Começar

NetApp Copy and Sync

NetApp
December 16, 2025

Índice

Começar

Saiba mais sobre o NetApp Copy and Sync

O NetApp Copy and Sync oferece uma maneira simples, segura e automatizada de migrar seus dados para qualquer destino, na nuvem ou em suas instalações. Seja um conjunto de dados NAS baseado em arquivo (NFS ou SMB), formato de objeto do Amazon Simple Storage Service (S3), um dispositivo NetApp StorageGRID ou qualquer outro armazenamento de objetos de provedor de nuvem, o Copy and Sync pode convertê-lo e movê-lo para você.

NetApp Console

O NetApp Copy and Sync pode ser acessado por meio do NetApp Console.

O NetApp Console fornece gerenciamento centralizado de serviços de armazenamento e dados da NetApp em ambientes locais e na nuvem em nível empresarial. O Console é necessário para acessar e usar os serviços de dados do NetApp . Como uma interface de gerenciamento, ele permite que você gerencie muitos recursos de armazenamento a partir de uma única interface. Os administradores do console podem controlar o acesso ao armazenamento e aos serviços de todos os sistemas da empresa.

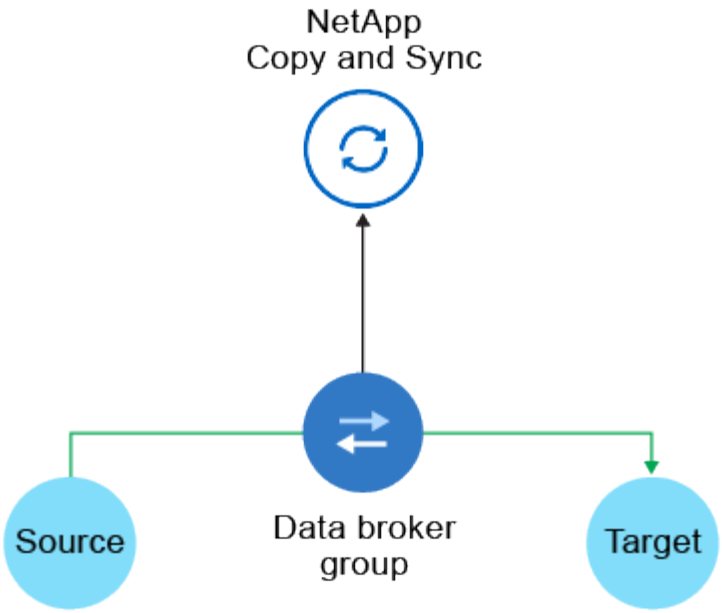
Você não precisa de uma licença ou assinatura para começar a usar o NetApp Console e só incorrerá em cobranças quando precisar implantar agentes do Console na sua nuvem para garantir a conectividade com seus sistemas de armazenamento ou serviços de dados do NetApp . No entanto, alguns serviços de dados da NetApp acessíveis pelo Console são licenciados ou baseados em assinatura.

Saiba mais sobre o "NetApp Console" .

Como funciona o NetApp Copy and Sync

O NetApp Copy and Sync é uma plataforma de software como serviço (SaaS) que consiste em um grupo de corretores de dados, uma interface baseada em nuvem disponível por meio do NetApp Console e uma origem e um destino.

A imagem a seguir mostra a relação entre os componentes Copiar e Sincronizar:



O software NetApp Data Broker sincroniza dados de uma origem para um destino (isso é chamado de *relacionamento de sincronização*). Você pode executar o data broker na AWS, Azure, Google Cloud Platform ou em suas instalações. Um grupo de corretores de dados, que consiste em um ou mais corretores de dados, precisa de uma conexão de saída com a Internet pela porta 443 para poder se comunicar com o Copy and Sync e entrar em contato com alguns outros serviços e repositórios. "Ver a lista de pontos de extremidade" .

Após a cópia inicial, o Copiar e Sincronizar sincroniza todos os dados alterados com base na programação definida por você.

Tipos de armazenamento suportados

O Copy and Sync oferece suporte aos seguintes tipos de armazenamento:

- Qualquer servidor NFS
- Qualquer servidor SMB
- Amazon EFS
- Amazon FSx para ONTAP
- Amazon S3
- Blob do Azure
- Armazenamento do Azure Data Lake Gen2
- Azure NetApp Files
- Caixa (disponível como prévia)
- Cloud Volumes ONTAP
- Armazenamento em nuvem do Google
- Google Drive
- Armazenamento de objetos em nuvem da IBM
- Cluster ONTAP local
- Armazenamento ONTAP S3

- SFTP (usando somente API)
- StorageGRID

"Exibir os relacionamentos de sincronização suportados" .

Custos

Há dois tipos de custos associados ao uso do Copy and Sync: taxas de recursos e taxas de serviço.

Taxas de recursos

Os encargos de recursos estão relacionados aos custos de computação e armazenamento para executar um ou mais corretores de dados na nuvem.

Taxas de serviço

Há duas maneiras de pagar pelos relacionamentos de sincronização após o término do teste gratuito de 14 dias. A primeira opção é assinar o AWS ou o Azure, o que permite que você pague por hora ou anualmente. A segunda opção é comprar licenças diretamente da NetApp.

"Aprenda como funciona o licenciamento" .

Início rápido para NetApp Copy and Sync

Começar a usar o NetApp Copy and Sync inclui algumas etapas.

Efetue login e configure o NetApp Console

Você deve ter começado a usar o NetApp Console, o que inclui fazer login, configurar uma conta e possivelmente implantar um agente do Console e criar sistemas.

Se você quiser criar relacionamentos de sincronização para qualquer um dos seguintes, primeiro você precisa criar ou descobrir um sistema:

- Amazon FSx para ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Clusters ONTAP locais

Um agente de console é necessário para o Cloud Volumes ONTAP, clusters ONTAP locais e Amazon FSx for ONTAP.

- "Aprenda como começar a usar o NetApp Console"
- "Saiba mais sobre os agentes do Console"

Prepare sua fonte e alvo

Verifique se sua origem e destino são suportados e configurados. O requisito mais importante é verificar a conectividade entre o grupo de corretores de dados e os locais de origem e destino.

- "Exibir relacionamentos suportados"

- "Prepare a origem e o destino"

3 Preparar um local para o NetApp Data Broker

O software NetApp Data Broker sincroniza dados de uma origem para um destino (isso é chamado de *relacionamento de sincronização*). Você pode executar o data broker na AWS, Azure, Google Cloud Platform ou em suas instalações. Um grupo de corretores de dados, que consiste em um ou mais corretores de dados, precisa de uma conexão de saída com a Internet pela porta 443 para poder se comunicar com o NetApp Copy and Sync e entrar em contato com alguns outros serviços e repositórios. "Ver a lista de pontos de extremidade" .

O NetApp Copy and Sync orienta você no processo de instalação quando você cria um relacionamento de sincronização, momento em que você pode implantar um data broker na nuvem ou baixar um script de instalação para seu próprio host Linux.

- "Revisar a instalação da AWS"
- "Revisar a instalação do Azure"
- "Revisar a instalação do Google Cloud"
- "Revisar a instalação do host Linux"

4 Crie seu primeiro relacionamento de sincronização

Entrar para "o NetApp Console" , selecione **Sincronizar** e arraste e solte suas seleções para a origem e o destino. Siga as instruções para concluir a configuração. "Saber mais" .

5 Pague pelos seus relacionamentos de sincronização após o término do seu teste gratuito

Assine na AWS ou no Azure para pagar conforme o uso ou anualmente. Ou compre licenças diretamente da NetApp. Basta acessar a página Configurações de licença no NetApp Copy and Sync para configurá-lo. "Saber mais" .

Relacionamentos de sincronização suportados no NetApp Copy and Sync

O NetApp Copy and Sync permite que você sincronize dados de uma origem para um destino. Isso é chamado de relacionamento de sincronização. Você deve entender os relacionamentos suportados antes de começar.

Localização da fonte	Locais de destino suportados
Amazon EFS	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Servidor SMB • StorageGRID
Amazon FSx para ONTAP	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Servidor SMB • StorageGRID

Localização da fonte	Locais de destino suportados
Amazon S3	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Caixa [1] • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Armazenamento ONTAP S3 • Servidor SMB • StorageGRID
Blob do Azure	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Servidor SMB • StorageGRID

Localização da fonte	Locais de destino suportados
Armazenamento do Azure Data Lake Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • FSx para ONTAP • Armazenamento de objetos em nuvem da IBM • Servidor NFS • ONTAP • Armazenamento ONTAP S3 • Servidor SMB • StorageGRID
Azure NetApp Files	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Servidor SMB • StorageGRID
Caixa [1]	• Amazon FSx para ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Servidor SMB • StorageGRID

Localização da fonte	Locais de destino suportados
Cloud Volumes ONTAP	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Servidor SMB • StorageGRID
Armazenamento em nuvem do Google	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Armazenamento ONTAP S3 • Servidor SMB • StorageGRID
Google Drive	• Servidor NFS • Servidor SMB

Localização da fonte	Locais de destino suportados
Armazenamento de objetos em nuvem da IBM	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Caixa [1] • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Servidor SMB • StorageGRID
Servidor NFS	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Google Drive • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Armazenamento ONTAP S3 • Servidor SMB • StorageGRID

Localização da fonte	Locais de destino suportados
Cluster ONTAP local (NFS ou SMB)	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Servidor SMB • StorageGRID
Armazenamento ONTAP S3	• Amazon S3 • Armazenamento do Azure Data Lake Gen2 • Armazenamento em nuvem do Google • Servidor NFS • Servidor SMB • StorageGRID • Armazenamento ONTAP S3
SFTP [2]	S3

Localização da fonte	Locais de destino suportados
Servidor SMB	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Google Drive • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Armazenamento ONTAP S3 • Servidor SMB • StorageGRID
StorageGRID	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob do Azure • Armazenamento do Azure Data Lake Gen2 • Azure NetApp Files • Caixa [1] • Cloud Volumes ONTAP • Armazenamento em nuvem do Google • Armazenamento de objetos em nuvem da IBM • Servidor NFS • Cluster ONTAP local (NFS ou SMB) • Armazenamento ONTAP S3 • Servidor SMB • StorageGRID

Observações:

1. O suporte para caixa está disponível como uma prévia.
2. Os relacionamentos de sincronização com esta origem/destino são suportados somente usando a API Copiar e Sincronizar.

3. Você pode escolher uma camada específica de armazenamento de Blobs do Azure quando um contêiner de Blobs for o destino:
    - Armazenamento quente
    - Armazenamento refrigerado
4. Você pode escolher uma classe de armazenamento S3 específica quando o Amazon S3 for o destino:
    - Padrão (esta é a classe padrão)
    - Camadas inteligentes
    - Acesso Padrão-Infrequente
    - Uma Zona - Acesso Infrequente
    - Arquivo Glacier Deep
    - Recuperação Flexível de Geleira
    - Recuperação instantânea de geleira
5. Você pode escolher uma classe de armazenamento específica quando um bucket do Google Cloud Storage for o destino:
    - Padrão
    - Nearline
    - Linha Fria
    - Arquivo

Preparar a origem e o destino no NetApp Copy and Sync

Verifique se sua origem e destinos atendem aos seguintes requisitos no NetApp Copy and Sync.

Rede

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

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

- A NetApp recomenda configurar os agentes de origem, de destino e de dados para usar um serviço NTP (Network Time Protocol). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Diretório de destino

Ao criar um relacionamento de sincronização, Copiar e Sincronizar permite que você selecione um diretório de destino existente e, opcionalmente, crie uma nova pasta dentro desse diretório. Portanto, certifique-se de que seu diretório de destino preferido já exista.

Permissões para ler diretórios

Para mostrar todos os diretórios ou pastas em uma origem ou destino, o Copiar e Sincronizar precisa de permissões de leitura no diretório ou pasta.

NFS

As permissões devem ser definidas na origem/destino com uid/gid em arquivos e diretórios.

Armazenamento de objetos

- Para AWS e Google Cloud, um corretor de dados deve ter permissões de lista de objetos (essas permissões são fornecidas por padrão se você seguir as etapas de instalação do corretor de dados).
- Para Azure, StorageGRID e IBM, as credenciais inseridas ao configurar um relacionamento de sincronização devem ter permissões de lista de objetos.

PMEs

As credenciais SMB inseridas ao configurar um relacionamento de sincronização devem ter permissões de lista de pastas.

O corretor de dados ignora os seguintes diretórios por padrão: .snapshot, ~snapshot, .copy-offload

Ao copiar dados SMB para o Cloud Volumes ONTAP usando a função Copiar e Sincronizar, a propriedade de arquivos e pastas do sistema de origem não é preservada. Esse comportamento ocorre porque o Copy and Sync usa um cliente SMB do Linux, que atribui a propriedade ao usuário ou à conta de serviço usada para autenticar a transferência. Embora as listas de controle de acesso possam ser mantidas, as informações de propriedade e auditoria podem diferir do sistema de origem. Este é o comportamento esperado.

Requisitos do bucket Amazon S3

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

Locais de corretores de dados com suporte para Amazon S3

Relacionamentos de sincronização que incluem armazenamento S3 exigem um corretor de dados implantado na AWS ou em suas instalações. Em ambos os casos, o Copy and Sync solicita que você associe o data broker a uma conta da AWS durante a instalação.

- "Aprenda a implantar o AWS Data Broker"
- "Aprenda a instalar o data broker em um host Linux"

Regiões AWS suportadas

Todas as regiões são suportadas, exceto as regiões da China.

Permissões necessárias para buckets S3 em outras contas AWS

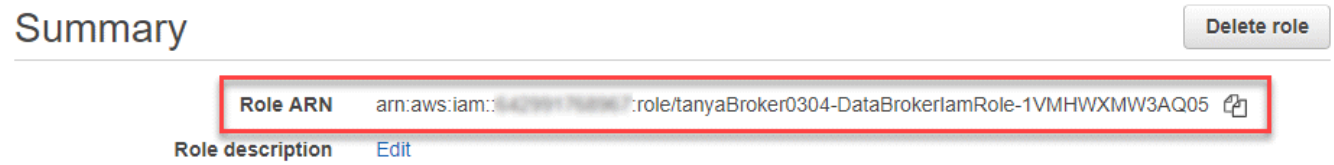
Ao configurar um relacionamento de sincronização, você pode especificar um bucket do S3 que reside em uma conta da AWS que não está associada a um corretor de dados.

"As permissões incluídas neste arquivo JSON"deve ser aplicado ao bucket S3 para que um corretor de dados possa acessá-lo. Essas permissões permitem que o data broker 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 a um corretor de dados.
2. *<RoleARN>* deve ser substituído por um dos seguintes:
   - Se um 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 um corretor de dados.
   - Se um data broker foi implantado na AWS usando o modelo CloudFormation, *RoleARN* deve ser o ARN da função do IAM criada pelo modelo.

     Você pode encontrar o ARN da função acessando o console do EC2, selecionando a instância do data broker e, em seguida, selecionando a função do IAM na guia Descrição. Você deverá ver a página Resumo no console do IAM que contém o ARN da função.



Requisitos de armazenamento do Azure Blob

Certifique-se de que seu armazenamento de Blobs do Azure atenda aos seguintes requisitos.

Locais de corretores de dados com suporte para o Azure Blob

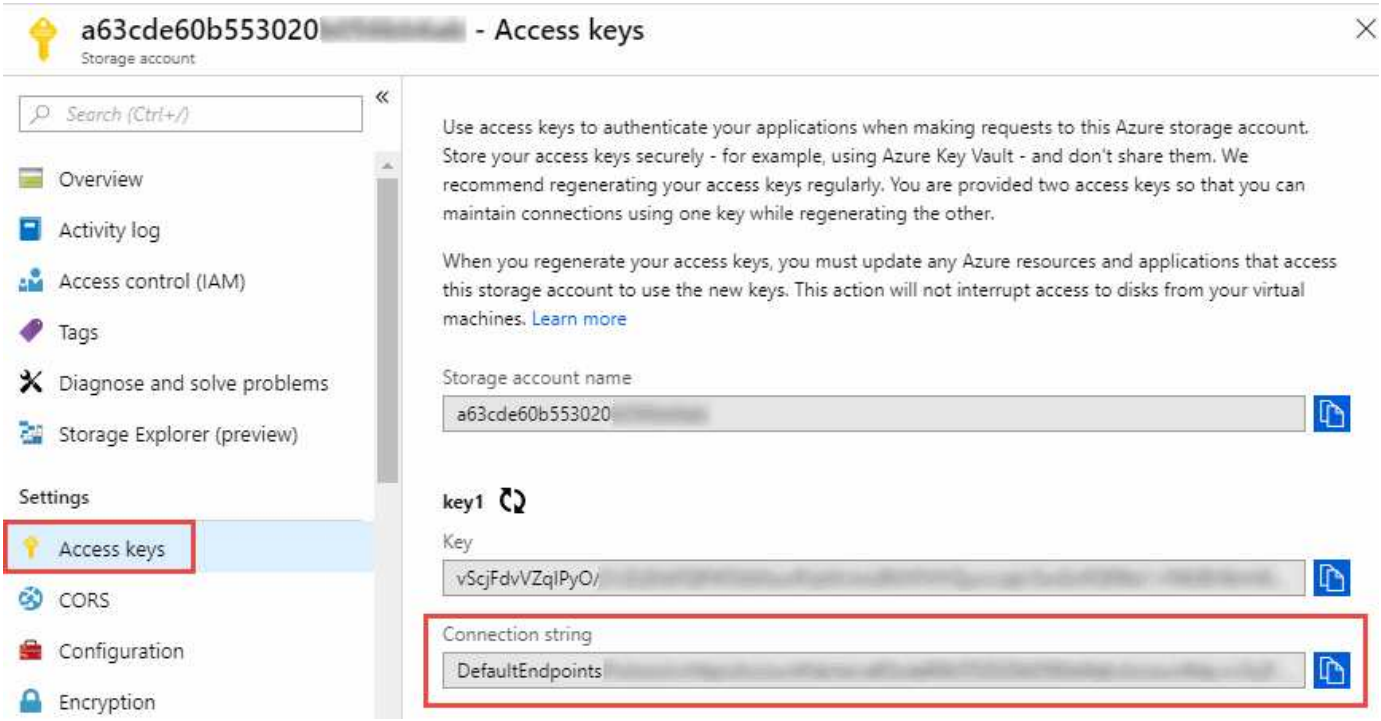
Um corretor de dados pode residir em qualquer local quando um relacionamento de sincronização inclui armazenamento de Blobs do Azure.

Regiões do Azure com suporte

Todas as regiões são suportadas, exceto as regiões da China, Governo dos EUA e Departamento de Defesa dos EUA.

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

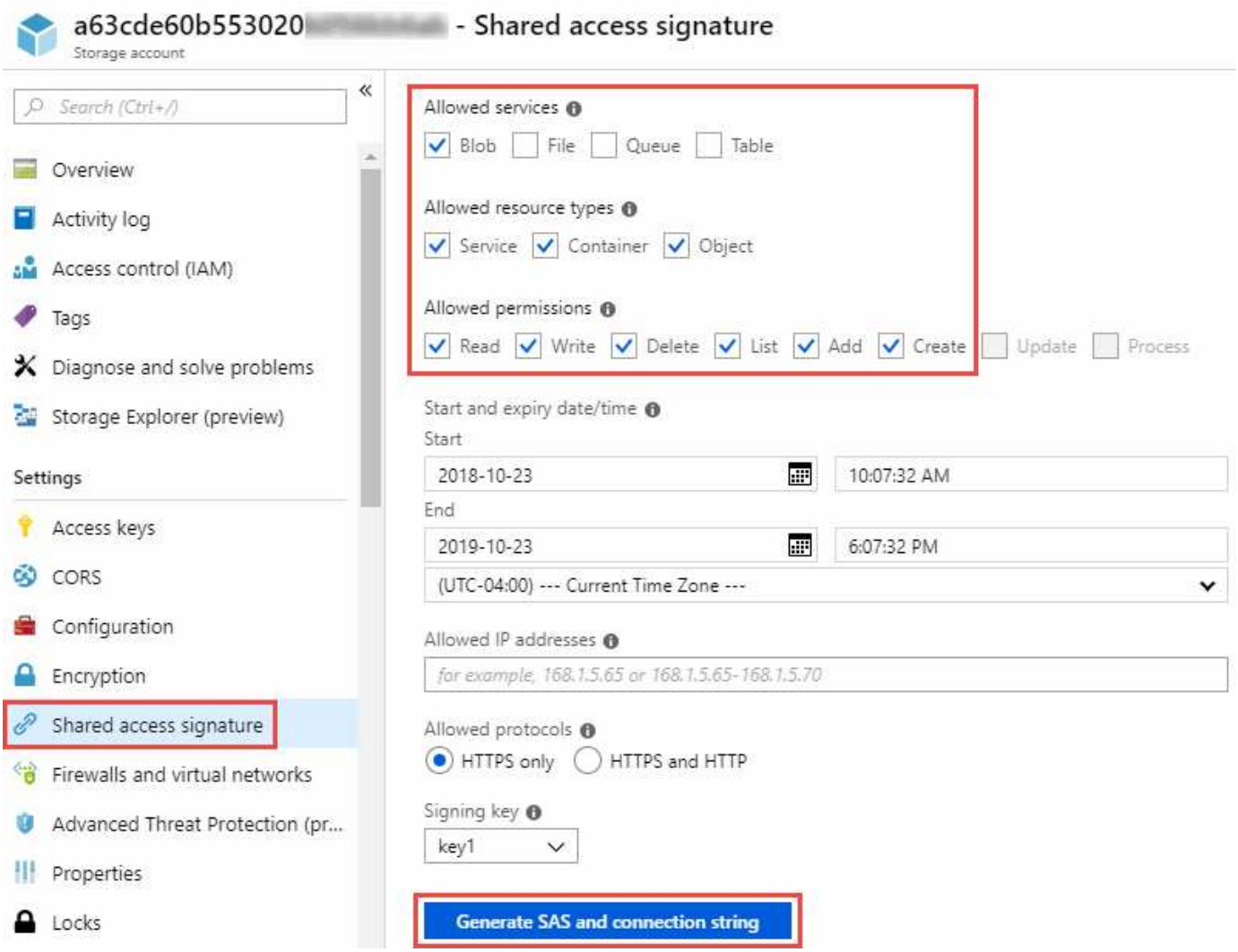
Ao criar um relacionamento de sincronização entre um contêiner de Blobs do Azure e um servidor NFS ou SMB, você precisa fornecer ao Copy and Sync a sequência de conexão da conta de armazenamento:



Se você quiser sincronizar dados entre dois contêineres de Blobs do Azure, a cadeia de conexão deverá 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 contêiner Blob de origem: Ler e Listar
- Para o contêiner Blob de destino: Ler, Escrever, Listar, Adicionar e Criar



Se você optar por implementar um relacionamento de Sincronização Contínua que inclua um contêiner de Blobs do Azure, poderá usar uma cadeia de conexão regular ou uma cadeia de conexão SAS. Se estiver usando uma string de conexão SAS, ela não deve ser configurada para expirar em um futuro próximo.

Armazenamento do Azure Data Lake Gen2

Ao criar um relacionamento de sincronização que inclui o Azure Data Lake, você precisa fornecer ao Copy and Sync a sequência de conexão da conta de armazenamento. Deve ser uma string de conexão regular, não uma assinatura de acesso compartilhado (SAS).

Requisito do Azure NetApp Files

Use o nível de serviço Premium ou Ultra ao sincronizar dados de ou para o Azure NetApp Files. Você poderá enfrentar falhas e problemas de desempenho se o nível de serviço do disco for Padrão.

Consulte um arquiteto de soluções se precisar de ajuda para determinar o nível de serviço correto. O tamanho do volume e o nível 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 da caixa

- Para criar um relacionamento de sincronização que inclua o Box, você precisará fornecer as seguintes credenciais:
  - ID do cliente
  - Segredo do cliente
  - Chave privada
  - ID da chave pública
  - Senha
  - ID da empresa
- Se você criar um relacionamento de sincronização do Amazon S3 para o Box, deverá usar um grupo de corretores de dados que tenha uma configuração unificada em que as seguintes configurações estejam definidas como 1:
  - Concorrência do Scanner
  - Limite de processos do scanner
  - Concorrência do Transferidor
  - Limite de Processos de Transferência

  "Aprenda a definir uma configuração unificada para um grupo de corretores de dados" .

Requisitos do bucket do Google Cloud Storage

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

Locais de corretores de dados com suporte para o Google Cloud Storage

Relacionamentos de sincronização que incluem o Google Cloud Storage exigem um corretor de dados implantado no Google Cloud ou em suas instalações. O Copy and Sync orienta você no processo de instalação do data broker quando você cria um relacionamento de sincronização.

- "Aprenda a implantar o Google Cloud Data Broker"
- "Aprenda a instalar o data broker em um host Linux"

Regiões do Google Cloud com suporte

Todas as regiões são suportadas.

Permissões para buckets em outros projetos do Google Cloud

Ao configurar um relacionamento de sincronização, você pode escolher entre buckets do Google Cloud em diferentes projetos, se fornecer as permissões necessárias para a conta de serviço do data broker. "Aprenda a configurar a conta de serviço" .

Permissões para um destino SnapMirror

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

Criptografando um bucket do Google Cloud

Você pode criptografar um bucket de destino do Google Cloud com uma chave KMS gerenciada pelo cliente ou com a chave padrão gerenciada pelo Google. Se o bucket já tiver uma criptografia KMS adicionada, ela substituirá a criptografia padrão gerenciada pelo Google.

Para adicionar uma chave KMS gerenciada pelo cliente, você precisará usar um corretor de dados com o "permissões corretas" , e a chave deve estar na mesma região que o bucket.

Google Drive

Ao configurar um relacionamento de sincronização que inclui o Google Drive, você precisará fornecer o seguinte:

- O endereço de e-mail de um usuário que tem acesso ao local do Google Drive onde você deseja sincronizar os dados
- O endereço de e-mail de uma conta de serviço do Google Cloud que tem permissões para acessar o Google Drive
- Uma chave privada para a conta de serviço

Para configurar a conta de serviço, siga as instruções na documentação do Google:

- "Crie a conta de serviço e as credenciais"
- "Delegar autoridade de todo o domínio à sua conta de serviço"

Ao editar o campo Escopos do OAuth, insira os seguintes escopos:

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

Requisitos do servidor NFS

- O servidor NFS pode ser um sistema NetApp ou um sistema não NetApp .
- O servidor de arquivos deve permitir que um host do corretor de dados acesse as exportações pelas portas necessárias.
  - 111 TCP/UDP
  - 2049 TCP/UDP
  - 5555 TCP/UDP
- As versões 3, 4.0, 4.1 e 4.2 do NFS são suportadas.

  A versão desejada deve estar habilitada no servidor.
- Se você quiser sincronizar dados NFS de um sistema ONTAP , certifique-se de que o acesso à lista de exportação NFS para uma SVM esteja habilitado (vserver nfs modify -vserver *svm_name* -showmount enabled).

  A configuração padrão para showmount é *habilitado* a partir do ONTAP 9.2.

Requisitos do ONTAP

Se o relacionamento de sincronização incluir o Cloud Volumes ONTAP ou um cluster ONTAP local e você tiver selecionado NFSv4 ou posterior, será necessário habilitar as ACLs do NFSv4 no sistema ONTAP . Isso é necessário para copiar as ACLs.

Requisitos de armazenamento do ONTAP S3

Quando você configura um relacionamento de sincronização que inclui "Armazenamento ONTAP S3" , você precisará fornecer o seguinte:

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

Requisitos do servidor SMB

- O servidor SMB pode ser um sistema NetApp ou um sistema não NetApp .
- Você precisa fornecer ao Copy and Sync credenciais que tenham permissões no servidor SMB.
  - Para um servidor SMB de origem, as seguintes permissões são necessárias: listar e ler.

    Os membros do grupo Operadores de backup são suportados com um servidor SMB de origem.

  - Para um servidor SMB de destino, as seguintes permissões são necessárias: listar, ler e gravar.
- O servidor de arquivos deve permitir que um host do corretor de dados acesse as exportações pelas portas necessárias.
  - 139 TCP
  - 445 TCP
  - 137-138 UDP
- As versões SMB 1.0, 2.0, 2.1, 3.0 e 3.11 são suportadas.
- Conceda ao grupo "Administradores" permissões de "Controle total" para as pastas de origem e destino.

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

Limitação de SMB para diretórios e arquivos ocultos

Uma limitação do 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 à limitação de diferenciação entre maiúsculas e minúsculas

O protocolo SMB não diferencia maiúsculas de minúsculas, o que significa que letras maiúsculas e minúsculas são tratadas como se fossem iguais. Esse comportamento pode resultar em arquivos substituídos e erros de cópia de diretório, se um relacionamento 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 Copiar e Sincronizar copia o arquivo chamado "a" para o destino, o arquivo "A" é substituído pelo arquivo "a" da origem.

No caso de diretórios, digamos que há um diretório chamado "b" na origem e um diretório chamado "B" no destino. Quando o Copy and Sync tenta copiar o diretório chamado "b" para o destino, o Copy and Sync recebe um erro informando que o diretório já existe. Como resultado, o Copiar e Sincronizar sempre falha ao copiar o diretório chamado “b”.

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

Visão geral de rede para NetApp Copy and Sync

A rede para o NetApp Copy and Sync inclui conectividade entre o grupo de corretores de dados e os locais de origem e destino, além de uma conexão de saída de internet dos corretores de dados pela porta 443.

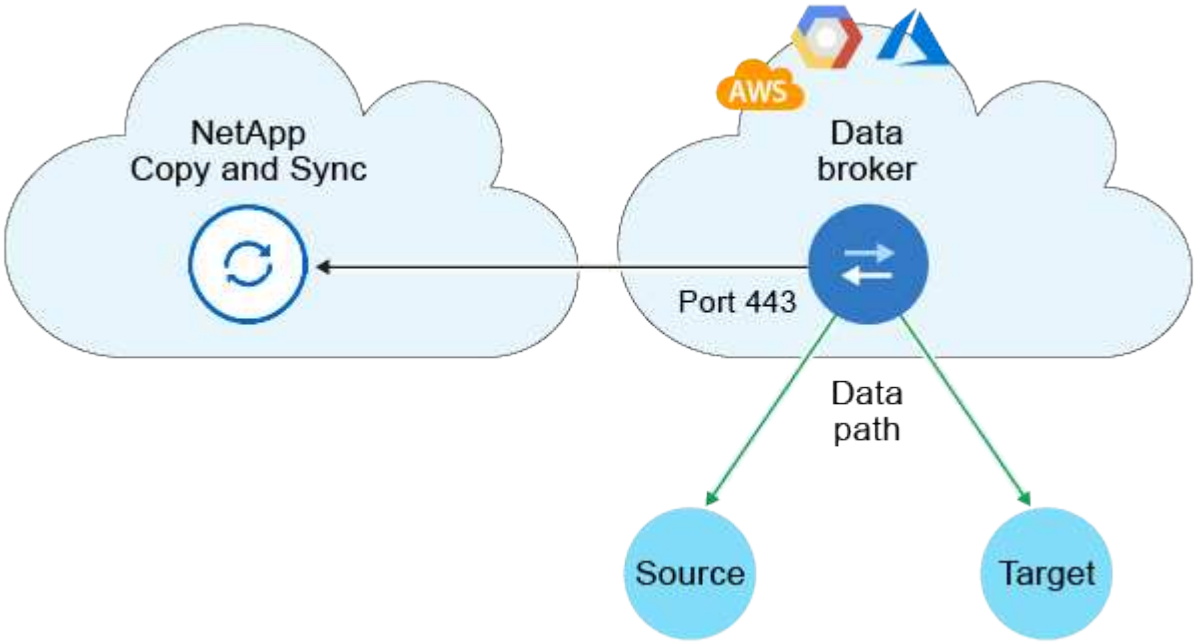
Localização do corretor de dados

Um grupo de corretores de dados consiste em um ou mais corretores de dados instalados na nuvem ou em suas instalações.

Corretor de dados na nuvem

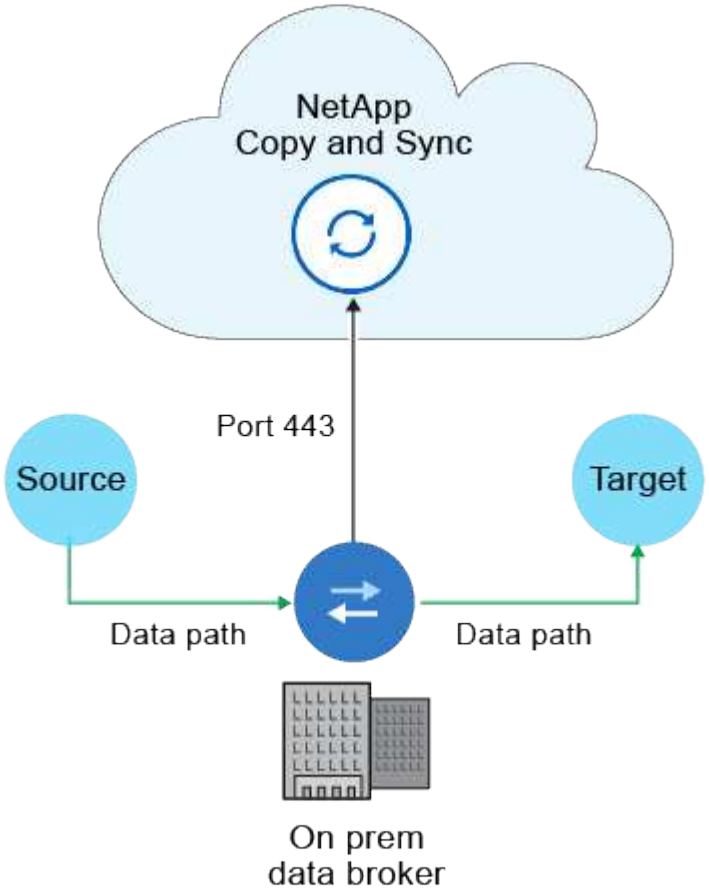
A imagem a seguir mostra um corretor de dados em execução na nuvem, na AWS, no Google Cloud ou no Azure. A origem e o destino podem estar em qualquer local, desde que haja uma conexão com o corretor de dados. Por exemplo, você pode ter uma conexão VPN do seu data center para seu provedor de nuvem.

Quando o Copy and Sync implanta o data broker na AWS, Azure ou Google Cloud, ele cria um grupo de segurança que permite a comunicação de saída necessária.



Corretor de dados em suas instalações

A imagem a seguir mostra o data broker em execução no local em um data center. Novamente, a origem e o destino 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 grupo de corretores de dados.

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

- Um corretor de dados precisa de uma conexão de saída com a Internet para poder consultar o Copy and Sync para tarefas na porta 443.
- A NetApp recomenda configurar os agentes de origem, destino e dados para usar um serviço NTP (Network Time Protocol). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Pontos de extremidade de rede

O NetApp Data Broker requer acesso de saída à Internet pela porta 443 para se comunicar com o Copy and Sync e para entrar em contato com alguns outros serviços e repositórios. Seu navegador 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 corretor de dados

Um corretor de dados contata os seguintes terminais:

Pontos finais	Propósito
\ https://olcentgbl.trafficmanager.net	Para entrar em contato com um repositório para atualizar pacotes CentOS para o host do data broker. Este ponto de extremidade será contatado somente se você instalar manualmente o data broker em um host CentOS.
\ https://rpm.nodesource.com \ https://registry.npmjs.org \ https://nodejs.org:	Para entrar em contato com repositórios para atualização de Node.js, npm e outros pacotes de terceiros usados no desenvolvimento.
\ https://tgz.pm2.io	Para acessar um repositório para atualização do PM2, que é um pacote de terceiros usado para monitorar o Copy and Sync.
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	Para entrar em contato com os serviços da AWS que o Copy and Sync usa para operações (enfileiramento de arquivos, registro de ações e entrega de atualizações ao data broker).
\ https://s3.*region*.amazonaws.com Por exemplo: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["Consulte a documentação da AWS para obter uma lista de endpoints S3"^]	Para entrar em contato com o Amazon S3 quando um relacionamento de sincronização inclui um bucket do S3.
\ https://s3.amazonaws.com/	Quando você baixa os logs do data broker do Copy and Sync, o data broker compacta seu diretório de logs e carrega os logs em um bucket S3 predefinido na região us-east-1.
\ https://storage.googleapis.com/	Para entrar em contato com o Google Cloud quando um relacionamento de sincronização usa um bucket do GCP.
https://storage-account.blob.core.windows.netSe estiver usando o Azure Data Lake Gen2:https://storage-account.dfs.core.windows.net[] Onde storage-account é a conta de armazenamento de origem do usuário.	Para abrir o proxy para o endereço da conta de armazenamento do Azure de um usuário.
\ https://cf.cloudsync.netapp.com \ https://repo.cloudsync.netapp.com	Para entrar em contato com Copy and Sync.
\ https://support.netapp.com	Para entrar em contato com o suporte da NetApp ao usar uma licença BYOL para relacionamentos de sincronização.
\ https://fedoraproject.org	Para instalar o 7z na máquina virtual do data broker durante a instalação e atualizações. O 7z é necessário para enviar mensagens do AutoSupport ao suporte técnico da NetApp .

Pontos finais	Propósito
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	Para verificar as credenciais da AWS quando o data broker é implantado na AWS ou quando é implantado em suas instalações e as credenciais da AWS são fornecidas. O corretor de dados entra em contato com esse ponto de extremidade durante a implantação, quando é atualizado e quando é reiniciado.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com	Para entrar em contato com a NetApp Data Classification ao usar a classificação para selecionar os arquivos de origem para um novo relacionamento de sincronização.
\ https://pubsub.googleapis.com	Se estiver criando um relacionamento de sincronização contínua a partir de uma conta de armazenamento do Google.
https://storage-account</ em>.queue.core.windows.net\ https://management.azure.com/subscriptions/ ${subscriptionId} /resourceGroups/${resourceGroup}/providers/Microsoft.EventGrid/* Onde storage-account é a conta de armazenamento de origem do usuário, subscriptionid é o ID da assinatura de origem e resourceGroup é o grupo de recursos de origem.	Se estiver criando um relacionamento de sincronização contínua de uma conta de armazenamento do Azure.

Pontos finais do navegador da Web

Seu navegador precisa acessar o seguinte endpoint para baixar logs para fins de solução de problemas:

logs.cloudsync.netapp.com:443

Efetue login no NetApp Copy and Sync

Use o NetApp Console para efetuar login no NetApp Copy and Sync.

Para fazer login no Console, você pode usar suas credenciais do Site de Suporte da NetApp ou pode se inscrever para um login na nuvem da NetApp usando seu e-mail e uma senha. "Saiba mais sobre como fazer login" .

O NetApp Copy and Sync usa o gerenciamento de acesso de identidade para controlar o acesso que cada usuário tem a ações específicas.

*Função necessária do NetApp Console * Função de administrador da organização. "Saiba mais sobre as funções de acesso do NetApp Console" .

Passos

1. Abra um navegador da web e vá para o "NetApp Console" .

   A página de login do NetApp Console é exibida.

2. Efetue login no Console.
3. Na navegação à esquerda do Console, selecione **Mobilidade** > **Copiar e sincronizar**.

Instalar um corretor de dados

Crie um novo data broker na AWS para NetApp Copy and Sync

Ao criar um novo grupo de corretores de dados para o NetApp Copy and Sync, escolha Amazon Web Services para implantar o software do corretor de dados em uma nova instância do EC2 em uma VPC. O NetApp Copy and Sync orienta você durante o processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudar você a se preparar para a instalação.

Você também tem a opção de instalar o data broker em um host Linux existente na nuvem ou em suas instalações. "Saber mais" .

Regiões AWS suportadas

Todas as regiões são suportadas, exceto as regiões da China.

Privilégios de root

O software do data broker é executado automaticamente como root no host Linux. Executar como root é um requisito para operações do data broker. Por exemplo, para montar ações.

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída com a Internet para poder consultar o Copy and Sync em busca de tarefas pela porta 443.

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

  Se você precisar limitar a conectividade de saída, consulte"a lista de endpoints que o corretor de dados contata" .

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

Permissões necessárias para implantar o data broker na AWS

A conta de usuário da AWS que você usa para implantar o data broker deve ter as permissões incluídas em "esta política fornecida pela NetApp" .

Requisitos para usar sua própria função do IAM com o AWS Data Broker

Quando o Copy and Sync implanta o data broker, ele cria uma função do IAM para a instância do data broker.

Você pode implantar o data broker usando sua própria função do IAM, se preferir. Você pode usar esta opção se sua organização tiver políticas de segurança rígidas.

A função IAM deve atender aos seguintes requisitos:

- O serviço EC2 deve ter permissão para assumir a função de IAM como uma entidade confiável.
- "As permissões definidas neste arquivo JSON"deve ser anexado à função do IAM para que o data broker possa funcionar corretamente.

Siga as etapas abaixo para especificar a função do IAM ao implantar o data broker.

Crie o corretor de dados

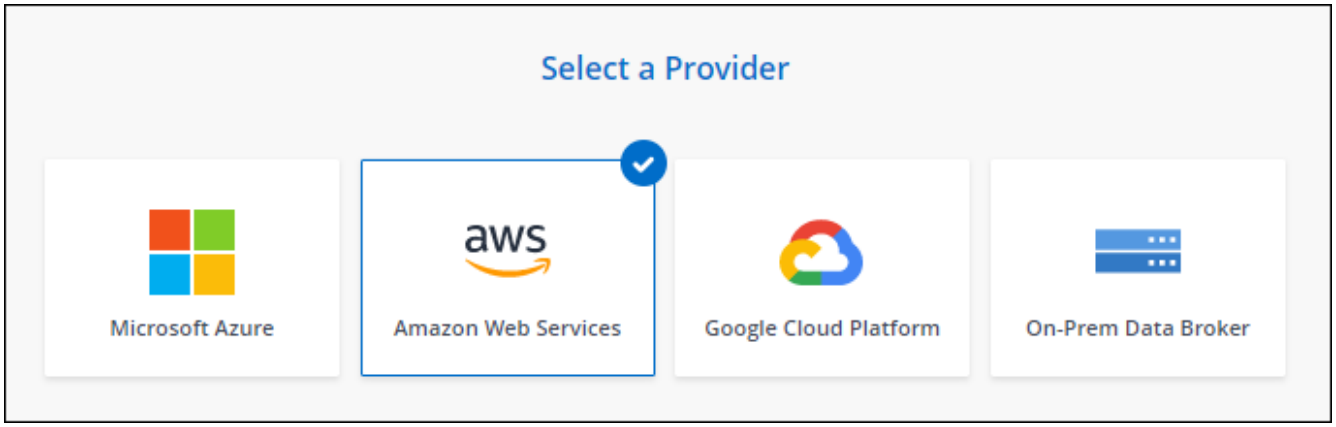
Existem algumas maneiras de criar um novo corretor de dados. Estas etapas descrevem como instalar um data broker na AWS ao criar um relacionamento de sincronização.

Passos

1. "Efetue login para copiar e sincronizar" .
2. Selecione **Criar nova sincronização**.
3. Na página **Definir relacionamento de sincronização**, escolha uma origem e um destino e selecione **Continuar**.

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

4. Na página **Grupo de Data Broker**, selecione **Criar Data Broker** e depois selecione **Amazon Web Services**.



5. Digite um nome para o corretor de dados e selecione **Continuar**.
6. Insira uma chave de acesso da AWS para que o Copy and Sync possa criar o data broker na AWS em seu nome.

   As chaves não são salvas nem usadas para nenhuma outra finalidade.

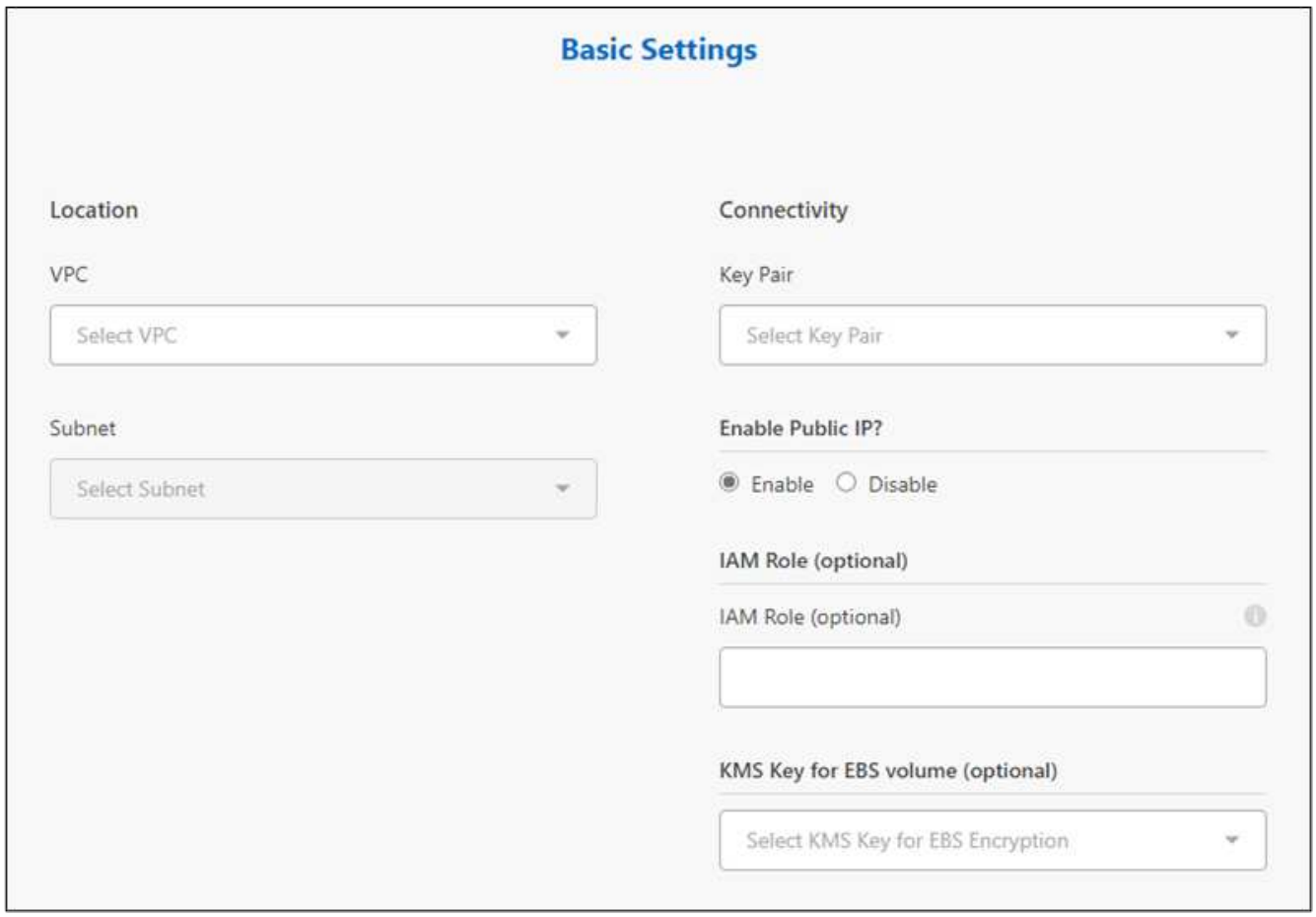
   Se preferir não fornecer chaves de acesso, selecione o link na parte inferior da página para usar um modelo do CloudFormation. Ao usar esta opção, você não precisa fornecer credenciais porque está efetuando login diretamente na AWS.

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

   Inicie um corretor de dados a partir de um modelo do AWS CloudFormation

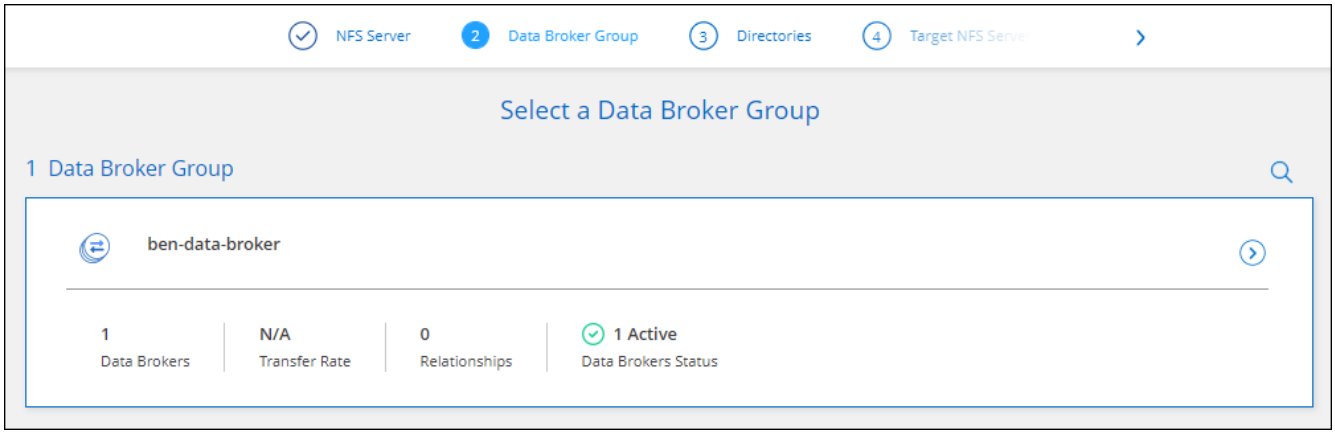
7. Se você inseriu uma chave de acesso da AWS, selecione um local para a instância, selecione um par de chaves, escolha se deseja habilitar um endereço IP público e selecione uma função do IAM existente ou deixe o campo em branco para que o Copiar e Sincronizar crie a função para você. Você também tem a opção de criptografar seu corretor de dados usando uma chave KMS.

   Se você escolher sua própria função de IAM,você precisará fornecer as permissões necessárias .



8. Especifique uma configuração de proxy, se um proxy for necessário para acesso à Internet na VPC.
9. Depois que o corretor de dados estiver disponível, selecione **Continuar** em Copiar e sincronizar.

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



10. Preencha as páginas do assistente para criar o novo relacionamento de sincronização.

Resultado

Você implantou um data broker na AWS e criou um novo relacionamento de sincronização. Você pode usar este grupo de corretores de dados com relacionamentos de sincronização adicionais.

Detalhes sobre a instância do data broker

O Copy and Sync cria um data broker na AWS usando a seguinte configuração.

Compatibilidade com Node.js
v21.2.0

Tipo de instância
m5n.xlarge quando disponível na região, caso contrário m5.xlarge

vCPUs
4

BATER
16 GB

Sistema operacional
Amazon Linux 2023

Tamanho e tipo de disco
SSD GP2 de 10 GB

Crie um novo corretor de dados no Azure para o NetApp Copy and Sync

Ao criar um novo grupo de data brokers para o NetApp Copy and Sync, escolha o Microsoft Azure para implantar o software de data broker em uma nova máquina virtual em uma VNet. O NetApp Copy and Sync orienta você durante o processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudar você a se preparar para a instalação.

Você também tem a opção de instalar o data broker em um host Linux existente na nuvem ou em suas instalações. "Saber mais" .

Regiões do Azure com suporte

Todas as regiões são suportadas, exceto as regiões da China, Governo dos EUA e Departamento de Defesa dos EUA.

Privilégios de root

O software do data broker é executado automaticamente como root no host Linux. Executar como root é um requisito para operações do data broker. Por exemplo, para montar ações.

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída com a Internet para poder consultar o serviço Copiar e Sincronizar em busca de tarefas pela porta 443.

  Quando o Copy and Sync implanta o data broker no Azure, ele cria um grupo de segurança que permite a comunicação de saída necessária.

  Se você precisar limitar a conectividade de saída, consulte"a lista de endpoints que o corretor de dados contata" .

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

Permissões necessárias para implantar o data broker no Azure

Certifique-se de que a conta de usuário do Azure que você usa para implantar o data broker tenha as seguintes permissões:

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

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

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

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

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

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

"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
```

```
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/virtualNetworks/read",
                    "Microsoft.Network/publicIPAddresses/write",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/publicIPAddresses/read",

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

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

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

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

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

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

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write"

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

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

Observação:

1. As seguintes permissões são necessárias somente se você planeja habilitar o "Configuração de sincronização contínua" em um relacionamento de sincronização do Azure para outro local de armazenamento em nuvem:

    - 'Microsoft.Storage/storageAccounts/leitura',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/leitura',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/ação',
    - 'Microsoft.EventGrid/systemTopics/leitura',
    - 'Microsoft.EventGrid/systemTopics/write',
    - 'Microsoft.EventGrid/systemTopics/excluir',
    - 'Microsoft.EventGrid/eventSubscriptions/write',
    - 'Microsoft.Storage/storageAccounts/write'

    Além disso, o escopo atribuível deve ser definido como escopo de assinatura e **não** escopo de grupo de recursos se você planeja implementar a Sincronização Contínua no Azure.

2. As seguintes permissões só serão necessárias se você planeja escolher sua própria segurança para a criação do data broker:

    - "Microsoft.Network/networkSecurityGroups/securityRules/leitura"
    - "Microsoft.Network/networkSecurityGroups/leitura"

Método de autenticação

Ao implantar o data broker, você precisará escolher um método de autenticação para a máquina virtual: uma senha ou um par de chaves pública-privada SSH.

Para obter ajuda na criação de um par de chaves, consulte "Documentação do Azure: Criar e usar um par de chaves pública-privada SSH para VMs Linux no Azure" .

Crie o corretor de dados

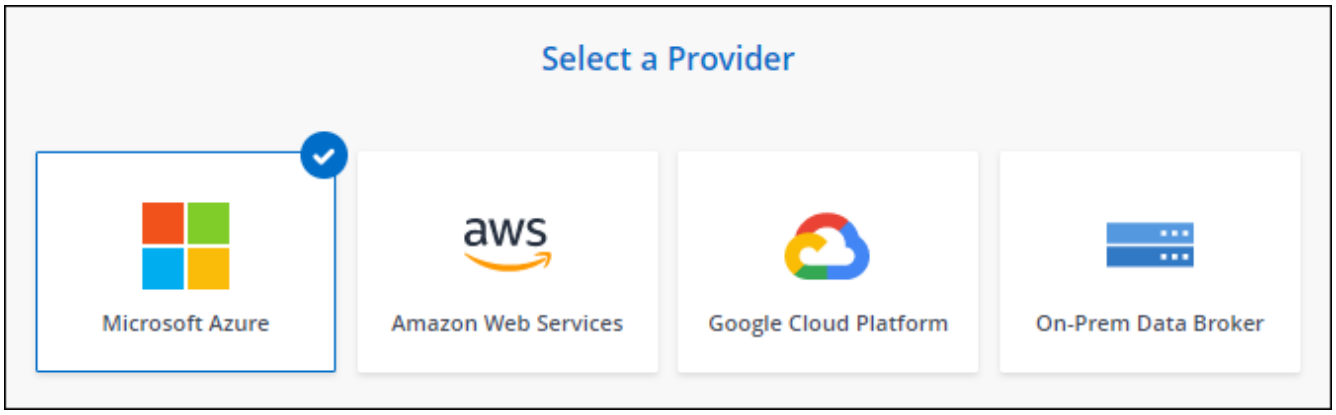
Existem algumas maneiras de criar um novo corretor de dados. Estas etapas descrevem como instalar um data broker no Azure ao criar um relacionamento de sincronização.

Passos

1. "Efetue login para copiar e sincronizar" .
2. Selecione **Criar nova sincronização**.
3. Na página **Definir relacionamento de sincronização**, escolha uma origem e um destino e selecione **Continuar**.

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

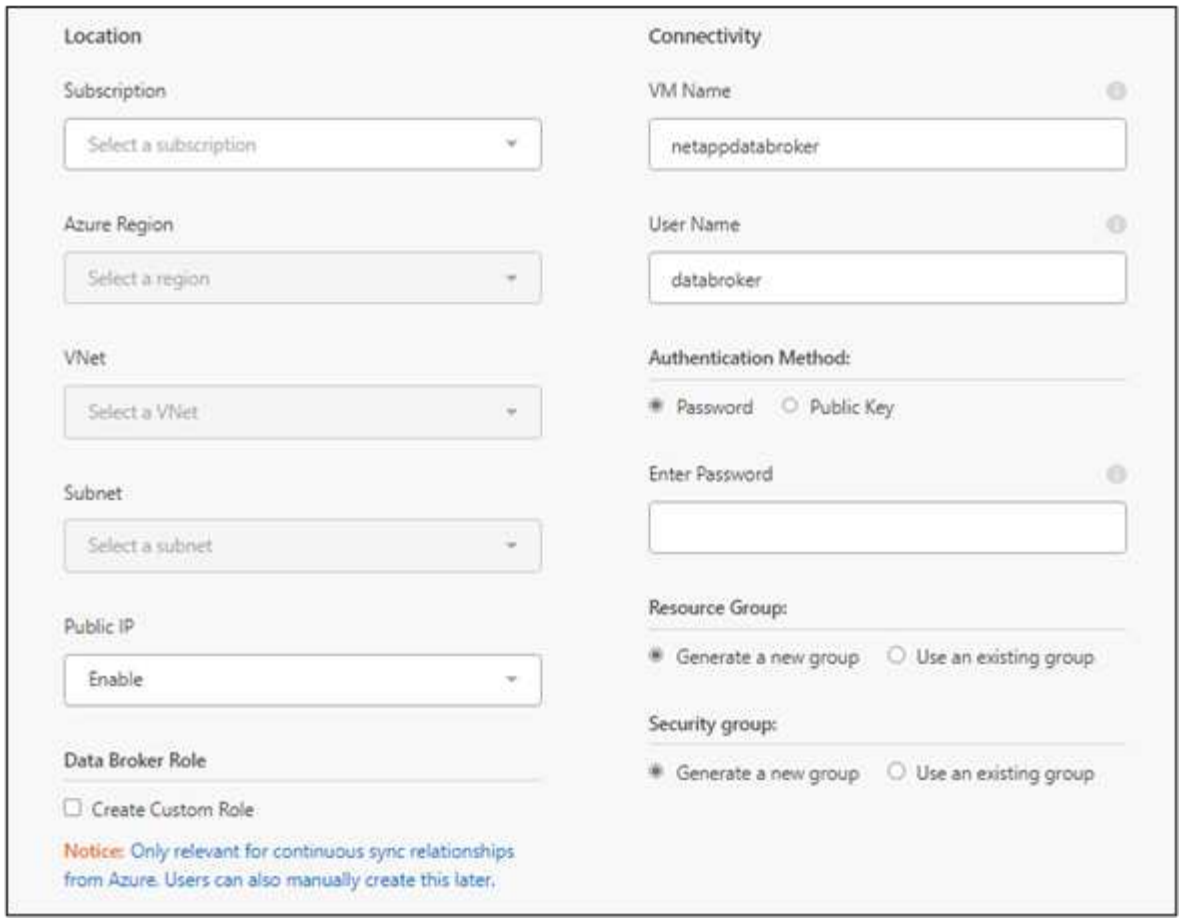
4. Na página **Grupo do Data Broker**, selecione **Criar Data Broker** e, em seguida, selecione **Microsoft Azure**.



5. Digite um nome para o corretor de dados e selecione **Continuar**.
6. Se solicitado, faça login na sua conta da Microsoft. Se não for solicitado, selecione **Fazer login no Azure**.

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

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



Se você planeja implementar um relacionamento de Sincronização Contínua, deverá atribuir uma função personalizada ao seu corretor de dados. Isso também pode ser feito manualmente após a criação do corretor.

8. Especifique uma configuração de proxy, se um proxy for necessário para acesso à Internet na VNet.
9. Selecione **Continuar**. Se você quiser adicionar permissões do S3 ao seu corretor de dados, insira suas chaves secretas e de acesso da AWS.
10. Selecione **Continuar** e mantenha a página aberta até que a implantação seja concluída.

    O processo pode levar até 7 minutos.

11. Em Copiar e sincronizar, selecione **Continuar** quando o corretor de dados estiver disponível.
12. Preencha as páginas do assistente para criar o novo relacionamento de sincronização.

Resultado

Você implantou um corretor de dados no Azure e criou um novo relacionamento de sincronização. Você pode usar este corretor de dados com relacionamentos de sincronização adicionais.

Recebeu uma mensagem sobre a necessidade de consentimento do administrador?

Se a Microsoft notificar você de que a aprovação do administrador é necessária porque o Copiar e Sincronizar precisa de permissão para acessar recursos na sua organização em seu nome, você terá duas opções:

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

   No Azure, acesse **Centros de administração > Azure AD > Usuários e grupos > Configurações do usuário** e habilite **Os usuários podem consentir que aplicativos acessem dados da empresa em seu nome**.

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

   \ https://login.microsoftonline.com/ {PREENCHA AQUI SEU ID DE LOCATÁRIO}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   Conforme mostrado na URL, a URL do nosso aplicativo é \ https://cloudsync.netapp.com e o ID do cliente do aplicativo é 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Detalhes sobre a VM do corretor de dados

O Copy and Sync cria um data broker no Azure usando a seguinte configuração.

Compatibilidade com Node.js
v21.2.0

Tipo VM
DS4 v2 padrão

vCPUs
8

BATER
28 GB

Sistema operacional
Rocky Linux 9,0

Tamanho e tipo de disco
SSD Premium de 64 GB

Crie um novo corretor de dados no Google Cloud para NetApp Copy and Sync

Ao criar um novo grupo de data broker para o NetApp Copy and Sync, escolha Google Cloud Platform para implantar o software de data broker em uma nova instância de

máquina virtual em um Google Cloud VPC. O NetApp Copy and Sync orienta você durante o processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudar você a se preparar para a instalação.

Você também tem a opção de instalar o data broker em um host Linux existente na nuvem ou em suas instalações. "Saber mais" .

Regiões do Google Cloud com suporte

Todas as regiões são suportadas.

Privilégios de root

O software do data broker é executado automaticamente como root no host Linux. Executar como root é um requisito para operações do data broker. Por exemplo, para montar ações.

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída com a Internet para poder consultar o Copy and Sync em busca de tarefas pela porta 443.

  Quando o Copy and Sync implanta o data broker no Google Cloud, ele cria um grupo de segurança que permite a comunicação de saída necessária.

  Se você precisar limitar a conectividade de saída, consulte"a lista de endpoints que o corretor de dados contata" .

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

Permissões necessárias para implantar o data broker no Google Cloud

Certifique-se de que o usuário do Google Cloud que implanta o data broker 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 data broker, 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.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update
- iam.serviceAccounts.signJwt
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

Observações:

1. A permissão "iam.serviceAccounts.signJwt" é necessária somente se você estiver planejando configurar o data broker para usar um cofre externo da HashiCorp.
2. As permissões "pubsub.*" e "storage.buckets.update" são necessárias somente se você planeja habilitar a configuração de Sincronização Contínua em um relacionamento de sincronização do Google Cloud Storage para outro local de armazenamento em nuvem. "Saiba mais sobre a opção Sincronização Contínua" .
3. As permissões "cloudkms.cryptoKeys.list" e "cloudkms.keyRings.list" são necessárias somente se você planeja usar uma chave KMS gerenciada pelo cliente em um bucket de destino do Google Cloud Storage.

Crie o corretor de dados

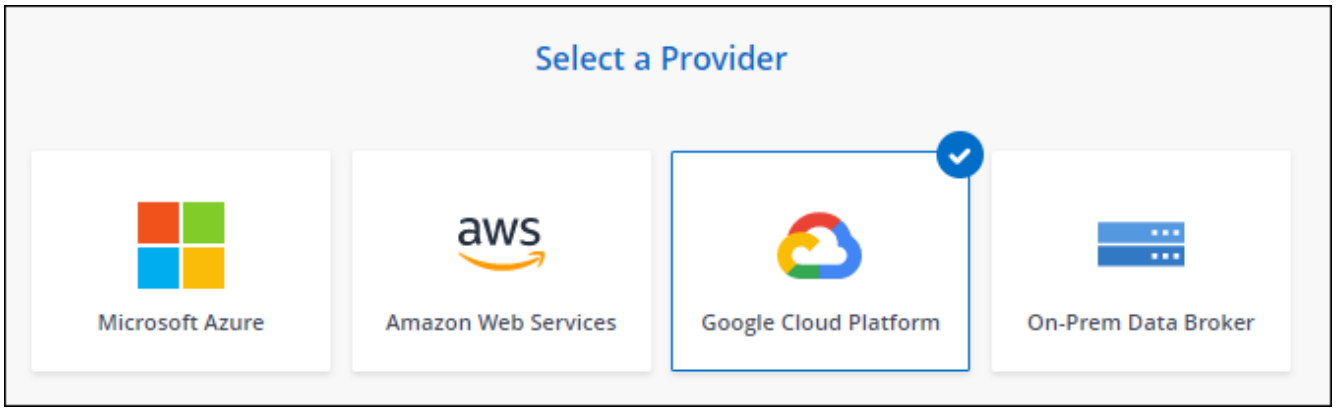
Existem algumas maneiras de criar um novo corretor de dados. Estas etapas descrevem como instalar um data broker no Google Cloud ao criar um relacionamento de sincronização.

Passos

1. "Efetue login para copiar e sincronizar" .
2. Selecione **Criar nova sincronização**.
3. Na página **Definir relacionamento de sincronização**, escolha uma origem e um destino e selecione **Continuar**.

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

4. Na página **Grupo de Data Broker**, selecione **Criar Data Broker** e depois selecione **Google Cloud Platform**.

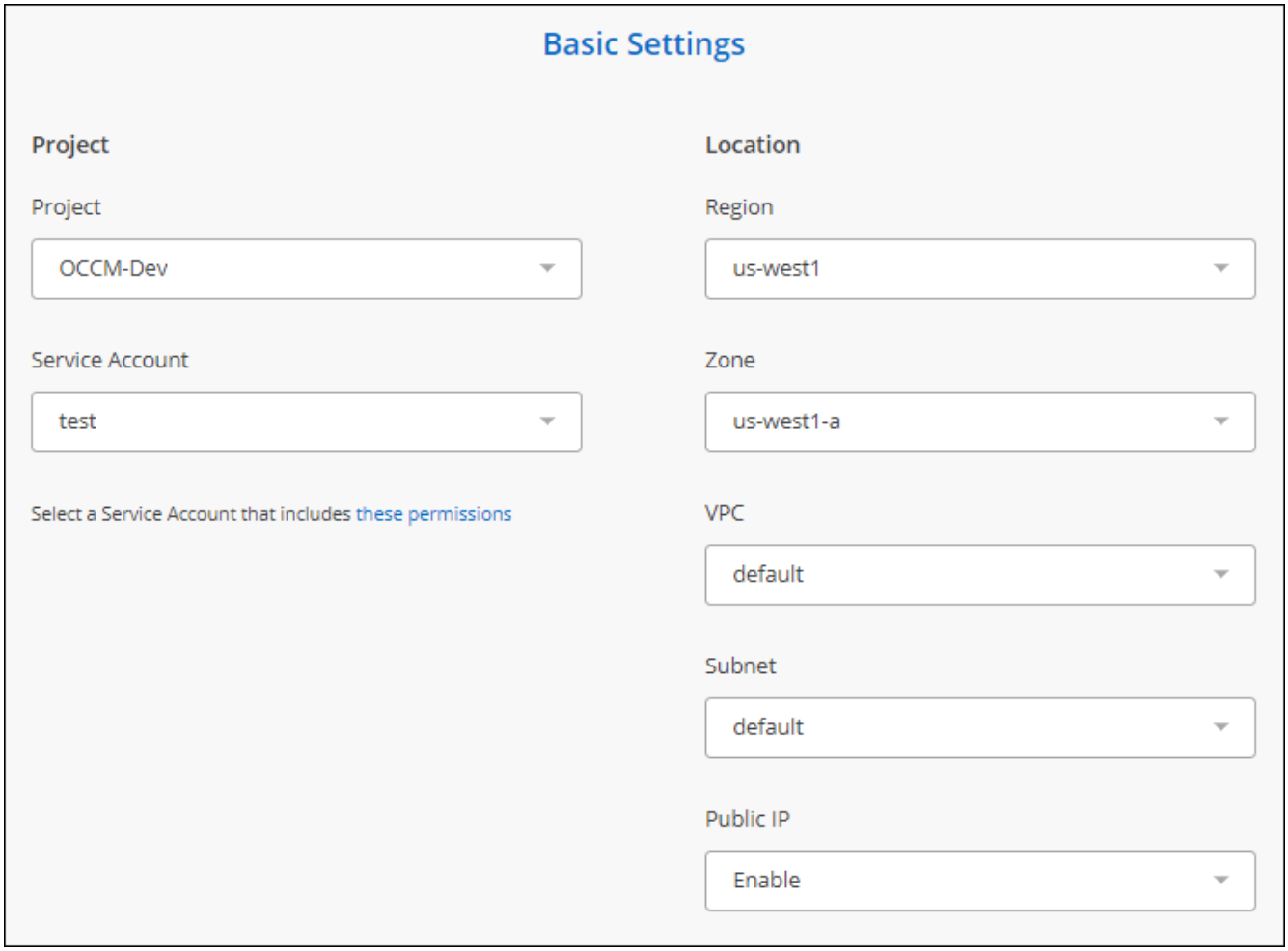


5. Digite um nome para o corretor de dados e selecione **Continuar**.
6. Se solicitado, faça login com sua conta do Google.

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

7. Selecione um projeto e uma conta de serviço e, em seguida, escolha um local para o data broker, incluindo se você deseja habilitar ou desabilitar um endereço IP público.

   Se você não habilitar um endereço IP público, precisará definir um servidor proxy na próxima etapa.



8. Especifique uma configuração de proxy, se um proxy for necessário para acesso à Internet na VPC.

   Se um proxy for necessário para acesso à Internet, o proxy deverá estar no Google Cloud e usar a mesma conta de serviço que o corretor de dados.

9. Quando o corretor de dados estiver disponível, selecione **Continuar** em Copiar e sincronizar.

   A instância leva aproximadamente de 5 a 10 minutos para ser implantada. Você pode monitorar o progresso em Copiar e Sincronizar, que é atualizado automaticamente quando a instância está disponível.

10. Preencha as páginas do assistente para criar o novo relacionamento de sincronização.

Resultado

Você implantou um corretor de dados no Google Cloud e criou um novo relacionamento de sincronização. Você pode usar este corretor de dados com relacionamentos de sincronização adicionais.

Conceder permissões para usar buckets em outros projetos do Google Cloud

Quando você cria um relacionamento de sincronização e escolhe o Google Cloud Storage como origem ou destino, Copiar e sincronizar permite que você escolha entre os buckets que a conta de serviço do data broker tem permissão para usar. Por padrão, isso inclui os buckets que estão no *mesmo* projeto que a conta de serviço do data broker. Mas você pode escolher buckets de *outros* projetos se fornecer as permissões necessárias.

Passos

1. Abra o console do Google Cloud Platform e carregue o serviço Cloud Storage.
2. Selecione o nome do bucket que você gostaria de usar como origem ou destino em um relacionamento de sincronização.
3. Selecione **Permissões**.
4. Selecione **Adicionar**.
5. Insira o nome da conta de serviço do corretor de dados.
6. Selecione uma função que forneçaas mesmas permissões mostradas acima .
7. Selecione **Salvar**.

Resultado

Ao configurar um relacionamento de sincronização, agora você pode escolher esse bucket como origem ou destino no relacionamento de sincronização.

Detalhes sobre a instância da VM do data broker

O Copy and Sync cria um data broker no Google Cloud usando a seguinte configuração.

Compatibilidade com Node.js
v21.2.0

Tipo de máquina
n2-padrão-4

vCPUs
4

BATER
15 GB

Sistema operacional
Rocky Linux 9,0

Tamanho e tipo de disco
20 GB HDD PD-padrão

Instale o data broker em um host Linux para NetApp Copy and Sync

Ao criar um novo grupo de data broker para o NetApp Copy and Sync, escolha a opção On-Prem Data Broker para instalar o software de data broker em um host Linux local ou em um host Linux existente na nuvem. O NetApp Copy and Sync orienta você durante o processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudar você a se preparar para a instalação.

Requisitos do host Linux

- **Compatibilidade com Node.js**: v21.2.0
- **Sistema operacional**:

- CentOS 8.0 e 8.5

  O CentOS Stream não é suportado.

- Red Hat Enterprise Linux 8.5, 8.8, 8.9 e 9.4
- Rocky Linux 9
- Ubuntu Server 20.04 LTS, 23.04 LTS e 24.04 LTS
- Servidor SUSE Linux Enterprise 15 SP1

  O comando `yum update` deve ser executado no host antes de instalar o data broker.

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

- **RAM**: 16 GB
- **CPU**: 4 núcleos
- **Espaço livre em disco**: 10 GB
- **SELinux**: Recomendamos que você desabilite o SELinux no host.

  O SELinux aplica uma política que bloqueia atualizações de software do data broker e pode impedir que o data broker entre em contato com os endpoints necessários para a operação normal.

Privilégios de root

O software do data broker é executado automaticamente como root no host Linux. Executar como root é um requisito para operações do data broker. Por exemplo, para montar ações.

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 data broker se comunica constantemente com o serviço Amazon SQS).
- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço NTP (Network Time Protocol). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Habilitar acesso à AWS

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

Passos

1. Crie uma política de IAM usando "esta política fornecida pela NetApp"

   "Ver instruções da AWS"

2. Crie um usuário do IAM que tenha acesso programático.

"Ver instruções da AWS"

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

Habilitar acesso ao Google Cloud

Se você planeja usar o data broker com um relacionamento de sincronização que inclui um bucket do Google Cloud Storage, você deve preparar o host Linux para acesso ao Google Cloud. Ao instalar o data broker, você precisará fornecer uma chave para uma conta de serviço que tenha permissões específicas.

Passos

1. Crie uma conta de serviço do Google Cloud que tenha permissões de administrador de armazenamento, caso você ainda não tenha uma.
2. Crie uma chave de conta de serviço salva no formato JSON.

   "Ver instruções do Google Cloud"

   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.

Habilitar acesso ao Microsoft Azure

O acesso ao Azure é definido por relacionamento, fornecendo uma conta de armazenamento e uma sequência de conexão no assistente de Sincronização de Relacionamento.

Instalar o corretor de dados

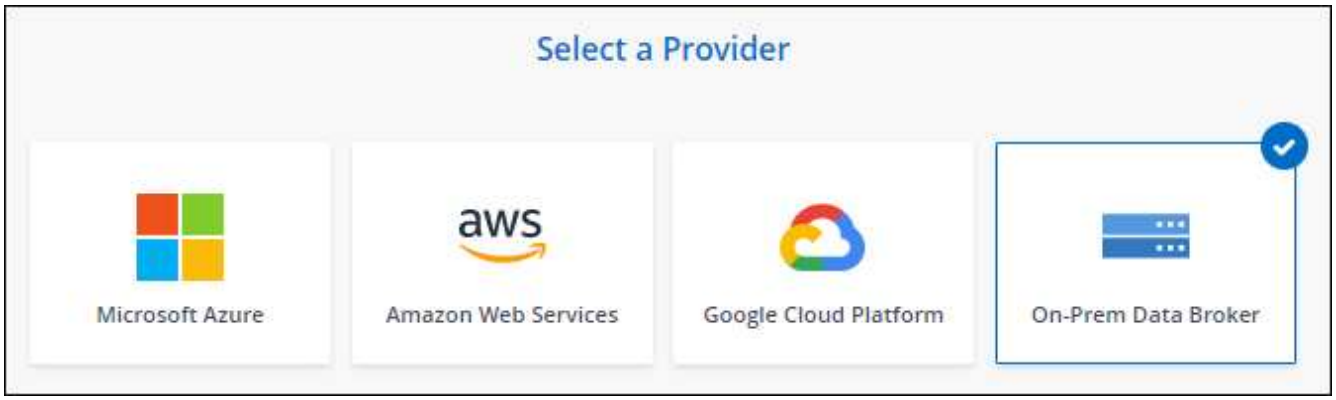
Você pode instalar um data broker em um host Linux ao criar um relacionamento de sincronização.

Passos

1. "Efetue login para copiar e sincronizar" .
2. Selecione **Criar nova sincronização**.
3. Na página **Definir relacionamento de sincronização**, escolha uma origem e um destino e selecione **Continuar**.

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

4. Na página **Grupo de Data Broker**, selecione **Criar Data Broker** e depois selecione **On-Prem Data Broker**.



Embora a opção esteja rotulada como ***On-Prem*** **Data Broker**, ela se aplica a um host Linux em suas instalações ou na nuvem.

5. Digite um nome para o corretor de dados e selecione **Continuar**.

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

6. Na página de instruções:
   a. Selecione se deseja habilitar o acesso ao **AWS**, **Google Cloud** ou ambos.
   b. Selecione uma opção de instalação: **Sem proxy**, **Usar servidor proxy** ou **Usar servidor proxy com autenticação**.

      O usuário deve ser um usuário local. Usuários de domínio não são suportados.

   c. Use os comandos para baixar e instalar o data broker.

      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 sua opção de instalação.

   d. Baixe o instalador:
      - Sem proxy:

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

      - Usar 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

        Copiar e sincronizar exibe o URI do arquivo de instalação na página de instruções, que é carregado quando você segue os prompts para implantar o On-Prem Data Broker. Esse URI não é repetido aqui porque o link é gerado dinamicamente e pode ser usado apenas uma vez. Siga estas etapas para obter o URI do Copy and Sync .

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

> Cada comando listado abaixo inclui parâmetros para acesso à AWS e ao Google Cloud. Siga a página de instruções para obter o comando exato com base na sua opção de instalação.

- Nenhuma 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 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> -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 AWS

Estas são as chaves para o usuário que você deve ter preparadoseguindo estes passos . As chaves da AWS são armazenadas no data broker, que é executado na sua rede local ou na nuvem. A NetApp não usa as chaves fora do data broker.

arquivo JSON

Este é o arquivo JSON que contém uma chave de conta de serviço que você deve ter preparadoseguindo estes passos .

7. Quando o corretor de dados estiver disponível, selecione **Continuar** em Copiar e sincronizar.
8. Preencha as páginas do assistente para criar o novo relacionamento de sincronização.

Informações sobre direitos autorais

Informações sobre marcas comerciais