



Sauvegarde et restauration des données Kubernetes

Cloud Backup

NetApp
January 06, 2023

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/aws/concept-kubernetes-backup-to-cloud.html> on January 06, 2023. Always check docs.netapp.com for the latest.

Table des matières

- Sauvegarde et restauration des données Kubernetes 1
 - Protection des données du cluster Kubernetes à l'aide de Cloud Backup 1
 - Sauvegarde des données de volume persistant Kubernetes dans Amazon S3 5
 - Gestion des sauvegardes pour vos systèmes Kubernetes 11
 - Restauration de données Kubernetes à partir de fichiers de sauvegarde 22

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".](#)

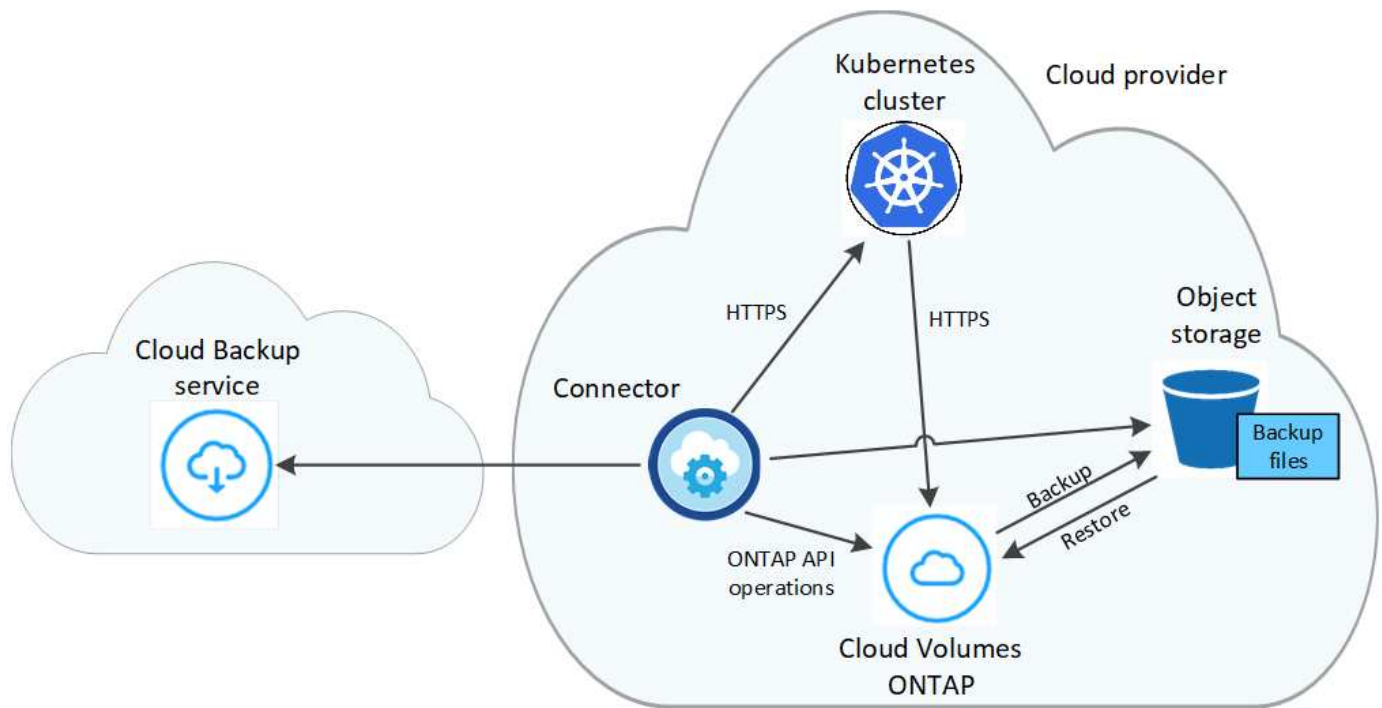
Fonctionnement de Cloud Backup

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 AWS, les sauvegardes commencent dans la classe de stockage *Standard* et la transition vers la classe de stockage *Standard-Infrequent Access* après 30 jours.

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

Sauvegarde des données de volume persistant Kubernetes dans Amazon S3

Procédez comme suit pour sauvegarder les données à partir de volumes persistants sur des clusters EKS Kubernetes vers un stockage Amazon S3.

Démarrage rapide

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

1

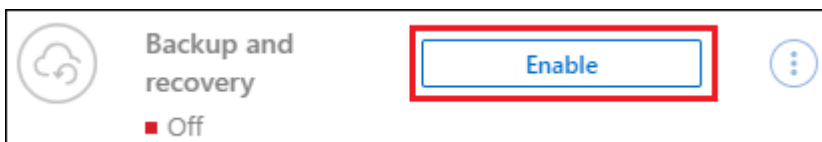
Passer en revue les prérequis

- 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 AWS 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 valide au fournisseur cloud pour l'espace de stockage où vos sauvegardes seront stockées.
- Vous avez souscrit au "[Offre de sauvegarde BlueXP Marketplace](#)", un "[Contrat annuel AWS](#)", ou vous avez acheté "[et activé](#)" Licence Cloud Backup BYOL de NetApp.
- Le rôle IAM qui fournit le connecteur BlueXP avec des autorisations inclut des autorisations S3 à partir de la dernière version "[Politique BlueXP](#)".

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 |

S3 Bucket
Cloud Manager will create the S3 bucket after you complete the wizard

4

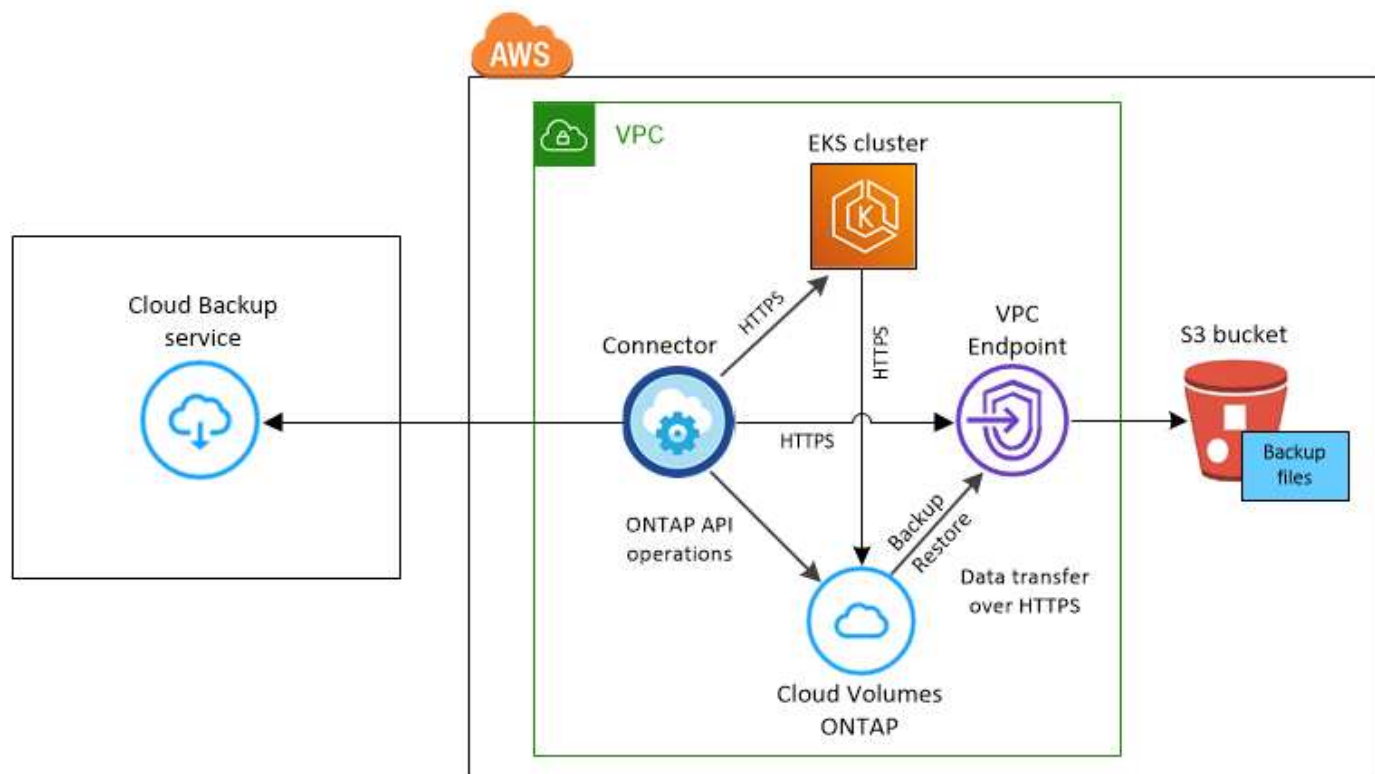
Sélectionnez les volumes à sauvegarder

Identifiez les volumes à sauvegarder dans la page Sélectionner les volumes. Un compartiment S3 est créé automatiquement dans le même compte et la même région AWS que le système Cloud Volumes ONTAP, et les fichiers de sauvegarde y sont stockés.

De formation

Avant de commencer à sauvegarder des volumes persistants de Kubernetes vers S3, 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 terminal VPC 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 AWS pour le stockage interne de son système.
- Le système Cloud Volumes ONTAP doit se trouver dans la même région AWS 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

```

Conditions de licence

Pour le modèle de licence PAYGO, un abonnement est disponible sur AWS Marketplace et permet de déployer Cloud Volumes ONTAP et Cloud Backup. Vous devez le faire ["Abonnez-vous à cet abonnement BlueXP"](#) Avant d'activer Cloud Backup. La facturation pour Cloud Backup s'effectue via cet abonnement.

Pour bénéficier d'un contrat annuel qui vous permet de sauvegarder à la fois les données Cloud Volumes ONTAP et les données ONTAP sur site, vous devez vous abonner à la ["Page AWS Marketplace"](#) puis ["Associez l'abonnement à vos identifiants AWS"](#).

Pour un contrat annuel qui vous permet de regrouper Cloud Volumes ONTAP et Cloud Backup, vous devez définir le contrat annuel lors de la création d'un environnement de travail Cloud Volumes ONTAP. Avec cette option, vous ne pouvez pas sauvegarder les données sur site.

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 compte AWS pour l'espace de stockage où vos sauvegardes seront stockées.

Régions AWS prises en charge

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

Autorisations AWS Backup requises

Le rôle IAM qui fournit à BlueXP des autorisations doit inclure des autorisations S3 à partir des dernières "Politique BlueXP".

Voici les autorisations S3 spécifiques de la règle :

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource": [
    "arn:aws:s3:::netapp-backup-*"
  ]
},
```

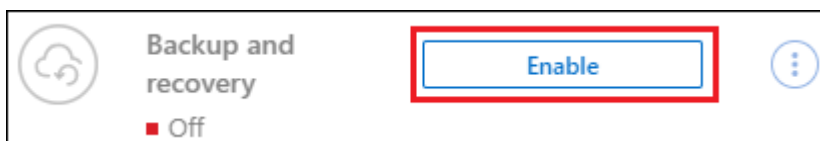
Activation de Cloud Backup

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.

Si la destination Amazon S3 pour vos sauvegardes existe en tant qu'environnement de travail sur la Canvas, vous pouvez faire glisser le cluster Kubernetes vers l'environnement de travail Amazon S3 pour lancer l'assistant d'installation.



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.

Define Policy

Policy - Retention & Schedule

☐ Hourly Number of backups to retain 24

☒ Daily Number of backups to retain 30

☐ Weekly Number of backups to retain 52

☐ Monthly Number of backups to retain 12

S3 Bucket Cloud Manager will create the S3 bucket after you complete the wizard

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).

Select Volumes

57 Volumes

| <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"/> | PV 1 On | Namespace 2 | 10 TB | Not Active |
| <input checked="" type="checkbox"/> | PV 2 On | Namespace 2 | 10 TB | Not Active |

☒ 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

Un compartiment S3 est créé automatiquement dans le même compte et la même région AWS que le système Cloud Volumes ONTAP, et les fichiers de sauvegarde y sont stockés.

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 autre cluster dans AWS (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.

The screenshot shows the AWS Backup console interface for the 'Kubernetes' tab. At the top, there's a navigation bar with 'Backup & Restore' and several tabs: 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes' (selected), and 'Job Monitoring'. Below the navigation bar, there's a dropdown menu for 'All Clusters (1)' and a 'Backup Settings' button. The main content area displays summary statistics: 1 Kubernetes Cluster, 5 Protected PVs, and 976.56 KB Total Backups Size. To the right, a 'Protected Persistent Volumes Status' box shows 0 Healthy Backups and 0 Failed Backups. Below this, a table titled '5 Backup Jobs' lists backup jobs with columns: Source K8s Cluster, Source Persistent Volume, Source Namespace, Last Backup, Backup Copies, and Backup Status. The table contains three rows of backup jobs, all with a status of 'Unknown'. A search icon is visible in the top right corner of the table area.

| 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 |

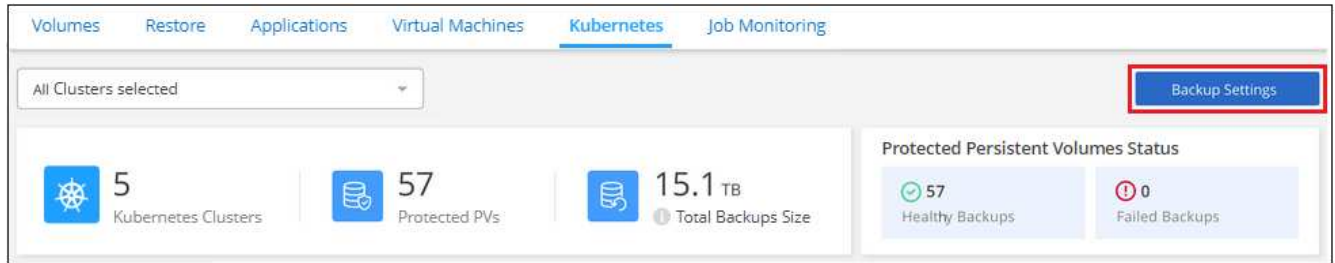
Si vous recherchez des volumes spécifiques dans certains clusters, vous pouvez affiner la liste par cluster et volume ou utiliser le filtre de recherche.

Activation et désactivation des sauvegardes des volumes

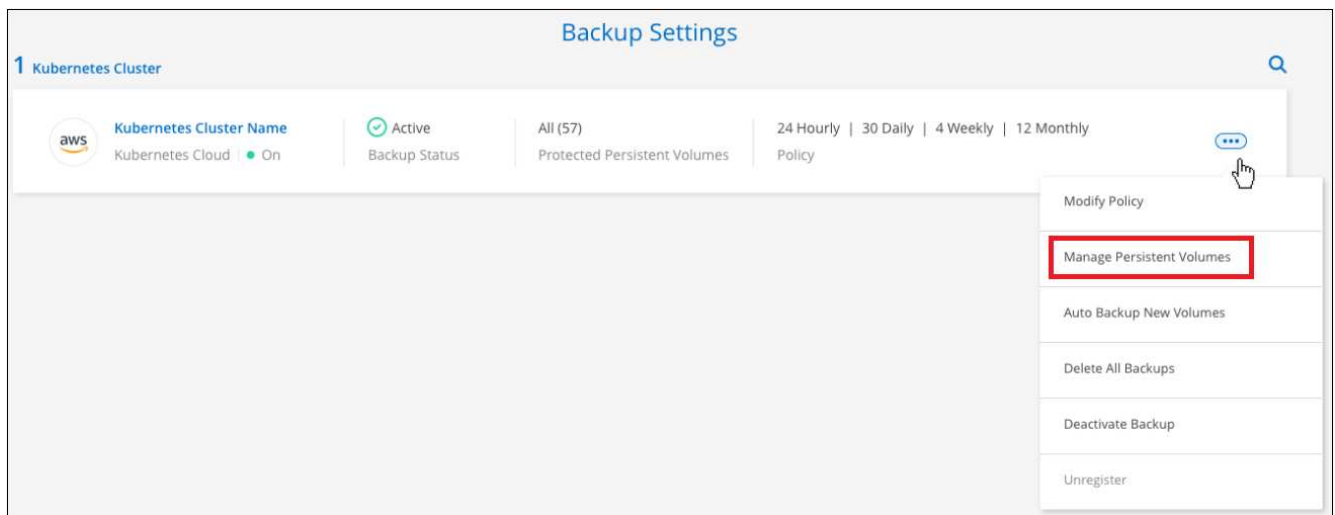
Vous pouvez arrêter la sauvegarde d'un volume si vous n'avez pas besoin de copies de sauvegarde de ce volume et si vous ne voulez pas payer pour le coût de stockage des sauvegardes. Vous pouvez également ajouter un nouveau volume à la liste des sauvegardes si ce n'est pas actuellement le cas.

Étapes

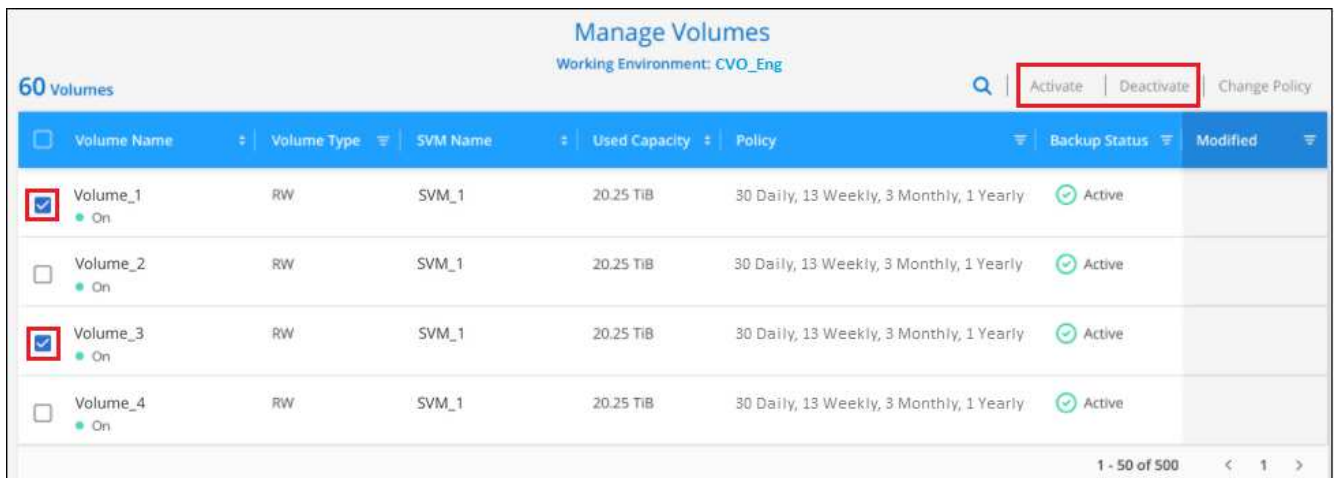
1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.



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.



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

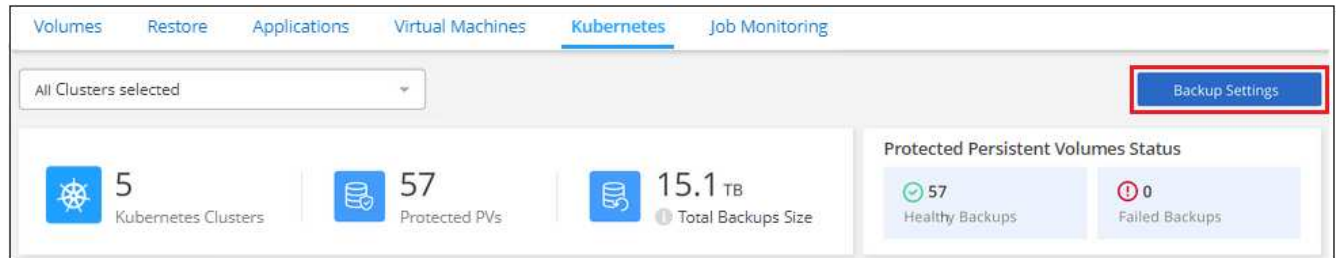
Remarque : lors de l'arrêt de la sauvegarde d'un volume, vous continuerez à être facturé par votre fournisseur de cloud pour les coûts de stockage objet pour la capacité que les sauvegardes utilisent, sauf si vous [supprimez les sauvegardes](#).

Modification d'une stratégie de sauvegarde existante

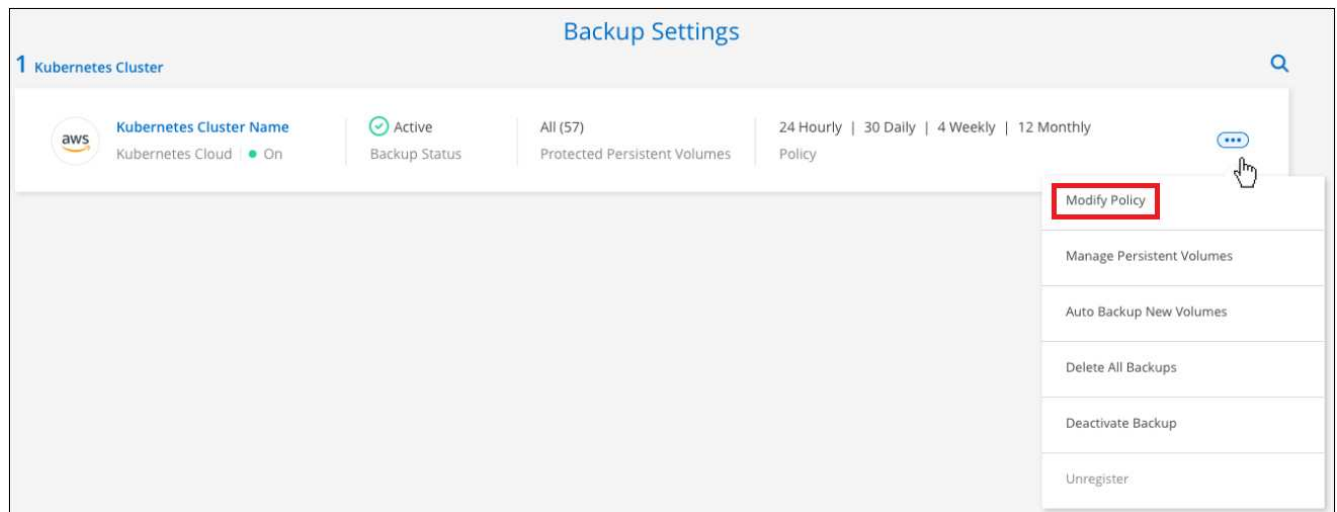
Vous pouvez modifier les attributs d'une stratégie de sauvegarde actuellement appliquée aux volumes d'un environnement de travail. La modification de la stratégie de sauvegarde affecte tous les volumes existants utilisant la règle.

Étapes

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



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**.

[Edit Policy](#)

Working Environment: Cluster Dev Lab

| | | |
|--------------------|------------------|---|
| Name | Daily 30 backups | ▼ |
| Labels & Retention | 30 Daily | ▼ |

Définition d'une stratégie de sauvegarde à attribuer aux nouveaux volumes

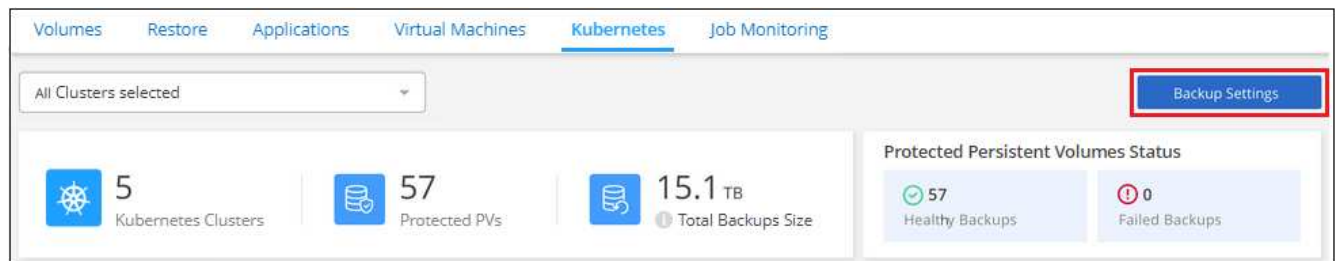
Si vous n'avez pas sélectionné l'option permettant d'attribuer automatiquement une stratégie de sauvegarde aux volumes nouvellement créés lorsque vous avez activé Cloud Backup pour la première fois sur votre cluster Kubernetes, vous pouvez choisir cette option ultérieurement dans la page *Backup Settings*. 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.](#)

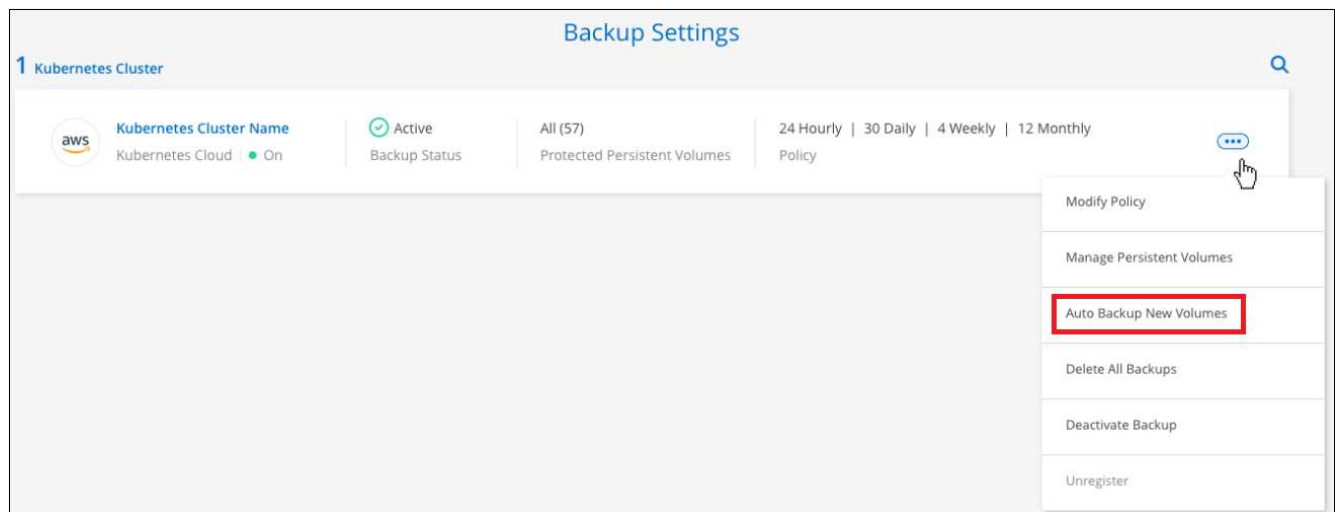
Vous pouvez également désactiver ce paramètre afin que les volumes nouvellement créés ne soient pas sauvegardés automatiquement. Dans ce cas, vous devrez activer manuellement les sauvegardes pour tous les volumes que vous souhaitez effectuer ultérieurement.

Étapes

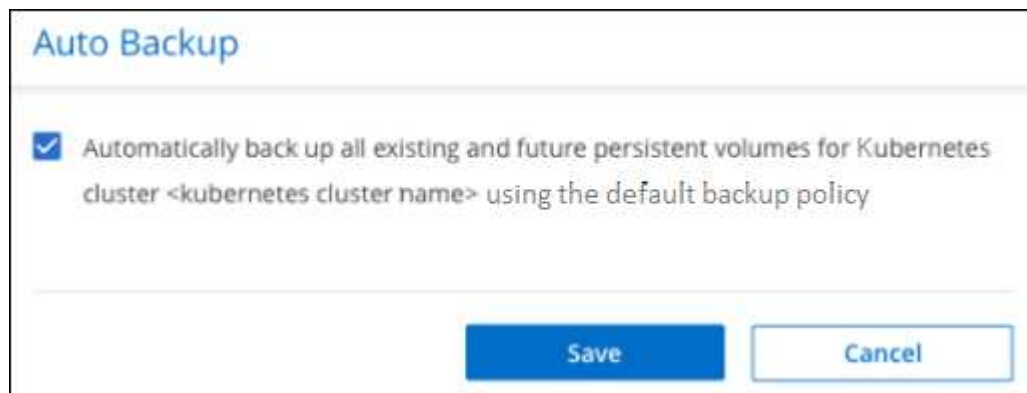
1. Dans l'onglet **Kubernetes**, sélectionnez **Paramètres de sauvegarde**.



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**.



Auto Backup

☒ Automatically back up all existing and future persistent volumes for Kubernetes cluster <kubernetes cluster name> using the default backup policy

Save **Cancel**

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

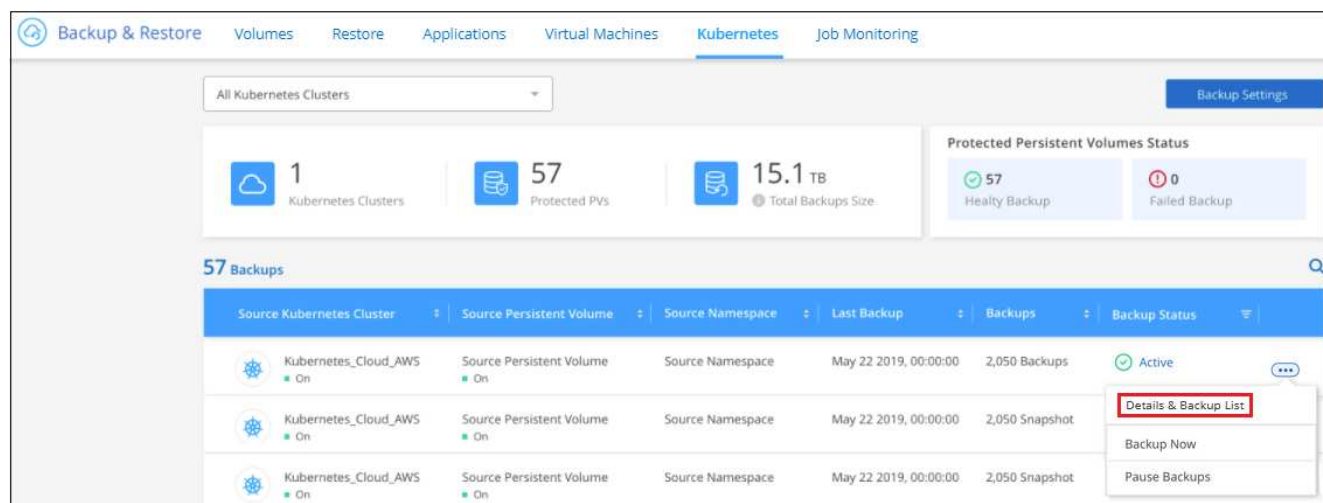
Vous pouvez afficher la liste de tous les fichiers de sauvegarde existants pour chaque volume. Cette page affiche des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde, tels que la dernière sauvegarde effectuée, la stratégie de sauvegarde actuelle,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



Backup & Restore | Volumes | Restore | Applications | Virtual Machines | **Kubernetes** | Job Monitoring

All Kubernetes Clusters

1 Kubernetes Clusters | **57** Protected PVs | **15.1 TB** Total Backups Size

Protected Persistent Volumes Status

57 Healthy Backup | **0** Failed Backup

57 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 | |

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.

| 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.



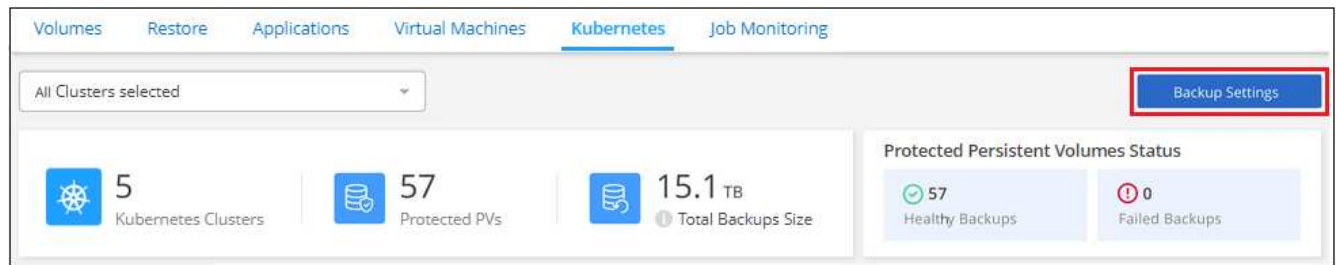
Si vous prévoyez de supprimer un environnement ou un cluster de travail qui dispose de sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. Cloud Backup ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système et l'interface utilisateur ne prend 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

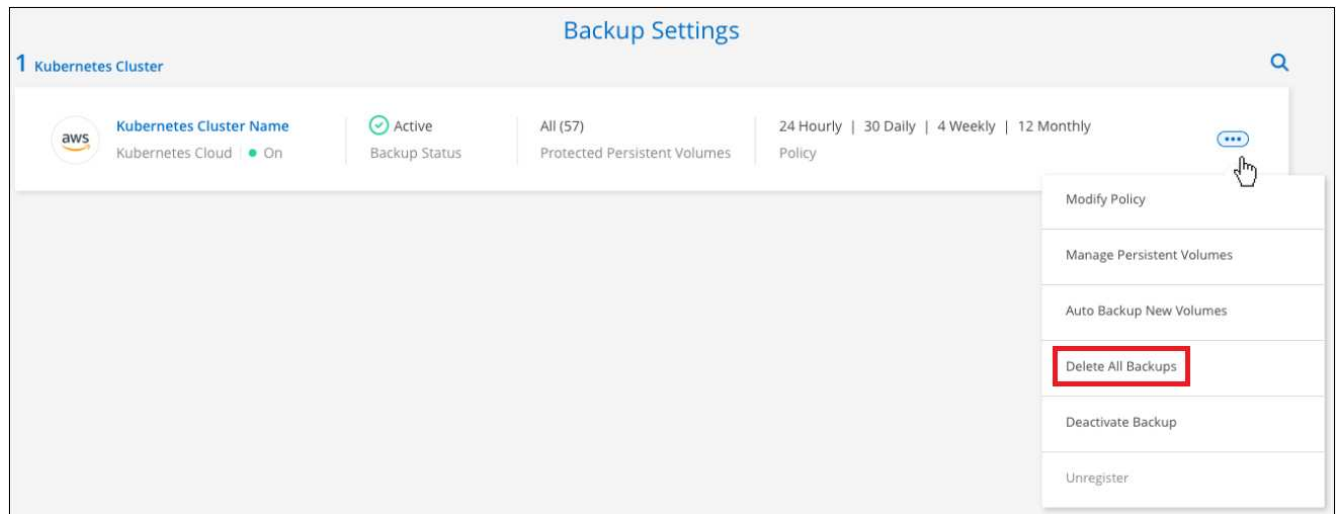
La suppression de toutes les sauvegardes d'un environnement de travail ne désactive pas les futures sauvegardes des volumes de cet environnement de travail. Si vous souhaitez arrêter la création de sauvegardes de tous les volumes d'un environnement de travail, vous pouvez désactiver les sauvegardes [comme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

Étapes

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



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**.

Backup & Restore | Volumes | Restore | Applications | Virtual Machines | **Kubernetes** | Job Monitoring

All Kubernetes Clusters

1 Kubernetes Clusters | 57 Protected PVs | 15.1 TB Total Backups Size

Protected Persistent Volumes Status: 57 Healthy Backup, 0 Failed Backup

57 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 | |

Details & Backup List
Backup Now
Pause Backups

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

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

2,050 Backups

| 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**.

2,050 Backups

Select Timeframe

Actions

Delete All Backups
Download Backup Report

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**.

The screenshot shows the NetApp Backup & Restore interface with the **Kubernetes** tab selected. The top navigation bar includes **Backup & Restore**, **Volumes**, **Restore**, **Applications**, **Virtual Machines**, **Kubernetes**, and **Job Monitoring**. Below the navigation bar, there's a summary section with **1** Kubernetes Clusters, **57** Protected PVS, and **15.1 TB** Total Backups Size. To the right, a **Protected Persistent Volumes Status** section 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 row shows **Kubernetes_Cloud_AWS** as the source cluster, **Source Persistent Volume** as the source persistent volume, **Source Namespace** as the source namespace, **May 22 2019, 00:00:00** as the last backup, **2,050 Backups** as the number of backups, and **Active** as the backup status. A dropdown menu is open for the first row, showing options: **Details & Backup List**, **Backup Now**, and **Pause Backups**.

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

The screenshot shows the NetApp Backup & Restore interface with the **Details & Backup List** view selected. The interface is divided into three main sections: **Source**, **Destination**, and **Backup Information**. The **Source** section shows **Working Environment** as **Working Environment N...**, **Type** as **Cloud Volumes ONTAP (HA)**, **Provider** as **AWS**, **Volume** as **Volume Name**, and **SVM** as **SVM Name**. The **Destination** section shows **Cloud Provider** as **AWS**, **Region** as **us-east-1**, **Bucket** as **netapp-backup**, and **Account ID** as **012345678901234567890**. The **Backup Information** section shows **Relationship Status** as **Active**, **Last Backup** as **Oct 05 2021, 2:41:33 pm**, **Lag Duration** as **14 days 3 hours, 38 mi...**, **Backups** as **2,050**, and **Backup Policy** as **Netapp7YearsRetention**. Below these sections, a table lists **2,050 Backups**. The table has columns: **Backup Name**, **Date**, and **Size**. The first row shows **Backup_2020_Jan** as the backup name, **May 22 2019, 00:00:00** as the date, and **19,001** as the size. The second row shows **Backup_2020_Mar** as the backup name, **May 22 2019, 00:00:00** as the date, and **19,002** as the size. The third row shows **Backup_2020_Apr** as the backup name, **May 22 2019, 00:00:00** as the date, and **19,009** as the size.

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**.

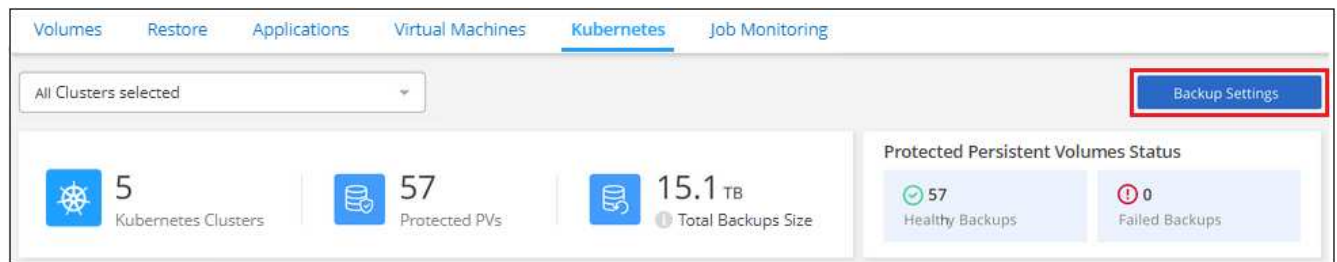
Désactivation de Cloud Backup pour un environnement de travail

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.

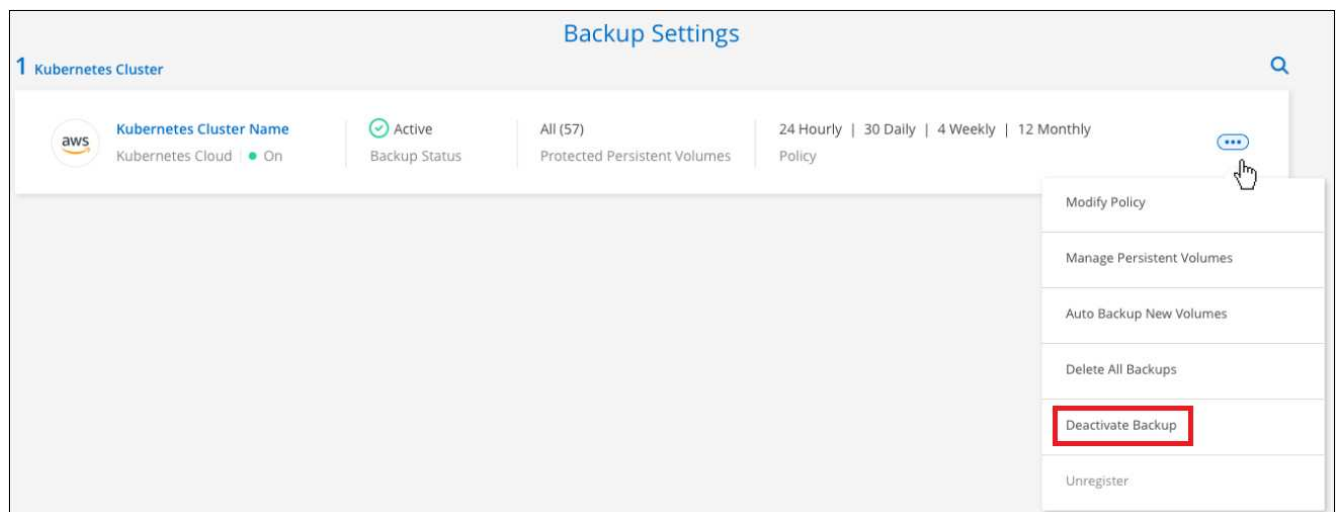
Notez que vous continuerez d'être facturé par votre fournisseur cloud pour les coûts de stockage objet correspondant à la capacité que vos sauvegardes utilisent, sauf si vous [supprimez les sauvegardes](#).

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.

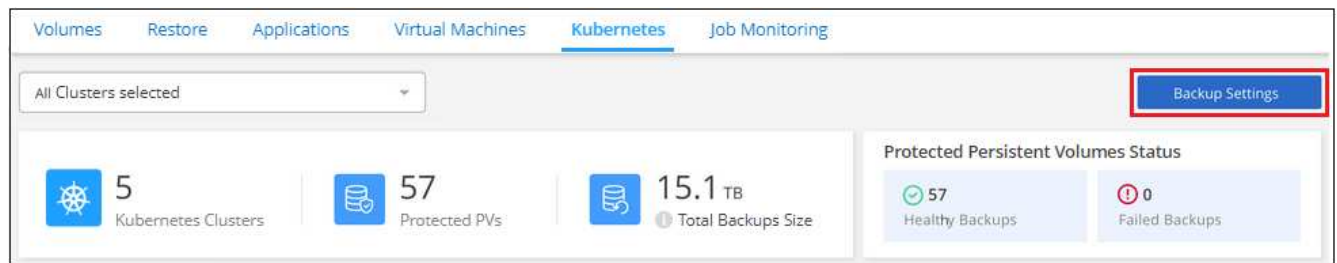
Avant de pouvoir annuler l'enregistrement de Cloud Backup, vous devez effectuer les opérations suivantes dans cet ordre :

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

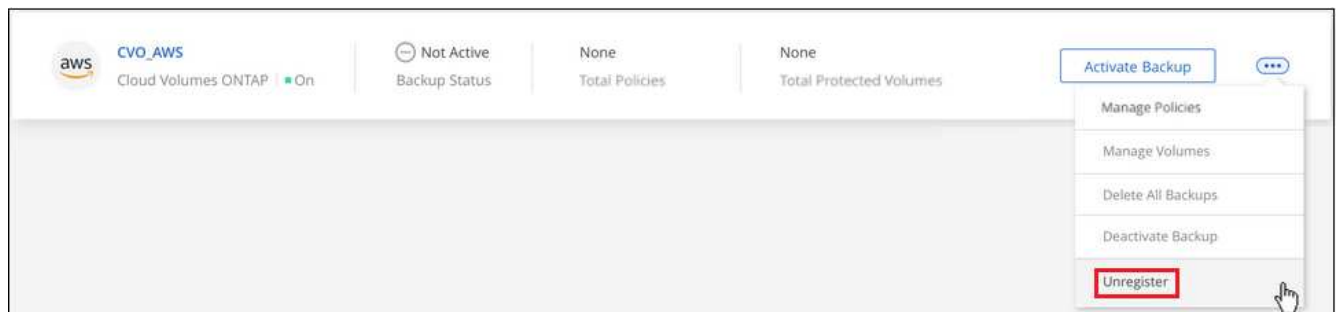
L'option de désenregistrer n'est pas disponible tant que ces deux actions ne sont pas terminées.

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 |
| 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.

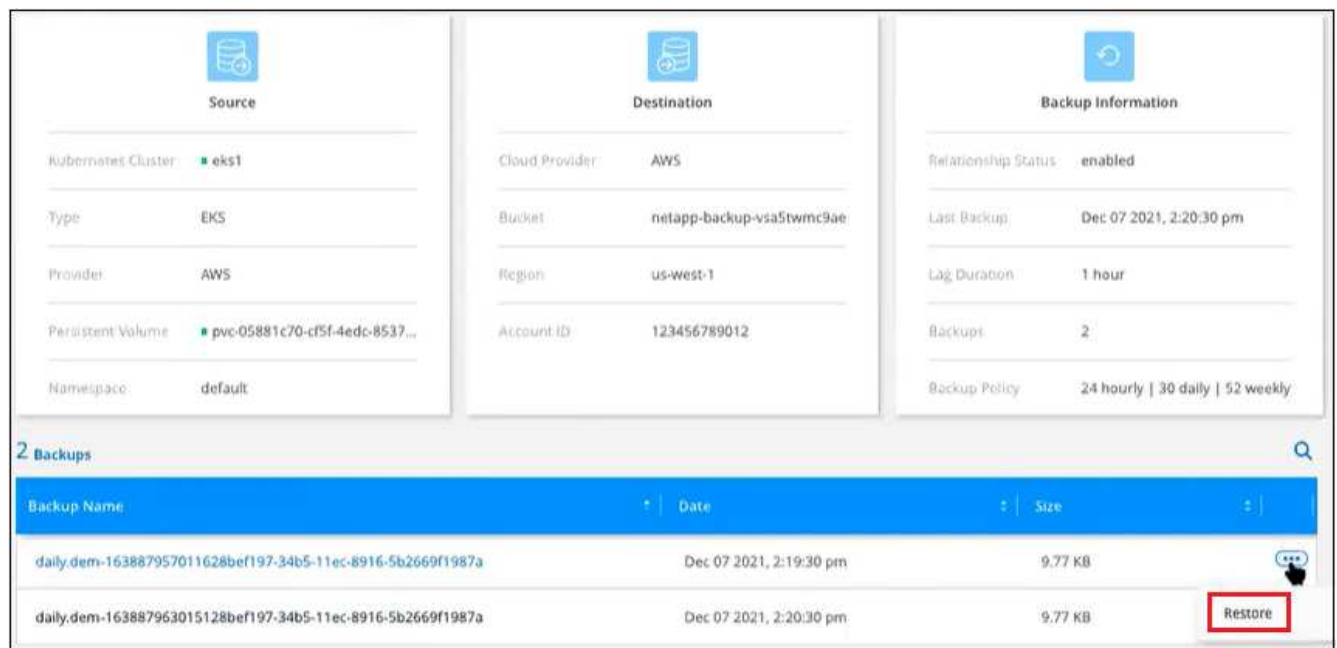
Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Kubernetes** pour afficher le tableau de bord Kubernetes.



- 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.



- 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-restore

Cancel Restore

6. 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.

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.