la sauvegarde dans le cloud

Découvrez les nouveautés de Cloud Backup.

## 6 décembre 2022

### Modifications du point de terminaison d'accès Internet sortant du connecteur requises

Du fait d'un changement dans Cloud Backup, vous devez modifier les terminaux de connecteur suivants pour assurer la réussite des opérations de sauvegarde dans le cloud :

Ancien terminal	Nouveau terminal
https://cloudmanager.cloud.netapp.com	https://api.bluelxp.netapp.com
https://*.cloudmanager.cloud.netapp.com	https://*.api.bluelxp.netapp.com

Consultez la liste complète des terminaux de votre ["AWS"](#), ["Google Cloud"](#), ou ["Azure"](#) de cloud hybride.

### Prise en charge de la sélection de la classe de stockage d'archivage Google dans l'interface utilisateur

Les fichiers de sauvegarde sont initialement créés dans la classe de stockage Google Standard. Vous pouvez désormais utiliser l'interface utilisateur de Cloud Backup pour transférer les anciennes sauvegardes vers le stockage Google Archive après un certain nombre de jours afin d'optimiser les coûts.

Cette fonctionnalité est actuellement prise en charge par les clusters ONTAP sur site avec ONTAP 9.12.1 (ou version ultérieure). Elle n'est pas actuellement disponible pour les systèmes Cloud Volumes ONTAP.

### Prise en charge des volumes FlexGroup

Cloud Backup prend désormais en charge la sauvegarde et la restauration des volumes FlexGroup. Avec ONTAP 9.12.1 ou version supérieure, vous pouvez sauvegarder des volumes FlexGroup sur un stockage de cloud public et privé. Si vous disposez d'environnements de travail intégrant des FlexVol et des volumes FlexGroup, vous pouvez sauvegarder tous les volumes FlexGroup sur ces systèmes une fois la mise à jour du logiciel ONTAP effectuée.

["Consultez la liste complète des types de volumes pris en charge"](#).

### Possibilité de restaurer les données à partir de sauvegardes vers un agrégat spécifique sur les systèmes Cloud Volumes ONTAP

Dans les versions précédentes, vous pouviez sélectionner l'agrégat uniquement lors de la restauration des données sur des systèmes ONTAP sur site. Cette fonctionnalité fonctionne désormais lors de la restauration des données sur des systèmes Cloud Volumes ONTAP.

## 2 novembre 2022

### Possibilité d'exporter d'anciennes copies Snapshot dans vos fichiers de sauvegarde de base

Si des copies Snapshot locales des volumes de votre environnement de travail correspondent aux étiquettes de votre planning de sauvegarde (par exemple, quotidienne, hebdomadaire, etc.), vous pouvez exporter ces snapshots historiques vers le stockage objet sous forme de fichiers de sauvegarde. Cela vous permet d'initialiser vos sauvegardes dans le cloud en déplaçant d'anciennes copies Snapshot vers la copie de sauvegarde de base.

Cette option est disponible lors de l'activation de Cloud Backup pour vos environnements de travail. Vous pouvez également modifier ce paramètre ultérieurement dans ["Page Paramètres avancés"](#).

### Cloud Backup peut désormais être utilisé pour l'archivage des volumes dont vous n'avez plus besoin sur le système source

Vous pouvez maintenant supprimer la relation de sauvegarde d'un volume. Vous disposez ainsi d'un mécanisme d'archivage pour arrêter la création de nouveaux fichiers de sauvegarde et supprimer le volume source, mais conserver tous les fichiers de sauvegarde existants. Cela vous permet de restaurer ultérieurement le volume à partir du fichier de sauvegarde, si nécessaire, tout en libérant de l'espace du système de stockage source. ["Découvrez comment"](#).

### Le service de support a été ajouté pour recevoir les alertes Cloud Backup par e-mail et dans le centre de notification

Cloud Backup a été intégré au service BlueXP notification. Vous pouvez afficher les notifications Cloud Backup en cliquant sur la cloche de notification dans la barre de menus BlueXP. Vous pouvez également configurer BlueXP pour envoyer des notifications par e-mail en tant qu'alertes afin de vous informer de l'activité système importante, même lorsque vous n'êtes pas connecté au système. Cet e-mail peut être envoyé aux destinataires qui doivent connaître les activités de sauvegarde et de restauration. ["Découvrez comment"](#).

### La nouvelle page Paramètres avancés vous permet de modifier les paramètres de sauvegarde au niveau du cluster

Cette nouvelle page vous permet de modifier de nombreux paramètres de sauvegarde au niveau du cluster que vous avez définis lors de l'activation de Cloud Backup pour chaque système ONTAP. Vous pouvez également modifier certains paramètres appliqués comme paramètres de sauvegarde par défaut. L'ensemble des paramètres de sauvegarde que vous pouvez modifier comprend :

- Les clés de stockage qui donnent à votre système ONTAP l'autorisation d'accéder au stockage objet
- Bande passante réseau allouée pour télécharger les sauvegardes dans le stockage objet
- Paramètre de sauvegarde automatique (et règle) pour les volumes futurs
- Classe de stockage d'archivage (AWS uniquement)
- Indique si des copies Snapshot historiques sont incluses dans les fichiers de sauvegarde de base initiaux
- Si les snapshots « annuels » sont supprimés du système source
- L'IPspace ONTAP connecté au stockage objet (en cas de sélection incorrecte lors de l'activation)

["En savoir plus sur la gestion des paramètres de sauvegarde au niveau du cluster"](#).

## **Vous pouvez désormais restaurer des fichiers de sauvegarde à l'aide de la fonction de recherche et de restauration lors de l'utilisation d'un connecteur sur site**

Dans la version précédente, la prise en charge a été ajoutée pour créer des fichiers de sauvegarde dans le cloud public lorsque le connecteur est déployé sur site. Dans cette version, le service de support a continué d'être utilisé pour restaurer des sauvegardes à partir d'Amazon S3 ou d'Azure Blob lorsque le connecteur est déployé sur site. La fonction de recherche et restauration prend également en charge la restauration des sauvegardes depuis les systèmes StorageGRID vers les systèmes ONTAP sur site.

À l'heure actuelle, le connecteur doit être déployé dans Google Cloud Platform lorsque vous utilisez les fonctions de recherche et de restauration pour restaurer des sauvegardes à partir de Google Cloud Storage.

## **La page surveillance des travaux a été mise à jour**

Les mises à jour suivantes ont été effectuées sur le ["Surveillance des travaux"](#):

- Une colonne pour « charge de travail » est disponible. Vous pouvez donc filtrer la page pour afficher les travaux des services de sauvegarde suivants : volumes, applications, machines virtuelles et Kubernetes.
- Vous pouvez ajouter de nouvelles colonnes pour « Nom d'utilisateur » et « Type de travail » si vous souhaitez afficher ces détails pour une tâche de sauvegarde spécifique.
- La page Détails du travail affiche tous les sous-travaux en cours d'exécution pour terminer le travail principal.
- La page est automatiquement réactualisée toutes les 15 minutes pour que vous puissiez toujours voir les derniers résultats d'état des travaux. Et vous pouvez cliquer sur le bouton **Actualiser** pour mettre la page à jour immédiatement.

## **Améliorations de la sauvegarde entre plusieurs comptes AWS**

Si vous souhaitez utiliser un autre compte AWS pour vos sauvegardes Cloud Volumes ONTAP que celui que vous utilisez pour les volumes source, vous devez ajouter les identifiants de compte AWS de destination dans BlueXP. Vous devez également ajouter les autorisations « s3:PutBuckePolicy » et « s3:PutketOwnershipControls » au rôle qui fournit BlueXP avec les autorisations. Auparavant, il fallait configurer de nombreux paramètres sur la console AWS. Plus besoin de le faire.

## **28 septembre 2022**

### **Améliorations de Cloud Backup pour les applications**

- Prise en charge de Google Cloud Platform (GCP) et de StorageGRID pour sauvegarder des copies Snapshot cohérentes au niveau des applications
- Création de règles personnalisées
- Prend en charge le stockage d'archivage
- Sauvegarde des applications SAP HANA
- Sauvegardez les applications Oracle et SQL qui se trouvent sur l'environnement VMware
- Sauvegarder les applications à partir d'un système de stockage secondaire sur site
- Désactiver les sauvegardes
- Annuler l'enregistrement du serveur SnapCenter

## Améliorations de Cloud Backup pour les machines virtuelles

- Prend en charge StorageGRID pour sauvegarder un ou plusieurs datastores
- Création de règles personnalisées

## 19 septembre 2022

### **Vous pouvez configurer le verrouillage des données et les attaques par ransomware pour les fichiers de sauvegarde dans les systèmes StorageGRID**

La dernière version a introduit *DataLock et ransomware protection* pour les sauvegardes stockées dans des compartiments Amazon S3. Cette version étend la prise en charge des fichiers de sauvegarde stockés dans les systèmes StorageGRID. Si votre cluster utilise ONTAP 9.11.1 ou version ultérieure et que votre système StorageGRID exécute la version 11.6.0.3 ou ultérieure, cette nouvelle option de règles de sauvegarde est disponible. ["Découvrez comment protéger vos sauvegardes avec DataLock et des attaques par ransomware"](#).

Notez que vous devrez exécuter un connecteur avec la version 3.9.22 ou une version ultérieure du logiciel. Le connecteur doit être installé dans vos locaux et peut être installé sur un site avec ou sans accès à Internet.

### **La restauration au niveau des dossiers est désormais disponible à partir de vos fichiers de sauvegarde**

Vous pouvez maintenant restaurer un dossier à partir d'un fichier de sauvegarde si vous avez besoin d'accéder à tous les fichiers de ce dossier (répertoire ou partage). La restauration d'un dossier est bien plus efficace que la restauration d'un volume entier. Cette fonctionnalité est disponible pour les opérations de restauration à l'aide de la méthode Parcourir et restaurer et de la méthode Rechercher et restaurer lors de l'utilisation de ONTAP 9.11.1 ou version ultérieure. Pour le moment, vous ne pouvez sélectionner et restaurer qu'un seul dossier, et seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans des sous-dossiers, n'est restauré.

### **La restauration au niveau des fichiers est désormais disponible à partir des sauvegardes qui ont été transférées vers le stockage d'archivage**

Auparavant, il était possible de restaurer uniquement les volumes à partir des fichiers de sauvegarde déplacés vers un stockage d'archivage (AWS et Azure uniquement). Vous pouvez désormais restaurer des fichiers individuels à partir de ces fichiers de sauvegarde archivés. Cette fonctionnalité est disponible pour les opérations de restauration à l'aide de la méthode Parcourir et restaurer et de la méthode Rechercher et restaurer lors de l'utilisation de ONTAP 9.11.1 ou version ultérieure.

### **La restauration au niveau des fichiers offre désormais la possibilité d'écraser le fichier source d'origine**

Par le passé, un fichier restauré sur le volume d'origine a toujours été restauré en tant que nouveau fichier avec le préfixe « Restore\_<nom\_fichier> ». Vous pouvez maintenant choisir d'écraser le fichier source d'origine lors de la restauration du fichier à l'emplacement d'origine du volume. Cette fonctionnalité est disponible pour les opérations de restauration à l'aide de la méthode Browse & Restore et de la méthode Search & Restore.



## Effectuez un glisser-déposer pour activer la sauvegarde dans le cloud sur les systèmes StorageGRID

Si le "StorageGRID" Destination de vos sauvegardes existe en tant qu'environnement de travail sur la toile. Vous pouvez faire glisser votre environnement de travail ONTAP sur site vers la destination pour lancer l'assistant de configuration de Cloud Backup.

## 18 août 2022

### Des fonctionnalités de prise en charge ont été ajoutées pour protéger les données d'applications 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 BlueXP offre des sauvegardes et des restaurations efficaces et cohérentes avec les applications, basées sur des règles, de bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP.<https://docs.netapp.com/us-en/cloud-manager-backup-restore/concept-protect-cloud-app-data-to-cloud.html>["En savoir plus >>^"].

### La fonction de recherche et de restauration est désormais prise en charge avec les fichiers de sauvegarde dans Azure Blob

La méthode de recherche et de restauration des volumes et des fichiers est désormais disponible pour les utilisateurs qui stockent leurs fichiers de sauvegarde dans le stockage Azure Blob. ["Découvrez comment restaurer vos volumes et fichiers à l'aide de Search Restore"](#).

Notez que des autorisations supplémentaires sont nécessaires dans le rôle connecteur pour utiliser cette fonctionnalité. Un connecteur déployé avec la version 3.9.21 du logiciel (août 2022) inclut ces autorisations. Vous devrez ajouter manuellement les autorisations si vous avez déployé le connecteur à l'aide d'une version antérieure. ["Voir comment ajouter ces autorisations, si nécessaire"](#).

### Nous avons ajouté la possibilité de protéger vos fichiers de sauvegarde contre les suppressions et les attaques par ransomware

Cloud Backup dispose désormais de la prise en charge du verrouillage des objets pour les sauvegardes sécurisées par ransomware. Si votre cluster utilise ONTAP 9.11.1 ou version ultérieure et que votre destination de sauvegarde est Amazon S3, une nouvelle option de stratégie de sauvegarde appelée *DataLock et protection contre les attaques par ransomware* est maintenant disponible. DataLock protège vos fichiers de sauvegarde contre la modification ou la suppression, et la protection contre les ransomwares analyse vos fichiers de sauvegarde pour rechercher des signes d'attaque par ransomware sur vos fichiers de sauvegarde. ["Découvrez comment protéger vos sauvegardes avec DataLock et des attaques par ransomware"](#).

Notez que des autorisations supplémentaires sont nécessaires dans le rôle connecteur pour utiliser cette fonctionnalité. Un connecteur déployé à l'aide du logiciel version 3.9.21 inclut ces autorisations. Vous devrez ajouter manuellement les autorisations si vous avez déployé le connecteur à l'aide d'une version antérieure. ["Voir comment ajouter ces autorisations, si nécessaire"](#).

### Cloud Backup prend désormais en charge les règles créées à l'aide d'étiquettes SnapMirror personnalisées

Apravant, Cloud Backup prenait uniquement en charge les étiquettes SnapMirror prédéfinies : toutes les heures, tous les jours, toutes les semaines, toutes les heures et tous les ans. Désormais, Cloud Backup peut

détecter les règles SnapMirror qui comportent des étiquettes SnapMirror personnalisées que vous avez créées à l'aide de System Manager ou de l'interface de ligne de commande. Ces nouvelles étiquettes sont accessibles dans l'interface utilisateur de Cloud Backup, ce qui vous permet de sauvegarder des volumes avec le label SnapMirror de votre choix dans le cloud.

## **Autres améliorations de la politique de sauvegarde pour les systèmes ONTAP**

Certaines pages de stratégie de sauvegarde ont été redessinées afin de faciliter l'affichage de toutes les règles de sauvegarde disponibles pour les volumes de chaque cluster ONTAP. Vous pouvez ainsi consulter les détails des règles disponibles de façon à appliquer les meilleures règles à vos volumes.

## **Effectuez un glisser-déposer pour activer Cloud Backup sur Azure Blob et Google Cloud Storage**

Si le "[Blob d'Azure](#)" ou "[Google Cloud Storage](#)" La destination de vos sauvegardes existe en tant qu'environnement de travail sur la toile. Vous pouvez faire glisser votre environnement de travail ONTAP ou Cloud Volumes ONTAP sur site (installé dans Azure ou GCP) vers la destination pour lancer l'assistant de configuration de la sauvegarde.

Cette fonctionnalité existe déjà pour les compartiments Amazon S3.

## **13 juillet 2022**

### **La prise en charge a été ajoutée pour la sauvegarde des volumes SnapLock Enterprise**

Vous pouvez désormais utiliser Cloud Backup pour sauvegarder des volumes SnapLock Enterprise dans des clouds publics et privés. Cette fonctionnalité requiert que votre système ONTAP exécute ONTAP 9.11.1 ou une version ultérieure. Cependant, les volumes de conformité SnapLock ne sont pas pris en charge actuellement.

### **Vous pouvez désormais créer des fichiers de sauvegarde dans le cloud public lorsque vous utilisez un connecteur sur site**

Auparavant, vous deviez déployer le connecteur dans le même fournisseur de cloud que où vous créez des fichiers de sauvegarde. Un connecteur déployé dans votre environnement sur site permet désormais de créer des fichiers de sauvegarde à partir de systèmes ONTAP sur site vers Amazon S3, Azure Blob et Google Cloud Storage. (Un connecteur sur site était toujours nécessaire pour créer des fichiers de sauvegarde sur les systèmes StorageGRID.)

### **Des fonctionnalités supplémentaires sont disponibles lors de la création de stratégies de sauvegarde pour les systèmes ONTAP**

- Nous pouvons maintenant sauvegarder chaque année. La valeur de conservation par défaut est 1 pour les sauvegardes annuelles, mais vous pouvez modifier cette valeur si vous souhaitez accéder à de nombreux fichiers de sauvegarde des années précédentes.
- Vous pouvez nommer vos stratégies de sauvegarde de façon à ce que vous puissiez identifier vos stratégies avec un texte plus descriptif.

## **14 juin 2022**

## Un service de support a été ajouté pour sauvegarder les données d'un cluster ONTAP sur site dans des sites sans accès à Internet

Si votre cluster ONTAP sur site se trouve sur un site sans accès à Internet ou hors ligne, vous pouvez maintenant utiliser Cloud Backup pour sauvegarder des données de volume sur un système NetApp StorageGRID qui réside sur le même site. Cette fonctionnalité nécessite que le connecteur BlueXP (version 3.9.19 ou ultérieure) soit également déployé sur le site hors ligne.

["Découvrez comment installer le connecteur dans votre site hors ligne"](https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html). <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html>["Découvrez comment sauvegarder des données ONTAP dans StorageGRID sur un site hors ligne"]].

## Cloud Backup pour machines virtuelles 1.1.0 est désormais GA

Vous pouvez protéger les données de vos machines virtuelles en intégrant le plug-in SnapCenter pour VMware vSphere avec BlueXP. Vous pouvez sauvegarder des datastores dans le cloud et restaurer facilement les serveurs virtuels depuis le plug-in SnapCenter sur site pour VMware vSphere.

["En savoir plus sur la protection des machines virtuelles dans le cloud"](#).

## L'instance de restauration dans le cloud n'est pas requise pour la fonctionnalité ONTAP Browse & Restore

Une instance Cloud Restore/machine virtuelle séparée, utilisée pour les opérations de navigation et de restauration au niveau des fichiers à partir de S3 et du stockage Blob. Cette instance s'est arrêtée lorsqu'elle n'est pas utilisée — mais elle a encore ajouté du temps et des coûts lors de la restauration des fichiers. Cette fonctionnalité a été remplacée par un conteneur sans coût qui est déployé sur le connecteur en cas de besoin. Il offre les avantages suivants :

- Aucun coût supplémentaire pour les opérations de restauration au niveau des fichiers
- Accélération des opérations de restauration au niveau des fichiers
- Prise en charge des opérations Browse & Restore pour les fichiers provenant du cloud lorsque le connecteur est installé sur votre site

Notez que l'instance/la machine virtuelle de Cloud Restore est automatiquement supprimée si vous l'utilisez auparavant. Un processus de sauvegarde dans le cloud s'exécute une fois par jour pour supprimer toutes les anciennes instances de restauration cloud. Ce changement est complètement transparent — il n'y a pas d'impact sur vos données et vous ne remarquerez aucune modification de vos tâches de sauvegarde ou de restauration.

## Parcourir et restaurer les fichiers pris en charge par Google Cloud et StorageGRID Storage

En ajoutant le conteneur pour les opérations de navigation et de restauration (comme décrit ci-dessus), les opérations de restauration de fichiers peuvent désormais être effectuées à partir de fichiers de sauvegarde stockés dans les systèmes Google Cloud et StorageGRID. Désormais, l'option Browse & Restore permet de restaurer des fichiers entre tous les fournisseurs de cloud public et depuis StorageGRID. ["Découvrez comment utiliser Browse ; Restore pour restaurer des volumes et des fichiers à partir de vos sauvegardes ONTAP"](#).

## Effectuez un glisser-déposer pour activer Cloud Backup sur le stockage S3

Si la destination Amazon S3 pour vos sauvegardes existe dans l'environnement de travail sur la Canvas, vous pouvez faire glisser votre cluster ONTAP sur site ou votre système Cloud Volumes ONTAP (installé dans AWS)

vers l'environnement de travail Amazon S3 pour lancer l'assistant d'installation.

## **Appliquez automatiquement une règle de sauvegarde aux volumes créés dans les clusters Kubernetes**

Si vous avez ajouté de nouveaux volumes persistants à vos clusters Kubernetes après l'activation de Cloud Backup, il fallait auparavant vous rappeler de configurer les sauvegardes de ces volumes. Vous pouvez maintenant sélectionner une règle qui sera appliquée automatiquement aux nouveaux volumes créés "[À partir de la page Backup Settings](#)" Pour les clusters qui ont déjà activé Cloud Backup.

## **Les API Cloud Backup sont désormais disponibles pour la gestion des opérations de sauvegarde et de restauration**

Les API sont disponibles à l'adresse <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>. Voir "[cette page](#)" Pour un aperçu des API.

## **2 mai 2022**

## **La fonction de recherche et de restauration est désormais prise en charge avec les fichiers de sauvegarde dans Google Cloud Storage**

La méthode de recherche et de restauration des volumes et des fichiers a été introduite en avril pour les utilisateurs qui stockent leurs fichiers de sauvegarde dans AWS. Une fonctionnalité est désormais disponible pour les utilisateurs qui stockent leurs fichiers de sauvegarde dans Google Cloud Storage. "[Découvrez comment restaurer vos volumes et fichiers à l'aide de Search Restore](#)".

## **Configurez une règle de sauvegarde à appliquer automatiquement aux volumes nouvellement créés dans les clusters Kubernetes**

Si vous avez ajouté de nouveaux volumes persistants à vos clusters Kubernetes après l'activation de Cloud Backup, il fallait auparavant vous rappeler de configurer les sauvegardes de ces volumes. Vous pouvez maintenant sélectionner une règle qui sera appliquée automatiquement aux nouveaux volumes créés. Cette option est disponible dans l'assistant d'installation lors de l'activation de Cloud Backup pour un nouveau cluster Kubernetes.

## **Cloud Backup requiert désormais une licence avant d'être activée dans un environnement de travail**

La mise en œuvre des licences avec Cloud Backup modifie quelques-unes des modifications :

- Vous devez vous inscrire à un abonnement PAYGO Marketplace auprès de votre fournisseur de cloud ou acheter une licence BYOL auprès de NetApp avant d'activer Cloud Backup.
- La version d'évaluation gratuite de 30 jours est disponible uniquement si vous utilisez un abonnement PAYGO auprès de votre fournisseur de services cloud. Elle n'est pas disponible si vous utilisez la licence BYOL.
- L'essai gratuit commence le jour où l'abonnement Marketplace commence. Par exemple, si vous activez la version d'évaluation gratuite après avoir utilisé un abonnement Marketplace pendant 30 jours pour un système Cloud Volumes ONTAP, la version d'évaluation Cloud Backup ne sera pas disponible.

["En savoir plus sur les modèles de licence disponibles"](#).

## 4 avril 2022

### **Cloud Backup pour les applications 1.1.0 (optimisée par SnapCenter) est désormais GA**

La nouvelle fonctionnalité de sauvegarde dans le cloud pour les applications vous permet de télécharger des snapshots cohérents avec les applications (sauvegardes) pour Oracle et Microsoft SQL du stockage primaire sur site vers le stockage objet dans le cloud dans Amazon S3 ou Azure Blob.

Lorsque cela est nécessaire, les données peuvent être restaurées depuis le cloud vers une infrastructure sur site.

["En savoir plus sur la protection des données des applications sur site vers le cloud"](#).

### **Nouvelle fonction de recherche et de restauration permettant de rechercher des volumes ou des fichiers sur tous les fichiers de sauvegarde ONTAP**

Vous pouvez maintenant rechercher un volume ou un fichier sur **tous les fichiers de sauvegarde ONTAP** par nom de volume partiel ou complet, nom de fichier partiel ou complet, plage de tailles et filtres de recherche supplémentaires. C'est une excellente nouvelle façon de trouver les données à restaurer si vous n'êtes pas sûr de savoir quel cluster ou volume était la source des données. ["Découvrez comment utiliser la fonction Rechercher et restaurer"](#).

## 3 mars 2022

### **Possibilité de sauvegarder des volumes persistants depuis vos clusters GKE Kubernetes vers le stockage Google Cloud**

Si votre cluster GKE est équipé de NetApp Astra Trident et qu'il utilise Cloud Volumes ONTAP pour GCP comme stockage interne du cluster, vous pouvez sauvegarder et restaurer vos volumes persistants vers et depuis le stockage Google Cloud. ["Cliquez ici pour plus d'informations"](#).

### **La fonctionnalité bêta permettant d'utiliser Cloud Data Sense pour analyser vos fichiers Cloud Backup a été abandonnée dans cette version**

## 14 février 2022

### **Vous pouvez désormais attribuer des stratégies de sauvegarde à des volumes individuels dans un seul cluster**

Auparavant, vous ne pouviez attribuer qu'une seule stratégie de sauvegarde à tous les volumes d'un cluster. Vous pouvez désormais créer plusieurs règles de sauvegarde pour un seul cluster et appliquer différentes règles à plusieurs volumes. ["Découvrez comment créer de nouvelles politiques de sauvegarde pour un cluster et les affecter à des volumes sélectionnés"](#).

### **Une nouvelle option vous permet d'appliquer automatiquement une stratégie de sauvegarde par défaut aux nouveaux volumes créés**

Auparavant, les nouveaux volumes créés dans un environnement de travail après l'activation de Cloud Backup nécessitaient une application manuelle d'une règle de sauvegarde. Désormais, que le volume ait été créé dans BlueXP, System Manager, la CLI ou encore via des API, Cloud Backup détecte le volume et applique la règle

de sauvegarde que vous avez choisie comme règle par défaut.

Cette option est disponible lors de l'activation de la sauvegarde dans un nouvel environnement de travail ou à partir de la page *Manage volumes* pour les environnements de travail existants.

## **Le nouveau moniteur de tâches permet de voir l'état en cours de traitement de toutes les tâches de sauvegarde et de restauration**

Le Job Monitor peut être très utile lorsque vous avez lancé une opération sur plusieurs volumes, comme la modification de la stratégie de sauvegarde ou la suppression de sauvegardes, de sorte que vous pouvez voir quand l'opération s'est terminée sur tous les volumes. "[Voir comment utiliser le moniteur de tâches](#)".

## **2 janvier 2022**

### **Sauvegarde des volumes persistants à partir de clusters AKS Kubernetes vers un stockage Azure Blob**

Si votre cluster AKS est équipé de NetApp Astra Trident et qu'il utilise Cloud Volumes ONTAP pour Azure comme stockage back-end pour le cluster, vous pouvez sauvegarder et restaurer des volumes vers et à partir d'Azure Blob Storage. "[Cliquez ici pour plus d'informations](#)".

### **Cette version a modifié les frais Cloud Backup Service afin de s'aligner plus étroitement sur les normes du secteur**

Au lieu de payer les capacités NetApp en fonction de la taille des fichiers de sauvegarde, vous payez uniquement pour les données que vous protégez, calculé par la capacité logique utilisée (avant l'efficacité ONTAP) des volumes ONTAP source qui sont sauvegardés. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

# Commencez

## Découvrir Cloud Backup

Cloud Backup est un service pour les environnements de travail BlueXP (anciennement Cloud Manager). Il offre des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé.

Si nécessaire, vous pouvez restaurer un *volume* entier à partir d'une sauvegarde vers le même environnement de travail ou vers un environnement de travail différent. Lorsque vous sauvegardez des données ONTAP, vous pouvez également choisir de restaurer un ou plusieurs *fichiers* d'une sauvegarde vers le même environnement de travail ou vers un environnement de travail différent.

["En savoir plus sur Cloud Backup"](#).

La fonction de sauvegarde et de restauration permet de :

- Sauvegarde et restauration de volumes ONTAP à partir de systèmes Cloud Volumes ONTAP et ONTAP sur site ["Voir les fonctionnalités détaillées ici"](#).
- Sauvegarde et restauration de volumes persistants Kubernetes. ["Voir les fonctionnalités détaillées ici"](#).
- Sauvegarde des copies Snapshot cohérentes au niveau des applications à partir d'un système ONTAP sur site vers le cloud à l'aide de Cloud Backup pour les applications ["Voir les fonctionnalités détaillées ici"](#).
- Sauvegardez des datastores dans le cloud et restaurez des machines virtuelles dans vCenter sur site à l'aide de Cloud Backup pour VMware. ["Voir les fonctionnalités détaillées ici"](#).

["Regarder une démonstration rapide"](#)



Lorsque BlueXP Connector est déployé dans une région gouvernementale dans le cloud ou dans un site sans accès à Internet (site sombre), Cloud Backup prend uniquement en charge les opérations de sauvegarde et de restauration à partir des systèmes ONTAP. Avec ces méthodes de déploiement alternatives, Cloud Backup ne prend pas en charge les opérations de sauvegarde et de restauration à partir de clusters Kubernetes, d'applications ou de machines virtuelles.

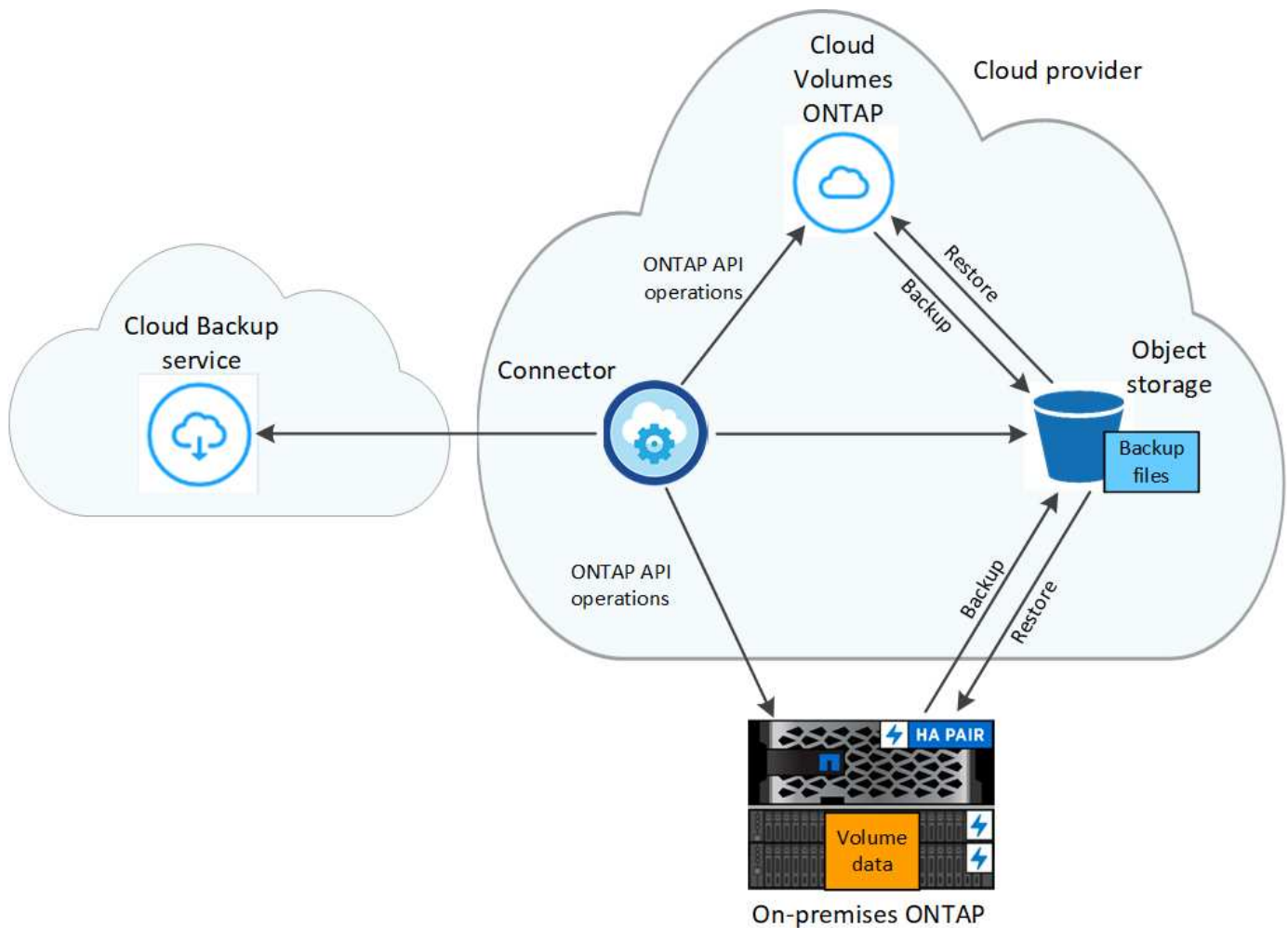
## Fonctionnement de Cloud Backup

Lorsque vous activez Cloud Backup sur un système ONTAP Cloud Volumes ONTAP ou sur site, le service effectue une sauvegarde complète de vos données. Les instantanés de volume ne sont pas inclus dans l'image de sauvegarde. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés. Le trafic réseau est ainsi réduit au minimum.

Dans la plupart des cas, vous utiliserez l'interface utilisateur BlueXP pour toutes les opérations de sauvegarde. Depuis ONTAP 9.9.1, vous pouvez toutefois lancer des opérations de sauvegarde volume de vos clusters ONTAP sur site à l'aide de ONTAP System Manager. ["Découvrez comment utiliser System Manager pour sauvegarder vos volumes dans le cloud à l'aide de Cloud Backup."](#)

L'image suivante montre la relation entre chaque composant :





## L'emplacement des sauvegardes

Les copies de sauvegarde sont stockées dans un magasin d'objets créé par BlueXP dans votre compte cloud. Il y a un magasin d'objets par cluster/environnement de travail, et BlueXP nomme le magasin d'objets comme suit : « netapp-backup-clusterUUID ». Veillez à ne pas supprimer ce magasin d'objets.

- Dans GCP, BlueXP utilise un projet nouveau ou existant avec un compte de stockage pour le compartiment Google Cloud Storage.
- Dans StorageGRID, BlueXP utilise un compte de stockage existant pour le compartiment de magasin d'objets.

## Les sauvegardes sont effectuées à minuit

- Les sauvegardes horaires commencent 5 minutes après l'heure, toutes les heures.
- Les sauvegardes quotidiennes commencent juste après minuit chaque jour.
- Les sauvegardes hebdomadaires commencent juste après minuit le dimanche matin.
- Les sauvegardes mensuelles commencent juste après minuit le premier jour de chaque mois.
- Les sauvegardes annuelles commencent juste après minuit le premier jour de l'année.

L'heure de début est basée sur le fuseau horaire défini sur chaque système ONTAP source. Vous ne pouvez pas planifier d'opérations de sauvegarde à une heure spécifiée par l'utilisateur à partir de l'interface utilisateur. Pour plus d'informations, contactez votre ingénieur système.



## Les copies de sauvegarde sont associées à votre compte NetApp

Les copies de sauvegarde sont associées à l' "[Compte NetApp](#)" Dans lequel réside le connecteur.

Si vous avez plusieurs connecteurs dans le même compte NetApp, chaque connecteur affiche la même liste de sauvegardes. Cela inclut les sauvegardes associées à Cloud Volumes ONTAP et aux instances ONTAP sur site à partir d'autres connecteurs.

## Configuration des licences pour Cloud Backup

Vous pouvez obtenir une licence Cloud Backup en achetant une formule de paiement basé sur l'utilisation (PAYGO) ou un abonnement annuel sur un marché depuis votre fournisseur cloud, ou en achetant une licence BYOL (Bring Your Own License) auprès de NetApp. Une licence valide est requise pour activer Cloud Backup dans un environnement de travail, créer des sauvegardes de vos données de production et restaurer les données de sauvegarde sur un système de production.

Quelques remarques avant de lire plus loin :

- Si vous vous êtes déjà abonné à l'abonnement PayGo-as-Go (PAYGO) dans le Marketplace de votre fournisseur de cloud pour un système Cloud Volumes ONTAP, vous êtes également automatiquement abonné à Cloud Backup. Vous n'aurez pas besoin de vous abonner à nouveau.
- Le modèle BYOL (Cloud Backup Bring Your Own License) est une licence flottante que vous pouvez utiliser sur tous les systèmes associés à votre compte BlueXP. Par conséquent, si vous disposez de suffisamment de capacité de sauvegarde sur une licence BYOL, vous n'avez pas besoin d'acheter une autre licence BYOL.
- Si vous utilisez une licence BYOL, il est également recommandé d' souscrire à un abonnement PAYGO. Si vous sauvegardez plus de données que ce que votre licence BYOL est autorisé, la sauvegarde se poursuit via votre abonnement au paiement à l'utilisation - aucune perturbation du service n'est possible.
- La sauvegarde de données ONTAP sur site vers StorageGRID nécessite une licence BYOL, mais les besoins en espace de stockage du fournisseur cloud sont réduits.

["En savoir plus sur les coûts d'utilisation de Cloud Backup."](#)

### essai gratuit de 30 jours

Un essai gratuit de 30 jours est disponible sur l'abonnement avec paiement à l'utilisation disponible sur le marché de votre fournisseur cloud. L'essai gratuit commence au moment où vous vous abonnez à la liste Marketplace. Notez que si vous payez pour l'abonnement Marketplace lors du déploiement d'un système Cloud Volumes ONTAP, puis lancez l'essai gratuit de Cloud Backup 10 jours plus tard, vous aurez 20 jours pour utiliser l'essai gratuit.

À la fin de l'essai gratuit, vous serez automatiquement transféré à l'abonnement PAYGO sans interruption. Si vous décidez de ne pas continuer à utiliser Cloud Backup, juste ["Annuler l'enregistrement de Cloud Backup dans l'environnement de travail"](#) avant la fin de l'essai, vous ne serez pas facturé.

### Utilisation d'un abonnement Cloud Backup PAYGO

Avec le paiement à l'utilisation, vous payez le coût du stockage objet pour votre fournisseur cloud et les coûts des licences de sauvegarde NetApp à l'heure sur un seul abonnement. Vous devez vous abonner même si vous disposez d'une période d'essai gratuite ou si vous apportez votre propre licence (BYOL) :

- L'abonnement garantit l'absence de perturbation du service après la fin de votre essai gratuit. À la fin de l'essai, vous serez facturé toutes les heures en fonction de la quantité de données que vous sauvegardez.
- Si vous sauvegardez plus de données que ce que votre licence BYOL, la sauvegarde des données se poursuit avec votre abonnement au paiement basé sur l'utilisation. Par exemple, si vous disposez d'une licence BYOL 10 Tio, toute la capacité au-delà de l'année 10 Tio est facturée via l'abonnement PAYGO.

Vous ne serez pas facturé à partir de votre abonnement au paiement à l'utilisation pendant votre essai gratuit ou si vous n'avez pas dépassé votre licence BYOL.

Voici quelques plans de facturation PAYGO pour la sauvegarde dans le cloud :

- Un pack « Cloud Backup » vous permet de sauvegarder les données Cloud Volumes ONTAP et ONTAP sur site.
- Bundle CVO pour créer des Cloud Volumes ONTAP et Cloud Backup Cela inclut un nombre illimité de sauvegardes pour le système Cloud Volumes ONTAP utilisant la licence (la capacité de sauvegarde n'est pas comptée par rapport à la capacité sous licence). Cette option ne permet pas de sauvegarder les données ONTAP sur site.

["En savoir plus sur ces packs de licence basés sur la capacité"](#).

Utilisez ces liens pour vous abonner à Cloud Backup sur le marché de votre fournisseur cloud :

- GCP : ["Consultez l'offre BlueXP Marketplace pour obtenir des informations sur les tarifs"](#).

## Utilisez un contrat annuel

Payez Cloud Backup chaque année par l'achat d'un contrat annuel.

Si vous utilisez GCP, contactez votre ingénieur commercial NetApp pour acheter un contrat annuel. Le contrat est disponible en tant qu'offre privée dans Google Cloud Marketplace. Une fois que NetApp vous a proposé de partager son offre privée, vous pouvez sélectionner le plan annuel lorsque vous vous inscrivez auprès de Google Cloud Marketplace au moment de l'activation de Cloud Backup.

## Utilisez une licence Cloud Backup BYOL

Modèle BYOL de 1, 2 ou 3 ans avec les licences Bring Your Own. Vous ne payez que les données que vous protégez, calculées par la capacité logique utilisée (*avant* toutes les efficacités) des volumes ONTAP source qui sont sauvegardés. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

La licence BYOL Cloud Backup est une licence flottante qui permet de partager la capacité totale sur tous les systèmes associés à votre compte BlueXP. Pour les systèmes ONTAP, vous pouvez obtenir une estimation approximative de la capacité dont vous avez besoin en exécutant la commande d'interface de ligne de commande `volume show -fields logical-used-by-afs` pour les volumes que vous prévoyez de sauvegarder.

Si vous ne disposez pas de licence Cloud Backup BYOL, cliquez sur l'icône de chat dans le coin inférieur droit de BlueXP pour en acheter un.

Si vous disposez d'une licence de nœud non attribuée pour Cloud Volumes ONTAP que vous n'utilisez pas, vous pouvez la convertir en licence Cloud Backup avec la même équivalence en dollars et la même date d'expiration. ["Cliquez ici pour plus d'informations"](#).

Utilisez la page porte-monnaie numérique de BlueXP pour gérer les licences BYOL. Vous pouvez ajouter de nouvelles licences, mettre à jour des licences existantes et afficher l'état de la licence à partir du porte-

monnaie numérique.

## Procurez-vous votre fichier de licence Cloud Backup

Après avoir acheté votre licence Cloud Backup, vous activez la licence dans BlueXP en saisissant le numéro de série et le compte NSS Cloud Backup ou en téléchargeant le fichier de licence NLF. Les étapes ci-dessous montrent comment obtenir le fichier de licence NLF si vous prévoyez d'utiliser cette méthode.

Si vous exécutez Cloud Backup sur un site sur site qui ne dispose pas d'un accès Internet, ce qui signifie que vous avez déployé le connecteur BlueXP sur un hôte sur le site hors ligne sur site, vous devrez obtenir le fichier de licence d'un système connecté à Internet. L'activation de la licence à l'aide du numéro de série et le compte NSS n'est pas disponible pour les installations hors ligne (site sombre).

### Étapes

1. Connectez-vous au "[Site de support NetApp](#)" Et cliquez sur **systèmes > licences logicielles**.
2. Entrez le numéro de série de votre licence Cloud Backup.

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		CLOUD_BKP_SERVICE	<a href="#">Get NetApp License File</a>		100	12/31/9998

3. Dans la colonne **License Key**, cliquez sur **Get NetApp License File**.
4. Saisissez votre identifiant de compte BlueXP (il s'agit d'un identifiant de locataire sur le site d'assistance) et cliquez sur **Submit** pour télécharger le fichier de licence.

**Get License**

SERIAL NUMBER: 4810

LICENSE: CLOUD\_BKP\_SERVICE

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

[Cancel](#) [Submit](#)

Vous pouvez trouver votre identifiant de compte BlueXP en sélectionnant le menu déroulant **compte** en haut de BlueXP, puis en cliquant sur **gérer compte** en regard de votre compte. Votre ID de compte se trouve dans l'onglet vue d'ensemble.

## Ajoutez des licences Cloud Backup BYOL à votre compte

Après avoir acheté une licence Cloud Backup pour votre compte NetApp, vous devez ajouter la licence à BlueXP.

### Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > porte-monnaie numérique**, puis sélectionnez l'onglet **licences de services de données**.
2. Cliquez sur **Ajouter une licence**.
3. Dans la boîte de dialogue *Add License*, entrez les informations de licence et cliquez sur **Add License**:
  - Si vous disposez du numéro de série de la licence de sauvegarde et connaissez votre compte NSS, sélectionnez l'option **entrer le numéro de série** et saisissez ces informations.

Si votre compte sur le site de support NetApp n'est pas disponible dans la liste déroulante, "[Ajoutez le compte NSS à BlueXP](#)".

- Si vous disposez du fichier de licence de sauvegarde (requis lorsqu'il est installé sur un site sombre), sélectionnez l'option **Télécharger le fichier de licence** et suivez les invites pour joindre le fichier.

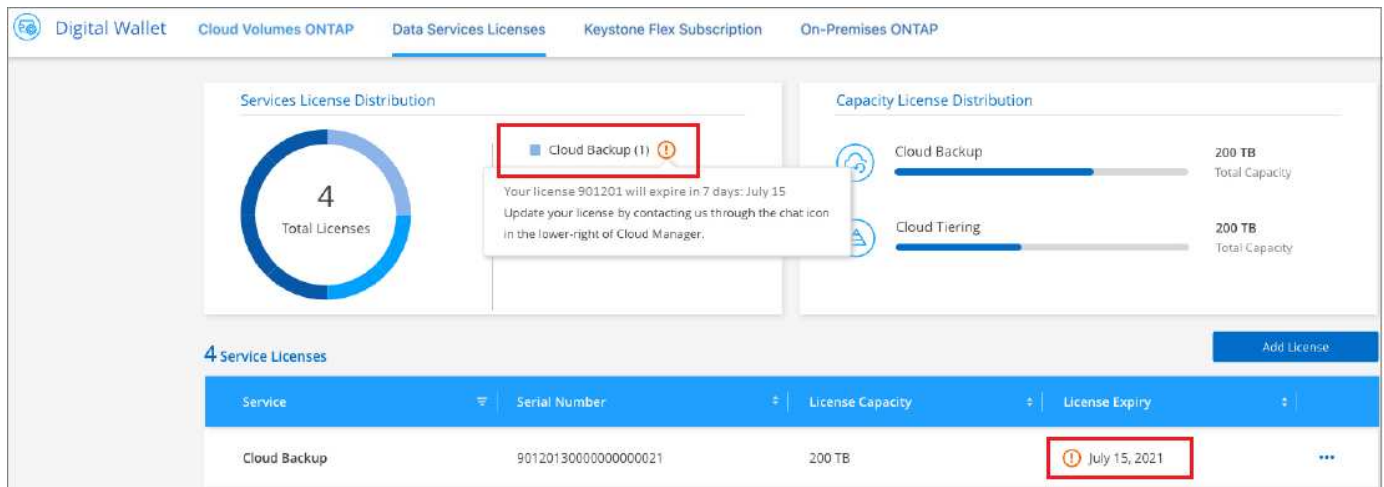
The image displays two versions of the 'Add Cloud Backup License' dialog box. The left version has the 'Enter Serial Number' radio button selected, showing input fields for the serial number and the NetApp support site account. The right version has the 'Upload License File' radio button selected, showing a list of instructions for obtaining the license file and an 'Upload' button to select the file.

### Résultat

BlueXP ajoute la licence pour que Cloud Backup soit actif.

## Mettez à jour une licence Cloud Backup BYOL

Si la durée de votre licence approche de la date d'expiration ou si votre capacité sous licence atteint la limite, vous serez informé dans l'interface utilisateur de la sauvegarde. Cet état apparaît également dans la page Portefeuille numérique et dans "[Notifications](#)".



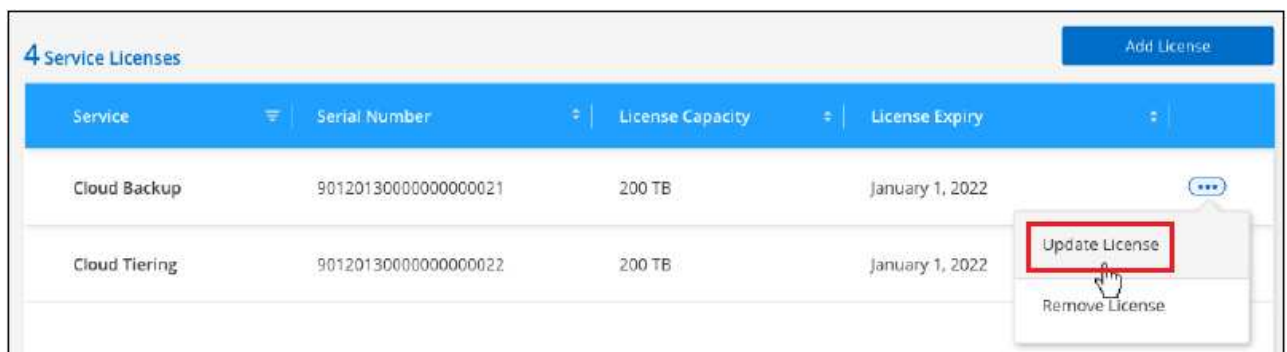
Vous pouvez mettre à jour votre licence Cloud Backup avant son expiration pour qu'il n'y ait aucune interruption dans votre possibilité de sauvegarder et de restaurer vos données.

## Étapes

1. Cliquez sur l'icône de chat dans le coin inférieur droit de BlueXP, ou contactez le service d'assistance pour demander une extension à votre terme ou une capacité supplémentaire à votre licence Cloud Backup pour le numéro de série spécifique.

Une fois que vous avez payé la licence et qu'elle est enregistrée sur le site de support NetApp, BlueXP met automatiquement à jour la licence dans Digital Wallet et la page des licences des services de données reflétera la modification dans 5 à 10 minutes.

2. Si BlueXP ne peut pas mettre à jour automatiquement la licence (par exemple, lorsqu'elle est installée sur un site sombre), vous devrez charger manuellement le fichier de licence.
  - a. C'est possible [Procurez-vous le fichier de licence sur le site de support NetApp](#).
  - b. Sur la page Portefeuille numérique *licences de services de données*, cliquez sur **...** Pour le numéro de série de service que vous mettez à jour, cliquez sur **mettre à jour la licence**.



- c. Dans la page *Update License*, téléchargez le fichier de licence et cliquez sur **Update License**.

## Résultat

BlueXP met à jour la licence pour que Cloud Backup reste actif.

## Considérations relatives aux licences BYOL

Lorsque vous utilisez une licence Cloud Backup BYOL, BlueXP affiche un avertissement dans l'interface utilisateur lorsque la taille de toutes les données sauvegardées approche de la limite de capacité ou approche

de la date d'expiration de la licence. Vous recevrez ces avertissements :

- Lorsque les sauvegardes atteignent 80 % de la capacité sous licence, et lorsque vous en avez atteint la limite
- 30 jours avant l'expiration d'une licence, et encore une fois à l'expiration de celle-ci

Utilisez l'icône de chat en bas à droite de l'interface BlueXP pour renouveler votre licence lorsque vous voyez ces avertissements.

Deux éléments peuvent se produire lorsque la licence BYOL expire :

- Si le compte que vous utilisez possède un compte Marketplace, le service de sauvegarde continue de s'exécuter, mais vous êtes basculé vers un modèle de licence PAYGO. Vous utilisez la capacité de vos sauvegardes.
- Si le compte que vous utilisez ne dispose pas d'un compte Marketplace, le service de sauvegarde continue à fonctionner, mais vous continuerez à voir les avertissements.

Une fois votre abonnement BYOL renouvelé, BlueXP met automatiquement à jour la licence. Si BlueXP ne parvient pas à accéder au fichier de licence via la connexion Internet sécurisée (par exemple, lorsqu'il est installé sur un site sombre), vous pouvez obtenir le fichier vous-même et le télécharger manuellement vers BlueXP. Pour obtenir des instructions, reportez-vous à la section "[Comment mettre à jour une licence Cloud Backup](#)".

Les systèmes qui ont basculé vers une licence PAYGO sont automatiquement renvoyés vers la licence BYOL. De plus, les systèmes fonctionnant sans licence ne voient plus les avertissements.

## Surveillance de l'état des tâches de sauvegarde et de restauration

Vous pouvez surveiller l'état des tâches de sauvegarde et de restauration que vous avez lancées 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 également configurer les notifications à envoyer par e-mail pour vous informer de l'activité système importante, même lorsque vous n'êtes pas connecté au système.

### Utilisez le moniteur des tâches pour afficher l'état des tâches de sauvegarde et de restauration

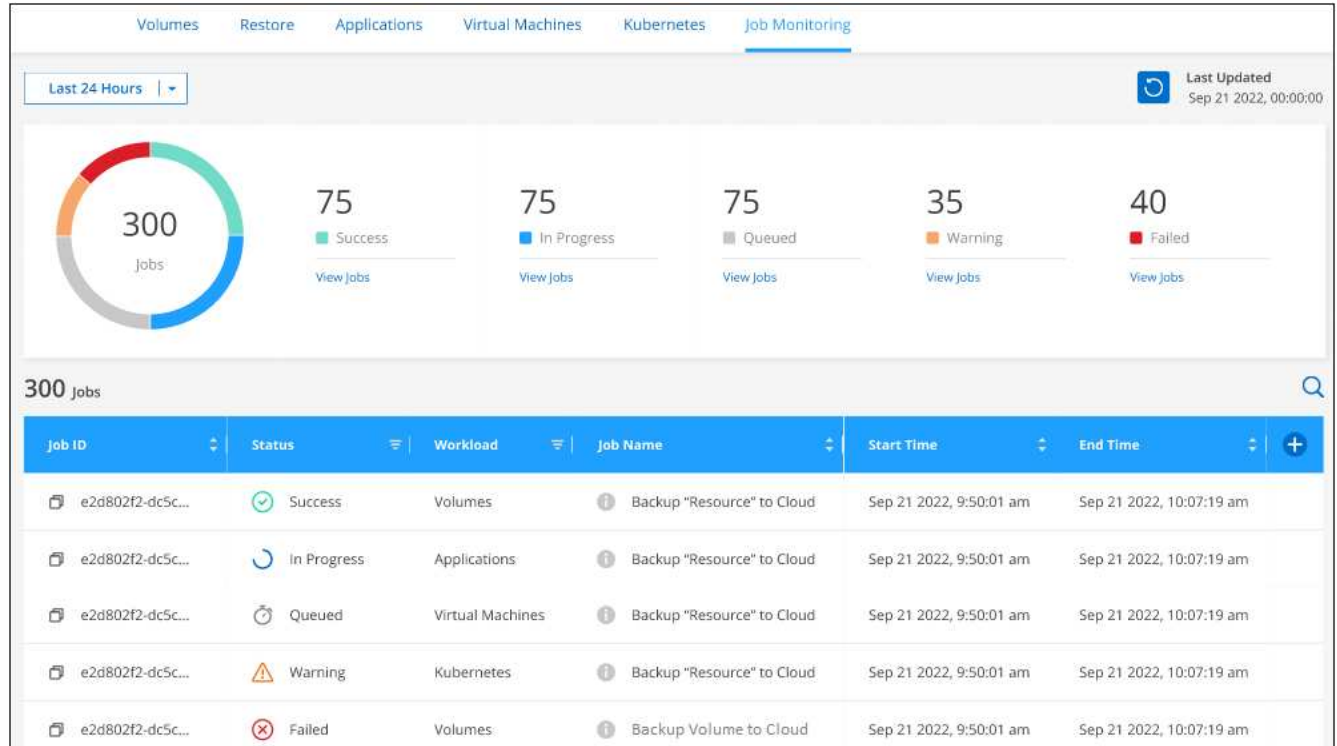
Vous pouvez afficher la liste de toutes les opérations de sauvegarde et de restauration ainsi que leur état actuel dans l'onglet **surveillance des travaux**. Il s'agit notamment des opérations de vos systèmes Cloud Volumes ONTAP, ONTAP sur site, applications, machines virtuelles et Kubernetes. Chaque opération, ou tâche, a un ID et un état uniques. Le statut peut être :

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

Notez que les tâches lancées par le système, telles que les opérations de sauvegarde en cours, ne sont pas reflétées dans l'onglet **surveillance des tâches** — seules les tâches exécutées par l'utilisateur sont affichées.

## Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **surveillance des travaux**.



Cette capture d'écran affiche les en-têtes de colonne/champ par défaut. Vous pouvez cliquer sur **+** Pour afficher et masquer les en-têtes de colonne, ou pour ajouter 2 en-têtes supplémentaires pour « Nom d'utilisateur » et « Type ».

Si vous recherchez des emplois spécifiques, vous pouvez :

- utilisez le sélecteur de temps en haut à gauche de la page pour afficher les travaux pendant un certain temps
- Entrez une partie du nom du travail dans le champ Rechercher
- Cliquez sur **Afficher les travaux** pour un certain état, par exemple sous "échec" pour afficher uniquement les travaux ayant échoué
- pour trier les résultats, utilisez le filtre de chaque en-tête de colonne. Par exemple, le filtre de la colonne « charges de travail » vous permet d'afficher les tâches des catégories suivantes :
  - Volumes (volumes Cloud Volumes ONTAP et ONTAP sur site)
  - En termes de latence
  - Ordinateurs virtuels
  - Kubernetes

Notez que cette page est automatiquement actualisée toutes les 15 minutes afin que vous puissiez toujours voir les résultats d'état des travaux les plus récents. Vous pouvez cliquer sur le bouton **Actualiser** pour mettre



la page à jour immédiatement.

Pour afficher les détails correspondant à un travail spécifique, cliquez sur le nom du travail. Vous verrez tous les sous-travaux en cours d'exécution pour terminer le travail principal dans la page Détails du travail.

Job Details					
Job ID: 2f1f7c7e-a592-45dc-ba5d-d391f20c7eb8					
7 Sub - Jobs <span>Expand All</span>					
Job Name	Job ID	Start Time	End Time	Duration	
Backup Volume to Cloud	e2d802f2-dc5c...	Sep 21 2022, 9:50:01 am	Sep 21 2022, 10:07:19 am	30 Minutes	
Sub Job 7	e2d802f2-dc5c...	Sep 21 2022, 9:50:01 am	Sep 21 2022, 10:07:19 am	5 Minutes	
Sub Job 6	e2d802f2-dc5c...	Sep 21 2022, 9:50:01 am	Sep 21 2022, 10:07:19 am	5 Minutes	
Unable to back up volume reason					
Sub Job 5	e2d802f2-dc5c...	Sep 21 2022, 9:50:01 am	Sep 21 2022, 10:07:19 am	5 Minutes	

## Utilisez le Centre de notification pour consulter les alertes de sauvegarde et de restauration

Le Centre de notification suit la progression des travaux de sauvegarde et de restauration que vous avez lancés afin de vérifier si l'opération a réussi ou non. Vous pouvez afficher les notifications en cliquant sur le bouton Dans la barre de menus BlueXP. Vous pouvez également configurer BlueXP pour qu'il envoie des notifications par e-mail en tant qu'alertes de sorte que vous puissiez être informé de l'activité système importante, même lorsque vous n'êtes pas connecté au système.

À ce stade, quatre événements déclenchent des alertes par e-mail :

- L'activation de Cloud Backup a échoué sur l'environnement de travail
- Échec de l'opération de restauration de Cloud Backup
- Échec de la sauvegarde du volume ad hoc (à la demande)
- Attaques par ransomware potentielles détectées sur votre système

Par défaut, les administrateurs de compte BlueXP recevront des e-mails pour toutes les alertes « critiques » et « recommandations ». Par défaut, tous les autres utilisateurs et destinataires sont configurés pour ne pas recevoir d'e-mails de notification. Il est possible d'envoyer des e-mails aux utilisateurs BlueXP qui font partie de votre compte Cloud NetApp, ou à tous les destinataires qui doivent avoir connaissance des activités de sauvegarde et de restauration.

Vous devez sélectionner les types de notification « critique » et « erreur » pour recevoir les alertes e-mail relatives à Cloud Backup.

["En savoir plus sur le Centre de notification et sur la manière d'envoyer des e-mails d'alerte pour les tâches de sauvegarde et de restauration".](#)



# Sauvegarde et restauration des données ONTAP

## Protection des données du cluster ONTAP à l'aide de Cloud Backup

Cloud Backup inclut des fonctionnalités de sauvegarde et de restauration pour une protection et un archivage à long terme des données de votre cluster ONTAP. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé, indépendamment des copies Snapshot de volume utilisées pour la restauration ou le clonage à court terme.

Si nécessaire, vous pouvez restaurer tout un *volume*, un *dossier*, ou un ou plusieurs *fichiers*, d'une sauvegarde vers le même environnement de travail ou vers un environnement de travail différent.

### Caractéristiques

Fonctionnalités de sauvegarde :

- Sauvegardez des copies indépendantes de vos volumes de données dans un stockage objet à faible coût.
- Appliquer une seule stratégie de sauvegarde à tous les volumes d'un cluster, ou attribuer différentes règles de sauvegarde aux volumes ayant des objectifs de point de restauration uniques.
- Créer une policy de sauvegarde à appliquer à tous les futurs volumes créés dans le cluster.
- Créez des fichiers de sauvegarde immuables afin qu'ils soient verrouillés pour la période de conservation.
- Analysez les fichiers de sauvegarde afin d'obtenir un risque d'attaque par ransomware. Enfin, supprimez/remplacez automatiquement les sauvegardes infectées.
- Transférez les anciens fichiers de sauvegarde vers le stockage d'archivage pour réduire les coûts.
- Supprimez la relation de sauvegarde afin d'archiver les volumes source inutiles tout en conservant les sauvegardes de volume.
- Sauvegarder des données dans le cloud et depuis des systèmes sur site vers un cloud public ou privé.
- Pour les systèmes Cloud Volumes ONTAP, vos sauvegardes peuvent résider sur un abonnement/compte différent ou sur une autre région.
- Les données de sauvegarde sont sécurisées par chiffrement AES 256 bits au repos et TLS 1.2 HTTPS en transit.
- Utilisez vos propres clés gérées par le client pour le chiffrement des données au lieu d'utiliser les clés de chiffrement par défaut fournies par votre fournisseur cloud.
- Prise en charge de 4,000 sauvegardes maximum d'un seul volume.

Fonctions de restauration :

- Restauration des données à partir d'un point dans le temps spécifique
- Restaurez un volume, un dossier ou des fichiers individuels vers le système source ou vers un autre système.
- Restaurez les données dans un environnement de travail à l'aide d'un autre abonnement/compte ou dans une autre région.
- Restaurez les données au niveau bloc en les plaçant directement à l'emplacement que vous indiquez, tout

en conservant les ACL d'origine.

- Catalogues de fichiers consultables pour la sélection de dossiers et de fichiers individuels pour la restauration de fichiers uniques.

## Environnements de travail ONTAP pris en charge et fournisseurs de stockage objet

Cloud Backup vous permet de sauvegarder des volumes ONTAP à partir de ces environnements de travail vers un stockage objet dans plusieurs fournisseurs de cloud public et privé :

Environnement de travail source	Destination du fichier de sauvegarde <code>ifdef::aws[]</code>
Cloud Volumes ONTAP dans AWS	Amazon S3 <code>endif::aws[]</code> <code>ifdef::Azure[]</code>
Cloud Volumes ONTAP dans Azure	Azure Blob <code>endif::Azure[]</code> <code>ifdef::gcp[]</code>
Cloud Volumes ONTAP dans Google	Google Cloud Storage <code>endif::gcp[]</code>
Système ONTAP sur site	<code>ifdef::aws[]</code> Amazon S3 <code>endif::aws[]</code> <code>ifdef::Azure[]</code> Azure Blob <code>endif::Azure[]</code> <code>ifdef::gcp[]</code> Google Cloud Storage <code>endif::gcp[]</code> NetApp StorageGRID

Vous pouvez restaurer un volume, un dossier ou des fichiers individuels depuis un fichier de sauvegarde ONTAP vers les environnements de travail suivants :

Emplacement du fichier de sauvegarde	Destination Environnement de travail <code>ifdef::aws[]</code>
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS <code>endif::aws[]</code> <code>ifdef::Azure[]</code>
Blob d'Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure <code>endif::Azure[]</code> <code>ifdef::gcp[]</code>
Google Cloud Storage	Cloud Volumes ONTAP dans le système ONTAP sur site Google <code>endif::gcp[]</code>
NetApp StorageGRID	Système ONTAP sur site

Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select.

### Assistance pour les sites sans connexion Internet

Cloud Backup peut être utilisé sur un site sans connectivité Internet (également appelée site « hors ligne » ou « sombre ») pour sauvegarder les données en volume des systèmes ONTAP locaux sur site vers des systèmes StorageGRID NetApp locaux. La restauration de volumes et de fichiers est également prise en charge dans cette configuration. Dans ce cas, vous devrez déployer le connecteur BlueXP (version minimale 3.9.20) sur le site sombre. Voir "[La sauvegarde des données ONTAP sur site dans StorageGRID](#)" pour plus d'informations.

## Volumes pris en charge

Cloud Backup prend en charge plusieurs types de volumes :

- Volumes FlexVol de lecture/écriture
- Volumes de destination SnapMirror avec protection des données (DP)
- Volumes SnapLock Enterprise (requiert ONTAP 9.11.1 ou version ultérieure)

- Les volumes de conformité SnapLock ne sont actuellement pas pris en charge.
- Volumes FlexGroup (requiert ONTAP 9.12.1 ou version ultérieure)

#### Limitations de restauration de volume FlexGroup :



- La restauration de volume complet est prise en charge uniquement sur les systèmes ONTAP sur site (les systèmes Cloud Volumes ONTAP ne sont pas pris en charge actuellement).
- La restauration au niveau fichier est prise en charge à la fois pour les systèmes ONTAP et Cloud Volumes ONTAP sur site.
- La restauration des répertoires/dossiers n'est pas prise en charge actuellement.
- Actuellement, les volumes peuvent être restaurés sur un seul agrégat.

## Le coût

Deux types de coûts sont associés à l'utilisation de Cloud Backup avec les systèmes ONTAP : les frais en ressources et les frais de service.

### Frais de ressources

Les frais en ressources sont facturés au fournisseur cloud pour la capacité de stockage objet et pour l'écriture et la lecture des fichiers de sauvegarde dans le cloud.

- En matière de sauvegarde, vous payez votre fournisseur cloud pour les coûts de stockage objet.

Étant donné que Cloud Backup préserve l'efficacité du stockage du volume source, vous payez les coûts de stockage objet du fournisseur cloud pour les données *après* efficacité ONTAP (pour la quantité de données plus faible après l'application de la déduplication et de la compression).

- Pour la restauration des données à l'aide de Search & Restore, certaines ressources sont provisionnées par votre fournisseur de cloud. Le coût par Tio est associé à la quantité de données analysées par vos requêtes de recherche. (Ces ressources ne sont pas nécessaires pour la fonction Parcourir et restaurer.)
- Dans Google, un nouveau compartiment est déployé, et le "[Services Google Cloud BigQuery](#)" sont provisionnées au niveau compte/projet.
- Si vous avez besoin de restaurer des données de volume à partir d'un fichier de sauvegarde déplacé vers un stockage d'archivage, un coût de récupération supplémentaire par Gio et des frais par demande sont facturés par le fournisseur cloud.

### Frais de service

Les frais de service sont payés à NetApp et couvrent le coût de *créer* sauvegardes et de *restaurer* volumes ou fichiers à partir de ces sauvegardes. Vous ne payez que les données que vous protégez, calculées par la capacité logique utilisée source (*before* ONTAP *before\_* ONTAP) des volumes qui sont sauvegardés sur le stockage objet. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

Vous pouvez payer le service de sauvegarde de trois façons. La première option consiste à vous abonner à votre fournisseur cloud pour un paiement mensuel. La deuxième option consiste à obtenir un contrat annuel. La troisième option consiste à acheter des licences directement auprès de NetApp. Lire le [Licences](#) pour plus de détails.

## Licences

Cloud Backup est disponible avec les modèles de consommation suivants :

- **BYOL** : licence achetée auprès de NetApp et utilisable avec n'importe quel fournisseur cloud.
- **PAYGO** : un abonnement à l'heure sur le marché de votre fournisseur de services cloud.
- **Annuel** : contrat annuel sur le marché de votre fournisseur cloud.

Si vous achetez une licence BYOL auprès de NetApp, vous devez également vous abonner à l'offre PAYGO depuis le marché de votre fournisseur cloud. Votre licence est toujours facturée en premier, mais vous devrez payer à l'heure sur le marché dans les cas suivants :



- Si vous dépassez votre capacité autorisée
- Si la durée de votre licence expire

Si vous disposez d'un contrat annuel sur un marché, l'ensemble de la consommation de Cloud Backup est facturée sur votre contrat. Vous ne pouvez pas combiner un contrat annuel de vente avec un contrat BYOL.

### Bring your own license (BYOL)

BYOL est basé sur la durée (12, 24 ou 36 mois) et sur la capacité par incréments de 1 Tio. Vous payez NetApp pour utiliser le service pendant une période, disons 1 an, et pour une capacité maximale, dites 10 Tio.

Vous recevrez un numéro de série que vous entrez dans la page BlueXP Digital Wallet pour activer le service. Lorsque l'une ou l'autre limite est atteinte, vous devez renouveler la licence. La licence de sauvegarde BYOL s'applique à tous les systèmes source associés à votre ["Compte BlueXP"](#).

["Découvrez comment gérer vos licences BYOL"](#).

### Abonnement avec paiement à l'utilisation

Cloud Backup propose un modèle de paiement à l'utilisation avec des licences basées sur la consommation. Après votre abonnement sur le marché de votre fournisseur cloud, vous payez par Gio pour les données sauvegardées, sans paiement initial. Votre fournisseur cloud vous facture mensuellement.

["Découvrez comment configurer un abonnement avec paiement à l'utilisation"](#).

Notez qu'une version d'essai gratuite de 30 jours est disponible lorsque vous vous abonnez initialement à un abonnement PAYGO.

### Contrat annuel

- Lorsque vous utilisez GCP, vous pouvez demander une offre privée auprès de NetApp, puis sélectionner le plan lorsque vous vous abonnez à Google Cloud Marketplace au moment de l'activation de Cloud Backup.

["Découvrez comment configurer des contrats annuels"](#).

## Fonctionnement de Cloud Backup

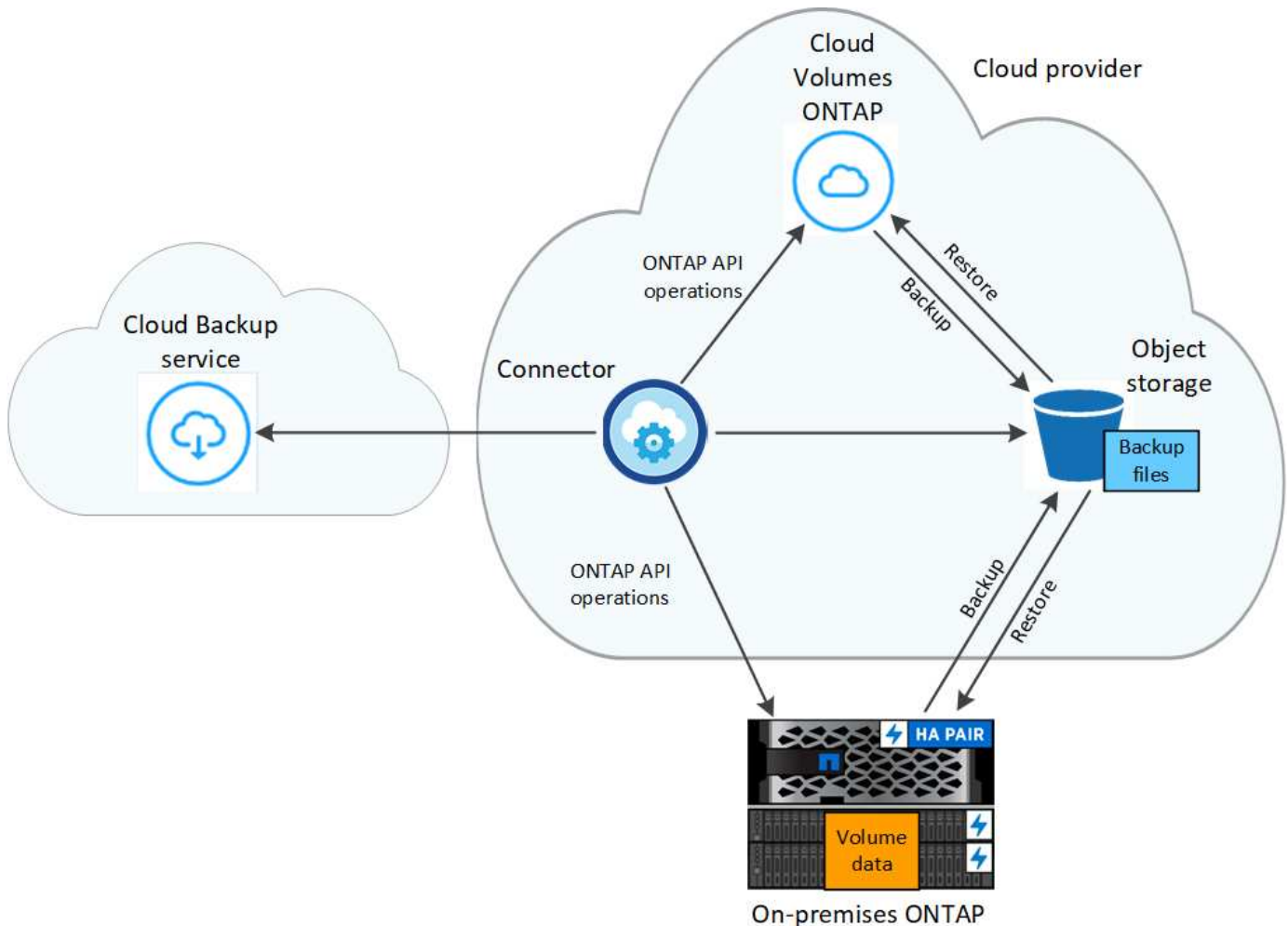
Lorsque vous activez Cloud Backup sur un système ONTAP Cloud Volumes ONTAP ou sur site, le service effectue une sauvegarde complète de vos données. Les instantanés de volume ne sont pas inclus dans l'image de sauvegarde. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont

incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés. Le trafic réseau est ainsi réduit au minimum. Cloud Backup repose sur le ["Technologie NetApp SnapMirror Cloud"](#).



Toute action effectuée directement depuis votre environnement de fournisseur cloud pour gérer ou modifier des fichiers de sauvegarde peut corrompre les fichiers et entraîner une configuration non prise en charge.

L'image suivante montre la relation entre chaque composant :



## L'emplacement des sauvegardes

Les copies de sauvegarde sont stockées dans un magasin d'objets créé par BlueXP dans votre compte cloud. Chaque cluster/environnement de travail est équipé d'un magasin d'objets, et BlueXP a indiqué le magasin d'objets comme suit : « netapp-backup-clusterUUID ». Veillez à ne pas supprimer ce magasin d'objets.

- Dans GCP, BlueXP utilise un projet nouveau ou existant avec un compte de stockage pour le compartiment Google Cloud Storage.
- Dans StorageGRID, BlueXP utilise un compte de stockage existant pour le compartiment de magasin d'objets.

Pour modifier ultérieurement le magasin d'objets de destination d'un cluster, vous devez ["Annuler l'inscription de Cloud Backup pour l'environnement de travail"](#), Puis activez Cloud Backup à l'aide des informations du nouveau fournisseur cloud.

## Programme de sauvegarde et paramètres de conservation personnalisables

Lorsque vous activez Cloud Backup pour un environnement de travail, tous les volumes que vous sélectionnez initialement sont sauvegardés à l'aide de la stratégie de sauvegarde par défaut que vous définissez. Si vous souhaitez attribuer différentes règles de sauvegarde à certains volumes ayant des objectifs de point de récupération différents, vous pouvez créer des règles supplémentaires pour ce cluster et les attribuer aux autres volumes une fois que Cloud Backup est activé.

Vous pouvez choisir une combinaison de sauvegardes toutes les heures, tous les jours, toutes les semaines, tous les mois et tous les ans pour tous les volumes. Vous pouvez également sélectionner l'une des stratégies définies par le système qui assure les sauvegardes et la conservation pendant 3 mois, 1 an et 7 ans. Ces règles sont les suivantes :

Nom de la stratégie de sauvegarde	Sauvegardes par intervalle...			Capacité Sauvegardes
	Tous les jours	Hebdomadaire	Mensuel	
Netap3MonthsRetention	30	13	3	46
Fidélisation Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Les règles de protection des sauvegardes que vous avez créées sur le cluster à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP s'affichent également comme sélections. Cela inclut les règles créées à l'aide d'étiquettes SnapMirror personnalisées.

Lorsque vous avez atteint le nombre maximal de sauvegardes pour une catégorie ou un intervalle, les anciennes sauvegardes sont supprimées ainsi toujours les sauvegardes les plus récentes (et les sauvegardes obsolètes ne continuent pas à prendre de l'espace dans le cloud).

Voir "[Planifications de sauvegarde](#)" pour plus de détails sur la façon dont les options de planification disponibles.

Notez que vous pouvez "[création d'une sauvegarde à la demande d'un volume](#)" À tout moment à partir du tableau de bord de sauvegarde, en plus des fichiers de sauvegarde créés à partir des sauvegardes planifiées.



La période de conservation pour les sauvegardes de volumes de protection de données est identique à la période définie dans la relation SnapMirror source. Vous pouvez le modifier si vous le souhaitez à l'aide de l'API.

## Sauvegarder les paramètres de protection des fichiers

Si votre cluster utilise ONTAP 9.11.1 ou supérieur, vous pouvez protéger vos sauvegardes contre la suppression et les attaques par ransomware. Chaque stratégie de sauvegarde fournit une section pour *DataLock et protection contre les attaques par ransomware* qui peut être appliquée à vos fichiers de sauvegarde pendant une période spécifique - la *période de rétention*. *DataLock* protège vos fichiers de sauvegarde contre leur modification ou leur suppression. *Protection par ransomware* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware lors de la création d'un fichier de sauvegarde, et lorsque les données d'un fichier de sauvegarde sont en cours de restauration.

La période de conservation des sauvegardes est identique à la période de conservation du programme de sauvegarde, plus 14 jours. Par exemple, les *sauvegardes hebdomadaires* avec 5 copies conservées

verrouillent chaque fichier de sauvegarde pendant 5 semaines. *Monthly* backups avec 6 copies conservées verrouilleront chaque fichier de sauvegarde pendant 6 mois.

Le support est actuellement disponible lorsque votre destination de sauvegarde est Amazon S3 ou NetApp StorageGRID. D'autres destinations de fournisseurs de stockage seront ajoutées dans les prochaines versions.

Voir "[Protection des données par verrouillage et protection contre les ransomwares](#)" Pour plus d'informations sur le fonctionnement des fonctionnalités DataLock et de protection contre les attaques par ransomware.



DataLock ne peut pas être activé si vous effectuez le Tiering des sauvegardes sur le stockage d'archivage.

## Stockage d'archivage pour les fichiers de sauvegarde plus anciens

Si vous utilisez un certain stockage cloud, vous pouvez déplacer d'anciens fichiers de sauvegarde vers un Tier de stockage/accès moins onéreux après un certain nombre de jours. Notez que le stockage d'archives ne peut pas être utilisé si vous avez activé DataLock.

- Dans GCP, les sauvegardes sont associées à la classe de stockage *Standard*.

Si votre cluster sur site utilise ONTAP 9.12.1 ou version ultérieure, vous pouvez choisir de transférer d'anciennes sauvegardes vers le stockage *Archive* dans l'interface utilisateur de sauvegarde dans le cloud au bout d'un certain nombre de jours afin d'optimiser les coûts. (Cette fonctionnalité n'est pas disponible actuellement pour les systèmes Cloud Volumes ONTAP.) "[En savoir plus sur le stockage des archives Google](#)".

- Dans StorageGRID, les sauvegardes sont associées à la classe de stockage *Standard*.

Voir "[Paramètres de stockage d'archivage](#)" pour plus d'informations sur l'archivage d'anciens fichiers de sauvegarde.

## Considérations relatives à la hiérarchisation FabricPool

Certains éléments doivent être conscients de l'emplacement du volume de sauvegarde sur un agrégat FabricPool et d'une règle autre que `none`:

- La première sauvegarde d'un volume FabricPool exige la lecture de toutes les données locales et hiérarchisées (depuis le magasin d'objets). Une opération de sauvegarde ne « réchauffe pas les données inactives hiérarchisées dans le stockage objet.

La lecture des données de votre fournisseur de cloud peut s'accélérer et générer des coûts supplémentaires.

- Les sauvegardes suivantes sont incrémentielles et n'ont pas cet effet.
- Si la règle de hiérarchisation est attribuée au volume lors de sa création initiale, ce problème ne s'affiche pas.
- Tenez compte de l'impact des sauvegardes avant d'affecter le `all` tiering des règles sur les volumes. Les données étant hiérarchisées immédiatement, Cloud Backup les lit dans le Tier cloud plutôt que dans le Tier local. Étant donné que les opérations de sauvegarde simultanées partagent la liaison réseau avec le magasin d'objets cloud, les performances peuvent être affectées si les ressources réseau deviennent saturées. Dans ce cas, il peut être nécessaire de configurer de manière proactive plusieurs interfaces réseau (LIF) afin de réduire ce type de saturation réseau.

## Limites des sauvegardes

- Pour effectuer le Tiering des anciens fichiers de sauvegarde dans un stockage d'archivage, le cluster exécute ONTAP 9.10.1 ou une version ultérieure. La restauration de volumes à partir de fichiers de sauvegarde qui résident dans un stockage d'archivage nécessite également que le cluster de destination exécute ONTAP 9.10.1+.
- Lors de la création ou de la modification d'une stratégie de sauvegarde lorsqu'aucun volume n'est affecté à la stratégie, le nombre de sauvegardes conservées peut atteindre un maximum de 1018. Pour contourner ce problème, vous pouvez réduire le nombre de sauvegardes pour créer la stratégie. Vous pouvez ensuite modifier la stratégie pour créer jusqu'à 4000 sauvegardes après avoir affecté des volumes à la stratégie.
- Lors de la sauvegarde de volumes de protection des données (DP) :
  - Relations avec les libellés SnapMirror `app_consistent` et `all_source_snapshot` elles ne seront pas sauvegardées dans le cloud.
  - Si vous créez des copies Snapshot locales sur le volume de destination SnapMirror (indépendamment des étiquettes SnapMirror utilisées), ces snapshots ne seront pas déplacés vers le cloud en tant que sauvegardes. Pour le moment, vous devrez créer une règle Snapshot avec les étiquettes souhaitées pour le volume DP source afin que Cloud Backup puisse les sauvegarder.
- Les sauvegardes de volumes FlexGroup ne peuvent pas être déplacées vers le stockage d'archivage. Elles ne peuvent pas non plus utiliser le verrouillage des données et la protection par ransomware.
- La sauvegarde du volume SVM-DR est prise en charge avec les restrictions suivantes :
  - Seules les sauvegardes sont prises en charge à partir du système secondaire ONTAP.
  - La règle Snapshot appliquée au volume doit être l'une des règles reconnues par Cloud Backup, y compris les règles quotidiennes, hebdomadaires, mensuelles, etc. La stratégie par défaut « `sm_create` » (utilisée pour **Mirror All snapshots**) N'est pas reconnu et le volume DP n'apparaît pas dans la liste des volumes pouvant être sauvegardés.
- La sauvegarde MetroCluster (MCC) est prise en charge à partir d'un système secondaire ONTAP uniquement : MCC > SnapMirror > ONTAP > sauvegarde dans le cloud > stockage objet.
- La sauvegarde de volume ad-hoc à l'aide du bouton **Backup Now** n'est pas prise en charge sur les volumes de protection des données.
- Les configurations SM-BC ne sont pas prises en charge.
- ONTAP ne prend pas en charge la « fan-out » des relations SnapMirror depuis un volume unique vers plusieurs magasins d'objets. Par conséquent, cette configuration n'est pas prise en charge par Cloud Backup.
- Le mode WORM/Compliance d'un magasin d'objets est actuellement pris en charge uniquement sur Amazon S3 et StorageGRID. Il s'agit de la fonctionnalité DataLock, qui doit être gérée à l'aide des paramètres Cloud Backup.

## Limites de restauration des fichiers et des dossiers

Ces limitations s'appliquent à la fois aux méthodes de recherche et de restauration et de navigation pour restaurer des fichiers et des dossiers, sauf indication contraire.

- Parcourir et restaurer peut restaurer jusqu'à 100 fichiers individuels à la fois.
- La fonction de recherche et de restauration permet de restaurer 1 fichier à la fois.
- Parcourir et restaurer et Rechercher et restaurer peut restaurer 1 dossier à la fois.
- La restauration des volumes FlexGroup vers des volumes FlexVol, ou des volumes FlexVol vers des volumes FlexGroup n'est pas prise en charge.



- La restauration du niveau fichier à l'aide de la fonction Rechercher et restaurer n'est pas prise en charge lorsque le connecteur est installé sur un site sans accès à Internet (site sombre).
- Vous ne pouvez pas restaurer des dossiers individuels si le fichier de sauvegarde réside dans le stockage d'archivage.
- Le fichier en cours de restauration doit être dans la même langue que celle du volume de destination. Vous recevrez un message d'erreur si les langues ne sont pas les mêmes.

## Sauvegarde des données Cloud Volumes ONTAP dans Google Cloud Storage

Procédez comme suit pour commencer à sauvegarder des données d'Cloud Volumes ONTAP vers Google Cloud Storage.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

1

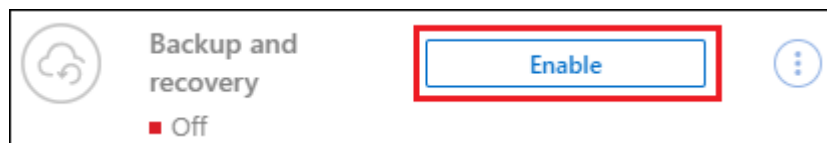
#### Vérifiez la prise en charge de votre configuration

- Vous exécutez Cloud Volumes ONTAP 9.7P5 ou une version ultérieure dans GCP.
- Vous disposez d'un abonnement GCP valide pour l'espace de stockage où se trouvent vos sauvegardes.
- Vous disposez d'un compte de service dans votre projet Google Cloud avec le rôle d'administrateur de stockage prédéfini.
- Vous avez souscrit au "[Offre de sauvegarde BlueXP Marketplace](#)", ou vous avez acheté "[et activé](#)" Licence Cloud Backup BYOL de NetApp.

2

#### Activation de Cloud Backup sur votre système nouveau ou existant

- Nouveaux systèmes : Cloud Backup peut être activé lorsque vous suivez l'assistant du nouvel environnement de travail.
- Systèmes existants : sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service de sauvegarde et de restauration dans le panneau de droite, puis suivez l'assistant d'installation.



3

#### Entrez les détails du fournisseur

Sélectionnez le compartiment Google Cloud Project où vous souhaitez créer le compartiment Google Cloud Storage pour les sauvegardes.

**Provider Settings**

Google Cloud Project  
Default Project

Region  
us-east-2

4

#### Définissez la stratégie de sauvegarde par défaut

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passage à des sauvegardes toutes les heures, tous les jours, toutes les semaines, tous les mois ou tous les ans vous pouvez également sélectionner l'une des règles définies par le système qui offrent plus d'options. Vous pouvez également modifier le nombre de copies de sauvegarde à conserver.

**Define Policy**

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

*i* Cloud Backup will create the Google Cloud Storage bucket after you complete the wizard

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
Archival Policy	Disabled	▼

5

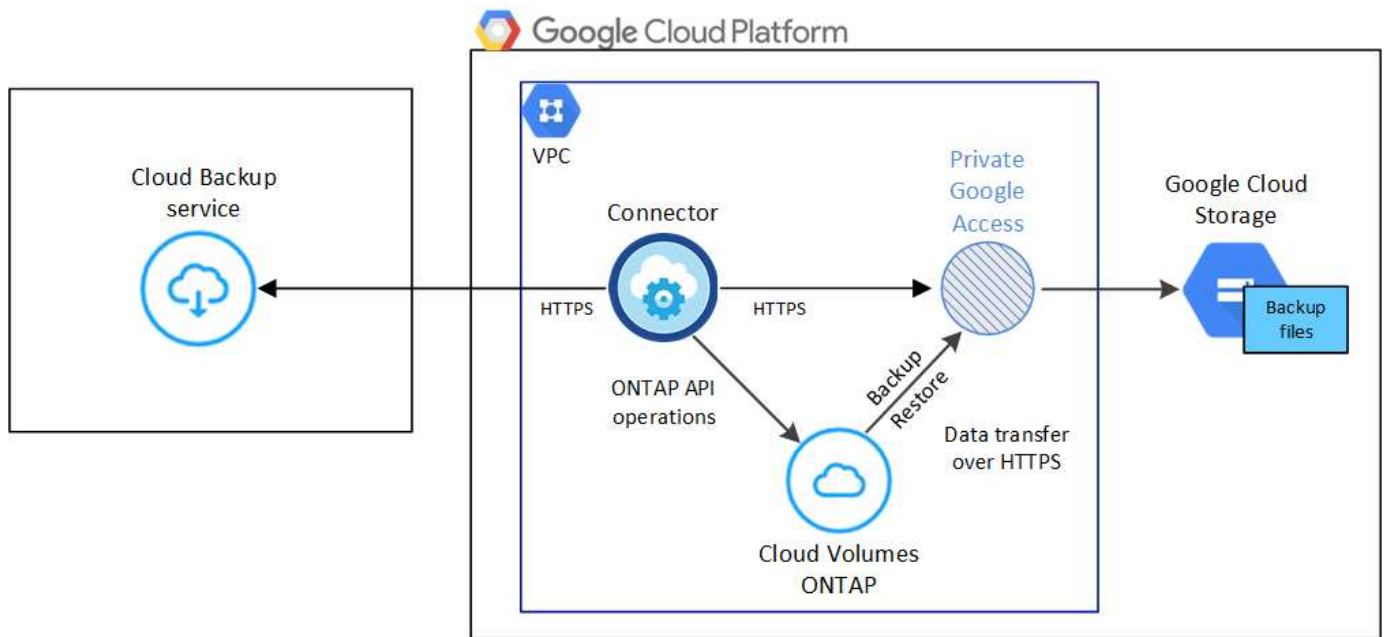
#### Sélectionnez les volumes à sauvegarder

Identifiez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde par défaut dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des règles supplémentaires et les appliquer ultérieurement aux volumes.

## De formation

Avant de commencer à sauvegarder des volumes sur Google Cloud, lisez les informations suivantes pour vous assurer que la configuration est prise en charge.

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



### Versions de ONTAP prises en charge

Minimum de ONTAP 9.7P5 ; ONTAP 9.8P13 et version ultérieure est recommandé.

### Conditions de licence

Pour le modèle de licence Cloud Backup PAYGO, un abonnement BlueXP via le ["Marketplace GCP"](#) Est requise avant d'activer Cloud Backup. La facturation pour Cloud Backup s'effectue via cet abonnement. ["Vous pouvez vous abonner à la page Détails et amp ; informations d'identification de l'assistant de l'environnement de travail"](#).

Pour les licences BYOL, vous avez besoin du numéro de série NetApp qui permet d'utiliser le service pendant la durée et la capacité du contrat. ["Découvrez comment gérer vos licences BYOL"](#).

Vous devez également disposer d'un abonnement Google pour l'espace de stockage où vos sauvegardes seront stockées.

### Régions GCP prises en charge

Cloud Backup est pris en charge dans toutes les régions GCP ["Dans ce cas, Cloud Volumes ONTAP est pris en charge"](#).

### Compte de services GCP

Vous devez disposer d'un compte de service dans votre projet Google Cloud avec le rôle d'administrateur de stockage prédéfini. ["Découvrez comment créer un compte de service"](#).

### Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité « recherche et restauration » de Cloud Backup, vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder au service Google Cloud BigQuery. Reportez-vous aux autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

1. Dans ["Console cloud"](#), Allez à la page **rôles**.
2. A l'aide de la liste déroulante située en haut de la page, sélectionnez le projet ou l'organisation qui contient le rôle que vous souhaitez modifier.
3. Cliquez sur un rôle personnalisé.

4. Cliquez sur **Modifier le rôle** pour mettre à jour les autorisations du rôle.
5. Cliquez sur **Ajouter des autorisations** pour ajouter les nouvelles autorisations suivantes au rôle.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Cliquez sur **Update** pour enregistrer le rôle modifié.

## Activation de Cloud Backup sur un nouveau système

Cloud Backup peut être activé lorsque vous suivez l'assistant de l'environnement de travail pour créer un nouveau système Cloud Volumes ONTAP.

Un compte de service doit déjà être configuré. Si vous ne sélectionnez pas de compte de service lors de la création du système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP depuis la console GCP.

Voir "[Lancement d'Cloud Volumes ONTAP dans GCP](#)" Pour connaître les conditions requises et les détails relatifs à la création du système Cloud Volumes ONTAP.

### Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Google Cloud Platform**.
3. **Choisissez le type** : sélectionnez **Cloud Volumes ONTAP** (à un seul nœud ou haute disponibilité).
4. **Détails et informations d'identification** : saisissez les informations suivantes :
  - a. Cliquez sur **Modifier le projet** et sélectionnez un nouveau projet si celui que vous souhaitez utiliser est différent du projet par défaut (où réside le connecteur).
  - b. Spécifier le nom du cluster
  - c. Activez le commutateur **compte de service** et sélectionnez le compte de service qui possède le rôle d'administrateur de stockage prédéfini. Cette opération est nécessaire pour activer les sauvegardes et le Tiering.
  - d. Spécifiez les informations d'identification.

Assurez-vous qu'un abonnement GCP Marketplace est en place.

Details & Credentials

Project1 Google Cloud Project	MPAWSSubscription1222 Marketplace Subscription	<a href="#">Edit Project</a>
----------------------------------	---	------------------------------

**Details**

Working Environment Name (Cluster Name)

Service Account ⓘ ☒

Service Account Name

[+ Add Labels](#)    Optional Field | Up to four labels

**Credentials**

User Name

Password

Confirm Password

5. **Services** : laissez le Cloud Backup Service activé et cliquez sur **Continuer**.

Services

Backup to Cloud

☒
▼

6. Complétez les pages de l'assistant pour déployer le système comme décrit à la section "[Lancement d'Cloud Volumes ONTAP dans GCP](#)".

## Résultat

Cloud Backup est activé sur le système. Il sauvegarde le volume que vous créez chaque jour et conserve les 30 copies de sauvegarde les plus récentes.

## Activation de Cloud Backup sur un système existant

Vous pouvez activer Cloud Backup à tout moment directement depuis l'environnement de travail.

### Étapes

1. Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service de sauvegarde et de restauration dans le panneau de droite.

Si la destination Google Cloud Storage pour vos sauvegardes existe en tant qu'environnement de travail sur la Canvas, vous pouvez faire glisser le cluster vers l'environnement de travail Google Cloud Storage pour lancer l'assistant d'installation.



2. Sélectionnez Google Cloud Project et la région dans laquelle vous souhaitez créer le compartiment Google Cloud Storage pour les sauvegardes, puis cliquez sur **Next**.

Notez que le projet doit disposer d'un compte de service avec le rôle d'administrateur de stockage prédéfini.

3. Entrez les détails de la stratégie de sauvegarde qui seront utilisés pour votre stratégie par défaut et cliquez sur **Suivant**. Vous pouvez sélectionner une stratégie existante ou créer une nouvelle stratégie en entrant vos sélections dans chaque section :
  - a. Entrez le nom de la stratégie par défaut. Il n'est pas nécessaire de modifier le nom.
  - b. Définissez le programme de sauvegarde et choisissez le nombre de sauvegardes à conserver.  
["Consultez la liste des règles que vous pouvez choisir"](#).

Policy Type	
<input checked="" type="radio"/> Create a new Policy	<input type="radio"/> Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
Archival Policy	Disabled	▼

4. Sélectionnez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde définie dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des stratégies supplémentaires et les appliquer ultérieurement à ces volumes.
  - Pour sauvegarder tous les volumes existants et les volumes ajoutés à l'avenir, cochez la case « Sauvegarder tous les volumes existants et futurs... ». Nous vous recommandons cette option afin que tous vos volumes soient sauvegardés et que vous n'aurez jamais à vous souvenir de pouvoir effectuer des sauvegardes pour de nouveaux volumes.
  - Pour sauvegarder uniquement les volumes existants, cochez la case de la ligne de titre

(☒ Volume Name).

- Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☒ Volume\_1).

Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy

☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 ● On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 ● On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 ● On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 ● On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 ● On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100 < 1 >

Previous

Activate Backup

- Si dans cet environnement de travail contient des copies Snapshot locales pour les volumes en lecture/écriture qui correspondent au libellé de la planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidien, hebdomadaire, etc.), une invite supplémentaire s'affiche « Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde ». Cochez cette case si vous souhaitez que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin d'assurer la protection la plus complète de vos volumes.

5. Cliquez sur **Activer la sauvegarde** et Cloud Backup commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

## Résultat

Un compartiment Google Cloud Storage est créé automatiquement dans le compte de service indiqué par la clé d'accès Google et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés. Le tableau de bord de sauvegarde de volume s'affiche pour vous permettre de surveiller l'état des sauvegardes. Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l' "[Panneau surveillance des tâches](#)".

Les sauvegardes sont associées par défaut à la classe de stockage *Standard*. Vous pouvez utiliser les classes de stockage *Nearline*, *Coldline* ou *Archive* moins coûteuses. Toutefois, vous configurez la classe de stockage via Google, et non via l'interface utilisateur de Cloud Backup. Consultez la rubrique Google "[Modification de la classe de stockage par défaut d'un compartiment](#)" pour plus d'informations.

## Et la suite ?

- C'est possible "[gérez vos fichiers de sauvegarde et vos règles de sauvegarde](#)". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la

planification des sauvegardes, etc.

- C'est possible "[gérez les paramètres de sauvegarde au niveau du cluster](#)". Cela inclut notamment la modification de la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus encore.
- Vous pouvez également "[restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde](#)" Vers un système Cloud Volumes ONTAP dans Google ou vers un système ONTAP sur site.

## Sauvegarde des données ONTAP sur site dans Google Cloud Storage

Procédez comme suit pour commencer à sauvegarder des données depuis vos systèmes ONTAP sur site vers Google Cloud Storage.

Notez que les « systèmes ONTAP sur site » comprennent les systèmes FAS, AFF et ONTAP Select.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Vérifiez la prise en charge de votre configuration

- Vous avez découvert le cluster sur site et l'avez ajouté à un environnement de travail dans BlueXP. Voir "[Découverte des clusters ONTAP](#)" pour plus d'informations.
  - Le cluster exécute ONTAP 9.7P5 ou version ultérieure.
  - Le cluster est doté d'une licence SnapMirror — elle est incluse dans le bundle Premium ou Data protection.
  - Le cluster doit disposer des connexions réseau requises vers le stockage Google et vers le connecteur.
- Le connecteur doit disposer des connexions réseau requises vers le stockage Google et vers le cluster.
- Vous disposez d'un abonnement Google valide pour l'espace de stockage objet sur lequel vos sauvegardes seront stockées.
- Vous disposez d'un compte Google avec une clé d'accès et une clé secrète pour que le cluster ONTAP puisse sauvegarder et restaurer des données.

2

#### Activation de Cloud Backup sur le système

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau droit, puis suivez l'assistant d'installation.





3

### Sélectionnez le fournisseur de cloud et entrez les informations relatives au fournisseur

Sélectionnez Google Cloud comme fournisseur, puis saisissez les informations relatives au fournisseur. Vous devez également spécifier l'IPspace dans le cluster ONTAP où les volumes résident.

4

### Définissez la stratégie de sauvegarde par défaut

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passage à des sauvegardes toutes les heures, tous les jours, toutes les semaines, tous les mois ou tous les ans vous pouvez également sélectionner l'une des règles définies par le système qui offrent plus d'options. Vous pouvez également modifier le nombre de copies de sauvegarde à conserver.

Les sauvegardes sont stockées dans le stockage standard par défaut. Si votre cluster utilise ONTAP 9.12.1 ou version ultérieure, vous pouvez choisir de transférer les sauvegardes vers le stockage Google Archive après un certain nombre de jours afin d'optimiser les coûts. ["En savoir plus sur les paramètres de configuration des règles de sauvegarde dans le cloud"](#).

#### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

i Cloud Backup will create the **Google Cloud Storage** bucket after you complete the wizard

**Policy Type**
☒ Create a new Policy
☐ Select an existing Policy

<b>Name</b>	Default_Policy_Name <span style="float: right;">▼</span>
<b>Labels &amp; Retention</b>	30 Daily <span style="float: right;">▼</span>
<b>Archival Policy</b>	Disabled <span style="float: right;">▼</span>

5

### Sélectionnez les volumes à sauvegarder

Identifiez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde par défaut dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des règles supplémentaires et les appliquer ultérieurement aux volumes.

## De formation

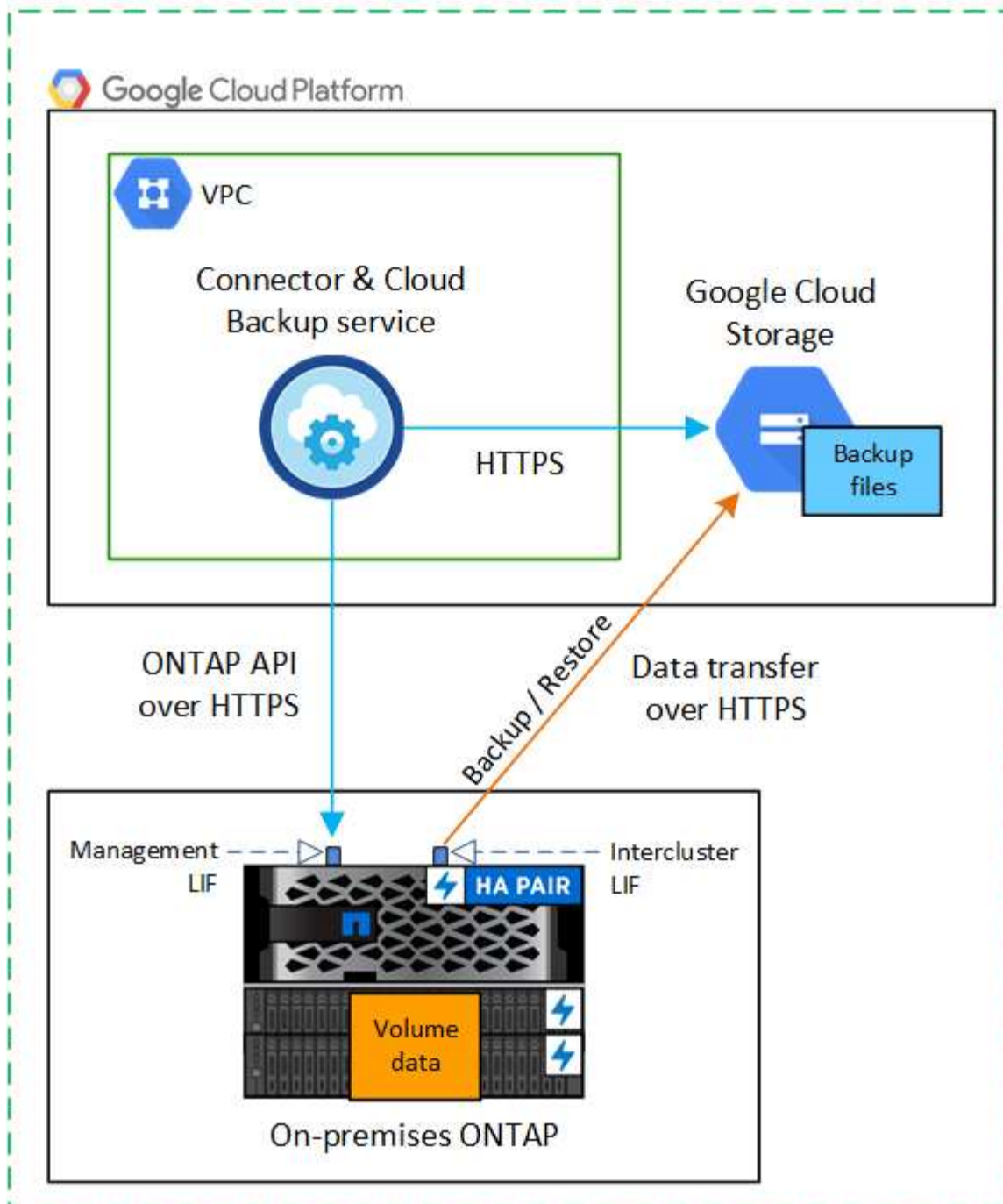
Avant de commencer à sauvegarder des volumes sur site vers Google Cloud, lisez les sections suivantes pour vérifier que votre configuration est prise en charge.

Deux méthodes de connexion sont disponibles pour la configuration des sauvegardes depuis les systèmes ONTAP sur site vers Google Cloud Storage.

- Connexion publique : connectez directement le système ONTAP à Google Cloud Storage à l'aide d'un terminal Google public.
- Connexion privée : utilisez une connexion VPN ou Google Cloud Interconnect et acheminez le trafic via une interface privée Google Access qui utilise une adresse IP privée.

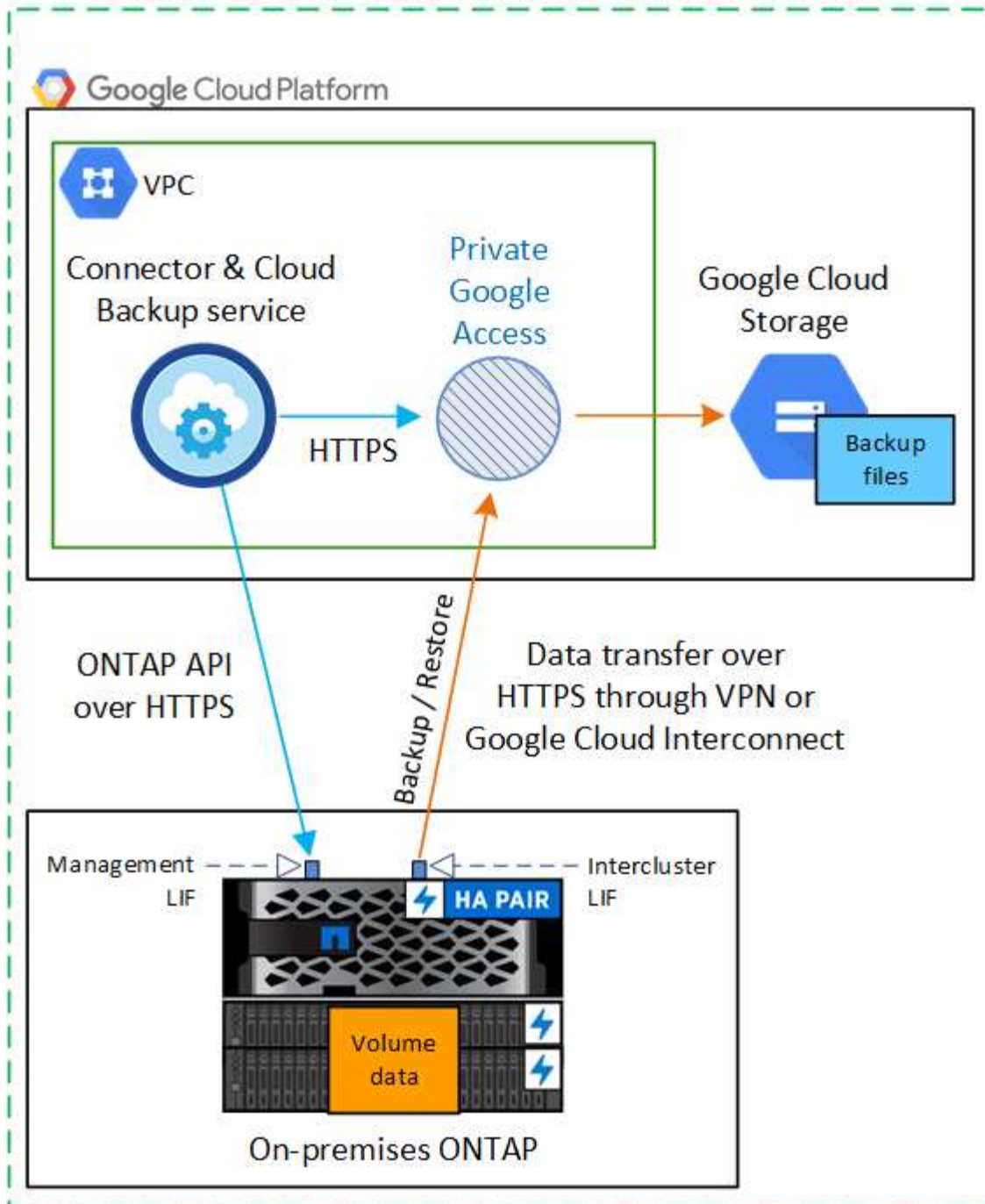
Le schéma suivant montre la méthode **connexion publique** et les connexions que vous devez préparer entre les composants. Le connecteur doit être déployé dans le VPC Google Cloud Platform.

## Connector deployed in Google Cloud VPC



Le schéma suivant montre la méthode **connexion privée** et les connexions que vous devez préparer entre les composants. Le connecteur doit être déployé dans le VPC Google Cloud Platform.

## Connector deployed in Google Cloud VPC



### Préparation des clusters ONTAP

Vous devez découvrir vos clusters ONTAP sur site dans BlueXP avant de pouvoir commencer à sauvegarder des données de volumes.

["Découvrez comment détecter un cluster"](#).

### Conditions requises pour le ONTAP

- Minimum de ONTAP 9.7P5 ; ONTAP 9.8P13 et version ultérieure est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

**Remarque :** le « bundle Cloud hybride » n'est pas requis pour l'utilisation de Cloud Backup.

Découvrez comment ["gérez les licences du cluster"](#).

- L'heure et le fuseau horaire sont correctement réglés.

Découvrez comment ["configurez l'heure du cluster"](#).

### Configuration requise pour la mise en réseau des clusters

- Le cluster ONTAP établit une connexion HTTPS via le port 443 entre le LIF intercluster et Google Cloud Storage pour les opérations de sauvegarde et de restauration.

Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur peut résider dans un VPC Google Cloud Platform.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. ["En savoir plus sur les IPspaces"](#).

Lors de la configuration de Cloud Backup, vous êtes invité à utiliser l'*IPspace*. Vous devez choisir l'*IPspace* auquel chaque LIF est associée. Il peut s'agir de l'*IPspace* par défaut ou d'un *IPspace* personnalisé que vous avez créé.

- Les LIFs intercluster des nœuds peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment ["Configuration des services DNS pour le SVM"](#).

Si vous utilisez Private Google Access ou Private Service Connect, assurez-vous que vos serveurs DNS ont été configurés pour pointer `storage.googleapis.com` vers l'adresse IP interne (privée) correcte.

- Notez que si vous utilisez un *IPspace* différent de celui utilisé par défaut, vous devrez peut-être créer une route statique pour obtenir l'accès au stockage objet.
- Mettre à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions Cloud Backup Service de ONTAP au stockage objet via le port 443 et le trafic de résolution de nom entre le VM de stockage et le serveur DNS via le port 53 (TCP/UDP).

### Création ou commutation de connecteurs

Si un connecteur est déjà déployé dans votre VPC Google Cloud Platform, vous devez le configurer. Dans le cas contraire, créez un connecteur sur cet emplacement pour sauvegarder les données ONTAP dans un stockage Google Cloud. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur cloud ou sur site.

- ["En savoir plus sur les connecteurs"](#)
- ["Mise en route des connecteurs"](#)
- ["Installation d'un connecteur dans GCP"](#)

### Préparation de la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

## Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
  - Une connexion Internet sortante vers le Cloud Backup Service over port 443 (HTTPS)
  - Une connexion HTTPS via le port 443 vers votre stockage Google Cloud
  - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
2. Activez Private Google Access (ou Private Service Connect) sur le sous-réseau où vous prévoyez de déployer le connecteur. "[Accès privé à Google](#)" ou "[Service privé Connect](#)" Sont nécessaires si vous disposez d'une connexion directe entre votre cluster ONTAP et le VPC et que vous souhaitez que la communication entre le connecteur et Google Cloud Storage reste dans votre réseau privé virtuel (une connexion **privée**).

Suivez les instructions Google pour configurer ces options d'accès privé. Assurez-vous que vos serveurs DNS ont été configurés aux points [www.googleapis.com](http://www.googleapis.com) et [storage.googleapis.com](http://storage.googleapis.com) pour les adresses IP internes (privées) correctes.

## Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité « recherche et restauration » de Cloud Backup, vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder au service Google Cloud BigQuery. Reportez-vous aux autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

### Étapes

1. Dans "[Console cloud](#)", Allez à la page **rôles**.
2. A l'aide de la liste déroulante située en haut de la page, sélectionnez le projet ou l'organisation qui contient le rôle que vous souhaitez modifier.
3. Cliquez sur un rôle personnalisé.
4. Cliquez sur **Modifier le rôle** pour mettre à jour les autorisations du rôle.
5. Cliquez sur **Ajouter des autorisations** pour ajouter les nouvelles autorisations suivantes au rôle.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Cliquez sur **Update** pour enregistrer le rôle modifié.

## Vérification des besoins en licence

- Avant d'activer Cloud Backup pour votre cluster, vous devez vous abonner à une offre BlueXP Marketplace sur Google, ou acheter et activer une licence Cloud Backup BYOL auprès de NetApp. Ces licences sont

destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.

- Pour acquérir une licence Cloud Backup PAYGO, vous devez souscrire un abonnement à la ["Google" Offre BlueXP Marketplace](#) pour utiliser Cloud Backup. La facturation pour Cloud Backup s'effectue via cet abonnement.
- Dans le cas des licences BYOL, vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité du contrat. ["Découvrez comment gérer vos licences BYOL"](#).
- Vous devez disposer d'un abonnement Google pour l'espace de stockage objet dans lequel vos sauvegardes seront stockées.

Vous pouvez créer des sauvegardes à partir de systèmes sur site vers Google Cloud Storage dans toutes les régions ["Dans ce cas, Cloud Volumes ONTAP est pris en charge"](#). Vous spécifiez la région dans laquelle les sauvegardes seront stockées lors de la configuration du service.

## Préparation de Google Cloud Storage pour les sauvegardes

Lorsque vous configurez la sauvegarde, vous devez fournir des clés d'accès au stockage pour un compte de service avec des autorisations d'administrateur du stockage. Un compte de service permet à Cloud Backup d'authentifier et d'accéder aux compartiments Cloud Storage utilisés pour stocker les sauvegardes. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

### Étapes

1. ["Créez un compte de service avec le rôle d'administrateur de stockage prédéfini"](#).
2. Accédez à ["Paramètres de stockage GCP"](#) et créez des clés d'accès pour le compte de service :
  - a. Sélectionnez un projet et cliquez sur **interopérabilité**. Si ce n'est déjà fait, cliquez sur **Activer l'accès à l'interopérabilité**.
  - b. Sous **clés d'accès pour les comptes de service**, cliquez sur **Créer une clé pour un compte de service**, sélectionnez le compte de service que vous venez de créer, puis cliquez sur **Créer une clé**.

Lorsque vous configurez le service de sauvegarde, vous devrez saisir les clés dans Cloud Backup.

## Activation de Cloud Backup

Activation de Cloud Backup à tout moment directement depuis l'environnement de travail sur site

### Étapes

1. Dans Canvas, sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.

Si la destination Google Cloud Storage pour vos sauvegardes existe en tant qu'environnement de travail sur la Canvas, vous pouvez faire glisser le cluster vers l'environnement de travail Google Cloud Storage pour lancer l'assistant d'installation.





2. Sélectionnez Google Cloud comme fournisseur et cliquez sur **Suivant**.
3. Entrez les détails du fournisseur et cliquez sur **Suivant**.
  - a. Google Cloud Project où vous souhaitez créer le compartiment Google Cloud Storage pour la sauvegarde. (Le projet doit disposer d'un compte de service avec le rôle d'administrateur de stockage prédéfini.)
  - b. Clé d'accès Google et clé secrète utilisées pour stocker les sauvegardes.
  - c. Région Google où les sauvegardes seront stockées.
  - d. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.

4. Si vous ne disposez pas d'une licence Cloud Backup pour votre compte, vous êtes invité à sélectionner le type de mode de facturation que vous souhaitez utiliser. Vous pouvez vous abonner à une offre de paiement basé sur l'utilisation (PAYGO) BlueXP Marketplace de Google (ou si vous disposez de plusieurs abonnements, vous pouvez en sélectionner un), ou acheter et activer une licence Cloud Backup BYOL auprès de NetApp. ["Découvrez comment configurer les licences Cloud Backup."](#)
5. Entrez les détails de la stratégie de sauvegarde qui seront utilisés pour votre stratégie par défaut et cliquez sur **Suivant**. Vous pouvez sélectionner une stratégie existante ou créer une nouvelle stratégie en entrant vos sélections dans chaque section :
  - a. Entrez le nom de la stratégie par défaut. Il n'est pas nécessaire de modifier le nom.
  - b. Définissez le programme de sauvegarde et choisissez le nombre de sauvegardes à conserver. ["Consultez la liste des règles que vous pouvez choisir"](#).
  - c. Si vous utilisez ONTAP 9.12.1 ou version ultérieure, vous pouvez choisir de transférer les sauvegardes vers le stockage d'archivage après un certain nombre de jours afin d'optimiser les coûts. ["En savoir plus sur les paramètres de configuration des règles de sauvegarde dans le cloud"](#).



### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Cloud Backup will create the **Google Cloud Storage** bucket after you complete the wizard

**Policy Type** ☒ Create a new Policy ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
Archival Policy	Disabled	▼

6. Sélectionnez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde définie dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des stratégies supplémentaires et les appliquer ultérieurement à ces volumes.

- Pour sauvegarder tous les volumes existants et les volumes ajoutés à l'avenir, cochez la case « Sauvegarder tous les volumes existants et futurs... ». Nous vous recommandons cette option afin que tous vos volumes soient sauvegardés et que vous n'aurez jamais à vous souvenir de pouvoir effectuer des sauvegardes pour de nouveaux volumes.
- Pour sauvegarder uniquement les volumes existants, cochez la case de la ligne de titre **Volume Name** ).
- Pour sauvegarder des volumes individuels, cochez la case de chaque volume ( **Volume\_1** ).

### Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy

☒ Export existing Snapshot copies to object storage as backup files

100 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 <span style="color: green;">●</span> On	RW	SVM_1	12.125 GiB	25 GiB	Not Active
<input checked="" type="checkbox"/>	Volume 2 <span style="color: green;">●</span> On	RW	SVM_1	1.1 GiB	2 GiB	Not Active
<input checked="" type="checkbox"/>	Volume 3 <span style="color: green;">●</span> On	RW	SVM_1	15 GiB	25 GiB	Not Active
<input checked="" type="checkbox"/>	Volume 4 <span style="color: green;">●</span> On	RW	SVM_1	1.125 GiB	5 GiB	Not Active
<input checked="" type="checkbox"/>	Volume 5 <span style="color: green;">●</span> On	RW	SVM_1	12 GiB	25 GiB	Not Active

1 - 50 of 100 < 1 >

Previous
Activate Backup

- Si dans cet environnement de travail contient des copies Snapshot locales pour les volumes en lecture/écriture qui correspondent au libellé de la planification de sauvegarde que vous venez de

sélectionner pour cet environnement de travail (par exemple, quotidien, hebdomadaire, etc.), une invite supplémentaire s'affiche « Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde ». Cochez cette case si vous souhaitez que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin d'assurer la protection la plus complète de vos volumes.

7. Cliquez sur **Activer la sauvegarde** et Cloud Backup commence à effectuer les sauvegardes initiales de vos volumes.

## Résultat

Un compartiment Google Cloud Storage est créé automatiquement dans le compte de service indiqué par la clé d'accès Google et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés. Le tableau de bord de sauvegarde de volume s'affiche pour vous permettre de surveiller l'état des sauvegardes. Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l' "[Panneau surveillance des tâches](#)".

## Et la suite ?

- C'est possible "[gérez vos fichiers de sauvegarde et vos règles de sauvegarde](#)". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "[gérez les paramètres de sauvegarde au niveau du cluster](#)". Il s'agit notamment de changer les clés de stockage que ONTAP utilise pour accéder au stockage cloud, de modifier la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, de modifier le paramètre de sauvegarde automatique pour les volumes futurs, etc.
- Vous pouvez également "[restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde](#)" Vers un système Cloud Volumes ONTAP dans Google ou vers un système ONTAP sur site.

# La sauvegarde des données ONTAP sur site dans StorageGRID

Suivez quelques étapes pour commencer à sauvegarder les données depuis vos systèmes ONTAP sur site vers le stockage objet dans vos systèmes NetApp StorageGRID.

Notez que les « systèmes ONTAP sur site » comprennent les systèmes FAS, AFF et ONTAP Select.

## Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

### Vérifiez la prise en charge de votre configuration

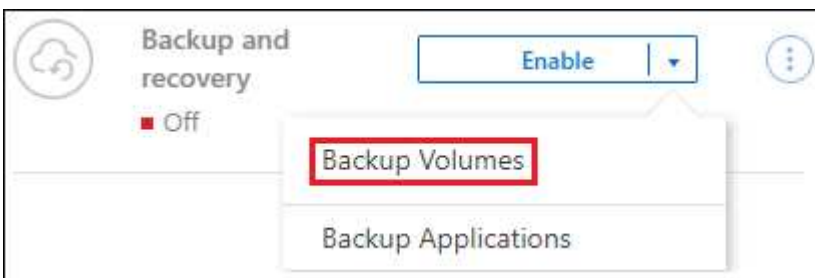
- Vous avez découvert le cluster sur site et l'avez ajouté à un environnement de travail dans BlueXP. Voir "[Découverte des clusters ONTAP](#)" pour plus d'informations.
  - Le cluster exécute ONTAP 9.7P5 ou version ultérieure.
  - Le cluster est doté d'une licence SnapMirror — elle est incluse dans le bundle Premium ou Data protection.

- Le cluster doit disposer des connexions réseau requises vers le StorageGRID et vers le connecteur.
- Un connecteur est installé sur votre site.
  - Le connecteur peut être installé sur un site avec ou sans accès à Internet.
  - La mise en réseau du connecteur permet une connexion HTTPS sortante vers le cluster ONTAP et vers StorageGRID.
- Vous avez acheté "et activé" Licence Cloud Backup BYOL de NetApp.
- Votre StorageGRID possède la version 10.3 ou ultérieure avec des clés d'accès qui disposent des autorisations S3.

## 2

### Activation de Cloud Backup sur le système

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau droit, puis suivez l'assistant d'installation.



## 3

### Entrer les détails StorageGRID

Sélectionnez StorageGRID comme fournisseur, puis entrez les informations du serveur StorageGRID et du compte de locataire S3. Vous devez également spécifier l'IPspace dans le cluster ONTAP où les volumes résident.

### Storage Settings

i Notice : There is no option to change the provider settings after the service has started

<p><b>Storage Information</b></p> <p>StorageGRID Gateway Node FQDN</p> <input style="width: 90%;" type="text" value="s3.storagegrid.company.com"/> <p>Port</p> <input style="width: 90%;" type="text" value="10443"/> <p>Access Key</p> <input style="width: 90%;" type="text" value="Enter Access Key"/> <p>Secret Key</p> <input style="width: 90%;" type="text" value="Enter Secret Key"/>	<p><b>Connectivity</b></p> <p>IPspace</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> <span>Default</span> <span>▼</span> </div>
---	--

## 4

### Définissez la stratégie de sauvegarde par défaut

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passage à des sauvegardes toutes les heures, tous les jours, toutes les semaines, tous les mois ou tous les ans vous pouvez également sélectionner l'une des règles définies par le système qui offrent plus d'options. Vous pouvez également modifier le nombre de copies de sauvegarde à conserver.

Si vous utilisez ONTAP 9.11.1 ou version ultérieure, vous pouvez choisir de protéger vos sauvegardes contre les suppressions et les attaques par ransomware en configurant l'un des paramètres *DataLock et ransomware protection*. ["En savoir plus sur les paramètres de configuration des règles de sauvegarde dans le cloud"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy Type

☒ Create a new Policy
 ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼

## 5

### Sélectionnez les volumes à sauvegarder

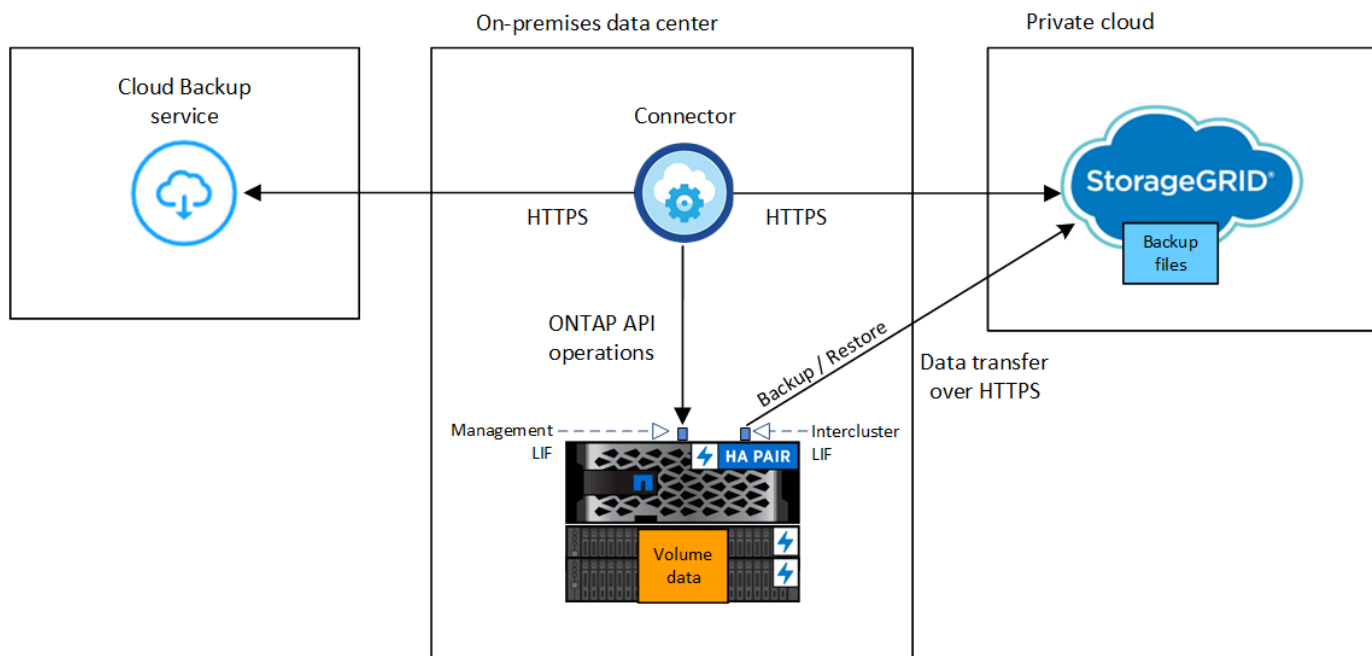
Identifiez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde par défaut dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des règles supplémentaires et les appliquer ultérieurement aux volumes.

Un compartiment S3 est créé automatiquement dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisie, et les fichiers de sauvegarde y sont stockés.

## De formation

Avant de commencer à sauvegarder des volumes sur site vers StorageGRID, lisez les informations suivantes pour vous assurer que votre configuration est prise en charge.

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP sur site vers StorageGRID et les connexions dont vous avez besoin pour les préparer :



Lorsque le connecteur et le système ONTAP sur site sont installés sur site sans accès à Internet, le système StorageGRID doit se trouver dans le même data Center sur site.

## Préparation des clusters ONTAP

Vous devez découvrir vos clusters ONTAP sur site dans BlueXP avant de pouvoir commencer à sauvegarder des données de volumes.

["Découvrez comment détecter un cluster"](#).

## Conditions requises pour le ONTAP

- Minimum de ONTAP 9.7P5 ; ONTAP 9.8P13 et version ultérieure est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

**Remarque :** le « bundle Cloud hybride » n'est pas requis pour l'utilisation de Cloud Backup.

Découvrez comment ["gérez les licences du cluster"](#).

- L'heure et le fuseau horaire sont correctement réglés.

Découvrez comment ["configurez l'heure du cluster"](#).

## Configuration requise pour la mise en réseau des clusters

- Le cluster ONTAP établit une connexion HTTPS via un port spécifié par l'utilisateur depuis le LIF intercluster vers le nœud de passerelle StorageGRID pour les opérations de sauvegarde et de restauration. Le port est configurable lors de la configuration de la sauvegarde.

Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur doit résider sur votre site.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous

souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. ["En savoir plus sur les IPspaces"](#).

Lors de la configuration de Cloud Backup, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs intercluster des nœuds peuvent accéder au magasin d'objets (non requise lorsque le connecteur est installé sur un site « foncé »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment ["Configuration des services DNS pour le SVM"](#).
- Notez que si vous utilisez un IPspace différent de celui utilisé par défaut, vous devrez peut-être créer une route statique pour obtenir l'accès au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour autoriser les connexions Cloud Backup Service de ONTAP au stockage objet via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de nom entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

## Préparation de StorageGRID

StorageGRID doit remplir les conditions suivantes. Voir la ["Documentation StorageGRID"](#) pour en savoir plus.

### Versions de StorageGRID prises en charge

StorageGRID 10.3 et versions ultérieures sont prises en charge.

Pour utiliser DataLock & protection contre les attaques par ransomware pour vos sauvegardes, vos systèmes StorageGRID doivent exécuter la version 11.6.0.3 ou ultérieure.

### Identifiants S3

Vous devez avoir créé un compte de locataire S3 pour contrôler l'accès à votre stockage StorageGRID. ["Pour plus d'informations, consultez la documentation StorageGRID"](#).

Lorsque vous configurez la sauvegarde sur StorageGRID, l'assistant de sauvegarde vous demande une clé d'accès S3 et une clé secrète pour un compte de locataire. Le compte locataire permet à Cloud Backup d'authentifier et d'accéder aux compartiments StorageGRID utilisés pour stocker les sauvegardes. Les clés sont requises afin que StorageGRID sache qui effectue la demande.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",  
"s3:ListBucket",  
"s3:GetObject",  
"s3:PutObject",  
"s3:DeleteObject",  
"s3:CreateBucket"
```

### Gestion des versions d'objet

Vous ne devez pas activer manuellement la gestion des versions d'objets StorageGRID sur le compartiment de magasin d'objets.

## Création ou commutation de connecteurs

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.

- ["En savoir plus sur les connecteurs"](#)
- ["Installation du connecteur sur un hôte Linux avec accès à Internet"](#)
- ["Installation du connecteur sur un hôte Linux sans accès à Internet"](#)
- ["Basculement entre les connecteurs"](#)



La fonctionnalité Cloud Backup est intégrée dans le connecteur BlueXP. Lorsqu'il est installé sur un site sans connexion Internet, vous devez mettre à jour régulièrement le logiciel Connector pour accéder aux nouvelles fonctionnalités. Vérifier le ["Nouveautés de Cloud Backup"](#) Pour découvrir les nouvelles fonctionnalités de chaque version de Cloud Backup, puis suivez les étapes à ["Mettez à niveau le logiciel du connecteur"](#) lorsque vous voulez utiliser de nouvelles fonctions.

## Préparation de la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

### Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
  - Une connexion HTTPS via le port 443 vers le nœud de passerelle StorageGRID
  - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
  - Une connexion Internet sortante via le port 443 vers Cloud Backup (inutile lorsque le connecteur est installé sur un site « foncé »)

## Conditions de licence

Avant de pouvoir activer Cloud Backup pour votre cluster, vous devez acheter une licence Cloud Backup BYOL auprès de NetApp, puis l'activer. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

Vous aurez besoin du numéro de série de NetApp qui vous permettra d'utiliser le service pendant la durée et la capacité de la licence. ["Découvrez comment gérer vos licences BYOL"](#).



Les licences PAYGO ne sont pas prises en charge lors de la sauvegarde des fichiers vers StorageGRID.

## Activation de Cloud Backup vers StorageGRID

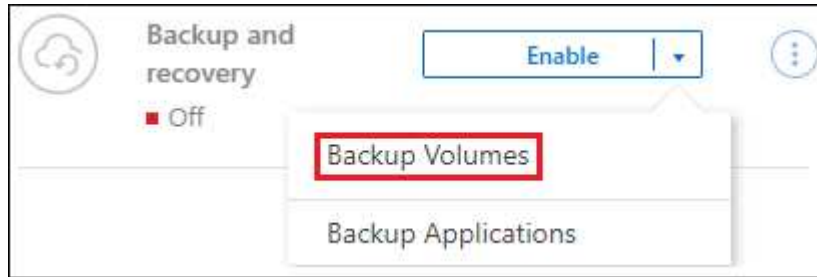
Activation de Cloud Backup à tout moment directement depuis l'environnement de travail sur site

### Étapes

1. Dans Canvas, sélectionnez l'environnement de travail sur site et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.

Si la destination StorageGRID de vos sauvegardes existe en tant qu'environnement de travail dans la

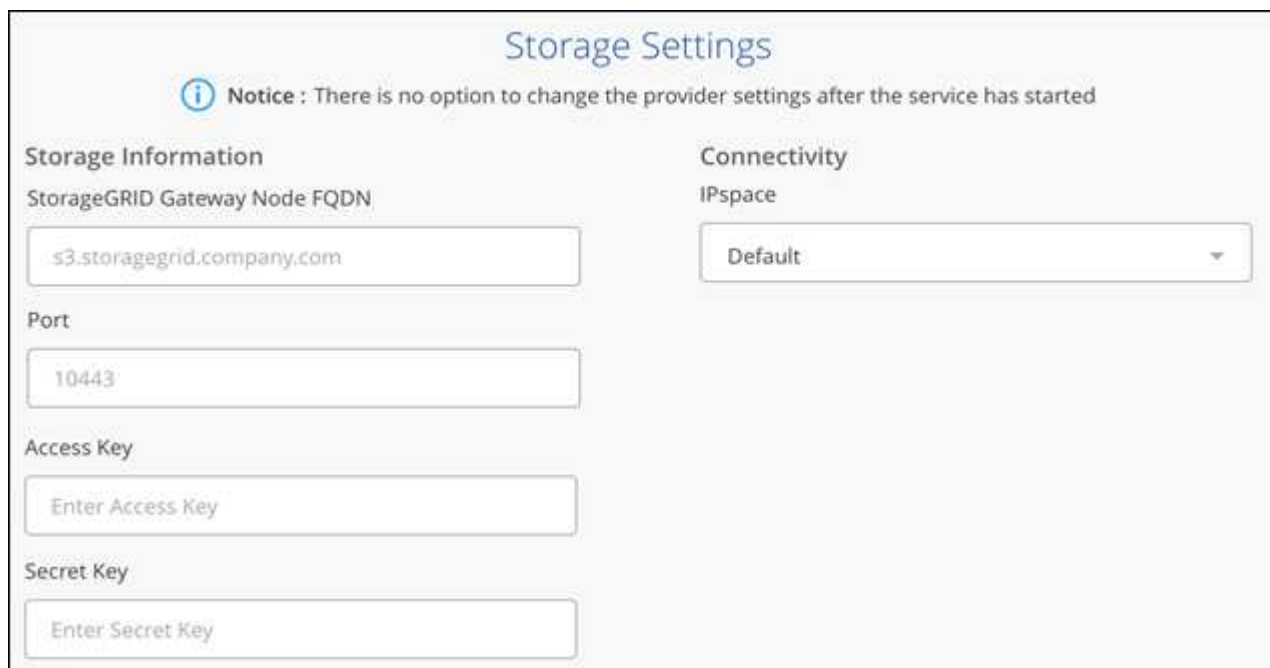
fenêtre Canvas, vous pouvez faire glisser le cluster dans l'environnement de travail StorageGRID pour lancer l'assistant d'installation.



2. Sélectionnez **StorageGRID** comme fournisseur, cliquez sur **Suivant**, puis entrez les détails du fournisseur :

- Nom de domaine complet du nœud de passerelle StorageGRID.
- Port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID.
- La clé d'accès et la clé secrète utilisées pour accéder au compartiment afin de stocker des sauvegardes.
- L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster de cet IPspace doivent disposer d'un accès Internet sortant (non requis lorsque le connecteur est installé sur un site « foncé »).

Le choix du bon IPspace garantit que Cloud Backup peut configurer une connexion de ONTAP à votre stockage objet StorageGRID.



3. Entrez les détails de la stratégie de sauvegarde qui seront utilisés pour votre stratégie par défaut et cliquez sur **Suivant**. Vous pouvez sélectionner une stratégie existante ou créer une nouvelle stratégie en entrant vos sélections dans chaque section :

- Entrez le nom de la stratégie par défaut. Il n'est pas nécessaire de modifier le nom.
- Définissez le programme de sauvegarde et choisissez le nombre de sauvegardes à conserver.



["Consultez la liste des règles que vous pouvez choisir".](#)

- c. Si vous utilisez ONTAP 9.11.1 ou version supérieure, vous pouvez choisir de protéger vos sauvegardes contre la suppression et les attaques par ransomware en configurant *DataLock et protection contre les attaques par ransomware*. *DataLock* protège vos fichiers de sauvegarde contre la modification ou la suppression, et *Attack protection* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware dans vos fichiers de sauvegarde. ["En savoir plus sur les paramètres DataLock disponibles"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼

**Important:** si vous prévoyez d'utiliser DataLock, vous devez l'activer dans votre première stratégie lors de l'activation de Cloud Backup.

4. Sélectionnez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde définie dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des stratégies supplémentaires et les appliquer ultérieurement à ces volumes.
- Pour sauvegarder tous les volumes existants et les volumes ajoutés à l'avenir, cochez la case « Sauvegarder tous les volumes existants et futurs... ». Nous vous recommandons cette option afin que tous vos volumes soient sauvegardés et que vous n'aurez jamais à vous souvenir de pouvoir effectuer des sauvegardes pour de nouveaux volumes.
  - Pour sauvegarder uniquement les volumes existants, cochez la case de la ligne de titre (☒ Volume Name).
  - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☒ Volume\_1).

**Select Volumes**

☒ Back up all existing and future volumes using the selected Backup policy  
☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes
🔍

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 <span style="color: green;">●</span> On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 <span style="color: green;">●</span> On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 <span style="color: green;">●</span> On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 <span style="color: green;">●</span> On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 <span style="color: green;">●</span> On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100    < 1 >

Previous
Activate Backup

- Si dans cet environnement de travail contient des copies Snapshot locales pour les volumes en lecture/écriture qui correspondent au libellé de la planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidien, hebdomadaire, etc.), une invite supplémentaire s'affiche « Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde ». Cochez cette case si vous souhaitez que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin d'assurer la protection la plus complète de vos volumes.

5. Cliquez sur **Activer la sauvegarde** et Cloud Backup commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

## Résultat

Un compartiment S3 est créé automatiquement dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisie, et les fichiers de sauvegarde y sont stockés. Le tableau de bord de sauvegarde de volume s'affiche pour vous permettre de surveiller l'état des sauvegardes. Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l' "[Panneau surveillance des tâches](#)".

## Et la suite ?

- C'est possible "[gérez vos fichiers de sauvegarde et vos règles de sauvegarde](#)". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "[gérez les paramètres de sauvegarde au niveau du cluster](#)". Il s'agit notamment de changer les clés de stockage que ONTAP utilise pour accéder au stockage cloud, de modifier la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, de modifier le paramètre de sauvegarde automatique pour les volumes futurs, etc.
- Vous pouvez également "[restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde](#)" Sur un système ONTAP local.

# Gestion des sauvegardes de vos systèmes ONTAP

Vous pouvez gérer les sauvegardes de vos systèmes Cloud Volumes ONTAP et ONTAP sur site en modifiant la planification de sauvegarde, en créant de nouvelles stratégies de sauvegarde, en activant/désactivant les sauvegardes de volume, en pause des sauvegardes, en supprimant les sauvegardes, etc.



Ne gérez ni ne modifiez pas de fichiers de sauvegarde directement depuis votre environnement cloud fournisseur. Cela peut corrompre les fichiers et entraîner une configuration non prise en charge.

## Affichage des volumes en cours de sauvegarde

Vous pouvez afficher la liste de tous les volumes actuellement sauvegardés dans le tableau de bord de sauvegarde.

### Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **volumes** pour afficher la liste des volumes sauvegardés pour les systèmes Cloud Volumes ONTAP et ONTAP sur site.

The screenshot shows the 'Volumes' tab in the BlueXP interface. At the top, there's a navigation bar with tabs: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below this, a dropdown menu is set to 'All Backed Up Working Environments'. A summary section displays: 6 Working Environments, 2,011 Protected Volumes, and 125.75 TB Total Backup Size. To the right, a 'Backup Volumes Status' box shows 1,924 Healthy Backup Volumes and 87 Failed Backup Volumes. A search icon is visible in the top right corner of the main content area. Below the summary, a table titled '2,011 Backed Up Volumes' lists individual volumes. The table has columns: Source Volume, Source Working Environment, Source SVM, Ransomware Protection, Backup Status, Last Backup, Backups, and Tiering to Archive. Three volumes are shown as examples.

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup	Backups	Tiering to Archive
Volume 1 On	Working Environment 1 On	Source SVM 1	None	Active	June 12 2022,	125 Backups	Active
Volume 2 On	Working Environment 1 On	Source SVM 2	Governance	Active	June 12 2022,	25 Backups	Disabled
Volume 3 On	Working Environment 1 On	Source SVM 1	Compliance	Active	June 12 2022,	15 Backups	Disabled

Si vous recherchez des volumes spécifiques dans certains environnements de travail, vous pouvez affiner la liste par environnement de travail et volume, ou vous pouvez utiliser le filtre de recherche.

## Activation et désactivation des sauvegardes des volumes

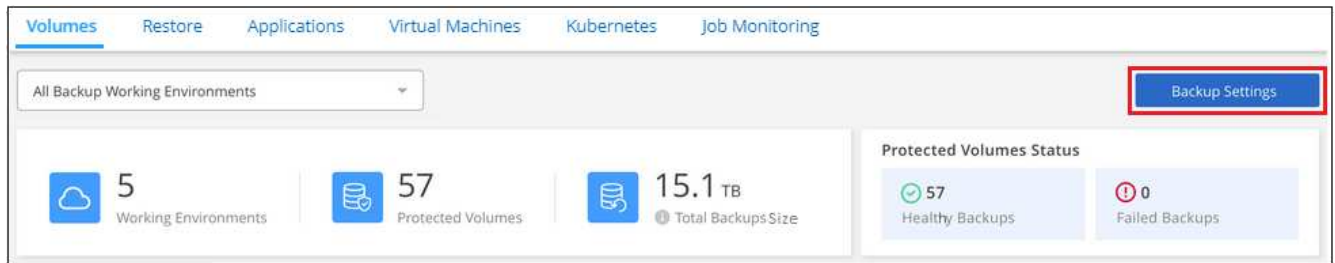
Vous pouvez activer les sauvegardes de tout nouveau volume s'ils ne sont pas actuellement sauvegardés. Vous pouvez également activer les sauvegardes de tous les volumes que vous avez précédemment désactivés.

Vous pouvez désactiver les sauvegardes pour les volumes de manière à ce qu'aucune sauvegarde supplémentaire ne soit générée. Cela désactive également la restauration des données de volume à partir d'un fichier de sauvegarde. Cette opération vous permet en fait d'interrompre l'ensemble des activités de sauvegarde et de restauration pendant une période donnée. Les sauvegardes existantes ne seront pas

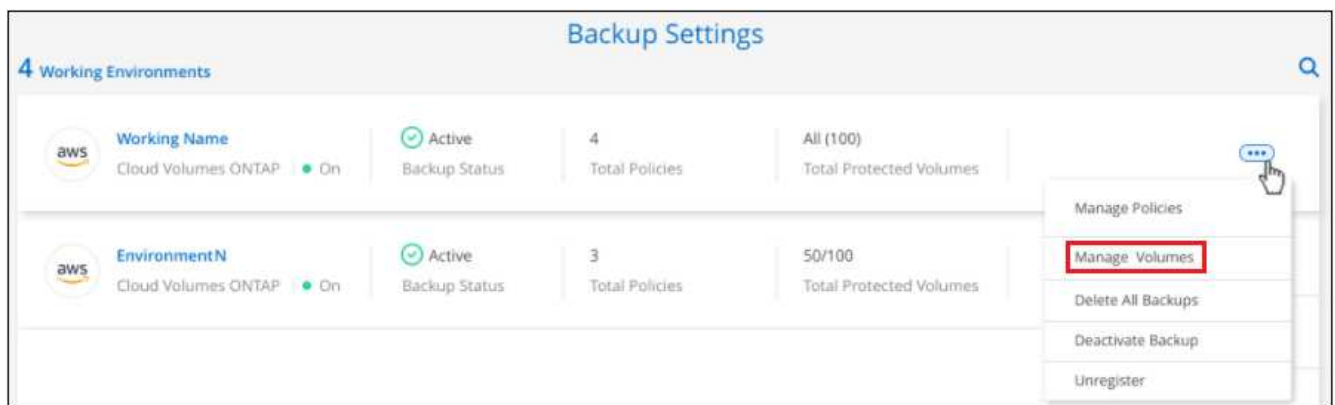
supprimées. Votre fournisseur cloud reste donc facturé pour les coûts de stockage objet correspondant à la capacité que vos sauvegardes utilisent, sauf vous [supprimez les sauvegardes](#).

## Étapes

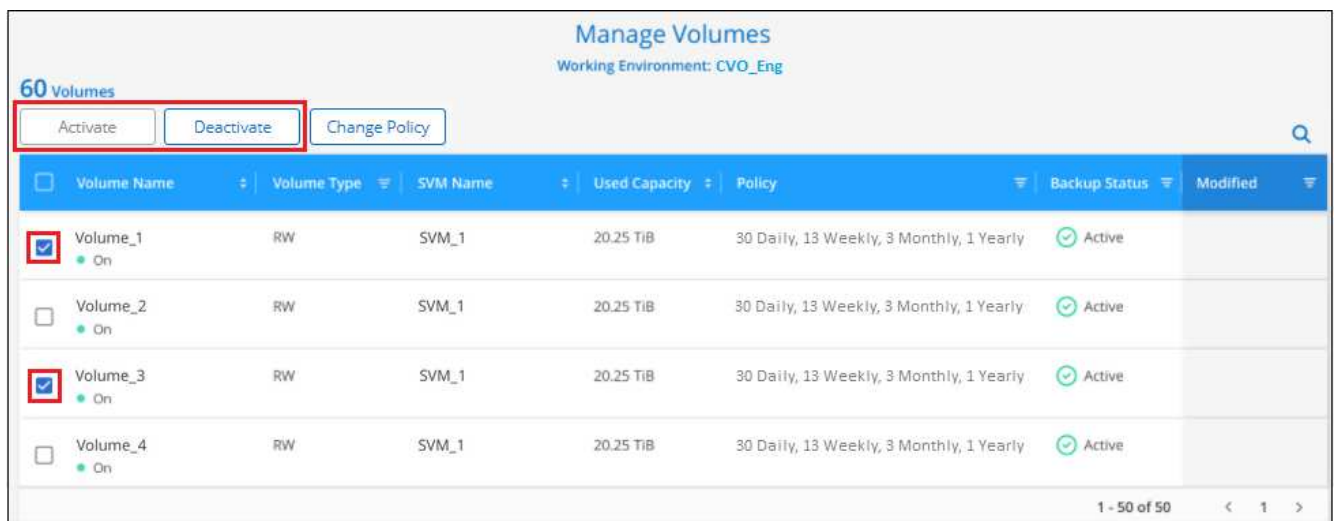
1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail et sélectionnez **gérer les volumes**.



3. Cochez la case d'un volume ou des volumes que vous souhaitez modifier, puis cliquez sur **Activer** ou sur **Désactiver** selon que vous souhaitez démarrer ou arrêter les sauvegardes du volume.



4. Cliquez sur **Enregistrer** pour valider vos modifications.

## Modification d'une stratégie de sauvegarde existante

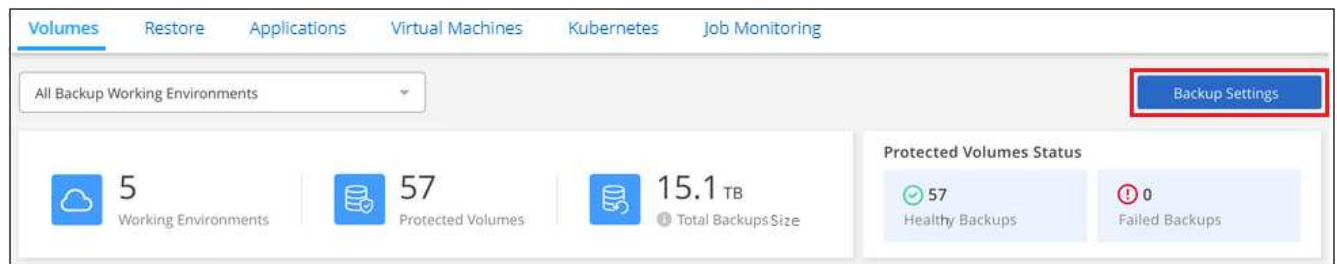
Vous pouvez modifier les attributs d'une stratégie de sauvegarde actuellement appliquée aux volumes d'un environnement de travail. La modification de la stratégie de sauvegarde affecte tous les volumes existants utilisant la règle.



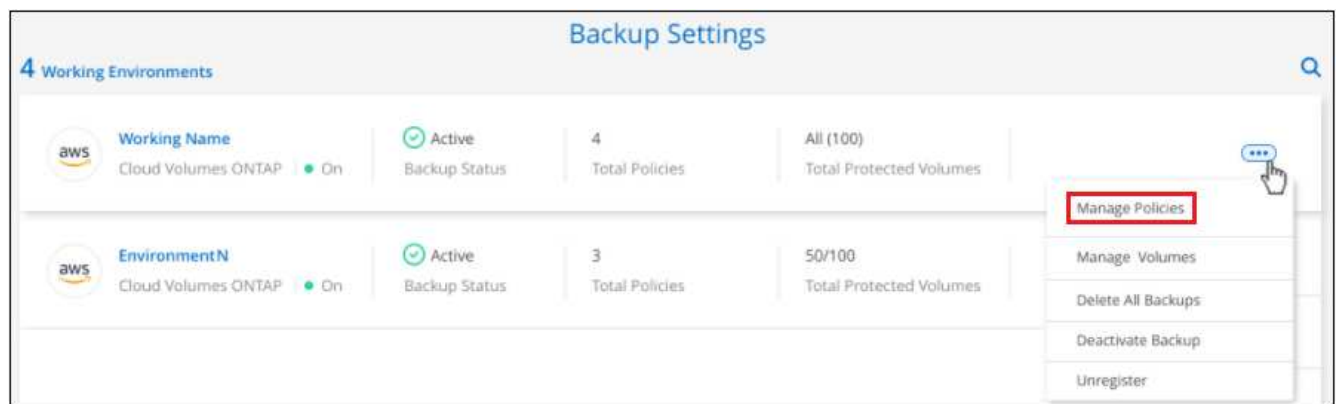
- Si vous avez activé *DataLock et protection contre les attaques par ransomware* dans la stratégie initiale lors de l'activation de Cloud Backup pour ce cluster, toutes les stratégies que vous modifiez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les attaques par ransomware* lors de l'activation de Cloud Backup, vous ne pouvez pas activer DataLock maintenant.
- Lors de la création de sauvegardes sur AWS, si vous choisissez *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de Cloud Backup, ce Tier sera le seul niveau d'archivage disponible lors de l'édition de stratégies de sauvegarde. Si vous avez sélectionné aucun niveau d'archivage dans votre première stratégie de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage lors de la modification d'une stratégie.

### Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur **...** Pour l'environnement de travail dans lequel vous souhaitez modifier les paramètres de la stratégie, sélectionnez **gérer les stratégies**.



3. Dans la page *Manage Policies*, cliquez sur **Edit** pour la stratégie de sauvegarde que vous souhaitez modifier dans cet environnement de travail.

Remarque vous pouvez cliquer sur  pour afficher tous les détails de la police.

Manage Policies


Add New Policy

Working Environment: Cluster Dev Lab

Only Custom policies are editable.


4 Policies

<div>Policy_Number_01</div> <div>Custom Policy</div> <div>Edit</div>	<div>3 Labels: Daily (30), Weekly...</div> <div>Labels &amp; Retention</div>	<div>Active   Archive After 50 Days</div> <div>Archival Policy</div>	<div>50 Out Of 100</div> <div>Associated Volumes</div>
<div>Policy_Number_02</div> <div>Custom Policy</div> <div>Edit</div>	<div>5 Labels: Daily (30), Weekly...</div> <div>Labels &amp; Retention</div>	<div>Not Active</div> <div>Archival Policy</div>	<div>10 Out Of 50</div> <div>Associated Volumes</div>

4. Dans la page *Edit Policy*, cliquez sur  Pour développer la section *Labels & Retention* afin de modifier la planification et/ou la rétention des sauvegardes, puis cliquez sur **Enregistrer**.

Edit Policy

Working Environment: Cluster Dev Lab

Name	Policy_Number_01	
Labels & Retention	30 Daily   2 Weekly   1 Yearly	
DataLock & Ransomware Protection	 None	
Archival Policy	Active   Archive After 50 Days	

Si votre cluster exécute ONTAP 9.10.1 ou version supérieure, vous pouvez également activer ou désactiver le Tiering des sauvegardes dans le stockage d'archivage après un certain nombre de jours.

["En savoir plus sur l'utilisation du stockage d'archives Google"](#). (Nécessite ONTAP 9.12.1.)

Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

Azure

☒ Tier Backups to Archival

Archive after (Days)

Access Tier

Azure Archive

---

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

AWS

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

S3 Glacier
S3 Glacier
S3 Glacier Deep Archive

---

Archival Policy

Backups reside in Google Cloud Standard storage for frequently accessed data. Optionally, you can tier backups to Google Cloud Archive storage for further cost optimization.

Google

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

Google Cloud Archive

+ Notez que tous les fichiers de sauvegarde qui ont été hiérarchisés vers le stockage d'archivage sont conservés dans ce niveau si vous arrêtez le Tiering des sauvegardes vers l'archivage - ils ne sont pas automatiquement déplacés vers le niveau standard. Seules les sauvegardes de volume nouveaux résident dans le niveau standard.

## Ajout d'une nouvelle politique de sauvegarde

Lorsque vous activez Cloud Backup pour un environnement de travail, tous les volumes que vous sélectionnez initialement sont sauvegardés à l'aide de la stratégie de sauvegarde par défaut que vous avez définie. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes ayant des objectifs de point de récupération différents, vous pouvez créer des règles supplémentaires pour ce cluster et les affecter à d'autres volumes.

Si vous souhaitez appliquer une nouvelle stratégie de sauvegarde à certains volumes d'un environnement de travail, vous devez d'abord ajouter la stratégie de sauvegarde à l'environnement de travail. C'est alors possible [appliquer la policy aux volumes de cet environnement de travail](#).

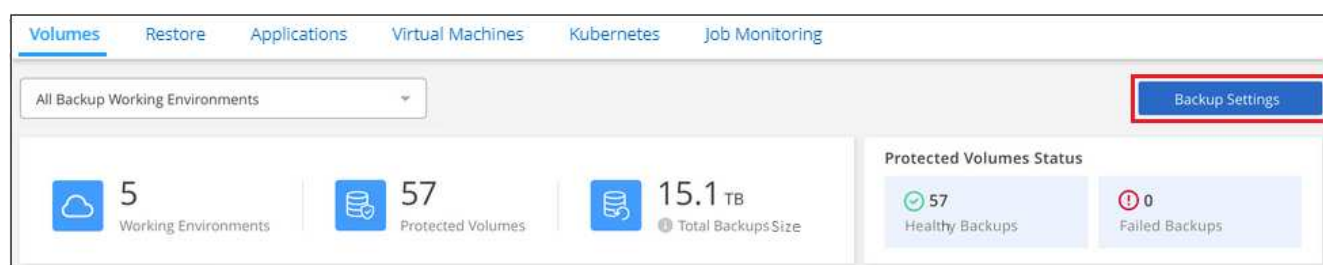




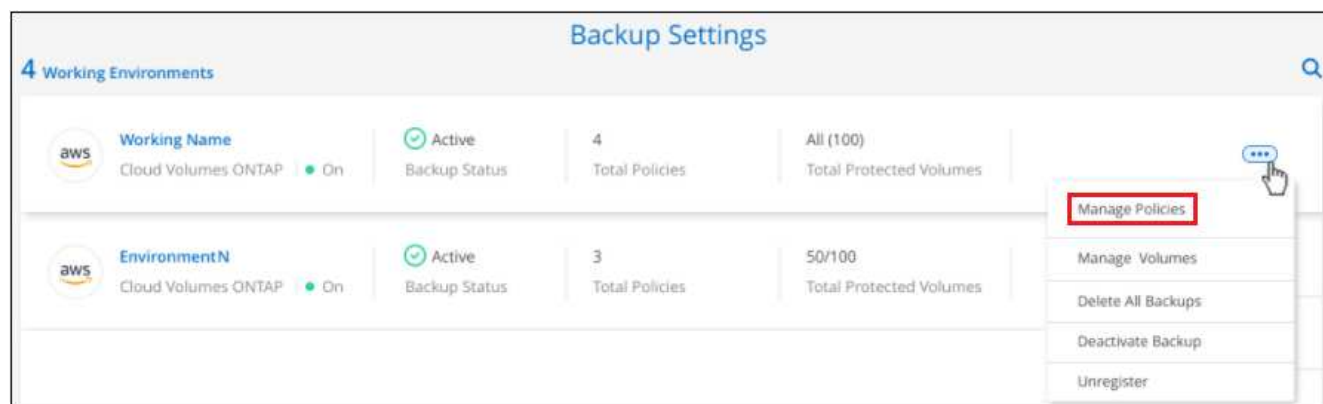
- Si vous avez activé *DataLock et protection contre les attaques par ransomware* dans la stratégie initiale lors de l'activation de Cloud Backup pour ce cluster, toutes les stratégies supplémentaires que vous créez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les attaques par ransomware* lors de l'activation de Cloud Backup, vous ne pouvez pas créer de nouvelles stratégies qui utilisent DataLock.
- Lors de la création de sauvegardes sur AWS, si vous choisissez *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de Cloud Backup, ce Tier sera le seul niveau d'archivage disponible pour les futures stratégies de sauvegarde pour ce cluster. Si vous avez sélectionné aucun niveau d'archivage dans votre première stratégie de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage pour les stratégies futures.

## Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail où vous souhaitez ajouter la nouvelle stratégie, sélectionnez **gérer les stratégies**.



3. Dans la page *Manage Policies*, cliquez sur **Add New Policy**.



Manage Policies

Working Environment: Cluster Dev Lab

Only Custom policies are editable.

Add New Policy

4 Policies

Policy\_Number\_01

Custom Policy

Edit

3 Labels: Daily (30), Weekly...

Labels & Retention

Active | Archive After 50 Days

Archival Policy

50 Out Of 100

Associated Volumes

Policy\_Number\_02

Custom Policy

Edit

5 Labels: Daily (30), Weekly...


Labels & Retention

Not Active

Archival Policy

10 Out Of 50

Associated Volumes

4. Dans la page *Ajouter une nouvelle stratégie*, cliquez sur  Pour développer la section *Labels & Retention* afin de définir la planification et la conservation des sauvegardes, puis cliquez sur **Enregistrer**.

Add New Policy

Working Environment: Working Environment 1

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼
Archival Policy	Disabled	▼

Si votre cluster exécute ONTAP 9.10.1 ou version supérieure, vous pouvez également activer ou désactiver le Tiering des sauvegardes dans le stockage d'archivage après un certain nombre de jours.

"[En savoir plus sur l'utilisation du stockage d'archives Google](#)". (Nécessite ONTAP 9.12.1.)

Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

Azure

☒ Tier Backups to Archival

Archive after (Days)

Access Tier  

Azure Archive

---

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

AWS

☒ Tier Backups to Archival

Archive after (Days)

Storage Class  

S3 Glacier

S3 Glacier

S3 Glacier Deep Archive

---

Archival Policy

Backups reside in Google Cloud Standard storage for frequently accessed data. Optionally, you can tier backups to Google Cloud Archive storage for further cost optimization.

Google

☒ Tier Backups to Archival

Archive after (Days)

Storage Class  

Google Cloud Archive

## Modification de la règle attribuée aux volumes existants

Vous pouvez modifier la stratégie de sauvegarde attribuée à vos volumes existants si vous souhaitez modifier la fréquence des sauvegardes ou si vous souhaitez modifier la valeur de rétention.

Notez que la règle que vous souhaitez appliquer aux volumes doit déjà exister. [Découvrez comment ajouter une nouvelle stratégie de sauvegarde pour un environnement de travail.](#)

### Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.

Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

All Backup Working Environments

Backup Settings

5

Working Environments

57

Protected Volumes

15.1 TB

Total Backups Size

Protected Volumes Status

57

Healthy Backups

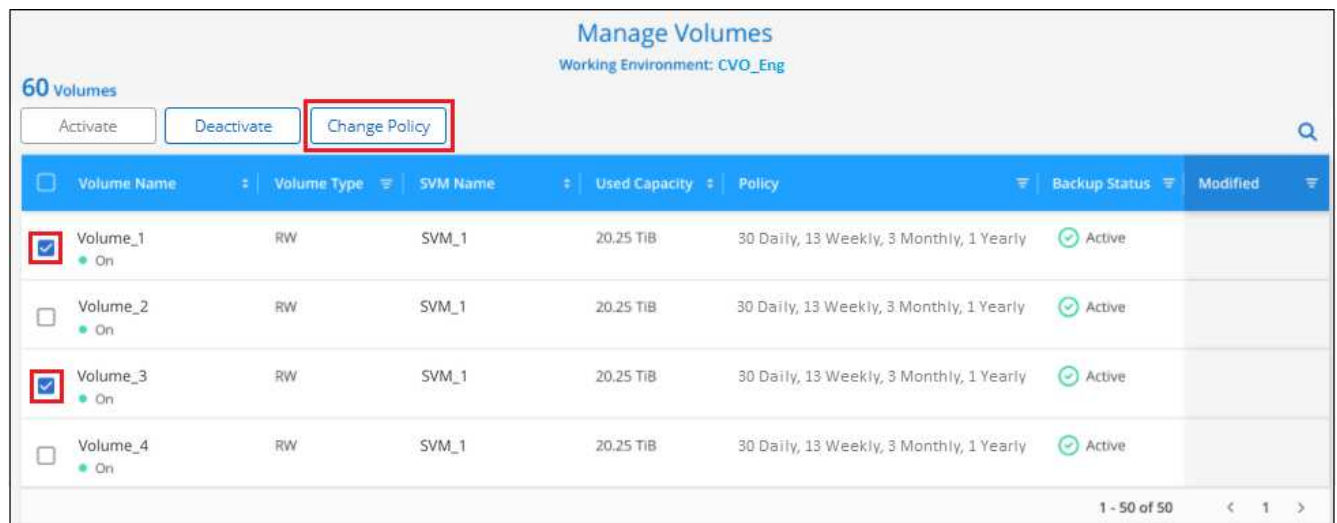
0

Failed Backups

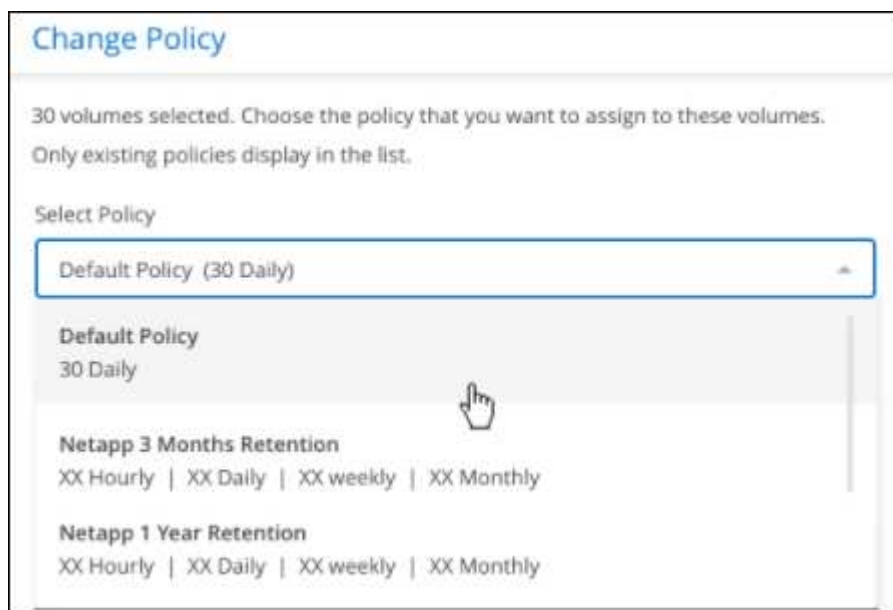
2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail où existent les volumes, sélectionnez **gérer les volumes**.



3. Cochez la case pour un volume ou des volumes pour lesquels vous souhaitez modifier la règle, puis cliquez sur **Modifier la stratégie**.



4. Dans la page *change Policy*, sélectionnez la stratégie à appliquer aux volumes, puis cliquez sur **change Policy**.





Si vous avez activé *DataLock et protection contre les attaques par ransomware* dans la stratégie initiale lors de l'activation de Cloud Backup pour ce cluster, vous ne verrez que les autres stratégies qui ont été configurées avec DataLock. Et si vous n'avez pas activé *DataLock et protection contre les attaques par ransomware* lors de l'activation de Cloud Backup, vous ne verrez que d'autres stratégies qui n'ont pas configuré DataLock.

5. Cliquez sur **Enregistrer** pour valider vos modifications.

## Création d'une sauvegarde de volume manuelle à tout moment

Vous pouvez créer une sauvegarde à la demande à tout moment pour capturer l'état actuel du volume. Cela peut être utile si des modifications importantes ont été apportées à un volume et que vous ne souhaitez pas attendre la prochaine sauvegarde planifiée pour protéger ces données, ou si le volume n'est pas actuellement sauvegardé et que vous voulez capturer son état actuel.

Le nom de la sauvegarde inclut l'horodatage afin que vous puissiez identifier votre sauvegarde à la demande à partir d'autres sauvegardes planifiées.

Si vous avez activé *DataLock et protection contre les attaques par ransomware* lors de l'activation de Cloud Backup pour ce cluster, la sauvegarde à la demande sera également configurée avec DataLock, et la période de conservation sera de 30 jours. Les analyses par ransomware ne sont pas prises en charge pour les sauvegardes ad hoc. ["En savoir plus sur le verrouillage des données et la protection contre les attaques par ransomware"](#).

Notez que lors de la création d'une sauvegarde ad hoc, un Snapshot est créé sur le volume source. Cet instantané ne faisant pas partie d'une planification Snapshot normale, il ne sera pas désactivé. Vous pouvez supprimer manuellement cet instantané du volume source une fois la sauvegarde terminée. Ainsi, les blocs liés à cette copie Snapshot peuvent être libérés. Le nom de l'instantané commence par `cbs-snapshot-adhoc-`. ["Reportez-vous à la section mode de suppression d'une copie Snapshot à l'aide ONTAP de l'interface de ligne de commandes de"](#).



La sauvegarde de volumes à la demande n'est pas prise en charge sur les volumes de protection des données.

### Étapes

1. Dans l'onglet **volumes**, cliquez sur **...** Pour le volume et sélectionnez **Sauvegarder maintenant**.

The screenshot shows the Veeam Backup & Replication console. The top navigation bar includes 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below the navigation bar, there's a summary section with 'All Backup Working Environments' (1), 'Protected Volumes' (57), and 'Total Backup Capacity' (15.1 TB). A 'Protected Volumes Status' box shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. The main section displays '2,011 Backed Up Volumes'. A table lists three volumes: Volume 1, Volume 2, and Volume 3. Each row shows source volume status, source working environment, source SVM, ransomware protection, backup status, and last backup date. A context menu is open for Volume 2, showing options: 'Details & Backup List', 'Backup Now' (highlighted with a red box), and 'Pause Backups'.

La colonne État de la sauvegarde de ce volume affiche « en cours » jusqu'à ce que la sauvegarde soit créée.

## Affichage de la liste des sauvegardes pour chaque volume

Vous pouvez afficher la liste de tous les fichiers de sauvegarde existants pour chaque volume. Cette page affiche des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde, tels que la dernière sauvegarde effectuée, la stratégie de sauvegarde actuelle, la taille du fichier de sauvegarde, etc.

Cette page permet également d'effectuer les tâches suivantes :

- Supprimez tous les fichiers de sauvegarde du volume
- Supprimez les fichiers de sauvegarde individuels du volume
- Téléchargez un rapport de sauvegarde pour le volume

### Étapes

1. Dans l'onglet **volumes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

Navigation: Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

All Backup Working Environments

Backup Settings

1 Working Environments | 57 Protected Volumes | 15.1 TB Total Backup Capacity

Protected Volumes Status: 57 Healthy Backup Volumes | 0 Failed Backup Volumes

2,011 Backed Up Volumes

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup
Volume 1 On	Working Environment 1 On	Source SVM 1	None	Active	June 12, 2022
Volume 2 On	Working Environment 1 On	Source SVM 2	Governance	Active	
Volume 3 On	Working Environment 1 On	Source SVM 1	Compliance	Active	

Actions for Volume 1: Details & Backup List, Backup Now, Pause Backups

La liste de tous les fichiers de sauvegarde s'affiche avec des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde.

**Source**

Volume: Volume Name

Working Environment: Working Environment N...

Type: Cloud Volumes ONTAP (HA)

Provider: AWS

SVM: SVM Name

**Destination**

Cloud Provider: AWS

Bucket: Backup Bucket Name

Region: US East (N.Virginia)

Account ID: 01234567890123456789

**Backup Information**

Relationship Status: Active

Last Backup: Oct 26 2022, 8:27:34 pm

Lag Duration: 1 day ago

Backups: 125

Policy Name: My\_First\_Policy

125 Backups

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	Protected	Standard

## Exécution d'une analyse par ransomware sur une sauvegarde de volume

Le logiciel de protection par ransomware de NetApp analyse vos fichiers de sauvegarde pour détecter la preuve d'une attaque par ransomware lors de la création d'un fichier de sauvegarde, et lorsque les données d'un fichier de sauvegarde sont en cours de restauration. Vous pouvez également exécuter une analyse de protection par ransomware à la demande à tout moment pour vérifier la facilité d'utilisation d'un fichier de sauvegarde spécifique. Ceci peut être utile si vous avez eu un problème de ransomware sur un volume en particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

Cette fonctionnalité est disponible uniquement si la sauvegarde du volume a été créée à partir d'un système

avec ONTAP 9.11.1 ou version ultérieure et si vous avez activé *DataLock et protection contre les attaques par ransomware* dans la stratégie de sauvegarde.

## Étapes

1. Dans l'onglet **volumes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

The screenshot shows the 'Volumes' tab in the backup management interface. At the top, there are tabs for 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below these, there's a dropdown for 'All Backup Working Environments' and a 'Backup Settings' button. A summary section shows '1 Working Environments', '57 Protected Volumes', and '15.1 TB Total Backup Capacity'. A 'Protected Volumes Status' box indicates '57 Healthy Backup Volumes' and '0 Failed Backup Volumes'. Below this, it says '2,011 Backed Up Volumes'. A table lists three volumes with columns: Source Volume, Source Working Environment, Source SVM, Ransomware Protection, Backup Status, and Last Backup. A three-dot menu is open for Volume 3, showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

La liste de tous les fichiers de sauvegarde s'affiche.

2. Cliquez sur ... Pour le fichier de sauvegarde de volume à analyser, cliquez sur **analyse de ransomware**.

The screenshot shows the 'Backups' page with a search bar and a 'Select Timeframe' dropdown. A table lists 125 backups with columns: Backup Name, Date, Size, Ransomware Scan, and Storage Class. The 'Ransomware Scan' column shows various statuses: 'Potential Ransomware identified', 'Protected', 'In Progress', and 'Failed'. A three-dot menu is open for the first backup, showing options: 'Delete', 'Restore', and 'Ransomware Scan' (highlighted with a red box).

La colonne analyse des attaques par ransomware indique que l'analyse est en cours.

## Suppression de sauvegardes

Cloud Backup vous permet de supprimer un seul fichier de sauvegarde, de supprimer toutes les sauvegardes d'un volume ou de supprimer toutes les sauvegardes de tous les volumes d'un environnement de travail. Vous pouvez supprimer toutes les sauvegardes si vous n'avez plus besoin des sauvegardes, ou si vous avez supprimé le volume source et que vous souhaitez supprimer toutes les sauvegardes.

Notez que vous ne pouvez pas supprimer les fichiers de sauvegarde que vous avez verrouillés à l'aide de DataLock et de la protection contre les attaques par ransomware. L'option « Supprimer » n'est pas disponible



dans l'interface utilisateur si vous avez sélectionné un ou plusieurs fichiers de sauvegarde verrouillés.



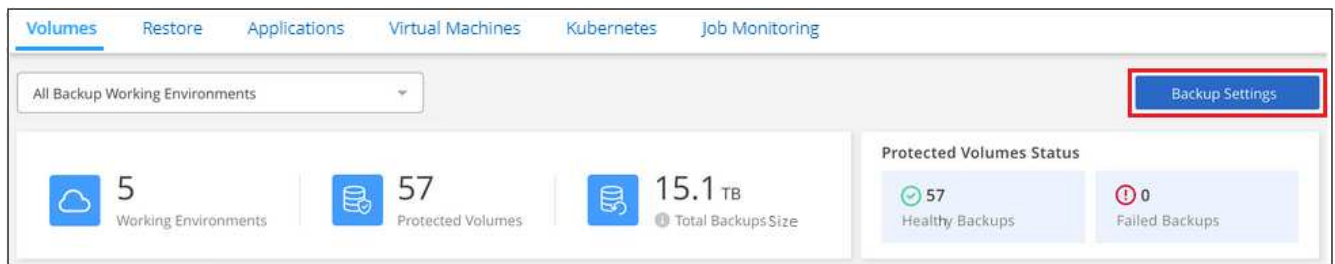
Si vous prévoyez de supprimer un environnement ou un cluster de travail qui dispose de sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. Cloud Backup ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système et l'interface utilisateur ne prend pas en charge la suppression des sauvegardes après la suppression du système. Vous continuerez d'être facturé pour les coûts de stockage objet pour les sauvegardes restantes.

## Suppression de tous les fichiers de sauvegarde d'un environnement de travail

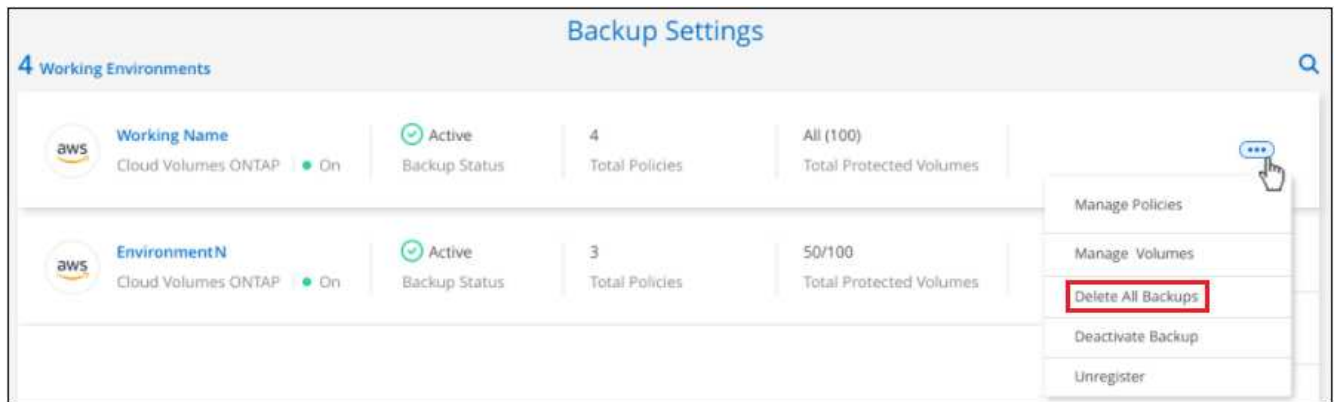
La suppression de toutes les sauvegardes d'un environnement de travail ne désactive pas les futures sauvegardes des volumes de cet environnement de travail. Si vous souhaitez arrêter la création de sauvegardes de tous les volumes d'un environnement de travail, vous pouvez désactiver les sauvegardes [comme décrit ici](#).

### Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Cliquez sur ... Pour l'environnement de travail où vous souhaitez supprimer toutes les sauvegardes et sélectionnez **Supprimer toutes les sauvegardes**.



3. Dans la boîte de dialogue de confirmation, entrez le nom de l'environnement de travail et cliquez sur **Supprimer**.

## Suppression de tous les fichiers de sauvegarde d'un volume

La suppression de toutes les sauvegardes d'un volume désactive également les futures sauvegardes de ce volume.

C'est possible [relancez les sauvegardes pour le volume](#) À tout moment à partir de la page gérer les sauvegardes.



## Étapes

1. Dans l'onglet **volumes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

The screenshot shows the 'Volumes' tab in the backup management interface. At the top, there are navigation tabs: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below these, there's a dropdown menu for 'All Backup Working Environments' and a 'Backup Settings' button. A summary section displays '1 Working Environments', '57 Protected Volumes', and '15.1 TB Total Backup Capacity'. A 'Protected Volumes Status' box shows '57 Healthy Backup Volumes' and '0 Failed Backup Volumes'. Below this, it says '2,011 Backed Up Volumes'. A table lists the backed up volumes with columns: Source Volume, Source Working Environment, Source SVM, Ransomware Protection, Backup Status, and Last Backup. Three volumes are listed: Volume 1, Volume 2, and Volume 3. A dropdown menu is open for 'Volume 1', showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

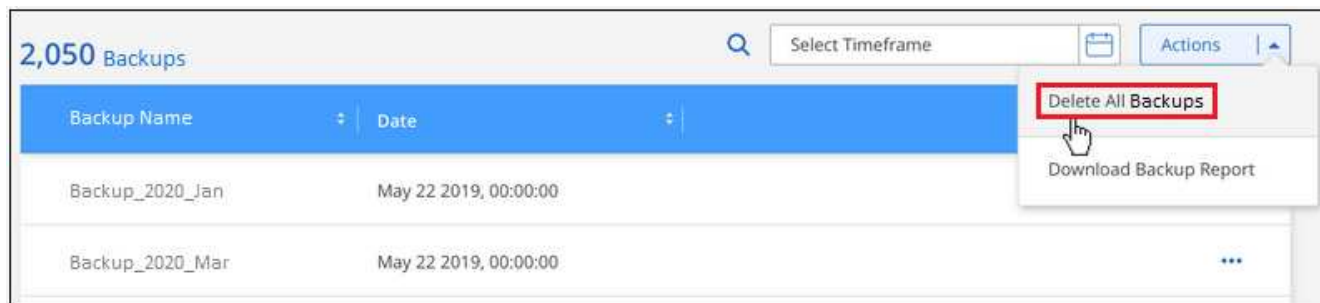
Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup
Volume 1 ● On	aws Working Environment 1 ● On	Source SVM 1	None	● Active	June 12 2022
Volume 2 ● On	aws Working Environment 1 ● On	Source SVM 2	i Governance	● Active	
Volume 3 ● On	aws Working Environment 1 ● On	Source SVM 1	⚠ Compliance	● Active	

La liste de tous les fichiers de sauvegarde s'affiche.

The screenshot shows the 'Backup Information' page. It is divided into three main sections: Source, Destination, and Backup Information. The Source section lists: Volume (● Volume Name), Working Environment (● Working Environment N...), Type (Cloud Volumes ONTAP (HA)), Provider (AWS), and SVM (SVM Name). The Destination section lists: Cloud Provider (AWS), Bucket (Backup Bucket Name), Region (US East (N.Virginia)), and Account ID (01234567890123456789). The Backup Information section lists: Relationship Status (● Active), Last Backup (Oct 26 2022, 8:27:34 pm), Lag Duration (1 day ago), Backups (125), and Policy Name (My\_First\_Policy). Below these sections, it says '125 Backups'. A table lists the backups with columns: Backup Name, Date, Size, Ransomware Scan, and Storage Class. Three backups are listed: Backup 1, Backup 2, and Backup 3. A dropdown menu is open for 'Backup 2', showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	● Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	⚠ Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	● Protected	Standard

2. Cliquez sur **actions** > **Supprimer toutes les sauvegardes**.



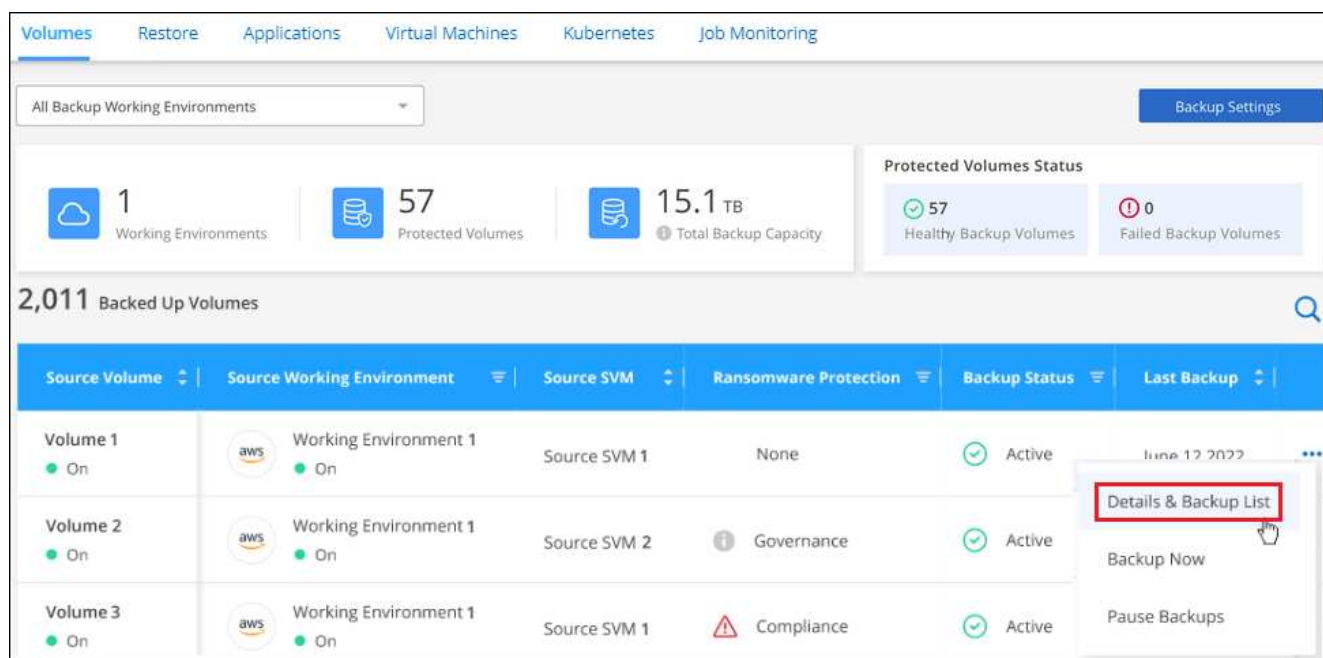
3. Dans la boîte de dialogue de confirmation, entrez le nom du volume et cliquez sur **Supprimer**.

## Suppression d'un fichier de sauvegarde unique pour un volume

Vous pouvez supprimer un seul fichier de sauvegarde. Cette fonctionnalité n'est disponible que si la sauvegarde du volume a été créée à partir d'un système avec ONTAP 9.8 ou version ultérieure.

### Étapes

1. Dans l'onglet **volumes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.



La liste de tous les fichiers de sauvegarde s'affiche.

Source

Volume

Volume Name

Working Environment

Working Environment N...

Type

Cloud Volumes ONTAP (HA)

Provider

AWS

SVM

SVM Name

Destination

Cloud Provider

AWS

Bucket

Backup Bucket Name

Region

US East (N.Virginia)

Account ID

01234567890123456789

Backup Information

Relationship Status

Active

Last Backup

Oct 26 2022, 8:27:34 pm

Lag Duration

1 day ago

Backups

125

Policy Name

My\_First\_Policy

125 Backups

Select Timeframe

Actions

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	Protected	Standard

2. Cliquez sur **...** Pour le fichier de sauvegarde de volume que vous souhaitez supprimer, cliquez sur **Supprimer**.

125 Backups

Select Timeframe

Actions

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 00:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 2	June 12 2022, 00:00:00	2.5 GiB	Protected	Standard
Backup 12	June 12 2022, 00:00:00	20 GiB	Protected	Standard
Backup 20	June 12 2022, 00:00:00	125 GiB	Failed	Standard

Delete

Restore

Ransomware Scan

3. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

## Suppression des relations de sauvegarde de volume

La suppression de la relation de sauvegarde d'un volume vous fournit un mécanisme d'archivage si vous souhaitez arrêter la création de nouveaux fichiers de sauvegarde et supprimer le volume source, mais conserver tous les fichiers de sauvegarde existants. Cela vous permet de restaurer ultérieurement le volume à partir du fichier de sauvegarde, si nécessaire, tout en libérant de l'espace du système de stockage source.

Vous n'avez pas nécessairement besoin de supprimer le volume source. Vous pouvez supprimer la relation de sauvegarde d'un volume et conserver le volume source. Dans ce cas, vous pouvez activer la sauvegarde sur le volume ultérieurement. La copie de sauvegarde de base d'origine continue d'être utilisée dans ce cas. Une nouvelle copie de sauvegarde de base n'est pas créée et exportée vers le cloud. Notez que si vous réactivez une relation de sauvegarde, la stratégie de sauvegarde par défaut est attribuée au volume.

Cette fonction n'est disponible que si votre système exécute ONTAP 9.12.1 ou une version ultérieure.

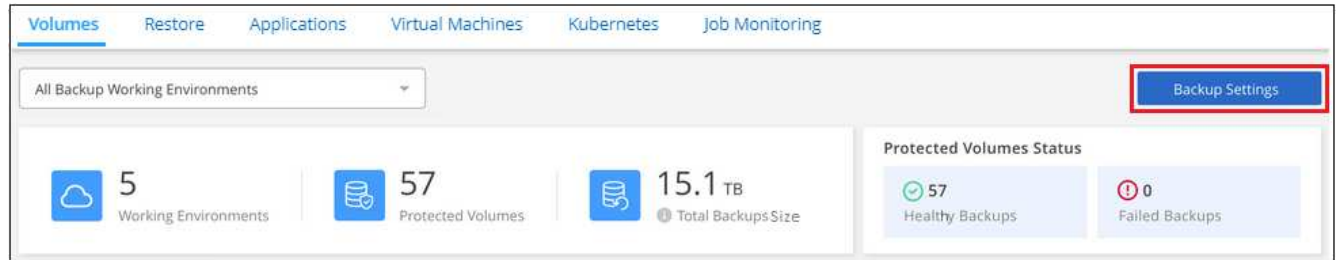
Vous ne pouvez pas supprimer le volume source de l'interface utilisateur de Cloud Backup. Cependant, vous pouvez ouvrir la page Détails du volume sur la toile, et ["supprimez le volume de ce site"](#).



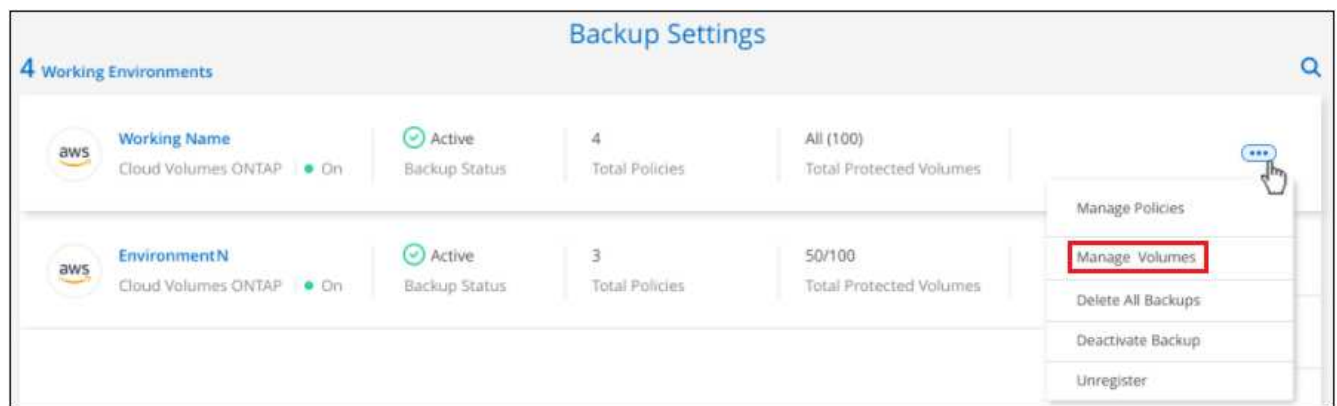
Une fois la relation supprimée, vous ne pouvez pas supprimer des fichiers de sauvegarde de volume individuels. Vous pouvez cependant "[supprimez toutes les sauvegardes du volume](#)" si vous souhaitez supprimer tous les fichiers de sauvegarde.

## Étapes

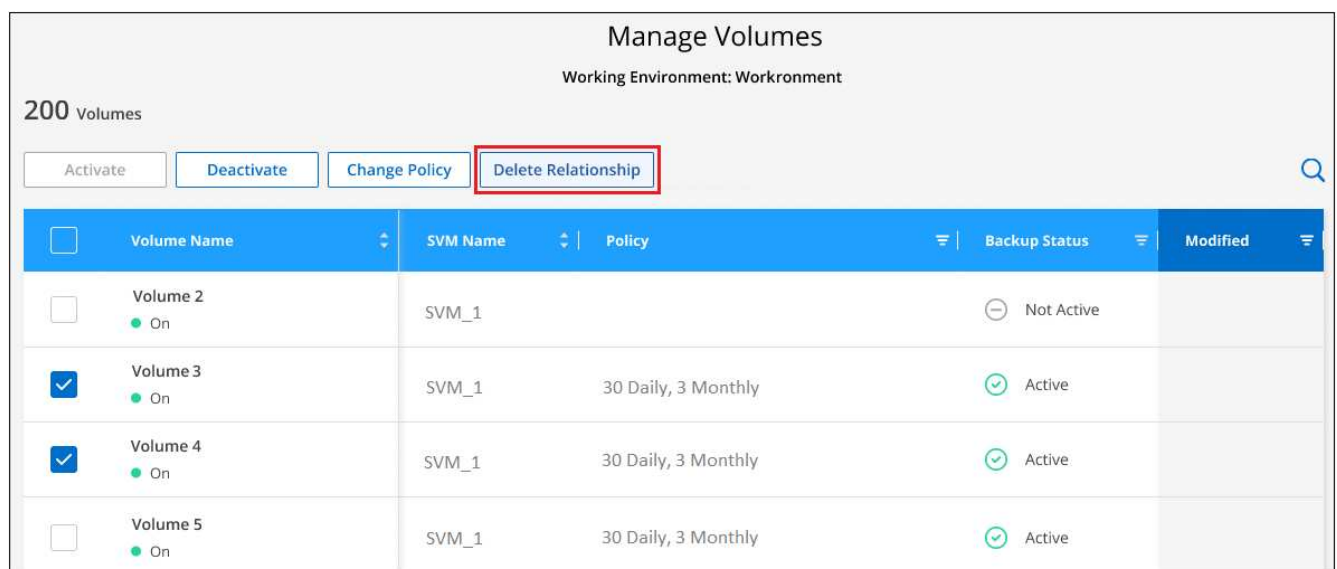
1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail et sélectionnez **gérer les volumes**.



3. Cochez la case d'un volume ou de volumes que vous souhaitez supprimer la relation de sauvegarde, puis cliquez sur **Supprimer la relation**.



4. Cliquez sur **Enregistrer** pour valider vos modifications.

Vous pouvez également supprimer la relation de sauvegarde d'un volume unique sur la page volumes.

2,011 Backed Up Volumes

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	
Volume 1 On	aws Working Env On	SVM-1	Compliance	Active	⋮
Vol 3 On	aws Working Env On	SVM-1		Active	
Volume 2 On	aws Working Env On	SVM-1	Compliance	Active	

Details & Backup List

Backup Now

Pause Backups

Delete Relationship

Lorsque vous affichez la liste des sauvegardes pour chaque volume, vous verrez l'« état de la relation » répertorié comme **relation supprimée**.

Source

Volume  
Working Environment  
Type  
Provider  
SVM

Volume Name  
Working Environment N...  
Cloud Volumes ONTAP (HA)  
AWS  
SVM Name

Destination

Cloud Provider  
Bucket  
Region  
Account ID

AWS  
Backup Bucket Name  
US East (N.Virginia)  
01234567890123456789

Backup Information

Relationship Status  
Last Backup  
Lag Duration  
Backups  
Policy Name

Relationship Deleted  
Oct 26 2022, 8:27:34 pm  
  
125  
My\_First\_Policy

125 Backups

Backup Name	Date	Size	Ransomware Scan	Storage Class	
Backup 1	June 12 2022, 12:00:00	20.12 GiB	None	Standard	⋮
Backup 2	June 12 2022, 13:00:00	20.125 GiB	None	Standard	⋮
Backup 3	June 12 2022, 14:00:00	20.12 GiB	None	Standard	⋮

Désactivation de Cloud Backup pour un environnement de travail

La désactivation de Cloud Backup pour un environnement de travail désactive les sauvegardes de chaque volume du système et désactive également la restauration d'un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne désinscrit pas le service de sauvegarde de cet environnement de travail, car il vous permet de suspendre l'ensemble de l'activité de sauvegarde et de restauration pendant une période donnée.

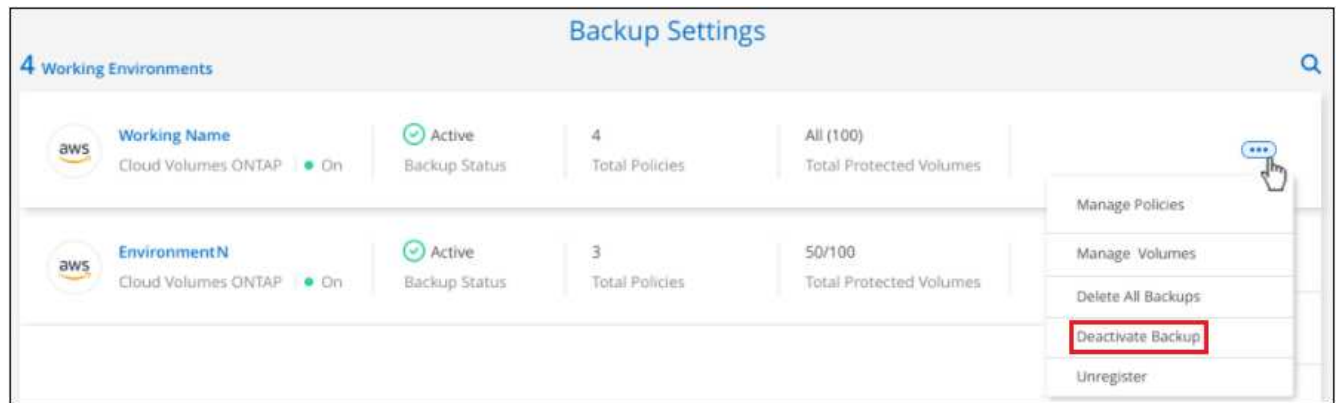
Notez que vous continuerez d'être facturé par votre fournisseur cloud pour les coûts de stockage objet correspondant à la capacité que vos sauvegardes utilisent, sauf si vous [supprimez les sauvegardes](#).

Étapes

- 1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail dans lequel vous souhaitez désactiver les sauvegardes et sélectionnez **Désactiver la sauvegarde**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Désactiver**.



Un bouton **Activer la sauvegarde** apparaît pour cet environnement de travail alors que la sauvegarde est désactivée. Vous pouvez cliquer sur ce bouton lorsque vous souhaitez réactiver la fonctionnalité de sauvegarde pour cet environnement de travail.

## Annulation de l'enregistrement de Cloud Backup pour un environnement de travail

Vous pouvez annuler l'enregistrement de Cloud Backup pour un environnement de travail si vous ne souhaitez plus utiliser la fonctionnalité de sauvegarde et que vous souhaitez interrompre la facturation des sauvegardes dans cet environnement de travail. Cette fonction est généralement utilisée lorsque vous prévoyez de supprimer un environnement de travail et que vous souhaitez annuler le service de sauvegarde.

Vous pouvez également utiliser cette fonction si vous souhaitez modifier le magasin d'objets de destination dans lequel vos sauvegardes de cluster sont stockées. Une fois que vous désenregistrez Cloud Backup pour l'environnement de travail, vous pouvez activer Cloud Backup pour ce cluster en utilisant les informations du nouveau fournisseur cloud.

Avant de pouvoir annuler l'enregistrement de Cloud Backup, vous devez effectuer les opérations suivantes dans cet ordre :

- Désactivez Cloud Backup pour l'environnement de travail
- Supprimer toutes les sauvegardes de cet environnement de travail

L'option de désenregistrer n'est pas disponible tant que ces deux actions ne sont pas terminées.

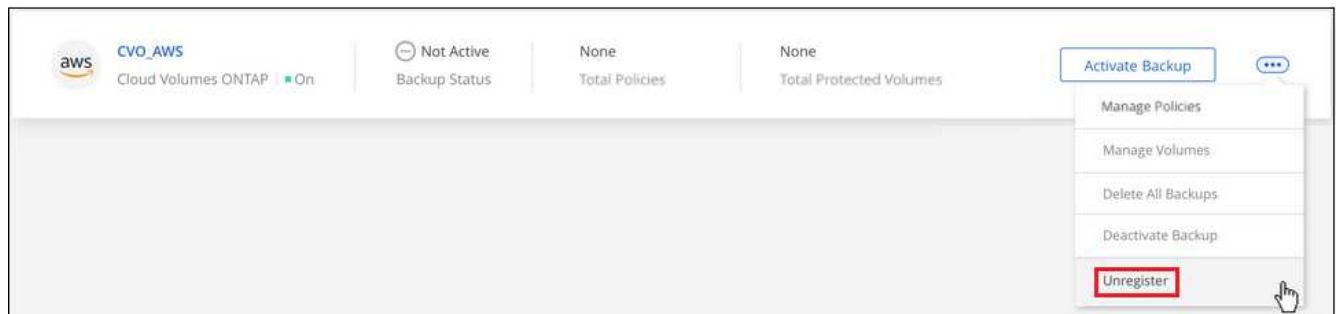
### Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.





2. Dans la page *Backup Settings*, cliquez sur **...** Pour l'environnement de travail où vous souhaitez annuler l'enregistrement du service de sauvegarde et sélectionnez **Annuler l'enregistrement**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Annuler l'enregistrement**.

## Gestion des paramètres de sauvegarde au niveau du cluster

Vous pouvez modifier de nombreux paramètres de sauvegarde au niveau du cluster que vous définissez lors de l'activation de Cloud Backup pour chaque système ONTAP. Vous pouvez également modifier certains paramètres appliqués comme paramètres de sauvegarde par défaut. Cela vous permet notamment de modifier les clés de stockage, le taux de transfert des sauvegardes vers le stockage objet ou non, l'exportation des copies Snapshot historiques sous forme de fichiers de sauvegarde, etc.

Les paramètres de sauvegarde au niveau du cluster sont disponibles dans la page *Advanced Settings*.

L'ensemble des paramètres de sauvegarde que vous pouvez modifier comprend :

- Modification des clés de stockage qui donnent à votre système ONTAP l'autorisation d'accéder au stockage objet
- Modification de l'IPspace ONTAP connecté au stockage objet
- Modification de la bande passante réseau allouée pour charger les sauvegardes dans le stockage objet
- Modification du paramètre (et de la règle) de sauvegarde automatique pour les volumes futurs
- Modification de l'inclusion ou non de copies Snapshot historiques dans vos fichiers de sauvegarde de base initiaux pour les volumes futurs
- Modification de la suppression des snapshots « annuels » du système source

### Afficher les paramètres de sauvegarde au niveau du cluster

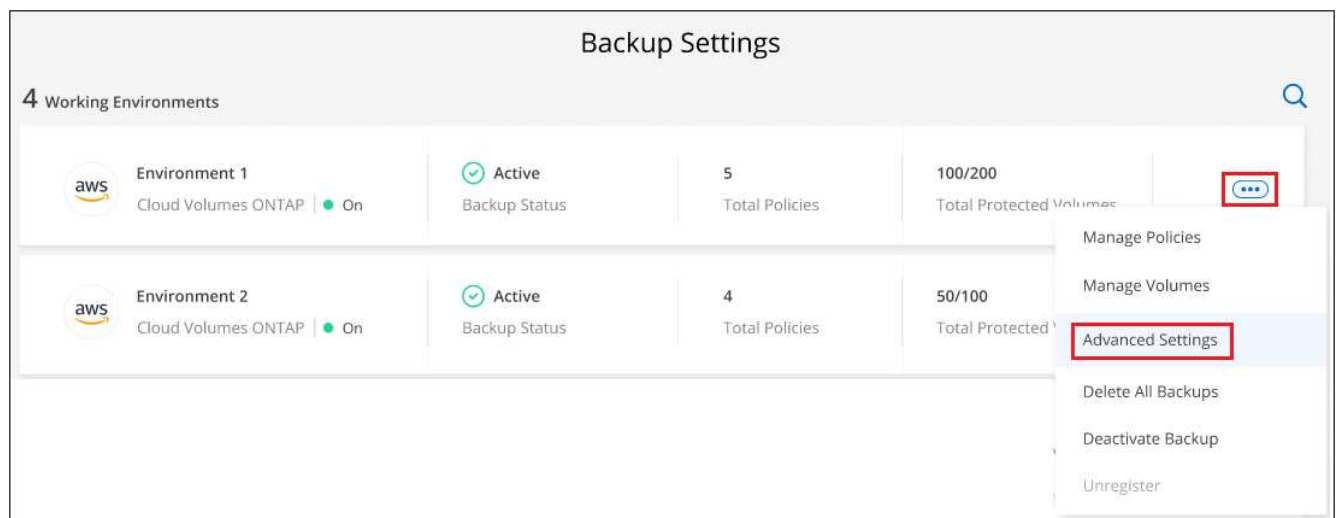
Vous pouvez afficher les paramètres de sauvegarde au niveau du cluster pour chaque environnement de travail.

## Étapes

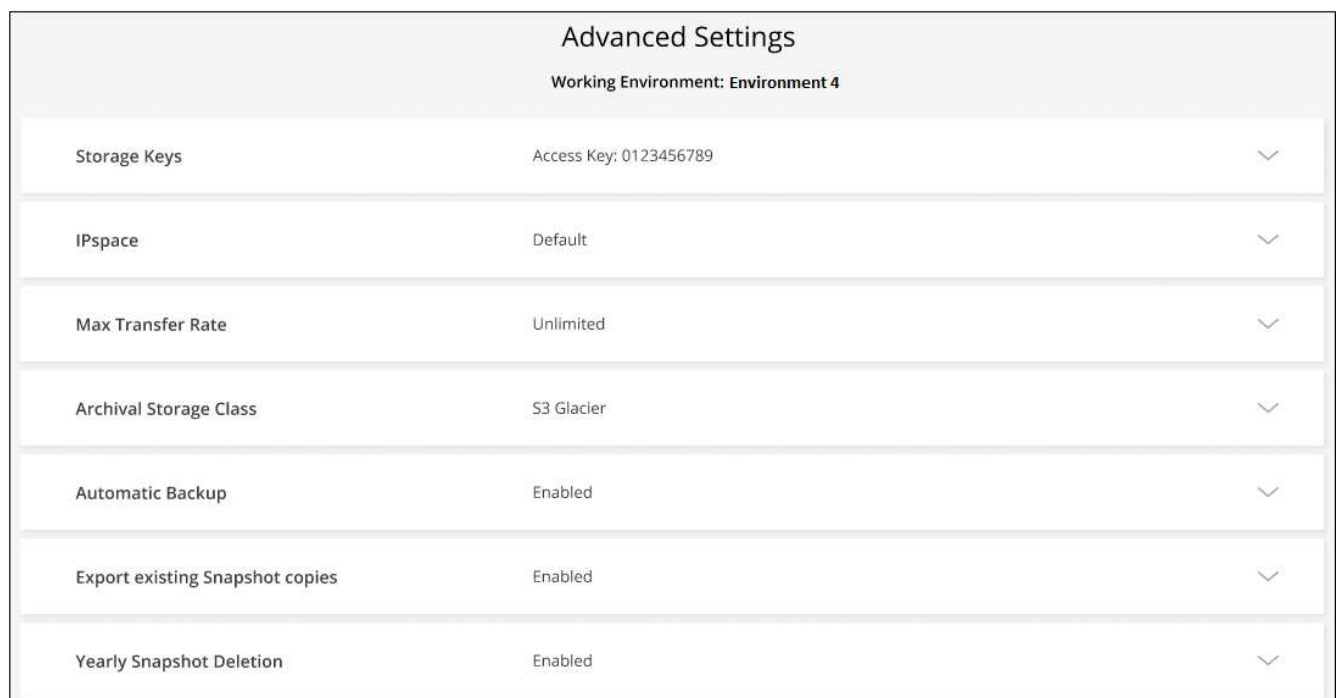
1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



3. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail et sélectionnez **Paramètres avancés**.



La page *Paramètres avancés* affiche les paramètres actuels de cet environnement de travail.





Si vous devez apporter des modifications, développez simplement l'option et apportez les modifications nécessaires. Toutes les opérations de sauvegarde après la modification utiliseront les nouvelles valeurs.

Certaines options ne sont plus disponibles en fonction de la version de ONTAP sur le cluster source et en fonction du fournisseur cloud où résident les sauvegardes.

## Changer les clés de stockage pour que ONTAP puisse accéder au stockage cloud

Si vous devez appliquer une politique d'entreprise régulièrement la rotation de toutes les références, par exemple tous les 6 mois ou un an, il s'agit de la façon dont vous synchroniserez la clé d'accès et la clé secrète de votre fournisseur cloud avec votre système ONTAP. Ainsi, vous pouvez mettre à jour vos identifiants du fournisseur cloud, puis modifier les clés de votre système ONTAP de sorte que les deux systèmes continuent de communiquer.

Cette option n'est disponible que pour les systèmes ONTAP sur site et uniquement pour les sauvegardes vers Amazon S3, Google Cloud Storage et StorageGRID.

<b>Storage Keys</b>		Access Key: 0123456789
Access Key	Secret Key	
<input type="text" value="1111111111"/>	<input type="text" value="*****"/>	
<a href="#">Apply</a>	<a href="#">Cancel</a>	

Il vous suffit d'entrer la nouvelle clé d'accès et la clé secrète, puis de cliquer sur **appliquer**.

## Modifiez l'IPspace ONTAP connecté au stockage objet

Vous pouvez modifier l'IPspace ONTAP connecté au stockage objet. Cette option est disponible uniquement lors de la sauvegarde des données depuis les systèmes ONTAP sur site ; elle n'est pas disponible pour les systèmes Cloud Volumes ONTAP.

Ne doit pas être utilisé sur un système qui sauvegarde activement les données de volume dans le stockage objet. Il ne doit être utilisé que si un IPspace a été sélectionné lors de l'activation initiale de la sauvegarde sur un système ONTAP sur site.

Consultez la documentation mise en route pour sauvegarder les données de vos systèmes ONTAP sur site vers votre fournisseur de cloud spécifique afin de vous assurer que la configuration de votre ONTAP est correctement configurée pour le nouvel IPspace. Par exemple :

- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder.
- Le LIF doit être associé à l'IPspace que ONTAP doit utiliser pour se connecter au stockage objet.
- Les LIFs intercluster des nœuds doivent pouvoir accéder au magasin d'objets.
- Si vous utilisez un IPspace différent de celui de *default*, vous devrez peut-être créer une route statique pour accéder au stockage objet.

The screenshot shows a dialog box titled "IPspace" with a close button in the top right corner. Inside, there is a label "IPspace" above a dropdown menu currently showing "Default". At the bottom, there are two buttons: "Apply" and "Cancel".

IPspace

IPspace

Default

Apply Cancel

Il vous suffit de sélectionner le nouvel IPspace et de cliquer sur **appliquer**. Ensuite, vous pourrez sélectionner les volumes à sauvegarder à partir d'agrégats dans cet IPspace.

## Modifiez la bande passante réseau disponible pour charger les sauvegardes dans le stockage objet

Lorsque vous activez Cloud Backup pour un environnement de travail, par défaut, ONTAP peut utiliser une quantité illimitée de bande passante pour transférer les données de sauvegarde depuis les volumes de l'environnement de travail vers le stockage objet. Si vous remarquez que le trafic de sauvegarde affecte les charges de travail normales des utilisateurs, vous pouvez limiter la quantité de bande passante réseau utilisée pendant le transfert. Vous pouvez choisir une valeur comprise entre 1 et 1,000 Mbit/s comme vitesse de transfert maximale.

The screenshot shows a dialog box titled "Max Transfer Rate" with a close button in the top right corner. It contains two radio buttons: "Unlimited" and "Limited". The "Limited" option is selected. To the right of "Limited" is a text field labeled "Limited to:" containing the value "1-1,000 Mbps". At the bottom, there are two buttons: "Apply" and "Cancel".

Max Transfer Rate

☐ Unlimited

☒ Limited Limited to: 1-1,000 Mbps

Apply Cancel

Sélectionnez le bouton radio **Limited** et saisissez la bande passante maximale utilisable, ou sélectionnez **Unlimited** pour indiquer qu'il n'y a pas de limite.

## Modifier le paramètre de sauvegarde automatique pour les volumes futurs

Si vous n'avez pas activé la sauvegarde automatique des futurs volumes lorsque vous avez activé Cloud Backup, vous pouvez commencer à effectuer des sauvegardes automatiques de nouveaux volumes dans la section sauvegarde automatique. Vous pouvez également sélectionner la stratégie de sauvegarde qui sera appliquée à ces nouveaux volumes. L'affectation d'une règle de sauvegarde aux nouveaux volumes permet de garantir la protection de toutes vos données.

Si vous avez activé la sauvegarde automatique des futurs volumes lorsque vous avez activé Cloud Backup, vous pouvez modifier la règle de sauvegarde qui sera utilisée pour les nouveaux volumes créés dans la section sauvegarde automatique.

Notez que la règle que vous souhaitez appliquer aux nouveaux volumes doit déjà exister. ["Découvrez comment créer une nouvelle stratégie de sauvegarde pour un environnement de travail"](#).

Automatic Backup

☒ Back up all future volumes using the selected Backup policy

Choose the policy that will be assigned to new volumes.

Select Backup Policy

Policy1 (1 Daily,1Weekly)

Apply Cancel

Une fois activée, cette stratégie de sauvegarde sera appliquée à tout nouveau volume créé dans cet environnement de travail à l'aide de BlueXP, System Manager, de l'interface de ligne de commande ONTAP ou des API.

## Indiquer si les copies Snapshot historiques sont exportées en tant que fichiers de sauvegarde

S'il existe des copies Snapshot locales pour les volumes correspondant au libellé de planification des sauvegardes que vous utilisez dans cet environnement de travail (par exemple, quotidienne, hebdomadaire, etc.), vous pouvez exporter ces snapshots historiques vers le stockage objet sous forme de fichiers de sauvegarde. Cela vous permet d'initialiser vos sauvegardes dans le cloud en déplaçant d'anciennes copies Snapshot vers la copie de sauvegarde de base.

Notez que cette option s'applique uniquement aux nouveaux fichiers de sauvegarde pour les nouveaux volumes de lecture/écriture et qu'elle n'est pas prise en charge avec les volumes DP (protection des données).

Export existing Snapshot copies

☒ Export existing Snapshot copies to object storage as backup files

All historical Snapshot copies of read/write volumes that match the Backup schedule label (daily, weekly, etc.) will be copied to object storage as backup files to ensure the most complete data protection.

Apply Cancel

Il vous suffit d'indiquer si vous souhaitez exporter les copies Snapshot existantes, puis de cliquer sur **appliquer**.

## Modifier si les snapshots « annuels » sont supprimés du système source

Lorsque vous sélectionnez l'étiquette de sauvegarde « annuelle » pour une règle de sauvegarde pour l'un de vos volumes, la copie Snapshot créée est extrêmement volumineuse. Par défaut, ces snapshots annuels sont supprimés automatiquement du système source après leur transfert vers le stockage objet. Vous pouvez modifier ce comportement par défaut à partir de la section Suppression annuelle de l'instantané.

Yearly Snapshot Deletion
Enabled

☒ Enabled  
Yearly Snapshot copies are deleted from the source system after being transferred to object storage as backups.

☐ Disabled  
Yearly Snapshot copies are retained on the source system. Note that these snapshots can be large.

Apply Cancel

Sélectionnez **Disabled** et cliquez sur **Apply** si vous souhaitez conserver les instantanés annuels sur le système source.

## Restauration de données ONTAP à partir des fichiers de sauvegarde

Les sauvegardes sont stockées dans un magasin d'objets de votre compte cloud, de sorte que vous puissiez restaurer les données à partir d'un point dans le temps spécifique. Vous pouvez restaurer un volume ONTAP entier à partir d'un fichier de sauvegarde ou, si vous n'avez qu'à restaurer quelques fichiers, vous pouvez restaurer un dossier ou des fichiers individuels à partir d'un fichier de sauvegarde.


Vous pouvez restaurer un **volume** (en tant que nouveau volume) dans l'environnement de travail d'origine, vers un environnement de travail différent qui utilise le même compte cloud ou sur un système ONTAP sur site.

Vous pouvez restaurer un **dossier** sur un volume de l'environnement de travail d'origine, sur un volume dans un environnement de travail différent qui utilise le même compte cloud ou sur un volume situé sur un système ONTAP sur site.

Vous pouvez restaurer **les fichiers** sur un volume de l'environnement de travail d'origine, sur un volume dans un autre environnement de travail qui utilise le même compte cloud ou sur un volume d'un système ONTAP sur site.

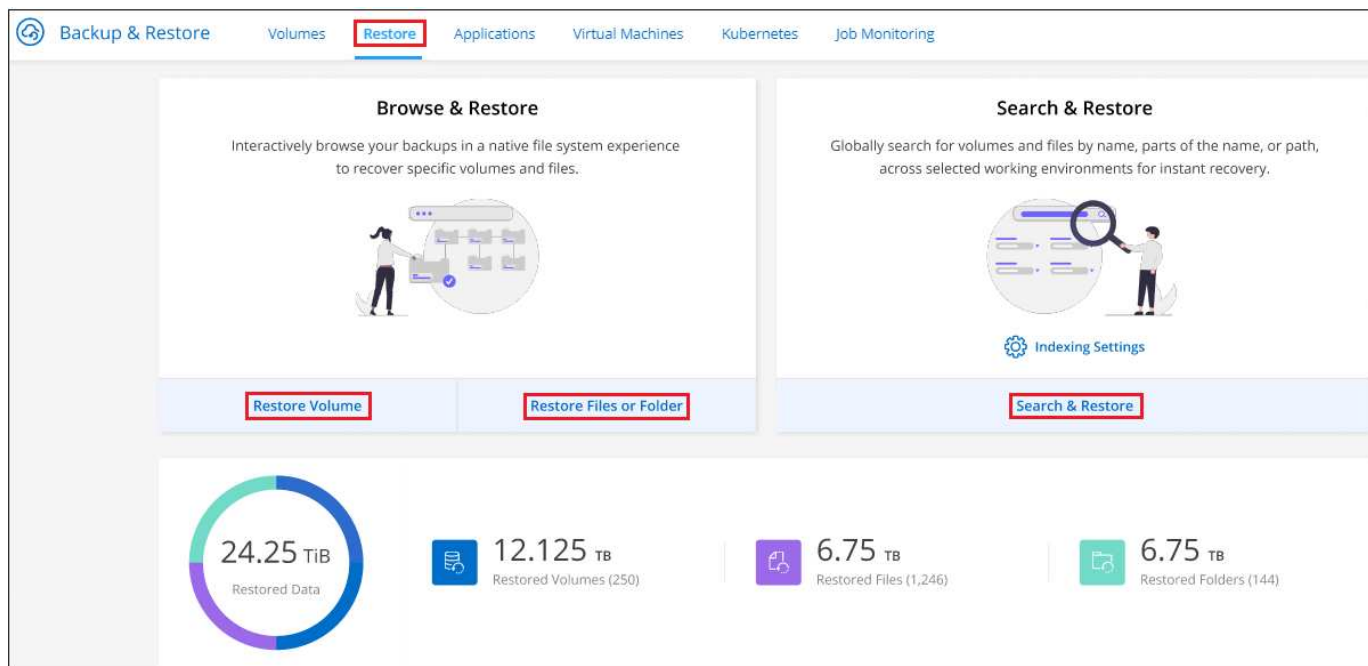
Une licence Cloud Backup valide est requise pour restaurer les données à partir des fichiers de sauvegarde vers un système de production.

### Le tableau de bord de restauration

Le tableau de bord de restauration permet d'effectuer des opérations de restauration de volumes, de dossiers et de fichiers. Pour accéder au Tableau de bord de restauration, cliquez sur **Backup and Recovery** dans le menu BlueXP, puis cliquez sur l'onglet **Restore**. Vous pouvez également cliquer sur  > **Afficher le tableau de bord de restauration** à partir du service de sauvegarde et de récupération du panneau Services.



Cloud Backup doit déjà être activé pour au moins un environnement de travail et les fichiers de sauvegarde initiaux doivent exister.



Comme vous pouvez le voir, le tableau de bord de restauration propose deux façons différentes de restaurer des données à partir de fichiers de sauvegarde : **Browse & Restore** et **Search & Restore**.

## Comparer l'utilisation et la restauration et la recherche et la restauration

En termes généraux, *Browse & Restore* est généralement mieux lorsque vous devez restaurer un volume, un dossier ou un fichier spécifique de la semaine ou du mois précédent — vous connaissez le nom et l'emplacement du fichier, et la date à laquelle il a été en bonne forme. *Search & Restore* est généralement préférable lorsque vous devez restaurer un volume, un dossier ou un fichier, mais vous ne vous souvenez pas du nom exact, du volume dans lequel il réside, ou de la date à laquelle il était en forme.

Ce tableau permet de comparer les deux méthodes.

Parcourir et restaurer	Recherche et restauration
Parcourez une structure de type dossier pour trouver le volume, le dossier ou le fichier dans un seul fichier de sauvegarde	Recherchez un volume, un dossier ou un fichier dans <b>tous les fichiers de sauvegarde</b> par nom de volume partiel ou complet, nom de dossier/fichier partiel ou complet, plage de tailles et filtres de recherche supplémentaires
La restauration de volumes et de fichiers fonctionne avec les fichiers de sauvegarde stockés dans Amazon S3, Azure Blob, Google Cloud et NetApp StorageGRID	La restauration de volumes et de fichiers fonctionne avec les fichiers de sauvegarde stockés dans Amazon S3, Azure Blob, Google Cloud et NetApp StorageGRID
Restaurez des volumes, des dossiers et des fichiers depuis StorageGRID sur des sites sans accès à Internet	Non pris en charge sur les sites sombres
Ne gère pas les fichiers qui ont été renommés ou supprimés	Gère les répertoires nouvellement créés/supprimés/renommés et les fichiers nouvellement créés/supprimés/renommés

Parcourir et restaurer	Recherche et restauration
Parcourez les résultats sur les clouds publics et privés	Parcourez les résultats dans les clouds publics et les copies Snapshot locales
Aucune ressource supplémentaire n'est requise du fournisseur de cloud	Ressources supplémentaires requises par compte pour les fournisseurs de compartiment et de cloud public
Aucun coût supplémentaire n'est requis du fournisseur de cloud	Coût associé aux ressources des fournisseurs de cloud public lors de l'analyse des sauvegardes et des volumes pour les résultats de recherche

Avant de pouvoir utiliser l'une ou l'autre méthode de restauration, assurez-vous d'avoir configuré votre environnement en fonction des besoins de ressources uniques. Ces exigences sont décrites dans les sections ci-dessous.

Reportez-vous aux étapes de configuration requise et de restauration pour le type d'opération de restauration que vous souhaitez utiliser :

- <<Restoring volumes using Browse & Restore, Restaurez les volumes à l'aide de Browse ; restaurez
- <<Restoring folders and files using Browse & Restore, Restaurez les dossiers et les fichiers à l'aide de Browse Restore
- <<Restoring ONTAP data using Search & Restore, Restaurez des volumes, des dossiers et des fichiers à l'aide de Search ; Restore

## Restauration de données ONTAP à l'aide de Browse & Restore

Avant de commencer la restauration d'un volume, d'un dossier ou d'un fichier, vous devez connaître le nom du volume à partir duquel vous souhaitez restaurer, le nom de l'environnement de travail où réside le volume et la date approximative du fichier de sauvegarde à partir duquel vous souhaitez restaurer.

**Remarque :** si le fichier de sauvegarde du volume que vous souhaitez restaurer réside dans le stockage d'archives (à partir de ONTAP 9.10.1), l'opération de restauration prendra plus de temps et entraînera un coût. En outre, le cluster de destination doit également exécuter ONTAP 9.10.1 ou version ultérieure pour la restauration du volume, 9.11.1 pour la restauration des fichiers et 9.12.1 pour Google Archive.

["En savoir plus sur la restauration à partir du stockage d'archivage Google".](#)

### Parcourir et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer un volume, un dossier ou des fichiers individuels depuis un fichier de sauvegarde ONTAP vers les environnements de travail suivants :

Emplacement du fichier de sauvegarde	Destination Environnement de travail ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS endif::aws[] ifdef::Azure[]
Blob d'Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]

Emplacement du fichier de sauvegarde	Destination Environnement de travail ifdef::aws[]
NetApp StorageGRID	Système ONTAP sur site

Pour l'utilisation et la restauration, le connecteur peut être installé aux emplacements suivants :

- Pour Google Cloud Storage, le connecteur doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, le connecteur doit être déployé sur site

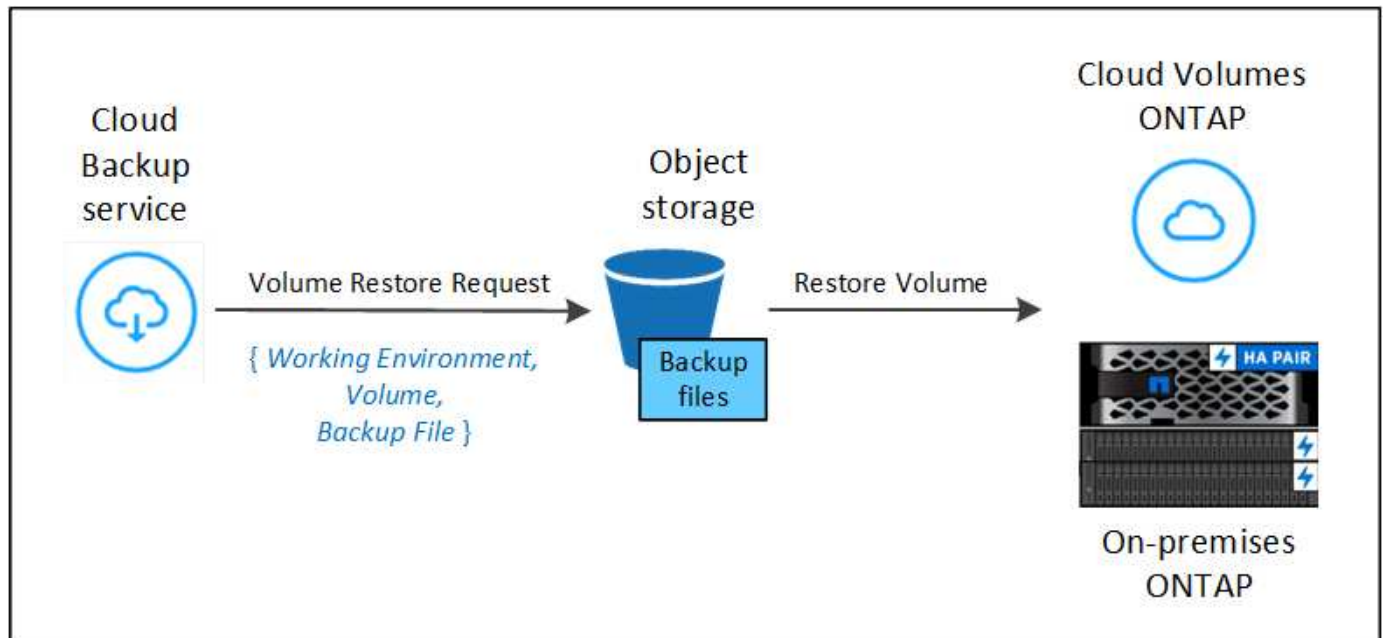
Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select.



Vous ne pouvez pas restaurer des dossiers ou des fichiers si le fichier de sauvegarde a été configuré avec DataLock & ransomware. Dans ce cas, vous pouvez restaurer tout le volume à partir du fichier de sauvegarde, puis accéder aux fichiers dont vous avez besoin.

### Restauration de volumes à l'aide de Browse & Restore

Lorsque vous restaurez un volume à partir d'un fichier de sauvegarde, Cloud Backup crée un *nouveau* volume en utilisant les données de la sauvegarde. Vous pouvez restaurer les données sur un volume de l'environnement de travail d'origine ou sur un autre environnement de travail situé dans le même compte cloud que l'environnement de travail source. Vous pouvez également restaurer des volumes sur un système ONTAP sur site.



Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail, le nom du volume et la date du fichier de sauvegarde pour pouvoir restaurer un volume.

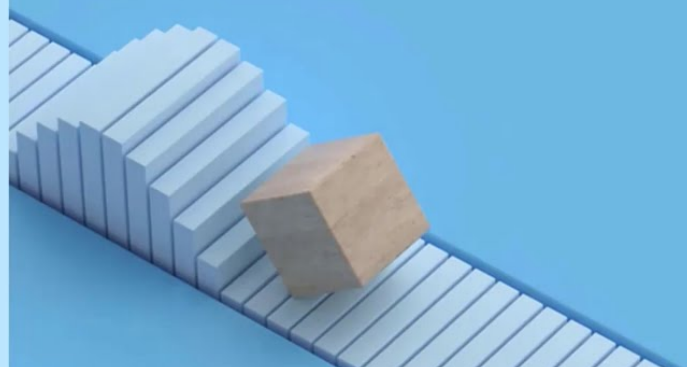
La vidéo suivante montre une présentation rapide de la restauration d'un volume :

# Cloud Backup Service: Restore Demo

Powered by Cloud Manager

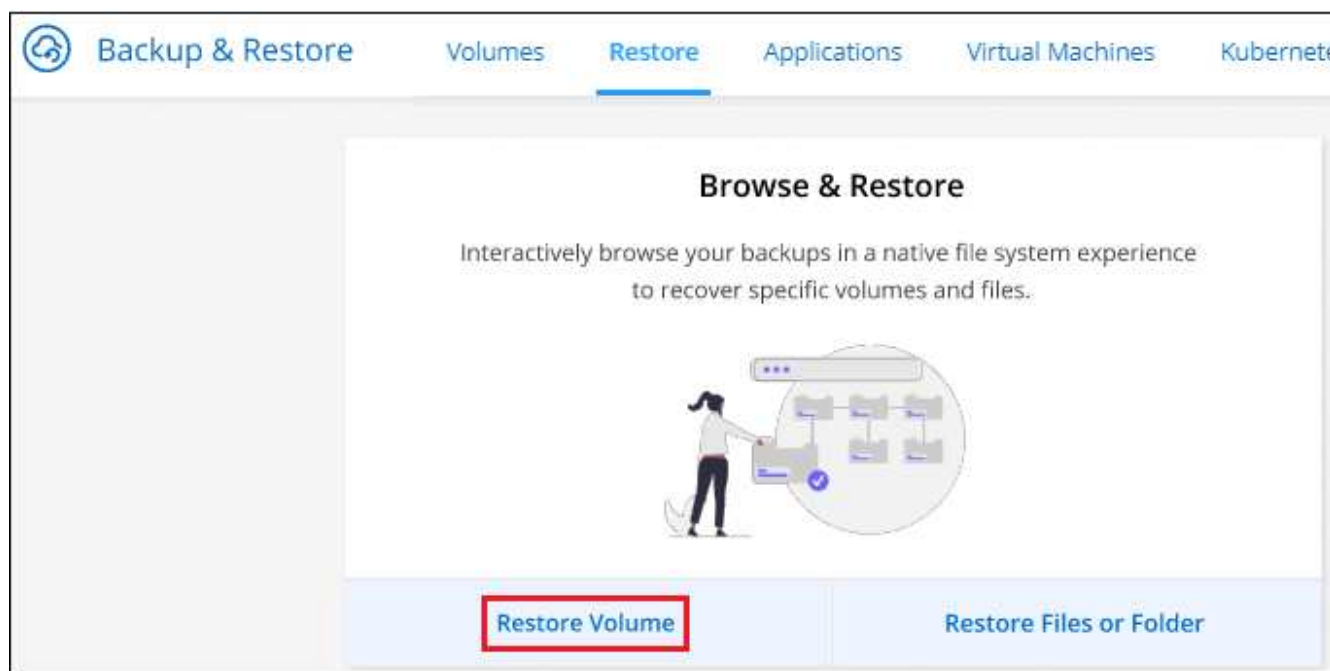
January 2022

 NetApp



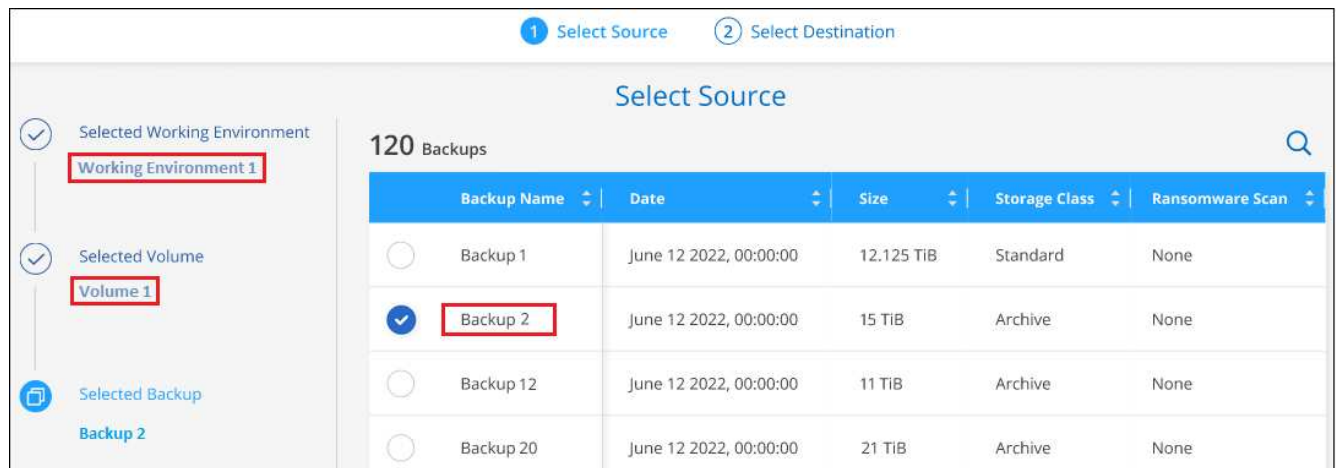
## Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Restore** pour afficher le tableau de bord de restauration.
3. Dans la section *Browse & Restore*, cliquez sur **Restore Volume**.



4. Dans la page *Select Source*, accédez au fichier de sauvegarde du volume que vous souhaitez restaurer. Sélectionnez le **Environnement de travail**, le **Volume** et le fichier **Backup** dont l'horodatage doit être restauré.

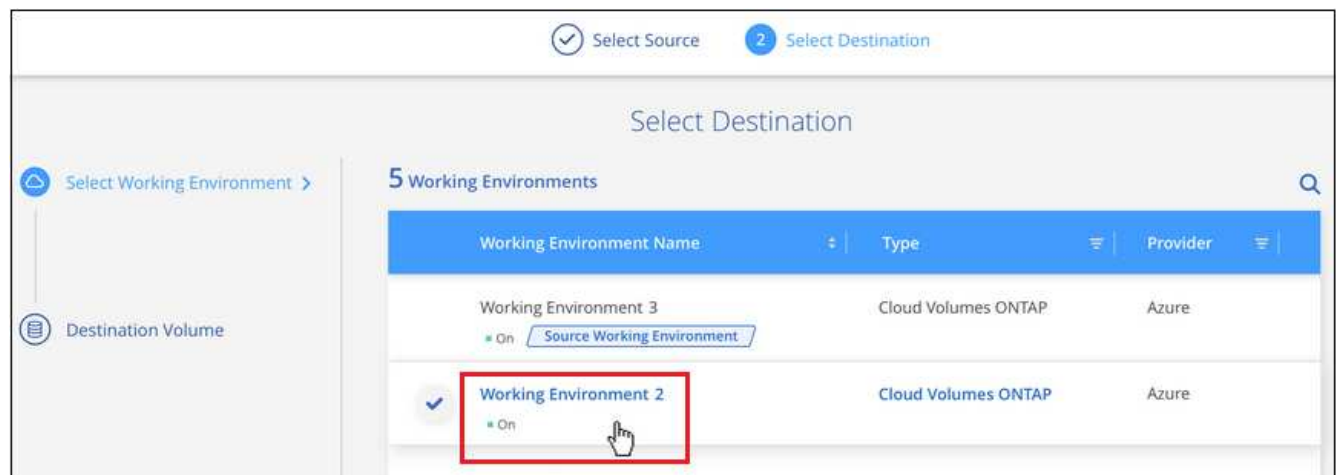




5. Cliquez sur **Suivant**.

Si la protection par ransomware est active pour le fichier de sauvegarde (si vous avez activé DataLock et ransomware protection dans la stratégie de sauvegarde), vous êtes invité à exécuter une analyse par ransomware supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons de scanner le fichier de sauvegarde à des fins d'attaques par ransomware.

6. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer le volume.



7. Si vous sélectionnez un système ONTAP sur site et que vous n'avez pas encore configuré la connexion de cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires :

- Lors d'une restauration à partir de Google Cloud Storage, sélectionnez Google Cloud Project, la clé d'accès et la clé secrète pour accéder au stockage objet, la région dans laquelle les sauvegardes sont stockées, et l'IPspace dans le cluster ONTAP où réside le volume de destination.
- Lors de la restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où le volume de destination résidera.
  - a. Entrez le nom à utiliser pour le volume restauré, puis sélectionnez le VM de stockage et l'agrégat dans lequel le volume sera stocké. Par défaut, **<source\_volume\_name>\_restore** est utilisé comme nom de volume.

Select Destination

Selected Working Environment  
Working Environment Name 2

Destination Volume >  
General\_restore

A new volume will be created in the working environment based on the backup you selected

Volume Name  
General\_restore

Storage VM  
svm1

Aggregate  
aggr2

Restore Priority  
Low

Volume Information

Volume Size: 50.00 GB
Backup Policy: CloudBackupService
Protocol: NFS
Disk Type: RW

Et si vous restaurez le volume à partir d'un fichier de sauvegarde résidant sur un niveau de stockage d'archives (disponible à partir de ONTAP 9.10.1), vous pouvez sélectionner la priorité de restauration.

"[En savoir plus sur la restauration à partir du stockage d'archivage Google](#)". Les fichiers de sauvegarde du niveau de stockage Google Archive sont restaurés presque immédiatement, sans priorité de restauration.

1. Cliquez sur **Restaurer** et vous revenez au Tableau de bord de restauration pour vérifier la progression de l'opération de restauration.

## Résultat

Cloud Backup crée un nouveau volume en fonction de la sauvegarde que vous avez sélectionnée. C'est possible "[gérez les paramètres de sauvegarde de ce nouveau volume](#)" selon les besoins.

Notez que la restauration d'un volume à partir d'un fichier de sauvegarde qui réside dans le stockage d'archivage peut prendre plusieurs minutes ou heures, selon le niveau d'archivage et la priorité de restauration. Vous pouvez cliquer sur l'onglet **surveillance des travaux** pour voir la progression de la restauration.

## Restauration des dossiers et des fichiers à l'aide de la fonction Parcourir et Restaurer

Si vous n'avez besoin de restaurer que quelques fichiers depuis la sauvegarde d'un volume ONTAP, vous avez la possibilité de restaurer un dossier ou des fichiers individuels au lieu de restaurer tout le volume. Vous pouvez restaurer des dossiers et des fichiers vers un volume existant dans l'environnement de travail d'origine ou vers un autre environnement de travail utilisant le même compte cloud. Vous pouvez également restaurer des dossiers et des fichiers vers un volume situé sur un système ONTAP sur site.

Si vous sélectionnez plusieurs fichiers, tous les fichiers sont restaurés sur le même volume de destination que vous choisissez. Si vous souhaitez restaurer des fichiers sur différents volumes, vous devez exécuter le processus de restauration plusieurs fois.

Pour le moment, vous ne pouvez sélectionner et restaurer qu'un seul dossier. Et seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni aucun fichier dans des sous-dossiers, n'est restauré.



- Vous ne pouvez pas restaurer des dossiers ou des fichiers si le fichier de sauvegarde a été configuré avec DataLock & ransomware. Dans ce cas, vous pouvez restaurer tout le volume à partir du fichier de sauvegarde, puis accéder aux fichiers dont vous avez besoin.
- La restauration au niveau des dossiers n'est actuellement pas prise en charge lorsque le fichier de sauvegarde se trouve dans le stockage d'archivage. Dans ce cas, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer le volume entier à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.

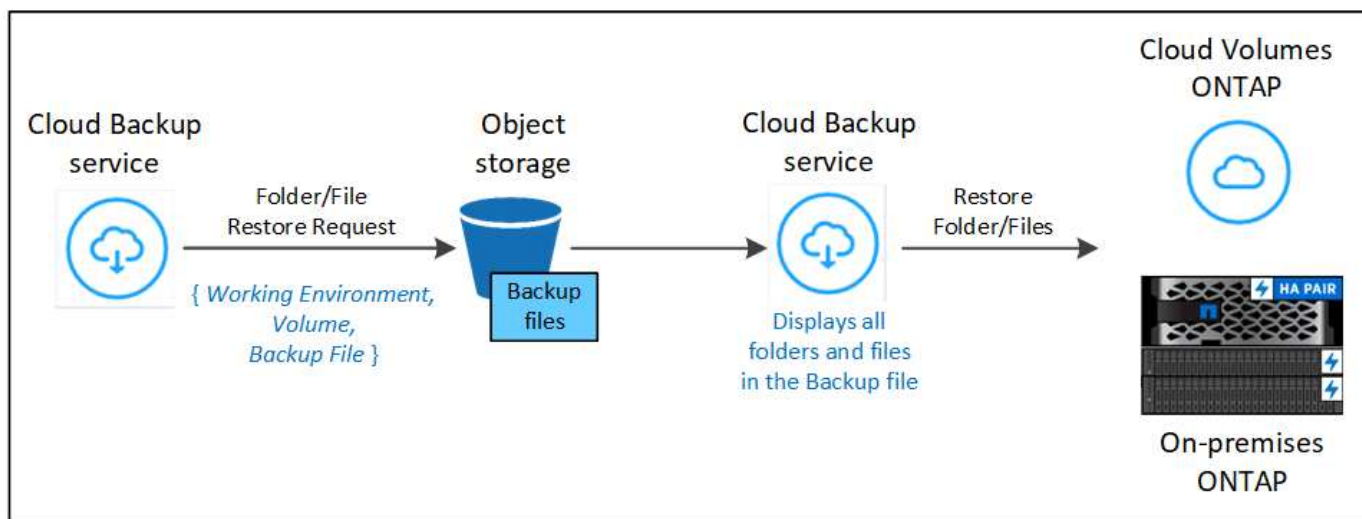
## Prérequis

- La version ONTAP doit être 9.6 ou supérieure pour effectuer des opérations *file restore*.
- La version ONTAP doit être 9.11.1 ou supérieure pour effectuer des opérations *folder restore*. `ifdef::aws[]`

## Processus de restauration des dossiers et des fichiers

Le processus se présente comme suit :

1. Lorsque vous souhaitez restaurer un dossier ou un ou plusieurs fichiers à partir d'une sauvegarde de volume, cliquez sur l'onglet **Restaurer**, puis sur **Restaurer les fichiers ou le dossier** sous *Parcourir et Restaurer*.
2. Sélectionnez l'environnement de travail source, le volume et le fichier de sauvegarde dans lequel le dossier ou le fichier(s) résident(s).
3. Cloud Backup affiche les dossiers et les fichiers qui existent dans le fichier de sauvegarde sélectionné.
4. Sélectionnez le ou les fichiers que vous souhaitez restaurer à partir de cette sauvegarde.
5. Sélectionnez l'emplacement de destination où vous souhaitez restaurer le dossier ou le fichier(s) (l'environnement de travail, le volume et le dossier), puis cliquez sur **Restaurer**.
6. Les fichiers sont restaurés.

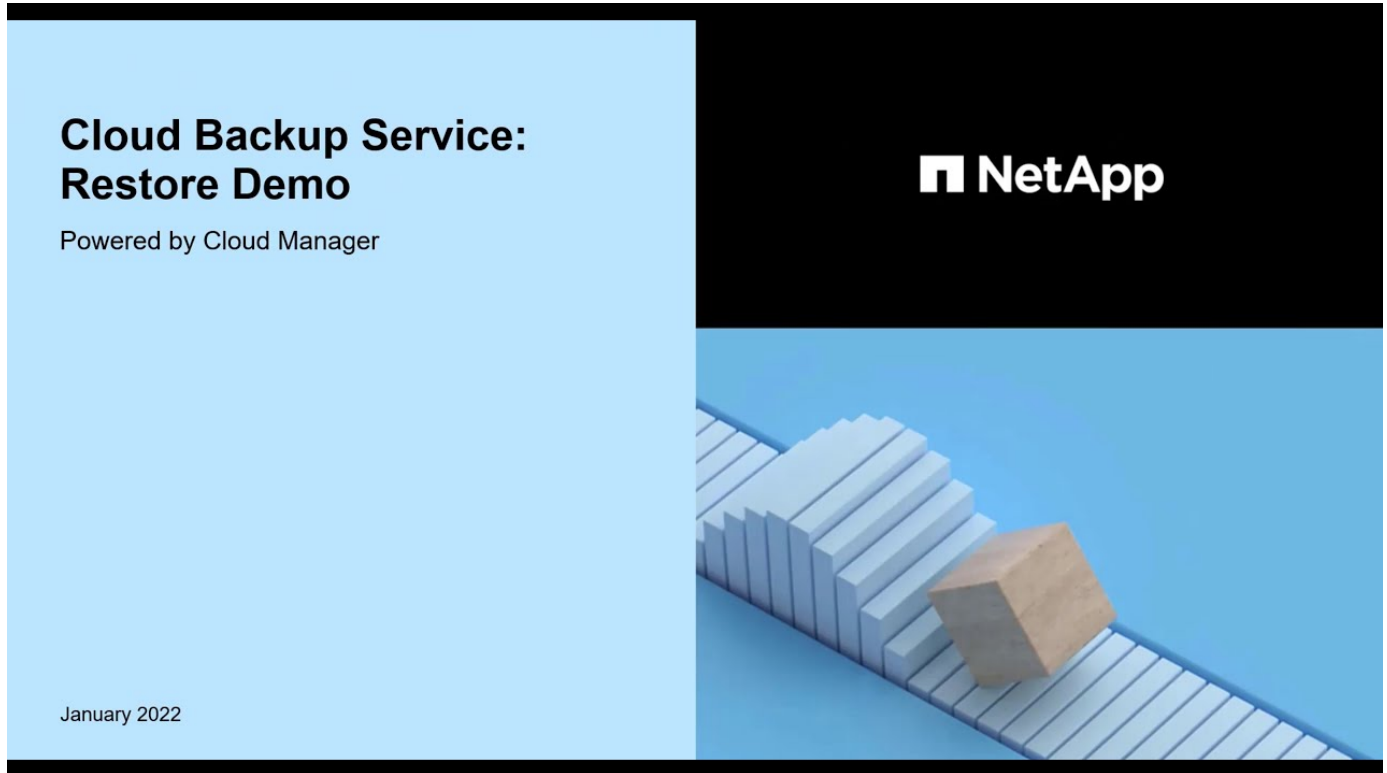


Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail, le nom du volume, la date du fichier de sauvegarde et le nom du dossier/fichier pour effectuer la restauration d'un dossier ou d'un fichier.

## Restauration des dossiers et des fichiers

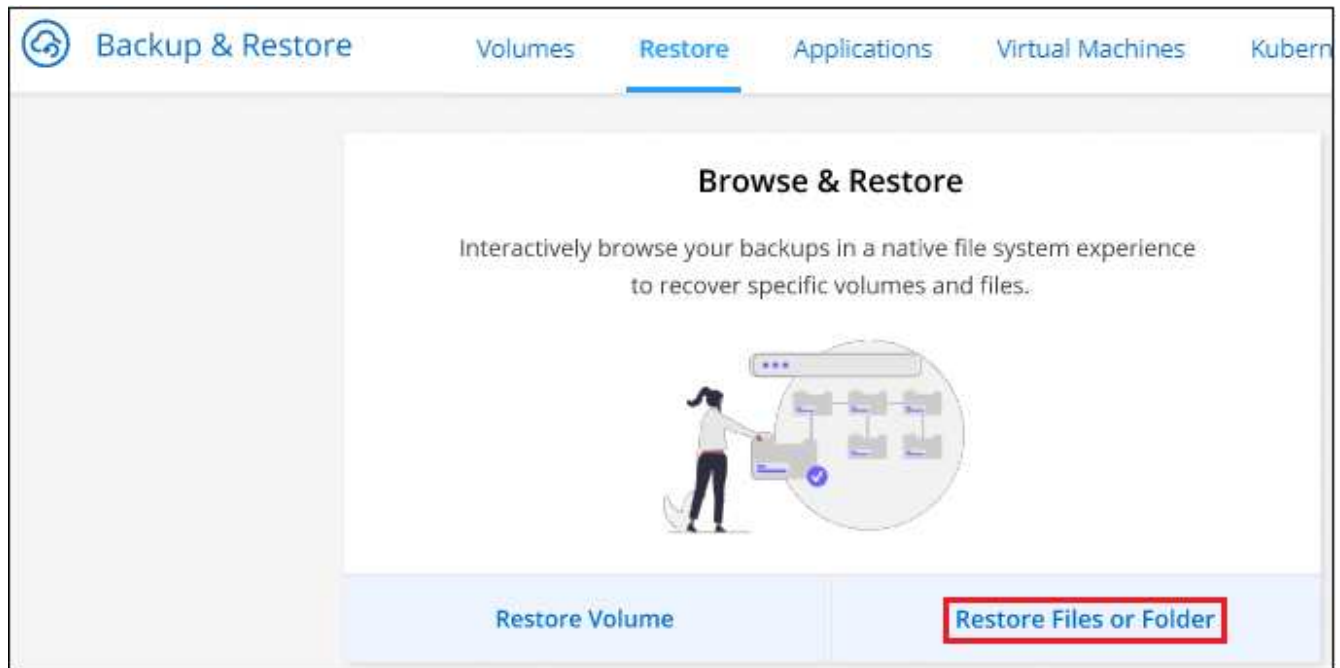
Procédez comme suit pour restaurer des dossiers ou des fichiers vers un volume à partir d'une sauvegarde de volume ONTAP. Vous devez connaître le nom du volume et la date du fichier de sauvegarde que vous souhaitez utiliser pour restaurer le dossier ou le(s) fichier(s). Cette fonctionnalité utilise la navigation en direct pour afficher la liste des répertoires et des fichiers de chaque fichier de sauvegarde.

La vidéo suivante montre une présentation rapide de la restauration d'un seul fichier :

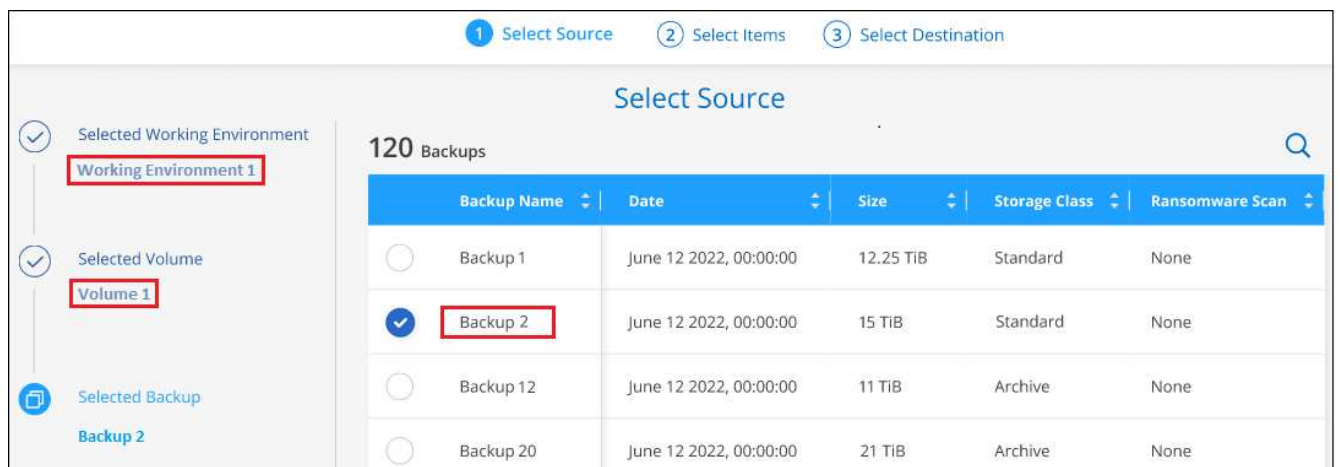


### Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Restore** pour afficher le tableau de bord de restauration.
3. Dans la section *Browse & Restore*, cliquez sur **Restore files ou Folder**.



4. Dans la page *Select Source*, accédez au fichier de sauvegarde du volume contenant le ou les fichiers à restaurer. Sélectionnez **Environnement de travail**, **Volume** et **Backup** qui possède l'horodatage à partir duquel vous souhaitez restaurer les fichiers.



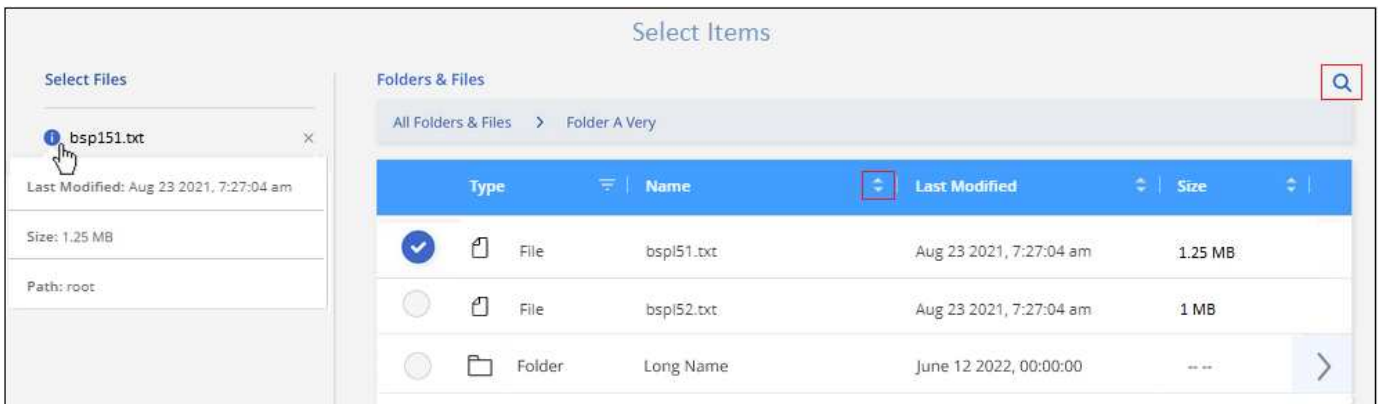
5. Cliquez sur **Suivant** et la liste des dossiers et fichiers de la sauvegarde de volume s'affiche.


Si vous restaurez des dossiers ou des fichiers à partir d'un fichier de sauvegarde résidant sur un niveau de stockage d'archives (disponible à partir de ONTAP 9.10.1), vous pouvez sélectionner la priorité de restauration.

"[En savoir plus sur la restauration à partir du stockage d'archivage Google](#)". Les fichiers de sauvegarde du niveau de stockage Google Archive sont restaurés presque immédiatement, sans priorité de restauration.

+ et si la protection par ransomware est active pour le fichier de sauvegarde (si vous avez activé DataLock et ransomware protection dans la stratégie de sauvegarde), vous êtes invité à exécuter une analyse par ransomware supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons de scanner le fichier de sauvegarde à des fins d'attaques par ransomware.

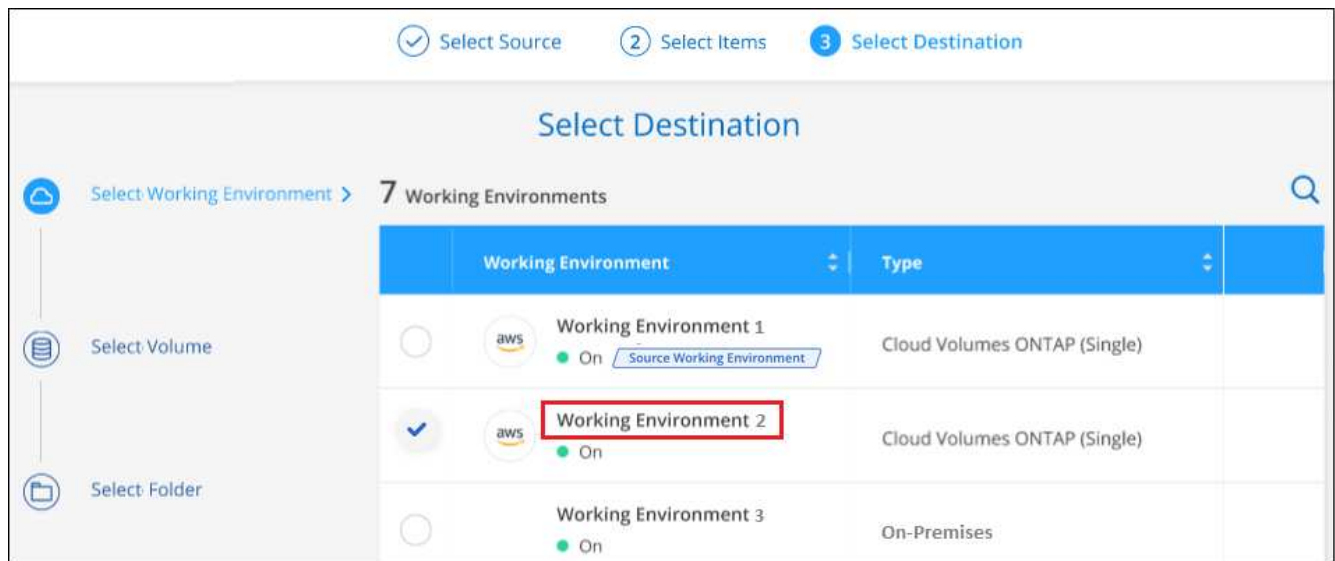
+



1. Dans la page *Select Items*, sélectionnez le ou les fichiers que vous souhaitez restaurer et cliquez sur **Continuer**. Pour vous aider à trouver l'élément :
  - Vous pouvez cliquer sur le nom du dossier ou du fichier si vous le voyez.
  - Vous pouvez cliquer sur l'icône de recherche et saisir le nom du dossier ou du fichier pour naviguer directement vers l'élément.
  - Vous pouvez naviguer vers le bas niveaux dans les dossiers à l'aide de  à la fin de la ligne pour trouver des fichiers spécifiques.

Lorsque vous sélectionnez des fichiers, ils sont ajoutés à gauche de la page pour voir les fichiers que vous avez déjà sélectionnés. Si nécessaire, vous pouvez supprimer un fichier de cette liste en cliquant sur **x** en regard du nom du fichier.

2. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer les éléments.



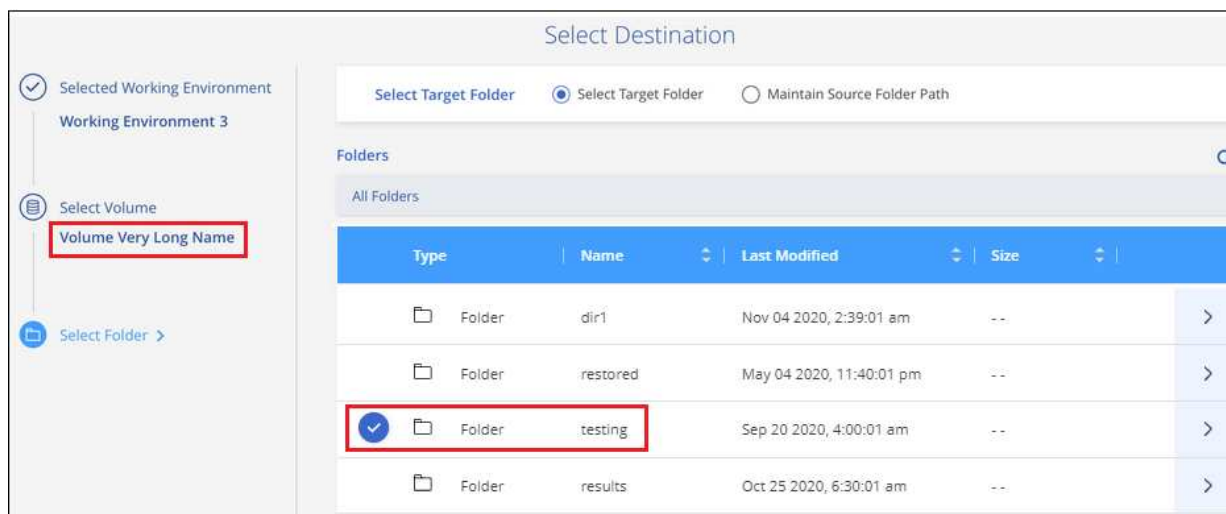
Si vous sélectionnez un cluster sur site et que vous n'avez pas encore configuré la connexion de cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires :

- Lors d'une restauration à partir de Google Cloud Storage, entrez l'IPspace dans le cluster ONTAP où résident les volumes de destination, ainsi que la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet.
- Lors d'une restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la




clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où réside le volume de destination.

- a. Sélectionnez ensuite le **Volume** et le **dossier** où vous souhaitez restaurer le ou les dossiers.



Vous disposez de quelques options pour l'emplacement de restauration des dossiers et des fichiers.

- Lorsque vous avez choisi **Sélectionner le dossier cible**, comme indiqué ci-dessus :
  - Vous pouvez sélectionner n'importe quel dossier.
  - Vous pouvez passer le curseur de la souris sur un dossier et cliquer sur  à la fin de la ligne pour accéder aux sous-dossiers, puis sélectionner un dossier.
- Si vous avez sélectionné le même environnement de travail et le même volume que le dossier/fichier source, vous pouvez sélectionner **gérer le chemin du dossier source** pour restaurer le dossier ou les fichiers dans le dossier où ils existent dans la structure source. Tous les mêmes dossiers et sous-dossiers doivent déjà exister ; les dossiers ne sont pas créés. Lorsque vous restaurez les fichiers à leur emplacement d'origine, vous pouvez choisir d'écraser le ou les fichiers source ou de créer de nouveaux fichiers.
  - a. Cliquez sur **Restaurer** et vous revenez au Tableau de bord de restauration pour vérifier la progression de l'opération de restauration. Vous pouvez également cliquer sur l'onglet **surveillance des travaux** pour voir la progression de la restauration.

## Restauration de données ONTAP à l'aide de la fonction de recherche et de restauration

Vous pouvez restaurer un volume, un dossier ou des fichiers à partir d'un fichier de sauvegarde ONTAP à l'aide de la fonction Rechercher et restaurer. La fonction de recherche et restauration vous permet de rechercher un volume, un dossier ou un fichier spécifique à partir de toutes les sauvegardes stockées dans le stockage cloud pour un fournisseur spécifique, puis d'effectuer une restauration. Il n'est pas nécessaire de connaître le nom exact de l'environnement de travail ou le nom du volume ; la recherche s'effectue via tous les fichiers de sauvegarde de volume.

L'opération de recherche examine également toutes les copies Snapshot locales existant pour vos volumes ONTAP. Étant donné que la restauration des données à partir d'une copie Snapshot locale peut être plus rapide et moins coûteuse que la restauration à partir d'un fichier de sauvegarde, il est possible de restaurer les données à partir d'une copie Snapshot. Vous pouvez restaurer l'instantané en tant que nouveau volume à partir de la page Détails du volume de la zone de travail.

Lorsque vous restaurez un volume à partir d'un fichier de sauvegarde, Cloud Backup crée un *nouveau* volume en utilisant les données de la sauvegarde. Vous pouvez restaurer les données en tant que volume dans l'environnement de travail d'origine ou vers un autre environnement de travail situé dans le même compte cloud que l'environnement de travail source. Vous pouvez également restaurer des volumes sur un système ONTAP sur site.

Vous pouvez restaurer des dossiers ou des fichiers vers l'emplacement du volume d'origine, vers un autre volume dans le même environnement de travail ou vers un autre environnement de travail qui utilise le même compte cloud. Vous pouvez également restaurer des dossiers et des fichiers vers un volume situé sur un système ONTAP sur site.

Si le fichier de sauvegarde du volume que vous souhaitez restaurer se trouve dans le stockage d'archives (disponible à partir de ONTAP 9.10.1), l'opération de restauration prend plus de temps et entraînera des coûts supplémentaires. Notez que le cluster de destination doit également exécuter ONTAP 9.10.1 ou version ultérieure pour la restauration de volume, 9.11.1 pour la restauration de fichiers et 9.12.1 pour Google Archive.

["En savoir plus sur la restauration à partir du stockage d'archivage Google".](#)



- Vous ne pouvez pas restaurer des dossiers ou des fichiers si le fichier de sauvegarde a été configuré avec DataLock & ransomware. Dans ce cas, vous pouvez restaurer tout le volume à partir du fichier de sauvegarde, puis accéder aux fichiers dont vous avez besoin.
- La restauration au niveau des dossiers n'est actuellement pas prise en charge lorsque le fichier de sauvegarde se trouve dans le stockage d'archivage. Dans ce cas, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer le volume entier à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.

Avant de commencer, vous devriez avoir une idée du nom ou de l'emplacement du volume ou du fichier à restaurer.

La vidéo suivante montre une présentation rapide de la restauration d'un seul fichier :



# Cloud Backup : Search and Restore

Indexed Catalog Preview Feature

February 2022

© 2022 NetApp, Inc. All rights reserved.



## Rechercher et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer un volume, un dossier ou des fichiers individuels depuis un fichier de sauvegarde ONTAP vers les environnements de travail suivants :

Emplacement du fichier de sauvegarde	Destination Environnement de travail ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS endif::aws[] ifdef::Azure[]
Blob d'Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]
NetApp StorageGRID	Système ONTAP sur site

Pour la recherche et la restauration, le connecteur peut être installé aux emplacements suivants :

- Pour Google Cloud Storage, le connecteur doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, le connecteur doit être déployé dans vos locaux avec une connexion Internet

Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select.

## Prérequis

- Configuration requise pour le cluster :
  - La version ONTAP doit être supérieure ou égale à 9.8.
  - La VM de stockage (SVM) sur laquelle réside le volume doit avoir une LIF de données configurée.

- NFS doit être activé sur le volume.
- Le serveur RPC SnapDiff doit être activé sur le SVM. BlueXP le fait automatiquement lorsque vous activez l'indexation sur l'environnement de travail.
- Exigences Google Cloud :
  - Des autorisations Google BigQuery spécifiques doivent être ajoutées au rôle utilisateur qui fournit des autorisations BlueXP. ["Assurez-vous que toutes les autorisations sont correctement configurées"](#).

Notez que si vous utilisiez déjà Cloud Backup avec un connecteur que vous avez configuré auparavant, vous devrez ajouter maintenant les autorisations BigQuery au rôle utilisateur BlueXP. Ils sont nouveaux et sont requis pour la recherche et la restauration.

- Configuration minimale requise pour StorageGRID :

En fonction de votre configuration, la recherche et la restauration peuvent être mises en œuvre de deux façons :

- S'il n'y a pas d'identifiants de fournisseur de cloud dans votre compte, les informations de catalogue indexées sont stockées sur le connecteur.
- Si vous l'avez ["Identifiants AWS"](#) ou ["Identifiants Azure"](#) Dans le compte, le catalogue indexé est stocké sur le fournisseur cloud, comme avec un connecteur déployé dans le cloud. (Si vous disposez des deux identifiants, AWS est sélectionné par défaut.)

Même si vous utilisez un connecteur sur site, les exigences du fournisseur cloud doivent être respectées tant pour les autorisations de connecteur que pour les ressources du fournisseur cloud. Consultez les exigences AWS et Azure ci-dessus lors de l'utilisation de cette implémentation.

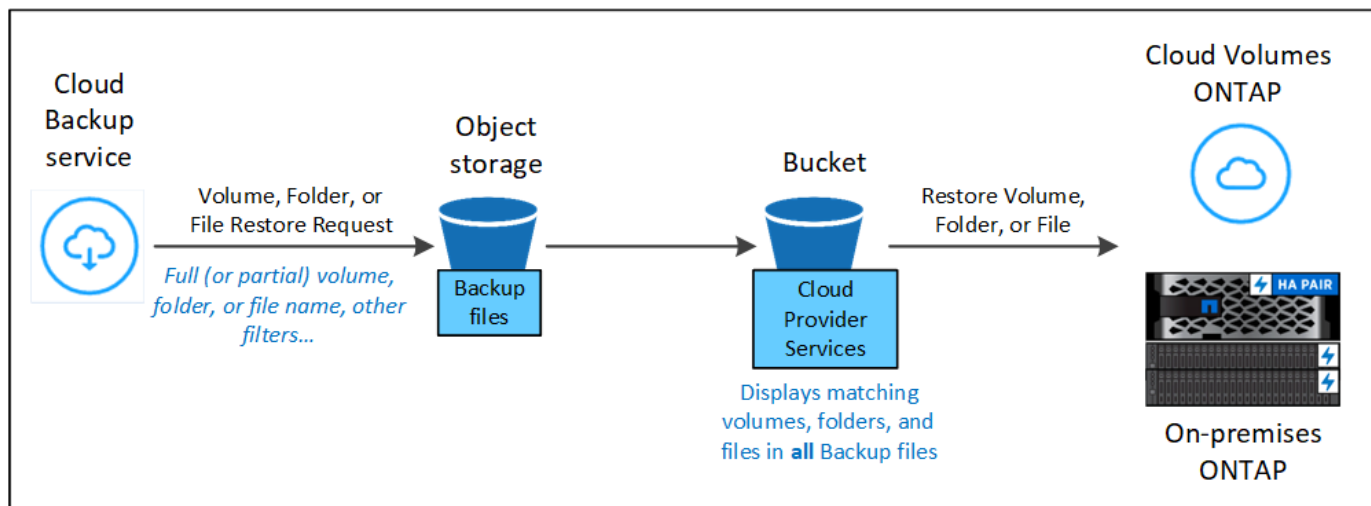
## Processus de recherche et de restauration

Le processus se présente comme suit :

1. Avant de pouvoir utiliser la fonction de recherche et de restauration, vous devez activer « indexation » sur chaque environnement de travail source à partir duquel vous souhaitez restaurer les données du volume. Cela permet au catalogue indexé de suivre les fichiers de sauvegarde pour chaque volume.
2. Lorsque vous souhaitez restaurer un ou plusieurs volumes à partir d'une sauvegarde de volume, sous *Rechercher et Restaurer*, cliquez sur **Rechercher et restaurer**.
3. Entrez les critères de recherche d'un volume, d'un dossier ou d'un fichier par nom de volume partiel ou complet, nom de fichier partiel ou complet, plage de tailles, plage de dates de création, autres filtres de recherche, puis cliquez sur **Rechercher**.

La page Résultats de la recherche affiche tous les emplacements qui ont un fichier ou un volume correspondant à vos critères de recherche.

4. Cliquez sur **Afficher toutes les sauvegardes** pour l'emplacement que vous souhaitez utiliser pour restaurer le volume ou le fichier, puis cliquez sur **Restaurer** sur le fichier de sauvegarde réel que vous souhaitez utiliser.
5. Sélectionnez l'emplacement où vous souhaitez restaurer le volume, le dossier ou le(s) fichier(s) et cliquez sur **Restaurer**.
6. Le volume, le dossier ou le(s) fichier(s) sont restaurés(s).



Comme vous pouvez le voir, vous n'avez besoin que d'un nom partiel et de recherches sur Cloud Backup dans tous les fichiers de sauvegarde qui correspondent à votre recherche.

### Activation du catalogue indexé pour chaque environnement de travail

Avant de pouvoir utiliser la fonction de recherche et de restauration, vous devez activer l'indexation sur chaque environnement de travail source à partir duquel vous prévoyez de restaurer des volumes ou des fichiers. Cela permet au catalogue indexé de suivre chaque volume et chaque fichier de sauvegarde, ce qui rend vos recherches très rapides et efficaces.

Lorsque vous activez cette fonctionnalité, Cloud Backup permet à SnapDiff v3 sur le SVM pour vos volumes, et effectue les actions suivantes :

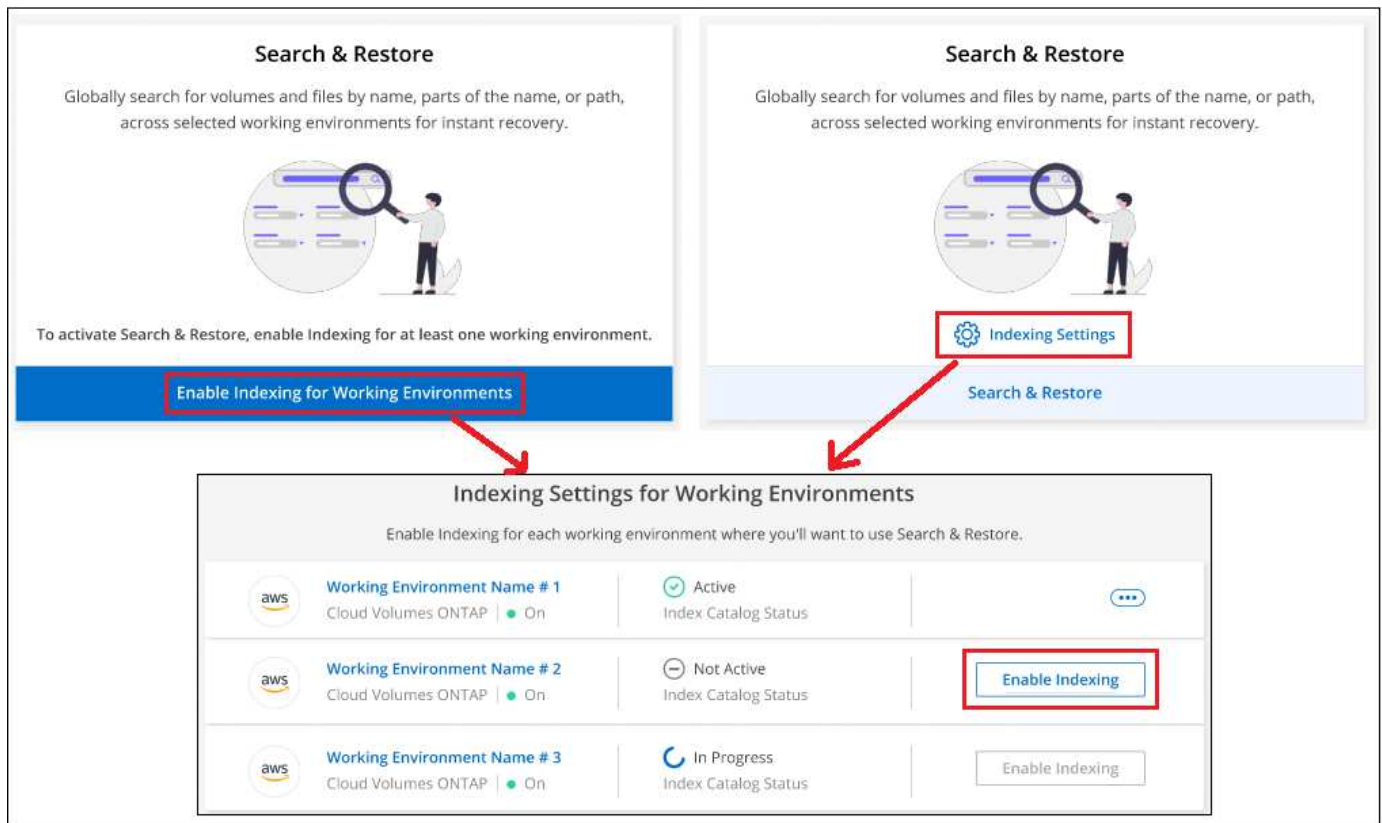
- Pour les sauvegardes stockées dans Google Cloud, un nouveau compartiment est provisionné, et le **"Services Google Cloud BigQuery"** sont provisionnées au niveau compte/projet.
- Pour les sauvegardes stockées dans StorageGRID, l'espace est provisionné sur le connecteur ou sur l'environnement du fournisseur cloud.

Si l'indexation a déjà été activée pour votre environnement de travail, passez à la section suivante pour restaurer vos données.

Pour activer l'indexation pour un environnement de travail :

- Si aucun environnement de travail n'a été indexé, dans le tableau de bord de restauration sous **Search & Restore**, cliquez sur **Activer l'indexation pour les environnements de travail**, puis sur **Activer l'indexation** pour l'environnement de travail.
- Si au moins un environnement de travail a déjà été indexé, dans le tableau de bord de restauration sous **Search & Restore**, cliquez sur **Indexing Settings**, puis sur **Enable Indexing** pour l'environnement de travail.

Une fois que tous les services sont provisionnés et que le catalogue indexé a été activé, l'environnement de travail est affiché comme « actif ».



Selon la taille des volumes de l'environnement de travail et le nombre de fichiers de sauvegarde dans le cloud, le processus d'indexation initial peut prendre jusqu'à une heure. Par la suite, elle est mise à jour de manière transparente toutes les heures avec des modifications incrémentielles pour maintenir des données à jour.

### Restauration de volumes, de dossiers et de fichiers à l'aide de la fonction Rechercher et Restaurer

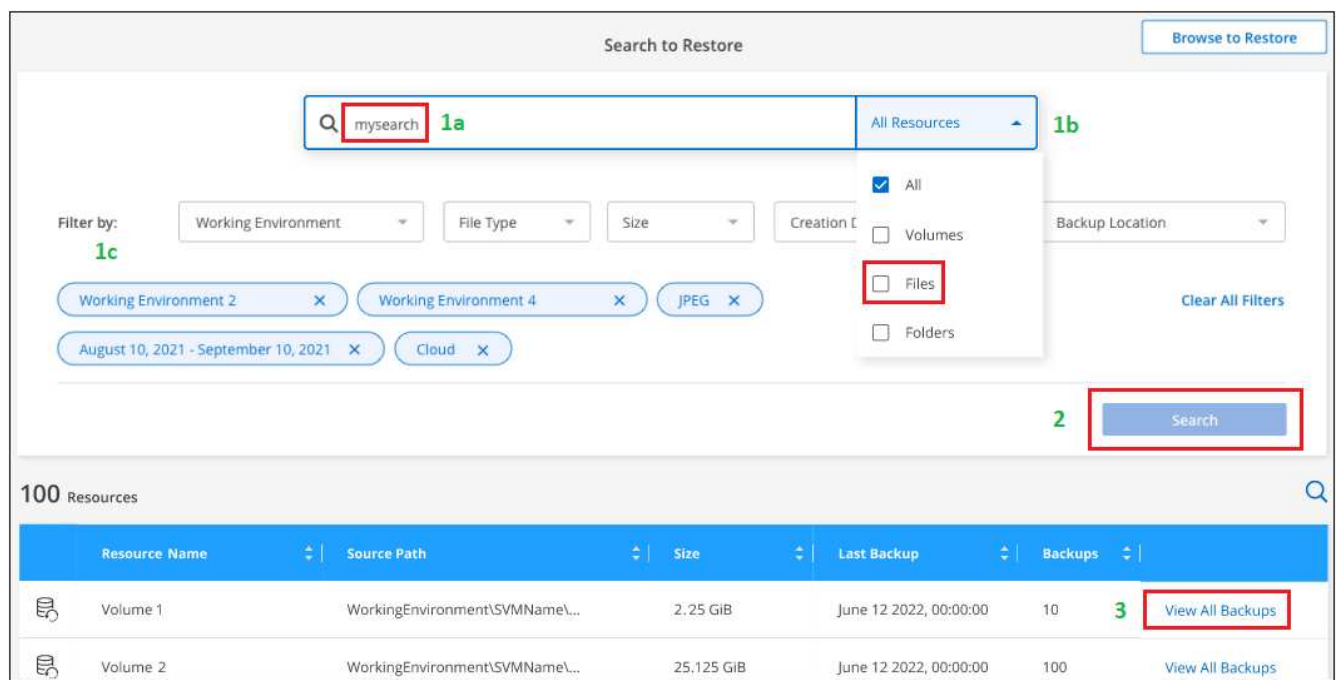
Après vous [Indexation activée pour votre environnement de travail](#), Vous pouvez restaurer des volumes, des dossiers et des fichiers à l'aide de la fonction Rechercher et restaurer. Cela vous permet d'utiliser une large gamme de filtres pour trouver le fichier ou volume exact que vous souhaitez restaurer à partir de tous les fichiers de sauvegarde.

#### Étapes

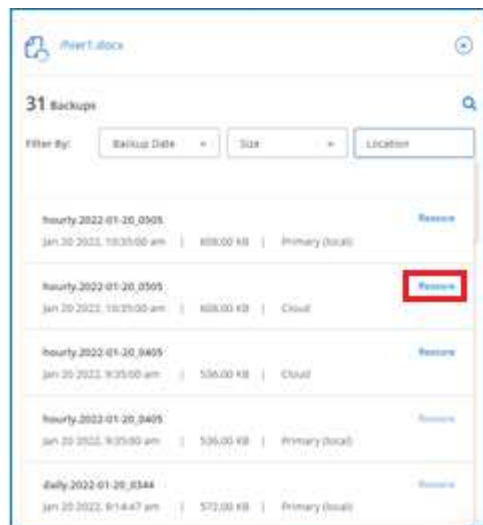
1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Restore** pour afficher le tableau de bord de restauration.
3. Dans la section *Search & Restore*, cliquez sur **Search & Restore**.



4. À partir de la page Rechercher pour restaurer :
  - a. Dans la barre de recherche *Search*, entrez un nom de volume complet ou partiel, un nom de dossier ou un nom de fichier.
  - b. Sélectionnez le type de ressource : **volumes**, **fichiers**, **dossiers** ou **tous**.
  - c. Dans la zone *Filter by*, sélectionnez les critères de filtre. Par exemple, vous pouvez sélectionner l'environnement de travail où se trouvent les données et le type de fichier, par exemple un fichier .JPEG.
5. Cliquez sur **Rechercher** et la zone Résultats de la recherche affiche toutes les ressources qui ont un fichier, un dossier ou un volume correspondant à votre recherche.



6. Cliquez sur **Afficher toutes les sauvegardes** pour la ressource contenant les données à restaurer pour afficher tous les fichiers de sauvegarde contenant le volume, le dossier ou le fichier correspondant.



7. Cliquez sur **Restaurer** pour le fichier de sauvegarde que vous souhaitez utiliser pour restaurer l'élément à partir du nuage.

Notez que les résultats identifient également les copies Snapshot de volume local contenant le fichier dans votre recherche. Le bouton **Restore** n'est pas fonctionnel pour les instantanés à ce moment, mais si vous souhaitez restaurer les données à partir de la copie Snapshot au lieu du fichier de sauvegarde, notez le nom et l'emplacement du volume, ouvrez la page Détails du volume sur la toile, Et utilisez l'option **Restaurer à partir de la copie Snapshot**.

8. Sélectionnez l'emplacement de destination où vous souhaitez restaurer le volume, le dossier ou le(s) fichier(s) et cliquez sur **Restaurer**.
  - Pour les volumes, vous pouvez sélectionner l'environnement de travail de destination d'origine ou sélectionner un autre environnement de travail.
  - Pour les dossiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, y compris l'environnement de travail, le volume et le dossier.
  - Pour les fichiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, y compris l'environnement de travail, le volume et le dossier. Lorsque vous sélectionnez l'emplacement d'origine, vous pouvez choisir d'écraser le ou les fichiers source ou de créer de nouveaux fichiers.

Si vous sélectionnez un système ONTAP sur site et que vous n'avez pas encore configuré la connexion de cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires :

- Lors de la restauration à partir de Google Cloud Storage, sélectionnez l'IPspace dans le cluster ONTAP où réside le volume de destination, ainsi que la clé d'accès et la clé secrète pour accéder au stockage objet. ["Reportez-vous aux détails de ces exigences"](#).
- Lors d'une restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où réside le volume de destination. ["Reportez-vous aux détails de ces exigences"](#).

## Résultats

Le volume, le dossier ou le(s) fichier(s) sont restaurés et vous revenez au tableau de bord de restauration pour vérifier la progression de l'opération de restauration. Vous pouvez également cliquer sur l'onglet **surveillance des travaux** pour voir la progression de la restauration.

Pour les volumes restaurés, vous pouvez ["gérer les paramètres de sauvegarde de ce nouveau volume"](#) selon les besoins.

# Sauvegarde et restauration des données Kubernetes

## Protection des données du cluster Kubernetes à l'aide de Cloud Backup

Cloud Backup inclut des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme des données de votre cluster Kubernetes. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé.

Si nécessaire, vous pouvez restaurer un *volume* entier à partir d'une sauvegarde vers le même environnement de travail ou vers un environnement de travail différent.

### Caractéristiques

Fonctionnalités de sauvegarde :

- Sauvegardez des copies indépendantes de vos volumes persistants sur un stockage objet à faible coût.
- Appliquer une seule stratégie de sauvegarde à tous les volumes d'un cluster, ou attribuer différentes règles de sauvegarde aux volumes ayant des objectifs de point de restauration uniques.
- Les données de sauvegarde sont sécurisées par chiffrement AES 256 bits au repos et TLS 1.2 HTTPS en transit.
- Prise en charge de 4,000 sauvegardes maximum d'un seul volume.

Fonctions de restauration :

- Restauration des données à partir d'un point dans le temps spécifique
- Restaurer un volume vers le système source ou vers un autre système.
- Restaure les données au niveau bloc en les plaçant directement à l'emplacement que vous indiquez, tout en conservant les ACL d'origine.

### Environnements de travail Kubernetes et fournisseurs de stockage objet pris en charge

Cloud Backup vous permet de sauvegarder des volumes Kubernetes à partir de ces environnements de travail vers un stockage objet dans plusieurs fournisseurs de cloud public et privé :

Environnement de travail source	Destination du fichier de sauvegarde ifdef::aws[]
Cluster Kubernetes dans AWS	Amazon S3 endif::aws[] ifdef::Azure[]
Cluster Kubernetes dans Azure	Azure Blob endif::Azure[] ifdef::gcp[]
Cluster Kubernetes dans Google	Google Cloud Storage endif::gcp[]

Vous pouvez restaurer un volume à partir d'un fichier de sauvegarde Kubernetes vers les environnements de travail suivants :



Emplacement du fichier de sauvegarde	Destination Environnement de travail <code>ifdef::aws[]</code>
Amazon S3	Cluster Kubernetes dans AWS <code>endif::aws[] ifdef::Azure[]</code>
Blob d’Azure	Cluster Kubernetes dans Azure <code>endif::Azure[] ifdef::gcp[]</code>
Google Cloud Storage	Cluster Kubernetes dans Google <code>endif::gcp[]</code>

## Le coût

Deux types de coûts sont associés à Cloud Backup : les frais de ressources et les frais de service.

### Frais de ressources

Les frais en ressources sont payés au fournisseur cloud pour la capacité de stockage objet dans le cloud. Étant donné que Cloud Backup préserve l’efficacité du stockage du volume source, vous payez les coûts de stockage objet du fournisseur cloud pour les données *après* efficacité ONTAP (pour la quantité de données plus faible après l’application de la déduplication et de la compression).

### Frais de service

Les frais de service sont payés à NetApp et couvrent à la fois le coût de *créer* sauvegardes et de *restaurer* volumes à partir de ces sauvegardes. Vous ne payez que les données que vous protégez, calculées par la capacité logique utilisée source (*before* ONTAP efficacités) des volumes sauvegardés sur le stockage objet. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

Vous pouvez payer le service de sauvegarde de deux façons. La première option consiste à vous abonner à votre fournisseur cloud pour un paiement mensuel. La deuxième option consiste à acheter des licences directement auprès de NetApp. Lire le [Licences](#) pour plus de détails.

## Licences

Deux options de licence sont disponibles pour Cloud Backup : le paiement à l’utilisation (PAYGO) et le modèle de licence BYOL (Bring Your Own License). Un essai gratuit de 30 jours est disponible si vous n’avez pas de licence.

### Essai gratuit

Lorsque vous utilisez l’essai gratuit de 30 jours, vous êtes averti du nombre de jours d’essai gratuits qui restent. À la fin de votre essai gratuit, les sauvegardes cessent d’être créées. Vous devez vous abonner au service ou acheter une licence pour continuer à utiliser le service.

Les fichiers de sauvegarde ne sont pas supprimés lorsque le service est désactivé. Votre fournisseur cloud continuera de vous facturer les coûts de stockage objet pour la capacité de vos sauvegardes, à moins de supprimer les sauvegardes.

### Abonnement avec paiement à l’utilisation

Cloud Backup propose un modèle de paiement à l’utilisation avec des licences basées sur la consommation. Après vous être abonné sur le marché de votre fournisseur cloud, vous payez par Go pour les données sauvegardées, sans paiement initial there. Votre fournisseur cloud vous facturé mensuellement.

Vous devez vous abonner même si vous disposez d’une période d’essai gratuite ou si vous apportez votre propre licence (BYOL) :

- L'abonnement garantit l'absence de perturbation du service après la fin de votre essai gratuit.

À la fin de l'essai, vous serez facturé toutes les heures en fonction de la quantité de données que vous sauvegardez.

- Si vous sauvegardez plus de données que ce que votre licence BYOL, la sauvegarde des données se poursuit avec votre abonnement au paiement basé sur l'utilisation.

Par exemple, si vous disposez d'une licence BYOL 10 To, toute la capacité au-delà de 10 To est facturée via l'abonnement PAYGO.

Vous ne serez pas facturé à partir de votre abonnement au paiement à l'utilisation pendant votre essai gratuit ou si vous n'avez pas dépassé votre licence BYOL.

["Découvrez comment configurer un abonnement avec paiement à l'utilisation"](#).

### **Bring your own license (BYOL)**

BYOL est basé sur la durée (12, 24 ou 36 mois) et sur la capacité par incréments de 1 To. Vous payez NetApp pour une utilisation du service pendant une période, disons 1 an, et pour une capacité maximale, disons 10 To.

Vous recevrez un numéro de série que vous entrez dans la page BlueXP Digital Wallet pour activer le service. Lorsque l'une ou l'autre limite est atteinte, vous devez renouveler la licence. La licence de sauvegarde BYOL s'applique à tous les systèmes source associés à votre ["Compte BlueXP"](#).

["Découvrez comment gérer vos licences BYOL"](#).

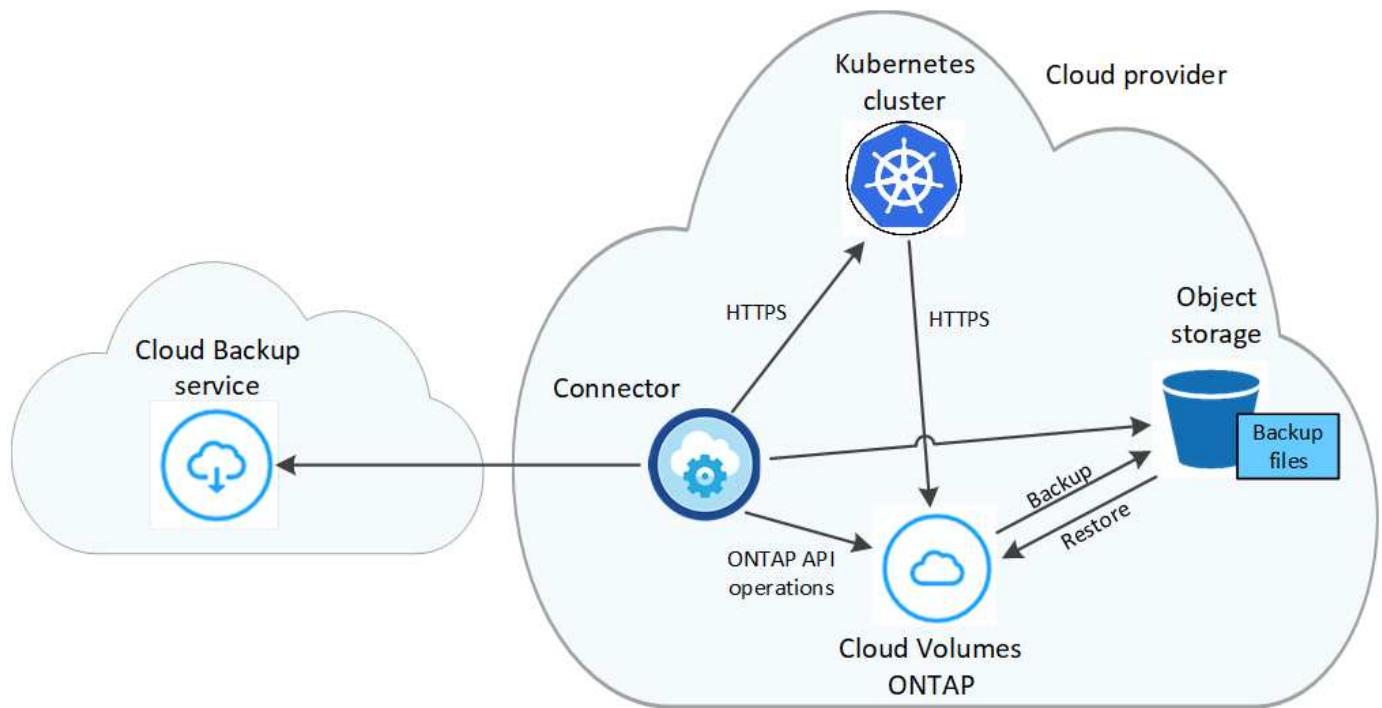
## **Fonctionnement de Cloud Backup**

Lorsque vous activez Cloud Backup sur un système Kubernetes, le service effectue une sauvegarde complète de vos données. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés. Le trafic réseau est ainsi réduit au minimum.



Toute action effectuée directement depuis votre environnement de fournisseur cloud pour gérer ou modifier des fichiers de sauvegarde peut corrompre les fichiers et entraîner une configuration non prise en charge.

L'image suivante montre la relation entre chaque composant :



## Classes de stockage ou niveaux d'accès pris en charge

- Dans GCP, les sauvegardes sont associées par défaut à la classe de stockage *Standard*.

## Personnalisation des paramètres de planification des sauvegardes et de conservation pour chaque cluster

Lorsque vous activez Cloud Backup pour un environnement de travail, tous les volumes que vous sélectionnez initialement sont sauvegardés à l'aide de la stratégie de sauvegarde par défaut que vous définissez. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes ayant des objectifs de point de récupération différents, vous pouvez créer des règles supplémentaires pour ce cluster et les affecter à d'autres volumes.

Vous avez le choix entre des sauvegardes toutes les heures, tous les jours, toutes les semaines et tous les mois,

Lorsque vous avez atteint le nombre maximal de sauvegardes pour une catégorie ou un intervalle, les anciennes sauvegardes sont supprimées, ce qui vous permet d'avoir toujours les sauvegardes les plus récentes.

## Volumes pris en charge

Cloud Backup prend en charge les volumes persistants (PVS).

## Limites

- Lors de la création ou de la modification d'une stratégie de sauvegarde lorsqu'aucun volume n'est affecté à la stratégie, le nombre de sauvegardes conservées peut atteindre un maximum de 1018. Pour contourner ce problème, vous pouvez réduire le nombre de sauvegardes pour créer la stratégie. Vous pouvez ensuite modifier la stratégie pour créer jusqu'à 4000 sauvegardes après avoir affecté des volumes à la stratégie.
- Les sauvegardes de volume ad hoc utilisant le bouton **Backup Now** ne sont pas prises en charge sur les volumes Kubernetes.

# Sauvegarde des données de volume persistant Kubernetes dans un stockage Google Cloud

Réalisez quelques étapes pour sauvegarder les données des volumes persistants sur des clusters GKE Kubernetes vers un stockage Google Cloud.

## Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

1

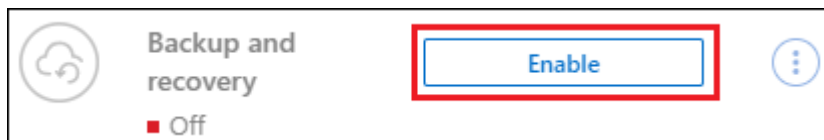
### Passer en revue les prérequis

- Vous avez découvert le cluster Kubernetes en tant qu'environnement de travail BlueXP.
  - Trident doit être installé sur le cluster, et la version de Trident doit être égale ou supérieure à 21.1.
  - Toutes les demandes de volume persistant qui seront utilisées pour créer des volumes persistants que vous souhaitez sauvegarder doivent avoir une « politique des snapshots » définie sur « par défaut ».
  - Le cluster doit utiliser Cloud Volumes ONTAP sur GCP pour le stockage interne de son système.
  - Le système Cloud Volumes ONTAP doit exécuter ONTAP 9.7P5 ou une version ultérieure.
- Vous disposez d'un abonnement GCP valide pour l'espace de stockage où se trouvent vos sauvegardes.
- Vous disposez d'un compte de service dans votre projet Google Cloud avec le rôle d'administrateur de stockage prédéfini.
- Vous avez souscrit au ["Offre de sauvegarde BlueXP Marketplace"](#), ou vous avez acheté ["et activé"](#) Licence Cloud Backup BYOL de NetApp.

2

### Activation de Cloud Backup sur votre cluster Kubernetes existant

Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service de sauvegarde et de récupération dans le panneau de droite, puis suivez l'assistant d'installation.



3

### Définissez la stratégie de sauvegarde

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Vous pouvez passer aux sauvegardes toutes les heures, tous les jours, hebdomadaires ou mensuelles ou sélectionner l'une des règles définies par le système et qui offrent plus d'options. Vous pouvez également modifier le nombre de copies de sauvegarde à conserver.

Define Policy

**Policy - Retention & Schedule**

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

**Storage Account** Cloud Manager will create the storage account after you complete the wizard

## 4

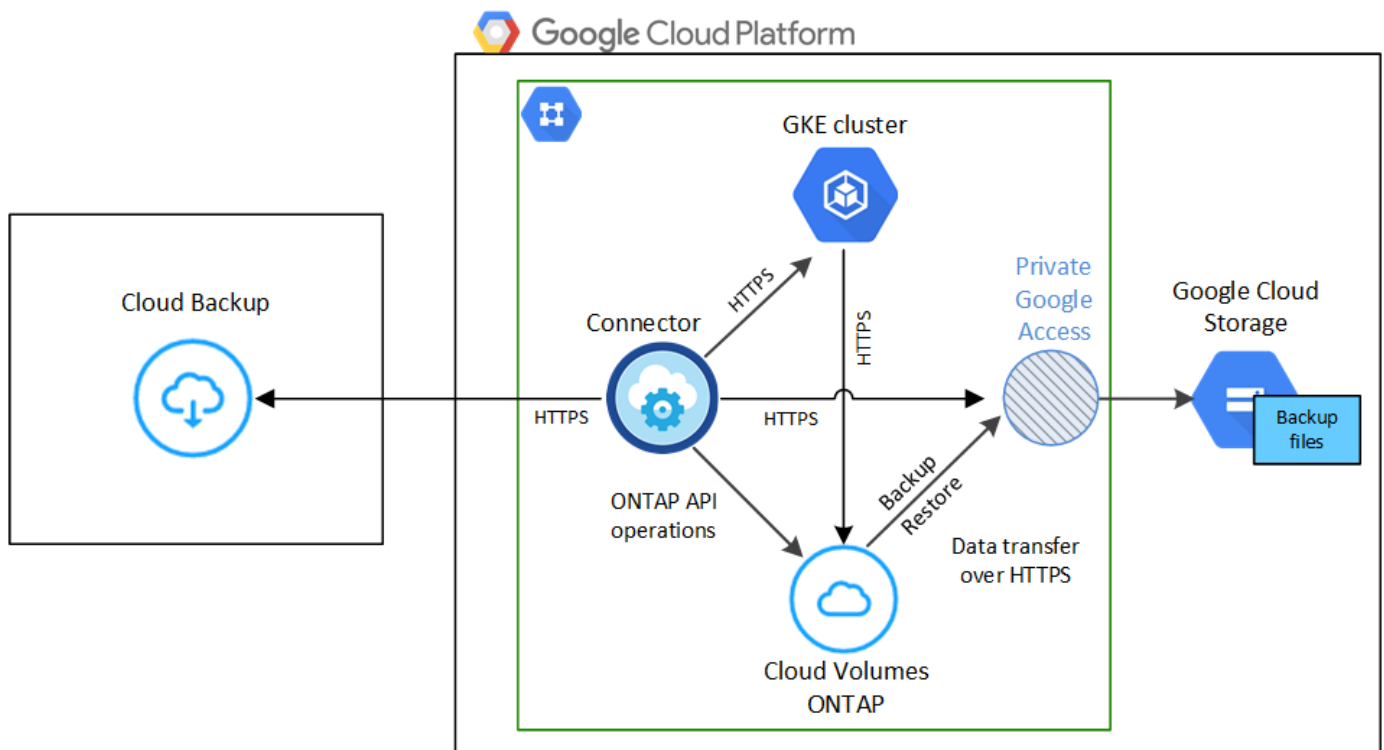
### Sélectionnez les volumes à sauvegarder

Identifiez les volumes à sauvegarder dans la page Sélectionner les volumes. Les fichiers de sauvegarde sont stockés dans un compartiment Google Cloud Storage avec le même abonnement GCP et la même région que le système Cloud Volumes ONTAP.

## De formation

Avant de commencer à sauvegarder les volumes persistants de Kubernetes sur Google Cloud, lisez les sections suivantes pour vérifier que la configuration est prise en charge.

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



Notez que le noeud final privé est facultatif.

## Exigences relatives aux clusters Kubernetes

- Vous avez découvert le cluster Kubernetes en tant qu'environnement de travail BlueXP. ["Découvrez comment découvrir le cluster Kubernetes"](#).
- Trident doit être installé sur le cluster, et la version de Trident doit être au moins 21.1. Voir ["Comment installer Trident"](#) ou ["Comment mettre à niveau la version de Trident"](#).
- Le cluster doit utiliser Cloud Volumes ONTAP sur GCP pour le stockage interne de son système.
- Le système Cloud Volumes ONTAP doit se trouver dans la même région GCP que le cluster Kubernetes et doit exécuter ONTAP 9.7P5 ou version ultérieure (ONTAP 9.8P11 et version ultérieure est recommandée).

Notez que les clusters Kubernetes situés dans des emplacements sur site ne sont pas pris en charge. Seuls les clusters Kubernetes dans les déploiements cloud qui utilisent des systèmes Cloud Volumes ONTAP sont pris en charge.

- Pour créer les volumes persistants que vous souhaitez sauvegarder, tous les objets utilisés pour la demande de volume persistant doivent avoir une « politique des snapshots » définie sur « par défaut ».

Vous pouvez le faire pour les ESV individuels en ajoutant `snapshotPolicy` sous annotations :

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

Vous pouvez effectuer cette opération pour tous les ESV associés à un stockage back-end particulier en ajoutant le `snapshotPolicy` champ sous valeurs par défaut dans `backend.json` fichier :

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

## Régions GCP prises en charge

Cloud Backup est pris en charge dans toutes les régions GCP "[Dans ce cas, Cloud Volumes ONTAP est pris en charge](#)".

## Conditions de licence

Pour le modèle de licence PAYGO Cloud Backup, un abonnement via le "[Marketplace GCP](#)" Est requise avant d'activer Cloud Backup. La facturation pour Cloud Backup s'effectue via cet abonnement. "[Vous pouvez vous abonner à la page Détails et amp ; informations d'identification de l'assistant de l'environnement de travail](#)".

Pour les licences BYOL, vous avez besoin du numéro de série NetApp qui permet d'utiliser le service pendant la durée et la capacité du contrat. "[Découvrez comment gérer vos licences BYOL](#)".

Vous devez également disposer d'un abonnement Google pour l'espace de stockage où vos sauvegardes seront stockées.

## Compte de services GCP

Vous devez disposer d'un compte de service dans votre projet Google Cloud avec le rôle d'administrateur de stockage prédéfini. "[Découvrez comment créer un compte de service](#)".

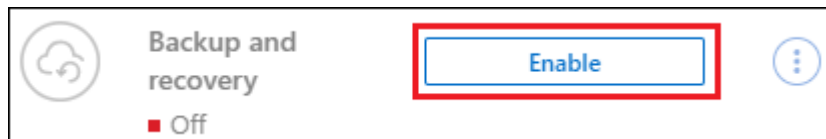
## Activation de Cloud Backup

Activation de Cloud Backup à tout moment directement depuis l'environnement de travail Kubernetes.

## Étapes

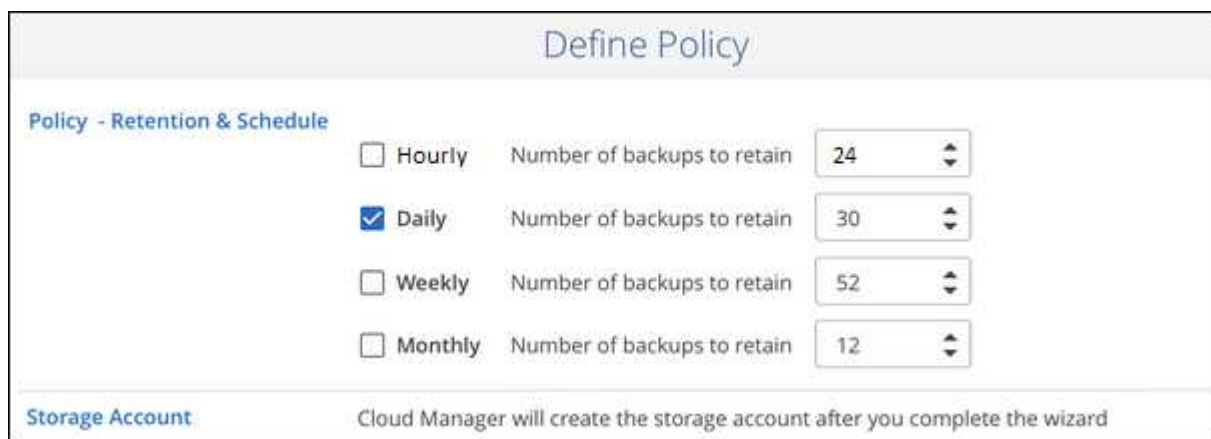


1. Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service de sauvegarde et de restauration dans le panneau de droite.



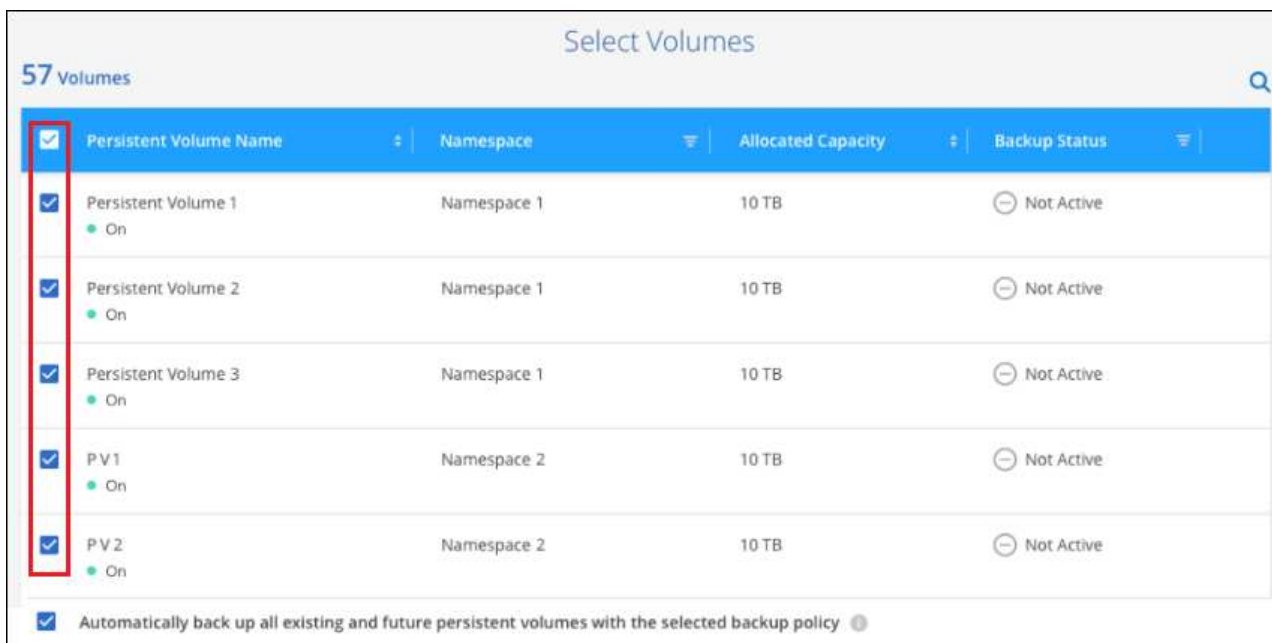
2. Entrez les détails de la stratégie de sauvegarde et cliquez sur **Suivant**.

Vous pouvez définir le planning de sauvegarde et choisir le nombre de sauvegardes à conserver.



3. Sélectionnez les volumes persistants que vous souhaitez sauvegarder.

- Pour sauvegarder tous les volumes, cochez la case de la ligne de titre (☒ Volume Name).
- Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☒ Volume\_1).



<input checked="" type="checkbox"/>	Persistent Volume Name	Namespace	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Persistent Volume 1 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 2 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 3 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	PV1 On	Namespace 2	10 TB	Not Active
<input checked="" type="checkbox"/>	PV2 On	Namespace 2	10 TB	Not Active
<input checked="" type="checkbox"/>	Automatically back up all existing and future persistent volumes with the selected backup policy			

4. Si vous souhaitez que la sauvegarde soit activée pour tous les volumes actuels et futurs, ne cochez pas la case "sauvegarde automatique des volumes futurs...". Si vous désactivez ce paramètre, vous devrez activer manuellement les sauvegardes pour les volumes futurs.

5. Cliquez sur **Activer la sauvegarde** et Cloud Backup commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

## Résultat

Les fichiers de sauvegarde sont stockés dans un compartiment Google Cloud Storage avec le même abonnement GCP et la même région que le système Cloud Volumes ONTAP.

Le tableau de bord Kubernetes s'affiche pour vous permettre de contrôler l'état des sauvegardes.

## Et la suite ?

C'est possible "[démarrer et arrêter les sauvegardes de volumes ou modifier le planning de sauvegarde](#)". Vous pouvez également "[restaurez des volumes entiers à partir d'un fichier de sauvegarde](#)". En tant que nouveau volume sur le même cluster Kubernetes ou un cluster différent dans GCP (dans la même région).

# Gestion des sauvegardes pour vos systèmes Kubernetes

Vous pouvez gérer les sauvegardes de vos systèmes Kubernetes en modifiant la planification des sauvegardes, en activant/désactivant les sauvegardes de volumes, en supprimant les sauvegardes, etc.



Ne gérez ni ne modifiez pas de fichiers de sauvegarde directement depuis votre environnement cloud fournisseur. Cela peut corrompre les fichiers et entraîner une configuration non prise en charge.

## Affichage des volumes en cours de sauvegarde

Vous pouvez afficher la liste de tous les volumes actuellement sauvegardés par Cloud Backup.

## Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Kubernetes** pour afficher la liste des volumes persistants pour les systèmes Kubernetes.

Source K8s Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backup Copies	Backup Status
aws eks1 Unknown	pvc-1704aa1f-af1d-49e9-87fd-6edd86125855 Unknown	default	Jun 09 2022, 10:00:24 am	20	Unknown
aws eks1 Unknown	pvc-1615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6 Unknown	default	Jun 09 2022, 10:00:24 am	20	Unknown
aws eks1 Unknown	pvc-d1f839c1-d932-4f49-b620-33321dbe939e Unknown	trident	Jun 09 2022, 10:00:24 am	20	Unknown

Si vous recherchez des volumes spécifiques dans certains clusters, vous pouvez affiner la liste par cluster et

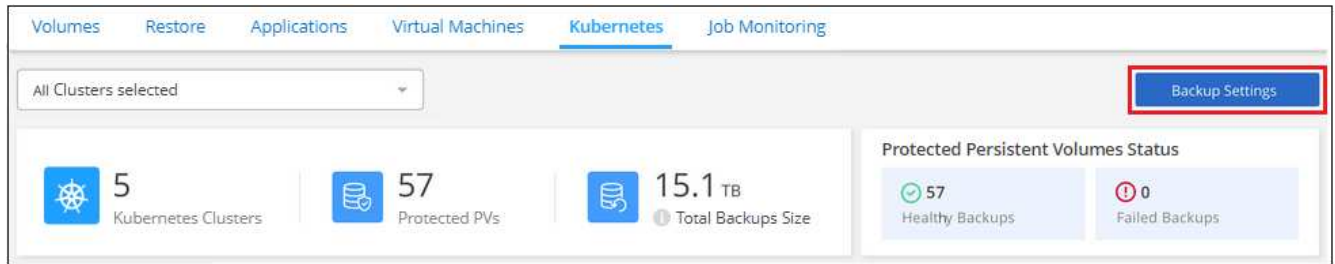
volume ou utiliser le filtre de recherche.

## Activation et désactivation des sauvegardes des volumes

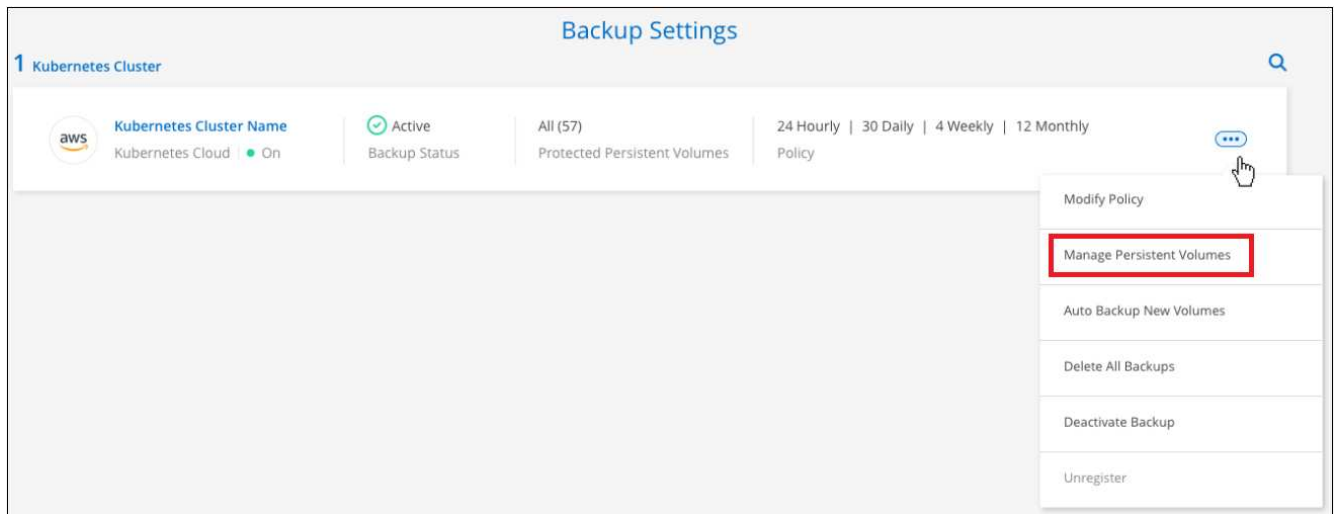
Vous pouvez arrêter la sauvegarde d'un volume si vous n'avez pas besoin de copies de sauvegarde de ce volume et si vous ne voulez pas payer pour le coût de stockage des sauvegardes. Vous pouvez également ajouter un nouveau volume à la liste des sauvegardes si ce n'est pas actuellement le cas.

### Étapes

1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour le cluster Kubernetes et sélectionnez **gérer les volumes persistants**.



3. Cochez la case d'un volume ou des volumes que vous souhaitez modifier, puis cliquez sur **Activer** ou sur **Désactiver** selon que vous souhaitez démarrer ou arrêter les sauvegardes du volume.

Manage Volumes							
60 Volumes		Working Environment: CVO_Eng		<input type="text"/> <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Change Policy"/>			
<input type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Policy	Backup Status	Modified
<input checked="" type="checkbox"/>	Volume_1 ● On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	● Active	
<input type="checkbox"/>	Volume_2 ● On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	● Active	
<input checked="" type="checkbox"/>	Volume_3 ● On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	● Active	
<input type="checkbox"/>	Volume_4 ● On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	● Active	
1 - 50 of 500 < 1 >							

4. Cliquez sur **Enregistrer** pour valider vos modifications.

**Remarque :** lors de l'arrêt de la sauvegarde d'un volume, vous continuerez à être facturé par votre fournisseur de cloud pour les coûts de stockage objet pour la capacité que les sauvegardes utilisent, sauf si vous [supprimez les sauvegardes](#).

## Modification d'une stratégie de sauvegarde existante

Vous pouvez modifier les attributs d'une stratégie de sauvegarde actuellement appliquée aux volumes d'un environnement de travail. La modification de la stratégie de sauvegarde affecte tous les volumes existants utilisant la règle.

### Étapes

1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

All Clusters selected

Backup Settings

5

Kubernetes Clusters

57

Protected PVs

15.1 TB

Total Backups Size

Protected Persistent Volumes Status

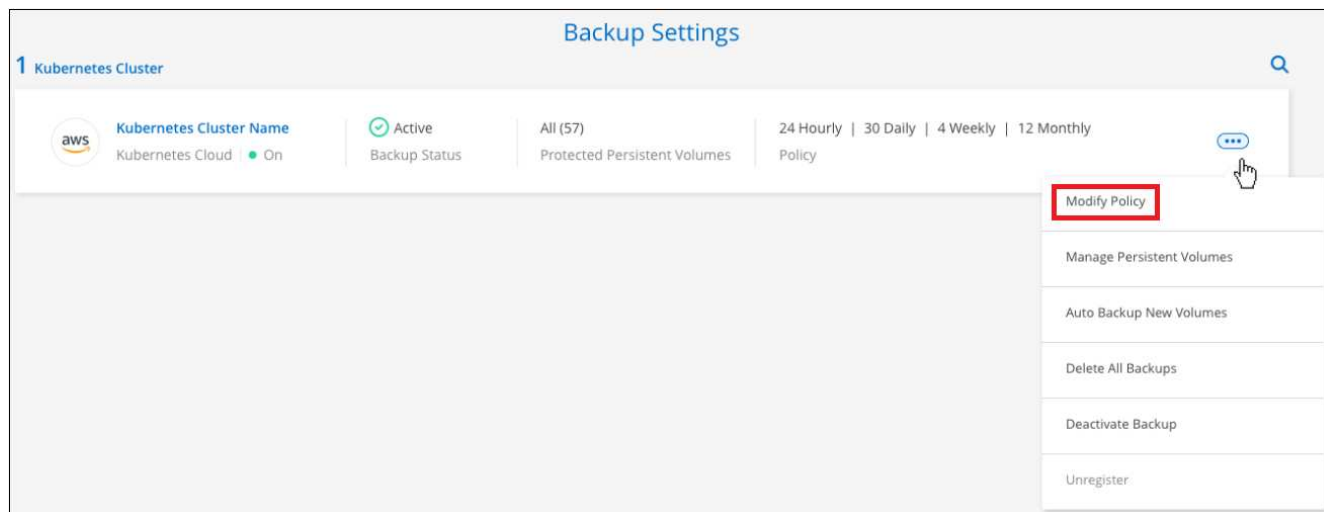
57

Healthy Backups

0

Failed Backups

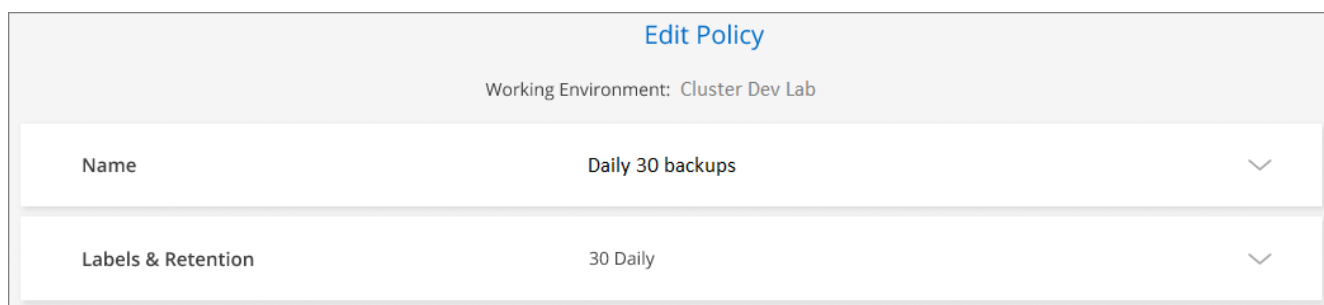
2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail dans lequel vous souhaitez modifier les paramètres, sélectionnez **gérer les stratégies**.



3. Dans la page *Manage Policies*, cliquez sur **Edit Policy** pour la stratégie de sauvegarde que vous souhaitez modifier dans cet environnement de travail.



4. Dans la page *Edit Policy*, modifiez la planification et la rétention des sauvegardes et cliquez sur **Save**.



## Définition d'une stratégie de sauvegarde à attribuer aux nouveaux volumes

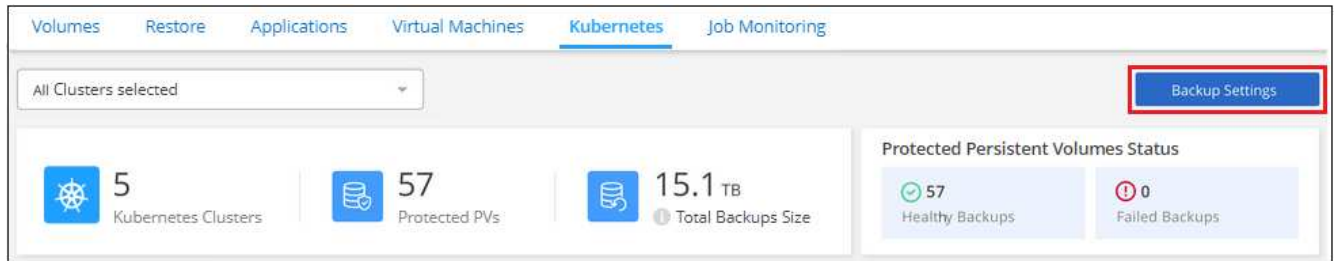
Si vous n'avez pas sélectionné l'option permettant d'attribuer automatiquement une stratégie de sauvegarde aux volumes nouvellement créés lorsque vous avez activé Cloud Backup pour la première fois sur votre cluster Kubernetes, vous pouvez choisir cette option ultérieurement dans la page *Backup Settings*. L'affectation d'une règle de sauvegarde aux nouveaux volumes permet de garantir la protection de toutes vos données.

Notez que la règle que vous souhaitez appliquer aux volumes doit déjà exister. [Découvrez comment ajouter une nouvelle stratégie de sauvegarde pour un environnement de travail.](#)

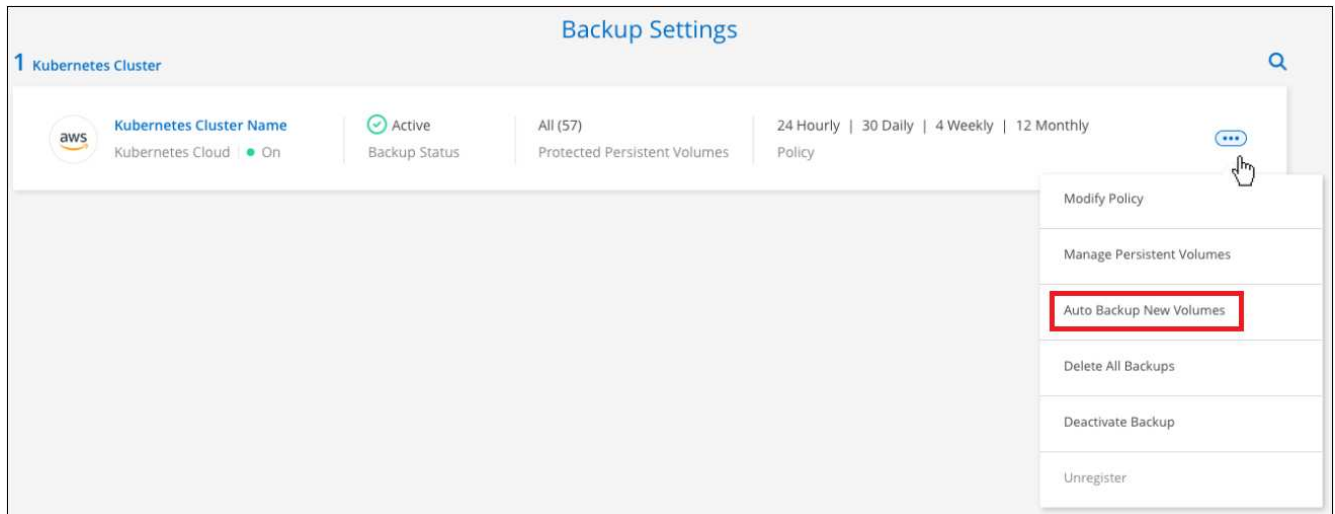
Vous pouvez également désactiver ce paramètre afin que les volumes nouvellement créés ne soient pas sauvegardés automatiquement. Dans ce cas, vous devrez activer manuellement les sauvegardes pour tous les volumes que vous souhaitez effectuer ultérieurement.

## Étapes

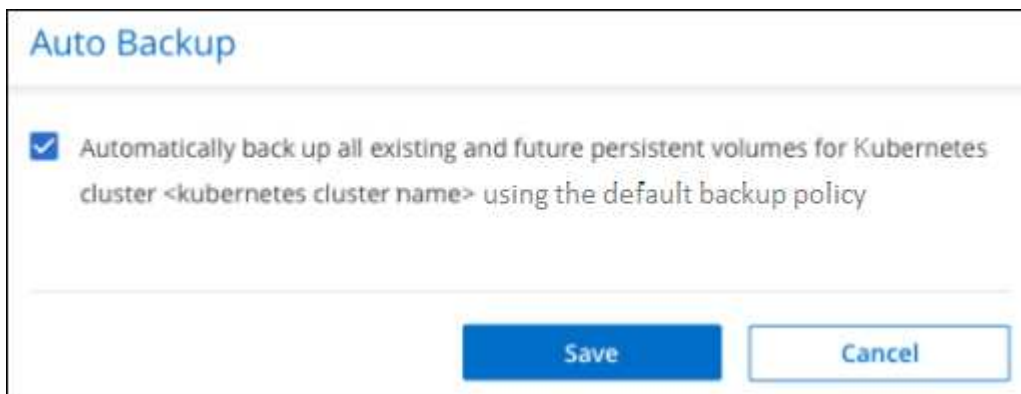
1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour le cluster Kubernetes où les volumes existent, sélectionnez **sauvegarde automatique de nouveaux volumes**.



3. Cochez la case « sauvegarde automatique des volumes persistants futurs... », choisissez la stratégie de sauvegarde que vous souhaitez appliquer aux nouveaux volumes, puis cliquez sur **Enregistrer**.



## Résultat

Désormais, cette règle de sauvegarde sera appliquée à tout nouveau volume créé dans ce cluster Kubernetes.

## Affichage de la liste des sauvegardes pour chaque volume

Vous pouvez afficher la liste de tous les fichiers de sauvegarde existants pour chaque volume. Cette page affiche des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde, tels que la dernière sauvegarde effectuée, la stratégie de sauvegarde actuelle, la taille du fichier de sauvegarde, etc.

Cette page permet également d'effectuer les tâches suivantes :

- Supprimez tous les fichiers de sauvegarde du volume
- Supprimez les fichiers de sauvegarde individuels du volume
- Téléchargez un rapport de sauvegarde pour le volume

### Étapes

1. Dans l'onglet **Kubernetes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

The screenshot shows the 'Backup & Restore' interface with the 'Kubernetes' tab selected. At the top, there are navigation tabs: 'Backup & Restore', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below these, there's a summary section with three cards: '1 Kubernetes Clusters', '57 Protected PVs', and '15.1 TB Total Backups Size'. To the right, a 'Protected Persistent Volumes Status' box shows '57 Healthy Backup' and '0 Failed Backup'. Below this, a table lists 57 backups. The table has columns: 'Source Kubernetes Cluster', 'Source Persistent Volume', 'Source Namespace', 'Last Backup', 'Backups', and 'Backup Status'. The first three rows show 'Kubernetes\_Cloud\_AWS' as the source cluster, 'Source Persistent Volume' as the source PV, and 'Source Namespace' as the source namespace. The 'Last Backup' column shows 'May 22 2019, 00:00:00'. The 'Backups' column shows '2,050 Backups' for the first row and '2,050 Snapshot' for the others. The 'Backup Status' column shows 'Active' for the first row. A dropdown menu is open for the first row, showing options: 'Details & Backup List', 'Backup Now', and 'Pause Backups'.

Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	

La liste de tous les fichiers de sauvegarde s'affiche avec des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde.



Source

Kubernetes Cluster: eks1
Type: EKS
Provider: AWS
Persistent Volume: pvc-05881c70-cf5f-4edc-8537...
Namespace: default

Destination

Cloud Provider: AWS
Bucket: netapp-backup-vsa5twmc9ae
Region: us-west-1
Account ID: 123456789012

Backup Information

Relationship Status: enabled
Last Backup: Dec 07 2021, 2:20:30 pm
Lag Duration: 1 hour
Backups: 2
Backup Policy: 24 hourly | 30 daily | 52 weekly

2 Backups

Backup Name	Date	Size	
daily-dem-163887957011628bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:19:30 pm	9.77 KB	
daily-dem-163887963015128bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:20:30 pm	9.77 KB	Restore

## Suppression de sauvegardes

Cloud Backup vous permet de supprimer un seul fichier de sauvegarde, de supprimer toutes les sauvegardes d'un volume ou de supprimer toutes les sauvegardes de tous les volumes d'un cluster Kubernetes. Vous pouvez supprimer toutes les sauvegardes si vous n'avez plus besoin des sauvegardes ou si vous avez supprimé le volume source et que vous souhaitez supprimer toutes les sauvegardes.



Si vous prévoyez de supprimer un environnement ou un cluster de travail qui dispose de sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. Cloud Backup ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système et l'interface utilisateur ne prend pas en charge la suppression des sauvegardes après la suppression du système. Vous continuerez d'être facturé pour les coûts de stockage objet pour les sauvegardes restantes.

## Suppression de tous les fichiers de sauvegarde d'un environnement de travail

La suppression de toutes les sauvegardes d'un environnement de travail ne désactive pas les futures sauvegardes des volumes de cet environnement de travail. Si vous souhaitez arrêter la création de sauvegardes de tous les volumes d'un environnement de travail, vous pouvez désactiver les sauvegardes [comme décrit ici](#).

### Étapes

1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.

Volumes
Restore
Applications
Virtual Machines
**Kubernetes**
Job Monitoring

All Clusters selected

Backup Settings

5
Kubernetes Clusters

57
Protected PVs

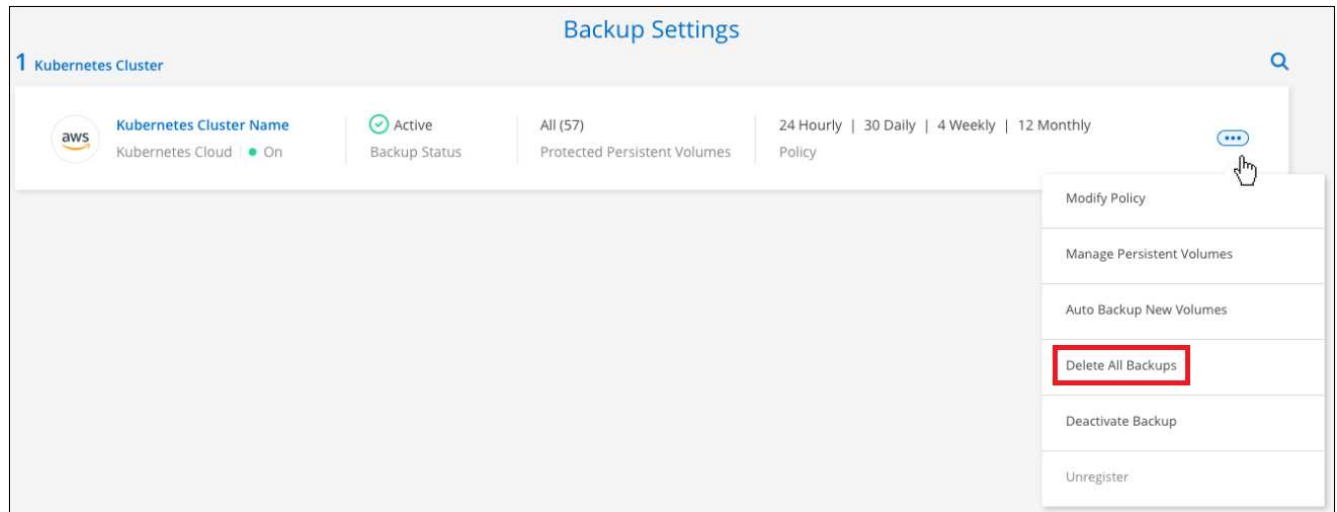
15.1 TB
Total Backups Size

Protected Persistent Volumes Status

57
Healthy Backups

0
Failed Backups

2. Cliquez sur ... Pour le cluster Kubernetes où vous voulez supprimer toutes les sauvegardes et sélectionnez **Supprimer toutes les sauvegardes**.



3. Dans la boîte de dialogue de confirmation, entrez le nom de l'environnement de travail et cliquez sur **Supprimer**.

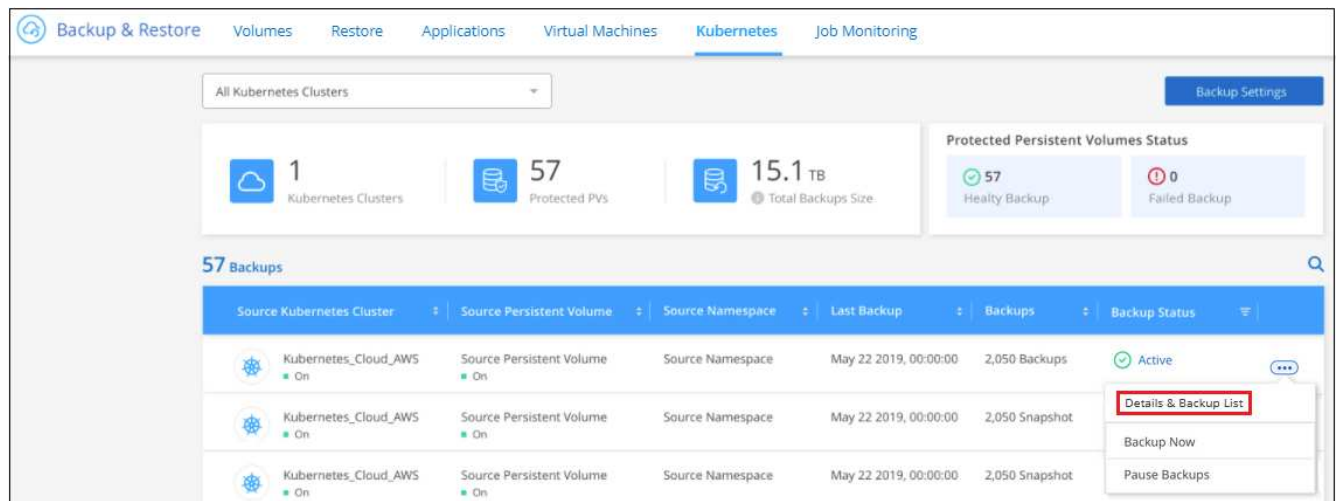
### Suppression de tous les fichiers de sauvegarde d'un volume

La suppression de toutes les sauvegardes d'un volume désactive également les futures sauvegardes de ce volume.

C'est possible [relancez les sauvegardes pour le volume](#) À tout moment à partir de la page gérer les sauvegardes.

### Étapes

1. Dans l'onglet **Kubernetes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.



La liste de tous les fichiers de sauvegarde s'affiche.

The screenshot displays the NetApp backup management interface. It is divided into three main sections: Source, Destination, and Backup Information.

- Source:**
  - Working Environment: Working Environment N...
  - Type: Cloud Volumes ONTAP (HA)
  - Provider: AWS
  - Volume: Volume Name
  - SVM: SVM Name
- Destination:**
  - Cloud Provider: AWS
  - Region: us-east-1
  - Bucket: netapp-backup
  - Account ID: 012345678901234567890
- Backup Information:**
  - Relationship Status: Active
  - Last Backup: Oct 05 2021, 2:41:33 pm
  - Lag Duration: 14 days 3 hours, 38 mi...
  - Backups: 2,050
  - Backup Policy: Netapp7YearsRetention

Below these sections, there is a table titled "2,050 Backups". The table has columns for Backup Name, Date, and Size. The first three rows are visible:

Backup Name	Date	Size
Backup_2020_Jan	May 22 2019, 00:00:00	19,001
Backup_2020_Mar	May 22 2019, 00:00:00	19,002
Backup_2020_Apr	May 22 2019, 00:00:00	19,009

2. Cliquez sur **actions** > **Supprimer toutes les sauvegardes**.

The screenshot shows the "2,050 Backups" table with the "Actions" menu open. The "Delete All Backups" option is highlighted with a red box. The "Download Backup Report" option is also visible below it.

3. Dans la boîte de dialogue de confirmation, entrez le nom du volume et cliquez sur **Supprimer**.

### Suppression d'un fichier de sauvegarde unique pour un volume

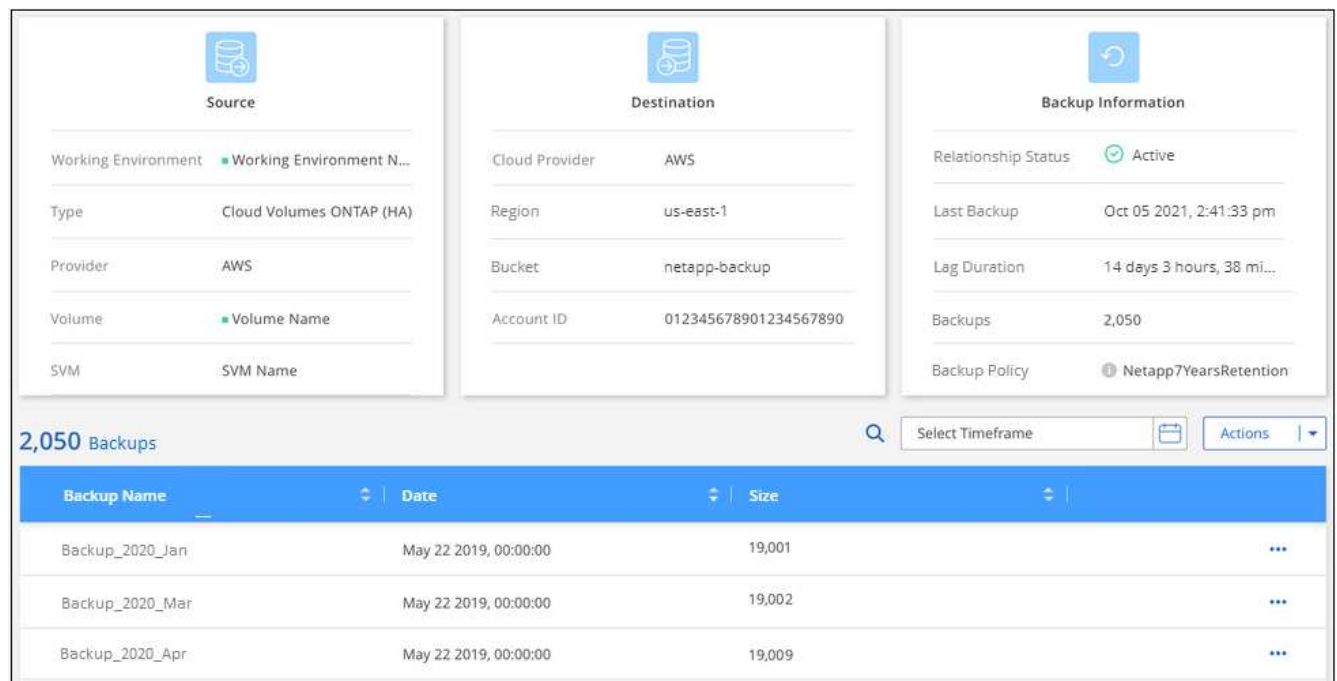
Vous pouvez supprimer un seul fichier de sauvegarde. Cette fonctionnalité n'est disponible que si la sauvegarde du volume a été créée à partir d'un système avec ONTAP 9.8 ou version ultérieure.

#### Étapes

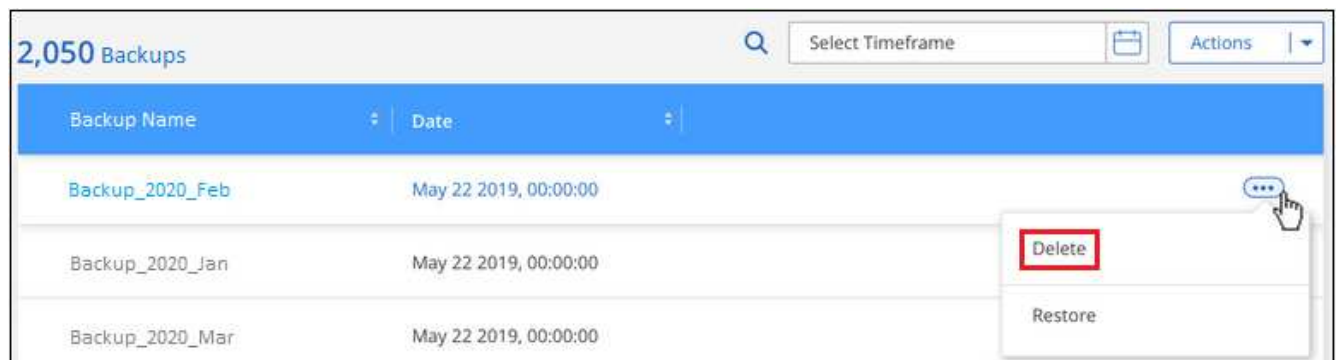
1. Dans l'onglet **Kubernetes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.



La liste de tous les fichiers de sauvegarde s'affiche.



2. Cliquez sur ... Pour le fichier de sauvegarde de volume que vous souhaitez supprimer, cliquez sur **Supprimer**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

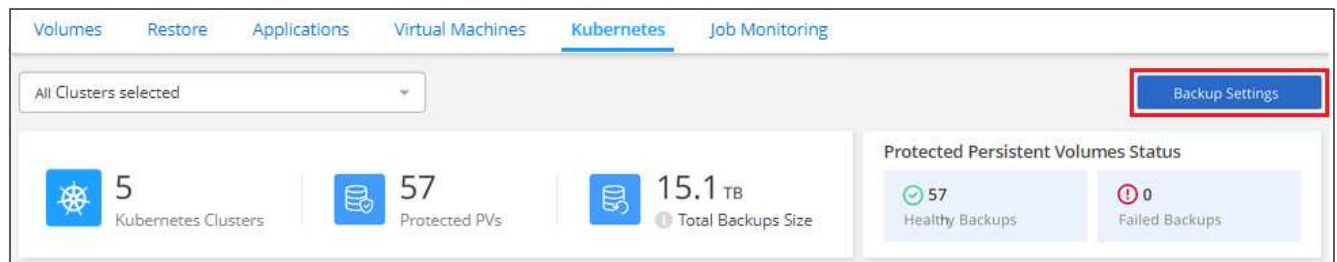
## Désactivation de Cloud Backup pour un environnement de travail

La désactivation de Cloud Backup pour un environnement de travail désactive les sauvegardes de chaque volume du système. Elle désactive également la restauration d'un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne désinscrit pas le service de sauvegarde de cet environnement de travail, car il vous permet de suspendre l'ensemble de l'activité de sauvegarde et de restauration pendant une période donnée.

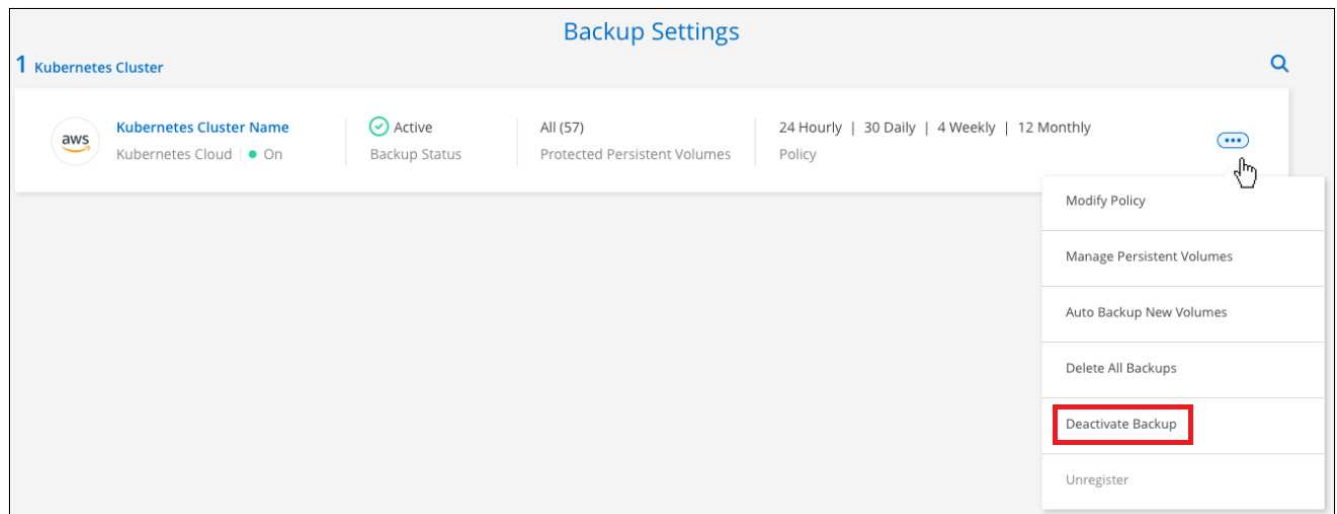
Notez que vous continuerez d'être facturé par votre fournisseur cloud pour les coûts de stockage objet correspondant à la capacité que vos sauvegardes utilisent, sauf si vous [supprimez les sauvegardes](#).

### Étapes

1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur **...** Pour l'environnement de travail ou le cluster Kubernetes, où vous souhaitez désactiver les sauvegardes et sélectionner **Désactiver la sauvegarde**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Désactiver**.



Un bouton **Activer la sauvegarde** apparaît pour cet environnement de travail alors que la sauvegarde est désactivée. Vous pouvez cliquer sur ce bouton lorsque vous souhaitez réactiver la fonctionnalité de sauvegarde pour cet environnement de travail.

## Annulation de l'enregistrement de Cloud Backup pour un environnement de travail

Vous pouvez annuler l'enregistrement de Cloud Backup pour un environnement de travail si vous ne souhaitez plus utiliser la fonctionnalité de sauvegarde et que vous souhaitez interrompre la facturation des sauvegardes dans cet environnement de travail. Cette fonctionnalité est généralement utilisée lorsque vous prévoyez de supprimer un cluster Kubernetes et que vous souhaitez annuler le service de sauvegarde.

Vous pouvez également utiliser cette fonction si vous souhaitez modifier le magasin d'objets de destination dans lequel vos sauvegardes de cluster sont stockées. Une fois que vous désenregistrez Cloud Backup pour l'environnement de travail, vous pouvez activer Cloud Backup pour ce cluster en utilisant les informations du nouveau fournisseur cloud.

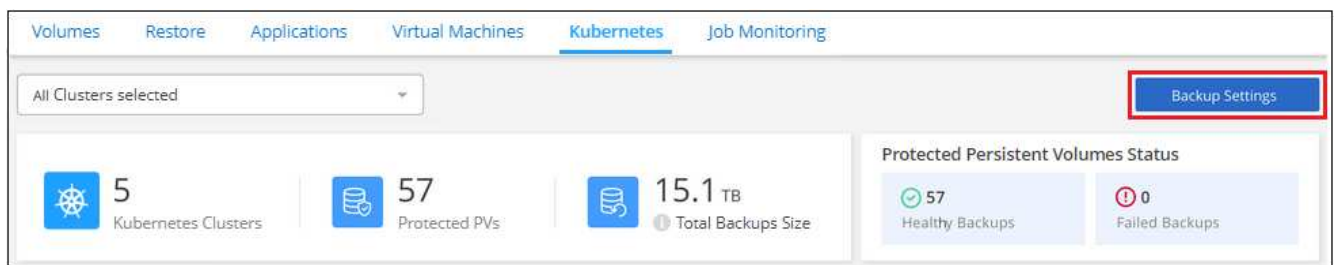
Avant de pouvoir annuler l'enregistrement de Cloud Backup, vous devez effectuer les opérations suivantes dans cet ordre :

- Désactivez Cloud Backup pour l'environnement de travail
- Supprimer toutes les sauvegardes de cet environnement de travail

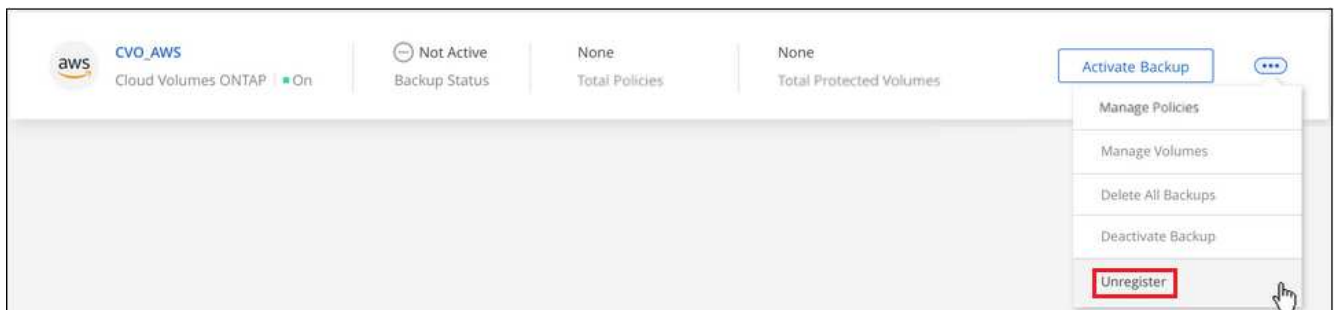
L'option de désenregistrer n'est pas disponible tant que ces deux actions ne sont pas terminées.

## Étapes

1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour le cluster Kubernetes où vous souhaitez annuler l'enregistrement du service de sauvegarde et sélectionnez **Unregister**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Annuler l'enregistrement**.

## Restauration de données Kubernetes à partir de fichiers de sauvegarde

Les sauvegardes sont stockées dans un magasin d'objets de votre compte cloud, de sorte que vous puissiez restaurer les données à partir d'un point dans le temps spécifique. Vous pouvez restaurer un volume persistant Kubernetes entier à partir d'un fichier de sauvegarde enregistré.

Vous pouvez restaurer un volume persistant (comme un nouveau volume) vers le même environnement de travail ou vers un autre environnement de travail qui utilise le même compte cloud.

## Environnements de travail et fournisseurs de stockage objet pris en charge

Vous pouvez restaurer un volume à partir d'un fichier de sauvegarde Kubernetes vers les environnements de travail suivants :

Emplacement du fichier de sauvegarde	Destination Environnement de travail
Amazon S3	Cluster Kubernetes dans AWS Cluster Kubernetes dans Azure
Blob d'Azure	Cluster Kubernetes dans Azure
Google Cloud Storage	Cluster Kubernetes dans Google

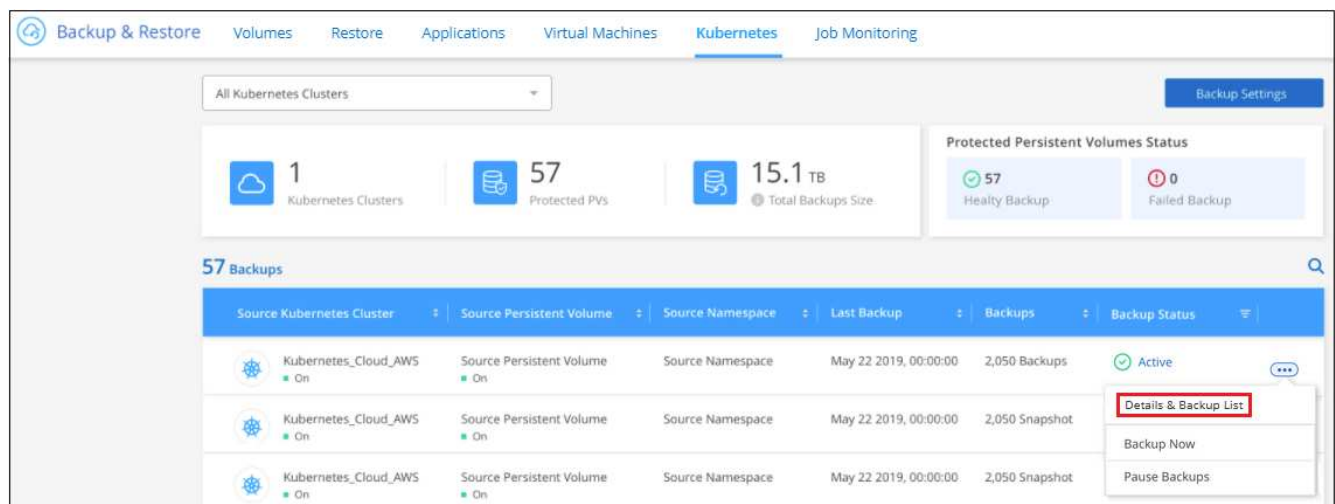
## Restauration de volumes à partir d'un fichier de sauvegarde Kubernetes

Lorsque vous restaurez un volume persistant à partir d'un fichier de sauvegarde, BlueXP crée un *nouveau* volume en utilisant les données de la sauvegarde. Vous pouvez restaurer les données sur un volume du même cluster Kubernetes ou sur un autre cluster Kubernetes situé dans le même compte cloud que le cluster Kubernetes source.

Avant de commencer, vous devez connaître le nom du volume que vous souhaitez restaurer et la date du fichier de sauvegarde que vous souhaitez utiliser pour créer le volume récemment restauré.

### Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Kubernetes** pour afficher le tableau de bord Kubernetes.



3. Recherchez le volume à restaurer, cliquez sur **...**, Puis cliquez sur **Détails et liste de sauvegarde**.

La liste de tous les fichiers de sauvegarde de ce volume s'affiche avec des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde.



**Source**

Kubernetes Cluster: eks1

Type: EKS

Provider: AWS

Persistent Volume: pvc-05881c70-cf5f-4edc-8537...

Namespace: default

**Destination**

Cloud Provider: AWS

Bucket: netapp-backup-vsa5twmc9ae

Region: us-west-1

Account ID: 123456789012

**Backup Information**

Relationship Status: enabled

Last Backup: Dec 07 2021, 2:20:30 pm

Lag Duration: 1 hour

Backups: 2

Backup Policy: 24 hourly | 30 daily | 52 weekly

**2 Backups**

Backup Name	Date	Size	
daily.dem-163887957011628bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:19:30 pm	9.77 KB	...
daily.dem-163887963015128bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:20:30 pm	9.77 KB	Restore

- Recherchez le fichier de sauvegarde spécifique à restaurer en fonction de l'horodatage, cliquez sur **...**, Puis **Restaurer**.
- Dans la page *Select destination*, sélectionnez la *Kubernetes cluster* où vous voulez restaurer le volume, la *namespace*, la *Storage Class* et le nouveau *persistent volume name*.

**Select Destination**

Select Kubernetes Cluster: eks1

Namespace: default

Storage Class: basic

PVC Name: pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1-restoi

Cancel Restore

- Cliquez sur **Restore** et vous revenez au tableau de bord Kubernetes pour vérifier la progression de l'opération de restauration.

## Résultat

BlueXP crée un nouveau volume dans le cluster Kubernetes en fonction de la sauvegarde que vous avez sélectionnée. C'est possible "gérez les paramètres de sauvegarde de ce nouveau volume" selon les besoins.

# 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

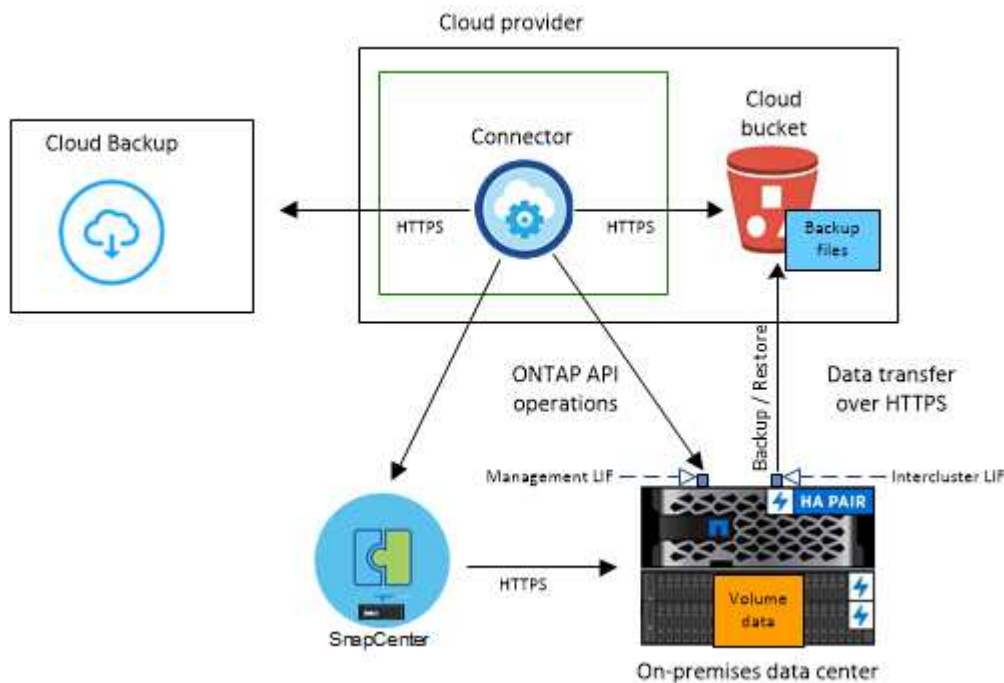
Avant de commencer à sauvegarder les données applicatives sur les services cloud, lisez les informations qui suivent pour vous assurer que la configuration est prise en charge.

- 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.

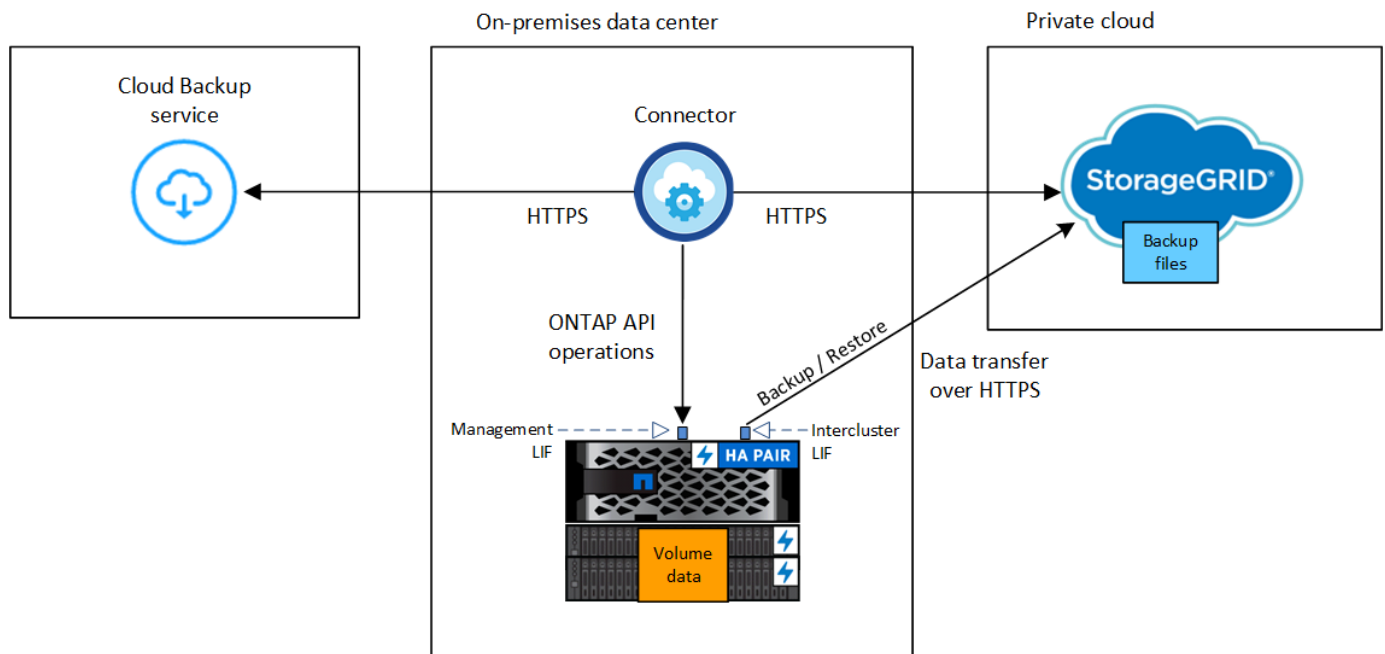


Cloud Backup pour les applications ne prend pas en charge la protection des applications qui se trouvent sur des SVM ajoutés avec un FQDN ou une adresse IP.

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 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 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 **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 <b>tous les journaux</b> .
Que vous souhaitez récupérer à un numéro de changement de système (SCN) spécifique	Sélectionnez <b>jusqu'à ce que SCN (numéro de changement du système)</b> .
Veulent restaurer des données et un temps spécifique	Sélectionnez <b>Date et heure</b> .  Vous devez spécifier la date et l'heure du fuseau horaire de l'hôte de la base de données.
Ne pas récupérer	Sélectionnez <b>pas de récupération</b> .
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 <b>Restaurer la base de données sur un autre hôte</b> 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.

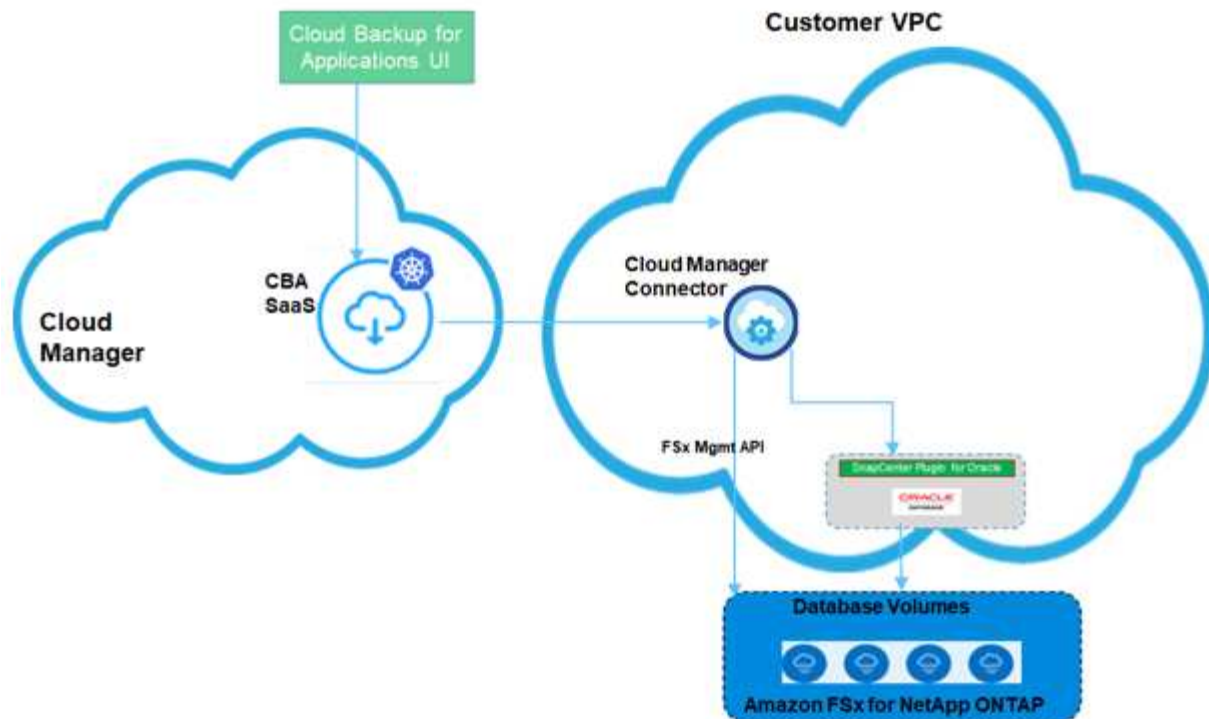
- L'interface utilisateur Cloud Backup pour applications est intégrée à l'interface utilisateur BlueXP.

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 -srcaalias 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 <https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/gcp/Configurer les informations d'identification de la base de données Oracle>.
  - 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 certificat.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 :

- Accédez au dossier contenant le magasin de clés de la SPL `/var/opt/snapcenter/spl/etc`.
- 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 :

- Connectez-vous au connecteur en tant qu'utilisateur non-root.
- 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

- 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 cliquer 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 <b>tous les fichiers de données</b> .
Vous souhaitez restaurer uniquement les fichiers de contrôle	Sélectionnez <b>fichiers de contrôle</b>
Veulent restaurer à la fois les fichiers de données et les fichiers de contrôle	Sélectionnez <b>tous les fichiers de données et fichiers de contrôle</b> .



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 <b>tous les journaux</b> .
Que vous souhaitez récupérer à un numéro de changement de système (SCN) spécifique	Sélectionnez <b>jusqu'à ce que Numéro de changement de système</b> et spécifiez le SCN.
Vous souhaitez effectuer une restauration à une date et une heure précises	Sélectionnez <b>Date et heure</b> .
Ne pas récupérer	Sélectionnez <b>pas de récupération</b> .

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**.

# Sauvegarde et restauration des données des ordinateurs virtuels

## Protection des données des machines virtuelles

Vous pouvez protéger les données stockées sur vos machines virtuelles en intégrant le plug-in SnapCenter pour VMware vSphere à BlueXP (anciennement Cloud Manager). Vous pouvez sauvegarder des datastores dans le cloud et restaurer facilement les serveurs virtuels depuis le plug-in SnapCenter sur site pour VMware vSphere.

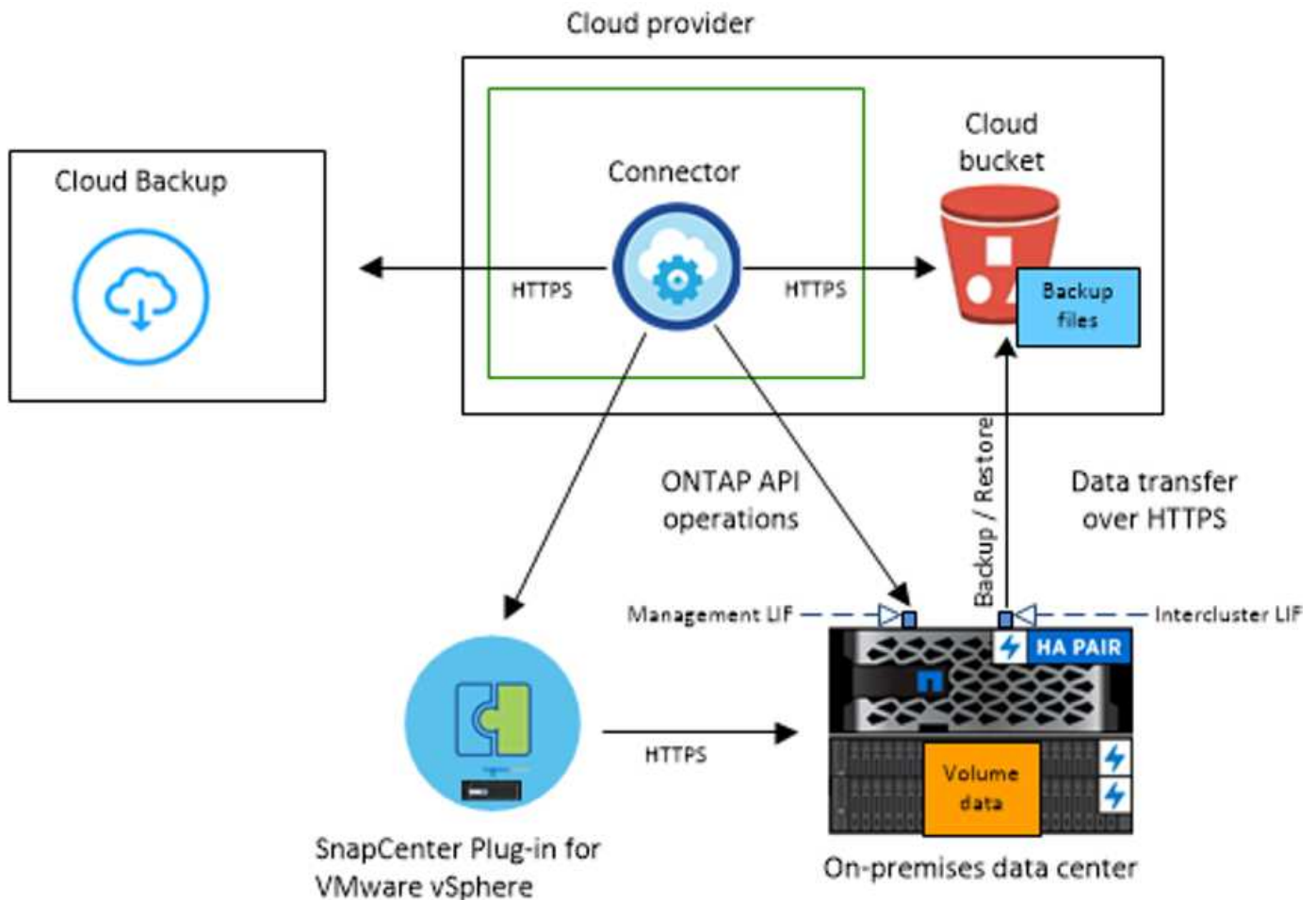
Vous pouvez sauvegarder des datastores Amazon Web Services S3, Microsoft Azure Blob et StorageGRID.

### De formation

Avant de commencer à sauvegarder des datastores et des machines virtuelles sur des services cloud, lisez les éléments suivants pour vous assurer que la configuration est prise en charge.

- Plug-in SnapCenter pour VMware vSphere 4.6P1 ou version ultérieure
- ONTAP 9.8 ou version ultérieure
- BlueXP 3.9 ou version ultérieure
- Au moins une sauvegarde doit avoir été incluse dans le plug-in SnapCenter pour VMware vSphere 4.6P1.
- Au moins une règle quotidienne, hebdomadaire ou mensuelle du plug-in SnapCenter pour VMware vSphere sans étiquette ni même étiquette que la politique de Cloud Backup pour machines virtuelles dans BlueXP.
- Dans le cas d'une règle prédéfinie, le niveau de planification doit être le même pour le datastore dans le plug-in SnapCenter pour VMware vSphere et dans le cloud.
- Assurez-vous qu'il n'y a pas de volumes FlexGroup dans le datastore, car la sauvegarde et la restauration des volumes FlexGroup ne sont pas prises en charge.
- Assurez-vous qu'aucun volume n'est chiffré car la restauration des volumes chiffrés n'est pas prise en charge.
- Désactivez "**\_Recent**" sur les groupes de ressources requis. Si « **\_Recent** » est activé pour le groupe de ressources, les sauvegardes de ces groupes de ressources ne peuvent pas être utilisées pour la protection des données dans le cloud et ne peuvent plus être utilisées pour l'opération de restauration.
- Assurez-vous que le datastore de destination sur lequel la machine virtuelle sera restaurée dispose d'un espace suffisant pour prendre en charge une copie de tous les fichiers des machines virtuelles tels que VMDK, VMX, VMDSX, etc.
- Assurez-vous que le datastore de destination ne contient pas de fichiers de machine virtuelle obsolètes au format restore\_XXX\_filename des échecs précédents de l'opération de restauration. Vous devez supprimer les fichiers obsolètes avant de lancer une opération de restauration.

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



## Enregistrez le plug-in SnapCenter pour VMware vSphere

Nous vous recommandons d'enregistrer le plug-in SnapCenter pour VMware vSphere dans BlueXP pour les datastores et les machines virtuelles à afficher dans BlueXP. Seul un utilisateur disposant d'un accès administratif peut enregistrer le plug-in SnapCenter pour VMware vSphere.



Vous pouvez enregistrer plusieurs plug-in SnapCenter pour VMware vSphere. Cependant, une fois enregistré, vous ne pouvez pas supprimer le plug-in SnapCenter pour VMware vSphere.

### Étapes

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

Assurez-vous que le port est ouvert pour la communication entre le plug-in SnapCenter pour VMware vSphere et Cloud Backup pour les machines virtuelles.

- c. Dans le champ Nom d'utilisateur et Mot de passe, indiquez les informations d'identification de l'utilisateur ayant le rôle d'administrateur.

5. Cliquez sur **Enregistrer**.

### Après la fin

Cliquez sur **sauvegarde et restauration > machines virtuelles** pour afficher tous les datastores et toutes les machines virtuelles qui peuvent être protégés à l'aide du plug-in SnapCenter enregistré pour VMware vSphere.

## Créez une règle pour sauvegarder des machines virtuelles

Vous pouvez créer une stratégie ou utiliser l'une des stratégies prédéfinies suivantes disponibles dans BlueXP.

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

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

### Étapes

1. Sur la page machines virtuelles, dans la liste déroulante Paramètres, sélectionnez **stratégies**.
2. Cliquez sur **Créer une stratégie**.
3. Spécifiez un nom de stratégie.
4. Spécifiez la planification et les informations de conservation.

Par défaut, la source de sauvegarde est sélectionnée comme source principale.

5. Cliquez sur **Créer**.

## Sauvegarde des datastores sur StorageGRID

Vous pouvez sauvegarder un ou plusieurs datastores sur StorageGRID en intégrant le plug-in SnapCenter pour VMware vSphere à BlueXP. Ils peuvent ainsi sauvegarder et archiver des données facilement et rapidement à des fins d'efficacité du stockage et d'accélération de la transition vers le cloud.



Assurez-vous que vous avez rempli toutes les "de formation" avant de sauvegarder des datastores dans le cloud.

## Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > machines virtuelles**.
2. Cliquez sur **...** Correspondant au datastore à sauvegarder 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 les clusters ONTAP que vous souhaitez que BlueXP découvre pour sauvegarder vos datastores. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

- a. Cliquez sur **Ajouter un environnement de travail** correspondant à la SVM.
  - b. Dans l'assistant Ajouter un environnement de travail :
    - i. Spécifier l'adresse IP du cluster ONTAP
    - ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
  - c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **StorageGRID**.
    - a. Spécifiez l'adresse IP du serveur de stockage.
    - b. Sélectionnez la clé d'accès et la clé secrète.
  6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

## Gérer la protection des machines virtuelles

Vous pouvez afficher les règles, les datastores et les machines virtuelles avant de sauvegarder et de restaurer des données. En fonction des modifications apportées à la base de données, aux stratégies ou aux groupes de ressources, vous pouvez actualiser les mises à jour à partir de l'interface utilisateur BlueXP.

### Afficher les règles

Vous pouvez afficher toutes les règles prédéfinies par défaut. Pour chacune de ces règles, lorsque vous affichez les détails, toutes les stratégies Cloud Backup pour les machines virtuelles associées et toutes les machines virtuelles associées sont répertoriées.

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > machines virtuelles**.
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 règles de Cloud Backup pour machines virtuelles associées et toutes les machines virtuelles sont répertoriées.



## Afficher les datastores et les machines virtuelles

Les datastores et les machines virtuelles protégés à l'aide du plug-in SnapCenter enregistré pour VMware vSphere sont affichés.

### À propos de cette tâche

- Seuls les datastores NFS sont affichés.
- Seuls les datastores pour lesquels au moins une sauvegarde réussie a été effectuée dans le plug-in SnapCenter pour VMware vSphere sont affichés.

### Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > machines virtuelles > Paramètres > SnapCenter Plug-in pour VMware vSphere**.
2. Cliquez sur le plug-in SnapCenter pour VMware vSphere pour lequel vous souhaitez voir les datastores et les machines virtuelles.

## Modifiez le plug-in SnapCenter pour l'instance VMware vSphere

Vous pouvez modifier les détails du plug-in SnapCenter pour VMware vSphere dans BlueXP

### Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et récupération > machines virtuelles > Paramètres > SnapCenter Plug-in pour VMware vSphere**.
2. Cliquez sur et sélectionnez **Modifier**
3. Modifiez les détails si nécessaire
4. Cliquez sur **Enregistrer**.

## Actualiser l'état de protection

Lorsque de nouveaux volumes sont ajoutés à la base de données, ou si la règle ou le groupe de ressources est modifié, vous devez actualiser la protection.

1. Cliquez sur **sauvegarde et restauration > machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **Plug-in SnapCenter pour VMware vSphere**.
3. Cliquez sur **...** Correspondant au plug-in SnapCenter pour VMware vSphere qui héberge la machine virtuelle et cliquez sur **Refresh**.

Les nouvelles modifications sont découvertes.

4. Cliquez sur **...** Correspondant au datastore et cliquez sur **Actualiser la protection** pour activer la protection du cloud pour les modifications.

## 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.

## Restaurer des machines virtuelles à partir du cloud

Vous pouvez restaurer des machines virtuelles à partir du cloud vers vCenter sur site. La sauvegarde sera restaurée au même emplacement que celui où elle a été effectuée. Vous ne pouvez pas restaurer la sauvegarde à un autre emplacement. Vous pouvez restaurer des machines virtuelles depuis le datastore ou depuis la vue VM.



Vous ne pouvez pas restaurer des machines virtuelles qui sont fractionnés entre les datastores.

### Ce dont vous avez besoin

Assurez-vous que vous avez rempli toutes les "[de formation](#)" avant de restaurer des machines virtuelles à partir du cloud.

### Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection > sauvegarde et restauration > machines virtuelles > Plug-in SnapCenter pour VMware vSphere** et sélectionnez le plug-in SnapCenter pour VMware vSphere dont vous souhaitez restaurer la machine virtuelle.



Si la machine virtuelle source est déplacée vers un autre emplacement (vMotion) et si l'utilisateur déclenche une restauration de cette machine virtuelle depuis BlueXP, la machine virtuelle sera restaurée vers l'emplacement source d'origine à partir duquel la sauvegarde a été effectuée.

1. Pour effectuer une restauration à partir du datastore :
  - a. Cliquez sur **...** Correspondant au datastore que vous souhaitez restaurer et cliquez sur **Afficher les détails**.
  - b. Cliquez sur **Restaurer** correspondant à la sauvegarde que vous souhaitez restaurer.
  - c. Sélectionnez la machine virtuelle à restaurer à partir de la sauvegarde et cliquez sur **Suivant**.
  - d. Vérifiez les détails et cliquez sur **Restaurer**.
2. Pour restaurer à partir de machines virtuelles :
  - a. Cliquez sur **...** Correspondant à la machine virtuelle que vous souhaitez restaurer et cliquez sur **Restaurer**.
  - b. Sélectionnez la sauvegarde par laquelle vous souhaitez restaurer la machine virtuelle et cliquez sur **Suivant**.
  - c. Vérifiez les détails et cliquez sur **Restaurer**.

La machine virtuelle est restaurée au même emplacement depuis lequel la sauvegarde a été effectuée.

# API Cloud Backup

Les fonctionnalités Cloud Backup disponibles via l'interface utilisateur web sont également disponibles via l'API RESTful.

Il existe neuf catégories de terminaux définis dans Cloud Backup :

- backup : gère les opérations de sauvegarde des ressources cloud et sur site et récupère les détails des données de sauvegarde
- Catalogue : gère la recherche de fichiers dans le catalogue indexé en fonction d'une requête (recherche et restauration)
- Cloud - récupère des informations sur les différentes ressources du fournisseur de cloud à partir de BlueXP
- Jobs : gère les entrées de détail de travail dans la base de données BlueXP
- Licence - récupère la validité de la licence des environnements de travail à partir de BlueXP
- analyse par ransomware : démarre une analyse par ransomware sur un fichier de sauvegarde spécifique
- restaurer : permet d'effectuer des opérations de restauration au niveau du volume et du fichier
- sfr - récupère les fichiers d'un fichier de sauvegarde pour des opérations de restauration uniques au niveau des fichiers (Browse & Restore)
- environnement de travail : gère les stratégies de sauvegarde et configure le magasin d'objets de destination associé à un environnement de travail

## Pour commencer

Pour commencer à utiliser les API Cloud Backup, vous devez obtenir un jeton utilisateur, votre identifiant de compte BlueXP et l'ID connecteur BlueXP.

Lorsque vous passez des appels API, vous ajoutez le jeton utilisateur dans l'en-tête autorisation et l'ID connecteur BlueXP dans l'en-tête x-agent-ID. Vous devez utiliser l'ID de compte BlueXP dans les API.

### Étapes

1. Procurez-vous un jeton utilisateur sur le site Web NetApp BlueXP.

Veillez à générer le jeton de rafraîchissement à partir du lien suivant : <https://services.cloud.netapp.com/refresh-token/>. Le jeton d'actualisation est une chaîne alphanumérique que vous utiliserez pour générer un jeton utilisateur.

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
  "grant_type": "refresh_token",
  "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
  "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```



Le token utilisateur du site Web BlueXP a une date d'expiration. La réponse de l'API inclut un champ "expire\_in" qui indique la date d'expiration du jeton. Pour actualiser le token, vous devez à nouveau appeler cette API.

## 2. Obtenez votre identifiant de compte BlueXP.

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.....
```

Cette API renvoie une réponse comme suit. Vous pouvez récupérer l'ID de compte en analysant la sortie à partir de **[0].[accountPublicId]**.

```
[{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}].....
```

## 3. Procurez-vous l'ID-agent-x qui contient l'ID du connecteur BlueXP.

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
-H 'authority: api.services.cloud.netapp.com' \
-H 'accept: application/json' \
-H 'accept-language: en-GB,en;q=0.9' \
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5.....
```

Cette API renvoie une réponse comme suit. Vous pouvez récupérer l'ID de l'agent en analysant la sortie à partir de **ocm.[0].[agent].[agentID]**.

```
{
  "occms": [
    {
      "account": "account-OOnAR4ZS",
      "accountName": "cbs",
      "occm": "imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
      "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
      "status": "ready",
      "occmName": "cbsgcpdevcntsg-asia",
      "primaryCallbackUri": "http://34.93.197.21",
      "manualOverrideUris": [],
      "automaticCallbackUris": [
        "http://34.93.197.21",
        "http://34.93.197.21/occmui",
        "https://34.93.197.21",
        "https://34.93.197.21/occmui",
        "http://10.138.0.16",
        "http://10.138.0.16/occmui",
        "https://10.138.0.16",
        "https://10.138.0.16/occmui",
        "http://localhost",
        "http://localhost/occmui",
        "http://localhost:1337",
        "http://localhost:1337/occmui",
        "https://localhost",
        "https://localhost/occmui",
        "https://localhost:1337",
        "https://localhost:1337/occmui"
      ],
      "createDate": "1652120369286",
      "agent": {
        "useDockerInfra": true,
        "network": "default",
        "name": "cbsgcpdevcntsg-asia",
        "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients",
        "provider": "gcp",
        "systemId": "a3aa3578-bfee-4d16-9e10-"
      }
    }
  ]
}
```

## Exemple d'utilisation des API

L'exemple suivant montre un appel d'API pour activer Cloud Backup dans un environnement de travail avec une nouvelle règle dont les libellés sont quotidiens, horaires et hebdomadaires, archivés après les jours définis sur 180 jours, dans la région est-US-2 dans le cloud Azure. Notez que cela n'active que la sauvegarde de l'environnement de travail, mais qu'aucun volume n'est sauvegardé.

Si vous choisissez « auto-backup-enabled » : « true », tous les volumes déjà existants du système seront sauvegardés, de plus tous les volumes futurs seront également sauvegardés.

### Demande d'API

Vous verrez que nous utilisons l'ID de compte BlueXP `account-DpTFcxN3`, ID connecteur BlueXP `iZwFFeVCZjWnzG1w8RgD0QQNANZvpP7Iclients`, et jeton utilisateur Bearer `eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSx1PVFUzUWpZek1E...y6nyhBjwkeMwHc4ValobjUmju2x0xUH48g` dans cette commande.

```

curl --location --request POST
'https://api.blueexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSx1PVFUzUWpZek1E...y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
  "provider": "AZURE",
  "backup-policy": {
    "archive-after-days": 180,
    "rule": [
      {
        "label": "hourly",
        "retention": "2"
      },
      {
        "label": "daily",
        "retention": "30"
      },
      {
        "label": "weekly",
        "retention": "52"
      }
    ]
  },
  "ip-space": "Default",
  "region": "eastus2",
  "azure": {
    "resource-group": "rn-test-backup-rg",
    "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
  }
}'

```

La réponse est un ID de tâche que vous pouvez ensuite surveiller.

```

{
  "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}

```

### Surveiller la réponse.

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSx1PVFUzUWpZek1E...hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

### Réponse.

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

### Surveiller jusqu'à ce que l'état soit « TERMINÉ ».

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

## Référence API

La documentation de chaque API Cloud Backup est disponible à partir de <https://docs.netapp.com/us-en/>





# Référence

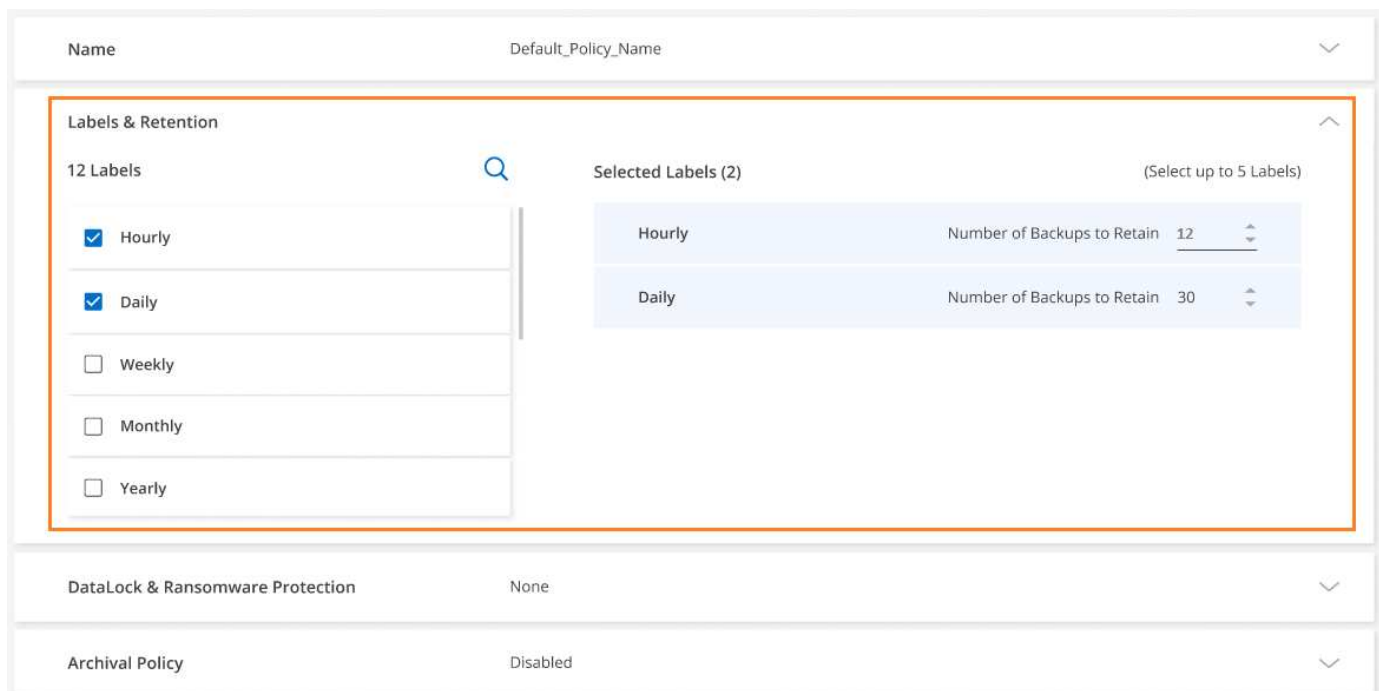
## Paramètres de configuration de la politique de Cloud Backup

Ce document décrit les paramètres de configuration de la stratégie de sauvegarde des systèmes ONTAP sur site et Cloud Volumes ONTAP utilisés avec Cloud Backup Service.

### Planifications de sauvegarde

Cloud Backup vous permet de créer plusieurs règles de sauvegarde avec des planifications uniques pour chaque environnement de travail (cluster). Vous pouvez attribuer différentes stratégies de sauvegarde à des volumes ayant différents objectifs de point de récupération (RPO).

Chaque stratégie de sauvegarde fournit une section pour *Labels & Retention* que vous pouvez appliquer à vos fichiers de sauvegarde.



Name	Default_Policy_Name
<b>Labels &amp; Retention</b>	
12 Labels	Selected Labels (2) (Select up to 5 Labels)
<input checked="" type="checkbox"/> Hourly	Hourly Number of Backups to Retain 12
<input checked="" type="checkbox"/> Daily	Daily Number of Backups to Retain 30
<input type="checkbox"/> Weekly	
<input type="checkbox"/> Monthly	
<input type="checkbox"/> Yearly	
DataLock & Ransomware Protection	None
Archival Policy	Disabled

Il y a deux parties du calendrier : l'étiquette et la valeur de conservation :

- Le **label** définit la fréquence à laquelle un fichier de sauvegarde est créé (ou mis à jour) à partir du volume. Vous pouvez sélectionner l'un des types d'étiquettes suivants :
  - Vous pouvez choisir une ou une combinaison de **horaire**, **quotidien**, **hebdomadaire**, **mensuel**, et **calendriers annuels**.
  - Vous pouvez sélectionner une des règles définies par le système qui assure la sauvegarde et la conservation pendant 3 mois, 1 an ou 7 ans.
  - Si vous avez créé des règles de protection des sauvegardes personnalisées sur le cluster à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes ONTAP, vous pouvez sélectionner l'une de ces règles.
- La valeur **rétenion** définit le nombre de fichiers de sauvegarde pour chaque étiquette (délai). Lorsque le

nombre maximal de sauvegardes est atteint dans une catégorie ou un intervalle, les anciennes sauvegardes sont supprimées afin que vous ayez toujours les sauvegardes les plus récentes. Cela vous permet également d'économiser de l'espace de stockage, car les sauvegardes obsolètes ne prennent pas toujours de l'espace dans le cloud.

Par exemple, dites que vous créez une stratégie de sauvegarde qui crée 7 sauvegardes **hebdomadaires** et 12 **mensuelles** :

- chaque semaine et chaque mois, un fichier de sauvegarde est créé pour le volume
- au cours de la 8e semaine, la première sauvegarde hebdomadaire est supprimée, et la nouvelle sauvegarde hebdomadaire est ajoutée pour la 8e semaine (pour un maximum de 7 sauvegardes hebdomadaires).
- au 13ème mois, la première sauvegarde mensuelle est supprimée, et la nouvelle sauvegarde mensuelle du 13ème mois est ajoutée (en conservant un maximum de 12 sauvegardes mensuelles)

Notez que les sauvegardes annuelles sont automatiquement supprimées du système source après leur transfert vers le stockage objet. Ce comportement par défaut peut être modifié "[Dans la page Paramètres avancés](#)" Pour l'environnement de travail.

## Protection des données par verrouillage et protection contre les ransomwares

Cloud Backup prend en charge le verrouillage des données et la protection contre les attaques par ransomware pour vos sauvegardes de volumes. Ces fonctionnalités vous permettent de verrouiller vos fichiers de sauvegarde et de les analyser afin de détecter un ransomware possible dans les fichiers de sauvegarde. Il s'agit d'un paramètre facultatif que vous pouvez définir dans vos stratégies de sauvegarde lorsque vous souhaitez bénéficier d'une protection supplémentaire pour vos sauvegardes de volume d'un cluster.

Ces deux fonctionnalités protègent vos fichiers de sauvegarde, afin que vous puissiez toujours disposer d'un fichier de sauvegarde valide à même de récupérer vos données en cas d'attaque par ransomware lorsqu'elles sont présentes sur vos données source. Il est également utile de respecter certaines exigences réglementaires dans lesquelles les sauvegardes doivent être verrouillées et conservées pendant un certain temps. Lorsque le verrouillage des données et la protection contre les attaques par ransomware sont activés, le compartiment cloud provisionné dans le cadre de l'activation de Cloud Backup active le verrouillage des objets et le contrôle des versions des objets.

Cette fonction n'assure pas la protection de vos volumes source, uniquement pour les sauvegardes de ces volumes source. Faites confiance à NetApp "[Cloud Insights et Cloud Secure](#)", ou une partie du "[Protections contre les ransomwares fournies par ONTAP](#)" pour protéger vos volumes source.



- Si vous prévoyez d'utiliser DataLock et protection contre les attaques par ransomware, vous devez l'activer lors de la création de votre première stratégie de sauvegarde et de l'activation de Cloud Backup pour ce cluster.
- Il est impossible de désactiver le verrouillage des données et la protection contre les attaques par ransomware pour un cluster après sa configuration. N'activez pas cette fonctionnalité sur un cluster pour l'essayer.

### Qu'est-ce que DataLock

DataLock protège vos fichiers de sauvegarde contre les modifications ou les suppressions pendant un certain temps. Cette fonctionnalité utilise la technologie du fournisseur de stockage objet pour le « verrouillage des objets ». La période pendant laquelle le fichier de sauvegarde est verrouillé (et conservé) est appelée période de rétention de DataLock. Il est basé sur le programme de stratégie de sauvegarde et le paramètre de conservation que vous avez définis, plus une mémoire tampon de 14 jours. Toute stratégie de rétention

DataLock inférieure à 30 jours est arrondie à 30 jours minimum.

Notez que les anciennes sauvegardes sont supprimées après l'expiration de la période de rétention de DataLock, et non après l'expiration de la période de conservation de la stratégie de sauvegarde.

Voyons quelques exemples de fonctionnement de cette méthode :

- Si vous créez un programme de sauvegarde mensuel avec 12 rétentions, chaque sauvegarde est verrouillée pendant 12 mois (plus 14 jours) avant sa suppression.
- Si vous créez une stratégie de sauvegarde qui crée 30 sauvegardes quotidiennes, 7 sauvegardes hebdomadaires et 12 sauvegardes mensuelles, trois périodes de conservation seront verrouillées. Les 30 sauvegardes quotidiennes seront conservées pendant 44 jours (30 jours plus 14 jours de mémoire tampon), les 7 sauvegardes hebdomadaires seraient conservées pendant 9 semaines (7 semaines plus 14 jours) et les 12 sauvegardes mensuelles seront conservées pendant 12 mois (plus 14 jours).
- Si vous créez un programme de sauvegarde horaire avec 24 rétentions, vous pensez peut-être que les sauvegardes sont verrouillées pendant 24 heures. Cependant, étant donné qu'elle est inférieure au minimum de 30 jours, chaque sauvegarde est verrouillée et conservée pendant 44 jours (30 jours plus 14 jours de mémoire tampon).

Dans ce dernier cas, si chaque fichier de sauvegarde est verrouillé pendant 44 jours, vous obtenez beaucoup plus de fichiers de sauvegarde qu'avec une stratégie de rétention horaire/24. En règle générale, lorsque Cloud Backup crée le 25e fichier de sauvegarde, il supprime la sauvegarde la plus ancienne pour conserver le maximum de rétentions à 24 (selon la règle). Dans ce cas, le paramètre de rétention DataLock remplace le paramètre de conservation de la stratégie de sauvegarde de votre stratégie de sauvegarde. Cela peut affecter vos coûts de stockage car vos fichiers de sauvegarde seront enregistrés dans le magasin d'objets pendant une période plus longue.

## Protection contre les ransomwares

La protection par ransomware analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware. La détection des attaques par ransomware est effectuée à l'aide d'une comparaison des checksums. Si un ransomware potentiel est identifié dans un fichier de sauvegarde par rapport au fichier de sauvegarde précédent, ce fichier de sauvegarde plus récent est remplacé par le fichier de sauvegarde le plus récent, qui ne montre aucun signe d'attaque par un ransomware. (Le fichier identifié comme ayant subi une attaque par ransomware est supprimé 1 jour après son remplacement.)

Les analyses par ransomware se produisent à 3 points lors du processus de sauvegarde et de restauration :

- Lorsqu'un fichier de sauvegarde est créé

Le scan n'est pas effectué sur le fichier de sauvegarde lors de l'écriture initiale sur le stockage cloud, mais lorsque le fichier de sauvegarde **Next** est écrit. Par exemple, si vous avez défini un programme de sauvegarde hebdomadaire pour mardi, le mardi 14, une sauvegarde est créée. Puis, mardi, une nouvelle sauvegarde est créée. Le scan par ransomware est alors exécuté sur le fichier de sauvegarde depuis le 14.

- Lorsque vous tentez de restaurer des données à partir d'un fichier de sauvegarde

Vous pouvez choisir d'exécuter une analyse avant de restaurer les données d'un fichier de sauvegarde ou d'ignorer cette analyse.

- Manuellement

Vous pouvez à tout moment exécuter une analyse de protection par ransomware à la demande pour

vérifier l'état d'un fichier de sauvegarde spécifique. Ceci peut être utile si vous avez rencontré un problème de ransomware sur un volume en particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

## Paramètres de verrouillage des données et de protection contre les ransomwares

Chaque stratégie de sauvegarde fournit une section pour *DataLock et protection contre les attaques par ransomware* que vous pouvez appliquer à vos fichiers de sauvegarde.

The screenshot shows the AWS Backup console interface. At the top, there are two tabs: 'Name' (selected) and 'Default\_Policy\_Name'. Below these, there's a section for 'Labels & Retention' showing '30 Daily'. The main section is 'DataLock & Ransomware Protection', which is highlighted with an orange border. It contains a description: 'Backup copies are protected from being modified or deleted, and they are scanned for ransomware threats.' Below this, there are three radio button options: 'None' (selected), 'Governance' (with a hand icon), and 'Compliance'. To the right of these options is a 'DataLock & Ransomware Protection Information' box with three bullet points: 'DataLock protection mode can't be changed after the policy is created', 'Each backup file will be locked during the retention period as defined above, or for a minimum of 30 days, plus a buffer period of up to 14 days. [Learn more.](#)', and 'Ransomware detection scans are run automatically on each protected backup copy: once during the retention period, and again before a restore operation. You can run detection scans on demand as well.' At the bottom, there's an 'Archival Policy' section showing 'Disabled'.

Vous pouvez choisir parmi les paramètres suivants pour chaque stratégie de sauvegarde :

- Aucun (par défaut)

La protection contre les verrous et les attaques par ransomware sont désactivées.

- Gouvernance (non disponible avec StorageGRID)

DataLock est défini sur *Governance* mode où les utilisateurs avec des autorisations spécifiques ("[voir ci-dessous](#)") peut écraser ou supprimer des fichiers de sauvegarde pendant la période de rétention. La protection contre les ransomwares est activée.

- La conformité

DataLock est défini sur le mode *Compliance*, où aucun utilisateur ne peut écraser ou supprimer des fichiers de sauvegarde pendant la période de rétention. La protection contre les ransomwares est activée.



La fonction de verrouillage d'objet StorageGRID S3 fournit un mode de verrouillage de données unique équivalent au mode de conformité. Un mode de gouvernance équivalent n'est pas pris en charge. Par conséquent, aucun utilisateur n'a la possibilité de contourner les paramètres de rétention, d'écraser les sauvegardes protégées ou de supprimer les sauvegardes verrouillées.

## Environnements de travail et fournisseurs de stockage objet pris en charge

Vous pouvez activer la protection des données et des attaques par ransomware sur les volumes ONTAP à partir de plusieurs environnements de travail lorsque vous utilisez le stockage objet dans plusieurs fournisseurs de cloud public et privé. D'autres fournisseurs de cloud seront ajoutés dans les prochaines versions.

Environnement de travail source	Destination du fichier de sauvegarde <code>ifdef::aws[]</code>
Cloud Volumes ONTAP dans AWS	Amazon S3 <code>endif::aws[]</code> <code>ifdef::Azure[]</code> <code>endif::Azure[]</code> <code>ifdef::gcp[]</code> <code>endif::gcp[]</code>
Système ONTAP sur site	<code>ldef::aws[]</code> Amazon S3 <code>endif::aws[]</code> <code>ifdef::Azure[]</code> <code>endif::Azure[]</code> <code>ifdef::gcp[]</code> <code>fdef::gcp[]</code> <code>dnif::gcp[]</code> NetApp StorageGRID

### De formation

- Vos clusters doivent exécuter ONTAP 9.11.1 ou version supérieure
- Vous devez utiliser BlueXP 3.9.21 ou supérieur
- Pour StorageGRID :
  - Le connecteur doit être déployé sur votre site (il peut être installé sur un site avec ou sans accès Internet)
  - StorageGRID 11.6.0.3 et supérieur sont requis pour la prise en charge complète des capacités de verrouillage de données

### Restrictions

- Data Lock et protection contre les attaques par ransomware n'est pas disponible si vous avez configuré le stockage d'archivage dans la stratégie de sauvegarde.
- L'option DataLock que vous sélectionnez lors de l'activation de Cloud Backup (gouvernance ou conformité) doit être utilisée pour toutes les stratégies de sauvegarde de ce cluster. Vous ne pouvez pas utiliser le verrouillage des modes gouvernance et conformité sur un seul cluster.
- Si vous activez DataLock, toutes les sauvegardes de volume seront verrouillées. Vous ne pouvez pas combiner des sauvegardes de volume verrouillées et non verrouillées pour un même cluster.
- La protection des données et des attaques par ransomware est applicable pour les nouvelles sauvegardes de volumes grâce à une stratégie de sauvegarde avec DataLock et protection contre les attaques par ransomware activées. Vous ne pouvez pas activer cette fonctionnalité après l'activation de Cloud Backup.

## Paramètres de stockage d'archivage

Si vous utilisez un certain stockage cloud, vous pouvez déplacer d'anciens fichiers de sauvegarde vers un Tier de stockage/accès moins onéreux après un certain nombre de jours. Notez que le stockage d'archives ne peut pas être utilisé si vous avez activé DataLock.

Vous n'avez pas accès immédiatement aux données des niveaux d'archivage quand vous en avez besoin. Par conséquent, vos coûts de récupération sont plus élevés, vous devez déterminer la fréquence à laquelle restaurer les données à partir des fichiers de sauvegarde archivés.

Chaque politique de sauvegarde fournit une section pour *Archival* que vous pouvez appliquer à vos fichiers de sauvegarde.

Name	Default_Policy_Name	⌵
Labels & Retention	30 Daily	⌵
DataLock & Ransomware Protection	None	⌵
Archival Policy	<p>Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archive</p> <div> <div>Archive After (Days)</div> <div>Storage Class</div> </div> <div> <div>30</div> <div>S3 Glacier</div> </div>	

- Dans GCP, les sauvegardes sont associées par défaut à la classe de stockage *Standard*.

Si votre cluster sur site utilise ONTAP 9.12.1 ou version ultérieure, vous pouvez choisir de transférer d'anciennes sauvegardes vers le stockage *Archive* dans l'interface utilisateur de sauvegarde dans le cloud au bout d'un certain nombre de jours afin d'optimiser les coûts. (Cette fonctionnalité n'est pas disponible actuellement pour les systèmes Cloud Volumes ONTAP.) ["En savoir plus sur le stockage des archives Google"](#).

- Dans StorageGRID, les sauvegardes sont associées à la classe de stockage *Standard*.

Il n'y a pas de niveau d'archivage disponible pour le moment.

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

Cloud Backup prend en charge deux classes de stockage d'archivage S3 ainsi que la plupart des régions.

### Classes de stockage d'archivage S3 prises en charge pour Cloud Backup

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. 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 choisissez S3 *Glacier* ou S3 *Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de Cloud Backup, ce Tier sera le seul niveau d'archivage disponible pour les futures stratégies de sauvegarde de ce cluster. Si vous sélectionnez aucun niveau d'archivage dans votre première stratégie de

sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage pour les futures stratégies.

Notez que, lorsque vous configurez Cloud Backup 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

Cloud Backup prend en charge un Tier d'accès d'archivage Azure ainsi que la plupart des régions.

## Tiers d'accès Azure Blob pris en charge pour la sauvegarde dans le cloud

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 Cloud Backup 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"](#).

### 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

Cloud Backup prend en charge une classe de stockage d'archivage Google et la plupart des régions.

### Classes de stockage d'archivage Google prises en charge pour Cloud Backup

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 version supérieure, vous pouvez choisir de transférer d'anciennes sauvegardes vers *Archive* le stockage dans l'interface utilisateur de sauvegarde dans le cloud au bout d'un certain nombre de jours (généralement plus de 30 jours) afin d'optimiser les coûts. (Cette fonctionnalité n'est pas disponible actuellement pour les systèmes Cloud Volumes ONTAP.) 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 Cloud Backup 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 Cloud Backup, vous pouvez créer des fichiers de sauvegarde dans un compte Azure différents de l'emplacement de vos volumes Cloud Volumes ONTAP source. Et ces deux comptes peuvent être différents du compte où réside le connecteur BlueXP.

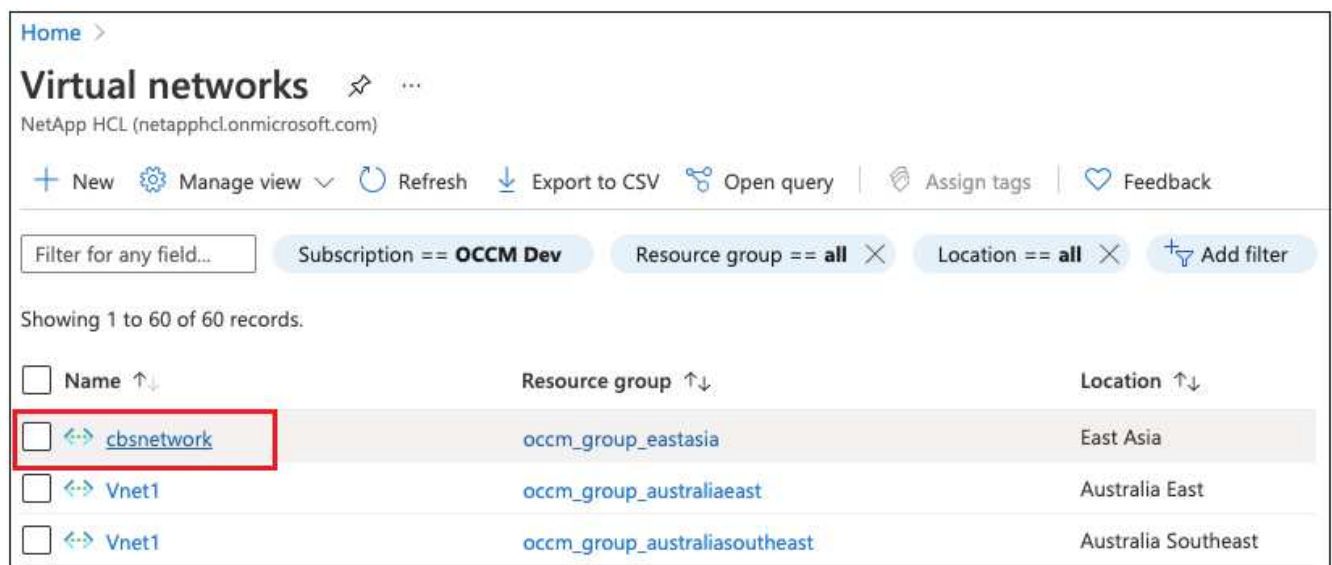
Ces étapes sont requises uniquement lorsque vous l'êtes "[Sauvegarde des données Cloud Volumes ONTAP dans le stockage Azure Blob](#)".

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.



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

Subscription \* ⓘ  
OCCM Automation

Virtual network \*  
cbse2evnet

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

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.


**cbsnetwork | Peerings**

Virtual network

«
+ Add
↻ Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
  - Address space
  - Connected devices
  - Subnets
  - DDoS protection
  - Firewall
  - Security
  - DNS servers
  - Peerings**

Name	Peering status	Peer
cbsnetwork	Connected	cbse2evnet

- 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

<<
+ Add
↻ Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

Name	Peering status	Peer
<a href="#">cbsnetworkpeer</a>	Connected	<a href="#">cbsnetwork</a>

## 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.



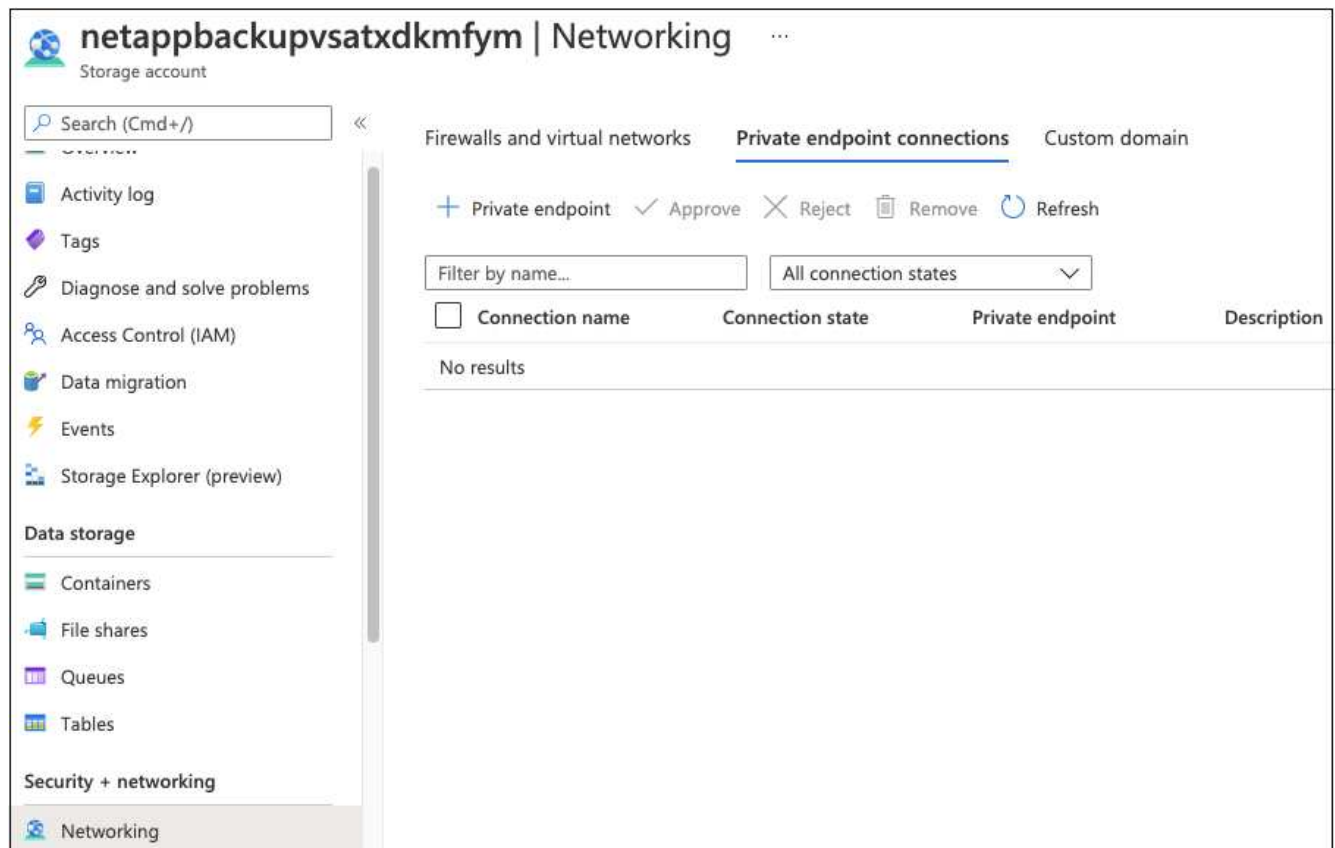
Vous avez besoin de l'autorisation de contributeur réseau pour effectuer l'action suivante.

```

{
  "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 au compte de stockage > réseau > connexions de noeuds finaux privés et cliquez sur **+ noeud final 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 \* ⓘ

**i** 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"/>
		<div> <div>occm_group_centralus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus2</div> <div>privatelink.blob.core.windows.net</div> </div>

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 dans le cloud sur le système Cloud Volumes ONTAP. Cette fois-ci, vous devriez réussir.

# Connaissances et support

## S'inscrire pour obtenir de l'aide

Avant d'ouvrir un dossier de demande de support auprès du support technique NetApp, vous devez ajouter un compte sur le site du support NetApp (NSS) à BlueXP, puis vous inscrire pour obtenir du support.

### Présentation de l'inscription au support

Il existe deux types d'inscription pour activer les droits d'assistance :

- Enregistrement de votre abonnement au support pour les identifiants de compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxx se trouve sur la page des ressources de support de BlueXP).

Il sert d'ID d'abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxxx).

Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L'enregistrement des deux types de numéros de série offre des fonctionnalités telles que l'ouverture de tickets de support et la génération automatique de tickets.

La façon dont vous vous inscrivez dépend de votre présence ou de votre présence chez un client ou un partenaire nouveau ou existant.

- Client ou partenaire existant

En tant que client ou partenaire NetApp, vous pouvez utiliser votre compte SSO du site de support NetApp pour effectuer les enregistrements suivants. Dans le tableau de bord support, BlueXP fournit une page **NSS Management** où vous pouvez ajouter votre compte NSS. Une fois votre compte NSS ajouté, BlueXP enregistre automatiquement ces numéros de série pour vous.

[Découvrez comment ajouter votre compte NSS.](#)

- Nouveaux partenaires NetApp

Si vous êtes nouveau chez NetApp, vous devez enregistrer votre numéro de série BlueXP sur le site d'inscription du support NetApp. Une fois que vous avez terminé cette inscription et créé un nouveau compte NSS, vous pouvez utiliser ce compte dans BlueXP pour vous inscrire automatiquement à l'avenir.

[Découvrez comment vous inscrire auprès de NetApp.](#)

### Ajouter un compte NSS à BlueXP

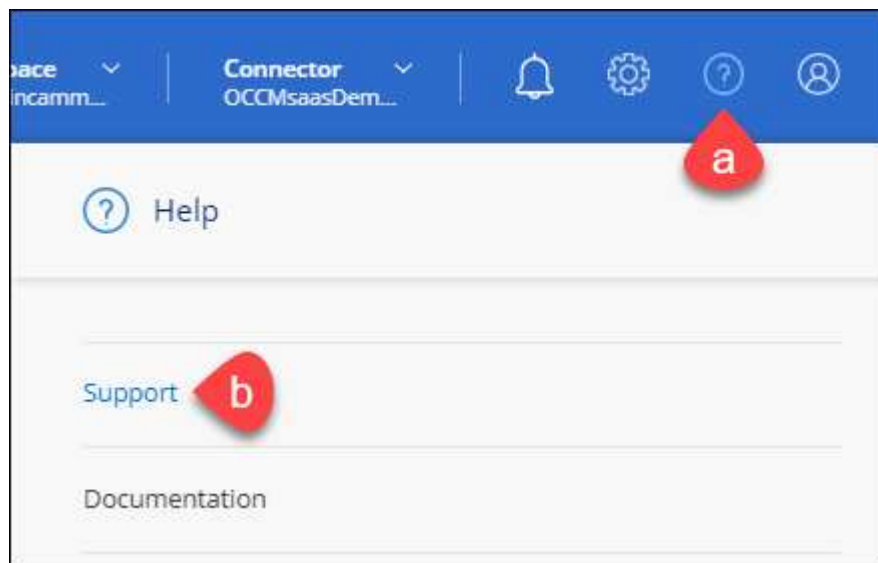
Le tableau de bord du support vous permet d'ajouter et de gérer vos comptes du site de support NetApp pour BlueXP.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.

- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

## Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

Notez ce qui suit :

- Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
- Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS. Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du **...** menu.
- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le **...** menu. Cette option vous invite à vous reconnecter.

## Inscrivez-vous auprès de NetApp

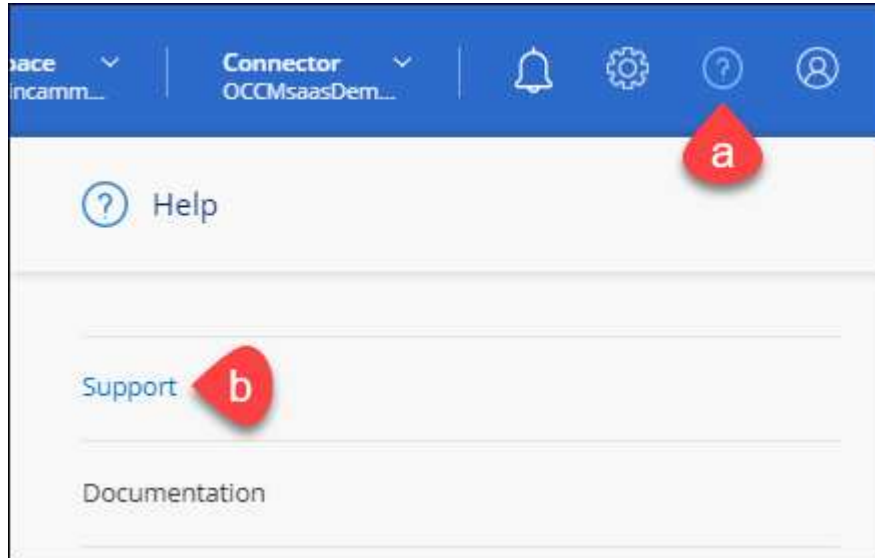
Le fait de vous inscrire au support NetApp dépend de la présence ou non d'un compte sur le site de support NetApp (NSS).

## Client existant avec un compte NSS

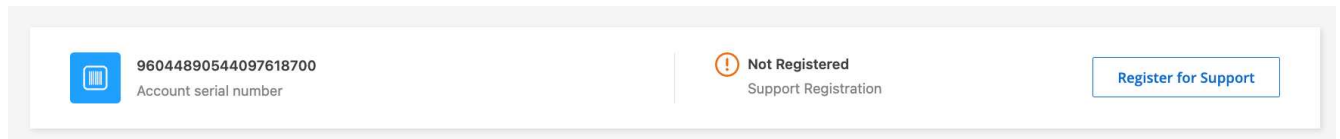
Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Si ce n'est déjà fait, ajoutez votre compte NSS à BlueXP.
3. Sur la page **Ressources**, cliquez sur **s'inscrire au support**.



## Client existant mais aucun compte NSS

Si vous êtes déjà client NetApp avec des licences et des numéros de série existants mais que *no* NSS, il vous suffit de créer un compte NSS.

### Étapes

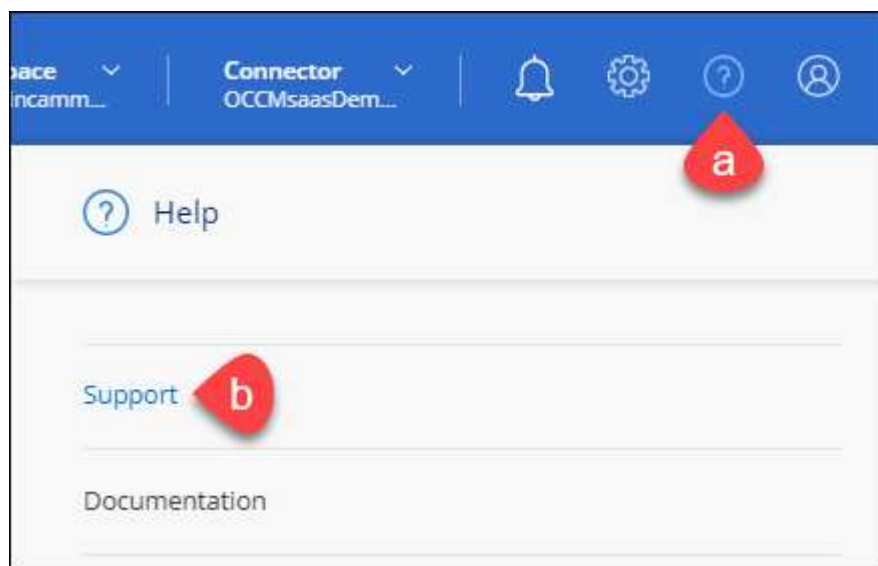
1. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
  - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
  - b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

## Découvrez la toute nouvelle gamme NetApp

Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Recherchez le numéro de série de l'ID de compte sur la page d'inscription au support.



3. Accédez à "[Site d'inscription au support NetApp](#)" Et sélectionnez **je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

La confirmation de la soumission de votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp.

8. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
  - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
  - b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

#### Une fois que vous avez terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois votre compte sur le site de support NetApp, vous pouvez accéder à BlueXP et ajouter ce compte NSS pour les inscriptions futures.

## Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

### Auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- ["Base de connaissances"](#)

Recherchez dans la base de connaissances BlueXP des articles utiles pour résoudre les problèmes.

- ["Communautés"](#)

Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

- Documentation

La documentation BlueXP que vous consultez actuellement.

- Courrier électronique : [ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)[E-mail de commentaires]

Nous accordons une grande importance à vos commentaires. Envoyez vos commentaires pour nous aider à améliorer BlueXP.

### Support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

#### Avant de commencer

Pour utiliser la fonction **Créer un cas**, vous devez d'abord effectuer un enregistrement unique de votre numéro de série d'ID de compte BlueXP (par exemple 960xxxx) avec NetApp. ["Découvrez comment vous inscrire à de l'aide"](#).

#### Étapes

1. Dans BlueXP, cliquez sur **aide > support**.
2. Choisissez l'une des options disponibles sous support technique :
  - a. Cliquez sur **appelez-nous** si vous souhaitez parler avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.
  - b. Cliquez sur **Créer un dossier** pour ouvrir un dossier auprès des spécialistes du support NetApp :
    - **Compte sur le site de support NetApp** : sélectionnez le compte NSS applicable associé à la personne qui ouvre le dossier de support. Cette personne sera le contact principal avec NetApp en plus de l'e-mail ci-dessous.

Si vous ne voyez pas votre compte NSS, vous pouvez accéder à l'onglet **NSS Management** de la section support de BlueXP pour l'ajouter.

- **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
- **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.

La liste des environnements de travail est comprise dans le cadre du compte, de l'espace de travail et du connecteur BlueXP que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information située à côté du nom du champ.

- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.

Create a Case

TESTCLOUD2NTAP 

NetApp Support Site Account

Service

Cloud Manager 

Working Environment

Select... 

Case Priority 

Low- General Guidance 

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected 

### Une fois que vous avez terminé

Une fenêtre contextuelle contenant votre numéro de dossier de support s'affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour consulter l'historique de vos dossiers d'assistance, vous pouvez cliquer sur **Paramètres > Chronologie** et rechercher les actions nommées "Créer un dossier de support". Un bouton à l'extrême droite vous permet de développer l'action pour voir les détails.

Il est possible que vous rencontriez le message d'erreur suivant lors de la création d'un dossier :

« Vous n'êtes pas autorisé à créer un dossier pour le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement auquel il est associé n'est pas la



même société d'enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez consulter votre liste de comptes NSS en haut du formulaire **Créer un dossier** pour trouver la correspondance appropriée, ou vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à <https://mysupport.netapp.com/site/help>

# Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

## Droits d'auteur

<http://www.netapp.com/us/legal/copyright.aspx>

## Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/us/media/patents-page.pdf>

## Politique de confidentialité

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- ["Note pour BlueXP"](#)
- ["Notification relative à Cloud Backup"](#)
- ["Remarque concernant la restauration de fichiers uniques"](#)

## 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.