



Documentation Cloud Sync

Cloud Sync

NetApp

November 17, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-sync/index.html> on November 17, 2022. Always check docs.netapp.com for the latest.

Table des matières

Documentation Cloud Sync	1
Notes de mise à jour	2
Quelles sont les nouveautés de Cloud Sync	2
Limites	17
Commencez	19
Présentation de Cloud Sync	19
Démarrage rapide de Cloud Sync	21
Relations de synchronisation prises en charge	22
Préparer la source et la cible	30
Présentation de la mise en réseau pour Cloud Sync	37
Installer un courtier de données	40
Utiliser Cloud Sync	57
Synchronisation des données entre une source et une cible	57
Payer pour la synchronisation après la fin de votre essai gratuit	75
Gestion des relations de synchronisation	78
Gérez les groupes de courtiers de données	84
Création et affichage de rapports pour ajuster votre configuration	92
Désinstallation du courtier de données	95
API Cloud Sync	97
Pour commencer	97
Référence API	98
Utilisation d'API de liste	98
Concepts	101
Présentation des licences	101
Confidentialité des données	102
FAQ technique sur Cloud Sync	102
Connaissances et support	110
S'inscrire pour obtenir de l'aide	110
Obtenez de l'aide	114
Mentions légales	118
Droits d'auteur	118
Marques déposées	118
Brevets	118
Politique de confidentialité	118
Source ouverte	118

Documentation Cloud Sync

Notes de mise à jour

Quelles sont les nouveautés de Cloud Sync

Découvrez les nouveautés de Cloud Sync.

30 octobre 2022

Synchronisation continue de Microsoft Azure

Le paramètre Continuous Sync est désormais pris en charge depuis un compartiment de stockage Azure source vers un stockage cloud via un courtier de données Azure.

Après la synchronisation initiale des données, Cloud Sync écoute les modifications apportées au compartiment de stockage Azure source et synchronise en continu les modifications apportées à la cible lorsqu'elles se produisent. Ce paramètre est disponible lors de la synchronisation à partir d'un compartiment de stockage Azure vers le stockage Azure Blob, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS et StorageGRID.

Le courtier de données Azure a besoin d'un rôle personnalisé et des autorisations suivantes pour utiliser ce paramètre :

```
'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'
```

["En savoir plus sur le paramètre de synchronisation continue".](#)

4 septembre 2022

Assistance Google Drive supplémentaire

- Cloud Sync prend désormais en charge des relations de synchronisation supplémentaires pour Google Drive :
 - Google Drive vers les serveurs NFS
 - Google Drive vers les serveurs SMB
- Vous pouvez également générer des rapports pour les relations de synchronisation incluant Google Drive.

["En savoir plus sur les rapports"](#).

Amélioration de la synchronisation continue

Vous pouvez maintenant activer le paramètre de synchronisation continue sur les types de relations de synchronisation suivants :

- Un compartiment S3 vers un serveur NFS
- Google Cloud Storage sur un serveur NFS

["En savoir plus sur le paramètre de synchronisation continue"](#).

Notifications par e-mail

Vous pouvez désormais recevoir des notifications Cloud Sync par e-mail.

Pour recevoir les notifications par e-mail, vous devez activer le paramètre **Notifications** sur la relation de synchronisation, puis configurer les paramètres alertes et notification dans BlueXP.

["Apprenez à configurer les notifications"](#).

31 juillet 2022

Google Drive

Vous pouvez désormais synchroniser les données d'un serveur NFS ou SMB vers Google Drive. « Mon lecteur » et « lecteurs partagés » sont pris en charge en tant que cibles.

Avant de créer une relation de synchronisation incluant Google Drive, vous devez configurer un compte de service disposant des autorisations requises et d'une clé privée. ["En savoir plus sur les exigences de Google Drive"](#).

["Affichez la liste des relations de synchronisation prises en charge"](#).

Prise en charge supplémentaire d'Azure Data Lake

Cloud Sync prend désormais en charge des relations de synchronisation supplémentaires pour Azure Data Lake Storage Gen2 :

- Amazon S3 vers Azure Data Lake Storage Gen2
- Stockage objet cloud IBM sur Azure Data Lake Storage Gen2
- De StorageGRID à Azure Data Lake Storage Gen2

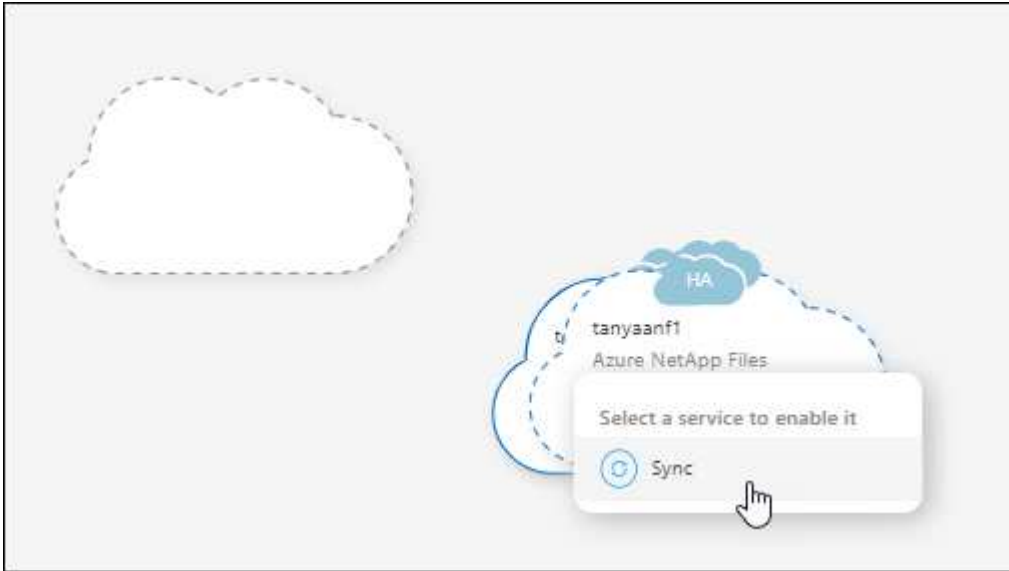
["Affichez la liste des relations de synchronisation prises en charge"](#).

Nouvelles façons de configurer les relations de synchronisation

Nous avons ajouté des moyens supplémentaires pour configurer les relations de synchronisation directement à partir de BlueXP Canvas.

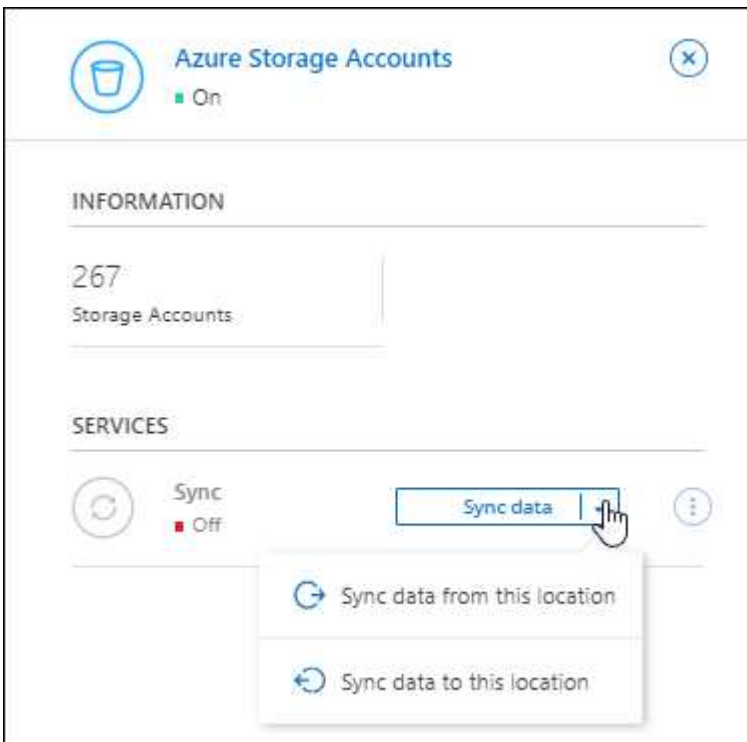
Glisser-déposer

Vous pouvez maintenant configurer une relation de synchronisation à partir du Canvas en faisant glisser et en déposant un environnement de travail sur un autre.



Configuration du panneau droit

Vous pouvez maintenant configurer une relation de synchronisation pour le stockage Azure Blob ou pour Google Cloud Storage en sélectionnant l'environnement de travail dans Canvas, puis en sélectionnant l'option de synchronisation dans le panneau de droite.



3 juillet 2022

Prise en charge d’Azure Data Lake Storage Gen2

Vous pouvez désormais synchroniser les données d’un serveur NFS ou SMB vers 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).

["Affichez la liste des relations de synchronisation prises en charge"](#).

Synchronisation continue depuis Google Cloud Storage

Le paramètre Continuous Sync est désormais pris en charge à partir d’un compartiment Google Cloud Storage source vers une cible de stockage cloud.

Après la synchronisation initiale des données, Cloud Sync écoute les modifications apportées au compartiment Google Cloud Storage source et synchronise en continu les modifications apportées à la cible au fur et à mesure de leur apparition. Ce paramètre est disponible lors de la synchronisation à partir d’un compartiment Google Cloud Storage vers S3, Google Cloud Storage, Azure Blob Storage, StorageGRID ou IBM Storage.

Le compte de service associé à votre courtier de données nécessite les autorisations suivantes pour utiliser ce paramètre :

```
- 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
```

["En savoir plus sur le paramètre de synchronisation continue"](#).

Prise en charge de la région Google Cloud

Le courtier en données Cloud Sync est désormais pris en charge dans les régions Google Cloud suivantes :

- Columbus (US-east5)
- Dallas (US-south1)
- Madrid (europe-Sud-Ouest 1)
- Milan (europe-Ouest 8)
- Paris (europe-Ouest 9)

Nouveau type de machine Google Cloud

Le type de machine par défaut pour le courtier en données dans Google Cloud est maintenant n2-standard-4.

6 juin 2022

Synchronisation continue

Un nouveau paramètre vous permet de synchroniser en continu les modifications d'un compartiment S3 source vers une cible.

Après la synchronisation initiale des données, Cloud Sync écoute les modifications apportées au compartiment S3 source et synchronise en continu les modifications apportées à la cible lorsqu'elles se produisent. Il n'est pas nécessaire d'effectuer une nouvelle analyse de la source à intervalles réguliers. Ce paramètre est disponible uniquement lors de la synchronisation à partir d'un compartiment S3 vers S3, Google Cloud Storage, Azure Blob Storage, StorageGRID ou IBM Storage.

Notez que le rôle IAM associé à votre courtier de données aura besoin des autorisations suivantes pour utiliser ce paramètre :

```
"s3:GetBucketNotification",  
"s3:PutBucketNotification"
```

Ces autorisations sont automatiquement ajoutées à tous les nouveaux courtiers de données que vous créez.

["En savoir plus sur le paramètre de synchronisation continue"](#).

Affiche tous les volumes ONTAP

Lorsque vous créez une relation de synchronisation, Cloud Sync affiche désormais tous les volumes d'un système Cloud Volumes ONTAP source, d'un cluster ONTAP sur site ou d'un système de fichiers FSX pour ONTAP.

Dans les versions antérieures, Cloud Sync affiche uniquement les volumes correspondant au protocole sélectionné. Tous les volumes s'affichent à présent, mais tous les volumes qui ne correspondent pas au protocole sélectionné ou qui n'ont pas de partage ou d'exportation sont grisés et ne peuvent pas être sélectionnés.

Copie de balises vers Azure Blob

Lorsque vous créez une relation de synchronisation où Azure Blob est la cible, Cloud Sync vous permet désormais de copier des balises dans le conteneur Azure Blob :

- Sur la page **Paramètres**, vous pouvez utiliser le paramètre **copie pour objets** pour copier des balises de la source vers le conteneur Azure Blob. Outre la copie des métadonnées.
- Sur la page **Tags/Metadata**, vous pouvez spécifier des balises d'index Blob à définir sur les objets copiés dans le conteneur Azure Blob. Auparavant, vous pouviez uniquement spécifier les métadonnées de relation.

Ces options sont prises en charge lorsque Azure Blob est la cible et que la source est Azure Blob ou un terminal compatible S3 (S3, StorageGRID ou stockage objet dans le cloud IBM).

1er mai 2022

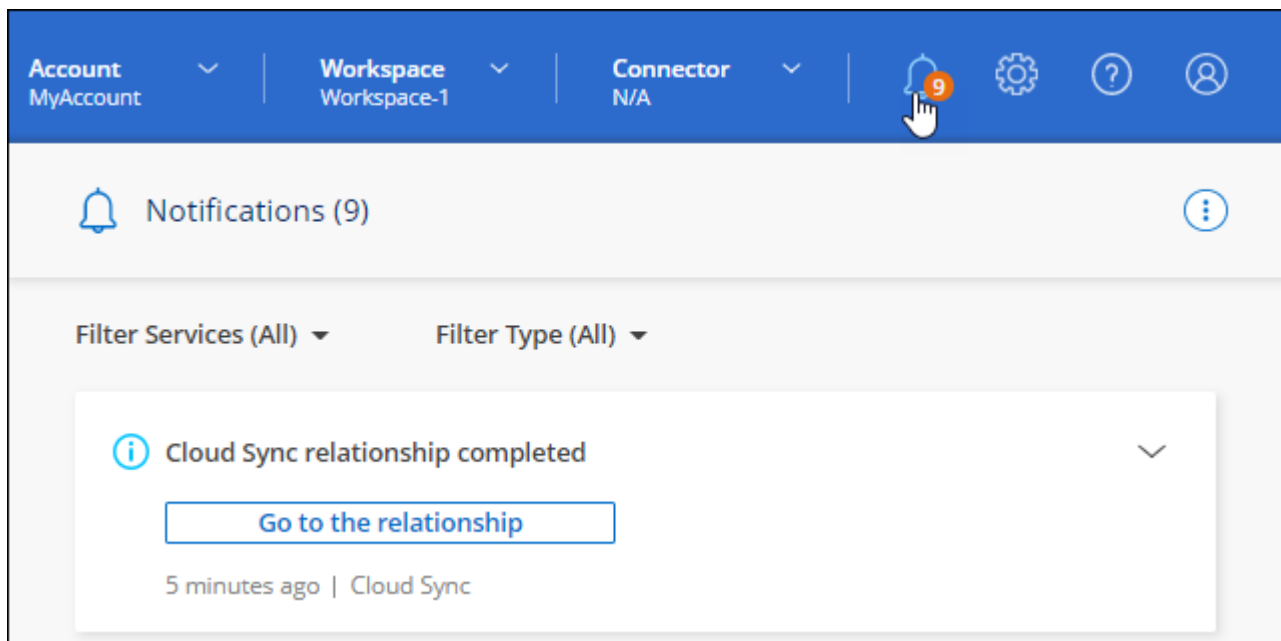
Délai d'expiration de la synchronisation

Un nouveau paramètre **délai de synchronisation** est maintenant disponible pour les relations de synchronisation. Ce paramètre vous permet de définir si Cloud Sync doit annuler une synchronisation de données si la synchronisation n'a pas été effectuée dans le nombre d'heures ou de jours spécifié.

["En savoir plus sur la modification des paramètres d'une relation de synchronisation"](#).

Notifications

Un nouveau paramètre **Notifications** est désormais disponible pour les relations de synchronisation. Ce paramètre vous permet de choisir de recevoir ou non des notifications Cloud Sync dans le Centre de notification de BlueXP. Vous pouvez activer des notifications pour la synchronisation des données avec succès, les échecs de synchronisation et les synchronisations de données annulées.



["En savoir plus sur la modification des paramètres d'une relation de synchronisation"](#).

3 avril 2022

Améliorations des groupes de courtiers de données

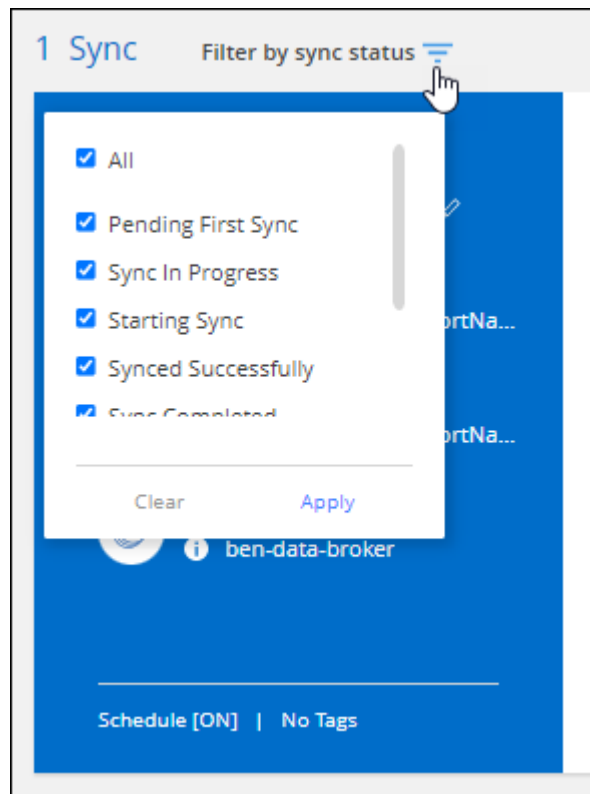
Nous avons apporté plusieurs améliorations aux groupes de courtiers de données :

- Vous pouvez maintenant déplacer un courtier de données vers un nouveau groupe ou un groupe existant.
- Vous pouvez maintenant mettre à jour la configuration du proxy pour un courtier de données.
- Enfin, vous pouvez également supprimer des groupes de courtiers de données.

["Découvrez comment gérer les groupes de courtiers de données"](#).

Filtre du tableau de bord

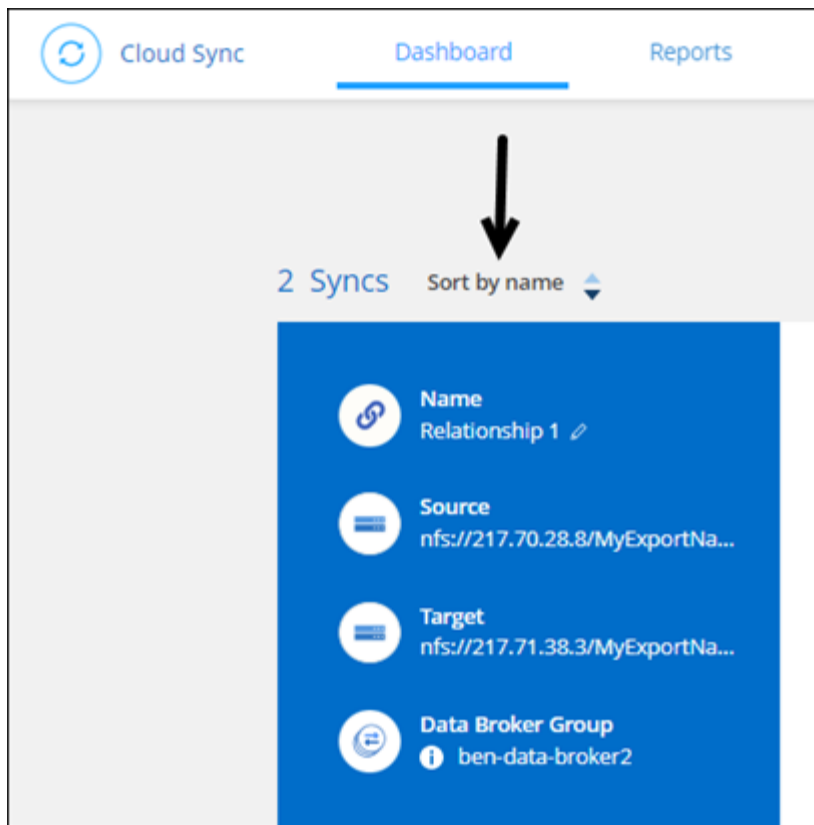
Vous pouvez désormais filtrer le contenu du tableau de bord de synchronisation afin de trouver plus facilement les relations de synchronisation qui correspondent à un certain état. Par exemple, vous pouvez filtrer les relations de synchronisation dont l'état a échoué



3 mars 2022

Tri dans le tableau de bord

Vous triez le tableau de bord par nom de relation de synchronisation.



Amélioration de l'intégration de Data Sense

Dans la version précédente, nous avons introduit l'intégration de Cloud Sync avec Cloud Data Sense. Dans cette mise à jour, nous avons amélioré l'intégration en facilitant la création de la relation de synchronisation. Une fois la synchronisation des données effectuée à partir du cloud Data SENSE, toutes les informations source le sont en une seule étape et vous devez saisir quelques informations clés.

The screenshot shows the 'Sync Relationship' configuration page with a progress bar indicating four steps: 1. Data Sense Integration (active), 2. Data Broker Group, 3. NFS Server, and 4. Directories. The main section is titled 'Selected Data Sense Source' and contains a table with the following information:

Azure NetApp Files	/cifs1 Source	1.1.1.1 Host	cifs Working Environment	\\1.1.1.1\\cifs1 Volume
--------------------	------------------	-----------------	-----------------------------	----------------------------

Below the table, the text 'A few more things before we continue' is displayed. Under the heading 'Define SMB Credentials:', there are three input fields:

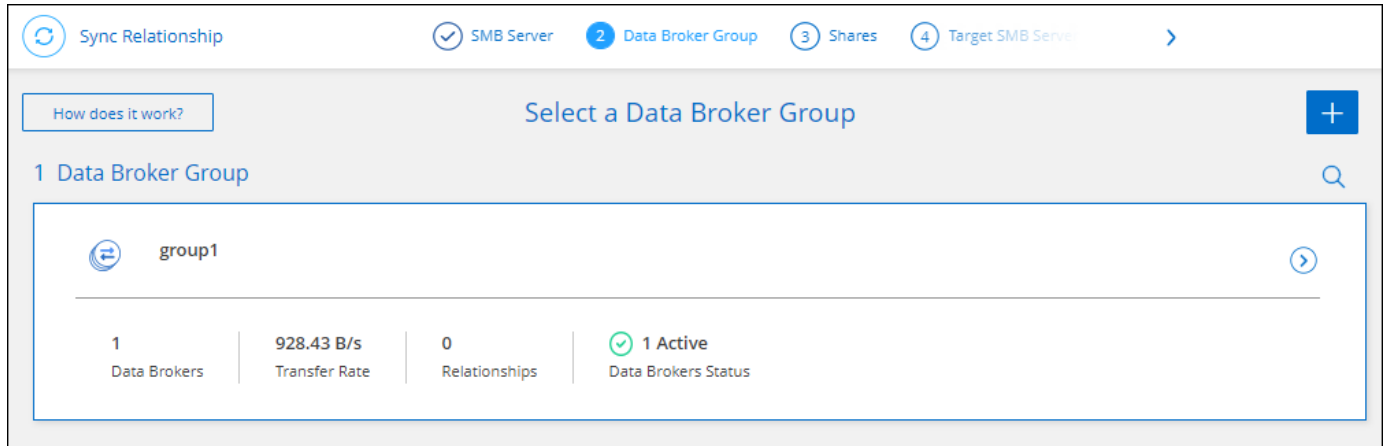
- User Name
- Password
- Domain (Optional)

6 février 2022

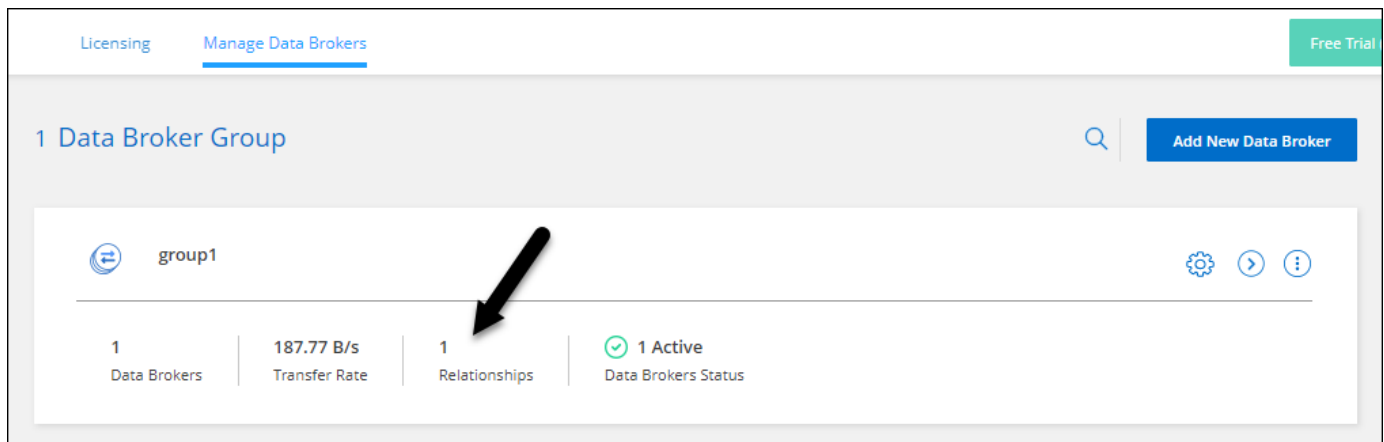
Amélioration des groupes de courtiers de données

Nous avons modifié votre manière d'interagir avec les courtiers de données en mettant l'accent sur le courtier de données *groups*.

Par exemple, lorsque vous créez une nouvelle relation de synchronisation, vous sélectionnez le courtier de données *group* à utiliser avec la relation, plutôt qu'un courtier de données spécifique.



Dans l'onglet **Manage Data Brokers**, nous avons également indiqué le nombre de relations de synchronisation gérées par un groupe de courtiers de données.



Télécharger les rapports au format PDF

Vous pouvez à présent télécharger un PDF d'un rapport.

["En savoir plus sur les rapports"](#).

2 janvier 2022

Nouvelles relations de synchronisation Box

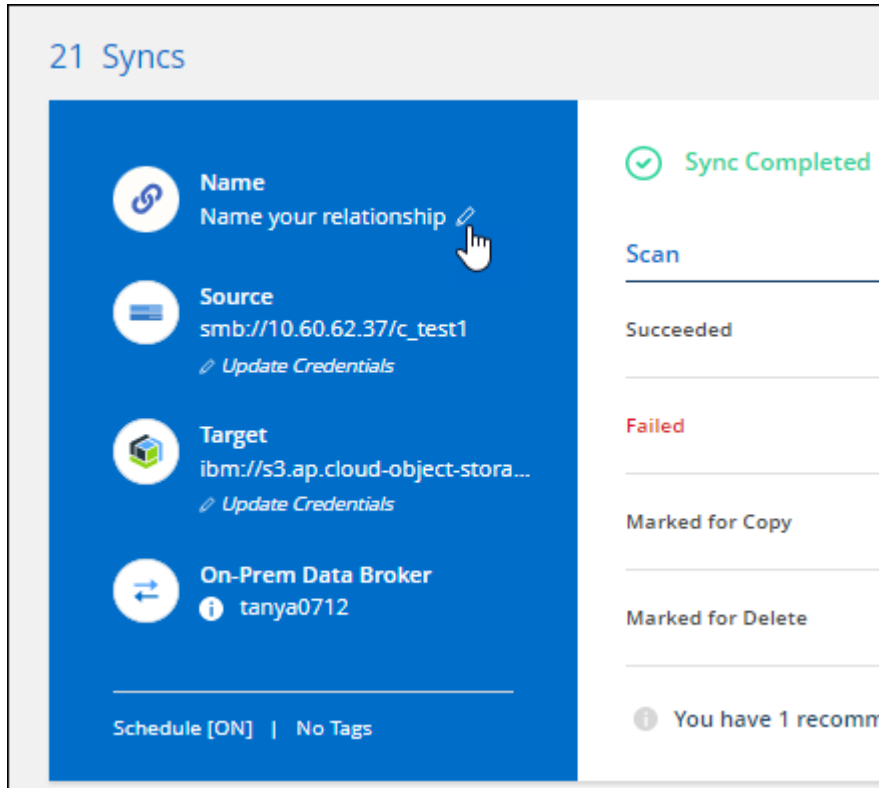
Deux nouvelles relations de synchronisation sont prises en charge :

- Box pour Azure NetApp Files
- Box vers Amazon FSX pour ONTAP

"Affichez la liste des relations de synchronisation prises en charge".

Noms des relations

Vous pouvez désormais donner un nom significatif à chacune de vos relations de synchronisation afin d'identifier plus facilement le but de chaque relation. Vous pouvez ajouter le nom lorsque vous créez la relation et à tout moment après.



Liens privés S3

Lorsque vous synchronisez les données vers ou depuis Amazon S3, vous pouvez utiliser une liaison privée S3. Lorsque le courtier copie les données de la source vers la cible, il passe par la liaison privée.

Notez que le rôle IAM associé à votre courtier de données aura besoin de l'autorisation suivante pour utiliser cette fonction :

```
"ec2:DescribeVpcEndpoints"
```

Cette autorisation est automatiquement ajoutée à tous les nouveaux courtiers de données que vous créez.

Récupération instantanée Glacier

Vous pouvez maintenant choisir la classe de stockage *Glacier Instant Retrieval* quand Amazon S3 est la cible d'une relation de synchronisation.

ACL du stockage objet aux partages SMB

Cloud Sync prend désormais en charge la copie de listes de contrôle d'accès depuis le stockage objet vers les partages SMB. Auparavant, nous prenions uniquement en charge la copie de listes de contrôle d'accès

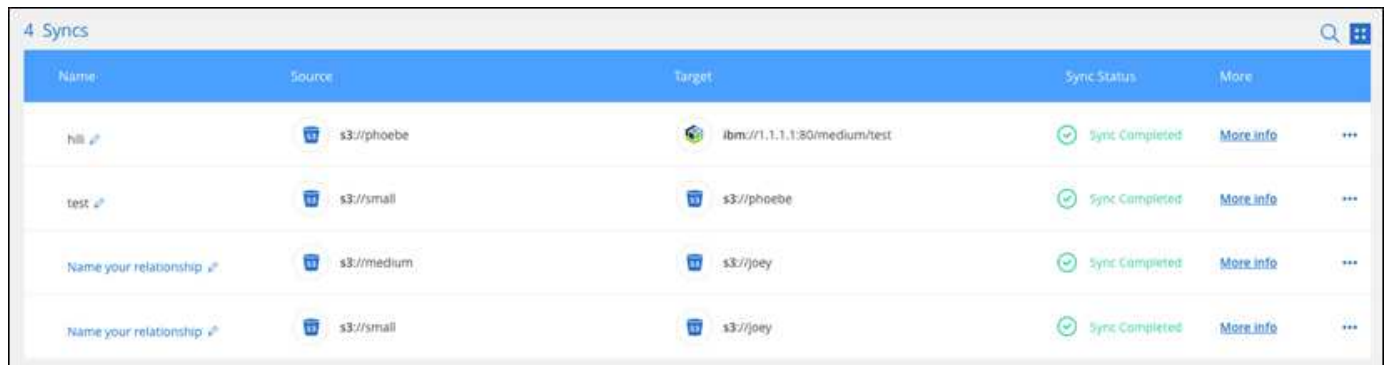
depuis un partage SMB vers le stockage objet.

SFTP à S3

La création d'une relation de synchronisation entre SFTP et Amazon S3 est désormais prise en charge dans l'interface utilisateur. Cette relation de synchronisation était auparavant prise en charge avec l'API uniquement.

Amélioration de la vue de tableau

Pour plus de facilité d'utilisation, nous avons repensé la vue des tableaux de bord. Si vous cliquez sur **plus d'info**, Cloud Sync filtre le tableau de bord pour afficher plus d'informations sur cette relation spécifique.



Name	Source	Target	Sync Status	More
hili	s3://phoebe	ibm://1.1.1.1:80/medium/test	Sync Completed	More info
test	s3://small	s3://phoebe	Sync Completed	More info
Name your relationship	s3://medium	s3://joey	Sync Completed	More info
Name your relationship	s3://small	s3://joey	Sync Completed	More info

Soutien pour la région de Jarkarta

Cloud Sync prend désormais en charge le déploiement de l'courtier en données dans la région AWS Asie-Pacifique (Jakarta).

28 novembre 2021

ACL du protocole SMB au stockage objet

Cloud Sync peut désormais copier les listes de contrôle d'accès (ACL) lors de la configuration d'une relation de synchronisation à partir d'un partage SMB source vers le stockage objet (à l'exception de ONTAP S3).

Cloud Sync ne prend pas en charge la copie de listes de contrôle d'accès depuis le stockage objet vers les partages SMB.

["Découvrez comment copier des listes de contrôle d'accès à partir d'un partage SMB".](#)

Mettre à jour les licences

Vous pouvez maintenant mettre à jour les licences Cloud Sync que vous avez étendues.

Si vous avez prolongé une licence Cloud Sync que vous avez achetée auprès de NetApp, vous pouvez ajouter de nouveau la licence pour actualiser la date d'expiration.

["Découvrez comment mettre à jour une licence".](#)

Mettre à jour les informations d'identification de la

Vous pouvez maintenant mettre à jour les informations d'identification Box pour une relation de synchronisation existante.

["Découvrez comment mettre à jour les informations d'identification".](#)

31 octobre 2021

Support de boîtier

La prise en charge de Box est désormais disponible dans l'interface utilisateur de Cloud Sync sous forme d'aperçu.

La boîte peut être la source ou la cible dans plusieurs types de relations de synchronisation. ["Affichez la liste des relations de synchronisation prises en charge".](#)

Paramètre de date de création

Lorsqu'un serveur SMB est source, un nouveau paramètre de relation de synchronisation appelé *Date de création* permet de synchroniser les fichiers créés après une date spécifique, avant une date spécifique ou entre une plage de temps spécifique.

["En savoir plus sur les paramètres Cloud Sync".](#)

4 octobre 2021

Prise en charge supplémentaire de Box

Cloud Sync prend désormais en charge des relations de synchronisation supplémentaires pour ["Boîtier"](#) Lorsque vous utilisez l'API Cloud Sync :

- Amazon S3 vers Box
- Solution de stockage objet cloud IBM
- StorageGRID to Box
- Box à un serveur NFS
- Box à un serveur SMB

["Découvrez comment configurer une relation de synchronisation à l'aide de l'API".](#)

Rapports pour les chemins SFTP

C'est possible maintenant ["créer un rapport"](#) Pour les chemins SFTP.

2 septembre 2021

Prise en charge de FSX pour ONTAP

Vous pouvez désormais synchroniser des données vers ou depuis un système de fichiers Amazon FSX pour ONTAP.

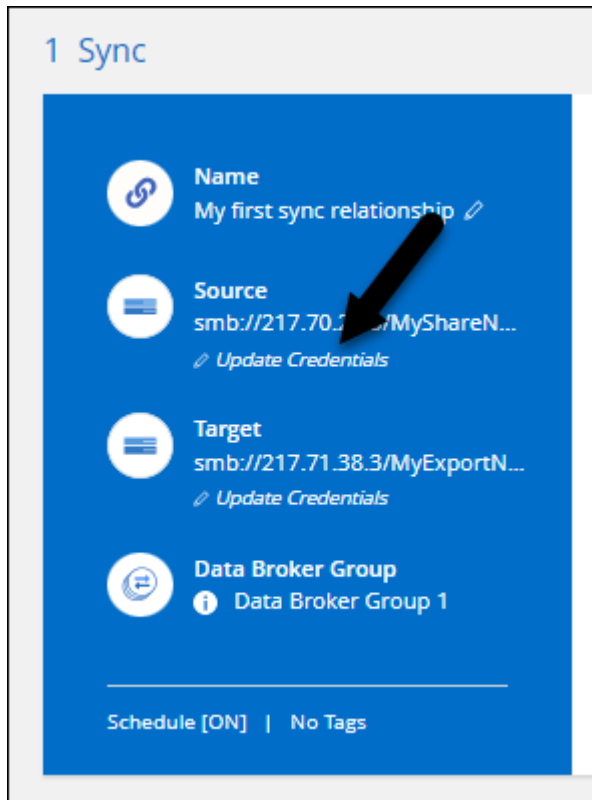
- ["En savoir plus sur Amazon FSX pour ONTAP"](#)
- ["Afficher les relations de synchronisation prises en charge"](#)
- ["Découvrez comment créer une relation de synchronisation pour Amazon FSX pour ONTAP"](#)

1er août 2021

Mettre à jour les informations d'identification

Cloud Sync vous permet désormais de mettre à jour le courtier de données avec les dernières informations d'identification de la source ou de la cible dans une relation de synchronisation existante.

Cette amélioration peut vous aider si vos stratégies de sécurité exigent la mise à jour périodique des informations d'identification. "[Découvrez comment mettre à jour les informations d'identification](#)".



Balises pour les cibles de stockage objet

Lors de la création d'une relation de synchronisation, vous pouvez désormais ajouter des balises à la cible de stockage objet d'une relation de synchronisation.

L'ajout de balises est pris en charge avec Amazon S3, Azure Blob, Google Cloud Storage, IBM Cloud Object Storage et StorageGRID.

< AWS S3 Bucket > Settings > 6 Tags/Metadata > 7 Review

Relationship Tags

Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket.
This enables you to search for the transferred files by using the tag values.

☒ Save on Object's Tags ☐ Save On Object's Metadata

Tag Key

Tag Value

+ Add Relationship Tag

Optional Field | [Up to 5]

Prise en charge de Box

Cloud Sync prend désormais en charge "Boîtier" En tant que source dans une relation de synchronisation avec Amazon S3, StorageGRID et IBM Cloud Object Storage lors de l'utilisation de l'API Cloud Sync.

["Découvrez comment configurer une relation de synchronisation à l'aide de l'API".](#)

Adresse IP publique pour courtier en données dans Google Cloud

Lorsque vous déployez un courtier de données dans Google Cloud, vous pouvez désormais activer ou désactiver une adresse IP publique pour l'instance de machine virtuelle.

["Découvrez comment déployer un courtier en données dans Google Cloud".](#)

Volume à double protocole pour Azure NetApp Files

Lorsque vous choisissez le volume source ou cible pour Azure NetApp Files, Cloud Sync affiche désormais un volume à double protocole, quel que soit le protocole choisi pour la relation de synchronisation.

7 juillet 2021

ONTAP S3 Storage et Google Cloud Storage

Cloud Sync prend désormais en charge les relations synchronisées entre ONTAP S3 Storage et un compartiment de stockage Google Cloud à partir de l'interface utilisateur.

["Affichez la liste des relations de synchronisation prises en charge".](#)

Balises de métadonnées d'objet

Lorsque vous créez une relation de synchronisation et que vous définissez un paramètre, Cloud Sync peut désormais copier des métadonnées et des balises d'objet entre le stockage objet.

["En savoir plus sur le paramètre copie pour objets".](#)

Prise en charge des coffres-forts HachiCorp

Vous pouvez maintenant configurer le courtier de données pour accéder aux informations d'identification à partir d'un coffre-fort externe HashiCorp en vous authentifiant avec un compte de service Google Cloud.

["En savoir plus sur l'utilisation d'un coffre-fort HashiCorp avec un courtier de données"](#).

Définissez des balises ou des métadonnées pour le compartiment S3

Lors de la configuration d'une relation de synchronisation avec un compartiment Amazon S3, l'assistant de synchronisation permet de définir les balises ou les métadonnées à enregistrer sur les objets du compartiment S3 cible.

L'option de balisage faisait auparavant partie des paramètres de la relation de synchronisation.

7 juin 2021

Classes de stockage dans Google Cloud

Lorsqu'un compartiment de stockage Google Cloud est la cible d'une relation synchrone, il est à présent possible de choisir la classe de stockage que vous souhaitez utiliser. Cloud Sync prend en charge les classes de stockage suivantes :

- Standard
- Nearline
- Ligne de refroidissement
- Archivage

2 mai 2021

Erreurs dans les rapports

Vous pouvez maintenant afficher les erreurs détectées dans les rapports et supprimer le dernier rapport ou tous les rapports.

["En savoir plus sur la création et l'affichage de rapports pour ajuster votre configuration"](#).

Comparer les attributs

Un nouveau paramètre **Comparer par** est maintenant disponible pour chaque relation de synchronisation.

Ce paramètre avancé vous permet de choisir si Cloud Sync doit comparer certains attributs lorsqu'il détermine si un fichier ou un répertoire a changé et doit être synchronisé à nouveau.

["En savoir plus sur la modification des paramètres d'une relation de synchronisation"](#).

11 avril 2021

Le service Cloud Sync autonome est retiré

Le service autonome Cloud Sync a été supprimé. Vous devez maintenant accéder à Cloud Sync directement à partir de BlueXP où toutes les mêmes fonctionnalités sont disponibles.

Après vous être connecté à BlueXP, vous pouvez passer à l'onglet Sync en haut et afficher vos relations, comme avant.

Google Cloud : des compartiments dans différents projets

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.

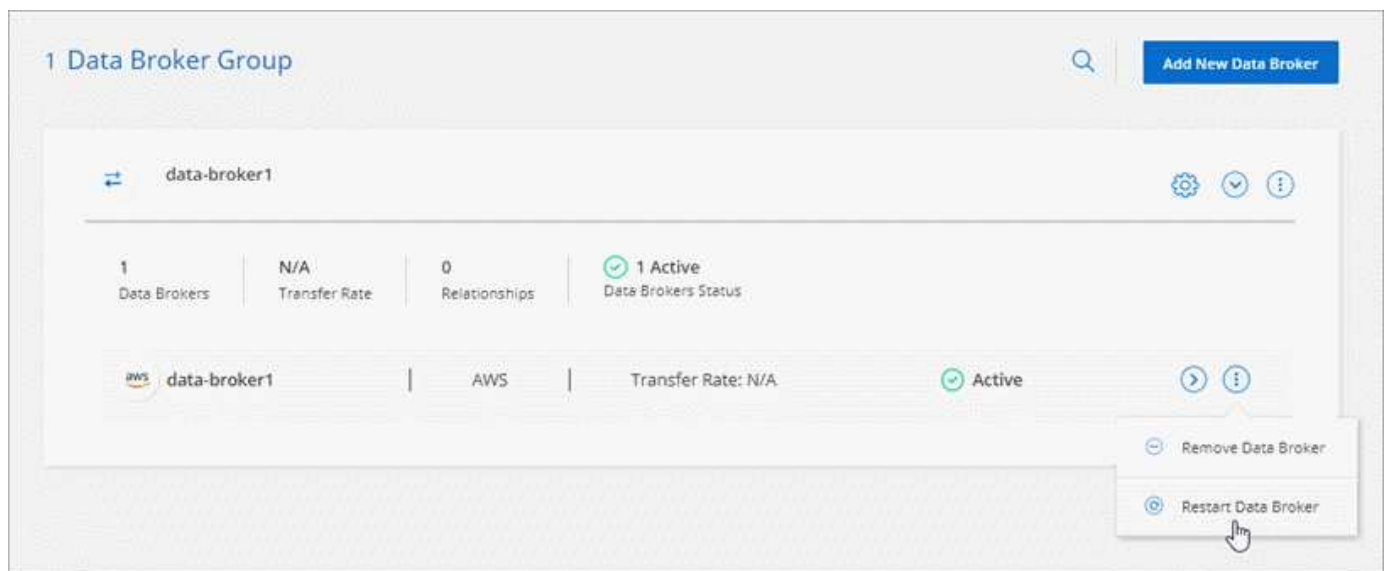
["Découvrez comment configurer le compte de service".](#)

Métadonnées entre Google Cloud Storage et S3

Cloud Sync copie désormais les métadonnées entre Google Cloud Storage et les fournisseurs S3 (AWS S3, StorageGRID et IBM Cloud Object Storage).

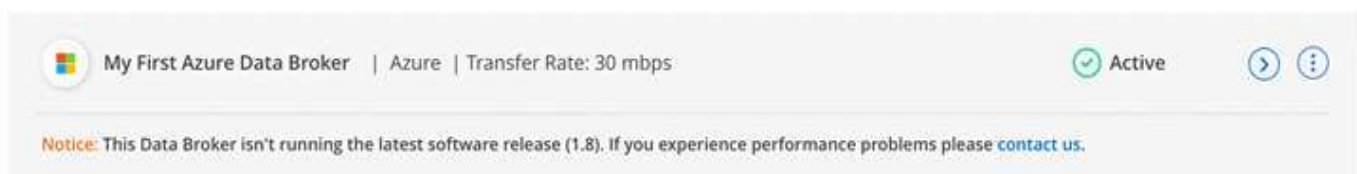
Redémarrer les courtiers de données

Vous pouvez maintenant redémarrer un courtier de données depuis Cloud Sync.



Message lorsque la dernière version n'est pas exécutée

Cloud Sync identifie désormais les cas où un courtier en données n'exécute pas la dernière version du logiciel. Ce message peut vous aider à bénéficier des dernières fonctionnalités.



Limites

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas

correctement avec elle. Examinez attentivement ces limites.

Cloud Sync n'est pas pris en charge dans les régions suivantes :

- Régions du gouvernement AWS
- Régions du gouvernement Azure
- Chine

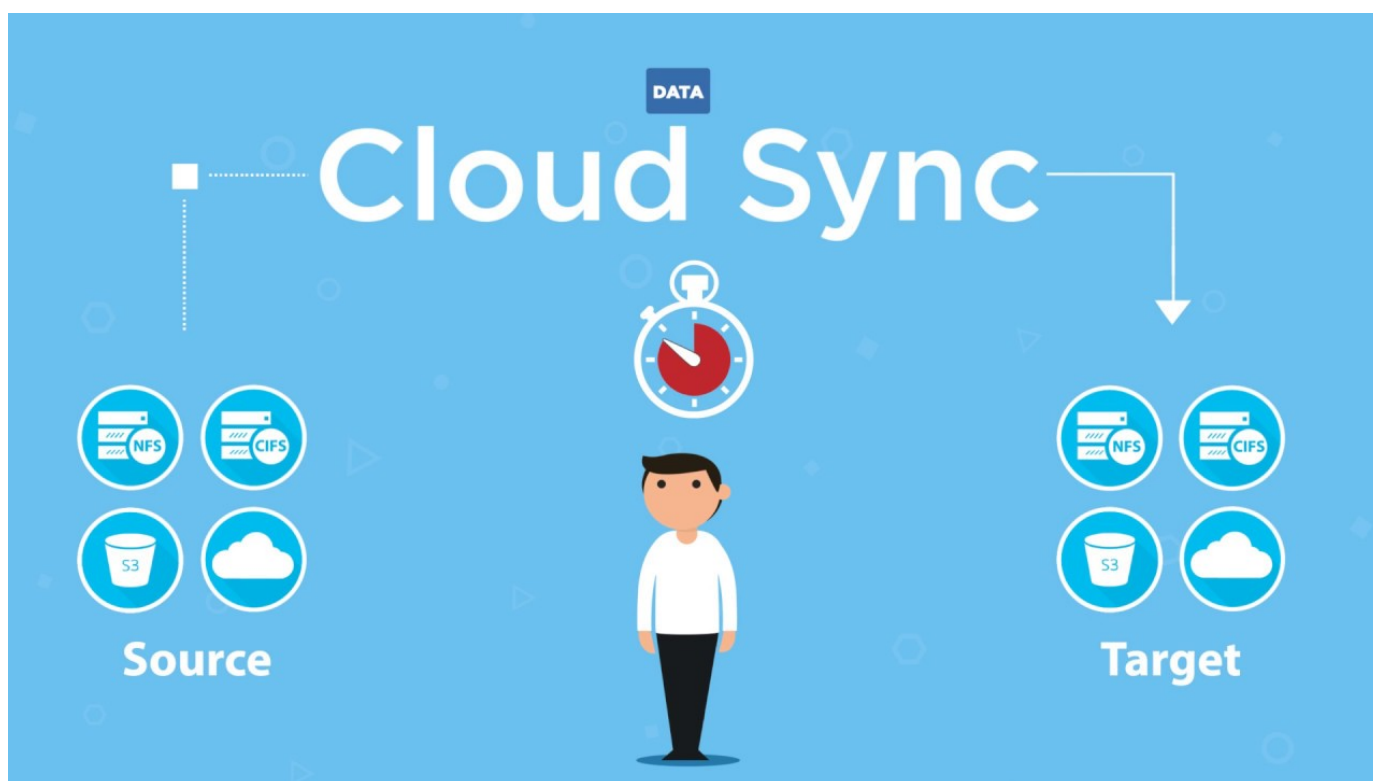
Commencez

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

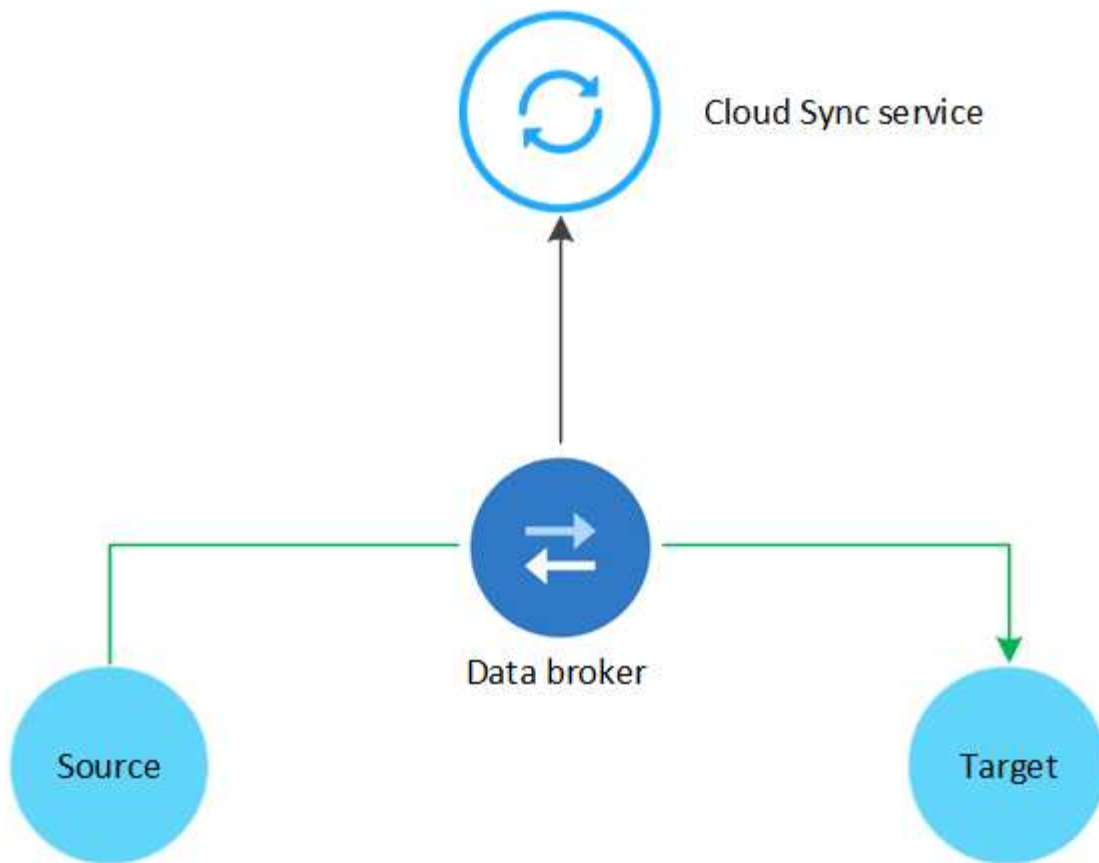
Regardez la vidéo suivante pour une présentation de Cloud Sync :



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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Amazon FSX pour ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM Cloud Object Storage • Serveur NFS • Serveur SMB • StorageGRID
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Serveur NFS • Serveur SMB

Emplacement de la source	Emplacements cibles pris en charge
IBM Cloud Object Storage	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Google Cloud Storage • Serveur SMB • StorageGRID • Stockage ONTAP S3
SFTP ²	S3
Serveur SMB	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

Summary

Delete role

Role ARN	arn:aws:iam::142581749262:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05	
Role description	Edit	

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

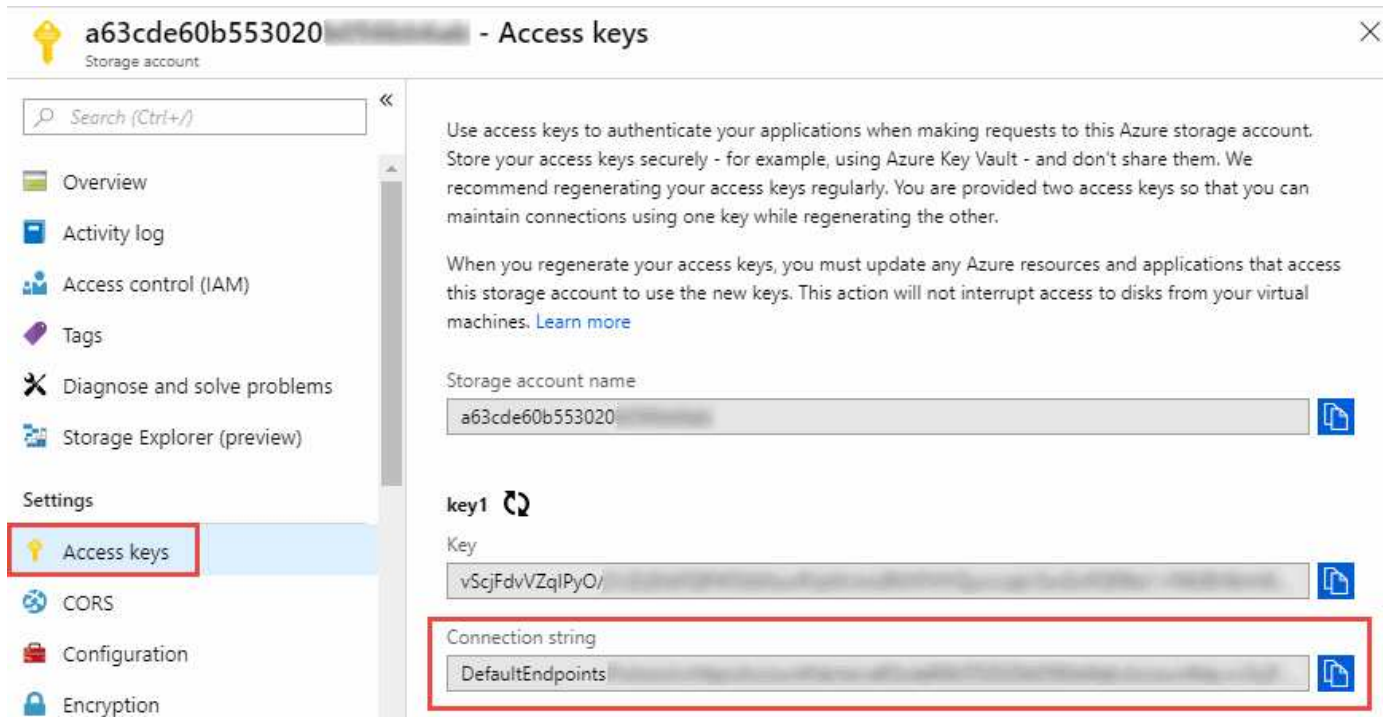
Un courtier en données peut résider en tout lieu lorsqu'une relation de synchronisation inclut le stockage Azure Blob.

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

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 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

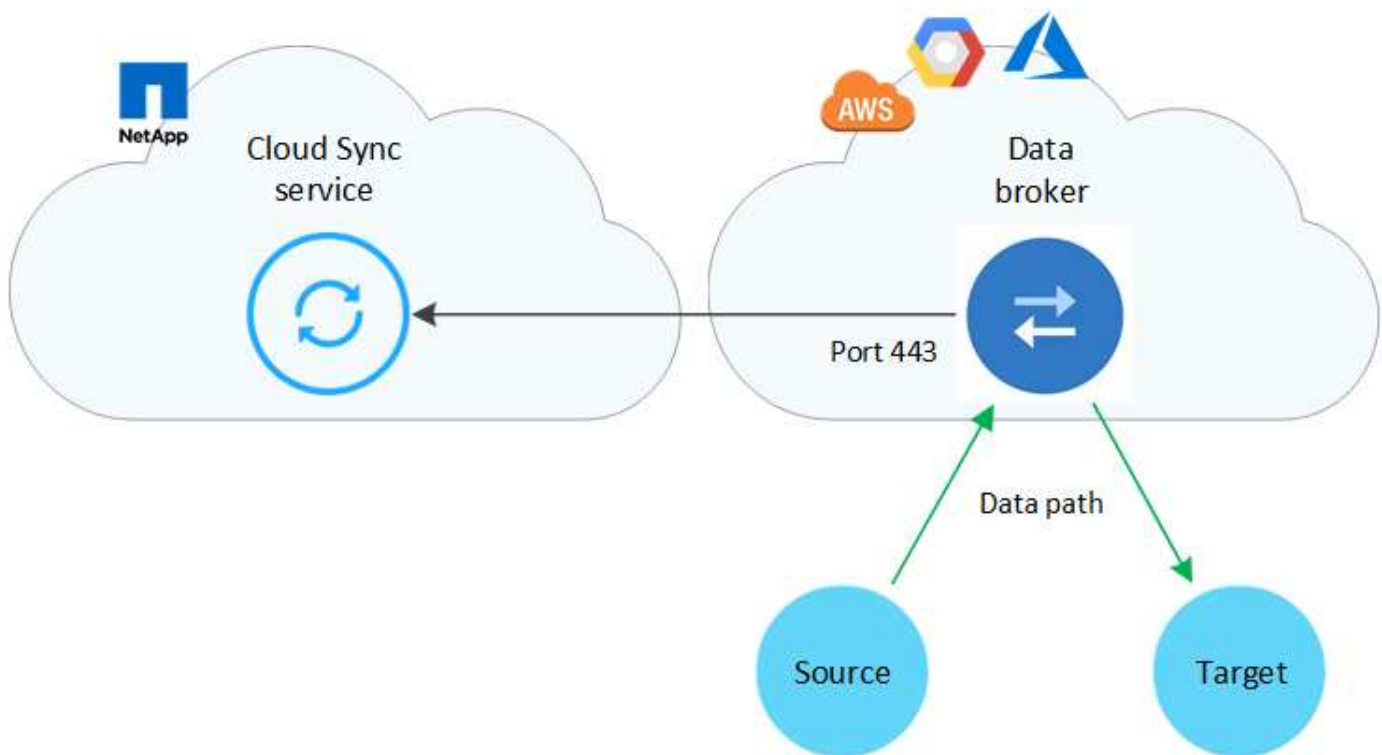
Un courtier en données est constitué d'un ou plusieurs courtiers de données installés dans le cloud ou sur site.

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.

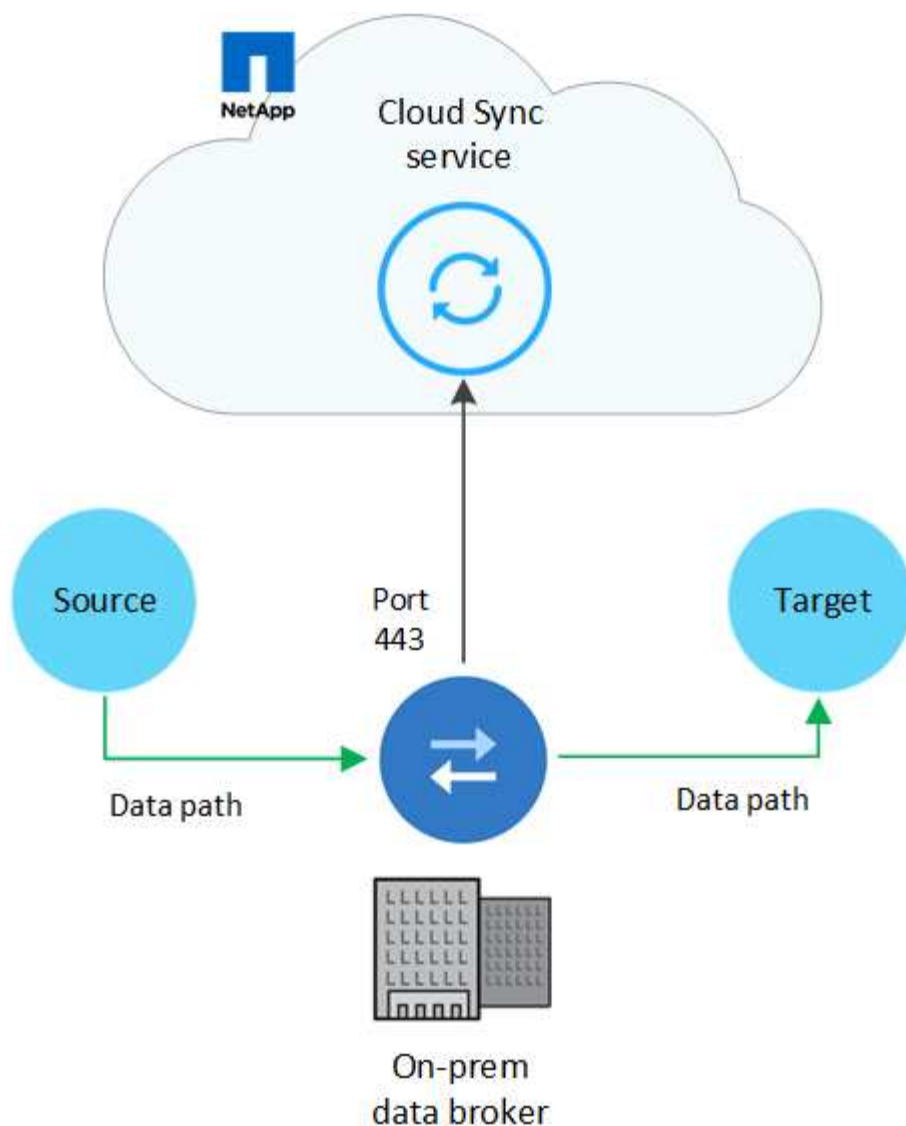


Lorsque Cloud Sync déploie le courtier en données dans AWS, Azure ou Google Cloud, il crée un groupe de sécurité qui assure la communication sortante requise.



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

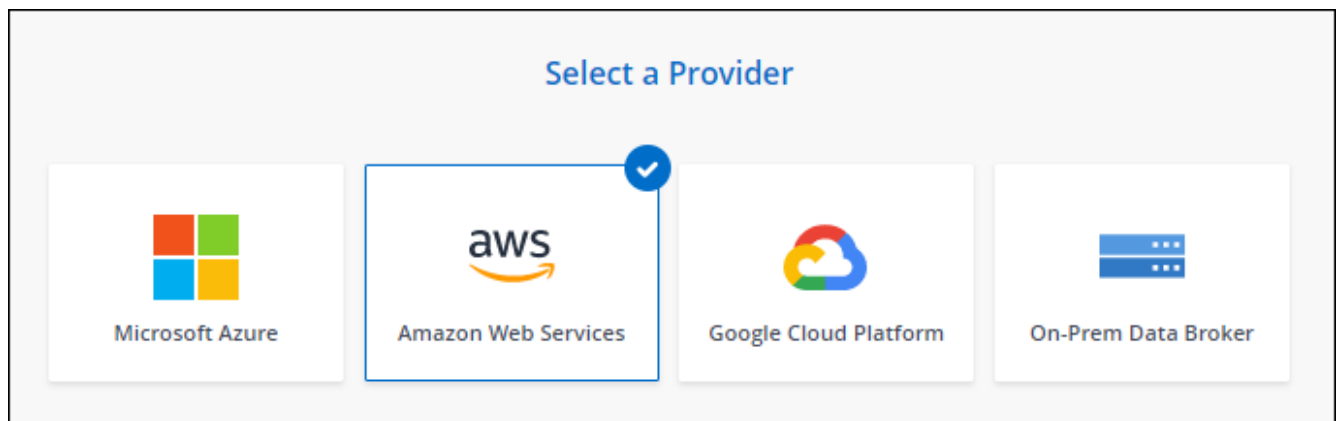
Il existe plusieurs façons de créer un nouveau courtier de données. Décrivez comment installer un courtier de données dans AWS lors de la création d'une relation de synchronisation.

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.

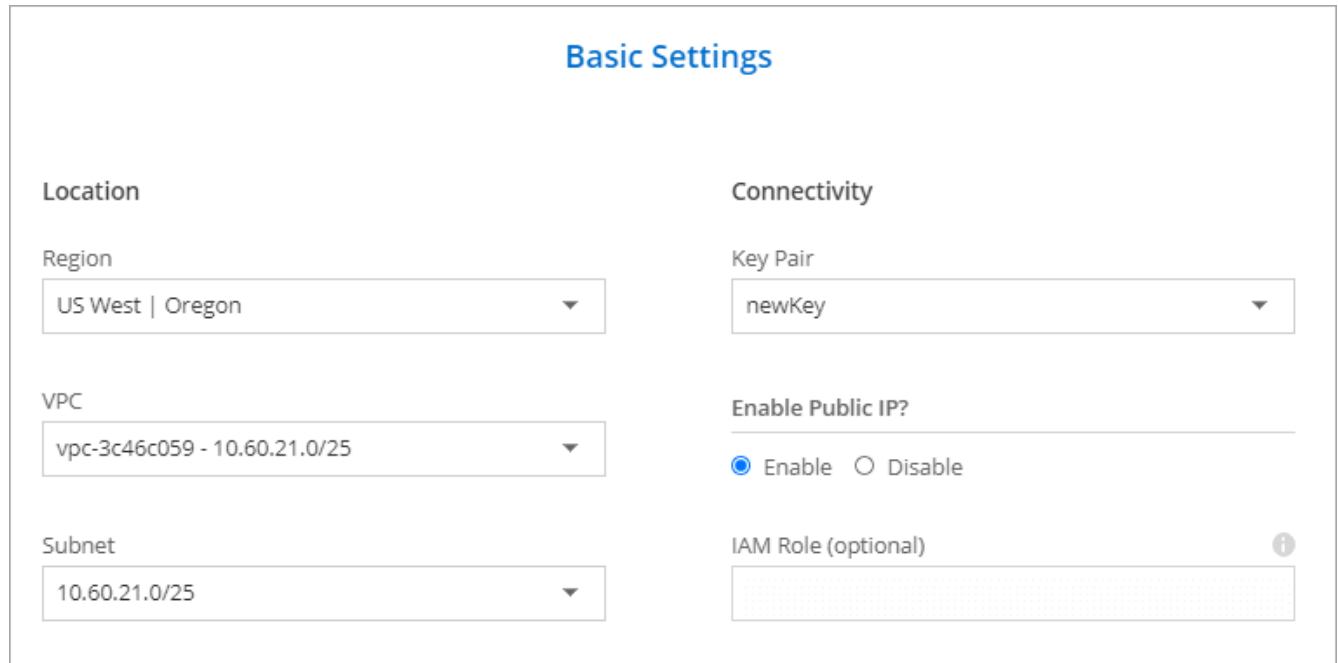
Si vous préférez ne pas fournir de touches d'accès, cliquez sur le lien en bas de la page pour utiliser un modèle CloudFormation. Lorsque vous utilisez cette option, vous n'avez pas besoin de fournir des identifiants, car vous vous connectez directement à AWS.

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)

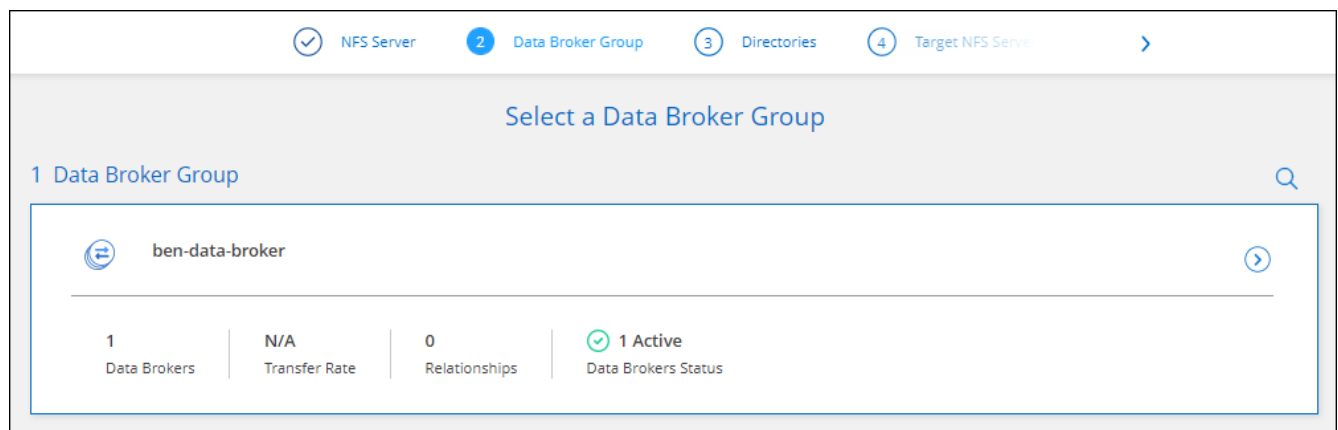
- Si vous avez saisi une clé d'accès AWS, sélectionnez un emplacement pour l'instance, sélectionnez une paire de clés, choisissez d'activer ou non une adresse IP publique, puis sélectionnez un rôle IAM existant, ou laissez le champ vide afin que Cloud Sync crée le rôle pour vous.

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



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

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



- 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',
 - 'Microsoft.EventGrid/systemTopics/read',
 - 'Microsoft.EventGrid/systemTopics/write',
 - 'Microsoft.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

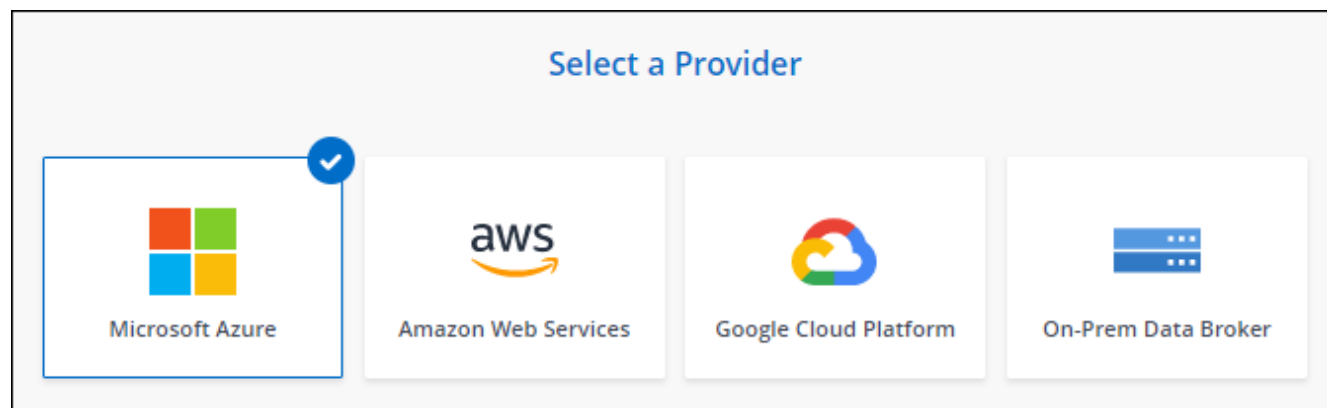
Il existe plusieurs façons de créer un nouveau courtier de données. Lors de la création d'une relation de synchronisation, procédez comme suit pour installer un courtier de données dans Azure.

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.

Location	Virtual Machine
Subscription <div>OCCM Dev ▼</div>	VM Name <div>netappdatabroker ⓘ</div>
Azure Region <div>West US 2 ▼</div>	User Name <div>databroker ⓘ</div>
VNet <div>Vnet1 ▼</div>	Authentication Method: <input checked="" type="radio"/> Password <input type="radio"/> Public Key
Subnet <div>Subnet1 ▼</div>	Enter Password ⓘ <div>.....</div>
	Resource Group: <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group



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

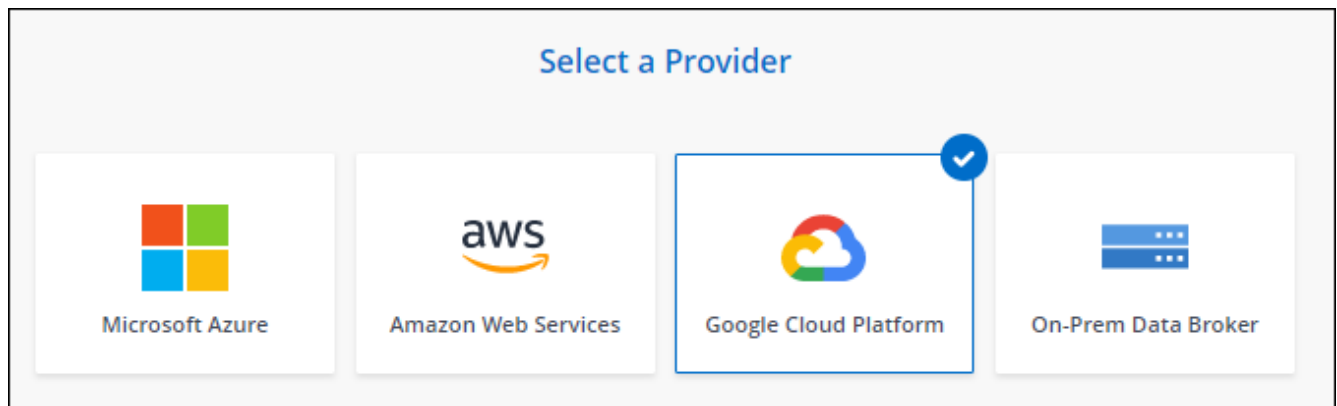
Il existe plusieurs façons de créer un nouveau courtier de données. Lors de la création d'une relation de synchronisation, procédez comme suit pour installer un courtier de données dans Google Cloud.

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.

The screenshot shows the 'Basic Settings' configuration page. It is divided into two main sections. The left section is titled 'Project' and contains two dropdown menus: 'Project' with the value 'OCCM-Dev' and 'Service Account' with the value 'test'. Below these is a link that says 'Select a Service Account that includes these permissions'. The right section is titled 'Location' and contains five dropdown menus: 'Region' with 'us-west1', 'Zone' with 'us-west1-a', 'VPC' with 'default', 'Subnet' with 'default', and 'Public IP' with 'Enable'.

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.

- 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.

- 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

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

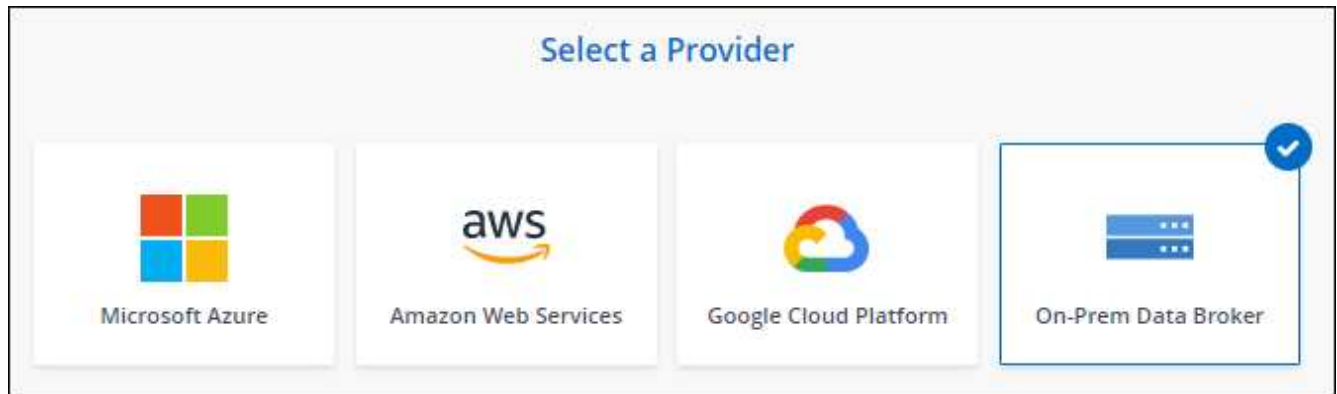
Vous pouvez installer un courtier de données sur un hôte Linux lorsque vous créez une relation de synchronisation.

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.

Utiliser Cloud Sync

Synchronisation des données entre une source et une cible

Création de relations synchronisées

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

Avant de pouvoir créer certains types de relations de synchronisation, vous devez d'abord créer un environnement de travail dans BlueXP.

Créer des relations de synchronisation pour des types spécifiques d'environnements de travail

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

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

Étapes

1. Créer ou découvrir l'environnement de travail.
 - ["Créez un environnement de travail Amazon FSX pour ONTAP"](#)
 - ["Configuration et détection d'Azure NetApp Files"](#)
 - ["Lancement d'Cloud Volumes ONTAP dans AWS"](#)
 - ["Lancement d'Cloud Volumes ONTAP dans Azure"](#)
 - ["Lancement d'Cloud Volumes ONTAP dans Google Cloud"](#)
 - ["Ajout de systèmes Cloud Volumes ONTAP existants"](#)
 - ["Découverte des clusters ONTAP"](#)
2. Cliquez sur **Canvas**.
3. Sélectionnez un environnement de travail correspondant à l'un des types répertoriés ci-dessus.
4. Sélectionnez le menu d'action en regard de Synchroniser.



5. Sélectionnez **Synchroniser les données de cet emplacement** ou **Synchroniser les données à cet emplacement** et suivez les invites pour configurer la relation de synchronisation.

Créez d'autres types de relations de synchronisation

Procédez comme suit pour synchroniser des données depuis ou vers un type de stockage pris en charge autre que Amazon FSX pour les clusters ONTAP, Azure NetApp Files, Cloud Volumes ONTAP ou ONTAP sur site. Les étapes ci-dessous fournissent un exemple de configuration d'une relation de synchronisation à partir d'un serveur NFS vers un compartiment S3.

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

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

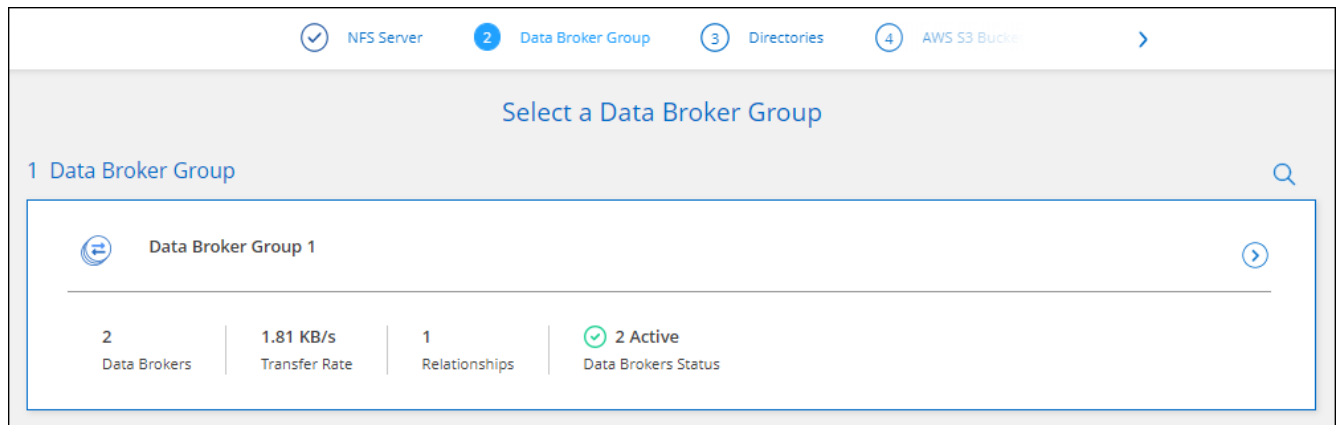


3. Sur la page **NFS Server**, entrez l'adresse IP ou le nom de domaine complet du serveur NFS que vous souhaitez synchroniser avec AWS.
4. Sur la page **Data Broker Group**, suivez les invites pour créer une machine virtuelle de courtier de données dans AWS, Azure ou Google Cloud Platform ou pour installer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

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

- ["Créer un courtier en données dans AWS"](#)
- ["Créer un courtier en données dans Azure"](#)
- ["Créer un courtier en données dans Google Cloud"](#)
- ["Installation du data broker sur un hôte Linux"](#)

5. Après avoir installé le courtier de données, cliquez sur **Continuer**.



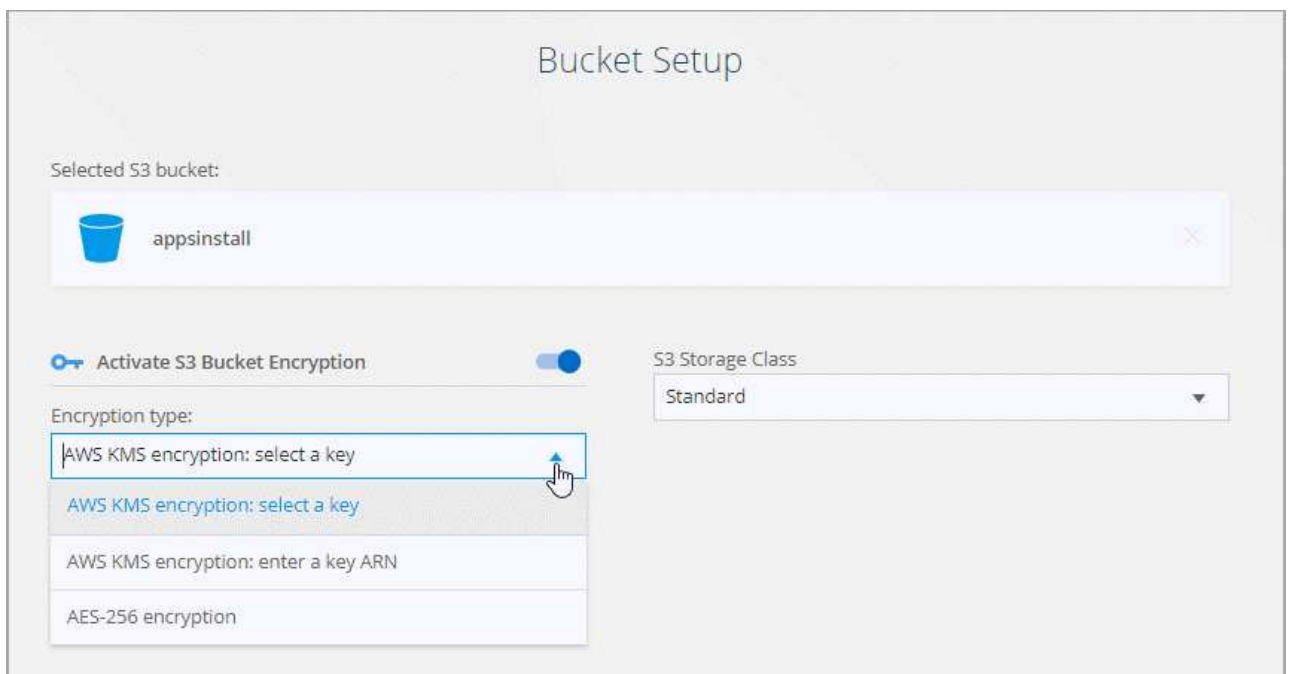
6. sur la page **répertoires**, sélectionnez un répertoire ou un sous-répertoire de niveau supérieur.

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



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

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



9. dans la page **Settings**, définissez comment les fichiers et dossiers source sont synchronisés et conservés à l'emplacement cible :

Planification

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

Délai d'expiration de la synchronisation

Définissez si Cloud Sync doit annuler une synchronisation de données si la synchronisation n'a pas été effectuée dans le nombre d'heures ou de jours spécifié.

Notifications

Vous permet de choisir de recevoir ou non des notifications Cloud Sync dans le Centre de notification de BlueXP. Vous pouvez activer des notifications pour la synchronisation des données avec succès, les échecs de synchronisation et les synchronisations de données annulées.

Tentatives

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

Synchronisation continue

Après la synchronisation initiale des données, Cloud Sync écoute les modifications apportées au compartiment S3 source ou au compartiment Google Cloud Storage, et synchronise en continu les modifications apportées à la cible au fur et à mesure de leur apparition. Il n'est pas nécessaire d'effectuer une nouvelle analyse de la source à intervalles réguliers.

Ce paramètre est disponible uniquement lors de la création d'une relation de synchronisation et lors de la synchronisation des données à partir d'un compartiment S3 ou de Google Cloud Storage vers le stockage Azure Blob, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3, Et StorageGRID * ou* à partir d'Azure Blob Storage vers le stockage Azure Blob, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS et StorageGRID.

Si vous activez ce paramètre, il affecte d'autres fonctions comme suit :

- La planification de synchronisation est désactivée.
- Les paramètres suivants sont rétablis à leurs valeurs par défaut : délai de synchronisation, fichiers récemment modifiés et Date de modification.
- Si S3 est la source, le filtre par taille sera actif uniquement lors des événements de copie (et non lors des événements de suppression).
- Une fois la relation créée, vous ne pouvez accélérer ou supprimer que la relation. Vous ne pouvez pas annuler les synchronisations, modifier les paramètres ou afficher les rapports.

Comparer par

Choisissez si Cloud Sync doit comparer certains attributs lorsqu'il détermine si un fichier ou un répertoire a été modifié et doit être à nouveau synchronisé.

Même si vous décochez ces attributs, Cloud Sync compare toujours la source à la cible en cochant les chemins, la taille des fichiers et les noms des fichiers. En cas de modifications, il synchronise ces fichiers et répertoires.

Vous pouvez choisir d'activer ou de désactiver Cloud Sync pour comparer les attributs suivants :

- **Mtime** : dernière heure modifiée pour un fichier. Cet attribut n'est pas valide pour les répertoires.
- **Uid, gid et mode** : indicateurs d'autorisation pour Linux.

Copier pour objets

Activez cette option pour copier les métadonnées et les balises de stockage objet. Si un utilisateur modifie les métadonnées sur la source, Cloud Sync copie cet objet dans la prochaine synchronisation, mais si un utilisateur modifie les balises de la source (et non les données en soi), Cloud Sync ne copie pas l'objet dans la prochaine synchronisation.

Vous ne pouvez pas modifier cette option après avoir créé la relation.

La copie des balises est prise en charge avec les relations de synchronisation incluant Azure Blob ou un terminal compatible avec S3 (S3, StorageGRID ou stockage objet dans le cloud IBM) comme cible.

La copie de métadonnées est prise en charge avec des relations « cloud à cloud » entre l'un des terminaux suivants :

- AWS S3
- Blob d'Azure
- Google Cloud Storage
- IBM Cloud Object Storage
- StorageGRID

Fichiers récemment modifiés

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

Supprimer des fichiers sur la source

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

Si vous activez cette option, vous devez également modifier un paramètre dans le fichier local.json du courtier de données. Ouvrez le fichier et mettez-le à jour comme suit :

```
{
  "workers":{
    "transferrer":{
      "delete-on-source": true
    }
  }
}
```

Supprimer des fichiers sur la cible

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

Types de fichiers

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

Exclure les extensions de fichier

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

► https://docs.netapp.com/fr-fr/cloud-manager-sync//media/video_file_extensions.mp4 (video)

Taille du fichier

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

Date de modification

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

Date de création

Lorsqu'un serveur SMB est source, ce paramètre vous permet de synchroniser les fichiers créés après une date spécifique, avant une date spécifique ou entre une plage horaire spécifique.

ACL - liste de contrôle d'accès

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

10. Sur la page **Tags/Metadata**, choisissez d'enregistrer une paire clé-valeur en tant qu'étiquette sur tous les fichiers transférés dans le compartiment S3 ou d'attribuer une paire clé-valeur de métadonnées sur tous les fichiers.

The screenshot shows the 'Relationship Tags' configuration page. At the top, there is a navigation bar with tabs: '<', 'AWS S3 Bucket', 'Settings', '6 Tags/Metadata', and '7 Review'. The main heading is 'Relationship Tags'. Below it, a text block states: 'Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket. This enables you to search for the transferred files by using the tag values.' There are two radio buttons: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below this, there are two input fields: 'Tag Key' with a placeholder 'Up to 128 characters' and 'Tag Value' with a placeholder 'Up to 256 characters'. At the bottom left, there is a button '+ Add Relationship Tag'. At the bottom right, there is a text 'Optional Field | [Up to 5]'.



Cette même fonctionnalité est disponible lors de la synchronisation de données sur StorageGRID et IBM Cloud Object Storage. Pour Azure et Google Cloud Storage, seule l'option de métadonnées est disponible.

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

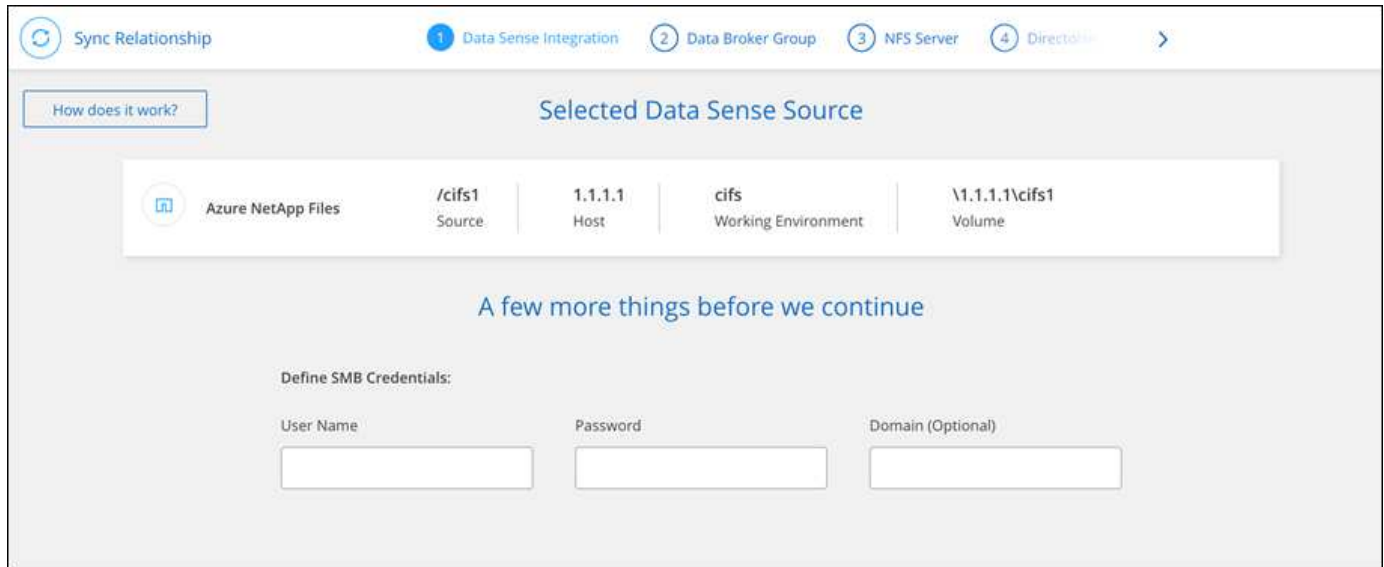
Résultat

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

Créez des relations synchronisées à partir du cloud Data Sense

Cloud Sync est intégré au sens des données dans le cloud. Dans Data Sense, vous pouvez sélectionner les fichiers source à synchroniser vers un emplacement cible à l'aide de Cloud Sync.

Une fois la synchronisation des données effectuée à partir du cloud Data SENSE, toutes les informations source le sont en une seule étape et vous devez saisir quelques informations clés. Choisissez ensuite l'emplacement cible de la nouvelle relation de synchronisation.



["Découvrez comment établir une relation synchrone à partir du Cloud Data SENSE".](#)

Copie des listes de contrôle d'accès à partir des partages SMB

Cloud Sync peut copier les listes de contrôle d'accès (ACL) entre les partages SMB et entre un partage SMB et le stockage objet (à l'exception de ONTAP S3). Si nécessaire, vous avez également la possibilité de conserver manuellement des listes de contrôle d'accès entre les partages SMB à l'aide de robocopy.

Choix

- up Cloud Sync to copy ACLs from an SMB server, Configurez Cloud Sync pour copier automatiquement les ACL
- copying ACLs between SMB shares, Copiez manuellement les listes de contrôle d'accès entre les partages SMB

Configuration de Cloud Sync pour copier les ACL

Copie de listes de contrôle d'accès entre les partages SMB et entre les partages SMB et le stockage objet en activant un paramètre lors de la création d'une relation ou après la création d'une relation.

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

Étapes d'une nouvelle relation

1. Dans Cloud Sync, cliquez sur **Créer une nouvelle synchronisation**.

2. Faites glisser un serveur SMB ou un stockage objet en tant que source et un serveur SMB ou un stockage objet en tant que cible, puis cliquez sur **Continuer**.
3. Sur la page **SMB Server** :
 - a. Entrez un nouveau serveur SMB ou sélectionnez un serveur existant et cliquez sur **Continuer**.
 - b. Saisissez les informations d'identification du serveur SMB.
 - c. Sélectionnez **Copier les listes de contrôle d'accès vers la cible** et cliquez sur **Continuer**.

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

Lorsque vous copiez des listes de contrôle d'accès depuis SMB vers le stockage objet, vous pouvez choisir de copier ces listes de contrôle d'accès vers les balises de l'objet ou sur les métadonnées de l'objet, en fonction de la cible. Pour Azure et Google Cloud Storage, seule l'option de métadonnées est disponible.

La capture d'écran suivante montre un exemple de l'étape où vous pouvez faire ce choix.

Étapes d'une relation existante

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

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

Copie manuelle des listes de contrôle d'accès entre partages SMB

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

Étapes

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

Vous devez effectuer cette étape avant d'utiliser Robocopy.

3. Dans Cloud Sync, créez une nouvelle relation entre les partages SMB source et cible ou synchronisez une relation existante.
4. Une fois la synchronisation des données terminée, exécutez la commande suivante à partir de l'hôte Windows pour synchroniser les ACL et la propriété :

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

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

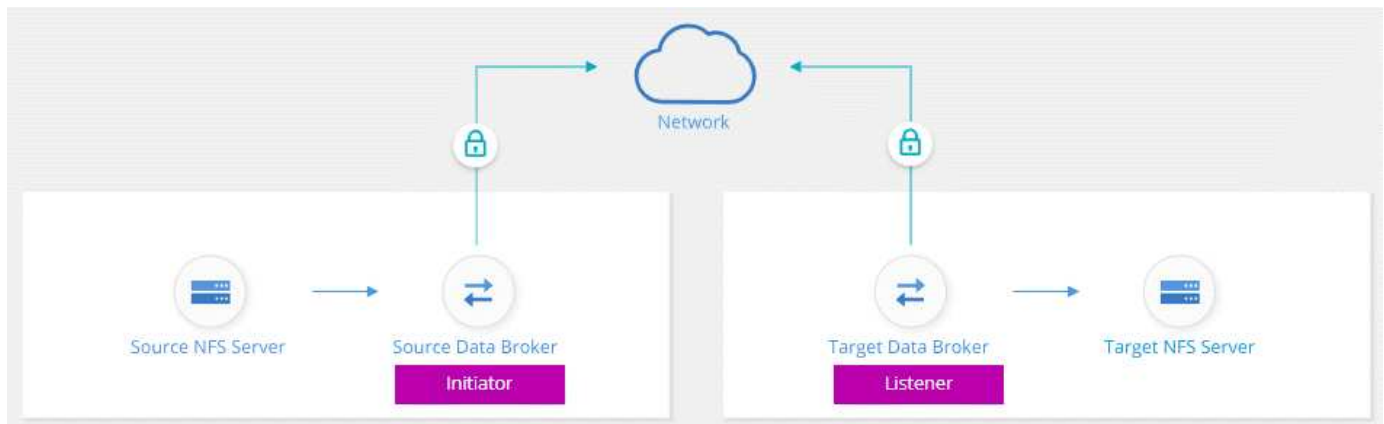
Synchronisation des données NFS à l'aide du chiffrement des données à la volée

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

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

Fonctionnement du chiffrement des données en vol.

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



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

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

Voici le fonctionnement du chiffrement à la volée :

1. Après avoir créé la relation de synchronisation, l'initiateur démarre une connexion chiffrée avec l'autre courtier de données.
2. Le courtier de données source crypte les données à partir de la source à l'aide de TLS 1.3.
3. Il envoie ensuite les données via le réseau au data broker cible.
4. Le courtier de données cible décrypte les données avant de les envoyer à la cible.
5. Après la copie initiale, le service synchronise les données modifiées toutes les 24 heures. S'il y a des données à synchroniser, le processus commence par l'initiateur qui ouvre une connexion chiffrée avec l'autre courtier de données.

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

Versions NFS prises en charge

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

Limitation du serveur proxy

Si vous créez une relation de synchronisation chiffrée, les données cryptées sont envoyées via HTTPS et ne sont pas routables via un serveur proxy.

Ce dont vous aurez besoin pour commencer

Assurez-vous d'avoir les éléments suivants :

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

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

Si vous souhaitez utiliser un groupe de courtiers de données existant, le groupe ne doit avoir qu'un seul courtier de données. Plusieurs courtiers de données d'un groupe ne sont pas pris en charge avec des relations de synchronisation chiffrées.

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

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

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

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

Étapes

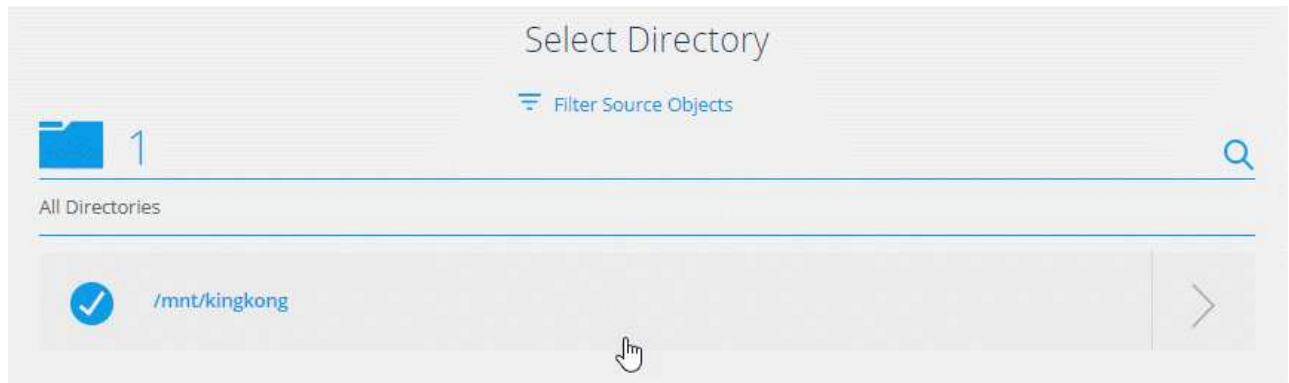
1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser **serveur NFS** vers les emplacements source et cible ou **Azure NetApp Files** vers les emplacements source et cible et sélectionnez **Oui** pour activer le cryptage des données en transit.
3. Suivez les invites pour créer la relation :
 - a. **NFS Server/Azure NetApp Files** : Choisissez la version NFS, puis spécifiez une nouvelle source NFS ou sélectionnez un serveur existant.

- b. **Définir la fonctionnalité de Data Broker** : définissez le courtier de données *écoute* pour les demandes de connexion sur un port et lequel *lance* la connexion. Faites votre choix en fonction de vos besoins en matière de mise en réseau.
- c. **Data Broker** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.

Notez ce qui suit :

- Si vous souhaitez utiliser un groupe de courtiers de données existant, le groupe ne doit avoir qu'un seul courtier de données. Plusieurs courtiers de données d'un groupe ne sont pas pris en charge avec des relations de synchronisation chiffrées.
 - Si le courtier de données source agit en tant qu'auditeur, il doit alors être un nouveau courtier de données.
 - Si vous avez besoin d'un nouveau courtier de données, Cloud Sync vous invite à suivre les instructions d'installation. Vous pouvez déployer le data broker dans le cloud ou télécharger un script d'installation pour votre propre hôte Linux.
- d. **Répertoires** : Choisissez les répertoires que vous souhaitez synchroniser en sélectionnant tous les répertoires ou en descendant et en sélectionnant un sous-répertoire.

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




- e. **Serveur NFS cible/Azure NetApp Files cible** : Choisissez la version NFS, puis entrez une nouvelle cible NFS ou sélectionnez un serveur existant.
- f. **Courtier de données cible** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.


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

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


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform

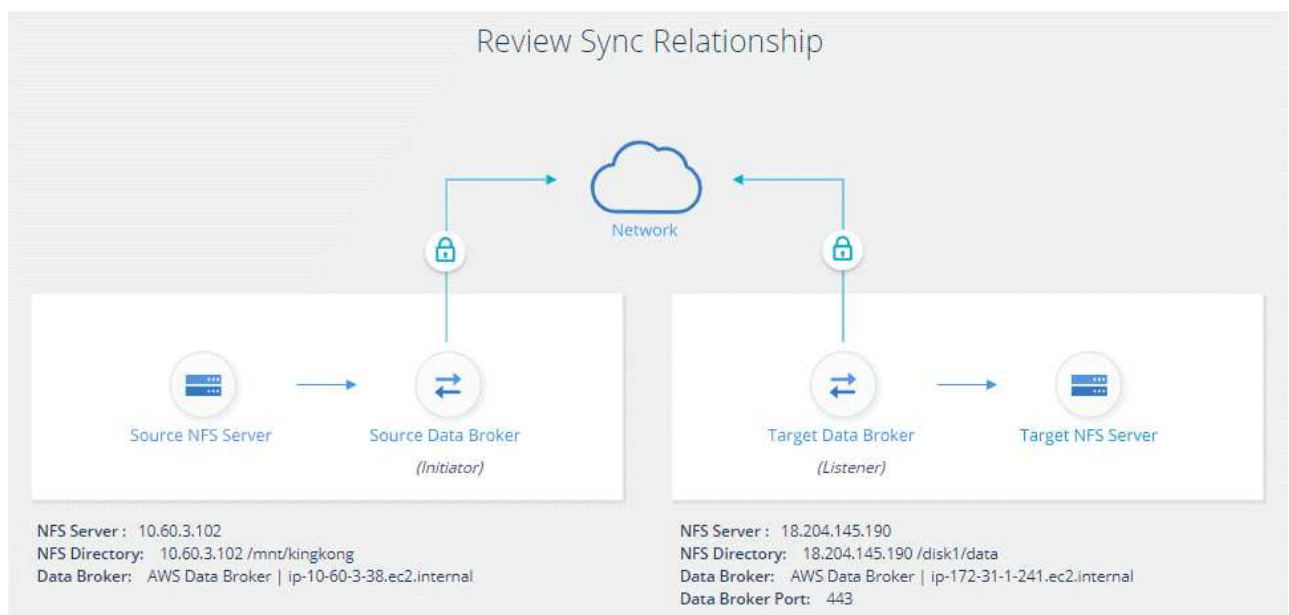


On-Prem Data Broker

Data Broker Name

Port

- a. **Répertoires cibles** : sélectionnez un répertoire de niveau supérieur ou accédez à la recherche pour sélectionner un sous-répertoire existant ou créer un nouveau dossier à l'intérieur d'une exportation.
- b. **Paramètres** : définissez comment les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible.
- c. **Revue** : consultez les détails de la relation de synchronisation, puis cliquez sur **Créer une relation**.



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

Configuration d'un groupe de courtier de données pour utiliser un coffre-fort externe HashiCorp

Lorsque vous créez une relation de synchronisation qui requiert des identifiants Amazon S3, Azure ou Google Cloud, vous devez spécifier ces identifiants via l'interface ou l'API utilisateur de Cloud Sync. Une alternative consiste à configurer le groupe de courtiers de données pour accéder aux informations d'identification (ou

secrets) directement à partir d'un coffre-fort externe HashiCorp.

Cette fonctionnalité est prise en charge par le biais de l'API Cloud Sync avec des relations synchronisées qui requièrent des identifiants Amazon S3, Azure ou Google Cloud.

Préparez le coffre-fort pour fournir les informations d'identification au groupe de courtiers de données en configurant les URL. Les URL des secrets dans le coffre-fort doivent se terminer par *creds*.

Préparez le groupe de courtier de données pour extraire les informations d'identification du coffre-fort externe en modifiant le fichier de configuration local de chaque courtier de données du groupe.

Maintenant que tout est configuré, vous pouvez envoyer un appel API pour créer une relation de synchronisation qui utilise votre coffre-fort pour obtenir les secrets.

Préparation du coffre-fort

Vous devrez fournir à Cloud Sync l'URL des secrets de votre coffre-fort. Préparez le coffre-fort en configurant ces URL. Vous devez configurer des URL pour les identifiants de chaque source et cible dans les relations de synchronisation que vous prévoyez de créer.

L'URL doit être configurée comme suit :

```
/<path>/<requestid>/<endpoint-protocol>Creds
```

Chemin

Chemin du préfixe vers le secret. Tous ces atouts peuvent être uniques à votre entreprise.

ID de la demande

ID de demande que vous devez générer. Vous devrez fournir l'ID dans l'un des en-têtes de la demande POST API lorsque vous créez la relation de synchronisation.

Protocole de terminal

L'un des protocoles suivants, tel que défini "[dans la documentation post-relation v2](#)": S3, AZURE ou GCP (chacun doit être en majuscules).

Creds

L'URL doit se terminer par *creds*.

Exemples

Les exemples suivants montrent des URL vers des secrets.

Exemple pour l'URL complète et le chemin d'accès pour les informations d'identification source

```
http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds
```

Comme vous pouvez le voir dans l'exemple, le chemin du préfixe est */mon-chemin/tous-secrets/*, l'ID de la demande est *hb312vdasr2* et le noeud final source est S3.

Exemple pour l'URL complète et le chemin des informations d'identification de la cible

```
http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds
```

Le chemin du préfixe est */my-path/all-secrets/*, l'ID de la demande est *n32hcbnejk2*, et le noeud final cible est Azure.

Préparation du groupe de courtiers de données

Préparez le groupe de courtier de données pour extraire les informations d'identification du coffre-fort externe en modifiant le fichier de configuration local de chaque courtier de données du groupe.

Étapes

1. SSH vers un courtier de données dans le groupe.
2. Modifiez le fichier local.json qui se trouve dans /opt/netapp/Dataroker/config.
3. Définissez l'option enable sur **true** et définissez les champs des paramètres de configuration sous *external-integrations.haschicorp* comme suit :

activé

- Valeurs valides : vrai/faux
- Type : booléen
- Valeur par défaut : FALSE
- Vrai: Le courtier de données obtient des secrets de votre propre coffre-fort externe HashiCorp
- FALSE : le courtier de données stocke les informations d'identification dans son coffre-fort local

url

- Type : chaîne
- Valeur : l'URL de votre coffre-fort externe

chemin

- Type : chaîne
- Valeur : chemin du préfixe vers le secret avec vos informations d'identification

Rejet non autorisé

- Détermine si vous souhaitez que le courtier de données rejette le coffre-fort externe non autorisé
- Type : booléen
- Par défaut : FALSE

méthode-auth

- Méthode d'authentification que le courtier de données doit utiliser pour accéder aux informations d'identification à partir du coffre-fort externe
- Type : chaîne
- Valeurs valides : "aws-iam" / "Role-app" / "gcp-iam"

nom-rôle

- Type : chaîne
- Nom du rôle (si vous utilisez aws-iam ou gcp-iam)

Secretid et rotide

- Type : chaîne (si vous utilisez APP-role)

Espace de noms

- Type : chaîne

- Votre espace de noms (en-tête X-Vault-namespace, le cas échéant)

4. Répétez ces étapes pour tous les autres courtiers de données du groupe.

Exemple d'authentification aws-role

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "https://example.vault.com:8200",
      "path": "my-path/all-secrets",
      "reject-unauthorized": false,
      "auth-method": "aws-role",
      "aws-role": {
        "role-name": "my-role"
      }
    }
  }
}
```

Exemple d'authentification gcp-iam

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "http://ip-10-20-30-55.ec2.internal:8200",
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
      "gcp-iam": {
        "role-name": "my-iam-role"
      }
    }
  }
}
```

Configuration des autorisations lors de l'utilisation de l'authentification gcp-iam

Si vous utilisez la méthode d'authentification *gcp-iam*, le courtier de données doit disposer de l'autorisation GCP suivante :

```
- iam.serviceAccounts.signJwt
```

["En savoir plus sur les exigences d'autorisation GCP pour le courtier de données"](#).

Création d'une nouvelle relation de synchronisation à l'aide des secrets du coffre-fort

Maintenant que tout est configuré, vous pouvez envoyer un appel API pour créer une relation de synchronisation qui utilise votre coffre-fort pour obtenir les secrets.

Publiez la relation à l'aide de l'API REST de Cloud Sync.

```
Headers:  
Authorization: Bearer <user-token>  
Content-Type: application/json  
x-account-id: <accountid>  
x-netapp-external-request-id-src: request ID as part of path for source  
credentials  
x-netapp-external-request-id-trg: request ID as part of path for target  
credentials  
Body: post relationship v2 body
```

- Pour obtenir un jeton utilisateur et votre identifiant de compte BlueXP, ["reportez-vous à cette page dans la documentation"](#).
- Pour créer un corps pour votre relation post, ["Reportez-vous à l'appel de l'API relations-v2"](#).

Exemple

Exemple pour la demande POST :

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik..."
Body:
{
  "dataBrokerId": "5e6e111d578dtyuu1555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    }
  },
  "target": {
    "protocol": "s3",
    "s3": {
      "bucket": "my-target-bucket"
    }
  }
}
```

Payer pour la synchronisation après la fin de votre essai gratuit

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

Vous pouvez vous abonner à AWS Marketplace ou à Azure Marketplace. Vous ne pouvez pas vous abonner des deux.

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

["En savoir plus sur le fonctionnement des licences".](#)

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

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

Abonnement à AWS

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

Les étapes à payer en tant que vous-même

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

La vidéo suivante montre le processus :

► https://docs.netapp.com/fr-fr/cloud-manager-sync//media/video_cloud_sync_registering.mp4 (video)

Étapes à payer annuellement

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

S'abonner à Azure

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

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

Étapes

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

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

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

La vidéo suivante montre le processus :

► https://docs.netapp.com/fr-fr/cloud-manager-sync//media/video_cloud_sync_registering_azure.mp4

(video)

Achat de licences auprès de NetApp et ajout de ces licences à Cloud Sync

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

Vous devez disposer du numéro de série correspondant à votre licence, ainsi que du nom d'utilisateur et du mot de passe du compte sur le site de support NetApp auquel la licence est associée.

Étapes

1. Achetez une licence par [contacter NetApp](#).
2. Dans BlueXP, cliquez sur **Sync > licences**.
3. Cliquez sur **Ajouter une licence** et ajoutez les informations requises :
 - a. Saisissez le numéro de série.
 - b. Sélectionnez le compte sur le site de support NetApp associé à la licence que vous ajoutez :
 - Si votre compte a déjà été ajouté à BlueXP, sélectionnez-le dans la liste déroulante.
 - Si votre compte n'a pas encore été ajouté, cliquez sur **Ajouter des informations d'identification NSS**, entrez le nom d'utilisateur et le mot de passe, cliquez sur **Enregistrer**, puis sélectionnez-le dans la liste déroulante.
 - c. Cliquez sur **Ajouter**.

Mise à jour d'une licence

Si vous avez prolongé une licence Cloud Sync que vous avez achetée auprès de NetApp, la nouvelle date d'expiration ne sera pas automatiquement mise à jour dans Cloud Sync. Vous devez ajouter de nouveau la licence pour actualiser la date d'expiration.

Étapes

1. Dans BlueXP, cliquez sur **Sync > licences**.
2. Cliquez sur **Ajouter une licence** et ajoutez les informations requises :
 - a. Saisissez le numéro de série.
 - b. Sélectionnez le compte du site de support NetApp associé à la licence que vous ajoutez.
 - c. Cliquez sur **Ajouter**.

Cloud Sync met à jour la licence existante avec la nouvelle date d'expiration.


Gestion des relations de synchronisation

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

Synchronisez immédiatement les données

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

Étapes

1. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
2. Cliquez sur **Synchroniser maintenant**, puis sur **Sync** pour confirmer.

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

Accélération des performances de synchronisation

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


Si le groupe du courtier gère d'autres relations de synchronisation, le nouveau courtier de données que vous ajoutez au groupe accélère également les performances de ces relations de synchronisation.

Imaginons par exemple que vous ayez trois relations :

- La relation 1 est gérée par le groupe de courtiers de données A
- La relation 2 est gérée par le groupe de courtiers de données B
- La relation 3 est gérée par le groupe de courtiers de données A.

Vous voulez accélérer les performances de la relation 1 pour ajouter un nouveau courtier de données au groupe de courtier de données A. Dans la mesure où le groupe A gère également la relation de synchronisation 3, les performances de synchronisation de la relation sont également automatiquement accélérées.

Étapes

1. Assurez-vous qu'au moins un des courtiers de données existants dans la relation est en ligne.
2. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
3. Cliquez sur **accélérer**.
4. Suivez les invites pour créer un nouveau courtier de données.

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

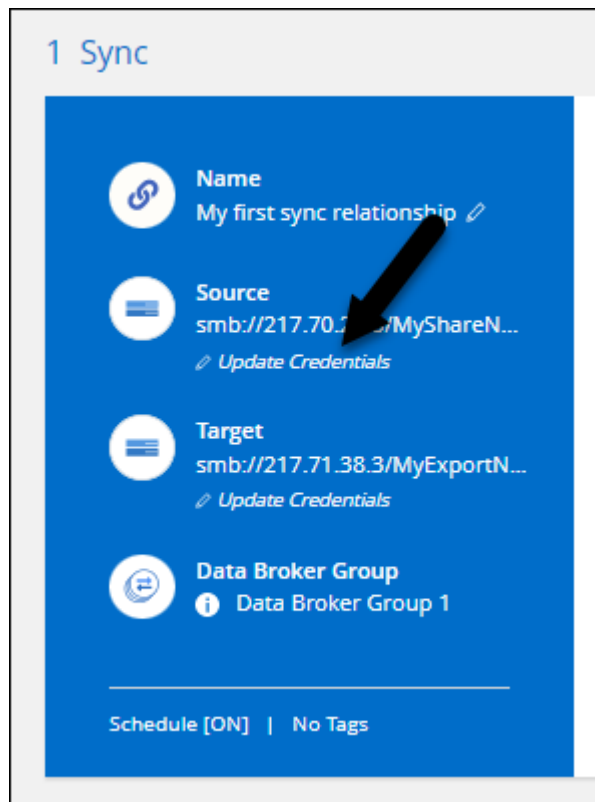
Mise à jour des identifiants

Vous pouvez mettre à jour le courtier de données avec les informations d'identification les plus récentes de la source ou de la cible dans une relation de synchronisation existante. La mise à jour des informations d'identification peut vous aider si vos stratégies de sécurité vous obligent à mettre à jour les informations d'identification de manière périodique.

La mise à jour des identifiants est prise en charge avec toute source ou cible pour laquelle Cloud Sync nécessite des identifiants pour : Azure Blob, Box, IBM Cloud Object Storage, StorageGRID, ONTAP S3 Storage, SFTP et les serveurs SMB.

Étapes

1. Dans le tableau de bord **Sync**, accédez à une relation de synchronisation qui nécessite des informations d'identification, puis cliquez sur **mettre à jour les informations d'identification**.



2. Entrez les informations d'identification et cliquez sur **Update**.

Remarque sur les serveurs SMB : si le domaine est nouveau, vous devez le spécifier lors de la mise à jour des informations d'identification. Si le domaine n'a pas changé, vous n'avez pas besoin de le saisir à nouveau.

Si vous avez entré un domaine lors de la création de la relation de synchronisation, mais que vous n'entrez pas de nouveau domaine lorsque vous mettez à jour les informations d'identification, Cloud Sync utilisera alors le domaine d'origine que vous avez fourni.

Cloud Sync met à jour les identifiants du courtier en données. Le 10 courtier en données peut prendre jusqu'à ce que ses identifiants soient utilisés pour la synchronisation des données.


Configuration des notifications

Un paramètre **Notifications** pour chaque relation de synchronisation vous permet de choisir de recevoir ou non des notifications Cloud Sync dans le Centre de notification de BlueXP. Vous pouvez activer des notifications pour la synchronisation des données avec succès, les échecs de synchronisation et les synchronisations de données annulées.



Vous pouvez également recevoir des notifications par e-mail.


Étapes

1. Modifiez les paramètres d'une relation de synchronisation :
 - a. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
 - b. Cliquez sur **Paramètres**.
 - c. Activez **Notifications**.
 - d. Cliquez sur **Enregistrer les paramètres**.
2. Si vous souhaitez recevoir des notifications par e-mail, configurez les paramètres d'alerte et de notification :
 - a. Cliquez sur **Paramètres > Paramètres d'alertes et de notifications**.
 - b. Sélectionnez un ou plusieurs utilisateurs et choisissez le type de notification **Info**.
 - c. Cliquez sur **appliquer**.

Vous recevrez maintenant des notifications Cloud Sync dans le Centre de notification de BlueXP, avec quelques notifications envoyées par e-mail, si vous avez configuré cette option.

Modification des paramètres d'une relation de synchronisation

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

1. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
2. Cliquez sur **Paramètres**.
3. Modifiez l'un des paramètres.

General

Schedule

ON | Every 1 Day

▼

Retries

Retry 3 times before skipping file

▼

Files and Directories

Compare By

The following attributes (and size): uid, gid, mode, mtime

▼

Recently Modified Files

Exclude files that are modified up to 30 Seconds before a scheduled sync

▼

Delete Files On Source

Never delete files from the source location

▼

Delete Files On Target

Never delete files from the target location

▼

File Types

Include All: Files, Directories, Symbolic Links

▼

Exclude File Extensions

None

▼

File Size

All

▼

Date Modified

All

▼

Date Created

All

▼

ACL - Access Control List

Inactive

▼

Reset to defaults

Voici une brève description de chaque paramètre :

Planification

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

Délai d'expiration de la synchronisation

Définissez si Cloud Sync doit annuler une synchronisation de données si la synchronisation n'a pas été effectuée dans le nombre d'heures ou de jours spécifié.

Notifications

Vous permet de choisir de recevoir ou non des notifications Cloud Sync dans le Centre de notification de BlueXP. Vous pouvez activer des notifications pour la synchronisation des données avec succès, les échecs de synchronisation et les synchronisations de données annulées.

Si vous souhaitez recevoir des notifications pour

Tentatives

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

Comparer par

Choisissez si Cloud Sync doit comparer certains attributs lorsqu'il détermine si un fichier ou un répertoire a été modifié et doit être à nouveau synchronisé.

Même si vous décochez ces attributs, Cloud Sync compare toujours la source à la cible en cochant les chemins, la taille des fichiers et les noms des fichiers. En cas de modifications, il synchronise ces fichiers et répertoires.

Vous pouvez choisir d'activer ou de désactiver Cloud Sync pour comparer les attributs suivants :

- **Mtime** : dernière heure modifiée pour un fichier. Cet attribut n'est pas valide pour les répertoires.
- **Uid, gid et mode** : indicateurs d'autorisation pour Linux.

Copier pour objets

Vous ne pouvez pas modifier cette option après avoir créé la relation.

Fichiers récemment modifiés

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

Supprimer des fichiers sur la source

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

Si vous activez cette option, vous devez également modifier un paramètre dans le fichier local.json du courtier de données. Ouvrez le fichier et mettez-le à jour comme suit :

```
{
  "workers": {
    "transferrer": {
      "delete-on-source": true
    }
  }
}
```

Supprimer des fichiers sur la cible

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

Types de fichiers

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

Exclure les extensions de fichier

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

► https://docs.netapp.com/fr-fr/cloud-manager-sync//media/video_file_extensions.mp4 (video)

Taille du fichier

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

Date de modification

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

Date de création

Lorsqu'un serveur SMB est source, ce paramètre vous permet de synchroniser les fichiers créés après une date spécifique, avant une date spécifique ou entre une plage horaire spécifique.

ACL - liste de contrôle d'accès

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


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

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

Suppression de relations

Vous pouvez supprimer une relation de synchronisation si vous n'avez plus besoin de synchroniser les données entre la source et la cible. Cette action ne supprime pas le groupe du courtier de données (ou les instances individuelles du courtier de données) et ne supprime pas les données de la cible.

Étapes

1. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur 
2. Cliquez sur **Supprimer**, puis cliquez à nouveau sur **Supprimer** pour confirmer.

Cloud Sync supprime la relation de synchronisation.

Gérez les groupes de courtiers de données

Un groupe de courtier de données synchronise les données d'un emplacement source vers un emplacement cible. Au moins un courtier de données est requis dans un groupe pour chaque relation de synchronisation que vous créez. Gérer les groupes de courtiers de données en ajoutant un nouveau courtier de données à un groupe, en affichant des informations sur les groupes, etc.

Fonctionnement des groupes de courtiers de données

Un groupe de courtiers de données peut comprendre un ou plusieurs courtiers de données. Le regroupement de courtiers de données entre eux permet d'améliorer les performances des relations de synchronisation.

Les groupes peuvent gérer plusieurs relations

Un groupe de courtiers de données peut gérer une ou plusieurs relations synchronisées à la fois.

Imaginons par exemple que vous ayez trois relations :

- La relation 1 est gérée par le groupe de courtiers de données A
- La relation 2 est gérée par le groupe de courtiers de données B
- La relation 3 est gérée par le groupe de courtiers de données A.

Vous voulez accélérer les performances de la relation 1 pour ajouter un nouveau courtier de données au groupe de courtier de données A. Dans la mesure où le groupe A gère également la relation de synchronisation 3, les performances de synchronisation de la relation sont également automatiquement accélérées.

Nombre de courtiers de données dans un groupe

Dans de nombreux cas, un seul courtier de données peut répondre aux exigences de performance d'une relation de synchronisation. Si ce n'est pas le cas, vous pouvez accélérer les performances de synchronisation en ajoutant des courtiers de données supplémentaires au groupe. Mais vous devez d'abord vérifier d'autres facteurs qui peuvent avoir un impact sur les performances de synchronisation. ["En savoir plus sur la façon de déterminer si plusieurs courtiers de données sont nécessaires"](#).

Recommandations en matière de sécurité

Pour assurer la sécurité de votre courtier en données, NetApp recommande les éléments suivants :

- SSH ne doit pas autoriser X11 Forwarding
- SSH ne doit pas autoriser le transfert de connexion TCP
- SSH ne doit pas autoriser les tunnels
- SSH ne doit pas accepter les variables d'environnement client

Ces recommandations de sécurité peuvent aider à empêcher toute connexion non autorisée à la machine du courtier de données.

Ajouter un nouveau courtier de données à un groupe

Il existe plusieurs façons de créer un nouveau courtier de données :

- Lors de la création d'une nouvelle relation de synchronisation

["Découvrez comment créer un nouveau courtier de données lors de la création d'une relation de synchronisation"](#).

- Dans la page **gérer les courtiers de données** en cliquant sur **Ajouter un nouveau courtier de données** qui crée le courtier de données dans un nouveau groupe

- À partir de la page **gérer les courtiers de données** en créant un nouveau courtier de données dans un groupe existant

Avant de commencer

- Vous ne pouvez pas ajouter de courtiers de données à un groupe qui gère une relation de synchronisation chiffrée.
- Si vous souhaitez créer un courtier en données au sein d'un groupe existant, le courtier en données doit être un courtier en données sur site ou le même type de courtier.

Par exemple, si un groupe inclut un courtier en données AWS, vous pouvez créer un courtier en données AWS ou un courtier en données sur site dans ce groupe. Vous ne pouvez pas créer de courtier en données Azure ou de courtier en données Google Cloud, car ils ne sont pas le même type de courtier.

Étapes pour créer un courtier de données dans un nouveau groupe

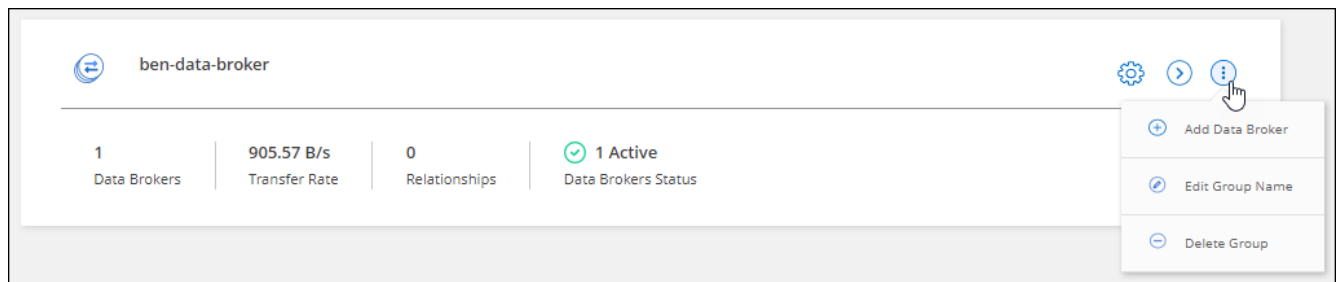
1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur **Ajouter un nouveau courtier de données**.
3. Suivez les invites pour créer le courtier de données.

Pour obtenir de l'aide, reportez-vous aux pages suivantes :

- ["Créer un courtier en données dans AWS"](#)
- ["Créer un courtier en données dans Azure"](#)
- ["Créer un courtier en données dans Google Cloud"](#)
- ["Installation du data broker sur un hôte Linux"](#)

Étapes pour créer un courtier de données dans un groupe existant

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur le menu d'action et sélectionnez **Ajouter un courtier de données**.



3. Suivez les invites pour créer le courtier de données dans le groupe.

Pour obtenir de l'aide, reportez-vous aux pages suivantes :

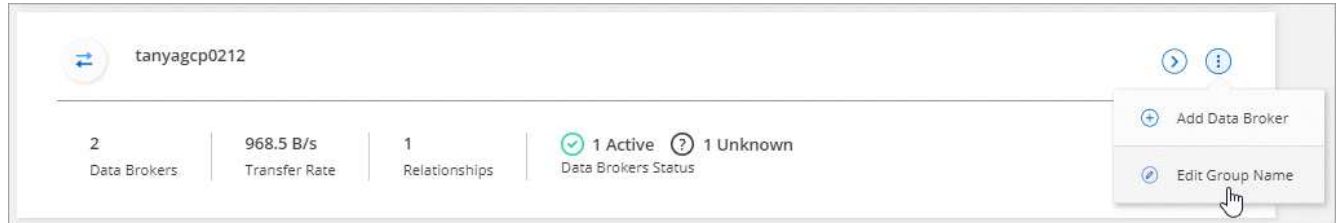
- ["Créer un courtier en données dans AWS"](#)
- ["Créer un courtier en données dans Azure"](#)
- ["Créer un courtier en données dans Google Cloud"](#)
- ["Installation du data broker sur un hôte Linux"](#)

Modifier le nom d'un groupe

Modifier le nom d'un groupe de courtiers de données à tout moment.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur le menu d'action et sélectionnez **Modifier le nom du groupe**.



3. Entrez un nouveau nom et cliquez sur **Enregistrer**.

Cloud Sync met à jour le nom du groupe de courtiers de données.

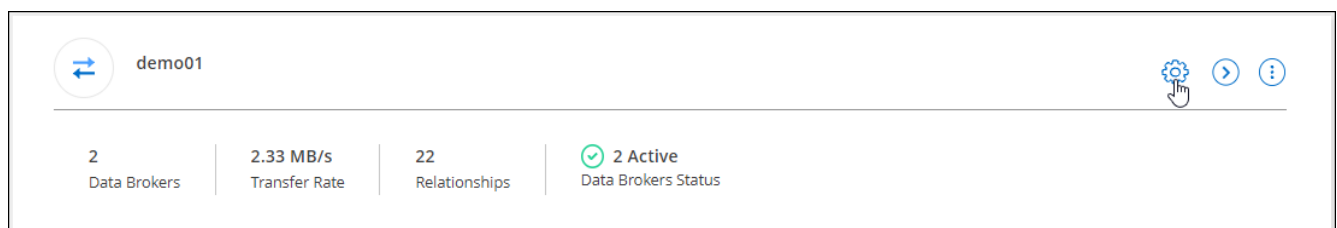
Configurez une configuration unifiée

Si une relation de synchronisation rencontre des erreurs lors du processus de synchronisation, l'unification de la simultanéité du groupe de courtiers de données peut aider à diminuer le nombre d'erreurs de synchronisation. Notez que les modifications apportées à la configuration du groupe peuvent affecter les performances en ralentissant le transfert.

Nous ne recommandons pas de modifier par vous-même la configuration. Consultez NetApp pour savoir quand modifier la configuration et comment la modifier.

Étapes

1. Cliquez sur **gérer les courtiers de données**.
2. Cliquez sur l'icône Paramètres d'un groupe de courtiers de données.



3. Modifiez les paramètres selon vos besoins, puis cliquez sur **Unify Configuration**.

Notez ce qui suit :

- Vous pouvez choisir les paramètres à modifier, mais vous n'avez pas besoin de les modifier simultanément.
- Une fois qu'une nouvelle configuration est envoyée à un courtier de données, le courtier redémarre automatiquement et utilise la nouvelle configuration.
- Un délai peut s'effectuer jusqu'à ce que cette modification soit visible dans l'interface de Cloud Sync.
- Si un courtier de données n'est pas en cours d'exécution, sa configuration ne change pas, car Cloud Sync ne peut pas communiquer avec lui. La configuration change après le redémarrage du courtier de

données.

- Une fois la configuration unifiée définie, tous les nouveaux courtiers de données utilisent automatiquement la nouvelle configuration.

Déplacez les courtiers de données d'un groupe à l'autre


Déplacez un courtier de données d'un groupe à un autre si vous avez besoin d'accélérer les performances du groupe de courtiers de données cible.

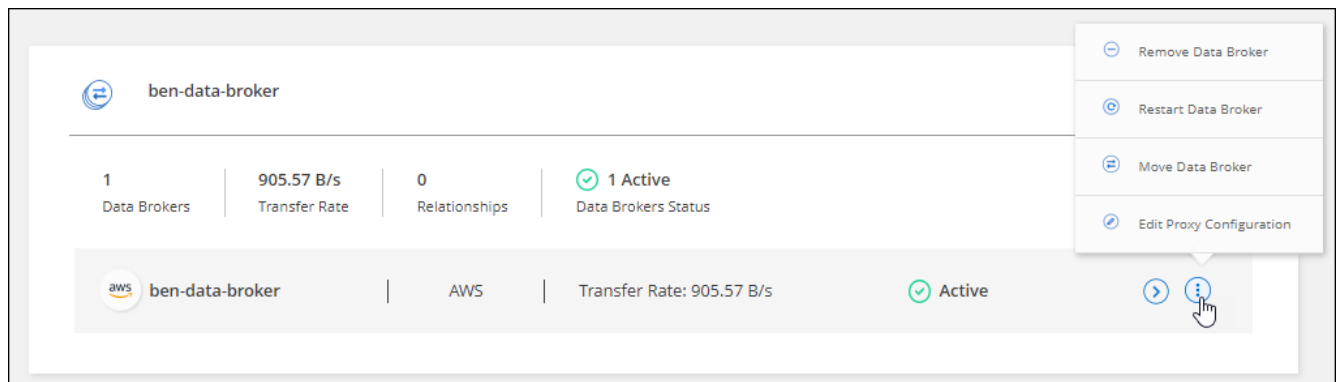
Par exemple, si un courtier de données ne gère plus une relation synchrone, vous pouvez facilement la déplacer vers un autre groupe gérant les relations de synchronisation.

Limites

- Si un groupe de courtiers de données gère une relation de synchronisation et qu'il n'y a qu'un seul courtier de données dans le groupe, vous ne pouvez pas transférer ce courtier de données vers un autre groupe.
- Vous ne pouvez pas déplacer un courtier de données vers ou depuis un groupe qui gère les relations de synchronisation chiffrées.
- Vous ne pouvez pas déplacer un courtier en données actuellement déployé.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur le menu d'action d'un courtier de données et sélectionnez **déplacer le courtier de données**.



4. Créez un nouveau groupe de courtiers de données ou sélectionnez un groupe de courtiers de données existant.
5. Cliquez sur **déplacer**.


Cloud Sync déplace le courtier en données vers un groupe de courtiers de données nouveau ou existant. S'il n'y a pas d'autres courtiers de données dans le groupe précédent, Cloud Sync le supprime.

Mettre à jour la configuration du proxy

Mettez à jour la configuration du proxy pour un courtier de données en ajoutant des détails sur une nouvelle configuration de proxy ou en modifiant la configuration de proxy existante.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.

2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur le menu d'action d'un courtier de données et sélectionnez **Modifier la configuration du proxy**.
4. Spécifiez des détails sur le proxy : nom d'hôte, numéro de port, nom d'utilisateur et mot de passe.
5. Cliquez sur **mettre à jour**.

Cloud Sync met à jour le courtier de données pour utiliser la configuration proxy pour l'accès à Internet.

Afficher la configuration d'un courtier de données

Vous pouvez consulter des détails sur un courtier de données pour identifier des éléments tels que son nom d'hôte, son adresse IP, son CPU et sa mémoire vive disponibles, etc.



Cloud Sync fournit les informations suivantes concernant un courtier en données :

- Informations de base : ID d'instance, nom d'hôte, etc
- Réseau : région, réseau, sous-réseau, IP privée, etc
- Logiciel : distribution Linux, version de courtier de données, etc
- Matériel : processeur et RAM
- Configuration : détails sur les deux types de processus principaux du courtier de données : scanner et transfert



Le scanner numérise la source et la cible et décide de ce qui doit être copié. Le transfert effectue la copie réelle. L'équipe NetApp peut utiliser ces détails de configuration pour suggérer des actions permettant d'optimiser les performances.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur  pour afficher les détails d'un courtier de données.

tanyagcp0212

2 Data Brokers | 968.5 B/s Transfer Rate | 1 Relationships | 1 Active 1 Unknown Data Brokers Status

	tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active	
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project Id	
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP	
Software	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version	
Hardware	4 Available CPUs	62.22 MB Available RAM			
Configuration	50 Scanner Concurrency	4 Scanner CPUs	50 Transferer Concurrency	4 Transferer CPUs	

Résoudre les problèmes avec un courtier de données

Cloud Sync affiche un statut pour chaque courtier de données qui peut vous aider à résoudre les problèmes.

Étapes

1. Identifiez tous les courtiers de données dont l'état est « Inconnu » ou « en échec ».

tanyagcp0212

2 Data Brokers | 968.5 B/s Transfer Rate | 1 Relationships | 1 Active 1 Unknown Data Brokers Status

tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active	
tanya1	ONPREM	Transfer Rate: N/A	Unknown	

2. Placez le pointeur de la souris sur le pour voir la raison de l'échec.
3. Corrigez le problème.

Par exemple, vous devrez peut-être redémarrer le courtier en données si celui-ci est hors ligne, ou supprimer le courtier en données si le déploiement initial a échoué.

Supprimer un courtier de données d'un groupe


Vous pouvez supprimer un courtier de données d'un groupe s'il n'est plus nécessaire ou si le déploiement

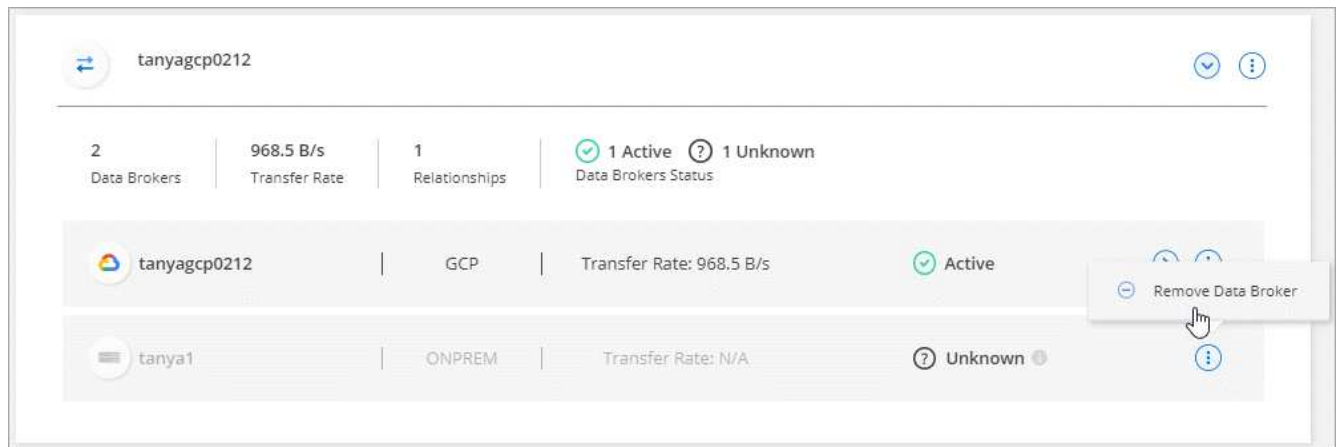
initial a échoué. Cette action supprime uniquement le courtier en données des enregistrements de Cloud Sync. Vous devrez supprimer manuellement le courtier en données et toutes les ressources cloud supplémentaires.

Ce que vous devez savoir

- Cloud Sync supprime un groupe lorsque vous supprimez le dernier courtier de données du groupe.
- Vous ne pouvez pas supprimer le dernier courtier de données d'un groupe s'il existe une relation utilisant ce groupe.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur le menu d'action d'un courtier de données et sélectionnez **Supprimer le courtier de données**.



4. Cliquez sur **Supprimer le courtier de données**.

Cloud Sync supprime le courtier de données du groupe.

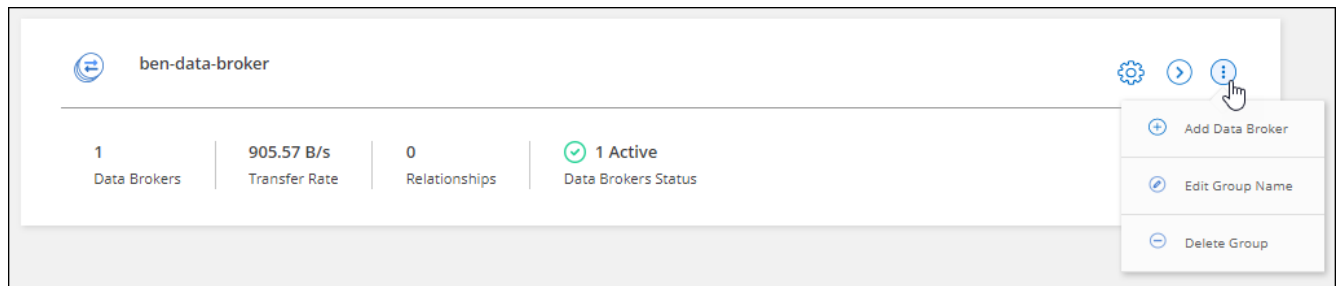
Supprimer un groupe de courtier de données

Si un groupe de courtiers de données ne gère plus de relations de synchronisation, vous pouvez supprimer le groupe, qui supprime tous les courtiers de données de Cloud Sync.

Les courtiers de données supprimés par Cloud Sync ne sont supprimés que des enregistrements de Cloud Sync. Vous devrez supprimer manuellement l'instance de courtier en données de votre fournisseur de cloud, ainsi que toutes les ressources cloud supplémentaires.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur le menu d'action et sélectionnez **Supprimer le groupe**.



3. Pour confirmer, entrez le nom du groupe et cliquez sur **Supprimer le groupe**.

Cloud Sync supprime les courtiers de données et supprime le groupe.

Création et affichage de rapports pour ajuster votre configuration

Créez et consultez des rapports pour obtenir des informations utiles avec l'aide du personnel NetApp afin de régler la configuration d'un courtier de données et d'améliorer les performances.

Chaque rapport fournit des détails détaillés sur un chemin dans une relation de synchronisation. Par exemple, le rapport d'un système de fichiers indique le nombre de répertoires et de fichiers qu'il y a, la répartition de la taille du fichier, la profondeur et la largeur des répertoires, et plus encore.

Création de rapports

Chaque fois que vous créez un rapport, Cloud Sync analyse le chemin, puis compile les informations dans un rapport.

Étapes

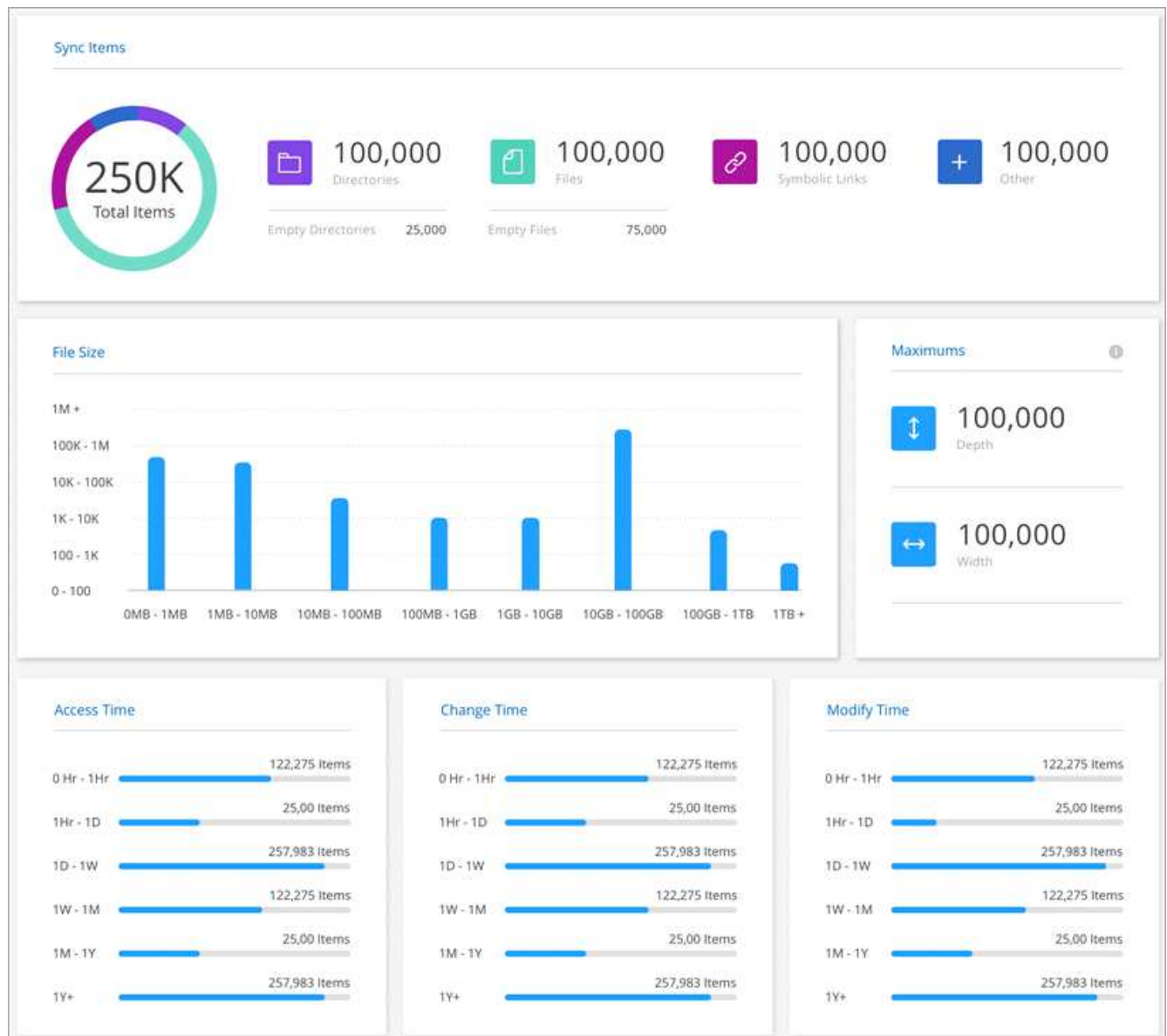
1. Cliquez sur **Sync > Rapports**.

Les chemins (source ou cible) de chacune de vos relations de synchronisation s'affichent dans une table.

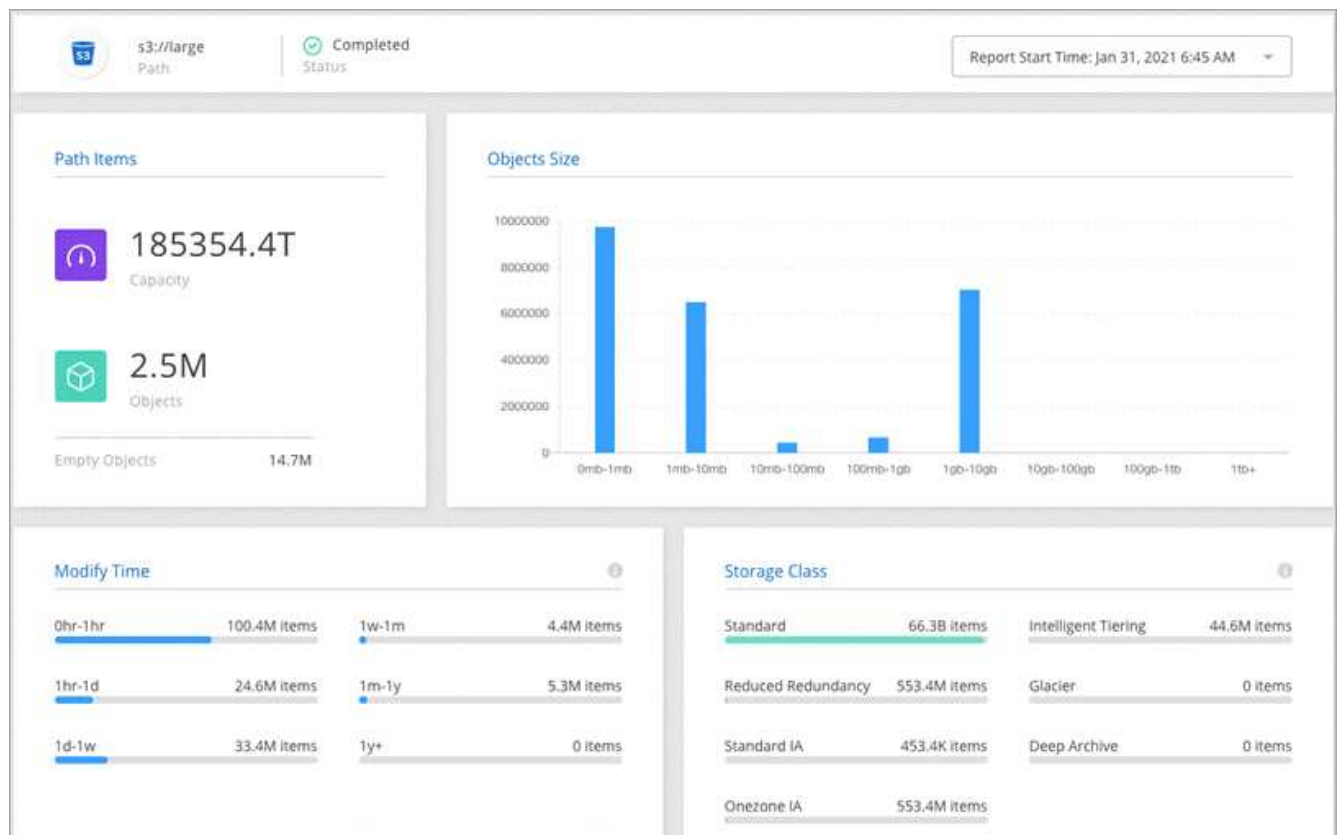
2. Dans la colonne **Rapports actions**, allez à un chemin spécifique et cliquez sur **Créer**, ou cliquez sur le menu d'action et sélectionnez **Créer nouveau**.

3. Lorsque le rapport est prêt, cliquez sur le menu d'action et sélectionnez **Affichage**.

Voici un exemple de rapport pour un chemin de système de fichiers.



Et voici un exemple de rapport sur le stockage objet.

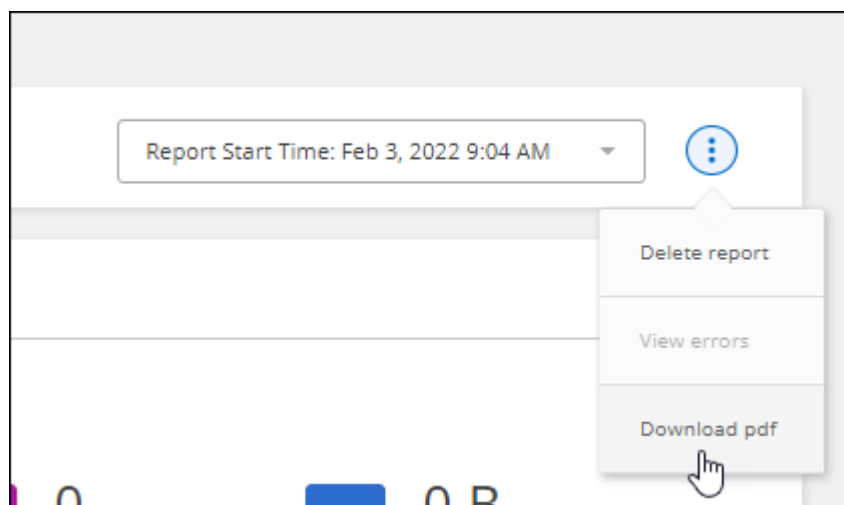


Téléchargement de rapports

Vous pouvez télécharger un rapport au format PDF pour le visualiser hors ligne ou le partager.

Étapes

1. Cliquez sur **Sync > Rapports**.
2. Dans la colonne **Rapports actions**, cliquez sur le menu d'action et sélectionnez **Affichage**.
3. Dans le coin supérieur droit du rapport, cliquez sur le menu d'action et sélectionnez **Télécharger PDF**.



Affichage des erreurs de rapport

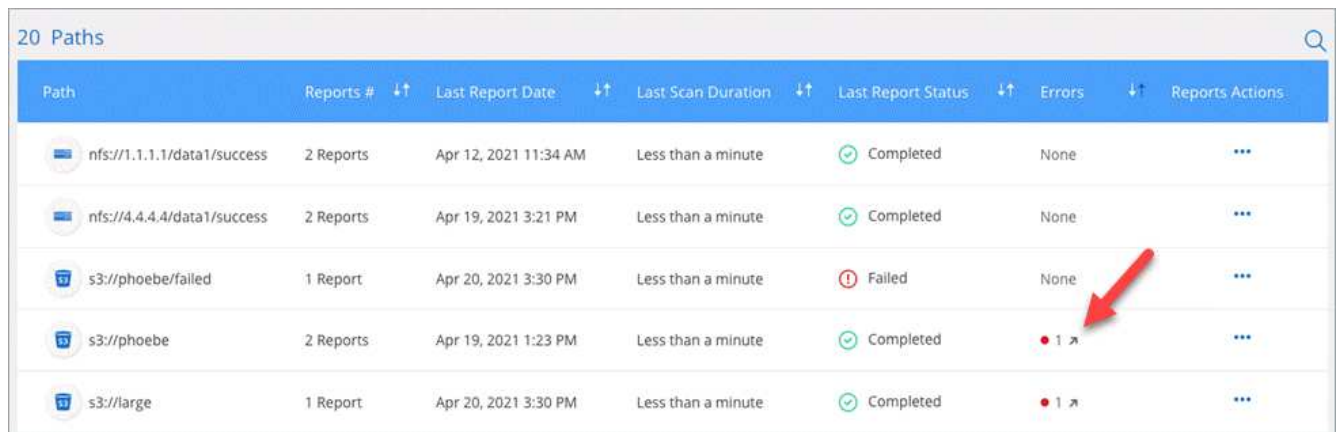
Le tableau chemins identifie si des erreurs sont présentes dans le rapport le plus récent. Une erreur identifie un problème rencontré par Cloud Sync lors de la numérisation du chemin.

Par exemple, un rapport peut contenir des erreurs d'autorisation refusée. Ce type d'erreur peut affecter la capacité de Cloud Sync à analyser l'ensemble des fichiers et des répertoires.

Après avoir vu la liste des erreurs, vous pouvez résoudre les problèmes et exécuter à nouveau le rapport.

Étapes

1. Cliquez sur **Sync > Rapports**.
2. Dans la colonne **erreurs**, identifiez si des erreurs sont présentes dans un rapport.
3. Si des erreurs sont présentes, cliquez sur la flèche en regard du nombre d'erreurs.



Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

4. Utilisez les informations de l'erreur pour corriger le problème.

Après avoir résolu le problème, l'erreur ne devrait pas apparaître lors de la prochaine exécution du rapport.

Suppression de rapports

Vous pouvez supprimer un rapport contenant une erreur que vous avez corrigée ou si le rapport est associé à une relation de synchronisation que vous avez supprimée.

Étapes

1. Cliquez sur **Sync > Rapports**.
2. Dans la colonne **Rapports actions**, cliquez sur le menu d'action d'un chemin et sélectionnez **Supprimer le dernier rapport** ou **Supprimer tous les rapports**.
3. Confirmez que vous souhaitez supprimer le ou les rapports.

Désinstallation du courtier de données

Si nécessaire, exécutez un script de désinstallation pour supprimer le courtier de données et les packages et répertoires créés lors de l'installation du courtier de données.

Étapes

1. Connectez-vous à l'hôte du courtier de données.

2. Accédez au répertoire du courtier de données : `/opt/netapp/databroker`

3. Exécutez les commandes suivantes :

```
chmod +x uninstaller-DataBroker.sh  
./uninstaller-DataBroker.sh
```

4. Appuyez sur 'y' pour confirmer la désinstallation.

API Cloud Sync

Les fonctionnalités de Cloud Sync disponibles via l'interface utilisateur web sont également disponibles via l'API RESTful.

Pour commencer

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

Étapes

1. Obtenez un jeton utilisateur auprès de NetApp BlueXP.

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

2. Obtenez votre identifiant de compte BlueXp.

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

Cette API renvoie une réponse comme suit :

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

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

Exemple

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

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

Que dois-je faire lorsque le jeton expire ?

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

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

Référence API

La documentation de chaque API Cloud Sync est disponible à partir de <https://api.cloudsync.netapp.com/docs>.

Utilisation d'API de liste

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

Étapes

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

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

Exemple

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

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

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

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

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

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

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

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

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

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

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

Concepts

Présentation des licences

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

Abonnement Marketplace

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

Abonnement à l'heure

Avec un abonnement avec paiement à l'heure basé sur l'utilisation, vous payez à l'heure en fonction du nombre de relations de synchronisation que vous créez.

- ["Voir les tarifs à Azure"](#)
- ["Consultez les tarifs à la carte dans AWS"](#)

Abonnement annuel

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

["Voir les tarifs annuels dans AWS"](#)

Licences de NetApp

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

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

["Découvrez comment acheter des licences et les ajouter à Cloud Sync"](#).

Termes de la licence

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

- Les clients ont le droit de tirer parti de la licence BYOL pour une durée maximale d'un an à compter de la date de livraison.
- Les clients ont le droit de tirer parti de la licence BYOL pour établir et ne pas dépasser un total de 20 connexions individuelles entre une source et une cible (chaque " relation de synchronisation ").

- Le droit d'un client expire à la fin de la période d'un an de licence, que le Client ait atteint la limite de 20 relations de synchronisation.
- Si le Client choisit de renouveler sa licence, les relations de synchronisation non utilisées associées à l'octroi de licence précédent ne passent PAS au renouvellement de la licence.

Confidentialité des données

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

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

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

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

FAQ technique sur Cloud Sync

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

Pour commencer

Les questions suivantes concernent la mise en route de Cloud Sync.

Comment fonctionne Cloud Sync ?

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

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

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

Comment fonctionne l'essai gratuit de 14 jours ?

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

Combien coûte Cloud Sync ?

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

Frais de service

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

- ["Consultez les tarifs à la carte dans AWS"](#)
- ["Voir les tarifs annuels dans AWS"](#)
- ["Voir les tarifs à Azure"](#)

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

["En savoir plus sur les licences"](#).



Les relations Cloud Sync sont gratuites pour Cloud Volumes Service et Azure NetApp Files.

Frais de ressources

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

Comment le service Cloud Sync est-il facturé ?

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

Puis-je utiliser Cloud Sync en dehors du cloud ?

Oui, vous pouvez utiliser Cloud Sync dans une architecture non cloud. La source et la cible peuvent résider sur le site, de sorte que le logiciel de courtier en données peut être utilisé.

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

- Un groupe de courtiers de données a besoin d'une connexion Internet pour communiquer avec le service Cloud Sync.
- Si vous n'achetez pas de licence directement auprès de NetApp, vous devrez acquérir un compte AWS ou Azure pour la facturation du service PAYGO Cloud Sync.

Comment accéder à Cloud Sync ?

Cloud Sync est disponible sur le site Web BlueXP dans l'onglet **Sync**.

Qu'est-ce qu'un groupe de courtiers de données ?

Chaque courtier appartient à un groupe de courtier en données. Le regroupement de courtiers de données permet d'améliorer les performances des relations synchronisées.

Sources et cibles prises en charge

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

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

Cloud Sync prend en charge de nombreux types de relations de synchronisation. ["Afficher la liste complète"](#).

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

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

["En savoir plus sur les exigences de synchronisation"](#).

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

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

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

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

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

- Stockage à chaud
- Stockage cool

Prenez-vous en charge les tiers de stockage Google Cloud ?

Oui, vous pouvez choisir une classe de stockage spécifique lorsqu'un compartiment Google Cloud Storage est la cible :

- Standard
- Nearline
- Ligne de refroidissement
- Archivage

Mise en réseau

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

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

L'environnement Cloud Sync requiert qu'un groupe de courtier soit connecté à la source et à la cible à l'aide du protocole ou de l'API de stockage objet sélectionné (Amazon S3, Azure Blob, IBM Cloud Object Storage).

De plus, un groupe de courtiers de données a besoin d'une connexion Internet sortante sur le port 443 afin de pouvoir communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels.

Pour en savoir plus, ["examiner les besoins en matière de mise en réseau"](#).

Puis-je utiliser un serveur proxy avec le courtier de données ?

Oui.

Cloud Sync prend en charge les serveurs proxy avec ou sans authentification de base. Si vous spécifiez un serveur proxy lorsque vous déployez un courtier de données, tout le trafic HTTP et HTTPS du courtier de données est acheminé via le proxy. Notez que le trafic non HTTP tel que NFS ou SMB ne peut pas être routé via un serveur proxy.

La seule limitation du serveur proxy est liée au chiffrement des données à la volée avec une relation de synchronisation NFS ou Azure NetApp Files. Les données cryptées sont envoyées via HTTPS et ne sont pas routables via un serveur proxy.

Synchronisation des données

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

À quelle fréquence la synchronisation se produit-elle ?

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

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

Quel est le programme de synchronisation minimal ?

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

Le groupe de courtier de données est-il réessaie-t-il lorsqu'un fichier ne se synchronise pas ? Ou est-ce que ce délai ?

Un groupe de courtiers de données n'expire pas lorsqu'un seul fichier ne parvient pas à être transféré. Le groupe de courtiers de données tente 3 fois de nouveau avant de sauter le fichier. La valeur de la nouvelle tentative est configurable dans les paramètres d'une relation de synchronisation.

["Découvrez comment modifier les paramètres d'une relation de synchronisation"](#).

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

Si un seul répertoire contient 600,000 fichiers ou plus, [contactez-nous](#) pour que nous puissions vous aider à configurer le groupe de courtiers de données pour gérer la charge utile. Il nous faudra peut-être ajouter de la mémoire au groupe de courtiers de données.

Notez que le nombre total de fichiers dans le point de montage n'est pas limité. La mémoire supplémentaire est requise pour les grands répertoires contenant 600,000 fichiers ou plus, quel que soit leur niveau dans la hiérarchie (répertoire supérieur ou sous-répertoire).

Sécurité

Les questions suivantes ont trait à la sécurité.

Cloud Sync est-il sécurisé ?

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

Toutes les communications entre le groupe de courtier en données et Amazon S3, Azure Blob, Google Cloud Storage et IBM Cloud Object Storage sont effectuées via le protocole HTTPS.

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

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

Chacune de ces méthodes établit une connexion sécurisée entre vos serveurs NAS sur site et un groupe de courtiers de données Cloud Sync.

Les données sont-elles chiffrées par Cloud Sync ?

- Cloud Sync prend en charge le chiffrement des données en vol entre les serveurs NFS source et cible. ["En savoir plus >>"](#).
- Pour SMB, Cloud Sync prend en charge les données SMB 3.0 et 3.11 chiffrées côté serveur. Cloud Sync copie les données chiffrées de la source vers la cible, où elles restent chiffrées.

Cloud Sync ne peut pas chiffrer les données SMB lui-même.

- Lorsqu'un compartiment Amazon S3 est la cible d'une relation synchrone, vous pouvez choisir d'activer le chiffrement des données à l'aide du chiffrement AWS KMS ou AES-256.

Autorisations

Les questions suivantes concernent les autorisations de données.

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

Vous pouvez configurer Cloud Sync pour maintenir les listes de contrôle d'accès (ACL) entre un partage SMB source et un partage SMB cible, et entre un partage SMB source et un stockage objet (à l'exception de ONTAP S3).



Cloud Sync ne prend pas en charge la copie de listes de contrôle d'accès depuis le stockage objet vers les partages SMB.

["Découvrez comment copier des listes de contrôle d'accès entre partages SMB".](#)

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

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

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

Métadonnées de stockage objet

Cloud Sync copie les métadonnées de stockage objet de la source vers la cible pour les types de relations de synchronisation suivants :

- Amazon S3 → Amazon S3 ¹
- Amazon S3 → StorageGRID
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID
- StorageGRID → Google Cloud Storage
- Google Cloud Storage → StorageGRID ¹
- Google Cloud Storage → stockage objet cloud IBM ¹
- Google Cloud Storage → Amazon S3 ¹
- Amazon S3 → Google Cloud Storage
- IBM Cloud Object Storage → Google Cloud Storage
- StorageGRID → stockage objet cloud IBM
- IBM Cloud Object Storage → StorageGRID
- IBM Cloud Object Storage → stockage objet cloud IBM

¹ pour ces relations de synchronisation, vous devez le faire ["Activez le paramètre Copier pour les objets lorsque vous créez la relation de synchronisation"](#).

Performance

Les questions suivantes concernent les performances de Cloud Sync.

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

La relation de synchronisation indique le débit de la carte réseau du groupe de courtiers de données. Si vous accélérez les performances de synchronisation en utilisant plusieurs courtiers de données, le débit est la

somme de tout le trafic. Ce débit est actualisé toutes les 20 secondes.

J'éprouve des problèmes de performance. Pouvons-nous limiter le nombre de transferts simultanés ?

Si vous avez des fichiers très volumineux (plusieurs Tbs chacun), le processus de transfert peut prendre beaucoup de temps et les performances peuvent être affectées.

Limiter le nombre de transferts simultanés peut vous aider. [Mailto:ng-cloudsync-support@netapp.com](mailto:ng-cloudsync-support@netapp.com)[Contactez-nous pour obtenir de l'aide].

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

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

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

["En savoir plus sur le débit et les niveaux de service de Azure NetApp Files"](#).

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

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

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

Combien de courtiers de données sont requis dans un groupe ?

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

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

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

Vous pouvez alors envisager d'accélérer la synchronisation en ajoutant un courtier de données supplémentaire à un groupe pour partager la charge de cette relation. ["Découvrez comment accélérer les performances de synchronisation"](#).

Suppression de choses

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

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

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

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

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

["Découvrez comment modifier les paramètres d'une relation de synchronisation"](#).

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

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

Dépannage

["Base de connaissances NetApp : FAQ Cloud Sync : support et dépannage"](#)

Data broker plongez en profondeur

La question suivante concerne le courtier de données.

Pouvez-vous expliquer l'architecture du data broker ?

Bien sûr. Voici les points les plus importants :

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

Connaissances et support

S'inscrire pour obtenir de l'aide

Avant d'ouvrir un dossier de demande de support auprès du support technique NetApp, vous devez ajouter un compte sur le site du support NetApp (NSS) à BlueXP, puis vous inscrire pour obtenir du support.

Présentation de l'inscription au support

Il existe deux types d'inscription pour activer les droits d'assistance :

- Enregistrement de votre abonnement au support pour les identifiants de compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxx se trouve sur la page des ressources de support de BlueXP).

Il sert d'ID d'abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxx).

Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L'enregistrement des deux types de numéros de série offre des fonctionnalités telles que l'ouverture de tickets de support et la génération automatique de tickets.

La façon dont vous vous inscrivez dépend de votre présence ou de votre présence chez un client ou un partenaire nouveau ou existant.

- Client ou partenaire existant

En tant que client ou partenaire NetApp, vous pouvez utiliser votre compte SSO du site de support NetApp pour effectuer les enregistrements suivants. Dans le tableau de bord support, BlueXP fournit une page **NSS Management** où vous pouvez ajouter votre compte NSS. Une fois votre compte NSS ajouté, BlueXP enregistre automatiquement ces numéros de série pour vous.

an NSS account to BlueXP, Découvrez comment ajouter votre compte NSS.

- Nouveaux partenaires NetApp

Si vous êtes nouveau chez NetApp, vous devez enregistrer votre numéro de série BlueXP sur le site d'inscription du support NetApp. Une fois que vous avez terminé cette inscription et créé un nouveau compte NSS, vous pouvez utiliser ce compte dans BlueXP pour vous inscrire automatiquement à l'avenir.

with NetApp, Découvrez comment vous inscrire auprès de NetApp.

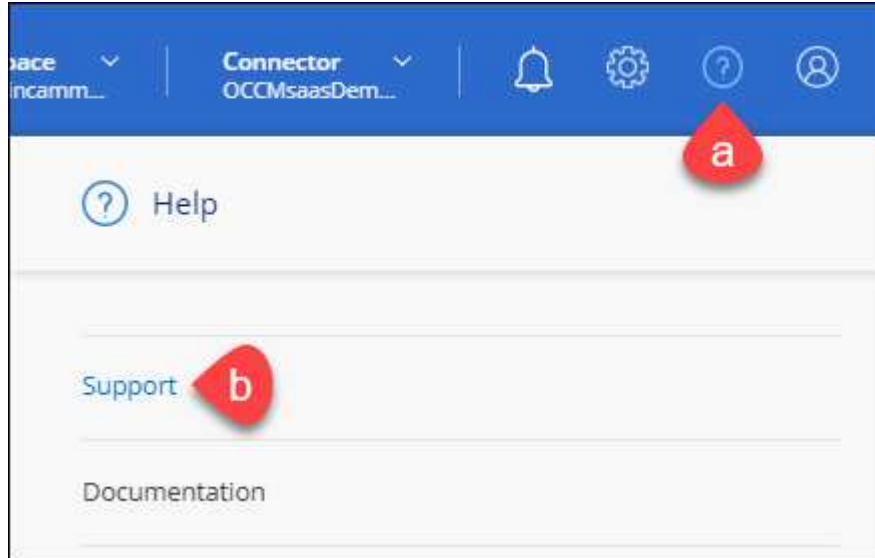
Ajouter un compte NSS à BlueXP

Le tableau de bord du support vous permet d'ajouter et de gérer vos comptes du site de support NetApp pour les utiliser avec Cloud Manager.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

Notez ce qui suit :

- Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
- Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS. Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du **...** menu.
- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le **...** menu. Cette option vous invite à vous reconnecter.

Inscrivez-vous auprès de NetApp

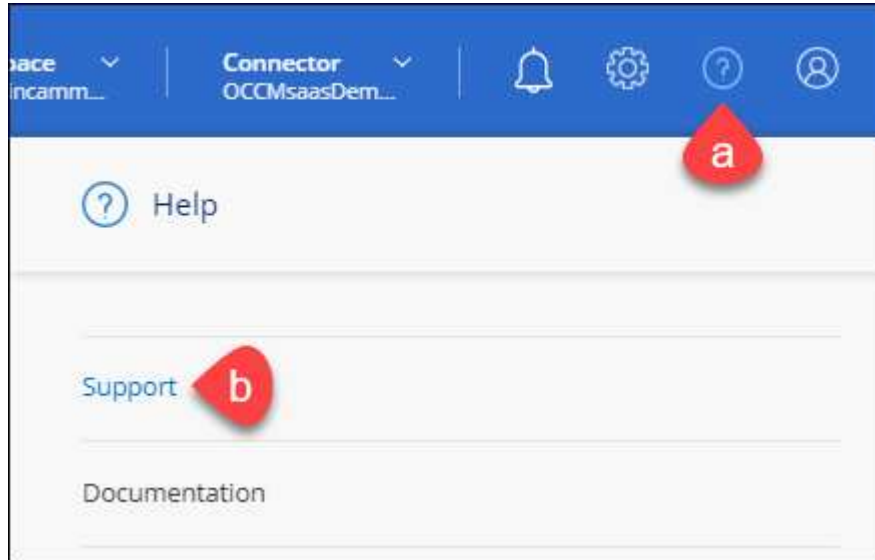
Le fait de vous inscrire au support NetApp dépend de la présence ou non d'un compte sur le site de support NetApp (NSS).

Client existant avec un compte NSS

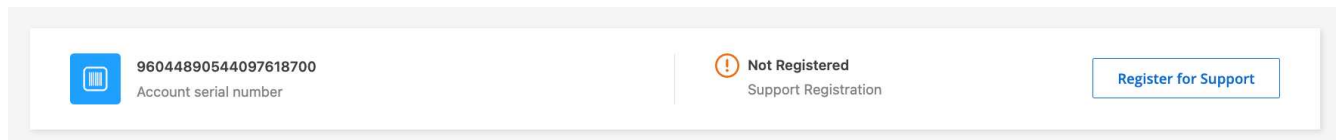
Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Si ce n'est déjà fait, ajoutez votre compte NSS à BlueXP.
3. Sur la page **Ressources**, cliquez sur **s'inscrire au support**.



Client existant mais aucun compte NSS

Si vous êtes déjà client NetApp avec des licences et des numéros de série existants mais que *no* NSS, il vous suffit de créer un compte NSS.

Étapes

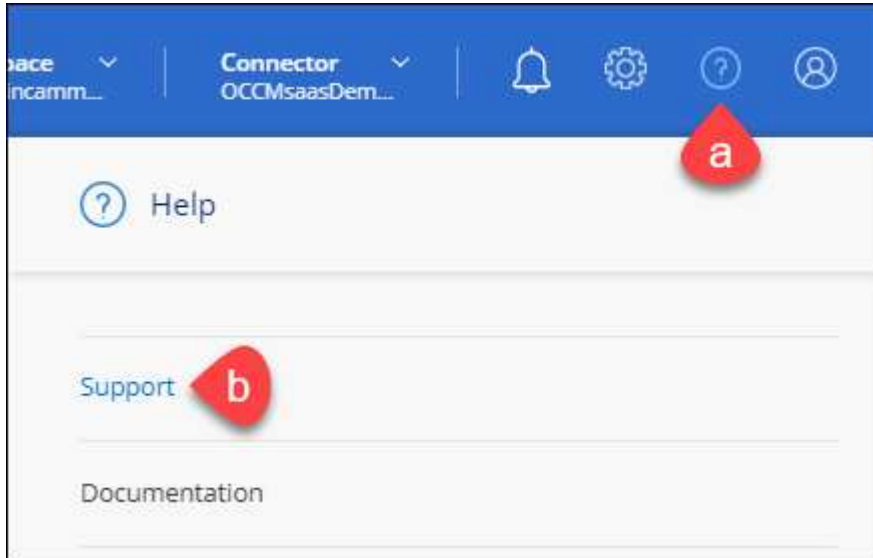
1. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
 - b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

Découvrez la toute nouvelle gamme NetApp

Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Recherchez le numéro de série de votre compte Cloud Manager sur la page d'inscription au support.



3. Accédez à "[Site d'inscription au support NetApp](#)" Et sélectionnez **je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte Cloud Manager depuis l'étape 2 ci-dessus, vérifiez la sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

La confirmation de la soumission de votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp.

8. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.

- b. Veillez à copier le numéro de série du compte Cloud Manager (960xxxx) utilisé ci-dessus pour le numéro de série. Le traitement du compte sera ainsi accéléré.

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois votre compte sur le site de support NetApp, vous pouvez accéder à BlueXP et ajouter ce compte NSS pour les inscriptions futures.

Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

Auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- ["Base de connaissances"](#)

Recherchez dans la base de connaissances BlueXP des articles utiles pour résoudre les problèmes.

- ["Communautés"](#)

Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

- Documentation

La documentation BlueXP que vous consultez actuellement.

- Courrier électronique : ng-cloudmanager-feedback@netapp.com[E-mail de commentaires]

Nous accordons une grande importance à vos commentaires. Envoyez vos commentaires pour nous aider à améliorer BlueXP.

Support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Pour utiliser la fonction **Créer un cas**, vous devez d'abord effectuer un enregistrement unique de votre numéro de série d'ID de compte BlueXP (par exemple 960xxxx) avec NetApp. ["Découvrez comment vous inscrire à de l'aide"](#).

Étapes

1. Dans BlueXP, cliquez sur **aide > support**.
2. Choisissez l'une des options disponibles sous support technique :
 - a. Cliquez sur **appelez-nous** si vous souhaitez parler avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.
 - b. Cliquez sur **Créer un dossier** pour ouvrir un dossier auprès des spécialistes du support NetApp :

- **Compte sur le site de support NetApp** : sélectionnez le compte NSS applicable associé à la personne qui ouvre le dossier de support. Cette personne sera le contact principal avec NetApp en plus de l'e-mail ci-dessous.

Si vous ne voyez pas votre compte NSS, vous pouvez accéder à l'onglet **NSS Management** de la section support de BlueXP pour l'ajouter.

- **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
- **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.


La liste des environnements de travail est comprise dans le cadre du compte, de l'espace de travail et du connecteur BlueXP que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information située à côté du nom du champ.


- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.

Create a Case


TESTCLOUD2NTAP 


NetApp Support Site Account


Service

Cloud Manager 

Working Environment


Select... 

Case Priority 


Low- General Guidance 

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected 

Une fenêtre contextuelle contenant votre numéro de dossier de support s’affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour consulter l’historique de vos dossiers d’assistance, vous pouvez cliquer sur **Paramètres > Chronologie** et rechercher les actions nommées "Créer un dossier de support". Un bouton à l’extrême droite vous permet de développer l’action pour voir les détails.

Il est possible que vous rencontriez le message d’erreur suivant lors de la création d’un dossier :

« Vous n’êtes pas autorisé à créer un dossier pour le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d’enregistrement auquel il est associé n’est pas la même société d’enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l’environnement de travail. Vous pouvez consulter votre liste de comptes NSS en haut du

formulaire **Créer un dossier** pour trouver la correspondance appropriée, ou vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à <https://mysupport.netapp.com/site/help>

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

<http://www.netapp.com/us/legal/copyright.aspx>

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/us/media/patents-page.pdf>

Politique de confidentialité

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

["Avis pour Cloud Sync"](#)

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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