Guia do usuário

# AWS Data Transfer Terminal

# AWS Data Transfer Terminal: Guia do usuário

# Table of Contents

# O que é o Data Transfer Terminal?

O AWS Data Transfer Terminal é um local físico pronto para a rede ao qual é possível levar dispositivos de armazenamento de dados para transferir dados rapidamente de ou para seu serviço da Nuvem AWS. Faça upload dos dados capturados remotamente para facilitar o acesso aos dados capturados remotamente.

Agende uma reserva em uma de nossas instalações físicas do Data Transfer Terminal via Console de Gerenciamento da AWS, chegue no horário agendado e faça upload dos seus dados para seus serviços da Nuvem AWS usando seus próprios dispositivos. Depois que sua reserva agendada for concluída e você for embora, a instalação será protegida novamente e preparada para a próxima reserva agendada.

> **Note**
>
> O AWS Data Transfer Terminal está disponível no momento apenas para clientes AWS Enterprise.

Para acessar o Data Transfer Terminal:

- Console do AWS Data Transfer Terminal: https://console.aws.amazon.com/datatransferterminal
- Instalações do Data Transfer Terminal: a localização das instalações do Data Transfer Terminal é fornecida assim que a reserva é feita no console. Para saber mais. consulte Fazer uma transferência de dados.

## Atributos

O uso do AWS Data Transfer Terminal facilita enviar dados para seu serviço da Nuvem AWS desde locais remotos. A seguir estão algumas das vantagens do Data Transfer Terminal para suas necessidades de upload remoto de dados:

Seguro, privado e exclusivo

Cada instalação do Data Transfer Terminal é um local seguro e privado para você fazer grandes transferências de dados entre seu dispositivo de armazenamento de dados e seus serviços da AWS por meio de uma conexão de rede rápida.

Um console de reservas dedicado

Adicione pessoal aprovado à sua equipe de transferência e agende uma reserva do Data Transfer Terminal usando o console do AWS Data Transfer Terminal.

Conexões de rede de fibra óptica

Cada instalação do Data Transfer Terminal inclui duas conexões de fibra óptica (LR4) de 100 Gigabits (Gbps) para permitir uploads rápidos de dados e redundância.

Controle dos seus dispositivos de armazenamento de dados

Não é necessário enviar seu dispositivo Snowball e esperar que os dados sejam carregados para seus serviços da Nuvem AWS. Você controla seus dispositivos físicos de armazenamento de dados durante todo o processo de transferência de dados, fazendo com que os dados cheguem aonde precisam mais rapidamente.

# Principais conceitos

O uso do AWS Data Transfer Terminal exige que o responsável por um processo agende uma reserva para que um especialista em transferência de dados possa acessar uma instalação do Data Transfer Terminal. Consulte as seções a seguir para saber mais sobre a terminologia do Data Transfer Terminal.

Tópicos



## Equipe de transferência

Equipe de transferência é um grupo de funcionários definido pelo proprietário de uma conta da AWS que pode ser selecionado para realizar transferências de dados em nome da sua organização. Configurar uma equipe de transferência inclui atribuir um nome à equipe de transferência e especificar o pessoal para a equipe. Recomendamos grupos de quatro ou menos especialistas em transferência de dados para uma única reserva.

Para saber mais, consulte Agendar uma reserva do Data Transfer Terminal.

## Pessoal

O termo pessoal se refere aos indivíduos que podem fazer e gerenciar reservas ou podem acessar e usar as instalações do Data Transfer Terminal. Um indivíduo pode ser um responsável pelo processo, especialista em transferência de dados ou ambos.

Responsável pelo processo

- Um responsável pelo processo é um proprietário da conta da AWS que pode adicionar, editar e remover pessoal da sua conta do AWS Data Transfer Terminal.

Especialista em transferência de dados

- Um especialista em transferência de dados é um indivíduo que pode comparecer às instalações do Data Transfer Terminal para realizar transações de upload de dados. Esse pessoal deve ser autorizado pelo responsável pelo processo e adicionado à sua conta do AWS Data Transfer Terminal. Ao acessar uma instalação do Data Transfer Terminal, um documento de identidade oficial emitido pelo governo será necessário.

## Instalações

As instalações do Data Transfer Terminal são centros de dados pertencentes a e gerenciados por um ou mais provedores de serviços. Cada instalação exige que os especialistas em transferência de dados do Data Transfer Terminal forneçam documentos de identidade oficiais emitidos pelo governo que correspondam aos registros da reserva para acessar a suíte do Data Transfer Terminal.

# Considerações sobre o agendamento

As reservas podem ser feitas no console do Data Transfer Terminal por uma a seis horas, em qualquer dia da semana, durante todo o ano. Reservas individuais podem ser agendadas consecutivamente com separação mínima de uma hora entre cada reserva. Todas as reservas devem ser feitas com pelo menos 24 horas de antecedência.

O tempo necessário para transferir os dados varia dependendo das velocidades de performance do upload. Considere os seguintes fatores que afetam a performance do upload ao planejar e agendar sua reserva do Data Transfer Terminal.

Equipamento

- Alguns equipamentos podem incluir configurações que podem afetar a performance do upload. Consulte as especificações do seu equipamento para obter as velocidades de performance de upload sugeridas.

Condições de rede

- Horários com tráfego intenso na rede afetarão as velocidades de upload de dados e devem ser levados em consideração ao selecionar um horário para sua sessão de transferência de dados. Planejar sua sessão de transferência de dados fora do horário de pico ou em horários de menor atividade na rede pode melhorar a velocidade de upload.

Tamanho da transferência de dados

- A conectividade de rede do Data Transfer Terminal foi projetada para grandes transferências de dados. No entanto, o tamanho dos dados que estão sendo transferidos afetará a duração da sessão.

# Casos de uso

Embora qualquer cliente AWS Enterprise possa acessar o sistema do data Transfer Terminal, alguns cenários de casos de uso específicos podem se beneficiar mais dele.

Direção autônoma e sistemas avançados de assistência ao motorista (AD/ADAS): fabricantes de equipamentos originais (OEM) automotivos e fornecedores geram grandes conjuntos de dados de suas frotas de veículos autônomos que operam e coletam dados em várias regiões metropolitanas na América do Norte, Europa e ASEAN. Com o Data Transfer Terminal, os dados coletados por esses veículos da frota podem ser enviados para o serviço da Nuvem AWS e usados para treinar modelos AD/ADAS.

Mídia e entretenimento: estúdios e outros criadores de conteúdo geralmente geram arquivos digitais de vídeo e áudio (AV) em locais remotos. É importante que esses arquivos AV sejam enviados rapidamente para a nuvem para que as equipes de produção e edição geograficamente dispersas possam iniciar fluxos de trabalho em paralelo e em tempo real. Quando o Data Transfer Terminal é usado para carregar dados remotamente, os cronogramas de produção podem ser reduzidos, o que se traduz em custos de produção menores.

Mapas, fotogrametria e imagens 3D: organizações que trabalham com aplicações de mapeamento ou imagens coletam dados em locais remotos e precisam carregar esses arquivos visuais para a Nuvem AWS para análise ou treinamento. O Data Transfer Terminal minimiza o tempo entre a

coleta e a análise desses grandes conjuntos de dados, o que ajuda a manter os dados geoespaciais atualizados para motoristas, agricultores e outros usuários dessas informações.

## Serviços relacionados

Os seguintes serviços da AWS fornecem uma experiência ideal ao usar o Data Transfer Terminal.

| Serviço da AWS | Descrição |
| --- | --- |
| AWS Snowball Edge | O AWS Data Transfer Terminal complementa os produtos Snowball ao oferecer um local que possibilita carregar seus dados de forma mais rápida para a Nuvem AWS, minimizando os tempos de espera para acessar seus dados. |
| Amazon S3 | Leve seu próprio dispositivo a um Data Transfer Terminal para carregar seus dados de forma rápida e segura para o serviço Amazon S3. |

# Requisitos técnicos para usar o Data Transfer Terminal

Antes de agendar uma reserva em um Data Transfer Terminal, você precisará garantir que tenha o equipamento e as configurações necessárias para se conectar à rede. Consulte as diretrizes a seguir para poder usufruir da melhor conectividade e experiência de rede.

## Equipamento

Leve dispositivos de conectividade portáteis, incluindo monitores, teclado, mouse e computador ou laptop, às instalações do Data Transfer Terminal para sua reserva agendada.

Seu hardware deve ser capaz de funcionar com conexões de fibra óptica (L4)

> **Note**
>
> Como prática recomendada de segurança de dados, garanta que seus dados estejam criptografados e protegidos nos dispositivos de armazenamento que você traz para o Data Transfer Terminal e aplique políticas de criptografia de dados ao usar a instalação do Data Transfer Terminal. Para saber mais, consulte Segurança do AWS Data Transfer Terminal

## Requisitos de rede

Certifique-se de que seu dispositivo, servidor ou equipamento de upload (laptop) esteja preparado para se conectar à rede e que ele ofereça suporte a DHCP. Você deve ter o seguinte para usufruir de uma experiência ideal de upload de dados:

- Um transceptor óptico QSFP 100G QSFP28 LR4 (100GBASE-LR4) compatível com os conectores NIC e LC para as conexões de cabo de fibra fornecidas na instalação do Data Transfer Terminal.
- Configuração automática de endereço IP DHCP habilitada. Os servidores DNS são atribuídos automaticamente pelo DHCP.
- Software e drivers de NIC atualizados.

## Otimização de desempenho

Para maximizar o throughput ao usar o AWS Data Transfer Terminal, considere as recomendações a seguir.

- Hardware recomendado:
  - Placa de interface de rede de 100 Gbps
  - CPU de 16 núcleos
  - 128 GB de RAM
  - Várias unidades SSD NVMe em uma matriz RAID
- Use a biblioteca AWS Common Runtime (AWS CRT) para uploads via AWS Command Line Interface ou AWS SDK.

  Otimize as configurações de transferência do Amazon S3 configurando os parâmetros abaixo. Defina esses valores sob a chave do `s3` de nível superior no arquivo de configuração AWS, local padrão `~/.aws/config`.

  ```
  [default]
  s3 =
      preferred_transfer_client = crt
      target_bandwidth = 100Gb/s
      max_concurrent_requests = 20
      multipart_chunksize = 16MB
  ```

  Observe que todos os valores de configuração do Amazon S3 são indentados e aninhados sob a chave do `s3` de nível superior.

  - Opcional: você pode definir os valores acima programaticamente usando o comando `aws configure set`. Por exemplo, para definir os valores acima para o perfil padrão, você pode executar os seguintes comandos:

    ```
    aws configure set default.s3.preferred_transfer_client crt
    aws configure set default.s3.target_bandwidth 100Gb/s
    aws configure set default.s3.max_concurrent_requests 20
    aws configure set default.s3.multipart_chunksize 16MB
    ```

- Para definir programaticamente esses valores para um perfil diferente do padrão, forneça o sinalizador `--profile`. Por exemplo, para definir a configuração de um perfil chamado `test-profile`, execute um comando como o exemplo abaixo.

  ```
  aws configure set s3.max_concurrent_requests 20 --profile test-profile
  ```

- Habilite o BBR (Linux) no dispositivo para melhorar o throughput.

```
sysctl -w net.core.default_qdisc=fq
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

# Mais informações

Para obter mais informações sobre as configurações do Amazon S3 na linha de comandos da AWS para otimizar sua conectividade e a performance da rede, consulte os recursos a seguir.

- Configuração do Amazon S3 via AWS CLI, na Referência de comandos da AWS
- Use um cliente Amazon S3 de alto desempenho: cliente baseado em AWS CRT no SDK do Amazon S3 para Java
- Como otimizar a performance ao usar a AWS CLI para fazer upload de arquivos grandes no Amazon S3?, no Centro de Conhecimentos da AWS

# Começar

Comece a transferir dados remotos para seus serviços da Nuvem AWS fazendo uma reserva em uma das instalações do Data Transfer Terminal. Para começar, você precisará de um equipamento compatível com as instalações do Data Transfer Terminal e de uma conta AWS Enterprise.

Revise a seção Requisitos técnicos para usar o Data Transfer Terminal deste guia antes de agendar uma reserva do Data Transfer Terminal para garantir que você tenha um equipamento com as configurações ideais para a transferência de dados. Nem todos os dispositivos de armazenamento de dados e equipamentos de conexão de rede são compatíveis com as conexões de rede de fibra óptica disponíveis nas suítes.

Quando você se cadastra na AWS, sua conta da AWS é automaticamente cadastrada em todos os serviços da AWS incluindo o Data Transfer Terminal. A cobrança incorrerá apenas pelos serviços utilizados.

Para configurar o Data Transfer Terminal, use as etapas nas seções a seguir.

Ao se cadastrar na AWS e configurar o Data Transfer Terminal, você poderá, se desejar, alterar o idioma de exibição no Console de Gerenciamento da AWS. Para obter mais informações, consulte Alterar o idioma do Console de Gerenciamento da AWS, no Guia de conceitos básicos do Console de Gerenciamento da AWS.

Após criar uma conta da AWS, você poderá acessar o Data Transfer Terminal. Para obter mais informações sobre como configurar e usar o AWS Data Transfer Terminal, consulte Agendar uma reserva do Data Transfer Terminal.

## Cadastrar-se em uma conta da AWS

Para começar a usar a AWS, você precisa de uma conta da AWS. Para obter mais informações sobre como criar uma conta da AWS, consulte Criar uma conta da AWS no Guia de referência para gerenciamento de contas da AWS.

# Agendar uma reserva no Data Transfer Terminal

Para começar a usar o AWS Data Transfer Terminal, é necessário ter uma conta da AWS e estar conectado ao console do Data Transfer Terminal em https://console.aws.amazon.com/datatransferterminal. Após fazer login no console do Data Transfer Terminal, você poderá ver as reservas existentes ou fazer uma nova reserva. Para agendar uma reserva, é necessário fazer o seguinte:

1. Criar uma equipe de transferência. Você precisará criar um grupo designado de usuários para criar uma reserva e acessar as instalações do Data Transfer Terminal para fazer uma transferência de dados. Para saber mais sobre esse tópico, consulte Criar uma equipe de transferência.
2. Após a criação da equipe, você precisará adicionar pessoal a ela. Para saber mais sobre como adicionar pessoal à sua equipe de transferência, consulte Adicionar pessoal.
3. O responsável pelo processo pode agendar a transferência de dados com as equipes da conta. Para obter mais informações sobre como agendar a reserva, consulte Especificar detalhes da reserva.
4. Certifique-se de que os detalhes da reserva estejam corretos antes de enviar a solicitação. Depois de enviada, a solicitação de reserva não poderá ser modificada por pelo menos 24 horas. Para obter mais informações, consulte Revisar e confirmar sua reserva.

Depois que sua reserva for processada e confirmada, sua equipe de transferência poderá acessar as instalações do Data Transfer Terminal no horário programado. Para obter mais informações, consulte Fazer uma transferência de dados na instalação do Data Transfer Terminal.

## Criar uma equipe de transferência

Para acessar uma instalação do Data Transfer Terminal, será necessário agendar uma reserva no Console de Gerenciamento da AWS. Faça login na sua conta da AWS para acessar o console do Data Transfer Terminal e conclua as etapas a seguir para agendar sua reserva.

1. Na página inicial do Data Transfer Terminal, selecione o botão Começar.
2. Se você ainda não tiver uma equipe de transferência configurada em sua conta, o botão Criar reserva estará desabilitado. Você precisará criar e nomear uma equipe de transferência para começar.

a. Selecione o botão Criar equipe de transferência.

b. Atribua um nome à equipe.

- O nome deve conter entre dois e 64 caracteres e começar por uma letra ou um número.
- Use apenas letras, números, pontos e traços. Caracteres especiais não são reconhecidos.
- Não inclua nenhuma informação de identificação confidencial.

c. Crie uma descrição da equipe de transferência.

- Forneça uma descrição que ajude a identificar a equipe, como descrever o propósito da equipe para um período, campanha ou projeto específico.

d. Selecione o botão Criar equipe de transferência.

Você será levado de volta à página da equipe de transferência e sua equipe recém-criada aparecerá na seção Equipes de transferência.

## Atualizar equipes de transferência em sua conta do Data Transfer Terminal

Para configurar uma nova equipe de transferência, consulte a seção Agendar uma reserva do Data Transfer Terminal deste guia.

Para modificar ou remover uma equipe de transferência, faça o seguinte:

1. Na página Equipes de transferência, selecione a equipe de transferência que gostaria de modificar.
2. Para modificar o nome e a descrição da equipe de transferência, selecione o botão Editar.
3. Para adicionar ou remover funcionários, selecione a guia Pessoal e conclua as etapas descritas na seção Como faço para modificar, adicionar ou remover funcionários da minha conta? deste documento de Perguntas mais frequentes.
4. Para adicionar ou cancelar uma reserva para a equipe de transferência selecionada, consulte a seção Atualizar o pessoal na sua conta do Data Transfer Terminal destas Perguntas mais frequentes.

# Adicionar pessoal

Adicione responsáveis pelo processo e especialistas em transferência de dados à sua equipe de transferência para configurar a transferência de dados e acessar as instalações do Data Transfer Terminal. Para adicionar pessoal à sua equipe de transferência, faça o seguinte:

1. Na página Equipes de transferência, selecione o cartão da equipe de transferência desejada entre os listados na seção Equipes de transferência. A página de resumo da equipe de transferência será exibida.
2. Escolha a guia Pessoal e, em seguida, o botão Registrar pessoa para adicionar a pessoa à equipe de transferência.
3. Preencha os campos com as informações necessárias sobre a pessoa que você está adicionando à equipe de transferência na página Registrar pessoal.
   a. Alias da pessoa: crie um alias exclusivo para identificar a pessoa.
      - O alias é usado para identificar a pessoa e, ao mesmo tempo, proteger sua identidade.
      - Ele pode conter até 64 caracteres e incluir letras, números e traços.
      - Caracteres especiais não são permitidos.
   b. Primeiro nome: forneça o primeiro nome da pessoa conforme consta na identificação oficial emitida pelo governo.
   c. Sobrenome: forneça o sobrenome da pessoa conforme consta na identificação oficial emitida pelo governo.
   d. Endereço de e-mail: inclua um endereço de e-mail válido para que a pessoa receba informações de reserva e instruções para acessar as instalações do Data Transfer Terminal.
4. Selecione o botão Registrar pessoa para concluir a adição da pessoa à sua equipe de Transferência.

## Atualizar pessoal em sua conta do Data Transfer Terminal

No momento, não há suporte à modificação de pessoal existentes em sua conta no console do Data Transfer Terminal. AWS No momento, os responsáveis pelo processo do Data Transfer Terminal só podem adicionar ou excluir pessoal.

Para remover pessoal de sua conta do Data Transfer Terminal, faça o seguinte:

1. Na página Transferir equipes, selecione a equipe de transferência associada à pessoa que gostaria de remover.
2. Na página de resumo da equipe de transferência selecionada, selecione a guia Pessoal.
3. Clique no botão de opção ao lado do alias que gostaria de remover. Observe que você só poderá ver o alias da pessoa ao excluir o respectivo perfil.

4. Selecione o botão Excluir. Um aviso aparecerá para confirmar a ação pretendida para a pessoa selecionada. Clique no botão Excluir para continuar. Um banner aparecerá na parte superior do console confirmando que a pessoa foi excluída com êxito.

# Especificar os detalhes da reserva

As instruções a seguir explicam como agendar sua reserva do Data Transfer Terminal no Console de Gerenciamento da AWS. Para obter informações sobre como usar a instalação do Data Transfer Terminal, consulte Fazer uma transferência de dados.

1. Selecione o botão Fazer reserva na guia Próximas reservas.
2. Preencha os campos na página Especificar os detalhes da reserva.
   a. Seleção da equipe de transferência: a equipe de transferência selecionada como padrão aparece primeiro. Caso prefira escolher uma equipe diferente, clique na seta suspensa para selecionar na lista de equipes de transferência disponíveis.
   b. Responsável pelo processo: selecione o alias da pessoa que você gostaria que fosse responsável por gerenciar a reserva.
      - Cada reserva permite somente um responsável, o qual deve ser uma pessoa autorizada na sua conta da AWS.

        O responsável pelo processo também pode ser incluído como um dos especialistas em transferência de dados para realizar a atividade de transferência de dados.
   c. Especialista em transferência de dados: selecione quem você deseja que tenha acesso às instalações do Data Transfer Terminal para concluir a atividade de transferência de dados. É possível selecionar mais de uma pessoa, conforme necessário.
      - A melhor prática é limitar sua equipe de transferência a no máximo quatro (4) especialistas em transferência de dados.
   d. Informações do Data Transfer Terminal: especifique a instalação do Data Transfer Terminal, a data desejada e a hora específica para a sessão de transferência de dados.
      i. Instalação do Data Transfer Terminal: clique na seta suspensa para selecionar uma instalação do Data Transfer Terminal.

> **Note**
>
> Somente as descrições das instalações serão fornecidas durante o processo de reserva. Informações adicionais sobre a localização serão fornecidas no e-mail de confirmação da reserva.

ii. Data e hora do Data Transfer Terminal: clique no campo Pesquisar data e hora para sua reserva para ver o calendário e agendar sua reserva.

- As reservas devem ser feitas com no mínimo 24 horas e no máximo seis (6) meses de antecedência. A duração máxima de cada reserva é de seis (6) horas. Uma única reserva pode se estender por mais de um dia para acomodar cenários noturnos, se necessário.
- A hora é indicada por um relógio no formato de 24 horas, e os horários só podem ser reservados em incrementos de hora inteira.
- Para fazer reservas consecutivas, é necessário criar reservas separadas com pelo menos uma hora entre cada sessão de transferência de dados.
- Para obter mais informações, consulte Considerações de agendamento.

3. Confirme se os detalhes da reserva estão corretos e selecione o botão Criar para continuar. Você será direcionado para a página de confirmação, a qual fornece um resumo da sua reserva.

## Revise e confirme sua reserva

Depois de especificar os detalhes da sua reserva, selecione o botão Avançar para continuar e abrir a página de visão geral. Revise os detalhes da sua solicitação de reserva do Data Transfer Terminal na página Revisar e criar.

- Se estiver satisfeito com a solicitação, selecione o botão Criar.
- Se precisar alterar sua reserva, selecione o botão Anterior.

Depois que a solicitação de reserva for enviada, o responsável pelo processo receberá um e-mail confirmando que a solicitação foi recebida e está sendo processada. Depois que a solicitação for aprovada, outro e-mail confirmará a reserva e fornecerá instruções para localizar e acessar as instalações do Data Transfer Terminal. Para obter informações sobre como acessar a instalação do Data Transfer Terminal, consulte Fazer uma transferência de dados.

# Fazendo alterações na sua reserva

Há um período de processamento de 24 horas antes que qualquer alteração possa ser feita em sua solicitação de reserva do Data Transfer Terminal.

Após o período de processamento, para visualizar, editar ou excluir sua reserva, navegue até a página Equipes de transferência no console.

1. Localize e selecione a reserva desejada no cartão da equipe.
2. Clique no menu Ações e selecione a ação desejada.
   - Visualizar: selecionar a opção de visualização permite ver os detalhes da sua reserva, incluindo data, hora, local e pessoal designado.
   - Editar: permite revisar os detalhes da reserva, incluindo data, hora, local e pessoal designado. Observe que as alterações devem ser feitas 24 horas antes da data de reserva desejada e que as revisões não são aceitas nem aplicadas imediatamente. O responsável pelo processo receberá a confirmação da solicitação atualizada.
   - Excluir: a opção de exclusão permite cancelar sua reserva. A solicitação de cancelamento deve ser feita no mínimo 24 horas antes da data agendada para a reserva. O responsável pelo processo receberá a confirmação da reserva cancelada quando a solicitação for aprovada.

# Fazer uma transferência de dados nas instalações do Data Transfer Terminal

O Data Transfer Terminal é um local seguro e de propriedade compartilhada que fornece acesso seguro à rede da AWS. Para acessar as instalações do Data Transfer Terminal, certifique-se de ter um e-mail de confirmação com a descrição do local e as instruções de acesso. Consulte os tópicos a seguir para obter mais informações sobre como acessar e usar as instalações do Data Transfer Terminal.

Tópicos



## O que trazer

Os especialistas em transferência de dados devem trazer os itens necessários para realizar uma transferência de dados, como um laptop, pen drives, unidades de estado sólido (SSDs) e AWS Snowball Edge. Certifique-se de que seu equipamento esteja otimizado para usar os cabos de rede de fibra existentes nas instalações do Data Transfer Terminal. Para saber mais sobre os equipamentos e as configurações ideais, consulte Requisitos técnicos para o uso do Data Transfer Terminal.

Você é responsável pela instalação, pelo uso e pela remoção dos equipamentos e itens que você e os especialistas em transferência de dados acompanhantes trazem para as instalações do Data Transfer Terminal. Qualquer item trazido para a suíte deverá ser removido na ocasião da saída. AWS O Data Transfer Terminal não é responsável por itens esquecidos ou perdidos.

## O endereço físico da instalação do Data Transfer Terminal

O endereço físico da instalação do Data Transfer Terminal não será fornecido. Em vez disso, o responsável pelo processo e os especialistas em transferência de dados especificados na reserva receberão um e-mail com o nome público pesquisável da instalação do Data Transfer Terminal. AWS

O Data Transfer Terminal usa o mesmo sistema de identificação de localização que o AWS Direct Connect para que você possa pesquisar o nome público na Internet para localizar sua respectiva instalação. Se você não tiver um e-mail com essas informações, confirme com seu gerente de conta do AWS Data Transfer Terminal se você faz parte da equipe de transferência e se suas informações de e-mail estão corretas.

## Acessar o prédio

Para acessar as instalações do Data Transfer Terminal, cada especialista em transferência de dados deve fornecer prova de identidade ou um documento de identidade oficial. Uma vez no prédio, a segurança acompanhará você até sua suíte do Data Transfer Terminal.

## Equipamento esperado na suíte do Data Transfer Terminal.

Cada instalação do Data Transfer Terminal deve ter apenas dois (2) cabos de fibra óptica, uma mesa ou bancada e cadeiras. Se houver algum outro equipamento ou item na sala, comunique imediatamente ao Suporte.

# Solução de problemas de conexão de rede

Em caso de problemas para se conectar à rede ao usar o AWS Data Transfer Terminal, por exemplo, não conseguir se conectar à Internet ou velocidades de conexão lentas, considere as dicas de solução de problemas a seguir.

Tópicos



## Problemas de conexão do equipamento

Se você tiver dificuldade para estabelecer uma conexão física enquanto estiver na suíte do Data Transfer Terminal, considere o seguinte:

- Cada instalação do Data Transfer Terminal terá dois (2) cabos de fibra LC monomodo. Se um ou ambos os cabos estiverem faltando, entre em contato com o AWS Support imediatamente.
- Se um cabo de fibra óptica não estiver funcionando, tente inverter o cabo primeiro. Se ainda assim você não conseguir se conectar com o primeiro cabo, tente usar o outro cabo.

Se você ainda não conseguir usar os cabos para se conectar, entre em contato com o AWS Support imediatamente.

## Solução de problemas de conectividade

Se você conseguir conectar seu equipamento, mas não conseguir se conectar à rede, experimente as sugestões de solução de problemas a seguir.

- Confirme se a configuração do seu equipamento atende aos requisitos de rede especificados. Para saber mais, consulte Requisitos técnicos para usar o Data Transfer Terminal
- Mude para o outro cabo de fibra óptica para se conectar.
- Reinicie o dispositivo enquanto mantém os cabos de fibra óptica conectados.
- Execute diagnósticos básicos de rede no dispositivo para garantir que:
  - O DHCP está habilitado

- Um endereço IP é atribuído à interface de rede conectada
- Os servidores DNS estão configurados
- O relógio do sistema está sincronizado com o NTP

Se você ainda não conseguir se conectar, entre em contato com o AWS Support e forneça as seguintes saídas, dependendo do sistema operacional (SO) em execução no seu dispositivo.

## Linux/UNIX

- Obtenha informações de endereço IP e roteamento em um terminal ou na interface de linha de comandos (CLI). Verifique se um endereço IP está atribuído à interface de rede e se uma rota padrão com um endereço de gateway padrão foi adicionada à tabela de rotas.

```
ip address show
ip route show
```

  - Como alternativa, se `iproute2` não estiver instalado no dispositivo e os comandos `ip` não estiverem disponíveis, use os seguintes comandos:

```
ifconfig
netstat -rn
```

- Colete informações do servidor DNS. Isso deve mostrar dois endereços IP começando com a palavra-chave `nameserver`.

```
cat /etc/resolv.conf
```

- Colete a saída dos testes básicos de conectividade. Substitua `default_gateway_address` pelo endereço IP do gateway padrão atribuído.

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- Colete a saída do teste de conectividade HTTPS. O comando a seguir deve mostrar uma resposta `HTTP 200 OK` do Amazon S3.

```
curl -i https://s3.amazonaws.com/ping
```

## Windows

- Obtenha as informações de endereço IP, roteamento e servidor DNS no prompt de comando. Verifique se um endereço IP está atribuído à interface de rede, se dois servidores DNS estão atribuídos e se uma rota padrão com um endereço de gateway padrão foi adicionada à tabela de rotas.

```
ipconfig /all
route print
```

- Colete a saída dos testes de conectividade básicos no prompt de comando. Substitua o `default_gateway_address` pelo endereço IP do gateway padrão atribuído.

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- Colete a saída do teste de conectividade HTTPS no PowerShell. O comando a seguir deve mostrar uma resposta `HTTP 200 OK`.

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

# Throughput na rede

O throughput de rede, que mede a taxa real de transferência de dados em uma rede, pode ser influenciado por vários fatores. Os seguintes fatores podem afetar suas velocidades de transferência de dados:

- Hardware: os componentes de hardware do dispositivo podem causar velocidades de conexão reduzidas durante o upload de dados. A CPU e os discos usados no dispositivo podem estar atingindo seus limites de performance. Considere usar SSDs NVMe em uma matriz RAID. Certifique-se de usar a biblioteca CRT AWS para melhorar o desempenho e reduzir o uso da CPU.
- Sobrecarga de criptografia: transmissões seguras, como HTTPS, aumentam o tempo de processamento devido à sobrecarga de criptografia.
- Latência: latência se refere ao tempo necessário para um pacote de dados viajar da origem ao destino. Uma latência mais alta pode ser observada durante o upload para um bucket do Amazon S3 em uma região geográfica diferente, o que pode levar a atrasos na transferência de dados e

reduzir o throughput. Sempre que possível, recomenda-se fazer transferências de dados dentro da mesma região.

- Perda de pacotes: pacotes perdidos exigem retransmissão, o que torna a transferência de dados mais lenta.

# Segurança do AWS Data Transfer Terminal

O AWS Data Transfer Terminal fornece um ambiente seguro para transferências com a Nuvem AWS. Como qualquer outra conexão de fibra de rede física, a conexão do Data Transfer Terminal não fornece criptografia padrão. Portanto, você é responsável por aplicar as melhores práticas de criptografia de dados para garantir que sua transferência de dados seja segura.

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de data centers e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Data Transfer Terminal, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Data Transfer Terminal. Os tópicos a seguir mostram como proteger seus dados durante a utilização do Data Transfer Terminal. Você também aprenderá como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Data Transfer Terminal.

Tópicos

- Segurança da infraestrutura no AWS Data Transfer Terminal

# Proteção de dados no AWS Data Transfer Terminal

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no AWS Data Transfer Terminal. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo que hospeda nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter informações sobre proteção de dados na Europa, consulte a postagem de blog Modelo de responsabilidade compartilhada da AWS e o RGPD no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da AWS e configure usuários individuais com o Centro de Identidade do AWS IAM ou o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log de atividades da API e dos usuários com o AWS CloudTrail. Para obter informações sobre como usar as trilhas do CloudTrail para capturar atividades da AWS, consulte Trabalhar com trilhas do CloudTrail no Guia do usuário do AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome.

Isso inclui quando você trabalha com o Data Transfer Terminal ou outros serviços da AWS usando o console, a API, a AWS CLI ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

## Criptografia de dados

O AWS Data Transfer Terminal fornece acesso a uma conexão de rede de alta velocidade para que você possa transferir dados com segurança entre sistemas de armazenamento autogerenciados e os serviços de armazenamento da AWS. A forma como seus dados de armazenamento são criptografados em trânsito depende, em parte, das políticas habilitadas em seus dispositivos e dos serviços para os quais seus dados são transferidos. O gerenciamento de dados e sua criptografia em trânsito são de responsabilidade do indivíduo que usa o Data Transfer Terminal.

### Criptografia em repouso

O AWS Data Transfer Terminal criptografa todos os dados em repouso.

O Data Transfer Terminal captura apenas os dados necessários para as reservas, incluindo os nomes, sobrenomes e endereços de e-mail das pessoas especificadas para comparecer e agendar a reserva. O objetivo dessa coleta de dados é confirmar os detalhes da reserva e garantir o acesso à sala para realizar a transferência de dados. Essas informações transacionais são armazenadas por no máximo 35 dias. No entanto, as informações da conta da AWS são retidas por 10 anos.

## Criptografia em trânsito

O AWS Data Transfer Terminal não criptografa dados em trânsito. Os dados são criptografados em trânsito quando você interage com os endpoints da API do Data Transfer Terminal para configurar equipes de transferência, adicionar pessoal e agendar reservas no console. Como parte do modelo de responsabilidade compartilhada da AWS, você tem opções sobre como se conectar aos serviços da AWS por meio do Data Transfer Terminal. Recomendamos enfaticamente que você escolha se conectar aos serviços da AWS usando criptografia em trânsito forte, como TLS 1.2 e 1.3.

Por exemplo, use apenas conexões criptografadas por HTTPS (TLS) usando a condição aws:SecureTransport nas políticas de bucket do Amazon S3, conforme ilustrado na política de bucket abaixo.

Para saber mais sobre criptografia de dados em trânsito com outros serviços da AWS, como o Amazon S3, consulte Proteção de dados com criptografia do lado do servidor no Guia do usuário do Amazon S3.

### Gerenciamento de chaves

O AWS Data Transfer Terminal não oferece suporte direto a chaves gerenciadas pelo cliente. Use o suporte a chaves gerenciadas pelo cliente disponível para os serviços da AWS aos quais você se conecta durante a reserva do Data Transfer Terminal. Saiba mais sobre chaves gerenciadas pelo cliente e como criptografar seus dados em repouso na seção Chaves do AWS KMS do Guia do desenvolvedor do AWS Key Management Service.

### Privacidade do tráfego entre redes

O acesso ao console do Data Transfer Terminal é feito por meio de APIs de serviço publicadas. Os recursos do Data Transfer Terminal são independentes da nuvem privada virtual (VPC).

## Gerenciamento de identidade e acesso para o Data Transfer Terminal

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda administradores a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para usar os recursos do Data Transfer Terminal. O IAM é um AWS serviço da que pode ser usado sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como o Data Transfer Terminal funciona com o IAM

### Público

A forma de usar o AWS Identity and Access Management (IAM) varia em função do trabalho realizado no Data Transfer Terminal.

Usuário do serviço: se você usa o serviço Data Transfer Terminal para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Data Transfer Terminal forem usados para realizar o trabalho, talvez sejam necessárias permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se não for possível acessar um recurso no Data Transfer Terminal, consulte Solução de problemas de identidade e acesso no AWS Data Transfer Terminal.

Administrador do serviço: se você for o responsável pelos recursos do Data Transfer Terminal em sua empresa, provavelmente terá acesso total ao Data Transfer Terminal. Cabe a você determinar quais funcionalidades e recursos do Data Transfer Terminal os usuários do seu serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Data Transfer Terminal, consulte Como o Data Transfer Terminal funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez deseje saber detalhes sobre como escrever políticas para gerenciar o acesso ao Data Transfer Terminal. Para ver exemplos de políticas baseadas em identidade do Data Transfer Terminal que você pode usar no IAM, consulte Exemplos de políticas baseadas em identidade do AWS Data Transfer Terminal.

## Autenticação com identidades

A autenticação é a forma como fazer login na AWS usando suas credenciais de identidade. É necessário estar autenticado (conectado à AWS) como usuário raiz da conta AWS, como usuário do IAM ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS Os usuários do Centro de Identidade do IAM, a autenticação de logon único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

Dependendo do seu tipo de usuário, você pode acessar o Console de Gerenciamento da AWS ou o portal de acesso da AWS. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login na sua conta AWS no  Guia do usuário de login AWS.

Se você acessar a AWS de forma programática, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar de forma criptográfica

as solicitações usando as suas credenciais. Se você não utilizar as ferramentas AWS, deverá designar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do Centro de Identidade do AWS e Autenticação multifator da AWS no IAM no Guia do usuário do IAM.

### Usuário raiz de conta da AWS

Ao criar uma conta AWS, você começa com uma identidade de login que tem acesso completo a todos os serviços e recursos da conta AWS. Essa identidade é denominada usuário-raiz da conta da AWS e é acessada pelo login com o endereço de e-mail e a senha usados para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

### Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar os serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da Web, AWS Directory Service, o diretório do Centro de Identidade ou qualquer usuário que acesse os serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam as contas da AWS, elas assumem perfis, e os perfis fornecem credenciais temporárias.

Para obter um gerenciamento centralizado de acesso, recomendamos o uso do Centro de Identidade do AWS IAM. É possível criar usuários e grupos diretamente no Centro de Identidade do IAM ou conectar e sincronizar um conjunto de usuários e de grupos usando sua própria fonte de identidades para utilizá-los em todas as suas contas e aplicações da AWS. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM?, no Guia do usuário do Centro de Identidade do AWS IAM.

## Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

## Perfis do IAM

Perfil do IAM é uma identidade dentro da sua conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente um perfil do IAM no Console de Gerenciamento da AWS, você pode alternar de um usuário para um perfil do IAM (console). É possível assumir um perfil chamando uma operação da AWS CLI ou da AWS API, ou usando um URL personalizado. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a

um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no  Guia do usuário do Centro de Identidade do AWS IAM.

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços: alguns serviços da AWS usam recursos em outros serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS): qualquer pessoa que utilizar um perfil ou usuário do IAM para executar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. A FAS usa as permissões do entidade principal que chama um serviço da AWS, combinadas com o serviço da AWS solicitante, para fazer solicitações a serviços downstream. As solicitações FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros serviços ou recursos do AWS para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um serviço da AWS no Guia do usuário do IAM.
  - Perfil vinculado a serviço: um perfil vinculado a um serviço é um tipo de função de serviço vinculada a um serviço da AWS. O serviço pode assumir o perfil de executar uma ação em seu nome. Os Perfis vinculados a serviços aparecem em sua conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer

solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

## Gerenciar o acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário-raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações do perfil no Console de Gerenciamento da AWS, na AWS CLI ou na API da AWS.

### Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e funções em sua conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

### Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os principais podem incluir contas, usuários, funções, usuários federados ou serviços da AWS.

Políticas baseadas em recursos são políticas embutidas que estão localizadas nesse serviço. Não é possível usar as políticas do IAM gerenciadas por AWS em uma política baseada em recursos.

### Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que suportam ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

### Outros tipos de política

A AWS oferece compatibilidade com tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade.

As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recursos que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) - SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS O Organizations é um serviço para agrupar e gerenciar de forma centralizada várias contas do AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. Uma SCP limita as permissões para entidades em contas-membro, incluindo cada usuário root da conta da AWS. Para obter mais informações sobre Organizações e SCPs, consulte Políticas de controle de serviços no  Guia do Usuário de Organizações AWS.
- Políticas de controle de recursos (RCPs): RCPs são políticas JSON que podem ser usadas para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. A RCP limita as permissões para recursos nas contas-membro e pode afetar as permissões efetivas para identidades, incluindo o usuário-raiz da conta da AWS, independentemente de pertencerem a sua organização. Para obter mais informações sobre o Organizations e as RCPs, incluindo uma lista de serviços da AWS compatíveis com RCPs, consulte Políticas de controle de recursos (RCP) no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e as políticas da sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

## Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir ou não uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Guia do usuário do IAM.

# Como o Data Transfer Terminal funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Data Transfer Terminal, entenda quais recursos do IAM estão disponíveis para uso com o Data Transfer Terminal.

| Recurso do IAM | Suporte ao Data Transfer Terminal |
|---|---|
| Políticas baseadas em identidade | Sim |
| Políticas baseadas em recurso | Não |
| Ações de políticas | Sim |
| Recursos de políticas | Sim |
| Chaves de condição de políticas | Sim |
| ACLs | Não |
| ABAC (tags em políticas) | Não |
| Credenciais temporárias | Sim |
| Permissões de entidade principal | Não |
| Perfis de serviço | Não |
| Funções vinculadas ao serviço | Não |

Para obter uma visão geral de como o Data Transfer Terminal e outros serviços da AWS funcionam com a maioria dos recursos do IAM, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

## Políticas baseadas em identidade para o Data Transfer Terminal

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que

condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o Data Transfer Terminal

Para ver exemplos de políticas baseadas em identidade do Data Transfer Terminal, consulte Exemplos de políticas baseadas em identidade do AWS Data Transfer Terminal.

## Políticas baseadas em recursos no Data Transfer Terminal

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os principais podem incluir contas, usuários, funções, usuários federados ou serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em contas AWS diferentes, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

## Ações de política para o Data Transfer Terminal

Compatível com ações de políticas: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como Ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do Data Transfer Terminal, consulte Ações definidas pelo AWS Data Transfer Terminal na Referência de autorização de serviços.

As ações de políticas no Data Transfer Terminal usam o seguinte prefixo antes da ação:

```
datatransferterminal
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "datatransferterminal:action1",
      "datatransferterminal:action2"
         ]
```

Para ver exemplos de políticas baseadas em identidade do Data Transfer Terminal, consulte Exemplos de políticas baseadas em identidade do AWS Data Transfer Terminal.

## Recursos de política para o Data Transfer Terminal

Compatível com recursos de políticas: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática

recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Data Transfer Terminal e seus ARNs, consulte Recursos definidos pelo AWS Data Transfer Terminal na Referência de autorização de serviços. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Data Transfer Terminal

Para ver exemplos de políticas baseadas em identidade do Data Transfer Terminal, consulte Exemplos de políticas baseadas em identidade do AWS Data Transfer Terminal.

## Chaves de condição de políticas para o Data Transfer Terminal

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou elemento `Condition`*`block`*`) lets you specify conditions in which a statement is in effect. The `Condition`) é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece compatibilidade com chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do Data Transfer Terminal, consulte Chaves de condição para o AWS Data Transfer Terminal na Referência de autorização de serviços. Para saber com quais ações e recursos você pode usar a chave de condição, consulte Ações definidas pelo AWS Data Transfer Terminal.

Para ver exemplos de políticas baseadas em identidade do Data Transfer Terminal, consulte Exemplos de políticas baseadas em identidade do AWS Data Transfer Terminal.

## ACLs no Data Transfer Terminal

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## ABAC com o Data Transfer Terminal

Oferece compatibilidade com ABAC (tags em políticas): não

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos recursos da AWS. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso com base em etiquetas, você fornece informações de etiqueta no elemento de condição de uma política usando o `aws:ResourceTag/[replaceable]`nome da chave `, , or aws:TagKeys condition keys.`. Se um serviço suportar todas as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM.

Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Data Transfer Terminal

Compatível com credenciais temporárias: sim

Alguns serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais serviços da AWS funcionam com credenciais temporárias, consulte serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login no Console de Gerenciamento da AWS por qualquer método, exceto nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

É possível criar credenciais temporárias de forma manual por meio da AWS CLI ou da API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidades principais entre serviços para o Data Transfer Terminal

Compatível com sessões de acesso direto (FAS): não

O usuário ou perfil do IAM usado para executar ações na AWS é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. A FAS usa as permissões do entidade principal que chama um serviço da AWS, combinadas com o serviço da AWS solicitante, para fazer solicitações a serviços downstream. As solicitações FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros serviços ou recursos do AWS para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Perfis de serviço para o Data Transfer Terminal

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais

informações, consulte Criar um perfil para delegar permissões a um serviço da AWS no Guia do usuário do IAM.

> **Warning**
>
> Alterar as permissões de um perfil de serviço pode prejudicar a funcionalidade do Data Transfer Terminal. Edite os perfis de serviço somente quando o Data Transfer Terminal fornecer orientação para isso.

Perfis vinculados a serviços para o Data Transfer Terminal

Compatível com perfis vinculados ao serviço: Não

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um serviço da AWS. O serviço pode assumir o perfil de executar uma ação em seu nome. Os Perfis vinculados a serviços aparecem em sua conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

## Exemplos de políticas baseadas em identidade para o AWS Data Transfer Terminal

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Data Transfer Terminal. Além disso, eles não podem executar tarefas ao usar o Console de Gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) ou a API da AWS. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo , incluindo o formato dos ARNs para cada tipo de recurso, consulte Ações, na Referência de autorização de serviço.

Tópicos

- Práticas recomendadas de política
- Usar o console do Data Transfer Terminal
- Permitir que os usuários visualizem suas próprias permissões

### Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Data Transfer Terminal em sua conta. Essas ações podem incorrer em custos para sua conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece a usar as políticas gerenciadas do AWS e avance para as permissões de privilégios mínimos - Para começar a conceder permissões aos seus usuários e workloads, use as políticas gerenciadas do AWS que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis em sua conta AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS que são específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço se elas forem usadas por meio de um serviço específico do AWS, como o AWS CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) - se você tiver um cenário que exija usuários do IAM ou um usuário raiz na sua conta AWS, ative a MFA para obter segurança adicional. Para exigir MFA

quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do Data Transfer Terminal

Para acessar o console do AWS Data Transfer Terminal, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Data Transfer Terminal em sua conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa conceder permissões mínimas do console para os usuários que estão fazendo ligações somente com a CLI da AWS ou a API da AWS. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que os usuários e perfis ainda possam usar o console do Data Transfer Terminal, anexe também o `ConsoleAccess` do Data Transfer Terminal a ou a política `ReadOnly` gerenciada pela AWS às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
```

```
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Solução de problemas de identidade e acesso do AWS Data Transfer Terminal

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que podem ocorrer ao trabalhar com o Data Transfer Terminal e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Data Transfer Terminal
- Quero permitir que pessoas não pertencentes à minha conta da AWS acessem meus recursos do Data Transfer Terminal

### Não tenho autorização para executar uma ação no Data Transfer Terminal

Se você não conseguir visualizar ou agendar reservas no console do AWS Data Transfer Terminal, talvez não tenha as permissões necessárias. Entre em contato com o administrador da sua conta para configurar uma política de identidade do IAM que conceda o acesso e as permissões apropriados.

Quero permitir que pessoas não pertencentes à minha conta da AWS acessem meus recursos do Data Transfer Terminal

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), é possível usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Data Transfer Terminal é compatível com esses recursos, consulte Como o Data Transfer Terminal funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra conta da AWS pertencente a você no Guia de Usuário do IAM.
- Para saber como conceder acesso aos recursos para contas da AWS de terceiros, consulte Fornecer acesso a contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

## Referências da API do Data Transfer Terminal: ações e recursos

Ao criar políticas do AWS Identity and Access Management (IAM), esta página pode ajudar você a entender a relação entre as operações da API do AWS Data Transfer Terminal, as ações correspondentes às quais você pode conceder permissões para executar e os recursos da AWS ao qual você pode conceder as permissões.

Em geral, veja como adicionar permissões do Data Transfer Terminal à sua política:

- Especifique uma ação no elemento `Action`. O valor inclui um prefixo `datatransferterminal:` e o nome da operação da API. Por exemplo, `datatransferterminal:CreateTask`.
- Especifique um recurso AWS relacionado à ação no elemento `Resource`.

Você também pode usar chaves de condição da AWS em suas políticas do Data Transfer Terminal. Para obter uma lista completa das chaves da AWS, consulte Chaves disponíveis no Guia do usuário do IAM.

Operações da API do Data Transfer Terminal e ações correspondentes

CreateTransferTeam

- Ação: `datatransferterminal:CreateTransferTeam`

  Recurso: None

GetTransferTeam

- Ação: `datatransferterminal:GetTransferTeam`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

UpdateTransferTeam

- Ação: `datatransferterminal:UpdateTransferTeam`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

DeleteTransferTeam

- Ação: `datatransferterminal:DeleteTransferTeam`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

ListTransferTeams

- Ação: `datatransferterminal:ListTransferTeams`

  Recurso: None

RegisterPerson

- Ação: `datatransferterminal:RegisterPerson`

Recurso: arn:aws::$[replaceable]Partição:datatransferterminal:
$[replaceable]Região:$[replaceable]Conta:transfer-team/
$[replaceable]TransferTeamId````

GetPerson

- Ação: datatransferterminal:GetPerson

  Recurso: arn:aws::$[replaceable]Partição:datatransferterminal:
  $[replaceable]Região:$[replaceable]Conta:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  Ação dependente: datatransferterminal:GetTransferTeam

  Recurso dependente: arn:aws::$[replaceable]Partição:datatransferterminal:
  $[replaceable]Região:$[replaceable]Conta:transfer-team/
  $[replaceable]TransferTeamId````

DeregisterPerson

- Ação: datatransferterminal:DeregisterPerson

  Recurso: arn:aws::$[replaceable]Partição:datatransferterminal:
  $[replaceable]Região:$[replaceable]Conta:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  Ação dependente: datatransferterminal:GetTransferTeam

  Recurso dependente: arn:aws::$[replaceable]Partição:datatransferterminal:
  $[replaceable]Região:$[replaceable]Conta:transfer-team/
  $[replaceable]TransferTeamId````

ListPersons

- Ação: datatransferterminal:ListPersons

  Recurso: arn:aws::$[replaceable]Partição:datatransferterminal:
  $[replaceable]Região:$[replaceable]Conta:transfer-team/
  $[replaceable]TransferTeamId````

CreateReservation

- Ação: datatransferterminal:CreateReservation

Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

Ação dependente: `datatransferterminal:GetTransferTeam`

Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

Ação dependente: `datatransferterminal:GetPerson`

Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

Ação dependente: `datatransferterminal:GetFacility`

Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:::facility/$[replaceable]FacilityId````

GetReservation

- Ação: `datatransferterminal:GetReservation`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  Ação dependente: `datatransferterminal:GetTransferTeam`

  Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

UpdateReservation

- Ação: `datatransferterminal:UpdateReservation`

Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

Ação dependente: `datatransferterminal:GetTransferTeam`

Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

Ação dependente: `datatransferterminal:GetPerson`

Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

DeleteReservation

- Ação: `datatransferterminal:DeleteReservation`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  Ação dependente: `datatransferterminal:GetTransferTeam`

  Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

ListReservations

- Ação: `datatransferterminal:ListReservations`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:$[replaceable]Região:$[replaceable]Conta:transfer-team/$[replaceable]TransferTeamId````

ListFacilities

- Ação: `datatransferterminal:ListFacilities`

  Recurso: None

GetFacility

- Ação: `datatransferterminal:GetFacility`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:::facility/$[replaceable]FacilityId````

GetFacilityAvailability

- Ação: `datatransferterminal:GetFacilityAvailability`

  Recurso: `arn:aws::$[replaceable]Partição:datatransferterminal:::facility/$[replaceable]FacilityId/availability`

  Ação dependente: `datatransferterminal:GetFacility`

  Recurso dependente: `arn:aws::$[replaceable]Partição:datatransferterminal:::facility/$[replaceable]FacilityId/availability`

# Validação de conformidade para o AWS Data Transfer Terminal

Para saber se um serviço AWS está dentro do escopo de programas de conformidade específicos, consulte AWS services in Scope by Compliance Program e escolha o programa de conformidade do seu interesse. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Fazer o download de Relatórios no AWS Artifact.

Sua responsabilidade com relação à conformidade ao usar os serviços da AWS é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos os serviços da AWS são qualificados para a HIPAA.
- Recursos de compatibilidade da AWS – Esta coleção de guias e pastas de trabalho pode ser aplicada ao seu setor e local.

- https://d1-awsstatic-com-whitepapers-compliance-AWS-Customer-Compliance-Guides-pdf [Guias de conformidade do cliente da AWS] – Compreenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteger os serviços do AWS e mapeiam as orientações para os controles de segurança em várias estruturas (incluindo National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI) e International Organization for Standardization (ISO)).
- Avaliação de recursos com regras no  AWS Config Developer Guide - O serviço AWS Config avalia a conformidade das configurações do seus recursos com as práticas internas, as diretrizes do setor e as normas.
- AWS Security Hub - Esse serviço AWS fornece uma visão abrangente do seu estado de segurança em AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty - Este serviço AWS detecta possíveis ameaças às suas contas AWS, workloads, contêineres e dados, monitorando seu ambiente em busca de atividades suspeitas e mal-intencionadas. O GuardDuty pode ajudar você a atender a diversos requisitos de conformidade, como o PCI DSS, com o cumprimento dos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: esse serviço da AWS ajuda a auditar continuamente o uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

# Resiliência no AWS Data Transfer Terminal

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, conectadas com baixa latência, throughput elevado e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

O AWS Data Transfer Terminal está disponível em vários locais ao redor do mundo. Você pode se conectar a qualquer Região da AWS que seja acessível pela internet.

# Registrar em log e monitorar no Data Transfer Terminal

O AWS Data Transfer Terminal é integrado com o AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço da AWS no Data Transfer Terminal. O CloudTrail captura as chamadas de API para o Data Transfer Terminal na forma de eventos. As chamadas capturadas incluem as chamadas do console do Data Transfer Terminal e chamadas de código para as operações da API do Data Transfer Terminal. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Data Transfer Terminal. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos. Com as informações coletadas pelo CloudTrail, determine a solicitação feita para o Data Transfer Terminal, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e os detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do Usuário doAWS CloudTrail.

## Informações do Data Transfer Terminal no CloudTrail

O CloudTrail é habilitado em sua conta AWS ao criá-la. Quando ocorre uma atividade no Data Transfer Terminal, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS no Histórico de eventos. É possível visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para manter um registro contínuo de eventos na sua conta da AWS, incluindo os eventos do Data Transfer Terminal, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando uma trilha é criada no console, a mesma é aplicada a todas as regiões da AWS. A trilha registra logs de eventos de todas as Regiões na AWS divisória e entrega os arquivos do log para o bucket Amazon S3 especificado. Além disso, é possível configurar outros AWS serviços para melhor analisar e agir de acordo com dados coletados do evento nos logs CloudTrail. Para saber mais, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configuração notificações do Amazon SNS para o CloudTrail

- Como receber arquivos de log do CloudTrail de várias regiões e Como receber arquivos de log do CloudTrail de várias contas

Todas as ações do Data Transfer Terminal são registradas pelo CloudTrail e são documentadas na seção Referências da API do Data Transfer Terminal: Ações e recursos deste guia.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais raiz ou com credenciais de usuário do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para saber mais, consulte Elemento userIdentity do CloudTrail.

## Entender as entradas do arquivo de log do Data Transfer Terminal

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros da solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenado das chamadas de API públicas, portanto, não aparecem em nenhuma ordem específica.

# Segurança da infraestrutura no AWS Data Transfer Terminal

Como serviço gerenciado, o AWS Data Transfer Terminal é protegido pelos procedimentos de segurança global de redes da AWS descritos no whitepaper {https---d0-awsstatic-com-whitepapers-Security-AWS-Security-Whitepaper-pdf}[Amazon Web Services: Visão geral dos processos de segurança].

Você usa chamadas de API publicadas da AWS para acessar o Data Transfer Terminal via rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve

Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o serviço de token de segurança da AWS (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

# Histórico do documento do Guia do usuário do Data Transfer Terminal

A tabela a seguir descreve o histórico de documentos deste guia.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Atualização do layout | Atualizações no layout do documento e pequenas edições de conteúdo e na forma da redação. | 1 de janeiro de 2025 |
| Publicação inicial | A data de lançamento da documentação original. | 1.º de dezembro de 2024 |