Commencez

Cloud Sync

NetApp
November 17, 2022

Table des matières

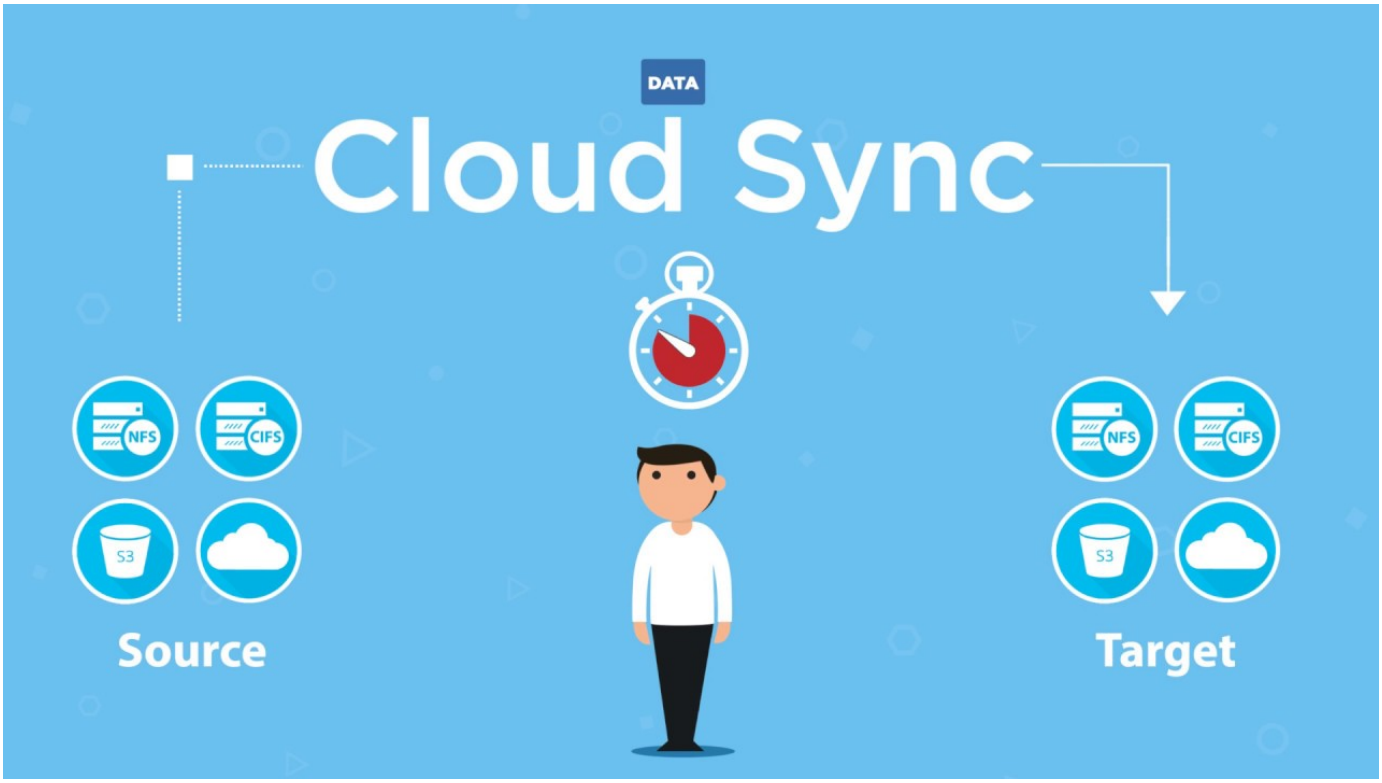
Commencez

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

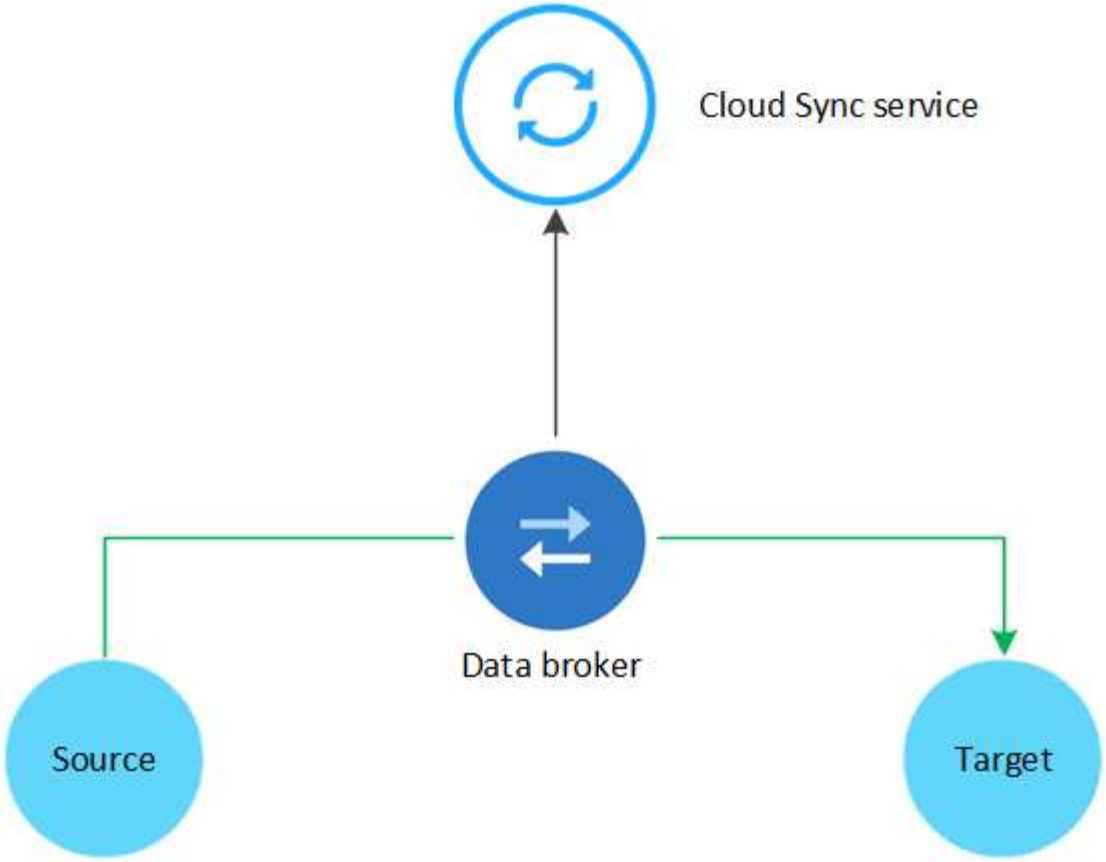
Regardez la vidéo suivante pour une présentation de Cloud Sync :



Fonctionnement de Cloud Sync

Cloud Sync est une plateforme SaaS (Software-as-a-Service) qui regroupe un groupe de courtiers de données, une interface cloud disponible via BlueXP, et 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. Un groupe de courtiers de données, qui comprend un ou plusieurs courtiers de données, a besoin d'une connexion Internet sortante sur le port 443 afin que le service IT puisse 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
- Amazon EFS
- Amazon FSX pour ONTAP
- Amazon S3
- Blob d'Azure
- Azure Data Lake Storage Gen2
- Azure NetApp Files
- (Disponible en tant qu'aperçu)
- Cloud Volumes Service

- Cloud Volumes ONTAP
- Google Cloud Storage
- Google Drive
- IBM Cloud Object Storage
- Cluster ONTAP sur site
- Stockage ONTAP S3
- SFTP (avec API uniquement)
- StorageGRID

"Affichez les relations de synchronisation prises en charge".

Coûts

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 d'un ou plusieurs courtiers de 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.

"Découvrez le fonctionnement des licences".

Démarrage rapide de Cloud Sync

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

Vous devriez avoir commencé avec BlueXP, qui inclut la connexion, la configuration d'un compte, et éventuellement le déploiement d'un connecteur et la création d'environnements de travail.

Si vous souhaitez créer des relations de synchronisation pour l'un des éléments suivants, vous devez d'abord créer ou découvrir un environnement de travail :

- Amazon FSX pour ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Clusters ONTAP sur site

Un connecteur est requis pour Cloud Volumes ONTAP, les clusters ONTAP sur site et Amazon FSX pour ONTAP.

- "Apprenez à vous lancer avec BlueXP"
- "En savoir plus sur les connecteurs"

Vérifiez que la source et la cible sont prises en charge et configurées. L'exigence la plus importante consiste à

vérifier la connectivité entre le groupe de courtiers de données et les emplacements source et cible.

- "Afficher les relations prises en charge"
- "Préparer la source et la cible"

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. Un groupe de courtiers de données, qui comprend un ou plusieurs courtiers de données, a besoin d'une connexion Internet sortante sur le port 443 afin que le service IT puisse 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 partir de laquelle vous pouvez déployer un courtier de données dans le Cloud ou télécharger un script d'installation pour votre propre hôte Linux.

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

Connectez-vous à "BlueXP", 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 >>".

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 >>".

Relations de synchronisation prises en charge

Cloud Sync vous permet de synchroniser les données d'une source vers une cible. Il s'agit d'une relation de synchronisation. Vous devez comprendre les relations prises en charge avant de commencer.

Emplacement de la source	Emplacements cibles pris en charge
Amazon EFS	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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
Amazon FSX pour ONTAP	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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
Amazon S3	• Amazon EFS • Amazon FSX pour ONTAP • Amazon S3 • Blob d'Azure • Azure Data Lake Storage Gen2 • Azure NetApp Files • Case [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Blob d'Azure	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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
Azure NetApp Files	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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
Case [1]	• Amazon FSX pour ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM Cloud Object Storage • Serveur NFS • Serveur SMB • StorageGRID
Cloud Volumes ONTAP	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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
Cloud Volumes Service	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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
Google Cloud Storage	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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 • Stockage ONTAP S3 • Serveur SMB • StorageGRID
Google Drive	• Serveur NFS • Serveur SMB

Emplacement de la source	Emplacements cibles pris en charge
IBM Cloud Object Storage	• Amazon EFS • Amazon FSX pour ONTAP • Amazon S3 • Blob d'Azure • Azure Data Lake Storage Gen2 • Azure NetApp Files • Case [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Serveur NFS	• Amazon EFS • Amazon FSX pour ONTAP • Amazon S3 • Blob d'Azure • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Google Drive • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Cluster ONTAP sur site	• Amazon EFS • Amazon FSX pour ONTAP • Amazon 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
Stockage ONTAP S3	• Google Cloud Storage • Serveur SMB • StorageGRID • Stockage ONTAP S3
SFTP [2]	S3
Serveur SMB	• Amazon EFS • Amazon FSX pour ONTAP • Amazon S3 • Blob d'Azure • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Google Drive • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Stockage ONTAP S3 • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
StorageGRID	• Amazon EFS • Amazon FSX pour ONTAP • Amazon S3 • Blob d'Azure • Azure Data Lake Storage Gen2 • Azure NetApp Files • Case [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Stockage ONTAP S3 • Serveur SMB • StorageGRID

Remarques :

1. La prise en charge de Box est disponible sous forme d'aperçu.
2. Les relations de synchronisation avec cette source/cible sont prises en charge via l'API Cloud Sync uniquement.
3. Vous pouvez choisir un niveau de stockage spécifique à Azure Blob lorsqu'un conteneur Blob est la cible :
    - Stockage à chaud
    - Stockage cool
4. lorsque Amazon 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
    - Archives profondes des Glaciers
    - Récupération flexible Glacier
    - Récupération instantanée Glacier
5. Vous pouvez choisir une classe de stockage spécifique lorsqu'un compartiment Google Cloud Storage est la cible :
    - Standard
    - Nearline

- Ligne de refroidissement
- Archivage

Préparer la source et la cible

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

Mise en réseau

- La source et la cible doivent disposer d'une connexion réseau au groupe de courtiers de données.

  Par exemple, si un serveur NFS se trouve dans votre data Center et qu'un courtier en données est dans AWS, vous devez disposer d'une connexion réseau (VPN ou Direct Connect) entre votre réseau et le VPC.

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

Répertoire cible

Lorsque vous créez une relation de synchronisation, Cloud Sync vous permet de sélectionner un répertoire cible existant, puis de créer éventuellement un nouveau dossier dans ce répertoire. Assurez-vous que votre répertoire cible préféré existe déjà.

Autorisations de lecture des répertoires

Pour afficher tous les répertoires ou dossiers d'une source ou d'une cible, Cloud Sync a besoin d'autorisations de lecture sur le répertoire ou le dossier.

NFS

Les autorisations doivent être définies sur la source/cible avec uid/gid sur les fichiers et les répertoires.

Stockage objet

- Pour AWS et Google Cloud, un courtier de données doit avoir des autorisations d'accès aux objets de liste (ces autorisations sont fournies par défaut si vous suivez les étapes d'installation du courtier de données).
- Pour Azure, StorageGRID et IBM, les informations d'identification saisies lors de la configuration d'une relation de synchronisation doivent disposer d'autorisations d'objet de liste.

PME

Les informations d'identification SMB que vous saisissez lors de la configuration d'une relation de synchronisation doivent disposer d'autorisations de dossier de liste.

Le courtier de données ignore les répertoires suivants par défaut : .snapshot, ~snapshot, .copy-load

Exigences des compartiments Amazon S3

Vérifiez que votre compartiment Amazon S3 répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour Amazon 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 de Chine.

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

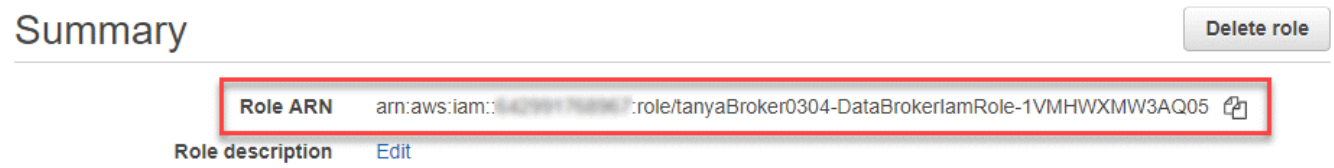
Lors de la configuration d'une relation de synchronisation, vous pouvez spécifier un compartiment S3 qui réside dans un compte AWS non associé à un courtier de données.

"Les autorisations incluses dans ce fichier JSON" Doit être appliqué au compartiment S3 pour que un 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 à un courtier en données.
2. *<RoleARN>* doit être remplacé par l'un des éléments suivants :
    - Si un 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 d'un courtier de données.
    - Si un 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

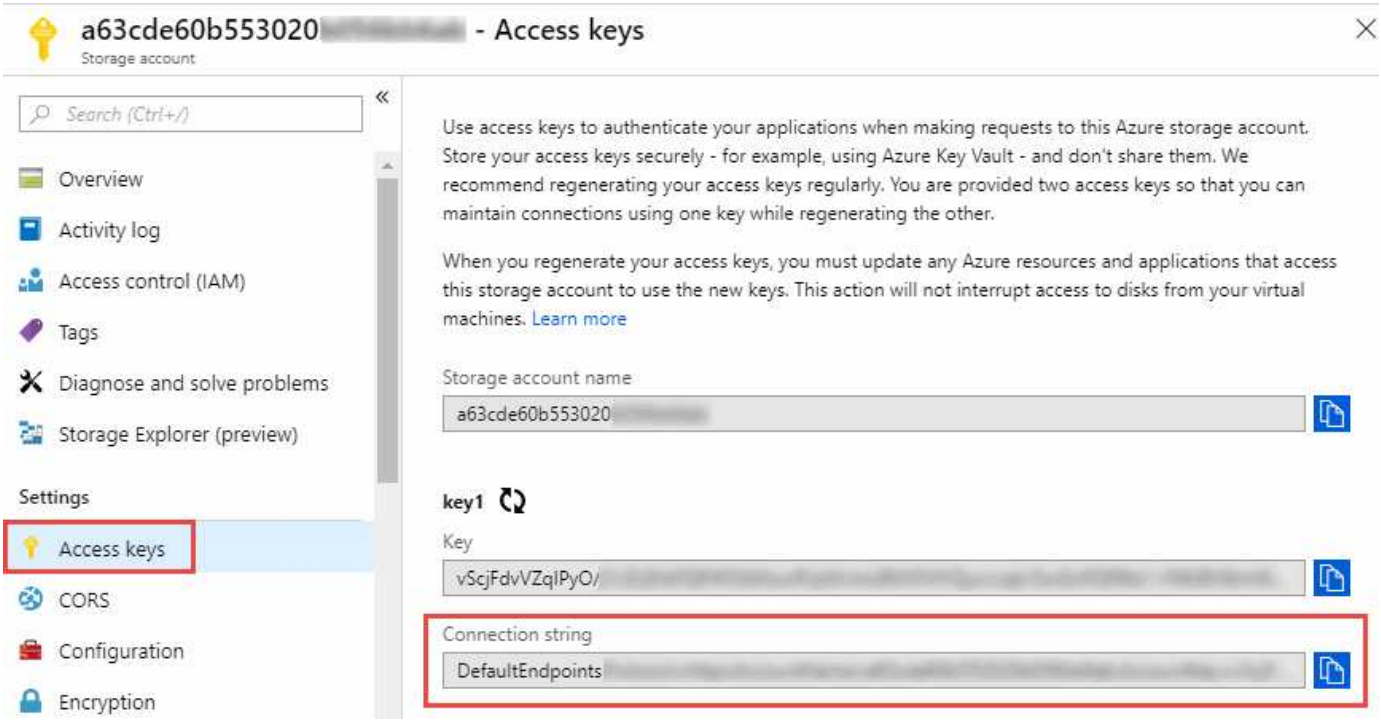
Un courtier en données peut résider en tout lieu lorsqu'une relation de synchronisation inclut le stockage Azure Blob.

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 pour les relations qui incluent Azure Blob et NFS/SMB

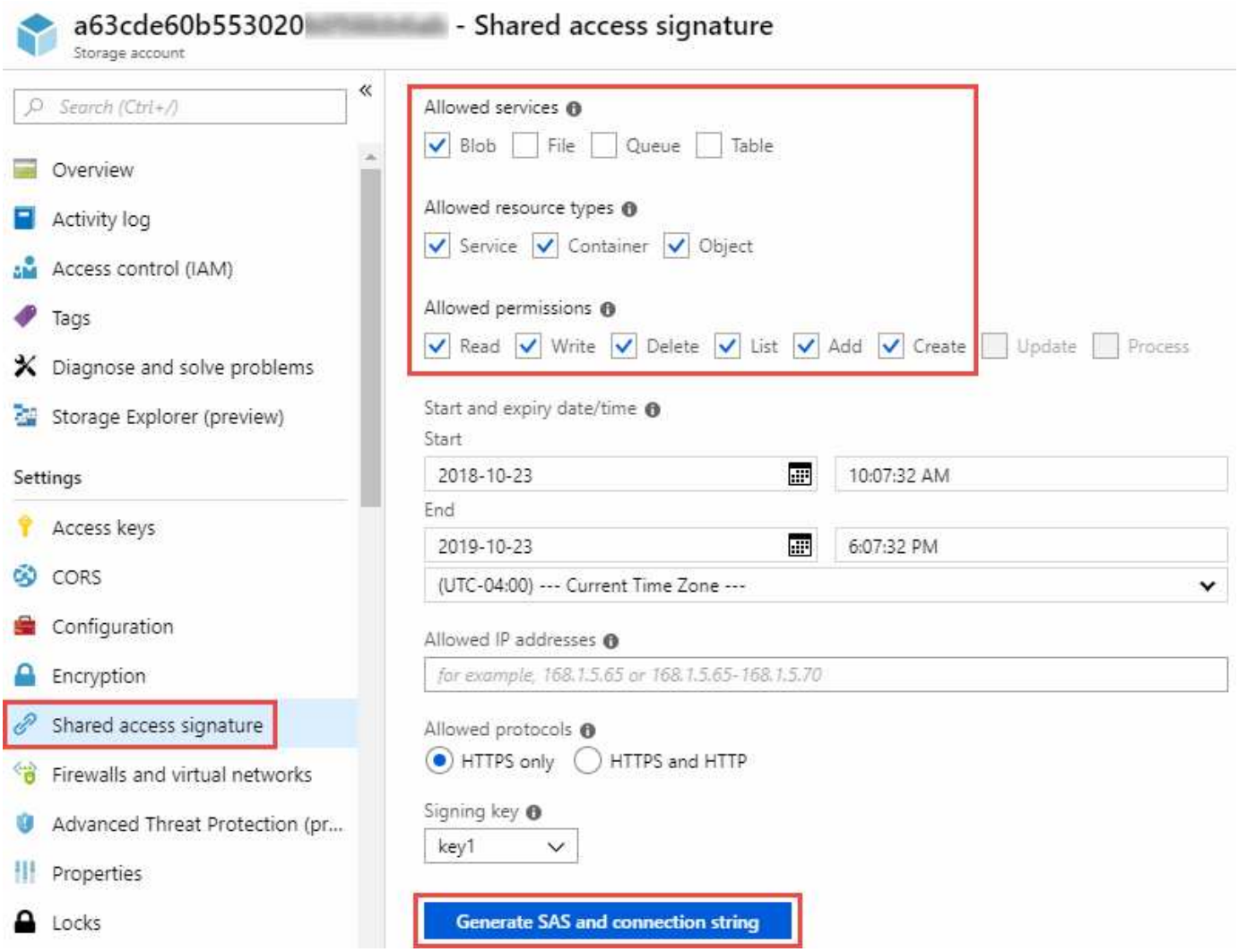
Lors de la création d'une relation synchrone entre un conteneur Azure Blob et un serveur NFS ou SMB, vous devez fournir à Cloud Sync la chaîne de connexion du compte de stockage :



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



Si vous choisissez d'implémenter une relation de synchronisation continue qui inclut un conteneur Azure Blob, vous pouvez utiliser une chaîne de connexion standard ou une chaîne de connexion SAS. Si vous utilisez une chaîne de connexion SAS, elle ne doit pas être définie pour expirer dans un futur proche.

Azure Data Lake Storage Gen2

Lors de la création d'une relation de synchronisation incluant Azure Data Lake, vous devez fournir à Cloud Sync la chaîne de connexion du compte de stockage. Il doit s'agir d'une chaîne de connexion standard et non d'une signature d'accès partagée (SAS).

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 à l'emballage

- Pour créer une relation de synchronisation incluant Box, vous devez fournir les informations d'identification suivantes :
  - ID client
  - Secret client
  - Clé privée
  - ID de clé publique
  - Phrase de passe
  - ID entreprise
- Si vous créez une relation de synchronisation entre Amazon S3 et Box, vous devez utiliser un groupe de courtier de données qui dispose d'une configuration unifiée où les paramètres suivants sont définis sur 1 :
  - Simultanéité du scanner
  - Limite des processus du scanner
  - Simultanéité de transfert
  - Limite des processus de transfert

  "Découvrez comment définir une configuration unifiée pour un groupe de courtiers de données".

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

Avec les relations de synchronisation qui incluent Google Cloud Storage, un courtier en données déployé dans Google Cloud ou sur site est nécessaire. 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 en données Google Cloud"
- "Découvrez comment installer le courtier de données sur un hôte Linux"

Régions Google Cloud prises en charge

Toutes les régions sont prises en charge.

Autorisations pour les compartiments dans d'autres projets Google Cloud

Lors de la configuration d'une relation de synchronisation, vous avez le choix entre plusieurs compartiments Google Cloud dans différents projets, si vous fournissez les autorisations requises pour le compte de service du courtier de données. "Découvrez comment configurer le compte de service".

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.

Google Drive

Lorsque vous configurez une relation de synchronisation incluant Google Drive, vous devez fournir les éléments suivants :

- L'adresse électronique d'un utilisateur qui a accès à l'emplacement Google Drive où vous souhaitez synchroniser des données
- L'adresse e-mail d'un compte de service Google Cloud disposant d'autorisations d'accès à Google Drive
- Une clé privée pour le compte de service

Pour configurer le compte de service, suivez les instructions de la documentation Google :

- "Créez le compte de service et les informations d'identification"
- "Déléguer l'autorité de l'ensemble du domaine à votre compte de service"

Lorsque vous modifiez le champ OAuth Scopes, entrez les étendues suivantes :

- https://www.googleapis.com/auth/drive
- https://www.googleapis.com/auth/drive.file

Configuration requise pour le serveur NFS

- Le serveur NFS peut être un système NetApp ou un système non NetApp.
- Le serveur de fichiers doit autoriser un hôte de courtier de données à accéder aux exportations via les ports requis.
  - 111 TCP/UDP
  - 2049 TCP/UDP
  - 5555 TCP/UDP
- 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.

Conditions requises pour le ONTAP

Si la relation synchrone inclut Cloud Volumes ONTAP ou un cluster ONTAP sur site et que vous avez sélectionné NFSv4 ou version ultérieure, vous devez activer les ACL NFSv4 sur le système ONTAP. Cette opération est nécessaire pour copier les listes de contrôle d'accès.

Exigences du stockage ONTAP S3

Lorsque vous configurez une relation de synchronisation incluant "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.
- Vous devez fournir à Cloud Sync des identifiants disposant d’autorisations sur le serveur SMB.
  - Pour un serveur SMB source, les autorisations suivantes sont requises : list et read.

    Les membres du groupe opérateurs de sauvegarde sont pris en charge par un serveur SMB source.
  - Pour un serveur SMB cible, les autorisations suivantes sont requises : liste, lecture et écriture.
- Le serveur de fichiers doit autoriser un hôte de courtier de données à accéder aux exportations via les ports requis.
  - 139 TCP
  - 445 TCP
  - 137-138 UDP
- 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.

Présentation de la mise en réseau pour Cloud Sync

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

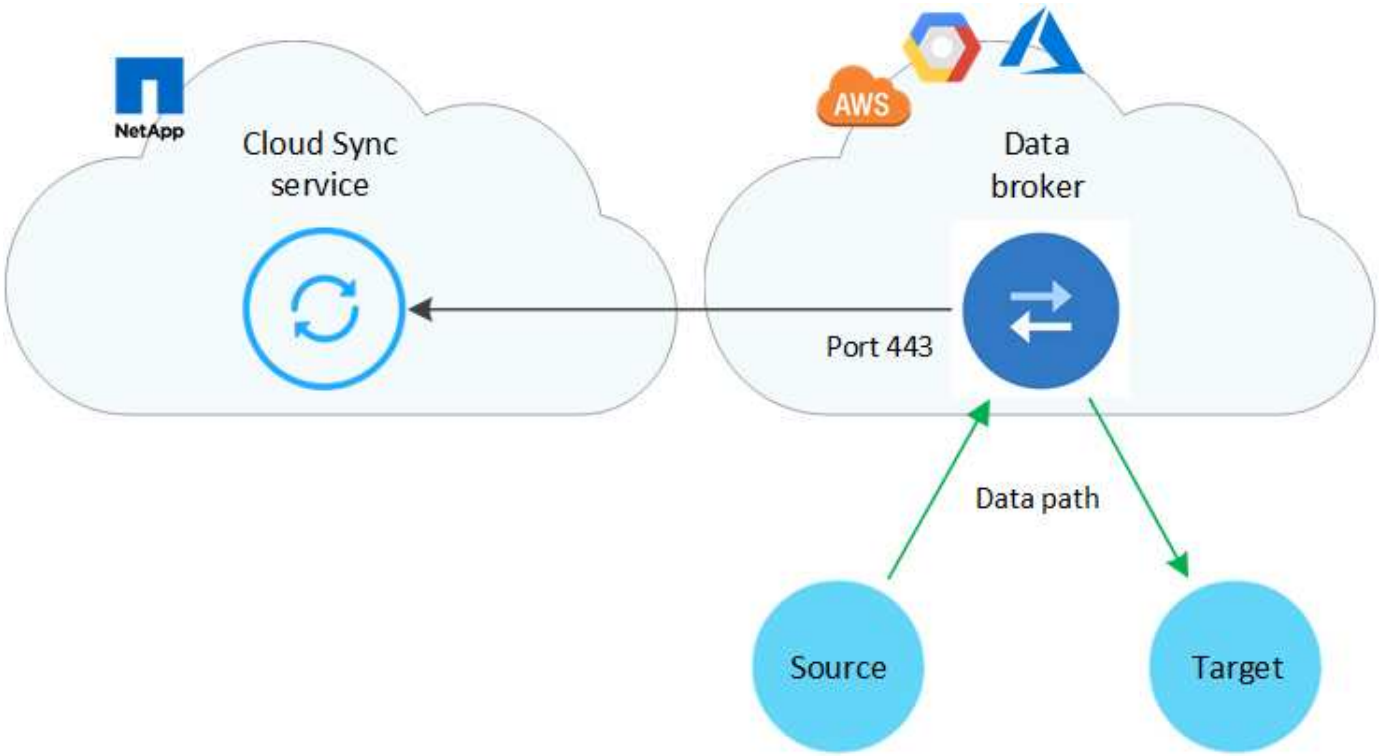
Emplacement du courtier en données

Un courtier en données est constitué d'un ou plusieurs courtiers de données installés dans le cloud ou sur site.

Data broker dans le cloud

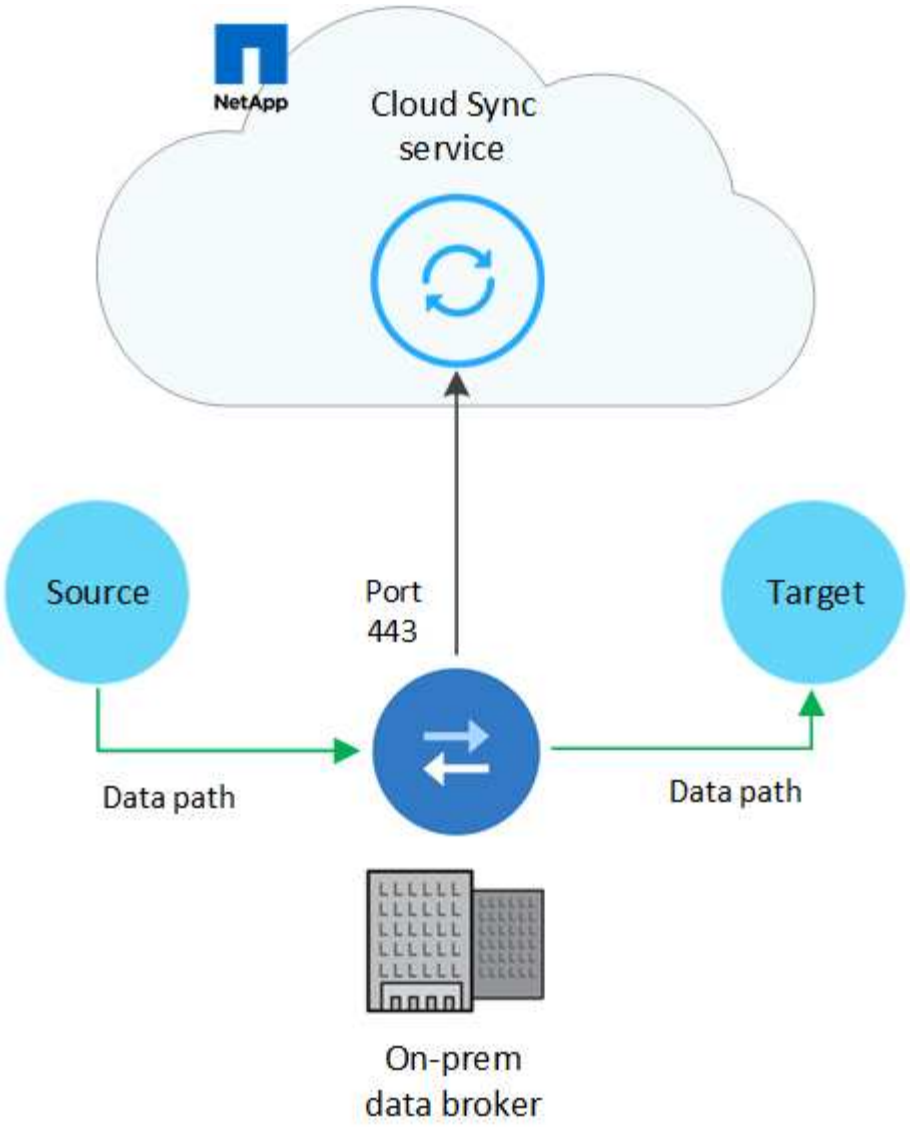
L'image suivante montre un courtier en données exécuté dans le cloud, soit dans AWS, Google Cloud, soit dans Azure. La source et la cible peuvent être hébergées quel que soit le lieu, à condition que le courtier soit connecté. Par exemple, vous pouvez disposer d'une connexion VPN entre votre data center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

Lorsque Cloud Sync déploie le courtier en données dans AWS, Azure ou Google Cloud, il crée un groupe de sécurité qui assure 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 groupe de courtiers de données.

  Par exemple, si un serveur NFS se trouve dans votre data Center et qu'un courtier en données est dans AWS, vous devez disposer d'une connexion réseau (VPN ou Direct Connect) entre votre réseau et le VPC.

- Un courtier de données a besoin d'une connexion Internet sortante pour interroger le service Cloud Sync pour les tâches sur le port 443.
- NetApp recommande d'utiliser le service NTP (Network Time Protocol) pour configurer les courtiers source, cible et données. 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

Un courtier de données contacte les terminaux suivants :

Terminaux	Objectif
https://olcentgbl.trafficmanager.net	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.
https://rpm.nodesource.com https://registry.npmjs.org https://nodejs.org:	Pour contacter des référentiels pour mettre à jour Node.js, npm et d'autres packages tiers utilisés dans le développement.
https://tgz.pm2.io	Pour accéder à un référentiel de mise à jour de PM2, un package tiers utilisé pour surveiller Cloud Sync.
https://sqs.us-east-1.amazonaws.com https://kinesis.us-east-1.amazonaws.com	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).
https://s3.*region*.amazonaws.com 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.
https://s3.us-east-1.amazonaws.com	Lorsque vous téléchargez les journaux de courtier de données depuis Cloud Sync, le courtier zippe son répertoire des journaux et télécharge les journaux vers un compartiment S3 prédéfini dans la région US-East-1.
https://cf.cloudsync.netapp.com https://repo.cloudsync.netapp.com	Pour contacter le service Cloud Sync.
https://support.netapp.com	Pour contacter le support NetApp lors de l'utilisation d'une licence BYOL pour les relations de synchronisation.
https://fedoraproject.org	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.
https://sts.amazonaws.com	Pour vérifier les identifiants AWS lorsque le courtier est déployé dans AWS ou lorsqu'il est déployé sur vos sites et que les identifiants AWS sont fournis. Le courtier de données contacte ce point final pendant le déploiement, lorsqu'il est mis à jour et lorsqu'il est redémarré.
https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour contacter Cloud Data SENSE lorsque vous utilisez Data Sense pour sélectionner les fichiers source d'une nouvelle relation de synchronisation.

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

Installer un courtier de données

Création d'un nouveau courtier en données dans AWS

Lorsque vous créez un nouveau groupe de courtiers de données, choisissez Amazon Web Services pour déployer le logiciel de courtier de données 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 de Chine.

Privilèges root

Le logiciel de courtier de données s'exécute automatiquement en tant que root sur l'hôte Linux. L'exécution en tant que racine est une exigence pour les opérations de courtier de données. Par exemple, pour monter des partages.

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".

Exigences relatives à l'utilisation de 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.

Création du courtier de données

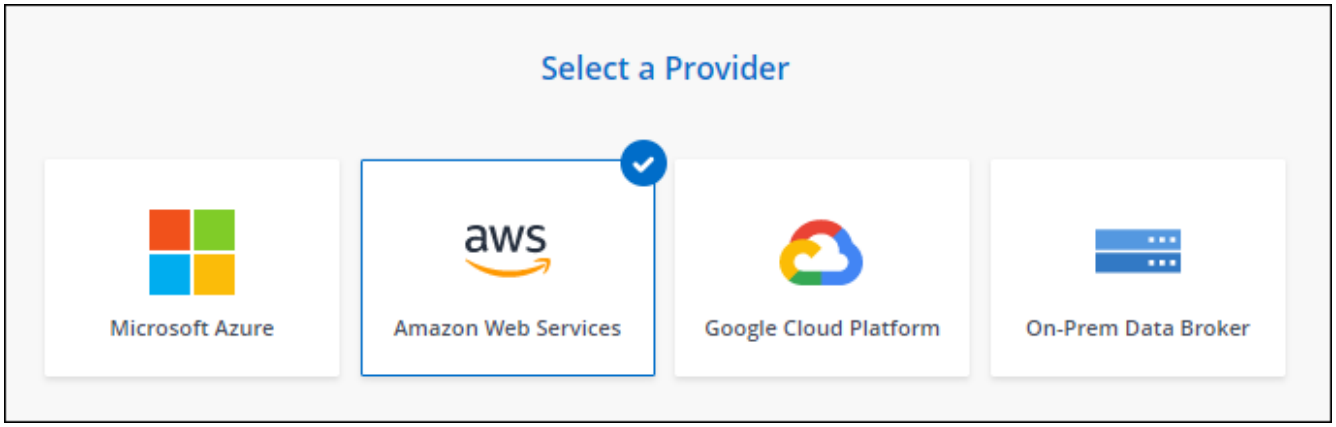
Il existe plusieurs façons de créer un nouveau courtier de données. Décrivez comment installer un courtier de données dans AWS lors de la création d'une relation de synchronisation.

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 **Groupe de courtiers de données**.

3. Sur la page **Groupe de courtiers de données**, cliquez sur **Créer courtier de données**, puis sélectionnez **Amazon Web Services**.



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.

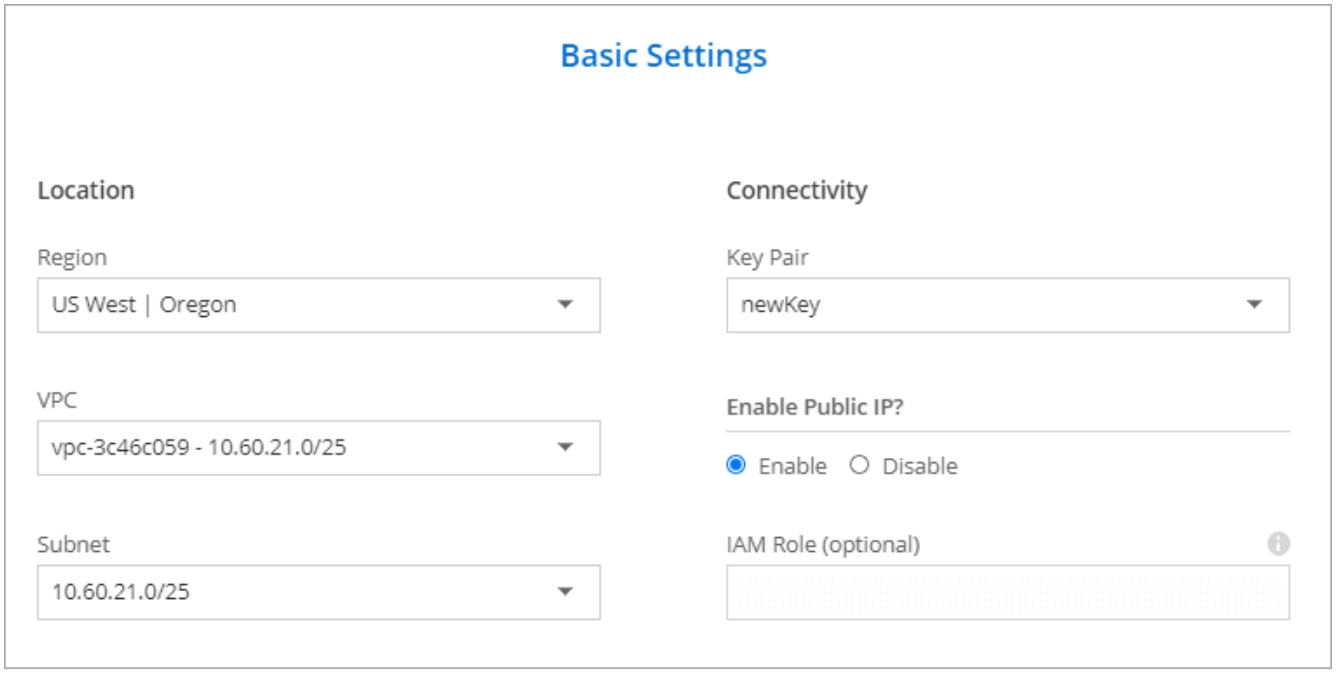
   Si vous préférez ne pas fournir de touches d'accès, cliquez sur le lien en bas de la page pour utiliser un modèle CloudFormation. Lorsque vous utilisez cette option, vous n'avez pas besoin de fournir des identifiants, car vous vous connectez directement à AWS.

   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/cloud-manager-sync//media/video_cloud_sync.mp4 *(video)*

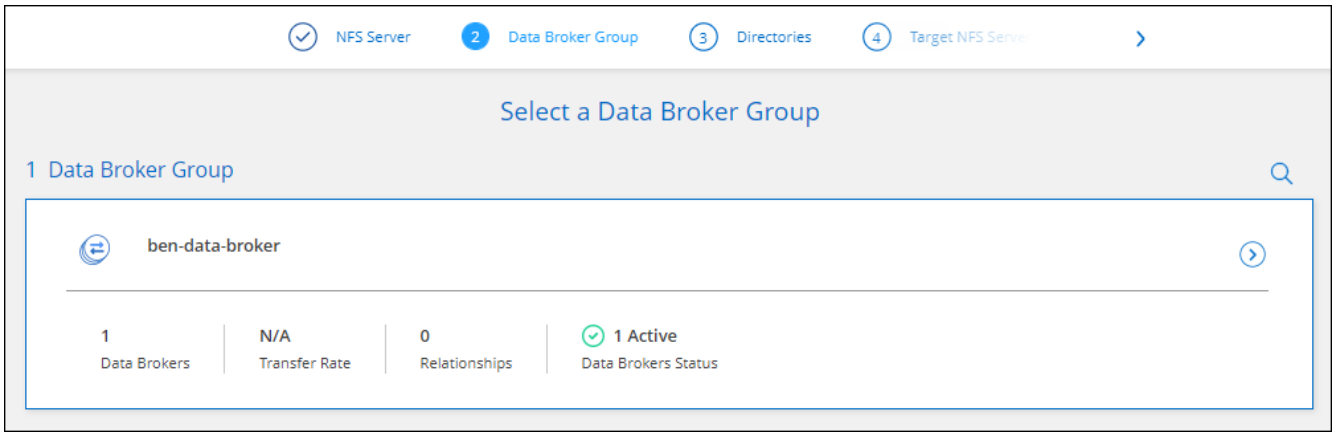
6. Si vous avez saisi une clé d'accès AWS, sélectionnez un emplacement pour l'instance, sélectionnez une paire de clés, choisissez d'activer ou non une adresse IP publique, puis sélectionnez un rôle IAM existant, ou laissez le champ vide afin que Cloud Sync crée le rôle pour vous.

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



7. Spécifiez une configuration proxy, si un proxy est requis pour l'accès Internet dans le VPC.
8. Une fois le courtier de données disponible, cliquez sur **Continuer** dans Cloud Sync.

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



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

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

Détails sur l'instance du courtier de données

Cloud Sync crée un courtier en données dans AWS à l'aide de la configuration suivante.

Type d'instance
m5n.xlarge lorsque disponible dans la région, sinon m5.xlarge

VCPU
4

RAM
16 GO

Système d'exploitation
Amazon Linux 2

Taille et type de disque
SSD GP2 10 GO

Création d'un nouveau courtier en données dans Azure

Lorsque vous créez un nouveau groupe de courtiers de données, choisissez Microsoft Azure pour déployer le logiciel de courtier de données 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.

Privilèges root

Le logiciel de courtier de données s'exécute automatiquement en tant que root sur l'hôte Linux. L'exécution en tant que racine est une exigence pour les opérations de courtier de données. Par exemple, pour monter des partages.

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.

Autorisations requises pour déployer le courtier en données dans Azure

Assurez-vous que le compte utilisateur Azure que vous utilisez pour déployer le courtier de données dispose des autorisations suivantes :

```
{
    "Name": "Azure Data Broker",
    "Actions": [
                    "Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/deployments/operationstatuses/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Resources/deployments/cancel/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/publicIPAddresses/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",

"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/virtualNetworks/read",
                    "Microsoft.Network/publicIPAddresses/write",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/publicIPAddresses/read",
```

```
"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Network/publicIPAddresses/join/action",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Storage/storageAccounts/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/write",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/delete",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action",
                    "Microsoft.EventGrid/systemTopics/read",
                    "Microsoft.EventGrid/systemTopics/write",
                    "Microsoft.EventGrid/systemTopics/delete",
                    "Microsoft.EventGrid/eventSubscriptions/write",
                    "Microsoft.Storage/storageAccounts/write"
```

```
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}
```

Remarque :

1. Les autorisations suivantes sont uniquement nécessaires si vous prévoyez d'activer le paramètre de synchronisation continue d'une relation de synchronisation depuis Azure vers un autre emplacement de stockage cloud :
    - « Microsoft.Storage/storageAccounts/read »,
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action',
    - 'Microcrosoft.EventGrid/systemTopics/read',
    - 'Crossoft.EventGrid/systemTopics/write',
    - 'Crosoft.EventGrid/systemTopics/delete',

- 'Icrosoft.EventGrid/souscriptions/écriture d'événements',
- « Microsoft.Storage/storageAccounts/write »

En outre, le périmètre attribuable doit être défini sur étendue de l'abonnement et **pas** étendue du groupe de ressources si vous prévoyez d'implémenter la synchronisation continue dans Azure.

"En savoir plus sur le paramètre de synchronisation continue".

METHODE d'authentification

Lorsque vous déployez le courtier de données, vous devrez choisir une méthode d'authentification pour la machine virtuelle : 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".

Création du courtier de données

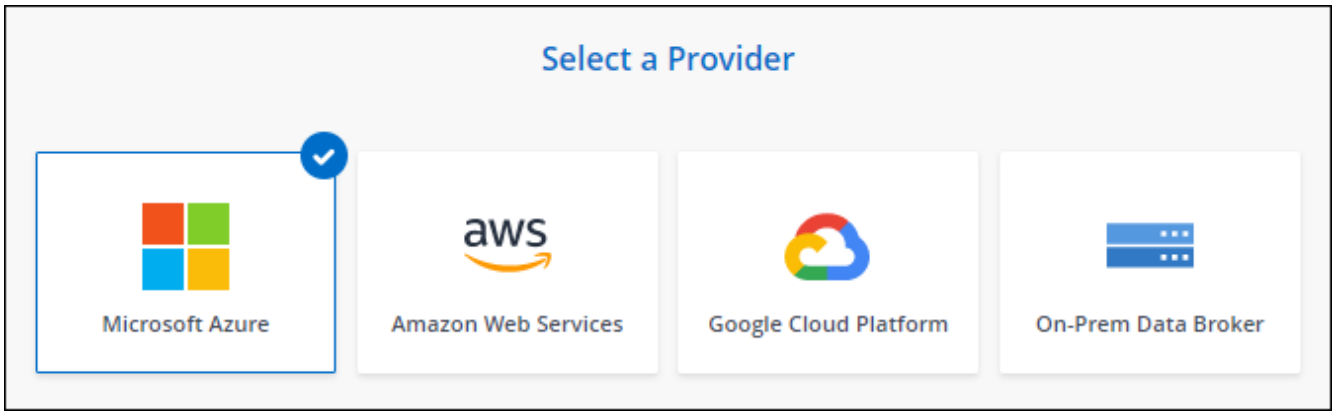
Il existe plusieurs façons de créer un nouveau courtier de données. Lors de la création d'une relation de synchronisation, procédez comme suit pour installer un courtier de données dans Azure.

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 **Groupe de courtiers de données**.

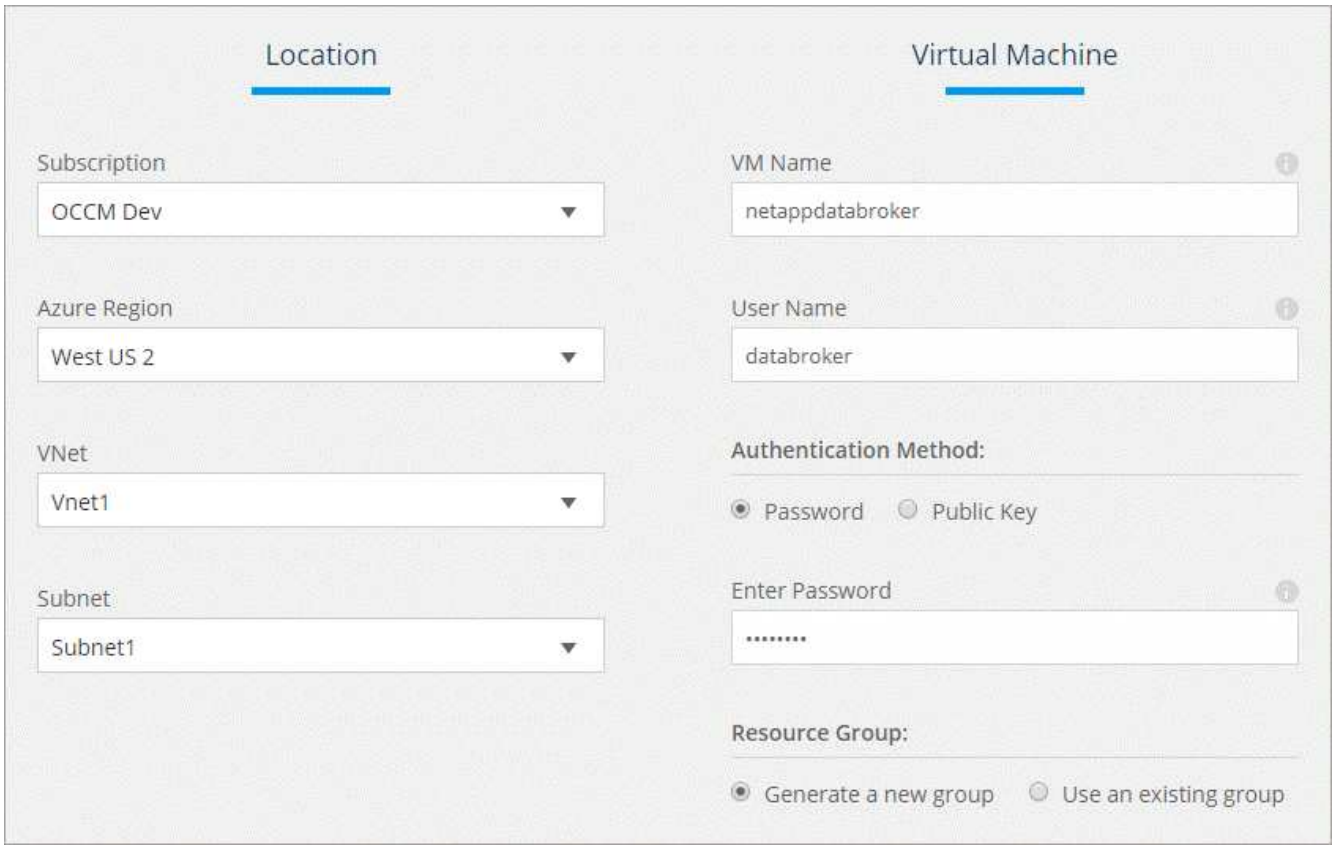
3. Sur la page **Groupe de courtiers de données**, cliquez sur **Créer courtier de données**, puis sélectionnez **Microsoft Azure**.



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.



Si vous prévoyez d'implémenter une relation de synchronisation continue, vous devez attribuer un rôle personnalisé à votre courtier de données. Cela peut également être effectué manuellement après la création du courtier.

7. Spécifiez une configuration proxy, si un proxy est requis pour l'accès Internet dans le vnet.
8. Cliquez sur **Continuer** et maintenez la page ouverte jusqu'à ce que le déploiement soit terminé.

   Ce processus peut prendre jusqu'à 7 minutes.

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

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.

Détails sur la machine virtuelle du courtier de données

Cloud Sync crée un courtier de données dans Azure à l'aide de la configuration suivante.

Type de VM
Standard DS4 v2

VCPU
8

RAM
28 GO

Système d'exploitation
CentOS 7.7

Taille et type de disque
SSD premium de 64 Go

Création d'un nouveau courtier en données dans Google Cloud

Lorsque vous créez un nouveau groupe de courtiers de données, choisissez Google Cloud Platform pour déployer le logiciel de courtier de données sur une nouvelle instance de machine virtuelle dans un VPC Google 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.

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 Google Cloud prises en charge

Toutes les régions sont prises en charge.

Privilèges root

Le logiciel de courtier de données s'exécute automatiquement en tant que root sur l'hôte Linux. L'exécution en tant que racine est une exigence pour les opérations de courtier de données. Par exemple, pour monter des partages.

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 en données dans Google Cloud, il crée un groupe de sécurité qui assure 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 en données dans Google Cloud

Assurez-vous que l'utilisateur Google Cloud 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.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update
- iam.serviceAccounts.signJwt
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
```

Remarques :

1. L'autorisation "iam.serviceAccounts.signJwt" n'est requise que si vous prévoyez de configurer le courtier de données pour utiliser un coffre-fort externe HashiCorp.
2. Les autorisations « pubsub.* » et « Storage.seaux.update » sont uniquement requises si vous prévoyez d'activer le paramètre de synchronisation continue sur une relation de synchronisation depuis Google Cloud Storage vers un autre emplacement de stockage cloud. "En savoir plus sur l'option de synchronisation continue".

Création du courtier de données

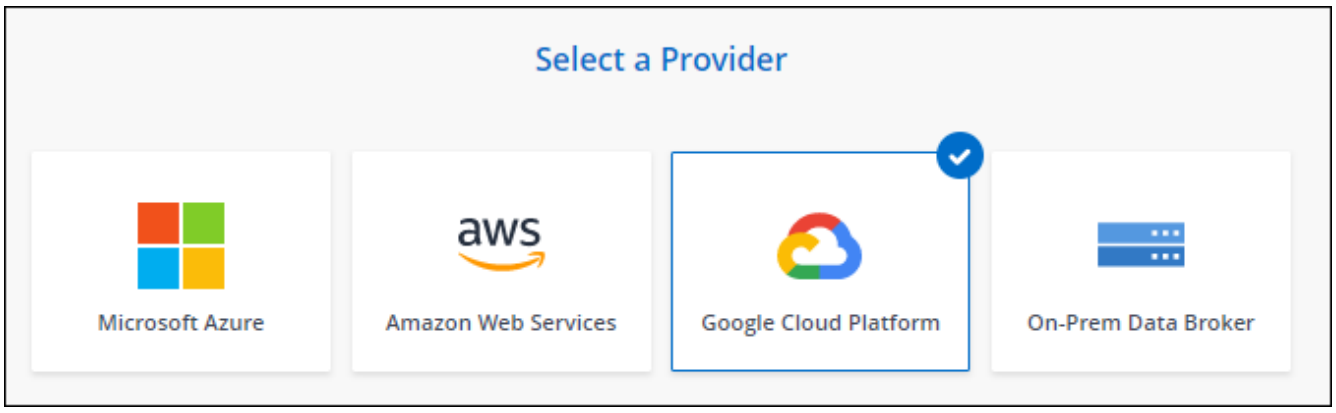
Il existe plusieurs façons de créer un nouveau courtier de données. Lors de la création d'une relation de synchronisation, procédez comme suit pour installer un courtier de données dans Google Cloud.

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 **Groupe de courtiers de données**.

3. Sur la page **Groupe de courtiers de données**, cliquez sur **Créer courtier de données**, puis sélectionnez **Google Cloud Platform**.

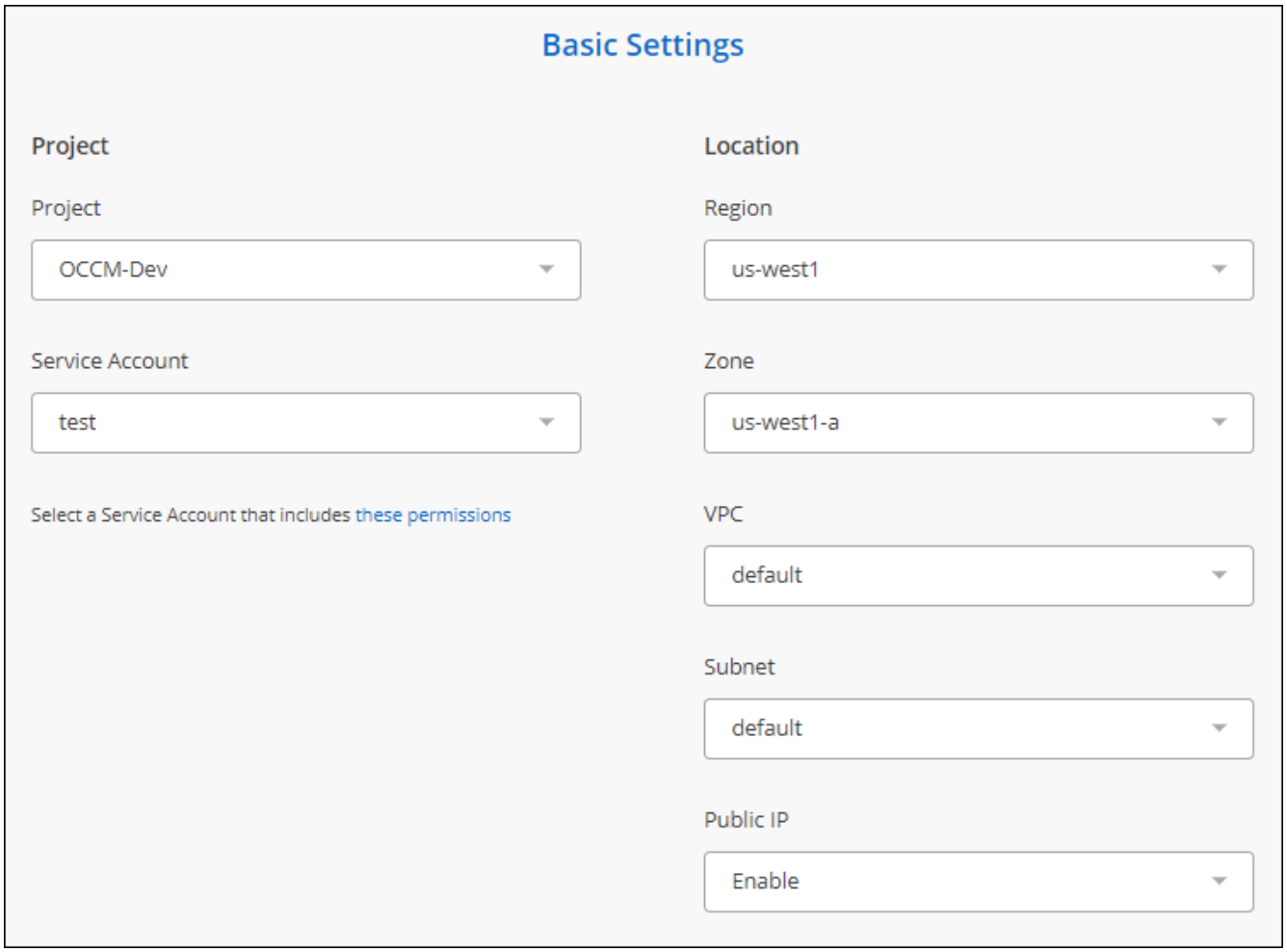


4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à l'aide de votre compte Google.

   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, y compris si vous souhaitez activer ou désactiver une adresse IP publique.

   Si vous n'activez pas d'adresse IP publique, vous devez définir un serveur proxy à l'étape suivante.



7. Spécifiez une configuration proxy, si un proxy est requis pour l'accès Internet dans le VPC.

Si un proxy est requis pour l'accès Internet, il doit être dans Google Cloud et utiliser le même compte de service que le courtier de données.

8. 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.

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

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

Fourniture d'autorisations d'utilisation de compartiments dans d'autres projets Google Cloud

Lorsque vous créez une relation synchrone et que vous choisissez Google Cloud Storage comme source ou cible, Cloud Sync vous permet de choisir dans les compartiments que le compte de service du courtier de données est autorisé à utiliser. Par défaut, cela inclut les rubriques qui se trouvent dans le *same* projet comme le compte de service du courtier de données. Mais vous pouvez choisir des compartiments dans *Other* projets si vous fournissez les autorisations requises.

Étapes

1. Ouvrez la console Google Cloud Platform et chargez le service Cloud Storage.
2. Cliquez sur le nom du compartiment à utiliser en tant que source ou cible dans une relation de synchronisation.
3. Cliquez sur **autorisations**.
4. Cliquez sur **Ajouter**.
5. Entrez le nom du compte de service du courtier de données.
6. Sélectionnez un rôle required for the service account,les mêmes autorisations que celles indiquées ci-dessus.
7. Cliquez sur **Enregistrer**.

Lorsque vous configurez une relation de synchronisation, vous pouvez désormais choisir ce compartiment en tant que source ou cible dans la relation de synchronisation.

Détails sur l'instance de VM du courtier de données

Cloud Sync crée un courtier en données dans Google Cloud à l'aide de la configuration suivante.

Type de machine
n2-standard-4

VCPU
4

RAM
15 GO

Système d'exploitation
Red Hat Enterprise Linux 7.7

Taille et type de disque

Disque dur pd-standard 20 Go

Installation du data broker sur un hôte Linux

Lorsque vous créez un nouveau groupe de courtiers de données, choisissez l'option courtier de données sur site 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

    CentOS Stream n'est pas pris en charge.
  - Red Hat Enterprise Linux 7.7 et 8.0
  - Ubuntu Server 20.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    La commande `yum update` 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.

Privilèges root

Le logiciel de courtier de données s'exécute automatiquement en tant que root sur l'hôte Linux. L'exécution en tant que racine est une exigence pour les opérations de courtier de données. Par exemple, pour monter des partages.

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 Google Cloud. 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 Google Cloud disposant des autorisations d'administrateur de stockage, si vous n'en avez pas encore.
2. Créez une clé de compte de service enregistrée au format JSON.

   "Consultez les instructions relatives à Google Cloud"

   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

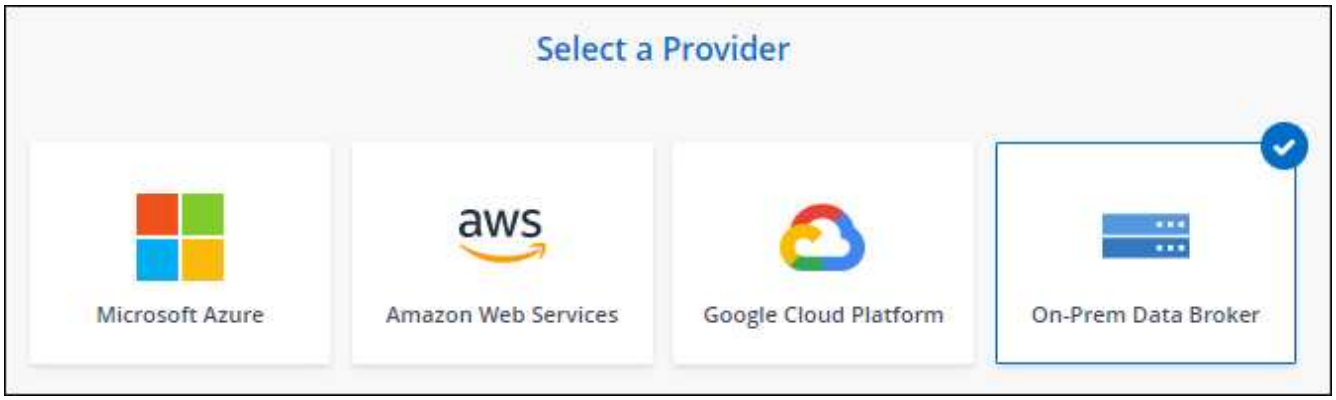
Vous pouvez installer un courtier de données sur un hôte Linux lorsque vous créez une relation de synchronisation.

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 **Groupe de courtiers de données**.

3. Sur la page **Groupe de courtiers de données**, cliquez sur **Créer courtier de données**, puis sélectionnez **Agent de données sur site**.



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. the data broker,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 Google Cloud. 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 access to AWS,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 access to Google Cloud,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.