



Copiar e sincronizar dados

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

- Copiar e sincronizar dados 1
 - Visão geral do Cloud Sync 1
 - Comece agora 4
- Tutoriais 36
- Gerenciando relacionamentos de sincronização 42
- APIs da Cloud Sync 47
- Perguntas frequentes técnicas do Cloud Sync 50

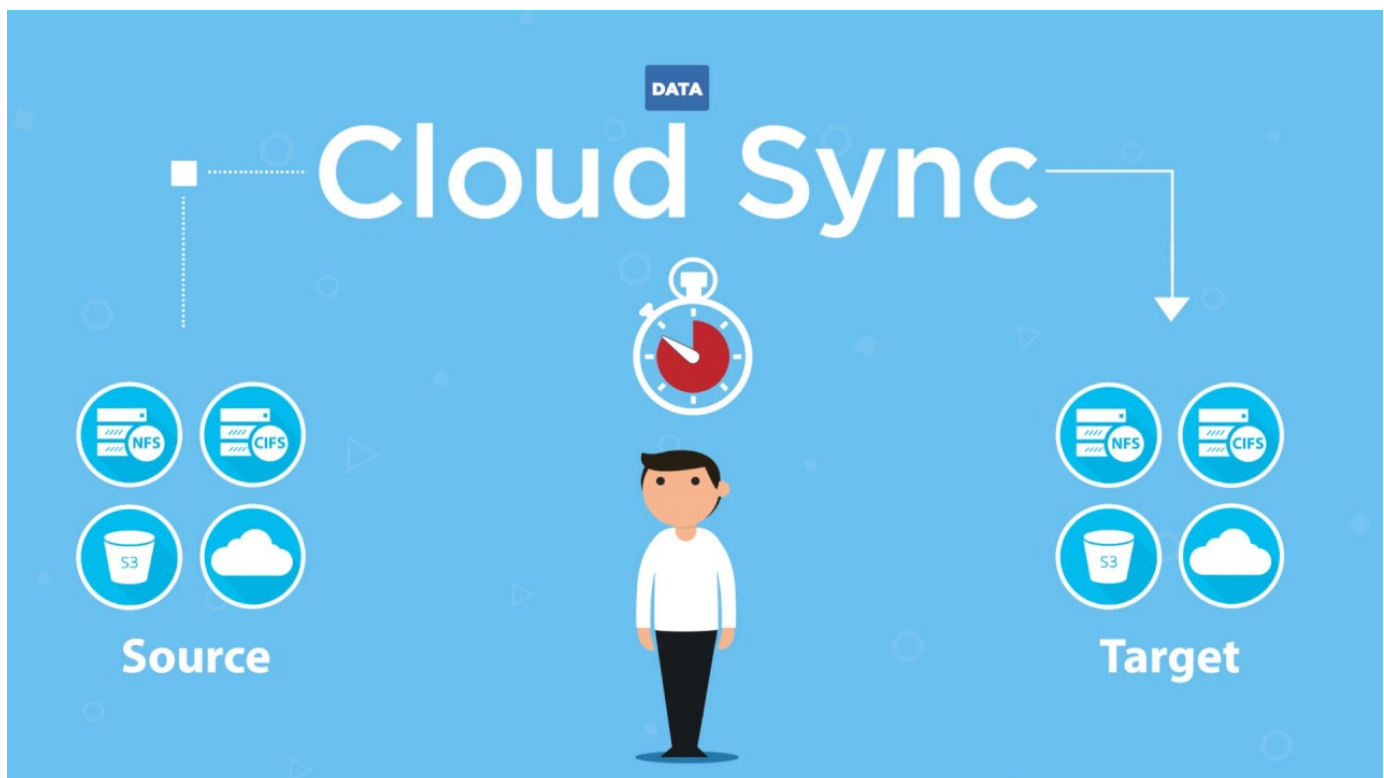
Copiar e sincronizar dados

Visão geral do Cloud Sync

O serviço NetApp Cloud Sync oferece uma maneira simples, segura e automatizada de migrar seus dados para qualquer destino, na nuvem ou no local. Seja um conjunto de dados nas baseado em arquivo (NFS ou SMB), formato de objeto Amazon Simple Storage Service (S3), um dispositivo NetApp StorageGRID ou qualquer outro armazenamento de objetos de fornecedor de nuvem, o Cloud Sync pode convertê-lo e movê-lo para você.

Caraterísticas

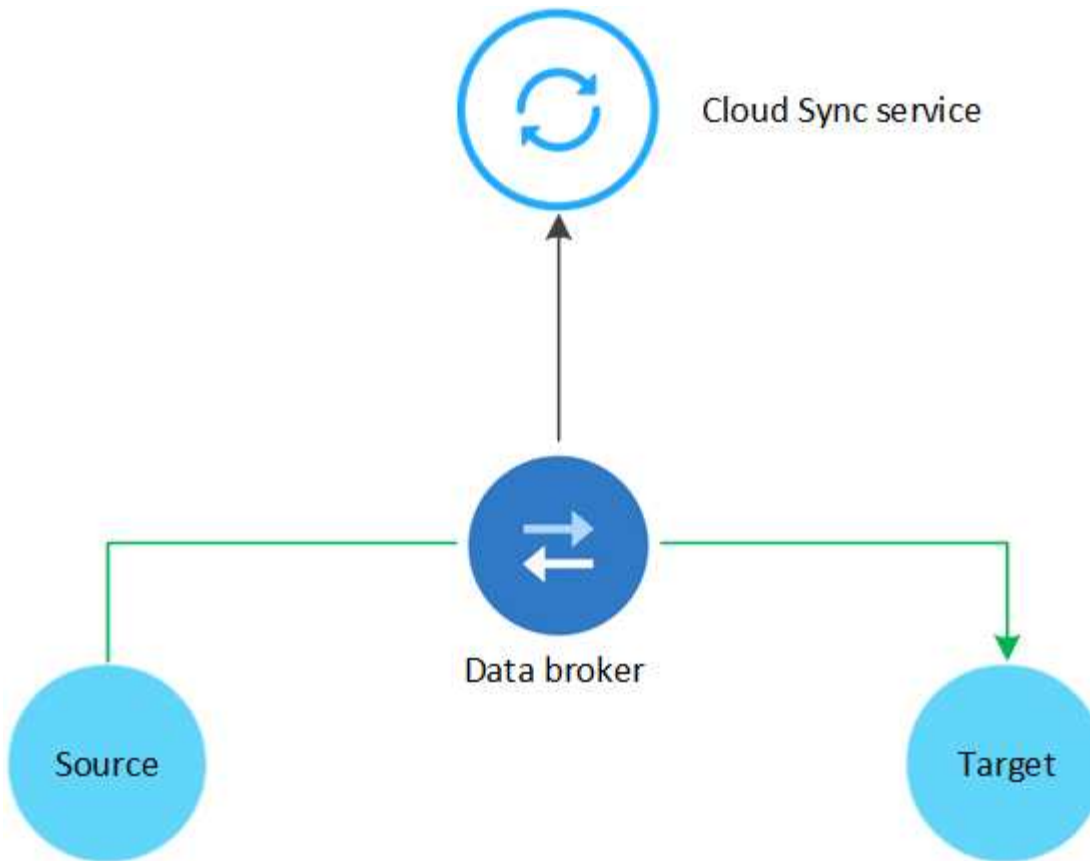
Assista ao vídeo a seguir para uma visão geral do Cloud Sync:



Como o Cloud Sync funciona

O Cloud Sync é uma plataforma de software como serviço (SaaS) que consiste em um agente de dados, uma interface baseada em nuvem disponível pelo Cloud Manager e uma fonte e destino.

A imagem a seguir mostra a relação entre os componentes do Cloud Sync:



O software de corretor de dados NetApp sincroniza dados de uma origem para um destino (isso é chamado de *relação de sincronização*). Você pode executar o agente de dados na AWS, Azure, Google Cloud Platform ou no local. O corretor de dados precisa de uma conexão de saída de Internet pela porta 443 para que possa se comunicar com o serviço Cloud Sync e entrar em Contato com alguns outros serviços e repositórios. ["Exibir a lista de endpoints"](#).

Após a cópia inicial, o serviço sincroniza todos os dados alterados com base na programação definida.

Tipos de armazenamento suportados

O Cloud Sync é compatível com os seguintes tipos de storage:

- Qualquer servidor NFS
- Qualquer servidor SMB
- AWS EFS
- AWS S3
- Blob do Azure
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- IBM Cloud Object Storage
- Cluster ONTAP on-premises

- Storage ONTAP S3
- StorageGRID

["Reveja as relações de sincronização suportadas"](#).

Custo

Existem dois tipos de custos associados ao uso do Cloud Sync: Taxas de recursos e taxas de serviço.

Cobranças de recursos

As cobranças de recursos estão relacionadas aos custos de computação e storage para executar o agente de dados na nuvem.

Taxas de serviço

Há duas maneiras de pagar pelas relações de sincronização após o término da avaliação gratuita de 14 dias. A primeira opção é se inscrever na AWS ou no Azure, o que permite que você pague por hora ou anualmente. A segunda opção é comprar licenças diretamente da NetApp. Leia as seções a seguir para obter mais detalhes.

Subscrição do mercado

A assinatura do serviço Cloud Sync da AWS ou Azure permite que você pague por uma taxa por hora ou pague anualmente. ["Você pode se inscrever na AWS ou no Azure"](#), dependendo de onde você deseja ser cobrado.

Assinaturas por hora

Com uma assinatura paga conforme o uso por hora, o serviço Cloud Sync cobra por hora com base no número de relacionamentos de sincronização criados.

- ["Ver preços no Azure"](#)
- ["Veja a definição de preço para pagamento conforme o uso na AWS"](#)

Assinaturas anuais

Uma assinatura anual fornece uma licença para 20 relacionamentos de sincronização que você paga antecipadamente. Se você passar acima de 20 relacionamentos de sincronização e se inscreveu através do Azure, você paga pelas relações adicionais por hora.

["Veja os preços anuais na AWS"](#)

Licenças da NetApp

Outra forma de pagar antecipadamente pelas relações de sincronização é comprando licenças diretamente da NetApp. Cada licença permite criar até 20 relações de sincronização.

Você pode usar essas licenças com uma assinatura da AWS ou do Azure. Por exemplo, se você tiver 25 relacionamentos de sincronização, poderá pagar pelas primeiras 20 relações de sincronização usando uma licença e pagar conforme o uso da AWS ou do Azure com as 5 relações de sincronização restantes.

["Saiba como comprar licenças e adicioná-las ao Cloud Sync"](#).

Termos da licença

Os clientes que comprarem uma licença bring Your own License (BYOL) para o serviço Cloud Sync devem estar cientes das limitações associadas ao direito de licença.

- Os clientes têm o direito de utilizar a licença BYOL por um prazo não superior a um ano a partir da data de entrega.
- Os clientes têm o direito de utilizar a licença BYOL para estabelecer e não exceder um total de 20 conexões individuais entre uma fonte e um destino (cada uma uma "relação de sincronização").
- O direito de um cliente expira na conclusão do prazo de licença de um ano, independentemente de o Cliente ter atingido a limitação de relação de sincronização de 20.
- No caso de o Cliente optar por renovar a sua licença, as relações de sincronização não utilizadas associadas à concessão de licença anterior NÃO serão transferidas para a renovação da licença.

Privacidade de dados

O NetApp não tem acesso a quaisquer credenciais que você fornecer ao usar o serviço Cloud Sync. As credenciais são armazenadas diretamente na máquina do data broker, que reside na sua rede.

Dependendo da configuração escolhida, o Cloud Sync poderá solicitar credenciais ao criar uma nova relação. Por exemplo, ao configurar um relacionamento que inclua um servidor SMB ou ao implantar o agente de dados na AWS.

Essas credenciais são sempre salvas diretamente no próprio corretor de dados. O agente de dados reside em uma máquina em sua rede, seja no local ou na sua conta na nuvem. As credenciais nunca são disponibilizadas ao NetApp.

As credenciais são criptografadas localmente na máquina do corretor de dados usando o HashiCorp Vault.

Limitações

- O Cloud Sync não é suportado na China.
- Além da China, o corretor de dados Cloud Sync não é suportado nas seguintes regiões:
 - AWS GovCloud (EUA)
 - Azure US Gov
 - Azure US DoD

Comece agora

Início rápido para Cloud Sync

A introdução ao serviço Cloud Sync inclui alguns passos.



Prepare sua fonte e destino

Verifique se sua origem e destino são suportados e configurados. O requisito mais importante é verificar a conectividade entre o agente de dados e os locais de origem e destino. ["Saiba mais"](#).

2

Prepare um local para o agente de dados do NetApp

O software de corretor de dados NetApp sincroniza dados de uma origem para um destino (isso é chamado de *relação de sincronização*). Você pode executar o agente de dados na AWS, Azure, Google Cloud Platform ou no local. O corretor de dados precisa de uma conexão de saída de Internet pela porta 443 para que possa se comunicar com o serviço Cloud Sync e entrar em Contato com alguns outros serviços e repositórios. ["Exibir a lista de endpoints"](#).

O Cloud Sync orienta você pelo processo de instalação quando você cria uma relação de sincronização, momento em que você pode implantar o agente de dados na nuvem ou baixar um script de instalação para seu próprio host Linux.

- ["Revise a instalação da AWS"](#)
- ["Revise a instalação do Azure"](#)
- ["Revise a instalação da GCP"](#)
- ["Revise a instalação do host Linux"](#)

3

Crie sua primeira relação de sincronização

Faça login no ["Cloud Manager"](#), clique em **Sincronizar** e arraste e solte suas seleções para a origem e destino. Siga as instruções para concluir a configuração. ["Saiba mais"](#).

4

Pague pelos seus relacionamentos de sincronização depois que a avaliação gratuita terminar

Inscreva-se na AWS ou Azure para pagar conforme o uso ou pagar anualmente. Ou compre licenças diretamente da NetApp. Basta ir para a página Configurações de Licença no Cloud Sync para configurá-lo. ["Saiba mais"](#).

Preparando a fonte e o alvo

Prepare-se para sincronizar dados verificando se sua origem e destino são suportados e configurados.

Relações de sincronização suportadas

O Cloud Sync permite sincronizar dados de uma origem para um destino (isso é chamado de *relação de sincronização*). Você deve entender os relacionamentos suportados antes de começar.

Localização da origem	Locais de destino suportados
AWS EFS	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
AWS S3	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID

Localização da origem	Locais de destino suportados
Blob do Azure	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID
Azure NetApp Files (NFS)	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Azure NetApp Files (SMB)	<ul style="list-style-type: none"> • AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID

Localização da origem	Locais de destino suportados
Cloud Volumes ONTAP (NFS)	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Cloud Volumes ONTAP (SMB)	<ul style="list-style-type: none"> • AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
Cloud Volumes Service (NFS)	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID

Localização da origem	Locais de destino suportados
Cloud Volumes Service (SMB)	<ul style="list-style-type: none"> • AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
Google Cloud Storage	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID
IBM Cloud Object Storage	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID

Localização da origem	Locais de destino suportados
Servidor NFS	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Cluster ONTAP on-premise (NFS)	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Cluster ONTAP on-premise (SMB)	<ul style="list-style-type: none"> • AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
Storage ONTAP S3	<ul style="list-style-type: none"> • StorageGRID

Localização da origem	Locais de destino suportados
Servidor SMB	<ul style="list-style-type: none"> • AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
StorageGRID	<ul style="list-style-type: none"> • AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • Storage ONTAP S3 • SMB Server • StorageGRID

Notas:

1. Você pode escolher uma categoria de storage específica do Azure Blob quando um contêiner de Blob é o destino:
 - Armazenamento a quente
 - Armazenamento frio
2. você pode escolher uma classe de armazenamento S3 específica quando o AWS S3 é o destino:
 - Standard (esta é a classe padrão)
 - Disposição em camadas inteligente
 - Acesso padrão-infrequente
 - Uma zona de acesso pouco frequente
 - Glacier

- Glacier Deep Archive

Rede para a origem e o destino

- A origem e o destino devem ter uma conexão de rede com o corretor de dados.

Por exemplo, se um servidor NFS estiver no data center e o agente de dados estiver na AWS, você precisará de uma conexão de rede (VPN ou Direct Connect) da rede para a VPC.

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Requisitos de origem e destino

Verifique se sua origem e seus destinos atendem aos seguintes requisitos.

requisitos de bucket do AWS S3

Certifique-se de que seu bucket do AWS S3 atenda aos seguintes requisitos.

Localizações de corretores de dados compatíveis para AWS S3

As relações de sincronização que incluem o storage S3 exigem que um agente de dados seja implantado na AWS ou no local. Em ambos os casos, o Cloud Sync solicita que você associe o agente de dados a uma conta da AWS durante a instalação.

- ["Saiba como implantar o agente de dados da AWS"](#)
- ["Saiba como instalar o corretor de dados em um host Linux"](#)

Regiões AWS compatíveis

Todas as regiões são suportadas, exceto as regiões China e GovCloud (EUA).

Permissões necessárias para buckets do S3 em outras contas da AWS

Ao configurar um relacionamento de sincronização, você pode especificar um bucket do S3 que reside em uma conta da AWS que não está associada ao agente de dados.

["As permissões incluídas neste arquivo JSON"](#) Deve ser aplicado a esse bucket do S3 para que o agente de dados possa acessá-lo. Essas permissões permitem que o agente de dados copie dados de e para o bucket e liste os objetos no bucket.

Observe o seguinte sobre as permissões incluídas no arquivo JSON:

1. *<BucketName>* é o nome do bucket que reside na conta da AWS que não está associado ao corretor de dados.
2. *<RoleARN>* deve ser substituído por um dos seguintes:
 - Se o corretor de dados foi instalado manualmente em um host Linux, *RoleARN* deve ser o ARN do usuário da AWS para o qual você forneceu credenciais da AWS ao implantar o corretor de dados.
 - Se o corretor de dados foi implantado na AWS usando o modelo CloudFormation, *RoleARN* deve ser o ARN da função IAM criada pelo modelo.

Você pode encontrar a função ARN indo para o console EC2, selecionando a instância do data broker

e clicando na função IAM na guia Descrição. Você deve então ver a página Resumo no console do IAM que contém a função ARN.

Summary

Delete role

Role ARN `arn:aws:iam::142281742614:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05`

Role description [Edit](#)

requisitos de armazenamento de Blobs do Azure

Certifique-se de que seu storage Azure Blob atenda aos requisitos a seguir.

Localizações de corretores de dados compatíveis para Azure Blob

O agente de dados pode residir em qualquer local quando uma relação de sincronização inclui o armazenamento Azure Blob.

Regiões Azure compatíveis

Todas as regiões são suportadas, exceto as regiões China, US Gov e US DoD.

Cadeia de conexão necessária para relacionamentos que incluem Azure Blob e NFS/SMB

Ao criar uma relação de sincronização entre um contêiner de Blob do Azure e um servidor NFS ou SMB, você precisa fornecer à Cloud Sync a cadeia de conexão de conta de storage:

a63cde60b553020 - Access keys

Storage account

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Storage Explorer (preview)

Settings

- Access keys**
- CORS
- Configuration
- Encryption

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. [Learn more](#)

Storage account name
a63cde60b553020

key1

Key
vScjFdvVZqIPyO/

Connection string
DefaultEndpoints

Se você quiser sincronizar dados entre dois contentores Blob do Azure, a cadeia de conexão deve incluir um "assinatura de acesso compartilhado" (SAS). Você também tem a opção de usar um SAS ao sincronizar entre um contêiner Blob e um servidor NFS ou SMB.

O SAS deve permitir acesso ao serviço Blob e a todos os tipos de recursos (Serviço, contêiner e Objeto). O

SAS também deve incluir as seguintes permissões:

- Para o contentor Blob de origem: Leitura e Lista
- Para o contentor Blob de destino: Leitura, gravação, Lista, Adicionar e criar

a63cde60b553020 - Shared access signature

Storage account

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

Requisito Azure NetApp Files

Use o nível de serviço Premium ou Ultra ao sincronizar dados com ou a partir do Azure NetApp Files. Você pode ter falhas e problemas de desempenho se o nível de serviço de disco for padrão.



Consulte um arquiteto de soluções se precisar de ajuda para determinar o nível de serviço certo. O tamanho do volume e a camada de volume determinam a taxa de transferência que você pode obter.

["Saiba mais sobre os níveis de serviço e a taxa de transferência do Azure NetApp Files".](#)

Requisitos de bucket do Google Cloud Storage

Certifique-se de que seu bucket do Google Cloud Storage atenda aos seguintes requisitos.

Localizações de corretores de dados compatíveis com o Google Cloud Storage

Relacionamentos de sincronização que incluem o Google Cloud Storage exigem que um agente de dados seja implantado no GCP ou no local. O Cloud Sync orienta você pelo processo de instalação do data broker quando você cria uma relação de sincronização.

- ["Saiba como implantar o agente de dados da GCP"](#)
- ["Saiba como instalar o corretor de dados em um host Linux"](#)

Regiões GCP compatíveis

Todas as regiões são suportadas.

Requisitos do servidor NFS

- O servidor NFS pode ser um sistema NetApp ou um sistema que não seja NetApp.
- O servidor de arquivos deve permitir que o host do data broker acesse as exportações.
- As versões de NFS 3, 4,0, 4,1 e 4,2 são compatíveis.

A versão desejada deve estar ativada no servidor.

- Se você quiser sincronizar dados NFS de um sistema ONTAP, verifique se o acesso à lista de exportação NFS de um SVM está ativado (`vserver nfs modificar -vserver svm_name -showmount` habilitado).



A configuração padrão para showmount é *enabled* começando com ONTAP 9.2.

Requisitos de storage do ONTAP S3

O ONTAP 9.7 oferece suporte ao Amazon Simple Storage Service (Amazon S3) como uma prévia pública. ["Saiba mais sobre o suporte do ONTAP para o Amazon S3"](#).

Ao configurar uma relação de sincronização que inclua o armazenamento ONTAP S3, você precisará fornecer o seguinte:

- O endereço IP do LIF conectado ao ONTAP S3
- A chave de acesso e a chave secreta que o ONTAP está configurado para usar

Requisitos de servidor SMB

- O servidor SMB pode ser um sistema NetApp ou um sistema que não seja NetApp.
- O servidor de arquivos deve permitir que o host do data broker acesse as exportações.
- As versões SMB 1,0, 2,0, 2,1, 3,0 e 3,11 são suportadas.
- Conceda ao grupo "Administradores" permissões "Controle total" para as pastas de origem e destino.

Se você não conceder essa permissão, o corretor de dados pode não ter permissões suficientes para obter as ACLs em um arquivo ou diretório. Se isso ocorrer, você receberá o seguinte erro: "Erro getxattr 95"

Limitação SMB para diretórios e arquivos ocultos

Uma limitação SMB afeta diretórios e arquivos ocultos ao sincronizar dados entre servidores SMB. Se algum dos diretórios ou arquivos no servidor SMB de origem estiver oculto pelo Windows, o atributo oculto não será copiado para o servidor SMB de destino.

Comportamento de sincronização SMB devido a limitação de insensibilidade de caso

O protocolo SMB é insensível a maiúsculas e minúsculas, o que significa que as letras maiúsculas e minúsculas são tratadas como sendo as mesmas. Esse comportamento pode resultar em arquivos sobrescritos e erros de cópia de diretório, se uma relação de sincronização incluir um servidor SMB e os dados já existirem no destino.

Por exemplo, digamos que há um arquivo chamado "a" na origem e um arquivo chamado "A" no destino. Quando o Cloud Sync copia o arquivo chamado "a" para o destino, o arquivo "A" é substituído pelo arquivo "a" da origem.

No caso dos diretórios, digamos que há um diretório chamado "b" na fonte e um diretório chamado "B" no destino. Quando o Cloud Sync tenta copiar o diretório chamado "b" para o destino, o Cloud Sync recebe um erro que diz que o diretório já existe. Como resultado, o Cloud Sync sempre falha em copiar o diretório chamado "B."

A melhor maneira de evitar essa limitação é garantir que você sincronize dados para um diretório vazio.

Permissões para um destino SnapMirror

Se a origem de um relacionamento de sincronização for um destino SnapMirror (que é somente leitura), as permissões "leitura/lista" são suficientes para sincronizar dados da origem para um destino.

Visão geral de rede para Cloud Sync

A rede para Cloud Sync inclui conectividade entre o agente de dados e os locais de origem e destino, e uma conexão de saída à Internet do agente de dados através da porta 443.

Localização do agente de dados

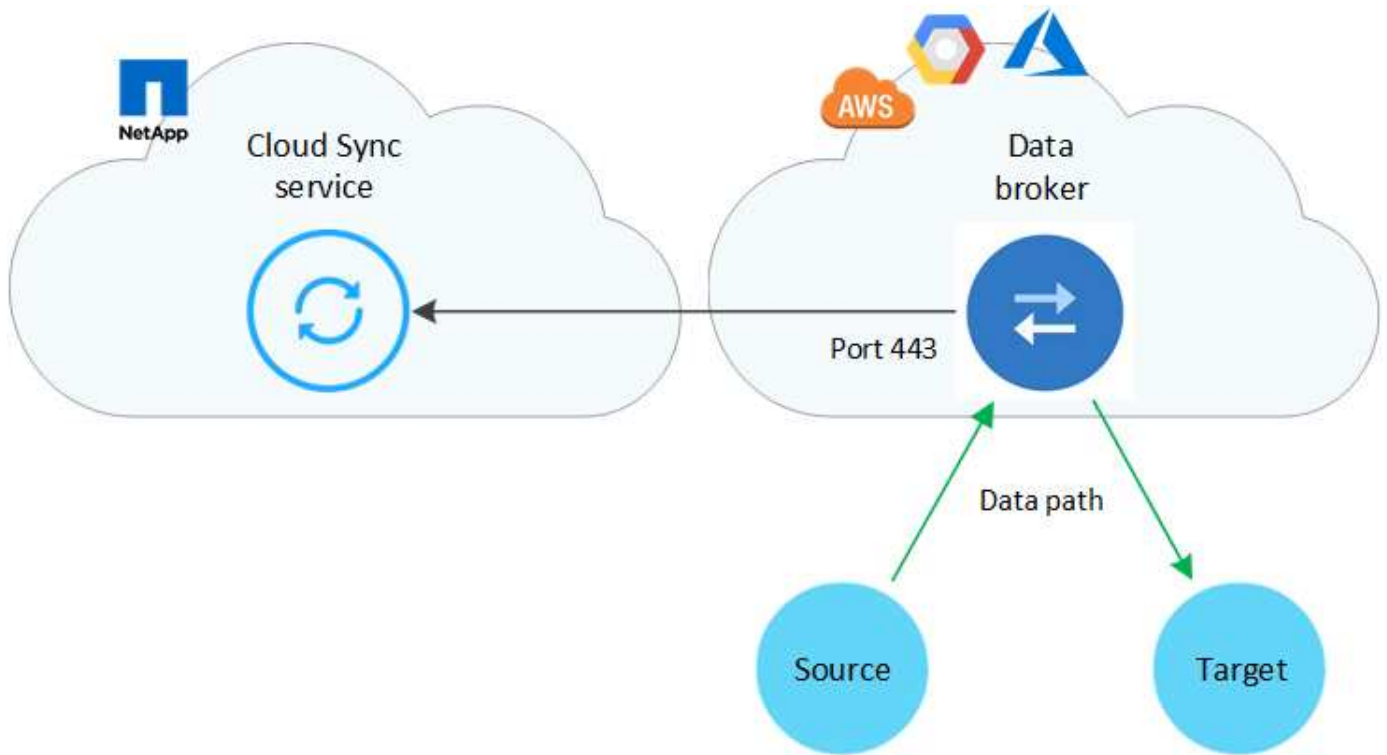
É possível instalar o agente de dados na nuvem ou no local.

Agente de dados na nuvem

A imagem a seguir mostra o agente de dados em execução na nuvem, na AWS, GCP ou Azure. A origem e o destino podem estar em qualquer local, desde que haja uma conexão com o corretor de dados. Por exemplo, você pode ter uma conexão VPN do seu data center para o seu provedor de nuvem.

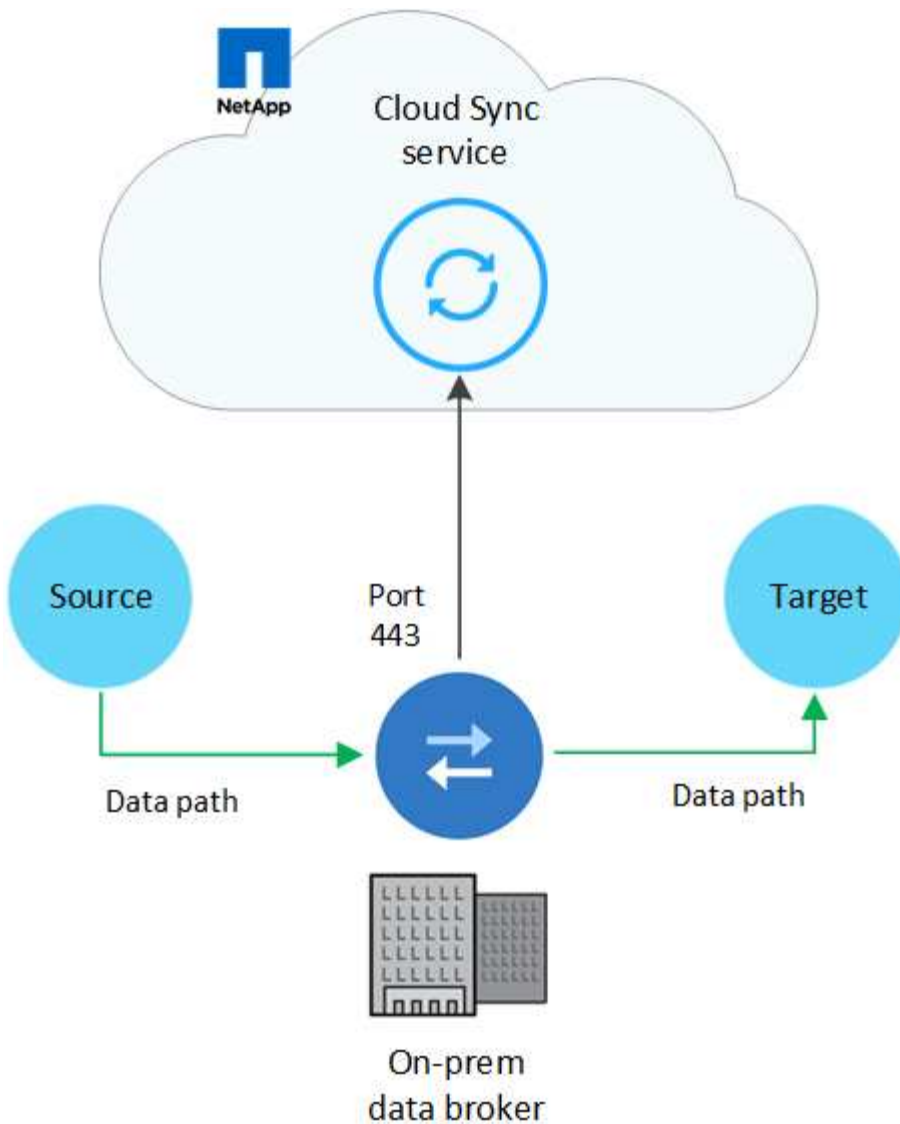


Quando o Cloud Sync implanta o agente de dados na AWS, Azure ou GCP, ele cria um grupo de segurança que ativa a comunicação de saída necessária.



Agente de dados no local

A imagem a seguir mostra o agente de dados em execução no local, em um data center. Novamente, a fonte e o alvo podem estar em qualquer local, desde que haja uma conexão com o corretor de dados.



Requisitos de rede

- A origem e o destino devem ter uma conexão de rede com o corretor de dados.

Por exemplo, se um servidor NFS estiver no data center e o agente de dados estiver na AWS, você precisará de uma conexão de rede (VPN ou Direct Connect) da rede para a VPC.

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.
- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Endpoints de rede

O corretor de dados NetApp requer acesso de saída à Internet pela porta 443 para se comunicar com o serviço Cloud Sync e entrar em contato com alguns outros serviços e repositórios. Seu navegador da Web local também requer acesso a endpoints para determinadas ações. Se você precisar limitar a conectividade de saída, consulte a seguinte lista de endpoints ao configurar seu firewall para tráfego de saída.

Pontos de extremidade do agente de dados

O corretor de dados entra em Contato com os seguintes pontos finais:

Endpoints	Finalidade
olcentgbl.trafficmanager.net:443	Para entrar em Contato com um repositório para atualizar pacotes CentOS para o host do data broker. Esse endpoint é contatado somente se você instalar manualmente o data broker em um host CentOS.
rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Para contatar repositórios para atualizar o Node.js, npm e outros pacotes de 3rd partes usados no desenvolvimento.
tgz.pm2.io:443	Para acessar um repositório para atualizar o PM2, que é um pacote de 3rd partes usado para monitorar o Cloud Sync.
sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	Para entrar em Contato com os serviços da AWS que o Cloud Sync usa para operações (enfileirando arquivos, registrando ações e fornecendo atualizações para o agente de dados).
s3.region.amazonaws.com:443 por exemplo: s3.us-east-2.amazonaws.com:443 "Consulte a documentação da AWS para obter uma lista de endpoints do S3"	Para entrar em Contato com o Amazon S3 quando um relacionamento de sincronização incluir um bucket do S3.
cf.cloudsync.NetApp.com:443 repo.cloudsync.NetApp.com:443	Para contactar o serviço Cloud Sync.
support.NetApp.com:443	Para entrar em Contato com o suporte da NetApp ao usar uma licença BYOL para relacionamentos de sincronização.
fedoraproject.org:443	Para instalar o 7z na máquina virtual do corretor de dados durante a instalação e atualizações. O 7z é necessário para enviar mensagens AutoSupport para o suporte técnico da NetApp.

Endpoints do navegador da Web

O seu navegador da Web precisa de acesso ao seguinte ponto final para transferir registros para fins de resolução de problemas:

logs.cloudsync.NetApp.com:443

Como instalar um corretor de dados

Instalar o agente de dados na AWS

Quando você cria um relacionamento de sincronização, escolha a opção AWS Data Broker para implantar o software de corretor de dados em uma nova instância do EC2 em uma VPC. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Você também tem a opção de instalar o agente de dados em um host Linux existente na nuvem ou no local. ["Saiba mais"](#).

Regiões AWS compatíveis

Todas as regiões são suportadas, exceto as regiões China e GovCloud (EUA).

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.

Quando o Cloud Sync implanta o agente de dados na AWS, ele cria um grupo de segurança que permite a comunicação de saída necessária. Observe que você pode configurar o agente de dados para usar um servidor proxy durante o processo de instalação.

Se precisar limitar a conectividade de saída, ["a lista de endpoints que o corretor de dados entra em contato"](#) consulte .

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Permissões necessárias para implantar o agente de dados na AWS

A conta de usuário da AWS que você usa para implantar o agente de dados deve ter as permissões incluídas no ["Esta política fornecida pela NetApp"](#).

requisitos para usar sua própria função do IAM com o agente de dados da AWS

Quando o Cloud Sync implanta o agente de dados, ele cria uma função do IAM para a instância do agente de dados. Você pode implantar o agente de dados usando sua própria função do IAM, se preferir. Você pode usar essa opção se sua organização tiver políticas de segurança rígidas.

A função do IAM deve atender aos seguintes requisitos:

- O serviço EC2 deve ter permissão para assumir a função IAM como uma entidade confiável.
- ["As permissões definidas neste arquivo JSON"](#) Deve ser anexado à função do IAM para que o corretor de dados possa funcionar corretamente.

Siga as etapas abaixo para especificar a função do IAM ao implantar o corretor de dados.

Instalar o agente de dados

Você pode instalar um agente de dados na AWS ao criar um relacionamento de sincronização.

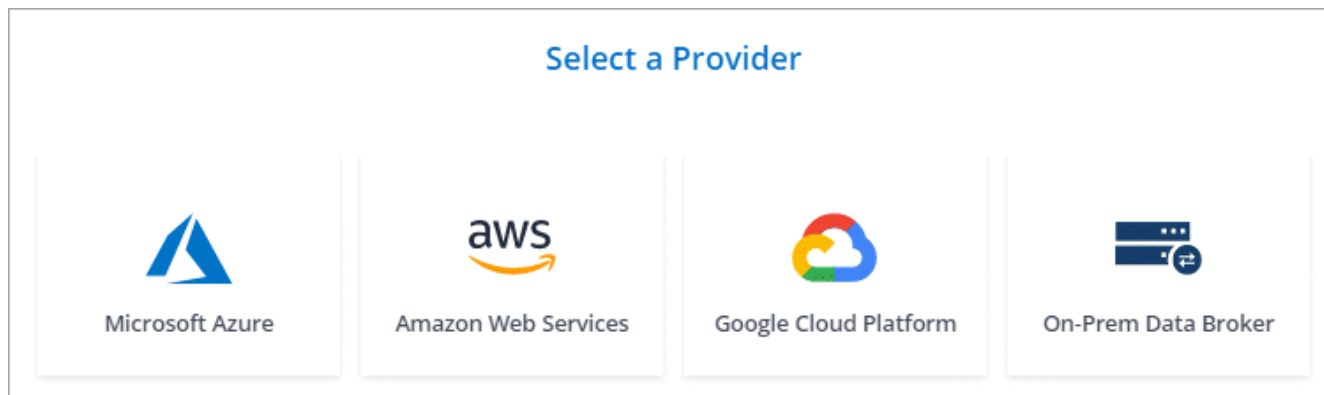
Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.

Conclua as etapas até chegar à página **Data Broker**.

3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **Amazon Web Services**.

Se você já tem um corretor de dados, você precisará clicar no  ícone primeiro.



4. Digite um nome para o corretor de dados e clique em **continuar**.
5. Insira uma chave de acesso da AWS para que o Cloud Sync possa criar o agente de dados na AWS em seu nome.

As chaves não são salvas ou usadas para quaisquer outros fins.

Se você preferir não fornecer chaves de acesso, clique no link na parte inferior da página para usar um modelo do CloudFormation. Ao usar essa opção, você não precisa fornecer credenciais porque está fazendo login diretamente na AWS.

o vídeo a seguir mostra como iniciar a instância do data broker usando um modelo do CloudFormation:

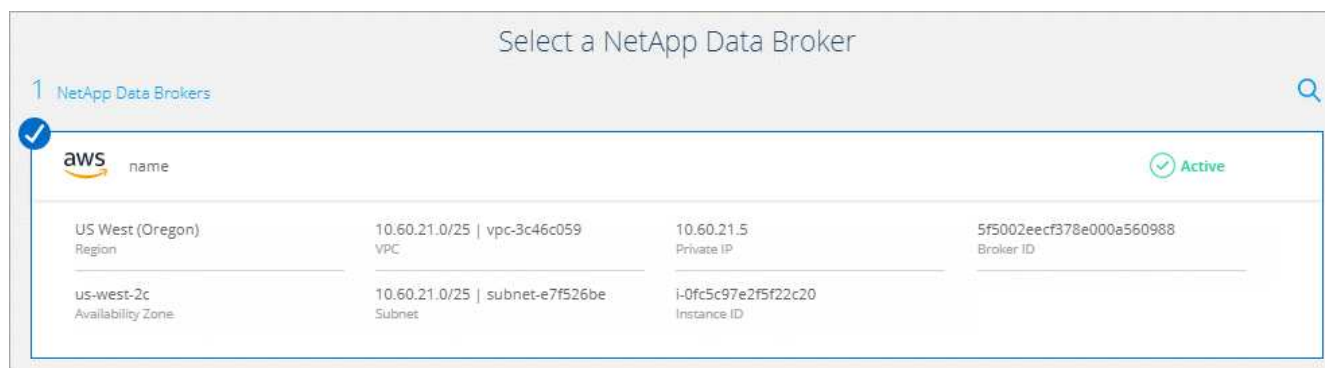
► https://docs.netapp.com/pt-br/occm38//media/video_cloud_sync.mp4 (video)

6. Se você inseriu uma chave de acesso da AWS, selecione um local para a instância, selecione um par de chaves, escolha se deseja habilitar um endereço IP público e, em seguida, selecione uma função do IAM existente ou deixe o campo em branco para que o Cloud Sync crie a função para você.

Se você escolher sua própria função do IAM, [você precisará fornecer as permissões necessárias](#).

7. Depois que o corretor de dados estiver disponível, clique em **continuar** no Cloud Sync.

A imagem a seguir mostra uma instância implantada com sucesso na AWS:



8. Complete as páginas no assistente para criar a nova relação de sincronização.

Resultado

Você implantou um agente de dados na AWS e criou uma nova relação de sincronização. Você pode usar esse corretor de dados com relações de sincronização adicionais.

Instalar o corretor de dados no Azure

Ao criar uma relação de sincronização, escolha a opção Agente de dados do Azure para implantar o software de corretor de dados em uma nova máquina virtual em uma VNet. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Você também tem a opção de instalar o agente de dados em um host Linux existente na nuvem ou no local. ["Saiba mais"](#).

Regiões Azure compatíveis

Todas as regiões são suportadas, exceto as regiões China, US Gov e US DoD.

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.

Quando o Cloud Sync implanta o agente de dados no Azure, ele cria um grupo de segurança que permite a comunicação de saída necessária.

Se precisar limitar a conectividade de saída, ["a lista de endpoints que o corretor de dados entra em contato"](#) consulte .

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Método de autenticação

Ao implantar o corretor de dados, você precisará escolher um método de autenticação: Uma senha ou um par de chaves SSH público-privadas.

Para obter ajuda sobre a criação de um par de chaves, ["Documentação do Azure: Crie e use um par de](#)


[chaves SSH público-privada para VMs Linux no Azure](#)" consulte .

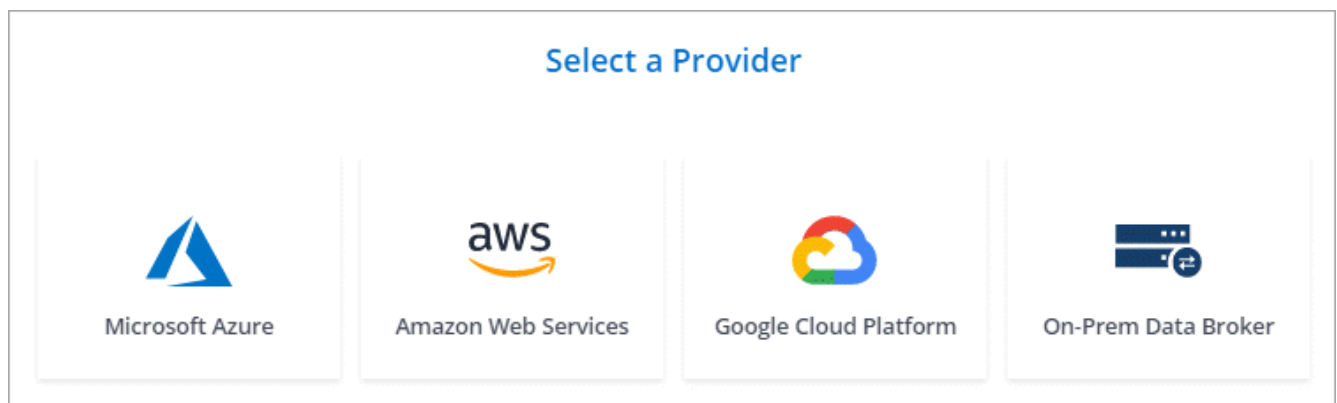
Instalar o agente de dados

Você pode instalar um corretor de dados no Azure quando criar uma relação de sincronização.

Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.
Complete as páginas até chegar à página **Data Broker**.
3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **Microsoft Azure**.

Se você já tem um corretor de dados, você precisará clicar no  ícone primeiro.



4. Digite um nome para o corretor de dados e clique em **continuar**.
5. Se lhe for solicitado, inicie sessão na sua conta Microsoft. Se você não for solicitado, clique em **entrar no Azure**.

O formulário é de propriedade e hospedado pela Microsoft. Suas credenciais não são fornecidas ao NetApp.

6. Escolha um local para o corretor de dados e insira detalhes básicos sobre a máquina virtual.

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

7. Clique em **continuar** e mantenha a página aberta até que a implantação esteja concluída.

O processo pode levar até 7 minutos.

8. No Cloud Sync, clique em **continuar** quando o corretor de dados estiver disponível.

9. Complete as páginas no assistente para criar a nova relação de sincronização.

Resultado

Você implantou um agente de dados no Azure e criou uma nova relação de sincronização. Você pode usar esse corretor de dados com relações de sincronização adicionais.

Recebendo uma mensagem sobre a necessidade de consentimento do administrador?

Se a Microsoft notificar você de que a aprovação de administrador é necessária porque o Cloud Sync precisa de permissão para acessar recursos em sua organização em seu nome, então você tem duas opções:

1. Peça ao administrador do AD para fornecer a você a seguinte permissão:

No Azure, acesse a **Centros de administração > Azure AD > utilizadores e grupos > Definições de utilizador** e ative **os utilizadores podem autorizar as aplicações a acederem aos dados da empresa em seu nome**.

2. Peça ao administrador do AD para consentir em seu nome para **CloudSync-AzureDataBrokerCreator** usando o seguinte URL (este é o endpoint de consentimento do administrador):

```
https://login.microsoftonline.com/{FILL HERE YOUR TENANT ID/v2.0/adminconsent?client_id_8e4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri_https://cloudsync.NetApp.com&scope-https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read
```

Como mostrado na URL, o URL do nosso aplicativo é <https://cloudsync.NetApp.com> e o ID do cliente do aplicativo é 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Instalar o agente de dados no Google Cloud Platform

Quando você cria um relacionamento de sincronização, escolha a opção Data Broker do GCP para implantar o software de agente de dados em uma nova instância de máquina virtual em uma VPC. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Você também tem a opção de instalar o agente de dados em um host Linux existente na nuvem ou no local. ["Saiba mais"](#).

Regiões GCP compatíveis

Todas as regiões são suportadas.

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.

Quando o Cloud Sync implanta o agente de dados no GCP, ele cria um grupo de segurança que ativa a comunicação de saída necessária.

Se precisar limitar a conectividade de saída, ["a lista de endpoints que o corretor de dados entra em contato"](#) consulte .

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Permissões necessárias para implantar o agente de dados na GCP

Certifique-se de que o usuário do GCP que implanta o agente de dados tenha as seguintes permissões:

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

Permissões necessárias para a conta de serviço

Ao implantar o agente de dados, você precisa selecionar uma conta de serviço que tenha as seguintes permissões:

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

Instalar o agente de dados

É possível instalar um agente de dados no GCP ao criar um relacionamento de sincronização.

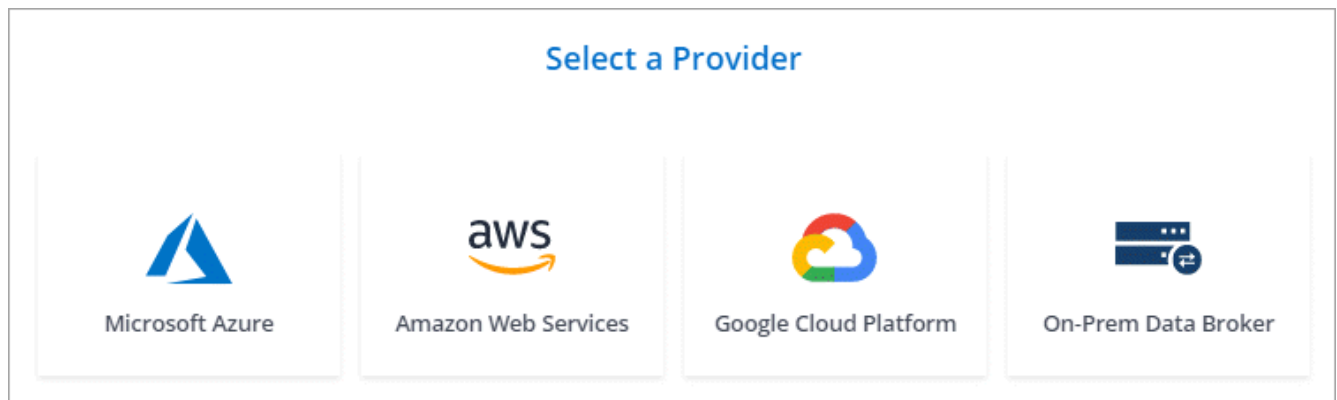
Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.

Conclua as etapas até chegar à página **Data Broker**.

3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **Google Cloud Platform**.

Se você já tem um corretor de dados, você precisará clicar no  ícone primeiro.



4. Digite um nome para o corretor de dados e clique em **continuar**.
5. Se você for solicitado, faça login com sua conta do Google.

O formulário é de propriedade e hospedado pelo Google. Suas credenciais não são fornecidas ao NetApp.

6. Selecione uma conta de projeto e serviço e escolha um local para o corretor de dados.

Basic Settings	
Project	Location
Project OCCM-Dev	Region us-west1
Service Account test	Zone us-west1-a
Select a Service Account that includes these permissions	VPC default
	Subnet default

7. Quando o corretor de dados estiver disponível, clique em **continuar** no Cloud Sync.

A instância leva aproximadamente 5 a 10 minutos para implantar. Você pode monitorar o andamento do serviço Cloud Sync, que é atualizado automaticamente quando a instância está disponível.

8. Complete as páginas no assistente para criar a nova relação de sincronização.

Resultado

Você implantou um agente de dados no GCP e criou uma nova relação de sincronização. Você pode usar esse corretor de dados com relações de sincronização adicionais.

Instalar o corretor de dados em um host Linux

Quando você cria uma relação de sincronização, escolha a opção Data Broker local para instalar o software Data Broker em um host Linux local ou em um host Linux existente na nuvem. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Requisitos de host do Linux

- **Sistema operacional:**

- CentOS 7,0, 7,7 e 8,0
- Red Hat Enterprise Linux 7,7 e 8,0
- Ubuntu Server 18,04 LTS
- SUSE Linux Enterprise Server 15 SP1

O comando `yum update all` deve ser executado no host antes de instalar o corretor de dados.

Um sistema Red Hat Enterprise Linux deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o sistema não poderá acessar os repositórios para atualizar o software de 3rd partes necessário durante a instalação.

- **RAM:** 16 GB
- * CPU*: 4 núcleos
- * Espaço livre em disco *: 10 GB
- **SELinux:** Recomendamos que você desative "[SELinux](#)" no host.

O SELinux aplica uma política que bloqueia atualizações de software de corretor de dados e pode impedir que o corretor de dados entre em Contato com os endpoints necessários para a operação normal.

- * OpenSSL*: OpenSSL deve ser instalado no host Linux.

Requisitos de rede

- O host Linux deve ter uma conexão com a origem e o destino.
- O servidor de arquivos deve permitir que o host Linux acesse as exportações.
- A porta 443 deve estar aberta no host Linux para tráfego de saída para a AWS (o agente de dados se comunica constantemente com o serviço Amazon SQS).
- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Habilitando o acesso à AWS

Se você planeja usar o agente de dados com um relacionamento de sincronização que inclui um bucket do S3, então você deve preparar o host Linux para o AWS Access. Ao instalar o agente de dados, você precisará fornecer chaves da AWS para um usuário da AWS que tenha acesso programático e permissões específicas.

Passos

1. Crie uma política do IAM usando "[Esta política fornecida pela NetApp](#)" ou "[Veja as instruções da AWS](#)".

2. Crie um usuário do IAM que tenha acesso programático. ["Veja as instruções da AWS"](#).

Certifique-se de copiar as chaves da AWS porque você precisa especificá-las ao instalar o software de data broker.

Habilitando o acesso ao Google Cloud

Se você planeja usar o agente de dados com uma relação de sincronização que inclua um bucket do Google Cloud Storage, prepare o host Linux para acesso ao GCP. Ao instalar o corretor de dados, você precisará fornecer uma chave para uma conta de serviço que tenha permissões específicas.

Passos

1. Crie uma conta de serviço do GCP que tenha permissões de Administrador de armazenamento, se você ainda não tiver uma.
2. Crie uma chave de conta de serviço salva no formato JSON. ["Veja as instruções da GCP"](#).

O arquivo deve conter pelo menos as seguintes propriedades: "Project_id", "private_key" e "client_email"



Quando você cria uma chave, o arquivo é gerado e baixado para sua máquina.

3. Salve o arquivo JSON no host Linux.

Habilitando o acesso ao Microsoft Azure

O acesso ao Azure é definido por relacionamento fornecendo uma conta de armazenamento e uma cadeia de conexão no assistente de relacionamento de sincronização.

Instalar o agente de dados

Você pode instalar um corretor de dados em um host Linux quando você cria uma relação de sincronização.

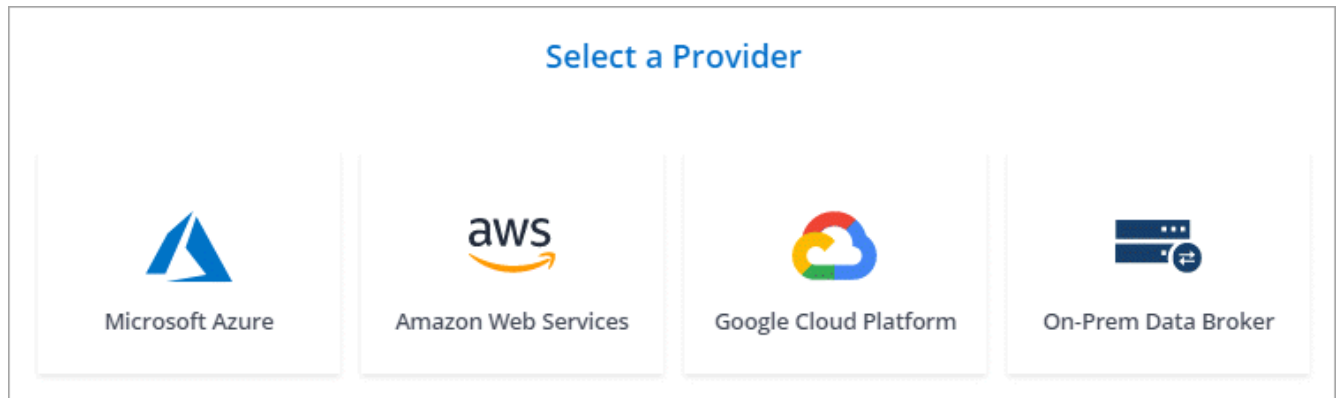
Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.

Conclua as etapas até chegar à página **Data Broker**.

3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **On-Prem Data Broker**.

Se você já tem um corretor de dados, você precisará clicar no ícone primeiro.



Mesmo que a opção seja rotulada **on-Prem Data Broker**, ela se aplica a um host Linux em suas instalações ou na nuvem.

4. Digite um nome para o corretor de dados e clique em **continuar**.

A página de instruções é carregada em breve. Você precisará seguir estas instruções - elas incluem um link exclusivo para baixar o instalador.

5. Na página de instruções:

- a. Selecione se deseja habilitar o acesso a **AWS**, **Google Cloud** ou ambos.
- b. Selecione uma opção de instalação: **No proxy**, **Use proxy Server** ou **Use proxy Server with Authentication**.
- c. Use os comandos para baixar e instalar o corretor de dados.

As etapas a seguir fornecem detalhes sobre cada opção de instalação possível. Siga a página de instruções para obter o comando exato com base na opção de instalação.

- d. Faça o download do instalador:

- Sem proxy:

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

- Use o servidor proxy:

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

- Use o servidor proxy com autenticação:

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

URI

O Cloud Sync exibe o URI do arquivo de instalação na página de instruções, que é carregado quando você segue os prompts para implantar o Data Broker local. Esse URI não é repetido aqui porque o link é gerado dinamicamente e pode ser usado apenas uma vez. [Siga estes passos para obter o URI do Cloud Sync.](#)

- e. Mude para superusuário, torne o instalador executável e instale o software:



Cada comando listado abaixo inclui parâmetros para o AWS Access e o GCP Access. Siga a página de instruções para obter o comando exato com base na opção de instalação.

- Sem configuração de proxy:

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

- Configuração do 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>
```

- Configuração de proxy com autenticação:

```
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>
```

Chaves da AWS

Estas são as chaves para o usuário que você deve ter preparado [seguindo estes passos](#). As chaves da AWS são armazenadas no agente de dados, que é executado em sua rede local ou na nuvem. O NetApp não usa as chaves fora do corretor de dados.

Ficheiro JSON

Este é o arquivo JSON que contém uma chave de conta de serviço que você deve ter preparado [seguindo estes passos](#).

6. Quando o corretor de dados estiver disponível, clique em **continuar** no Cloud Sync.
7. Complete as páginas no assistente para criar a nova relação de sincronização.

Criando uma relação de sincronização

Quando você cria uma relação de sincronização, o serviço Cloud Sync copia arquivos da origem para o destino. Após a cópia inicial, o serviço sincroniza todos os dados alterados a cada 24 horas.

As etapas abaixo fornecem um exemplo que mostra como configurar uma relação de sincronização de um servidor NFS para um bucket do S3.

Passos

1. No Cloud Manager, clique em **Sync**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino.

As etapas a seguir fornecem um exemplo de como criar uma relação de sincronização de um servidor NFS para um bucket do S3.



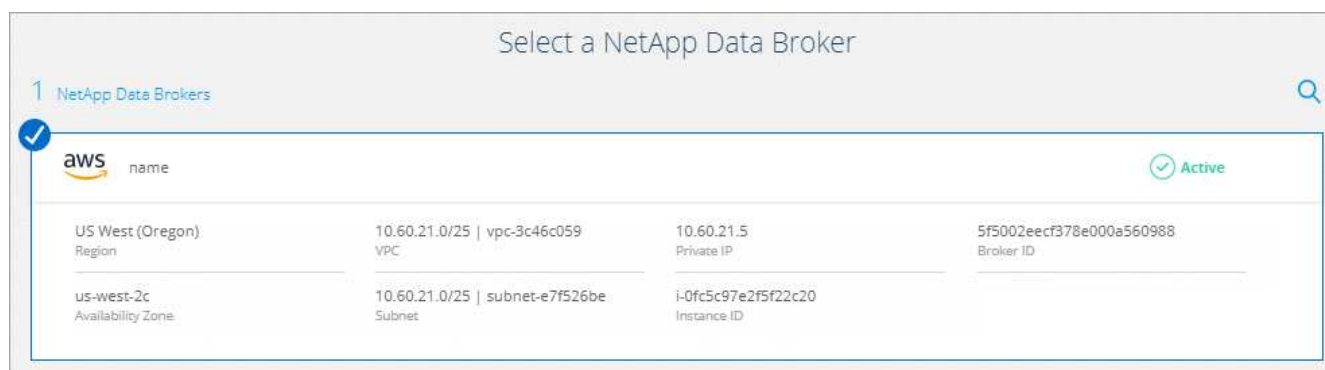
3. Na página **servidor NFS**, insira o endereço IP ou o nome de domínio totalmente qualificado do servidor NFS que você deseja sincronizar com a AWS.
4. Na página **Data Broker**, siga as instruções para criar uma máquina virtual de agente de dados na AWS, Azure ou Google Cloud Platform, ou para instalar o software de corretor de dados em um host Linux existente.

Para obter mais detalhes, consulte as seguintes páginas:

- ["Instalar o agente de dados na AWS"](#)
- ["Instalar o corretor de dados no Azure"](#)
- ["Instalar o agente de dados no GCP"](#)
- ["Instalar o corretor de dados em um host Linux"](#)

5. Depois de instalar o corretor de dados, clique em **continuar**.

A imagem a seguir mostra um corretor de dados implantado com sucesso na AWS:



6. na página **diretórios**, selecione um diretório ou subdiretório de nível superior.

Se o Cloud Sync não conseguir recuperar as exportações, clique em **Adicionar exportação manualmente** e insira o nome de uma exportação NFS.



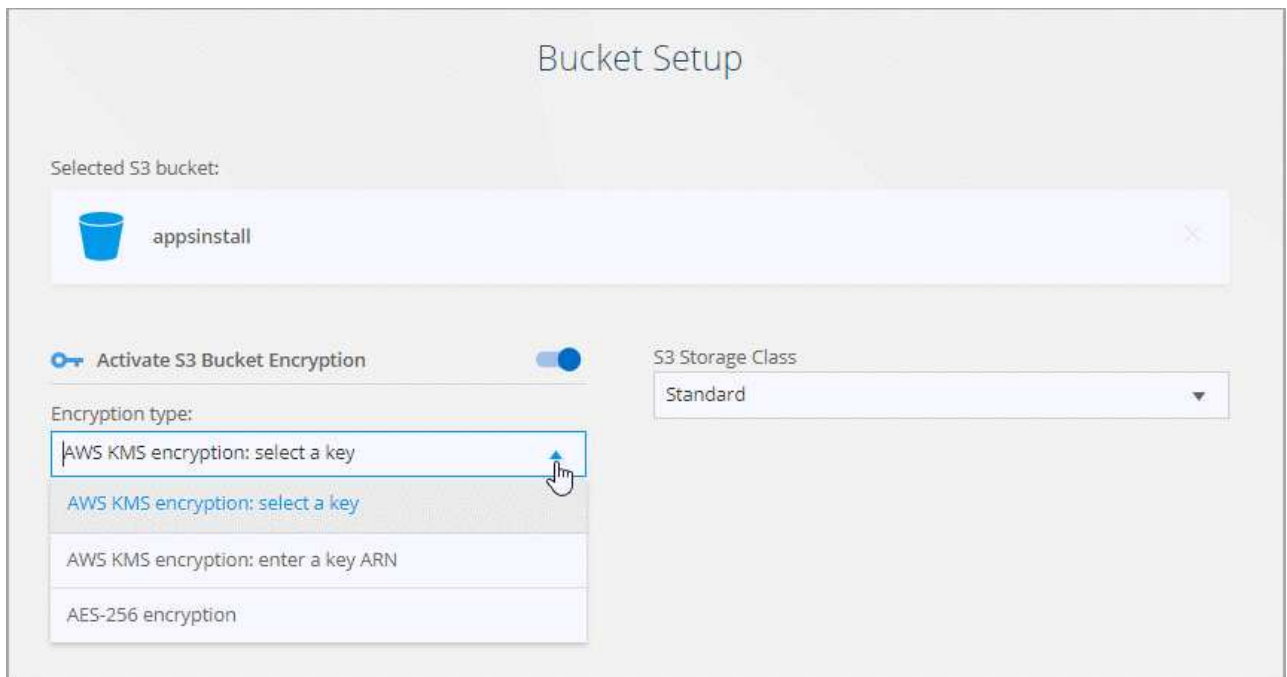
Se você quiser sincronizar mais de um diretório no servidor NFS, então você deve criar relações de sincronização adicionais depois que terminar.

7. Na página **AWS S3 Bucket**, selecione um bucket:

- Faça uma pesquisa detalhada para selecionar uma pasta existente dentro do intervalo ou para selecionar uma nova pasta criada dentro do intervalo.
- Clique em **Adicionar à lista** para selecionar um bucket do S3 que não esteja associado à sua conta da AWS. "[Permissões específicas devem ser aplicadas ao bucket do S3](#)".

8. Na página **Bucket Setup**, configure o bucket:

- Escolha se deseja ativar a criptografia de bucket S3 e, em seguida, selecione uma chave AWS KMS, insira o ARN de uma chave KMS ou selecione criptografia AES-256.
- Selecione uma classe de armazenamento S3. "[Veja as classes de armazenamento suportadas](#)".



9. Na página **Configurações**, defina como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino:

Programação

Escolha uma programação recorrente para futuras sincronizações ou desative a programação de sincronização. Você pode agendar uma relação para sincronizar dados a cada 1 minutos.

Tenta novamente

Defina o número de vezes que o Cloud Sync deve tentar sincronizar um arquivo antes de ignorá-lo.

Ficheiros modificados recentemente

Escolha excluir arquivos que foram modificados recentemente antes da sincronização programada.

Eliminar ficheiros na origem

Escolha excluir arquivos do local de origem depois que o Cloud Sync copiar os arquivos para o local de destino. Essa opção inclui o risco de perda de dados porque os arquivos de origem são excluídos após serem copiados.

Se você ativar essa opção, também precisará alterar um parâmetro no arquivo local.json no corretor de dados. Abra o arquivo e altere o parâmetro chamado *workers.transferrer.delete-on-source* para **true**.

Excluir arquivos no destino

Escolha excluir arquivos do local de destino, se eles foram excluídos da origem. O padrão é nunca excluir arquivos do local de destino.

Marcação de objetos

Quando o AWS S3 é o destino em uma relação de sincronização, o Cloud Sync marca objetos S3 com metadados relevantes para a operação de sincronização. Você pode desativar a marcação de objetos S3, se não for desejado em seu ambiente. Não há impactos no Cloud Sync se você desabilitar a marcação: O Cloud Sync apenas armazena os metadados de sincronização de uma maneira diferente.

Tipos de ficheiros

Defina os tipos de arquivo a serem incluídos em cada sincronização: Arquivos, diretórios e links simbólicos.

Excluir extensões de arquivos

Especifique extensões de arquivo para excluir da sincronização digitando a extensão do arquivo e pressionando **Enter**. Por exemplo, digite *log* ou *.log* para excluir arquivos **.log*. Não é necessário um separador para várias extensões. O vídeo a seguir fornece uma breve demonstração:

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

Tamanho do ficheiro

Escolha sincronizar todos os arquivos, independentemente do seu tamanho ou apenas arquivos que estão em um intervalo de tamanho específico.

Data de modificação

Escolha todos os arquivos independentemente da data da última modificação, arquivos modificados após uma data específica, antes de uma data específica ou entre um intervalo de tempo.

10. Na página **Tags de relacionamento**, insira até 9 tags de relacionamento e clique em **continuar**.

O serviço Cloud Sync atribui as tags a cada objeto que ele sincroniza com o bucket do S3.

11. Revise os detalhes da relação de sincronização e clique em **criar relacionamento**.

Resultado

O Cloud Sync inicia a sincronização de dados entre a origem e o destino.

Pagando por relacionamentos de sincronização após o término da avaliação gratuita

Há duas maneiras de pagar pelas relações de sincronização após o término da avaliação gratuita de 14 dias. A primeira opção é se inscrever na AWS ou no Azure para pagar conforme o uso ou pagar anualmente. A segunda opção é comprar licenças diretamente da NetApp.

Você pode usar licenças do NetApp com uma assinatura da AWS ou do Azure. Por exemplo, se você tiver 25 relacionamentos de sincronização, poderá pagar pelas primeiras 20 relações de sincronização usando uma licença e pagar conforme o uso da AWS ou do Azure com as 5 relações de sincronização restantes.

["Saiba mais sobre como as licenças funcionam"](#).

E se eu não pagar imediatamente após o fim da minha avaliação gratuita? 8217

Você não será capaz de criar relacionamentos adicionais. Relacionamentos existentes não são excluídos, mas você não pode fazer alterações a eles até que você assine ou insira uma licença.

assinatura da AWS

A AWS permite que você pague conforme o uso ou pague anualmente.

Passos para pagar conforme o uso

1. Clique em **Sync > Licensing**.
2. Selecione **AWS**
3. Clique em **Subscribe** e, em seguida, clique em **Continue**.
4. Inscreva-se no AWS Marketplace e faça login novamente no serviço Cloud Sync para concluir o Registro.

O vídeo a seguir mostra o processo:

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

Passos para pagar anualmente

1. "Vá para a página do AWS Marketplace".
2. Clique em **continuar para assinar**.
3. Selecione suas opções de contrato e clique em **criar contrato**.

subscrição do Azure

O Azure permite que você pague conforme o uso ou pague anualmente.

O que você vai precisar

Uma conta de usuário do Azure que tenha permissões de Colaborador ou proprietário na assinatura relevante.

Passos

1. Clique em **Sync > Licensing**.
2. Selecione **Azure**.
3. Clique em **Subscribe** e, em seguida, clique em **Continue**.
4. No portal do Azure, clique em **criar**, selecione suas opções e clique em **Inscrever-se**.

Selecione **mensal** para pagar por hora, ou **anual** para pagar por um ano antes.

5. Quando a implementação estiver concluída, clique no nome do recurso SaaS no pop-up de notificação.
6. Clique em **Configurar conta** para retornar ao Cloud Sync.

O vídeo a seguir mostra o processo:

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

comprando licenças da NetApp e adicionando-as ao Cloud Sync

Para pagar antecipadamente pelas relações de sincronização, você deve comprar uma ou mais licenças e adicioná-las ao serviço Cloud Sync.

Passos

1. Compre uma licença por mailto:ng-cloudsync-Contact at NetApp.com?subject: Cloud%20Sync%20Service%20-%20BYOL%20License%20Purchase%20Request[contactar o NetApp].
2. No Cloud Manager, clique em **Sync > Licensing**.
3. Clique em **Adicionar licença** e adicione a licença.

Tutoriais

Cópia de ACLs entre compartilhamentos SMB

O Cloud Sync pode copiar listas de controle de acesso (ACLs) entre um compartilhamento SMB de origem e um compartilhamento SMB de destino. Se necessário, você pode preservar manualmente as ACLs usando robocopy.

Opções

- [Configure o Cloud Sync para copiar ACLs automaticamente](#)
- [Copie manualmente as ACLs](#)

Configurando o Cloud Sync para copiar ACLs entre servidores SMB

Copie ACLs entre servidores SMB habilitando uma configuração quando você cria um relacionamento ou depois de criar um relacionamento.

Observe que esse recurso está disponível para novas relações de sincronização criadas após a versão de 23 de fevereiro de 2020. Se você quiser usar esse recurso com relacionamentos existentes criados antes dessa data, precisará recriar o relacionamento.

O que você vai precisar

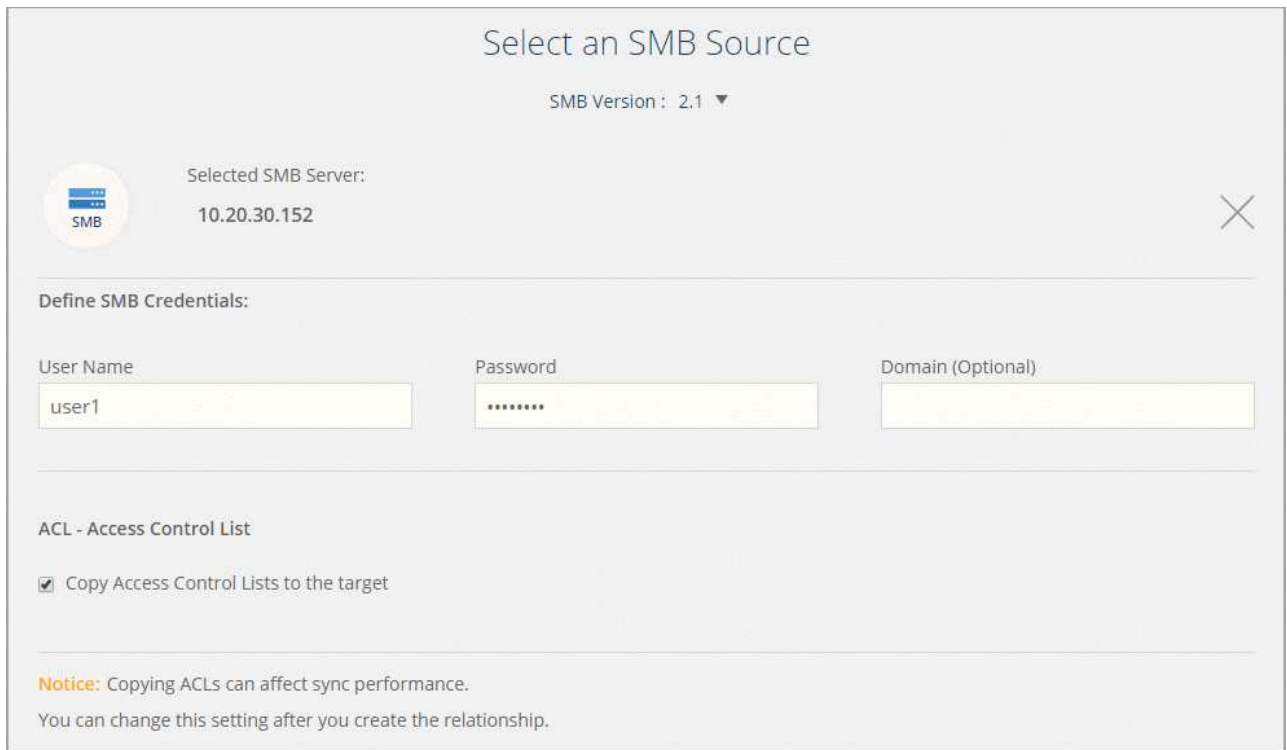
- Uma nova relação de sincronização ou uma relação de sincronização existente criada após a versão de 23 de fevereiro de 2020.
- Qualquer tipo de corretor de dados.

Esse recurso funciona com *qualquer* tipo de agente de dados: AWS, Azure, Google Cloud Platform ou agente de dados local. O agente de dados local pode executar "[qualquer sistema operacional suportado](#)"o

Passos para um novo relacionamento

1. No Cloud Sync, clique em **criar nova sincronização**.
2. Arraste e solte **servidor SMB** para a origem e destino e clique em **continuar**.
3. Na página **servidor SMB**:
 - a. Introduza um novo servidor SMB ou selecione um servidor existente e clique em **continuar**.
 - b. Insira credenciais para o servidor SMB.

c. Selecione **Copiar listas de controle de acesso para o destino** e clique em **continuar**.



4. Siga as instruções restantes para criar a relação de sincronização.

Etapas para um relacionamento existente

1. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
2. Clique em **Configurações**.
3. Selecione **Copiar listas de controle de acesso para o destino**.
4. Clique em **Salvar configurações**.

Resultado

Ao sincronizar dados, o Cloud Sync preserva as ACLs entre os compartilhamentos SMB de origem e destino.

Copiar manualmente ACLs

Você pode preservar manualmente ACLs entre compartilhamentos SMB usando o comando Windows robocopy.

Passos

1. Identifique um host do Windows que tenha acesso total a ambos os compartilhamentos SMB.
2. Se qualquer um dos endpoints exigir autenticação, use o comando **uso líquido** para se conectar aos endpoints a partir do host do Windows.

Você deve executar esta etapa antes de usar o robocopy.

3. A partir do Cloud Sync, crie uma nova relação entre os compartilhamentos SMB de origem e destino ou sincronize um relacionamento existente.
4. Após a conclusão da sincronização de dados, execute o seguinte comando a partir do host do Windows para sincronizar as ACLs e a propriedade:

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

Tanto *source* quanto *target* devem ser especificados usando o formato UNC. Por exemplo:
<server>/<share>/<path>

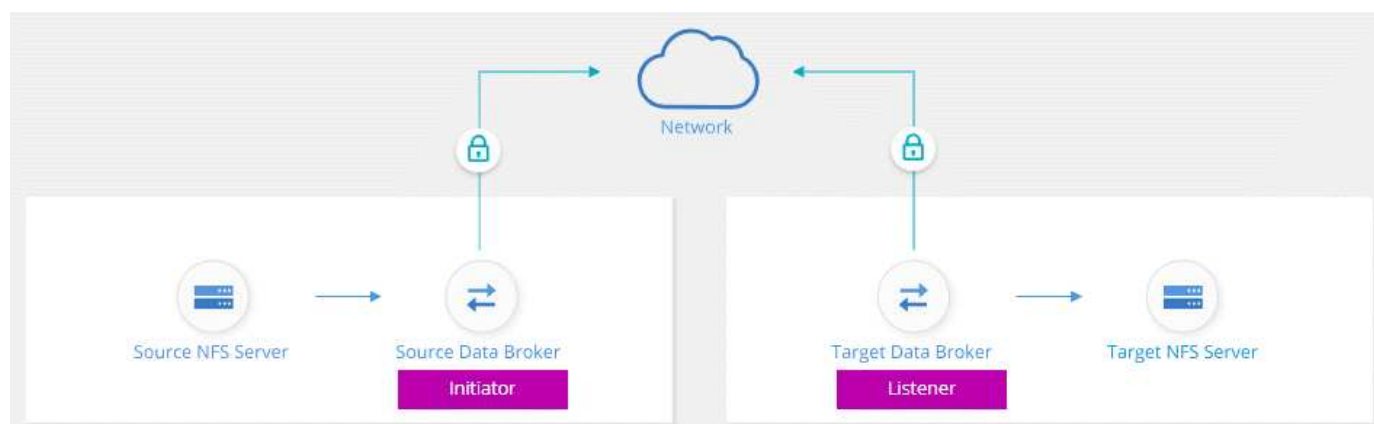
Sincronização de dados NFS com a criptografia de dados em trânsito

Se sua empresa tiver políticas de segurança rígidas, você poderá sincronizar dados NFS com a criptografia de dados em trânsito. Esse recurso é compatível de um servidor NFS para outro servidor NFS e de Azure NetApp Files para Azure NetApp Files.

Por exemplo, você pode querer sincronizar dados entre dois servidores NFS que estão em redes diferentes. Ou talvez seja necessário transferir dados com segurança no Azure NetApp Files entre sub-redes ou regiões.

Como funciona a criptografia de dados em trânsito

A criptografia de dados em trânsito criptografa os dados NFS quando eles são enviados pela rede entre dois corretores de dados. A imagem a seguir mostra uma relação entre dois servidores NFS e dois data brokers:



Um corretor de dados funciona como *iniciador*. Quando é hora de sincronizar dados, ele envia uma solicitação de conexão para o outro corretor de dados, que é o *listener*. Esse corretor de dados escuta solicitações na porta 443. Você pode usar uma porta diferente, se necessário, mas certifique-se de verificar se a porta não está em uso por outro serviço.

Por exemplo, se você sincronizar dados de um servidor NFS no local para um servidor NFS baseado na nuvem, poderá escolher qual agente de dados escuta as solicitações de conexão e quais as envia.

Veja como funciona a criptografia em trânsito:

1. Depois de criar a relação de sincronização, o iniciador inicia uma conexão criptografada com o outro corretor de dados.
2. O corretor de dados de origem criptografa os dados da fonte usando TLS 1,3.
3. Em seguida, ele envia os dados pela rede para o agente de dados de destino.
4. O corretor de dados de destino descriptografa os dados antes de enviá-los para o destino.
5. Após a cópia inicial, o serviço sincroniza todos os dados alterados a cada 24 horas. Se houver dados para sincronizar, o processo começa com o iniciador abrindo uma conexão criptografada com o outro corretor

de dados.

Se preferir sincronizar dados com mais frequência, ["você pode alterar a programação depois de criar o relacionamento"](#).

Versões de NFS compatíveis

- Para servidores NFS, a criptografia de dados em trânsito é compatível com NFS versões 3, 4,0, 4,1 e 4,2.
- Para Azure NetApp Files, a criptografia de dados em trânsito é compatível com NFS versões 3 e 4,1.

O que você precisará para começar

Certifique-se de que tem o seguinte:

- Dois servidores NFS que atendem ["requisitos de origem e destino"](#) ou Azure NetApp Files em duas sub-redes ou regiões.
- Os endereços IP ou nomes de domínio totalmente qualificados dos servidores.
- Locais de rede para dois corretores de dados.

Você pode selecionar um corretor de dados existente, mas ele deve funcionar como o iniciador. O corretor de dados do ouvinte deve ser um *new* corretor de dados.

Se você ainda não implantou um agente de dados, revise os requisitos do agente de dados. Como você tem políticas de segurança rígidas, certifique-se de rever os requisitos de rede, que incluem tráfego de saída da porta 443 e o ["endpoints da internet"](#) que o agente de dados contacta.

- ["Revise a instalação da AWS"](#)
- ["Revise a instalação do Azure"](#)
- ["Revise a instalação da GCP"](#)
- ["Revise a instalação do host Linux"](#)

Sincronização de dados NFS com a criptografia de dados em trânsito

Crie uma nova relação de sincronização entre dois servidores NFS ou entre Azure NetApp Files, ative a opção de criptografia em trânsito e siga as instruções.

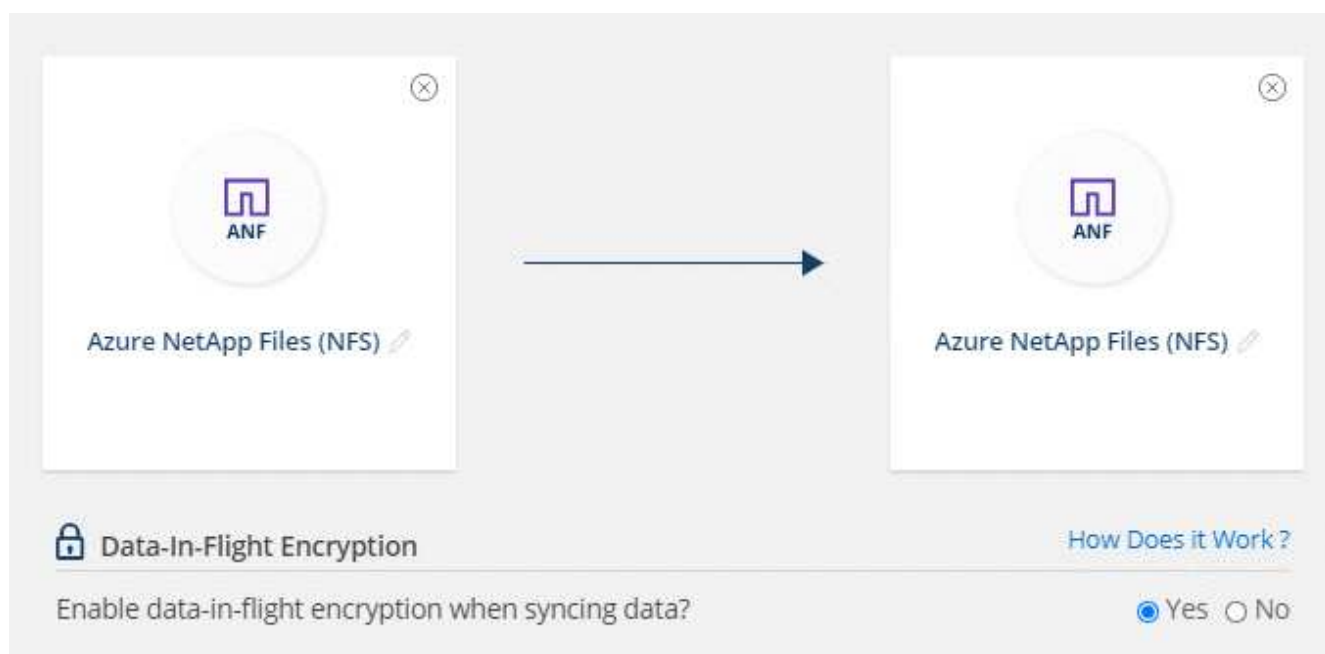
Passos

1. Clique em **criar nova sincronização**.
2. Arraste e solte **servidor NFS** para os locais de origem e destino ou **Azure NetApp Files** para os locais de origem e destino e selecione **Sim** para ativar a criptografia de dados em trânsito.

A imagem a seguir mostra o que você selecionaria para sincronizar dados entre dois servidores NFS:



A imagem a seguir mostra o que você selecionaria para sincronizar dados entre o Azure NetApp Files:

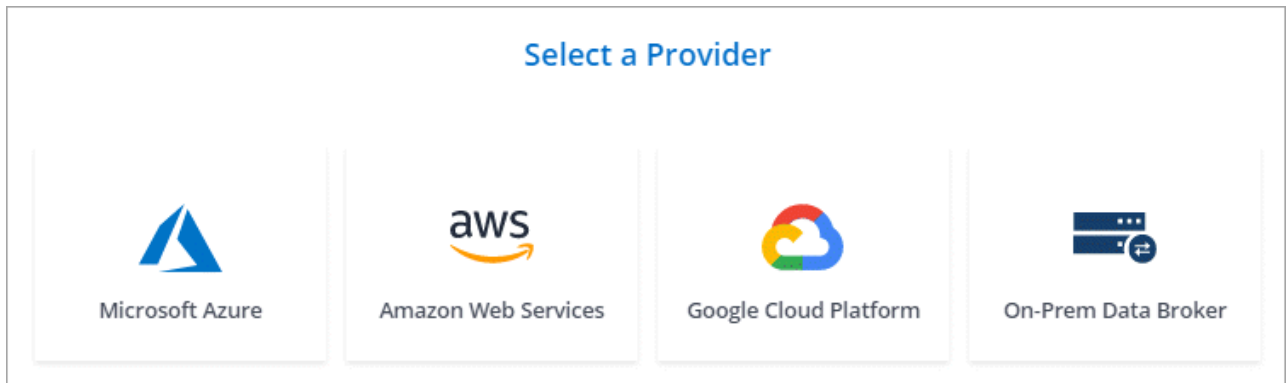


3. Siga as instruções para criar a relação:

- a. **Servidor NFS/Azure NetApp Files:** Escolha a versão NFS e especifique uma nova fonte NFS ou selecione um servidor existente.
- b. **Definir funcionalidade do Data Broker:** Defina qual agente de dados *escuta* para solicitações de conexão em uma porta e qual *inicia* a conexão. Faça sua escolha com base em seus requisitos de rede.
- c. **Data Broker:** Siga as instruções para adicionar um novo corretor de dados de origem ou selecionar um corretor de dados existente.

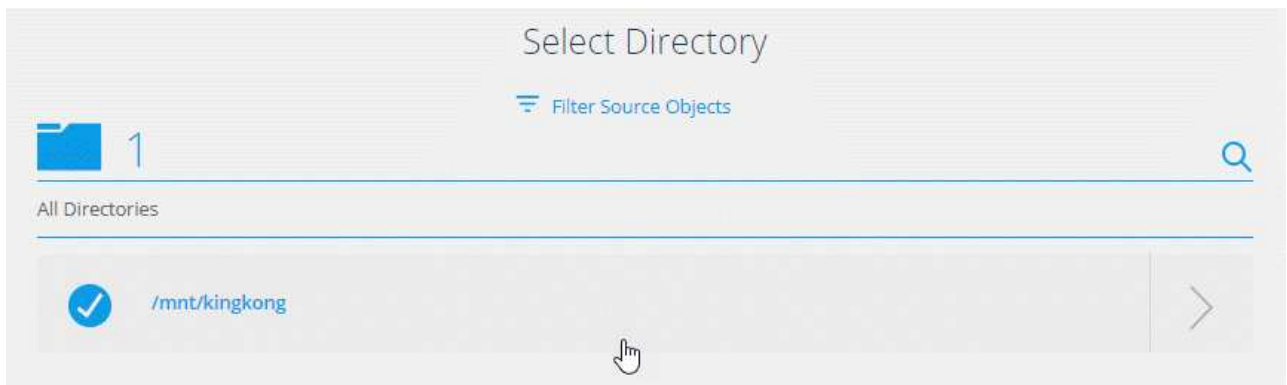
Se o corretor de dados de origem age como o ouvinte, então ele deve ser um novo corretor de dados.

Se você precisar de um novo corretor de dados, o Cloud Sync solicitará as instruções de instalação. Você pode implantar o agente de dados na nuvem ou baixar um script de instalação para seu próprio host Linux.



- d. **Diretórios:** Escolha os diretórios que você deseja sincronizar selecionando todos os diretórios, ou pesquisando e selecionando um subdiretório.

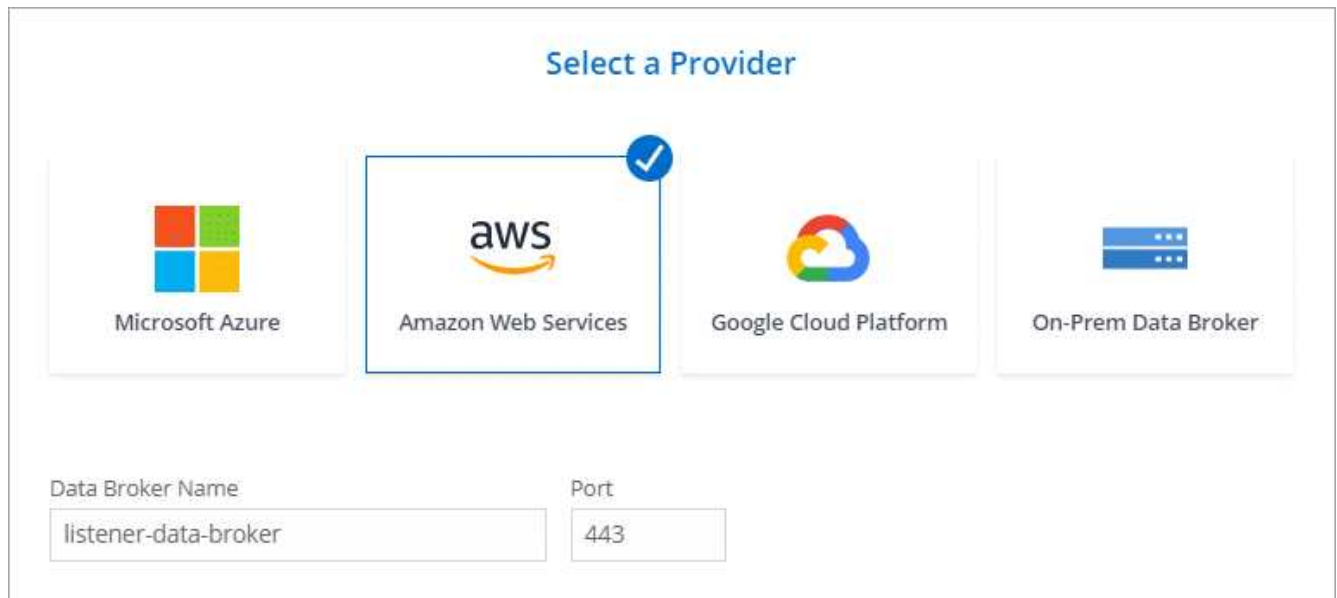
Clique em **Filtrar objetos de origem** para modificar as configurações que definem como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino.



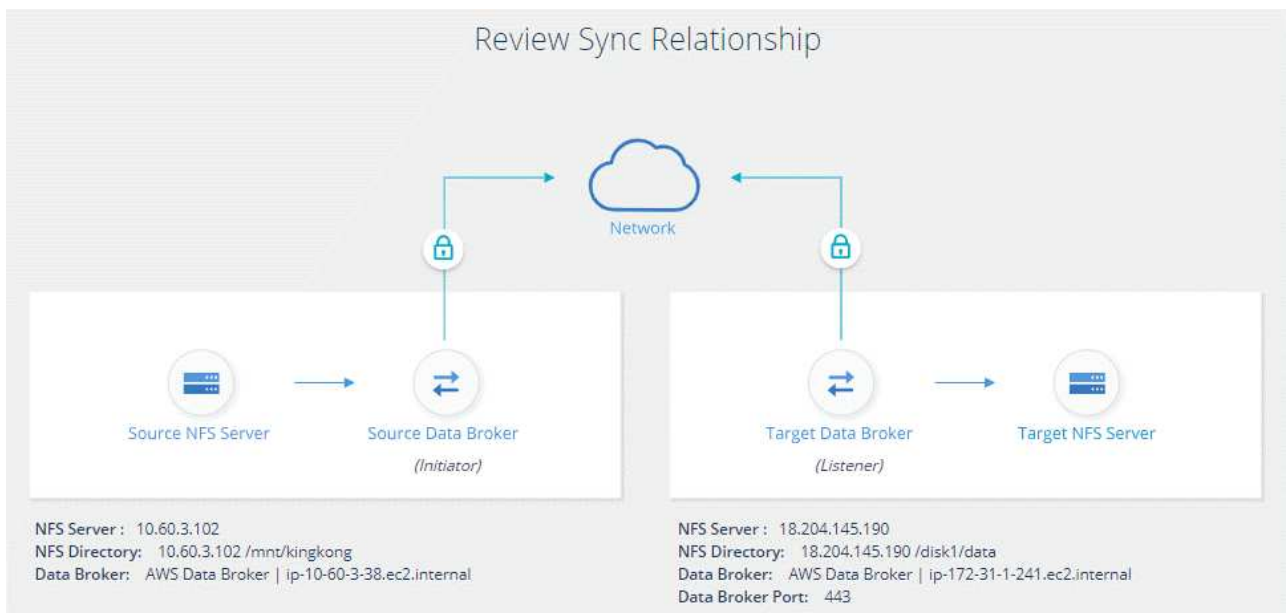
- e. **Servidor NFS de destino/Azure NetApp Files de destino:** Escolha a versão NFS e insira um novo destino NFS ou selecione um servidor existente.
- f. **Target Data Broker:** Siga as instruções para adicionar um novo corretor de dados de origem ou selecionar um corretor de dados existente.

Se o corretor de dados de destino age como ouvinte, então ele deve ser um novo corretor de dados.

Aqui está um exemplo do prompt quando o corretor de dados de destino funciona como ouvinte. Observe a opção de especificar a porta.



- Diretórios de destino:** Selecione um diretório de nível superior ou faça uma pesquisa para selecionar um subdiretório existente ou criar uma nova pasta dentro de uma exportação.
- Configurações:** Defina como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino.
- Revisão:** Revise os detalhes da relação de sincronização e clique em **criar relacionamento**.



Resultado

O Cloud Sync começa a criar a nova relação de sincronização. Quando terminar, clique em **Exibir no Dashboard** para ver detalhes sobre o novo relacionamento.

Gerenciando relacionamentos de sincronização

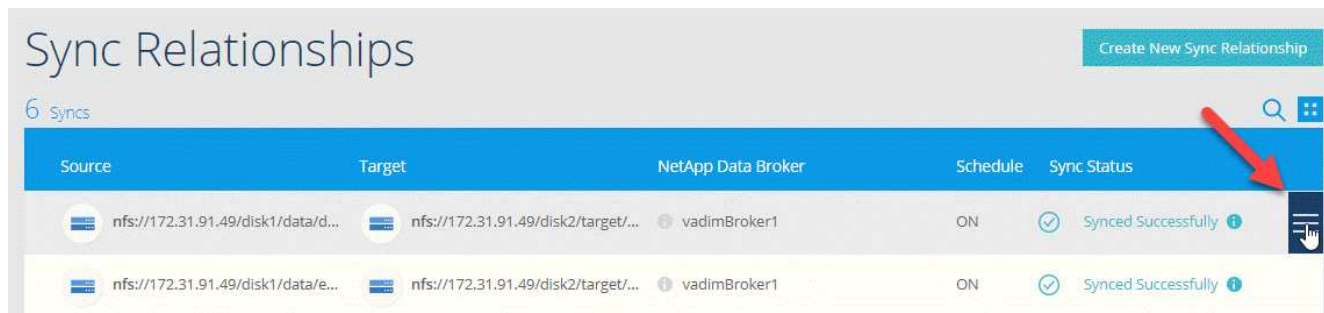
Você pode gerenciar relacionamentos de sincronização a qualquer momento sincronizando dados imediatamente, alterando horários e muito mais.

Realizar uma sincronização de dados imediata

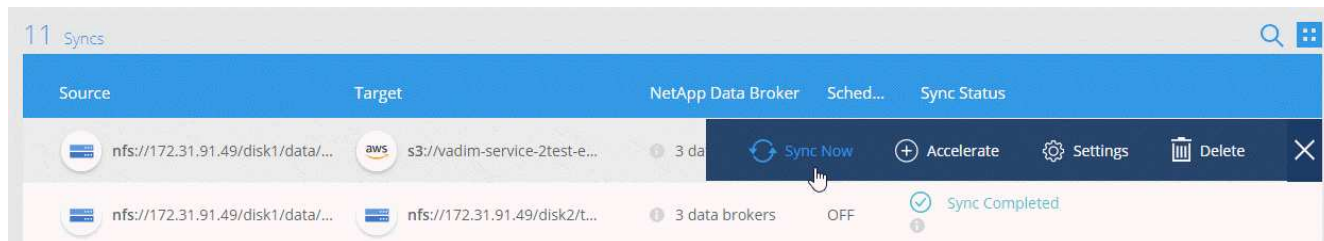
Em vez de esperar pela próxima sincronização agendada, você pode pressionar um botão para sincronizar imediatamente os dados entre a origem e o destino.

Passos

1. No **Painel de sincronização**, passe o Mouse sobre a relação de sincronização e clique no menu de ação.



2. Clique em **Sincronizar agora** e, em seguida, clique em **Sincronizar** para confirmar.



Resultado

O Cloud Sync inicia o processo de sincronização de dados para a relação.

Acelerando o desempenho de sincronização

Acelere o desempenho de uma relação de sincronização adicionando um agente de dados adicional ao relacionamento. O corretor de dados adicional deve ser um corretor de dados *new*.

Como isso funciona

Se os corretores de dados existentes no relacionamento forem usados em outras relações de sincronização, o Cloud Sync também adicionará automaticamente o novo corretor de dados a essas relações.

Por exemplo, digamos que você tenha três relacionamentos:

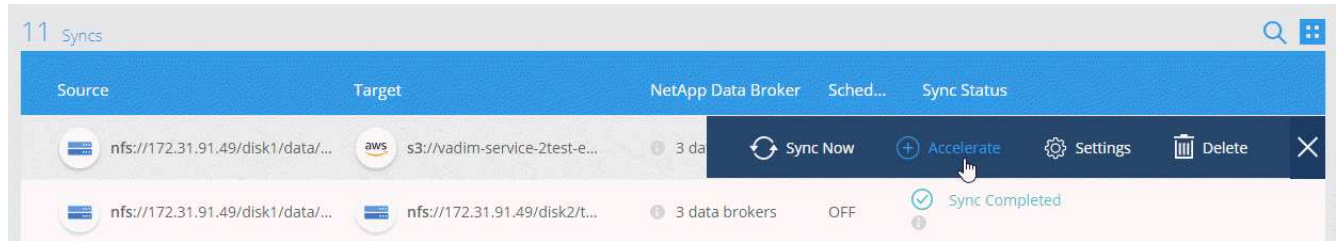
- O relacionamento 1 usa o agente de dados A.
- O relacionamento 2 usa o corretor de dados B
- O relacionamento 3 usa o agente de dados A.

Você quer acelerar o desempenho do relacionamento 1 para adicionar um novo agente de dados a esse relacionamento (agente de dados C). Como o corretor de dados A também é usado no relacionamento 3, o novo corretor de dados também é automaticamente adicionado ao relacionamento 3.

Passos

1. Certifique-se de que pelo menos um dos corretores de dados existentes no relacionamento esteja on-line.

2. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
3. Clique em **Accelerate**.



4. Siga as instruções para criar um novo corretor de dados.

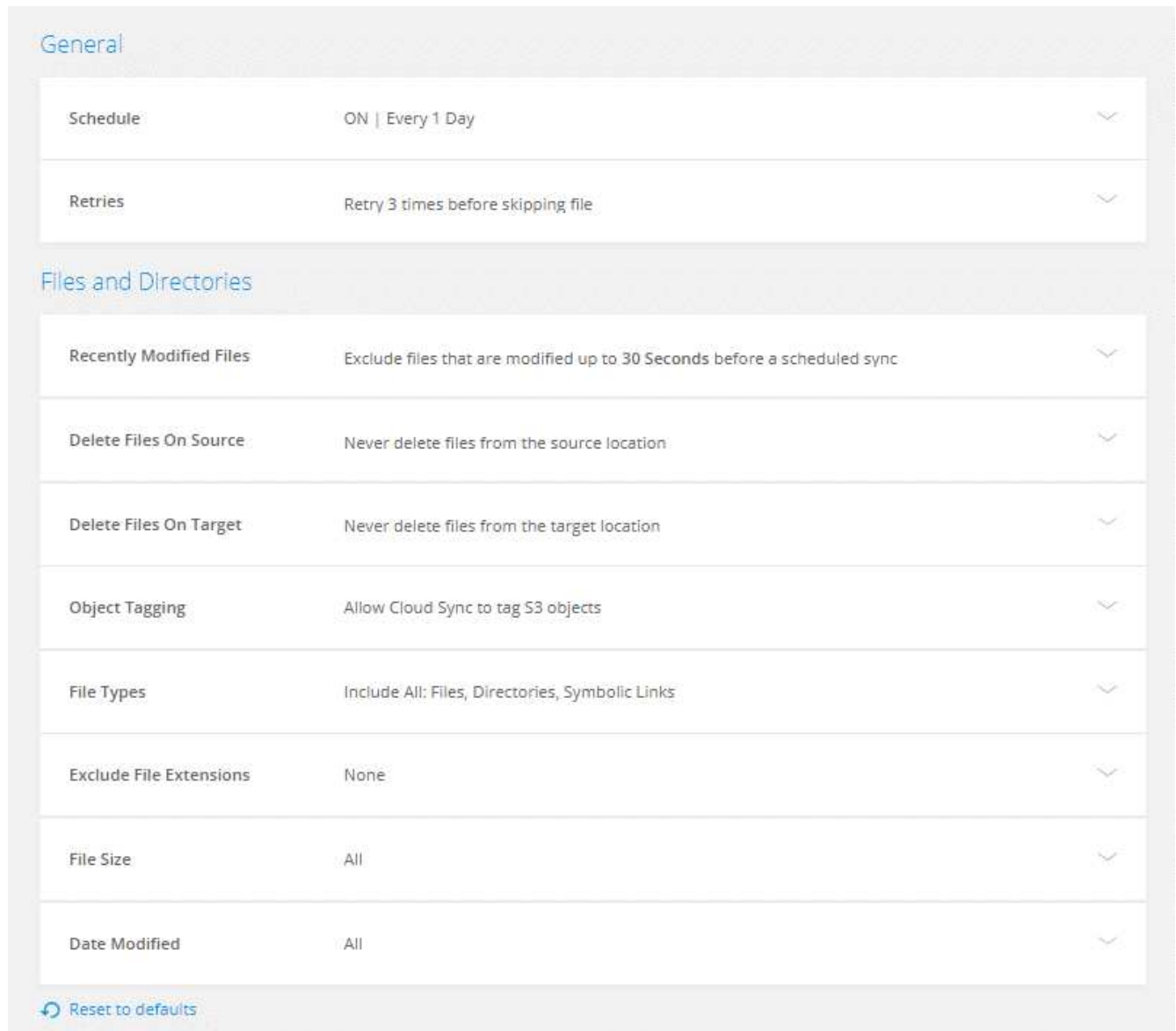
Resultado

O Cloud Sync adiciona o novo agente de dados às relações de sincronização. O desempenho da próxima sincronização de dados deve ser acelerado.

Alterar as definições de uma relação de sincronização

Modifique as configurações que definem como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino.

1. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
2. Clique em **Configurações**.
3. Modifique qualquer uma das definições.



aqui está uma breve descrição de cada configuração:

Programação

Escolha uma programação recorrente para futuras sincronizações ou desative a programação de sincronização. Você pode agendar uma relação para sincronizar dados a cada 1 minutos.

Tenta novamente

Defina o número de vezes que o Cloud Sync deve tentar sincronizar um arquivo antes de ignorá-lo.

Ficheiros modificados recentemente

Escolha excluir arquivos que foram modificados recentemente antes da sincronização programada.

Eliminar ficheiros na origem

Escolha excluir arquivos do local de origem depois que o Cloud Sync copiar os arquivos para o local de destino. Essa opção inclui o risco de perda de dados porque os arquivos de origem são excluídos após serem copiados.

Se você ativar essa opção, também precisará alterar um parâmetro no arquivo `local.json` no corretor de dados. Abra o arquivo e altere o parâmetro chamado `workers.transferrer.delete-on-source` para **true**.

Excluir arquivos no destino

Escolha excluir arquivos do local de destino, se eles foram excluídos da origem. O padrão é nunca excluir arquivos do local de destino.

Marcação de objetos

Quando o AWS S3 é o destino em uma relação de sincronização, o Cloud Sync marca objetos S3 com metadados relevantes para a operação de sincronização. Você pode desativar a marcação de objetos S3, se não for desejado em seu ambiente. Não há impactos no Cloud Sync se você desabilitar a marcação: O Cloud Sync apenas armazena os metadados de sincronização de uma maneira diferente.

Tipos de ficheiros

Defina os tipos de arquivo a serem incluídos em cada sincronização: Arquivos, diretórios e links simbólicos.

Excluir extensões de arquivos

Especifique extensões de arquivo para excluir da sincronização digitando a extensão do arquivo e pressionando **Enter**. Por exemplo, digite *log* ou *.log* para excluir arquivos **.log*. Não é necessário um separador para várias extensões. O vídeo a seguir fornece uma breve demonstração:

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

Tamanho do ficheiro

Escolha sincronizar todos os arquivos, independentemente do seu tamanho ou apenas arquivos que estão em um intervalo de tamanho específico.

Data de modificação

Escolha todos os arquivos independentemente da data da última modificação, arquivos modificados após uma data específica, antes de uma data específica ou entre um intervalo de tempo.

Copiar listas de controlo de acesso para o destino

Escolha copiar listas de controle de acesso (ACLs) entre compartilhamentos SMB de origem e compartilhamentos SMB de destino. Observe que essa opção só está disponível para relacionamentos de sincronização criados após a versão de 23 de fevereiro de 2020.

4. Clique em **Salvar configurações**.

Resultado

O Cloud Sync modifica a relação de sincronização com as novas configurações.

Excluindo relacionamentos

Você pode excluir uma relação de sincronização, se não precisar mais sincronizar dados entre a origem e o destino. Esta ação não exclui a instância do corretor de dados e não exclui dados do destino.

Passos

1. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
2. Clique em **Delete** e, em seguida, clique em **Delete** novamente para confirmar.

Resultado

O Cloud Sync exclui a relação de sincronização.

APIs da Cloud Sync

Os recursos do Cloud Sync disponíveis pela IU da Web também estão disponíveis por meio de APIs RESTful.

Como começar

Para começar a usar as APIs do Cloud Sync, você precisa obter um token de usuário e seu ID de conta do Cloud Central. Você precisará adicionar o token e o ID da conta ao cabeçalho de autorização ao fazer chamadas de API.

Passos

1. Obtenha um token de usuário do NetApp Cloud Central.

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

2. Obtenha seu ID de conta do Cloud Central.

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

Esta API retornará uma resposta como a seguinte:

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

3. Adicione o token de usuário e o ID da conta no cabeçalho de autorização de cada chamada de API.

Exemplo

O exemplo a seguir mostra uma chamada de API para criar um corretor de dados no Microsoft Azure. Você simplesmente substituiria o <user_token> e o <accountId> pelo token e ID obtidos nas etapas anteriores.

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

O que devo fazer quando o token expirar?

O token de usuário do NetApp tem uma data de expiração. Para atualizar o token, você precisa chamar a API da etapa 1 novamente.

A resposta da API inclui um campo "expires_in" que indica quando o token expira.

Referência da API

A documentação para cada API do Cloud Sync está disponível no ["Centro de nuvem da NetApp"](#).

Usando APIs de lista

As APIs de lista são APIs assíncronas, portanto, o resultado não retorna imediatamente (por exemplo: GET /data-brokers/{id}/list-nfs-export-folders E GET /data-brokers/{id}/list-s3-buckets). A única resposta do servidor é o status HTTP 202. Para obter o resultado real, você deve usar a GET /messages/client API.

Passos

1. Chame a API de lista que você deseja usar.
2. Use a GET /messages/client API para exibir o resultado da operação.
3. Use a mesma API anexando-a com o ID que você acabou de receber: GET `http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

Observe que o ID muda sempre que você chamar a GET /messages/client API.

Exemplo

Quando você chama a list-s3-buckets API, um resultado não é retornado imediatamente:

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

O resultado é o código de status HTTP 202, o que significa que a mensagem foi aceita, mas ainda não foi processada.

Para obter o resultado da operação, você precisa usar a seguinte API:

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

O resultado é uma matriz com um objeto que inclui um campo de ID. O campo ID representa a última mensagem enviada pelo servidor. Por exemplo:

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

Agora você faria a seguinte chamada de API usando o ID que acabou de receber:

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

O resultado é uma matriz de mensagens. Dentro de cada mensagem há um objeto payload, que consiste no nome da operação (como chave) e seu resultado (como valor). Por exemplo:

```
[
  {
    "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"
  }
]
```

Perguntas frequentes técnicas do Cloud Sync

Esta FAQ pode ajudar se você está apenas procurando uma resposta rápida para uma pergunta.

Como começar

As perguntas a seguir estão relacionadas a como começar a usar o Cloud Sync.

Como funciona o Cloud Sync?

O Cloud Sync usa o software de corretor de dados NetApp para sincronizar dados de uma origem para um destino (isso é chamado de *relação de sincronização*).

O corretor de dados controla as relações de sincronização entre suas fontes e alvos. Depois de configurar uma relação de sincronização, o Cloud Sync analisa o sistema de origem e o divide em vários fluxos de replicação para enviar para os dados de destino selecionados.

Após a cópia inicial, o serviço sincroniza todos os dados alterados com base na programação definida.

Como funciona o teste gratuito de 14 dias?

A avaliação gratuita de 14 dias começa quando você se inscreve no serviço Cloud Sync. Você não está sujeito a cobranças do NetApp para relacionamentos do Cloud Sync criados por 14 dias. No entanto, todas as cobranças de recursos para qualquer agente de dados que você implantar ainda se aplicam.

Quanto custa o Cloud Sync?

Existem dois tipos de custos associados ao uso do Cloud Sync: Taxas de serviço e taxas de recursos.

Taxas de serviço

Para os preços de pagamento conforme o uso, as taxas de serviço do Cloud Sync são de hora em hora, com base no número de relacionamentos de sincronização criados por você.

- ["Veja a definição de preço para pagamento conforme o uso na AWS"](#)
- ["Veja os preços anuais na AWS"](#)
- ["Ver preços no Azure"](#)

As licenças do Cloud Sync também estão disponíveis através do seu representante da NetApp. Cada licença permite 20 relações de sincronização por 12 meses.

["Saiba mais sobre licenças"](#).

Cobranças de recursos

As cobranças por recursos estão relacionadas aos custos de computação e storage para executar o agente de dados na nuvem.

Como é cobrado o Cloud Sync?

Há duas maneiras de pagar pelas relações de sincronização após o término da avaliação gratuita de 14 dias. A primeira opção é se inscrever na AWS ou no Azure, o que permite que você pague conforme o uso ou pague anualmente. A segunda opção é comprar licenças diretamente da NetApp.

Posso usar o Cloud Sync fora da nuvem?

Sim, você pode usar o Cloud Sync em uma arquitetura que não seja na nuvem. A origem e o destino podem residir no local, assim como o agente de dados.

Observe os seguintes pontos-chave sobre o uso do Cloud Sync fora da nuvem:

- Para sincronização no local, um bucket privado do Amazon S3 está disponível por meio do NetApp StorageGRID.
- O corretor de dados precisa de uma conexão com a Internet para se comunicar com o serviço Cloud Sync.
- Se você não comprar uma licença diretamente da NetApp, precisará de uma conta da AWS ou do Azure para a cobrança do serviço PAYGO Cloud Sync.

Como faço para acessar o Cloud Sync?

O Cloud Sync está disponível no Gerenciador de nuvem na guia **Sincronizar**.

Fontes e alvos suportados

As perguntas a seguir relacionadas à origem e aos destinos que são suportados em um relacionamento de sincronização.

Quais fontes e alvos o Cloud Sync suporta?

O Cloud Sync suporta muitos tipos diferentes de relações de sincronização. ["Veja a lista inteira"](#).

Quais versões de NFS e SMB são compatíveis com o Cloud Sync?

O Cloud Sync é compatível com NFS versão 3 e posterior, e SMB versão 1 e posterior.

["Saiba mais sobre os requisitos de sincronização"](#).

Quando o Amazon S3 é o destino, os dados podem ser dispostos em camadas em uma classe de armazenamento S3 específica?

Sim, você pode escolher uma classe de armazenamento S3 específica quando o AWS S3 for o destino:

- Standard (esta é a classe padrão)
- Disposição em camadas inteligente
- Acesso padrão-infrequente
- Uma zona de acesso pouco frequente
- Glacier
- Glacier Deep Archive

E quanto às camadas de storage do Azure Blob?

Você pode escolher uma categoria de storage específica do Azure Blob quando um contêiner de Blob é o destino:

- Armazenamento a quente
- Armazenamento frio

Rede

As perguntas a seguir referem-se aos requisitos de rede para o Cloud Sync.

Quais são os requisitos de rede para o Cloud Sync?

O ambiente do Cloud Sync exige que o agente de dados esteja conectado à origem e ao destino por meio do protocolo selecionado (NFS, SMB, EFS) ou da API de storage de objetos (Amazon S3, Azure Blob, IBM Cloud Object Storage).

Além disso, o corretor de dados precisa de uma conexão de saída de Internet pela porta 443 para que possa se comunicar com o serviço Cloud Sync e entrar em Contato com alguns outros serviços e repositórios.

Para mais detalhes, ["rever os requisitos de rede"](#).

Há limitações de rede relacionadas à conectividade do data broker?

Os corretores de dados exigem acesso à Internet. Não oferecemos suporte a um servidor proxy ao implantar o corretor de dados no Azure ou no Google Cloud Platform.

Sincronização de dados

As perguntas a seguir referem-se a como a sincronização de dados funciona.

Com que frequência ocorre a sincronização?

A programação padrão é definida para sincronização diária. Após a sincronização inicial, você pode:

- Modifique a programação de sincronização para o número desejado de dias, horas ou minutos
- Desative a programação de sincronização
- Eliminar a programação de sincronização (nenhum dado será perdido; apenas a relação de sincronização será removida)

Qual é a programação mínima de sincronização?

Você pode agendar uma relação para sincronizar dados a cada 1 minutos.

O corretor de dados tenta novamente quando um arquivo não consegue sincronizar? Ou o tempo limite?

O corretor de dados não expira quando um único arquivo falha na transferência. Em vez disso, o corretor de dados tenta novamente 3 vezes antes de pular o arquivo. O valor de repetição é configurável nas definições de uma relação de sincronização.

["Saiba como alterar as configurações de uma relação de sincronização"](#).

E se eu tiver um conjunto de dados muito grande?

Se um único diretório contém 600.000 arquivos ou mais, <mailto:ng-cloudsync-support@NetApp.com> [Contact US] para que possamos ajudá-lo a configurar o corretor de dados para lidar com a carga útil. Talvez seja necessário adicionar memória adicional à máquina do corretor de dados.

Segurança

As seguintes perguntas relacionadas à segurança.

O Cloud Sync é seguro?

Sim. Toda a conectividade de rede do serviço Cloud Sync é feita usando ["Amazon Simple Queue Service \(SQS\)"](#)o .

Toda a comunicação entre o agente de dados e o Amazon S3, Azure Blob, Google Cloud Storage e IBM Cloud Object Storage é feita por meio do protocolo HTTPS.

Se você estiver usando o Cloud Sync com sistemas locais (de origem ou destino), veja algumas opções de conectividade recomendadas:

- Uma conexão AWS Direct Connect, Azure ExpressRoute ou Google Cloud Interconnect, que não é roteada pela Internet (e só pode se comunicar com as redes de nuvem especificadas)

- Uma conexão VPN entre seu dispositivo de gateway local e suas redes na nuvem
- Para transferência de dados extra segura com buckets do S3, armazenamento de Blobs do Azure ou Google Cloud Storage, é possível estabelecer um endpoint Amazon Private S3, pontos de extremidade de serviço da rede virtual do Azure ou o acesso privado do Google.

Qualquer um desses métodos estabelece uma conexão segura entre seus servidores nas locais e um agente de dados Cloud Sync.

Os dados são criptografados pelo Cloud Sync?

- O Cloud Sync é compatível com criptografia de dados em trânsito entre servidores NFS de origem e destino. "[Saiba mais](#)".
- A criptografia não é suportada com SMB.
- Quando um bucket do Amazon S3 é o destino em uma relação de sincronização, você pode escolher se deseja ativar a criptografia de dados usando a criptografia AWS KMS ou AES-256.

Permissões

As perguntas a seguir estão relacionadas às permissões de dados.

As permissões de dados SMB são sincronizadas com o local de destino?

Você pode configurar o Cloud Sync para preservar listas de controle de acesso (ACLs) entre um compartilhamento SMB de origem e um compartilhamento SMB de destino. Ou você mesmo pode copiar manualmente as ACLs. "[Saiba como copiar ACLs entre compartilhamentos SMB](#)".

As permissões de dados NFS são sincronizadas com o local de destino?

O Cloud Sync copia automaticamente as permissões NFS entre servidores NFS da seguinte forma:

- NFS versão 3: O Cloud Sync copia as permissões e o proprietário do grupo de usuários.
- NFS versão 4: O Cloud Sync copia as ACLs.

Desempenho

As perguntas a seguir referem-se ao desempenho do Cloud Sync.

O que representa o indicador de progresso de uma relação de sincronização?

A relação de sincronização mostra a taxa de transferência do adaptador de rede do corretor de dados. Se você acelerou o desempenho de sincronização usando vários corretores de dados, a taxa de transferência será a soma de todo o tráfego. Essa taxa de transferência é atualizada a cada 20 segundos.

Estou enfrentando problemas de desempenho. Podemos limitar o número de transferências simultâneas?

O corretor de dados pode sincronizar arquivos 4 de cada vez. Se você tiver arquivos muito grandes (vários TBs cada), pode levar muito tempo para concluir o processo de transferência e o desempenho pode ser afetado.

Limitar o número de transferências simultâneas pode ajudar. [Mailto:ng-cloudsync-support@NetApp.com](mailto:ng-cloudsync-support@NetApp.com)[Contacte-nos para obter ajuda].

Por que estou tendo baixo desempenho com o Azure NetApp Files?

Quando você sincroniza dados com ou do Azure NetApp Files, você pode ter falhas e problemas de desempenho se o nível de serviço de disco for padrão.

Altere o nível de serviço para Premium ou Ultra para melhorar o desempenho de sincronização.

["Saiba mais sobre os níveis de serviço e a taxa de transferência do Azure NetApp Files"](#).

Por que estou tendo baixo desempenho com o Cloud Volumes Service para AWS?

Ao sincronizar dados de ou para um volume de nuvem, você pode ter falhas e problemas de desempenho se o nível de performance do volume de nuvem for padrão.

Altere o nível de serviço para Premium ou Extreme para melhorar o desempenho de sincronização.

Quanto corretores de dados são necessários?

Ao criar um novo relacionamento, você começa com um único agente de dados (a menos que você tenha selecionado um agente de dados existente que pertence a um relacionamento de sincronização acelerada). Em muitos casos, um único agente de dados pode atender aos requisitos de desempenho de um relacionamento de sincronização. Se isso não acontecer, você pode acelerar o desempenho de sincronização adicionando corretores de dados adicionais. Mas você deve primeiro verificar outros fatores que podem afetar o desempenho da sincronização.

Vários fatores podem afetar o desempenho da transferência de dados. O desempenho geral da sincronização pode ser afetado devido à largura de banda, latência e topologia da rede, bem como às especificações de VM do agente de dados e ao desempenho do sistema de armazenamento. Por exemplo, um único corretor de dados em um relacionamento de sincronização pode atingir 100 MB/s, enquanto a taxa de transferência de disco no destino pode permitir apenas 64 MB/s. Como resultado, o agente de dados continua tentando copiar os dados, mas o destino não consegue atender ao desempenho do agente de dados.

Portanto, certifique-se de verificar o desempenho de sua rede e a taxa de transferência de disco no destino.

Depois, você pode considerar acelerar o desempenho de sincronização adicionando um agente de dados adicional para compartilhar a carga desse relacionamento. ["Saiba como acelerar o desempenho de sincronização"](#).

Eliminar coisas

As perguntas a seguir referem-se à exclusão de relacionamentos de sincronização e dados de fontes e destinos.

O que acontece se eu excluir meu relacionamento com o Cloud Sync?

A exclusão de um relacionamento interrompe todas as futuras sincronizações de dados e encerra o pagamento. Todos os dados sincronizados com o alvo permanecem no estado em que se encontram.

O que acontece se eu excluir algo do meu servidor de origem? É removido do alvo também?

Por padrão, se você tiver uma relação de sincronização ativa, o item excluído no servidor de origem não será excluído do destino durante a próxima sincronização. Mas há uma opção nas configurações de sincronização para cada relacionamento, onde você pode definir que o Cloud Sync excluirá arquivos no local de destino se eles foram excluídos da origem.

["Saiba como alterar as configurações de uma relação de sincronização"](#).

O que acontece se eu excluir algo do meu alvo? É removido da minha fonte também?

Se um item for excluído do destino, ele não será removido da origem. O relacionamento é unidirecional, da origem ao destino. No próximo ciclo de sincronização, o Cloud Sync compara a origem com o destino, identifica que o item está ausente e o Cloud Sync o copia novamente da origem para o destino.

Solução de problemas

["Base de Conhecimento da NetApp: Perguntas frequentes do Cloud Sync: Suporte e solução de problemas"](#)

Mergulho profundo do agente de dados

A seguinte pergunta diz respeito ao corretor de dados.

Você pode explicar a arquitetura do corretor de dados?

Claro. Aqui estão os pontos mais importantes:

- O corretor de dados é um aplicativo node.js executado em um host Linux.
- O Cloud Sync implanta o agente de dados da seguinte forma:
 - AWS: A partir de um modelo do AWS CloudFormation
 - Azure: Do Azure Resource Manager
 - Google: Do Google Cloud Deployment Manager
 - Se você usa seu próprio host Linux, você precisa instalar manualmente o software
- O software de data broker atualiza-se automaticamente para a versão mais recente.
- O corretor de dados usa o AWS SQS como um canal de comunicação confiável e seguro e para controle e monitoramento. SQS também fornece uma camada de persistência.
- Você pode adicionar corretores de dados adicionais a um relacionamento para aumentar a velocidade de transferência e adicionar alta disponibilidade. Há resiliência de serviços se um agente de dados falhar.

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.