



Tutoriais

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

- Tutoriais 1
 - Cópia de ACLs entre compartilhamentos SMB 1
 - Sincronização de dados NFS com a criptografia de dados em trânsito 3

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.

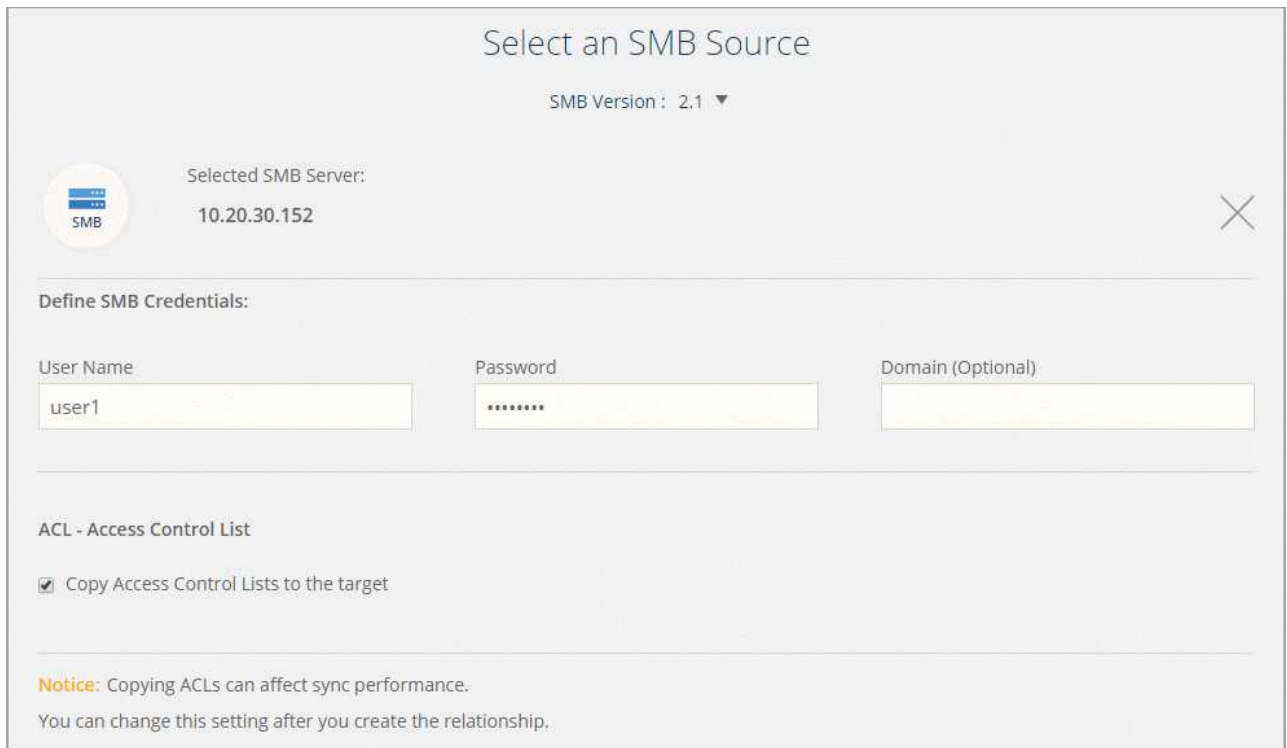
O que você vai precisar

- 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**.



Select an SMB Source

SMB Version : 2.1 ▼

Selected SMB Server:
10.20.30.152

Define SMB Credentials:

User Name: user1 Password: Password Domain (Optional):

ACL - Access Control List

Copy Access Control Lists to the target

Notice: Copying ACLs can affect sync performance.
You can change this setting after you create the relationship.

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>

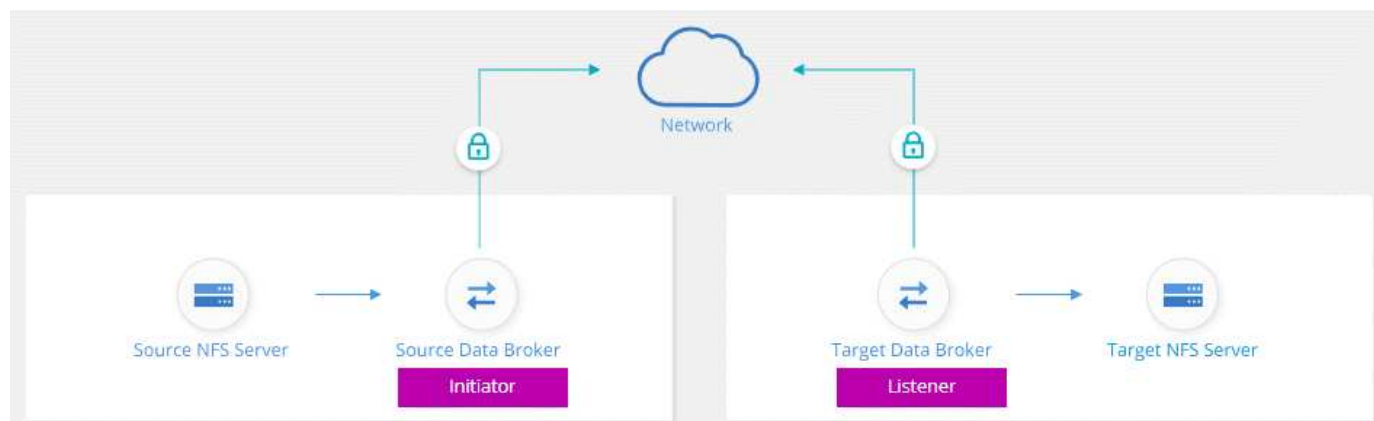
Sincronização de dados NFS com a criptografia de dados em trânsito

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.

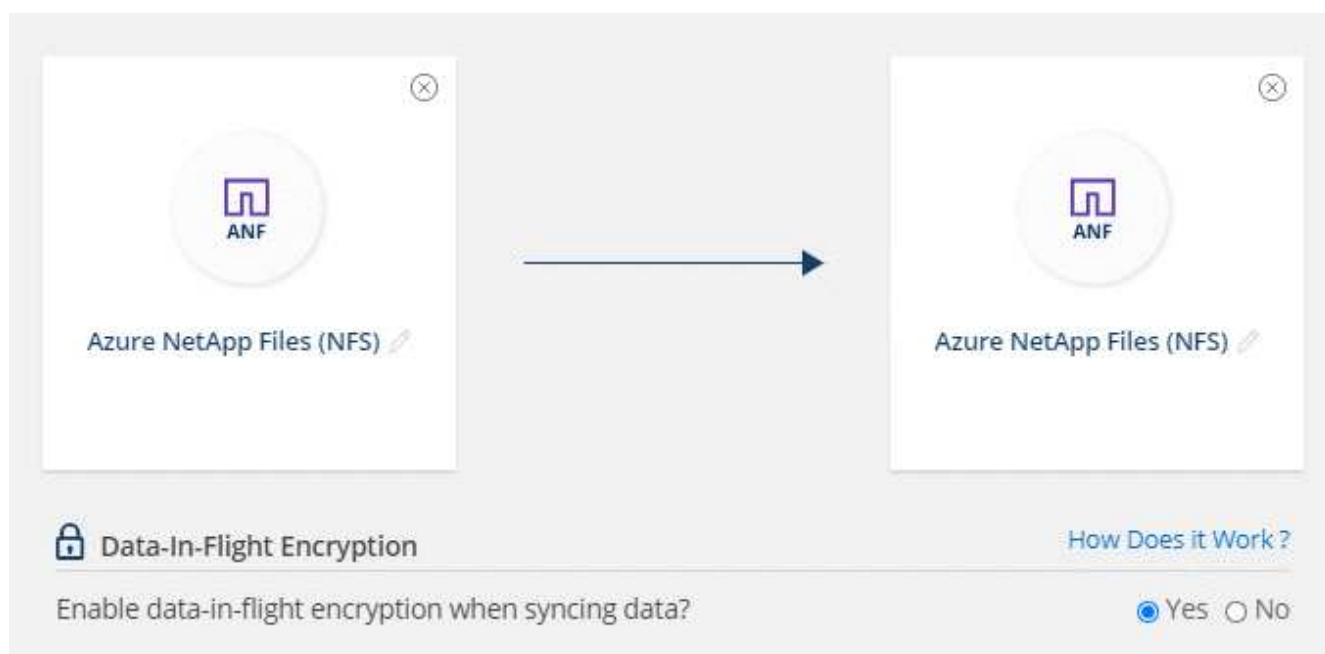
Passos

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:

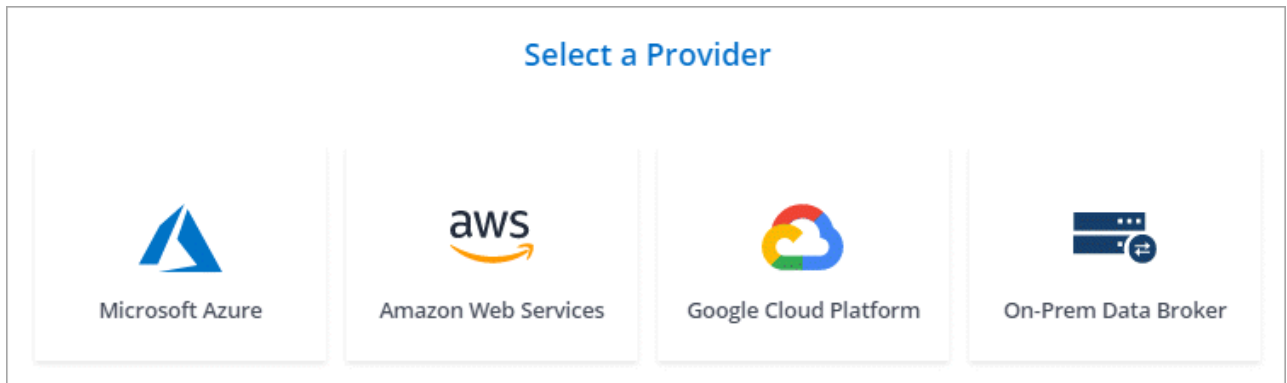


3. Siga as instruções para criar a relação:

- 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.

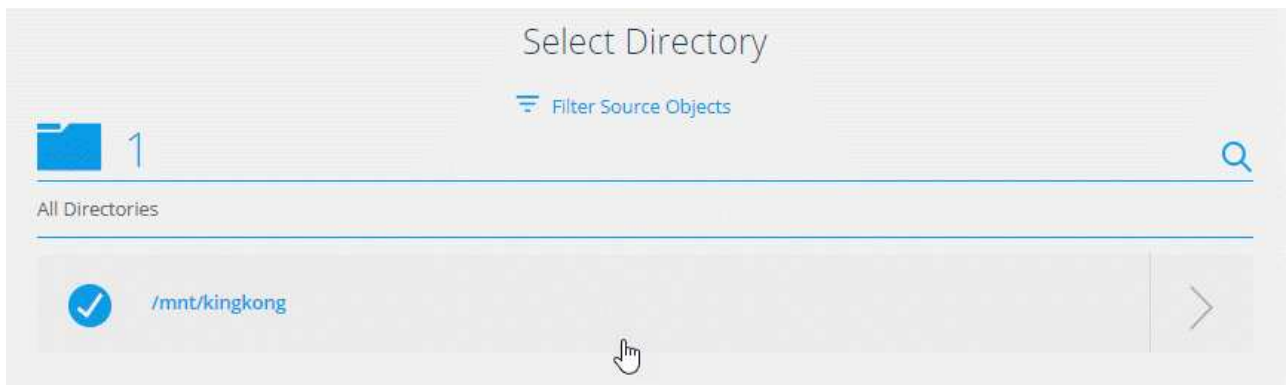
Se o corretor de dados de origem age como o ouvinte, então ele deve ser um novo corretor de dados.

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.

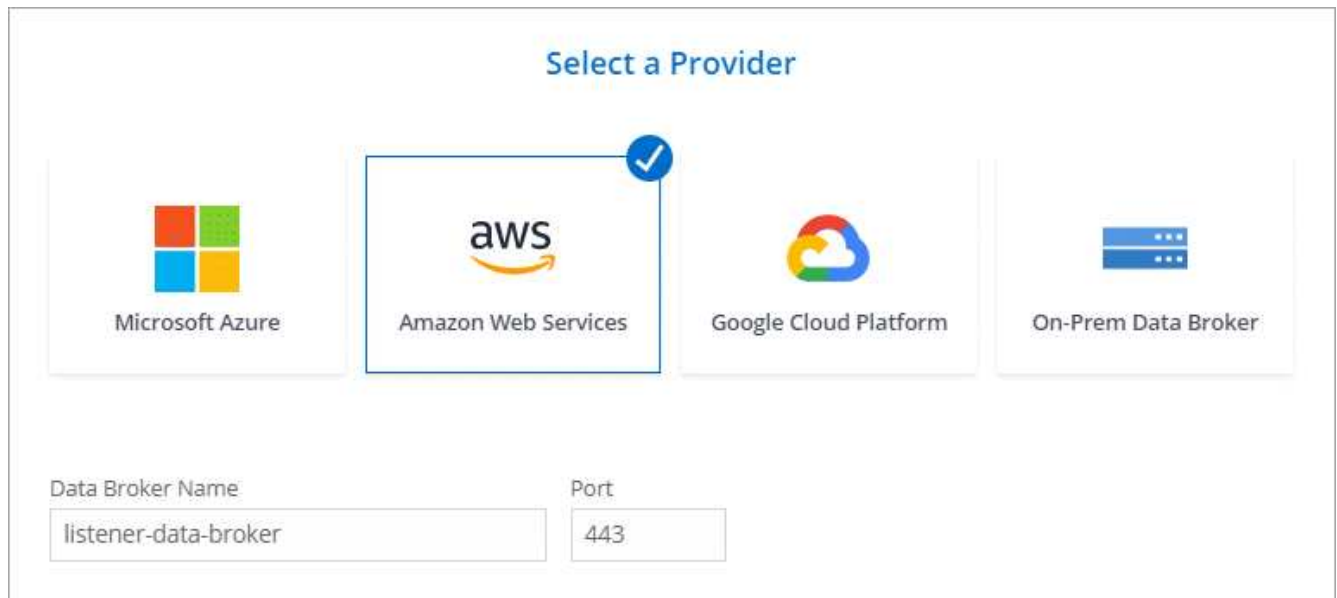
Clique em **Filtrar objetos de origem** para modificar as configurações que definem como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino.



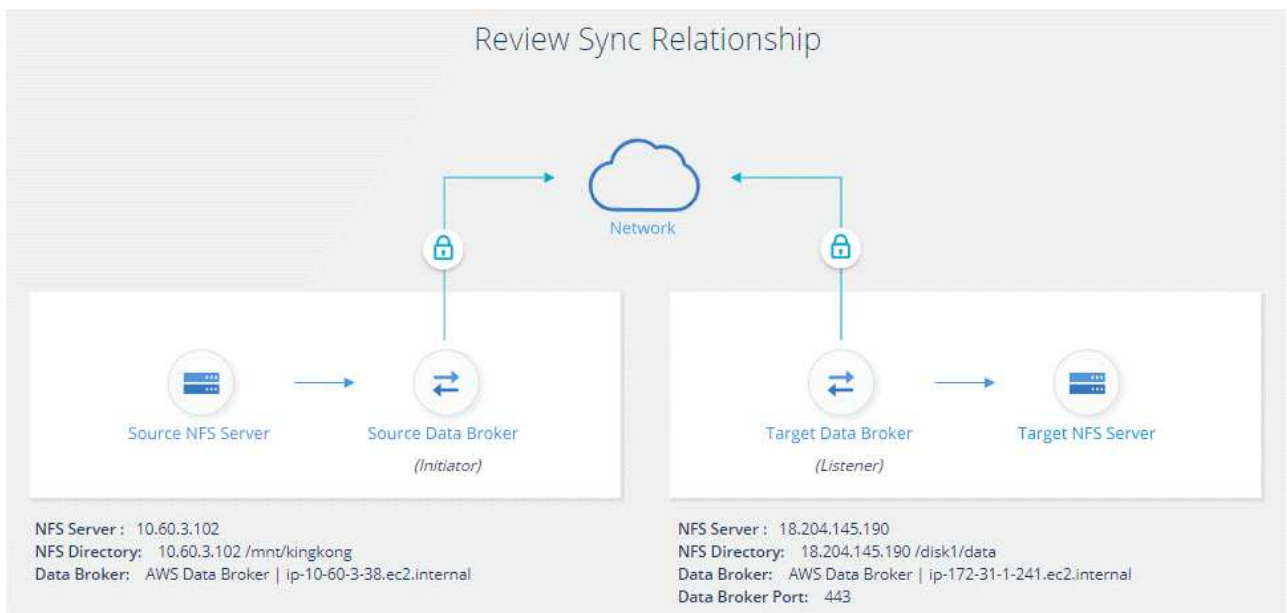
- e. **Servidor NFS de destino/Azure NetApp Files de destino:** Escolha a versão NFS e insira um novo destino NFS ou selecione um servidor existente.
- f. **Target Data Broker:** Siga as instruções para adicionar um novo corretor de dados de origem ou selecionar um corretor de dados existente.

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.

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.