Copiez et synchronisez les données

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

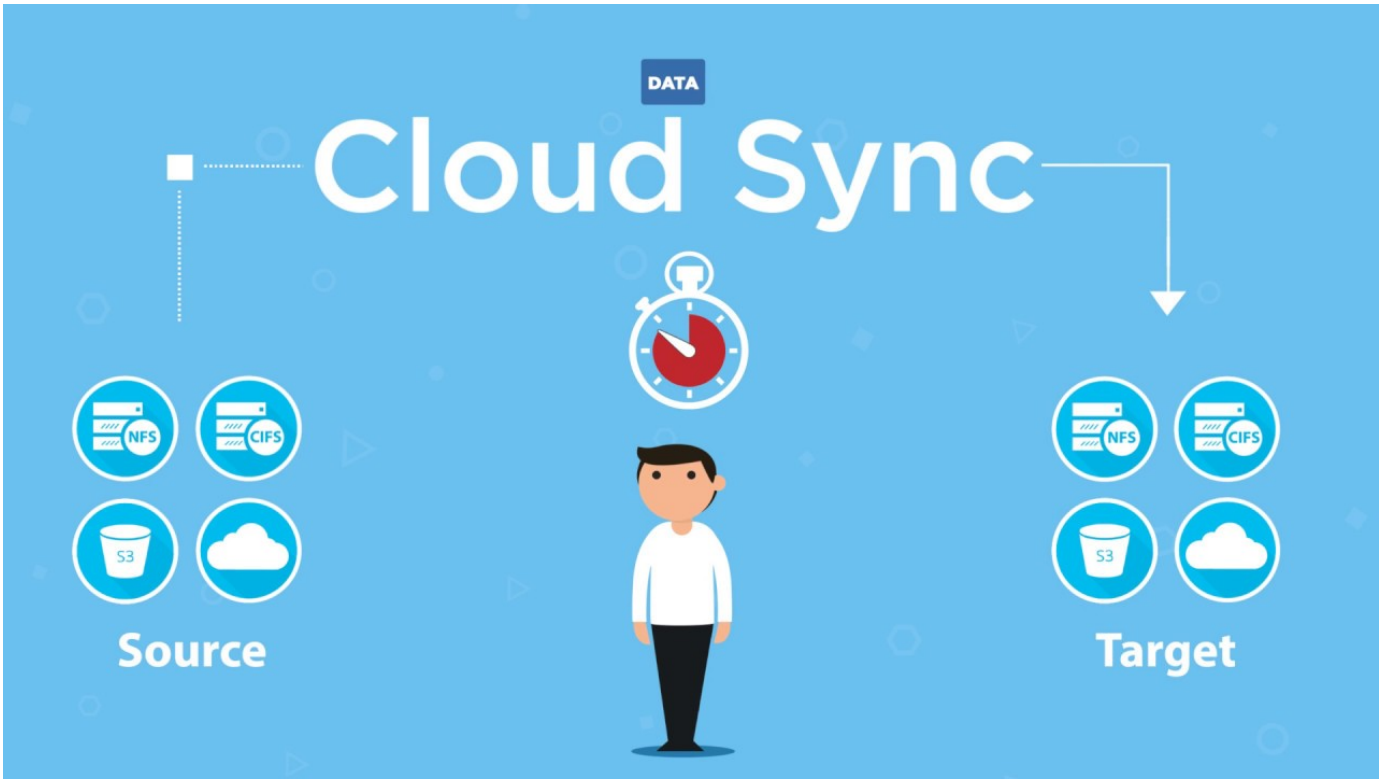
Copiez et synchronisez les données

Présentation de Cloud Sync

Le service NetApp Cloud Sync offre un moyen simple, sécurisé et automatisé de migrer vos données vers n'importe quelle cible, dans le cloud ou sur votre site. Qu'il s'agisse d'un dataset NAS basé sur fichiers (NFS ou SMB), d'un format d'objet Amazon simple Storage Service (S3), d'une appliance NetApp StorageGRID® ou de tout magasin d'objets d'un autre fournisseur cloud, Cloud Sync peut la convertir et la déplacer pour vous.

Caractéristiques

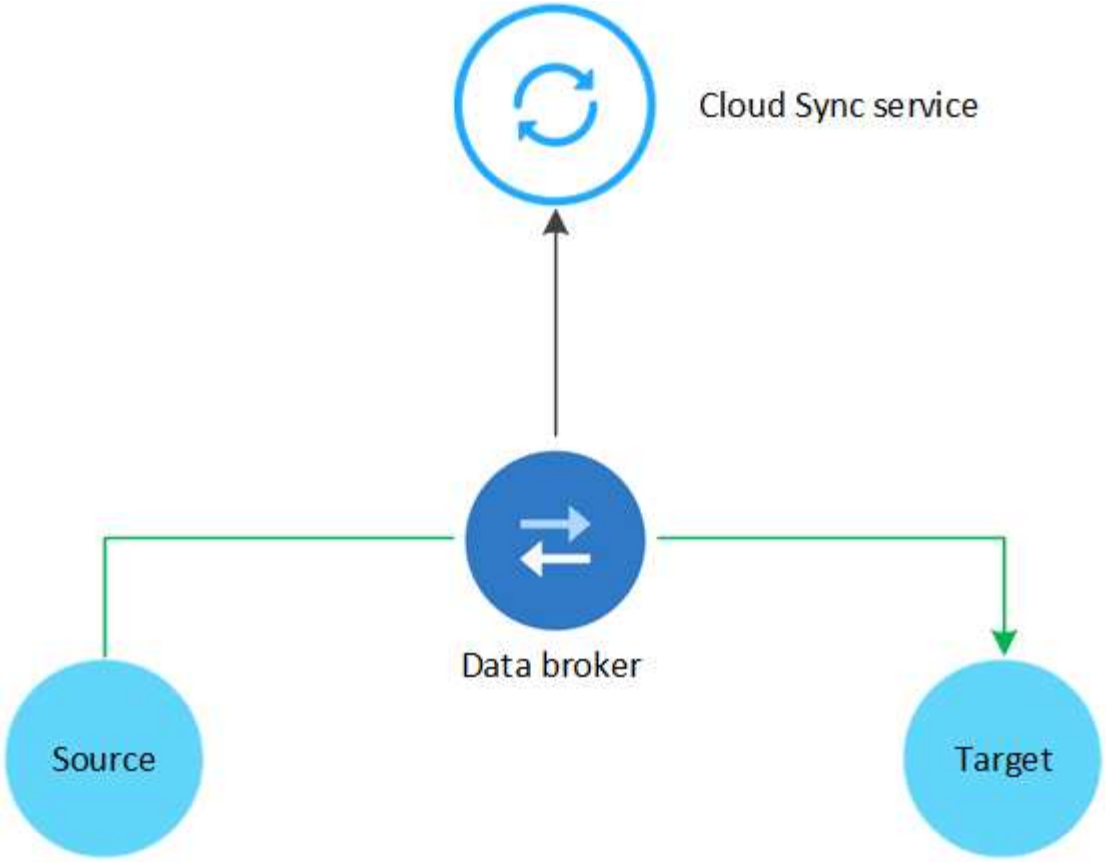
Regardez la vidéo suivante pour une présentation de Cloud Sync :



Fonctionnement de Cloud Sync

Cloud Sync est une plateforme de services à la demande (SaaS), qui consiste en un courtier en données, une interface cloud disponible via Cloud Manager, ainsi qu'une source et une cible.

L'image suivante montre la relation entre les composants Cloud Sync :



Le logiciel de courtier de données NetApp synchronise les données d'une source vers une cible (appelée « relation synchrone »). Vous pouvez exécuter le data broker dans AWS, Azure, Google Cloud Platform ou sur votre site. Le courtier de données a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels. "Afficher la liste des noeuds finaux".

Après la copie initiale, le service synchronise toutes les données modifiées en fonction de la planification que vous avez définie.

Types de stockage pris en charge

Cloud Sync prend en charge les types de stockage suivants :

- Tout serveur NFS
- Tout serveur SMB
- EFS AWS
- AWS S3
- Blob d'Azure
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- IBM Cloud Object Storage

- Cluster ONTAP sur site
- Stockage ONTAP S3
- StorageGRID

"Vérifiez les relations de synchronisation prises en charge".

Le coût

Il existe deux types de coûts associés à l'utilisation de Cloud Sync : les frais de ressources et les frais de service.

Frais de ressources

Les coûts en ressources sont liés aux coûts de calcul et de stockage pour l'exécution du courtier en données dans le cloud.

Frais de service

Il existe deux façons de payer les relations de synchronisation après la fin de votre essai gratuit de 14 jours. La première option consiste à vous abonner à AWS ou à Azure, ce qui vous permet de payer une heure ou une année. La deuxième option consiste à acheter des licences directement auprès de NetApp. Pour plus d'informations, lisez les sections suivantes.

Abonnement Marketplace

L'abonnement au service Cloud Sync d'AWS ou d'Azure vous permet de payer à un tarif horaire ou de payer annuellement. "Vous pouvez vous abonner via AWS ou Azure", selon l'endroit où vous voulez être facturé.

Abonnements horaires

Avec un abonnement au paiement à l'utilisation à l'heure, le service Cloud Sync facture l'heure en fonction du nombre de relations de synchronisation créées.

- "Voir les tarifs à Azure"
- "Consultez les tarifs à la carte dans AWS"

Abonnements annuels

Un abonnement annuel fournit une licence pour 20 relations de synchronisation que vous payez avant. Si vous utilisez plus de 20 relations synchronisées et que vous vous êtes abonné à Azure, vous payez les relations supplémentaires à l'heure.

"Voir les tarifs annuels dans AWS"

Licences de NetApp

L'achat de licences directement auprès de NetApp constitue une autre façon de payer les relations de synchronisation. Chaque licence vous permet de créer jusqu'à 20 relations de synchronisation.

Vous pouvez utiliser ces licences avec un abonnement AWS ou Azure. Par exemple, si vous disposez de 25 relations de synchronisation, vous pouvez payer les 20 premières relations de synchronisation à l'aide d'une licence, puis effectuer des opérations de paiement à la demande à partir d'AWS ou d'Azure avec les 5 autres relations de synchronisation.

"Découvrez comment acheter des licences et les ajouter à Cloud Sync".

Termes de la licence

Les clients qui achètent une licence BYOL (Bring Your Own License) au service Cloud Sync doivent être conscients des limites associées au droit de licence.

- Les clients ont le droit de tirer parti de la licence BYOL pour une durée maximale d'un an à compter de la date de livraison.
- Les clients ont le droit de tirer parti de la licence BYOL pour établir et ne pas dépasser un total de 20 connexions individuelles entre une source et une cible (chaque " relation de synchronisation ").
- Le droit d'un client expire à la fin de la période d'un an de licence, que le Client ait atteint la limite de 20 relations de synchronisation.
- Si le Client choisit de renouveler sa licence, les relations de synchronisation non utilisées associées à l'octroi de licence précédent ne passent PAS au renouvellement de la licence.

Confidentialité des données

NetApp n'a pas accès aux identifiants que vous indiquez lors de l'utilisation du service Cloud Sync. Les informations d'identification sont stockées directement sur l'ordinateur du courtier de données, qui réside dans votre réseau.

Selon la configuration choisie, Cloud Sync peut vous demander des informations d'identification lorsque vous créez une nouvelle relation. Par exemple, lors de la configuration d'une relation qui inclut un serveur SMB, ou lors du déploiement du courtier en données dans AWS.

Ces informations d'identification sont toujours enregistrées directement dans le data broker lui-même. Le courtier en données réside sur une machine de votre réseau, qu'elle soit hébergée sur site ou dans votre compte cloud. Les informations d'identification ne sont jamais mises à la disposition de NetApp.

Les informations d'identification sont chiffrées localement sur la machine du courtier de données à l'aide de HashiCorp Vault.

Limites

- Cloud Sync n'est pas pris en charge en Chine.
- Outre la Chine, le courtier de données Cloud Sync n'est pas pris en charge dans les régions suivantes :
  - AWS GovCloud (États-Unis)
  - Azure US Gov
  - Azure US DoD

Commencez

Démarrage rapide de Cloud Sync

La mise en route du service Cloud Sync comprend quelques étapes.

Préparez votre source et votre cible

Vérifiez que la source et la cible sont prises en charge et configurées. L'exigence la plus importante est de vérifier la connectivité entre le courtier de données et les emplacements source et cible. "En savoir plus >>".

Préparez un emplacement pour le data broker NetApp

Le logiciel de courtier de données NetApp synchronise les données d'une source vers une cible (appelée « relation synchrone »). Vous pouvez exécuter le data broker dans AWS, Azure, Google Cloud Platform ou sur votre site. Le courtier de données a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels. "Afficher la liste des noeuds finaux".

Cloud Sync vous guide tout au long du processus d'installation lorsque vous créez une relation de synchronisation, à quel point vous pouvez déployer le data broker dans le cloud ou télécharger un script d'installation pour votre propre hôte Linux.

- "Consultez l'installation d'AWS"
- "Vérifiez l'installation d'Azure"
- "Vérifiez l'installation de GCP"
- "Vérifiez l'installation de l'hôte Linux"

Créez votre première relation de synchronisation

Connectez-vous à "Le gestionnaire Cloud", Cliquez sur **Sync**, puis faites glisser et déposez vos sélections pour la source et la cible. Suivez les invites pour terminer la configuration. "En savoir plus >>".

Payez vos relations de synchronisation après la fin de votre essai gratuit

Abonnez-vous à AWS ou Azure pour payer à votre gré ou pour payer chaque année. Ou achetez des licences directement auprès de NetApp. Il vous suffit d'aller à la page Paramètres de licence de Cloud Sync pour la configurer. "En savoir plus >>".

Préparation de la source et de la cible

Préparez la synchronisation des données en vérifiant que votre source et votre cible sont prises en charge et configurées.

Relations de synchronisation prises en charge

Cloud Sync vous permet de synchroniser des données d'une source vers une cible (appelée *sync relationship*). Vous devez comprendre les relations prises en charge avant de commencer.

Emplacement de la source	Emplacements cibles pris en charge
EFS AWS	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
AWS S3	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Blob d'Azure	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Fichiers NetApp Azure (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Azure NetApp Files (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Cloud Volumes ONTAP (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Cloud Volumes ONTAP (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Service de volumes cloud (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Cloud Volumes Service (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Google Cloud Storage	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID
IBM Cloud Object Storage	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Serveur NFS	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Cluster ONTAP sur site (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Cluster ONTAP sur site (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Stockage ONTAP S3	• StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Serveur SMB	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
StorageGRID	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • Stockage ONTAP S3 • Serveur SMB • StorageGRID

Remarques :

1. Vous pouvez choisir un niveau de stockage spécifique à Azure Blob lorsqu'un conteneur Blob est la cible :
    - Stockage à chaud
    - Stockage cool
2. lorsque AWS S3 est la cible, vous pouvez choisir une classe de stockage S3 spécifique :
    - Standard (il s'agit de la classe par défaut)
    - Le Tiering intelligent
    - Accès autonome et peu fréquent
    - Un seul accès à Zone-Infrequent
    - Glacier
    - Archives profondes des Glaciers

Mise en réseau de la source et de la cible

- La source et la cible doivent disposer d'une connexion réseau au data broker.

  Par exemple, si un serveur NFS se trouve dans votre data center et que le data broker est dans AWS, vous avez besoin d'une connexion réseau (VPN ou Direct Connect) entre votre réseau et le VPC.

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Exigences source et cible

Vérifiez que votre source et vos cibles répondent aux exigences suivantes.

exigences du compartiment AWS S3

Assurez-vous que votre seau AWS S3 répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour AWS S3

Les relations de synchronisation qui incluent le stockage S3 nécessitent un data broker déployé dans AWS ou sur votre site. Dans les deux cas, Cloud Sync vous invite à associer le courtier de données à un compte AWS lors de l'installation.

- "Découvrez comment déployer le courtier de données AWS"
- "Découvrez comment installer le courtier de données sur un hôte Linux"

Régions AWS prises en charge

Toutes les régions sont prises en charge à l'exception des régions Chine et GovCloud (États-Unis).

Autorisations requises pour les compartiments S3 dans d'autres comptes AWS

Lors de la configuration d'une relation de synchronisation, vous pouvez spécifier un compartiment S3 qui réside dans un compte AWS non associé au courtier de données.

"Les autorisations incluses dans ce fichier JSON" Doit être appliqué au compartiment S3 pour que le courtier de données puisse y accéder. Ces autorisations permettent au courtier de copier des données depuis et vers la rubrique et de lister les objets dans la rubrique.

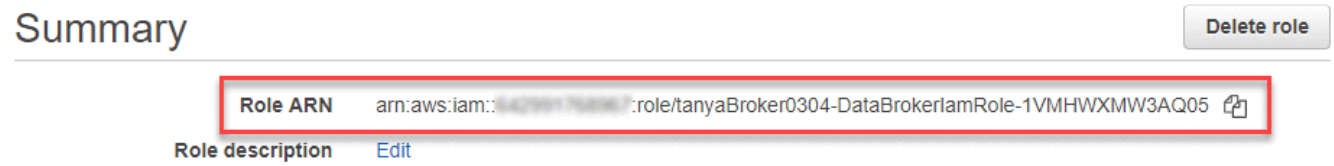
Notez les informations suivantes sur les autorisations incluses dans le fichier JSON :

1. *<BucketName>* est le nom du compartiment qui réside dans le compte AWS non associé au courtier en données.
2. *<RoleARN>* doit être remplacé par l'un des éléments suivants :

   - Si le courtier de données a été installé manuellement sur un hôte Linux, *RoleARN* doit être l'ARN de l'utilisateur AWS pour lequel vous avez fourni des informations d'identification AWS lors du déploiement du courtier de données.
   - Si le courtier de données a été déployé dans AWS à l'aide du modèle CloudFormation, *RoleARN* doit être l'ARN du rôle IAM créé par le modèle.

     Vous pouvez trouver le nom ARN du rôle en accédant à la console EC2, en sélectionnant l'instance du

courtier de données et en cliquant sur le rôle IAM dans l'onglet Description. La page Résumé de la console IAM qui contient le numéro de référence du rôle doit apparaître.



exigences de stockage Azure Blob

Assurez-vous que votre stockage Azure Blob répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour Azure Blob

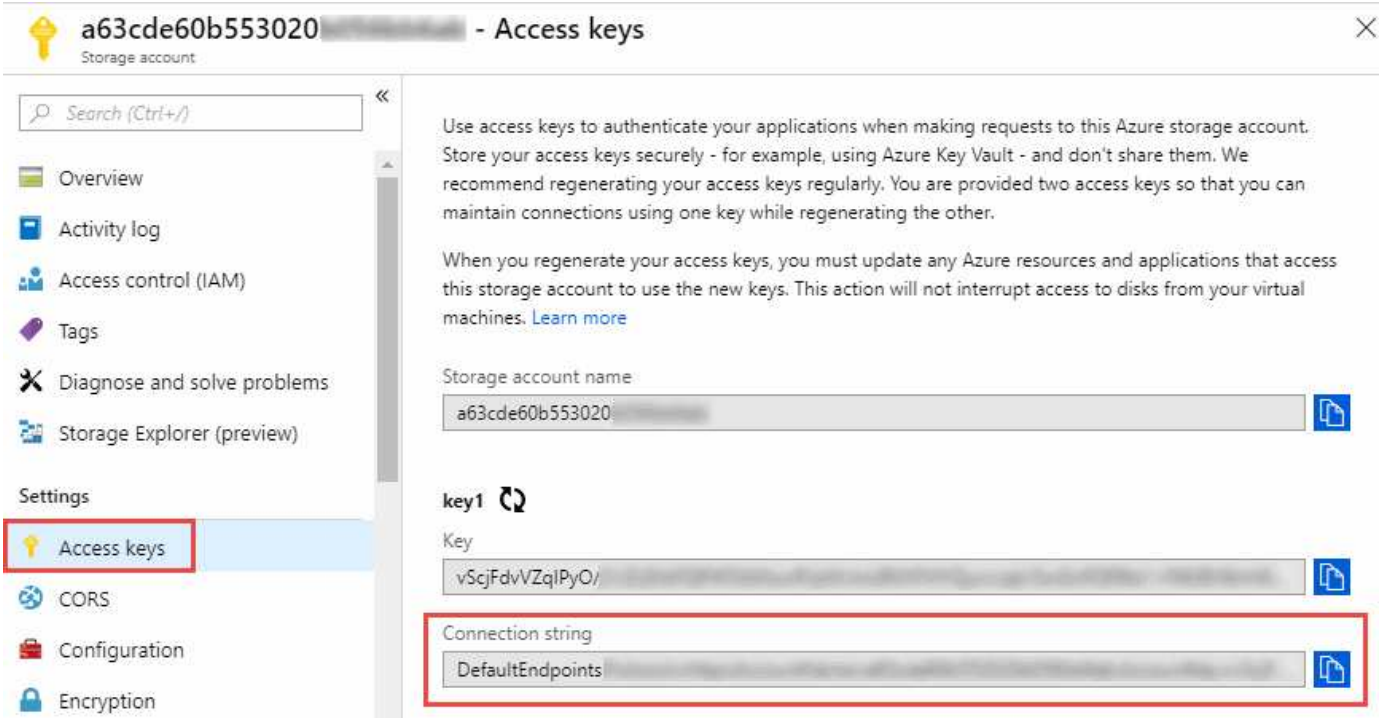
Le courtier de données peut résider dans n'importe quel emplacement lorsqu'une relation de synchronisation inclut le stockage Blob d'Azure.

Régions Azure prises en charge

Toutes les régions sont prises en charge à l'exception des régions China, US Gov et US DoD.

Chaîne de connexion requise pour les relations qui incluent Azure Blob et NFS/SMB

Lors de la création d'une relation synchrone entre un conteneur Azure Blob et un serveur NFS ou SMB, vous devez fournir à Cloud Sync la chaîne de connexion du compte de stockage :

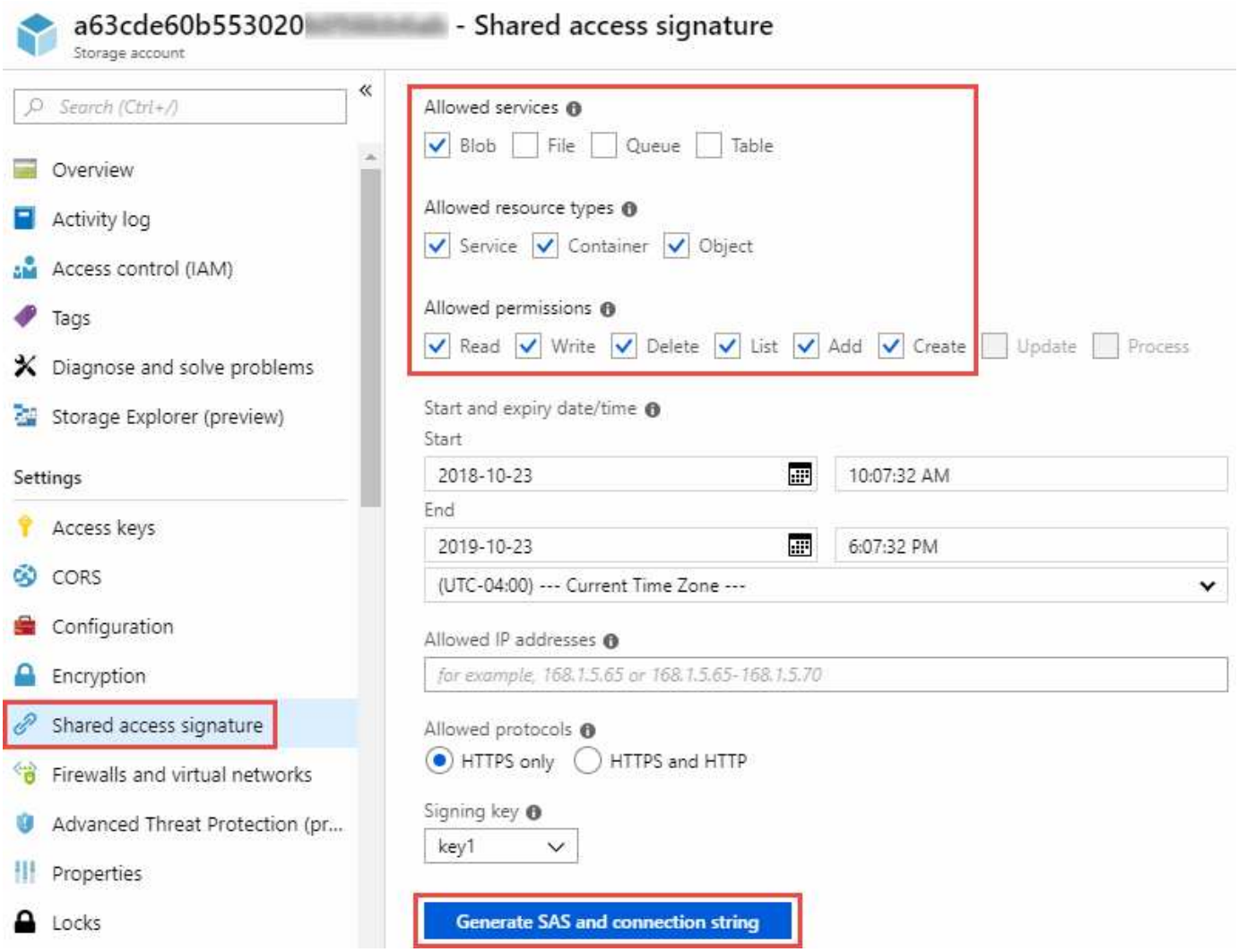


Pour synchroniser les données entre deux conteneurs Azure Blob, la chaîne de connexion doit inclure une "signature d'accès partagé" (SAS). Vous avez également la possibilité d'utiliser un SAS lors de la synchronisation entre un conteneur Blob et un serveur NFS ou SMB.

Le SAS doit autoriser l'accès au service Blob et à tous les types de ressources (Service, Conteneur et Objet).

Le SAS doit également inclure les autorisations suivantes :

- Pour le conteneur Blob source : Lecture et liste
- Pour le conteneur Blob cible : lecture, écriture, liste, ajout et création



Condition Azure NetApp Files

Utilisez le niveau de service Premium ou Ultra lorsque vous synchronisez des données vers ou depuis Azure NetApp Files. Vous risquez de rencontrer des défaillances et des problèmes de performances si le niveau de service des disques est standard.

Consultez un architecte de solutions si vous avez besoin d'aide pour déterminer le niveau de service adapté à vos besoins. La taille et le niveau de volume déterminent le débit pouvant être optimal.

"En savoir plus sur le débit et les niveaux de service de Azure NetApp Files".

Exigences relatives au compartiment de stockage Google Cloud

Assurez-vous que votre rayon de stockage Google Cloud Storage répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour Google Cloud Storage

Les relations de synchronisation qui incluent Google Cloud Storage nécessitent un data broker déployé dans GCP ou sur votre site. Cloud Sync vous guide tout au long du processus d'installation du courtier de données lorsque vous créez une relation de synchronisation.

- "Découvrez comment déployer le courtier de données GCP"
- "Découvrez comment installer le courtier de données sur un hôte Linux"

Régions GCP prises en charge

Toutes les régions sont prises en charge.

Configuration requise pour le serveur NFS

- Le serveur NFS peut être un système NetApp ou un système non NetApp.
- Le serveur de fichiers doit permettre à l'hôte du courtier de données d'accéder aux exportations.
- Les versions NFS 3, 4.0, 4.1 et 4.2 sont prises en charge.

  La version souhaitée doit être activée sur le serveur.

- Si vous souhaitez synchroniser les données NFS à partir d'un système ONTAP, assurez-vous que l'accès à la liste d'export NFS pour un SVM est activé (vserver nfs modify -vserver *svm_name* -showmount activé).

  Le paramètre par défaut de showmount est *Enabled* commençant par ONTAP 9.2.

Exigences du stockage ONTAP S3

ONTAP 9.7 prend en charge Amazon simple Storage Service (Amazon S3) comme préversion publique. "En savoir plus sur la prise en charge d'ONTAP pour Amazon S3".

Lorsque vous configurez une relation de synchronisation incluant le stockage ONTAP S3, vous devez fournir les éléments suivants :

- L'adresse IP du LIF connecté à ONTAP S3
- La clé d'accès et la clé secrète que ONTAP est configuré pour utiliser

Configuration requise pour le serveur SMB

- Le serveur SMB peut être un système NetApp ou un système non NetApp.
- Le serveur de fichiers doit permettre à l'hôte du courtier de données d'accéder aux exportations.
- Les versions SMB 1.0, 2.0, 2.1, 3.0 et 3.11 sont prises en charge.
- Accordez au groupe « administrateurs » les autorisations « contrôle total » aux dossiers source et cible.

  Si vous n'accordez pas cette autorisation, le courtier de données peut ne pas disposer des autorisations suffisantes pour obtenir les listes de contrôle d'accès sur un fichier ou un répertoire. Si cela se produit, vous recevrez l'erreur suivante : "erreur getxattr 95"

Limitation SMB pour les répertoires et les fichiers cachés

Une limitation SMB affecte les répertoires et les fichiers masqués lors de la synchronisation des données entre les serveurs SMB. Si l'un des répertoires ou des fichiers du serveur SMB source était masqué par Windows, l'attribut masqué n'est pas copié sur le serveur SMB cible.

Comportement de la synchronisation SMB en raison d'une limitation de la sensibilité au cas

Le protocole SMB n'est pas sensible à la casse, ce qui signifie que les lettres majuscules et minuscules sont traitées comme étant les mêmes. Ce comportement peut entraîner un écrasement des fichiers et des erreurs de copie de répertoire si une relation de synchronisation inclut un serveur SMB et que des données existent déjà sur la cible.

Par exemple, disons qu'il y a un fichier nommé « a » sur la source et un fichier nommé « A » sur la cible. Lorsque Cloud Sync copie le fichier nommé « a » sur la cible, le fichier « A » est remplacé par le fichier « a » de la source.

Dans le cas des répertoires, disons qu'il y a un répertoire nommé "b" sur la source et un répertoire nommé "B" sur la cible. Lorsque Cloud Sync tente de copier le répertoire nommé « b » vers la cible, Cloud Sync reçoit une erreur indiquant que le répertoire existe déjà. Par conséquent, Cloud Sync ne parvient toujours pas à copier le répertoire nommé "b."

La meilleure façon d'éviter cette limitation est de garantir la synchronisation des données vers un répertoire vide.

Autorisations d'accès à une destination SnapMirror

Si la source d'une relation de synchronisation est une destination SnapMirror (en lecture seule), des autorisations « read/list » suffisent pour synchroniser les données de la source vers une cible.

Présentation de la mise en réseau pour Cloud Sync

La mise en réseau pour Cloud Sync inclut la connectivité entre le courtier de données et les emplacements source et cible, ainsi qu'une connexion Internet sortante du courtier de données sur le port 443.

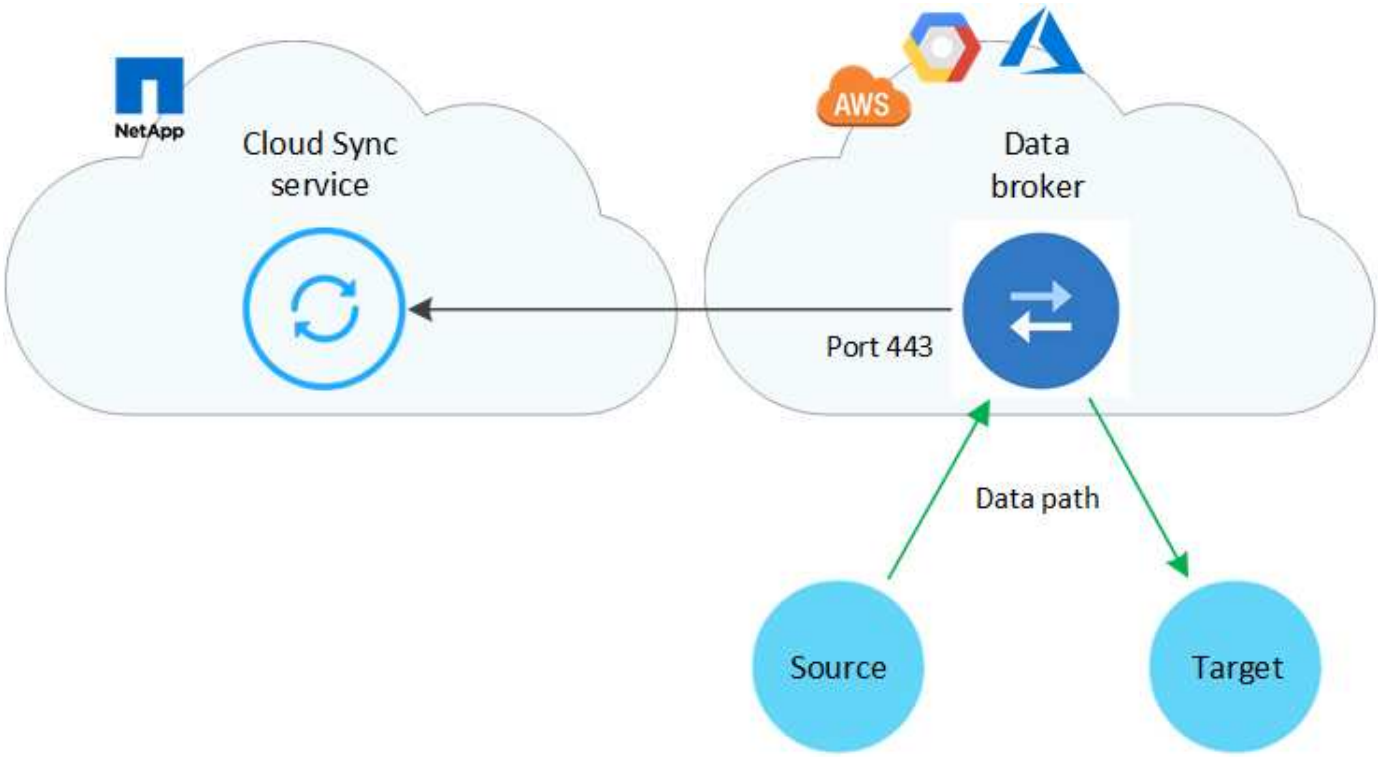
Emplacement du courtier en données

Vous pouvez installer le courtier en données dans le cloud ou sur site.

Data broker dans le cloud

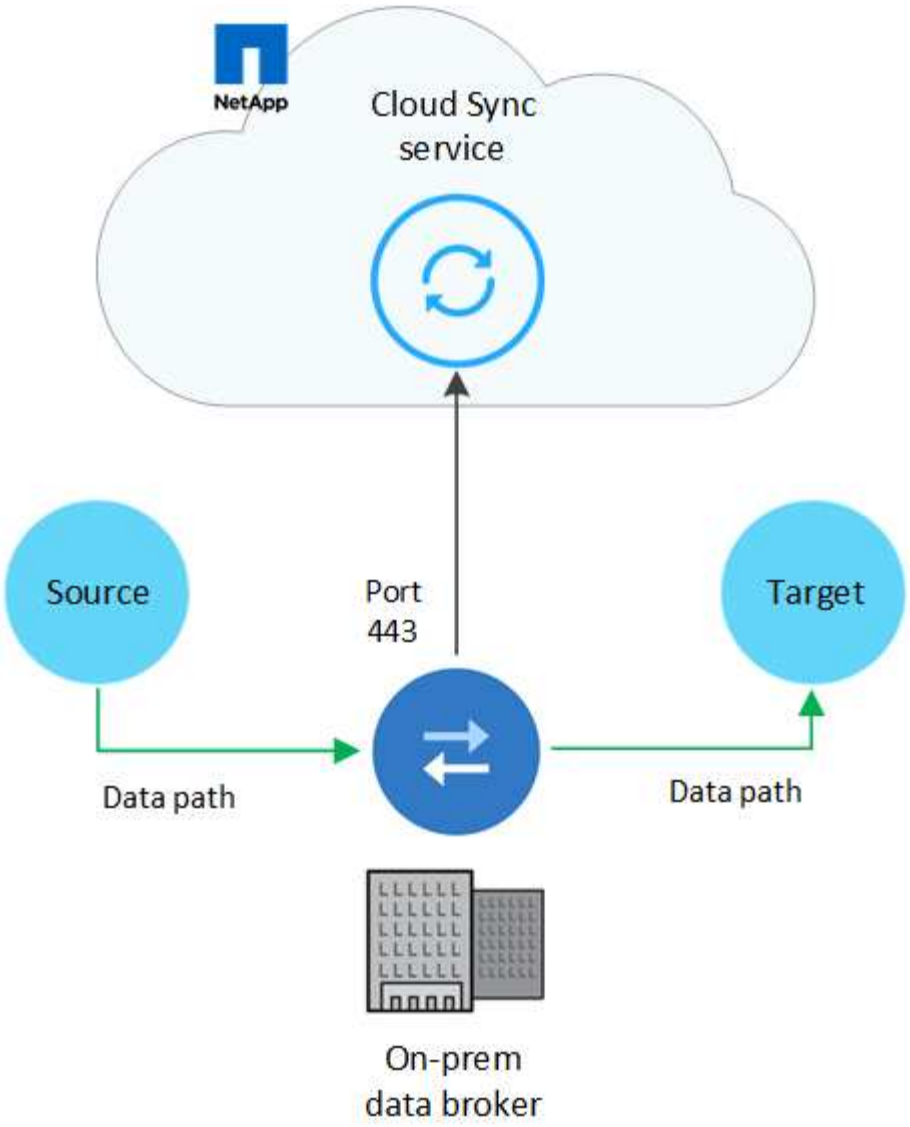
L'image suivante montre le courtier en données qui s'exécute dans le cloud, soit dans AWS, GCP ou Azure. La source et la cible peuvent être hébergées quel que soit le lieu, à condition que le courtier soit connecté. Par exemple, vous pouvez disposer d'une connexion VPN entre votre data center et votre fournisseur de cloud.

Lorsque Cloud Sync déploie le courtier de données dans AWS, Azure ou GCP, il crée un groupe de sécurité qui active la communication sortante requise.



Data broker sur votre site

L'image suivante montre le courtier de données qui s'exécute sur-prem, dans un data center. Là encore, la source et la cible peuvent être hébergées quel que soit le lieu, tant qu'il y a une connexion avec le courtier de données.



Configuration réseau requise

- La source et la cible doivent disposer d'une connexion réseau au data broker.

  Par exemple, si un serveur NFS se trouve dans votre data center et que le data broker est dans AWS, vous avez besoin d'une connexion réseau (VPN ou Direct Connect) entre votre réseau et le VPC.

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.
- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Terminaux de mise en réseau

Pour communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels, le courtier de données NetApp a besoin d'un accès Internet sortant sur le port 443. Votre navigateur Web local nécessite également l'accès aux points de terminaison pour certaines actions. Si vous devez limiter la connectivité sortante, reportez-vous à la liste de terminaux suivante lors de la configuration de votre pare-feu pour le trafic sortant.

Terminaux du courtier de données

Le courtier de données contacte les terminaux suivants :

Terminaux	Objectif
Olcentgbl.trafficmanager.net:443	Pour contacter un référentiel de mise à jour des packages CentOS pour l'hôte du data broker. Ce noeud final n'est contacté que si vous installez manuellement le courtier de données sur un hôte CentOS.
Rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Pour contacter des référentiels pour mettre à jour Node.js, npm et d'autres packages tiers utilisés dans le développement.
Tgz.pm2.io:443	Pour accéder à un référentiel de mise à jour de PM2, un package tiers utilisé pour surveiller Cloud Sync.
Www.myrc.com/fr/ www.myrc.com/fr/ www.myrc.com/fr/ www.myrc.com/fr/	Pour contacter les services AWS utilisés par Cloud Sync pour les opérations (mise en file d'attente de fichiers, enregistrement d'actions et mise à jour du data broker).
s3.*region*.amazonaws.com:443 par exemple : s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["Consultez la documentation AWS pour obtenir la liste des terminaux S3"^]	Pour contacter Amazon S3 lorsqu'une relation de synchronisation inclut une rubrique S3.
Cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	Pour contacter le service Cloud Sync.
Support.netapp.com:443	Pour contacter le support NetApp lors de l'utilisation d'une licence BYOL pour les relations de synchronisation.
fedoraproject.org:443	Pour installer 7z sur la machine virtuelle du courtier de données pendant l'installation et les mises à jour. 7z est nécessaire pour envoyer des messages AutoSupport au support technique NetApp.

Terminaux de navigateur Web

Votre navigateur Web doit accéder au point final suivant pour télécharger les journaux à des fins de dépannage :

logs.cloudsync.netapp.com:443

Comment installer un courtier de données

Installation du courtier de données dans AWS

Lorsque vous créez une relation de synchronisation, choisissez l'option AWS Data Broker pour déployer le logiciel Data Broker sur une nouvelle instance EC2 dans un VPC. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou sur votre site. "En savoir plus >>".

Régions AWS prises en charge

Toutes les régions sont prises en charge à l'exception des régions Chine et GovCloud (États-Unis).

Configuration réseau requise

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.

  Lorsque Cloud Sync déploie le courtier de données dans AWS, il crée un groupe de sécurité qui active la communication sortante requise. Notez que vous pouvez configurer le courtier de données pour qu'il utilise un serveur proxy pendant le processus d'installation.

  Si vous devez limiter la connectivité sortante, reportez-vous à la section "liste des noeuds finaux que le courtier de données contacte".

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Autorisations requises pour déployer le courtier de données dans AWS

Le compte utilisateur AWS que vous utilisez pour déployer le courtier de données doit disposer des autorisations incluses dans "Politique fournie par NetApp".

pour utiliser votre propre rôle IAM avec le courtier de données AWS

Lorsque Cloud Sync déploie le data broker, il crée un rôle IAM pour l'instance du data broker. Si vous le souhaitez, vous pouvez déployer le data broker à l'aide de votre propre rôle IAM. Vous pouvez utiliser cette option si votre entreprise dispose de règles de sécurité strictes.

Le rôle IAM doit répondre aux exigences suivantes :

- Le service EC2 doit être autorisé à assumer le rôle IAM en tant qu'entité de confiance.
- "Les autorisations définies dans ce fichier JSON" Doit être attaché au rôle IAM pour que le courtier de données puisse fonctionner correctement.

Suivez les étapes ci-dessous pour spécifier le rôle IAM lors du déploiement du courtier de données.

Installation du data broker

Vous pouvez installer un courtier de données dans AWS lorsque vous créez une relation de synchronisation.

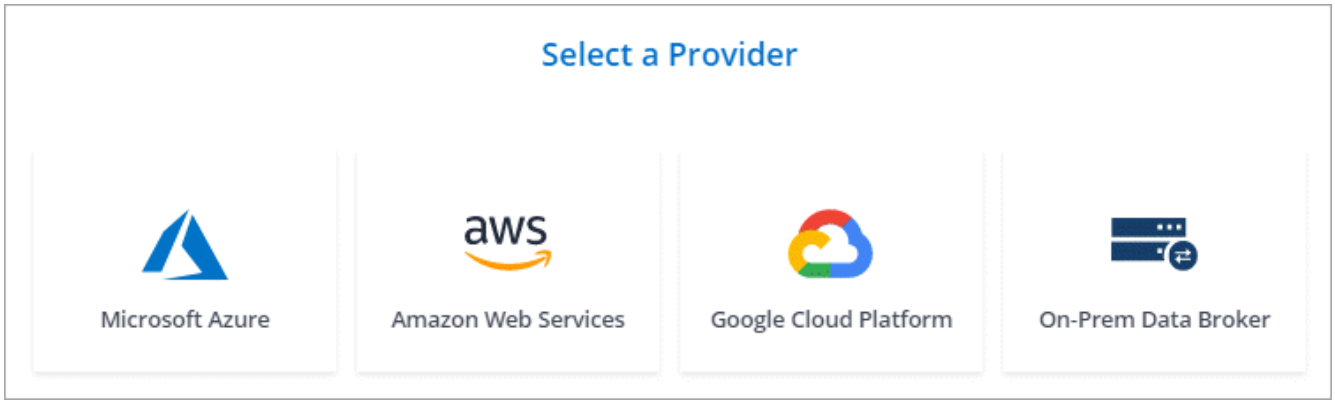
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Suivez les étapes jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **Amazon Web Services**.

   Si vous avez déjà un courtier de données, vous devez cliquer sur le + icône en premier.



4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.
5. Entrez une clé d'accès AWS pour que Cloud Sync crée le courtier en données dans AWS.

   Les touches ne sont pas enregistrées ou utilisées à d'autres fins.

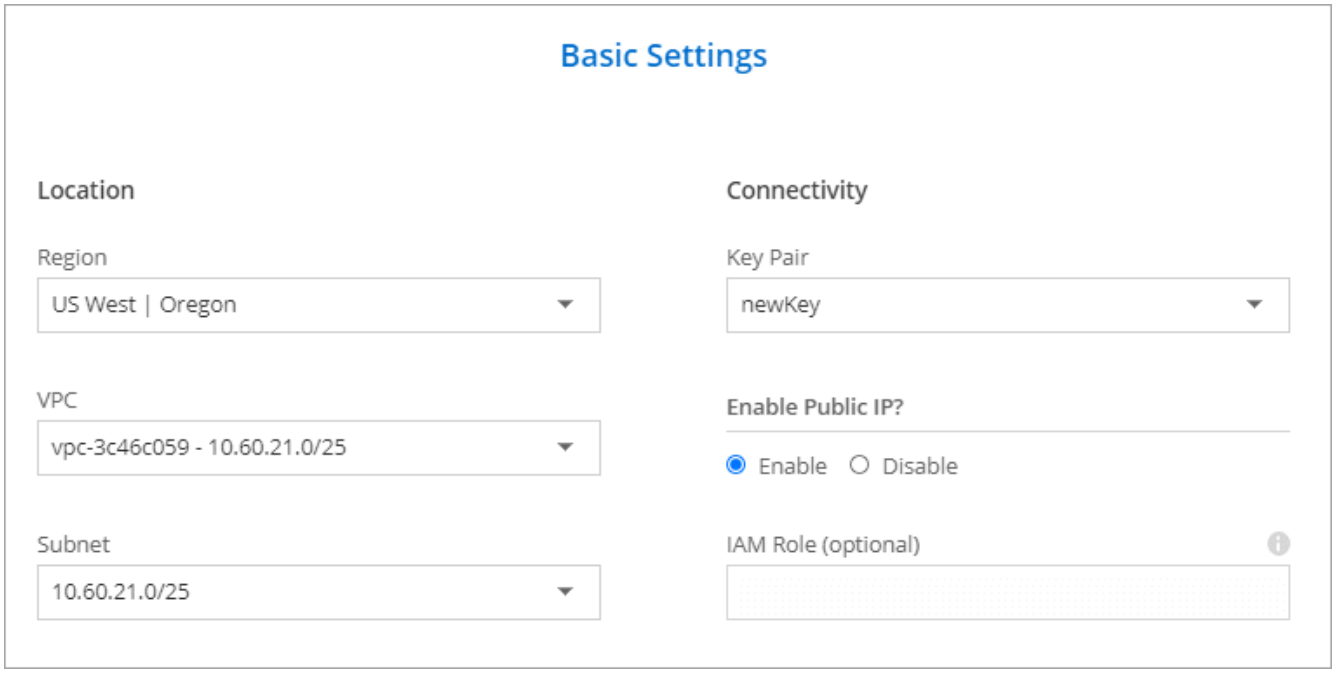
   Si vous préférez ne pas fournir de touches d'accès, cliquez sur le lien en bas de la page pour utiliser un modèle CloudFormation. Lorsque vous utilisez cette option, vous n'avez pas besoin de fournir des identifiants, car vous vous connectez directement à AWS.

   la vidéo suivante montre comment lancer l'instance de courtier de données à l'aide d'un modèle CloudFormation :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_cloud_sync.mp4 *(video)*

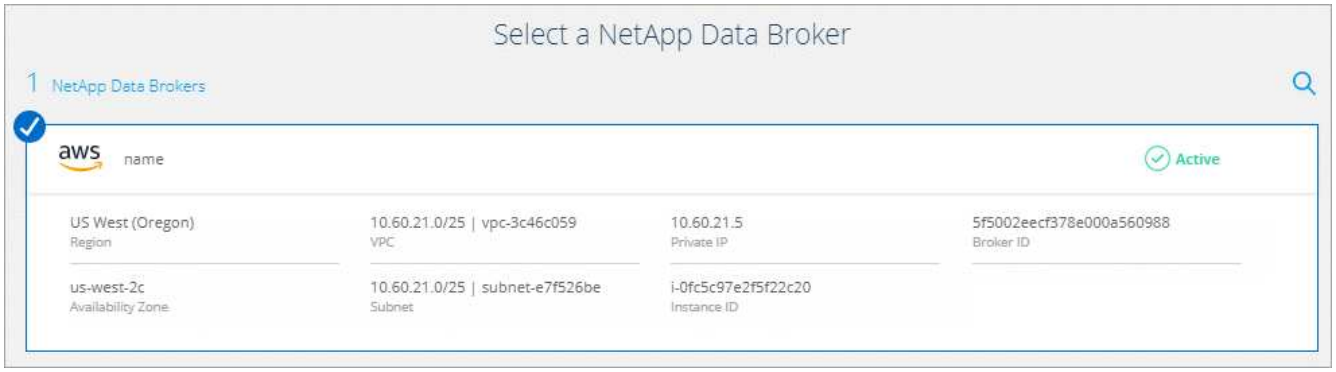
6. Si vous avez saisi une clé d'accès AWS, sélectionnez un emplacement pour l'instance, sélectionnez une paire de clés, choisissez d'activer ou non une adresse IP publique, puis sélectionnez un rôle IAM existant, ou laissez le champ vide afin que Cloud Sync crée le rôle pour vous.

   Si vous choisissez votre propre rôle IAM, vous devrez fournir les autorisations requises.



7. Une fois le courtier de données disponible, cliquez sur **Continuer** dans Cloud Sync.

L'image suivante montre une instance déployée avec succès dans AWS :



8. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Résultat

Vous avez déployé un courtier de données dans AWS et créé une nouvelle relation de synchronisation. Vous pouvez utiliser ce data broker avec des relations de synchronisation supplémentaires.

Installation du data broker dans Azure

Lorsque vous créez une relation de synchronisation, choisissez l'option Azure Data Broker pour déployer le logiciel Data Broker sur une nouvelle machine virtuelle dans un VNet. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou sur votre site. "En savoir plus >>".

Régions Azure prises en charge

Toutes les régions sont prises en charge à l'exception des régions China, US Gov et US DoD.

Configuration réseau requise

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.

  Lorsque Cloud Sync déploie le courtier de données dans Azure, il crée un groupe de sécurité qui active la communication sortante requise.

  Si vous devez limiter la connectivité sortante, reportez-vous à la section "liste des noeuds finaux que le courtier de données contacte".

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

METHODE d'authentification

Lorsque vous déployez le courtier de données, vous devrez choisir une méthode d'authentification : un mot de passe ou une paire de clés publiques-privées SSH.

Pour obtenir de l'aide sur la création d'une paire de clés, reportez-vous à la section "Documentation Azure : créez et utilisez une paire de clés publiques-privées SSH pour les machines virtuelles Linux dans Azure".

Installation du data broker

Vous pouvez installer un courtier de données dans Azure lorsque vous créez une relation de synchronisation.

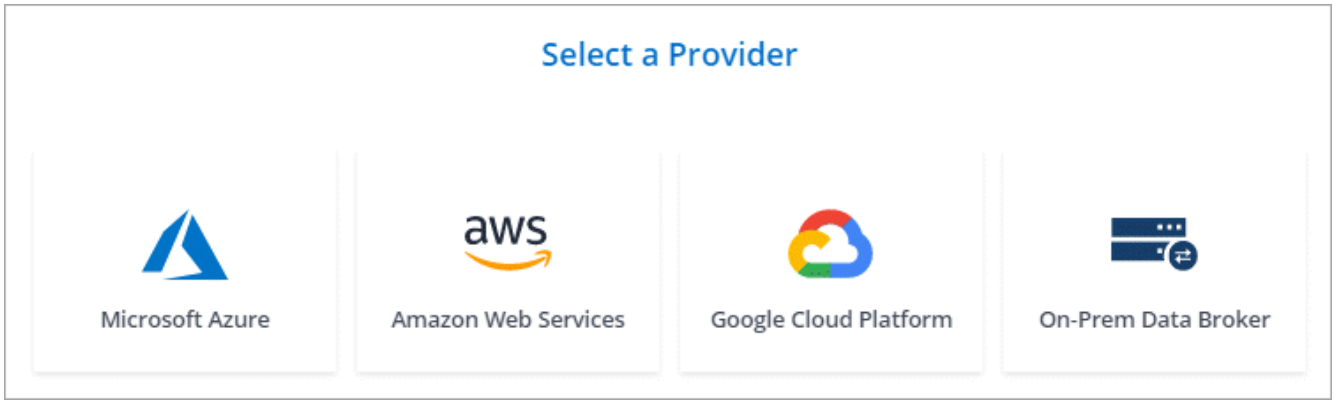
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Complétez les pages jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **Microsoft Azure**.

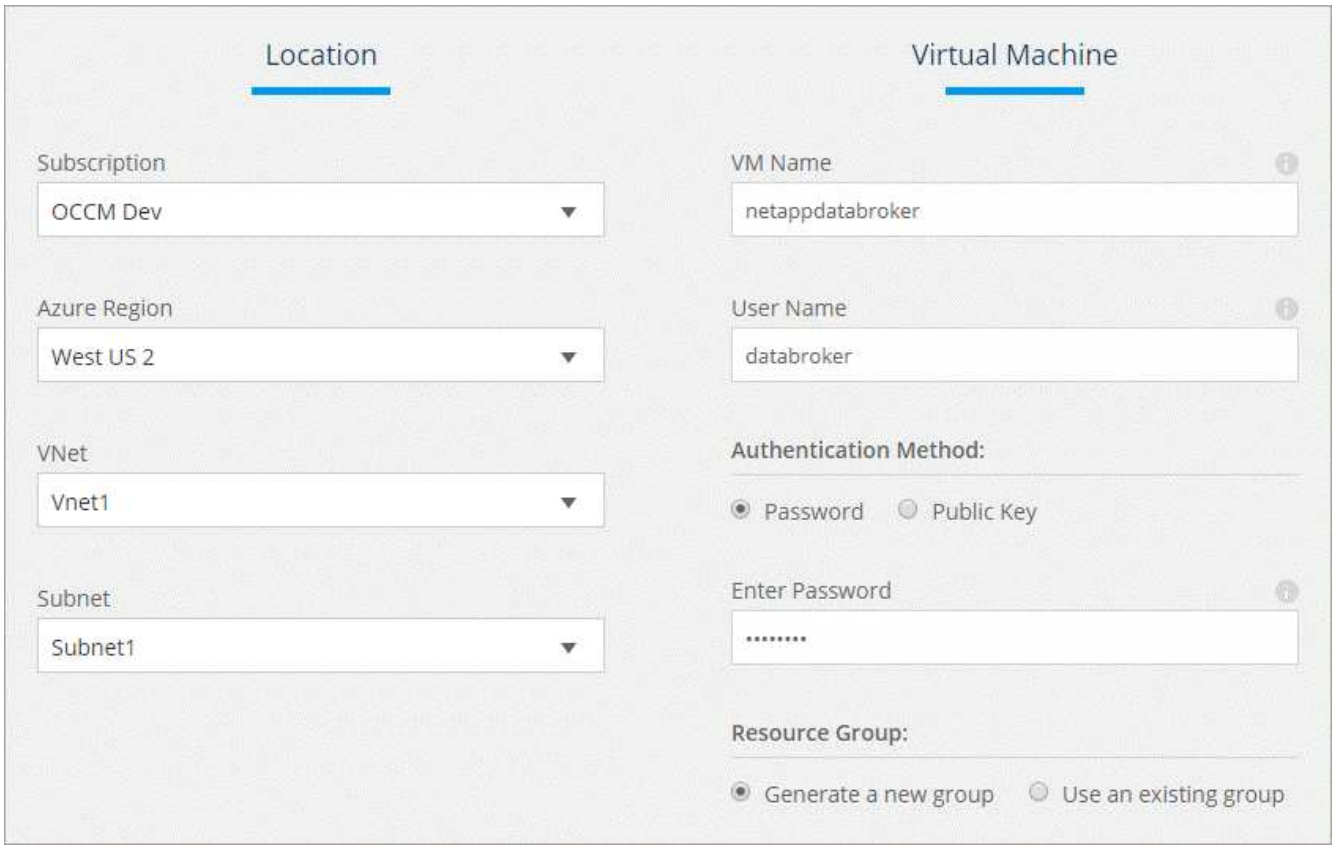
   Si vous avez déjà un courtier de données, vous devez cliquer sur le + icône en premier.



4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à votre compte Microsoft. Si vous n'êtes pas invité, cliquez sur **connexion à Azure**.

   Ce formulaire est détenu et hébergé par Microsoft. Vos identifiants ne sont pas fournis à NetApp.

6. Choisissez un emplacement pour le courtier de données et entrez les informations de base sur la machine virtuelle.



7. Cliquez sur **Continuer** et maintenez la page ouverte jusqu'à ce que le déploiement soit terminé.

   Ce processus peut prendre jusqu'à 7 minutes.

8. Dans Cloud Sync, cliquez sur **Continuer** une fois le courtier de données disponible.
9. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Résultat

Vous avez déployé un courtier en données dans Azure et créé une nouvelle relation de synchronisation. Vous pouvez utiliser ce data broker avec des relations de synchronisation supplémentaires.

Vous obtenez un message sur le besoin d'un consentement de l'administrateur ?

Si Microsoft vous informe que l'administrateur doit être approuvé, car Cloud Sync doit disposer d'une autorisation d'accès aux ressources de votre entreprise pour votre compte, vous disposez de deux options :

1. Demandez à votre administrateur AD de vous fournir l'autorisation suivante :

   Dans Azure, accédez à **Admin Centers > Azure AD > utilisateurs et groupes > User Settings** et activez **les utilisateurs peuvent autoriser les applications à accéder aux données de l'entreprise en leur nom**.

2. Demandez à votre administrateur AD de consentir en votre nom à **CloudSync-AzureDataBrokerCreator** à l'aide de l'URL suivante (il s'agit du point de terminaison du consentement de l'administrateur) :

   https://login.microsoftonline.com/{FILL ICI VOTRE identifiant DE LOCATAIRE}/v2.0/adminConcey?client_ID=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   Comme indiqué dans l'URL, notre URL d'application est https://cloudsync.netapp.com et l'ID client de l'application est 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Installation du courtier en données dans Google Cloud Platform

Lorsque vous créez une relation de synchronisation, choisissez l'option GCP Data Broker pour déployer le logiciel Data Broker sur une nouvelle instance de machine virtuelle dans un VPC. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou sur votre site. "En savoir plus >>".

Régions GCP prises en charge

Toutes les régions sont prises en charge.

Configuration réseau requise

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.

  Lorsque Cloud Sync déploie le courtier de données dans GCP, il crée un groupe de sécurité qui active la communication sortante requise.

  Si vous devez limiter la connectivité sortante, reportez-vous à la section "liste des noeuds finaux que le courtier de données contacte".

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Autorisations requises pour déployer le courtier de données dans GCP

Assurez-vous que l'utilisateur GCP qui déploie le courtier de données dispose des autorisations suivantes :

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

Autorisations requises pour le compte de service

Lorsque vous déployez le courtier de données, vous devez sélectionner un compte de service disposant des autorisations suivantes :

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
```

Installation du data broker

Vous pouvez installer un courtier de données dans GCP lorsque vous créez une relation de synchronisation.

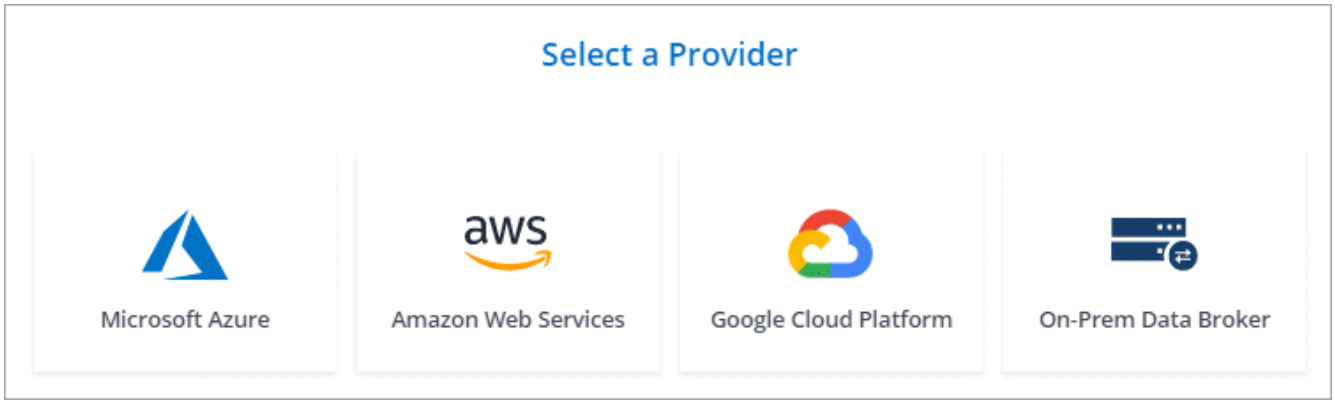
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Suivez les étapes jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **Google Cloud Platform**.

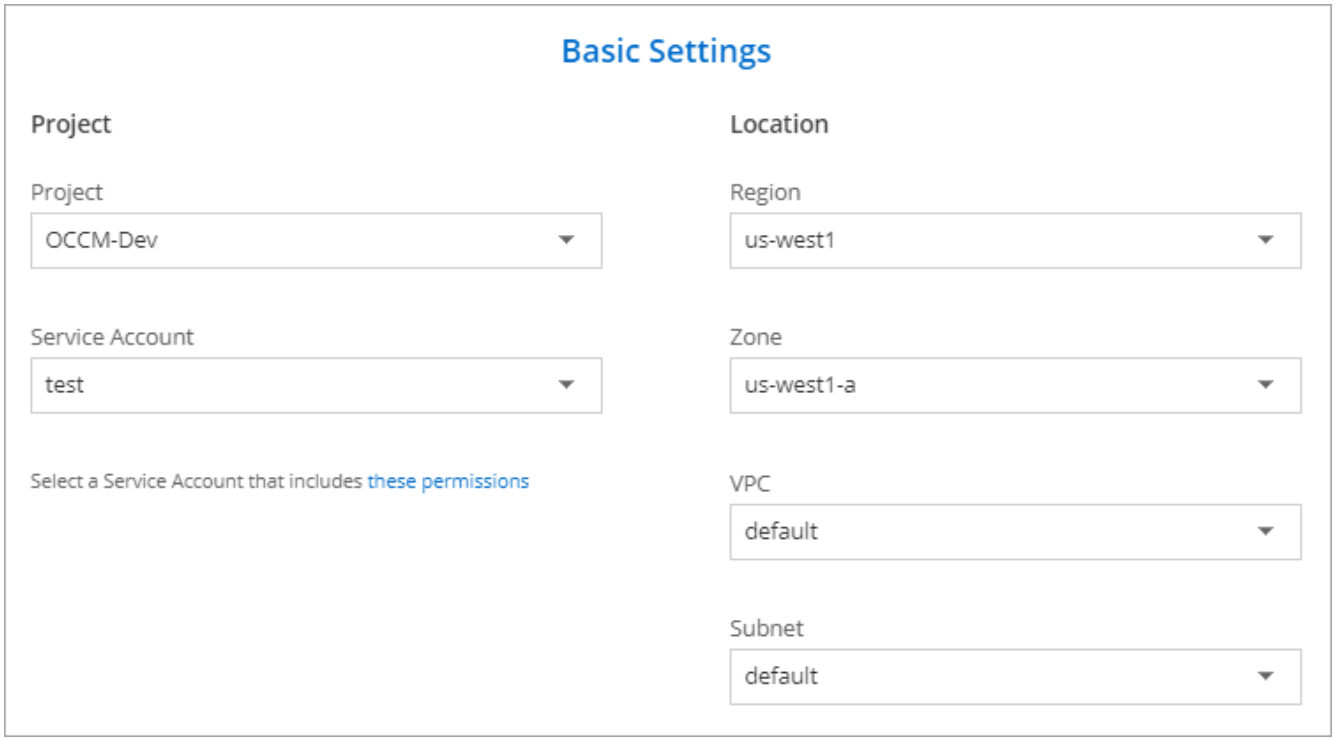
   Si vous avez déjà un courtier de données, vous devez cliquer sur le  icône en premier.



4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à l'aide de votre compte Google.

   Le formulaire est détenu et hébergé par Google. Vos identifiants ne sont pas fournis à NetApp.

6. Sélectionnez un compte de projet et de service, puis choisissez un emplacement pour le courtier de données.



7. Une fois le courtier de données disponible, cliquez sur **Continuer** dans Cloud Sync.

   Le déploiement de l'instance dure environ 5 à 10 minutes. Vous pouvez contrôler la progression à partir du service Cloud Sync, qui est automatiquement actualisé lorsque l'instance est disponible.

8. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Résultat

Vous avez déployé un courtier en données dans GCP et avez créé une nouvelle relation de synchronisation. Vous pouvez utiliser ce data broker avec des relations de synchronisation supplémentaires.

Installation du data broker sur un hôte Linux

Lorsque vous créez une relation de synchronisation, choisissez l'option On-Pem Data Broker pour installer le logiciel de courtier de données sur un hôte Linux sur site ou sur un hôte Linux existant dans le cloud. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Configuration requise pour l'hôte Linux

- **Système d'exploitation** :
  - CentOS 7.0, 7.7 et 8.0
  - Red Hat Enterprise Linux 7.7 et 8.0
  - Ubuntu Server 18.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    La commande `yum update all` doit être exécuté sur l'hôte avant d'installer le courtier de données.

  Un système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation.

- **RAM** : 16 GO
- **CPU** : 4 cœurs
- **Espace disque disponible**: 10 Go
- **SELinux**: Nous vous recommandons de désactiver "SELinux" sur l'hôte.

  SELinux applique une stratégie qui bloque les mises à jour logicielles des courtiers de données et peut empêcher le courtier de données de contacter les terminaux requis pour un fonctionnement normal.

- **OpenSSL** : OpenSSL doit être installé sur l'hôte Linux.

Configuration réseau requise

- L'hôte Linux doit être connecté à la source et à la cible.
- Le serveur de fichiers doit autoriser l'hôte Linux à accéder aux exportations.
- Le port 443 doit être ouvert sur l'hôte Linux pour le trafic sortant vers AWS (le courtier communique en permanence avec le service Amazon SQS).
- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Activation de l'accès à AWS

Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation incluant un compartiment S3, préparez l'hôte Linux pour l'accès AWS. Lorsque vous installez le courtier en données, vous devrez fournir les clés AWS pour un utilisateur AWS qui dispose d'un accès aux programmes et d'autorisations spécifiques.

Étapes

1. Créer une règle IAM à l'aide de "Politique fournie par NetApp". "Consultez les instructions AWS".
2. Créez un utilisateur IAM disposant d'un accès programmatique. "Consultez les instructions AWS".

   Assurez-vous de copier les clés AWS car vous devez les spécifier lors de l'installation du logiciel Data Broker.

Activation de l'accès à Google Cloud

Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation incluant un compartiment Google Cloud Storage, préparez l'hôte Linux pour l'accès GCP. Lorsque vous installez le courtier de données, vous devez fournir une clé pour un compte de service disposant d'autorisations spécifiques.

Étapes

1. Créez un compte de service GCP avec des autorisations d'administration du stockage, si vous n'en possédez pas déjà un.
2. Créez une clé de compte de service enregistrée au format JSON. "Affichez les instructions GCP".

   Le fichier doit contenir au moins les propriétés suivantes : "Project_ID", "Private_key" et "client_email"

   Lorsque vous créez une clé, le fichier est généré et téléchargé sur votre machine.

3. Enregistrez le fichier JSON sur l'hôte Linux.

Activation de l'accès à Microsoft Azure

L'accès à Azure est défini par relation en fournissant un compte de stockage et une chaîne de connexion dans l'assistant de synchronisation.

Installation du data broker

Vous pouvez installer un courtier de données sur un hôte Linux lorsque vous créez une relation de synchronisation.

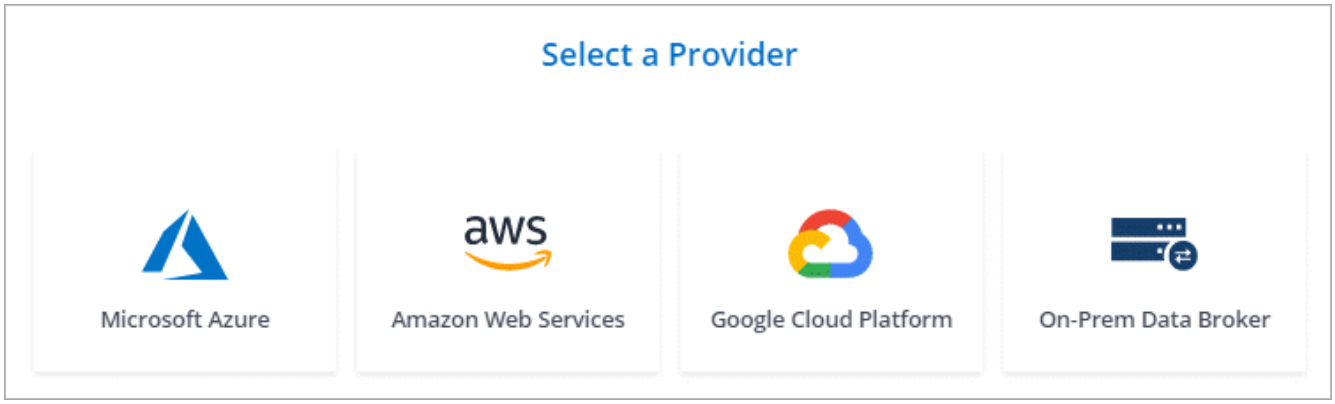
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Suivez les étapes jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **On-site Data Broker**.

   Si vous avez déjà un courtier de données, vous devez cliquer sur le + icône en premier.



Bien que cette option soit ***sur site*** **Data Broker**, elle s'applique à un hôte Linux sur site ou dans le cloud.

4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.

   La page d'instructions se charge sous peu. Vous devez suivre ces instructions --elles comprennent un lien unique pour télécharger le programme d'installation.

5. Sur la page d'instructions :
   a. Indiquez si vous souhaitez activer l'accès à **AWS**, **Google Cloud** ou aux deux.
   b. Sélectionnez une option d'installation : **pas de proxy**, **utilisez le serveur proxy** ou **utilisez le serveur proxy avec authentification**.
   c. Utilisez les commandes pour télécharger et installer le courtier de données.

      Les étapes suivantes fournissent des détails sur chaque option d'installation possible. Suivez la page d'instructions pour obtenir la commande exacte en fonction de votre option d'installation.

   d. Téléchargez le programme d'installation :
      - Aucun proxy :

        ```
        curl <URI> -o data_broker_installer.sh
        ```

      - Utiliser le serveur proxy :

        ```
        curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
        ```

      - Utilisez le serveur proxy avec l'authentification :

        ```
        curl <URI> -o data_broker_installer.sh -x
        <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
        ```

        URI

        Cloud Sync affiche l'URI du fichier d'installation sur la page d'instructions, qui se charge lorsque vous suivez les invites de déploiement du courtier de données sur site. Cet URI ne se répète pas ici car le lien est généré de manière dynamique et ne peut être utilisé qu'une seule fois. Procédez comme suit pour obtenir l'URI de Cloud Sync.

   e. Passez en mode superutilisateur, rendez le programme d'installation exécutable et installez le logiciel :

Chaque commande indiquée ci-dessous inclut des paramètres d'accès AWS et d'accès GCP. Suivez la page d'instructions pour obtenir la commande exacte en fonction de votre option d'installation.

- Pas de configuration proxy :

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file>
```

- Configuration du proxy :

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Configuration proxy avec authentification :

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

Clés AWS

Il s'agit des clés que vous devriez avoir préparées pour l'utilisateur voici la procédure à suivre. Les clés AWS sont stockées sur le courtier en données, qui s'exécute sur votre réseau sur site ou dans le cloud. NetApp n'utilise pas les clés en dehors du courtier en données.

Fichier JSON

Il s'agit du fichier JSON qui contient une clé de compte de service que vous devez avoir préparée voici la procédure à suivre.

6. Une fois le courtier de données disponible, cliquez sur **Continuer** dans Cloud Sync.
7. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Création d'une relation de synchronisation

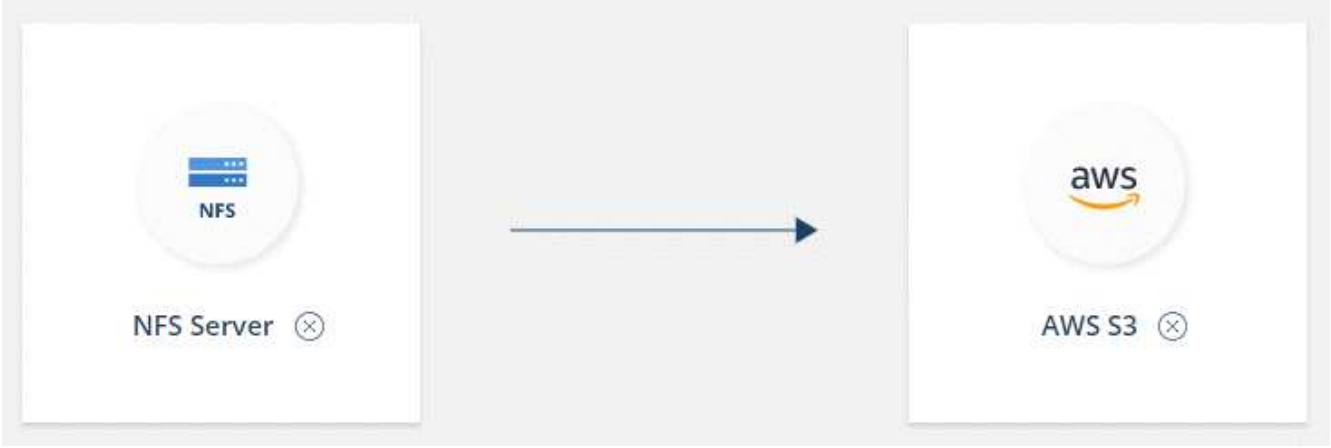
Lorsque vous créez une relation de synchronisation, le service Cloud Sync copie les fichiers de la source vers la cible. Après la copie initiale, le service synchronise les données modifiées toutes les 24 heures.

Les étapes ci-dessous fournissent un exemple de configuration d'une relation de synchronisation à partir d'un serveur NFS vers un compartiment S3.

Étapes

1. Dans Cloud Manager, cliquez sur **Sync**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible.

Les étapes suivantes fournissent un exemple de création d'une relation de synchronisation entre un serveur NFS et un compartiment S3.

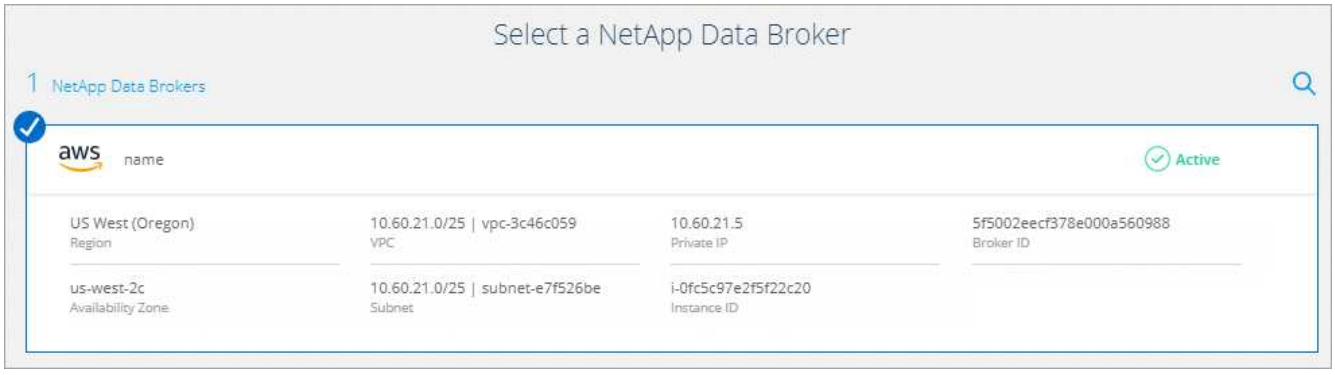


3. Sur la page **NFS Server**, entrez l'adresse IP ou le nom de domaine complet du serveur NFS que vous souhaitez synchroniser avec AWS.
4. Sur la page **Data Broker**, suivez les invites pour créer une machine virtuelle de courtier de données dans AWS, Azure ou Google Cloud Platform, ou pour installer le logiciel de courtier de données sur un hôte Linux existant.

   Pour plus de détails, reportez-vous aux pages suivantes :

   - "Installation du courtier de données dans AWS"
   - "Installation du data broker dans Azure"
   - "Installation du courtier de données dans GCP"
   - "Installation du data broker sur un hôte Linux"
5. Après avoir installé le courtier de données, cliquez sur **Continuer**.

   L'image suivante montre le déploiement réussi d'un courtier de données dans AWS :

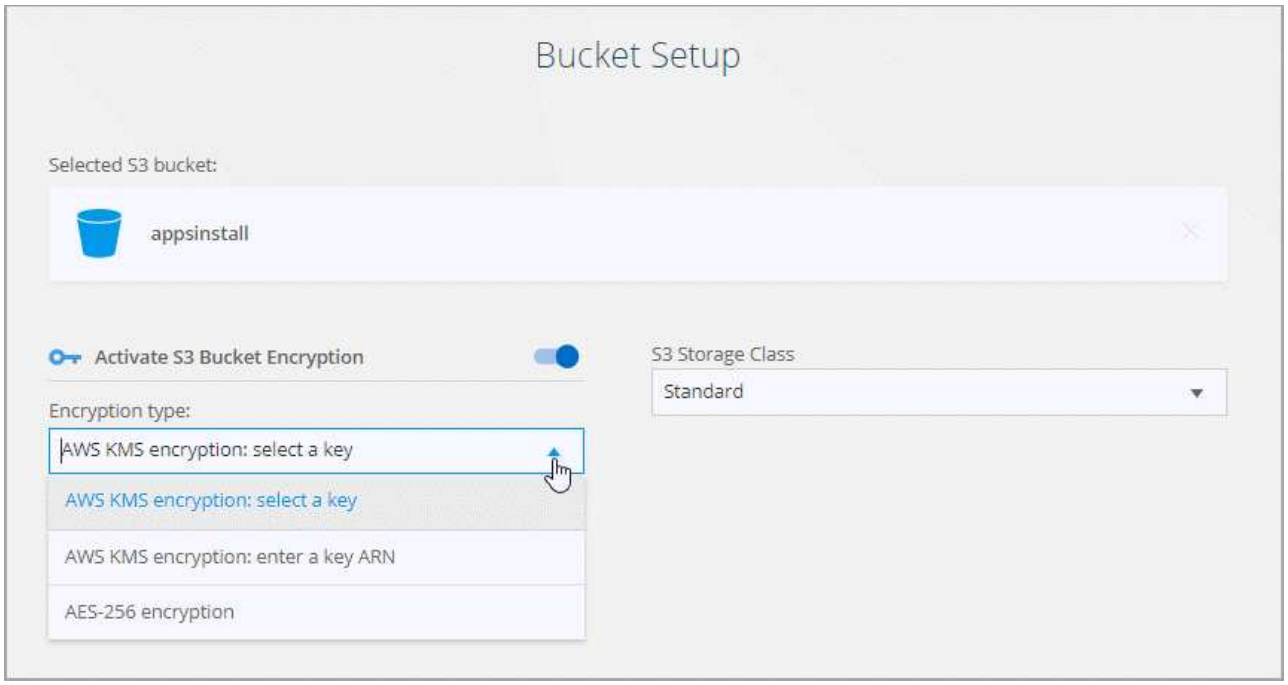


6. sur la page **répertoires**, sélectionnez un répertoire ou un sous-répertoire de niveau supérieur.

Si Cloud Sync ne parvient pas à récupérer les exportations, cliquez sur **Ajouter une exportation manuelle** et entrez le nom d'une exportation NFS.

Si vous souhaitez synchroniser plusieurs répertoires sur le serveur NFS, vous devez créer des relations de synchronisation supplémentaires après avoir terminé.

7. Sur la page **AWS S3 Bucket**, sélectionnez un compartiment :
   - Allez vers le bas pour sélectionner un dossier existant dans la rubrique ou pour sélectionner un nouveau dossier que vous créez dans la rubrique.
   - Cliquez sur **Ajouter à la liste** pour sélectionner un compartiment S3 qui n'est pas associé à votre compte AWS. "Des autorisations spécifiques doivent être appliquées au compartiment S3".
8. Sur la page **Configuration godet**, configurez le compartiment :
   - Optez pour l'activation du chiffrement des compartiments S3, puis sélectionnez une clé KMS AWS, saisissez l'ARN d'une clé KMS ou sélectionnez le chiffrement AES-256.
   - Sélectionnez une classe de stockage S3. "Afficher les classes de stockage prises en charge".



9. Sur la page **Paramètres**, définissez comment les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible :

Planification

Choisissez un programme récurrent pour les synchronisations ultérieures ou désactivez la planification de synchronisation. Vous pouvez planifier une relation pour synchroniser les données aussi souvent que toutes les 1 minute.

Tentatives

Définissez le nombre de tentatives de synchronisation d'un fichier par Cloud Sync avant de l'ignorer.

Fichiers récemment modifiés

Choisissez d'exclure les fichiers récemment modifiés avant la synchronisation planifiée.

Supprimer des fichiers sur la source

Choisissez de supprimer des fichiers de l'emplacement source une fois que Cloud Sync a copier les fichiers vers l'emplacement cible. Cette option inclut le risque de perte de données car les fichiers source sont supprimés après leur copie.

Si vous activez cette option, vous devez également modifier un paramètre dans le fichier local.json du courtier de données. Ouvrez le fichier et remplacez le paramètre nommé *workers.transferrer.delete-on-*

source par **true**.

Supprimer des fichiers sur la cible

Choisissez de supprimer des fichiers de l'emplacement cible, s'ils ont été supprimés de la source. La valeur par défaut est de ne jamais supprimer de fichiers de l'emplacement cible.

Balisage d'objets

Lorsque AWS S3 est la cible d'une relation de synchronisation, Cloud Sync balise les objets S3 avec des métadonnées pertinentes pour l'opération de synchronisation. Vous pouvez désactiver le balisage des objets S3 si ce n'est pas le cas dans votre environnement. Il n'y a aucun impact sur Cloud Sync si vous désactivez le balisage : Cloud Sync stocke simplement les métadonnées synchronisées d'une autre façon.

Types de fichiers

Définissez les types de fichiers à inclure dans chaque synchronisation : fichiers, répertoires et liens symboliques.

Exclure les extensions de fichier

Spécifiez les extensions de fichier à exclure de la synchronisation en tapant l'extension de fichier et en appuyant sur **entrée**. Par exemple, tapez *log* ou *.log* pour exclure les fichiers *.log. Un séparateur n'est pas nécessaire pour les extensions multiples. La vidéo suivante présente une courte démonstration :

► https://docs.netapp.com/fr-fr/occm38//media/video_file_extensions.mp4 *(video)*

Taille du fichier

Choisissez de synchroniser tous les fichiers, quelle que soit leur taille ou uniquement les fichiers qui se trouvent dans une plage de taille spécifique.

Date de modification

Choisissez tous les fichiers quelle que soit leur date de dernière modification, les fichiers modifiés après une date spécifique, avant une date spécifique ou entre une plage de temps.

10. Sur la page **Relationship Tags**, saisissez jusqu'à 9 balises de relation, puis cliquez sur **Continuer**.

    Le service Cloud Sync attribue les balises à chaque objet qu'il synchronise avec le compartiment S3.

11. Vérifiez les détails de la relation de synchronisation, puis cliquez sur **Créer une relation**.

Résultat

Cloud Sync démarre la synchronisation des données entre la source et la cible.

Payer pour la synchronisation après la fin de votre essai gratuit

Il existe deux façons de payer les relations de synchronisation après la fin de votre essai gratuit de 14 jours. La première option consiste à vous abonner à AWS ou Azure pour payer à votre gré ou à payer annuellement. La deuxième option consiste à acheter des licences directement auprès de NetApp.

Vous pouvez utiliser les licences de NetApp avec un abonnement AWS ou Azure. Par exemple, si vous disposez de 25 relations de synchronisation, vous pouvez payer les 20 premières relations de synchronisation à l'aide d'une licence, puis effectuer des opérations de paiement à la demande à partir d'AWS ou d'Azure avec les 5 autres relations de synchronisation.

"En savoir plus sur le fonctionnement des licences".

Que dois-je payer immédiatement après 8217 la fin de mon essai gratuit ?

Vous ne pourrez pas créer de relations supplémentaires. Les relations existantes ne sont pas supprimées, mais vous ne pouvez pas y apporter de modifications tant que vous n'êtes pas abonné ou que vous n'avez pas saisi de licence.

abonnement d'AWS

AWS vous permet de payer à votre gré ou de payer chaque année.

Les étapes à payer en tant que vous-même

1. Cliquez sur **Sync > licences**.
2. Sélectionnez **AWS**
3. Cliquez sur **s'abonner**, puis sur **Continuer**.
4. Abonnez-vous à AWS Marketplace, puis connectez-vous au service Cloud Sync pour terminer l'enregistrement.

   La vidéo suivante montre le processus :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_cloud_sync_registering.mp4 *(video)*

Étapes à payer annuellement

1. "Accédez à la page AWS Marketplace".
2. Cliquez sur **Continuer pour s'inscrire**.
3. Sélectionnez vos options de contrat et cliquez sur **Créer contrat**.

abonnement d'Azure

Azure vous permet de payer à votre gré ou de payer chaque année.

Ce dont vous avez besoin

Un compte utilisateur Azure disposant des autorisations Contributeur ou Propriétaire dans l'abonnement correspondant.

Étapes

1. Cliquez sur **Sync > licences**.
2. Sélectionnez **Azure**.
3. Cliquez sur **s'abonner**, puis sur **Continuer**.
4. Dans le portail Azure, cliquez sur **Créer**, sélectionnez vos options et cliquez sur **s'abonner**.

   Sélectionnez **mensuel** pour payer par heure, ou **annuel** pour payer une année avant.

5. Une fois le déploiement terminé, cliquez sur le nom de la ressource SaaS dans le menu contextuel de notification.
6. Cliquez sur **configurer le compte** pour revenir à Cloud Sync.

   La vidéo suivante montre le processus :

► https://docs.netapp.com/fr-fr/occm38//media/video_cloud_sync_registering_azure.mp4 *(video)*

achat de licences de NetApp et leur ajout à Cloud Sync

Pour payer vos relations de synchronisation, vous devez acheter une ou plusieurs licences et les ajouter au service Cloud Sync.

Étapes

1. Achetez une licence par contacter NetApp.
2. Dans Cloud Manager, cliquez sur **Sync > licences**.
3. Cliquez sur **Ajouter une licence** et ajoutez la licence.

Tutoriels

Copie de listes de contrôle d'accès entre partages SMB

Cloud Sync peut copier les listes de contrôle d'accès (ACL) entre un partage SMB source et un partage SMB cible. Si nécessaire, vous pouvez conserver manuellement les listes de contrôle d'accès vous-même en utilisant robocopy.

Choix

- Configurez Cloud Sync pour copier automatiquement les ACL
- Copiez manuellement les ACL vous-même

Configuration de Cloud Sync pour copier les ACL entre les serveurs SMB

Copiez les ACL entre serveurs SMB en activant un paramètre lors de la création d'une relation ou après la création d'une relation.

Notez que cette fonction est disponible pour les nouvelles relations de synchronisation créées après la version du 23 février 2020. Si vous souhaitez utiliser cette fonction avec des relations existantes créées avant cette date, vous devrez recréer la relation.

Ce dont vous avez besoin

- Une nouvelle relation de synchronisation ou une relation de synchronisation existante créée après la version 23 février 2020.
- Tout type de courtier en données.

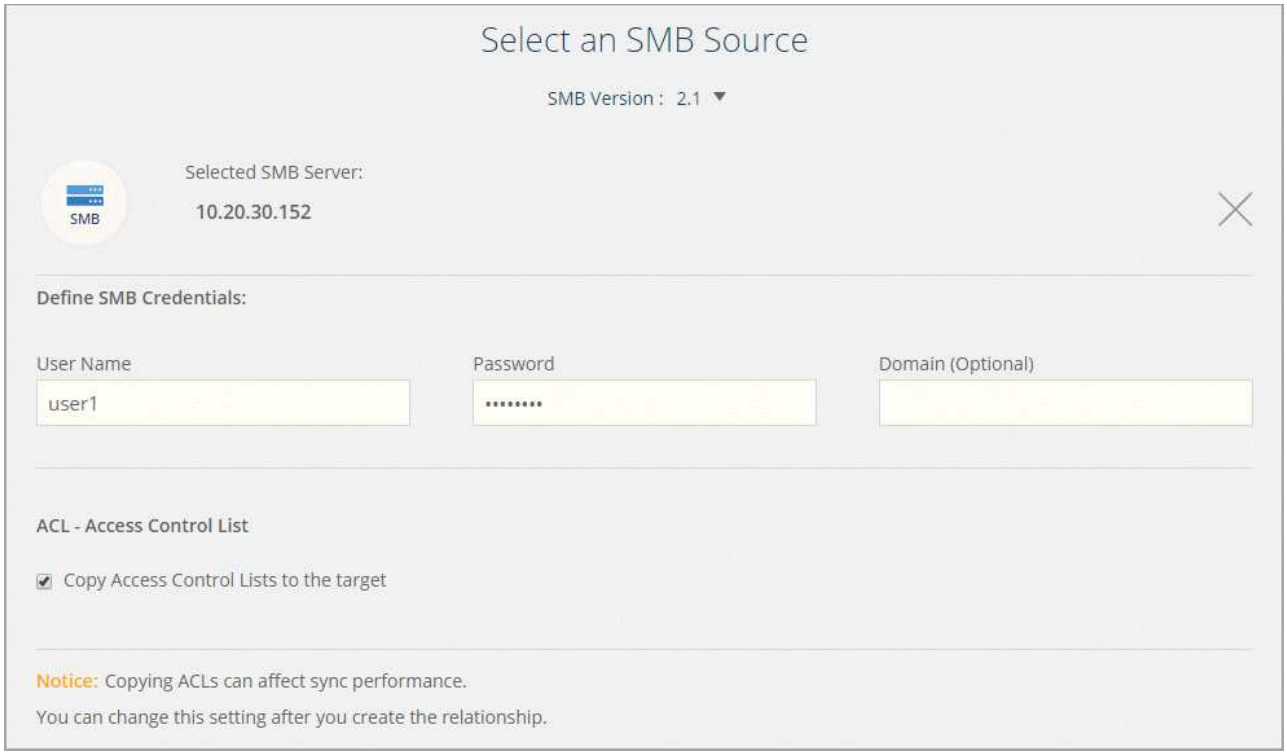
  Cette fonctionnalité fonctionne avec *tout* type de courtier en données : AWS, Azure, Google Cloud Platform ou comme courtier en données sur site. Le courtier en données sur site peut être exécuté "tout système d'exploitation pris en charge".

Étapes d'une nouvelle relation

1. Dans Cloud Sync, cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser **SMB Server** vers la source et la cible et cliquez sur **Continuer**.
3. Sur la page **SMB Server** :
   a. Entrez un nouveau serveur SMB ou sélectionnez un serveur existant et cliquez sur **Continuer**.

b. Saisissez les informations d'identification du serveur SMB.

c. Sélectionnez **Copier les listes de contrôle d'accès vers la cible** et cliquez sur **Continuer**.



4. Suivez les autres invites pour créer la relation de synchronisation.

Étapes d'une relation existante

1. Survolez la relation de synchronisation et cliquez sur le menu d'action.
2. Cliquez sur **Paramètres**.
3. Sélectionnez **Copier les listes de contrôle d'accès vers la cible**.
4. Cliquez sur **Enregistrer les paramètres**.

Résultat

Lors de la synchronisation des données, Cloud Sync préserve les ACL entre les partages SMB source et cible.

Copie manuelle des ACL

Vous pouvez conserver manuellement les listes de contrôle d'accès entre les partages SMB à l'aide de la commande Windows robocopy.

Étapes

1. Identifiez un hôte Windows qui dispose d'un accès complet aux deux partages SMB.
2. Si l'un des noeuds finaux nécessite une authentification, utilisez la commande **net use** pour vous connecter aux noeuds finaux à partir de l'hôte Windows.

   Vous devez effectuer cette étape avant d'utiliser Robocopy.

3. Dans Cloud Sync, créez une nouvelle relation entre les partages SMB source et cible ou synchronisez une relation existante.

4. Une fois la synchronisation des données terminée, exécutez la commande suivante à partir de l'hôte Windows pour synchroniser les ACL et la propriété :

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
/UNILOG:"[logfilepath]
```

Source et *target* doivent être spécifiés à l'aide du format UNC. Par exemple : \\<serveur>\<partage>\<chemin>

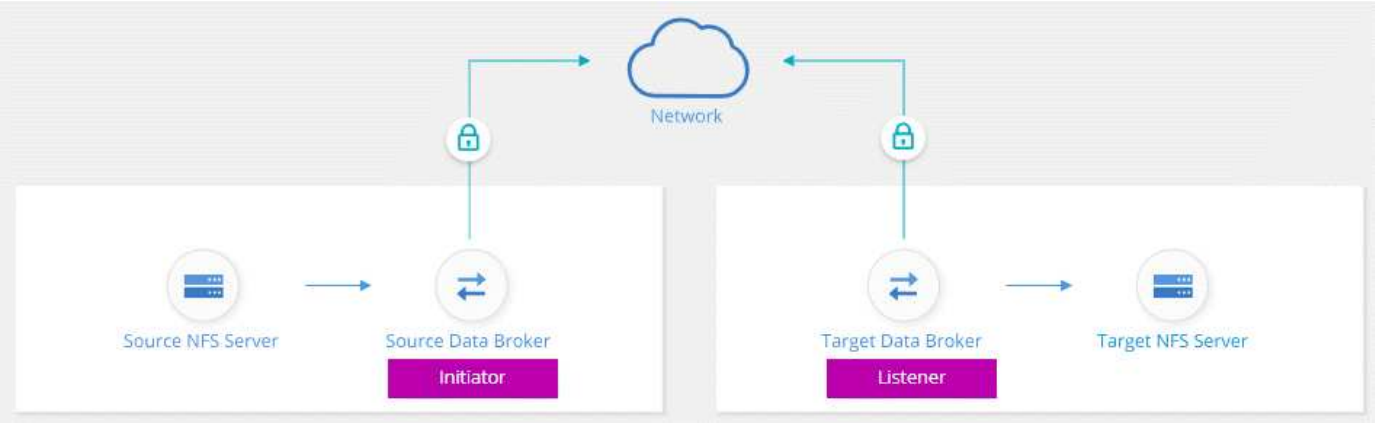
Synchronisation des données NFS à l'aide du chiffrement des données à la volée

Si votre entreprise dispose de règles de sécurité strictes, vous pouvez synchroniser les données NFS à l'aide du chiffrement des données à la volée. Cette fonctionnalité est prise en charge d'un serveur NFS vers un autre serveur NFS et de Azure NetApp Files vers Azure NetApp Files.

Par exemple, vous pouvez synchroniser des données entre deux serveurs NFS situés sur des réseaux différents. Ou bien vous devrez peut-être transférer des données sur Azure NetApp Files de manière sécurisée entre plusieurs sous-réseaux ou régions.

Fonctionnement du chiffrement des données en vol.

Le chiffrement des données à la volée crypte les données NFS lorsqu'elles sont transmises sur le réseau entre deux courtiers de données. L'image suivante montre une relation entre deux serveurs NFS et deux courtiers de données :



Un courtier de données fonctionne comme *initiator*. Lorsqu'il est temps de synchroniser des données, il envoie une demande de connexion à l'autre courtier de données, qui est le *listener*. Ce courtier de données écoute les demandes sur le port 443. Vous pouvez utiliser un autre port, si nécessaire, mais assurez-vous que le port n'est pas utilisé par un autre service.

Par exemple, si vous synchronisez des données d'un serveur NFS sur site vers un serveur NFS basé sur le cloud, vous pouvez choisir le courtier de données qui écoute les demandes de connexion et qui les envoie.

Voici le fonctionnement du chiffrement à la volée :

1. Après avoir créé la relation de synchronisation, l'initiateur démarre une connexion chiffrée avec l'autre courtier de données.
2. Le courtier de données source crypte les données à partir de la source à l'aide de TLS 1.3.

3. Il envoie ensuite les données via le réseau au data broker cible.
4. Le courtier de données cible décrypte les données avant de les envoyer à la cible.
5. Après la copie initiale, le service synchronise les données modifiées toutes les 24 heures. S'il y a des données à synchroniser, le processus commence par l'initiateur qui ouvre une connexion chiffrée avec l'autre courtier de données.

   Si vous préférez synchroniser les données plus fréquemment, "vous pouvez modifier le planning après avoir créé la relation".

Versions NFS prises en charge

- Pour les serveurs NFS, le chiffrement des données à la volée est pris en charge avec les versions 3, 4.0, 4.1 et 4.2 de NFS.
- Pour Azure NetApp Files, le chiffrement des données à la volée est pris en charge avec les versions 3 et 4.1 de NFS.

Ce dont vous avez besoin pour commencer

Assurez-vous d'avoir les éléments suivants :

- Deux serveurs NFS qui sont équipés "exigences source et cible" Ou Azure NetApp Files dans deux sous-réseaux ou régions.
- Les adresses IP ou noms de domaine complets des serveurs.
- Emplacements réseau pour deux courtiers de données.

  Vous pouvez sélectionner un courtier de données existant, mais il doit fonctionner comme initiateur. Le courtier de données de l'écouteur doit être un courtier de données *New*.

  Si vous n'avez pas encore déployé de courtier de données, consultez les exigences du courtier de données. Comme vous disposez de règles de sécurité strictes, passez en revue les exigences de mise en réseau, notamment le trafic sortant à partir du port 443 et du "terminaux internet" que le courtier de données contacte.

  - "Consultez l'installation d'AWS"
  - "Vérifiez l'installation d'Azure"
  - "Vérifiez l'installation de GCP"
  - "Vérifiez l'installation de l'hôte Linux"

Synchronisation des données NFS à l'aide du chiffrement des données à la volée

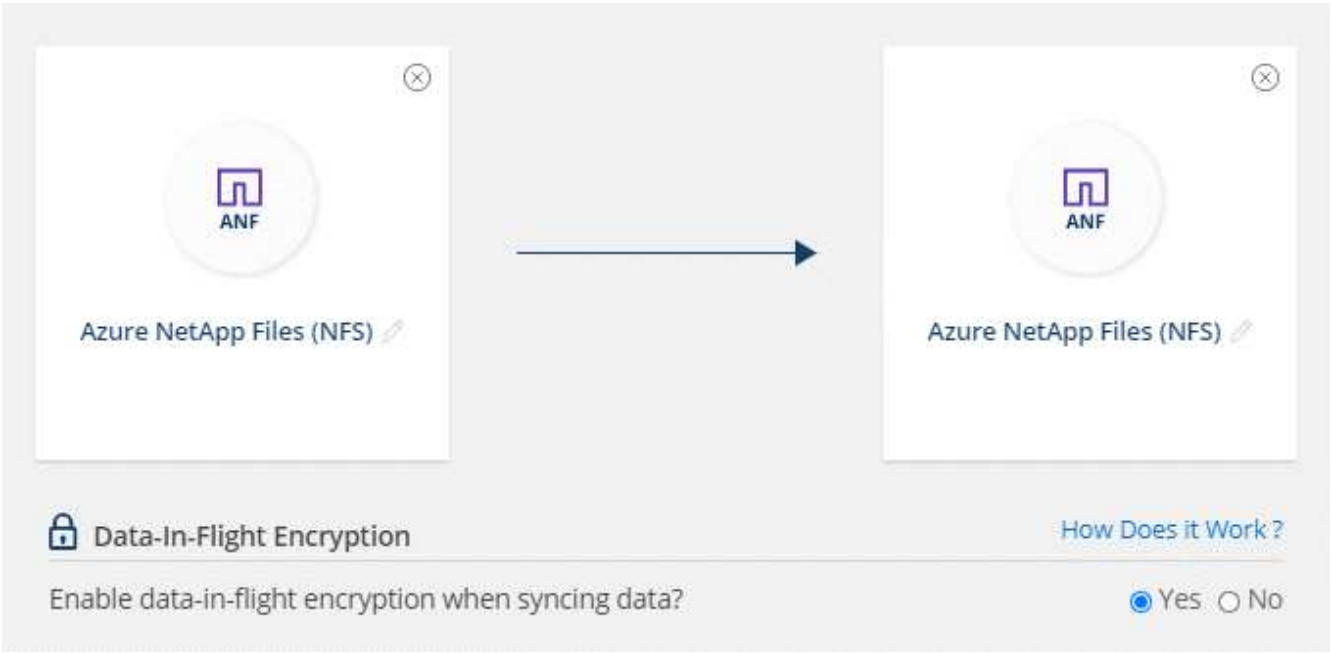
Créez une nouvelle relation de synchronisation entre deux serveurs NFS ou entre Azure NetApp Files, activez l'option de chiffrement à la volée et suivez les invites.

Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser **serveur NFS** vers les emplacements source et cible ou **Azure NetApp Files** vers les emplacements source et cible et sélectionnez **Oui** pour activer le cryptage des données en transit.

   L'image suivante montre ce que vous sélectionnez pour synchroniser des données entre deux serveurs NFS :

L'image suivante montre ce que vous choisissez de synchroniser des données entre Azure NetApp Files :



3. Suivez les invites pour créer la relation :

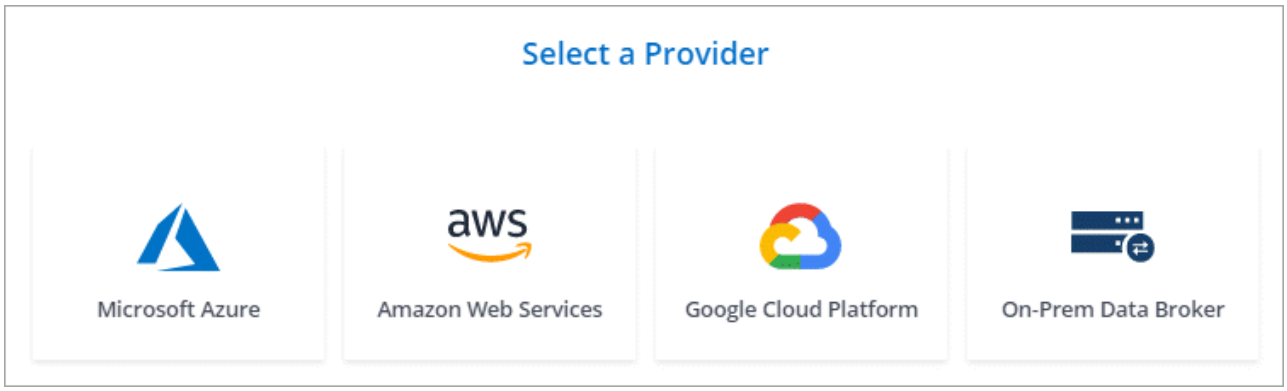
   a. **NFS Server/Azure NetApp Files** : Choisissez la version NFS, puis spécifiez une nouvelle source NFS ou sélectionnez un serveur existant.

   b. **Définir la fonctionnalité de Data Broker** : définissez le courtier de données *écoute* pour les demandes de connexion sur un port et lequel *lance* la connexion. Faites votre choix en fonction de vos besoins en matière de mise en réseau.

   c. **Data Broker** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.

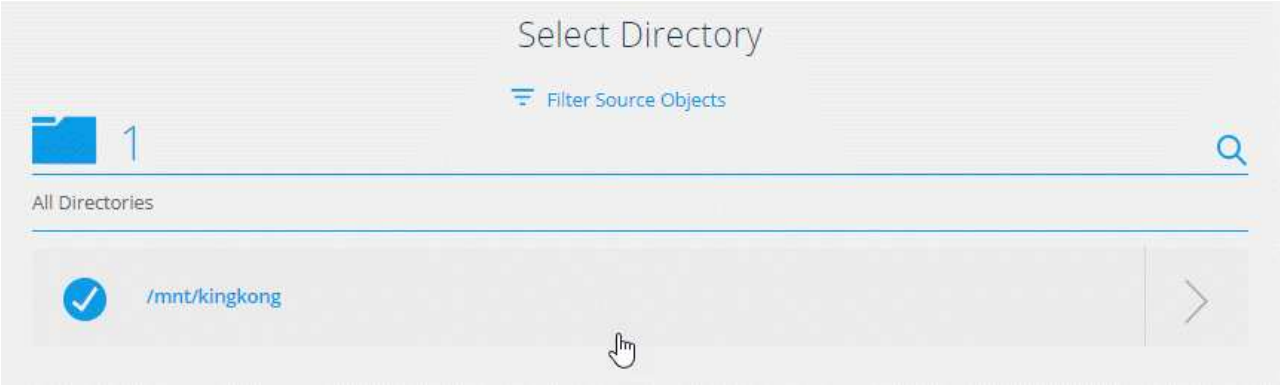
      Si le courtier de données source agit en tant qu'auditeur, il doit alors être un nouveau courtier de données.

Si vous avez besoin d'un nouveau courtier de données, Cloud Sync vous invite à suivre les instructions d'installation. Vous pouvez déployer le data broker dans le cloud ou télécharger un script d'installation pour votre propre hôte Linux.



d. **Répertoires** : Choisissez les répertoires que vous souhaitez synchroniser en sélectionnant tous les répertoires ou en descendant et en sélectionnant un sous-répertoire.

   Cliquez sur **Filtrer les objets source** pour modifier les paramètres qui définissent la synchronisation et la gestion des fichiers et dossiers source à l'emplacement cible.

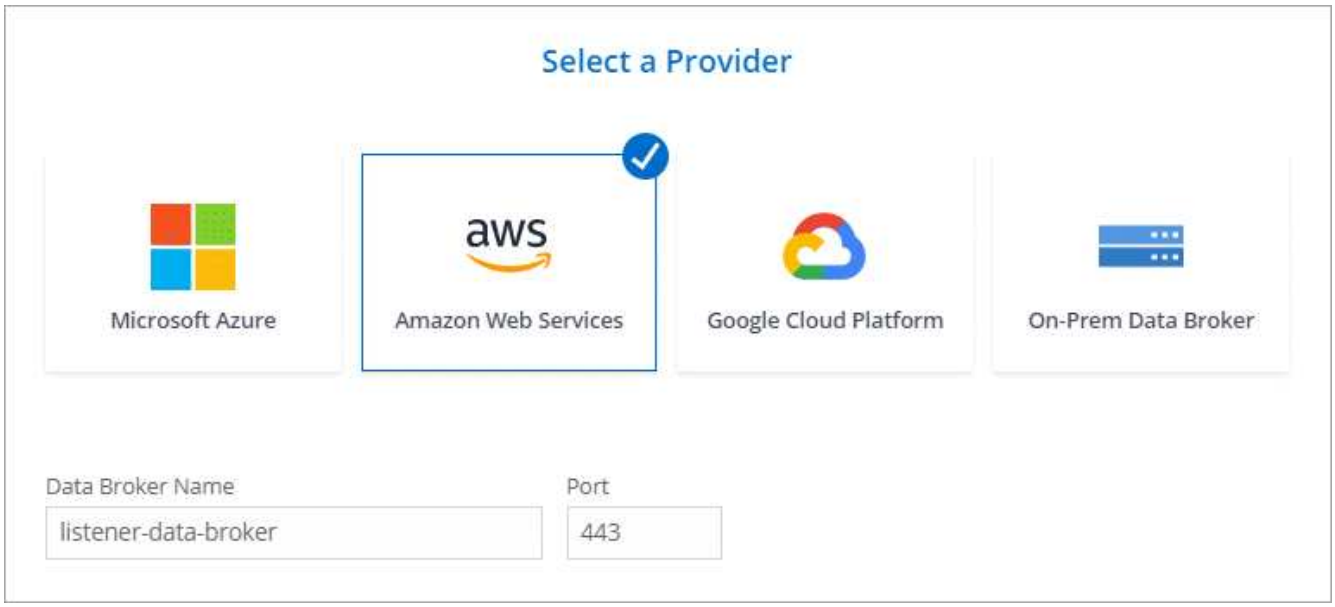


e. **Serveur NFS cible/Azure NetApp Files cible** : Choisissez la version NFS, puis entrez une nouvelle cible NFS ou sélectionnez un serveur existant.

f. **Courtier de données cible** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.

   Si le courtier de données cible agit en tant qu'auditeur, il doit alors être un nouveau courtier de données.

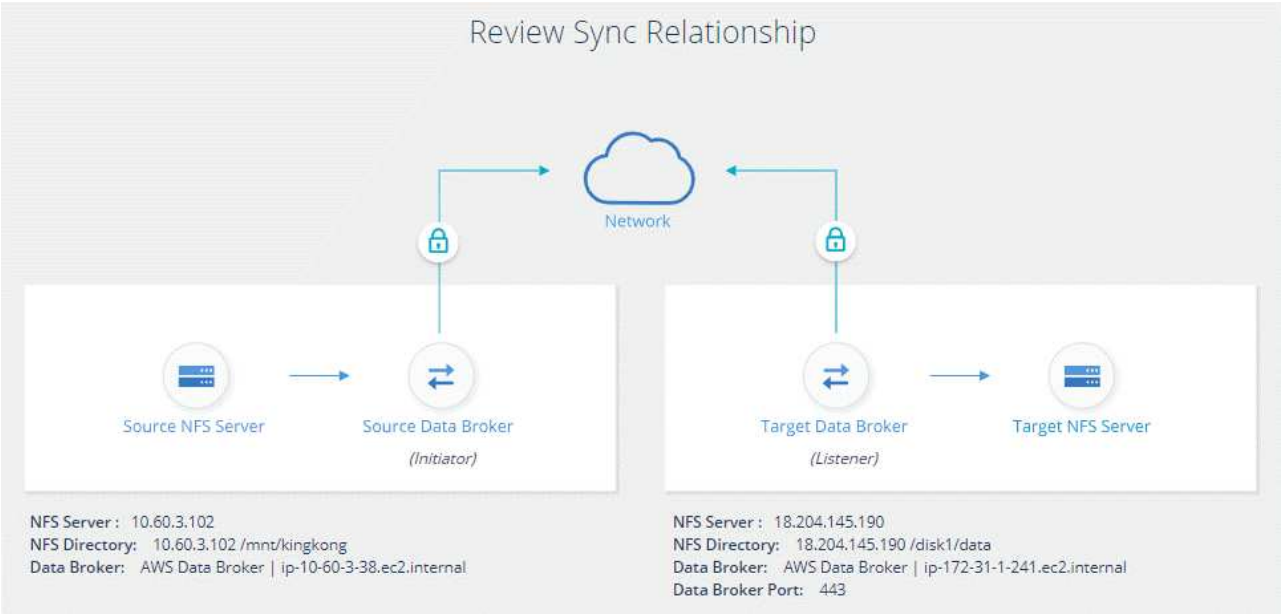
   Voici un exemple d'invite lorsque le courtier de données cible fonctionne comme écouteur. Notez l'option permettant de spécifier le port.



a. **Répertoires cibles** : sélectionnez un répertoire de niveau supérieur ou accédez à la recherche pour sélectionner un sous-répertoire existant ou créer un nouveau dossier à l'intérieur d'une exportation.

b. **Paramètres** : définissez comment les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible.

c. **Revue** : consultez les détails de la relation de synchronisation, puis cliquez sur **Créer une relation**.



Résultat

Cloud Sync commence à créer la nouvelle relation de synchronisation. Lorsque vous avez terminé, cliquez sur **Afficher dans le tableau de bord** pour afficher les détails de la nouvelle relation.

Gestion des relations de synchronisation

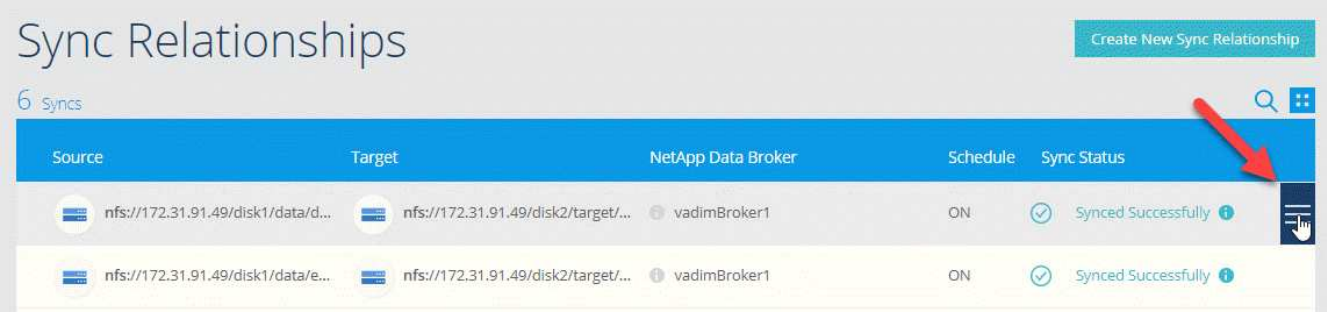
Vous pouvez gérer les relations de synchronisation à tout moment en synchronisant immédiatement les données, en modifiant les horaires, etc.

Effectuer une synchronisation immédiate des données

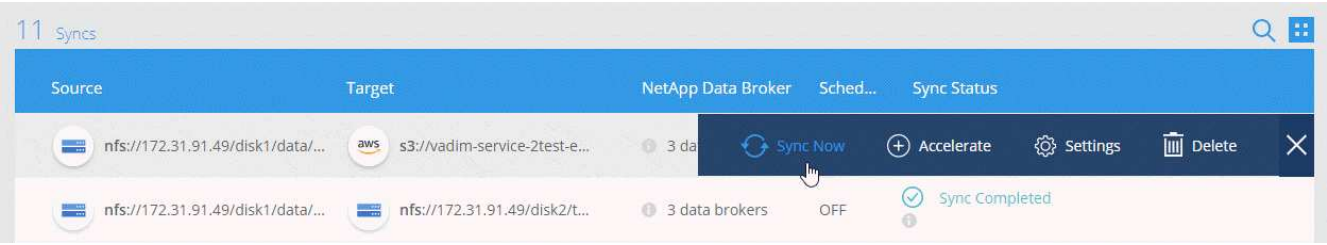
Au lieu d'attendre la synchronisation planifiée suivante, vous pouvez appuyer sur un bouton pour synchroniser immédiatement les données entre la source et la cible.

Étapes

1. Dans le tableau de bord **Sync**, survolez la relation de synchronisation et cliquez sur le menu d'action.



2. Cliquez sur **Synchroniser maintenant**, puis sur **Sync** pour confirmer.



Résultat

Cloud Sync démarre le processus de synchronisation des données pour la relation.

Accélération des performances de synchronisation

Accélérez les performances d'une relation de synchronisation en ajoutant un courtier de données supplémentaire à la relation. Le courtier de données supplémentaire doit être un *New* Data broker.

Comment cela fonctionne

Si les courtiers de données existants dans la relation sont utilisés dans d'autres relations de synchronisation, Cloud Sync ajoute automatiquement le nouveau courtier de données à ces relations.

Imaginons par exemple que vous ayez trois relations :

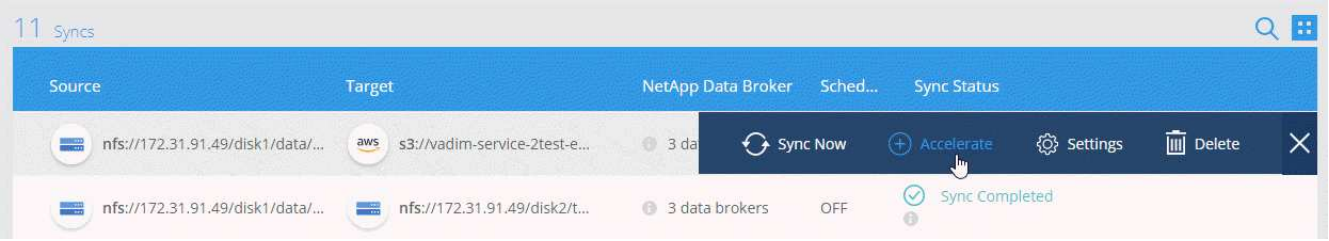
- La relation 1 utilise le courtier de données A
- La relation 2 utilise le courtier de données B
- La relation 3 utilise le courtier de données A

Vous souhaitez accélérer la performance de la relation 1 afin d'ajouter un nouveau courtier de données à cette relation (data broker C). Comme le courtier de données A est également utilisé dans la relation 3, le nouveau courtier de données est également automatiquement ajouté à la relation 3.

Étapes

1. Assurez-vous qu'au moins un des courtiers de données existants dans la relation est en ligne.

2. Survolez la relation de synchronisation et cliquez sur le menu d'action.
3. Cliquez sur **accélérer**.



4. Suivez les invites pour créer un nouveau courtier de données.

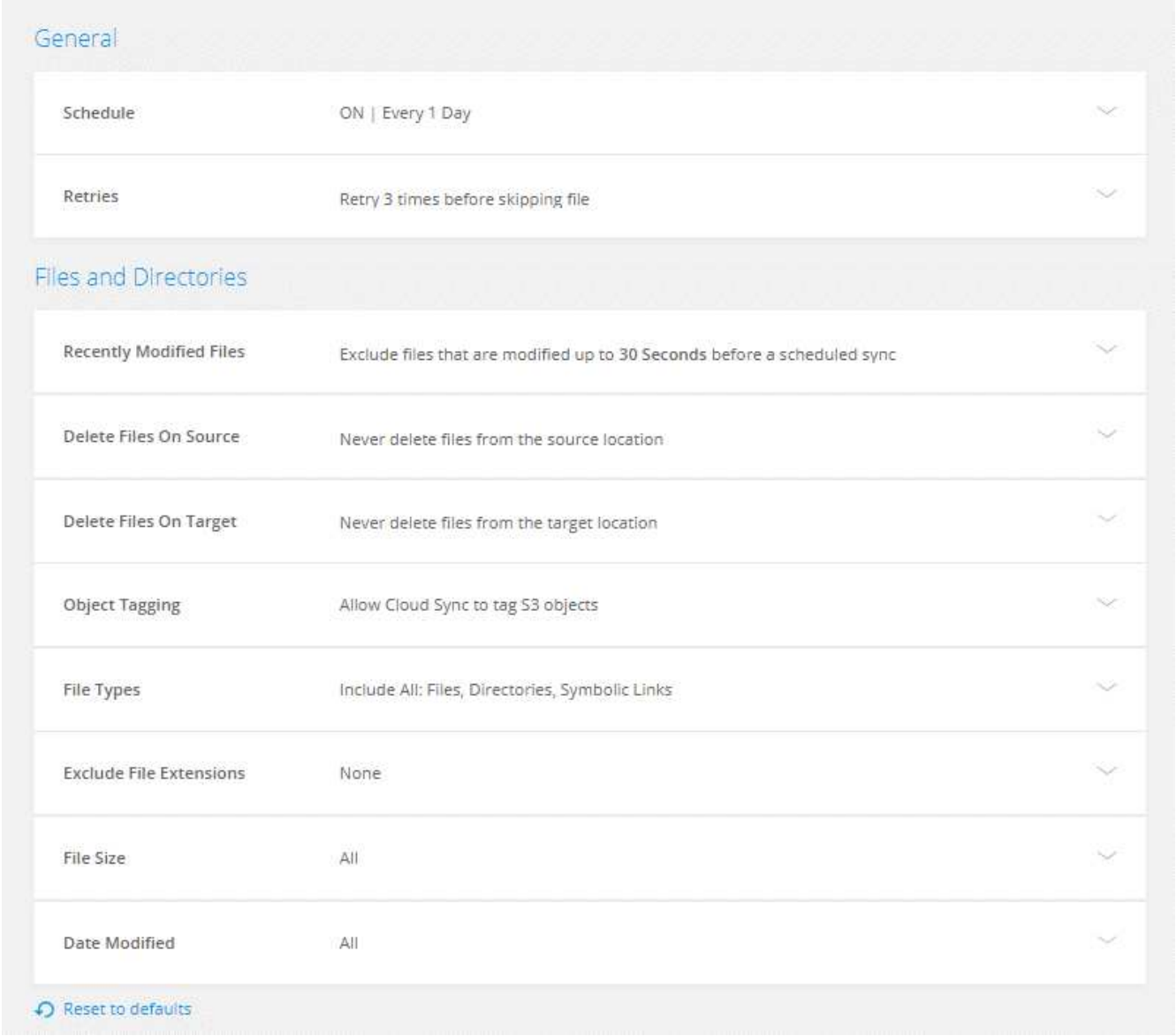
Résultat

Cloud Sync ajoute le nouveau courtier de données aux relations de synchronisation. Les performances de la prochaine synchronisation des données doivent être accélérées.

Modification des paramètres d'une relation de synchronisation

Modifiez les paramètres qui définissent la façon dont les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible.

1. Survolez la relation de synchronisation et cliquez sur le menu d'action.
2. Cliquez sur **Paramètres**.
3. Modifiez l'un des paramètres.



Voici une brève description de chaque paramètre :

Planification

Choisissez un programme récurrent pour les synchronisations ultérieures ou désactivez la planification de synchronisation. Vous pouvez planifier une relation pour synchroniser les données aussi souvent que toutes les 1 minute.

Tentatives

Définissez le nombre de tentatives de synchronisation d'un fichier par Cloud Sync avant de l'ignorer.

Fichiers récemment modifiés

Choisissez d'exclure les fichiers récemment modifiés avant la synchronisation planifiée.

Supprimer des fichiers sur la source

Choisissez de supprimer des fichiers de l'emplacement source une fois que Cloud Sync a copier les fichiers vers l'emplacement cible. Cette option inclut le risque de perte de données car les fichiers source sont supprimés après leur copie.

Si vous activez cette option, vous devez également modifier un paramètre dans le fichier local.json du

courtier de données. Ouvrez le fichier et remplacez le paramètre nommé *workers.transferrer.delete-on-source* par **true**.

Supprimer des fichiers sur la cible

Choisissez de supprimer des fichiers de l'emplacement cible, s'ils ont été supprimés de la source. La valeur par défaut est de ne jamais supprimer de fichiers de l'emplacement cible.

Balisage d'objets

Lorsque AWS S3 est la cible d'une relation de synchronisation, Cloud Sync balise les objets S3 avec des métadonnées pertinentes pour l'opération de synchronisation. Vous pouvez désactiver le balisage des objets S3 si ce n'est pas le cas dans votre environnement. Il n'y a aucun impact sur Cloud Sync si vous désactivez le balisage : Cloud Sync stocke simplement les métadonnées synchronisées d'une autre façon.

Types de fichiers

Définissez les types de fichiers à inclure dans chaque synchronisation : fichiers, répertoires et liens symboliques.

Exclure les extensions de fichier

Spécifiez les extensions de fichier à exclure de la synchronisation en tapant l'extension de fichier et en appuyant sur **entrée**. Par exemple, tapez *log* ou *.log* pour exclure les fichiers *.log. Un séparateur n'est pas nécessaire pour les extensions multiples. La vidéo suivante présente une courte démonstration :

► https://docs.netapp.com/fr-fr/occm38//media/video_file_extensions.mp4 *(video)*

Taille du fichier

Choisissez de synchroniser tous les fichiers, quelle que soit leur taille ou uniquement les fichiers qui se trouvent dans une plage de taille spécifique.

Date de modification

Choisissez tous les fichiers quelle que soit leur date de dernière modification, les fichiers modifiés après une date spécifique, avant une date spécifique ou entre une plage de temps.

Copier les listes de contrôle d'accès sur la cible

Choisir de copier les listes de contrôle d'accès (ACL) entre les partages SMB source et les partages SMB cibles. Notez que cette option n'est disponible que pour les relations de synchronisation créées après la version du 23 février 2020.

4. Cliquez sur **Enregistrer les paramètres**.

Résultat

Cloud Sync modifie la relation de synchronisation avec les nouveaux paramètres.

Suppression de relations

Vous pouvez supprimer une relation de synchronisation si vous n'avez plus besoin de synchroniser les données entre la source et la cible. Cette action ne supprime pas l'instance du courtier de données et ne supprime pas les données de la cible.

Étapes

1. Survolez la relation de synchronisation et cliquez sur le menu d'action.
2. Cliquez sur **Supprimer**, puis cliquez à nouveau sur **Supprimer** pour confirmer.

Résultat

Cloud Sync supprime la relation de synchronisation.

API Cloud Sync

Les fonctionnalités Cloud Sync disponibles via l'interface utilisateur Web sont également disponibles via les API RESTful.

Pour commencer

Pour commencer à utiliser les API Cloud Sync, vous devez obtenir un jeton d'utilisateur et votre identifiant de compte Cloud Central. Vous devrez ajouter le jeton et l'ID de compte à l'en-tête autorisation lorsque vous passez des appels API.

Étapes

1. Obtenez un jeton utilisateur auprès de NetApp Cloud Central.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
                "username": "<user_email>",
                "scope": "profile",
                "audience": "https://api.cloud.netapp.com",
                "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
                "grant_type": "password",
                "password": "<user_password>"
}
```

2. Obtenez votre ID de compte Cloud Central.

```
GET https://cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Cette API renvoie une réponse comme suit :

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. Ajoutez le jeton utilisateur et l'ID de compte dans l'en-tête autorisation de chaque appel d'API.

   Exemple

   L'exemple suivant montre un appel API pour créer un courtier de données dans Microsoft Azure. Il vous suffit de remplacer <user_token> et <AccountID> par le jeton et l'ID obtenus lors des étapes précédentes.

```
POST https://cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

Que dois-je faire lorsque le jeton expire ?

Le jeton utilisateur de NetApp Cloud Central a une date d'expiration. Pour actualiser le jeton, vous devez à nouveau appeler l'API à partir de l'étape 1.

La réponse de l'API inclut un champ " expire_in " qui indique la date d'expiration du jeton.

Référence API

La documentation de chaque API Cloud Sync est disponible à partir de "NetApp Cloud Central".

Utilisation d'API de liste

Les API de liste sont des API asynchrones. Les résultats ne reviennent donc pas immédiatement (par exemple : `GET /data-brokers/{id}/list-nfs-export-folders` et `GET /data-brokers/{id}/list-s3-buckets`). La seule réponse du serveur est l'état HTTP 202. Pour obtenir le résultat réel, vous devez utiliser le `GET /messages/client` API.

Étapes

1. Appelez l'API de liste que vous souhaitez utiliser.
2. Utilisez le `GET /messages/client` API pour afficher le résultat de l'opération.
3. Utilisez la même API en l'ajoutant avec l'ID que vous venez de recevoir : `GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   Notez que l'ID change chaque fois que vous appelez le `GET /messages/client` API.

Exemple

Lorsque vous appelez le `list-s3-buckets` API, le résultat n'est pas immédiatement renvoyé :

```
GET http://cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Le résultat est le code d'état HTTP 202, ce qui signifie que le message a été accepté, mais qu'il n'a pas encore été traité.

Pour obtenir le résultat de l'opération, vous devez utiliser l'API suivante :

```
GET http://cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Le résultat est un tableau avec un objet qui inclut un champ ID. Le champ ID représente le dernier message envoyé par le serveur. Par exemple :

```
[
    {
        "header": {
            "requestId": "init",
            "clientId": "init",
            "agentId": "init"
        },
        "payload": {
            "init": {}
        },
        "id": "5801"
    }
]
```

Vous devez maintenant passer l'appel API suivant à l'aide de l'ID que vous venez de recevoir :

```
GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Le résultat est un tableau de messages. Dans chaque message se trouve un objet Payload, qui se compose du nom de l'opération (en tant que clé) et de son résultat (en valeur). Par exemple :

```
[
    {
        "payload": {
            "list-s3-buckets": [
                {
                    "tags": [
                        {
                            "Value": "100$",
                            "Key": "price"
                        }
                    ],
                    "region": {
                        "displayName": "US West (Oregon)",
                        "name": "us-west-2"
                    },
                    "name": "small"
                }
            ]
        },
        "header": {
            "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
            "clientId": "5beb032f548e6e35f4ed1ba9",
            "agentId": "5bed61f4489fb04e34a9aac6"
        },
        "id": "5802"
    }
]
```


FAQ technique sur Cloud Sync

Cette FAQ peut vous aider si vous cherchez simplement une réponse rapide à une question.

Pour commencer

Les questions suivantes concernent le démarrage avec Cloud Sync.

Comment fonctionne Cloud Sync ?

Cloud Sync, qui utilise le logiciel de courtier de données NetApp, synchronise les données d'une source vers une cible (appelée « relation synchrone »).

Le courtier de données contrôle les relations de synchronisation entre vos sources et vos cibles. Après avoir configuré une relation de synchronisation, Cloud Sync analyse votre système source et le décompose en plusieurs flux de réplication afin de les transmettre aux données cible sélectionnées.

Après la copie initiale, le service synchronise toutes les données modifiées en fonction de la planification que

vous avez définie.

Comment fonctionne l'essai gratuit de 14 jours ?

L'essai gratuit de 14 jours commence lorsque vous vous inscrivez au service Cloud Sync. Vous n'êtes pas sujet aux frais NetApp liés aux relations Cloud Sync que vous créez pendant 14 jours. Cependant, tous les frais de ressources pour tout courtier de données que vous déployez s'appliquent toujours.

Combien coûte Cloud Sync ?

Il existe deux types de coûts associés à l'utilisation de Cloud Sync : les frais de service et les frais de ressources.

Frais de service

Pour les tarifs à la demande, les frais de service Cloud Sync sont horaires, en fonction du nombre de relations de synchronisation que vous créez.

- "Consultez les tarifs à la carte dans AWS"
- "Voir les tarifs annuels dans AWS"
- "Voir les tarifs à Azure"

Les licences Cloud Sync sont également disponibles auprès de votre représentant NetApp. Chaque licence permet 20 relations de synchronisation pendant 12 mois.

"En savoir plus sur les licences".

Frais de ressources

Les frais de ressources sont liés aux coûts de calcul et de stockage pour l'exécution du courtier de données dans le cloud.

Comment le service Cloud Sync est-il facturé ?

Il existe deux façons de payer les relations de synchronisation après la fin de votre essai gratuit de 14 jours. La première option consiste à vous abonner à AWS ou Azure, ce qui vous permet de payer à votre gré ou de payer chaque année. La deuxième option consiste à acheter des licences directement auprès de NetApp.

Puis-je utiliser Cloud Sync en dehors du cloud ?

Oui, vous pouvez utiliser Cloud Sync dans une architecture non cloud. La source et la cible peuvent résider sur site et ainsi de suite, le courtier de données.

Notez les points clés suivants sur l'utilisation de Cloud Sync en dehors du cloud :

- Pour la synchronisation sur site, un compartiment privé Amazon S3 est disponible via NetApp StorageGRID.
- Le courtier de données a besoin d'une connexion Internet pour communiquer avec le service Cloud Sync.
- Si vous n'achetez pas de licence directement auprès de NetApp, vous devrez acquérir un compte AWS ou Azure pour la facturation du service PAYGO Cloud Sync.

Comment accéder à Cloud Sync ?

Cloud Sync est disponible depuis Cloud Manager dans l'onglet **Sync**.

Sources et cibles prises en charge

Les questions suivantes concernent la source et les cibles prises en charge dans une relation de synchronisation.

Quelles sources et cibles Cloud Sync prend-il en charge ?

Cloud Sync prend en charge de nombreux types de relations de synchronisation. "Afficher la liste complète".

Quelles sont les versions de NFS et SMB prises en charge par Cloud Sync ?

Cloud Sync prend en charge NFS version 3 et ultérieure et SMB version 1 et ultérieure.

"En savoir plus sur les exigences de synchronisation".

Quand Amazon S3 est la cible, les données peuvent-elles être hiérarchisées vers une classe de stockage S3 spécifique ?

Oui, vous pouvez choisir une classe de stockage S3 spécifique lorsque AWS S3 est la cible :

- Standard (il s'agit de la classe par défaut)
- Le Tiering intelligent
- Accès autonome et peu fréquent
- Un seul accès à Zone-Infrequent
- Glacier
- Archives profondes des Glaciers

Qu'en est-il des niveaux de stockage pour le stockage Azure Blob ?

Vous pouvez choisir un niveau de stockage spécifique à Azure Blob lorsqu'un conteneur Blob est la cible :

- Stockage à chaud
- Stockage cool

Mise en réseau

Les questions suivantes concernent les exigences de mise en réseau pour Cloud Sync.

Quelles sont les exigences de mise en réseau pour Cloud Sync ?

L'environnement Cloud Sync requiert que le courtier de données soit connecté à la source et à la cible via le protocole sélectionné (NFS, SMB, EFS) ou l'API de stockage objet (Amazon S3, Azure Blob, IBM Cloud Object Storage).

En outre, le courtier de données a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels.

Pour en savoir plus, "examiner les besoins en matière de mise en réseau".

Y a-t-il des limites de mise en réseau liées à la connectivité des courtiers de données ?

Les courtiers de données ont besoin d'un accès Internet. Nous ne prenons pas en charge un serveur proxy lors du déploiement d'un courtier en données dans Azure ou dans Google Cloud Platform.

Synchronisation des données

Les questions suivantes concernent le fonctionnement de la synchronisation des données.

À quelle fréquence la synchronisation se produit-elle ?

Le planning par défaut est défini pour la synchronisation quotidienne. Après la synchronisation initiale, vous pouvez :

- Modifiez le programme de synchronisation en fonction du nombre de jours, d'heures ou de minutes souhaité
- Désactivez le programme de synchronisation
- Supprimer le programme de synchronisation (aucune donnée ne sera perdue ; seule la relation de synchronisation sera supprimée)

Quel est le programme de synchronisation minimal ?

Vous pouvez planifier une relation pour synchroniser les données aussi souvent que toutes les 1 minute.

Le courtier de données essaie-t-il lorsqu'un fichier ne parvient pas à se synchroniser ? Ou est-ce que ce délai ?

Le courtier de données n'expire pas lorsqu'un seul fichier ne parvient pas à être transféré. Au lieu de cela, le courtier de données essaie à nouveau 3 fois avant de sauter le fichier. La valeur de la nouvelle tentative est configurable dans les paramètres d'une relation de synchronisation.

"Découvrez comment modifier les paramètres d'une relation de synchronisation".

Que se passe-t-il si j'ai un très grand jeu de données ?

Si un seul répertoire contient 600,000 fichiers ou plus, contactez-nous afin que nous puissions vous aider à configurer le courtier de données pour gérer la charge utile. Il est possible que nous devions ajouter de la mémoire supplémentaire à la machine du courtier de données.

Sécurité

Les questions suivantes ont trait à la sécurité.

Cloud Sync est-il sécurisé ?

Oui. Toute la connectivité réseau des services Cloud Sync est utilisée "Service SQS (simple Queue) d'Amazon".

Toutes les communications entre le data broker et Amazon S3, Azure Blob, Google Cloud Storage et IBM Cloud Object Storage sont effectuées via le protocole HTTPS.

Si vous utilisez Cloud Sync avec des systèmes sur site (source ou destination), voici quelques options de connectivité recommandées :

- Une connexion AWS Direct Connect, Azure ExpressRoute ou Google Cloud Interconnect, qui n'est pas routée par Internet (et ne peut communiquer qu'avec les réseaux cloud que vous spécifiez)
- Une connexion VPN entre votre passerelle sur site et vos réseaux cloud
- Pour un transfert de données plus sécurisé avec des compartiments S3, le stockage Azure Blob ou Google Cloud Storage, un terminal Amazon Private S3, des terminaux de service Azure Virtual Network ou Private Google Access peuvent être établis.

L'une de ces méthodes établit une connexion sécurisée entre vos serveurs NAS sur site et un courtier de données Cloud Sync.

Les données sont-elles chiffrées par Cloud Sync ?

- Cloud Sync prend en charge le chiffrement des données en vol entre les serveurs NFS source et cible. "En savoir plus >>".
- Le chiffrement n'est pas pris en charge avec SMB.
- Lorsqu'un compartiment Amazon S3 est la cible d'une relation synchrone, vous pouvez choisir d'activer le chiffrement des données à l'aide du chiffrement AWS KMS ou AES-256.

Autorisations

Les questions suivantes concernent les autorisations de données.

Les autorisations de données SMB sont-elles synchronisées vers l'emplacement cible ?

Vous pouvez configurer Cloud Sync pour préserver les listes de contrôle d'accès (ACL) entre un partage SMB source et un partage SMB cible. Vous pouvez également copier manuellement les ACL vous-même. "Découvrez comment copier des listes de contrôle d'accès entre partages SMB".

Les autorisations de données NFS sont-elles synchronisées vers l'emplacement cible ?

Cloud Sync copie automatiquement les autorisations NFS entre les serveurs NFS comme suit :

- NFS version 3 : Cloud Sync copie les autorisations et le propriétaire du groupe d'utilisateurs.
- NFS version 4 : Cloud Sync copie les ACL.

Performance

Les questions suivantes concernent les performances de Cloud Sync.

Que représente l'indicateur de progression d'une relation de synchronisation ?

La relation de synchronisation indique le débit de l'adaptateur réseau du courtier de données. Si vous accélérez les performances de synchronisation en utilisant plusieurs courtiers de données, le débit est la somme de tout le trafic. Ce débit est actualisé toutes les 20 secondes.

J'ai des problèmes de performances. Pouvons-nous limiter le nombre de transferts simultanés ?

Le courtier de données peut synchroniser 4 fichiers à la fois. Si vous avez des fichiers de très grande taille (plusieurs To chacun), il peut prendre beaucoup de temps pour terminer le processus de transfert et les performances peuvent être affectées.

Limiter le nombre de transferts simultanés peut vous aider. Mailto:ng-cloudsync-

support@netapp.com[Contactez-nous pour obtenir de l'aide].

Pourquoi les performances avec Azure NetApp Files sont-elles faibles ?

Lorsque vous synchronisez les données depuis ou vers Azure NetApp Files, vous risquez de subir des défaillances et des problèmes de performances si le niveau de service des disques est Standard.

Définissez le niveau de service sur Premium ou Ultra pour améliorer les performances de synchronisation.

"En savoir plus sur le débit et les niveaux de service de Azure NetApp Files".

Pourquoi est-ce que j'ai de faibles performances avec Cloud Volumes Service pour AWS ?

Lorsque vous synchronisez des données vers ou à partir d'un volume cloud, vous risquez de rencontrer des problèmes de performances et de panne si le niveau de performance du volume cloud est Standard.

Définissez le niveau de service sur Premium ou Extreme pour améliorer les performances de synchronisation.

Combien de courtiers de données sont requis ?

Lorsque vous créez une nouvelle relation, vous commencez par un seul courtier de données (sauf si vous avez sélectionné un courtier de données existant qui appartient à une relation de synchronisation accélérée). Dans de nombreux cas, un seul courtier de données peut répondre aux exigences de performance d'une relation de synchronisation. Si ce n'est pas le cas, l'ajout de courtiers de données supplémentaires permet d'accélérer la synchronisation. Mais vous devez d'abord vérifier d'autres facteurs qui peuvent avoir un impact sur les performances de synchronisation.

Plusieurs facteurs peuvent avoir un impact sur les performances de transfert de données. Les performances globales de la synchronisation peuvent être affectées en raison de la bande passante du réseau, de la latence et de la topologie du réseau, ainsi que des spécifications des VM du courtier de données et des performances du système de stockage. Par exemple, un seul courtier de données dans une relation de synchronisation peut atteindre 100 Mo/s, tandis que le débit du disque sur la cible peut uniquement permettre 64 Mo/s. Par conséquent, le courtier en données essaie de copier les données, mais la cible ne peut pas répondre aux besoins de performances du courtier.

Assurez-vous donc de vérifier les performances de votre réseau et le débit du disque sur la cible.

Vous pouvez ensuite envisager d'accélérer les performances de synchronisation en ajoutant un courtier de données supplémentaire pour partager la charge de cette relation. "Découvrez comment accélérer les performances de synchronisation".

Suppression de choses

Les questions suivantes concernent la suppression des relations de synchronisation et des données des sources et des cibles.

Que se passe-t-il si je supprime ma relation Cloud Sync ?

La suppression d'une relation arrête toutes les synchronisations de données futures et met fin au paiement. Toutes les données synchronisées sur la cible restent en l'état.

Que se passe-t-il si je supprime quelque chose de mon serveur source ? Est-il également supprimé de la cible ?

Par défaut, si vous disposez d'une relation de synchronisation active, l'élément supprimé sur le serveur source n'est pas supprimé de la cible lors de la prochaine synchronisation. Il existe toutefois une option dans les paramètres de synchronisation pour chaque relation, dans laquelle vous pouvez définir que Cloud Sync supprimera les fichiers de l'emplacement cible s'ils ont été supprimés de la source.

"Découvrez comment modifier les paramètres d'une relation de synchronisation".

Que se passe-t-il si je supprime quelque chose de ma cible ? Est-il supprimé de ma source ?

Si un élément est supprimé de la cible, il ne sera pas supprimé de la source. La relation est unidirectionnelle, de la source à la cible. Au cours du cycle de synchronisation suivant, Cloud Sync compare la source à la cible, identifie que l'élément est manquant et Cloud Sync le copie à nouveau de la source à la cible.

Dépannage

"Base de connaissances NetApp : FAQ Cloud Sync : support et dépannage"

Data broker plongez en profondeur

La question suivante concerne le courtier de données.

Pouvez-vous expliquer l'architecture du data broker ?

Bien sûr. Voici les points les plus importants :

- Le courtier de données est une application node.js exécutée sur un hôte Linux.
- Cloud Sync déploie le courtier de données comme suit :
  - AWS : à partir d'un modèle AWS CloudFormation
  - Azure : d'Azure Resource Manager
  - Google : à partir de Google Cloud Deployment Manager
  - Si vous utilisez votre propre hôte Linux, vous devez installer manuellement le logiciel
- Le logiciel Data Broker se met automatiquement à niveau vers la dernière version.
- Le data broker utilise AWS SQS comme canal de communication fiable et sécurisé et pour le contrôle et la surveillance. Les LP fournissent également une couche de persistance.
- Vous pouvez ajouter des courtiers de données supplémentaires à une relation pour augmenter la vitesse de transfert et augmenter la haute disponibilité. La résilience des services est assurée en cas de défaillance d'un courtier de données.

Informations sur le copyright

Informations sur les marques commerciales