



Commencer

NetApp Copy and Sync

NetApp
December 16, 2025

This PDF was generated from <https://docs.netapp.com/fr-fr/data-services-copy-sync/concept-cloud-sync.html> on December 16, 2025. Always check docs.netapp.com for the latest.

Sommaire

Commencer	1
En savoir plus sur NetApp Copy and Sync	1
NetApp Console	1
Comment fonctionne NetApp Copy and Sync	1
Types de stockage pris en charge	2
Frais	3
Démarrage rapide pour NetApp Copy and Sync	3
Relations de synchronisation prises en charge dans NetApp Copy and Sync	4
Préparez la source et la cible dans NetApp Copy and Sync	12
Réseautage	12
Répertoire cible	12
Autorisations de lecture des répertoires	12
Exigences du bucket Amazon S3	13
Exigences de stockage Azure Blob	14
Stockage Azure Data Lake Gen2	16
Exigences relatives aux Azure NetApp Files	16
Exigences relatives à la boîte	17
Exigences relatives au bucket Google Cloud Storage	17
Google Drive	18
Configuration requise pour le serveur NFS	18
Exigences ONTAP	19
Exigences de stockage ONTAP S3	19
Configuration requise pour le serveur SMB	19
Présentation du réseau pour NetApp Copy and Sync	20
Localisation du courtier en données	20
Exigences de mise en réseau	21
Points de terminaison réseau	21
Connectez-vous à NetApp Copy and Sync	23
Installer un courtier de données	24
Créer un nouveau courtier de données dans AWS pour NetApp Copy and Sync	24
Créer un nouveau courtier de données dans Azure pour NetApp Copy and Sync	27
Créer un nouveau courtier de données dans Google Cloud pour NetApp Copy and Sync	33
Installer le courtier de données sur un hôte Linux pour NetApp Copy and Sync	38

Commencer

En savoir plus sur NetApp Copy and Sync

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

NetApp Console

NetApp Copy and Sync est accessible via la NetApp Console.

La NetApp Console fournit une gestion centralisée des services de stockage et de données NetApp dans les environnements sur site et cloud à l'échelle de l'entreprise. La console est requise pour accéder aux services de données NetApp et les utiliser. En tant qu'interface de gestion, il vous permet de gérer de nombreuses ressources de stockage à partir d'une seule interface. Les administrateurs de console peuvent contrôler l'accès au stockage et aux services pour tous les systèmes de l'entreprise.

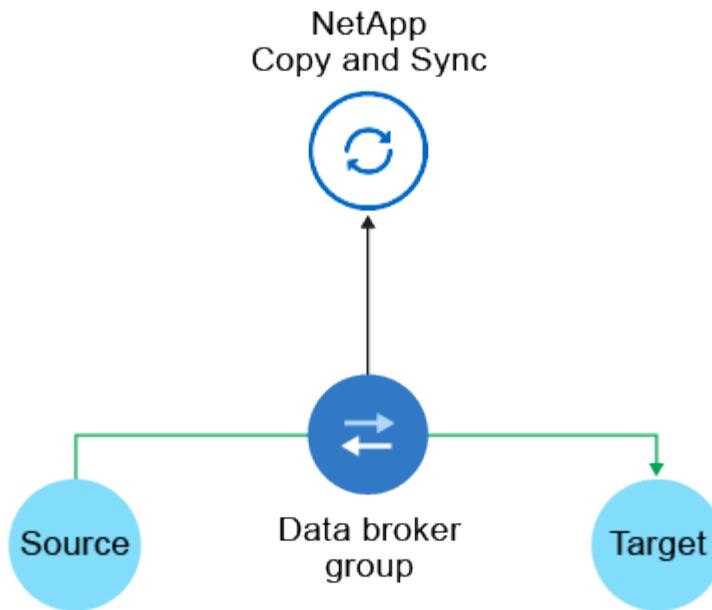
Vous n'avez pas besoin de licence ni d'abonnement pour commencer à utiliser NetApp Console et vous n'encourez des frais que lorsque vous devez déployer des agents de console dans votre cloud pour garantir la connectivité à vos systèmes de stockage ou à vos services de données NetApp . Cependant, certains services de données NetApp accessibles depuis la console sont sous licence ou basés sur un abonnement.

En savoir plus sur le ["NetApp Console"](#) .

Comment fonctionne NetApp Copy and Sync

NetApp Copy and Sync est une plate-forme SaaS (Software-as-a-Service) composée d'un groupe de courtiers en données, d'une interface basée sur le cloud disponible via la NetApp Console, ainsi que d'une source et d'une cible.

L'image suivante montre la relation entre les composants Copie et Synchronisation :



Le logiciel de courtier de données NetApp synchronise les données d'une source vers une cible (c'est ce qu'on appelle une *relation de synchronisation*). Vous pouvez exécuter le courtier de données dans AWS, Azure, Google Cloud Platform ou dans vos locaux. Un groupe de courtiers de données, composé d'un ou de plusieurs courtiers de données, a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec Copy and Sync et contacter quelques autres services et référentiels. ["Afficher la liste des points de terminaison"](#) .

Après la copie initiale, Copier et synchroniser synchronise toutes les données modifiées en fonction de la planification que vous avez définie.

Types de stockage pris en charge

Copy and Sync prend en charge les types de stockage suivants :

- N'importe quel serveur NFS
- N'importe quel serveur PME
- Amazon EFS
- Amazon FSx pour ONTAP
- Amazon S3
- Azure Blob
- Stockage Azure Data Lake Gen2
- Azure NetApp Files
- Coffret (disponible en avant-première)
- Cloud Volumes ONTAP
- Stockage Google Cloud
- Google Drive
- Stockage d'objets IBM Cloud
- Cluster ONTAP sur site

- Stockage ONTAP S3
- SFTP (en utilisant uniquement l'API)
- StorageGRID

["Afficher les relations de synchronisation prises en charge"](#) .

Frais

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

Frais de ressources

Les frais de 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 auprès d'AWS ou d'Azure, ce qui vous permet de payer à l'heure ou à l'année. La deuxième option consiste à acheter des licences directement auprès de NetApp.

["Découvrez comment fonctionnent les licences"](#) .

Démarrage rapide pour NetApp Copy and Sync

La mise en route de NetApp Copy and Sync comprend quelques étapes.

1

Connectez-vous et configurez la NetApp Console

Vous devriez avoir commencé à utiliser la NetApp Console, ce qui inclut la connexion, la configuration d'un compte et éventuellement le déploiement d'un agent de console et la création de systèmes.

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

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

Un agent de console est requis pour Cloud Volumes ONTAP, les clusters ONTAP sur site et Amazon FSx for ONTAP.

- ["Découvrez comment démarrer avec la NetApp Console"](#)
- ["En savoir plus sur les agents de console"](#)

2

Préparez votre source et votre cible

Vérifiez que votre source et votre cible sont prises en charge et configurées. L'exigence la plus importante est de vérifier la connectivité entre le groupe de courtiers de données et les emplacements source et cible.

- "[Afficher les relations prises en charge](#)"
- "[Préparez la source et la cible](#)"

3

Préparez un emplacement pour le courtier de données NetApp

Le logiciel de courtier de données NetApp synchronise les données d'une source vers une cible (c'est ce qu'on appelle une *relation de synchronisation*). Vous pouvez exécuter le courtier de données dans AWS, Azure, Google Cloud Platform ou dans vos locaux. Un groupe de courtiers de données, composé d'un ou de plusieurs courtiers de données, a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec NetApp Copy and Sync et contacter quelques autres services et référentiels. "[Afficher la liste des points de terminaison](#)" .

NetApp Copy and 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.

- "[Examen de l'installation d'AWS](#)"
- "[Examen de l'installation d'Azure](#)"
- "[Examen de l'installation de Google Cloud](#)"
- "[Examen de l'installation de l'hôte Linux](#)"

4

Créez votre première relation de synchronisation

Connectez-vous à "[la NetApp Console](#)" , sélectionnez **Synchroniser**, puis faites glisser et déposez vos sélections pour la source et la cible. Suivez les instructions pour terminer la configuration. "[Apprendre encore plus](#)" .

5

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

Abonnez-vous à AWS ou Azure pour payer à l'utilisation ou annuellement. Ou achetez des licences directement auprès de NetApp. Accédez simplement à la page Paramètres de licence dans NetApp Copy and Sync pour le configurer. "[Apprendre encore plus](#)" .

Relations de synchronisation prises en charge dans NetApp Copy and Sync

NetApp Copy and Sync vous permet de synchroniser les données d'une source vers une cible. C'est ce qu'on appelle une relation de synchronisation. Vous devez comprendre les relations prises en charge avant de commencer.

Localisation de la source	Emplacements cibles pris en charge
Amazon EFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • serveur SMB • StorageGRID
Amazon FSx pour ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • serveur SMB • StorageGRID

Localisation de la source	Emplacements cibles pris en charge
Amazon S3	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Boîte ¹ • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • Stockage ONTAP S3 • serveur SMB • StorageGRID
Azure Blob	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • serveur SMB • StorageGRID

Localisation de la source	Emplacements cibles pris en charge
Stockage Azure Data Lake Gen2	<ul style="list-style-type: none"> • Azure NetApp Files • Cloud Volumes ONTAP • FSx pour ONTAP • Stockage d'objets IBM Cloud • serveur NFS • ONTAP sur site • Stockage ONTAP S3 • serveur SMB • StorageGRID
Azure NetApp Files	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • serveur SMB • StorageGRID
Boîte ¹	<ul style="list-style-type: none"> • Amazon FSx pour ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • Stockage d'objets IBM Cloud • serveur NFS • serveur SMB • StorageGRID

Localisation de la source	Emplacements cibles pris en charge
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • serveur SMB • StorageGRID
Stockage Google Cloud	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • Stockage ONTAP S3 • serveur SMB • StorageGRID
Google Drive	<ul style="list-style-type: none"> • serveur NFS • serveur SMB

Localisation de la source	Emplacements cibles pris en charge
Stockage d'objets IBM Cloud	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Boîte ¹ • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • serveur SMB • StorageGRID
serveur NFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Google Drive • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • Stockage ONTAP S3 • serveur SMB • StorageGRID

Localisation de la source	Emplacements cibles pris en charge
Cluster ONTAP sur site (NFS ou SMB)	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • serveur SMB • StorageGRID
Stockage ONTAP S3	<ul style="list-style-type: none"> • Amazon S3 • Stockage Azure Data Lake Gen2 • Stockage Google Cloud • serveur NFS • serveur SMB • StorageGRID • Stockage ONTAP S3
SFTP ²	S3

Localisation de la source	Emplacements cibles pris en charge
serveur SMB	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Stockage Google Cloud • Google Drive • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • Stockage ONTAP S3 • serveur SMB • StorageGRID
StorageGRID	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx pour ONTAP • Amazon S3 • Azure Blob • Stockage Azure Data Lake Gen2 • Azure NetApp Files • Boîte ¹ • Cloud Volumes ONTAP • Stockage Google Cloud • Stockage d'objets IBM Cloud • serveur NFS • Cluster ONTAP sur site (NFS ou SMB) • Stockage ONTAP S3 • serveur SMB • StorageGRID

Remarques :

1. Le support Box est disponible en avant-première.
2. Les relations de synchronisation avec cette source/cible sont prises en charge uniquement à l'aide de l'API Copier et synchroniser.

3. Vous pouvez choisir un niveau de stockage Azure Blob spécifique lorsqu'un conteneur Blob est la cible :
 - Stockage à chaud
 - Stockage au frais
4. Vous pouvez choisir une classe de stockage S3 spécifique lorsque Amazon S3 est la cible :
 - Standard (c'est la classe par défaut)
 - Hiérarchisation intelligente
 - Accès standard-peu fréquent
 - Une zone - Accès peu fréquent
 - Archives des profondeurs des glaciers
 - Récupération flexible des glaciers
 - Récupération instantanée du glacier
5. Vous pouvez choisir une classe de stockage spécifique lorsqu'un bucket Google Cloud Storage est la cible :
 - Standard
 - Nearline
 - Coldline
 - Archive

Préparez la source et la cible dans NetApp Copy and Sync

Vérifiez que votre source et vos cibles répondent aux exigences suivantes dans NetApp Copy and Sync.

Réseautage

- 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 centre de données et qu'un courtier de données se trouve dans AWS, vous avez besoin d'une connexion réseau (VPN ou Direct Connect) de votre réseau au 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, Copier et synchroniser vous permet de sélectionner un répertoire cible existant, puis éventuellement de créer un nouveau dossier à l'intérieur de ce répertoire. Assurez-vous donc que votre répertoire cible préféré existe déjà.

Autorisations de lecture des répertoires

Afin d'afficher chaque répertoire ou dossier d'une source ou d'une cible, Copy and 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 d'objets

- Pour AWS et Google Cloud, un courtier de données doit disposer d'autorisations d'objet 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 que vous saisissez 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 par défaut les répertoires suivants : .snapshot, ~snapshot, .copy-offload



Lors de la copie de données SMB dans Cloud Volumes ONTAP à l'aide de la fonction Copier et synchroniser, la propriété des fichiers et des dossiers du système source n'est pas conservée. Ce comportement est dû au fait que Copy and Sync utilise un client SMB Linux, qui attribue la propriété au compte utilisateur ou de service utilisé pour authentifier le transfert. Bien que les listes de contrôle d'accès puissent être conservées, les informations relatives à la propriété et à l'audit peuvent différer du système source. C'est le comportement attendu.

Exigences du bucket Amazon S3

Assurez-vous 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 courtier de données déployé dans AWS ou sur vos locaux. Dans les deux cas, Copy and 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 qui n'est pas associé à un courtier de données.

["Les autorisations incluses dans ce fichier JSON"](#) doit être appliquée à ce compartiment S3 pour qu'un courtier de données puisse y accéder. Ces autorisations permettent au courtier de données de copier des données vers et depuis le bucket et de répertorier les objets dans le bucket.

Notez les points suivants concernant les autorisations incluses dans le fichier JSON :

1. <BucketName> est le nom du bucket qui réside dans le compte AWS qui n'est pas associé à un courtier de 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 les 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 l'ARN du rôle en accédant à la console EC2, en sélectionnant l'instance du courtier de données, puis en sélectionnant le rôle IAM dans l'onglet Description. Vous devriez alors voir la page Résumé dans la console IAM qui contient l'ARN du rôle.

Summary

[Delete role](#)

Role ARN	arn:aws:iam::123456789012:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05	
Role description	Edit	

Exigences de stockage Azure Blob

Assurez-vous que votre stockage d'objets blob Azure répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour Azure Blob

Un courtier de données peut résider à n'importe quel emplacement 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 Chine, Gouvernement américain et Département de la Défense américain.

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

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

The screenshot shows the Azure Storage account settings page for 'a63cde60b553020'. The 'Access keys' tab is selected. The page includes a search bar, a sidebar with various links, and a main content area with instructions about access keys. The 'Storage account name' is listed as 'a63cde60b553020'. Two access keys are shown: 'key1' with the value 'vScjFdVZqIPyO/' and 'key2' with a redacted value. A 'Connection string' field for 'key1' contains 'DefaultEndpoints' and is also highlighted with a red box. A 'Download' button is present next to each key and the connection string.

Si vous souhaitez synchroniser des données entre deux conteneurs Azure Blob, la chaîne de connexion doit inclure un "[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 : Lire et Lister
- Pour le conteneur Blob cible : lecture, écriture, liste, ajout et création

Storage account a63cde60b553020 - Shared access signature

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Storage Explorer (preview)

Settings

Access keys

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Advanced Threat Protection (pr...)

Properties

Locks

Allowed services

Blob File Queue Table

Allowed resource types

Service Container Object

Allowed permissions

Read Write Delete List Add Create Update Process

Start and expiry date/time

Start: 2018-10-23 10:07:32 AM

End: 2019-10-23 6:07:32 PM

(UTC-04:00) --- Current Time Zone ---

Allowed IP addresses

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

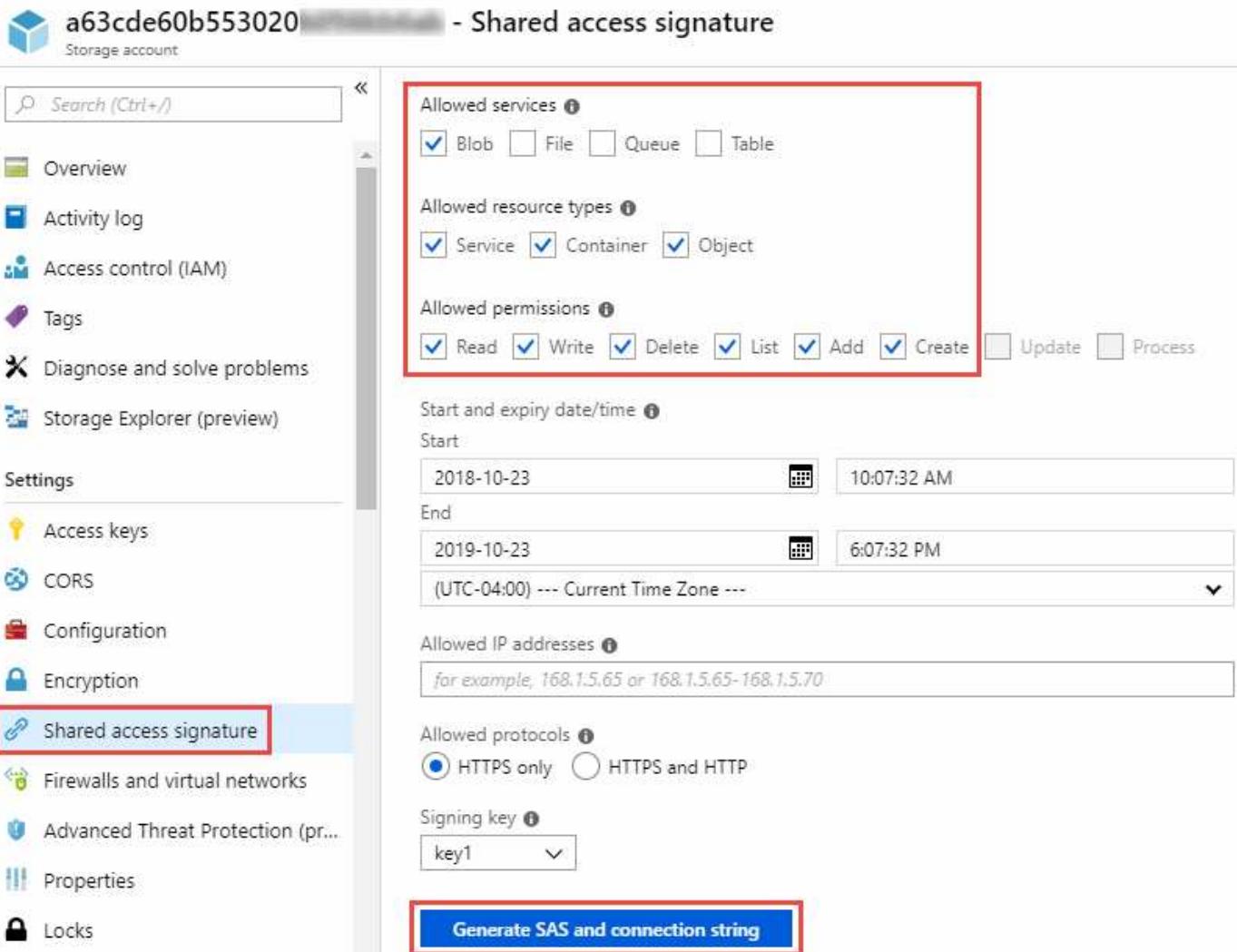
Allowed protocols

HTTPS only HTTPS and HTTP

Signing key

key1

Generate SAS and connection string



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 configurée pour expirer dans un avenir proche.

Stockage Azure Data Lake Gen2

Lors de la création d'une relation de synchronisation qui inclut Azure Data Lake, vous devez fournir Copie et synchronisation avec la chaîne de connexion du compte de stockage. Il doit s'agir d'une chaîne de connexion régulière et non d'une signature d'accès partagé (SAS).

Exigences relatives aux 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 échecs et des problèmes de performances si le niveau de service du disque est Standard.

Consultez un architecte de solutions si vous avez besoin d'aide pour déterminer le niveau de service approprié. La taille du volume et le niveau de volume déterminent le débit que vous pouvez obtenir.

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

Exigences relatives à la boîte

- Pour créer une relation de synchronisation qui inclut Box, vous devrez fournir les informations d'identification suivantes :
 - ID client
 - Secret client
 - Clé privée
 - ID de clé publique
 - Phrase de passe
 - ID d'entreprise
- Si vous créez une relation de synchronisation d'Amazon S3 vers Box, vous devez utiliser un groupe de courtiers de données doté d'une configuration unifiée où les paramètres suivants sont définis sur 1 :
 - Concurrence des scanners
 - Limite des processus du scanner
 - Concurrence du transféreur
 - Limite des processus de transfert

["Découvrez comment définir une configuration unifiée pour un groupe de courtiers de données" .](#)

Exigences relatives au bucket Google Cloud Storage

Assurez-vous que votre bucket 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 courtier de données déployé dans Google Cloud ou sur vos locaux. Copy and 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 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 buckets dans d'autres projets Google Cloud

Lors de la configuration d'une relation de synchronisation, vous pouvez choisir parmi les buckets Google Cloud dans différents projets, si vous fournissez les autorisations requises au compte de service du courtier de données. ["Apprenez à configurer le compte de service"](#) .

Autorisations pour une destination SnapMirror

Si la source d'une relation de synchronisation est une destination SnapMirror (qui est en lecture seule), les autorisations « lecture/liste » sont suffisantes pour synchroniser les données de la source vers une cible.

Chiffrer un bucket Google Cloud

Vous pouvez chiffrer un bucket Google Cloud cible avec une clé KMS gérée par le client ou la clé par défaut gérée par Google. Si le bucket dispose déjà d'un cryptage KMS, il remplacera le cryptage par défaut géré par Google.

Pour ajouter une clé KMS gérée par le client, vous devrez utiliser un courtier de données avec le "["autorisations correctes"](#)" , et la clé doit être dans la même région que le bucket.

Google Drive

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

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

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

- "["Créer le compte de service et les informations d'identification"](#)"
- "["Déléguez l'autorité à l'échelle du domaine à votre compte de service"](#)"

Lorsque vous modifiez le champ Étendues OAuth, saisissez 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 permettre à un hôte de courtier de données d'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'exportation NFS pour un SVM est activé (vserver nfs modify -vserver *svm_name* -showmount enabled).



Le paramètre par défaut pour showmount est *enabled* à partir d' ONTAP 9.2.

Exigences ONTAP

Si la relation de synchronisation inclut Cloud Volumes ONTAP ou un cluster ONTAP sur site et que vous avez sélectionné NFSv4 ou une version ultérieure, vous devrez activer les ACL NFSv4 sur le système ONTAP . Ceci est nécessaire pour copier les ACL.

Exigences de stockage ONTAP S3

Lorsque vous configurez une relation de synchronisation qui inclut "[Stockage ONTAP S3](#)" , vous devrez fournir les éléments suivants :

- L'adresse IP du LIF connecté à ONTAP S3
- La clé d'accès et la clé secrète 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 Copy and Sync des informations d'identification disposant d'autorisations sur le serveur SMB.
 - Pour un serveur SMB source, les autorisations suivantes sont requises : liste et lecture.
- Les membres du groupe Opérateurs de sauvegarde sont pris en charge avec un serveur SMB source.
- Pour un serveur SMB cible, les autorisations suivantes sont requises : liste, lecture et écriture.
- Le serveur de fichiers doit permettre à un hôte de courtier de données d'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 » sur les dossiers source et cible.

Si vous n'accordez pas cette autorisation, le courtier de données risque de ne pas disposer des autorisations suffisantes pour obtenir les ACL sur un fichier ou un répertoire. Si cela se produit, vous recevezrez l'erreur suivante : « getxattr error 95 »

Limitation SMB pour les répertoires et fichiers cachés

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

Comportement de synchronisation SMB en raison de la limitation de l'insensibilité à la casse

Le protocole SMB n'est pas sensible à la casse, ce qui signifie que les lettres majuscules et minuscules sont traitées comme étant identiques. Ce comportement peut entraîner des fichiers écrasés 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 Copier et Sync copie le fichier nommé « a » vers la cible, le fichier « A » est écrasé 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 Copy and Sync tente de copier le répertoire nommé « b » vers la cible, Copy and Sync reçoit une erreur indiquant que le répertoire existe déjà. Par conséquent, Copy and Sync ne parvient toujours pas à copier le répertoire nommé « b ».

La meilleure façon d'éviter cette limitation est de s'assurer de synchroniser les données dans un répertoire vide.

Présentation du réseau pour NetApp Copy and Sync

La mise en réseau pour NetApp Copy and 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 via le port 443.

Localisation du courtier en données

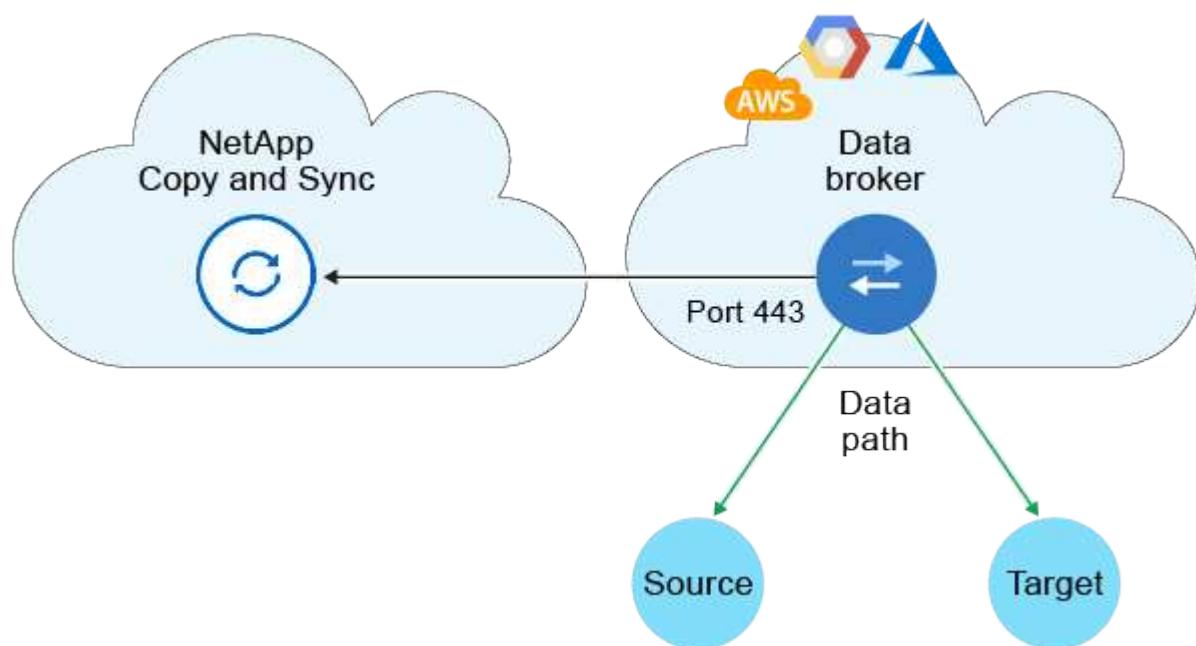
Un groupe de courtiers en données se compose d'un ou plusieurs courtiers en données installés dans le cloud ou dans vos locaux.

Courtier de données dans le cloud

L'image suivante montre un courtier de données exécuté dans le cloud, dans AWS, Google Cloud ou Azure. La source et la cible peuvent se trouver à n'importe quel endroit, à condition qu'il existe une connexion au courtier de données. Par exemple, vous pouvez disposer d'une connexion VPN entre votre centre de données et votre fournisseur de cloud.

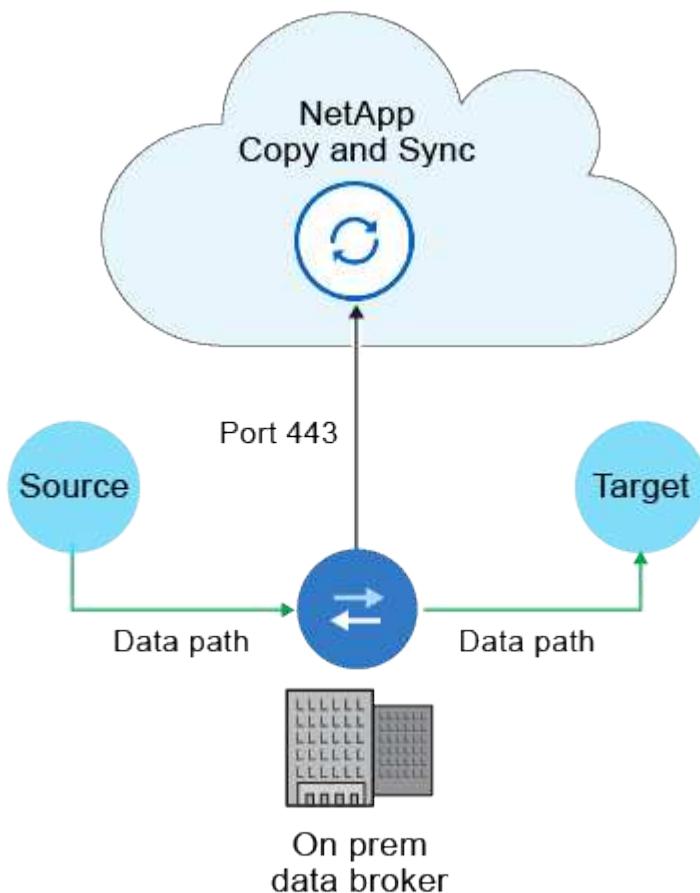


Lorsque Copy and Sync déploie le courtier de données dans AWS, Azure ou Google Cloud, il crée un groupe de sécurité qui active la communication sortante requise.



Courtier de données dans vos locaux

L'image suivante montre le courtier de données exécuté sur site dans un centre de données. Encore une fois, la source et la cible peuvent être situées à n'importe quel endroit, à condition qu'il existe une connexion au courtier de données.



Exigences de 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 centre de données et qu'un courtier de données se trouve dans AWS, vous avez besoin d'une connexion réseau (VPN ou Direct Connect) de votre réseau au VPC.

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

Points de terminaison réseau

Le courtier de données NetApp nécessite un accès Internet sortant via le port 443 pour communiquer avec Copy and Sync et pour contacter quelques autres services et référentiels. 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 points de terminaison suivante lors de la configuration de votre pare-feu pour le trafic sortant.

Points de terminaison du courtier en données

Un courtier en données contacte les points de terminaison suivants :

Points de terminaison	But
\ https://olcentgbl.trafficmanager.net	Pour contacter un référentiel pour mettre à jour les packages CentOS pour l'hôte du courtier de données. Ce point de terminaison est contacté uniquement 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 les référentiels pour la mise à jour de Node.js, npm et d'autres packages tiers utilisés dans le développement.
\ https://tgz.pm2.io	Pour accéder à un référentiel pour la mise à jour de PM2, qui est un package tiers utilisé pour surveiller la copie et la synchronisation.
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	Pour contacter les services AWS que Copy and Sync utilise pour les opérations (mise en file d'attente des fichiers, enregistrement des actions et livraison des mises à jour au courtier de données).
\ https://s3.region.amazonaws.com Par exemple : s3.us-east-2.amazonaws.com:443 https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region ["Consultez la documentation AWS pour obtenir la liste des points de terminaison S3."^]	Pour contacter Amazon S3 lorsqu'une relation de synchronisation inclut un compartiment S3.
\ https://s3.amazonaws.com/	Lorsque vous téléchargez les journaux du courtier de données à partir de Copy and Sync, le courtier de données compressé son répertoire de journaux et télécharge les journaux dans un compartiment S3 prédéfini dans la région us-east-1.
\ https://storage.googleapis.com/	Pour contacter Google Cloud lorsqu'une relation de synchronisation utilise un bucket GCP.
 https://storage-account.blob.core.windows.nethttps://storage-account.dfs.core.windows.net [] Où storage-account est le compte de stockage source de l'utilisateur.	Pour ouvrir le proxy vers l'adresse du compte de stockage Azure d'un utilisateur.
\ https://cf.cloudsync.netapp.com \ https://repo.cloudsync.netapp.com	Pour contacter Copy and Sync.
\ https://support.netapp.com	Pour contacter le support NetApp lors de l'utilisation d'une licence BYOL pour les relations de synchronisation.

Points de terminaison	But
\ 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 \ https://sts.us-east-1.amazonaws.com	Pour vérifier les informations d'identification AWS lorsque le courtier de données est déployé dans AWS ou lorsqu'il est déployé dans vos locaux et que les informations d'identification AWS sont fournies. Le courtier de données contacte ce point de terminaison pendant le déploiement, lorsqu'il est mis à jour et lorsqu'il est redémarré.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com	Pour contacter NetApp Data Classification lorsque vous utilisez la classification pour sélectionner les fichiers sources pour une nouvelle relation de synchronisation.
\ https://pubsub.googleapis.com	Si vous créez une relation de synchronisation continue à partir d'un compte de stockage Google.
<p>https://storage-account.queue.core.windows.net</p> <p>class="bare">>https://storage-account.queue.core.windows.net \ https://management.azure.com/subscriptions/</p> <p>class="bare">>https://management.azure.com/subscriptions/</p> <p> \${subscriptionId} /resourceGroups/\${resourceGroup} /providers/Microsoft.EventGrid/*</p> <p>Où storage-account est le compte de stockage source de l'utilisateur, subscriptionId est l'ID d'un abonnement source et resourceGroup est le groupe de ressources source.</p>	Si vous créez une relation de synchronisation continue à partir d'un compte de stockage Azure.

Points de terminaison du navigateur Web

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

logs.cloudsync.netapp.com:443

Connectez-vous à NetApp Copy and Sync

Utilisez la NetApp Console pour vous connecter à NetApp Copy and Sync.

Pour vous connecter à la console, vous pouvez utiliser vos informations d'identification du site de support NetApp ou vous inscrire pour une connexion au cloud NetApp à l'aide de votre e-mail et d'un mot de passe. ["En savoir plus sur la connexion"](#) .

NetApp Copy and Sync utilise la gestion des accès aux identités pour régir l'accès de chaque utilisateur à des actions spécifiques.

Rôle de NetApp Console requis Rôle d'administrateur d'organisation. ["En savoir plus sur les rôles d'accès à la NetApp Console"](#) .

Étapes

1. Ouvrez un navigateur Web et accédez à la ["NetApp Console"](#) .

La page de connexion à la NetApp Console s'affiche.

2. Connectez-vous à la console.
3. Dans la navigation de gauche de la console, sélectionnez **Mobilité > Copier et synchroniser**.

Installer un courtier de données

Créer un nouveau courtier de données dans AWS pour NetApp Copy and Sync

Lorsque vous créez un nouveau groupe de courtiers de données pour NetApp Copy and Sync, choisissez Amazon Web Services pour déployer le logiciel de courtier de données sur une nouvelle instance EC2 dans un VPC. NetApp Copy and 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 préparer l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou dans vos locaux. ["Apprendre encore 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 courtage de données s'exécute automatiquement en tant que root sur l'hôte Linux. L'exécution en tant que root est une exigence pour les opérations de courtier en données. Par exemple, pour monter des actions.

Exigences de mise en réseau

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger Copy and Sync pour les tâches sur le port 443.

Lorsque Copy and 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 utiliser un serveur proxy pendant le processus d'installation.

Si vous devez limiter la connectivité sortante, consultez ["la liste des points de terminaison contactés par le courtier de données"](#) .

- NetApp recommande de configurer la source, la cible et le courtier de données pour utiliser 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 "[cette politique fournie par NetApp](#)".

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

Lorsque Copy and Sync déploie le courtier de données, il crée un rôle IAM pour l'instance du courtier de données. Vous pouvez déployer le courtier de données à l'aide de votre propre rôle IAM, si vous préférez. Vous pouvez utiliser cette option si votre organisation dispose de politiques 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 approuvée.
- "[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.

Créer le courtier de données

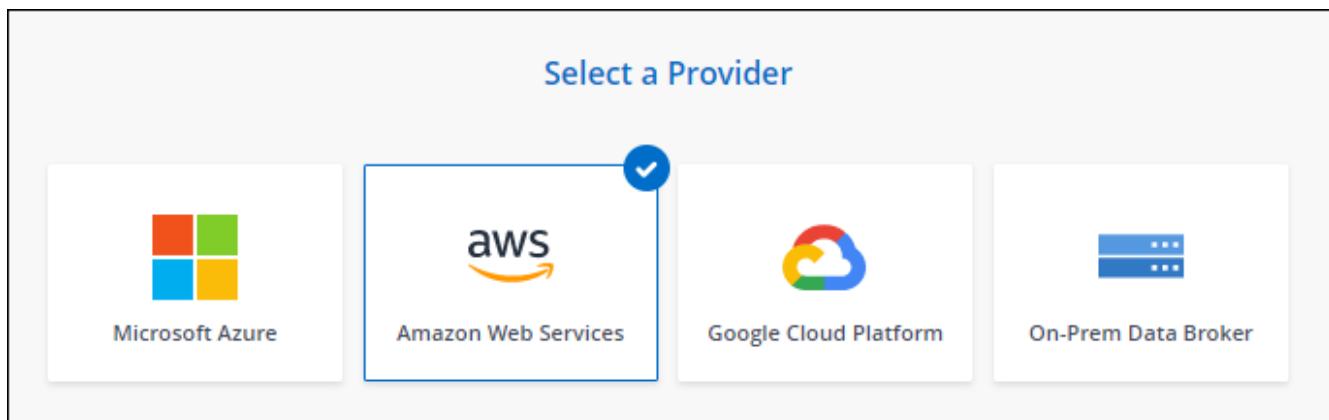
Il existe plusieurs façons de créer un nouveau courtier de données. Ces étapes décrivent comment installer un courtier de données dans AWS lors de la création d'une relation de synchronisation.

Étapes

1. "[Connectez-vous pour copier et synchroniser](#)".
2. Sélectionnez **Créer une nouvelle synchronisation**.
3. Sur la page **Définir la relation de synchronisation**, choisissez une source et une cible et sélectionnez **Continuer**.

Suivez les étapes jusqu'à atteindre la page **Data Broker Group**.

4. Sur la page **Groupe de courtiers de données**, sélectionnez **Créer un courtier de données**, puis sélectionnez **Amazon Web Services**.



5. Saisissez un nom pour le courtier de données et sélectionnez **Continuer**.
6. Saisissez une clé d'accès AWS afin que Copy and Sync puisse créer le courtier de données dans AWS en votre nom.

Les clés ne sont pas enregistrées ni utilisées à d'autres fins.

Si vous préférez ne pas fournir de clés d'accès, sélectionnez le lien en bas de la page pour utiliser un modèle CloudFormation à la place. Lorsque vous utilisez cette option, vous n'avez pas besoin de fournir d'informations d'identification car vous vous connectez directement à AWS.

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

[Lancer un courtier de données à partir d'un modèle AWS CloudFormation](#)

7. 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 et sélectionnez un rôle IAM existant, ou laissez le champ vide pour que Copy and Sync crée le rôle pour vous. Vous avez également la possibilité de crypter votre courtier de données à l'aide d'une clé KMS.

Si vous choisissez votre propre rôle IAM, [vous devrez fournir les autorisations requises](#).

Basic Settings

Location	Connectivity
VPC	Key Pair
Select VPC	Select Key Pair
Subnet	Enable Public IP?
Select Subnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IAM Role (optional)	
IAM Role (optional) ?	
KMS Key for EBS volume (optional)	
Select KMS Key for EBS Encryption	

8. Spécifiez une configuration de proxy, si un proxy est requis pour l'accès Internet dans le VPC.
9. Une fois le courtier de données disponible, sélectionnez **Continuer** dans Copier et synchroniser.

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

1 Data Broker Group

ben-data-broker

1 Data Brokers | N/A Transfer Rate | 0 Relationships | 1 Active Data Brokers Status

10. 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 groupe de courtiers de données avec des relations de synchronisation supplémentaires.

Détails sur l'instance du courtier de données

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

Compatibilité Node.js

v21.2.0

Type d'instance

m5n.xlarge lorsqu'il est disponible dans la région, sinon m5.xlarge

vCPU

4

BÉLIER

16 GB

Système opérateur

Amazon Linux 2023

Taille et type de disque

SSD GP2 de 10 Go

Créer un nouveau courtier de données dans Azure pour NetApp Copy and Sync

Lorsque vous créez un nouveau groupe de courtiers de données pour NetApp Copy and Sync, choisissez Microsoft Azure pour déployer le logiciel de courtier de données sur une nouvelle machine virtuelle dans un réseau virtuel. NetApp Copy and 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 préparer l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou dans vos locaux. ["Apprendre encore plus"](#) .

Régions Azure prises en charge

Toutes les régions sont prises en charge, à l'exception des régions Chine, Gouvernement américain et Département de la Défense américain.

Privilèges root

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

Exigences de mise en réseau

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service de copie et de synchronisation pour les tâches via le port 443.

Lorsque Copy and 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, consultez "[la liste des points de terminaison contactés par le courtier de données](#)".

- NetApp recommande de configurer la source, la cible et le courtier de données pour utiliser 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 Azure

Assurez-vous que le compte d'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"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements
```

```
ts/write"

"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/read",
```

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

Note:

1. Les autorisations suivantes ne sont requises que si vous prévoyez d'activer le ["Paramètre de synchronisation continue"](#) sur une relation de synchronisation d'Azure vers un autre emplacement de stockage cloud :

- 'Microsoft.Storage/storageAccounts/lecture',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/lecture',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/supprimer',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action',
- 'Microsoft.EventGrid/systemTopics/lecture',
- 'Microsoft.EventGrid/systemTopics/write',
- 'Microsoft.EventGrid/systemTopics/supprimer',
- 'Microsoft.EventGrid/eventSubscriptions/write',
- 'Microsoft.Storage/storageAccounts/write'

De plus, l'étendue attribuable doit être définie sur l'étendue de l'abonnement et **non** sur l'étendue du groupe de ressources si vous prévoyez d'implémenter la synchronisation continue dans Azure.

2. Les autorisations suivantes ne sont requises que si vous prévoyez de choisir votre propre sécurité pour la création d'un courtier de données :

- « Microsoft.Network/networkSecurityGroups/securityRules/lecture »
- « Microsoft.Network/networkSecurityGroups/lecture »

Méthode d'authentification

Lorsque vous déployez le courtier de données, vous devez choisir une méthode d'authentification pour la machine virtuelle : un mot de passe ou une paire de clés publique-privée SSH.

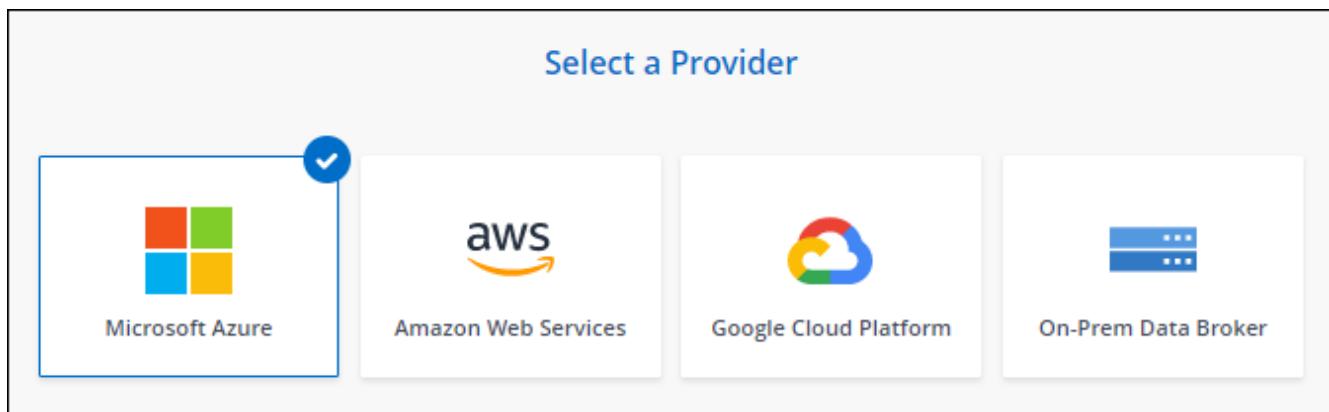
Pour obtenir de l'aide sur la création d'une paire de clés, reportez-vous à ["Documentation Azure : Créer et utiliser une paire de clés publique-privée SSH pour les machines virtuelles Linux dans Azure"](#) .

Créer le courtier de données

Il existe plusieurs façons de créer un nouveau courtier de données. Ces étapes décrivent comment installer un courtier de données dans Azure lorsque vous créez une relation de synchronisation.

Étapes

1. "Connectez-vous pour copier et synchroniser" .
 2. Sélectionnez **Créer une nouvelle synchronisation**.
 3. Sur la page **Définir la relation de synchronisation**, choisissez une source et une cible et sélectionnez **Continuer**.
- Suivez les étapes jusqu'à atteindre la page **Data Broker Group**.
4. Sur la page **Groupe de courtiers de données**, sélectionnez **Créer un courtier de données**, puis sélectionnez **Microsoft Azure**.



5. Saisissez un nom pour le courtier de données et sélectionnez **Continuer**.
6. Si vous y êtes invité, connectez-vous à votre compte Microsoft. Si vous n'y êtes pas invité, sélectionnez **Se connecter à Azure**.

Le formulaire est détenu et hébergé par Microsoft. Vos informations d'identification ne sont pas fournies à NetApp.

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

Location	Connectivity
Subscription	VM Name
Select a subscription	netappdatabroker
Azure Region	User Name
Select a region	databroker
VNet	Authentication Method:
Select a VNet	<input checked="" type="radio"/> Password <input type="radio"/> Public Key
Subnet	Enter Password
Select a subnet	<input type="password"/>
Public IP	Resource Group:
Enable	<input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group
Data Broker Role	Security group:
<input type="checkbox"/> Create Custom Role	<input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group
<p>Notice: Only relevant for continuous sync relationships from Azure. Users can also manually create this later.</p>	



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 fait manuellement après la création du courtier.

8. Spécifiez une configuration de proxy, si un proxy est requis pour l'accès Internet dans le réseau virtuel.
9. Sélectionnez **Continuer**. Si vous souhaitez ajouter des autorisations S3 à votre courtier de données, saisissez vos clés d'accès et secrètes AWS.
10. Sélectionnez **Continuer** et gardez la page ouverte jusqu'à ce que le déploiement soit terminé.

Le processus peut prendre jusqu'à 7 minutes.

11. Dans Copier et synchroniser, sélectionnez **Continuer** une fois que le courtier de données est disponible.
12. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Résultat

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

Vous recevez un message indiquant que vous avez besoin du consentement de l'administrateur ?

Si Microsoft vous informe que l'approbation de l'administrateur est requise parce que Copy and Sync a besoin d'une autorisation pour accéder aux ressources de votre organisation en votre nom, vous avez alors deux options :

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

Dans Azure, accédez à **Centres d'administration > Azure AD > Utilisateurs et groupes > Paramètres utilisateur** et activez **Les utilisateurs peuvent consentir à ce que les applications accèdent aux données de l'entreprise en leur nom**.

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

\ <https://login.microsoftonline.com/> {REmplissez ICI VOTRE ID DE LOCATAIRE}/v2.0/adminconsent?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, l'URL de notre 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

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

Compatibilité Node.js

v21.2.0

Type de VM

Norme DS4 v2

vCPU

8

BÉLIER

28 GB

Système opérateur

Rocky Linux 9,0

Taille et type de disque

SSD Premium de 64 Go

Créer un nouveau courtier de données dans Google Cloud pour NetApp Copy and Sync

Lorsque vous créez un nouveau groupe de courtiers de données pour NetApp Copy and

Sync, choisissez Google Cloud Platform pour déployer le logiciel de courtier de données sur une nouvelle instance de machine virtuelle dans un VPC Google Cloud. NetApp Copy and 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 préparer l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou dans vos locaux. ["Apprendre encore plus"](#) .

Régions Google Cloud prises en charge

Toutes les régions sont prises en charge.

Privilèges root

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

Exigences de mise en réseau

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger Copy and Sync pour les tâches sur le port 443.

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

Si vous devez limiter la connectivité sortante, consultez ["la liste des points de terminaison contactés par le courtier de données"](#) .

- NetApp recommande de configurer la source, la cible et le courtier de données pour utiliser 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 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
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

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 HashiCorp externe.
2. Les autorisations « pubsub.* » et « storage.buckets.update » ne sont requises que si vous prévoyez d'activer le paramètre Synchronisation continue sur une relation de synchronisation de Google Cloud Storage vers un autre emplacement de stockage cloud. ["En savoir plus sur l'option de synchronisation continue"](#) .
3. Les autorisations « cloudkms.cryptoKeys.list » et « cloudkms.keyRings.list » ne sont requises que si vous prévoyez d'utiliser une clé KMS gérée par le client sur un bucket Google Cloud Storage cible.

Créer le courtier de données

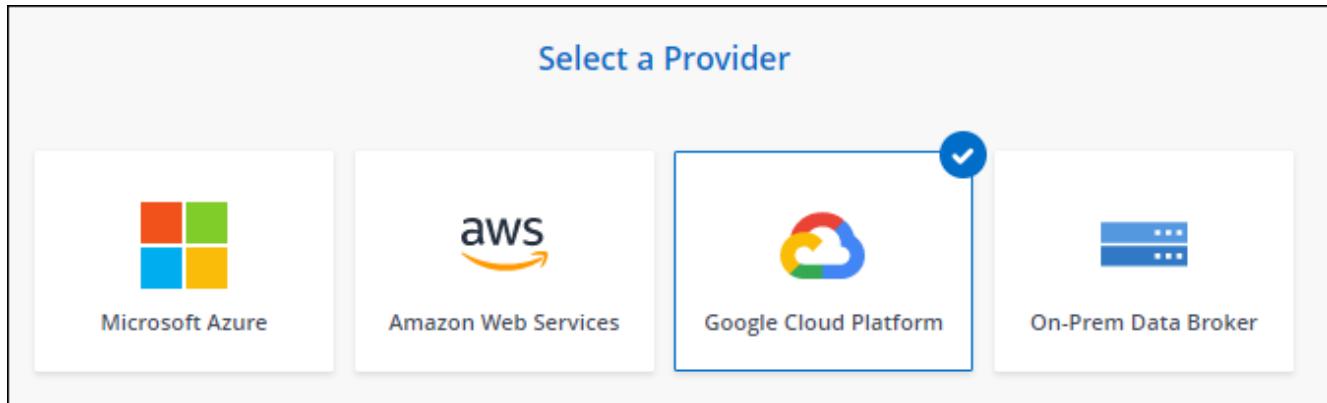
Il existe plusieurs façons de créer un nouveau courtier de données. Ces étapes décrivent comment installer un courtier de données dans Google Cloud lorsque vous créez une relation de synchronisation.

Étapes

1. ["Connectez-vous pour copier et synchroniser"](#) .
2. Sélectionnez **Créer une nouvelle synchronisation**.
3. Sur la page **Définir la relation de synchronisation**, choisissez une source et une cible et sélectionnez **Continuer**.

Suivez les étapes jusqu'à atteindre la page **Data Broker Group**.

4. Sur la page **Groupe de courtiers de données**, sélectionnez **Créer un courtier de données**, puis sélectionnez **Google Cloud Platform**.



5. Saisissez un nom pour le courtier de données et sélectionnez **Continuer**.
6. Si vous y êtes invité, connectez-vous avec votre compte Google.

Le formulaire appartient et est hébergé par Google. Vos informations d'identification ne sont pas fournies à NetApp.

7. Sélectionnez un projet et un compte de service, puis choisissez un emplacement pour le courtier de données, en indiquant notamment si vous souhaitez activer ou désactiver une adresse IP publique.

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

Basic Settings

<p>Project</p> <p>Project</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">OCCM-Dev</div>	<p>Location</p> <p>Region</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">us-west1</div>
<p>Service Account</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">test</div>	<p>Zone</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">us-west1-a</div>
<p>Select a Service Account that includes these permissions</p>	
<p>VPC</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">default</div>	
<p>Subnet</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">default</div>	
<p>Public IP</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">Enable</div>	

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

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

9. Une fois le courtier de données disponible, sélectionnez **Continuer** dans Copier et synchroniser.

Le déploiement de l'instance prend environ 5 à 10 minutes. Vous pouvez surveiller la progression à partir de Copier et Sync, qui s'actualise automatiquement lorsque l'instance est disponible.

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

Résultat

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

Accorder des autorisations pour utiliser des buckets dans d'autres projets Google Cloud

Lorsque vous créez une relation de synchronisation et choisissez Google Cloud Storage comme source ou cible, Copier et synchroniser vous permet de choisir parmi les compartiments que le compte de service du courtier de données est autorisé à utiliser. Par défaut, cela inclut les buckets qui se trouvent dans le *même* projet que le compte de service du courtier de données. Mais vous pouvez choisir des buckets à partir d'*autres* projets si vous fournissez les autorisations requises.

Étapes

1. Ouvrez la console Google Cloud Platform et chargez le service Cloud Storage.
2. Sélectionnez le nom du bucket que vous souhaitez utiliser comme source ou cible dans une relation de synchronisation.
3. Sélectionnez **Autorisations**.
4. Sélectionnez **Ajouter**.
5. Saisissez le nom du compte de service du courtier en données.
6. Sélectionnez un rôle qui fournit les mêmes autorisations que celles indiquées ci-dessus .
7. Sélectionnez **Enregistrer**.

Résultat

Lorsque vous configurez une relation de synchronisation, vous pouvez désormais choisir ce bucket comme source ou cible dans la relation de synchronisation.

Détails sur l'instance de machine virtuelle du courtier de données

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

Compatibilité Node.js

v21.2.0

Type de machine

n2-standard-4

vCPU

4

BÉLIER

15 Go

Système opérateur

Rocky Linux 9,0

Taille et type de disque

Disque dur 20 Go PD-standard

Installer le courtier de données sur un hôte Linux pour NetApp Copy and Sync

Lorsque vous créez un nouveau groupe de courtiers de données pour NetApp Copy and Sync, choisissez l'option Broker de données sur site pour installer le logiciel de courtier de données sur un hôte Linux local ou sur un hôte Linux existant dans le cloud. NetApp Copy and 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 préparer l'installation.

Configuration requise pour l'hôte Linux

- **Compatibilité Node.js** : v21.2.0
- **Système opérateur**:

- CentOS 8.0 et 8.5
CentOS Stream n'est pas pris en charge.
- Red Hat Enterprise Linux 8.5, 8.8, 8.9 et 9.4
- Rocky Linux 9
- Ubuntu Server 20.04 LTS, 23.04 LTS et 24.04 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 auprès de 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 lors de l'installation.

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

SELinux applique une politique qui bloque les mises à jour du logiciel du courtier de données et peut empêcher le courtier de données de contacter les points de terminaison requis pour un fonctionnement normal.

Privilèges root

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

Exigences de mise en réseau

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

Activer l'accès à AWS

Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation qui inclut un bucket S3, vous devez préparer l'hôte Linux pour l'accès AWS. Lorsque vous installez le courtier de données, vous devez fournir des clés AWS pour un utilisateur AWS disposant d'un accès programmatique et d'autorisations spécifiques.

Étapes

1. Créer une politique IAM en utilisant "[cette politique fournie par NetApp](#)"

["Afficher les instructions AWS"](#)

2. Créez un utilisateur IAM disposant d'un accès programmatique.

["Afficher les instructions AWS"](#)

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

Activer l'accès à Google Cloud

Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation qui inclut un bucket Google Cloud Storage, vous devez préparer l'hôte Linux pour l'accès à 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 doté d'autorisations d'administrateur de stockage, si vous n'en avez pas déjà un.
2. Créez une clé de compte de service enregistrée au format JSON.

["Afficher les instructions de 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.

Activer 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 des relations.

Installer le courtier de données

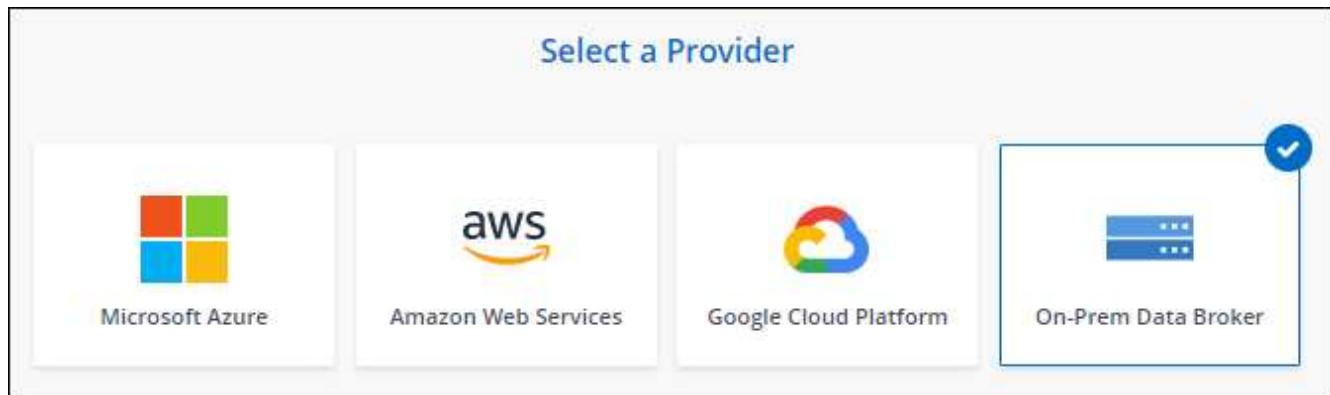
Vous pouvez installer un courtier de données sur un hôte Linux lorsque vous créez une relation de synchronisation.

Étapes

1. ["Connectez-vous pour copier et synchroniser"](#) .
2. Sélectionnez **Créer une nouvelle synchronisation**.
3. Sur la page **Définir la relation de synchronisation**, choisissez une source et une cible et sélectionnez **Continuer**.

Suivez les étapes jusqu'à atteindre la page **Data Broker Group**.

4. Sur la page **Groupe de courtiers de données**, sélectionnez **Créer un courtier de données**, puis sélectionnez **Courtier de données sur site**.



Même si l'option est intitulée **On-Prem Data Broker**, elle s'applique à un hôte Linux sur vos locaux ou dans le cloud.

5. Saisissez un nom pour le courtier de données et sélectionnez **Continuer**.

La page d'instructions se charge sous peu. Vous devrez suivre ces instructions : elles incluent un lien unique pour télécharger le programme d'installation.

6. Sur la page d'instructions :

- Sélectionnez si vous souhaitez activer l'accès à **AWS**, **Google Cloud** ou les deux.
- Sélectionnez une option d'installation : **Pas de proxy**, **Utiliser un serveur proxy** ou **Utiliser un serveur proxy avec authentification**.



L'utilisateur doit être un utilisateur local. Les utilisateurs de domaine ne sont pas pris en charge.

- 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.

- Téléchargez le programme d'installation :

- **Pas de proxy** :

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

- **Utiliser un serveur proxy** :

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

- **Utiliser un serveur proxy avec authentification** :

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

URI

Copy and Sync affiche l'URI du fichier d'installation sur la page d'instructions, qui se charge lorsque vous suivez les invites pour déployer le Data Broker sur site. Cet URI n'est pas répété ici car le lien est généré dynamiquement et ne peut être utilisé qu'une seule fois. [Suivez ces étapes pour obtenir l'URI à partir de Copy and Sync](#).

e. Passez en superutilisateur, rendez l'installateur exécutable et installez le logiciel :



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

- Aucune configuration de 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 du 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

Voici les clés pour l'utilisateur que vous devez avoir préparées [en suivant ces étapes](#). Les clés AWS sont stockées sur le courtier de données, qui s'exécute sur votre réseau local ou cloud. NetApp n'utilise pas les clés en dehors du courtier de données.

fichier JSON

Il s'agit du fichier JSON qui contient une clé de compte de service que vous devez avoir préparée [en suivant ces étapes](#).

7. Une fois le courtier de données disponible, sélectionnez **Continuer** dans Copier et synchroniser.

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

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.